

# **Understanding and Designing for Trust in Bitcoin Blockchain**



**Irni Eliana Khairuddin**

**This dissertation is submitted for the degree of**

**Doctor of Philosophy**

**April 2019**

**School of Computing and Communications**

## Declaration

This thesis has not been submitted in support of an application for another degree at this or any other university. It is the result of my own work and includes nothing that is the outcome of work done in collaboration except where specifically indicated. Many of the ideas in this thesis were the product of discussion with my supervisor Professor Corina Sas. The work in this thesis has not been published anywhere else except in the following publications:

1. Corina Sas and Irni Eliana Khairuddin. 2015. Exploring Trust in Bitcoin Technology: A Framework for HCI Research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (OzCHI '15)*, Bernd Ploderer, Marcus Carter, Martin Gibbs, Wally Smith, and Frank Vetere (Eds.). ACM, New York, NY, USA, 338-342. DOI=<http://dx.doi.org/10.1145/2838739.2838821>

*\* Irni Khairuddin contributed to the design of the study, conducted the literature review, an initial design of the framework, and produced a first draft.*

*Corina Sas proposed the study, contributed to the design of the study, produced revision of the framework and of the manuscript.*

2. Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 2872-2878. DOI=<http://dx.doi.org/10.1145/2851581.2892500>

*\* Irni Khairuddin contributed to the design of the study, conducted the study, transcribed the interviews, analysed the data, and produced iterative drafts of the manuscript.*

*Corina Sas proposed the study, contributed to the design of the study, and critically revised the drafts*

3. Corina Sas and Irni Eliana Khairuddin. 2017. Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 6499-6510. DOI: <https://doi.org/10.1145/3025453.3025886>

*\* Irni Khairuddin contributed to the design of the study, conducted the study, transcribed the interviews, an initial data analysis, and produced a first draft of the manuscript.*

*Corina Sas proposed the study, contributed to the design of the study, produced revision of data analysis and of the manuscript.*

4. Irni Eliana Khairuddin and Corina Sas. 2019. Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). ACM, New York, NY, USA, DOI: <https://doi.org/10.1145/3290605.3300859>

*\* Irni Khairuddin contributed to the design of the study, conducted the study, transcribed the interviews, analysed the data, and produced iterative drafts of the manuscript.*

*Corina Sas proposed the study, contributed to the design of the study, and critically revised the drafts of the manuscripts.*

5. Irni Eliana Khairuddin, Corina Sas and Chris Speed. 2019. BlocKit: A Physical Kit for Materializing and Designing for Blockchain Infrastructure. In Proceeding of the 2019 Designing Interactive System Conference (DIS '19). ACM New York, NY, USA, DOI: <https://doi.org/10.1145/3322276.332237>

*\* Irni Khairuddin contributed to the design of the study, iterative design and built the physical kit, conducted the study, transcribed the interviews, an initial data analysis, and produced iterative drafts of the manuscript.*

*Corina Sas proposed the study, contributed to the design of the study and the physical kit, supported the refinement of data analysis, and critically revised the drafts of the manuscripts.*

All studies have received appropriate ethics approval, and the relevant ethics documentation can be found in Appendices A, B and C.

# **Understanding and Designing for Trust in Bitcoin Blockchain**

**Irni Eliana Khairuddin**

**This thesis is submitted for the degree of Doctor of Philosophy**

**School of Computing and Communications**

**April 2019**

## **Abstract**

Bitcoin is a cryptocurrency that has created a new revolution in peer-to-peer technology. Built upon decentralised technology known as Blockchain, it supports transparent, fast, cost-effective and irreversible transactions, without the need for trusting the third-party financial institution. The privacy of Bitcoin users is protected, by the pseudoanonymous transaction. At present, Bitcoin holds the largest market share in cryptocurrency and the Blockchain technology had captured the interest of multi-corporations, such as Microsoft, Dell, and T-Mobile. However, Bitcoins have no legal tender in most and it is even worse with the illicit use by the irresponsible people and the cyber-attacks towards the application. Hence, these are the primary motivation of this Ph.D. work, to explore the trust between people and Bitcoin technology as well as identify the opportunities to design for the trust challenges. This thesis investigates the challenges and design works with 80 Bitcoin stakeholders such as users, miners, Blockchain experts and novices in six different but interrelated studies. The first and second studies report in-depth preliminary studies with 20 Bitcoin users and 20 miners to identify the trust challenges in people's daily practices in using Bitcoin. Based on the findings, users' risk related to dishonest partner in peer-to-peer Bitcoins transactions is the highlighted trust challenges to be addressed in this thesis. With a strong understanding of Bitcoin mining process, a

physical Blockchain design kit, namely BlocKit was developed based on the embodied cognition theories and material centred design. This BlocKit was evaluated by 15 Bitcoin Blockchain's experienced users and one of the important outcomes proposed the principles to design for trust application in peer-to-peer Bitcoins transactions. Later the algorithms of trust for Bitcoin application were developed based on the suggested principles and were validated by 10 Bitcoin Blockchain's experienced users. Finally, based on the designed algorithms as well as a newly identified heuristic evaluation for trust, a mock-up prototype of Bitcoin wallet application namely, BitXFps was developed and the interface was evaluated for trust by 15 Bitcoin Blockchain's experienced users.

## Acknowledgements

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Alhamdulillah, all praise to the most Gracious and Merciful Almighty who makes this journey possible, without whom nothing is possible. First and foremost I would like to dedicate my sincere appreciation to my supervisor Prof. Corina Sas for her valuable advice and for his regular supervisions during my PhD study. Prof. Corina has shown lots of enthusiasms and encouragement towards my work, which motivated me to go even further. I feel lucky to have her as my supervisor as her support has been mostly invaluable for me.

I would also like to express my sincere gratitude to my officemate Dr Vatsalla, Dr Faiza, Dr Roberto, Dr Richards, Dr Abdussalam, Dr Izhar, Paul, Wyatt and Alex for their support and advice for work and personal. I am so lucky to have a supportive friendly and pleasant working environment.

My sincere thanks to my beloved husband, Rihan Mohamad for his unconditional love and supported me a lot through thick and thin during my study. Not to forget, our beloved daughter, Raina Izzqaireen Rihan, for being good and understanding daughter. Also, to my beloved parents Khairuddin Mohamad and Roselinah Ismail, I am thankful for their love, prayers and for believing in my ability to undertake a PhD degree. I am also thankful to my siblings for their love and support.

Finally, to my beloved best friend, Ayu and her little family, thank you so much for the love and support. Also to Pandora Chics Lancaster, Kak Ju, Kak Azliza, Anis and Liana, thank you for lending me your shoulder. Not to forget my beloved sisters in Malaysia, Mazlina, Rina and Maryam, thank you for everything. Last but not least, thank you to my sponsorship, Universiti Teknologi MARA and The Ministry of Education Malaysia for making my dream come true.

# List of Figures

Figure 1.1 Thesis Structure .....	27
Figure 2.1: Chapter 2 of Thesis Structure .....	28
Figure 2.2: Research Framework for Exploring Levels of Trust in Bitcoin Technology (left) and across Stakeholders Groups (right) (Sas and Khairuddin, 2015).....	52
Figure 2.3: Framework for the material-centred interaction design method (Wiberg & Mikael, 2014) .....	72
Figure 3.1: Chapter 3 of Thesis Structure .....	74
Figure 3.2: Research Strategies (De Villiers, 2005) .....	80
Figure 4.1: Chapter 4 of Thesis Structure .....	92
Figure 4.2: Merchant’s Sign for Accepting Bitcoin Payment.....	99
Figure 4.3: Framework of Trust in Bitcoin for Users .....	113
Figure 5.1: Chapter 5 of Thesis Structure .....	120
Figure 5.2: Miner’s Real-time Proof-of-Work .....	130
Figure 5.3: Pyramid of types of miners .....	133
Figure 5.4: Framework of Bitcoin Trust for Miners.....	145
Figure 6.1: Chapter 6 of Thesis Structure .....	151
Figure 6.2: BloKit Representation of a Blockchain’s Entities.....	157
Figure 7.1: Chapter 7 of Thesis Structure .....	160
Figure 7.2: Experienced Users Interacting with BloKit Objects.....	168
Figure 7.3: Revised BloKit Objects.....	195
Figure 7.4: Organised Presentation of BloKit's Objects .....	197
Figure 8.1: Chapter 8 of Thesis Structure .....	200
Figure 8.2: Algorithm design to create a valid contract for Bitcoin peer-to-peer transaction .....	203
Figure 8.3: Algorithm design to create a transparent peer-to-peer Bitcoin transaction with decentralised witness .....	204
Figure 9.1: Chapter 9 of Thesis Structure .....	212
Figure 9.2: A navigation diagram of the BitXFps mobile app prototype and its functionalities.....	219
Figure 9.3: Wallet Backup Phrase .....	220
Figure 9.4: Setting the Wallet Passcode .....	221
Figure 9.5: The BitXFps Main Screen .....	222
Figure 9.6: Setting Options for BitXFps mobile app.....	224
Figure 9.7: Bitcoin Trading Pages.....	226
Figure 9.8: Merchant Pages .....	227
Figure 9.9: The Function of My Wallet in Detail .....	229
Figure 9.10: Details of the Multisignature Wallet Function.....	231
Figure 9.11: Details of the Witness Function.....	233
Figure 9.12: The Elements of Trust in the BitXFps Graphic Design.....	235
Figure 9.13: The Elements of Trust in the BitXFps Structure Design .....	236
Figure 9.14: The Elements of Trust in the BitXFps Content Design .....	238
Figure 9.15: The Elements of Trust in the BitXFps Social Cue Design.....	239
Figure 9.16: The Elements of Trust in the BitXFps Social Proof Design .....	240
Figure 9.17: The Elements of Trust in the BitXFps Peer-to-peer Transaction Design Cues .....	241
Figure 10.1: Chapter 10 of Thesis Structure .....	243

Figure 10.2: Icons on the homepage and the bottom menu of the BitXFps interface .....	249
Figure 10.3: Invite friends page .....	250
Figure 10.4: Link to Social Media in BitXFps .....	253
Figure 10.5: Support Service Email .....	254
Figure 10.6: Design for the BitXFps User Reputation Score.....	256
Figure 10.7: The Witness Interface Design Settings .....	269
Figure 10.8: Design for the Timer .....	269
Figure 10.9: The Revised Design of the App Logo.....	270
Figure 10.10: GitHub Icon to Link the Users to the App Source Code .....	270
Figure 10.11: The Icons for Sellers and Buyers are differentiated with Colours .....	271
Figure 10.12: Interface for the In-app Community Support Channel.....	272
Figure 10.13: The Official BitXFps Website URL.....	272
Figure 10.14: The Interface for the Group Video Call.....	273
Figure 11.1: Chapter 11 of Thesis Structure .....	274
Figure 11.2: Knowledge contributions across the studies in the thesis .....	276
Figure 11.3: Research Framework for Exploring Levels of Trust in Bitcoin Technology (left) and across Stakeholders Group (right) (Sas and Khairuddin, 2015) .....	278
Figure 11.4: Empirical Framework to Design in Blockchain for User's Trust in Peer-to-Peer Bitcoin Transactions .....	287
Figure 12.1: Chapter 12 of Thesis Structure .....	294

# List of Tables

Table 1.1 : The Structure of the Research .....	21
Table 2.1: Trust-Inducing Features of Website Interface Design .....	32
Table 2.2: Properties of Money (Bank of Canada, 2016; Jevons, 1890; Sykes, 1905) .....	46
Table 3.1: The basic differences between positivism and interpretivism (Pizam, Chon, & Mansfeld, 1999) .....	77
Table 3.2: Overview of studies conducted in the thesis .....	87
Table 5.1: Mining Approaches .....	128
Table 6.1: Properties of Blockchain's Key Entities .....	154
Table 6.2: Image Schemata of Blockchain Entities .....	156
Table 9.1: The Proposed Checklist in Designing and Evaluating the Trust in the Bitcoin Mobile Application Interface.....	217
Table 9.2: The Use of Colours in the BitXFps Design .....	235
Table 10.1: Trust-inducing features for the Bitcoin Peer-to-peer Transaction Mobile Application Interface Design .....	267

# CONTENTS

<b>1 Introduction</b>	<b>16</b>
1.1 Problem Definition	16
1.2 Research Aims	19
1.3 Research Objectives	19
1.4 Research Questions	20
1.5 The Thesis's Main Contributions	22
1.5.1 Theoretical Contributions	22
1.5.2 Methodological Contributions	23
1.5.3 Technological Design Contributions	23
1.6 Thesis Structure	24
<b>2 Literature Review</b>	<b>28</b>
2.1 Trust in HCI	29
2.1.1 Trust between People and Technology	29
2.1.2 Trust between People Interacting with Technology	33
2.1.3 Section Summary	39
2.2 History of Money	39
2.2.1 Alternative Currency	40
2.2.2 Digital Currency	42
2.2.3 Properties of Money	45
2.2.4 Alternative Currencies in HCI Study	46
2.2.5 Section Summary	47
2.3 Bitcoin Cryptocurrency	47
2.3.1 Bitcoin Stakeholders	48
2.3.2 Bitcoin Trust Research Framework	50
2.3.3 Section Summary	54
2.4 Blockchain Technology	55
2.4.1 Bitcoin Blockchain Protocol	56
2.4.2 Security Research on Mining-related Threats	59
2.4.3 The Comparison between Bitcoin and Ethereum Blockchain Ledger	59
2.4.4 Section Summary	63
2.5 Mental Model in HCI	63
2.5.1 Physical Interaction	65
2.5.2 Embodiment in HCI	69

2.5.3 DIY Kit Representation of Mental Model.....	70
<b>3 Methodology.....</b>	<b>74</b>
3.1 Introduction .....	75
3.2 Research Paradigm in HCI .....	75
3.2.1 Positivism versus Interpretivism .....	76
3.3 Research Method.....	78
3.3.1 Quantitative versus Qualitative .....	78
3.3.2 Mixed Methodology.....	80
3.4 User-centred Design and User Participatory Design.....	81
3.5 Usability Inspection Methods .....	83
3.6 Methodological Approach in this Thesis.....	85
3.6.1 Interview .....	85
3.6.2 User Participatory Design.....	86
3.6.3 Trust Evaluation .....	88
3.6.4 Qualitative Data Analysis Techniques.....	89
3.6.5 Triangulation.....	90
3.7 Chapter Summary .....	91
<b>4 The Trust Challenges and Opportunities among Bitcoin Users .....</b>	<b>92</b>
4.1 Introduction .....	93
4.2 Research Method.....	94
4.3 Findings .....	96
4.3.1 The Motivations for Using Bitcoin Currency .....	96
4.3.2 Blockchain’s Characteristics and their Impact on Trust.....	100
4.3.3 Insecure Transactions .....	104
4.3.4 Strategies for Mitigating the Risks of Dishonest Traders.....	107
4.4 Theoretical Implication .....	112
4.4.1 Towards a Framework of Trust among Bitcoin Users .....	112
4.5 Design Implications .....	116
4.5.1 Supporting Transparency of Two-way Transactions.....	116
4.5.2 Tools for Materialising Trust in Blockchain.....	117
4.5.3 Tools to Support Reversible Transactions.....	118
4.6 Chapter Summary .....	119
<b>5 The Trust Challenges and Opportunities among Bitcoin Miners .....</b>	<b>120</b>
5.1 Introduction .....	121

5.2 Research Method.....	122
5.3 Findings .....	124
5.3.1 Motivations of Bitcoin Miners .....	124
5.3.2 Blockchain’s Characteristics Impacting on Miners’ Trust .....	125
5.3.3 Social Organisation of Mining Practice: Competitiveness .....	127
5.3.4 Types of Miners.....	133
5.3.5 Trust Challenges of Collaborative Mining.....	135
5.3.6 Dishonest Mining Pool and Data Centre Administrators.....	139
5.3.7 Mitigating Trust Risks of Collaborative Mining .....	141
5.4 Theoretical Implication .....	143
5.4.1 Towards a Framework of Trust among Bitcoin Miners.....	144
5.5 Design Implication.....	147
5.5.1 Tools for Monitoring Hash Power & Reward Distribution .....	147
5.5.2 Decentralised Tools Tracking Data Centers’ Authorisation and Reputation .....	148
5.5.3 Tools for Developing Decentralised Pools .....	149
5.6 Chapter Summary .....	150
<b>6 Construction of BlockKit .....</b>	<b>151</b>
6.1 Introduction .....	152
6.2 Designing BlockKit.....	153
6.2.1 Identifying the Properties of Blockchain’s Key Entities .....	153
6.2.2 Image Schemata for Blockchain’s Key Entities.....	155
6.2.3 BlockKit’s Objects.....	156
6.3 Chapter Summary .....	159
<b>7 Evaluation of BlockKit.....</b>	<b>160</b>
7.1 Introduction .....	161
7.2 Research Method.....	162
7.2.1 Finding 1: Understanding BlockKit.....	163
7.2.2 Findings 2: Designing for Trust with BlockKit .....	175
7.2.3 Theoretical Implication .....	187
7.2.4 Design Implication.....	191
7.2.5 Summary for Study 3.....	194
7.3 The Revision of BlockKit.....	194
7.3.1 Minor Revisions of the Objects.....	194
7.3.2 Major Revisions of the Objects .....	196

7.3.3 Replacing the Static Objects with Smart Objects.....	197
7.3.4 Structuring the Arrangements of the Object .....	198
7.3.5 The New Object for the Newly Identified Blockchain’s Main Entity.....	198
7.4 Chapter Summary .....	199
<b>8 Design and Validation on Algorithms for Trust in Peer-to-peer Bitcoin Transactions on Blockchain.....</b>	<b>200</b>
8.1 Introduction .....	201
8.2 The design of algorithms for trust in peer-to-peer Bitcoin transactions.....	202
8.2.1 The design of valid contract in Ethereum smart contract supported with BTC Relay tool.....	202
8.2.2 The design of Bitcoin transparent transactions between buyer, seller and decentralised mediator with multisignature wallet contract.....	203
8.2.3 The design of reputation token in Blockchain ledger .....	204
8.3 The Main Stages of Algorithms for Trust in Bitcoin Transaction .....	205
8.4 Validations for the Design of the Trust Algorithms for Bitcoin Transaction.....	207
8.4.1 Validation Method .....	207
8.4.2 Validation Findings.....	207
8.4.3 Revisions of the Design for Trust Algorithms for Bitcoin Transaction .....	210
8.5 Chapter Summary .....	211
<b>9 Design for Trust in BitXFps Mobile Wallet Application and Its Interface .....</b>	<b>212</b>
9.1 Introduction .....	213
9.2 Proposed Trust-Inducing Features for the Bitcoin Application Design Interface .....	213
9.3 Navigation overview of the BitXFps.....	218
9.3.1 Design Overview of BitXFps .....	220
9.3.2 Reflections from the BitXFps User Interface Design according to the Proposed Guideline of Trust-Inducing Features for Bitcoin mobile applications.....	234
9.4 Chapter Summary .....	242
<b>10 Evaluation of BitXFps Mobile Wallet Application and How Its Interface Supports Trust .....</b>	<b>243</b>
10.1 Introduction .....	244
10.2 Research Method.....	245
10.3 Findings.....	247
10.3.1 The Elements of Trust Embedded in the BitXFps Interface Design .....	247
10.3.2 New Trust Elements for Peer-to-peer Transaction Design Cues .....	257
10.3.3 Risks Related to Trust.....	257
10.3.4 Suggestions to Mitigate the Risk.....	259

10.4 Theoretical Implications.....	261
10.4.1 Towards a Framework with Trust-inducing Features for Peer-to-peer Bitcoin Transactions .....	262
10.5 Design Implications .....	267
10.5.1 Blockchain Real-Time Communication Tool .....	267
10.5.2 Revision of the BitXFps Mobile App Design .....	268
10.6 Chapter Summary .....	273
<b>11 Discussion.....</b>	<b>274</b>
11.1 Introduction .....	275
11.2 Problem Identifications.....	277
11.2.1 The Design of the Theoretical Framework for the Exploration of People’s Trust in Bitcoin Technology.....	277
11.2.2 The Identified People’s Trust Challenges in Bitcoin Technology .....	278
11.3 Methods for Exploring Opportunities to Mitigate Trust challenges.....	280
11.3.1 Materialising the Blockchain Infrastructure .....	280
11.3.2 Principles to Design for User’s Trust in Bitcoin Transactions.....	281
11.4 Design of Proposed Solutions .....	282
11.4.1 The Design Algorithms with the Principles to Design for User’s Trust in Bitcoin Transactions.....	282
11.4.2 The Design of User Interface for Mobile Bitcoin Application with the Elements for User’s Trust in Bitcoin Transactions.....	284
11.5 Evaluation of BitXFps’s User Interface Design .....	284
11.5.1 The Evaluated Design of User Interface for Mobile Bitcoin Application with the Elements for User’s Trust in Bitcoin Transactions .....	284
11.6 Reflection on the Thesis Findings .....	286
11.7 Reflection on Thesis’ Research Questions .....	288
11.8 Chapter Summary .....	293
<b>12 Conclusion .....</b>	<b>294</b>
12.1 Introduction .....	295
12.2 Work Limitation .....	295
12.2.1 Time Constraints in Enacting Peer-to Peer Bitcoin-Transactions .....	295
12.2.2 Limited integration of BitXFps on Bitcoin Blockchain .....	295
12.3 Future Work .....	296
12.3.1 Exploring Motivations and Trust among Bitcoins Merchants and Exchanges .....	296
12.3.2 Design in Blockchain with BlockKit .....	296

12.3.3 Implementation of BitXFps Bitcoin Mobile Wallet .....	297
12.4 Thesis Conclusion.....	297
<b>References .....</b>	<b>299</b>
<b>Appendix A.....</b>	<b>320</b>
<b>Appendix B.....</b>	<b>327</b>
<b>Appendix C.....</b>	<b>331</b>
<b>Appendix D .....</b>	<b>335</b>
a. Step 1: Pre Transaction between Buyer and Seller.....	335
b. Step 2: Create a Valid Contract for the Transaction .....	339
c. Step 3: Enacting the Bitcoin Transactions.....	342
d. Step 4: Enacting Offline Transaction.....	345
e. Step 5: Sending Reputation Tokens .....	348

# Chapter 1

## Introduction

### 1.1 Problem Definition

*“Bitcoin is a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution” (Nakamoto, 2008, p. 1)*

Bitcoins were issued in 2009 by an anonymous entity called Satoshi Nakamoto, and have become the leader in peer-to-peer currency. Bitcoins have been adopted by the public at large with increased interest. Experts have foreseen that Bitcoin’s users will reach almost 200 million by 2024 (Young, 2017). This growing community buy Bitcoins in online marketplaces and get them sent to their digital Bitcoin’s wallet in exchange for fiat money, or use them to buy goods or services (Göbel, Keeler, Krzesinski, & Taylor, 2015). However, these transactions are somehow different from the traditional transactions involving fiat money. This is due to the concept of money; Bitcoins are not printed, but mined, through the widely distributed computing power supported on the Blockchain.

*“Blockchain is the public ledger of all executed Bitcoins” (Swan, 2015, p. x)*

Blockchain is a complex decentralised technology that consists of public distributed nodes involved in authorising Bitcoin transactions between anonymous parties (Nakamoto, 2008). These nodes are represented by miners, who are people that create Bitcoins in a controlled way, by running dedicated programs on their machines that are

connected within the Blockchain's network. By sharing Blockchain's characteristics, mining is a decentralised, transparent, and unregulated, yet lucrative practice, as miners are rewarded in Bitcoins for their successfully validated Bitcoin transactions. The core of Blockchain's ecosystem is miners, and their validation of Bitcoin transactions through the trustless mechanism. Other than Bitcoin, Blockchain has been widely explored by experts as a platform of other cryptocurrencies including Ethereum. Unlike Bitcoin's Blockchain that is designed specifically to record Bitcoin transactions, Ethereum Blockchain is able to record multiple types of arbitrary data (Karamitsos, Papadaki, Baker, & Barghuthi, 2018). This enables developers to build various types of systems on top of the Blockchain platform. Furthermore, its built-in smart contracts allow users to exchange money, properties or other valuable things in a transparent way (Ekblaw, Azaria, Halamka, Lippman, & Vieira, 2016; Singh & Singh, 2016). These exchange processes are validated by the miners and recorded in the Ethereum Blockchain.

*“Bitcoin is an electronic payment system that is based on cryptographic proof, allowing any two willing parties to transact directly with each other without the need for a trusted third party” (Nakamoto, 2008, p. 1)*

Bitcoin transactions are verified with sophisticated algorithms, and stored on miners' computers geographically distributed throughout the world (Nakamoto, 2008). Satoshi created the algorithms by allowing the transfer of Bitcoins' ownership from one user to another directly through the transaction being validated by the miners and permanently recorded in the Blockchain ledger (Swan, 2015). Hence, the dismissal of trusted third party for Bitcoins transactions such as in conventional banking systems has led to such transactions to be called trustless transactions.

Such an innovative form of financial transactions appears particularly appealing to Bitcoin users. However, Bitcoins are categorised as one of the alternative currencies, identified as a medium of exchange that emerged as substitute to national fiat currencies (Guadamuz & Marsden, 2015). Most alternative currencies were developed due to economic concerns, as well as to support local communities' needs, without being regulated by governments. The unregulated nature of alternative currencies such as Bitcoins poses challenges to their users who could no longer feel secured and protected by their central or governmental authority. The absence of central authority in Bitcoin technology is likely to lead to distrust. People's distrust towards Bitcoin Blockchain may be intensified by the characteristics of decentralisation and pseudo-anonymity. These can pose crucial challenges to Bitcoin users, such as those affected by illicit use and cyber-attacks (Costanza, 2003a; Wray, 2012). Additionally, the Bitcoin architecture differs significantly from prior electronic payment systems, which in turn could also lead to a lack of trust. This contrasts with most HCI trust models, many of which have been informed by empirical work on e-commerce or e-payment systems and are traditionally centralised, regulated, and non-anonymous. Hence, the feasibility of these models for theorising about users' trust in Bitcoin Blockchain requires exploration.

On the one hand, the emerging social organisation of mining practices brings forward issues of trust among miners such as the risk of 51% attack (Bradbury, 2013) and that of selfish miners (Buterin, 2013b), as explored mostly within the security research area. These security threats of mining contrast to the claim of trustless mining protocol (Nakamoto, 2008). Thus, they offer interesting opportunities for exploring miners' attitude towards such threats. However, in the HCI field, there has been limited exploration of miners' practices from the first-person perspective, and how the specific

Blockchain's characteristics impact on miners' trust. Thus, it is worth exploring the involvement of miners and their trust in this complex technology.

In order to explore miners' and users' practices and their trust in Bitcoin Blockchain, it is important to also explore their understanding of its underlying technology. However, the disruptive Blockchain technology has significantly challenged the traditional understanding of financial institutions. The Blockchain's inner working is not trivial to understand. In other words, a structural mental model of Blockchain technology is complex and arguably difficult to acquire, as it challenges the traditional understanding of similar financial or payment systems, which are traditionally centralised and regulated. Hence, new methods to support the process of understanding the Blockchain are much needed.

## 1.2 Research Aims

The thesis's overall aim is:

Understanding and designing for trust in Bitcoin Blockchain and this aim is broken down in the following main research objectives.

## 1.3 Research Objectives

- 1) To explore the challenges related to users' and miners' trust through empirically grounded understandings of their routine practices within Blockchain technology.
- 2) To explore new methods to understand the complex Bitcoin Blockchain technology.
- 3) To explore the design opportunities for Blockchain to mitigate the identified trust challenges.
- 4) To explore the design for people's trust in Bitcoin Blockchain.

- 5) To explore people's perceptions of trust in Bitcoin Blockchain by evaluating BitXFps, a novel mobile application's interface.

These objectives are intended to address the following main research questions.

#### 1.4 Research Questions

- 1) Why do people such as users and miners engage in Bitcoin transactions on Blockchain technology? What are the challenges they faced, and the specific trust issues?
- 2) What are the elements of BloKit – an innovative kit for materialising Blockchain - that could support people's understanding of Blockchain? What are the values of this approach for people to engage with Blockchain?
- 3) What are the principles to design for trust in peer-to-peer Bitcoins transaction? How should the design of Blockchain be supported?
- 4) What are the approaches to design new tools, such as wallet mobile apps, for users' trust? How to evaluate the design of such tools?
- 5) Which are the elements in the design of BitXFps support people's trust in Bitcoin transactions?

**Table 1.1** below offers an overview of the research aim, objectives and research questions, and their interrelationships.

Research Aims				
Research Objective 1	Research Objective 2	Research Objective 3	Research Objective 4	Research Objective 5
Research Question 1	Research Question 2	Research Question 3	Research Question 4	Research Question 5
Sub-Research Question 1	Sub-Research Question 2	Sub-Research Question 3	Sub-Research Question 4	Sub-Research Question 5
<p><i>Study 1, Chapter 4</i></p> <p>Which are the motives for early adoption and use of Bitcoins?</p> <p>How do people learn about Bitcoins and how do they use Bitcoins?</p> <p>How different Blockchain's characteristics impact on the various dimensions of trust?</p> <p>Which are the main trust challenges and how do people attempt to mitigate them?</p> <p><i>Study 2, Chapter 5</i></p> <p>Which are miners' motivations for Bitcoin mining?</p> <p>Which are Bitcoin Blockchain's characteristics impacting on miners' trust and its dimensions?</p> <p>Which is the social organisation of mining practices: are there different approaches and types of miners?</p> <p>Which are the main trust challenges and how do miners attempt to mitigate them?</p>	<p><i>Chapter 6</i></p> <p>What theories of design can enforce the BlocKit?</p> <p><i>Study 3, Chapter 7</i></p> <p>How complex infrastructures such as Blockchain technology can be thought about and communicated through a physical kit, such as Blockchain?</p> <p>How does the development and engagement with BlocKit support understanding of Blockchain's entities and their qualities?</p>	<p><i>Study 3, Chapter 7</i></p> <p>How does trust among Bitcoin users can be materialised and designed for through physical kit?</p> <p>What are the principles to design for user's trust in Bitcoin transaction?</p> <p>What are the requirements to build the design for user's trust?</p> <p><i>Study 4, Chapter 8</i></p> <p>How does the design can help to mitigate the users' trust problem?</p> <p>Which are significant elements in the design could mitigate user's trust problem?</p>	<p><i>Chapter 9</i></p> <p>What are the approaches to design the user interface for the mobile Bitcoin wallet app?</p> <p>How to evaluate the user's trust on the user interface of the Bitcoin wallet app?</p>	<p><i>Study 5, Chapter 10</i></p> <p>Which elements in the user interface design of the BitXFps wallet app support in peer-to-peer Bitcoin transaction?</p> <p>How does the design of user interface of the BitXFps wallet app could mitigate the trust challenges in peer-to-peer Bitcoin transaction?</p>

**Table 1.1 : The Structure of the Research**

## 1.5 The Thesis's Main Contributions

There are three types of contributions derived from this thesis, which are further described as theoretical, methodological and technological design contributions.

### 1.5.1 Theoretical Contributions

The theoretical contributions of this thesis are as follows:

#### **A research framework for exploring trust in Bitcoin Blockchain technology**

This is a novel research framework that is built on existing theories of trust, and the roles of the four Bitcoin Blockchain's main stakeholders: users, miners, merchants, and exchanges (*Sas and Khairuddin, 2015*). This framework has been further used as a supporting conceptual tool in the empirical studies exploring users' trust (*Sas and Khairuddin, 2017*) and miners' trust (*Khairuddin and Sas, 2019*).

#### **A framework of trust inducing features for Bitcoin mobile application**

This framework is built on two prevalent frameworks for websites and mobile apps which describe the characteristics of user interface design that induce trust. Initially, there were four characteristics offered by this framework, which consists of graphic design, structure design, content design, and social-cue design (Wang & Emurian, 2005). Later, underpinned by a study on e-commerce and banking websites (Seckler, Heinz, S., Tuch, & Opwis, 2015) the framework was extended with a new characteristic: personal and social proof design. In this thesis, this latter framework has been extended with a new characteristic, underpinned by the expert's evaluation of 20 Bitcoin mobile apps, as well as by an empirical evaluation with 15 Bitcoin users of our newly designed Bitcoin wallet app, BitXFps. Thus, from five characteristics, the framework of trust inducing features was extended to six with a

new characteristic, namely Bitcoin peer-to-peer transaction cues, which is particularly tailored for Bitcoin mobile applications.

### 1.5.2 Methodological Contributions

The methodological contributions of this thesis are as follows:

#### **BlocKit – Physical kit materialising the Blockchain infrastructure**

BlocKit materialises 12 main Blockchain's entities or key concepts through materials such as clays, plastic containers, or sticky-notes. The construction of BlocKit has been informed by embodied cognition theories (Hampe & Grady, 2005) and material centred-design (Wiberg & Mikael, 2014). BlocKit was evaluated by 15 Blockchain experienced users, and the findings indicate that this physical kit offers a novel approach to communicate about and design for Blockchain. BlocKit also benefits on learning and understanding the Blockchain. (*Khairuddin, Sas and Speed, 2019*).

### 1.5.3 Technological Design Contributions

The technological design contributions of this thesis are as follows:

#### **An Empirical Framework to Design Bitcoin Wallet app on Blockchain for Users' Trust in Peer-to-Peer Bitcoin Transactions**

This framework is built based on the outcomes of the five empirical studies conducted throughout this Ph.D thesis. It is constructed on the theoretical framework for exploring trust described in Chapter 2 which consists of technological trust, social trust, and institutional trust (*Sas and Khairuddin 2015*). Then, this empirical framework was used to explore the main trust challenges experienced by users while engaging in peer-to-peer Bitcoin transactions (*Khairuddin et al., 2016; Sas and Khairuddin, 2017*), which were classified under

social trust. Technological trust is supported by three principles to design for trust; the Blockchain Bitcoin mobile app to support the design for trust, and the design for trust of Bitcoin wallet app could be further explored using BlocKit (*Khairuddin, Sas and Speed, 2019*).

## 1.6 Thesis Structure

The remainder of this thesis is structured as follows:

### **Chapter 2: Literature Review**

This chapter presents the relevant literature, drawing from five research areas: trust in HCI, history of money, Bitcoin cryptocurrency, Blockchain technology, and mental models in HCI. One theoretical paper has been published based on the insights gained from this chapter (*Sas and Khairuddin, 2015*).

### **Chapter 3: Methodology**

This chapter highlights the relevant methodology applied in this thesis. Key research methods include interviews, user participatory design workshops, and heuristic evaluation method.

### **Chapter 4: The Trust Challenges and Opportunities among Bitcoin's Users**

This chapter presents the findings on the motivations and challenges related to trust among Bitcoin users. It also discusses relevant theoretical and design implications. Two papers have been published on the findings described in this chapter (*Khairuddin et al., 2016; Sas and Khairuddin, 2017*).

### **Chapter 5: The Trust Challenges and Opportunities among Bitcoin's Miners**

This chapter presents the findings on the motivations and challenges related to trust among Bitcoin miners. It also discusses relevant theoretical and design implications for the Bitcoin miners. One paper has been published on the findings described in this chapter (*Khairuddin and Sas, 2019*).

### **Chapter 6: Construction of BlocKit**

This chapter explores the materialisation of Blockchain infrastructure in the form of BlocKit. One paper has been published on the findings described in this chapter (*Khairuddin, Sas, and Speed, 2019*).

### **Chapter 7: Evaluation of BlocKit**

This chapter presents the findings on the evaluation of BlocKit with Blockchain experienced users. This chapter also describes the experts' suggestions for designing for trust in peer-to-peer Bitcoins transactions. One paper has been published on the findings described in this chapter (*Khairuddin, Sas and Speed, 2019*).

### **Chapter 8: Design and Validation on Algorithms for Trust Peer-to-Peer Bitcoin Transactions on Blockchain**

This chapter describes the design of algorithms for embedding trust in peer-to-peer Bitcoins transactions. It also discusses the findings from the validation of these algorithms with Bitcoin Blockchain users.

## **Chapter 9: Design for Trust User Interface of BitXFps Mobile Wallet Application**

This chapter describes the guidelines that were applied to design the interface for BitXFps apps. It also presents the design of BitXFps, a Bitcoin wallet mobile application, along with particular elements of trust implemented in its interface.

## **Chapter 10: Evaluation of Trust User Interface of BitXFps Mobile Wallet Application**

This chapter presents the evaluations of the trust elements of BitXFps's interface.

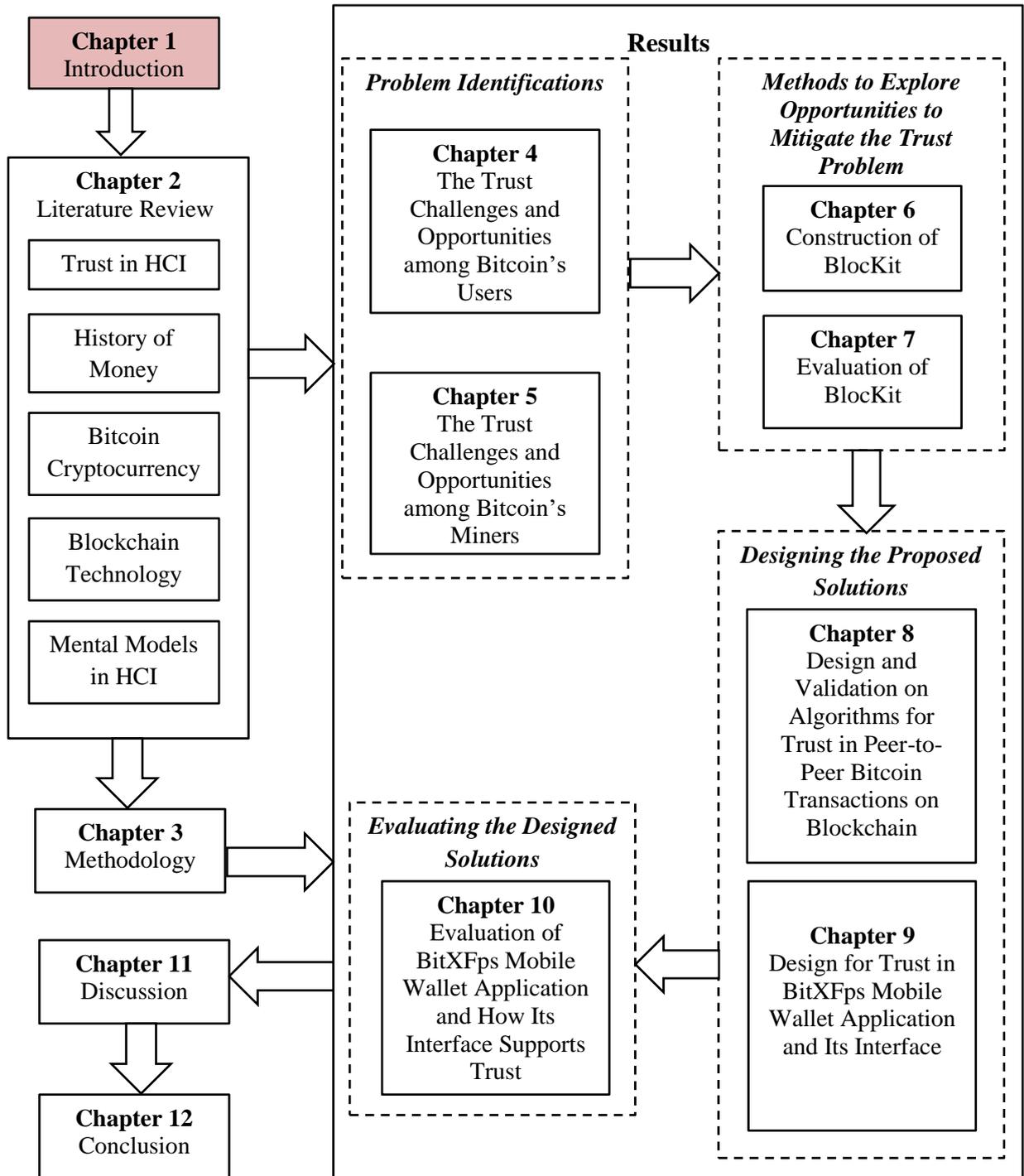
## **Chapter 11: Discussion**

This chapter discusses the overall findings of the thesis, revisits the research questions, and unpacks the main contributions of the thesis.

## **Chapter 12: Conclusion**

Finally, the conclusion chapter summarises the entire journey of the thesis. It also discusses limitations and proposes directions for future work.

**Figure 1.1** is a diagram of the overall thesis structure to show the links of each chapter in the thesis.



**Figure 1.1 Thesis Structure**

# Chapter 2

## Literature Review

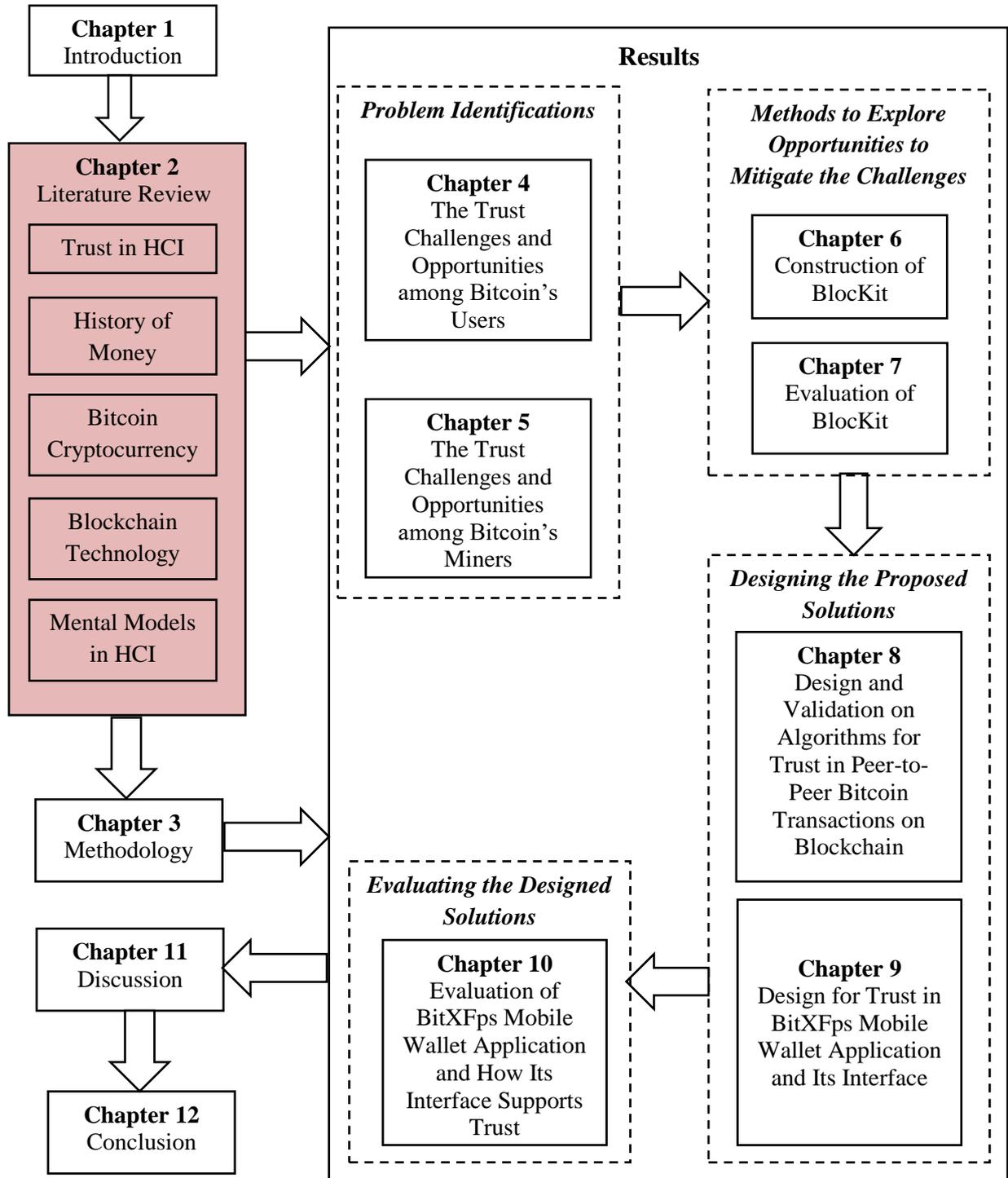


Figure 2.1: Chapter 2 of Thesis Structure

## 2.1 Trust in HCI

Trust is defined as the willingness to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party (Mayer, Davis, & Schoorman, 1995). Trust has also been described as a subjective belief in the character, ability, strength, reliability, honesty or truth of someone or something (Grandison et al., 2001). The multifaceted concept of trust has been explored across a large range of interactive systems, and consistent findings have shown the distinction between technological, social, and institutional trust (Leppanen, 2010; Lippert & Swiercz, 2005; Misiolek, Zakaria, & Zhang, 2002). In the Human-Computer Interaction (HCI) context, there are two main directions of conceptualising trust: trust between people and technology, and trust between people interacting with technology.

### 2.1.1 Trust between People and Technology

The technological trust consists of individual perceptions and assessments of technology-related trust issues (Leppanen, 2010). It can be better understood in the light of its three attributes: advantage to use, expectation of technology usability, and perception of user's skills. The advantage to use refers to the needs for implementing a technological system that will increase task performance (Goodhue, Lewis, & Thompson, 2006). The expectation of technology usability has been defined by Davis (Davis, 1989) in terms of user's initial presumption on what using the technology will be like. Usability can also be seen as a set of objectives and guidelines for system designers and software developers to create devices and applications that take minimal effort to use. For example, Nielsen (Nielsen, 2000) proposed guidelines for enhancing individual trust in website by assessing usability,

in contrast to the risk of making online transactions. The perception of user skills captures each individual's perception of his or her capabilities and motivations to use a computer or a technological system (Nielsen, 2000).

The prevalent model of trust related to trust between people and technology is the model of online trust. Corritore and colleagues (Corritore, Kracher, & Wiedenbeck, 2003) identified three trust factors: user perceptions of technology's credibility, ease of use, and risk. Their four dimensions of credibility include honesty (well intention, truthful and unbiased actions), expertise (knowledge, experience, and competence), predictability (the expectation that technology will act consistently based on past experience), and reputation (recognised past performance). The model has been extensively applied to web design in e-government, e-commerce, and e-banking, but its value for Blockchain technology has received limited attention. The model also shares similarities with that of Davis (Davis, 1989).

#### *2.1.1.1 User's Trust towards the User Interface Design*

In the landscape of people interacting with the website, the design of a website is vital for the initial user's trust. Wang and Emurian (Wang & Emurian, 2005) suggested a framework of trust-inducing features for website along four dimensions: graphic design, structure design, content design, and social-cue design. The graphic design refers to the graphical design factors on the website that generally impacts on consumers a first impression, which includes the uses of colors, layout design and the quality of the photos presented in the website (Karvonen & Parkkinen, 2001; Kim & Moon, 1998; Seckler et al., 2015; Wang & Emurian, 2005). Meanwhile, the structure design elements relate to website organisation. This presents the overall look of a website and the accessibility of

information. It also includes the usability of the website in terms of the effectiveness of the design, ease-of-use of the website navigation and avoidance of pop-up advertisements in the design. In addition, the structure design is also related to the demands by the website to persuade users in a good way to share their URL with others, to register an account with the website or to download a piece of software (Goodhue et al., 2006; Leppanen, 2010; Mayer et al., 1995; Seckler et al., 2015). Meanwhile, content design refers to the informational formats provided by the website providers, either graphical or textual, which includes the security signs, the branding of the website, expertise, privacy policy related to personal data collections and secondary use of the data, web address, implausible promise and the website policy (Davis, 1989; Karvonen & Parkkinen, 2001; Leppanen, 2010; Lippert & Swiercz, 2005; Seckler et al., 2015). The final dimension is the social cue design, which relates to the social signs that reduce the gap of social distance and increase intimacy. Social media integration with the website is one of the common ways to connect the web providers and enhance the communication between users (Kim & Moon, 1998; Leppanen, 2010; Nielsen 1998; Seckler et al., 2015). In building trust, it is important for websites to provide sufficient information on their personal branding also the service and product being offered (Fisher, Craig, & Bentley, 2007).

<b>Dimension</b>	<b>Description</b>	<b>Characteristics</b>	<b>Literature sources</b>
Graphic Design	Websites' graphical elements that trigger the users' first impressions.	<ul style="list-style-type: none"> <li>• Visual design</li> </ul>	(Karvonen & Parkkinen, 2001; Kim & Moon, 1998; Seckler et al., 2015; Wang & Emurian, 2005)
Structure Design	Accessibility by users to the information displayed on the website and how the website is generally organised.	<ul style="list-style-type: none"> <li>• Usability</li> <li>• Pop-ups/ads</li> <li>• Demands</li> </ul>	(Goodhue et al., 2006; Leppanen, 2010; Mayer et al., 1995; Seckler et al., 2015)
Content Design	Informational elements that are placed on the website, either textual or graphical	<ul style="list-style-type: none"> <li>• Security signs</li> <li>• Image/brand</li> <li>• Expertise</li> <li>• Privacy: collection</li> <li>• Privacy: secondary use</li> <li>• Content</li> <li>• Web address</li> <li>• Implausible promises</li> <li>• Policy</li> </ul>	(Davis, 1989; Karvonen & Parkkinen, 2001; Leppanen, 2010; Lippert & Swiercz, 2005; Seckler et al., 2015)
Social-cue Design	Social cues that are integrated into the website, such as photographs and names of customer service agents, chat and call-back opportunities.	<ul style="list-style-type: none"> <li>• Customer service</li> <li>• Real-world link</li> </ul>	(Kim & Moon, 1998; Leppanen, 2010; Nielsen 1998; Seckler et al., 2015)
Personal and social proof	Social remarks such as comments and ratings from other users	<ul style="list-style-type: none"> <li>• User's social proof</li> <li>• Friend's social proof</li> <li>• Prior experience</li> </ul>	(Seckler et al., 2015)

**Table 2.1: Trust-Inducing Features of Website Interface Design (Seckler et al., 2015; Wang & Emurian, 2005)**

This framework has been applied in variety studies of various types of websites, such as cloud computing services (Öksüz, 2014) and geographic information system (Skarlatidou, Cheng, & Haklay, 2013). Although the framework was initially designed for websites, it also has been adopted in the study on mobile applications trust design (Hasslacher, 2014). Interestingly,

Seckler et al. (Seckler et al., 2015) also adopted the framework and conducted an empirical study with 221 participants to measure the trust and distrust through several types of website design interface, including e-commerce and e-banking/finance websites. Based on the outcome of their study, they extended the framework by adding another dimension which is personal and social cues. This new element is associated with the design for users' social proof such as user's feedback and reviews. On top of that, this is also related to the friend's social proof, which can be identified through the website connection with social media channels that enable the users to see their mutual friends that engage with the website as well as shared experience by other users (Seckler et al., 2015). The extended trust-inducing features for the website interface design are summarised in **Table 2.1**.

### 2.1.2 Trust between People Interacting with Technology

Meanwhile, the trust between people interact with technology is associated with social and institutional trust. Social trust has been defined as the feeling of the good disposition of the other (Falcone & Castelfranchi, 2001). Leppanen (Leppanen, 2010) also identified four key concepts of trust: disposition to trust, perceived trustworthiness, situational factors, and shared attributes. Disposition to trust indicates the trustor's own willingness to be dependent on others, further determined by a trusting stance and faith in humanity (McKnight, Cummings, & Chervany, 1998). It has been argued that the disposition to this goodwill arises from positive trust concerning exchanges with people, which lead to a positive general belief on mankind. Boon and Holmes (Boon & Holmes, 1991) also discussed how an individual's disposition towards trust sets expectations for trustworthiness in

general. Hence, personal, first-hand positive experience towards a new context is paramount in building up the disposition to trust. Perceived trustworthiness has been defined as the expectation that another party will perform a particular action (Fisher et al., 2007). This is an important concept which relies on distinct categories of beliefs such as benevolence, competence, honesty, and predictability (McKnight et al., 1998). Situational factors are those targeting the context of an organisation (McKnight et al., 1998). Moorman and Purser (Moorman, Deshpandé, & Zaltman, 1993; Purser, 2001) argued for the importance of the context in which trust formation takes place. Sharing attributes with a trusting partner is crucial in building a trusted relationship (Grandison et al., 2001). These include the importance of positive past exchanges that have been emphasised in Boon and Holmes's (Boon & Holmes, 1991) model describing the continuous nature of the shared experience. According to this model, both short- and long-term exchanges can benefit from shared attributes of trust.

Meanwhile, institutional trust is defined as the party being initially willingly vulnerable to a counterpart's action (Mayer et al., 1995). It can be described in terms of power relations and organisational structure. Power relation becomes important for trustworthiness in social relationship where an individual has a position of power for decision making in an organisation (Tyler & Degoey, 1996). Trust in organisational structure reflects the importance of hierarchical relationships across the organisation (Kramer & Kennedy, 1996). In McKnight's (McKnight et al., 1998) trust model, the organisational trust is explained through the system of rules and regulations governing each activity in the organisation. There have also been attempts to conceptualize trust in decentralised systems. For example, Gutscher's (Gutscher, 2007) trust model integrates public key authenticity

verification to evaluate arbitrary trust structures which allow multiple keys per user. This also enables the sign of a trusted certificate to limit the length of the trust chains and to define the semantics of trust. This trust model consists of four building blocks. Two basic blocks define the existing trust and authentication relations together with inference rules for combining them. The other two blocks describe representations of trust values and how to compute them for trust relations.

On the other hand, Blaze and colleagues (Blaze, Feigenbaum, & Lacy, 1996) addressed the issue of decentralised trust management through four principles: unified mechanism; flexibility; the locality of control; and separation of mechanism and policy. The unified mechanism holds the policies, credentials, and relationships for network application security, while the complex trust relationship falls under the flexibility principle. The locality of control supports the trust of relationship across the community, while the separation of mechanism policy supports control of the verifying credentials of the applications.

In HCI, the prevailing trust model for technology-mediated trust between users that has been applied to e-commerce is the framework on mechanics of trust (Riegelsberger, Sasse, & McCarthy, 2005). This framework identifies two key properties warranting trust in a transaction's partner: *contextual and intrinsic properties*. Contextual properties are described as temporal, social and institutional embeddedness. *Temporal embeddedness* refers to parties' potential for engaging in future transactions, and interest in their relationship's longevity. This, in turn, prevents the risk of defection, as the present gains come at the cost of future lost ones. Temporal embeddedness requires traceability of action through "repeated interaction with stable identities" (Riegelsberger et al., 2005) so that the trustor can accumulate more knowledge and make better predictions about the trustee's future

behaviour. *Social embeddedness* captures the exchange of information among trustors about trustees' past performance. This motivates the trustee to fulfil the agreement in order to protect his reputation among the larger pool of trustors accessing information about his past performances. *Institutional embeddedness* captures the legal aspects of underpinning transactions, able to enforce sanctions such as litigation or punishment for the parties who do not fulfil their agreement. Given this protection by the law institutions, the trustors are comfortable to engage in transactions with trustors of whom they know little.

Intrinsic properties of the trustee include his *ability* or motivation to act in a trustworthy manner inferable on the basis of his credibility; *internalised norms* which capture trustee's integrity or respect for moral principles which can be supported by the parties' social identify and presence; and *benevolence* capturing trustee's concern for the wellbeing of the other (Riegelsberger et al., 2005). Benevolence resembles Hardin's (Hardin, 2002) theory of trust and the *encapsulated interest*: parties' interest in a relationship which tends to be rich and ongoing. He also discusses risk as the uncertainty of a trustee's choice to engage in betrayal or deflection. This type of risk is better mitigated in a group or *thick relationships* in which the trustee's reputation is socially embedded.

#### *2.1.2.1 Reputation System to Support Trust*

In line with the social embeddedness dimension in the framework of mechanics of trust (Riegelsberger et al., 2005), trust among strangers can be built based on the history of past interactions and connected to the expectation for future engagement that is reflected by present interaction behaviour (Resnick, Zeckhauser, Swanson, & Lockwood, 2006). These concepts of trust are the

important properties for a reputation system to provide feedback from a present consumer that can be relied on the future. The reputation system management system model has been widely applied in various areas such as e-commerce, peer-to-peer systems and social networks (Janiszewski, 2017). In order to ensure that a reputation system works effectively, there are three important elements. The system must be able to provide a long term reputation record to inspire the expectation of future interaction; capture and disseminate feedback on present interaction; and enable other users to refer to the feedback as guidance for trust decision (Resnick et al., 2006). It is also essential for a reputation system to provide information which allows buyers to distinguish between trustworthy and non-trustworthy sellers, encourage sellers to be trustworthy and discourage participation from those who are not (Resnick et al., 2006).

From a technical perspective, the trust reputation management systems are built based on the concept of trust and reputation between the nodes (users) of the system (Rahimi & Bakkali, 2014), while the network architecture is designed in the form of a centralised or distributed reputation system (Kinateder & Rothermel, 2003). The centralised reputation system is managed by the central authority, which will typically collect the feedback ratings from the participants, then generate reputation scores and share the scores publicly. Resnick and colleagues (Resnick et al., 2006) identified seven categories of centralised reputation system: feedback forums (auction site provides opportunity for seller and buyer to rate each other); expert sites (group of people that are willing to answer questions based on their experience and expertise and the group members are allowed to rate the answer given by the experts); product review sites (people's reviews towards products); discussion forums (ratings for the users who

contribute to the discussion topics); web page ranking systems (way for search engines to list the hyperlinks based on the page's reputation); supplier reputation systems (ratings on the supply chain process); and scientometrics (reputation for researchers in terms of the citation and publication). There are a few examples of centralised reputation systems, such as the well-known e-commerce website eBay, which facilitate a live rating system immediately after recent purchases for both the seller and buyer to rate each other with either positive, neutral or negative ratings and also an option for comments (Jøsang, 2007). Additionally, TripAdvisor and Yelp are both community reviews websites related to interesting places around the world. They allow members to give their feedback and reviews on the places that they have visited. For TripAdvisor, the community will drop reviews on the hotels that they have visited and at the same time, other members can give rate their preference whether the reviews given are helpful or not. Meanwhile, Yelp has a broader focus for reviews, with more than 20 categories and also discussion forums segmented by city (Brown, 2012).

Meanwhile, in the distributed reputation system, there is no central authority which manages reputation scores. The reputations are based on two types of mechanisms: distributed communication protocol (participants obtain ratings from community ratings) and reputation computation method (individual agent computer the ratings based on the rating received) (Blaze et al., 1996; Gutscher, 2007). One prevalent example of a decentralised reputation system is OpenBazaar, an online platform for vendors to sell their products in Bitcoins and other over fifty types of cryptocurrencies. The OpenBazaar reputation system allows the buyers to send the ratings to the vendor in five categories: feedback, item quality, item description, item delivery, and customer service. The ratings

can be sent in a form of 1-5 stars and the buyers are allowed to include text for the feedback with a limitation of words. The ratings in OpenBazaar are tied to Bitcoins transaction and involve a small cost to make the rating (Open Bazaar, 2015).

### 2.1.3 Section Summary

The trust concepts, models and principles described above either fail to address trust in decentralisation systems or address it from the sole perspective of users of such systems. In the case of Bitcoin Blockchain, it is not only a decentralised system, but a grassroots-driven technology involving multiple stakeholders. Thus, it offers a unique perspective to explore the development of trust within and across these stakeholders, together with its most challenging and promising issues. A thoughtful chronological history of the existence of Bitcoins as cryptocurrency would be able to reflect the exploration of people's motivation, practice, and trust in Bitcoins.

## 2.2 History of Money

In the past, humans created an object as a medium of exchange to replace the barter system (Schweikart, 1991). The object could be a shell, stone or anything that was valuable to both buyer and seller. The ancestors deposited their valuable belongings with goldsmiths as a way for safe keeping and in return were given a receipt called a goldsmith note (Wray, 2012). However, in the 17th century, the role of goldsmiths was replaced by the government central banks which issued a national currency or fiat money (Wray, 2012). This, in turn, creates a new transformation of money from individual assets and money management to a new centralised authority which manages the money movements from one to another. Today, fiat money is still dominant and the evolving

technology makes information move briskly. Though, with all these advanced technologies, money movement is still slow, expensive and needs to bypass the regulated central authority (Raul Carrillo, 2015), compared to ancestors' method of money movements in which the transactions were conducted spontaneously without any hassle. As a result, several types of alternative currencies have been created to generate and strengthen people purchasing power.

### 2.2.1 Alternative Currency

Alternative currencies are used as a substitute for national currency that has been privately developed. However, most alternative currency has no legal tender and is not regulated by national governments or banks (Lipkis, Sarah and Roth, 2014). Fontinelle (Fontinelle, 2011) stated that there are four main reasons for creating an alternative currency. Firstly is to promote and enrich the local economic development. Secondly, is to build up social capital. Other than that, the alternative currency may help to nurture a more sustainable lifestyle among the communities and to meet the needs that mainstream money would not be able to provide. Finally, there are complementary currencies that exist to help the local community to have an equal human right. Alternative currency is also known as a complementary currency. Costanza (Costanza, 2003a) listed three types of complementary currency: fiat-backed complementary currency, mutual credit complementary currency and commodity-backed complementary currency.

#### 2.2.1.1 *Fiat Backed Complementary Currency*

Fiat backed complementary currency is very similar to the way that national currencies work, as the value of the money is based on the faith of the users towards the organisation or community that create and manage the monetary

system (Costanza, 2003b). The vital difference between those two currencies is that the community currency promotes the cooperation and development of community bonds within the users of fiat-backed complementary currency, while the value of national currency is derived from the scarcity to their usefulness (Costanza, 2003a). A few examples of fiat-backed complementary currencies are the Brixton pound, Sardex, and Koru Kenya that have been used in the United Kingdom, Italy, and Kenya, respectively (Raul Carrillo, 2015).

#### *2.2.1.2 Mutual Credit Complementary Currency*

Mutual credit complementary currency works in a ledger system that records the credit and debit of member accounts (Migchels, 2012). For each item purchased, the credit will be subtracted from the account, and vice versa. Unlike with conventional banks, there is no interest collected for the debts. The system allows the debts to be paid off by trading with goods and services (Hub Culture, 2014). For example Bangla-Pesa, the alternative currency in Kenya uses a mutual credit system to serve a local community that provides goods and services to each other by circulating the Bangla-Pesa as money (Darby, 2018).

#### *2.2.1.3 Commodity Backed Complementary Currency*

The other type of complementary currency is the commodity-backed complementary money. Differing from fiat-backed complementary currency; this currency does not need the interference of the national currency. It is underlying on a physical commodity with an intrinsic value such as gold and silver, such as the Liberty Dollar, which is backed by silver (Costanza, 2003a).

All of these three types of currencies are not legal tender. However, those currencies are managed by the organisations that facilitate the money transactions

among the communities. In reflection to trust, although it is not governed by the government, the users' trusts toward the currencies and money transactions rely on the central entities that create and manage those currencies. This, in turns, mirrors the category of users' trust in those alternative currencies similarly to the users' trust towards the national fiat money. In the framework of mechanics of trust, this type of user's trust is known as institutional trust (Riegelsberger et al., 2005). Meanwhile, the internet revolution does bring different waves to alternative currency as well. People started to create alternative money through the paperless system. This is where the revolution of digital currency begins.

### 2.2.2 Digital Currency

Digital currency is an Internet-based medium of exchange which is dissimilar in terms of physicality compared to real currency. Digital currency exhibits similar possessions to real currencies and allows for prompt and borderless transfer of ownership (Tasca, 2015a). The previous studies suggested that electronic cash or cybercash and virtual currency are all forms of digital currencies (Antwerpen, 1990; Lim & Lee, 1993; Shoaib, Ilyas, & Hayat Khiyal, 2013; Wray, 2012).

#### 2.2.2.1 *Electronic Cash*

Electronic cash or cyber cash is a digital representation of money that can be found either on a smart card (credit or debit card) or computer hard drive (FinCEN, 2000). The smart card can be used by using a proper reader and the monetary value can be added or deducted in the electronic account (FinCEN, 2000). In addition to the smart card, electronic cash is also largely used to facilitate internet payment in the electronic commerce industry today. Banks have

introduced electronic banking systems to enhance and support the usage of electronic cash over the Internet (Bakare, 2015).

#### *2.2.2.2 Virtual Currency*

A virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers and used and accepted among the members of a specific virtual community (European Central Bank, 2012). The Consumer Financial Protection Bureau (Consumer Financial Protection Bureau, 2016) argued that virtual currencies are a kind of electronic money, which are not tangible and which users may agree to accept and treat like dollars, euros, or other forms of money. There are two ways to own virtual currencies: either users can purchase it using the real money from the community at the agreed conversion rate, or they can engage with specific online activities which will reward them with the virtual currencies (Darby, 2018; Tasca, 2015b). Allen and Overy (Allen and Overy, 2015) classified virtual currency into two (2) categories which are open (convertible) and closed (non-convertible) and both administrations may be centralised or decentralised. The closed virtual currencies can only be used within the designated community, such as a specific online game environment. Meanwhile, open virtual currencies allow the exchanges for the real currency and are categorised into two groups, non-cryptocurrency, and cryptocurrency (Consumer Financial Protection Bureau, 2016).

- **Non-cryptocurrency**

Non-cryptocurrency was first founded in 1996 as E-gold, which is backed by gold (White, 2014). Then in 2006, another alternative digital currency was

founded, named Liberty Reserve, allowed users to exchange dollars or euros to Liberty Dollars or Euros. However, those currencies were shut down by the US government due to excessive money laundering activities using both digital currencies (Lim & Lee, 1993; Resnick et al., 2006). In 2007, Stan Stalnaker (Knoop, 2015) forms a new virtual currency, Ven, which is backed by commodities such as oil, currencies or other exchange-traded assets that are chosen by the board (Ilett, 2013). Currently, there are more than 50 million units circulated among the communities. The price of Ven is controlled by the algorithm and is still actively used by the community (Hub Culture, 2014; Knoop, 2015). Hub Culture is the company which is responsible for managing the flow of the money as well as handling the disputes among the users. Hence, the trust of the users is categorised as institutional trust (Riegelsberger et al., 2005).

- **Cryptocurrency**

Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography (FATF, 2014). Bitcoin Satoshi Nakamoto is the anonymous entity who introduced the first cryptocurrency in 2009 known as Bitcoin. Bitcoin provides a solution to the digital money transfer without employing a third party institution (Nakamoto, 2008). Unlike fiat-backed currency or commodity currency, Bitcoin and other cryptocurrencies are created with a mathematical cryptographic algorithm, and are not backed by either fiat money or commodities (FATF, 2014). The fundamental feature of Bitcoin cryptocurrencies is the underlying technology, named Blockchain, which provides a transparent and a decentralised ledger to record the cryptocurrencies' transactions (Swan, 2015). However, due to the decentralisation of Bitcoin, the

user's trust is no longer dependent on any central authority. Thus, it offers negative spaces for scammers to create fraud transactions. This, in turn, has threatened the trust of the users.

### 2.2.3 Properties of Money

Be it a paper or digital money, the properties of money are important to allow it to be materialised and accepted by people and communities. Jevons (Jevons, 1890) suggested seven properties of money, which are: value of material, portability, durable, homogeneous, divisibility, the stability of value and being cognizable. However, Sykes (Sykes, 1905) argued that the value of the material to create money is not relevant in the new age as the banks have started to produce a banknote using a paper and yet people can still accept it as money and the stability of the value of money although it is important, it is very difficult to retain. **Table 2.2** described the six properties of money used in this study.

<b>Property of Money</b>	<b>Description</b>	<b>Literature source</b>
Durable	The durability of money is defined as physically able to use for a very long time without being damaged or need to be reworked	(Bank of Canada, 2016; Jevons, 1890; Sykes, 1905)
Divisible	Money must also be mechanically divisible into usable quantities or fractions and the aggregate value after division should be almost exactly the same as before division	(Bank of Canada, 2016; Jevons, 1890)
Portability	Money must always be easy to be moved and transferred from one to another	(Bank of Canada, 2016; Jevons, 1890)
Scarcity/ Stability of Value	Scarcity of money is described as money should not be easily produced and not fluctuate in value but at the same time it must be sufficient for economic exchanges	(Bank of Canada, 2016; Sykes, 1905)
Homogeneity/ Fungible	The homogeneity of money refers to the equal quality of materials and weight and size for money that has the same value	(Bank of Canada, 2016; Jevons, 1890)
Verifiable/ Cognizable	The capability to identify the	(Bank of Canada,

	originality of money to avoid people from using fake money	2016; Jevons, 1890
--	--	--------------------

**Table 2.2: Properties of Money (Bank of Canada, 2016; Jevons, 1890; Sykes, 1905)**

#### 2.2.4 Alternative Currencies in HCI Study

Meanwhile, the HCI community has recently started to engage with the topic of digital currency (Kaye, Vertesi, Ferreira, Brown, & Perry, 2014). Ferreira et al. (Ferreira, Mark, & Subramanian, 2015) explored user experience with the Bristol Pound (£B), a local complementary currency used in Bristol, UK. Authors run a survey with about 200 users on how people conduct mobile phone transactions via SMS and their motivations and challenges for using this currency. Study findings highlighted the payment's unpredictable and slow qualities and its value for strengthening social connections through ludic interactions, as well as increased mindfulness about their practice of purchase and consumption. This underlies the paradox of how a technology lacking trust, allows for strengthening the social trust between the actors involved in transactions, leading in turn to a more cohesive community. The study also emphasised that Bitcoin technology may benefit from leveraging such face to face social connections in small communities to mitigate the challenges of slow, unreliable transactions.

In a critique of alternative and complementary currency and exchange paradigms, Carroll and Bellotti (Carroll & Bellotti, 2015) discussed four technological innovations: local currencies, time banks, cryptocurrencies, and microenterprises. In particular, they highlighted the value of cryptocurrencies like Bitcoin for individual privacy and control, potentially subverting centralised governmental and financial institutions. Authors have placed this critique in the current global economic context, whose challenges may well benefit from such

novel, money centred design, and technologies, as a rich space for CSCW and HCI communities to engage with.

In contrast with gold or physical money, digital currencies have a more recent history but have witnessed a growing community of users. In addition to Bitcoin, other digital currencies such as Ripple, Litecoin, Dash, or Dogecoin have attracted a wide range of users from specific communities, i.e. online games (Glaser, Zimmermann, Haferkorn, Weber, & Siering, 2014). The functions and roles of money, largely explored in social and economic sciences, have been less explored with respect to cryptocurrencies. Such currency, however, may have both similar and distinct qualities from gold and national currencies.

#### 2.2.5 Section Summary

The main aim of the creation of alternative currencies as well as the digital currencies is to escalate the people's purchasing power as mediated by the government and limit the usage of their own money. Those currencies are created by a central entity with the aim to manage the flow of monetary transactions, according to the community issues and capabilities. However, indirectly, these organizations also act as an institutional trust for the users, unlike Bitcoin which was created by the anonymous entity and it is not governed by any central authority. Hence, it is worthwhile to explore the trust issues as well as mitigating action taken among the users.

### 2.3 Bitcoin Cryptocurrency

Issued in 2009 by an anonymous entity (Rogojanu & Badea, 2014), Bitcoin technology has become a leader in peer-to-peer crypto-currency, allowing secure transfer and exchange of digital tokens in a distributed and decentralised manner (Nakamoto,

2008). Bitcoin can be exchanged for other national fiat currencies at the agreed market rate (Coin Desk, 2019) through online marketplaces into a digital wallet. In addition to money, the exchange can also be done for goods and services, or use the Bitcoins to buy goods or properties (Göbel et al., 2015). At present, Bitcoin is a leader among more than 2000 peer-to-peer currencies on the market (Coin Market Cap, 2019b) and experts have foreseen that Bitcoin users will reach almost 200 million by 2024 (Young, 2017).

In the Bitcoin network, money is not printed, but mined through widely distributed peer-to-peer network computing power in a controlled way by the miners running a dedicated program in their computer system (Bradbury, 2013). The miners' job is to run the program to record the Bitcoins transactions from one user to another user. Those transactions will be recorded in a publicly distributed ledger called Blockchain (Swan, 2015). In a Blockchain ledger, the set of Bitcoins' transactions are publicly distributed throughout the peer-to-peer nodes across the network. The uniqueness of this underlying technology for Bitcoin is it allows for secure and transparent transactions while protecting the identity of transaction's parties (Nakamoto, 2008). Transactions are considered pseudoanonymous because although the transactions are publicly archived under an individual's Bitcoin address, the identity of the owner's address remains undisclosed. These processes in Bitcoin network are decentralised and supported by multiple stakeholders.

### 2.3.1 Bitcoin Stakeholders

Bitcoin is managed and applied by a community. Shcherbak (Shcherbak, 2014) grouped Bitcoin stakeholders in four categories: users, miners, exchanges, and merchants.

### *2.3.1.1 Bitcoin Users*

Bitcoin users are people who own the Bitcoins in their Bitcoin's wallet. The Bitcoin users use Bitcoins either to buy goods and services from the Bitcoin merchants or to buy and sell Bitcoins for other national fiat currencies such as USD and Pound Sterling (Shcherbak, 2014) or other types of cryptocurrencies such as Ether and Nem from the Bitcoin exchanges (Agrawal, 2018).

### *2.3.1.2 Bitcoin Miners*

Bitcoin miners are those who own the miner machine that is used to process Bitcoin transactions and record in the Blockchain. In return, the miner will be rewarded with Bitcoins for each new block of Bitcoin transactions recorded in the Blockchain ledger (Eyal & Sirer, 2014). The miner's machines range from the CPU of an ordinary personal computer to an ASIC Bitcoin miner, which is a machine that consists of an integrated circuit that is designed specifically for Bitcoin mining (Martindale, 2018).

### *2.3.1.3 Bitcoin Merchants*

Bitcoin merchants are businesses which accept Bitcoins as a medium of exchange for goods and services. The merchants can be either an online business or a physical store. For example, one of the famous franchises Kentucky Fried Chicken (KFC) in Canada does accept Bitcoins in their branches (Higgins, 2018) and Microsoft accepts Bitcoins in their online stores (Vanian, 2018).

#### *2.3.1.4 Bitcoins Exchanges*

Bitcoin exchanges are companies that provide the online trading platform for Bitcoins to be exchanged with fiat money or other types of cryptocurrencies. The Bitcoin exchanges act as a third party between the Bitcoin seller and buyer. However, users are required to register and de-anonymise themselves to the exchange company. In addition, for each Bitcoin transaction, there are also additional fees to be paid to the company (Coinbase, 2019).

#### 2.3.2 Bitcoin Trust Research Framework

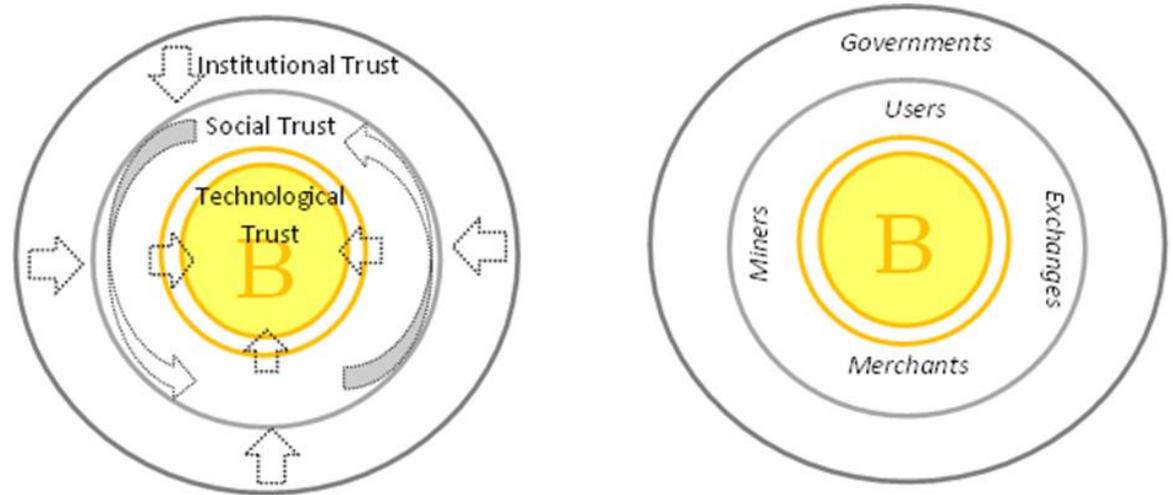
Based on the literature of trust and Bitcoin technology, I have collaborated with my supervisor, Professor Corina Sas, to propose a framework (**Figure 2.2**) for exploring trust in Bitcoin technology (Sas & Khairuddin, 2015) which integrates the key aspects of trust from HCI literature, with the main challenges posed by Bitcoin technology, to ensure the exploration of trust across all the Bitcoin stakeholders (Sas & Khairuddin, 2015). The framework places Bitcoin technology at its centre and highlights how different stakeholders are involved in shaping the three different levels of trust. The study defines technological trust as people's trust in Bitcoin technology as experienced before, during, and after engaging in online transactions. This could include users' trust that their Bitcoin account is secured and cannot be hacked or payees' trust that the transfer is authorised.

Social trust is the trust that Bitcoin stakeholders develop with each other. This trust is enlisted for each type of exchange occurring across (and within) different categories of stakeholders. For example, transactions involving the purchase of goods enlist trust between users and merchants. Upon completion, these transactions require miners' authorisation, so both users and merchants need to trust the miners

for completing their job. At the same time, selfish miners can raise issues of trust among miners (Eyal & Sirer, 2014). Social trust between users/merchants and exchanges can be also problematic. This study argues that because of its decentralised nature, the classic definition of institutional trust does not apply to Bitcoin. However, there is a higher authority to which Bitcoin technology is requested to be accountable, namely governmental institutions. The study defines institutional trust, the trust of governmental institutions in Bitcoin technology. The main issues here are related to money laundry and deflation.

#### *2.3.2.1 Applying the Framework to Identify Trust Challenges*

The study now explores how the framework can be applied to identify important trust issues which deserve stronger HCI engagement. It should be noted that there is limited empirical work exploring the experience of using Bitcoin and the issues of trust surrounding it. The study starts by describing the Bitcoin stakeholders, grouped by (Shcherbak, 2014) in four categories: users, miners, exchanges, and merchants. Users are people who use Bitcoin to buy goods and services from Bitcoin merchants. Merchants are businesses which accept Bitcoins as a medium of exchange for goods and services and are connected to the Bitcoin network. Exchanges are the providers of online trading platforms where the registered members can exchange their Bitcoins for traditional currency and vice versa. Miners are those Bitcoin stakeholders who can record transactions (and collect the reward) after they have successfully solved crypto puzzles (Eyal & Sirer, 2014).



**Figure 2.2: Research Framework for Exploring Levels of Trust in Bitcoin Technology (left) and across Stakeholders Groups (right) (Sas and Khairuddin, 2015)**

- **Users' Trust in Bitcoin**

One specific challenge pertaining to users is their limited knowledge of how Bitcoin technology works and how they need to protect their Bitcoins. Keeping Bitcoins on one's computer involves security risks similar to keeping large sums of cash in one's physical wallet (Bitcoin Wiki, n.d.). Although Bitcoin is decentralised and at large has no single point of failure, it is nevertheless susceptible to forms of denial of service or double-spending attacks (Karame et al., 2014).

- **Miners' and Exchanges Trust in Bitcoin**

There is a limited exploration of trust challenges faced by these stakeholders. However, exchanges are crucial in gaining users' and merchants' trust, and at large the social trust within the Bitcoin system. For example, exchanges have no audit process and no verification procedures (Talk, 2010). Equally, although each transaction should be digitally signed and secure after being verified by an

unknown miner, there has been a limited exploration into mechanisms concerning miners' competence and integrity. Recent work has shown that the reward structure which incentivises miners to contribute to the system and its decentralised nature, can motivate some miners to circumvent the Bitcoin protocol and mine selfishly at the cost of honest miners (Eyal & Sirer, 2014). This suggests that issues of trust can also develop within the same stakeholder category.

- **Merchants' Trust in Bitcoin**

Merchants' trust is challenged by their limited knowledge about buyers, and whether their payment will be received in time or at all (Shcherbak, 2014). They also lack the ability to track reliable buyers with whom they have previously engaged in positive transactions.

- **Governments' Trust in Bitcoin**

Bitcoin is a protocol promoted as the first peer-to-peer institution, offering an alternative to central banks (Abramowitz, 2014). It has been argued that the demand for peer-to-peer transactions can be an indication of the development of trust in Bitcoin (Nakamoto, 2008). In this context, it is useful to revisit the main components of peer-to-peer governances as a mechanism for institutional trust in Bitcoin: arbitration, trust, bank, business association, and public law. For example, peer-to-peer protocols can offer structure through a set of rules for controlling the Bitcoin technology. The peer-to-peer protocol can also be used by governments to develop a structured legal framework for Bitcoin technology. In peer-to-peer decision making, arbitration is one way to resolve disputes

(Thornburg, 2012). If peer-to-peer arbitration is able to serve decisions, then it could also serve as the foundation for peer-to-peer trust. It would be beneficial for the trustee to be able to invest deposited Bitcoins to grow their trust corpus (Abramowitz, 2014). However, the challenge in cryptocurrency is there is no mechanism allowing such accounts to own virtual assets. In order to own the assets, there is a need for an intermediary link between the virtual and the real world. Indeed a cryptocurrency bank may be able to establish this connection. If the peer-to-peer bank is able to accept bank funds, make investment decisions, and approve expenditures, then peer-to-peer decision making can be used to operate the peer-to-peer business association (Abramowitz, 2014). A significant obstacle to private peer-to-peer institutions is government hostility (Abramowitz, 2014). Despite lacking trust, peer-to-peer systems can yet produce decisions with a high degree of consensus. This limited form of decision-making inherent in Bitcoin technology could serve as a foundation for more sophisticated types of decision-making mechanisms, allowing legal institutions to be created without the designation of a central authority.

### 2.3.3 Section Summary

The research framework has shown that the challenges of trust are pervasive, affecting all Bitcoin stakeholders, albeit in different ways. They are also interdependent, as distinct user groups may have conflicting goals. Not least, some trust challenges are hidden, i.e., miners' activities are seldom open for scrutiny. The study argues that a user-centred approach to the exploration of trust can shed light into the challenges experienced by people using Bitcoin. This is radically different than the current algorithmic approach to trust in Bitcoin. Research supported by this

framework can also open up novel design opportunities to address the identified challenges and support trust. For example, one can imagine a new class of interactive technologies where trust is captured, materialised and gained or lost through exchanges. This new design space for decentralised interactive cryptocurrency technologies may not only support better adoption of Bitcoin technology, but also the digital currency economy at large.

## 2.4 Blockchain Technology

As a public ledger, Blockchain is known as a transparent system. Each machine connected to the Blockchain can download a full copy of the ledger, allowing for browsing or querying the global history of transactions as well as the remaining balance of the Bitcoins left in each wallet address (Swan, 2015). Since it no longer requires trust in third-party entities to keep the ledger, Blockchain technology has been called trustless. In Nakamoto's view (Nakamoto, 2008), the concepts of irreversible transactions and trust are strongly coupled. The Blockchain aims to address the key weakness of the traditional trust-based model where financial institutions act as trusted third parties to mediate e-payments. Bank transactions, however, are costly both in time and fees (Raul Carrillo, 2015). In contrast, Blockchain was intended to eliminate this middle link and its higher cost.

Another important aspect of Blockchain is protecting the privacy of the parties involved in Bitcoin transactions (Swan, 2015). Similar functionality is available in the banking system, in which privacy is ensured by limiting access to transaction information to the involved parties and the bank. However, the protection of privacy in Blockchain is even stronger, since it does not require any personally identifiable information to allow users to engage in Bitcoin transactions. This makes the Blockchain pseudoanonymous

(Caetano, 2015): the wallet address is public while the identity of its owner is not (Nakamoto, 2008). However, the pseudoanonymous nature of Blockchain technology leaves it open to misuse on the online black market such as the Silk Road, with negative consequences for Blockchain's reputation (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2016). Nevertheless, the Blockchain application has moved beyond Bitcoin and cryptocurrency. The unique decentralised platform offered by Blockchain has attracted plenty of multi corporations (Chen, 2014) to adopt the technology to be applied in various fields such as in medical, real estate and copyright management applications (Ekblaw et al., 2016; Elsdén et al., 2018; Karamitsos et al., 2018).

#### 2.4.1 Bitcoin Blockchain Protocol

The Blockchain protocol is known to be very complicated and complex, as it challenges understandings of the traditional banking system or other payment systems that are centralised and regulated. The protocol is associated with several entities and different functions which are described in this following section.

##### *2.4.1.1 Bitcoin Wallet*

In creating a Bitcoin transaction, the first thing needed is the Bitcoin wallet for both the sender and receiver. Similar to physical ordinary wallets which can hold several credit and debit cards, Bitcoin wallets also consist of several pairs of public and private keys that hold the Bitcoins (Latifa, Kiram, & Ahemed, 2017). The private key is hidden by the Bitcoin wallet, though it can be printed in a physical form as a backup for the owner. It is the responsibility of the wallet's owner to not disclose the private key to anyone and to keep it safe (Caetano, 2015). It is because it is not possible to retrieve the Bitcoins in the wallet if someone lost the private key. Meanwhile, the public key is used to generate the

Bitcoin address through a cryptographic hashing algorithm (Caetano, 2015). Just like an email address, public key and Bitcoin address are the main identity for the user to receive Bitcoins from the sender.

#### *2.4.1.2 Enacting Bitcoin Transaction*

In order to create a transaction, firstly the sender needs to specify all current Bitcoin addresses of the wallet owner (some wallets consist of more than one address) and the receiver's wallet address and the owner's own wallet address (Antonopoulos, 2010). The owner needs to send all Bitcoins in his wallet by specifying the number of Bitcoins to be sent to the receiver's wallet address, the mining fee and the balance of the Bitcoins to be sent back to his own wallet address. Then, this transaction needs to be digitally signed or encrypted by the sender's private key. The public key is used to decrypt the transaction or to verify the signature (Caetano, 2015).

Once the transaction is signed or encrypted, it will be sent for a verification to the full nodes (Caetano, 2015) to ensure that it meets the validity guidelines of the consensus rules for inclusion in a new block, i.e., to verify the signature by ensuring the private and public key are matched and checked the size of the transaction (Caetano, 2015). If the transaction has fulfilled the requirements of the consensus rules, the transaction will be broadcast and sent to the memory pool together with other unconfirmed transactions (Caetano, 2015).

#### *2.4.1.3 Bitcoin Mining*

From the memory pool, the unconfirmed transactions will be collected and put in a new block. This block can hold up to 1 MB of transactions (Abramowitz, 2014; Caetano, 2015; Swan, 2015). The selection of the unconfirmed transactions

to be included in a new block is based on the highest mining fee provided by the sender. This block will be processed by the miners in the network by using their computational power to solve the complex mathematical algorithm (Abramowitz, 2014; Caetano, 2015; Swan, 2015). The miners work to solve the block by using the hash function to generate a hash result. If the result is invalid, a nonce will be added to the block's data set and the data set will be hashed again by the miner using a different hash until it matches the target considered the solution.

The solution is broadcast to the network as a new block which also contains the difficulty target and the winning nonce (Abramowitz, 2014; Caetano, 2015; Swan, 2015). This is called proof-of-work. The other miner in the network will use the broadcasted solution to recompute the hash on the new block to verify the proof-of-work (Abramowitz, 2014; Caetano, 2015; Swan, 2015). Once the solution has been verified by the network, the winning miner sends the solved block back to the full nodes to check against the consensus, such as to ensure there are no double-spending Bitcoins in the transaction (Caetano, 2015). Finally, once the block is validated, it will be publicly recorded in the Blockchain ledger.

#### *2.4.1.4 Mining reward*

Once a new block is successfully recorded on the public ledger, the winning miner is rewarded with 12.5 Bitcoins. The number of rewards are halved in every four years. This process is named as halving which the algorithm created reflects the scarcity properties of Bitcoins, whose total supply of 21 million will be completed by 2140 (Donnelly, 2016). The winning miners are also rewarded with transaction fees, albeit these are covered not by the Blockchain system, but by the transaction parties (Caetano, 2015; Swan, 2015).

#### 2.4.2 Security Research on Mining-related Threats

Most work on mining's trust challenges has taken place in the security research area, and focused on the risk of an entity owning a large share of a network's computational power. The threat of 51% attack occurs when a group owns over 50% of the computational power of the whole Blockchain network, and is, therefore, able to behave dishonestly by performing changes to the protocol or the public ledger's records (Carroll & Bellotti, 2015; Latifa et al., 2017). The other threat is 25% or selfish miners' attack which occurs when miners work on their proof-of-work without releasing the solutions publicly until theirs is the longest (Antonopoulos, 2010; Cawrey, 2014; Eyal & Sirer, 2014; Torpey, 2015). There are also arguments that selfish miners need at least 25% (Eyal & Sirer, 2014), or even 50% of a network's computational power (Cawrey, 2014; Torpey, 2015).

#### 2.4.3 The Comparison between Bitcoin and Ethereum Blockchain Ledger

Trust in a decentralised ledger involves two main mechanisms: the security protocol and consensus (Salomaa, 1996). Firstly, the security protocol mechanism is related to the public cryptographic key representing the encryption scheme that uses two mathematically related, but not identical keys – a public and private key (Salomaa, 1996). These keys are to prove that the created transaction is authenticated and validated (Salomaa, 1996). Secondly, the consensus mechanism aims to ensure the validity and consistency of the newly created record (Stevens, 2018). Both mechanisms are applied in Blockchain technology (Ray, Ventresca, & Wan, 2018).

Blockchain was introduced in 2008 and described as a technology component underlying the Bitcoin cryptocurrency (Nakamoto, 2008). However, later people

started to look at Blockchain beyond Bitcoin by expanding the protocols and the architecture of the Blockchain. Today, there are more than 1000 cryptocurrencies available in the market, led by Bitcoin and followed by Ethereum (Coin Market Cap, 2019a). Both Bitcoin and Ethereum Blockchains are supported by the decentralised and distributed ledger, and the records in the ledger are cryptographically chained together. However, both cryptocurrencies were created with different aims.

#### *2.4.3.1 Usages and Capabilities*

The Bitcoin Blockchain was developed with the aim of serving as a peer-to-peer electronic cash system, enabling an online payment system for the community. Bitcoin allows people to send money without using a centralised payment system such as the banking system. Although there are studies to explore the methods to expand the Bitcoin Blockchain capabilities by inserting other arbitrary data including images, the current Bitcoin Blockchain still remains to only hold Bitcoin transactions (Sward, Vecna, & Forrest, 2018).

In contrast, the Ethereum Blockchain is an open software platform that was built in the decentralised Blockchain technology, which allows the developers to build and deploy decentralised applications (Buterin, 2013a). Unlike Bitcoin Blockchain, the Ethereum Blockchain enables the recording of multiple types of arbitrary data (Buterin, 2013a). This allows the developers to store the decentralised applications, also known as a smart contract in the Ethereum Blockchain (Vujicic, Jagodic, & Randic, 2018).

A smart contract is a decentralised way for people to make a transparent exchange for either money, real estate or anything that is valuable (Hertig, 2018;

Karamitsos et al., 2018). An exchange in the smart contract can be conducted in a conflict-free way, at the same time avoiding the service of a middleman. Each executed contract will be permanently stored in the form of a digital token on the Ethereum Blockchain (Buterin, 2013a). The Ethereum technology has been applied in many sectors including finance, healthcare, and supply chains (Bocek, Rodrigues, Strasser, & Stiller, 2017; Ekblaw et al., 2016; Singh & Singh, 2016).

#### *2.4.3.2 Cryptocurrency*

The Bitcoin Blockchain cryptocurrency is known as Bitcoin. The Blockchain acts as the ledger containing the historical records of all Bitcoin transactions that ever occurred in the network (Nakamoto, 2008). This is similar to the Ethereum Blockchain, but the cryptocurrency is known as Ether (Buterin, 2013a). Ether is also used by people on the network to pay mining fees for smart contract execution on the Ethereum Blockchain.

#### *2.4.3.3 Mining Works*

The mining protocols for Bitcoin and Ether are almost the same. Both require miners to solve a complex mathematical puzzle by working on the proof-of-work in order to record the new block on the Blockchain. There is only one miner who will be the winner for each block (Acheson, 2007; Swan, 2015). As for Bitcoins, each winning miner will receive Bitcoin as reward for their work, and the current amount of reward is 12.5 Bitcoins (Donnelly, 2016). The time for the miner to record a new block on Bitcoin Blockchain is approximately 10 minutes for each block (Acheson, 2007; Swan, 2015).

In comparison, the winning Ether miner for each block in Ethereum Blockchain will receive 2 Ether as a reward (Ogono, 2018) together with the gas

fees provided for the transactions of the block. The gas fee is also known as a transaction fee for each executed transaction on Ethereum network. Each user needs to include sufficient gas fees to cover the miner's computational resources used for the executed transaction to avoid the out of gas error (Buterin, 2013a). Just like Bitcoin, the highest gas fee provided has more opportunity to be selected from the memory pool. However, the time taken to record a new block in Ethereum Blockchain is much faster compared to Bitcoin, i.e., around 12-15 seconds (Buterin, 2013a).

#### *2.4.3.4 Multisignature technology*

A standard cryptocurrency transaction in Blockchain requires only one signature of the owner of the private key that is associated with the public key or a Bitcoin address (Nakamoto, 2008). This is known as a single signature. In contrast, multisignature technology requires more than one key or signature to authorise the transaction, which in turn makes the transaction safer and secure. This normally involves more than one user in a transaction, often referred to as M-of-N transaction (Davenport, 2015). The multisignature transactions require cooperation and agreement of more than one person in order to proceed with a transaction. The multisignature can be in either between 2 persons (1-of-2 or 2-of-2) or, to avoid any disputes, the transaction can also involve a third or more persons (2-of-3 or 3-of-5) (Davenport, 2015). Bitcoin network does support transactions that require the signatures of multiple people before the Bitcoins can be transferred. There are several Bitcoin wallets that support multisignature technology such as Armory, Electrum, Copay, and BitGo (Khatwani, 2018).

However, compared to Ethereum, the Bitcoin multisignature scheme is more rigid. In other words, if the transactions are signed by all required signatures, then it will be broadcasted to the network, but if it is not, then the transactions will remain in the wallet (Miller, 2017). An additional advantage of Ethereum multisignature includes allowing the transaction to be in 3 attributes which are the binary outcome, restricted functionality, and creation finality. The binary outcome means that the transaction can be either accepted or failed immediately. Restricted functionality allows the wallet to make the transaction, but it does not have any authority to move beyond that. In addition, the Ethereum multisignature allows the creation of finality that enables the developer to create a parameter and seal it in a smart contract (Miller, 2017). Thus, the transaction in the multisignature wallet can be automatically executed based on the parameters or rules that had been identified by the owners in the multisignature wallet.

#### 2.4.4 Section Summary

To conclude, Blockchain technology and its mining protocol have been purposefully designed as decentralised, transparent, and unregulated. While these contribute to its trust, they also raise risks and challenges when a mining pool acquires the majority of computational power to control the Blockchain. There is however a limited empirical work exploring Blockchain's characteristics and their impact on miners' trust through qualitative fieldwork.

## 2.5 Mental Model in HCI

In HCI research, the mental model concept has been used to describe a cognitive mechanism for representing and making inferences about a system or problem which the user builds as they interact with, and learn about the system (Borgman, 1999). The

historical findings by Craik (Craik, 1943) suggest that mental models offer ways for humans to translate physical interactions into their internal representations. This definition has become the main reference for further exploration of the mental model concepts. For example, Young (Young, 1981) defines mental models as human assumptions needed to create the mental representations of a system, in order to assist people to understand the system activities. Another view advanced by Clarke (Clarke, 1988) in his three-level human-computer interface model argues that the human intuition, creativity, strategy, conation, and memory are the important mental functions for designing a system interface.

From Norman's seminal work (Norman, 1990) distinguishing between a designer's and user's mental model capturing how the system is designed, or understood to work, much HCI research (Borgman, 1999) has shown the value of such models in supporting system learning (Kieras & Bovair, 1964), problem-solving (Klemmer, Li, Lin, & Landay, 2004), increased system's efficiency (Staggers & Norcio, 1993) or accuracy (Larkin, 1983). Previous findings indicate that mental models support the users' learning of complex devices which in turn allows for increased task performance (Fein, Olson, & Olson, 1993), an effect which is stronger for novice users (Staggers & Norcio, 1993). The distinction between novices' and experts' mental model is an important one, with consistent findings indicating that the latter is more accurate, complex, and abstract (Diesessa, 1981; Doane, 1982; Greeno, 1983) enabling a deeper understanding of the inner working of a system rather than merely how it can be used. In addition, a wealth of findings has shown that people have limited mental models of technological systems, such as personal or home technologies, including appliances (Caillot & Nguyen-Xuan, 1995; Doane, 1982; Kieras & Bovair, 1964) or energy monitors (Sas & Neustaedter, 2017). Such systems tend to be operated from superficial functional models rather than

structural ones. Other studies suggest that abstract concepts are particularly challenging to grasp as they lack materiality or visibility (Fischer, 2008; Pierce & Paulos, 2012b, 2012a). While much of previous work focused on mental models of interactive systems (Borgman, 1999) learning environment (Kieras & Bovair, 1964) or complex home technologies (Sas & Neustaedter, 2017), less work explored the mental models of large-scale distributed systems or technological infrastructures such as Blockchain. Current attempts to communicate mental models of how Blockchain works include mostly non-interactive visual representations, be they static such as infographics (Cartwright, 2018) or dynamic such as videos (The Guardian, 2014). Many of these representations have been developed in the private sector with a limited reflection on the analogies they aim to support.

A noticeable example of materialising the Blockchain and communicating its mental models through objects involved LEGO blocks, which both experts and novices may use to describe their understanding (Maxwell, Speed, & Campbell, 2015). Unlike commercial visual representation, such physical materialisation of Blockchain is interactive, allowing people to touch and move the Lego blocks in order to simulate interactions on the Blockchain. However, given the complexity of Blockchain infrastructure, this study argues for more specific objects rather than generic Lego blocks. A purposeful design of the kit and its objects which would more explicitly reflect the main properties of Blockchain's key entities, both in terms of their appearance and affordances for interaction, could allow stronger and more embodied engagement.

### 2.5.1 Physical Interaction

Mental models have been externalised in various of ways, from text, diagrams (Hegarty & Just, 1993), or animations (Lowe & Boucheix, 2008) to physical three-

dimensional models (Johnson-Laird, 2004). One way to explore a user's mental model is through a tangible user interface (TUI): the everyday physical objects and environment that has been used to describe the digital information (Ishii & Ullmer, 1997). Ishii and Ulmer (Ishii & Ullmer, 1997) described tangible interaction as giving physical form to digital information and its subsequent physical control. Their research focused on developing a new landscape of human, tangible interaction, from the Graphical User Interface (GUI) to Tangible User Interface (TUI). Previous research on GUI suggested a metaphor for a desktop computer workstation, with several HCI design principles that enable people to interact with the computer by using the mouse, windows, icons and property sheet (Ishii & Ullmer, 1997; Lowe & Boucheix, 2008).

Today, the GUI is widely used by Microsoft Windows (Microsoft, 2018). However, Ishii and Ulmer (Ishii & Ullmer, 1997) argued that the implementation of GUI screens limits the human skills in manipulating and interacting with the physical worlds which are supposed to be beyond the screen, windows, and keyboard. Hence, he suggested TUI, which aims to customize each application from the physical to the digital world. The basic concept of TUI design is the input and output, or control and representation (Ishii & Ullmer, 1997). For example, Ishii and Ulmer (Ishii & Ullmer, 1997) introduced the Tangible Bits that consists of three elements: interactive surfaces (e.g. wall, doors and ceiling), graspable objects (e.g. cards, books and models), and ambient media (e.g. sound, light and water) to represent the respective digital concepts of virtual space, digital information, and the background of cyberspace that indulges the human perception. One example is Clearboard which integrated shared drawing and interpersonal space for users to work simultaneously on design, regardless of their geographical location. The

interaction between the users of this device has transformed the concept of a passive structured “wall” into a new vision of architectural space whose all surfaces including walls, ceiling, and windows as active surfaces enabling people to interact in both real and virtual worlds (Ishii & Ullmer, 1997).

Later, Fishkin (Fishkin, 2004) adopted Ishii and Ulmer’s TUI theory (Ishii & Ullmer, 1997) and developed the TUI taxonomy as guidance for the tangible user interface design. The framework has two axes, which are the embodiment and metaphors. The embodiment describes the distance of the input and output of a system and how the users manipulate it. There are four characteristics of embodiment. The first is known as *full*, in which the output of a device is actually the input of a device. This can be seen in the application “Sketchpad” where whatever user writes or draws is also the display of the work (Fishkin, 2004). The second is *nearby*, the output is near to the input, as shown in the light pen. The third is *environmental*, where the output is around the user. For instance, the audio sound is the output of the music player, and the fourth is *distant*, where the output is far and input will be used to control the output, such as in the concepts of television and its remote control (Fishkin, 2004). The other axes of the framework are the metaphors which consist of five elements such as *none* to explain the object that does not have a specific metaphor, *noun* as the analogy that is based on shape, look, or sound of an object, *verb* as the analogy of the action or movement being performed (Fishkin & P., 2004). The metaphors of *noun and verb* can also be combined to describe an analogy, and lastly is *full*, in which there are no metaphors because the virtual system is built based on the physical system (Fishkin, 2004).

However, Hornecker and Buur (Hornecker & Buur, 2006) argued against Ishii and Ulmer’s theory on TUI by stating that tangible interaction is not only about

controlling digital data through tangible appliances but also as remote control of the real world through the user interface design. They placed the tangible interaction in a larger design space, in a broad range of systems and interfaces through exploiting the richness of bodily movements relying on embodied interaction, tangible manipulation and physical representation of data, embeddedness in real spaces and digitally augmented physical spaces (Bongers, 2002; Buur, Jensen, & Djajadiningrat, 2004) . To support these arguments, they developed a framework to explore the tangible interaction through four different perspectives (Hornecker & Buur, 2006):

- ***tangible manipulation*** refers to the material representations with distinct tactile qualities, which are typically physically manipulated in tangible interaction
- ***spatial interaction*** refers to the fact that tangible interaction is embedded in real space and interaction, therefore, occurs by movement in space
- ***embodied facilitation*** highlights how the configuration of material objects and space affects and directs emerging group behaviour
- ***expressive representation*** focuses on the material and digital representations employed by tangible interaction systems, their expressiveness, and legibility

In the light of these TUI and tangible interaction theories, HCI researchers could capture and communicate mental models through interaction design concepts, including sketches (Shaer & Jacob, 2009), storyboards (Truong, 2006), conceptual designs (Benyon, 2013) and more recently through physical prototyping kits such as Arduino, integrating computational power in physical devices that people can physically interact with and move in space (Greenberg & Fitchett, 2001; Hartmann

et al., 2006). One such landmark example is the marble answering machine where the marbles, placed in a dish are mapped to recorded messages or missed calls (Bishop & Durrell, 2009). However, there are limitations in terms of using a standard set of vocabularies to communicate the metaphors of physical interaction design and mental models.

### 2.5.2 Embodiment in HCI

Embodiment typically refers to people being living, feeling, bodily entities situated in a physical world (Marshall & Necker, 2013). It also described an important theory exploring bodily interactions with behaviour-responsive, adaptive architecture which integrates the body, cognition and physical world. Due to this universal understanding of the role of the body for cognition, it has been applied in many disciplines including sociology and HCI (Dalton, Zeidman, McCormick, & Maguire, 2018),

In embodied cognition theory, Dalton, et al. (Dalton et al., 2018) described how the mind and the body work separately. This understanding has been used in the computationalism which interprets the brain as a computer machine and embodiment as part of the cognitive system. However, phenomenologists rejected this prior theory and redefined it as cognition emerging from the embodiment and more important with the involvement of the active body in the world, through both physical objects and social interactions (Marshall & Necker, 2013). The latter concept of phenomenology has been widely applied in embodied cognitive science.

An interesting concept derived from embodied cognition theory is image schemata: the representations of repeated dynamic patterns of physical interactions structured in the way people understand the world (Hurtienne, 2009). There are

over 30 groups of image schemas (Hampe & Grady, 2005; Lakoff, 1987). One of it is containment that describes the image schemes of a container, in and out, content, full, empty and surface. The metaphors associated with image schemata create links between the target and source domain, i.e., “more is up” linking quantity with verticality (Lakoff, 1987) which can also be explored through linguistic analysis, as previously applied to the design of tangible interfaces (Hurtienne, 2009).

### 2.5.3 DIY Kit Representation of Mental Model

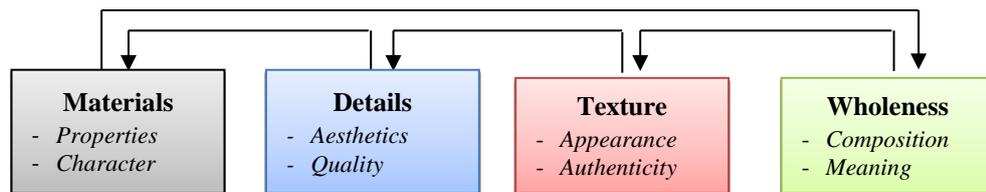
Over the last decade, there has been a growing HCI interest in design kits including those for the making of physical objects (Kuznetsov & Paulos, 2010) making of sensors (Kuznetsov et al., 2011), as well as the making of both low (Kuznetsov & Paulos, 2010) and high-tech devices (Lakoff, 1987). Such kits consist of the collection of basic components, electronics or non-electronics such as paper, or cards, which people can interact with to simulate interaction or to assemble them into an artefact. Much of this work has focused on low tech artefacts (S Kuznetsov et al., 2014), with much less research exploring the making of high tech one (Sas & Neustaedter, 2017), or the understanding of infrastructures, i.e., through Lego blocks (Maxwell et al., 2015). Framed under the DIY umbrella term, most such findings suggest that people enjoy working with their hands in the making of artefacts (Sas & Neustaedter, 2017). In order to be effective, physical design kits should allow for analogies between the models that can be built using them, i.e., assembled representations of the system, and what they model, i.e., the system (Hardy & Alexander, 2012). One useful approach to the development of such physical kits is the material-centred design framework consisting of four dimensions: materials, details, texture, and wholeness (Wiberg & Mikael, 2014).

Hardy and Alexander (Hardy & Alexander, 2012) outlined the design requirement for a DIY toolkit, which firstly is the design toolkit should match the current hardware or software as well as support the interactivity, content, geometries in various system life span. Secondly, the kit should also be supported by the abstraction of the display. For instance the surfaces of the physical object and the desired project display such as a door, table, and walls. The suitability and ease of abstraction are significant for the user to communicate and demonstrate the design kit and for the researcher to capture their mental models. The toolkit can be designed as software, hardware, or a physical representation (Hardy & Alexander, 2012).

Hardy and Alexander (Hardy & Alexander, 2012) applied these design requirements in their UbiDisplay, design toolkit which is an interactive surface using projection and a depth camera that can be used by users to get the idea to program in ubiquitous projection. Another example of the DIY toolkit was designed by Muszynska, Michels, and Zezschwitz (Muszynska, Michels, & Zezschwitz, 2018) to explore the user's mental model towards the privacy permission request on mobile phones. They designed a physical kit based on the physical embodiment of data type approach to support their research aim. They materialised the data on the typical smartphone into a DIY kit based on the physical embodiment of data type through permission cards, boxes, also info-cards and label those as x, y, and z and conducted a focus group study using those materials. The findings indicate that the materialisation contributed to the non-experts understanding of a complex topic of personal data privacy.

### 2.5.3.1 Material Exploration

Wiberg (Wiberg & Mikael, 2014) proposed a framework for the material-centred interaction design method (**Figure 2.3**), which could be used to inform the design of a physical representation or DIY kit. There are four interrelated dimensions in his framework: *materials*, *details*, *texture*, and *wholeness*.



**Figure 2.3: Framework for the material-centred interaction design method (Wiberg & Mikael, 2014)**

First is to focus on the selection of materials to represent the system. There are two elements associated with materials. The first is to have an in-depth understanding of the properties' of the materials in order to ensure that these can properly demonstrate the system function and further support the system design (Wiberg & Mikael, 2014). The other is the materials' character which describes the functionality of each material in the system flow. The craftsmanship of the materials to visualize the system is also significant. Second is to focus on the wholeness to ensure that the composition of the materials is able to provide support for digital exploration, and for the interpretation of the meaning of the material artefact and how it matches the real function of the system (Jung & Stolterman, 2012). The third is to focus on the texture, which communicates the appearance of the material properties such as the surface. The appearance of the texture is important in order to show the look and the feel of the compost materials. The authenticity of the design is also vital to connect the materials,

their composition, as well as appearance so that digital systems can be represented by normal objects of everyday life.

The framework also highlights the importance of focusing on the details of the implementation of the designed materials from the materials' selection, arrangement, composition until the analysis.

Section Summary: The exploration of users' mental models through the concepts of physical interaction and embodiment could be achieved through the development of a DIY kit. This method is valuable to materialise the complex Blockchain infrastructure and Bitcoin cryptocurrency in the form of physical representation or DIY kit to explore the opportunities to design trust in the Bitcoin transactions.

# Chapter 3

## Methodology

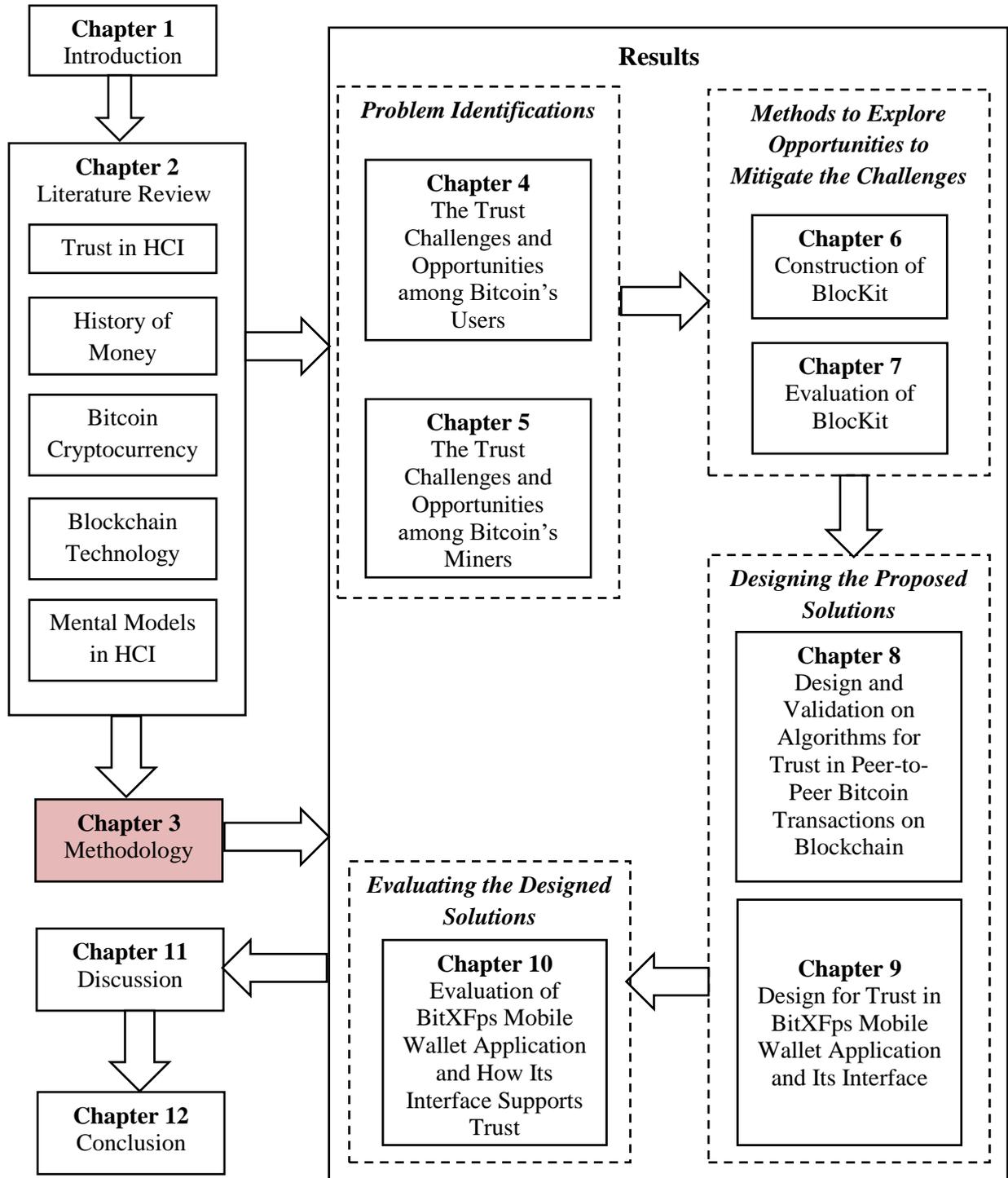


Figure 3.1: Chapter 3 of Thesis Structure

### 3.1 Introduction

The methodology adopted for this thesis is qualitative research. In order to understand the routines of Bitcoin stakeholders as well as to identify their trust challenges in using Bitcoins, the interview method was employed. Then, based on the identified trust challenges, BlocKit, a physical Blockchain kit was built to explore the opportunities to design for Bitcoin trust. The BlocKit was employed in a participatory workshop with experienced Bitcoin Blockchain users. The outcomes of this workshop consisted of a set of principles to design for Bitcoin trust, later used to inform the design of an algorithm as well as a mock-up prototype for the Bitcoin wallet app (BitXFps) embedding trust in Bitcoin peer-to-peer transactions. Those algorithms and app were evaluated by experienced Bitcoin Blockchain users under the framework of trust. Descriptions of each employed method are further detailed in this chapter.

### 3.2 Research Paradigm in HCI

Kuhn (Kuhn et al., 1970) defined a research paradigm as a specific way to represent the cognitive work to be shared by the scientists while solving problems in their own fields, as well as their commitments, beliefs, or values. Additionally, Schwandt (Schwandt, 2001) described research paradigm as a shared world view that represents the beliefs and values in disciplines and guides how problems are solved. There are four important elements in HCI research paradigms that are interdependent and grounded in deeper common conceptualisations as described below (Kuhn et al., 1970):

- the common understanding of the salient properties of interaction
- types of questions that appear to be both interesting and answerable about those properties of interaction

- a set of broad procedures which can be used to provide warrantable answers to those questions
- a common understanding of how to interpret the results of these procedures
- this set of elements is designed into two common research paradigms which are positivism and interpretivism

### 3.2.1 Positivism versus Interpretivism

Positivism is described as a structured research work which generalises the empirical findings by replicating the methods and measurements from prior work (Chilisa & Kawulich, 2015). Positivist researchers' works are underlying the set of theoretical propositions or hypotheses to be tested through the analysis of empirical data. The aim of the research is to produce an exact representation of reality, unbiased and value-free (Chilisa & Kawulich, 2015). However, Eklundh and Lantz (Eklundh & Lantz, n.d.) argued that in HCI, positivism is about analysing human as an object by ignoring the human differences. There are needs and preferences of human beings as end-users that need to be understood about how they used the technology as a tool in their daily task rather than focusing on the technical characteristics of the technology (Gay & Hembrooke, 2004).

In contrast, an interpretivist research paradigm is known as anti-positivism, and it is commonly related to human studies which aim for understanding and explaining processes rather than objective facts (Tharakan, 2006). In HCI, the aim of interpretivism is to understand and describe human nature in interaction with technology. Interpretivist approaches are subjective and constructed through the researcher's interpretations and study of participants (De Villiers, 2005). This

research paradigm is applicable to studies related to complex human being or other social phenomena (De Villiers, 2005).

These two research paradigms can also be contrasted. While positivism research is conducted to test hypotheses, interpretivism investigates research questions to understand the phenomena and situations (Thanh<sup>1</sup> and Thanh<sup>2</sup>, 2015). While positivism more commonly employs quantitative methods, the subjective aspect of interpretivism research makes it a suitable paradigm for qualitative methods (Goldkuhl, 2012). In addition, while the reliability of positivist research is measured by statistical tests, the reliability of interpretivist research is estimated based on the accuracy with which the findings reflect the natural settings or people's daily practices, and often benefits from triangulation of multiple methods of data collections (Thanh<sup>1</sup> and Thanh<sup>2</sup>, 2015). **Table 3.1** further describes the comparisons between positivism and interpretivism (Pizam, Chon, & Mansfeld, 1999).

<b>Assumptions</b>	<b>Positivism</b>	<b>Interpretivism</b>
Nature of reality	Objective, tangible, single	Socially constructed, multiple
Goal of research	Explanation of strong predictions	Understanding weak predictions
Focus of research	What is the general average and representative	What is specific, unique and deviant
Knowledge generated	Laws absolute (time, context and value-free)	Meaning relative (time context, culture, value bond)
Subject/ Researcher relationship	Rigid separation	Interactive, cooperative, participative
Desired information	How many people think a specific thing or have a specific problem	What some people think and do, what kind of problems they are confronted with, and how they deal with them

**Table 3.1: The basic differences between positivism and interpretivism (Pizam, Chon, & Mansfeld, 1999)**

### 3.3 Research Method

There are several research methods applied within and beyond the positivism and interpretivism that are described in this section.

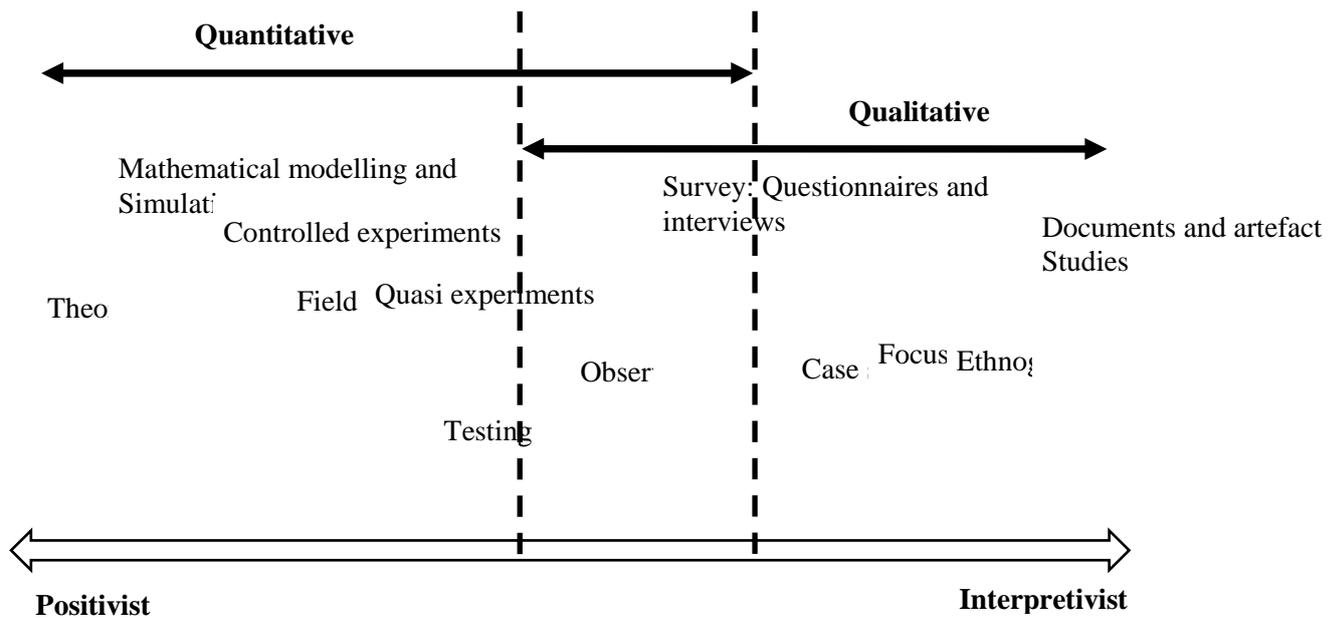
#### 3.3.1 Quantitative versus Qualitative

Amongst social scientists, the debate on the significance and applicability of quantitative and qualitative research methods have been longstanding (Bryman, 1984). These arguments reflected the pros and cons of both methods, and also emphasised their suitability for different types of studies and research paradigms (Bryman, 1984). Positivism is commonly conducted in the quantitative research method to test pre-determined research hypotheses (De Villiers, 2005). However, in human study and interactions with technology particularly in the context of trust in Bitcoin transactions, it is less appropriate to generate hypotheses regarding human behaviour. In HCI research, quantitative methods are useful for measuring the usability of the system or for comparing the use of different types of technology or interfaces (Cairns & Cox, 2008). There are several quantitative research methods, such as those for theorem proving, mathematical modelling and simulation, controlled experiments, field experiments, quasi-experiments and testing (**Figure 3.2**). The data analysis techniques for quantitative methods often involve statistics, and there are two types of statistical analysis associated with quantitative research which are descriptive and inferential statistics (Elst, 2013). Descriptive statistics are used to describe the basic features of the data in a study that enable researchers to understand the data (Elst, 2013). In contrast, inferential statistics allow an in-depth understanding of the data to decide on the pre-determined hypotheses to be tested in subsequent studies (Cairns & Cox, 2008).

Mertens (Mertens, 1998) described qualitative research as naturalistic interpretive science involving methods such as case study, focus group, ethnography or artefact studies (**Figure 3.2**). In HCI, quantitative research is often limited to measure the times and error rates of human interactions with technologies, but the scopes are broader in qualitative research. The latter places emphasis on people's behaviours, movements, cognitive work and reasons for actions when interacting with technologies. These, in turn, provide richer and contextualised data (Beyer & Holtzblatt, 1998) supporting the understanding of novel and complex phenomena.

However, the findings from qualitative research are not generalisable (Maykut & Morehouse, 1994) and cannot be used to test hypotheses (Popper, 1959) which are core to quantitative methods (Popper, 1959). The quantitative methods require a structured and standard procedure to measure data. Hence, they are fit for measuring the level of people understanding before and after interacting with the technologies. In contrast, qualitative analysis does not report numbers but subjective data in the form of users' subjective accounts, narratives and experiences (Yilmaz, 2013).

Although most elements in positivism and interpretivism reflect the quantitative and qualitative research method respectively, there are however overlapping spaces in between these two research paradigms, known as the mixed methods, as described in **Figure 3.2**.



**Figure 3.2: Research Strategies (De Villiers, 2005)**

### 3.3.2 Mixed Methodology

The combinations of qualitative and quantitative methods in different phases of the research process are known as mixed methods that are commonly employed under the pragmatism paradigm (Tashakkori & Teddlie, 1998). For instance, in a questionnaire, the data collection through mixed methods could involve both closed-ended and open-ended questions. The collected questionnaire will be analysed by two techniques, such as factor analysis of the Likert scaled items as well as using a constant comparative method for the narrative responses to the open-ended questions (Tashakkori & Teddlie, 1998). The types of studies that commonly employ mixed methods are sequential studies, parallel or simultaneous studies, equivalent status designs and designs with multilevel use of approaches (Tashakkori & Teddlie, 1998). Sequential studies are those where researchers begin with a

qualitative research phase, followed by a quantitative one, or vice versa (Tashakkori & Teddlie, 1998). There are two phases of studies conducted separately.

In parallel or simulation study designs, researchers tend to combine quantitative and qualitative research methods at the same time (Tashakkori & Teddlie, 1998). For example, in a study for measuring the usability and trust towards the interface of the system, there would be closed-ended questions to measure the interface based on the usability and trust models, and open-ended questions to capture users' feedback with the system interface. The equivalent status design involves using both quantitative and qualitative approaches to understand the phenomenon under study (Tashakkori & Teddlie, 1998), while the design with multilevel requires different types of methods at different levels of data aggregation (Tashakkori & Teddlie, 1998). For example, in education research, the data could be analysed quantitatively at the course and program level, but also qualitatively at the faculty and university level.

All collected data from the qualitative, quantitative or mixed method are required to be analysed with rigour and structure.

### 3.4 User-centred Design and User Participatory Design

User-centred design is an iterative approach to design and develop software or products by expert teams that focus on user needs throughout the product life cycle. Commonly, the teams consist of professionals with different skills and backgrounds such as information architects, visual designers, developers, project managers, or technical writers. They collaborate to strategise, plan, create and implement a project (Norman & Draper, 1986). Their main focus is to create interfaces, artefacts, products and services that are applicable, appropriate and accessible to as many users as possible within the

constraints of the design specifications (Keates, Clarkson, Keates, & Clarkson, 2003). Due to the aim to attend the users' needs, the final output of this design process will be used for the targeted audience.

Similarly, participatory design aims to develop technologies through the cycles of requirements gathering, prototype development, implementation and evaluation with the close involvement of end-users and stakeholders (Sharma et al., 2008). Their involvement is either to contribute to the design and content development process, or in order to manage the entire development processes on their own. It requires users' active participation in the process as co-designers by empowering them to propose and generate design alternatives themselves (Schuler & Namioka, 1993). This approach can be seen as an attempt to better understand and involve real users, and is imperative for creating more appropriate, and user-friendly products or services (Lindgaard et al., 2006; Muller & Druin, 2002).

Although both methods focus on building solutions for the targeted end-users, the approaches to conduct studies involving either of them are dissimilar. For example, in the case of user-centred design, the roles of researcher and designer to investigate the user requirements and design the solutions are often interdependent. However, in the case of participatory design, the end-user often acts as the designer, while the researchers are responsible to build appropriate tools and infrastructure to fulfil and facilitate the design work. In my view, both approaches are relevant to design the system for end-users, but the concern is to select the suitable users to be involved in each particular research stage.

### 3.5 Usability Inspection Methods

Nielsen and Mack (Nielsen & Mack, 1994) described usability inspection as a set of methods to evaluate user interface designs. The main focus of these methods is to identify the usability issues in interface design in order to address the most severe ones (Nielsen 1994). Under the usability inspections umbrella, there are eight associated methods described as follows (Nielsen 1994; Nielsen & Mack, 1994):

- **heuristic evaluation** is the most informal method to evaluate the design according to established principles, which is normally referred to as heuristics
- **guideline reviews** are inspections where the interface design is checked for conformance with a comprehensive list of usability guidelines
- **pluralistic walkthroughs** are meetings where users, developers, and human factors experts step through a scenario, discussing usability issues associated with dialogue elements involved in the scenario steps
- **consistency inspections** have designers representing multiple projects inspect an interface to see whether it does things in a way that is consistent with their own designs. Thus, consistency inspections are aimed at evaluating consistency across the family of products that have been evaluated by an inspection team
- **standard inspections** have an expert on some interface standard inspect the interface for compliance. Thus, standards are aimed at increasing the degree to which a given interface is in the range of another system on the market that follows the same standards
- **cognitive walkthroughs** use a more explicitly detailed procedure to stimulate a user's problem-solving process at each step in the human-computer dialogue, checking to see if the simulated user's goals and memory for actions can be assumed to lead to the next correct action

- **formal usability** inspections use the six-steps procedures (planning, kick-off meeting, preparation phase where inspectors' review - the interface individually, the main inspection review - when the inspectors' lists of usability problems are merged, and follow-up phase where the effectiveness of the inspection process itself is assessed) with strictly defined roles to combine the heuristic evaluation and a simplified form of cognitive walkthroughs
- **feature inspections** list sequence of features used to accomplish typical tasks, checks for long sequences, cumbersome steps, steps that would not be natural for users to try, and steps that require extensive knowledge/ experience in order to assess a proposed feature set

Each method described above is dedicated to different aims in usability testing. The testing processes could be ranged from complex to simple. For instance, formal usability testing requires multiple steps and combinations testings to be conducted in individual and group inspections (Nielsen, 1994), while pluralistic walkthroughs and consistency inspections are described as an unstructured method that requires the usability tester to collaborate in the tests (Nielsen, 1994). The heuristic evaluation, cognitive evaluation, feature inspection, standard inspection also guideline reviews require the tests to be conducted individually with different guidelines and procedures. Both heuristic evaluation and guideline review are conducted based on a specific principle: the testers need to evaluate the design based on a given list of principles. For instance, guideline review testing is associated with 1000 types of principles (Nelsen, 1994) making it the most complex method.

### 3.6 Methodological Approach in this Thesis

The research paradigm for this thesis is interpretative and consists of 5 studies which can be categorised into seven sections: understanding the Bitcoin stakeholders, constructing and evaluating the DIY Kit, designing and evaluating the trust algorithm for Bitcoin transaction, designing and evaluating the user interface for the Bitcoin wallet app (**Table 3.2**).

#### 3.6.1 Interview

Boyce and Neale (Boyce & Neale, 2006) defined interviews as a qualitative research technique which involves conducting intensive individual interviews with a small number of respondents to explore their perspectives on a particular idea, program or situation. It is a way to capture a great understanding of users' experiences, perceptions, and values such as trust, by requiring the interviewer to ask specific questions while remaining open to exploring participants' points of view (Qu & Dumay, 2011). Interviews can be conducted in three different formats: structured, semi-structured, or unstructured. The structured interviews consist of a set of questions in a specific order that will be delivered to all interviewees (Qu & Dumay, 2011). The data analysis enables the researchers to make comparisons among the interviewees' answers. In contrast, the unstructured interview has no predetermined set of questions and are often conducted in informal settings. The data analysis could be harder due to the variety of questions for different interviewees and the results are less reliable compared to the structured interview (Qu & Dumay, 2011). However, the structured interview may limit the explorations of the interviewees' viewpoints (Boyce & Neale, 2006).

Therefore, for this research, the semi-structured interviews that consist of both structured and unstructured questions were applied. A set of interview guidelines was prepared for each of the five studies. At the same time, additional questions related to the topic discussed during the interviews were asked to clarify or further describe certain issues. (**Chapter 4, Chapter 5, Chapter 7, Chapter 8, Chapter 10**).

### 3.6.2 User Participatory Design

As discussed in 3.4, user participatory design is a method involving users directly with the research in order to support the design of a system. HCI, research focusing on the design for complex systems such as Blockchain can benefit from participatory design methods.. For instance, Nissen et al. (Nissen et al., 2018), conducted a participatory design workshop by using the cryptocurrency named GeoCoin to engage novice users in designing smart contract applications for Blockchain. In that workshop, the participants were given an opportunity to experience the location-based platform application that was built with GeoCoin Blockchain and, based on their experience, users explored the opportunity to design another type of applications on top of the GeoCoin Blockchain.

In this research, the participatory design method was also used by experienced Bitcoin Blockchain users to explore the design opportunities for Bitcoin trust in Blockchain as well as to evaluate the users' trust in the designed algorithms and the Bitcoin mobile application interface.

	<i>Understanding the Bitcoin Stakeholders</i>		<i>Constructing BlocKit</i>	<i>Evaluating the BlocKit</i>	<i>Designing the Trust Algorithm for Bitcoin Transaction</i>	<i>Evaluating the Trust Algorithm for Bitcoin Transaction</i>	<i>Designing the User Interface for BitXFps</i>	<i>Evaluating the Trust in the BitXFps User Interface Design</i>
	Study 1	Study 2		Study 3		Study 4		Study 5
Chapter	4	5	6	7	8	8	9	10
Research Objective	1	1	2	2 and 3	3	3	4	5
Research Paradigm	Interpretative	Interpretative		Interpretative		Interpretative		Interpretative
Participants	Bitcoin users	Bitcoin miners		Bitcoin Blockchain experienced users		Bitcoin Blockchain experienced users		Bitcoin Blockchain experienced users
Data Collection Method	Interviews	Interviews		Interviews		Validation interviews		Trust evaluation; workshops; Interviews
Data Analysis Techniques	Hybrid approach: <i>Inductive and deductive thematic analysis</i>	Hybrid approach: <i>Inductive and deductive thematic analysis</i>		Hybrid approach: <i>Inductive and deductive thematic analysis</i>		Hybrid approach: <i>Inductive and deductive thematic analysis</i>		Hybrid approach: <i>Inductive and deductive thematic analysis</i>
Key Topic	Bitcoin users; Blockchain; trust; motivations; risks	Bitcoin miners; Blockchain; trust; motivations; risks	Blockchain; material exploration; image schemata; DIY kit	Blockchain; infrastructure; mental models; DIY kit; trust	Bitcoin; Blockchain; algorithm; trust	Bitcoin; Blockchain; algorithm; trust	Blockchain; Bitcoin wallet; Blockchain; user interface; trust	Blockchain; Bitcoin wallet; evaluation; user interface; trust

**Table 3.2: Overview of studies conducted in the thesis**

### 3.6.3 Trust Evaluation

As discussed in 3.5, heuristic evaluation is one of the elements under usability inspection methods that commonly aimed to locate the usability problem in interface design. It is usually applied to the set of generic usability principles to evaluate the website user interface (Nielsen, 1994). However, the evaluation is not limited to the Nielsen generic principles. It can also be applied to evaluate specific user interface applications with tailored principles and taxonomy. For example, Pinelle, Wong, and Stach (Pinelle, Wong, & Stach, 2008) had customised the heuristics for usability design principles for a video game design after conducting evaluations with 108 PC games. This method can also be applied to measure other key aspects of interface design, such as trust. For instance, Sillence et al. (Sillence et al, 2006) in their work to build the trust framework for web-based health, advised the employment of trust principles as the heuristic guidelines to evaluate user's trust in the interface design.

#### *3.6.3.1 Expert Reviews*

The expert reviews are conducted based on someone's past experience and knowledge on a particular tool. The outcome of the expert reviews normally will expand the guidelines for the evaluated tool (Harley, 2018).

In this thesis, a proposed guideline to design for trust in peer-to-peer Bitcoin transactions has been outlined based on the framework of trust inducing features for web design (Wang & Emurian, 2005) and from the findings in Study 3 that focused on the design for trust principles. This guideline was used by the recruited experienced Bitcoin users to evaluate the trust design for BitXFps app (**Chapter 10**).

### 3.6.4 Qualitative Data Analysis Techniques

The technology is rapidly changing and, for instance, cryptocurrency comes in different types and it offers diverse ways for people to use it. These abstractions of technological interactions had challenged researchers to look into the values underpinning trust in technology. HCI researchers tend to focus on understanding the qualities of a particular technology and how people use it in their lives, think and feel about it. In qualitative methods, there are no required hypotheses to be determined at the beginning of the study (Strauss et al., 1964) but the new theory emerged from the data sets. The qualitative data sets need to be fully transcribed and coded. The coding process involved six iterative processes known as thematic analysis that are described as follows (Braun & Clarke, 2006):

**Step 1:** Familiarising oneself with your data – re-reading the transcripts and making notes

**Step 2:** Generating initial codes – systematically coding the entire datasets and collating data that is relevant to each code

**Step 3:** Searching for themes – generating codes into candidate themes for further analysis

**Step 4:** Reviewing themes – checking whether the themes work with the data and creating a thematic map of analysis

**Step 5:** Defining and naming themes – refining the themes and the overall narrative iteratively

**Step 6:** Producing the report – which will, in turn, require a further level of reflection on the themes. The narrative and the examples used to illustrate the themes

The thematic analysis could be conducted in two ways, inductively or deductively. The inductive thematic analysis is applied when the researcher has little or no predetermined theory or framework for identifying the themes (Patton, 1990). In contrast, deductive thematic analysis is associated with a structured or predetermined framework used in analysing the data sets (Boyatzis, 1998). Basically, the researchers create their own structure or theories on the data and use these as a guide to analyse the data. This approach is particularly useful for the researchers who, after they identified the research questions and desired themes, can then to look at the similarities and differences in the data. Even though the latter thematic analysis is easier to be conducted, the predetermined thematic framework could lead to bias and limit the interpretation of data.

Hence, for this research, we applied thematic analysis by combining both inductive and deductive methods which is known as a hybrid approach (Fereday & Muir-Cochrane, 2006). This method integrated both types of thematic analysis by using the existing theory for the deductive coding while new theory grounded in the empirical data, contributed to the inductive coding (**Chapter 4, Chapter 5, Chapter 7, Chapter 8, Chapter 10**).

### 3.6.5 Triangulation

Patton (Patton, 1999) defined triangulation as qualitative research that employs multiple methods or data sources to acquire an in-depth understanding of phenomena. There are four types of triangulation that have been identified: data source triangulation, theory triangulation, investigator triangulation, and method triangulation (Denzin, 2006; Patton, 1999). The data source is when the researcher recruits different types of participants in a study including, for instance, those of

different race, religion, and expertise in order to gain multiple perspectives and validation of data (Denzin, 2006). Theory triangulation uses more than one theory to interpret the data, while investigator triangulation is a collaboration of more than one researcher in the same study to provide multiple observations and conclusions (Denzin, 2006). Method triangulation involves multiple methods of data collections in the same study (Polit & Beck, 2016).

This PhD project employed triangulation methods throughout, alongside several different methods such as interviews, workshops, and survey in five interrelated studies to support the objectives of this PhD research.

### 3.7 Chapter Summary

This chapter presented a thorough description of the research methodology. We linked all results from understanding the Bitcoin stakeholders (Chapter 4 and 5) to constructing and evaluating the methods to explore the design for trust (Chapter 6 and 7). It also describes the design and evaluating approaches for the trust algorithm for Bitcoin transactions (Chapter 8), and finally the details of the design and trust evaluation for the Bitcoin mobile application user interface (Chapter 9 and 10). The detailed descriptions of each study are further outlined in the Research Method sections and related Result chapters (Chapter 4, 5, 7, 8 and 9).

# Chapter 4

## The Trust Challenges and Opportunities among Bitcoin Users

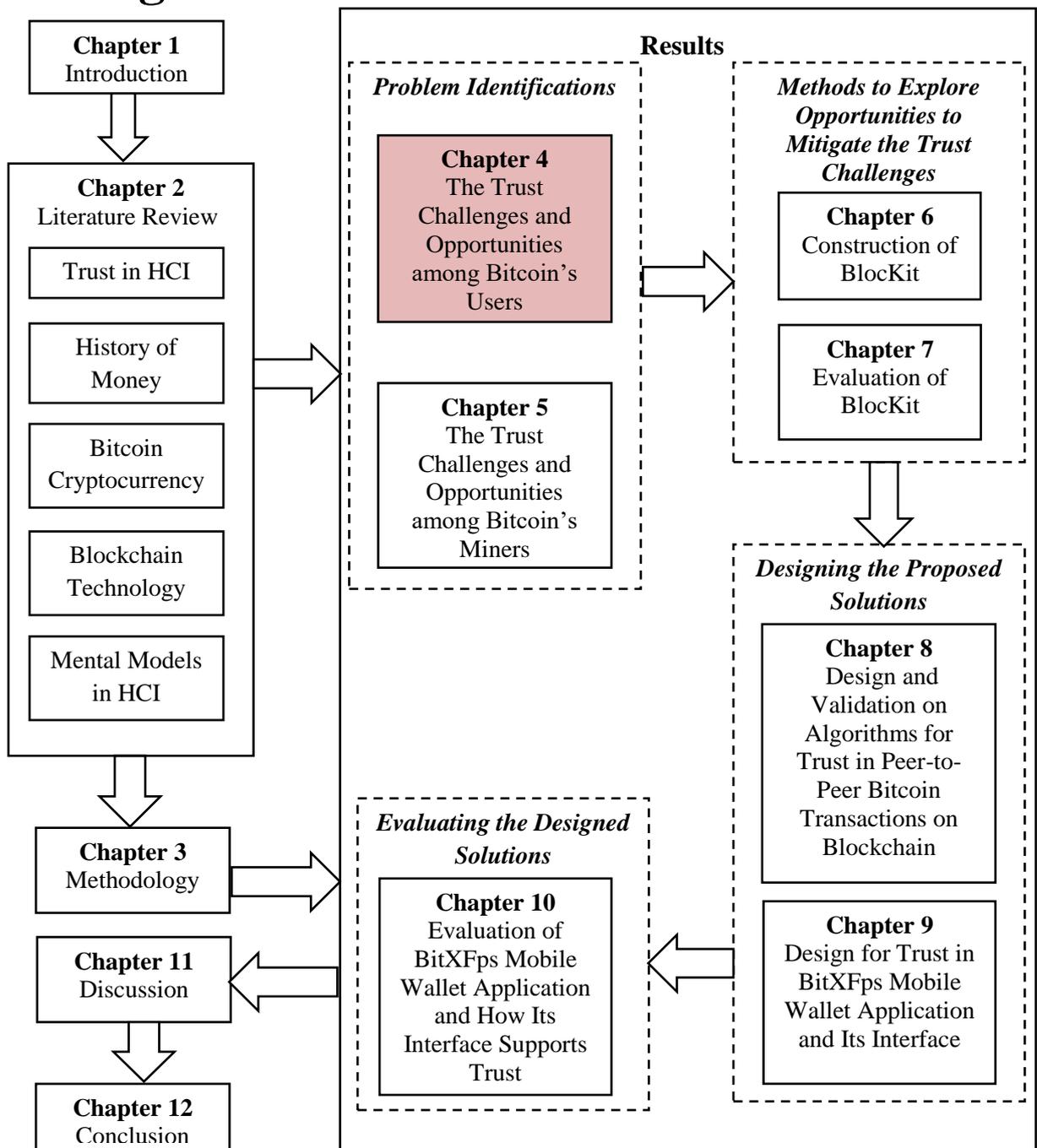


Figure 4.1: Chapter 4 of Thesis Structure

## 4.1 Introduction

This chapter presents the report on the explorations of people's motivation and experience with Bitcoin. It is known as the first cryptocurrency which has received increasing interest over the last five years. Built upon a decentralised peer-to-peer system called Blockchain, it supports transparent, fast, cost-effective, and irreversible transactions, without the need for trusting third party financial institutions. The Blockchain technology has steered increasing research interest predominantly in the areas of cryptography, security, and peer-to-peer computing. However, there are limited empirical researches that report about people's motivations and experience with Bitcoin and their trust-related issues.

In this regard, a study on the exploration of people's motivation, experience and trust on Bitcoin cryptocurrency has been conducted by addressing the following research questions:

- *what are the motives for early adoption and use of Bitcoins? How do people learn about Bitcoin and how do they use Bitcoins for?*
- *how different Blockchain characteristics impact on the various dimensions of trust?*
- *what are the main trust challenges and how do people attempt to mitigate them?*

It reports on interviews with 20 Bitcoin users in Malaysia about their experiences and trust challenges in using Bitcoin. The study advances the HCI theories on trust by identifying main Bitcoin characteristics and their impact on trust, such as decentralisation, unregulation, embedded expertise, and reputation, as well as transactions' transparency, low cost, and easiness to complete. Based on the outcomes, the study discusses the motivations of the users, the impact of Blockchain characteristics on users' trust, insecure transactions, the risk of dishonest traders and its mitigating

strategies. It concludes with theoretical implications on the construction of the theories on a model of trust for Bitcoin users, the paradox of unregulation and the challenge of pseudoanonymous transactions. Then finally, the chapter addresses the design implications including support for the transparency of two-way transactions, tools for materialising trust, and tools for supporting reversible transactions.

## 4.2 Research Method

Study 1 recruited 20 Bitcoin users, 18 male, 2 female, (mean age 30, range 21-50). Six participants had less than 6 months experience of using Bitcoins, 8 participants have between 6 months and 2 years, while the remaining 6 have more than 2 years. In terms of educational background, half of the participants had Bachelor degrees, 7 were school leavers, and 3 had Master degrees. Participants had a broad range of occupations: 8 in administrative roles, 4 in financial and marketing sector, 3 school teachers, 2 unemployed, 1 in medical field, 1 in IT and 1 student. Each participant was rewarded RM50 (equivalent to £10 in Malaysian currency). Participants were recruited from five Facebook and Telegram groups of Malaysian Bitcoin users. Malaysia offers a specific opportunity for the exploration of Bitcoin practices. On the one hand, despite five decades of economic growth, it is still a developing country with the increasing inflation rate, underdeveloped democracy and a financial system which is now under the scrutiny of law enforcement. On the other hand, Malaysia experiences a massive growth of remittance and payment market, and interest in cryptocurrency, being in 2016 the first developing country considering Fintech regulation (Central Bank of Malaysia, 2016). Over the last year, it also ranked fourth on Bitcoin searches on Google Trends (Young, 2016).

The invitations for taking part in the study were both publicly posted and privately sent to the most active members in each of the online groups. The study also applied snowball sampling so that six more participants were introduced by the interviewed ones. The semi-structured interviews have been conducted between October 2015 and December 2015, to explore users' motivation, understanding and use of Bitcoin. The participants were asked: "*why are you interested in Bitcoin*", "*how did you learn about Bitcoin*" and "*which are the benefits and challenges of using Bitcoins*". They were also asked about users' challenges and trust-related issues: "*what are the challenges that you face when using or engaging with Bitcoin technology*", and "*how much trust do you have in Bitcoin technology*", and followed up with additional questions on perceived security and anonymity. The study also explored participants' perception of risk and their mitigation strategies: "*did you experience any fraud*", and "*will you take any actions to prevent that in the future*".

The interviews took place via Skype or phone. They lasted for at least an hour, were audio recorded and fully transcribed. The analysis involved a hybrid approach where existing concepts were used for the deductive coding while new concepts grounded on the empirical data, contributed to the inductive coding (Fereday & Muir-Cochrane, 2006). The deductive coding included concepts from the HCI literature on trust such as technological, social and institutional dimensions of trust (Sas & Khairuddin, 2015), factors of user's trust in technology such as credibility, ease of use, and risk (Corritore et al., 2003), and properties warranting trust between technology users such as temporal, social and institutional embeddedness, as well as credibility, integrity and benevolence (Riegelsberger et al., 2005). In this study, the concepts related to Blockchain's characteristics such as decentralisation, unregulation, pseudo-anonymity, as well as transparent and irreversible transactions were also used. The coding list was iteratively

refined in the light of the interview data, as new codes emerged under the theme of motivation, insecure transactions and risk mitigating strategies.

### 4.3 Findings

The report of the findings begins with outlining users' motivation for engaging with Bitcoin technology, followed by a description of its key characteristics and their impact on users' trust. In particular, the study highlights the issue of insecure transactions and the associated human and technology-related risks. The study further unpacks the risks of dealing with dishonest traders, and the mitigating strategies for addressing them.

#### 4.3.1 The Motivations for Using Bitcoin Currency

This section highlights the motivation of end-users, people with limited knowledge of Bitcoin technology, who adopt and engage in the use of Bitcoins. The motivation and perception of early adopters towards Bitcoins can be grouped according to Davis' technology acceptance model (Davis, 1989) in perceived usefulness, and ease of use. The study further describes the perceived usefulness of Bitcoins as an external motivational factor and its key economic rationale.

##### *4.3.1.1 Economic Rationale*

The economic aspect captures people's distrust in financial institutions and the government legitimising them. Several participants referred to the importance of protecting one's savings in the face of an unstable economic climate, dominated not only by inflation but also by governments' decisions to control personal bank account holders' money and their movement (Christin, 2012). For example, the following quote is illustrative for a quarter of the participants: *"From what I learned from the Cyprus crisis, governments and banks have the authority to take*

*your money from your account [...] the trust in financial institution is gone forever. So I looked for alternatives and found Bitcoin to keep the savings” [P16].*

This outcome provides support for the security motive for acquiring money and Bitcoins’ perceived value for providing safety when people distrust the world and the future particularly in the context of inflation and economic downturn: *“currently our currency is falling and I am worried. As a backup plan, I converted my money in gold or Bitcoins, which are not influenced by any big parties or power” [P8].* This is interesting as it reflects the assumption of gold as a commodity, which wrongly conflates gold’s long-run price stability with the absence of power for regulating its price: while such power does not need to belong to centralised banks, it still requires government’s authority (Bordo, 1981).

A third economic reason underpinning the adoption of Bitcoins is speculation on their future value. Almost half of participants share this view: *“I keep my saving in Bitcoins [because] their future value will increase over time” [P11].* In such cases, participants purposely explored alternative means of exchange for replacing their volatile fiat currency in order to both protect savings and more importantly, to invest for future income.

#### *4.3.1.2 Social Learning*

Findings indicate that in order to learn about the Bitcoin currency, participants leverage the emerging social network of Bitcoin users. This social aspect underpinning the initial motivation of Bitcoin’s early adopters include online communities where most of the participants have heard for the first time what Bitcoin currency is: *“The first time I heard [about Bitcoins] was from the Reddit*

*forum*” [P1]. After finding out about the Bitcoin currency and its potential value, participants described their efforts to learn more through self-guided online research: “*First I read about Bitcoin online in 2009, [and] in 2013 I could see the price rising up, so I started to learn more about*” [P7]. An additional source of information about Bitcoin is peers and friends: “*I started to know about Bitcoin a few years ago, when my friend told me about the wallet, the process and how Bitcoins could eliminate banks’ transactions*” [P3]. This quote indicates how some early adopters champion the use of Bitcoin currency by highlighting its advantages against the national fiat currencies.

#### *4.3.1.3 Uses of Bitcoins*

While most of the literature describes Bitcoins as cryptocurrency (Carillo, 2015; Coin Market Cap, 2019a) the findings indicate that they are used predominantly as store of value, i.e., predictably valuable for later use. Eight participants used Bitcoins on a regular basis to generate income, 7 used them occasionally for investment, while 5 were full time investors. This is interesting, because Bitcoins experience high volatility which makes them on the long-term unreliable stores of value (Yermack, 2013). It appears that the complete control over one’s savings is preferred over the less volatile yet less controllable fiat currency. Such characteristics were shared by other cryptocurrencies such as Litecoin and Swisscoin also used by the participants.



**Figure 4.2: Merchant’s Sign for Accepting Bitcoin Payment**

Another surprising finding is that there were only three isolated accounts of the use of Bitcoin as a currency for buying goods or services, despite the growing number of merchants who accept Bitcoins (**Figure 4.2**). Most of the payments were for online utility or phone bills, food, or mining equipment. For example, one participant noted the payment of his mobile phone’s prepaid credit with Bitcoins [P10], while another referred to the payment of food supplement from a friend: *“he just sent me his QR code and I scanned the code and transferred the amount of Bitcoins”* [P19]. In addition, one participant mentioned both online and offline uses of Bitcoin currency: *“I pay my utility bills in Bitcoins from the cryptomarket.my. I even buy my cigarette from expedia.com, and use cheapair.com to buy my flight tickets and hotel bookings too. Then there is a restaurant in Johor where I pay in Bitcoins”* [P12]. This diverse way of spending Bitcoins as a currency is an exception rather than the norm, as the study failed to find any additional participants reporting similarly a rich use of Bitcoin currency. Interestingly, there is only one account of illegal purchase: *“I bought an unlimited Spotify account from the dark web using Bitcoin”* [P1].

#### 4.3.2 Blockchain's Characteristics and their Impact on Trust

This section describes the main characteristics of Bitcoin technology, and how they contribute to trust in Bitcoin. These include Blockchain's decentralisation, unregulation, embedded expertise and reputation, as well as transparent, low cost, easy, and insecure transactions.

##### *4.3.2.1 Decentralised Blockchain*

One of the main identified characteristics relates to the decentralised nature of Bitcoin technology (Swan, 2015). Findings indicate that most participants appreciate that Bitcoin transactions do not involve any third party involvement from financial institutions: *"A decentralised currency is a bit more secure in terms of handling it is same like an asset. So if nobody else [third party] handles the asset, it is more secure for me to handle it by myself"* [P20]. The decentralisation of Blockchain also fosters confidence in its clear intention to circumvent, arguably dishonest central financial institutions. This, in turn, provides support for honesty as a dimension of credibility in Corritore and colleagues' (Corritore et al., 2003) model of online trust.

People also understand the reduced need for the complicated authorisation process for sending and receiving money: *"if you look at the current banking system, it takes three working days to do the settlement, but with Blockchain you can settle it instantly"* [P3]. This quote illustrates the appreciation for a quicker transfer of money between accounts, and therefore the ease of use.

#### 4.3.2.2 Unregulated Blockchain

Participants also expressed appreciation for the unregulated aspect of Blockchain technology. As a result, more than half of participants perceive this as an opportunity to become more empowered and privileged to regain control over their own money: *“all governments love to control people [but] they cannot control Bitcoin, and that’s why they cannot accept it. Bitcoin is people’s money giving them financial freedom”* [P14]. This is a militant statement, which links back to the initial motivation for engaging with Blockchain technology: the erosion of trust in financial and government institutions coupled with the economic crisis (Sas & Khairuddin, 2015).

Unregulation sets no limits for sending and receiving money, which can take place either locally or worldwide: *“I see no boundaries for people to do trading globally or nationwide; a freedom to do the trading without any restriction from the authority”* [P2]. As a decentralised and unregulated system, the risk of abuse of power over individuals’ personal assets is highly restricted. This confirms a limitation of the perceived risk as the third dimension of the model of online trust (Corritore et al., 2003). Several participants referred to the benefits of Blockchain’s pseudoanonymity, and its value in supporting unregulation as illustrated by this quote: *“we can keep our money as much as we want and the government will not be able to freeze our wallet because of the pseudo-anonymity”* [P11].

#### 4.3.2.3 Blockchain’s Embedded Expertise

Another characteristic of Bitcoin technology is people’s appreciation for the expertise required for mining Bitcoins and verifying transactions. This is

interesting given that for example, mining a rig needs limited technical knowledge. Findings, however, indicate that the cost required by the mining process provides a guarantee for the invested expertise and ultimately for the credibility of the Blockchain technology: *“producing Bitcoins is not something easy. There are specific ways to mine and expensive equipment needed”* [P8]. As the competition and difficulty for mining Bitcoins increase over time, more computationally intense mining equipment is needed which in turn lead to higher costs for producing Bitcoins. Almost a quarter of participants mentioned this complexity and the cost of the mining procedure. Their appreciation for miners’ expertise fosters credibility in Bitcoin currency and transactions. This further confirms the credibility dimension of the online model of trust and its application to Bitcoin technology (Corritore et al., 2003).

#### 4.3.2.4 Blockchain’s Reputation

The reputation of the Blockchain technology has been notoriously damaged due to illicit activities on Silk Road, an anonymous online marketplace predominantly for narcotics, which uses Bitcoins as its exchange currency (Christin, 2012). Four participants mentioned such reputation issue due also to current cybercrimes, since Silk Road was closed down in 2013: *“there are lot of crimes due to Bitcoin’s anonymity: money laundering, terrorist financing and tax evasion”* [P15] but surprisingly, with limited reference to its negative impact on participants’ credibility in Bitcoin technology. Interestingly, the study also found instances where participants, in fact, valued the growing reputation of Bitcoin technology: *“in the long term, this technology has a very bright future. There are lots of big companies which start doing research on Blockchain”* [P17]. This

quote suggests that the large companies' interest in Blockchain offers alternative routes for legitimising its authenticity and ultimately credibility. Apart from trust in Blockchain, participants also referred to trust in Bitcoin transactions.

#### *4.3.2.5 Transparent Transactions*

The findings indicate an important and valued characteristic of Bitcoin transactions: their transparency (Swan, 2015). The public ledger allows public access to the movement of Bitcoins from one wallet to another. Users are able to track any Bitcoin transactions from the very first one, until the present day: *“because Bitcoin uses Blockchain, we can see the movement of the Bitcoins in a public ledger. It is very transparent”* [P11]. Transparency echoes technology's credibility dimension in Corritore and colleagues' (Corritore et al., 2003) model of online trust, and its honesty dimension.

#### *4.3.2.6 Easy and Quick Transactions*

Another valued characteristic of Bitcoin transactions is their ease and speed of completion: *“With Bitcoin, you can move your money globally in just a second; very easy”* [P11]. A similar quote emphasising the ease of completing worldwide transactions by comparing them with the ease of texting: *“It is easy to move money from one country to another. It is just like you send a text message and the transaction is done”* [P13]. The above outcomes suggest that through transparent, easy, and quick transactions, people experience the ease of use. According to Corritore and colleagues' (Corritore et al., 2003) model of online trust, ease of use is one of the three factors of trust.

#### 4.3.2.7 Low Cost Transactions

A third valued characteristic of Bitcoin transactions is their low cost. A few participants provided quotes to support this: *“it only costs me 10 cents for each transaction”* [P6]; or *“the main benefit of transactions is that they are easy, fast and cheap”* [P14]. These outcomes indicate that transactions’ low cost could further contribute to reducing transactions’ perceived risk, as participants do not have to fear hidden or higher costs. In their model of online trust, Corritore and colleagues’ (Corritore et al., 2003) referred to risk as the third factor of trust, and explained the direct relationship between users’ perception of control and their trust. If the above characteristics support users’ trust in their Bitcoin transactions, findings also indicate one characteristic which hinders trust which is further detailed.

#### 4.3.3 Insecure Transactions

An important finding is that despite the above characteristics supporting trust in Blockchain technology and Bitcoin transactions, participants also reported their concerns about the risk associated with insecure transactions. It is worth mentioning that insecure transactions do not concern miners’ cryptographic protocol for authorising transactions. Indeed, none of the participants reported concerns about the security of this protocol, but strong trust in miners’ expertise and in the predictability of the protocol. Instead, insecure transactions relate to human error or malice and technology’s limitation to address them. More specifically, the study identified four types of insecure transactions, three related to human factors: those due to users themselves, to the other person or entity engaged in a transaction, or to the third human parties not engaged in transactions; and one related to technology’s

limitation to address them. The next section will discuss the associated risks for each of these types of transactions.

#### *4.3.3.1 Risks Due to Users' Challenges of Handling Passwords*

Six participants mentioned the risk of losing the password for their wallets, or the risk of insufficiently protecting it. For example, the quote below illustrates this type of risk and its serious consequence of no longer being able to access one's Bitcoins from that wallet: *"Make sure you don't forget your password because Blockchain does not keep your password [...] it cannot be recovered and you will lose all your Bitcoins from that wallet"* [P16].

The second risk of insufficiently protecting the password can have equally serious consequence of having the Bitcoins stolen: *"I lost 30 Bitcoins in the last months because of my own security mistake. I set up my wallet password the same as my email password. One day, my wife clicked on a phishing email and the hackers were able to get my email password and use it to log in to my Bitcoin wallet"* [P12].

In order to address these risks, some users mentioned the importance of taking responsibility for securely storing and protecting their passwords: *"As users we must know how to make sure that our Bitcoins are secured. It is the same as protecting our own cash or any personal valuable thing that can be stolen by others"* [P15]. Some participants even installed additional security applications in their Bitcoin wallet such as double authentication [P12], since although *"the system is secured, the security responsibility is with the user. If anyone lost their Bitcoins, the first person to be blamed is themselves, not the system"* [P14].

#### 4.3.3.2 Risks Due to Hackers' Malicious Attacks

Three participants mentioned that insecure transactions are also due to malicious hacker attacks. The study has seen above that some of these involve phishing emails to target wallet passwords. Such attacks can penetrate even through double authentication: *“you must make sure that your password is difficult to guess. “A friend lost 14 Bitcoins even though he applied double authentication on multiple devices” [P11].*

#### 4.3.3.3 Risks Due to Failure to Recover from Human Error or Malice

Although a third of participants considered themselves responsible to secure their Bitcoins, a few also indicated that the recovery from users' failure to protect their passwords or from hackers' attacks is limitedly supported by the Bitcoin technology. The main limitation here is that transactions are irreversible: *“let's say the hacker has diverted the money to another Bitcoin wallet address; you will never know where your money has been transferred to and you cannot reverse the transaction either” [P1].* This is an interesting finding, indicating a drawback of the Blockchain technology. The rationale for irreversible transactions addresses the limitation of the centralised financial system which allows reversible transactions without being bound to enforce the parties' contract stating that the sale is final (Fui, Nah, & Davis, 2002). However, as suggested in the above quote, this design feature fails to account for malicious transactions due to hacking, or to the dishonesty of the trading parties, as further detailed.

It is important to make the distinction between how transactions are represented in Blockchain, i.e., data structure allowing the transfer of Bitcoins from one electronic wallet to another; and how the participants perceive

transactions: a two-way transfer of Bitcoins and money/goods. Unlike the one-way remittance transactions well supported by the Bitcoin technology (Kazan, Tan, & Lim, 2015), all transactions reported by participants are two-way, with both parties sending and receiving assets. Although most transactions involve buying or selling Bitcoins against fiat currency, participants were only able to track one side of the transaction, namely the movement of Bitcoins captured within the Blockchain. This raises major risks and trust issues particularly in relation to potentially dishonest trading partners, as the untracked part of a transaction does not allow for scrutiny. This issue is further emphasised when dealing with traders who are not authorised entities.

#### *4.3.3.4 Risks Related to Dishonest Partner of Transaction*

Findings indicate that a considerable risk factor is dishonest partners with whom one engages in Bitcoin transactions. A quarter of participants reported incidents where either them, or their close friends have been cheated and their trust betrayed: *“I transferred some Bitcoins but the buyer didn’t pay me”* [P6]. This quote illustrates the importance of knowing about the transaction partner. This point has been mentioned by other participants who expressed concerns about strangers’ unknown reputation: *“you don’t know whether the seller is a scam or not”* [P1].

#### 4.3.4 Strategies for Mitigating the Risks of Dishonest Traders

The study identified five strategies for dealing with dishonest transaction partners, and for mitigating their risks. These strategies involve two forms of trading: directly with another person, or through online exchanges, i.e. services for matching price and offer between Bitcoin sellers and buyers. These strategies are

further described starting with the most frequent one, and the running themes across these strategies are the traders' pseudoanonymity and the unregulation of Blockchain technology.

#### *4.3.4.1 Trade with Authorised Exchanges*

The online exchange is by far the first and most preferred form of transaction, mostly because its regulation supports users' trust. Indeed, although Bitcoin technology and its cryptographic protocol are unregulated, exchanges require authorisation from the financial services such as Financial Conduct Authority (Zanjani, 2004). For example, five participants mentioned their check of exchangers' credentials: *"I do look at their background and legal term conditions and from there I put trust on the exchange"* [P2]. The exchanges' websites are crucial for fostering trust: *"a proper website, [indicating the amount of trading, and testimonials [supports] trust on the exchange"* [P3].

This extends previous HCI findings on the value of website for trust (Fui et al., 2002) to the context of cryptocurrency transactions. An additional source of trust is the option to contact directly the exchange's agents: *"I prefer this exchange because they have their representative to contact if there is any problem or question to ask"* [P12]. In turn, this makes users' relationship with the exchanges, a more personal one. Apart from being authorised by financial services, and having credible websites, exchanges also foster trust in transaction partners, as they require sellers and buyers to register and have their identity verified. This is an important finding, indicating ways to address the extensive concerns around traders' pseudo-anonymity. Surprisingly, only one participant reported the use of the escrow service (the third party holding the assets to be released once both

parties are satisfied with the transaction). Findings indicate that ease of use is negatively impacted by the use of the escrow, because of its additional registration requirements: *“it is easier and faster to do the transaction [directly] with other traders”* [P10].

These findings provide support for the contextual properties described in the framework on mechanics of trust (Riegelsberger et al., 2005), warranting users’ trust in exchanges because of their successful performance and the expectation that they will perform consistently well in the future (temporal embeddedness), exchanges’ reputation (social embeddedness), and their legally authorised services (institutional embeddedness). The study also found evidence for the intrinsic properties warranting trust in exchanges, for example through social presence of professional websites and contactable local representatives (integrity), as well as reputation through testimonials (credibility).

#### *4.3.4.2 Trade with Socially Authorised Traders*

In comparison with exchanges, dealing with individual traders offers weaker risk mitigating strategies. The strongest strategy is dealing with socially authorised traders. These are well-known, de-anonymised members of online groups who regularly join discussions and trade Bitcoins. Thus they become trusted and their names are added by the group administrator to an online list of verified traders: *“I only buy from authorised traders as lots of friends experienced scam and huge losses”* [P18]. The label of authorised trader is usually provided within an online group of Bitcoin users on the basis of a series of successful de-anonymised transactions. This outcome indicates the crucial value of de-anonymity for credibility and trust. These findings also provide

evidence for the framework on mechanics of trust (Riegelsberger et al., 2005) warranting users' trust in authorised traders (temporal and social embeddedness), but limited institutional embeddedness.

#### *4.3.4.3 Trade with Reputable Individual Traders*

If an authorised trader cannot be found, participants engage in a weaker risk mitigating strategy: dealing with reputable traders. Unlike traders authorised by an online user group, reputable ones benefit only by credibility by proxy, from a few group members who have engaged in successful transactions with these traders. For example, participants indicated the use of peers' or friends' recommendations: *"I knew the trader from the telegram group, and a few recommendations from friends who can be trusted"* [P8]. Almost half of participants noted that their first point of contact for a background check on an unknown trader is their online groups *"if I am dealing with a stranger, I will ask in my online group to verify that particular person. If they don't know him I will not proceed with the transaction"* [P10]. In addition, more than half of participants mentioned their preference for known traders whom they have had successfully trusted in the past: *"most of them are my close friends, so I have no problem trusting them"* [P20]. This shows the value of reputation and benevolence in supporting traders' credibility (Corritore et al., 2003). These findings confirm the framework on mechanics of trust (Riegelsberger et al., 2005) warranting users' trust in traders because of their reputation (social embeddedness and credibility), and when dealing with friends, because of perceived integrity and benevolence.

#### 4.3.4.4 Trade with De-anonymised Individual Traders

Although less common and mostly due to lack of experience, sometimes Bitcoin users engage in transactions with unknown traders. In such cases, findings indicate that seldom the traders remain unknown, as the study identified two mechanisms for ensuring traders' de-anonymisation: face to face meeting, or online sharing of their IDs. For example, several participants expressed the view that they only proceed with the transaction if the trader is willing to de-anonymise. One way of achieving this is through face to face meeting, where both sides of the transaction take place simultaneously, i.e., the exchange of Bitcoins and fiat currency or goods: *"we cannot trust them online. We need to see that person and to do cash on delivery"* [P4]. Other participants require traders to de-anonymise by emailing their copy of personal ID: *"I need to know their identity"* [P5]. This strategy does not provide any contextual factors to allow users' trust in unknown traders for whom they have no reputation-related information (neither social nor institutional embeddedness) (Riegelsberger et al., 2005). Hence, users attempt to develop institutional embeddedness by de-anonymising the traders, or by reducing the risk of asynchronous transaction altogether through face to face meetings to perform synchronous two-way exchanges.

#### 4.3.4.5 Regulating Bitcoin

In order to address the challenge of dishonest traders, many participants expressed the wish that Bitcoin becomes regulated: *"I think we must demand to our politicians to regulate Bitcoin"* [P1]. This is an important finding indicating a

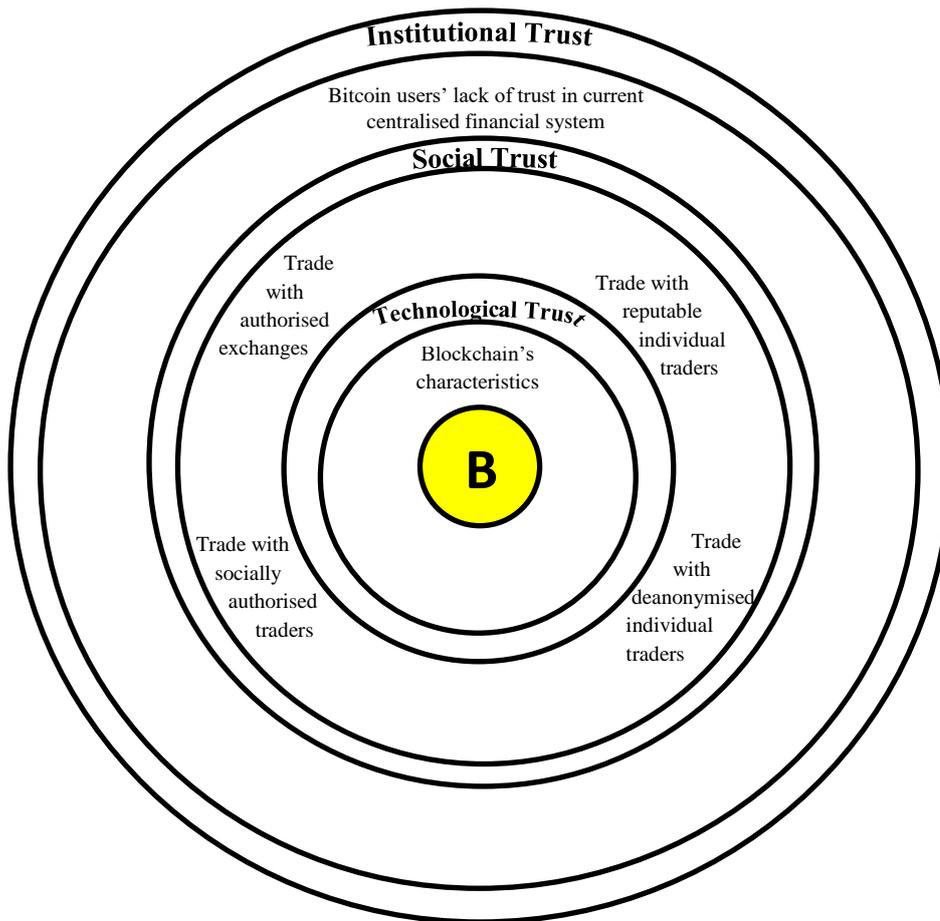
higher level strategy which does not address the trading itself but the unregulated nature of Blockchain.

#### 4.4 Theoretical Implication

Now the study reflects on the value of these findings for advancing the HCI discourse on trust. The study also discusses the specific tensions that unregulation and pseudo-anonymity bring to trust. The implications are mostly relevant for Bitcoin users in developing contexts. They may also hold value for understanding and supporting trust in cryptocurrencies in general in both developing and developed contexts, but future work is required to explore this.

##### 4.4.1 Towards a Framework of Trust among Bitcoin Users

The findings advance the understanding of users' trust in Blockchain technology and in transaction partners. The study argues for the feasibility of the considered HCI theories (Corritore et al., 2003; Riegelsberger et al., 2005; Sas & Khairuddin, 2015) for identifying key Blockchain's characteristics supporting users' trust: decentralisation, unregulation, miners' expertise, as well as transparent, easy, and low cost transactions. The main trust challenge experienced by Bitcoin users is the risk of insecure transactions and in particular that of dealing with dishonest traders.



**Figure 4.3: Framework of Trust in Bitcoin for Users**

The discussions begin with the findings in the light of Sas and Khairuddin's (Sas & Khairuddin, 2015) Bitcoin trust framework (**Figure 4.3**). The findings suggest that technological trust of Bitcoin users in Blockchain technology is strong, as participants value its secure cryptographic protocol. This extends prior findings on the users' challenges to secure their Bitcoins (Klontz, Britt, Mentzer, & Klontz, 2011) with their willingness to take responsibility for their weak, easy to break wallet passwords.

Findings also indicate novel insights into the social dimension of trust among Bitcoin users. The main challenge here relates to dishonest Bitcoin traders. With respect to different stakeholders, it is worth mentioning that the findings capture the

blurring of the boundaries between merchants and users when the object of transaction is Bitcoins. In fact, the study found little evidence that Bitcoin users engage with merchants to buy goods, indicating participants' preferential use of Bitcoin as a store of value rather than currency. In order to mitigate this trust issue, findings indicate four different alternatives that users applied to enact Bitcoin transactions: trade with authorised exchanges, trade with socially authorised traders, trade with reputable individual traders and trade with de-anonymised traders. However, the latter method is reported to be the most unsecured. The outcomes also suggest extending this framework's definition of institutional trust to include not only government trust in Blockchain technology, but also the trust of Bitcoin users in government and financial institutions. The study has also seen evidence on how the erosion of such institutional trust is crucial in users' adoption of Bitcoin and acceptance of its algorithmic authority (Kow & Lustig, 2018).

Probing further into the exploration of technological trust, the study applied the model of online trust (Corritore et al., 2003) to identify specific Blockchain's characteristics impacting on trust. The findings provide support for extending the applicability of this model to Bitcoin technology. Blockchain's characteristics supporting users' credibility include: honesty ensured by decentralisation and public ledger's transparency; expertise supported by miners' competence and hard labour; predictability supported by the cryptographic protocol; and reputation supported by large companies' interest in Bitcoin. Findings also identified Blockchain's characteristics supporting the other dimensions of trust: ease of use grounded in ease and quick transactions; and limited risk due to transactions' low cost and the decentralised, unregulated nature of Blockchain which limits the risk of institutional power abuse. Outcomes also suggest a specific technological characteristic

perceived as a risk factor: the Blockchain's purposeful design feature for irreversible transactions. The study found the challenge of two-way transactions and in particular the offline one which is not captured by the Blockchain. The challenge of irreversible transactions is not grounded in people's distrust on the transaction, but in potentially the dishonest part of the transaction, i.e., the payment of fiat currency for acquiring the Bitcoins. If this side of the agreement is not fulfilled, users would prefer to reverse the Bitcoin transaction, an operation which is not possible. An interesting design opportunity here would be exploring new ways of tracking this movement of fiat currency (currently not captured) in the Blockchain.

As a means of exploring users' support for trusting their transaction partners, the study applied the framework on mechanics of trust (Riegelsberger et al., 2005). This framework allowed the identification of different sources of trust for each of the risk mitigating strategies. Among these strategies for dealing with dishonest traders, Bitcoin users engage in decreasing order of preference with exchanges, authorised or reputable traders, and ultimately with unknown traders which they attempt to de-anonymise. Only the exchanges provide legal authorised services (Möser, 2013; Yermack, 2013) while trust in the other types of traders is supported mostly by the information about their credibility and reputation within the thick relationships (Hardin, 2002) of online user groups. The less reputation-related information users can gather about the traders, the stronger the need to de-anonymise them. Most participants went even further suggesting the value of regulating the Blockchain (institutional embeddedness for all types of traders).

## 4.5 Design Implications

This section discusses the design implications (Sas, Whittaker, Dow, Forlizzi, & Zimmerman, 2014) that the findings suggest. This study discusses the need to support the transparency of two-way transactions, tools for materialising trust, and tools for supporting reversible transactions. These design implications have been developed to address the identified trust challenges of dishonest traders, while respecting Blockchain's main characteristics such as decentralisation, unregulation and pseudo-anonymity.

### 4.5.1 Supporting Transparency of Two-way Transactions

All transactions reported in the study are two-way, most of them sequential and asynchronous, i.e., typically one party sends the fiat currency and after receiving it, the other party sends the Bitcoins. However, people can only track on the Blockchain the movement of Bitcoins. Sending fiat currency can be faked through fraudulent statements of transfer. This coupled with the lack of legally authorised partners warranting one's trust in them, i.e., institutional embeddedness, leads to increased risk of defraud from dishonest traders. Such traders are not known and cannot be made accountable for failing to complete their part of transaction, neither responsible for the retribution it entails.

One can imagine creative design methods (Salovaara et al., 2011) and new tools for digitally capturing the contents of transactions which is not Bitcoins, to ensure that their transfer is also verified, authorised and stored on the public ledger. The findings indicate that such content of transaction is often fiat currency. Blockchain already provides mechanisms for creating digital tokens backed by fiat currency, i.e., Colored Coin, Omni Layer (Tether, n.d.). Such mechanisms can also

be harnessed for creating digital tokens (metadata embedded in the Blockchain) backed by physical goods, such as the ones explored in the provenance context where tokens represent documents accompanying the transaction of goods or finances as means of tracking their ownership. Such mechanisms need to remain decentralised and to become integrated into the Blockchain interface so that end users with limited technical expertise can access and use them.

#### 4.5.2 Tools for Materialising Trust in Blockchain

Findings indicate that in the absence of known and stable identities, Bitcoin users who engage in transactions with each other rely mostly on social embeddedness. As one of the properties warranting trust in another party, social embeddedness is reflected in users' active effort to gather reputation-related information about unknown traders, either from people they already trust such as close friends, or from members of the online group where most of their social learning about Bitcoin technology takes place. One way to better support this data gathering is through designing mechanisms for capturing and visualising reputation as meta-data linked to a wallet address. Blockchain protocol already supports the creation of metadata within a transaction, by allowing the generation of a new secure address referencing the metadata. A reputation management system built on top of the Blockchain will strongly contribute to the social embeddedness for warranting trust among traders. This in turn, motivates traders to keep the same wallet address in order to grow their reputation, hence providing more stable, albeit still private, identities. For example, Carboni (Carboni et al., 2016) proposed vouchers attached to a transaction for the transfer of payment for a service. If the buyer is satisfied with the service, he can accept and co-sign the voucher which

contains an incentive fee paid by the service provider to the buyer for leaving a positive feedback. The reputation score of a service provider could be computed by adding the voting fees for that service across Blockchain's relevant transactions. Alternative mechanisms for supporting also the caption of negative feedback are much needed.

#### 4.5.3 Tools to Support Reversible Transactions

Findings indicate that in the case of dishonest traders, the irreversible Bitcoin transactions are problematic. This stems from the lack of transparency of the two-way transactions: while the transfer of Bitcoins is captured by the Blockchain, the counterpart asynchronous transfer of money (or goods) for which people receive (or pay Bitcoins) is not. One way of addressing this is by exploring novel mechanisms for reversing individual two-way transactions on top of the irreversible Blockchain protocol (El Bansarkhani & Sturm, 2016). This is not a trivial issue, as in its current form, the Blockchain protocol does not allow reversing transactions which have been already confirmed and added to the ledger. One solution would be new tools for enabling the de-anonymisation of the owner of disposable wallet addresses (discarded after one use). Besides hindering dishonesty, such tools would allow users' to protect their privacy on the Blockchain, while enabling them to contact the other party, and request reversing the Bitcoin transfer. This would also support social embeddedness, as the reputation of a given trader operating in a local online group can well extend beyond the lifetime of a disposable wallet. Other tools could leverage the support of multisignature transactions enabled by the Bitcoin protocol (El Bansarkhani & Sturm, 2016). A common example is 2-of-3 transaction model where money is placed in a joint address owned by both parties and a third

arbitrator, to be signed off once each party is satisfied. If there is a problem, the arbitrator will investigate and decide to transfer the payment back to the buyer or to the seller. Once the transaction receives 2 out of 3 signatures, it is completed. The multisignature tools differ from the escrow services as the arbitrator receives a fee agreed by all three parties, but cannot defraud as he will need two signatures for this. Surprisingly, no participant mentioned the use of multisignature tools, probably because of the same reason they do not engage with the escrow services: perceived difficulty of use, or limited awareness of such tools. Future work could further explore this.

#### 4.6 Chapter Summary

This empirical study investigated Blockchain's characteristics which support and challenge users' trust, alongside their motivation for Bitcoin use, and strategies for mitigating identified risks. The study advances the theory towards a model of trust among users of Bitcoin's decentralised, unregulated and pseudoanonymous technology in developing context, and provides insights into the specific tensions around these characteristics. Study findings led to a number of design implications that would support Bitcoin users develop increased trust in each other, including support for the transparency of two-way transactions, tools for materialising trust, and tools for supporting reversible transactions. However, those findings and implications designs are not reflected to the other types of Bitcoin stakeholders such as miners. Hence, in the next **Chapter 5**, the study on the exploration of trust among Bitcoin miners will be reported.

# Chapter 5

## The Trust Challenges and Opportunities among Bitcoin Miners

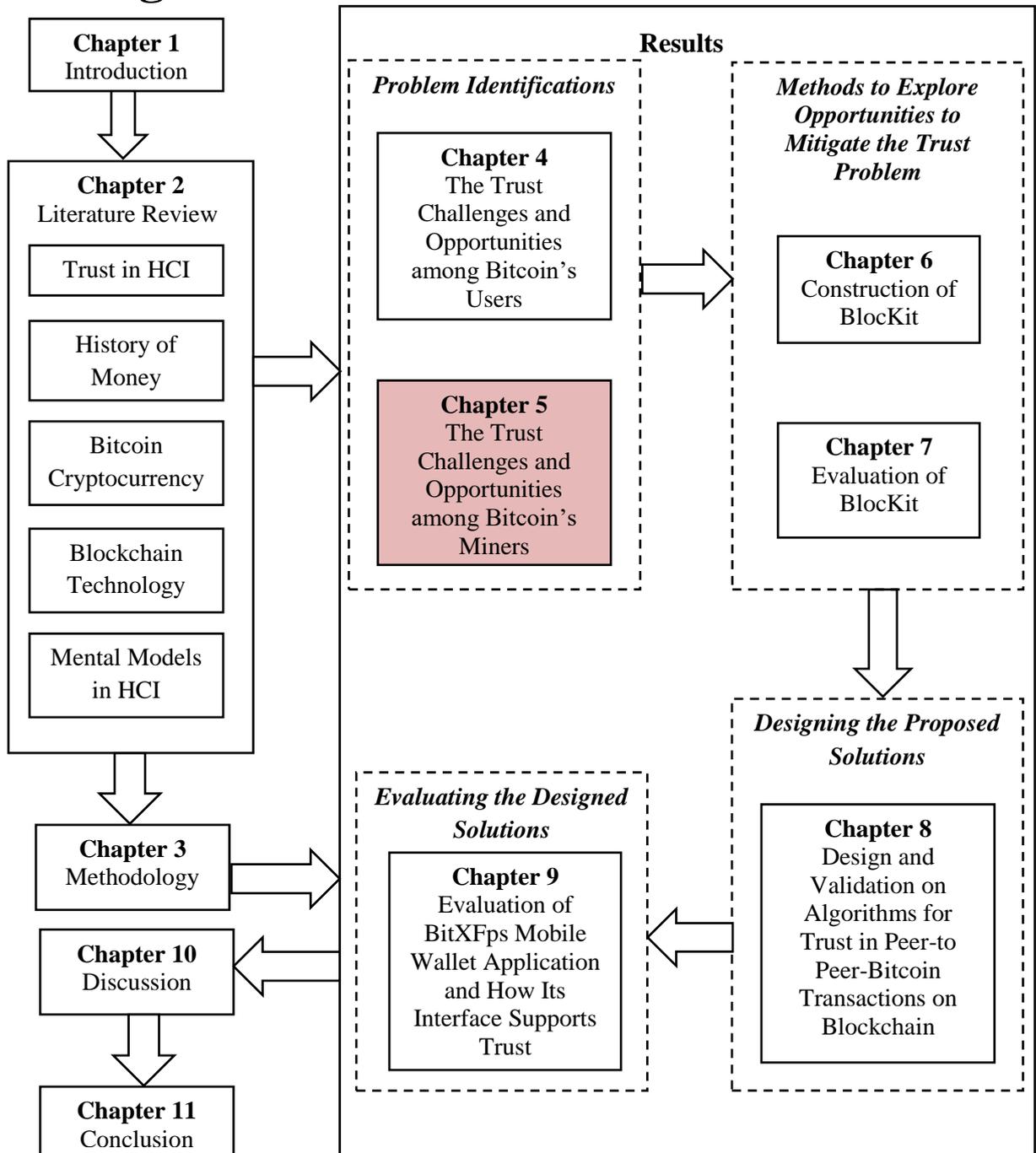


Figure 5.1: Chapter 5 of Thesis Structure

## 5.1 Introduction

This chapter presents the report on the explorations of Bitcoin miners' motivations and experience in mining the Bitcoin on Blockchain. Each of the enacted Bitcoin transactions was authorised by the Blockchain technology distributed ledger of nodes, which is known as miners. Its key actors are miners using computational power to solve mathematical problems for validating transactions. By sharing Blockchain's characteristics, mining is a decentralised, transparent and unregulated yet profitable practice as miners are rewarded in Bitcoins for their successfully validated proof-of-work. The reward together with the growing value of Bitcoins and their planned scarcity has attracted more miners to a practice which has become increasingly competitive and computationally demanding. However, apart from modelling-based security research on mining, there are limited explorations on miners' practices from their first-person perspective, such as the study on Bitcoin users' practices as described in **Chapter 4**.

In this sense, a study (**Study 2**) on miners' motivations, experiences, and how these may impact on Blockchain's different dimensions of trust were conducted. These concerns were explored by addressing the following research questions:

- what are miners' motivations for Bitcoin mining?
- what are *Bitcoin Blockchain's characteristics* impacting on miners' trust and its dimensions?
- what is the *social organisation* of mining practices: are there different approaches and types of miners?
- what are the main trust *challenges* and how do miners attempt to *mitigate* them?

It reports on interviews with 20 Bitcoin miners in Malaysia about their practices and trust challenge. In the light of HCI theories of trust, Bitcoin mining protocols, and its

security threats, findings discuss miners' motivations, the impact of Blockchain characteristics on miners' trust, social organisation of mining practices and the types of miners. The study also discusses the trust related topic including the trust challenges of collaborative mining and the way to mitigate the risk of collaborative mining. It concludes with the theoretical implications by building a theoretical model of trust among Bitcoin miners, the paradox of decentralisation and the challenge of unregulation. Finally, it reports on the design implications that include the tools for monitoring has power and reward distribution, decentralised tools tracking data centres' authorisation and reputation and tools for developing decentralised pools.

## 5.2 Research Method

For study 2, 20 miners in the age range 22-42 (Mean = 30.6) were recruited. They were all male, with different levels of mining expertise: 8 had over 4 years of mining experience, 8 had between 1 and 4 years, and the remaining 4 have less than one year. Participants had a wide range of professions, including 8 in IT, 1 in the legal services, 2 engineers, 1 in the medical field, 2 teachers, 2 in the financial sector, and 1 in administration. In terms of education, 14 have Bachelor degrees, 4 have Master degrees, and the remaining 4 are school leavers. Participants were all Malaysian and the recruitment took place via Facebook and Bitcoin Malaysia Telegram group. Prior work had also focused on a Malaysian context for exploring Bitcoin-related practices. For example, (Sas & Khairuddin, 2017) argued that it offers a unique opportunity as a developing country with steady economic growth, increased interest in cryptocurrency (FMT Reporters, 2016; MIGHT, 2017; Zhe, Noordin, & Yong, 2016). Malaysia has the first Blockchain ledger for the public consortium in Asia (BCE, 2016) aiming by 2025 to fully utilise the technology in the whole country (MIGHT, 2017).

The recruitment process started by approaching the founder and administrator of the Bitcoin Malaysia group on Facebook, followed by his invitation to join the Bitcoin Malaysia Telegram group. From within this group, the study publicly posted invitations for participating in the study. The study also sent private invitations to the most active members of the Telegram group, based on their interest in mining as reflected in their contribution to the group's discussion forum.

The study conducted semi-structured interviews either face to face or on Skype in both English and Bahasa language between May 2016 and June 2016. The aim of the study was to explore the mining process from the miners' perspective, their motivations and approaches to mining, as well as the main challenges of this process. The study also explored participants' strategies for mitigating their trust-related risks. The interviews lasted between 60 to 90 minutes, were audio recorded and fully transcribed. Data analysis followed a hybrid approach with existing concepts being used for the deductive coding while new ones, grounded on the empirical data, informed the inductive coding (Fereday & Muir-Cochrane, 2006). The deductive coding included concepts from literature on mining protocol such as the mining work process (Caetano, 2015; Nakamoto, 2008), mining trends (Acheson, 2007) mining threats (Bradbury, 2013; Buterin, 2013b; Corritore et al., 2003; Redman, 2016; Sapirshtein, Sompolinsky, & Zohar, 2015) and concepts from the HCI literature on trust such as technological, social and institutional dimensions of trust (Sas & Khairuddin, 2015), temporal, social and institutional embeddedness (Corritore et al., 2003). The codes were iteratively refined as new codes emerged under the theme of mining approaches, dishonest pool administrators, and strategies for risk mitigation.

### 5.3 Findings

To report the findings, we discuss miners' motivations, the main characteristics of Blockchain technology and their impact on miners' trust. In particular, the study highlights the social organisation and competitiveness of mining practices and how it is reflected in different approaches to mining and different types of miners. We further outline the risks of collaborative mining due to centralisation and dishonest administrators, and emerging mitigation strategies for addressing them.

#### 5.3.1 Motivations of Bitcoin Miners

In this section, we discuss the three sources of motivation for engaging in mining practice as highlighted by miners.

##### *5.3.1.1 Earning Potential through Fee-based Rewards*

Almost half of participants appreciated the earning potential of mining practice (Nakamoto, 2008) together with the increasing price of Bitcoins: *“Until today I am still continuously generating profit from this activity; this is my motivation”* [P14]. This steady revenue fosters miners' willingness to continue to invest in such lucrative practice by upgrading the mining equipment. Such capital costs are needed to ensure competitiveness in the context of increasing mining difficulty.

##### *5.3.1.2 Experimenting with Bitcoin Blockchain Technology*

The complexity of the Bitcoin mining process is also attractive in itself, as mentioned by 3 participants. For example, from initial curiosity, people developed an interest in both mining and using Bitcoins: *“I have the thought like “is this a real thing”? That was the initial direction. Then after mining Bitcoins, I*

*transferred mine to the wallet and tried to sell, thinking that if I can get USD for them then this is real*” [P16]. In such cases, participants appreciate the hands on experience and the knowledge that they gain: *“Even though it is considered a high capital investment [practice], mining is good in terms of learning”* [P11].

#### *5.3.1.3 Lack of Regulation Regarding Taxation of Miners’ Fees*

Despite its potential to generate income, the taxation regulation of this activity is not yet regulated. As it stands, the discretion to pay tax remains with the individual miners: *“[who may be] willing to pay tax whenever they get the Bitcoins from mining”* [P1]. There is also a concern that in the future the mining practice may become subject to taxation: *“if [governments] decide to monitor mining activities [like] gold or silver then [they] will ask all Bitcoin miners to register with the government”* [P2]. This can also have implications with respect to the anonymity of that mining practice.

### 5.3.2 Blockchain’s Characteristics Impacting on Miners’ Trust

Blockchain’s key design features related to mining are decentralisation, transparency, unregulation, ease of use, and social organisation which have shaped mining approach and the emergence of different types of miners.

#### *5.3.2.1 Decentralised and Transparent Mining Protocol*

More than a quarter of participants valued the mining protocol both in terms of its complex validation process: *“it uses the cryptographic hashing algorithm to secure the network so you cannot [fake] Bitcoins”* [P7], and security: *“I think it is rather difficult at the current computing power for people to hack it”* [P10]. Key to the mining protocol is the proof-of-work (Nakamoto, 2008), reflecting miners’

systematic and transparent competition for finding the quickest and longest solution to a block: *“this technology is based on the proof-of-work, where everything is calculated mathematically and is transparent”* [P18]. Participants also expressed appreciation for this cooperative work within the trustless Blockchain technology: *“the platform is standard; everyone uses the same Blockchain, so I don't think there is a trust issue”* [P2]. These quotes are illustrative of miners' trust in mining technology: competitive, transparent, and decentralised protocol under no control of central entities, which strengthens the credibility dimension of online trust outlined in Corritore and colleagues' model (Corritore et al., 2003).

#### 5.3.2.2 Non-Legally Binding Practice

No institutional authority such as banks or governments control Blockchain and its mining protocol, which in turn limits the risks of their abuse of power (Rolnick & Weber, 1997). Although there have been attempts to regulate mining as an arguably lucrative and thus taxable practice (Biegel, 2018), in many countries including Malaysia, it is not considered illegal. Four participants expressed satisfaction with the unregulation of mining practice: *“I don't see any issues here: mining is just like you are running a software on a computer”* [P17]. As a result, miners operate anonymously: *“all nodes in the network only know each other pseudo anonymously and they have the same privilege but yet they can come to the consensus to agree on which record can be written in the database”* [P11]. This unregulation limits miners' perceived risks as a dimension in the model of online trust (Corritore et al., 2003), increasing their trust in mining

practice. As shown earlier, there is however an awareness that income generated through mining may become subject of taxation.

#### 5.3.2.3 Ease of Use

Participants appreciated the ease of use of the mining protocol and the limited technical skills required. For example, four participants noted their casual experience of Bitcoin mining: *“I just let it run and once in a while, I just check to see [...] if it doesn't calculate or the block has been full, or if there is something to do with my wallet which does not allow to receive the Bitcoins”* [P2]. Such quotes indicate an important dimension of the online trust (Corritore et al., 2003), ease of use of the mining protocol which further supports miners' trust in it.

#### 5.3.3 Social Organisation of Mining Practice: Competitiveness

This section explores the complexity characterising the competitiveness of Bitcoin mining practices to produce the proof-of-work (**Figure 5.2**). It focusses on different forms of mining and types of miners. The identified forms of mining vary across computational power, its ownership and maintenance which showed increased complexity over time. The study grouped these forms in individual and collective mining, taking place on miners' home machines or those leased from data centres (**Table 5.1**).

	<b>Individual</b>	<b>Collective</b>
<b>Own machines</b>	Home-solo mining [P2, P5, P12, P18]	Home-pool mining [P1, P3, P4, P5, P7, P9, P10, P11, P15, P16, P17 & P19]
<b>Leased machines</b>	-	Data centre-pool mining Owned: P6; Leased: P8, P13, P14

**Table 5.1: Mining Approaches**

### 5.3.3.1 Home-Solo Mining

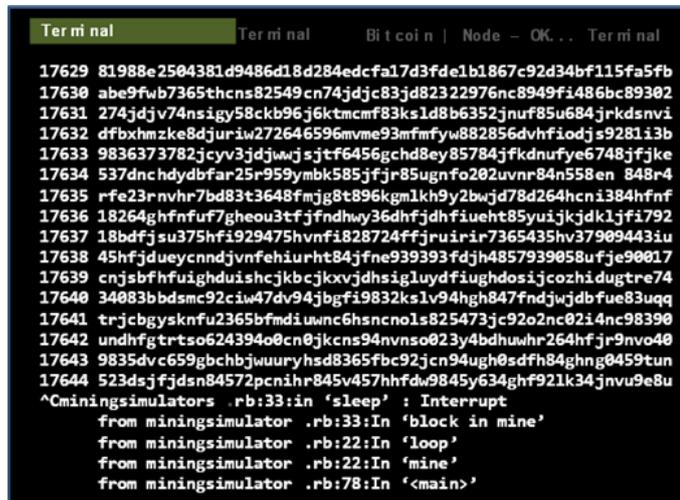
The first form of mining that has historically emerged consisted of individual miners working on their own home machines. A quarter of participants expressed appreciation for this cooperative and competitive work requiring limited computational power (Nakamoto, 2008). The findings indicate that most participants who mined during 2010-12 have engaged in this form of mining: “*I started as a home miner in 2011, mining on my computer; and at that time Bitcoin was not as popular as now*” [P5]. This quote is similar to others confirming the limited mining difficulty in those early days (Caetano, 2015). With this advantage, home miners worked solely enjoying the full rewards of their labor: “*in early days people used to do solo mining and all profits will straight away go into your wallet*” [P18]. With no intermediaries between the miners and the Bitcoin network, the trust consisted solely of trust in the mining protocol, as expressed by three of the participants: “*They didn't have any problem to trust each other [...] they mined by themselves and they were referring to the same ledger*” [P3]. This quote reflects the characteristics of trustless Blockchain mining protocol which provides a transparent and fair competition among miners for processing transactions (Nakamoto, 2008). However, at the end of 2010, the

mining difficulty has considerably increased (Bitcoin.org, 2019), This, in turn, affected solo miners, due to the small computational power of their individual machines. Two participants shared this view: “*due to high difficulty, solo mining is now no longer relevant*” [P12], and it paved the way for collaborative mining, and in particular for what the study calls home-pool mining.

#### 5.3.3.2 Home-Pool Mining

From solo mining, home miners started to shift towards collaborative mining. Mining pools consist of geographically distributed home miners and their network of machines pooling together computational resources and share of the profits (Acheson, 2007; Caetano, 2015) by acting as a sole entity in the competitive solving of blocks problems. A quarter of participants expressed this view: “*mining pool is actually the entity that controls the hash power in the network [and] the income that it generates is divided among miners, according to the hash power that they have contributed to that pool*” [P4]. This indicates that in addition to end miners, a new type of miner has emerged: the pool administrator, who creates his own pool, collects the computational power of end miners and divides the mining profits to each miner according to their individual contributed power. As a home pool tends to be small in size (Morrow, 2014) usually consisting of 10-15 miners, the equity of profit distribution is not usually an issue. The home-pool mining offers increased the likelihood of success, as reported by two participants: “*I shared with my friend back in the university to buy a second-hand computer and a powerful graphic card. Each of us spent around RM 1500 and we started to mine*” [P19]. Apart from creating such pools,

people also started to join existing pools, as mentioned by four participants: “I mined in a pool because with solo mining it is difficult to get profit” [P10].



```
Terminal Bitcoin | Node - OK... Terminal
17629 81988e2504381d9486d18d284edcfa17d3fde1b1867c92d34bf115fa5fb
17630 abe9fwb7365thcns82549cn74jdc83jd82322976nc8949fi486bc89302
17631 274jdv74nsigy58ckb96j6ktmcmf83ks1d8b6352jnurf85u684jrkdsnvi
17632 dfbxhmzke8djrurw272646596mvm93mfmfyw882856dvhfiodje9281i3b
17633 9836373782jcyv3jdwjwsjtf6456gchd8ey85784jfkdnufye6748jfjke
17634 537dnchdydbfar25r959ymbk585fjfr85ugnfo202uvnr84n558en 848r4
17635 rfe23rnhvr7bd83t3648fmjg8t896kgmlk9y2bwjd78d264hcn384hfnf
17636 18264ghfnuf7gheou3tfjfnhdwy36dhfjdhfueht85yujkjdklji792
17637 18bdfjsu375hfi929475hvnfi828724ffjrurir7365435hv37909443iu
17638 45hfjdueycnndjvnfehiurht84jfne939393fdjh4857939058ufje90017
17639 cnjsbfhfuighduishcjkbcjkxvjdhsigluydfiughdosijcozhi dugtre74
17640 34083bbdsmc92ciw47dv94jbgfi9832kslv94hgh847fndjwjd b fue83uqq
17641 trjcbgysknfu2365bfmdiuwnc6hsncno1s825473jc92o2nc02i4nc98390
17642 undhfgtrtso624394o0cn0jkcns94nvso023y4bdhuwhr264hfjr9nvo40
17643 9835dvc659gbchbjwuuryhsd8365fbc92jcn94ugh0sdfh84ghng0459tun
17644 523dsjfdsn84572pcnihr845v457hhfdw9845y634ghf921k34jnvu9e8u
^Cminingsimulators .rb:33:in 'sleep' : Interrupt
from miningsimulator .rb:33:In 'block in mine'
from miningsimulator .rb:22:In 'loop'
from miningsimulator .rb:22:In 'mine'
from miningsimulator .rb:78:In '<main>'
```

**Figure 5.2: Miner’s Real-time Proof-of-Work**

In late 2012, after the first halving period (Caetano, 2015), the difficulties of mining have further increased (Bitcoin.org, 2019), negatively affecting home miners, as noted by almost half of the participants: “*from normal CPU I upgraded to GPU. The difficulty level was increasing and my system did not generate enough coins. So I stop mining around 2012*” [P5]. This indicates that even though the miners had taken the efforts to improve their machines’ computational power, this did not suffice as they faced additional challenges due to higher maintenance costs. For example, four participants noted that in order to continue to mine competitively, the computational power needs upgrading even during the halving periods: “*for home mining, let’s say you bought the latest S7 mining machine and joined a pool, you can get a few Bitcoins for the first few months. [Then] you need to add more hashing power to your machine [because] the difficulty of mining keeps increasing. That’s why many home miners retire from doing this job*” [P17]. In addition, maintenance also relates to high electricity cost: “*machine is very expensive and the electricity bill can be around RM100k*

*per month. So you won't get your money back unless you go big scale*" [P3]. Furthermore, three participants pointed to the challenge of locating the machines in their homes due to the generated heat: *"because my house will be very hot"* [P3]. Together, these challenges have led twelve of the participants [P1, P3, P4, P5, P7, P9, P10, P11, P15, P16, P17 and P19] to retire from home mining, three [P2, P12 and P18] to continue upgrade their home mining system by creating so called *mining farms*, with a cluster of machines owned by one person, and located outside one's home, usually in a rented place. One participant considerably scaled up his mining systems so that *"today I own a data centre company for mining"* [P6]. The remaining four participants [P8, P13, P14, and P20] joined directly the cloud mining through data centres.

#### 5.3.3.3 Data Centre–Pool Mining

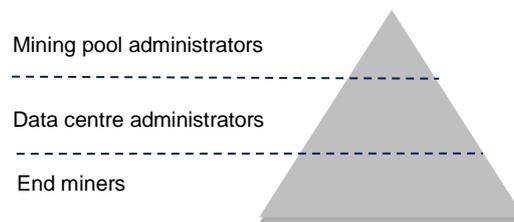
The increasing challenges of Bitcoin home mining have radically transformed it into large scale mining, beyond the confines of miners' own homes. As noted by three participants: *"as the difficulty of mining is increasing every day, for now, you can only mine at bigger scale"* [P10]. Data centres allow *"cloud mining, where people buy computational power in return for the share of the profit"* [P1]. As pointed out by one participant, data centres also need to mine in pools in order to sustain their profits: *"if you want to mine as an owner of a data centre then you need to have large capital [...] at the same time, you have to join a mining pool to make profit"* [P1]. To address these challenges Bitcoin data centres have started to emerge (Maurer, Nelms, & Swartz, 2013): *"the best option is joining the cloud mining, where you can buy a share from the owners of the data centre to do the mining for you"* [P9]. Compared to the home mining, data centres

require much larger capital and maintenance costs. These include not only the cost of electricity but also of the monitoring equipment and manpower to maintain the centre as illustrated in this quote of a data centre administrator: “*I used special software monitor [...] I can login from my mobile and I am able to gather data on the current temperature. I also hire a worker to ensure the cabling and network are well maintained*” [P6].

More than a quarter of participants valued the opportunity of data centre-pool mining because of the inability to setup their own mining pool: “*the difficulty today is very high and the electricity cost is expensive too. So it is not worth mining at small scale. I think for today, cloud mining is the best way*” [P13]. In addition, leasing the mining service does not require technical expertise: “*data centres offer a 3-year contract, when I get my daily profit from the hired miner [...] When I joined the program, I got the id and password to access to the company website, they also give me a wallet so all profit will be straight away sent to my wallet*” [P20]. Cloud mining is further appreciated because the challenge of machines’ maintenance is met by the data centre, as highlighted by a quarter of participants: “*for the cloud miners, you don’t have the miner at home. It is all maintained in the data centre [so] you don’t have to pay any utilities. But you have to pay to the owner of the data centre usually around 20% of the total profit*” [P5]. A similar quote: “*I need to pay around 30% of my daily profit for the maintenance fee to the company*” [P9]. These indicate that the skills of data centres’ administrators for setting and maintaining the mining machines comes at nontrivial cost for the end miners.

### 5.3.4 Types of Miners

Findings indicate four main types of miners: end miners, pool administrators, data centre administrators, and Bitcoin core developers. These types differ in their expertise, power over the practice, approach to mining and numbers, with the largest number represented by the end miners (Figure 5.3). Each of these is further discussed.



**Figure 5.3: Pyramid of types of miners**

#### 5.3.4.1 Mining Pool Administrators

Pool administrators have emerged within collaborative mining in order to facilitate miners' access to mining pools. Administrators' technical skills are more advanced than end miners' as they are required to set up, run and maintain the machines within the pools: *“currently there are many pools and all miners [...] need to go through those pools which are created by the Bitcoin administrators”* [P5], and *“such pools are hard to set up and maintain”* [P12]. Such specialised technical skills are not easy to master and have given administrators the advantage of controlling the mining activity and the distribution of reward. In addition, almost half of the participants also acknowledge the high level of skills required by administrators who act as pool manufacturers to develop more competitive mining chips. Mining pools could be

joined in by miners with different computational power from end miners owning own machines at home (increasingly unprofitable), to those owning mining farms, or data centres.

#### 5.3.4.2 Data Centre Administrators

The increased mining competition demanded higher computational power. This has made room for data centre administrators to enter the scene. They provided end miners the opportunity of leasing machines hosted and maintained within the data centres: *“my friend owns a data centre offering cloud mining service”* [P5]. The data centres also join mining pools in order to increase their likelihood of successful mining, but the decision of which pool to join is made solely by the administrator: *“the mining process is controlled by the mining pool”* [P6]. The privilege of pool administrator to distribute rewards to each entity in the pool according to the computational power brought in, cascades down to the data centre administrator who further distributes such reward to the end miners within the centre.

#### 5.3.4.3 End Miners

While miners, engaged in solo home mining, had to develop technical skills for setting and maintaining their own machines, the emergence of collective mining and of administrators supporting it, has led to end miners’ deskilling. More than half of the participants noted end miners’ limited technical expertise: *“it is very easy: I download the software from the pool, I do the setup [...] let my leased machine run for 24/7 [and] I monitor it to make sure that it doesn't crash and is connected to the internet”* [P10].

End miners have limited power, as they are at the discretion of pool administrators for distributing equitable profits. In order to remain competitive, they also have to follow the trend set by their pool administrator for upgrading their leased machines: *“as a miner, we must regularly update our mining machine according to the latest chips produced by the manufacturer, to ensure we are able to maintain the reward”* [P6].

### 5.3.5 Trust Challenges of Collaborative Mining

The benefits of collaborative mining are offset by some important trust-related challenges. These pertain to the risks of mining protocol and centralisation of mining practices, as well as the challenge of social trust between end miners and data centres/pool administrators.

#### 5.3.5.1 Risks of Mining Protocol

An important finding is the three challenges of the mining protocol pointed out by most of the participants. These relate to the increased time for acquiring block confirmation, limited block size, and limited number of full nodes. Interestingly, each of these technology-related risks stems from the purposefully designed Blockchain protocol. For instance, multiple confirmations required for recording a block was intended to limit the risk of double spending (Acheson, 2007; Caetano, 2015), but their numbers increased from 3 to 6 leading to delays: *“the 6 confirmations waiting time is bothering me a lot”* [P12], or unconfirmed blocks: *“there were also cases when there was no confirmation for quite sometimes, and the Bitcoins were eventually returned back to you”* [P19].

The current Blockchain protocol also limits the size of each block to 1MB and about half of the participants expressed concerns: *“this block size limits the*

*transactions acting as a bottleneck*” [P18]. This challenge has received considerable attention in the security field (Hearn, 2015), and led to increased mining’s competitiveness and incentive-based fees: *“people have to increase the mining fee to give a chance to their transactions to be included in the block; however, this removes the benefit of cheap transactions”* [P12]. Not at least, there is a shortage of full nodes designed to host a full copy of the Blockchain: *“we have about 6000 full nodes and the number is not sufficient to support the current demand”* [P1].

Although critical for the decentralisation of Blockchain, the full nodes are resource-demanding (Acheson, 2007), and many end miners lack the incentive to host them. Perceived risk in technology is one of the three factors in Corritore and colleagues’ model of online trust (Corritore et al., 2003). The findings point to these Blockchain design features as risks minimising end miners’ trust in the protocol, especially since they lack both control and high level expertise needed to address them.

#### *5.3.5.2 Dishonest End Miners: Selfish Attacks Unconfirmed*

A striking finding is our limited empirical evidence of selfish miners’ attacks commonly discussed in security research (Buterin, 2013b; Eyal & Sirer, 2014; Redman, 2016; Sapirshtein et al., 2015; Torpey, 2015). First, the majority of participants are not aware of such attacks. Second, for the few ones that were aware of selfish miners’ attacks, two out of three participants expressed optimism: *“for me, that is just a theoretical concern [because] such attack can only take place only if one has [considerable] computational power [which] I would say it is not possible”* [P1]. In addition, another participant extends this

argument claiming that even if selfish miners' attacks occur, they can be detected by the protocol: *"yes, this can happen [...] but after a while, the system will know [...] then the system will put the mining server to one side, so then other miners will know that they can't trust that particular mining server at this IP address"* [P7].

Thus, the findings support the theoretical perspective of Bitcoin core developers, as key stakeholders in the mining process (Kow & Lustig, 2018) on the reduced likelihood of such attacks (Buterin, 2013b; Torpey, 2015). Indeed, in his original white paper, Nakamoto (Nakamoto, 2008) mentioned that the Bitcoin network is secure, providing that the attacking power does not exceed the total collaborative power of the trust nodes. This may be different in the dystopian future suggested by two participants, where the advent of quantum computing may provide sufficient computational power to one pool for a 51% attack: *"current computing power is too high to hack [...] but with the future quantum computer [...] there is a possibility that the Bitcoin network will be affected"* [P18]. Although mining is an anonymous practice, the IP of the machine is visible online, acting as a proxy for its miner. While selfish miners can change their machines, this is unlikely to happen often, which means that the IP offers a history of the mining behavior's trustworthiness. This provides support for the temporal and social embeddedness as contextual properties of the framework on mechanics of trust (Rolnick & Weber, 1997).

#### *5.3.5.3 Centralisation of Mining Practices*

Findings indicate that mining is a highly competitive practice which requires increasing investment in computational power so that miners could continue to

generate profit. This trend is consistent with the planned scarcity of Bitcoins (Bitcoin.org, 2019). **Figure 5.3** shows that the distribution of power among miners is not equal, but concentrated towards the top and middle level of the pyramid.

Centralisation is critical with respect to miners' social trust as it entails power imbalance between end miners on the one hand, and mining administrators and core developers on the other hand. It is also aligned with higher technical skills, so that end miners joining pools face the risk of deskilling and of lower profit distributed by the pool administrators.

Centralisation of mining occurs both at pool level and between pools, with larger ones contributing with a higher percentage of computational power: *“there is a lot of centralisation in a mining pool. Each of the larger pools controls like 20-30% of the contributed hash rate. So miners were actually controlled by the pool that they joined”* [P12].

Findings also indicate centralisation by geography, with several participants acknowledging China's massive growth in miners' number [P6] and its dominance of Bitcoin mining practices: *“it may have the authority to control the Bitcoins price because its largest Bitcoin market share”* [P5]. This dominance is supported by China's low cost energy supply (Wilson, 2016) and effective mining techniques: *“they mine in a very professional way [through] lower and upper cooling systems and proper server racks [using] professional hydroelectric generator and water cooling system to reduce the cost”* [P16]. China also considers legalising mining practice (Evander, 2016) and is an innovation leader in mining manufacturing: *“capable of designing chips [...] to shrink the size and improve the mining process”* [P3]. These findings challenge the credibility of

mining behaviour, as a dimension of online trust in Corritore and colleagues' model (Corritore et al., 2003) suggesting that end miners' trust in higher level miners is negatively affected. It also indicates the perceived risk of centralisation, with risk being a limiting dimension of trust in the above model (Corritore et al., 2003).

### 5.3.6 Dishonest Mining Pool and Data Centre Administrators

This section further unpacks the challenge of social trust between end miners and data centres/ pool administrators. For this, the study describes its main sources, stemming from the limited regulatory framework for sanctioning dishonest behaviour: lack of audit for the distribution of rewards, invisibility of data centres offering cloud mining, and administrators' lack of accountability.

#### *5.3.6.1 Lack of Audit for the Distribution of Rewards*

The most common trust challenge of dishonest mining pools or data centre administrators relates to their privileged position of collecting the computational power of their end miners in order to proportionally distribute the rewards. Unfortunately, some administrators abuse this power, a trust issue mentioned by almost half of the participants: *“a trust issue between miners and pool administrators may arise because the administrators are responsible for collecting all the hashing power and distributing the accurate rewards to all miners”* [P3].

This challenge is due to the limited shared knowledge or audit trail of the pool's or data centre's overall hash power, which in turn, allows the administrators to report inaccurately smaller profits for their end miners. Indeed, dishonest administrators may claim higher hashes power to attract miners to join

in, but report underperformance with respect to the targeted amount of blocks, which in turn allows them to deliver unfairly smaller rewards: *“each [large] pool controls like 20-30% of the hash rate and this amount is not known by the miner”* [P12].

Prior work has confirmed this lack of transparency with respect to the pool’s hash power (Wirdum, 2016a). This outcome extends the value of online information for supporting website credibility (Beldad, Jong, & Steehouder, 2010; Fui et al., 2002) to mining pools and data centres, particularly the need for information regarding the overall computational power and transparent mechanisms for reward distribution.

#### 5.3.6.2 *The Invisibility of Data Centres*

An interesting finding relates to the lack of visibility of the cloud computing infrastructure underpinning data centres. Several participants pointed this out: *“I don’t have 100% trusts in all mining programs that I joined because it is something that I cannot see. I don’t even know if the data centre really exists”* [P8]. Even if the location of the data centre is known, the lack of visibility of the hired machine leads to additional trust challenges: *“I have invested my money, but actually, I don’t even see the machine that I bought. It is all kept in the data centre and all I was told is that it is based in Iceland”* [P20]. This lack of visibility of cloud computing is an important technology-based trust challenge which has started to be explored (Pearson & Benameur, 2010; Redman, 2016). The findings further highlight the importance of online information (Pearson & Benameur, 2010; Redman, 2016) to support trust in data centres, particularly in terms of their physical presence, contactable local representatives, testimonial-

based reputation, and authorisation from the local administration. Data centres are service providers which arguably should operate within a regulatory framework, and it is surprising that the findings suggest otherwise.

#### *5.3.6.3 Mining Program Scams: Lack of Accountability*

A critical trust challenge relates to deceitful mining programs mentioned by two participants, one of whom has been a scam victim: *“I have joined a mining program [...] at first everything looked fine: I received Bitcoins every day for 2 weeks, but then it stopped. I tried to contact the person who introduced me to that mining program but he couldn’t be reached and I realised that it was actually a scam”* [P8]. This quite illustrates the concern for leveraging data centres’ unfunded reputation for attracting end miners, since there are no legal implications of such dishonest behaviour. From the perspective of mechanics of trust’s framework, these findings shed light into end miners’ limited trust on higher level miners because of the lack of institutional embeddedness (Riegelsberger et al., 2005) for legally sanctioning more powerful miners acting dishonestly.

#### *5.3.7 Mitigating Trust Risks of Collaborative Mining*

Findings indicate that end miners employ two strategies for mitigating the risks of social trust in pool or data centre administrators. These include selecting reputable major pools, and decentralising collaborative mining.

##### *5.3.7.1 Selecting Reputable Major Pools*

To address the risk of mining program scams and of unfair distribution of rewards, most miners engage in careful scrutiny of the pool to be joined: *“you*

*must make sure to choose a reputable pool*” [P3]. This is not trivial as findings indicate that the information provided by the data centres to support such scrutiny is limited which in turn adds to their invisibility challenge.

Unsurprisingly, reputable pools are large and most miners select major pools: *“the main thing is to make sure that the pool is good enough, by looking at the pool contributions and if it is about 30% of the overall, then I think it is good enough”* [P18]. Through their proven history of acting in good faith, reputable major pools offer proxy ways towards reputation, through the motivation to preserve future behaviour. This strategy confirms the framework on mechanics of trust (Riegelsberger et al., 2005) on warranting end miners’ trust in pool administrators because of their reputation (social embeddedness and credibility), albeit not institutional embeddedness. Prior work has emphasised the importance of accountability in cloud computing to be supported both technically and legally (Riegelsberger et al., 2005). While reputable pools are perceived as fair, they are not necessarily regulated in terms of being accountable for failing to deliver their contracts with end miners. Indeed, pools do not divulge the identity of their administrators other than by their IP addresses.

#### *5.3.7.2 Decentralising Collaborative Mining*

A consequence of end miners’ preference for reputable large pools is their growth in size, to an extent that such pools could challenge the decentralisation principle of mining protocol (Caetano, 2015). A major concern here is that when largest pools are getting close to representing 50% of the network’s hash power, they can enable serious negative behaviours such as reversing transactions and double spending (Buterin, 2013b; Sapirshtein et al., 2015; Torpey, 2015). In an

attempt to address miners' centralisation and circumvent pool administrators, miners have engaged in "*initiatives to build decentralised pool such as the P2Pool*" [P12]. Such pools benefit from the advantage of collaborative mining but without the need of a central administrator (Gervais, Karame, Capkun, & Capkun, 2014). This strategy strengthens the pool's credibility and reputation, reducing the risk of administrators' abuse of power. A limitation of these decentralised pools is that they are challenging to build, currently small with limited share of the network's computational power and need time to grow (Gervais et al., 2014). An alternative strategy to address the challenge of centralisation of collaborative mining is its self-organisation, with miners voluntarily leaving those pools at the risk of gaining too much hash power, or administrators incentivising such behaviour by increasing the pool's fees (Hajdarbegovic, 2014). These strategies strengthen the credibility dimension of online trust depicted in Corritore and colleagues' model (Corritore et al., 2003), as well as the intrinsic properties warranting trust from the framework on mechanics of trust (Riegelsberger et al., 2005) such as benevolence and trustworthiness of end miners and pool administrators.

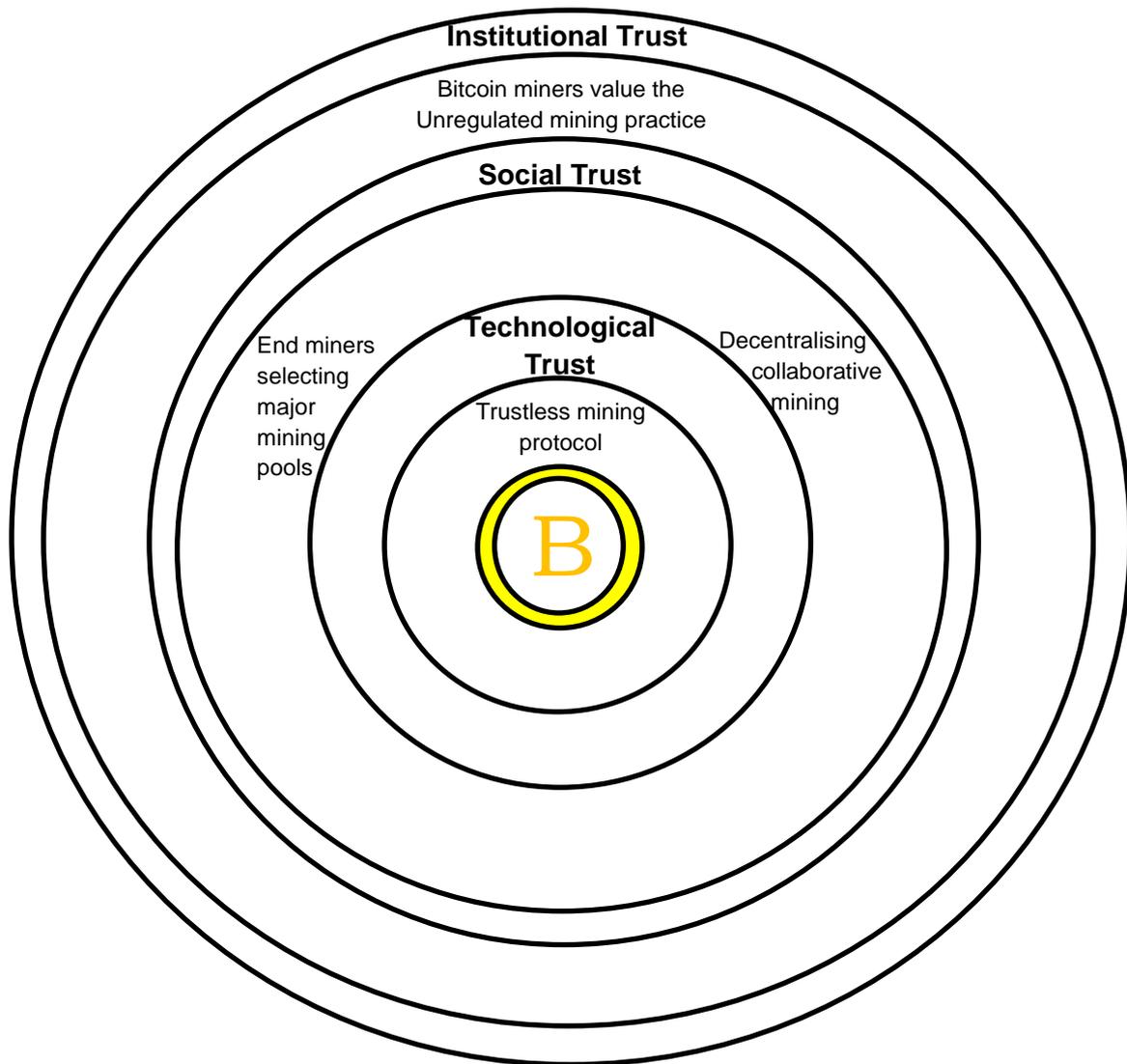
#### 5.4 Theoretical Implication

This section discusses the value of the findings for HCI research on trust. Recent work has argued that the exploration of Bitcoin-related practices offers unique opportunities to understand trust, as they challenge common assumptions of financial transactions' centralisation and regulation (Sas & Khairuddin, 2015). Given the study's focus on a developing country, the implications are mostly relevant for mining in such contexts. They may also hold value for understanding and supporting trust in Bitcoin mining

practices worldwide, as future work in this emerging research area may focus on exploring.

#### 5.4.1 Towards a Framework of Trust among Bitcoin Miners

The findings contribute towards a model of trust among Bitcoin miners. They extend previous outcomes on the feasibility of HCI trust theories (Corritore et al., 2003; Riegelsberger et al., 2005; Sas & Khairuddin, 2015) and their application not only to Bitcoin users (Sas & Khairuddin, 2017) but also to miners (**Figure 5.4**). The study identified Blockchain's characteristics impacting on trust. Those supporting trusts include the decentralisation, unregulation, and ease of use of the mining protocol, while those impeding trusts consist of specific protocol-related risks, the emerging centralisation of the mining practice, and dishonest pool and data centre administrators.



**Figure 5.4: Framework of Bitcoin Trust for Miners**

According to Sas and Khairuddin's (Sas & Khairuddin, 2015) Bitcoin trust framework, the findings indicate that the purposefully designed decentralisation and unregulation strengthen miners' technological trust. With respect to social trust, outcomes suggest that the main challenge is not among end miners, but between end miners and dishonest pool and data centre administrators. In return, findings suggest that the end miners who decided to mine in a major pool also prefer to create a decentralised pool for mining. In terms of institutional trust, similar to Bitcoin users, miners distrust financial and government institutions, but the unregulation of mining

practices mitigates their perceived risk of abuse of power (Subramanian & Chino, 2015). Interestingly, because of the unregulation, governments' trust in mining practice is lacking behind.

The application of the model of online trust (Corritore et al., 2003) indicates miners' ambivalence towards the technological trust in mining protocol. Findings highlight specific protocol related characteristics impacting on the three dimensions of trust: credibility, ease of use, and risks. In addition to decentralisation, the credibility of the trustless mining protocol is ensured by its transparency, social organisation, competitiveness, predictability, reputation, and embedded high level expertise of the core developers. Miners' trust in the protocol is also supported by its ease of use, but challenged by the risks of increased time for acquiring block confirmation, limited block size, and number of full nodes.

The framework on mechanics of trust (Riegelsberger et al., 2005) allowed the study to explore the social trust among different types of miners and in particular the end miners' risk mitigation strategies for dealing with dishonest pool and data centre administrators. Interestingly, although the trust among end miners has not been flagged as salient, the continual use of a mining machine offers through its IP a proxy indicator for miner's reputation (temporal and social embeddedness) (Pearson & Benameur, 2010). However, given the invisibility of cloud mining, administrators' reputation is more critical and therefore mechanisms for signalling it are much needed. Additional reasons include the risk of scam due to administrators' lack of accountability and lack of audit for the distribution of mining rewards. To address these risks, end miners' select large pools which have been around for a while and have gathered a large number of end miners. Pools' history offers a proxy for their reputation (social embeddedness and credibility), but their administrators

continue to lack the ability to be legally sanctioned for dishonest behaviour (Riegelsberger et al., 2005). The study also follows Sas and Khairuddin's (Sas & Khairuddin, 2015) Bitcoin trust framework which consists of three dimensions: institutional, social, and technological trust, to conceptualize miners' trust. Institutional trust can be seen as capturing miners' limited trust in the centralised financial system; social trust as describing the credibility of well-known, large mining pools, while technological trust as capturing perceived credibility of transparent mining procedures, perceived ease of use of such structured mining procedures, and perceived risk regarding for instance the timeliness of block confirmation, limitation of block size and that of insufficient number of full nodes.

## 5.5 Design Implication

This section discusses the design implications (Sas & Khairuddin, 2017) that the findings entailed. They highlight the value of new tools for monitoring hash power and reward distribution in data centres and mining pools, decentralised tools for tracking data centres' authorisation and reputation, and authoring tools for supporting end miners' development of decentralised pools. These design implications have been developed to address the identified social trust challenges of dishonest administrators, and the risk of centralisation of mining practices.

### 5.5.1 Tools for Monitoring Hash Power & Reward Distribution

Findings indicate that the most challenging social trust issue of collaborative mining is the unfair distribution of rewards that pools' and data centres' administrators are privileged to perform. This is rooted in a lack of audit of pool's and data centres' computational power. The contracts between miners and pool administrators state the fixed hash rate that the miner will contribute to the pool

over a period of time, for which s/he will be rewarded. The study knows little, however, about the legally bounding nature of such contracts or about the consequences for dishonest administrators. Moreover, because of anonymity and lack of regulation, miners tend to enjoy untaxed rewards, but this comes at the cost of limited opportunities to legally mobilize and unionize themselves as a workforce. Future work can explore miners' and administrators' contractual obligations and the feasibility of Blockchain smart contracts to support them and better protect miners from exploitative relationships. This opens up design opportunities regarding smart contracts to ensure fair rewards and to better support less regulated social contracts.

Another way to address this challenge is to design monitoring tools to support such an audit and provide transparent mechanisms for the distribution of rewards. Such tools will automatically capture and report key metrics involved in the calculation of profits: overall percentage of pools' or data centres' computing power contributed to the network, the number of solved blocks within time unit, the total computing power used to solve each block (Buterin, 2013b; Wirdum, 2016b) as well as daily total reward, together with the percentage of profit due to each end miner based on their individual power contribution. Mechanisms to implement these have started to emerge, for instance, in Slush Pool's transparent calculation of hash-proof-rate (Slush Pool, 2017). This could be extended with open source monitoring dashboards accessible to end miners.

#### 5.5.2 Decentralised Tools Tracking Data Centers' Authorisation and Reputation

Study outcomes also highlight social trust challenges related to the invisibility of cloud mining and lack of accountability of data centers' administrators. In addition to administrators' willingness to share online information regarding their

data centre's authorisation, their social and institutional embeddedness (Riegelsberger et al., 2005) can be further strengthened. For example, there are already attempts to centralise information on authorised data centres offering cloud mining services ( Adoga, Rabi, & Audu, 2014). Data centres' online resources can be aligned with heuristics for trustworthy websites (Sillence et al., 2006) that can be tailored to the data centres' websites to increase their trustworthiness among the miners, i.e., trust cues. In addition, the data centres themselves can become authorised and recorded in the Blockchain through smart contracts containing details such as data centre's physical location which will be transparent to all current and future miners. This again can open up opportunities to explore smart contracts and their affordances to better support communication of data centres' trustworthiness. The study can also imagine tools included in database interface for supporting end miners to provide reputation feedback. This, in turn, can help miners to make informed choices for joining specific data centres.

### 5.5.3 Tools for Developing Decentralised Pools

Findings indicate the risk of mining's centralisation in larger pools which conflicts with the decentralisation principle of Blockchain and mining protocol (Acheson, 2007). A strategy for addressing this challenge is the development of fully decentralised pools with no central administrator. Although this has been previously suggested, the development of such pools requires technical competency not easily available among end miners (Gervais et al., 2014). One solution would be new authoring tools supporting and incentivising end miners to develop decentralised pools. Their design can benefit by drawing from research on the end-user development of open source software and their design tools (Sas & Neustaedter,

2017). The study can also think of opportunities to create design platforms to not only train but also to incentivize miners to create their own mining pools. This design implication also aligns with prior views, such as Buterin's (Buterin, 2013a) suggestion for open source cross-platform applications (Sharma, 2017) allowing end miners to create mining pools through simple user interfaces.

## 5.6 Chapter Summary

The interview study described in this chapter explored Blockchain's characteristics fostering and hindering miners' trust, and, in particular, the risks of collaborative mining and miners' strategies for mitigating them. The study further advanced the theory towards a model of Blockchain trust by discussing how decentralisation, unregulation, ease of use, and social organisation impact on both technological and social trust among different types of miners. Findings also led to three design implications that will support Blockchain miners develop trust in pool and data centre administrators, or circumvent their role together. Advances the understanding of miners' work practices on Blockchain in this chapter, offers the opportunities for materialising the Blockchain infrastructures that will be discussed in the following **Chapter 6**.

# Chapter 6

## Construction of BlocKit

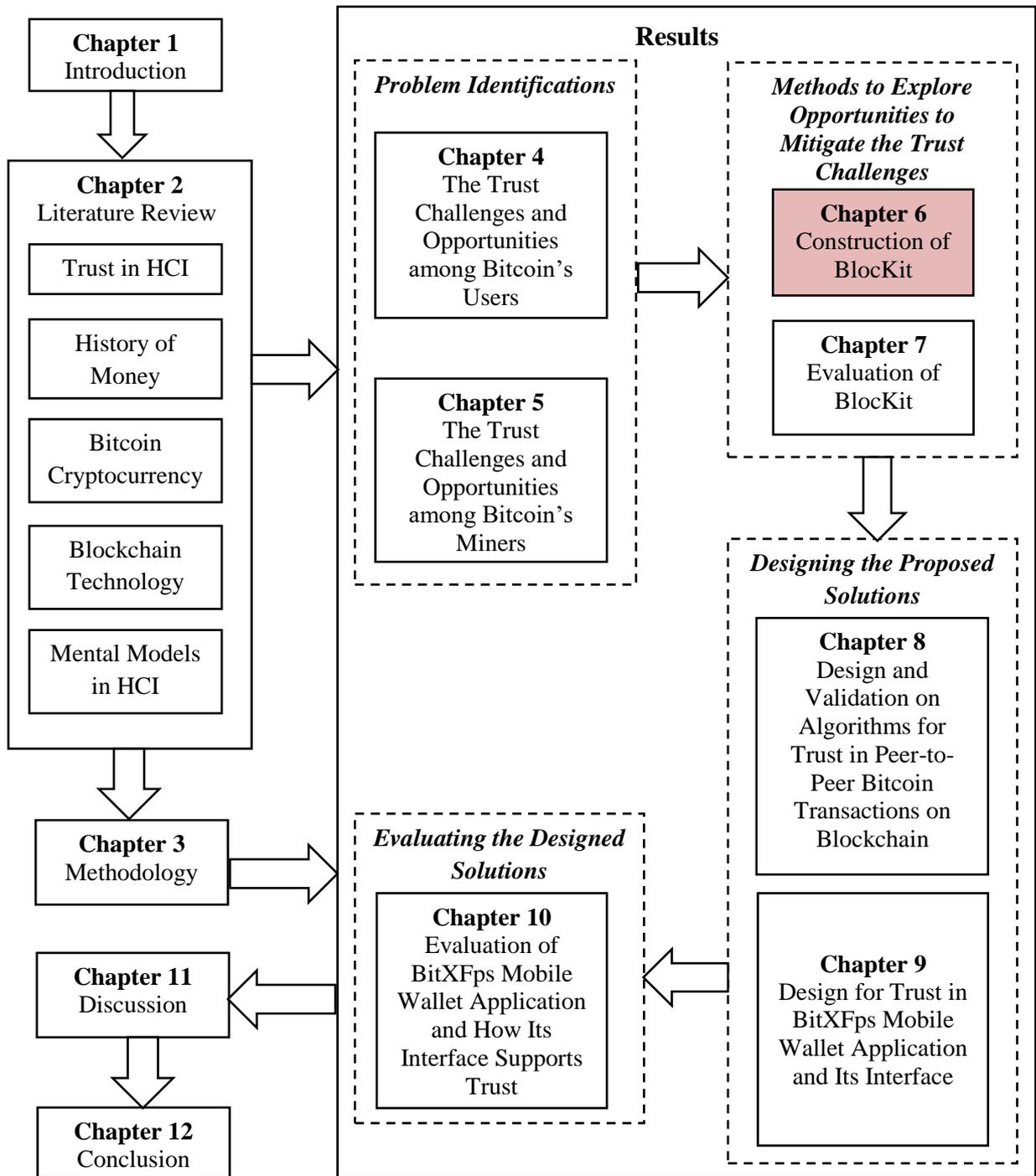


Figure 6.1: Chapter 6 of Thesis Structure

## 6.1 Introduction

Blockchain is a disruptive technology which has significantly challenged assumptions that underpin financial institutions and has provoked innovation strategies that have the potential to change many aspects of the digital economy. However, because of its novelty and complexity, Blockchain had challenged people's understanding of its inner working. Due to its complexity, different modalities have been explored to communicate the principles of the Blockchain, and support their understanding and learning primarily through visual representations in the form of infographics (Cartwright, 2018) or (The Guardian, 2014) video. In contrast, the value of physical objects for communicating about Blockchain has been limitedly explored, with some preliminary work suggesting the value of Lego blocks for Blockchain experts and novices to communicate and describe its entities (Maxwell et al., 2015). However, this study argues that there is an untapped potential of physical three-dimensional artefacts to not only communicate about Blockchain but also to support the understanding of the key properties of its core entities and the provision of a richer vocabulary to talk about them.

Thus, building on the understanding of miners' practices on Blockchain from **Chapter 5**, and the concepts of embodied cognition and material centred-design, this chapter reports an innovative approach to the design of BlocKit: a physical three-dimensional kit for materialising Blockchain infrastructure and its key entities. Through an engagement with different materials such as clay, paper, or transparent containers, the study identified important properties of 11 Blockchain entities and materialised them through physical artefacts.

## 6.2 Designing BlocKit

The study employed the physical design framework (Wiberg & Mikael, 2014) to design the BlocKit and its objects. Based on literatures (Antonopoulos, 2010; Nakamoto, 2008) and empirical findings (Khairuddin et al., 2016; Khairuddin & Sas, 2019; Sas & Khairuddin, 2015, 2017), the study identified 11 key entities of Blockchain infrastructure: Bitcoins wallet (Antonopoulos, 2010; Caetano, 2015; Sas & Khairuddin, 2017), wallet password (Caetano, 2015) private and public key as elements involved in transactions (Caetano, 2015), miners' computational power (Antonopoulos, 2010; Caetano, 2015; Khairuddin & Sas, 2019; Sas & Khairuddin, 2017), block (Antonopoulos, 2010; Caetano, 2015; Khairuddin & Sas, 2019) proof-of-work, and its timestamp (Antonopoulos, 2010; Caetano, 2015; Khairuddin & Sas, 2019), as elements reflecting miners' work on Blockchain ledger, and Blockchain technology itself. The study now outlines the key properties of these Blockchain entities and the linguistic analysis of their relevant image schemata (Hurtienne, 2009).

### 6.2.1 Identifying the Properties of Blockchain's Key Entities

The key properties of the identified Blockchain's entities are outlined in **Table 6.1**. A reflection on these concepts, grounded again on prior work, allowed the identification of their properties, briefly defined, alongside their rationale. For example, as a currency, the key properties of Bitcoins reflect traditional properties of money (Trivedi, 2018) such as fungible as Bitcoins are interchangeable (Hayes, 2015.), divisible as each Bitcoin can be divided into 100 million smaller parts (Antonopoulos, 2010), and scarce as the total number of Bitcoins is capped to 21 Million (Trivedi, 2018). Bitcoins are also portable as Bitcoins' ownership can be transferred and they can be hosted on multiple devices (Antonopoulos, 2010;

Caetano, 2015), and durable as Bitcoins are meant to last indefinitely (Trivedi, 2018), verifiable as each Bitcoin transaction is recorded in the public ledger (Antonopoulos, 2010), safe as they are protected by their owner (Khairuddin & Sas, 2019) and private as the ownership is private (IG Analyst, 2017). The wallet, its password as well as the public and private keys are also portable (Antonopoulos, 2010; Caetano, 2015), verifiable, and safe because of cryptographic protection (Antonopoulos, 2010; Caetano, 2015; Khairuddin & Sas, 2019). While all these elements are visible to their owners, the wallet and public key are also visible within the Blockchain, or transparent (Antonopoulos, 2010; Caetano, 2015; Khairuddin & Sas, 2019).

Entities	Properties									
	Fungible	Divisible	Scarce	Accepted	Durable	Transparent	Portability	Verifiable	Safe	Private
Bitcoins	✓	✓	✓	✓	✓	X	✓	✓	✓	✓
Wallet				X	X	✓	✓	✓	✓	✓
Wallet's password				X	✓	X	✓	✓	✓	✓
Public key				X	X	✓	✓	✓	✓	X
Private key				X	X	X	✓	✓	✓	✓
Miners' computational power				X	X	✓	✓	✓	✓	X
Consensus rule				✓	✓	✓	✓	✓	✓	X
Block				X	✓	✓	✓	✓	✓	X
Proof-of-work				✓	✓	✓	✓	✓	✓	X
Timestamp				X	✓	✓	✓	✓	✓	X
Blockchain ledger				✓	✓	✓	✓	✓	✓	X

**Table 6.1: Properties of Blockchain's Key Entities**

With respect to miners' work, their consensus rule, block, proof-of-work and its timestamp are all transparent, verifiable, durable and safe, being protected

through a secure cryptographic hash function (SHA-256) (Antonopoulos, 2010; Caetano, 2015). Underpinning the commonly agreed consensus rules for block verification (Caetano, 2015), the specific block of transactions to be verified, miners' proof-of-work and its timestamp are all publicly visible to be scrutinised (verifiable) by other miners before they are accepted (Caetano, 2015; Khairuddin & Sas, 2019).

The Blockchain technology itself is also transparent and verifiable, as with the exception of wallet password and private keys, all its other entities are visible and open for public scrutiny, or verification (Antonopoulos, 2010; Caetano, 2015). Blockchain technology has been also designed to be safe given its mathematical and cryptographic foundation (Caetano, 2015; Khairuddin & Sas, 2019) and portable as the public ledger can be accessed on multiple devices in the network. Although theoretically, it is possible for a large amount of computing power to change the existing records in the Blockchain, the ledger has been proven as durable and protected by the consensus rules (Bitcoin Wiki, n.d.; Caetano, 2015; Khairuddin & Sas, 2019).

### 6.2.2 Image Schemata for Blockchain's Key Entities

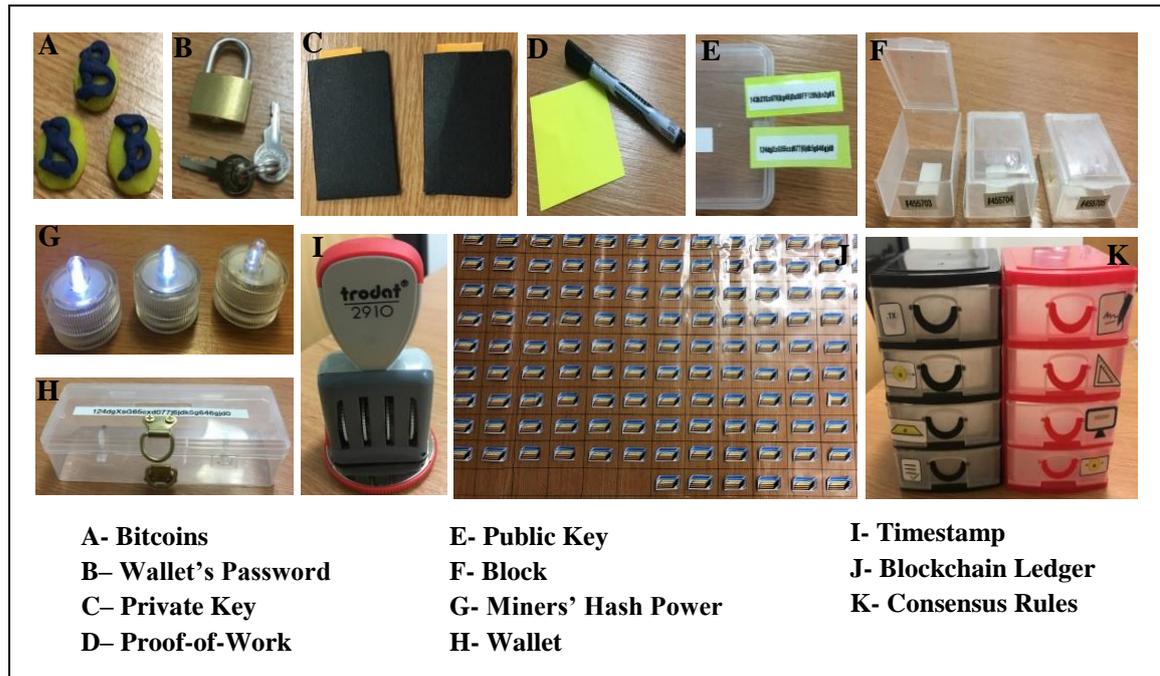
According to image schemata theory (Hampe & Grady, 2005; Johnson, 1987) and linguistic analysis, most entities can be best described as containers, while Bitcoins and blocks are described as part-whole schemata. For example, Bitcoins can be represented as a whole, i.e., 1 Bitcoin, or part, i.e., fractional Bitcoin amount in 8 decimal points; while wallet can be represented as a container in and out of which one can move Bitcoins, private key, and public key.

Entities	Linguistic Analysis of Entity's Activities	Image Schemata
Bitcoins	Whole → 1 Bitcoin Part → Any fractional Bitcoin amount in 8 decimal points	Part-whole
Wallet	In → Bitcoins, Private Key, Public Key Out → Bitcoins, Private Key, Public Key	Container
Wallet's password	In → Wallet Credential Out → Wallet Credential	Container
Public key	In → Wallet Identity Out → Wallet Identity	Container
Private key	In → Unspent Bitcoins Out → Spent Bitcoins	Container
Consensus rule	In → New Bitcoins transaction, New Block Out → Validated transaction, Confirmed block	Container
Block	Full → Unprocessed transaction in the memory pool Part → Selected unprocessed transaction in a block	Part-whole
Miners' computational power	In → New Unconfirmed block, Mining Difficulty Out → New confirmed block	Container
Proof- of- work	In → Mathematical Algorithm Out → Solution to Mathematical Algorithm	Container
Time Stamp	In → Proof-of-work Out → Time for proof-of-work	Container
Blockchain ledger	In → New confirmed block and its' metadata Out → New Bitcoins' ownership	Container

**Table 6.2: Image Schemata of Blockchain Entities**

### 6.2.3 BlocKit's Objects

To identify the physical objects to represent Blockchain's key entities (**Table 6.2**) and their image schemata, the study employed Wiberg's (Wiberg & Mikael, 2014) framework to inform the choice of their materials. For example, for Bitcoins the study first explored materials such as paper and magnetic sand this supports divisibility, i.e., splitting a unit into smaller parts. However, such material fails to provide support for other key properties such as durability, i.e., a paper is too fragile, and magnetic sand lacks firm structure. Hence, the study chose clay which is both divisible and durable, and shaped into small discs resembling coins with the symbol 'B' added on top.



**Figure 6.2: BloKit Representation of a Blockchain's Entities**

For the wallet, the study started exploring materials such as wood or metal-safe boxes, which can be locked. However, such materials fail to account for wallet's transparency thus; the study chose to represent the wallet through a clear plastic box with a coin slot to allow for the visibility of depositing coins, as well as a toggle latch ensuring security. In addition, as each wallet is protected by a password which cannot be retrieved, if the owner loses the wallet's key, the study chose a metal padlock and its physical key which can also be displaced and no longer found, but at the same time both the padlock and its key are made of durable, metal material symbolising the sturdy character of the password. To represent the public keys and their transient character, the study explored sticky notes which is made of paper is less durable or safe. Through their inherent ability to attach themselves to other objects, sticky notes are good candidates for communicating public keys' ability to be attached to and travel with the wallet (portable). The study

also provided an additional black envelope for the private key to communicate its privacy.

To represent the consensus rules, the study started using a container for each rule. However, rules are interlinked, and so should be these containers, hence, the study chose a transparent drawer on whose compartments the study placed symbols representing the rules, such as verifying the digital signature, double spending and the block file format. For the block whose role is to hold a collection of unconfirmed transactions, the study chose a transparent plastic box that can be opened and closed (but not necessarily locked). Miners' computational power is linked to their machines. At first, the study thought to represent it with a miniature model of a personal computer but realised that this fails to capture variation in miners' computational power. Thus, the study decided to use a battery powered-object such as candlelight whose variation in brightness level can be controlled and can metaphorically represent different levels of computational power, i.e., more bright is more power.

As proof-of-work involves solving a numerical problem, the study used post-it paper and pen as metaphorical tools for solving the problem. Given the importance of assigning time-stamp to the proof-of-work, the study used a physical stamp. The representation of Blockchain ledger consisted of a clear plastic sheet overlaid with an additional clear plastic sheet of equal size on which the study drew confirmed blocks organised in a grid or two-dimensional array. This was intended as a metaphor for the interrelationships among blocks (Hampe & Grady, 2005) shows the representations of the Blockchain entities.

### 6.3 Chapter Summary

BlocKit is a physical representation of Blockchain infrastructures that was built based on the entities properties, embodied cognition theories and material centred-design. The BlocKit was constructed as a new methodological approach to design on the Blockchain, in particular, with the aim to externalize the complex Blockchain infrastructure to facilitate the users' understanding and communication in the exploration to design for trust in Blockchain. However, it requires validations by the Blockchain's' experts as well as the novices that will be discussed in the next **Chapter 7**.

# Chapter 7

## Evaluation of BlockKit

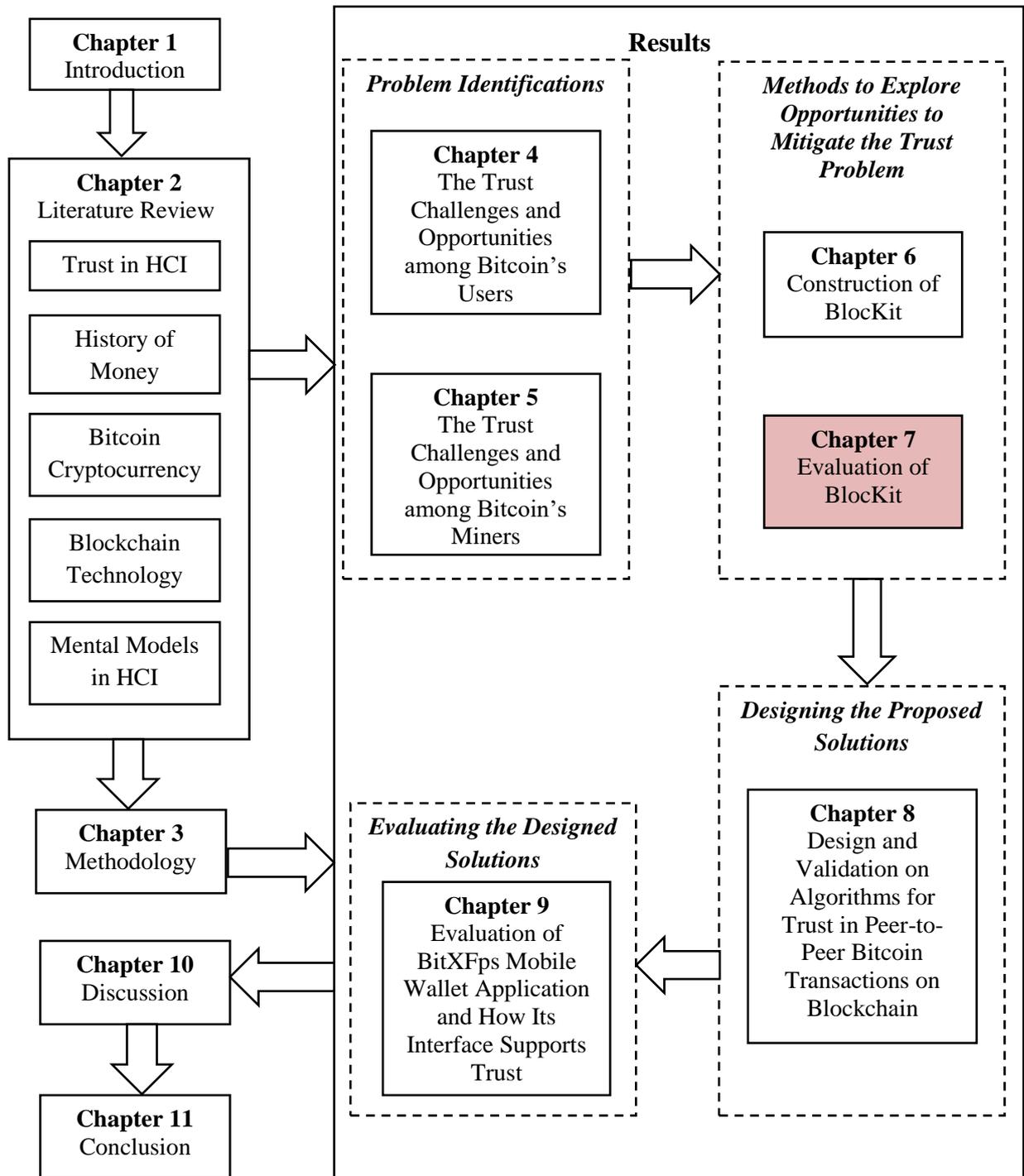


Figure 7.1: Chapter 7 of Thesis Structure

## 7.1 Introduction

The sophisticated technology of Blockchain was designed with core characteristics such as transparent and decentralised that support the users' trust towards the technology, as reported in Study 1 (Chapter 4). However, the highlighted issue from the finding in Study 1 is on the social trust among the users in conducting peer-to-peer transactions for the exchange of Bitcoin and physical goods or fiat money. Although Bitcoin transactions are transparent on Blockchain, the process of sending the physical goods or fiat money is not. This leads to issues of trust such as dishonest trader, scams and fraud. Mitigating actions among users have been taken such as by trading with authorised exchanges<sup>1</sup>, socially authorised traders<sup>2</sup>, reputable individual traders<sup>3</sup> or de-anonymised individual traders<sup>4</sup>. This study argues that there are opportunities to mitigate the issue on Blockchain. In making the efforts to explore the design for trust on Blockchain, it is hard to understand and communicate with the complex technology of Blockchain. Thus, the construction of BlocKit in Chapter 6 offers an exploration to verify the abilities of this DIY kit for design as well as to support the understanding of Blockchain.

In order to evaluate the BlocKit, a study has been conducted (Study 3) with Bitcoin Blockchain experienced users. The participants were presented with the 11 objects of BlocKit with the aim of addressing the following research questions:

- *how can complex infrastructure such as Blockchain technologies be thought about and communicated through a physical kit?*

---

<sup>1</sup> Authorised Exchanges – The registered company for Bitcoin exchange (Sas & Khairuddin, 2017)

<sup>2</sup> Socially authorised traders – The well-known members who are active in Bitcoin trading in online groups (Sas & Khairuddin, 2017)

<sup>3</sup> Reputable individual traders – Traders that are recognised by few members in online group who had experience trading with that particular trader (Sas & Khairuddin, 2017)

<sup>4</sup> De-anonymised individual traders – completely unknown trader and deanonymised actions are taken for the transactions, such as face to face meet up. (Sas & Khairuddin, 2017)

- *how does the development and engagement with a physical kit support understanding of Blockchain entities and their key qualities?*
- *how can trust among Bitcoin users be materialised and designed for through BlocKit?*
- *what are the requirements to design for trust among Bitcoin users?*

The findings describe the Bitcoin Blockchain experienced users' experience in interacting with the kit and its value as a model materialising Blockchain. In the light of this evaluation, the findings discussed the suggestion for objects revisions, as well as the BlocKit's impact on conforming, strengthening, or even challenging Bitcoin Blockchain experienced users mental models of Blockchain infrastructure. Their engagements with BlocKit to explore the design for trust are also reported, as well as their suggestions for the principles and requirements to design for trust in Bitcoin users.

## 7.2 Research Method

Study 3 reports on a workshop with 15 Bitcoin Blockchain experienced users, 12 males, 3 females, and (mean age 29, range 21-39). All participants had at least 2 years of engaging in Bitcoin transactions: 9 had between 2 and 3 years, 4 had between 4 and 5 years, 2 had more than 6 years. All participants have at least graduate education, i.e., 6 BSc, 7 MScs, and 2 PhD Participants were recruited through the mailing lists of two universities, and through a local Bitcoins meetup group.

The workshop involving the use of the BlocKit and consisted of two parts to explore the mental models of the Bitcoin Blockchain experienced users, also how they materialise trust. The study started by asking them how Bitcoins transactions take place on the Blockchain after the study showed them the BlocKit's 11 objects to simulate transactions while thinking aloud.

The participants were also been asked questions about challenges of identifying objects' and their role in Blockchain: "*what are you looking for*", "*why do you think this object does not work for you*" or "*how should this Blockchain entity be better represented*". In the second part, the study provided two round-shaped pieces of clay, one green and one red representing trust and distrust token, respectively, and asked participants to include them in Bitcoin transactions while thinking aloud. The whole workshops lasted between 60 and 90 minutes, were video recorded, and fully transcribed.

Data analysis involved a hybrid approach with concepts from the deductive coding and new ones emerging from the empirical data, contributing to the inductive coding (Fereday & Muir-Cochrane, 2006). The deductive codes included concepts such as functional and structural mental models (Hegarty & Just, 1993; Jack, Chen, & Jackson, 2017; Lowe & Boucheix, 2008) as well as the concepts related to image schemata (Hurtienne & Israel, 2007; Johnson, 1987) and elements required for the development of physical design kits (Wiberg & Mikael, 2014). The coding list was iteratively revised in the light of the interview data, as new codes emerged under the themes of properties of Blockchain's entities, and their materialisation.

### 7.2.1 Finding 1: Understanding BlocKit

This first finding section describes the outcomes from the study interviews focusing on the subjective experience of interacting with the kit, and its value as a model materialising Blockchain. For the latter, the study looked at BlocKit objects' effectiveness in conveying the appearance and meaning of the represented entities. In the light of this evaluation, the study also discussed the revised objects, as well as the BlocKit's impact on conforming, strengthening, or even challenging

experienced users' mental models of Blockchain's infrastructure and how the BlocKit supported the revision of some of its assumptions.

#### *7.2.1.1 Experienced Users' Experience of Interacting with BlocKit*

A striking finding was the overwhelmingly positive experience supported by BlocKit. Findings show that 10 participants deeply enjoyed physically touching its objects and enacting their movement in space while talking about Blockchain processes: *"there is going to be other transactions from other people essentially, so let's put a few Bitcoins in that box. I love this stuff, this is amazing"* [P12]. Participants suggested that BlocKit could be a valuable tool for learning about Blockchain: *"I think this all makes sense and would be fine to explain to the novices. It is cool, this is really an interesting kit"* [P7]. Other participants suggested leveraging gamification principles for learning about Blockchain: *"It's almost like you could turn this into some kind of cool game like a monopoly"* [P5].

Findings show that the enjoyment is due to the powerful analogies used as examples to represent miners' computational power [P1, P2, P3, P6, P7, P10, P13, P15], the timestamps [P1, P3, P4, P6, P7, P8], the Bitcoins [P1, P2, P3, P4, P6, P7, P8, P9, P12] and the wallet [P2, P4, P5, P6, P7, P9]. For instance: *"I like the analogy with different shades of lights. It means like this miner has higher computing power and more chances to solve the block"* [P15] and *"cool! I think that' this [wallet] is a perfect analogy. Yes, you can't think of anything really to physically represent it"* [P7]. Such strong positive responses to BlocKit were also reflected in participants' facial expressions while using it, such as intense smiling accompanied by utterance such as "wow" [P1, P2, P14], or *"this is pretty cool"*

[P7]. Such positive emotions lasted throughout the entire study, peaking when holding or moving the objects.

#### 7.2.1.2 Immediate Recognition of Kit's Objects

The study now reports participants' ability to immediately recognize each Blockchain's entity and the ways in which they interacted with them. In other words, the study explored the kit's ability to communicate affordances for gesture-based interaction with the artefacts. The study also reports participants' feedback on the kit and its objects.

- **Recognition Based on Objects' Properties and Appearance**

Findings indicate the importance of transparency as a key Blockchain property. Twelve participants recognised the objects because of the translucent materials that the study used, especially for the Bitcoin wallet and block: *“yeah, it is transparent [plastic box] and you can see the Bitcoins [...] I would rather go for this one for the wallet [compared to a wooden box]”* [P8]; and *“[the block] is transparent because you can see all transactions held in one block”* [P7]. This provides support for the choice of transparent materials representing entities with transparent properties.

Portability was clearly recognised as participants were engaged with the objects and moved them around. This worked particularly well for miners' computational power, as mentioned by more than half of participants: *“[computational power] can be arranged in a group to show that miners work in a pool, or it can be moved out from the group to work as a single miner”* [P11]. This suggests the value of artefacts for externalising and more importantly for

interacting with the mental models, which non-interactive models represented by either static or animated visual material cannot support. More importantly, with respect to computational power, portability allows for ad-hoc reconfiguration of miners' work, which in turn highlights different types of miners. Arguably, portability is supported by each physical entity – which can be held and moved in space – however, the study can see how it becomes even more relevant for representing entities which are shaped by spatial relationships, i.e., miners are geographically distributed. The study argues that portable objects are particularly important for representing infrastructures such as Blockchain, as their spatial organisation help reveal the distributed work of different stakeholders and their types.

Divisibility becomes apparent while handling the coins and simulating their movement in space during transactions. The clay material chosen to represent Bitcoins was found particularly evocative in supporting the affordance of divisibility: *“obviously this yellow plasticine is Bitcoins and I can pinch in whatever size, to show the amount spent”* [P6]. This quote is illustrative of most participants' perception and appreciation for the choice of clay, and its adequate support for the part-whole image schemata. The only security property recognised by most participants was the wallet: *“I presume this padlock would represent some form of security mechanism, so perhaps for the Bitcoin wallets, say the password”* [P2].

Findings also indicate the value of container as image schemata, whose affordances for interaction further supported such recognition: *“there is this hole on top [of the wallet box] for you to put in the Bitcoins, and you can open the lock to take out the Bitcoins”* [P10]. This quote illustrates similar views shared by the

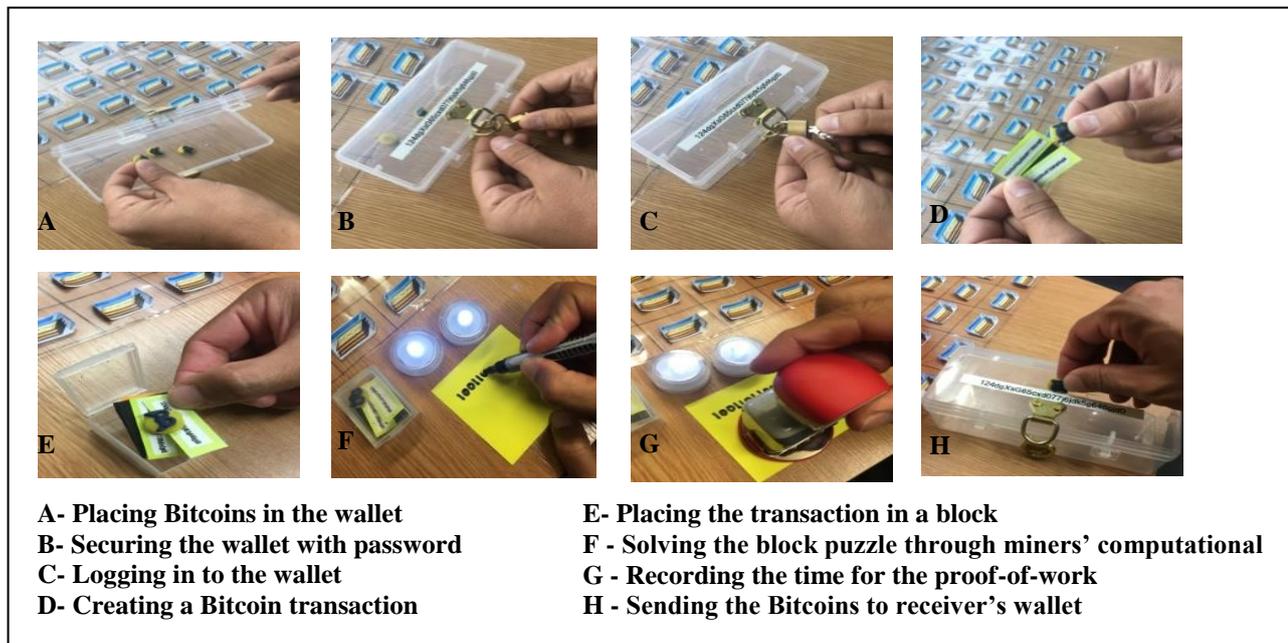
other five participants. Container schemata also provided support for the recognition of the block: *“I put the transaction in the box [and] once it is confirmed, I can open the box to take out the Bitcoins and send them to the receiver’s wallet”* [P5].

Object recognition was also facilitated by their physical appearance (Wiberg & Mikael, 2014) designed to mirror the characteristics of their counterpart entities. For instance, the rubber stamp was easily associated with the proof-of-work’s [P1]. More than half of participants appreciated the sticky notes paper that was used to represent the public key: *“this is the public key, it [alphanumeric on the sticky notes] matches the address on the wallet address here”* [P15].

- **The Role of Gestures in Understanding Connections among Objects**

In order to enact a transaction, most participants combined all the tangible objects involved in a transaction (**Figure 7.2: D**): *“let say I want to send one Bitcoin; I have the public key and private key and I need [receiver’s] wallet address”* [P15]. The collection of these objects was temporarily placed in the small transparent cube representing the block (**Figure 7.2: E**), mirroring the Blockchain’s protocol: *“now the miner selects this transaction [holding a set of public and private key] to be put in the block”* [P2]. Such actions were performed by nine participants, seven of whom continued to move the whole block near the miners in order to reflect the stage of working to process the block: *“the miner needs to process the block by solving the complicated mathematical problem in the block”* [P15]. Subsequently, two of them took on the miners’ role by writing on the provided paper the binary code mimicking miners’ work to solve the block’s puzzle, confirmed by stamping the time (**Figure 7.2: G**). Another

interesting finding is the similar gesture performed by all participants to mark completion of a Bitcoin transaction, by taking out the Bitcoin as yellow clay coin from the block's small cube and slotting it into the receiver's wallet represented by a larger transparent box: “now the Bitcoins are saved in the receiver's wallet” [P1] (**Figure 7.2: H**).



**Figure 7.2: Experienced Users Interacting with BlocKit Objects**

As shown by the quotes above, another important finding is that through its ability to support a bird's eye view of the Blockchain, the kit allowed participants to spontaneously take on different roles, enacting, for example, the actions of the Blockchain and its protocols (**Figure 7.2: D,E,H**), the miners' proof-of-work (**Figure 7.2: F,G**), and users' interaction with their wallets (**Figure 7.2: A,B,C**). Such changes between roles were surprisingly swift, indicating a surprising value of the kit to facilitate them.

- **Kit's Challenges and Opportunities for Revising the Physical Kit**

While most objects were immediately recognised as representing Blockchain's entities, a few were less so. These are described below together with the attempt to unpack the reasons for participants' uncertainty. Such difficulties relate to objects themselves or relationship among them. The former includes inappropriate or incomplete representations, while the latter relates to the perceived distance among connected objects.

Almost all participants face difficulties identifying the consensus rule, mostly because the symbols chosen which were inspired from Google Images to communicate the rules, such as the symbol of Bitcoins with two arrows pointing out to resemble the double spending, was not easily recognised: "*I know this is the signature [sender's digital signature], but how about this symbol?*" [P11]. An interesting finding regards the representation of Blockchain ledger itself, arguably the most abstract entity of Blockchain infrastructure. Even though most participants successfully recognised this object based on its properties, some disagreed with this representation: "*I understand that you want to show that the Blockchain is transparent. But I don't think that it is appropriate to arrange it in this grid*" [P10]. The reason for choosing the grid was to metaphorically represent Blockchain's nodes at the intersection of two grid's lines and to allow the placement of the completed blocks on such nodes. However, some participants argued that a more adequate representation of the Blockchain is through links in a chain: "*it should not be this way, if you want to use the grid then you just put one row, Blockchain should be represented like a chain not grid*" [P3]. This view was shared by 7 participants and was particularly important, as it highlighted different image schematas. The initial image schemata for the

Blockchain were that of a container holding all metadata of the confirmed transactions that reflected the change Bitcoins' ownership. What the experienced users suggested was a different image schema, that of a Link which belongs to the family of Force schematas, i.e., the force that links two objects together. Such finding argues for a shift in the underlying metaphor of Blockchain infrastructure, not so much as a container but as a force creating links (Geiger, 1993).

Findings regarding incomplete representations concerned mostly the private key and were noted by almost half of the participants. Although they agreed with the metaphor of black envelope and post-it note, they also noted that these were not sufficient as an additional representation was needed to illustrate how the private key is used when the transaction is created: *"That's perfect but how about the permission to use the private key?"* [P9]. The hidden private key needs a representation for showing that the owner of the Bitcoins grants the transfer of the Bitcoins' ownership.

The second type of challenge relates to understanding relationships among objects. In this respect, findings indicate that an important challenge was the lack of cues for bringing and/or merging objects together, i.e., bringing together two distinct objects in order to create a new one. For example, seven participants failed to connect the black envelope of the private key with the set of numbers written on a sticky note representing the private key. In this respect, the study used two different objects; one capturing the key entity, while another one as an added-on sleeve to capture its privacy quality. Although the link between them was less obvious for 9 participants, once provided with a cue, the connection was easily made: *"how about this tiny black envelope [maybe] we need something to cover up the number"* [interviewer]. A similar challenge concerned the proof-of-

work, where more than half of participants failed to link the permanent pen for writing the proof of work with its allocated piece of paper. Once again, upon the provision of a clue, the connection was easily recognised. These findings suggest the importance of reducing the physical distance between objects which are logically connected, either by bundling them together, or by providing visual cues for their connection.

### 7.2.1.3 Revising the BlocKit's Design

In the light of these findings, the study identified several directions for revising the kit to better represent the experienced users' mental models of how Blockchain works. To more accurately represent the objects, one important suggestion was to avoid less common graphical symbols such as those used to represent the consensus rule. Six participants suggested a more direct approach of naming the rule as such: *"the best way is to label the drawer with rules"* [P2]. Such labels could be extended to other objects which would provide an advantage to novice users to better understand the Blockchain, as mentioned by three participants, *"as for people who want to learn Blockchain, I think it is better if all objects here are labelled properly"* [P13]. A related outcome is the suggestion for a kit's description, which was advanced by six participants: *"I think you would probably have to give a lot of context around what those things actually represent [...] you are not necessarily always there to explain where everything is. Say you send me all this stuff and I was going through a project meeting and have to use this to explain the Blockchain work, I may need an information sheet for this"* [P5].

Findings indicated that the Blockchain should be represented in a single chain and five participants suggested keyring as a representation for linking the blocks within the Blockchain: *“the ledger should be in a chain; like it is connected from one block to another. You can use something like a keyring to connect them”* [P6]. Such suggestion to represent the Blockchain as a single long chain can be materialised through a metal keyring. With respect to incomplete representations, findings indicate that the representation of private key should be extended to include Bitcoin’s owner permission to transfer the ownership of the Bitcoins, as mentioned by four participants: *“it is the user’s responsibility to protect the private key which is to keep in this black envelope; but when the owner wants to transfer their Bitcoins they need to give permission [to receiver] to use their private key, this can be represented through the sender’s signature [to show the agreement to transfer the ownership of the Bitcoins]”* [P8].

In terms of representing relationships, a few suggestions have been made concerning objects such as the private key and the proof-of-work which involved more than one object. Five participants suggested placing such objects closer in space: *“I think the [private key] envelope should not be separated from [post-it notes with private key’s] numbers”* [P14]. Participants made similar suggestions for the proof-of-work: *“it is better to put the pen and paper [for writing the proof] together”* [P5]. Grouping connected objects together is a valuable insight for improving the presentation of the kit, which is also supported by an important gestalt principle (Caillot & Nguyen-Xuan, 1995). The only concern is that once people interact with these objects they may not place them back in each other’s proximity. An alternative way to address this is by digitally embodying spatial awareness in such connected objects. For example, one approach to represent the

connection between related objects could be through small sensors embedded in these objects, i.e., when one is picked up, a small light on both objects switches on.

Apart from revising some of the kit's existing objects, two participants also provided suggestions for including a new object to represent the concept of a pool, i.e., transparent container box. Even though the memory pool holds a temporary unprocessed transaction, there is an argument that it is important to be included in the kit: *"I think you missed the object representing memory pool that holds the unconfirmed transactions before they are selected to be put in a block"* [P3]. The memory pool works as a waiting place for the newly created unconfirmed transactions to be chosen by the miners to include in a block. It should be transparent so that miners could select these transactions and put in a block: *"a transparent box should be fine to represent the memory pool as it works transparently for the miners to select the transactions for a new block"* [P6]. These quotes describe the properties of the memory pool as transparent and temporarily holding the unconfirmed transactions matching the container image schemata (Hampe & Grady, 2005; Johnson, 1987).

#### *7.2.1.4 The Kit's Impact on Experienced Users' Mental Models*

A significant finding is the value of the kit in supporting experienced users to materialise and reflect on their understanding of Blockchain infrastructure and its inner working. The study argues that through its materiality, the kit allows bringing the mental models into question, which in turn helps experienced users confirm their understandings, develop more nuanced understandings, or even revise some previously held, less accurate assumptions.

The latter is a particularly important finding, as challenging such assumptions is notoriously difficult. The kit's ability to not only support this but to also engage an enjoyable experience is a surprising and much valuable outcome. More specifically, with respect to revising assumptions, findings indicate two ideologies about the block's confirmation on the Blockchain. Six participants mentioned that such confirmation is made at the end of the mining process, just before the block is recorded on the Blockchain: *"let say, this miner is able to solve the block, then the miner will inform other miners and show his proof-of-work, and let's say that there are more than three miners confirming that the work is correct; only then the block can be recorded in the Blockchain"* [P2].

The other 3 participants described a more nuanced understanding of these processes, extending the above explanation beyond the three miners' confirmation of a block, to multiple blocks' confirmation: *"let's say this is the Blockchain (arranging a few blocks cubes in a single line), and this new block has just received the consensus from other miners to be recorded in the Blockchain. [...] In order to be fully secured and confirmed, the new block needs awaits the confirmation of six more blocks following it"* [P3]. These quotes are important as they illustrate the kit's ability to support experienced users to communicate and reflect on their mental models. Findings further reveal the importance of waiting for 6 confirmations and its link to transaction's security: *"if the user doesn't wait for 6 confirmations [...] then there is a possibility for somebody else to double spend it. Let's say this block has only 1 confirmation block ahead (arranges 2 cubes in a row). Then one mining entity with enough [computational] hash power (gathers 7 lights in one place) would be able to record another few blocks here (creates a new branch from the previous row by adding 3 additional cubes). So*

*what happened to this [initial] block? It will be removed from the Blockchain (took out the first cube)” [P3]. This quote alludes to a known security concern related to the Blockchain, namely the double spending attack (Eyal & Sirer, 2014) whose understanding, however, is not trivial.*

In order to further test this understanding, in subsequent interviews with 4 participants who shared the first model of block confirmation, the study enacted through the kit this alternative second model and elicited feedback. Surprisingly, all 4 participants have changed their understanding of the confirmation process: *“I thought that the confirmation processes were done at the miner’s part [...] But I agree with the double spending attack and I can clearly see the reasons why as you said the confirmation [ultimately] stands for the number of confirmed blocks ahead and not by the [three] miners [confirming it initially]” [P15]. This finding indicates that the physical kit is not only able to communicate about the complex system (Jansen et al., 2015) which is Blockchain infrastructure, but to support learning about it. At least what’s important is that the kit also supports reflection on and even changes in experienced users’ mental models.*

### 7.2.2 Findings 2: Designing for Trust with BlocKit

The anonymity principle is central to design for trust in the Blockchain protocol, which in turn raises significant trust challenges for both users and miners (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017). Hence, designing for trust on Blockchain is an important challenge to be explored with experienced users. In the second part of the workshop, we provided tokens to explore experienced users’ design solutions for materialising the flow of trust on Blockchain. Findings indicate three themes consisting of rewarding honest transaction partners with trust token,

penalising dishonest ones with distrust tokens, and accounting for the mining fee associated with the flow of trust. Participants iteratively identified six ways of materialising trust flow on Blockchain by (i) placing the token of trust within the Bitcoin transaction (P1, P3, P7), (ii) ensuring 2 way transparent transactions (P1, P2, P4, P5, P7), (iii) centralised mediator (P2, P4, P6, P8, P10, P15), (iv) 2-of-2 multisignature address (P3, P4, P5, P6, P8, P9, P11, P12, P13), (v) 2-of-3 multisignature address (P8, P9, P10, P11, P12, P13, P14, P15), and (vi) crowdsourced, decentralised mediator (P8, P9, P10, P11, P12, P13, P14, P15).

Each of the first five solutions was discarded as they challenged Blockchain's assumptions of decentralisation, unregulation, or anonymity. The first solution was enacted by placing the green clay trust token together with the other objects representing a transaction, i.e., Bitcoin clay, sticky notes with wallet address and signature, but failed to recognize that Bitcoin transactions are often accompanied by transactions of fiat currency or goods in the physical world, whose trust is problematic to capture on Blockchain (Sas & Khairuddin, 2017).

The second solution resembles the existing Omni layer approach (Omni Layer, 2017) allowing two or more parties to trade transparently over the Bitcoin Blockchain, but fails to acknowledge the asynchronous nature of 2 way transaction, and that in case of fraud, transparency is not sufficient to reverse a fraudulent transaction nor to sanction the fraudulent user.

The third solution suggests centralised mediator: *"both parties have to commit [...] and when both money and Bitcoins arrives in here, both will get it at the same time"* [P4], and participants represented it through the object of a transparent container holding all the objects involved in a transaction. This solution resembles the current escrow or exchange services, addressing the asynchronous problem of

two-way transaction, but failing to account for the decentralisation, unregulation, or anonymity principles of Blockchain. Indeed, escrows prevent fraud by requiring both parties to register their identity (Local Bitcoin, n.d.).

One way to address the risk of de-anonymisation is through 2-of-2 multisignature address which requires both parties to co-sign for a newly created third address to temporarily hold the Bitcoins before released to the destination wallet (Electrum, 2017; MultiChain, n.d.). This solution fails in case of dispute or fraud, and therefore 8 partisans suggested the 2-of-3 multisignature where a third party assists the dispute by signing the transaction (Lerner, 2015; WeiDex, n.d.). This solution was represented by placing 2 sticky notes with a different wallet address in the novel transparent container representing the third address: *“you can have it signed as two of two to receive the Bitcoins and trust token). [...] However, if you have a disagreement then it’s obviously stuck in here [and you need a 2-of-3 signature]”* [P12].

To address this limitation, more than half of participants proposed placing the transaction in a smart contract and the novel approach to use a crowd-sourced mediator or witness for the contract. To represent it, participants extended the previous transparent container with 2 sticky notes, by placing an additional sticky note on the transparent container: *“you can add another user that is randomly assigned in a contract to validate the transaction [...] and signed by 2-of 3 [...] At the end of a successful transaction, this trust token can be sent by the buyer and seller (mimic the movements of green clay from buyer to seller, vice versa) [...] and appreciation token to the other user who helps to witness the transaction”* [P9]. This is a novel design solution, extending smart contracts and multisignature accounts (Horda, 2018; Lerner, 2015; Matzutt et al., 2018) which have started to be

used on Ethereum Blockchain (Horda, 2018) for instance for decentralised exchange such as WeiDex (WeiDex, n.d.). However, the development for a fully decentralised exchange for Bitcoin Blockchain is limited (Cuen, 2018), as it also the idea of trust token and witness token. In the case of dishonest transaction partner, the witness *“needs to take charge to verify the transaction by requesting the agreed quality of the offline transaction’s proofs as stated in the contract from both seller and buyer. [...] the witness will decide whether to move the Bitcoins (from multisignature wallet) to the buyer’s or reverse it to the seller’s wallet [...]. It also reflects the increments of trust and distrust token for both wallets as specified in the contract”* [P10].

All participants agreed on the associated cost related to trust, suggesting that both parties should have an agreement regarding the fee, before enacting any transaction. In addition, 8 participants also suggested a small fee for incentivising the witness.

#### *7.2.2.1 Principles to Design for Trust of Blockchain*

This section discusses the suggested design principles for trust in peer-to-peer Bitcoin transactions. Findings identified four important suggestions such as a valid contract, transparent transactions, decentralised mediator, and reputation token which are further described.

- **Valid Contract**

Prior to enacting a peer-to-peer Bitcoin transaction, an agreement between the seller and buyer to decide on the details of the transaction is vital. Indeed, our previous findings reported fraud cases caused by one of the parties not fulfilling

their promise (Sas & Khairuddin, 2017), One way to overcome this risk, is by creating a valid agreement between seller and buyer before enacting the transaction: “*write a proper contract for the transaction [...] so you don’t have to trust them (buyer) and they (buyer) don’t need to trust you as the seller, it is because the contract says everything and it is valid*” [P13]. Hence, with a valid agreement, both buyer and seller are bonded with the contract. The suggestion to create a contract is an extension to the usual practice by making the negotiation and agreement. These include their details of bank account for fiat money and wallet address for receiving Bitcoins. But those are just word-of-mouth and there is no guarantee they will follow the agreements. By having an agreement in a contract, they are not able to escape as they have to agree to bear the penalties if they commit frauds. This mentioned by 6 participants: “*if let’s say any of them break the contract, the Bitcoin is sent to the honest party [...] or any other punishments they can write in the contract [...] and there is no way to run (from fulfilling the contract)*” [P13]. Although there is no central authority that governs the transaction, by having a valid contract will permit a trustless transaction between both parties. It is because the social trust among buyer and seller is no longer required as the transaction is protected with the rules in the contract that have been agreed by them. In the framework on the mechanic of trust that facilitates the trust between people with mediated technology, which can be classified as institutional trust (Riegelsberger et al., 2005).

- **Transparent Transactions**

In normal practice for peer-to-peer Bitcoin transactions, it will begin with one party (buyer) sending money followed by the seller enacting the Bitcoins

transaction (Sas & Khairuddin, 2017). Regarding this, more than half of the participants described the possibility of fraud facilitated by this common practice: *“(the) buyer can claim, he has sent the (fiat) money although he actually did not and (the) seller can also cheat by claiming that she did not receive the buyer’s (fiat) money even though she did”* [P8]. Fraud can also happen in the transactions between Bitcoins exchanged for goods: *“Let’s say you want to buy a product from a Bitcoin merchant. You are lucky to get the correct product [...] but how if they fool you? [...] and yet you have sent them your Bitcoins?”* [P1]. Such challenges contribute to distrust towards the anonymised peer-to-peer transactions among Bitcoin users.

In order to mitigate these issues, 6 of participants suggested to create the rules for fair and transparent transactions between the seller and buyer through a multisignature wallet: *“it begins with the seller sending the Bitcoins to a created multisignature wallet address. Then when the buyer sees the Bitcoin is available in that wallet address, he will send the money to the seller’s offline account and immediately sign on that multisignature wallet to request to release the Bitcoin. [...] Once the seller received the money in the bank, he or she will also sign on the wallet, and the Bitcoin will be released to the buyer’s wallet”* [P11]. This quote mirrors that Bitcoin’s transaction should begin by sending Bitcoin to a multisignature wallet address. Hence, this will create a fair and transparent transaction, as both parties have access to the Bitcoin multisignature wallet as well as the control over it. In other words, once the Bitcoin is sent to the multisignature wallet, it will not be able to move to another wallet address, unless it gets the approval or signature from both seller and buyer. This algorithm will facilitate the trust between the buyer and seller in the credibility of the systems

assisting peer-to-peer transaction in such decentralised, unregulated infrastructure, such as Blockchain (Corritore et al., 2003).

- **Decentralised Mediator**

Findings also indicate a challenge in facilitating the transaction between buyer and seller through multisignature wallet: *“However if you have a disagreement then it’s obviously stuck in here (multisignature wallet) [P12].* Such view is shared by 6 participants, and they suggested an interesting solution to mitigate this issue: *“Another wallet address (Bitcoin user) from the network can be randomly assigned to validate the transaction” [P14].* This reflects on *crowdsourced mediator functions* that help to validate the peer-to-peer transaction. This, in turn, made the multisignature wallet now consist of three parties: seller, buyer and the crowdsourced mediator or also known as a witness for the transaction.

This is a novel finding as unlike most of the Bitcoin exchanges’ wallet, they embedded escrow service<sup>5</sup> in their system. This service acts as the third party for buyer and seller’s transactions by temporarily holding their money and Bitcoin in the escrow’s account then disburse to the respective wallet and bank account for the transactions. The similarity of escrow service<sup>5</sup> and crowdsourced mediator is that both are the mediator for Bitcoin and offline counterpart transactions. But the difference consists of being centralised and decentralised for the latter mediator. This in turns shows that the use of mediator is essential to facilitate trust in a transaction. In the framework of trust, the role of decentralised mediator supports

---

<sup>5</sup> Escrow service – the third party that manage Bitcoin transactions for buyer and seller (Local Bitcoin, n.d.)

the social trust for the peer-to-peer Bitcoin transactions (Riegelsberger et al., 2005).

- **Reputation Token**

Blockchain is originally designed with the anonymity concept. However, due to the issue of trust, people tend to de-anonymise themselves for enacting peer-to-peer transactions (Sas & Khairuddin, 2017). In this study, findings suggest to build a wallet reputation system: *“although the wallet is anonymous, the number of ratings received for that particular wallet, can reflect the credibility of the user (owner)”* [P10]. Seven participants shared similar opinion. The rating scores of the wallet will indicate the credibility of the wallet’s owner which the identity of the owner is remain anonymised. However, there may be an issue of one person handling more than one wallet and keeping on sending the rating to each of their accounts, as concerned by most participants. In order to mitigate this issue, seven participants suggested the initial date of the wallet creation is visible: *“the reputation for the wallet can also be seen on the date of the wallet created. So people will know how long the wallet exists and (will be) able to compare with the number of transaction made and reputation level”* [P10]. This reflects that the length of the presence of the wallet and the rating scores could also contribute to the paradigm of trust.

The findings further highlight the importance to know the regularity of transactions in between the same wallets, as mentioned by 5 participants: *“there should not be a limitation of transactions in between two wallets, but create a mechanism to show the sender of each trust token received. So people can see the*

*frequency of transactions between two wallets” [P15]. This transparent reputation system is essential to monitor such transactions.*

Meanwhile, for the new user, there is also a possibility for them to build the trust associates from a wallet: *“Yes the problem will be for the new user. But I think they got to start with a small amount I suppose [...] which is similar to other reputation systems [...]. The idea is to have the reputation sign that you can link with your wallet id” [P12]. For a new user, if they perform an honest transaction, the trust token will be rewarded to her wallet. The tokens gained should also be accompanied in a form of ratio, as mentioned by more than 7 participants: “The new account will start from zero tokens. Let say for one trusted transaction, she will get 1 token, then maybe next transaction she gets another trust token. But for the third transaction, she gets distrust token. So it will calculate the average of trust token that she received in a form of percentage for instance” [P14]. A trust ratio associated in a wallet should reflect on total trust and distrust token gained by the user.*

Participants also suggested ways to incentivise the decentralised witness of a transaction: *“the buyer and seller can also send him (witness) a witness token as an appreciation for them. This token will be showed in his wallet and visible to others. This will give an added advantage to the witness to build his reputation” [P8]. Referring to the trust model, the element of reputation is one of the principles for the trust system that is supported under the social trust dimension (Riegelsberger et al., 2005).*

### 7.2.2.2 *The Requirements for the Principles to Design for Trust Bitcoin*

#### *Transaction*

In this section, the study will describe the capabilities of Blockchain to build the identified principles to design for trust transactions. The findings had identified four important characteristics of Blockchain which are storing information in Blockchain, smart contract, multisignature wallet and low-cost transaction that will be further described in this section.

- **Storing Information in Blockchain**

One of the unique characteristics of Blockchain is the ability to store valid information as well as to make it transparent for users (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017; Swan, 2015). Other than storing the Bitcoins transactions, Blockchain is also capable to store other types of information, as mentioned by seven participants: *“you can send Bitcoins and include some arbitrary information with the transaction [...] and it will be recorded in the Blockchain. [...] For instance this token (trust token) or whatever information can be recorded in the Blockchain”* [P3]. This quote reflects the ability of Blockchain to be the underlying technology for the decentralised reputation system for the Bitcoin transaction. Moreover the unique characteristics of Blockchain for being decentralised, irreversible and permanent transactions (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017; Swan, 2015) enable the development of reputation systems to be reputable compared to the ordinary reputation systems in most e-commerce website: *“trust could be seen as a form of value that can be exchanged and enhanced people’s trustworthiness. So, I think somehow being able to use the Blockchain to do that is interesting, because*

*again, you can't tamper with it like eBay that you can affect the rating" [P5]. By building a reputation system in the Blockchain, it will enable the process of sending and receiving the reputation tokens to be transparent for not only between the seller and buyer but the entire world. It is because, decentralisation and transparency are among the core principles of Blockchain (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017; Swan, 2015).*

- **Smart Contract**

The details of agreements between seller and buyer could be sealed in the form of a valid contract in the Blockchain. Four of the respondents suggested building the contract using the Ethereum smart contract: *"Ethereum Blockchain has this concept called smart contract, so a smart contract is essentially a self-executing piece of code which only executes when certain conditions are met. For example, after the transaction, you could ask each party for feedback on whether they thought that the transaction went smoothly or [...] something was wrong. So, if they both say yes, it went smoothly on the smart contract you could say well this wallet address and this wallet address gets token of trust" [P6].* This in turn allows the buyer and seller to write their agreements in the smart contract. In the contract, they should state all the related details of the transactions including the agreed selling price, method of offline payment, trust tokens and penalties for being dishonest, such as to receive the dishonest token. The smart contract will automatically set specific computational algorithms to run the contract as mentioned in the quote. Thus, if they both met the details in the contract, the smart contract will execute the contract by sending trust tokens for both and if not, the dishonest will bear the penalty by getting the dishonest token.

- **Multisignature wallet**

Findings also suggest to include the crowdsource validator or witness as a mediator for each transaction. This can be built by using the multisignature features mentioned by two of the respondents: *“Yes, of course, you can add the multisignature function in Blockchain. I know Bitcoin Blockchain has the multisignature and Ethereum also do”* [P9]. This shows that the design of the trust system in Blockchain can be supported with multisignature features that include 3 parties, buyer, seller and witness. The function of multisignature wallet can be found in several exchanges wallet such as Coinbase (Khatwani, 2018). There also some Bitcoin wallet includes administrative mediator, which is centralised in the multisignature wallet to manage disputes (BTC.com, 2017). However, to combine buyer, seller and the crowdsourced mediator for a transaction in the multisignature wallet is a novel design.

- **Low cost of transaction fee**

In order to record contract also trust and witness token in Blockchain, the seller and buyer need to commit a small mining fee, almost ten of the respondents shared this view: *“it costs the transaction, they (buyer and seller) spend a very small amount of money, but apart from that, they can include that kind of token information in that transaction and build their own credibility”* [P3]. The minimum fee for the contract would be worth for the seller and buyer to build their trust reputation for the future peer-to-peer transaction.

Sections 7.21 and 7.22 report on the findings from the workshop with the Bitcoin Blockchain's experienced users on BlocKit. The theoretical and design implications will be discussed in the following section.

### 7.2.3 Theoretical Implication

Now we report on the significance of the findings, and the main contributions while addressing the initial research questions. Findings indicate that BlocKit has leveraged participants' expertise and structural mental models (Doane, 1982; Greeno, 1983) of Blockchain's inner working by materialising its abstract and intangible key concepts (Fischer, 2008; Pierce & Paulos, 2012b, 2012a). The outcomes mark a shift towards understanding and communicating about mental models, as well as for technology design away from the traditional focus on artefact-based systems, towards infrastructure-centric technologies. In particular, study findings shed light into the affordances of physical design kits such as BlocKit for exploring and supporting these models.

The work also contributes to the emerging HCI interest in understanding sociotechnical infrastructures (Zhang, Sas, Lambert, & Ahmad, 2019) such as Blockchain (Jabbar & Bjørn, 2017; Jack et al., 2017; Zhang et al., 2019) with the aim to support deeper understanding of, and designing for them. This, in turn, has the potential to support the development of Blockchain-centric business models that have started to be explored in the corporate world (IEEE Innovation, 2019; Mettler, 2016).

In designing the BlocKit, the study integrated findings from two research areas which have been limitedly integrated such as material-centred design approaches (Wiberg, 2014) and TUIs and embodied cognition theories (Hampe & Grady, 2005;

Hurtienne, 2009; Johnson, 1987; Santibáñez, 2002). From here, the study proposed an innovative approach to understand and design for Blockchain infrastructure, leading to BlocKit's physical design. BlocKit also advances the state-of-the-art of HCI work on physical kits, away from existing artefact-centric approaches (Hardy & Alexander, 2012; Jack et al., 2017; Kuznetsov, Hudson, & Paulos, 2013; Kuznetsov et al., 2011; Sas & Neustaedter, 2017).

The study provides an initial vocabulary to talk about the designing of such kits including, for example, the image schemata of container, part-whole, and link, and entities' properties such as transparency, durability, verifiability, safety, and privacy. The study argues that this approach and its initial vocabulary could guide the design of other physical kits for materialising the understanding of other sociotechnical infrastructures, i.e., IoT, healthcare, governance.

Findings also indicate BlocKit's value for user engagement. The Bitcoin Blockchain experienced users confirmed BlocKit's ability to engender surprisingly high levels of engagement and delight, which in turn supported communicating, understanding, reflecting on basic assumptions of Blockchain infrastructure, as well as designing for it. This is an important finding suggesting that people's enjoyment of working with their hands in the making of artefacts from DIY research in HCI (Pierce & Paulos, 2012a, 2012b) extends to the interaction with such crafted objects provided by BlocKit. This is also a significant outcome given that the exploration of user mental models of technological artefacts is notoriously challenging.(Caillot & Nguyen-Xuan, 1995; Fischer, 2008; Sas & Neustaedter, 2017)

Besides communicating and learning (Borgman, 1999; Kieras & Bovair, 1964) about the complex system (Jansen et al., 2015) such as Blockchain infrastructure, BlocKit also supports reflection on, and even changes in experienced users' mental

models (Gibbs, 1998) which are a particularly important outcome. By interacting with the BlocKit's objects, participants explored a range of solutions for implementing trust in Bitcoin Blockchain, which they critically reflected on and revised. For example, they discarded the available escrow (Local Bitcoin, n.d.), and multisignature (BTC.com, 2017; Lerner, 2015; WeiDex, n.d.) solutions because of these challenge Blockchain's' assumptions of decentralisation, unregulation, or anonymity. An important outcome is the novel final solution consisting of crowdsourced, decentralised mediator or witness.

Findings indicate that in addition to materialising the understanding of Blockchain, BlocKit also supports designing for it. The study chooses to focus on trust since it has been identified as an important challenge of Bitcoin users and miners (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017). For this, the study applied the developed approach to design two additional objects such as the trust tokens, illustrating thus the generative power of BlocKit. Arguably, other aspects of the social infrastructure such as resilience, diversity, or value creation can be considered and represented in BlocKit through physical objects, to support design solutions on Blockchain.

Future work could explore the potential of BlocKit in specific domains such as health. For example, the challenges of manually filling medical records may be addressed on Blockchain (IEEE Innovation, 2019). In designing such solutions, designers may start by looking into the properties of the entities involved in the design. For instance, in order to create new medical records on Blockchain, one may start with the qualities that these records should have, some of whom are already reflected in the set of key properties, i.e., private, safe, durable, verifiable, acceptable.

### *7.2.3.1 Principles to Design for Trust in Peer-to-Peer Bitcoin Transactions*

The findings advance the theories of trust in HCI (Corritore et al., 2003; Riegelsberger et al., 2005; Sas & Khairuddin, 2015) as well as the trust challenges in Bitcoin transactions (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017) to frame the findings for the principles to design for trust for the peer-to-peer Bitcoin transactions.

In the light of the Bitcoin trust framework (Sas & Khairuddin, 2015) and the technological trust model (Corritore et al., 2003), the findings suggest the principle to design transparent transactions in multisignature wallet is able to leverage users' technological trust. This is important to avoid fraud in the offline transaction. Underlying the uniqueness of the transparent Blockchain characteristic (Swan, 2015) the integration of the design principles and multisignature wallet (Horda, 2018) enable the seller to make the first move by sending the Bitcoin to the multisignature wallet address securely. It is because the wallet is transparent to both parties in the transactions as well as protected by the signature of seller and buyer. Hence the Bitcoin will not be able to transfer to the counterpart's wallet until the offline transactions with fiat money or product are completed. This opposed the usual practice of Bitcoin peer-to-peer transactions that had caused multiple fraud cases (Sas & Khairuddin, 2017).

The principles to design the transparent transaction is supported with a contract between the seller and buyer in the Blockchain smart contract (Horda, 2018) that stand as the legal evidence for the transaction (Huillet, 2018). The evidence in the smart contract did not involve the governmental support but interestingly it can be applied as a valid legislative document. This finding extends dimensions of institutional trust in the Bitcoin trust framework (Sas & Khairuddin, 2015), as it

proofs that the user's trust in Bitcoin transaction is not only relying on the government to legalise the transaction but also may depend on the decentralised evidence such smart contract. The similar arguments are used to stand as novel findings for the framework of trust in between users mediating the technology (Riegelsberger et al., 2005).

Findings also indicate novel insights into the social dimension of trust. Instead of applying technology to strengthen the social trust, findings indicate that the decentralised witness could act as the mediator for the transaction between seller and buyer, which replaced the centralised escrow service (Local Bitcoin, n.d.). This has transformed from using technology to mediate trust to the human capabilities as a mediator for trust. Hence this study argues that the decentralised witness is an extension characteristic of social trust dimension in the framework of mechanic trust (Riegelsberger et al., 2005). In addition, the findings also suggest to include the reputation system as one of the principles of trust to support the social trust (Riegelsberger et al., 2005) in peer-to-peer Bitcoin transactions.

#### 7.2.4 Design Implication

The study now reflects on three design implications intended to inspire HCI researchers to engage in designing for infrastructures.

##### *7.2.4.1 Novel Approaches to Design Infrastructure-based Kits*

Findings suggest the value of the innovative approach to the design of BlocKit, which draws from both embodied cognition theories (Lakoff, 1987; Maurer et al., 2013) and material centred-design (Wiberg & Mikael, 2014). The three iterative design activities underpinning this approach consists of (i) identifying the key

concepts or entities of the sociotechnical infrastructure and their properties, (ii) identifying their image schemata through linguistic analysis (Hurtienne & Israel, 2007), and (iii) engaging in the material exploration for materialising these entities and relationships among them (Wiberg & Mikael, 2014). The study proves the combination of these three theories as BlocKit helps experienced users to facilitate their cognitive work in designing the protocol of trust in Blockchain.

#### *7.2.4.2 Novel Tools for Infrastructure Design*

BlocKit's holds value for designing for Blockchain infrastructure, a much-recognised need in the corporate sector. BlocKit is an illustration of novel design tools which could contribute to the call to move beyond the traditional artefact-centric design and towards infrastructure-centric design (Jansen et al., 2015; Jung & Stolterman, 2012). The study argues that such a shift of emphasis will be valuable in both developed and developing contexts, and that novel design approaches such as BlocKit will be much needed to support it. To better support the representation of logical, spatial and temporal relationships among the key entities, one may consider augmenting such kits with smart objects (Alexander, Lucero, & Subramanian, 2012). One way to represent the connection between related objects could be through small sensors embedded in these objects, i.e., when one is picked up, a small light on both objects switches on. A smart tangible object such as Sifteo cubes (Wikipedia, n.d.) which are small, *spatially-aware* tangible device which could be programmed to represent the connection between objects.

#### *7.2.4.3 Sensitizing Cards to Augment BlocKit*

Findings indicate the importance of consistently checking that the explored solutions align with the Blockchain's design principles such as decentralization, unregulation, or anonymity. The study revealed that these principles can be easily overlooked and that external prompts may be beneficial to interrogate and revise the proposed solutions. For this, the study can think of augmenting BlocKit with external aids such as flash cards containing sensitising questions regarding Blockchain's design principles. Similar to InspiredDesign cards (Remy, 2017), these cards can be used alongside BlocKit, to prompt its users to the importance of reflecting on the fit between their proposed design solutions and Blockchain's principles.

#### *7.2.4.4 Novel Approach to Design the Decentralised Bitcoin Transaction with Trust*

Findings highlighted four important principles for decentralised trusted Bitcoins transactions that consist of (i) transparent transactions (ii) a valid contract, (iii) decentralised mediator, and (iv) reputation system. Findings also indicate that these four elements can be applied to develop a decentralised Bitcoin trust application underlying the Blockchain technology such as Ethereum. It is argued that Ethereum Blockchain consists of a unique tool that is not supported in Bitcoin Blockchain, which is named as the smart contract (Horda, 2018; Vujicic et al., 2018). The smart contract could be integrated with the multisignature wallet as well as capable to be customised with an identified algorithm by the users including for releasing reputation tokens to users' wallet at the end of each successful transaction (Davenport, 2015; Horda, 2018). Other than that, Ethereum

Blockchain is able to store beyond the cryptocurrency transactions, such as storing the real estate documents (Karamitsos et al., 2018; Matzutt et al., 2018). Hence it is capable to store the contract as well as the reputation tokens. We argue that although the proposed design for trust is draw for Bitcoin cryptocurrency, it can also be built by advancing the Ethereum smart contract technology and utilise the bridge tool such as BTC Relay (BTC Relay, 2016) to link Bitcoin Blockchain and Ethereum smart contract.

### 7.2.5 Summary for Study 3

This study reports on the evaluation of the design of BlocKit, by 15 Bitcoin Blockchain experienced users. Findings indicate BlocKit's ability to engender surprisingly high levels of user engagement which in turn supporting communicating, understanding, reflecting on basic assumptions of Blockchain infrastructure, as well as designing for it. In addition, the experienced users also suggested a few revisions to improve the usability of BlocKit to support the use as a learning tool.

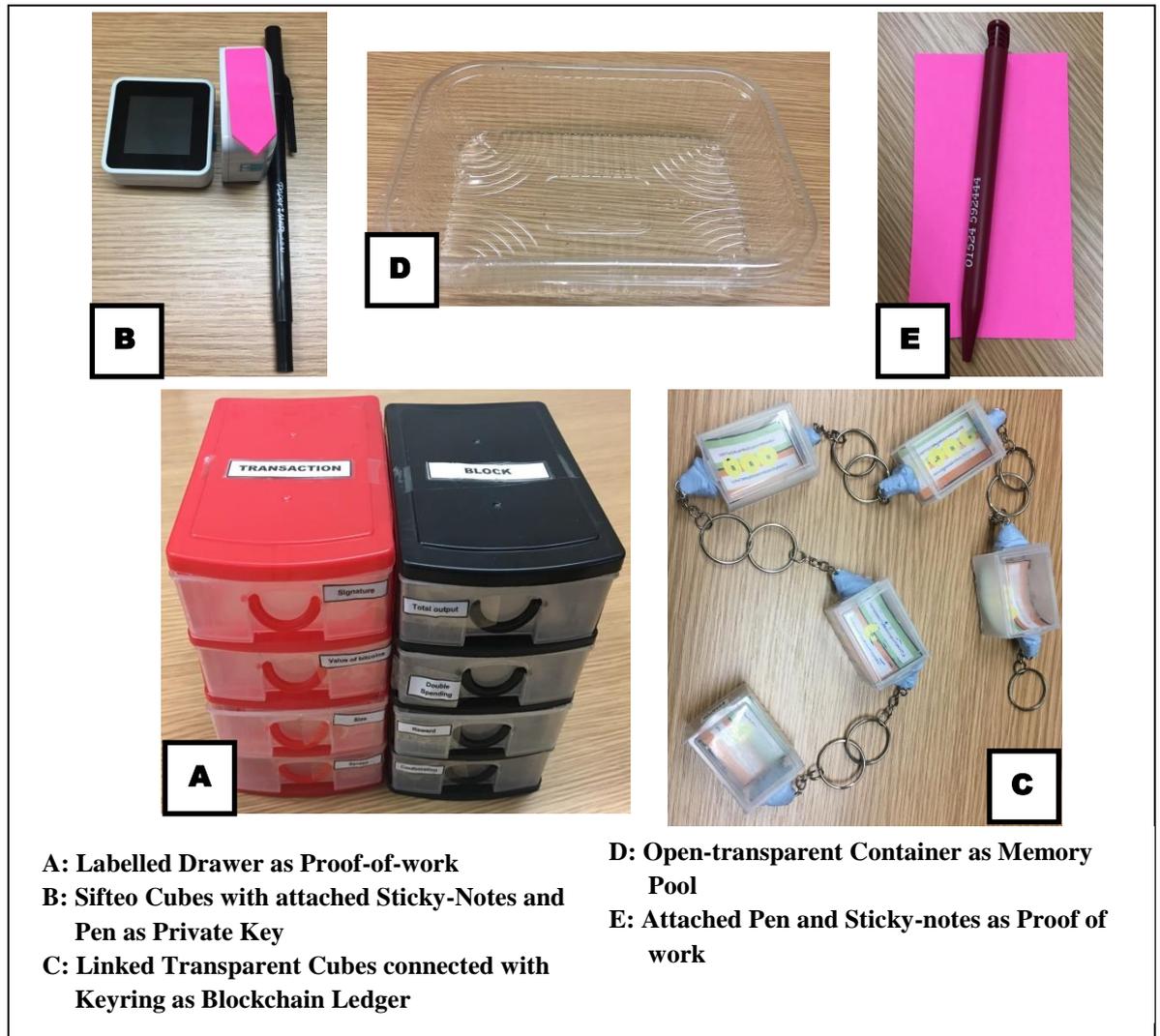
## 7.3 The Revision of BlocKit

Based on the experienced users' overview suggestions in Study 3 (7.2.1.3), there five physical representations of Blockchain entities have been revised and in addition, a new object has been constructed to represent newly identified important entity for Blockchain that will be discussed in this section.

### 7.3.1 Minor Revisions of the Objects

For f objects, most of the initial representations are to be kept unchanged. with only one object requiring minor revisions, namely the one representing the

consensus rule. As reported in the findings, the experienced users argued that , the icons pasted on the drawers to represent the rules could lead to confusion as the icons failed to help people recognise the rules. To address this concern, we followed the experienced users’ suggestions to replace the icons with labels mentioning the descriptions of the rules (**Figure 7.3 – A**).



**Figure 7.3: Revised BloKKit Objects**

### 7.3.2 Major Revisions of the Objects

Major revisions are much more complex as the object representation has been fully discarded by the experienced users. They argued that the presentation of the Blockchain ledger does not match its functions. They suggested that instead of using the concept of *container schemata*<sup>6</sup> (Hampe & Grady, 2005; Lakoff, 1987), the Blockchain should be designed based on the *link schemata*<sup>7</sup> (Hampe & Grady, 2005; Lakoff, 1987). Thus, each set of transaction block should be linked to the one before and the one after within the Blockchain ledger. Hence, the findings led to a major revision of the representation of Blockchain ledger from a translucent paper grid to the transparent cubes that are connected with keyrings. For each cube, 2 pieces of keyrings are stick at the front and back of the cube. The cubes are chained with one to another by using it's front and back of the keyrings (**Figure 7.3 – C**).

---

<sup>6</sup> Container schemata – The boundaries to prevent what is outside from affecting the entity or entities inside the container (Lakoff, 1987)

<sup>7</sup> Link schemata – It consists of two or more entities, connected physically or metaphorically, and the bond between them (Johnson, 1987)



**Figure 7.4: Organised Presentation of BlocKit's Objects**

### 7.3.3 Replacing the Static Objects with Smart Objects

The initial design of the object to represent a private key is sticky notes written with the alphanumeric and black envelope to hide the sticky notes. The problems with this representation are that the experienced users are not able to relate the envelope and sticky notes as those were not positioned together. Due to this, the experienced users faced some difficulties to articulate the relationship between the two objects. To address this issue, the researcher refined the object by replacing a smart object, named Sifteo to increase the visibility of objects connections (Wikipedia, n.d.). The Sifteo cubes were programmed by a programmer. The actual private key is displayed as 64 characters in the range 0-9 and A-F (Caetano, 2015)

and for the Sifteo cubes, each of the cubes' screen display 32 characters. This is to represent ways to protect the offline private key that commonly used for Bitcoin paper wallet. The paper wallet is not stored in any online devices. The owner of the wallet printed the private key on a piece of paper and stores it securely in a safe place. Then if they need to use the Bitcoin, they will activate the private key in the online device such as through a mobile wallet app.

Thus, for the new design of private key with Sifteo cubes, in order to use the private key, the users have to combine both cubes by arranging the cubes next to each other. Once they connect the two cubes, the alphanumeric on both screens is hidden. This is to represent the analogy for the private key as it is protected and cannot be revealed. In order to give a sign to users that both cubes are related, the cubes are programmed as if one of the cube is lifted up, then the other cube will lighten up. In addition, the representation of the private key has been extended by adding the sticky notes and pen to resemble the signature action by the owner of the private key (**Figure 7.3 – B**).

#### 7.3.4 Structuring the Arrangements of the Object

The arrangements for the presentation of all objects in BlocKit are also more organised and structured. All the related objects representing one entity such as the pen and paper to represent proof-of-work, are grouped into one place. Each group of objects are numbered from 1-12 to ensure that the participants will be able to see all the 12 objects of BlocKit (**Figure 7.4**).

#### 7.3.5 The New Object for the Newly Identified Blockchain's Main Entity

The experienced users also had identified memory pool as an important Blockchain entity that needs to be materialised in BlocKit. Memory pool

temporarily holds all the verified broadcasted Bitcoin transactions while waiting to be selected by the miners to group in a block for the confirmation works. Hence, this describes the memory pool as part-whole image schemata (Hurtienne, 2009; Hurtienne & Israel, 2007) as the miners can either select all of the transactions in the memory pool or just part of it. The properties of the memory pool are described as transparent, durable, portability, verifiable and safe. Thus, as suggested by the experienced users, a transparent and uncovered container is chosen as the new object of BlocKit to represent memory pool (**Figure 7.3 – C**).

#### 7.4 Chapter Summary

This chapter reports the findings on the evaluation of BlocKit. Study 3 reflects the capability of BlocKit to provide the vocabularies to communicate as well as giving the impact on conforming, strengthening, and challenging experienced users' mental models of Blockchain's infrastructure. They also use BlocKit as a design tool to explore the principles and the requirements to design for trust in peer-to-peer Bitcoin transactions Bitcoin. Other than that, the outcomes of the workshop also suggest the revisions on BlocKit objects to support a clear representation of Blockchain's entities. On the other hand, based on the experienced users' suggestions for the principles and requirements to design for trust in Bitcoin users, a set of algorithm was developed and validated, which will be discussed further in **Chapter 8**.

# Chapter 8

## Design and Validation on Algorithms for Trust in Peer-to-peer Bitcoin Transactions on Blockchain

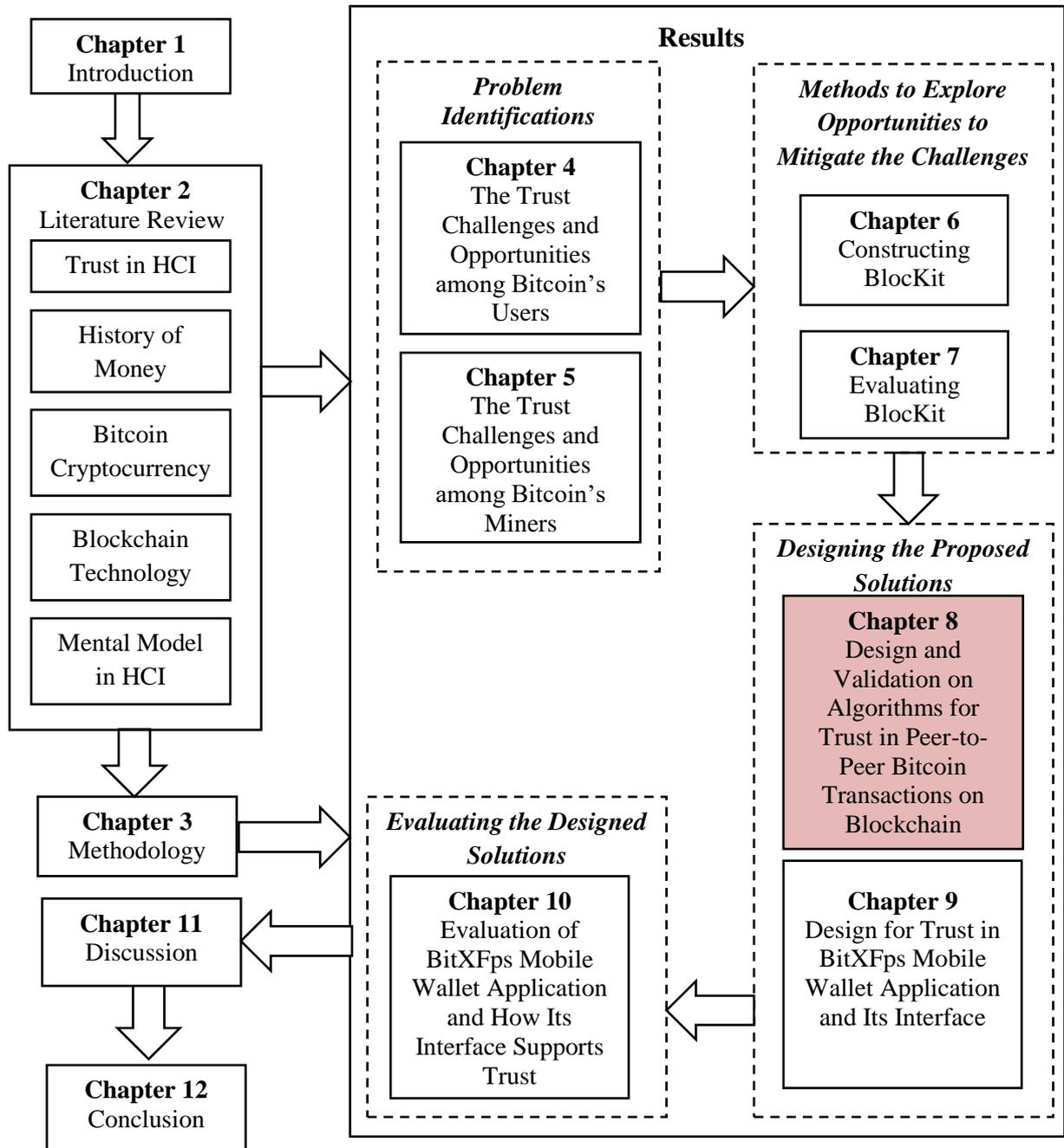


Figure 8.1: Chapter 8 of Thesis Structure

## 8.1 Introduction

By engaging with BloKit in Study 3 (**Chapter 7**), the Blockchain experienced users are able to suggest four principles to design for trust in Bitcoin peer-to-peer transactions in Blockchain. The principles are to create a valid contract between buyer and user, transparent transactions, decentralised mediator and reputation tokens. These design principles could be supported by using Ethereum smart contract to validate the agreement between seller and buyer, such as Bitcoin price, payment method and the reputation tokens. Based on the validated agreement, a customised protocol in Ethereum smart contract will be generated from self-execution code to release the reputation tokens of trust and witness. In addition, a smart contract (Hertig, 2018) could be connected with the multisignature wallet to manage the disbursement of Bitcoin in the wallet. The application of a multisignature wallet (Khatwani, 2018; Lerner, 2015) is to support the transparency and fairness of the transactions between buyer and seller also to allow a decentralised mediator to join the transactions as a witness. However, Bitcoin Blockchain and Ethereum Blockchain are two different decentralised public ledgers. Thus, in order to link Bitcoins transactions in the Ethereum smart contract, a bridge tool such as BTC Relay (BTC Relay, 2016) could be applied to facilitate the connections.

In this chapter, the design principles will be described precisely in the form of algorithms. There are five main steps in the algorithms: pre-transaction between seller and buyer, creating a smart contract, enacting online transaction with the witness, enacting offline transactions, and finally sending reputation tokens. All these steps of algorithms will be explained for two types of transactions: Bitcoin with fiat money and Bitcoin and product. Finally, the complete algorithms were presented to the Blockchain experienced users for validations.

## 8.2 The design of algorithms for trust in peer-to-peer Bitcoin transactions

Four principles for designing for trust in peer-to-peer Bitcoin transactions have been outlined by 15 experienced Bitcoin Blockchain users in Study 3: a valid contract, transparent transactions, decentralised mediator, and reputation token. Hence, based on those principles, the design of the algorithms in the Blockchain platform will be further discussed in this section.

### 8.2.1 The design of valid contract in Ethereum smart contract supported with BTC

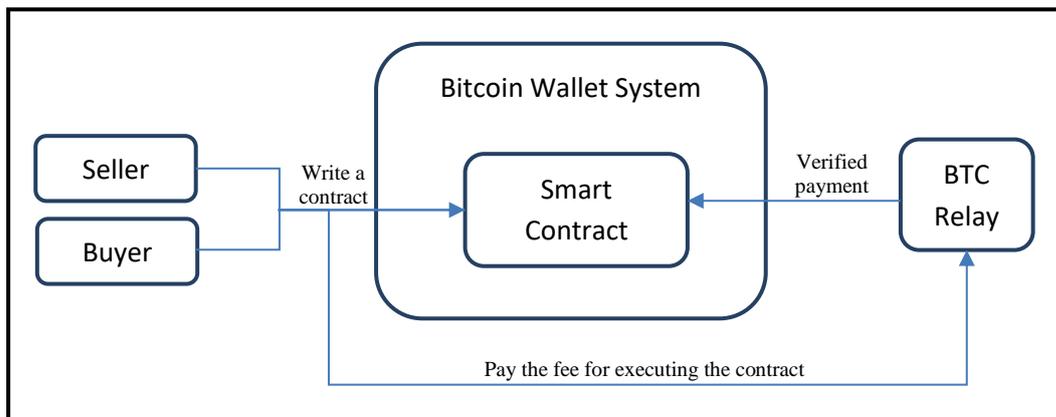
#### Relay tool

The Ethereum Blockchain offers a unique tool that allows users to write a set of contract that are automatically executed whenever the conditions in the contract are met (Horda, 2018). In order to execute the contract, users are required to pay a transaction fee in Ether for the miners. However, for Bitcoins transactions, the application of the BTC Relay allows Ethereum smart contracts to securely verify Bitcoins transactions including the contract execution fee that can be paid in Bitcoin instead of Ether (BTC Relay, 2016). The combinations of Ethereum smart contract and BTC Relay are novel design solutions for Bitcoin Blockchain. Meanwhile, as for Ethereum Blockchain, the smart contract has been widely applied in various apps such as CryptoKitties (CryptoKitties, n.d.).

Therefore, the design for trust in peer-to-peer Bitcoins transactions, the agreement between seller and buyer for the transactions of Bitcoins with fiat money or products could also be written in a smart contract. The details of the agreement, such as the selling price, method of payment for offline transactions, and timeframe for the transactions should be included in the contract. Both buyer and seller must also agree on the transaction fees for executing the contract. The smart contract is

connected to BTC Relay to verify the payment fees, made by users in Bitcoins.

Once the payment is verified, the contract will be executed (**Figure 8.2**).



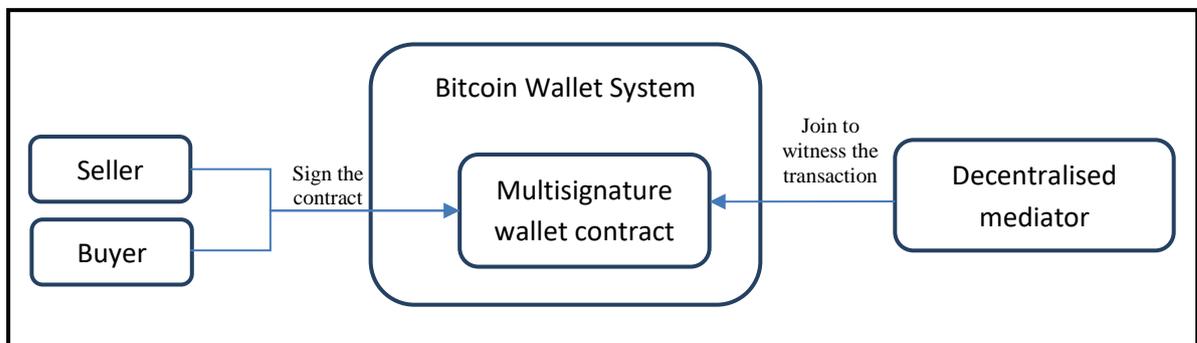
**Figure 8.2: Algorithm design to create a valid contract for Bitcoin peer-to-peer transaction**

### 8.2.2 The design of Bitcoin transparent transactions between buyer, seller and decentralised mediator with multisignature wallet contract

The multisignature wallet has been used in several Bitcoin wallets and exchanges, such as Coinbase and BTC.com wallet (BTC.com, 2017; Khatwani, 2018). The aim of using the multisignature wallet is to provide a transparent mechanism for all parties involved in the transaction. In addition, the Ethereum smart contract could also be linked with the multisignature wallet. Therefore, in order to write and execute a contract, all parties involved in a particular transaction would have the authority to sign the contract. These mechanisms have been applied in several types of system including the system for managing real estate documents (Karamitsos et al., 2018).

In addition, in Bitcoin peer-to-peer Bitcoins transactions, although the multisignature wallet enables transparent transactions between seller and buyer, who could also write the agreements for the transactions in the smart contract, there are still possibilities of conflicts among the buyer and seller which are beyond the

contract. Hence, as suggested by the experienced users in Study 3, together with the buyer and seller, we included the decentralised mediator in the smart contract embedded with the multisignature (multisignature wallet contract). The mediator is randomly appointed among the owners of Bitcoin wallets. Then the Bitcoin wallet owners that accept the offer to be the mediator will be responsible to witness that particular transaction between seller and buyer as well as to manage the dispute between them. In return, the decentralised mediator will be rewarded with a witness token and for any dispute managed by them, they will get some incentives. This is a novel design solution as currently there are plenty of Bitcoin wallets embedding the centralised administrators to monitor the dispute for each Bitcoin transaction (BTC.com, 2017) in their wallet system, however, there are limited findings for the type of Bitcoin wallet that embed a decentralised mediator in their system (**Figure 8.3**).



**Figure 8.3: Algorithm design to create a transparent peer-to-peer Bitcoin transaction with decentralised witness**

### 8.2.3 The design of reputation token in Blockchain ledger

The reputation system management model has been widely applied in various areas such as e-commerce, peer-to-peer system and social networks (Rahimi & Bakkali, 2014). The aim to apply reputation system is to provide the long term reputations records to inspire future interactions, and also to capture feedbacks on

present interactions and to allow other users to access the reputation ratings for trust decision (Janiszewski, 2017). The design of the reputation management system is commonly designed as centralised, which is managed by the website administrator (Resnick et al., 2006). Nevertheless, distributed reputation systems (Kinaterder & Rothermel, 2003) have also started to be applied in website design. For example, OpenBazaar an online platform for vendors to sell their products in Bitcoins allows their buyers to send reputation ratings to vendors and the ratings are transparently recorded in Blockchain (Open Bazaar, 2015).

The novel design of our reputation system is that the trust token is not only awarded to the seller and buyer, but also to the decentralised mediator who witnessed the enacted transaction. These reputation tokens are also recorded transparently in the Blockchain as an added advantage to the users to build their credibility.

### 8.3 The Main Stages of Algorithms for Trust in Bitcoin Transaction

The design of the algorithms consists of five main steps briefly described as follows:

**Step 1:** Pre Transaction between Buyer and Seller

The offline preliminary processes that connect the buyer and seller to communicate, negotiate and have a set of the agreement for the transaction. This includes the agreed Bitcoin price to sell, payment method, trust token fees and the expected completion time for the transactions.

**Step 2:** Creating a Smart Contract

This step describes the processes to transform the agreement from the previous step into the smart contract to make it valid in Blockchain. By having an agreement in

the form of a smart contract, it will support the first suggested design for trust principle, which is a **valid contract**. The contract is also linked with the multisignature that consists of the buyer and seller.

**Step 3:** Enacting the Online Transaction with Witness

Once the contract has been validated, a witness will be randomly invited to join the multisignature wallet as a **decentralised mediator**. Then, the seller will send the Bitcoin to the multisignature wallet. This will make the Bitcoin in the wallet is transparent to the buyer, seller and witness. To release the Bitcoin from the wallet requires at least two signatures. Thus, neither seller nor buyer could release the Bitcoin easily from the wallet without the approval from both of them. This contributes to fair and **transparent transactions**.

**Step 4:** Enacting the Offline Transaction

The offline processes involve the transaction of sending the fiat money to the bank account or product through a shipping company. The valid proof of the offline transaction is essential for the transaction's evidence.

**Step 5:** Sending the Reputation Tokens

Finally, once the offline transaction is accomplished, the buyer and seller may sign to release the Bitcoin from the multisignature wallet. Then the contract will automatically releases the trust tokens to the seller and buyer's wallet as well as witness token to the witness's wallet. These **trust and witness tokens** will be associated with their wallet addresses as well as visible on the Blockchain.

Please refer to Appendix D for the details of the algorithms for trust in peer-to-peer Bitcoins transactions.

#### 8.4 Validations for the Design of the Trust Algorithms for Bitcoin Transaction

The design of the algorithms for the trust on Bitcoin transactions is based on the principles that have been suggested by the Bitcoin Blockchain experienced users in Study 3. Hence, this section describes (Study 4) the feedbacks of Bitcoin Blockchain experienced users on the developed algorithms.

##### 8.4.1 Validation Method

In order to verify the algorithms, 10 Bitcoin Blockchain experienced users that were involved in the previous Study 3 (Chapter 7) participated in this validation study. They were presented with the complete diagrams of all five steps for both types of transactions (Bitcoin and fiat money, as well as Bitcoin and product) and provide with explanations on the processes. At the end of the presentation, they were asked to give their comments and suggestions for the algorithm design: “*What do you think about the algorithm?*” and “*Which part that needs to be improved and why?*” The entire validation study took about 30 - 40 minutes. Participants’ contributions were audio recorded and transcribed. The data analysis reports the algorithms’ improvement suggestions from the experienced users.

##### 8.4.2 Validation Findings

The algorithms received positive feedback from all participants. They were pleased that the algorithm design fulfilled their initial suggestions. Most of them were delighted with the crowdsourcing witness concept and the witness token, also

suggested a few minor changes on the algorithms to improve the design which will be further described in this section.

#### 8.4.2.1 *The Uniqueness of Crowdsourcing Witness with token incentives*

Findings indicate that all participants were satisfied with the appointment of an independent witness to manage the disputes on the transactions: *“I think the bold of the system is the function of the witness [...] they do not hold any of the money like those escrows [...] but they are more like a referee to ensure the transaction is done correctly”*[P4]. This quote reflects on the uniqueness of the decentralised mediator role, able to verify the transaction with human assistance, compared to most of the centralised Bitcoin exchanges that use the technology of escrow to validate the transactions (Local Bitcoin, n.d.). The incentives provided to the witness token will motivate users to participate as witnesses in the two-way transactions both online and offline: *“this token (witness token) is important to encourage people to be the witness”* [P9].

#### 8.4.2.2 *Recommendation for Revising the Design of the Algorithms*

Findings indicate that seven of the participants argued for the authenticity of the evidence provided for the money transaction: *“there is no problem with the tracking number (for the product) because is from the shipping company [...]. But the problem is for money transaction [...] what type of evidence they provide? [...] Everyone can make a fake bank slip and claim that they sent the money. This will also give a burden to the witness to verify the transaction”* [P8]. This is a similar finding in Study 1 (chapter 4), the printed bank slip is not strong evidence to verify the transaction. Alternatively, 5 participants suggested to use the intermediary company for bank transfer: *“if they send the money with PayPal*

*then it would be no issue as the receiver can make the money request straight away to the sender” [P5]. Although this is a trustless offline transaction method, the transaction fee may remain costly (PayPal, 2015).*

On the other hand, four participants suggested to provide real-time evidence: *“I suggest the money sender should make a video recording of the money transfer, starting from typing the bank URL, typing in the receiver’s bank account number till the money is sent, in a single loop without breaks but of course there are things that cannot be enclosed and need to be covered” [P2]. The real-time video proof of the offline transaction is a form of evidence accepted by legislation (Advocaten, 2017). Hence, it would be reliable to support offline transaction.*

Although the witnesses were given the witness tokens, the findings argue that the effort and time for the witness to manage the disputes are not reasonable. Six participants suggested to introduce a reward mechanism for the witness who manages disputes: *“This will consume a lot of time and effort for them to retrieve the proof and make a report for the dispute [...] other than the token, they should also be paid for the work they had done” [P5]. In the current design of the algorithms, although the witnesses had joined the contract, they are required to monitor the transaction until the end of the contract. If there is a dispute, then they will be invited to get in touch with the seller and buyer and make a report for the dispute. Hence, 4 participants suggested all parties involved in the transaction (buyer, seller and witness) to send a deposit to the multisignature wallet before enacting the transaction as a guarantee of honesty: “I suggest that the buyer, seller, and witness pay a small percentage of deposit based on the amount of transaction to the multi-signature wallet. This is to ensure that they are serious and responsible for the transaction. So at the end of a trusted transaction,*

*everyone will get the deposits back to their wallets. But, for the fraud case, the dishonest trader will not only lost their money and get the distrust token but also will lose the deposit. His deposit will be sent to the witness wallet as a reward for managing the disputes” [P4].* This is a striking finding for advising the issue of witness’ work incentives as well as to encourage them to perform honest transactions. Although it requires additional payment to enact the transaction, it is a good precaution to prevent fraud transaction also to ensure that the witnesses are more responsible.

#### 8.4.3 Revisions of the Design for Trust Algorithms for Bitcoin Transaction

Findings also suggest the importance of the type of proof for the offline transaction, in order to ensure that the transaction is protected from scams. Hence, for the algorithms revision, it is compulsory for the seller and buyer to include the type of evidence for the offline transaction with the bank or shipping company in the contract. These will allow the independent users, who will be offered to be the witness of the transaction, to view the details of the contract including the type of proof for the offline transaction as well as allow them to examine the format of the proof. If they are not familiar with the format of proof, they may decline the invitation for the witnessing.

The findings also suggest including a new mechanism as a guarantee of honesty in the algorithms that requires the buyer, seller, and witness to pay a deposit for the transaction. This would encourage them to be responsible, but also to be a reward for the witness who is in charge to manage the dispute.

## 8.5 Chapter Summary

This chapter describes the algorithms for trust in peer-to-peer Bitcoin transactions with fiat money and product exchanged in the real world. Those algorithms have been validated by Bitcoin Blockchain experienced users that initially suggested the principles to design for trust in Bitcoin peer-to-peer transactions. Thus, these validated algorithms will be used as the reference to design the user interface of a mobile Bitcoin wallet as discussed in **Chapter 9**.

# Chapter 9

## Design for Trust in BitXFps Mobile Wallet Application and Its Interface

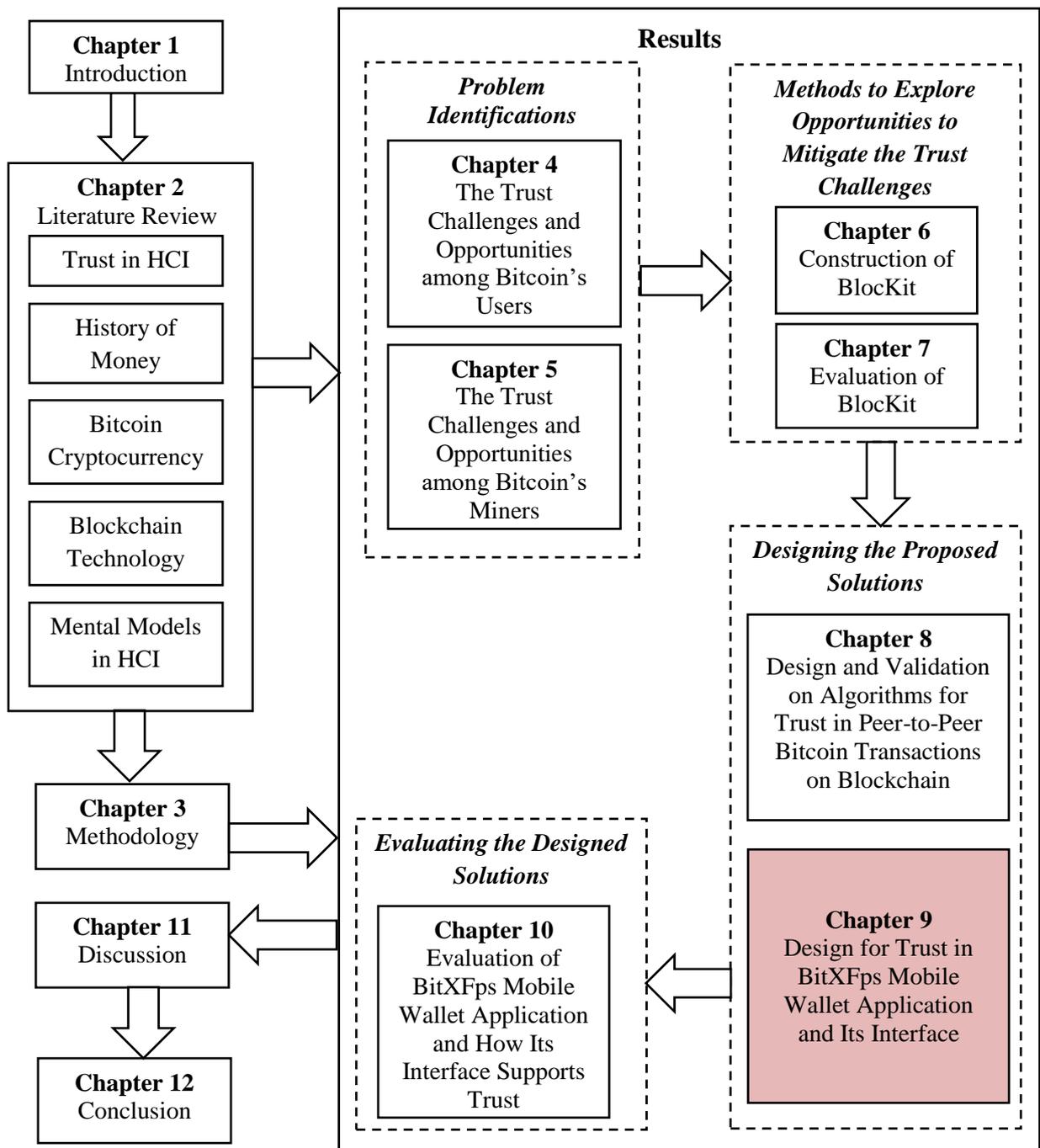


Figure 9.1: Chapter 9 of Thesis Structure

## 9.1 Introduction

The algorithms to develop trust in terms of peer-to-peer Bitcoin transactions have been described in **Chapter 8**. The algorithms were validated by the Bitcoin Blockchain experienced users who initially suggested the principles to develop trust in Study 3 (**Chapter 7**). This chapter aims to design the user interface for the prototype of a mobile Bitcoin wallet application, named BitXFps by adopting the validated algorithms. Prior to the design of this app, a set of guidelines to design for trust was identified. The guidelines were adopted from the existing frameworks (Seckler et al., 2015; Wang & Emurian, 2005) to evaluate trust in designing interfaces for websites and mobile apps (Hasslacher, 2014), which consist of five characteristics, namely graphic design, structure design, content design, social cue design and personal social proof. Based on the suggested design from trust principles in Study 3 (**Chapter 7**), another characteristic known as peer-to-peer transaction cue is also added to the guidelines. Thus, the guideline is used as the reference to design the BitXFps Bitcoin wallet app user interface. This chapter begins with the descriptions of the guidelines to gain trust in designing Bitcoin mobile wallet apps.

## 9.2 Proposed Trust-Inducing Features for the Bitcoin Application Design Interface

Wang and Eumarian (Wang & Emurian, 2005) designed the framework of trust-inducing features for websites consisting of four characteristics, namely structure design, graphic design, content design and social cue design. Graphic design refers to the design factors on the website that influence the first impression among consumers, which include the use of colour, layout design and photo quality in the website (Karvonen & Parkkinen, 2001; Kim & Moon, 1998; Seckler et al., 2015; Wang & Emurian, 2005). Next, the structure design relates to website organisation which depicts the overall look

of a website and the information accessibility. This includes the website usability in terms of the design effectiveness, ease of website navigation and lack of pop-up advertisements in the design. Also, the structure design is related to the website requests in persuading users to share their URL with others, to register an account or download a software via the website (Eremeev, 1999; Karvonen & Parkkinen, 2001; Nielsen, 1998; Ping et al., 1999.; Seckler et al., 2015). Content design refers to the format of information provided by the website providers, either graphical or textual, which includes security signs, website branding, expertise, privacy policy related to personal data collection and the secondary use of data, web address, implausible promise and website policy (Belanger, Hiller, & Smith, 2002; Egger, 2001; Eremeev, 1999; Hu, Hu, Lin, & Zhang, 2001; J Nielsen, 2000; Seckler et al., 2015; Shneiderman & Ben, 2000; Wang & Emurian, 2005). Another one is the social cue design, which relates to social signs that reduce the gap of social distance and increase intimacy. The integration of social media with the website is common to connect the users with web providers and enhance the communication between users (Basso, Goldberg, Greenspan, & Weimer, 2001; Riegelsberger et al., 2005; Seckler et al., 2015; Steinbrück, Schaumburg, Duda, & Krüger, 2002; Wang & Emurian, 2005).

Secklar et al. (Seckler et al., 2015) extended the framework after looking at many e-commerce and finance websites. Thus, the initial framework was modified with new characteristics, in terms of personal and social cue aspects. The new characteristics are related to the social proof among friends, which is identified through the connection between the website and social media channels, that enables users to view their mutual friends who are engaged with the website and share experience with other users (Seckler et al., 2015).

However, there is a limited exploration of the framework to explore trust in the Bitcoin or other cryptocurrencies' mobile app interface. Hence, the extended framework of trust-inducing features by Secklar et al. (Seckler et al., 2015) was Bitcoin adopted to design BitXFps.

In addition, from the outcomes of Study 3 (Chapter 7), the four principles to gain trust in peer-to-peer Bitcoin transactions were identified, they are transaction transparency, contract validity, decentralised mediator, and user reputation. Transaction transparency is defined as the app design that guarantees the visibility of two-way transaction for both seller and buyer. Contract validity is defined as the signs in the design that ensure the agreement between the two parties is valid in Blockchain's public ledger through smart contracts. Next, the decentralised mediator is defined as the third party involved in a transaction, who manages the two-way transaction to prevent failure or dispute in the case of claimed unfairness. Another one is user reputation that can be captured through trust tokens, to indicate users' honesty in the previous transactions. These four elements are also applied to evaluate the existing Bitcoin mobile applications. Hence, the trust-inducing features (Seckler et al., 2015), along with the principles for trust in peer-to-peer Bitcoin transactions, were adopted as a new proposed design guideline to design and evaluate BitXFps as in **Table 9.1**.

<b>Graphic Design</b>	
<i>Uses of Colours</i>	
1.	Suitable colours for Bitcoin Application
<i>Appropriate site layout</i>	
1	Easily accessible of the functions within the app
<i>Moderate layout complexity</i>	
1.	Moderate arrangements of contents for all pages
<i>Uses of photographs</i>	
1.	Appropriate quality of photos used in the app
<b>Structure Design</b>	
<i>Usability</i>	
1.	Effectiveness and efficacy with the task flow
2.	Easy navigation
<i>Broken Links</i>	
1.	No broken links throughout the app
<i>Demand</i>	
1.	Provide links to share the wallet app with friends and family
2.	Did not require an additional application to support the function of the app.
3.	Require users to create a wallet account
<b>Content Design</b>	
<i>Security signs</i>	
1.	The signs that the wallet account is protected
<i>Image/brand</i>	
1.	The features in the design that reflects the image of the wallet app
<i>Expertise</i>	
1.	Page that provide a comprehensive user guide for the users to use the app
<i>Privacy: Data Collection</i>	
1.	Page that stated the details of privacy policy related to users' data collection and storage
<i>Privacy: Secondary use</i>	
1.	Page that stated the details of privacy policy related to the uses of the collected users' data

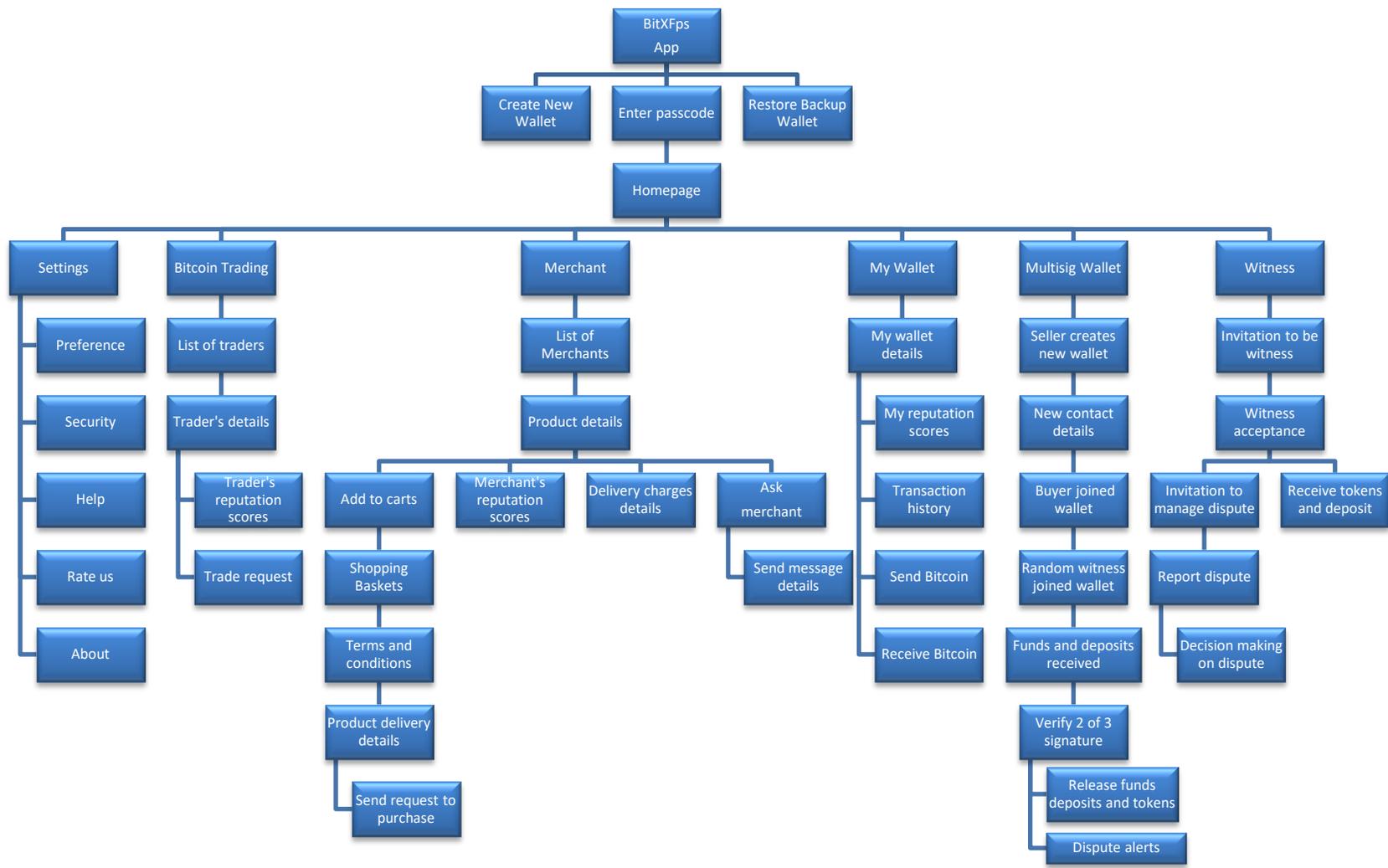
<i>Credibility of Content</i>	
1.	Updated contents for the app
<i>Implausible Promises</i>	
1.	There is no information that is not making sense
<i>Policy</i>	
1.	Page of details of terms and conditions of using the app
<b>Social Cue Design</b>	
<i>Customer Service</i>	
1.	Page for user's support service for the app
<i>Real-World Link</i>	
1.	Supporting links that is related to the development of the app
<b>Personal and Social Proof</b>	
<i>User's Social Proof</i>	
1.	Link or page for users to leave feedback and review
<i>Friend's Social Proof</i>	
1.	Users can connect with their friends and family that used the same app
<i>Shared User's Prior Experience</i>	
1.	Users can share their experiences with other users.
<b>Peer-to-peer Transaction Design Cues</b>	
<i>Unbiased Transaction</i>	
1.	The steps to create the transaction is fair for both side of users (seller and buyer)
<i>A Contract validity</i>	
1.	A page to show that the mutual agreement is stored in the smart contract
<i>Verifiable Transaction</i>	
1.	There is a mediator that verify the transaction between both parties
<i>User's Reputation</i>	
1.	Show the rating scores of the users

**Table 9.1: The Proposed Checklist in Designing and Evaluating the Trust in the Bitcoin Mobile Application Interface**

### 9.3 Navigation overview of the BitXFps

The app navigation diagram can be viewed in two layers of interface, which are the pre-access to the app and homepage. The pre-access is divided into three parts; create a new wallet, create a passcode, and backup wallet. For the users to access the homepage, they are required to create the wallet and passcode. The homepage consists of six parts; settings, Bitcoin trading, merchant, my wallet, multisignature wallet and witness. All these are accessible from the homepage and each of the main will be further explained in the following sections. (**Figure 9.2**).

While navigating between pages on the app, users can see a menu bar at the bottom of the page which links to other functions (**Figure 9.12: B**). The menu bar consists of icons similar to the homepage. When users enter a page, they can see an idle icon on the menu bar, which shows the current page. There is also a back button on each page to facilitate user navigation.



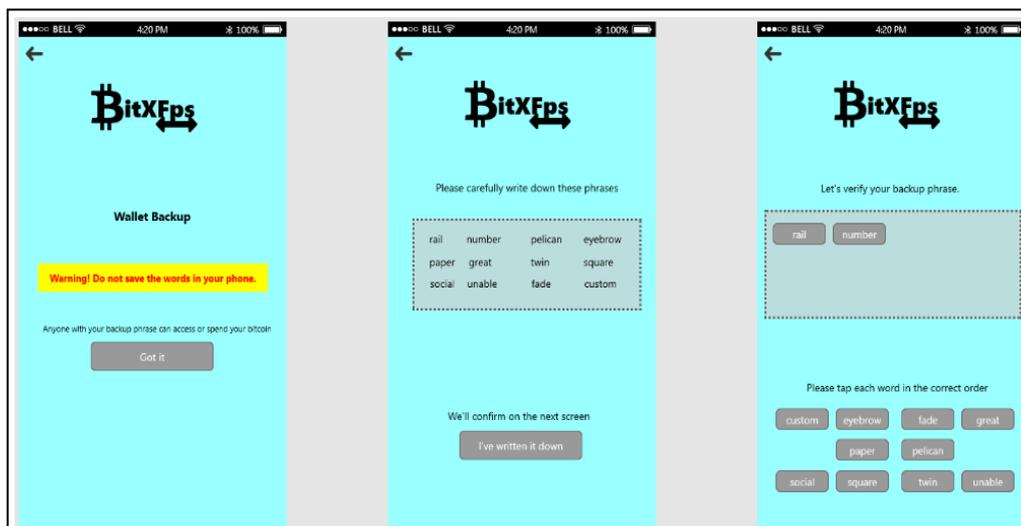
**Figure 9.2: A navigation diagram of the BitXFps mobile app prototype and its functionalities.**

### 9.3.1 Design Overview of BitXFps

Now, the design of the BitXFps prototype user interface will be described according to the algorithms identified in **Chapter 8** (Appendix D).

#### 9.3.1.1 Creating a new wallet

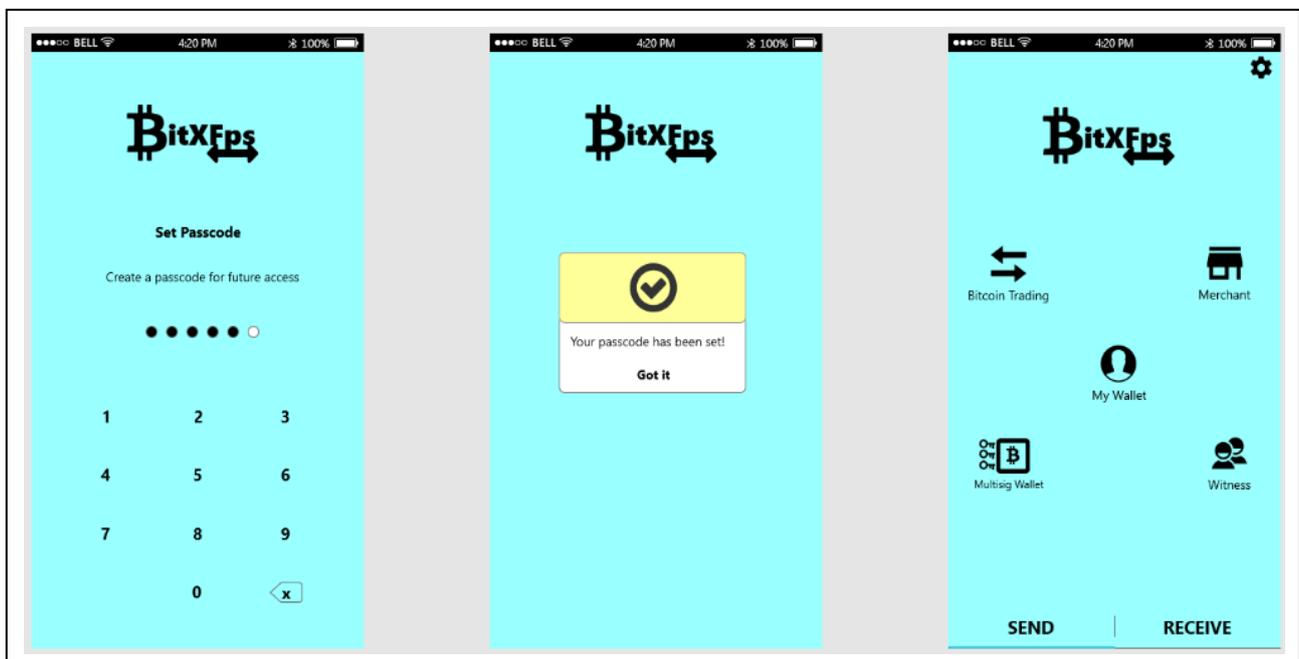
To get access to the wallet, users are required to have a valid BitXFps Bitcoin wallet. For new users, they can register by verifying the 12 random word phrases. The words are important for wallet backup. This means in the future, if users lose their mobile device, they can still recover the wallet by using the 12-word phrases, which resemble their private key. In the meantime, if someone is able to retrieve those words, he or she can log in to the wallet. Hence, it is vital for the users to keep those words a secret. This is one of the design security measures, as the mobile app does not manage or store their owner details (**Figure 9.3**). This is in contrast with most of Bitcoin exchange apps, which require the owner to provide personal details such as proof of ID and address to create the wallet (Coinbase, n.d.).



**Figure 9.3: Wallet Backup Phrase**

### 9.3.1.2 Set Wallet Passcode

Once the wallet is successfully created, users are required to set a passcode as another security measure. The passcode will be queried when the users try to gain access to the wallet, conduct a transaction, sign an agreement, or accept an invitation to join a multisignature wallet. Once the passcode has been set and verified, the user is allowed to access the wallet home screen (**Figure 9.4**).



**Figure 9.4: Setting the Wallet Passcode**

### 9.3.1.3 BitXFps Home Screen

Once the users have verified their wallet, they can view the BitXFps homepage. The logo and the main functions are available on the homepage via icons and labels. The icons are labelled so that users can get familiar with the terms in Bitcoin transactions. The wallet background colour is similar to the

previous page. Blue is chosen because this colour is suggested in the checklist besides being deemed to initiate trust (Alberts, Van Der Geest, & Thea M., 2011; Labrecque & Milne, 2012). For any Bitcoin wallets, the most important function is to send and receive Bitcoins. In addition, the setting function is essential to enable users to customise their preference in using the app. Hence for the BitXFps design, these three functions are placed on the homepage. Moreover, five wallet functions such as Bitcoin trading (trading between Bitcoin and fiat money), merchant (trading between Bitcoin and goods), my wallet, multisignature wallet, and witnesses are placed on the main screen to be explored by the users (Figure 9.5).



**Figure 9.5: The BitXFps Main Screen**

#### *9.3.1.4 Send and Receive Bitcoin*

The “SEND” and “RECEIVE” labels on the main screen allow users to send and receive Bitcoin instantly. These functions are available in most Bitcoin wallet apps, as users are required to key in the amount of Bitcoin to be transferred and the receiver’s wallet address. The latter can be keyed in, pasted or scanned from the QR code. Users can also set the transaction fee at low cost with lower priority, or choose faster transaction with a higher fee. There are two ways for users to receive Bitcoins. First, they can just share the copy of their wallet address or QR code to other users, and second, they can set the Bitcoin amount needed. The QR code is customised for each transaction accordingly. On the screen header, there is the app’s logo, title and down arrow to allow users return to the main screen. These help users for easy navigation.

### 9.3.1.5 Settings

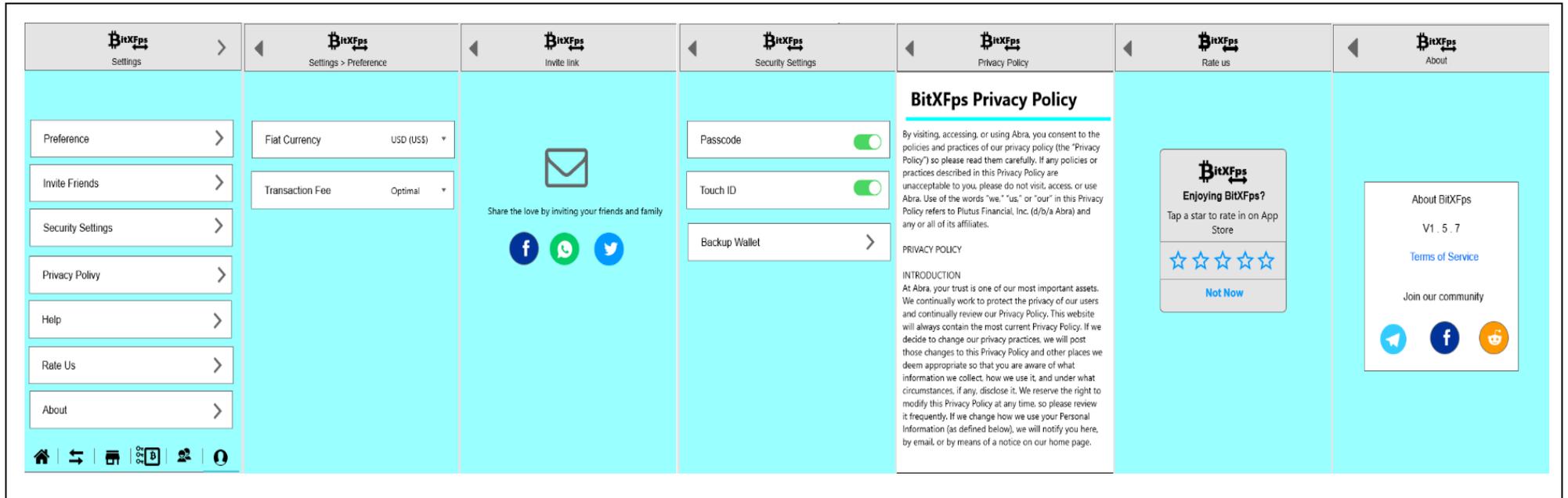


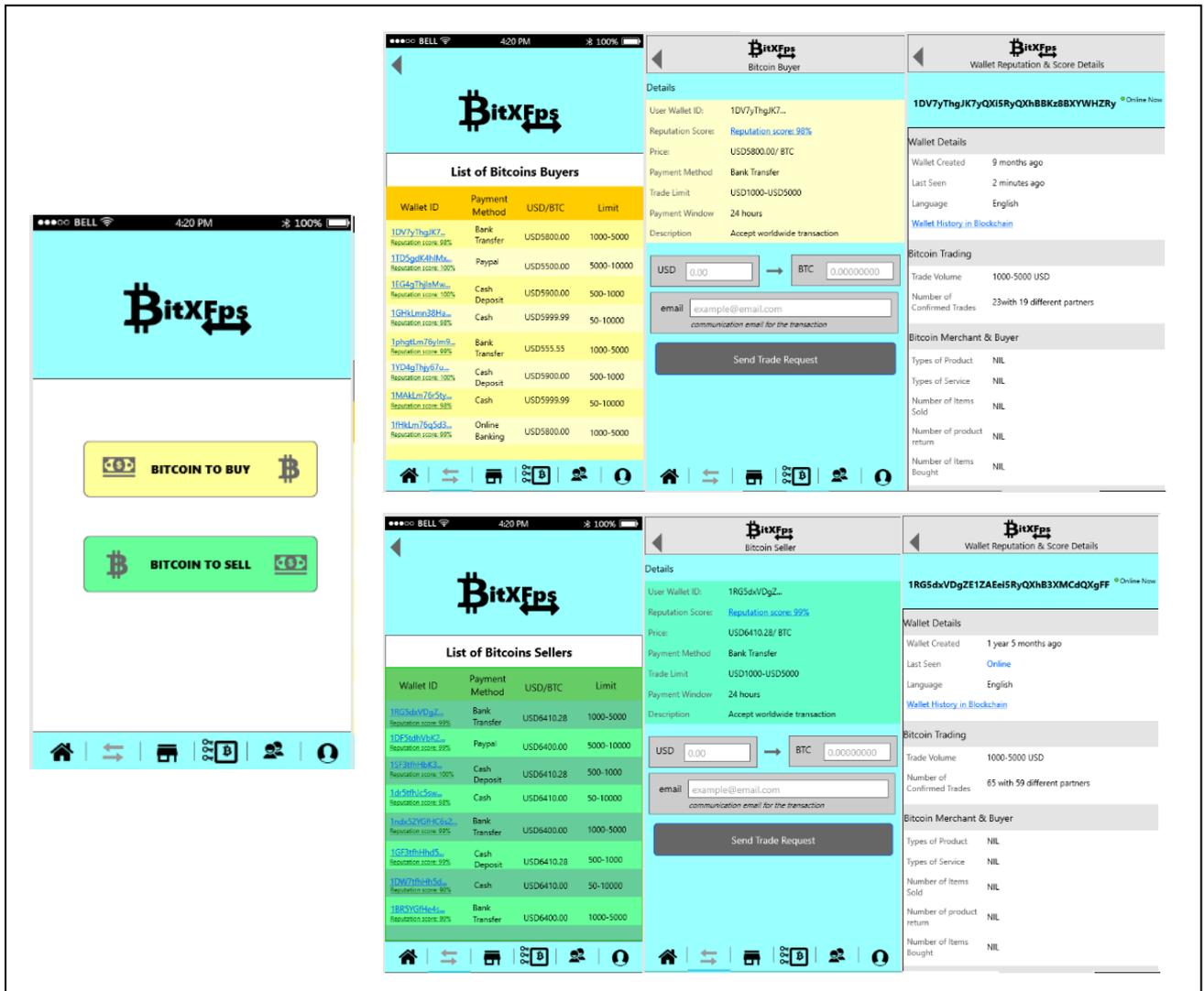
Figure 9.6: Setting Options for BitXFps mobile app

Besides sending and receiving Bitcoins, BitXFps main screen also features setting icons for users to customise the app based on their preference. Under the Settings menu, there are 6 submenus, which are “Preference”, “Invite Friends”, “Security Settings”, “Privacy Policy”, “Rate Us”, and “About”. At the bottom of the main setting page, there is a menu bar that consists of all the icons similar to the main screen. This allows users to navigate between pages or return to the home page. Each submenu will be further described.

The first submenu under the Settings menu is “Preference”, which allows users to choose the preferred fiat currency to be displayed on the app and set the transaction fee either high or low. The second submenu is “Invite Friends”, where users can share the link to the app with their friends and family, for them to use the same app to send and receive Bitcoins. This helps to increase the level of trust in transactions among the new users. The link can be shared with Facebook friends, Twitter followers, or via instant message applications. The third submenu is “Security Settings”, where users can change their passcode to enable touch ID function. So instead of keying in the passcode, they can use their fingerprint for quicker access. Besides, the users can retrieve the 12-word phrases to back up their wallet.

The fourth submenu under Settings is “Privacy Policy”. It consists of the app’s privacy policy in detail, while the next submenu allows users to leave feedback and rate the app. As the app is designed for iPhone, the rating page is then linked to the Apple Store. Another submenu is about the terms and conditions, and for users to connect with the social media community channels such as Twitter, Facebook and Reddit (**Figure 9.6**).

### 9.3.1.6 Bitcoin Trading



**Figure 9.7: Bitcoin Trading Pages**

On the Bitcoin trading page, buyers and sellers can advertise, sell and buy Bitcoins between each other. The list of buyers and sellers are listed with different colours in a table to enable users to distinguish them. The details such the Bitcoin’s price, reputation score, payment method or payment window of the sellers or buyers can be browsed from the list. To proceed with transactions, users have to key in the Bitcoin amount and send the trade request. The application

sends the request to the seller's email. Then, the seller and buyer may further negotiate the transaction via email before enacting the transaction.

### 9.3.1.7 Merchants

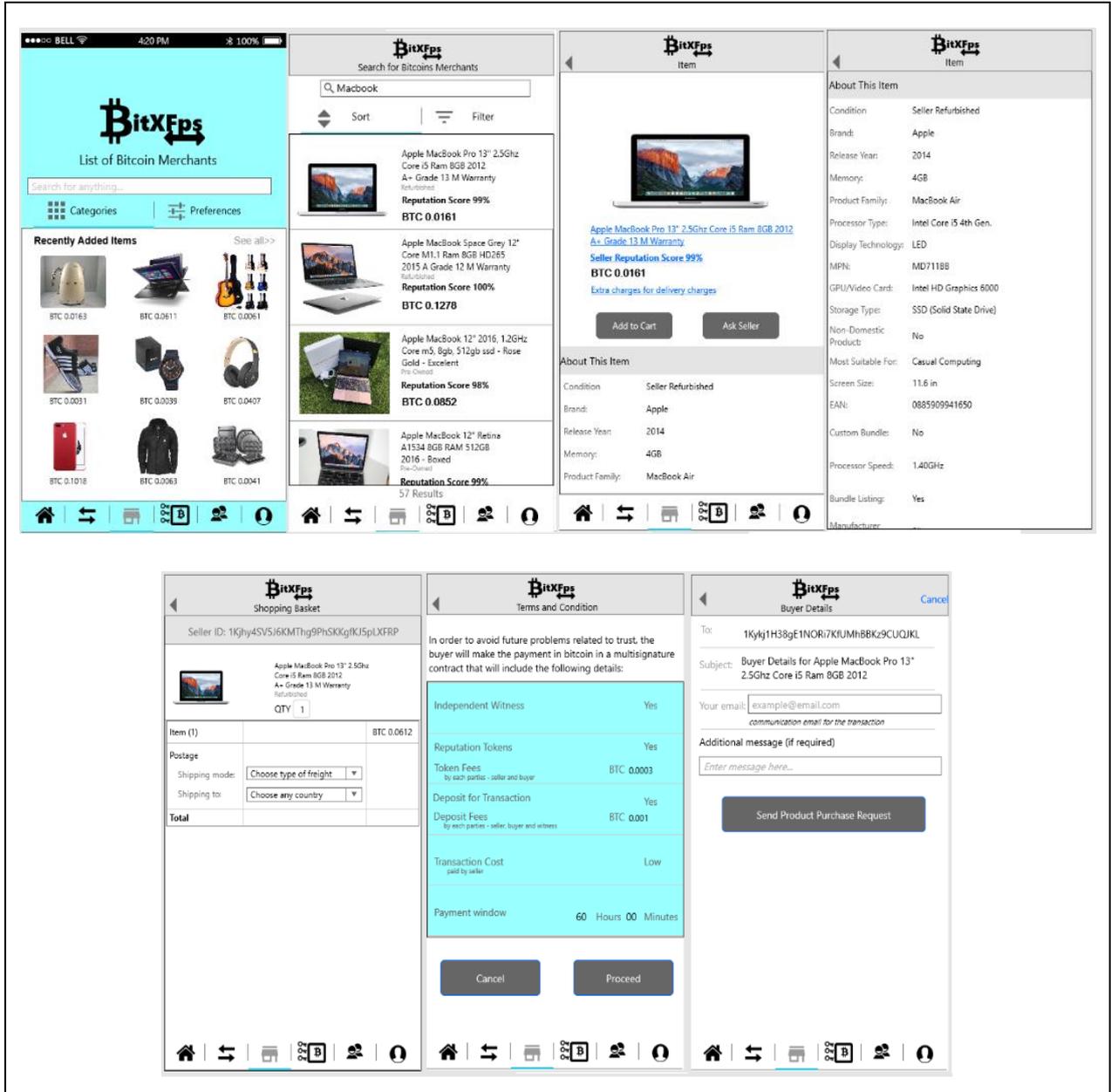
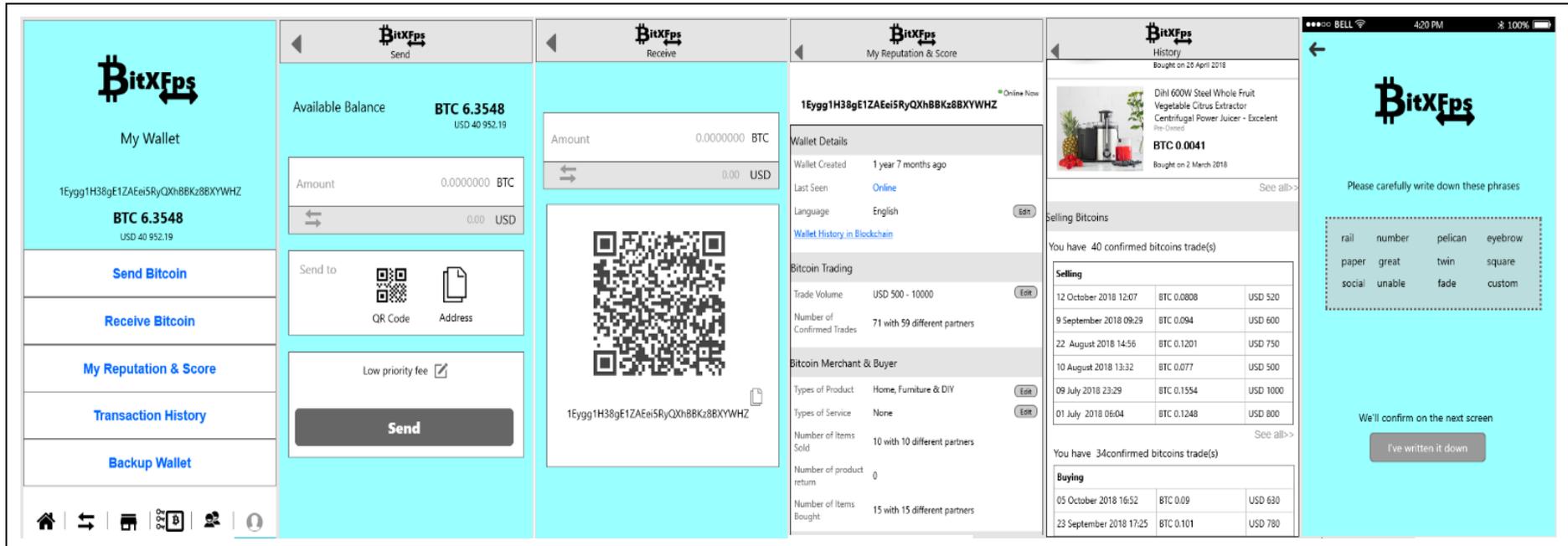


Figure 9.8: Merchant Pages

BitXFps app also supports users who want to be the product merchants and trade using Bitcoin. The merchant page is accessible from the merchant's icon on the main screen, the icon is also located at the bottom of most of all pages. Users can browse the products either by category or preferences such as price, colour and brand. There is also a search bar, where users can key the item name that they wish to search. The searched items are listed with details such as the item name, price, and merchant's reputation score. To view additional details, users can click on the item and the screen will show the page for the item. This includes the product images, specifications and delivery details. Users can also send messages to the merchant to ask about the item.

Once the users have agreed to purchase the product, they can click the "add cart" button, where the shopping basket page will appear. To proceed with the purchase, the user needs to choose the quantity, shipping mode and delivering country. Then the total price will be automatically calculated. If users agree with the price, then they may proceed with the transaction, and the screen will be directed to the terms and conditions page. This page describes the details regarding the transaction such as the witness, reputation score and deposit fee. If users agree with the terms and conditions, they can key in their contact address, and send the product purchase request to the seller. Once the merchants receive the email, they will contact the buyer and finalise the transaction details before enacting the transaction (**Figure 9.8**).

### 9.3.1.8 My Wallet

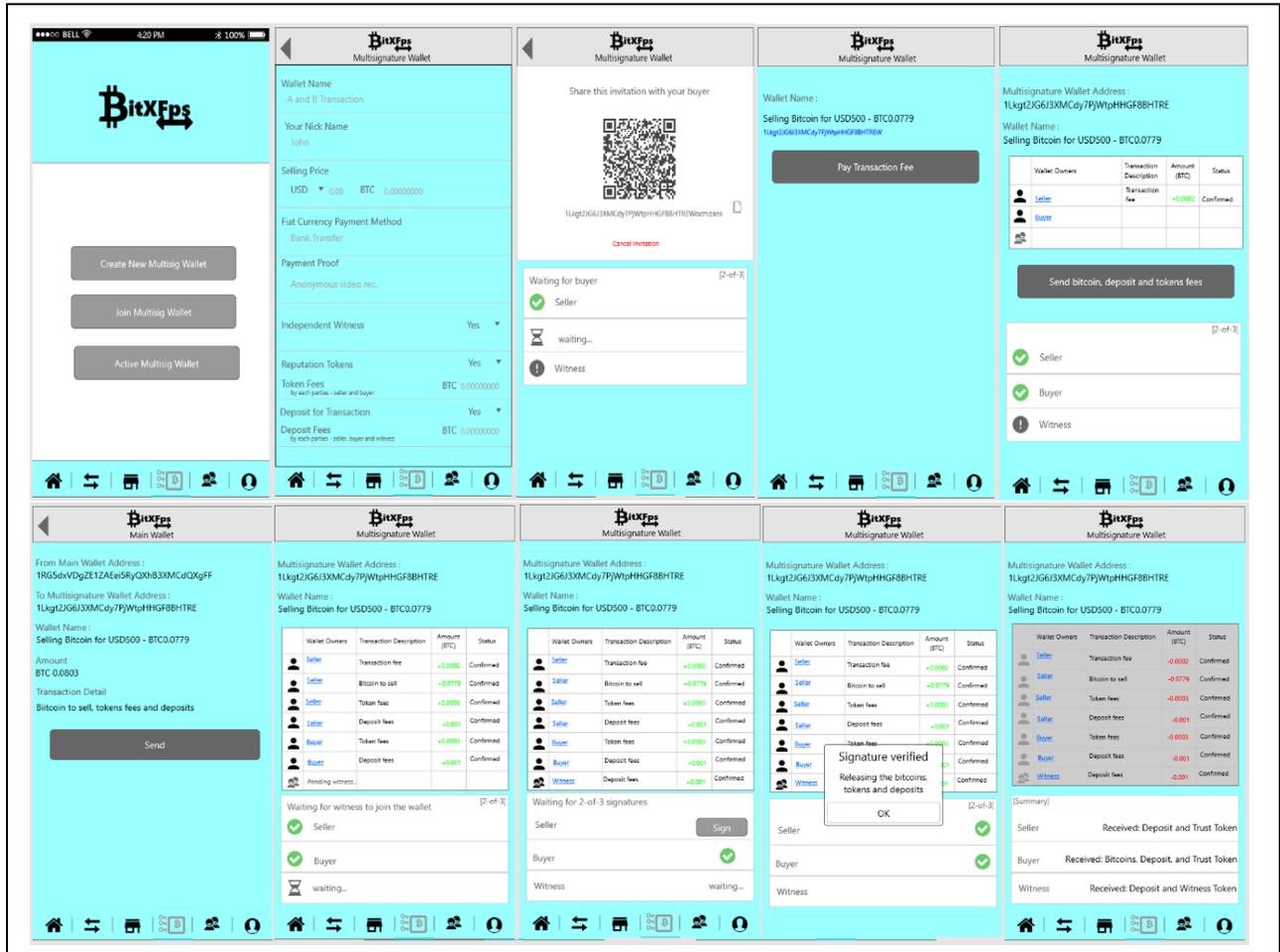


**Figure 9.9: The Function of My Wallet in Detail**

“My Wallet” function entails transactions in one’s personal wallet. The “My Wallet” main page shows the wallet address, and the total Bitcoins in the wallet. There are five “My Wallet” submenus, which are “Send Bitcoin”, “Receive Bitcoin”, “Personal Reputation Scores”, “Transaction History”, and “Backup Wallet”. To send and receive Bitcoins, the steps are similar to the ones on the home screen. Also, the backup wallet is a function which is accessible from the Security Settings. Reputation score shows the total trust tokens, witness tokens, and the number of successful transactions with details in the transaction history sub-menu (**Figure 9.9**).

#### *9.3.1.9 Multisignature Wallet*

The multisignature wallet in BitXFps is designed with a smart contract. Hence, it enables the buyer and seller to write the agreement details including the penalty if either of them fails to be honest in the transaction. The seller is responsible to draft the contract and invite the buyer to join the contract. Both signatures are required. Then they will pay the contract fee, as well as Bitcoin to sell, tokens fees and deposits. Then they have to wait for the app to randomly invite the witness of the transaction. Once the witness joins, the seller and buyer may proceed with the transaction as stated in the contract and sign the wallet to release the Bitcoin. Once the wallet receives signatures from both parties, it will automatically release the Bitcoin to buyer’s wallet and send the trust token to both wallets belonged to buyer and seller, while the witness will receive the witness token. All of them will also receive their own deposit. (**Figure 9.10**). However, if the wallet does not receive the signatures from both seller and buyer, it will alarm the witness to verify the transaction. This will be further explained in the witness user interface design.



**Figure 9.10: Details of the Multisignature Wallet Function**

### 9.3.1.10 Witness

The witness function is the most unique feature of BitXFps as it offers a decentralised mediator for peer-to-peer transactions. There are no other Bitcoin apps with this kind of witness function. The witness is crowdsourced from the BitXFps users. If a wallet ID is selected to be the witness, the owner will receive a notification of invitation. Before accepting the invitation, the owner may view the contact details including the type of offline proof to be used in the transaction such as video

recordings. If the owner is willing to act as a witness, he/she may accept the invitation and pay the deposit as stated in the contract. The deposit is sent to the multisignature wallet as a guarantee of honesty and responsibility. In the event of an honest transaction between buyer and seller, witness is not required to do anything during the transaction and will have the deposit returned in full at the end of the transaction besides being rewarded with a witness token. However, if there is any dispute, the witness will receive an alert to manage the dispute. To manage that, the witness has to check the contract and the proof of offline transaction from the seller to the buyer before making a decision regarding the dispute. The witness also has to sign the multisignature wallet to release the Bitcoins to the honest party. Once the wallet is verified with the signatures, it will release the Bitcoins, trust tokens, witness token and deposits according to the witness decision. In the case that the witness needs to work on the dispute, he/she will receive the full amount of his/her deposit, witness token and the deposit belonged to the dishonest party (**Figure 9.11**).

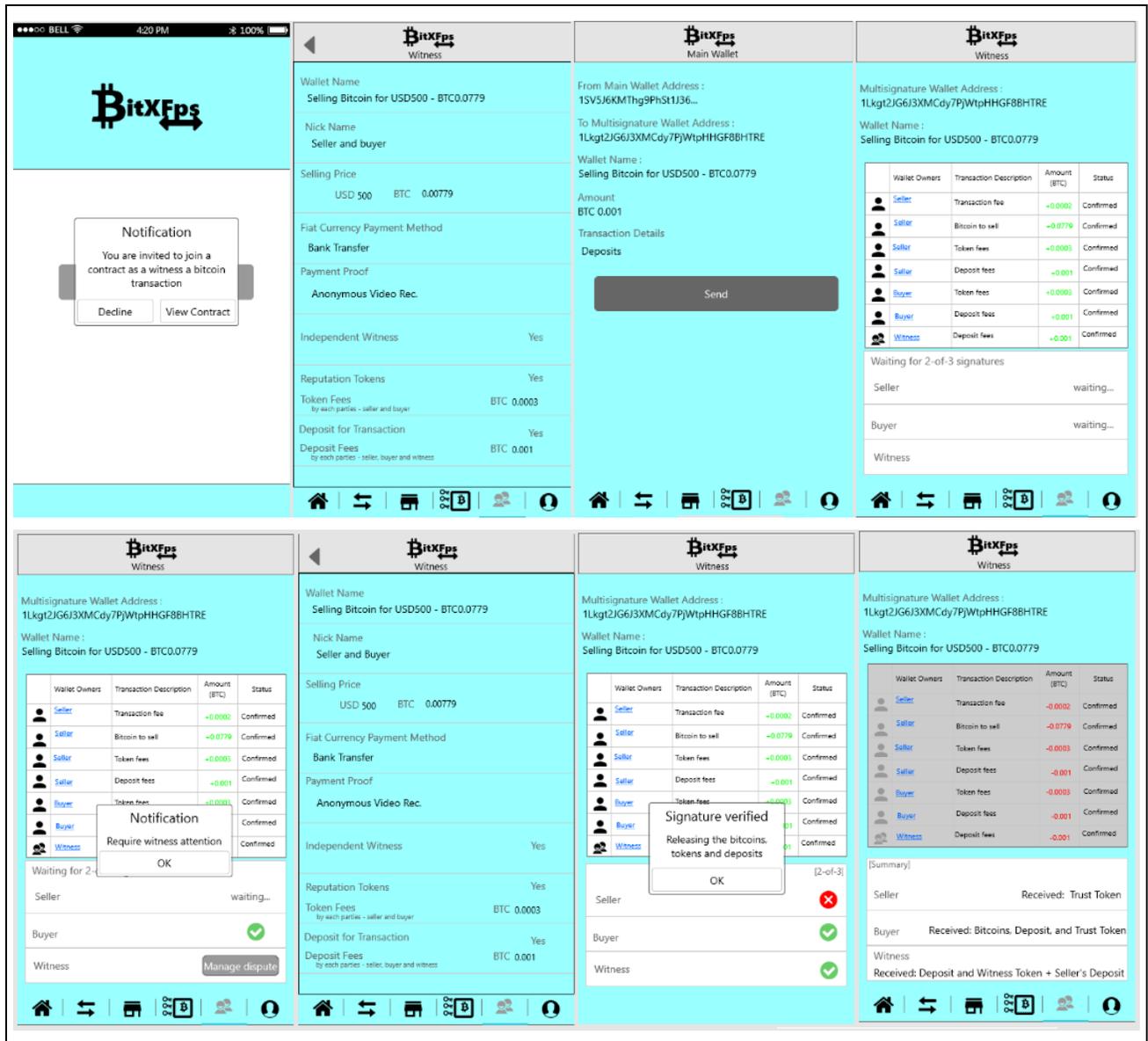


Figure 9.11: Details of the Witness Function

### 9.3.2 Reflections from the BitXFps User Interface Design according to the Proposed Guideline of Trust-Inducing Features for Bitcoin mobile applications

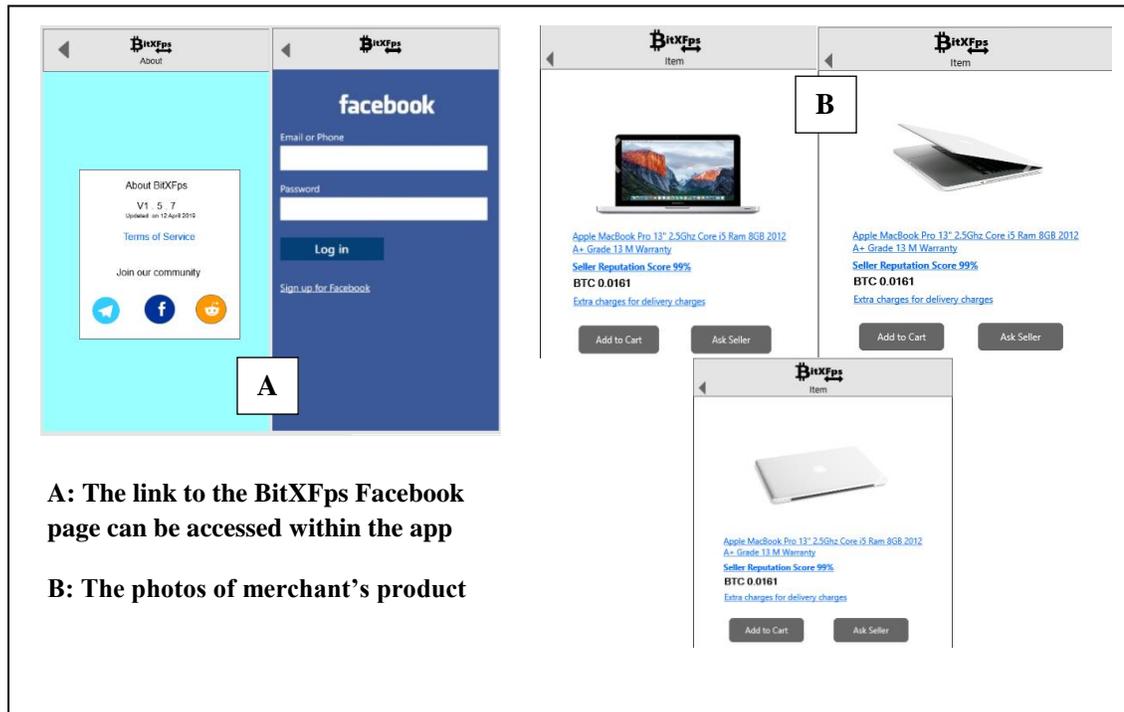
This section describes the trust cues of the BitXFps mobile application.

#### *9.3.2.1 Graphic Design*

Graphic design is described as the use of colours, layout compatibility, moderate layout complexity, and use of pictures. BitXFps app uses blue as the background colour for the wallet design like most of the Bitcoin applications. There are also other colours used BitXFps interfaces such as red, blue, green, and yellow **Figure 9.12**. For the wallet layout, the content in all pages is placed in a single column, and the height of the pages is kept short so the users no need to scroll for long. There are additional links to other social media such as Facebook because BitXFps is accessible via the app layout, as well as a link for users to exit from the app (**Figure 9.13: A**). Besides, pictures in BitXFps are displayed on the merchant page to describe the advertised products. The app allows merchants to upload up to three images for each product. The photo quality being uploaded must be good enough to attract users to purchase the product (**Figure 9.13: B**). This can strengthen the merchant credibility (Wang & Emurian, 2005).

Background					
Buttons					
Text					
Icons					
Tables					

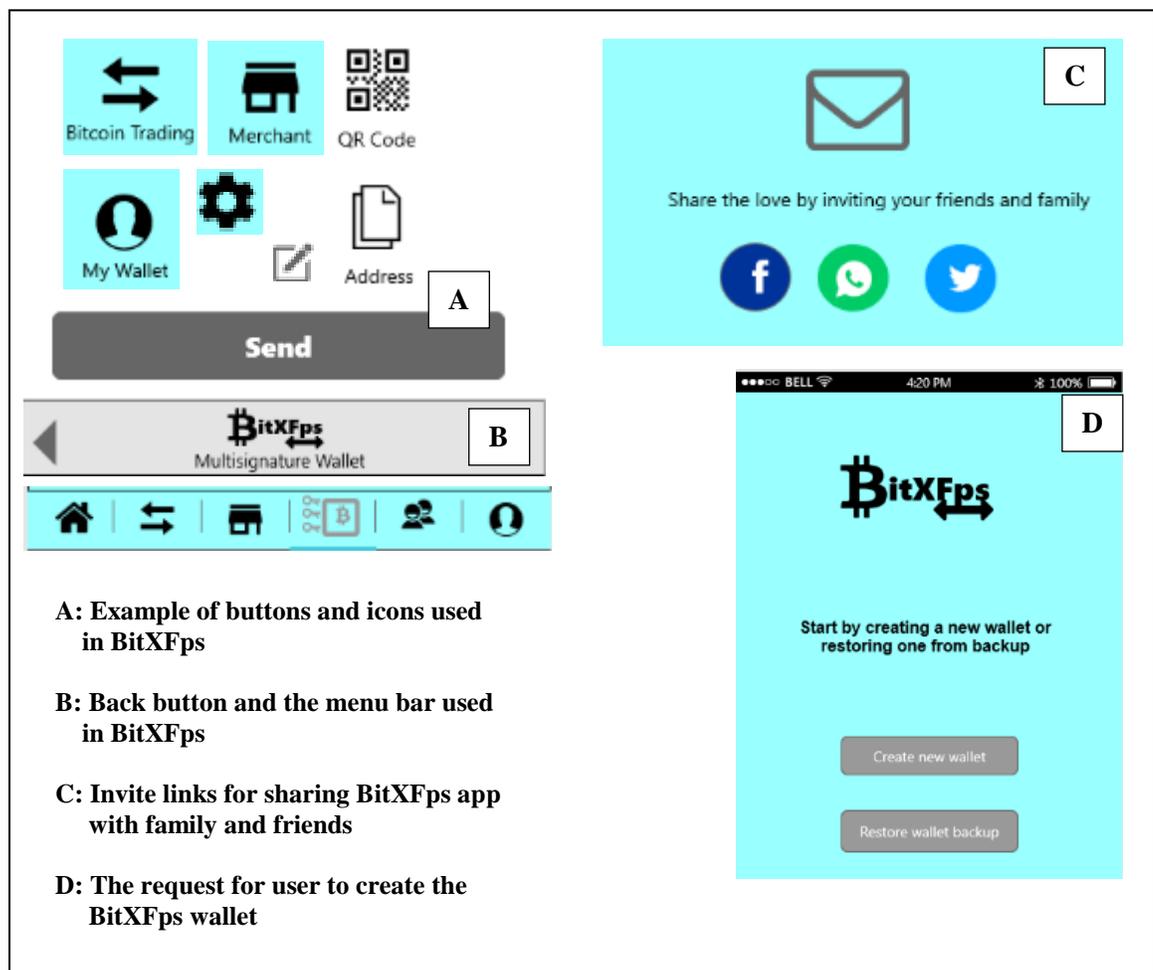
**Table 9.2: The Use of Colours in the BitXFps Design**



**Figure 9.12: The Elements of Trust in the BitXFps Graphic Design**

### 9.3.2.2 Structure Design

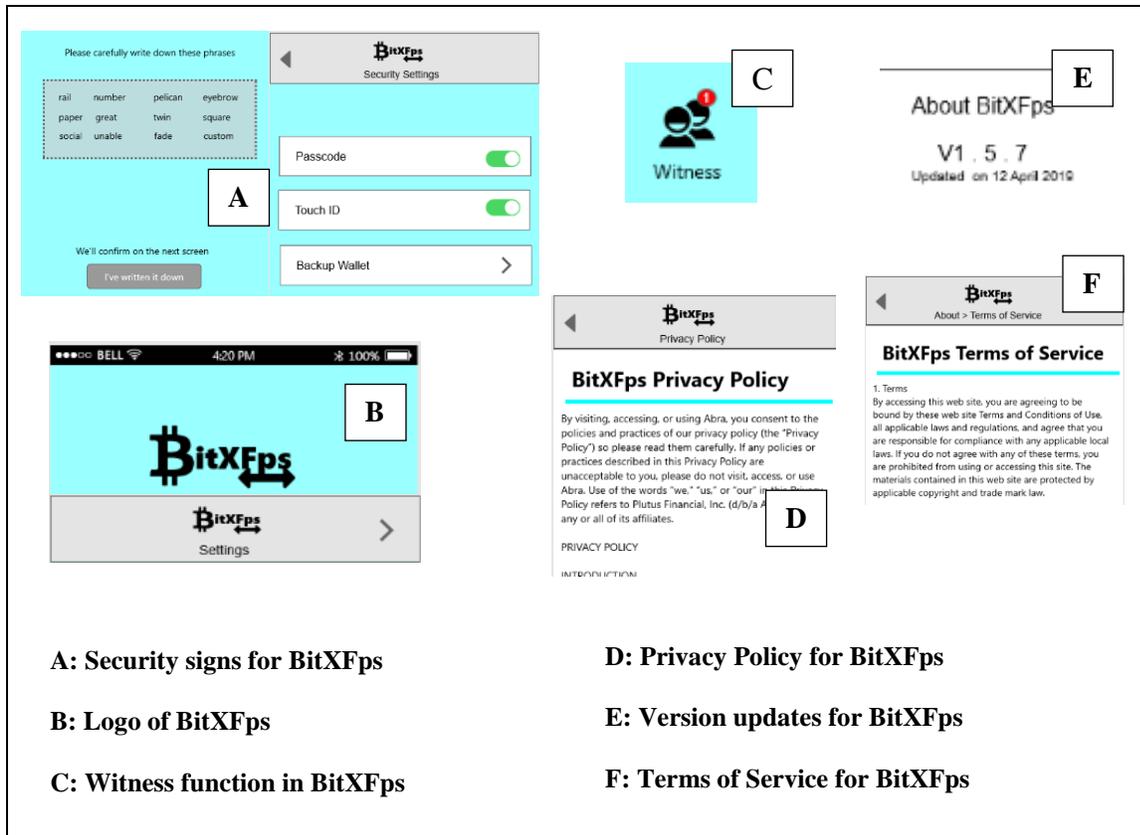
For structure design, there are three elements outlined in the checklist. First, in terms of usability, BitXFps app provides familiar icons and labels in the form of buttons to allow users to access the correct content before carrying out any tasks (**Figure 9.14: A**). There is also a menu bar at the bottom of pages and a back button at the top of pages. Those are navigation buttons to assist users to browse the app (**Figure 9.14: B**). Second, there is no broken link and the BitXFps app provides links for users to share the app with their friends (**Figure 9.14: C**), this requires the new users to create an anonymous wallet account (**Figure 9.14: D**).



**Figure 9.13: The Elements of Trust in the BitXFps Structure Design**

### 9.3.2.3 Content Design

There are eight elements under content design. First, regarding the security design, BitXFps uses phrases to resemble the wallet's private key for backup so that the app is fully managed by the wallet owner (**Figure 9.15: A**). BitXFps also enables users to activate the passcode, providing touch ID functions for wallet protection (**Figure 9.15: A**). Second, the brand is reflected throughout the app via the theme interface and colour (**Figure 9.15: B**). Third, the novel feature of the transaction method in BitXFps includes witness crowdsourcing from the large pool of Bitcoin users for the transaction to take place (**Figure 9.15: C**). In terms of privacy, BitXFps allows users to create the wallet anonymously and does not store any user details. There is also a specific page under "Settings" that describes the app's privacy policy (**Figure 9.15: D**). In terms of content credibility, since BitXFps is decentralised, there is no updated news but there are regular version updates to fix bugs and introduce new features (**Figure 9.15: E**). Then, the app terms and conditions are described in the "About" page (**Figure 9.15: F**).



**Figure 9.14: The Elements of Trust in the BitXFps Content Design**

### 9.3.2.4 Social Cue Design

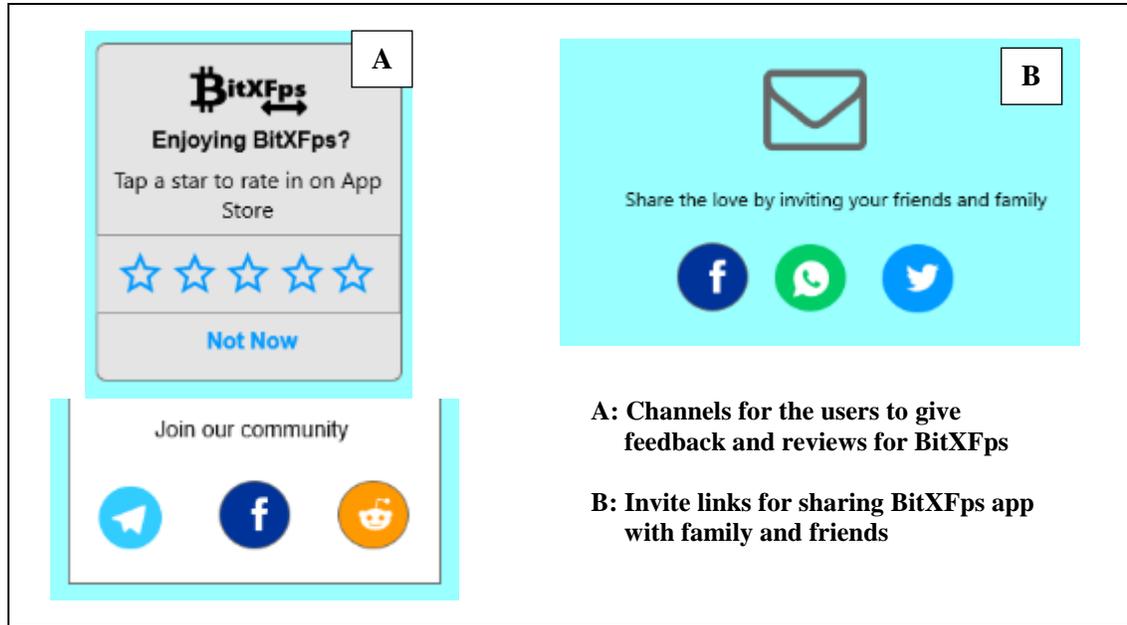
The social cue design describes the elements that develop trust among the users to the developers, for example via a link between the app and the developers’ personal blog. However, due to the BitXFps decentralisation concept, such connection is trivial. However, BitXFps fulfills the customer service criteria by providing the developers’ team contact email (**Figure 9.16: A**) and social media to connect users to the developers who share the updates regarding the app (**Figure 9.16: B**).



**Figure 9.15: The Elements of Trust in the BitXFps Social Cue Design**

#### 9.3.2.5 Personal and Social Proof Design

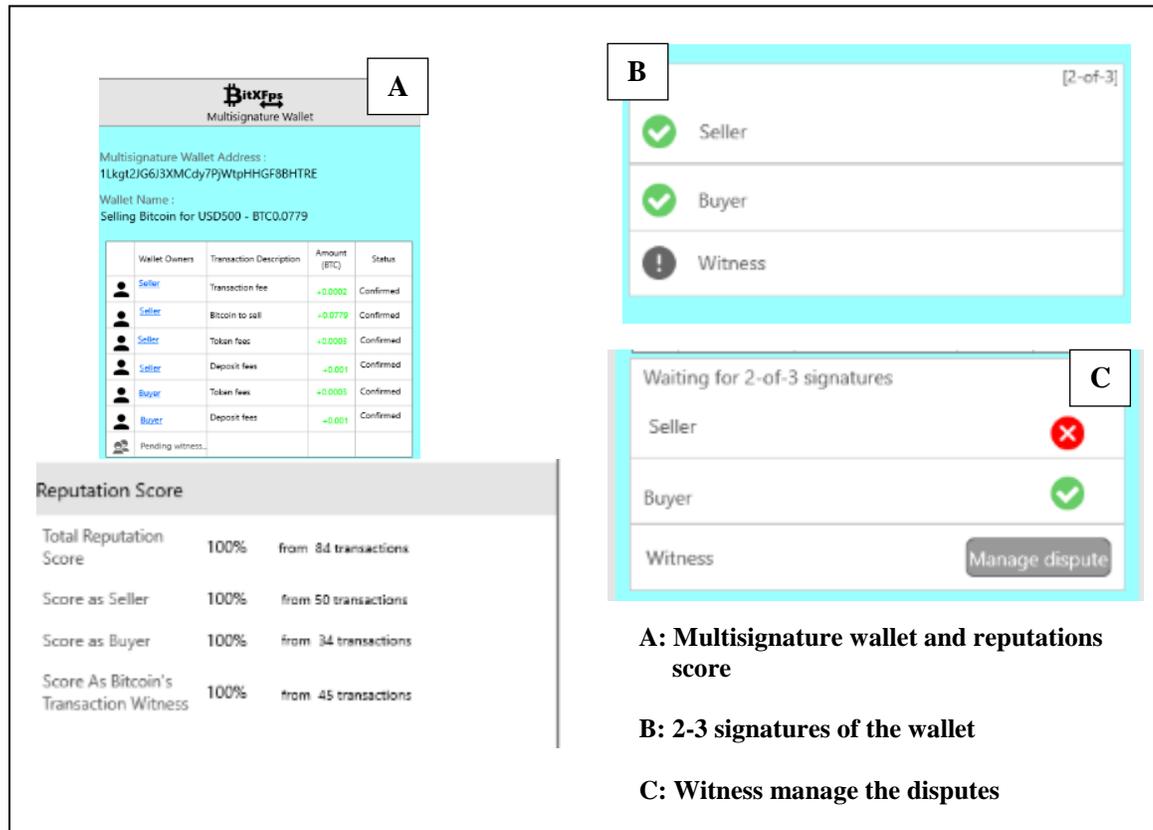
The personal and social proof is defined as the connection between users in the BitXFps app. BitXFps supports user social proof by providing rating and feedback functions through the app store and social media channels (**Figure 9.17: A**). Via social media, users can share their experience in using BitXFps. The app supports social proof design by providing users with links to the app to be shared with their friends and family (**Figure 9.17: B**). This extends the adoption of the app via social networks.



**Figure 9.16: The Elements of Trust in the BitXFps Social Proof Design**

### 9.3.2.6 Peer-to-peer Transaction Design Cues

The aim of the BitXFps design is to facilitate trust between users in enacting peer-to-peer transactions. The app is designed to support the multisignature feature that is embedded with a smart contract. This enables transparency in the transfer of Bitcoins in and out of the wallet according to the agreement between both parties (**Figure 9.18: A**). In addition, BitXFps allows users to send reputation token to symbolise their trust level of the parties involved in the previous transactions. Both smart contract and trust token features are designed to make peer-to-peer Bitcoin transactions transparent (**Figure 9.18: A**). In BitXFps, the written smart contract has to be verified by both seller and buyer to ensure that they both agree with the transaction details including the penalty imposed for being dishonest. Hence, the verified smart contract represents a valid contract between both parties (**Figure 9.18: B**).



**Figure 9.17: The Elements of Trust in the BitXFps Peer-to-peer Transaction**

### Design Cues

The transactions via BitXFps app are mediated by a decentralised witness who is randomly appointed from the app users. The witness plays a role to manage any dispute between the seller and buyer (**Figure 9.18: C**). At the end of the transaction, the app allows users to send a trust token to each other. In addition, they are required to send a witness token to the witness as an appreciation for being willing to mediate the transaction. However, if the witness is not responsible and does not respond to the dispute alert, the witness will receive penalty with zero witness token, and the witness's deposit will be transferred to another appointed witness. The trust and witness tokens are linked to the users' wallet and get recorded in the Blockchain

(**Figure 9.18: A**). Hence, this indicates the wallet owners' credibility and trustworthy.

#### 9.4 Chapter Summary

The outcomes in this chapter come from the list of guidelines to design for trust for a Bitcoin wallet app. Such guidelines are useful to examine the trustworthiness of Bitcoin wallet app interface designs, as well as for other types of cryptocurrency. In turn, the evaluation checklist is further applied in designing the user interface of BitXFps prototype. To better understand and explore the value of the BitXFps interface and its embedded trust elements, the app needs to be evaluated by Bitcoin users. So in the following **Chapter 10**, the BitXFps interface design will be evaluated by experienced Bitcoin users who can help to review the checklist and heuristic evaluation method.

# Chapter 10

## Evaluation of BitXFps Mobile Wallet Application and How Its Interface Supports Trust

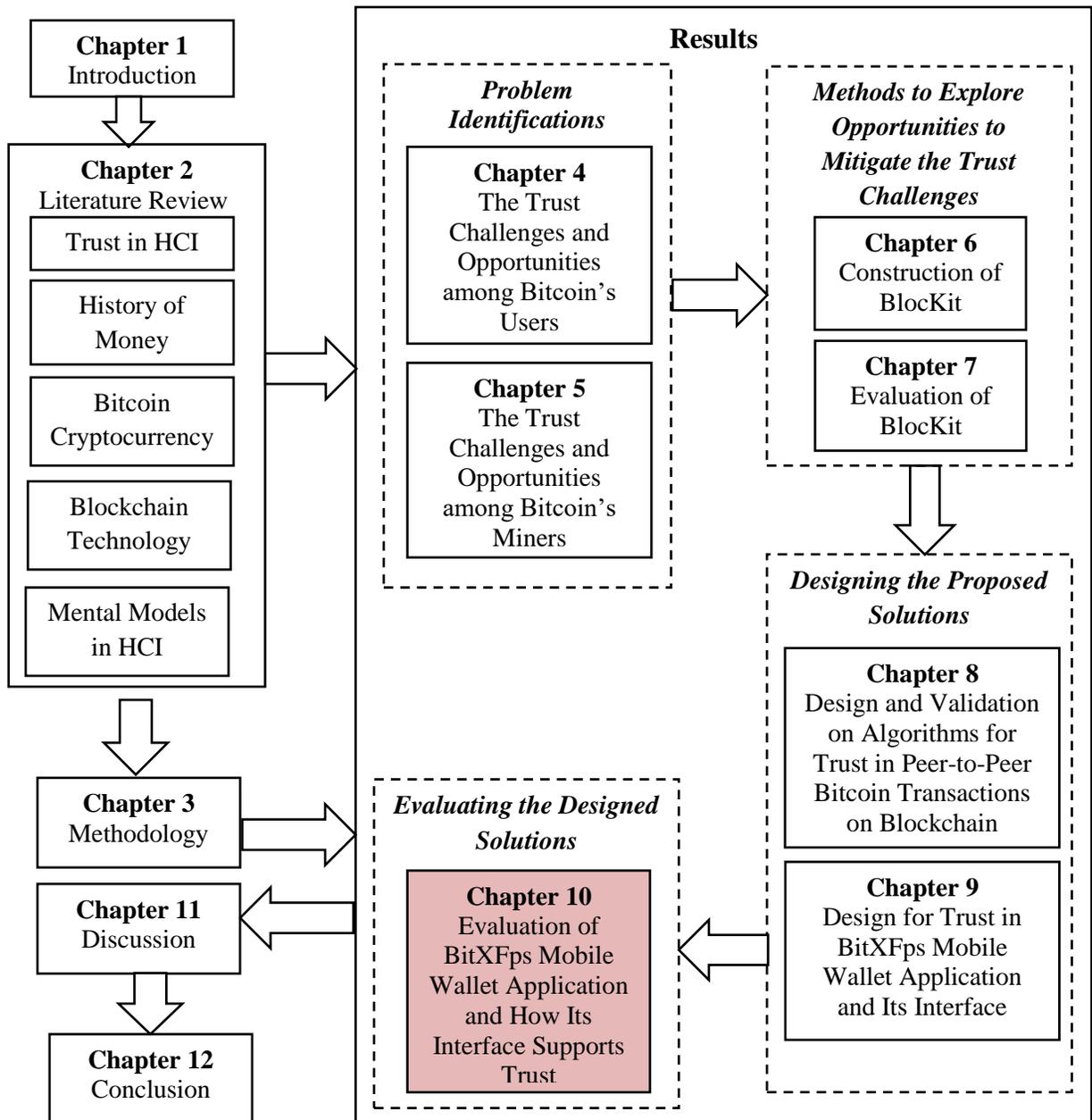


Figure 10.1: Chapter 10 of Thesis Structure

## 10.1 Introduction

A list of guidelines to design for trust for Bitcoin mobile application user interface has been identified in **Chapter 9**. The guidelines are also used as the reference to design the mobile wallet app user interface for peer-to-peer Bitcoin transactions (BitXFps). The uniqueness of BitXFps is the app interface which is designed based on the algorithms for trust elements in peer-to-peer Bitcoin transactions and its underlying design principles; transparent transactions, valid contract, decentralised mediator, and system reputation. The algorithms were identified and validated by the Bitcoin Blockchain experienced users in Study 3 and Study 4 (**Chapter 7 and 8**). However, it is essential to conduct the trust validation test among the BitXFps users when they are using the wallet app. In this chapter, a prototype of BitXFps is built and evaluated (Study 5) with 12 Bitcoin users to address the following research questions:

- *which elements of the BitXFps user interface design develop trust for peer-to-peer Bitcoin transactions?*
- *how does the design of the BitXFps interface mitigate the trust issues in peer-to-peer Bitcoin transactions?*

This chapter reports on the interviews conducted with 12 Bitcoin users while using the BitXFps app prototype. The study advances the theory of trust-inducing features of the interface design to highlight the important trust elements in BitXFps app besides identifying the new trust elements for peer-to-peer transactions and the trust-related risks in BitXFps and ways to mitigate them. The chapter is concluded with the framework of trust-inducing features for peer-to-peer Bitcoin transactions. It also proposes new features such as the Blockchain real-time communication to capture the proof of offline transaction for delivery

of goods and fiat money transaction as well as the revised BitXFps app interface to develop a higher level of trust.

## 10.2 Research Method

Twelve Bitcoin users were recruited in this study, 7 male, 5 female, (mean age of 31.4 with age range of 23-41). Five participants had experience of less than a year in using Bitcoins, three of them had 2 to 3 years of experience, while the remaining four had used Bitcoins more than 4 years. In terms of educational background, five of them have Bachelor's degree and the rest have Master's degree. Participants have a variety of career paths; 2 were in financial and marketing sector, 2 in the engineering field, 2 in the academic line, and 6 of them were students. 2 participants were recruited from Study 1 (exploring the Bitcoin practice among the users) and 3 were from Study 3 (evaluating BlocKit with the Bitcoin Blockchain experienced users). Then the study applied snowball sampling that seven more participants were introduced in the interview sessions.

Participants were asked to select the dates they are available in a Doodle pool and were grouped into 4 groups (3 for each group). The participants were instructed to engage with the BitXFps prototype in a workshop. The BitXFps app was developed using the Mockupplus Software (MockupPlus, 2019). The aim of the mock-up session is to evaluate the trust level to its interface among the users. In each group, the participants were given a role as the Bitcoin witness, seller or buyer. They were also given an iPhone 6 installed with the BitXFps customised designs specific to their role. Participants were asked to enact two types of Bitcoins transactions using the app. Firstly, they had to purchase a MacBook using Bitcoins, and second was to sell 0.0779 Bitcoins at the price of 500USD. Prior to the transaction, they were briefed with the BitXFps application, especially on the witness

function, as this new feature is not available in the typical Bitcoin wallet apps. Due to the fact that BitXFps is only a prototype, the interviewer assisted participants to use the app and manage their turns doing the transactions for each participant, for example, once the buyer has signed the multisignature wallet, they need to wait for the seller to sign to receive Bitcoins from the multisignature wallet. Once both transactions are completed, participants were asked about their perceptions of the interface design in app.

Then, they were interviewed based on the design for trust guidelines as described in Chapter 9 with the following questions: “*are there any important functions that are not included in the app?*” and “*do you find any difficulties while navigating the functions within the app?*” They were also asked with questions related to the app’s content and design: “*do you think that the security signs are good in building trust among users?*”, “*what else can be done to improve trust via the app image and branding?*”, and “*what kind of additional contents that are relevant to develop trust to be included in the app?*” There are also questions on graphic design; “*what choice of colours that can boost the trust?*” and “*what type of photos should be included in the app to improve trust?*” Personal and social Proof was explored through questions such as; “*do you think social media pages can help to increase personal and social proofs?*” while social cue design was explored via questions such as: “*do you have any suggestions to improve the social cue design for the app?*” Then, the questions related to trust elements in peer-to-peer transactions; “*do you think that the transparency in the transaction can improve trust?*”, “*do you agree that any agreements between the buyer and seller included in the contract will facilitate trust?*”, “*do you think the witness can be a good mediator to mitigate trust issues in the transaction?*”, and “*do you agree that the user’s reputation can help to build trust to proceed with the transaction?*”.

The workshops lasted between 45 and 60 minutes, the sessions conducted were video recorded and fully transcribed. Data analysis involved a hybrid approach with the deductive coding, and new ones from the data, contributing to the inductive coding (Fereday & Muir-Cochrane, 2006). The deductive codes include the trust-inducing features such as graphic design, content design, structure design, social cue design and personal and social proof design (Seckler et al., 2015; Wang & Emurian, 2005), and the principles to design for trust in peer-to-peer Bitcoin transactions that have been highlighted in the findings in Study 3 with the experienced Bitcoin Blockchain users (Chapter 7)The codes were iteratively revised based on the interview data, thus resulting in new codes under the theme of Bitcoin wallet app design for trust in peer-to-peer Bitcoin transactions.

### 10.3 Findings

This section outlines the elements of trust embedded in the BitXFps design, followed by the descriptions of the trust-related risks perceived in relation to the app's interface and ways to mitigate them.

#### 10.3.1 The Elements of Trust Embedded in the BitXFps Interface Design

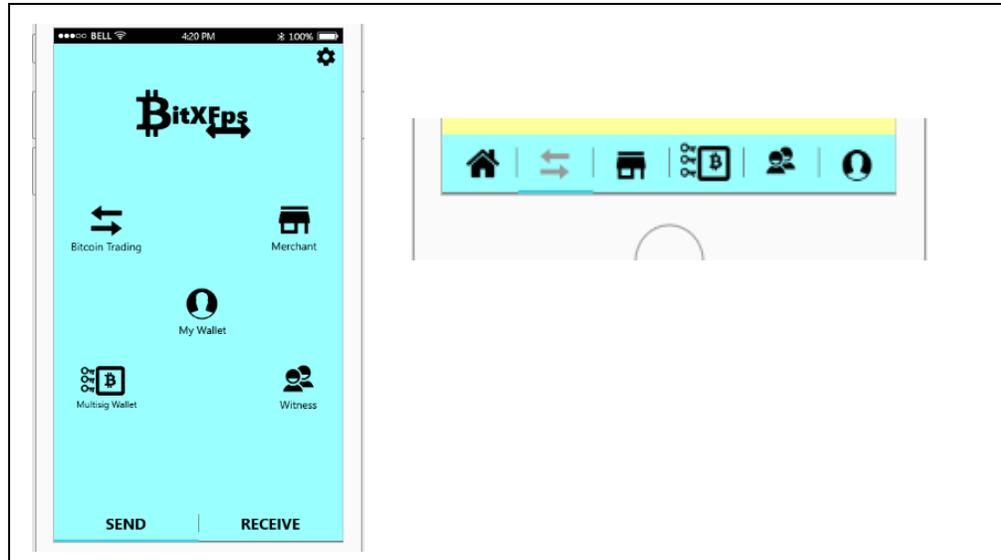
This section describes the trust elements associated with the BitXFps user interface such as graphic design, structure design, content design, personal and social proof, social cue designs, and peer-to-peer transaction design cues.

##### *10.3.1.1 Graphic Design*

It was found that the choice of blue for the app's layout is appropriate as all participants are satisfied with the selection; “*the colours suit the app*” [P12]. The

blue colour was selected based on the findings in previous research on users' trustworthiness towards corporate websites, where the blue scheme is perceived as the most trustworthy (Alberts et al., 2011). In addition, blue is also associated with competence as this colour signals intelligence, communication, trust and efficiency (Fraser & Banks, 2004; Mahnke, 1996; Shneiderman & Ben, 2000; Wright, 1988). Hence, the use of blue in the Bitcoin wallet app can contribute to the user's initial trust.

The findings also show that all participants appreciated the app layout interface: *"all the icons (in the homepage) are similar with the menu (at the bottom of all pages), [...] it helps the users to get familiar with the functions in the app"* [P11]. Every BitXFps functions were designed in the form of icons and the same icons are used in the site menu throughout the app. This enables users to navigate from one function to another (**Figure 10.2**). In addition, three participants liked the table summarising the ongoing transaction updates on the wallet page: *"it is transparent because we can see everything coming in and out as well as the signatures in this table"* [P5]. This allows all users that are involved in a transaction to have similar information regarding the transaction status. This is to prevent the attempts of scam or fraud that usually occur in peer-to-peer Bitcoin transactions with fiat money or goods. The main reason such fraud attempts take place is due to lack of transparency in the offline transaction. Hence, this reflects the importance of the transparency element in developing trust when it comes to Bitcoin transactions.



**Figure 10.2: Icons on the homepage and the bottom menu of the BitXFps interface**

3 participants suggested improving the table design: *“it is better if you differentiate the seller and buyer (in the active wallet table) by using different colours or icons. [...] The new users may get confused because they may mix up the (wallet) address with another”* [P7]. This suggests the icon’s design to be revised so that users can easily read the summary table. This, in turn, will increase the app information visibility and ease-of-use thus contributes to the credibility of the app.

### 10.3.1.2 Structure Design

It was found that all participants are familiar with the BitXFps functions; *“it has the common functions like other Bitcoin wallets”* [P2]. To design the user interface, it is important to ensure that the organisation of the interface is not too different from other Bitcoin wallet apps. This to make the users get familiar and comfortable in using the app to send and receive Bitcoins, allowing them to create simple transactions within the app: *“that’s easy [...] Click send (from the homepage) (then)*

*just type in 1 here (the Bitcoin amount in the text box) and paste or scan the receiver's address here (address textbox). I want it to be fast (transaction fee button) and send (send button)” [P4]. Similar actions were performed by all participants to send Bitcoins via the BitXFps app. This demonstrates that user familiarisation is essential in organising the structure within the app.*



**Figure 10.3: Invite friends page**

3 participants suggested to improve the witness function efficiency: *“I don’t want to be a witness anymore. Can I stop from receiving the notification to be a witness? [...] I think you should do this or else it will annoy the users” [P12].* This suggests the value of privacy in the app interface. This in turns highlights the importance to change the design for trust in Bitcoin apps.

Other suggestions are related to the design structure of the witness function, as mentioned by 6 participants: *“how long do we have to wait for the witness to join the wallet? [...] It is better if the user can see the timer for them to estimate the waiting time” [P9],* while 9 participants commented on the notifications: *“what happened if I*

*don't check my email [...] there should be another way to alert the users such as text message*" [P1]. This highlights the importance of users to be aware with the design. The timer is relevant for users to estimate the waiting time for the transaction, as well as the additional notification mechanisms to alert users to take actions in the transactions. This will help to enhance the app usability.

It was found that the suggestions to create an anonymous wallet account in BitXFps was well received by 6 participants: *"I need to take my picture while holding a paper written with my name and passport ID. This is ridiculous. [...] this app does not even ask about my email to create an account [...] It means they don't have my personal data, which is good"* [P5]. This reflects the importance to protect user personal details. In the most centralised Bitcoin exchange app such as, users are required to provide their personal details so that their identity can be verified. This is important to avoid fraudulent transactions. However, the exchange verification processes are tedious and the exchanges companies gain access to the user personal details. This is indeed inconvenient for the users.

### *10.3.1.3 Content Design*

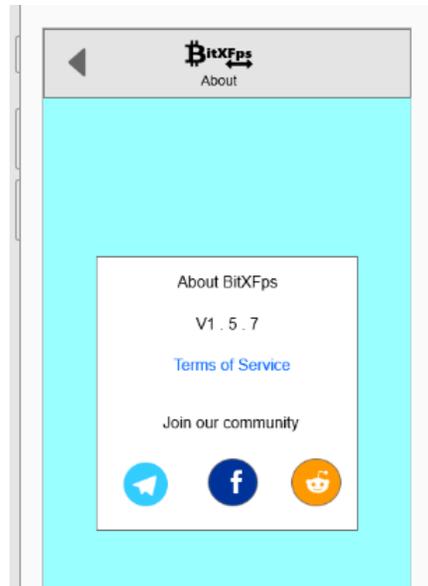
It was found that all participants are satisfied with the app security aspect. By providing the backup wallet features for the users to keep and protect their own private key, the app, in fact, does not store any user credentials. This reflects the app protects its users' privacy. Most of the participants agreed that the design in the app establishes positive image and branding: *"the app colour theme and logo are synchronised and consistent throughout the app"* [P10]. However, 3 participants argued that the app main characteristic is not properly highlighted: *"I can say the app*

*main selling point is the decentralised witness for the offline trade. However, it is not been highlighted (as a unique tool), making the app just like other Bitcoin apps”* [P8]. This reflects the importance of the design in the Bitcoin wallet app so that users can differentiate it from other wallet apps. This, in turn, reflects the credibility of the app.

Also, three participants suggested the developer to include documentation to strengthen the app credibility and its contents: *“it is good if you can provide a link to the white paper of the app development [...] or the source code in GitHub [...] this will definitely give a good impact to build credibility and trust towards the app”* [P10]. This suggestion is important as BitXFps is designed as an open source and decentralised Bitcoin mobile application. Hence, the source codes with supporting documents in the app are essential for the app developers and community to enhance its performance.

#### *10.3.1.4 Personal and Social Proof*

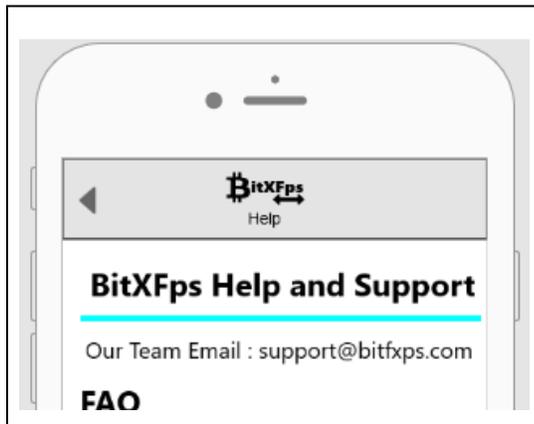
The feedback for the friend social proof is also positive, as mentioned by three participants who share this opinion: *“when I join the (BitXFps) Facebook page, I can see my mutual friends who are using the wallet as well. So in the future we can trade between each other”* [P6]. This shows that the app design has a strong proof for friends’ connections via BitXFps social media channel (**Figure 10.4**), which allow the users to do trusted transaction with their friends using the app.



**Figure 10.4: Link to Social Media in BitXFps**

#### *10.3.1.5 Social Cue Design*

The trust elements related to social signs reduce the gap of social distance and increase intimacy. The integration of social media and website is common to connect the users with web providers and enhance communication between the users (Basso et al., 2001; Riegelsberger et al., 2005; Seckler et al., 2015; Steinbrück et al., 2002; Wang & Emurian, 2005). It was shown that participants are not satisfied with the BitXFps customer service that provides an email address to reach the support team (**Figure 10.5**). Six participants suggested to create an in-app discussion channel: “*I can only find the team email address [...] There should be a channel for all users and developers to interact within the app like in-app discussion forum*” [P10]. This indicates that additional support function is important to strengthen the app’s credibility. Since BitXFps app is not centralised, the option to have an in-app community discussion channel is valuable to further assists the users.



**Figure 10.5: Support Service Email**

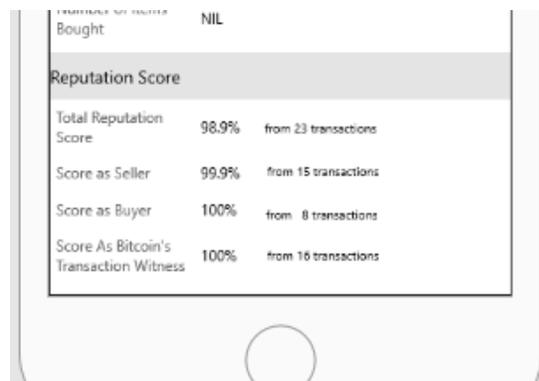
One of the criteria under social cue design is the real-world link, which is defined as the link to the website owner life or link to the real world such as a shop (Seckler et al., 2015). It was shown that participants are less satisfied with the real-world link of the app because it only uses social media. Therefore, nine participants suggested to create a website to support the app: *“although it is a crowdsourcing app, I think it would be good if there is a proper website to provide detailed explanations of the app, including its development, besides allowing the community to contribute and interact with the developers [in order] to enhance the app performance”* [P5]. This shows the demand for additional information to support the app. By connecting the users with the developer’s website, this enables users to contribute to app development, thus strengthening user confidence towards the app authenticity and its developers.

#### 10.3.1.6 Peer-to-peer Transaction Design Cues

To conduct peer-to-peer transaction, the trusts cues in the BitXFps interface are vital. In this aspect, all participants are satisfied with the BitXFps interface design. Three participants claimed that the transaction transparency involving cryptocurrency transfer such as Bitcoins and Ether are better than the offline transactions involving Bitcoins and fiat money or goods; *“the transaction between Bitcoin and Ether can be conducted synchronously [...] as you can track the crypto movements from one wallet to another through Blockchain. The same goes for Bitcoin and fiat money, but you need an exchange company to do it”* [P2]. This reflects the ability of centralised exchanges in managing the transactions transparently and synchronously, provided the users pay the fee to use this service.

BitXFps offers similar options in enacting peer-to-peer transaction transparently. Six participants like the decentralised quality of transactions supported by the app; *“it is brilliant to create the transaction in a multisignature wallet with a contract [...] we can include penalties for those who are dishonest”* [P11]. This shows that users appreciate the wallet app design that integrates two important elements to build trust, which is the multisignature wallet and smart contract. Although it is partially transparent, the use of both elements in BitXFps ensures the Bitcoin movements take place once the consensus involving the buyer and seller in the transaction is reached. Hence, the offline transaction needs to be completed before Bitcoin is released from the multisignature wallet. This enables users to enact two-way peer-to-peer Bitcoin transactions in a trusted way.

The next element under the peer-to-peer transaction cue is a valid agreement between buyer and seller. All participants agreed that BitXFps app is satisfactory and stressed the importance of the contract: *“the contract is important to protect users from scammers and fraud”*. [P2]. In the convention peer-to-peer transaction between strangers, they usually communicate via text messages and agree on terms of the transaction (Sas & Khairuddin, 2017). However, such terms are not legalised and no action can be taken against dishonest traders. So to prevent this, the agreements are sealed with smart contract in BitXFps. Six participants mentioned the validity of this approach in the Blockchain: *“everything that is included in the Blockchain is considered as a legal document, including the contract between seller and buyer”* [P3]. Hence, the contract can protect both parties during the transactions.



**Figure 10.6: Design for the BitXFps User Reputation Score**

Another element in the BitXFps design is the user reputation score, reflecting user trustworthiness in the previous transactions. BitXFps is designed with three reputation tokens, each for the seller, buyer and witness. For each wallet, the total reputation score is calculated as the average sum of the three tokens (**Figure 10.6**).

Findings indicate that all participants emphasise the importance of the reputation system; *“in a peer-to-peer transaction it is important to know whether the person we are dealing with is reputable or not. [...] This reputation score is a good indicator”* [P1]. This, in turn, supports the user reputation design to facilitate them in future decision while engaging in Bitcoin transactions with the respective user.

### 10.3.2 New Trust Elements for Peer-to-peer Transaction Design Cues

Interestingly, six participants identified a new element to develop trust in peer-to-peer Bitcoin transactions: *“if the witness finds that this person (buyer) is a scammer, then he will sign here (dispute page) to reverse the Bitcoin back to the seller [...] so the transaction is safe. [...] I think a reversible transaction is also important in peer-to-peer transaction”* [P3]. This indicates the ability to reverse transaction is essential in peer-to-peer Bitcoin transactions. Although in the original Bitcoin Blockchain reversible transaction is not allowed since the transactions are recorded in the ledger, the reversible transaction feature provided by BitXFps still maintains the Blockchain core characteristic, which is to be decentralised. Hence, the reversible transaction feature extends the core concept of Blockchain to develop trust in Bitcoin transactions because the transactions can be reversed before being recorded in the Blockchain ledger.

### 10.3.3 Risks Related to Trust

This section describes the trust issues related to the witness function in BitXFps.

#### *10.3.3.1 Concerns about the Role of Witness*

Nine participants are not confident with the witness function to manage dispute; *“the problem arise when, let say, the witness says the seller is a scammer, but actually the latter is innocent and it is the other way around (the buyer is the real scammer)”* [P7]. They raised concerns regarding the witness’s credibility in making the decision during the dispute. In BitXFps, the witness has to take decision during dispute based on the proof of transaction, as stated in the contract. The contract is written by the seller, and the details include the proof of offline transaction as has been agreed by the buyer. The proof can be in the form of a video file or image file of the offline transaction, which needs to be sent by the buyer to the seller via email. However, 6 participants questioned the authenticity of the proof; *“how can the witness prove that the evidence is not fake”* [P11]. This is similar to the findings from the workshop with the Bitcoin Blockchain experienced users on the algorithm design. Based on the experienced users’ feedback, the design of the algorithms is revised by introducing a new field in the contract for the users to mention the type of offline transaction proof that used in the transaction. However, the revisions still do not solve the issue. In other words, although the type of offline proof is recorded in the smart contract, the buyer or seller who performs the offline transaction can still provide counterfeit proof of transaction, such as fake bank slip. Thus, this issue needs a better solution and will be further described in 10.3.4.1.

#### *10.3.3.2 Deanonymising Confidential Details to the Witness*

On the other hand, six participants expressed concerns about sharing their personal data with the witness: *“I would rather give my details to the exchange because I*

*know they are bonded to the legislative body instead of giving them to the witness who I know nothing about” [P9].* In BitXFps, to enable the witness to make a decision in the event of dispute, he/she can request the proof of transaction from both seller and buyer, as stated in the contract. Although no personal details are recorded in this contract, the witness may request additional information from the seller or buyer, such as passport number as the supporting evidence to make decision for the dispute. This challenges the Blockchain anonymity feature and the witness may take advantage to misuse the buyer and seller’s personal details. A proposed solution to support this issue will be further discussed in 10.3.4.2.

#### 10.3.4 Suggestions to Mitigate the Risk

This section describes ways to improve the witness function in BitXFps to develop trust in peer-to-peer Bitcoin transactions.

##### *10.3.4.1 Standard Format of Proof of Evidence for Offline Transaction*

Six participants propose for the format of offline proof to be standardised: *“I think the type of evidence should be standardised” [P1].* At the moment in the BitXFps design, there is no specific type of proof for offline transaction is set for the app. The seller and buyer are free to decide on the type of proof and include it in the contract. By having a standard format of proof for the app, this enables the offline evidence to be managed in more systematically.

It is important to ensure a standard format of proof for offline transaction is properly used by the witness in managing dispute. Three participants suggested the use of video call to capture the offline transaction for fiat money and goods as the

proof of transaction; *“they (seller, buyer and witness) can make anonymous group video call while enacting the offline transaction by only showing the important parts of the transaction [...] At the end of the conversation, the witness must ensure that both parties are happy with the offline transaction”* [P10]. Instead of witness only plays a role in the event of dispute, this suggests that the witness joins the seller and buyer to verify the proof of offline transaction real-time. The anonymised video call can also overcome the issue of disclosing personal information to the witness thus protect both seller and buyer’s details.

In contrast, transactions involving the exchange between Bitcoins and goods, the format of evidence will be in the form of video file, as suggested by three participants: *“when they receive the parcel they can record a video, starting from unboxing until the product is examined in a single video”* [P6]. For the exchange of Bitcoins involving products, the delivery process involves the third party, so the courier company can provide proof of delivery. There is a possibility of dispute between seller and buyer involving the quality of goods being delivered. In BitXFps, it is compulsory for the seller and buyer to add in the detailed specifications of the goods in the contract. Thus, the video of unboxing goods from the original packaging on the same day of delivery can facilitate the witness to verify the transaction.

#### *10.3.4.2 Standard Guidelines for the Witness to Manage Dispute*

The witness makes decision based on the proof of transaction. Nine participants mentioned the importance of a standard guideline to be referred by the witness while working on the dispute: *“if there is no proper SOP for the witness to do their work, this will cause a problem [...] Different people have a different thoughts and views”*

[P4]. By having a standard guideline to manage the dispute, the decision will be made consistently, that involves a checklist for witness to analyse the proof via the video.

Three participants suggested a checklist to be referred by the witness while engaging in the video call *“the checklist can be used by the witness to ensure that there is no disagreement between seller and buyer [...] Similar checklist should be used by the seller and the buyer”* [P12]. This supports that the transactions are required to be verified consistently. A standard guideline to enact Bitcoin transactions in BitXFps should be created and all parties involved have to play their role according to the guideline. This, in turn, will prove the integrity of the users and transaction transparency.

#### 10.4 Theoretical Implications

The findings are from the evaluation of BitXFps interface in developing trust among users. The evaluation was conducted based on the theories of trust elements for the website and mobile application interfaces (Hasslacher, 2014; Seckler et al., 2015; Wang & Emurian, 2005). The findings in Study 3 and Study 5 (Chapter 7 and 8), as well as Chapter 9, serve as a guideline in the evaluation study. The guideline consists of six characteristics namely graphic design, structure design, content design, personal and social proof, social cue designs, and peer-to-peer Bitcoin transactions design cues. The use of trust elements on BitXFps interface are acknowledged by the users based on those characteristics and further described in the following section.

#### 10.4.1 Towards a Framework with Trust-inducing Features for Peer-to-peer Bitcoin Transactions

According to the Wang and Eumarian's (Wang & Emurian, 2005) framework of trust, as well as its value in the graphic design element, the study found that blue is preferable to be the BitXFps layout. This is similar to the colour selection for the top 20 Bitcoin mobile applications, in which blue is the most frequently used in the app background (Chapter 9). The literature also supports the use of blue can develop trustworthiness (Labrecque & Milne, 2012). In addition, blue is also linked to competence as this colour is associated with intelligence, communication, trust and efficiency (Fraser & Banks, 2004; Mahnke, 1996; Shneiderman & Ben, 2000; Wright, 1988). Hence, this extends the suggestions by Wang and Eumarian (Wang & Emurian, 2005) to consistently use moderate to low brightness and cool tone to induce trust among users.

Another finding for the graphic design characteristics is the design of the app layout to ensure transaction transparency. In peer-to-peer Bitcoin transactions, transaction transparency between buyer and seller is crucial to develop trust (Sas & Khairuddin, 2017). Since the transactions are not governed by any centralised party, BitXFps aims to ensure that the design is transparent for both parties. For example, user reputation score allows people to know one's history in Bitcoin transactions. This information is available (i.e. transparency) to help other users to make decisions while engaging in a transaction with a particular user (Gutscher, 2007). This extends the graphic design characteristics (Wang & Emurian, 2005) by adding transparency element in the app design besides other elements such as colour, layout and photo.

Also highlighted is the importance of content visibility for Bitcoin transactions in app design. This includes the selection of icons commonly used by other wallet apps to enhance the visibility of this function. This is because users are familiar with those icons. This allows them to capture and understand the app contents as well as reflect on the app credibility in initiating users' trust. Hence, information visibility is another graphic design element in the app (Wang & Emurian, 2005).

For structure design, the findings suggest the familiar features of Bitcoin functions such as to send and receive Bitcoins to support the app as the experienced Bitcoin users can easily adapt with the functions in the app. In addition, it is important to design the app by providing users with the flexibility to customise the app based on their preference. This extends the suggestions on the trust elements for structure design (Wang & Emurian, 2005), by adding Bitcoin function familiar features and flexibility for users to customise the app.

Looking at the demand to create an account, it was found that the identity of anonymous wallet account in the app can develop trust among users as their confidential details are not revealed to any parties. This is in contrast to the centralised Bitcoin exchange websites or mobile apps that require identification verification before users can create their wallet (Coinbase, n.d.). Nakamoto (Nakamoto, 2008) designed the Bitcoin Blockchain protocols that permit Bitcoins to be transferred from one owner to another pseudoanonymously using the users' wallet addresses. However, due to issues related to trust while dealing with transactions, users tend to prefer deanonymisation than the central exchanges, as they are governed by legal bodies (Sas & Khairuddin, 2017). Also, the user identity verification processes via exchanges are complicated. Hence, the app design that requests users to create their wallet

anonymously will address this issue, provided that the app supports additional features to protect users from dishonest parties. Thus, the anonymous wallet creation extends the demand elements for the structure design characteristic (Wang & Emurian, 2005).

Moving on to the content design, the app security design enables users to manage their wallet account private key. This is a trusted feature for peer-to-peer app, in contrast to the centralised apps or websites that store user passwords, as well as authentication questions and answers for password retrieval (Seckler et al., 2015). The findings also suggest that the content trustworthiness in peer-to-peer app can be improved by adding contents from the developers such as the app source code that explains the BitXFps back-end architecture. This helps to support the credibility of app development. The trust elements for content design (Wang & Emurian, 2005) is added by adding the wallet backup features as additional security elements as well as documentation from the developer to support the credibility of the app content.

It is also important to create a website for BitXFps that is linked to the app as support, this contributes to the social cue design characteristic. The integration between website and mobile app is to support the app social presence. The concise information in the mobile app is explained in details on the website. Hence, this is essential to develop trust among users. Besides, for decentralised applications, the customer service feature can be driven by the community. The introduction of a new in-app forum to facilitate community engagement helps to support customer service elements under the social cue design characteristic. In turn, this provides a room for social interaction between users, for them to share ideas to improve the app performance.

Furthermore, social media accounts linked to the app are important for personal and social proof. By engaging with app social media pages such as Facebook, users can

know their Facebook mutual friends who are using the Bitcoin app as well. This will help to develop the social trust (Seckler et al., 2015) among users.

The peer-to-peer transaction design cues are derived from the findings in Study 3 (**Chapter 7**) which consist of four elements; transaction transparency, contract validity, mediator decentralisation, and reputation system. Interestingly, the findings highlighted the importance of reversible function in peer-to-peer transaction. In the original Blockchain protocol, Bitcoin transactions are irreversible (Nakamoto, 2008), which leads to dishonest transaction between parties. Findings in Study 3 are extended by introducing the reversible transaction feature as the trust element in peer-to-peer Bitcoin transactions cues. This is done by holding the transaction in the multisignature wallet until the transactions (offline or online) are successfully completed. In the event of dishonesty, transactions can be reversed and not recorded on the ledger. So this justifies the use of irreversible transaction feature. Table 10.1 summarises the six characteristics of trust-inducing features tailored to the BitXFps mobile application interface (Seckler et al., 2015; Wang & Emurian, 2005); Study 3 (Chapter 7); Study 4 (Chapter 8); Study 5 (Chapter 10).

Dimensions	Key Elements	Source
<p><b>Graphic Design</b></p> <p><i>Definition:</i> The mobile application graphical elements that trigger users' first impressions.</p>	<p>Visual Design</p> <ul style="list-style-type: none"> <li>• Appropriate site layout</li> <li>• Moderate layout complexity</li> <li>• Uses of photographs</li> <li>• Uses moderate pastel colour</li> <li>• Apply blue colour in the design layout*</li> <li>• Provides transparent information for all users*</li> <li>• Increase visibility of the information for all users*</li> </ul>	<p>(Karvonen &amp; Parkkinen, 2001; Kim &amp; Moon, 1998; Seckler et al., 2015; Wang &amp; Emurian, 2005) Empirical Findings in Study 5</p>
<p><b>Structure Design</b></p> <p><i>Definition:</i> Users' accessibility to information displayed on the mobile app's interface and how it is organised.</p>	<p>Usability</p> <ul style="list-style-type: none"> <li>• Effectiveness and efficacy with the task flow <i>Flexibility users to customise the app according to their preference*</i></li> <li>• Easy navigation <i>Users' friendly structure for common Bitcoin transactions functions*</i></li> </ul> <p>Broken Links</p> <p>Demand</p> <ul style="list-style-type: none"> <li>• Anonymous wallet account creation*</li> </ul>	<p>(Karvonen &amp; Parkkinen, 2001; Kim &amp; Moon, 1998; Seckler et al., 2015; Wang &amp; Emurian, 2005)  Empirical Findings in Study 4</p>
<p><b>Content Design</b></p> <p><i>Definition:</i> Informational elements that are placed on the mobile app's interface either textual or graphical</p>	<p>Security signs</p> <ul style="list-style-type: none"> <li>• Enable users to manage the private key of their wallet accounts*</li> </ul> <p>Image/brand Expertise Privacy: collection Privacy: secondary use</p> <p>Content</p> <ul style="list-style-type: none"> <li>• Include resource documents related to the development of the app*</li> </ul> <p>Implausible promises Policy</p>	<p>(Belanger et al., 2002; Egger, 2001; Ereemeev, 1999; Hu et al., 2001; Nielsen, 2000; Seckler et al., 2015; Shneiderman &amp; Ben, 2000; Wang &amp; Emurian, 2005)  Empirical Findings in Study 4</p>
<p><b>Social cue Design</b></p> <p><i>Definition:</i> Social cues that are integrated into the mobile application showing the assistance provided by the mobile application to the users.</p>	<p>Customer service Real-world link</p>	<p>(Basso et al., 2001; Riegelsberger et al., 2005; Seckler et al., 2015; Steinbrück et al., 2002; Wang &amp; Emurian, 2005)</p>

<b>Personal and Social Proof</b>  <i>Definition:</i> Social remarks such as comments and rating scores for the app from other users	User's social proof Friend's social proof Prior experience	(Seckler et al., 2015)
<b>Peer-to-peer Transaction Design Cues</b>		
<i>Definition:</i> Trust elements that are embedded in the BitXFps application to support users' decision to enact a transaction without the governance from a centralised authority.		
Elements	Descriptions	Sources
Transparent transactions	The design cues that guarantee the two-way transaction is conducted transparently by both parties.	Empirical Findings in Study 3 and Study 4
Valid contract	The remarks in the design that ensure that the mutual agreement between the two parties is valid for in the Blockchain smart contract	
Decentralised mediator	The sign in the design to show that the transaction between two parties is validated by the crowdsourced mediator	
User's reputation	The indicator to show users' performance in previous transactions.	
Reversible transaction	The sign to show that the identified dishonest transaction is reversible in a provable way	Empirical Findings in Study 5

**Table 10.1: Trust-inducing features for the Bitcoin Peer-to-peer Transaction Mobile Application Interface Design**

### 10.5 Design Implications

The design implications focus on the Blockchain real-time communication to capture the proof of offline transaction for the delivery of goods or fiat money transactions as well as the revised BitXFps app interface to develop better trust.

#### 10.5.1 Blockchain Real-Time Communication Tool

The findings suggest that the role of witness as the decentralised mediator between seller and buyer can be improved by adding an anonymised video call feature to ensure the reliability of the offline transaction proof in terms of fiat money

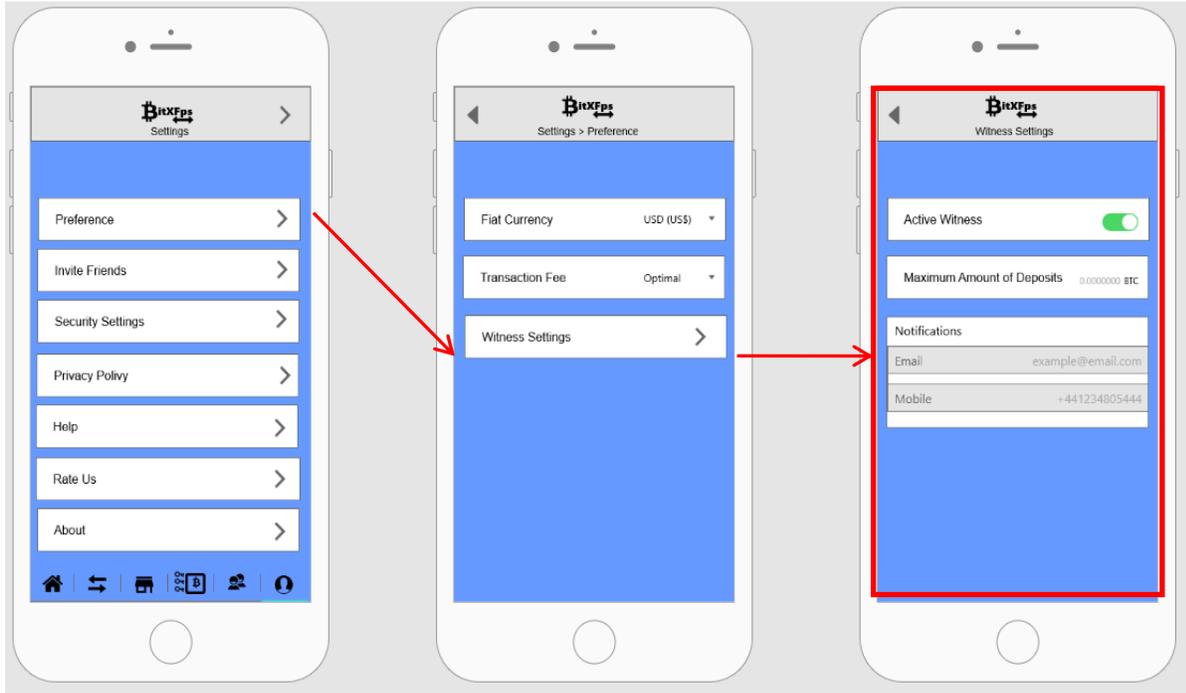
transaction and delivery of goods. The video call feature ensures that the offline transaction of fiat money or goods is transparent between the seller, buyer and witness. Using the standard guideline to monitor the transaction via group video call, the witness is responsible to ensure both parties are satisfied with the transaction. The anonymised video call is recorded and stored as the offline transaction proof for delivery of goods or fiat money transaction. This mechanism is implemented by integrating the BitXFps design with decentralised Blockchain video call feature (Steemit, 2017). This feature can protect the data related to the offline proof for delivery of goods or fiat money transactions by storing it on user device rather than on the centralised server (Lucas, 2018). This will further protect the confidentiality of parties involved in the offline transaction.

#### 10.5.2 Revision of the BitXFps Mobile App Design

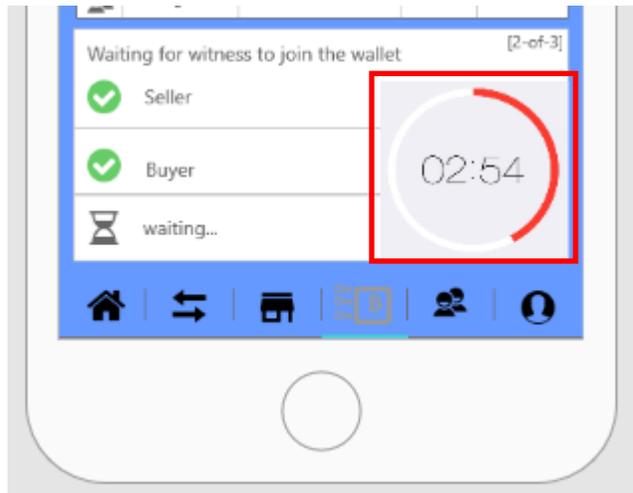
The findings provide some directions in revising the BitXFps design according to the six characteristics of trust-inducing features in the following section.

##### *10.5.2.1 Revision Based on Structure Design*

The additional witness function enables users to select their preference for a witness, including the minimum amount of deposit to guarantee honesty and responsibility in a transaction, the way for them to receive notifications of invitation to be a witness or manage dispute (**Figure 10.7**). In addition, BitXFps design can be improved by adding timer alert to let users know the exact waiting time for the transaction, such as the time for buyer and seller to wait for witnesses to join them (**Figure 10.8**).



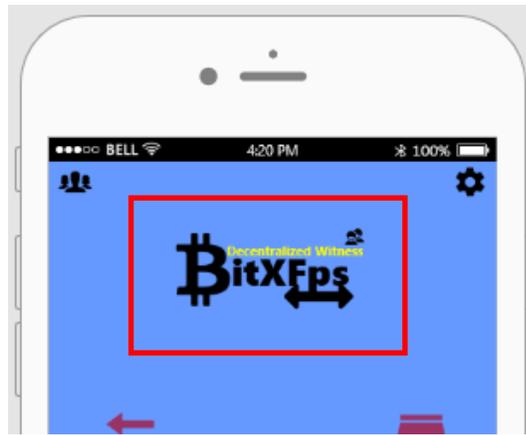
**Figure 10.7: The Witness Interface Design Settings**



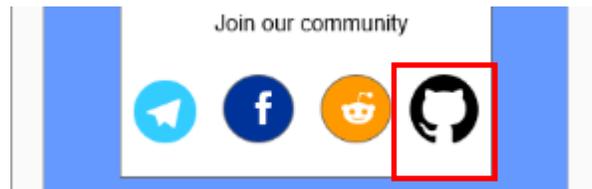
**Figure 10.8: Design for the Timer**

### 10.5.2.2 Revision Based on Content Design

The findings highlighted the limited emphasis on the unique features of the app, which is important for branding. To address this, the app's logo has been revised by adding the “decentralised witness” tagline (**Figure 10.9**). In addition, a new GitHub icon is added at the ‘About’ page to show the link to the BitXFps source code in GitHub (**Figure 10.10**). GitHub is the repository platform where developers store their projects and network with like-minded people (Orsini, 2013).



**Figure 10.9: The Revised Design of the App Logo**



**Figure 10.10: GitHub Icon to Link the Users to the App Source Code**

### 10.5.2.3 Revision Based on Graphic Design

The icons for seller and buyer in the multisignature wallet table page are revised by introducing new colours (purple and yellow) to distinguish the buyers and sellers in transactions (**Figure 10.11**).



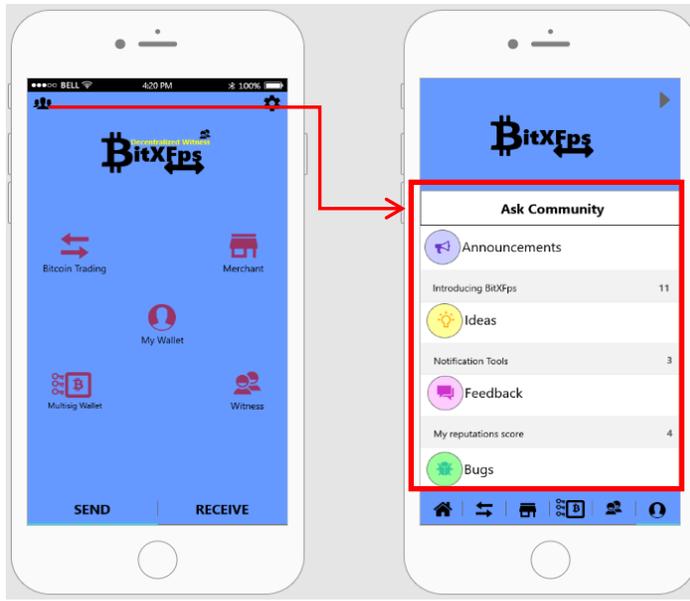
The screenshot shows the BitXFps Multisignature Wallet interface. At the top, it displays the wallet address: 1Lkgt2JG6J3XMCdy7PjWtpHHGF8BHTR and the wallet name: Selling Bitcoin for USD500 - BTC0.0779. Below this is a table of transactions. The 'Wallet Owners' column uses color-coded icons: purple for sellers and yellow for buyers. A red box highlights the first four rows, which are all seller transactions.

Wallet Owners	Transaction Description	Amount (BTC)	Status
 Seller	Transaction fee	+0.0002	Confirmed
 Seller	Bitcoin to sell	+0.0779	Confirmed
 Seller	Token fees	+0.0003	Confirmed
 Seller	Deposit fees	-0.001	Confirmed
 Buyer	Token fees	+0.0003	Confirmed
 Buyer	Deposit fees	-0.001	Confirmed

**Figure 10.11: The Icons for Sellers and Buyers are differentiated with Colours**

### 10.5.2.4 Revision Based on Social Cue Design

A new function was introduced to the BitXFps interface, which is the community forum to support interaction between users (**Figure 10.12**). To increase the app social presence, a website to support BitXFps will be created and the URL website link is also added in the 'About' page (**Figure 10.13**).



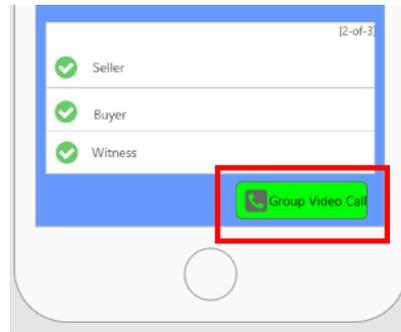
**Figure 10.12: Interface for the In-app Community Support Channel**



**Figure 10.13: The Official BitXFps Website URL**

#### *10.5.2.5 Revision Based on Peer-to-peer Transaction Design Cues*

The group video call button is introduced in the active multisignature page to capture the proof of offline transaction (**Figure 10.14**).



**Figure 10.14: The Interface for the Group Video Call**

## 10.6 Chapter Summary

This chapter presents the evaluation of trust elements via the mobile wallet interface to support peer-to-peer Bitcoin transactions between users for fiat money or goods based on the heuristic guidelines for trust elements in Bitcoin mobile applications (Chapter 9). The findings suggest a theoretical framework for the trust-inducing features in peer-to-peer Bitcoin transactions on BitXFps mobile application. From the evaluation study and findings, the framework was extended from the initial framework of the website trust-inducing features, by adding a new element customised to peer-to-peer Bitcoin transactions, via the interface design. The main characteristics of the framework include graphic design, structure design, content design, social cue design, personal and social proof, and peer-to-peer transaction design cues. There are also five elements under peer-to-peer transaction design cues namely transaction transparency, contract validity, mediator decentralisation, reputation system, and reversible transaction. Besides Bitcoin, the framework can be extended to evaluate trust features in other cryptocurrencies' peer-to-peer transaction and mobile app wallets.

# Chapter 11

## Discussion

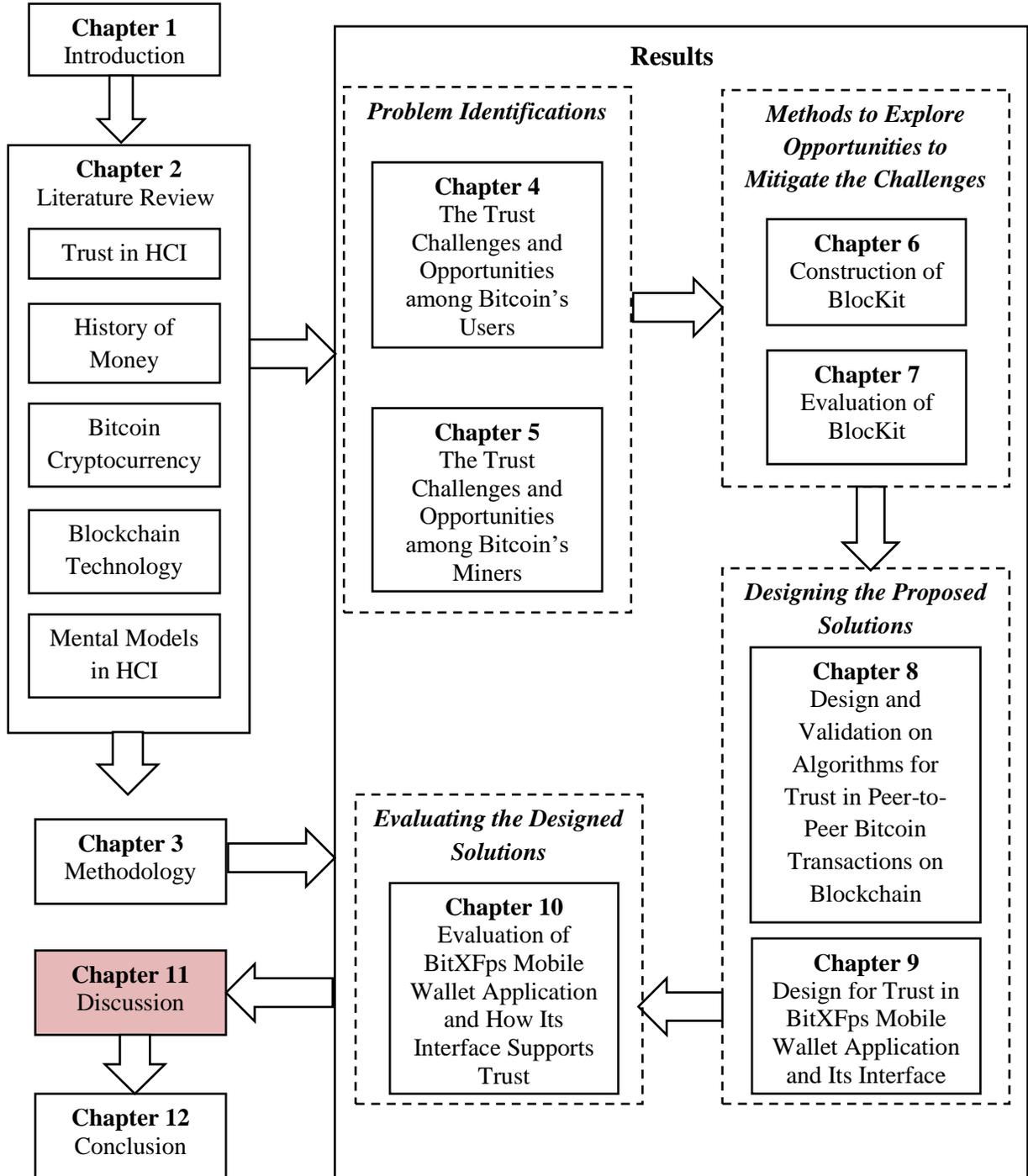
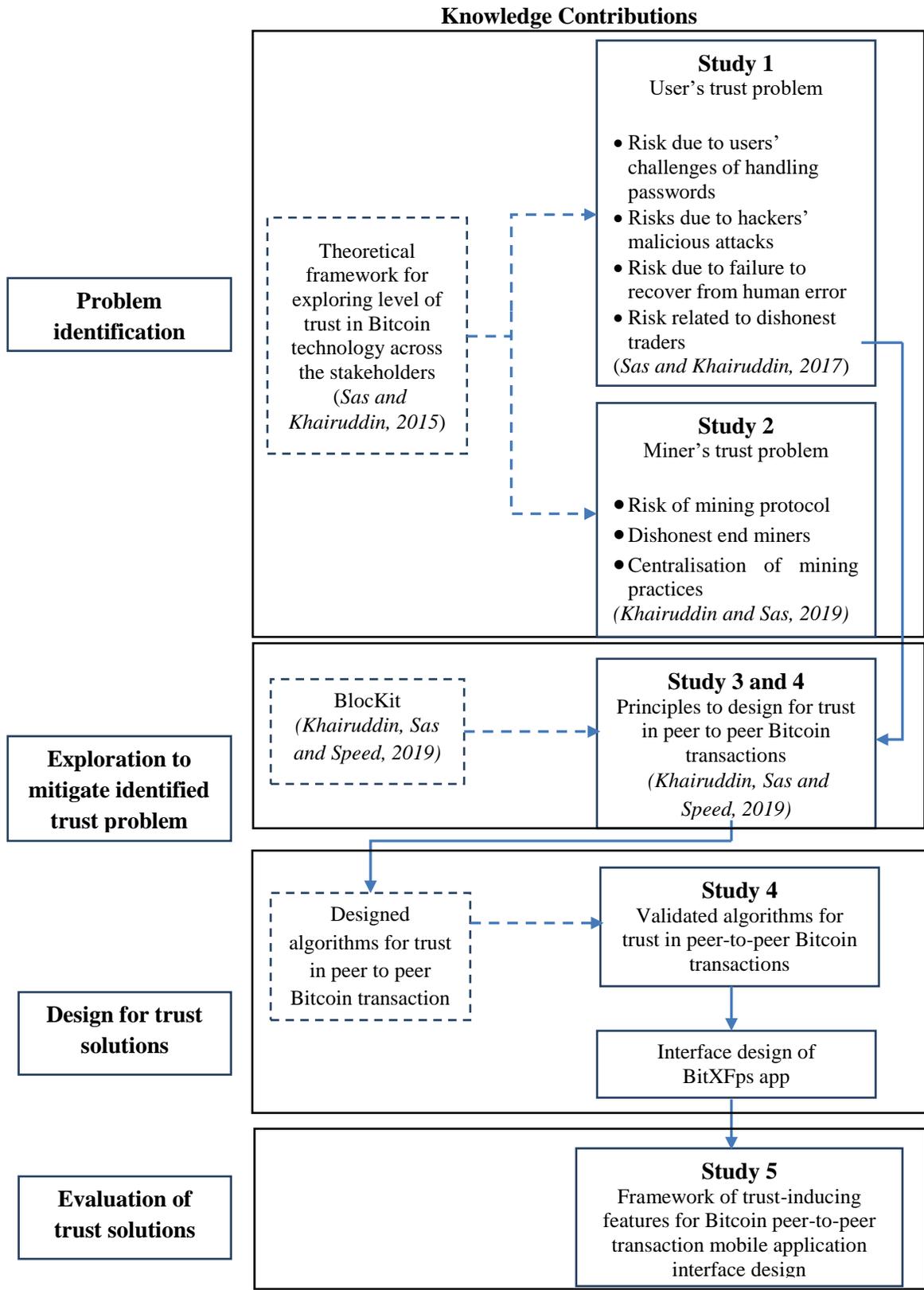


Figure 11.1: Chapter 11 of Thesis Structure

## 11.1 Introduction

This thesis presents five studies with 92 Bitcoin Blockchain's stakeholders to explore trust problems of people engaging with this technology, and ways to mitigate them. These studies were conducted in four different phases, focussing on problem identification; methods to explore the opportunities to mitigate trust problems; design of the proposed solution; and evaluation of the designed solution. Each of these phases consists of different but interrelated studies which aim to address the objectives and research questions of the thesis. This chapter discusses the main findings of the thesis and also revisits the main research questions of the thesis while highlighting the key findings and the novelty of the thesis' contributions. **Figure 11.2** is the diagram represents the connections and the knowledge contributions for each study in this thesis.



**Figure 11.2: Knowledge contributions across the studies in the thesis**

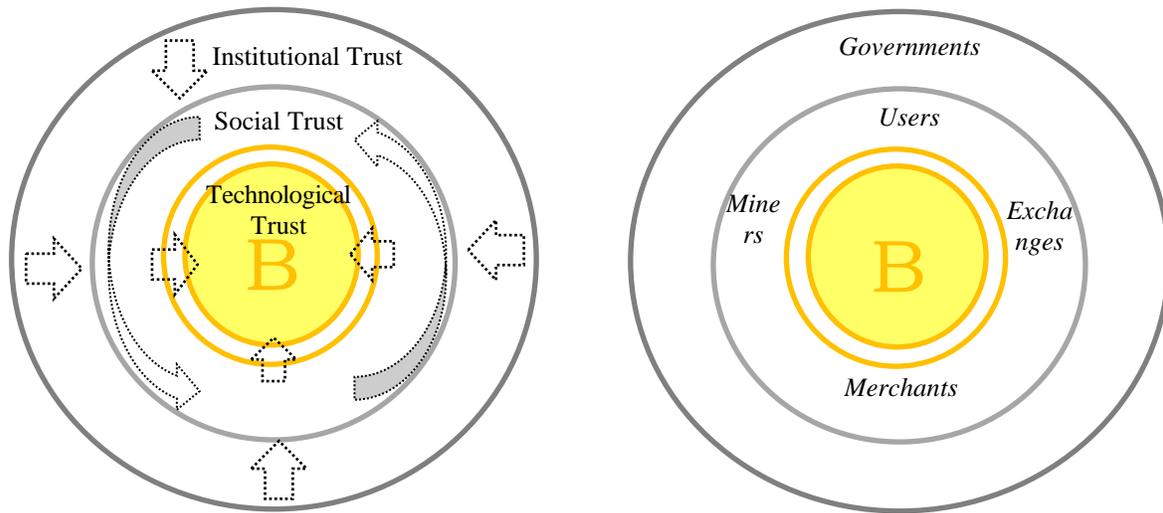
## 11.2 Problem Identifications

To identify the problem, a theoretical framework has been developed to explore people's trust in Bitcoin Blockchain technology, and their associated trust challenges. This theoretical framework is one of the references used to inform our next empirical work with Bitcoin Blockchain's stakeholders, particularly users and miners, as described in the following section.

### 11.2.1 The Design of the Theoretical Framework for the Exploration of People's Trust in Bitcoin Technology

The explorations of trust challenges of people engaging with Bitcoin Blockchain technology started with the revision of trust theories and models in HCI. The multifaceted concept of trust has been explored across a large range of interactive systems, and consistent findings have shown the distinction between technological, social, and institutional trust (Leppanen, 2010; Lippert & Swiercz, 2005; Misiolek et al., 2002) Thus, these three main aspects of trust were used as dimensions of trust in this novel theoretical framework developed through this thesis. The framework was expanded by mapping the relevant literature on Bitcoin Blockchain technology with trust concepts. The framework positioned technological trust as people's experience and trust in engaging with Bitcoin Blockchain technology. The framework also defines social trust as trust among Bitcoin Blockchain's stakeholders (users, merchants, exchanges, and miners). Finally, institutional trust captures the support from the central authorities such as governments towards Bitcoin Blockchain technology (**Figure 11.3**). This theoretical framework was published in the Proceedings of the OZCHI Conference in 2015 (*Sas and Khairuddin, 2015*).

The proposed theoretical framework addresses a gap in understanding people’s trust in Bitcoin Blockchain technology. Within the scope of the thesis, the framework has been used to discuss empirical findings on Bitcoin users’ and miners’ trust while engaging with the Bitcoin Blockchain technology.



**Figure 11.3: Research Framework for Exploring Levels of Trust in Bitcoin Technology (left) and across Stakeholders Group (right) (Sas and Khairuddin, 2015)**

### 11.2.2 The Identified People’s Trust Challenges in Bitcoin Technology

The proposed theoretical framework of trust is later used to discuss the findings from the empirical studies with 20 Bitcoin users, and 20 Bitcoin miners (Study 1, and Study 2). In addition to trust, these findings also report on their practices of engaging with Blockchain technology. Trust challenges, identified by the miners while conducting collaborative mining, and the actions they took to mitigate these trust challenges, were also discussed. The empirical work on miners’ practices has been published in the Proceeding of 2019 CHI Conference on Human Factors in Computing Systems (*Khairuddin and Sas, 2019*).

By reflecting on the theoretical framework for exploring Bitcoin trust, (*Sas and Khairuddin, 2015*), findings from Study 1 and 2 (*Sas and Khairuddin, 2017; Khairuddin and Sas, 2019*) report that users' technological trust is strong. Their trust relies on Blockchain's characteristics such as decentralised ledger, embedded expertise, low cost, and ease of use. Institutional trust indicates that users enjoyed the unregulated features of the Blockchain. In other words, they prefer to transact Bitcoins freely among themselves, without any governance from central authorities. However, findings also show that users' main trust challenges surface in the context of social trust. Users face risks related to dishonest traders, particularly for those Bitcoin transactions occurring offline when Bitcoins are exchanged for fiat money or products. Blockchain offers a record of transparent Bitcoin transactions on its public ledger (Nakamoto, 2008). However, offline transactions with banks or merchants are not captured on the ledger. In order to mitigate this problem, some Bitcoin users take action by trading with authorised exchanges. Some users prefer dealing through peer-to-peer transactions with a socially authorised trader, reputable individual trader, or de-anonymised individual trader. However, the latter strategy was reported as the weakest. This is due to the risk to trade with someone that is completely unidentified by any of the members in the Bitcoin online groups; also, their reputation in Bitcoin transactions is unknown. This empirical study with Bitcoin users has been published in the Proceedings of the 2016 CHI Conference Extended Abstracts, and 2017 CHI Conference on Human Factors in Computing Systems (*Khairuddin et al., 2016; Sas and Khairuddin, 2017*).

To further explore the opportunities to mitigate trust challenges in Blockchain, we also looked at miners' practices in Blockchain, more specifically to their mining approaches, and the main categories of miners (*Khairuddin and Sas, 2019*). However, mining is just a

piece of the complex Blockchain infrastructure that is arguably challenging to understand.

### 11.3 Methods for Exploring Opportunities to Mitigate Trust challenges

Users' trust challenges in peer-to-peer Bitcoin transactions are due to social factors rather than technological ones. In order to mitigate these challenges, it is crucial to better understand Blockchain's infrastructure. This section reports on the methods for materialising the main concepts of Blockchain in a physical way, and how these can be used to explore the opportunities to address the key Bitcoin users' trust challenges.

#### 11.3.1 Materialising the Blockchain Infrastructure

The decentralised Blockchain's infrastructure consists of distributed nodes geographically located world-wide. This is in contrast to the structure of the conventional centralised financial systems. Hence, the inner workings of the Blockchain's infrastructure are challenging to understand. This is the motivation for exploring the materialisation of Blockchain infrastructure.

By advancing the theories of embodied cognition (Hampe & Grady, 2005) and material centred-design (Wiberg & Mikael, 2014), BloKit was constructed to represent the initially identified 12 main entities of Blockchain: Bitcoin, wallet, wallet password, public key, private key, block, consensus rules, miner's computational powers, proof of work, time stamp, and Blockchain ledger. These Blockchain's entities were represented in physical forms through materials such as clays, plastic containers or sticky notes.

To evaluate BloKit, a workshop was conducted with 15 Blockchain experienced users. The outcomes of the workshop with the experienced users support the value of

BlocKit to communicate, and design for trust in Blockchain. They also suggested few revisions for the representations of the Blockchain main entities, and for creating a new object representing the memory pool. The construction and validation of BlocKit was published in the Proceeding of Designing Interactive Systems, DIS 2019 (*Khairuddin, Sas, and Speed 2019*).

Various modalities have been explored to communicate the principles of Blockchain technology, and to support users' understanding and learning about it, primarily through visual representations in the form of infographics, (Cartwright, 2018) or videos (The Guardian, 2014). In contrast, the value of physical objects for communicating about Blockchain has been limitedly explored, with some preliminary work suggesting the value of Lego blocks for Blockchain's experts and novices to communicate and describe its entities (Maxwell et al., 2015). Hence, it is argued that the physical three-dimensional artefacts offered by BlocKit provide a new methodological contribution for exploring people's learning, understanding, communicating about, and designing for Blockchain.

### 11.3.2 Principles to Design for User's Trust in Bitcoin Transactions

BlocKit was also explored with experienced users to understand its value for designing for trust in the peer-to-peer Bitcoins transactions. The outcome of Study 3 suggested four important principles for designing for trust which consist of transparent transactions, a valid contract between seller and buyer, decentralised mediator or witness, and trust reputation system (*Khairuddin, Sas, and Speed 2019*). Findings also support several requirements for designing those principles on Blockchain by utilising the Ethereum smart contract, and multisignature wallet. Thus, the proposed principles

and requirements were applied to design the solutions to mitigate the challenges of users' trust in Blockchain.

#### 11.4 Design of Proposed Solutions

From the physical design of BlocKit, we progressed to the design of algorithms for user trust. Then, the validated algorithms were used to design the user interface for BitXFps, a Bitcoin mobile application. This section describes the design of this Bitcoin wallet application.

##### 11.4.1 The Design Algorithms with the Principles to Design for User's Trust in Bitcoin Transactions

The experienced users outlined four important principles for the design of trust algorithms in Blockchain: transparent transactions, a valid contract between seller and buyer, decentralised mediator or witness, and trust reputation system (*Khairuddin, Sas, and Speed 2019*). They also suggested using Ethereum smart contract, and multisignature wallet to design a tool embedding those principles. Ethereum's smart contract was built to support Ether cryptocurrency transactions. However, the identified trust challenges in this thesis are related to peer-to-peer Bitcoins transactions and Bitcoin Blockchain technology did not support the Ethereum smart contract. Thus, another tool to assist the Ethereum smart contract to verify Bitcoin transactions namely, BTC Relay (BTC Relay, 2016) was applied to the algorithms' design.

The algorithms have five main steps. The first step describes the preliminary process of a transaction, such as creating the wallet account and searching for potential buyers or sellers. The second step is about creating the contract agreements between

seller and buyers which includes penalties for dishonest traders. This agreement is recorded in the smart contract. This, in turns, ensure the validity of the contract as listed in one of the principles. The third step describes the transactions in the multisignature wallet, including sending Bitcoins and randomly inviting a crowdsourced witness as the mediator of the transactions. The multisignature wallet provides transparency for both parties involved in transactions, as seller and buyer may observe the movements of the Bitcoin and have the authority to control it. The crowdsource witness is a decentralised mediator that helps to facilitate the dispute associated with a transaction. Fourthly is to proceed with an offline transaction with either bank or shipping company. Finally, the last step describes sending the trust tokens to the seller and buyer and witness token to the witness which reflects the principle of building a reputation system on Blockchain. These algorithms were validated by 10 Blockchain's experienced users. The outcome of the validation provides suggestions on minor revisions of the algorithms, mostly regarding witnesses.

The design for trust solution, extending smart contracts and multisignature, have started to be used on Ethereum Blockchain (Horda, 2018), for instance through decentralised exchanges such as WeiDEX (WeiDex, n.d.). However, the design of a fully decentralised exchange for Bitcoins transactions has been limited (Cuen, 2018), as well as the utilisation of the bridge tool (BTC Relay, 2016), and experienced users' suggestions for the four design principles for trust. Hence, it is argued that these algorithms for designing for trust in Bitcoin Blockchain are novel.

#### 11.4.2 The Design of User Interface for Mobile Bitcoin Application with the Elements for User's Trust in Bitcoin Transactions

The proposed algorithms for supporting users' trust in Bitcoin transactions were applied to the design of a user interface for a Bitcoin wallet mobile application which we called BitXFps. A guideline for the trust-inducing elements was proposed based on the prevalent framework of trust inducing features of websites interface, (Seckler et al., 2015; Wang & Emurian, 2005) for evaluating trust in interface design for websites and mobile applications. In addition, four design principles for trust (transparent transactions, a valid contract between seller and buyer, decentralised mediator or witness and trust reputation system) suggested by the Blockchain experienced users in Study 3 were also included in the design for trust guideline.

The new proposed guideline was then used as the main reference for designing the BitXFps user interface.

#### 11.5 Evaluation of BitXFps's User Interface Design

The final part of the thesis is the evaluation of BitXFps interface, the Bitcoin wallet application, with 15 Bitcoin experienced users. The evaluation's aim was to identify the elements in the user interface that could support users' trust in conducting peer-to-peer Bitcoin transactions.

##### 11.5.1 The Evaluated Design of User Interface for Mobile Bitcoin Application with the Elements for User's Trust in Bitcoin Transactions

An expert review method was applied to evaluate BitXFps' interface with 15 Bitcoin experienced users. The evaluation was based on the proposed guideline for

trust-inducing features (Seckler et al., 2015; Wang & Emurian, 2005) The outcomes of the evaluation method indicate the elements of interface design which support trust. They consist of suggestions to improve the effectiveness of witness functions by integrating the mobile app with group video call between the seller, buyer and witness while enacting offline transactions (sending money through banks or product to the shipping company). Other suggestions included a standard guideline for the witness to manage the transactions dispute between buyer and seller. In addition, a new element for trust was discovered, namely the reversible transaction. Participants realised the importance of reversible actions to mitigate the challenge of dishonest transactions.

The framework of users' trust-inducing features was initially proposed by Wang and Emurian (Wang & Emurian, 2005). In their initial framework, there are only four main characteristics of trust: graphic design, structure design, content design, and social cue design. This framework was used to evaluate various types of websites and mobile apps including a study by Secklar et al. (Seckler et al., 2015). In their study, they adopted the framework to evaluate various websites including financial and e-commerce websites. The outcome of the Secklar et al. (Seckler et al., 2015) study extended the initial framework with another characteristic, namely personal and social proof. However, the validation of the framework with any website or mobile application related to cryptocurrency has been limited. Hence, it is argued that the five principles for designing for trust (transparent transactions, a valid contract between seller and buyer, decentralised mediator or witness, trust reputation system, and reversible transaction) contribute to novel dimension to the framework. This new extended framework can be used to evaluate trust in other user interfaces, specifically for Bitcoin and other cryptocurrencies wallets on websites or mobile applications.

## 11.6 Reflection on the Thesis Findings

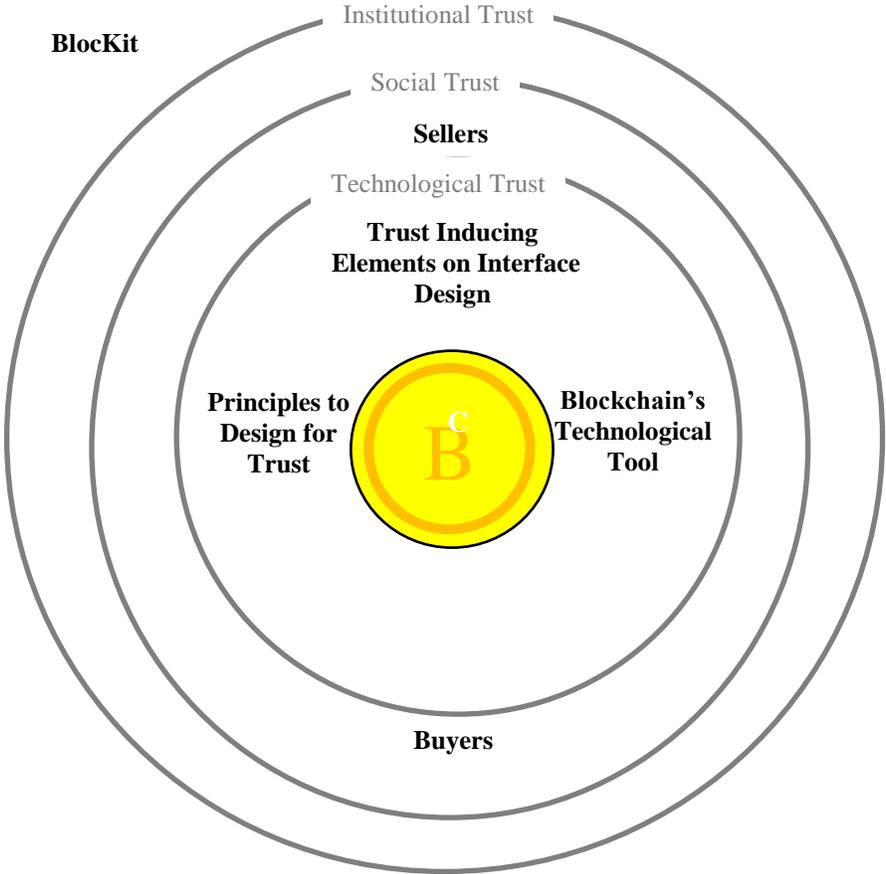
The main focus of this thesis is the Blockchain users' trust challenges for engaging in peer-to-peer Bitcoin transactions, particularly transactions involving Bitcoins and fiat money and/or Bitcoins and products. The theoretical framework to explore trust in Bitcoin Blockchain technology (*Sas and Khairuddin, 2015*) was applied to integrate the findings of the thesis (

Figure 11.4).

Social trust is the main trust challenge that we aimed to be addressed throughout the thesis. It consists of sellers and buyers enacting peer to peer Bitcoin transactions. Since the BitXFps app was designed to be fully decentralised, institutional trust is not applicable to the framework. However, technological trust was strengthened to mitigate social trust challenges.

The BiXFps app design for user trust was proposed by advanced Blockchain's technological tools, such as Ethereum smart contract, multisignature wallet and BTC Relay. These three unique technologies were successfully integrated to inform the design and development of BiXFps app. Positioned under the same umbrella of technological trust, those principles to design for trusts such as transparent transactions, a valid contract between seller and buyer, decentralised mediator or witness, trust reputation system and reversible transaction are the elements to support users' trust towards peer-to-peer Bitcoin transactions. In addition, elements in user trust-inducing features of BitXFps such as graphic

design, structure design, content design, social design cue, personal and social proof and peer-to-peer transaction design cues were also harnessed to support technological trust.



**Figure 11.4: Empirical Framework to Design in Blockchain for User's Trust in Peer-to-Peer Bitcoin Transactions**

BlocKit offers a physical form of Blockchain's infrastructure which may be used to explore the design of other solutions pertaining to Blockchain. Our framework to mitigate trust challenges could also benefit the exploration and design for other cryptocurrencies. In addition, the framework could also be extended to be applied to other decentralised peer-to-

peer systems that are exposed to the risk of dishonest transaction partners, such as the risk of cheating among multi-player online-games (Neumann, Prigent, Varvello, & Suh, 2007).

### 11.7 Reflection on Thesis' Research Questions

This thesis explored five research questions which are further unpacked in this section.

- 1) *Why do people such as users and miners engage in Bitcoin transactions on Blockchain technology? What are the challenges they faced, and the specific trust issues?*

The literature exploring the motivations, and trust challenges of Bitcoin Blockchain's stakeholders such as users and miners have been limited. Thus, by reflecting the relevant HCI literature on trust, a theoretical framework was developed to explore trust in Bitcoin Blockchain technology (Sas and Khairuddin, 2015). This model has been further applied to explore users' and miner's trust while engaging with Bitcoin transactions on Blockchain.

In Study 1, interviews with 20 Bitcoin users were conducted with the aim to explore their motivations and trust challenges. Findings reported that their motivations were underpinned by Bitcoin's predicted role in monetary revolutions, user empowerment from the characteristics of Blockchain such as decentralised, and unregulated, and perceived real value of Bitcoin currency (Khairuddin et al., 2016; Sas and Khairuddin, 2017). Findings also indicate trust challenges related to Bitcoin users while engaging in a transaction such as the risk due to users' challenges of handling passwords, risks due to hackers' malicious attacks, and risks related to dishonest partner of transaction (Sas and Khairuddin, 2017).

With a similar aim to Study 1, interviews with 20 Bitcoin miners were conducted in Study 2. The outcomes of the Study 2 report that miners' motivation are impacted by the Blockchain's characteristics such as decentralised, and transparent mining pool,

unregulated, and ease of use. In addition, the mining rewards, experimenting with mining technology, and lack of regulation regarding taxation of mining fees also contributed to miners' motivations. Findings indicate that miners' trust challenges are related to the risks of mining protocol such as increased time for acquiring block confirmation, limited block size, and limited number of full nodes. In addition, dishonest mining pool's and data centre's administrators, lack of audit for the distributions of rewards in a pool, invisibility of data centres, and mining program scams also represent trust challenges identified by miners (Khairuddin and Sas, 2019).

The new findings described in Study 1 and Study 2 offer further explorations for the mitigation of the trust challenges, as well as for expanding the research into other types of Bitcoin stakeholders such as exchanges and merchants.

*2) What are the elements of BlocKit – an innovative kit for materialising Blockchain - that could support people's understanding of Blockchain? What are the values of this approach for people to engage with Blockchain?*

Different modalities have been explored to communicate the principles of Blockchain technology, and support their understanding and learning, primarily through visual representations in the form of infographics (Cartwright, 2018) or videos (The Guardian, 2014). In contrast, the value of physical objects for communicating about Blockchain has been limitedly explored, with some preliminary work suggesting the value of Lego blocks for Blockchain's experienced and novice users to communicate and describe its entities (Maxwell et al., 2015).

By advancing the theories of embodied cognition (Hampe & Grady, 2005) and material centred-design (Wiberg & Mikael, 2014), BlocKit was constructed to represent the initially

identified 12 main entities of Blockchain, such as Bitcoin, wallet, wallet password, public key, private key, block, consensus rules, miner's computational powers, proof-of-work, time stamp, and Blockchain ledger. BlocKit has been evaluated in a workshop with 15 Blockchain's experienced users (Study 3). The outcomes of the workshop argued that BlocKit's physical three-dimensional artefacts provide a new methodological contribution for exploring, learning, understanding, communicating, and designing for Blockchain (Khairuddin, Sas and Speed, 2019).

3) *What are the principles to design for trust in peer-to-peer Bitcoins transaction?*

*How should the design of Blockchain be supported?*

In order to mitigate trust challenges of peer to peer Bitcoin transactions, the design workshop with 15 Blockchain's experienced users (Study 3) interacting with BlocKit suggested four principles to design for trust: transparent transactions, a valid contract between seller and buyer, decentralised mediator or witness, and trust reputation system. In order to design algorithms for these suggested principles for Blockchain, the experienced users suggested to use Ethereum Blockchain's supporting tools such as Ethereum smart contract and multisignature wallet. However, Ethereum Blockchain is only applicable to Ether cryptocurrency. Thus, BTC Relay was suggested to be included in the design of the algorithms to facilitate the verification of Bitcoin transactions on Ethereum smart contract (Khairuddin, Sas and Speed, 2019). The complete design of trust algorithms was validated by 10 Blockchain's experienced users (Study 4).

The solution for designing for trust in Blockchain, extending smart contracts and multisignature have started to be used on Ethereum Blockchain (Horda, 2018); for instance, by decentralised exchanges such as WeiDex (WeiDex, n.d.). However, the design of a fully

decentralised exchange for Bitcoin transactions has been limited (Cuen, 2018) as well as the utilisation of the bridge tool (BTC Relay, 2016), and experienced users' suggestions for the four design principles for trust. Hence, we argue that these algorithms for designing for trust in Bitcoin Blockchain are novel.

*4) What are the approaches to design new tools, such as wallet mobile apps, for users' trust? How to evaluate the design of such tools?*

The BitXFps Bitcoin wallet mobile app is a tool designed based on the proposed algorithms for users' trust in peer-to-peer Bitcoin transactions. In order to design the user interface of BitXFps app, a design guideline for the trust-inducing elements was proposed based on a prevalent framework (Seckler et al., 2015; Wang & Emurian, 2005) for evaluating trust in interface design for websites and mobile applications. In addition, the four design principles for trust (transparent transactions, a valid contract between seller and buyer, decentralised mediator or witness and trust reputation system) suggested by the Blockchain's experienced users were also applied. This proposed guideline was adopted to design the Bitcoin app (BitXFps) as well as the guidance for the experienced Bitcoin users to evaluate the trust elements in the app's interface.

Although this guideline was built based on Wang and Emurian's (Wang & Emurian, 2005) and Secklar et al.'s (Seckler et al., 2015) framework, the evaluations of the framework in the context of cryptocurrency mobile applications were limited. Hence, it is argued that the design guideline for evaluating users' trust in the interface of Bitcoin wallet mobile application provides novel guidelines for designing and evaluating Bitcoin wallet mobile app.

5) *Which are the elements in the design of BitXFps support people's trust in Bitcoin transactions?*

The mock up prototype of BitXFps app was evaluated by 15 Bitcoin users (Study 5), with the aim to identify elements in the user interface that support the trust in peer-to-peer transactions. The expert review method was applied to evaluate BitXFps design interface with 15 Bitcoin users. The evaluations were based on the proposed trust-inducing features for designing Bitcoin wallet mobile application (Seckler et al., 2015; Wang & Emurian, 2005) The outcomes of the evaluations indicate the elements of interface design supporting trust. They consist of suggestions to improve the effectiveness of witness functions by integrating the app with group video call between seller, buyer, and witness while enacting the offline transaction (sending money through banks or product through shipping companies). Other suggestions include the standard guideline for the witness to manage the transaction's dispute between buyer and seller. In addition, a new element supporting trust was discovered, namely facilitating reversible transactions. Participants realised the importance of reversible transactions required in the case of dishonest transaction's partners, by leveraging the role of the witness.

The framework of users' trust-inducing features was initially proposed by Wang and Emurian (Wang & Emurian, 2005). In their framework, there are only four main characteristics of trust: graphic design, structure design, content design, and social cue design. This framework was used to evaluate various types of websites and mobile apps including Secklar et al. (Seckler et al., 2015). In their study, they adopted a framework to evaluate various websites such as financial and e-commerce websites. The outcome of Secklar et al.'s (Seckler et al., 2015) study extended the initial framework with other characteristics, namely personal and social proof. However, the validation of this framework

with any website or mobile application related to cryptocurrency has been limited. Hence, it is argued that the five principles to design for trust (transparent transactions, a valid contract between seller and buyer, decentralised mediator or witness, trust reputation system, and reversible transaction) could contribute to a further revised framework. This new extended framework can be used to evaluate trust in other user interfaces, specifically for Bitcoin and other cryptocurrencies wallets developed for both websites and mobile applications.

### 11.8 Chapter Summary

This chapter presents the overall discussions of the thesis. It shows the interrelation of findings from all six studies. It begins to discuss the problem identifications, method to explore the opportunities to design trust solutions, proposed solution, design and evaluation of these solutions. The main identified problem is users' trust challenges related to dishonest traders in peer-to-peer Bitcoin transactions. The novel contribution of the thesis is BlocKit, a proposed method to design for trust in Bitcoin transactions, and the framework of trust inducing features for peer-to-peer Bitcoin transactions. Finally, the novel findings of this thesis contribute to the empirical framework of designing for the user's trust in peer-to-peer Bitcoin transactions. The research questions were also revisited to unpack the main contributions of the thesis.

# Chapter 12

## Conclusion

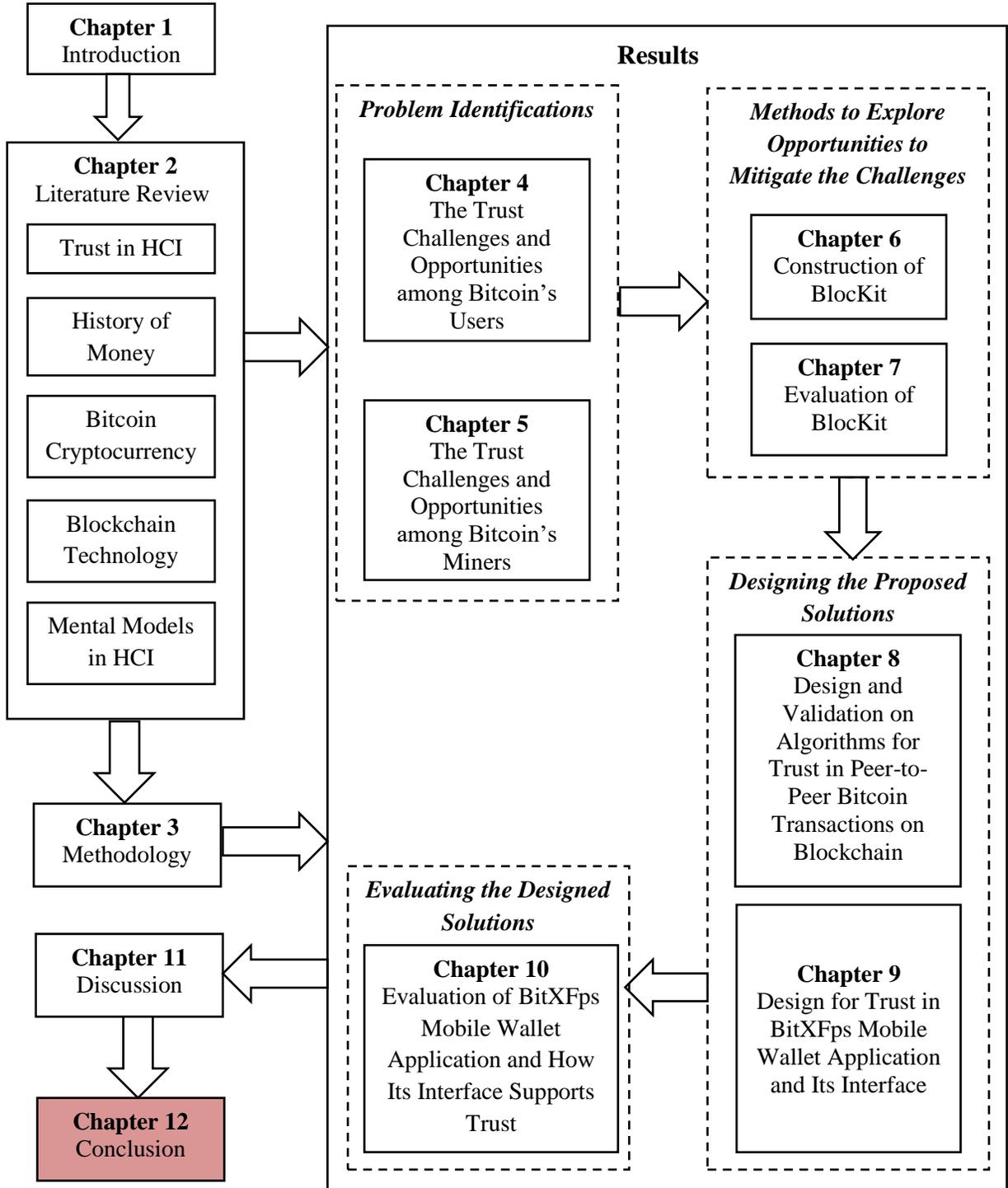


Figure 12.1: Chapter 12 of Thesis Structure

## 12.1 Introduction

This is the final chapter of the thesis, which highlights the limitations of this PhD work as well as the future works that could be further explored from the outcome of this thesis. Finally, in the last section of this chapter is described in the overall conclusion of this thesis.

## 12.2 Work Limitation

The following are the limitations for the research.

### 12.2.1 Time Constraints in Enacting Peer-to Peer Bitcoin-Transactions

The aim of the design of BitXFps was to create a decentralised platform on Blockchain technology to mitigate the issue of dishonest traders in peer-to-peer Bitcoin transactions. In return, BitXFps app prototype integrates technologies such as Ethereum smart contract, multisignature wallet, and BTC Relay as well as the decentralised mediator to witness the transactions. Although the design of the app fulfilled the aim of the research, the time consumed for the users to complete their transactions would be longer than other methods such as transaction with the centralised exchange company. This is due to the waiting time for the decentralised mediator to accept the invitation to join the transactions. Other than that, the multisignature mechanism could also contribute to time constraints.

### 12.2.2 Limited integration of BitXFps on Bitcoin Blockchain

Another limitation is that the developed interface is not actually integrated in Blockchain platform. It is merely illustrates a novel design solution for supporting trust, while its integration in Blockchain was beyond the aim of this work. Indeed, the latter

would not only require advanced technical competency, but also privileged access rights to modify Blockchain's code, such as the one available to core developers.

### 12.3 Future Work

This research can be further explored in three different studies, which are as follows:

#### 12.3.1 Exploring Motivations and Trust among Bitcoins Merchants and Exchanges

In this thesis the exploration of the motivations and trust challenges in engaging with Bitcoin Blockchain technology among the Bitcoins stakeholders are limited to users and miners. Advances the theoretical framework of exploring trust in Bitcoin technology (*Sas and Khairuddin, 2015*), the exploration can be further expanded with the other types of Bitcoin stakeholders, such as merchants and exchanges. This in turns will give a solid understanding of motivations and trust challenges across all types of Bitcoin stakeholders.

#### 12.3.2 Design in Blockchain with BlocKit

BlocKit is a physical kit that represents 12 objects of Blockchain main entities such as block, wallet, and memory pool. In this thesis, the design work on Blockchain is limited on the design for trust in peer-to-peer Bitcoins transactions. As for future research, BlocKit could be used to explore for design in other fields such as medical or business management on Blockchain. The 12 initial objects of BlocKit could also be expanded to cater particular design work in Blockchain.

### 12.3.3 Implementation of BitXFps Bitcoin Mobile Wallet

This thesis presents the validated and evaluated design for trust of the algorithm and user interface of BitXFps Bitcoin mobile wallet. The aim of the design work of this Bitcoin wallet app is to mitigate the trust challenges in peer-to-peer Bitcoins transactions. However, there is no development of BitXFps wallet as well as the evaluation on a working prototype in this PhD thesis. Hence, advance the designed algorithms and user interfaces, the research could be further expanded for the development and implementation work of BitXFps app.

### 12.4 Thesis Conclusion

This thesis has explored the motivations, practices and trust challenges of 20 Bitcoin users and 20 miners in engaging with Bitcoin Blockchain technology, as well as addressed the trust challenges for users in enacting peer-to-peer Bitcoin transactions. In respect to address the trust challenges, a novel method of using physical objects, namely BlockKit has been developed to explore the design in Blockchain. BlockKit has been evaluated by 15 Bitcoin Blockchain experienced users who indicate the kit as a medium to communicate for design, learning and understanding on Blockchain.

By using BlockKit, the study with 15 Bitcoin Blockchain experienced users had suggested novel principles to design for trust in peer-to-peer Bitcoin transactions, which are valid contract, transparent transactions, decentralised mediator, and user reputation system. These principles were adopted to design a Bitcoin wallet app, named BitXFps. The implementations of this wallet app could be supported with the Ethereum Blockchain's tools which are a smart contract, multisignature wallet and BTC Relay. Based on the suggested principles and supporting tools, two sets of algorithms for Bitcoin wallet app which are the

algorithm for transactions between Bitcoins with fiat money also Bitcoins with goods. These algorithms were validated by 10 Bitcoin Blockchain experienced users. The validated algorithms were used together with a set of newly identified heuristics for trust evaluation to design the user interface of Bitcoin wallet application namely, BitXFps. Finally, a mock up prototype of BitXFps app was developed to evaluate the users' trust in its interface with 12 Bitcoin experienced users in conducting peer-to-peer Bitcoins transactions.

The thesis has focused significantly on multiple layers of design works for trust such as in the physical kit, algorithms and user interfaces. On core message of this thesis is that the scope of the design work for trust can definitely be extended to the implementation works of the Bitcoin wallet app.

# References

- Abramowitz, M. (2014). Peer-to-peer law built on bitcoin. Retrieved April 5, 2019, from [https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2365&context=faculty\\_publications](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2365&context=faculty_publications)
- Acheson, N. (2007). How bitcoin mining works. Retrieved April 5, 2019, from <https://www.coindesk.com/information/how-Bitcoin-mining-works>
- Advocaten, P. (2017). The use of video recordings as evidence. Retrieved April 7, 2019, from <https://www.lexology.com/library/detail.aspx?g=00f5ffb3-a15a-4843-803d-621cf69b59be>
- Agrawal, H. (2018). How to instantly convert bitcoins into ethereum (or any other Altcoins). Retrieved April 1, 2019, from <https://coinsutra.com/how-to-convert-Bitcoin-into-ethereum-or-altcoins/>
- Alberts, W. A., Van D. Ge., & Thea M. (2011). Color matters: color as trustworthiness cue in web sites. *Technical Communication*, 58(2), 149-160.
- Alexander, J., Lucero, A., & Subramanian, S. (2012). Tilt displays. In *Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services - MobileHCI '12* (p. 161). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2371574.2371600>
- Allen and Overy. (2015). Virtual currencies. Retrieved April 7, 2019, from [www.allenoverly.com](http://www.allenoverly.com)
- Antonopoulos, A. M. (2010). *Mastering Bitcoin Mastering Bitcoin Editors: Indexer: FIXME FIXME Cover Designer*. O'reilly. Retrieved from <http://safaribooksonline.com>
- Antwerpen, H. V. (1990). *Electronic Cash*. Centrum Wiskunde & Informatica, Netherlands.
- Bakare, S. (2015). Varying impacts of electronic banking on the banking industry. *The Journal of Internet Banking and Commerce*, 20(111). Retrieved from <http://www.icommercecentral.com/open-access/varying-impacts-of-electronic-banking-on-the-banking-industry.php?aid=59264>
- Bank of Canada. (2016). Money and monetary policy in canada. Retrieved April 1, 2019 from [www.cfee.org](http://www.cfee.org)
- Basso, A., Goldberg, D., Greenspan, S., & Weimer, D. (2001). First impressions. In *Proceedings of the 3rd ACM conference on Electronic Commerce - EC '01* (pp. 137–143). New York, New York, USA: ACM Press. <https://doi.org/10.1145/501158.501173>
- BCE. (2016). Introducing the blockchain embassy of asia. Retrieved April 7, 2019, from <https://www.bce.asia/>
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3–4), 245–270. Retrieved from [www.elsevier.com/locate/jsis](http://www.elsevier.com/locate/jsis)
- Beldad, A., Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A

- literature review on the antecedents of online trust. *Computers in Human Behavior*, 26(5), 857–869. <https://doi.org/10.1016/J.CHB.2010.03.013>
- Benyon, D. (2013). *Designing Interactive Systems: A Comprehensive Guide to HCI, UX and interaction design*. Pearson Education
- Beyer, H., & Holtzblatt, K. (1998). *Contextual design : defining customer-centered systems*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA
- Biegel, O. (2018). Is bitcoin mining illegal. Retrieved April 7, 2019, from <https://99Bitcoins.com/is-Bitcoin-mining-illegal/>
- Bishop, D., & Durrell. (2009). Visualising and physicalising the intangible product. In *Proceedings of the 3rd International Conference on Tangible and Embedded Interaction - TEI '09* (p. 1). New York, New York, USA: ACM Press. <https://doi.org/10.1145/1517664.1517667>
- Bitcoin Wiki. (n.d.). Storing bitcoins. Retrieved April 1, 2019, from [https://en.Bitcoin.it/wiki/Storing\\_Bitcoins](https://en.Bitcoin.it/wiki/Storing_Bitcoins)
- Bitcoin.org. (2019). Bitcoin mining difficulty. Retrieved from <https://data.Bitcoin.org/Bitcoin/difficulty/5y?t=1>
- Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized trust management. *Proceeding of Symposium on Security and Privacy Oakland California*.
- Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere - a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 772–777). IEEE. <https://doi.org/10.23919/INM.2017.7987376>
- Bongers, B. (2002). Interactivating spaces. In *4th Annual Symposium on Systems Research in the Arts: Music, Environmental Design and The Choreography of Space*. Germany.
- Boon, S., & Holmes, J. (1991). The Dynamics of interpersonal trust: resolving uncertainty in the face of risk. In R. Hinde & J. Gorebel (Eds.), *Cooperation and Prosocial Behaviour*, (pp. 190–211). Cambridge University Press.
- Bordo, M. (1981). The classical gold standard some lessons for today. *Federal Reserve Bank of St. Louis Review*, May 1981, pp. 2-17.
- Borgman, C. L. (1999). The user's mental model of an information retrieval system: an experiment on a prototype online catalog. *International Journal of Human-Computer Studies*, 51(2), 435–452. <https://doi.org/10.1006/IJHC.1985.0318>
- Boyatzis, R. E. (1998). *Transforming Qualitative Information : Thematic Analysis and Code Development*. Sage Publications.
- Boyce, C., & Neale, P. (2006). Monitoring and evaluation-2 conducting in-depth interviews: a guide for designing and conducting in-depth interviews for evaluation input. Retrieved April 7, 2019, from [http://www2.pathfinder.org/site/DocServer/m\\_e\\_tool\\_series\\_indepth\\_interviews.pdf](http://www2.pathfinder.org/site/DocServer/m_e_tool_series_indepth_interviews.pdf)
- Bradbury, D. (2013). The problem with bitcoin. *Computer Fraud & Security*, 2013(11), 5–8.

[https://doi.org/10.1016/S1361-3723\(13\)70101-5](https://doi.org/10.1016/S1361-3723(13)70101-5)

- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Brown, B. (2012). Beyond recommendations: local review web sites and their impact. *ACM Trans. Comput.-Hum. Interact.*, 19(4), 27:1--27:24. <https://doi.org/10.1145/2395131.2395134>
- Bryman, A. (1984). The debate about quantitative and qualitative research: a question of method or epistemology? *The British Journal of Sociology*, 35(1). Retrieved from <https://www.jstor.org/stable/pdf/590553.pdf>
- BTC.com. (2017). Wallet for bitcoin and bitcoin cash. Retrieved April 7, 2019, from [https://wallet.btc.com/?\\_ga=2.71772819.124095.1554668742-553699307.1554668742#/setup/register](https://wallet.btc.com/?_ga=2.71772819.124095.1554668742-553699307.1554668742#/setup/register)
- BTC Relay. (2016). Frequently asked questions — BTC relay 1.0 documentation. Retrieved April 7, 2019, from <https://btc-relay.readthedocs.io/en/latest/frequently-asked-questions.html>
- Buterin, V. (2013a). *A next generation smart contract & decentralized application platform*. Retrieved from [http://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf)
- Buterin, V. (2013b). Selfish mining: a 25% attack against the Bitcoin network. Retrieved April 5, 2019, from <https://Bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-Bitcoin-network-1383578440/>
- Buur, J., Jensen, M. V., & Djajadiningrat, T. (2004). Hands-only scenarios and video action walls. In *Proceedings of the 2004 conference on Designing interactive systems processes, practices, methods, and techniques - DIS '04* (p. 185). New York, New York, USA: ACM Press. <https://doi.org/10.1145/1013115.1013141>
- Caetano, R. (2015). *Learning Bitcoin : Embrace the New World of Finance by Leveraging the Power of crypto-Currencies Using Bitcoin and the Blockchain*. Birmingham: Packt Publishing.
- Caillot, M., & Nguyen-Xuan, A. (1995). Adults' understanding of electricity. *Public Understanding of Science*, 4(2), 131–151. <https://doi.org/10.1088/0963-6625/4/2/003>
- Cairns, P., & Cox, A. L. (2008). *Research Methods for Human-computer Interaction*. Cambridge University Press.
- Thanh, N., & Thanh, T. (2015). The interconnection between interpretivist paradigm and qualitative methods in education. *American Journal of Educational Science*, 1(2), 24–27. Retrieved from <http://www.aiscience.org/journal/ajeshttp://creativecommons.org/licenses/by-nc/4.0/>
- Carboni, M., Münkemüller, T., Lavergne, S., Choler, P., Borgy, B., Violle, C., Thuiller, W. (2016). What it takes to invade grassland ecosystems: traits, introduction history and filtering processes. *Ecology Letters*, 19(3), 219–229. <https://doi.org/10.1111/ele.12556>
- Carillo, R. (2015). Alternative currencies are bigger than Bitcoin: how they're building prosperity from London to Kenya. Retrieved April 5, 2019, from

<https://www.yesmagazine.org/commonomics/alternative-currencies-bigger-than-bitcoin-bangla-pesa-brixton>

- Carroll, J. M., & Bellotti, V. (2015). Creating value together. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '15* (pp. 1500–1510). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2675133.2675270>
- Cartwright, K. (2018). A history of Bitcoin - get to know the cryptocurrency basics. Retrieved April 5, 2019, from <https://cartwrightking.co.uk/news/a-history-of-Bitcoin/>
- Cawrey, D. (2014). Are 51% attacks a real threat to Bitcoin? Retrieved April 5, 2019, from <https://www.coindesk.com/51-attacks-real-threat-Bitcoin>
- Central Bank of Malaysia. (2016). Issuance of a discussion paper on fintech regulatory sandbox. Retrieved April 5, 2019, from [http://www.bnm.gov.my/index.php?ch=en\\_announcement&pg=en\\_announcement&ac=456&lang=en](http://www.bnm.gov.my/index.php?ch=en_announcement&pg=en_announcement&ac=456&lang=en)
- Chen, C. (2014). Microsoft now accepts Bitcoin through bitpay. Retrieved January 15, 2019, from <https://www.ccn.com/microsoft-now-accepts-Bitcoin-bitpay/>
- Chilisa, B., & Kawulich, B. (2015). *Selecting a Research Approach: Paradigm, Methodology and Methods*. Retrieved from <https://www.researchgate.net/publication/257944787>
- Christin, N. (2012). Traveling the silk road: a measurement analysis of a large anonymous online marketplace. Retrieved April 5, 2019, from <http://arxiv.org/abs/1207.7139>
- Clarke, D. (1988). Framework for care. *Nursing Times*, 84(35), 33–35.
- Coin Desk. (2019). Bitcoin price index — real-time Bitcoin price charts . Retrieved January 21, 2019, from <https://www.coindesk.com/price/Bitcoin>
- Coin Market Cap. (2019a). Cryptocurrency market capitalizations. Retrieved April 1, 2019, from <https://coinmarketcap.com/>
- Coin Market Cap. (2019b). Cryptocurrency market capitalizations | coinmarketcap. Retrieved January 15, 2019, from <https://coinmarketcap.com/>
- Coinbase. (n.d.). Identity verification. Retrieved April 2, 2019, from <https://support.coinbase.com/customer/en/portal/articles/1220621-identity-verification>
- Coinbase. (2019). Coinbase pricing fees disclosures. Retrieved April 1, 2019, from <https://support.coinbase.com/customer/en/portal/articles/2109597-coinbase-pricing-fees-disclosures>
- Consumer Financial Protection Bureau. (2016). Risk to consumer posed by virtual currencies. Retrieved April 5, 2019, from <http://www.fatf-gafi.org/topics/>
- Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 58(6), 737–758. [https://doi.org/10.1016/S1071-5819\(03\)00041-7](https://doi.org/10.1016/S1071-5819(03)00041-7)
- Costanza, R. (2003a). Complementary currencies as a method to improve local sustainable economic

- welfare. Retrieved April 5, 2019, from <http://78.46.126.155/Record/632>
- Craik, K. (1943). *The Nature of Explanation*. Cambridge, UK: Cambridge University Press.
- Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain technology: beyond bitcoin. Retrieved April 5, 2019, from <https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>
- CryptoKitties. (n.d.). Collect and breed digital cats! Retrieved July 19, 2019, from <https://www.cryptokitties.co/>
- Cuen, L. (2018). A decentralizemd bitcoin exchange that's almost decentralized. Retrieved April 7, 2019, from <https://www.coindesk.com/Bitcoin-decentralized-exchange-dex-crypto-bisq-dao-monero>
- Dalton, M. A., Zeidman, P., McCormick, C., & Maguire, E. A. (2018). Differentiable processing of objects, associations, and scenes within the hippocampus. *The Journal of Neuroscience: The Official Journal of the Society for Neuroscience*, 38(38), 8146–8159. <https://doi.org/10.1523/JNEUROSCI.0263-18.2018>
- Darby, D. (2018). What's mutual credit, and what can we do to help? (plus webinar) Low impact living info, training, products & services. Retrieved January 21, 2019, from <https://www.lowimpact.org/interview-with-matthew-slater-whats-mutual-credit-how-can-it-help-the-solidarity-economy-and-what-can-we-do-to-help-plus-webinar/>
- Davenport, B. (2015). What is multi-sig, and what can it do? Retrieved April 5, 2019, from <https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319. <https://doi.org/10.2307/249008>
- De Villiers, M. R. (2005). Three approaches as pillars for interpretive information systems research: development research, action research and grounded theory. In *Proceedings of SAICSIT*. Retrieved from <https://core.ac.uk/download/pdf/43173636.pdf>
- Denzin, N. K. (2006). *Sociological Methods :A Sourcebook*. Aldine Transaction.
- Diesessa, A. (1981). *Phenomenology and the Evolution of Intuition*. USA.
- Doane, S. . (1982). *A Longitudinal Study of Unix User's Expertise, Unix Mental Models, and Task Performance*. University of California.
- Donnelly, J. (2016). Why bitcoin's halving was a boring vindication. Retrieved April 5, 2019, from <https://www.coindesk.com/Bitcoin-halving-event-boring-vindication-software>
- Egger, F. N. (2001). Affective design of e-commerce user interfaces : how to maximise perceived trustworthiness. Retrieved April 5, 2019, from <https://www.semanticscholar.org/paper/Affective-Design-of-E-Commerce-User-Interfaces-%3A-to-Egger/aa320c098c0557986250a903624b0980dbfcc40a>
- Eklblaw, A., Azaria, A., Halamka, J. D., Lippman, A., & Vieira, T. (2016). A case study for blockchain in healthcare: prototype for electronic health records and medical research data white paper medrec:

- using blockchain for medical data access and permission management ieee original authors. Retrieved April 5, 2019, from <https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf>
- Eklundh, K. S., & Lantz, A. (n.d.). Research methods in human-computer interaction. Retrieved April 5, 2019, from <https://www.nada.kth.se/kurser/kth/2D5339/Introduction.pdf>
- El Bansarkhani, R., & Sturm, J. (2016). An efficient lattice-based multisignature scheme with applications to Bitcoins. In *International Conference on Cryptology and Network Security* (pp. 140–155). Springer, Cham. [https://doi.org/10.1007/978-3-319-48965-0\\_9](https://doi.org/10.1007/978-3-319-48965-0_9)
- Electrum. (2017). Multisig wallets — electrum 3.1 documentation. Retrieved April 7, 2019, from <http://docs.electrum.org/en/latest/multisig.html>
- Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C., & Vines, J. (2018). Making sense of blockchain applications. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (pp. 1–14). New York, New York, USA: ACM Press. <https://doi.org/10.1145/3173574.3174032>
- Elst, H. Van. (2013). Foundations of descriptive and inferential statistics. Retrieved April 5, 2019, from <http://arxiv.org/abs/1302.2525>
- Eremeev, A. (1999). E-commerce trust study. Retrieved April 5, 2019, from <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.93.6753>
- European Central Bank. (2012). Virtual currency schemes. Retrieved April 5, 2019, from <http://www.ecb.europa.eu>
- Evander, S. (2016). Top 10 Countries in which bitcoin is banned. Retrieved April 5, 2019, from <https://www.cryptocoinsnews.com/top10countriesBitcoinbanned>
- Eyal, I., & Sirer, E. G. (2014). Majority is not enough: bitcoin mining is vulnerable. In *Financial Cryptography and Data Security*, 61(7), 436–454.
- Falcone, R., & Castelfranchi, C. (2001). Social trust: a cognitive approach. In *Trust and Deception in Virtual Societies* (pp. 55–90). Dordrecht: Springer Netherlands. [https://doi.org/10.1007/978-94-017-3614-5\\_3](https://doi.org/10.1007/978-94-017-3614-5_3)
- FATF. (2014). *Virtual currencies key definitions and potential aml/cft risks*. Retrieved April 5, 2019, from [www.fatf-gafi.org](http://www.fatf-gafi.org)
- Fein, R. M., Olson, G. M., & Olson, J. S. (1993). A mental model can help with learning to operate a complex device. In *INTERACT '93 and CHI '93 conference companion on Human factors in computing systems - CHI '93* (pp. 157–158). New York, New York, USA: ACM Press. <https://doi.org/10.1145/259964.260170>
- Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods* (Vol. 5). Retrieved April 5, 2019, from [http://www.ualberta.ca/~iiqm/backissues/5\\_1/pdf/fereday.pdf](http://www.ualberta.ca/~iiqm/backissues/5_1/pdf/fereday.pdf)

- Ferreira, J., Mark, P., & Subramanian, S. (2015). Spending time with money: from shared values to social connectivity. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (pp. 1222–1234). ACM. <https://doi.org/10.1145/2675133.2675230>
- FinCEN. (2000). A survey of electronic cash, electronic banking and internet gaming 2 3 a survey of electronic cash, electronic banking and internet gaming. Retrieved April 5, 2019, from <https://www.fincen.gov/sites/default/files/shared/e-cash.pdf>
- Fischer, C. (2008). Feedback on household electricity consumption: a tool for saving energy? *Energy Efficiency*, 1(1), 79–104. <https://doi.org/10.1007/s12053-008-9009-7>
- Fisher, J., Craig, A., & Bentley, J. (2007). Moving from a web presence to e-commerce: the importance of a business - web strategy for small-business owners. *Electronic Markets*, 17(4), 253–262. <https://doi.org/10.1080/10196780701635864>
- Fishkin, K. (2004). A taxonomy for and analysis of tangible interfaces. *Personal and Ubiquitous Computing*, 8(5), 347–358. <https://doi.org/10.1007/s00779-004-0297-4>
- FMT Reporters. (2016). penggunaan mata wang digital bitcoin meningkat mendadak di malaysia. Retrieved April 7, 2019, from <https://www.freemalaysiatoday.com/category/bahasa/2016/08/01/penggunaan-mata-wang-digital-Bitcoin-meningkat-mendadak-di-malaysia/>
- Fontinelle, A. (2011). An introduction to complementary currencies. Retrieved January 16, 2019, from <https://www.investopedia.com/articles/economics/11/introduction-complementary-currencies.asp>
- Fraser, T., & Banks, A. (2004). Designer's color manual: the complete guide to color theory and application. Chronicle Books. Retrieved April 5, 2019, from <https://books.google.co.uk/books?id=WXZNPaX-LvcC>
- Fui, F., Nah, H., & Davis, S. (2002). HCI research issues in e-commerce. *Journal of Electronic Commerce Research*, 3(3). Retrieved from <https://pdfs.semanticscholar.org/639a/a95f202493b4f9d40a42dabb22338277c8e3.pdf>
- Gay, G., & Hembrooke, H. (2004). *Activity-centered Design : An Ecological Approach to Designing Smart Tools and Usable Systems*. MIT Press. Retrieved from <https://mitpress.mit.edu/books/activity-centered-design>
- Geiger, R. A. (1993). *Conceptualizations and Mental Processing in Language*. (W. de G. & Co, Ed.). Berlin.
- Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is bitcoin a decentralized currency? *IEEE Security & Privacy*, 12(3), 54–60. <https://doi.org/10.1109/MSP.2014.49>
- Gibbs, G. (1998). *Learning by doing, a guide to teaching and learning methods*. Retrieved from <http://www2.glos.ac.uk/gdn/gibbs/index.htm>
- Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014). Bitcoin-asset or currency? revealing users' hidden intentions. In *ECIS 2014*. Tel Aviv. Retrieved from <http://secondlife.com/>

- Göbel, J., Keeler, P., Krzesinski, A. E., & Taylor, P. G. (2015). Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay. Retrieved from <http://arxiv.org/abs/1505.05343>
- Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research  
Pragmatism vs. interpretivism in qualitative information systems research. *European Journal of Information Systems*, 2(21), 135–146. <https://doi.org/10.1057/ejis.2011.54>
- Goodhue, D., Lewis, W., & Thompson, R. (2006). PLS, small sample size, and statistical power in mis research. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (pp. 202b-202b). IEEE. <https://doi.org/10.1109/HICSS.2006.381>
- Grandison, T., Sloman, M., Hupcey, J. E., Penrod, J., Morse, J. M., & Mitcham, C. (2001). A survey of trust in internet application communications. surveys & tutorials . & an exploration and advancement of the concept of trust. *Journal of Advanced Nursing* 36 2, 3(4), 282–293.
- Greenberg, S., & Fitchett, C. (2001). Phidgets: easy development of physical interfaces through physical widgets. In *proceedings of the ACM UIST* . Orlando. Retrieved from [www.midivid.com](http://www.midivid.com)
- Greeno, J. (1983). *Conceptual Entities*. ERIC. Retrieved from <https://catalogue.nla.gov.au/Record/5433453>
- Guadamuz, A., & Marsden, C. (2015). Blockchains and bitcoin: regulatory responses to cryptocurrencies. *First Monday*, 20(12). <https://doi.org/10.5210/fm.v20i12.6198>
- Gutscher, A. (2007). A trust model for open decentralized reputation system. *Journal of Federation for Information Processing* 238, 285–300.
- Hajdarbegovic, N. (2014). Bitcoin miners ditch ghash.io pool over fears of 51% attack. Retrieved April 7, 2019, from <https://www.coindesk.com/Bitcoin-miners-ditch-ghash-io-pool-51-attack>
- Hampe, B., & Grady, J. E. (2005). *From Perception to Meaning : Image Schemas in Cognitive Linguistics*. Mouton de Gruyter. Retrieved from [https://books.google.co.uk/books/about/From\\_Perception\\_to\\_Meaning.html?id=W7rfP-eliy0C&redir\\_esc=y](https://books.google.co.uk/books/about/From_Perception_to_Meaning.html?id=W7rfP-eliy0C&redir_esc=y)
- Hardin, R. (2002). *Trust and Trustworthiness*. Sage. Russell Sage Foundation.
- Hardy, J., & Alexander, J. (2012). Toolkit support for interactive projected displays. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia - MUM '12* (p. 1). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2406367.2406419>
- Harley, A. (2018). UX expert reviews. Retrieved April 5, 2019, from <https://www.nngroup.com/articles/ux-expert-reviews/>
- Hartmann, B., Klemmer, S. R., Bernstein, M., Abdulla, L., Burr, B., Robinson-Mosher, A., & Gee, J. (2006). *Reflective physical prototyping through integrated design, test, and analysis*. Montreux,
- Hasslacher, L. (2014). *Trust in mobile travel and meet new people applications*. Retrieved from <http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A724458&dswid=mainwindow>
- Hayes, A. (2015 Association for information systems ais electronic library (aisel) cryptocurrency value

- formation: an empirical analysis leading to a cost of production model for valuing Bitcoin. In *Mediterranean Conference on Information Systems (MCIS)* (p. 2015). Retrieved from <http://aisel.aisnet.org/mcis2015>
- Hearn, M. (2015). On block sizes. Retrieved April 7, 2019, from <https://medium.com/@octskyward/on-block-sizes-e047bc9f830>
- Hegarty, M., & Just, M. A. (1993). Constructing mental models of machines from text and diagrams. *Journal of Memory and Language*, 32(6), 717–742. <https://doi.org/10.1006/jmla.1993.1036>
- Hertig, A. (2018). how do ethereum smart contracts work? Retrieved April 5, 2019, from <https://www.coindesk.com/information/ethereum-smart-contracts-work>
- Higgins, S. (2018). KFC canada is accepting bitcoin for fried chicken. Retrieved April 1, 2019, from <https://www.coindesk.com/kfc-canada-is-accepting-Bitcoin-for-fried-chicken>
- Horda, T. (2018). What is a smart contract and how it relates to blockchain? Retrieved April 7, 2019, from <https://rubygarage.org/blog/guide-to-smart-contracts>
- Hornecker, E., & Buur, J. (2006). Getting a grip on tangible interaction. In *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06* (p. 437). New York, New York, USA: ACM Press. <https://doi.org/10.1145/1124772.1124838>
- Hu, X., Hu, X., Lin, Z., & Zhang, H. (2001). Myth or reality: effect of trust promoting seals in electronic markets. In *Proceeding Of The Eleventh Annual Workshop On Information Technologies And Systems* 65—70. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.521.9901>
- Hub Culture. (2014). Hub culture overview. Retrieved January 16, 2019, from <https://hubculture.com/hubs/hub/projects/62/wiki/>
- Huillet, M. (2018). China's supreme court rules that blockchain can legally authenticate evidence. Retrieved April 7, 2019, from <https://cointelegraph.com/news/chinas-supreme-court-rules-that-blockchain-can-legally-authenticate-evidence>
- Hurtienne, J. (2009). *Image Schemas and Design for Intuitive Use*. Technische Universität Berlin. Retrieved from <https://www.designsociety.org/publication/38248/Image+Schemas+and+Design+for+Intuitive+Use>
- Hurtienne, J., & Israel, J. H. (2007). Image schemas and their metaphorical extensions. In *Proceedings of the 1st international conference on Tangible and embedded interaction - TEI '07* (p. 127). New York, New York, USA: ACM Press. <https://doi.org/10.1145/1226969.1226996>
- IEEE Innovation. (2019). 6 Real-world challenges that blockchain technology is poised to solve iee innovation at work. Retrieved April 7, 2019, from <https://innovationatwork.ieee.org/6-real-world-challenges-that-blockchain-technology-is-poised-to-solve/>
- IG Analyst. (2017). Who owns bitcoin? Retrieved April 7, 2019, from <https://www.ig.com/uk/trading-opportunities/who-owns-Bitcoin--39703-170906>
- Ilett, D. (2013). What about ven? Stan Stalnaker talks digital currency. Retrieved January 21, 2019, from <https://www.coindesk.com/ven-qa>

- Ishii, H., & Ullmer, B. (1997). Tangible bits: towards seamless interfaces between people, bits, and atoms. In *Proceedings of CHI'97* (pp. 234–241).
- Jabbar, K., & Bjørn, P. (2017). Growing the blockchain information infrastructure. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17* (pp. 6487–6498). New York, New York, USA: ACM Press. <https://doi.org/10.1145/3025453.3025959>
- Jack, M., Chen, J., & Jackson, S. J. (2017). Infrastructure as creative action. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17* (pp. 6511–6522). New York, New York, USA: ACM Press. <https://doi.org/10.1145/3025453.3025889>
- Janiszewski, M. (2017). Towards an evaluation model of trust and reputation management systems. *International Journal of Electronics and Telecommunications*, 63(4), 411–416. <https://doi.org/10.1515/eletel-2017-0058>
- Jansen, Y., Dragicevic, P., Isenberg, P., Alexander, J., Karnik, A., Kildal, J., Hornbaek, K. (2015). Opportunities and challenges for data physicalization. In *Proceedings of the 2015 CHI Conference on Human Factors in Computing Systems - CHI '15* (pp. 3227-3236). Seoul, Republic of Korea: ACM Press. <https://doi.org/10.1145/2702123.2702180>
- Jevons, W. S. (1890). *Money and the Mechanism of Exchange*. (9th ed.). Kegan Paul, Trench, Trubner.
- Johnson, M. (1987). *The Body in the Mind. The Bodily Basis of Meaning, Imagination, and Reason*. Chicago & London: The University of Chicago Press.
- Adoga, J., Rabi, A. G. M., & Audu, A. (2014). Criteria for choosing an effective cloud storage provider. *International Journal of Computational Engineering Research*//Vol, 4(2). Retrieved from [http://www.ijceronline.com/papers/Vol4\\_issue02/Version-3/B042306013.pdf](http://www.ijceronline.com/papers/Vol4_issue02/Version-3/B042306013.pdf)
- Jøsang, A. (2007). Trust and reputation systems ★. Retrieved April 1, 2019, from <http://www.unik.no/people/josang/>
- Jung, H., & Stolterman, E. (2012). Digital form and materiality. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction Making Sense Through Design - NordiCHI '12* (p. 645). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2399016.2399115>
- Karame, G., Androulaki, E., Capkin, & S., Kaye, J (2014). Double-spending fast payments in bitcoin. *Proceedings Computer and Communications Security Pp ACM et Al CHI Money Financial Interactions Digital Cash Capital Exchange and Mobile Money CHI 14 Extended Abstracts on Human Factors in Computing 111114*, 906–917.
- Karamitsos, I., Papadaki, M., Baker, N., & Barghuthi, A. (2018). Design of the blockchain smart contract: A Use Case for Real Estate. *Journal of Information Security*, 9, 177–190. <https://doi.org/10.4236/jis.2018.93013>
- Karvonen, K., & Parkkinen, J. (2001). Signs of trust: a semiotic study of trust formation in the web. Retrieved April 1, 2019, from <http://carpoint.msn.com/home/New.asp>
- Kaye, J., Vertesi, J., Ferreira, J., Brown, B., & Perry, M. (2014). #CHImoney: financial interactions, digital cash, capital exchange and mobile money. In *CHI '14 Extended Abstracts on Human Factors*

- in Computing Systems* (pp. 111–114). New York, NY, USA: ACM.  
<https://doi.org/10.1145/2559206.2559221>
- Kazan, E., Tan, C. W., & Lim, E. T. K. (2015). Association for information systems ais electronic library (aisel) value creation in cryptocurrency networks: towards a taxonomy of digital business models for bitcoin companies. In *Pacific Asia Conference on Information Systems (PACIS)*. Retrieved from <http://aisel.aisnet.org/pacis2015>
- Keates, S., Clarkson, P. J., Keates, S., & Clarkson, P. J. (2003). Countering design exclusion through inclusive design. In *Proceedings of the 2003 conference on Universal usability - CUU '03* (p. 69). New York, New York, USA: ACM Press. <https://doi.org/10.1145/957205.957218>
- Khairuddin, I E, Sas, C., Clinch, S., & Davis, N. (2016). Exploring motivations for bitcoin technology usage. In *Proceedings of the Extended Abstracts on Human Factors in Computing Systems ACM* (pp. 2872–2878).
- Khairuddin, I. E., & Sas, C. (2019). An exploration of bitcoin mining practices: miners' trust challenges and motivations. In *Proceedings of ACM CHI 2019 Conference on Human Factors in Computing Systems*. Glasgow: ACM. DOI: <https://doi.org/10.1145/3290605.3300859>
- Khairuddin, I. E., Sas, C., and Chris, S. (2019). BlocKit: a physical kit for materializing and designing for blockchain infrastructure. In *Proceeding of the 2019 Designing Interactive System Conference (DIS '19)*. ACM New York, NY, USA, DOI: <https://doi.org/10.1145/3322276.332237>
- Khatwani, S. (2018). Best multi-signature bitcoin wallets [2019 Edition]. Retrieved April 5, 2019, from <https://coinsutra.com/best-multi-signature-Bitcoin-wallets/>
- Kieras, D. E., & Bovair, S. (1964). *The Role of a Mental Model in Learning to Operate a Device*. Cognitive Science (Vol. 8). Retrieved from [https://onlinelibrary.wiley.com/doi/pdf/10.1207/s15516709cog0803\\_3](https://onlinelibrary.wiley.com/doi/pdf/10.1207/s15516709cog0803_3)
- Kim, J., & Moon, J. Y. (1998). Designing towards emotional usability in customer interfaces—trustworthiness of cyber-banking system interfaces. *Interacting with Computers*, 10(1), 1–29. [https://doi.org/10.1016/S0953-5438\(97\)00037-4](https://doi.org/10.1016/S0953-5438(97)00037-4)
- Kinaterder, M., & Rothermel, K. (2003). Architecture and algorithms for a distributed reputation system (pp. 1–16). Springer, Berlin, Heidelberg. [https://doi.org/10.1007/3-540-44875-6\\_1](https://doi.org/10.1007/3-540-44875-6_1)
- Klemmer, S. R., Li, J., Lin, J., & Landay, J. A. (2004). *Papier-Mâché: Toolkit Support for Tangible Input*. Retrieved from <https://hci.stanford.edu/publications/2004/Papier-Mache.pdf>
- Klontz, B., Britt, S. L., Mentzer, J., & Klontz, T. (2011). Money beliefs and financial behaviors: development of the klontz money script inventory. *The Journal of Financial Therapy*, 2(1). <https://doi.org/10.4148/jft.v2i1.451>
- Knoop, M. W. (2015). Ven: a different digital currency. Retrieved January 16, 2019, from <https://www.digitalcurrencyperspectives.com/2015/04/06/ven-a-different-digital-currency/>
- Kow, Y. M., & Lustig, C. (2018). Imaginaries and crystallization processes in Bitcoin infrastructuring. In *Computer Supported Cooperative Work (CSCW)*, 27(2), 209–232. <https://doi.org/10.1007/s10606->

- Kramer, T., & Kennedy, R. S. (1996). Educational computing : column debut. *Academic Psychiatry : The Journal of the American Association of Directors of Psychiatric Residency Training and the Association for Academic Psychiatry*, 20(4), 242–243. <https://doi.org/10.1007/BF03341891>
- Kuhn, T. S., Joergensen, J., Rougier, L., Bohr, N., Von, R., Egon, M., Woodger, J. H. (1970). (paperbound) *Library of Congress Catalog Card Number. International Encyclopedia of Unified Science* (Vol. 2). Retrieved from [https://projektintegracija.pravo.hr/\\_download/repository/Kuhn\\_Structure\\_of\\_Scientific\\_Revolutions.pdf](https://projektintegracija.pravo.hr/_download/repository/Kuhn_Structure_of_Scientific_Revolutions.pdf)
- Kuznetsov, S., Hudson, P., Org, E., Kuznetsov, S., Hudson, S. E., & Paulos, E. (2014). UC Berkeley UC Berkeley Previously Published Works Title A low-tech sensing system for particulate pollution Publication Date License CC BY-NC-SA 4.0 Peer reviewed A Low-Tech Sensing System for Particulate Pollution. In *8th International Conference on Tangible, Embedded and Embodied Interaction (TEI'14)*. <https://doi.org/10.1145/2540930.2540955>
- Kuznetsov, S., Hudson, S. E., & Paulos, E. (2013). A low-tech sensing system for particulate pollution. In *Proceedings of the 8th International Conference on Tangible, Embedded and Embodied Interaction - TEI '14* (pp. 259–266). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2540930.2540955>
- Kuznetsov, S., Odom, W., Pierce, J., & Paulos, E. (2011). Nurturing natural sensors. In *UbiComp '11*. Retrieved from <http://staceyk.org/hci/KuznetsovBiomarkersUbiComp.pdf>
- Kuznetsov, S., & Paulos, E. (2010). Rise of the expert amateur. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction Extending Boundaries - NordiCHI '10* (p. 295). New York, New York, USA: ACM Press. <https://doi.org/10.1145/1868914.1868950>
- Labrecque, L. I., & Milne, G. R. (2012). Exciting red and competent blue: the importance of color in marketing. *Journal of the Academy of Marketing Science*, 40(5), 711–727. <https://doi.org/10.1007/s11747-010-0245-y>
- Lakoff, G. (1987). *George Lakoff Women, Fire, and Dangerous Things What Categories Reveal About the Mind*. Chicago and London: The University of Chicago Press. Retrieved from <https://pdfs.semanticscholar.org/9c85/d2dd7e6d924a1078fb93cac9baaa8a850d3e.pdf>
- Larkin, J. H. (1983). *The Role of Problem Representation in Physics, Mental Models*. Hillsdale, NJ: Lawrence Erlbaum Associates.
- Latifa, E. R., Kiram, E. L., & Ahemed, M. Y. (2017). Blockchain: bitcoin wallet cryptography security, challenges and counter measures. *Journal of Internet Banking and Commerce*, 22(3). Retrieved from <http://www.icommercecentral.com>
- Leppanen, A. (2010). *Technology Trust Antecedents: Building the Platform for Technology Enabled Performance*. Aalto University.
- Lerner, S. D. (2015). RSK white paper overview. Retrieved April 7, 2019, from

[https://docs.rsk.co/RSK\\_White\\_Paper-Overview.pdf](https://docs.rsk.co/RSK_White_Paper-Overview.pdf)

- Lim, C. H., & Lee, P. J. (1993). A practical electronic cash system for smart cards. *Technical Report of IEICE. ISEC*, 93(295), 33–41. Retrieved from <https://ci.nii.ac.jp/naid/110003297078/>
- Lindgaard, G., Dillon, R., Trbovich, P., White, R., Fernandes, G., Lundahl, S., & Pinnamaneni, A. (2006). User needs analysis and requirements engineering: theory and practice. *Interacting with Computers*, 18(1), 47–70. <https://doi.org/10.1016/J.INTCOM.2005.06.003>
- Lipkis, Sarah and Roth, A. (2014). Anatomy what is alternative currency. Retrieved April 7, 2019, from [https://worldpolicy.org/wp-content/uploads/2014/06/Summer14\\_12-13\\_Anatomy\\_0.pdf](https://worldpolicy.org/wp-content/uploads/2014/06/Summer14_12-13_Anatomy_0.pdf)
- Lippert, S. K., & Swiercz, P. M. (2005). Human resource information systems (HRIS) and technology trust. *Journal of Information Science*, 31(5), 340–353.
- Local Bitcoin. (n.d.). How to buy and sell bitcoins online on localbitcoins.com. Retrieved April 7, 2019, from <https://localBitcoins.com/guides/how-to-sell-Bitcoins-online>
- Lowe, R., & Boucheix, J.-M. (2008). Learning from animated diagrams: how are mental models built? In *Diagrammatic Representation and Inference* (pp. 266–281). Berlin, Heidelberg: Springer Berlin Heidelberg. [https://doi.org/10.1007/978-3-540-87730-1\\_25](https://doi.org/10.1007/978-3-540-87730-1_25)
- Lucas, D. (2018). Will blockchain video conferencing make video chats more secure? Retrieved April 3, 2019, from <https://www.videoconferencingdaily.com/latest-technology/will-Blockchain-video-conferencing-make-video-chats-more-secure/>
- Mahnke, F. H. (1996). *Color, Environment, and Human Response*. New York: Reinhold.
- Marshall, P., & Necker, E. H. (2013). Theories of embodiment in hci. In *The SAGE Handbook of Digital Technology Research* (pp. 144–158). 1 Oliver’s Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd. <https://doi.org/10.4135/9781446282229.n11>
- Martindale, J. (2018). What is an asic miner? Retrieved April 1, 2019, from <https://www.digitaltrends.com/computing/what-is-an-asic-miner/>
- Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Müllmann, D., Hohlfeld, O., & Wehrle, K. (2018). A quantitative analysis of the impact of arbitrary Blockchain content on Bitcoin. Retrieved from <https://www.semanticscholar.org/paper/A-Quantitative-Analysis-of-the-Impact-of-Arbitrary-Matzutt-Hiller/bb8cef06d139e0959232c471c21f1f7a429b8ddb>
- Maurer, B., Nelms, T. C., & Swartz, L. (2013). “When perhaps the real problem is money itself!”: the practical materiality of Bitcoin. *Social Semiotics*, 23(2), 261–277. <https://doi.org/10.1080/10350330.2013.777594>
- Maxwell, D., Speed, C., & Campbell, D. (2015). “Effing” the ineffable. In *Proceedings of the 2015 British HCI Conference on - British HCI ’15* (pp. 208–209). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2783446.2783593>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, 20(3), 709–734.

- Maykut, P. S., & Morehouse, R. (1994). *Beginning Qualitative Research : A Philosophic and Practical Guide*. Falmer Press.
- McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships . *The Academy of Management Review*, 23(3), 473–490.
- Mertens, D. M. (1998). *Research methods in education and psychology : integrating diversity with quantitative & qualitative approaches*. Sage Publications. Retrieved from [https://books.google.co.uk/books/about/Research\\_methods\\_in\\_education\\_and\\_psychology.html?id=pXWcAAAAMAAJ](https://books.google.co.uk/books/about/Research_methods_in_education_and_psychology.html?id=pXWcAAAAMAAJ)
- Mettler, M. (2016). Blockchain technology in healthcare: the revolution starts here. In *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 1–3). IEEE. <https://doi.org/10.1109/HealthCom.2016.7749510>
- Microsoft. (2018). User interface technologies. Retrieved April 5, 2019, from <https://docs.microsoft.com/en-us/windows/desktop/appuistart/user-interface-technologies-for-windows-applications>
- Migchels, A. (2012). A primer for recovering austrians: the many systems behind ‘violent statist fiat’ currencies! | real currencies. Retrieved January 16, 2019, from <https://realcurrencies.wordpress.com/2012/08/09/a-primer-for-recovering-austrians-the-many-systems-behind-violent-statist-fiat-currencies/>
- MIGHT. (2017). Malaysia sasar 2025 guna blockchain. Retrieved April 7, 2019, from <https://www.might.org.my/malaysia-sasar-2025-guna-Blockchain/>
- Miller, A. (2017). Toward an ethereum multisig standard. Retrieved April 5, 2019, from <https://blog.gridplus.io/toward-an-ethereum-multisig-standard-c566c7b7a3f6>
- Misiolek, N., Zakaria, N., & Zhang, P. (2002). Trust in organizational acceptance of information technology: a conceptual model and preliminary evidence. *Proceedings of the Decision Sciences Institute 33rd Annual Meeting San Diego California*, 1–7.
- MockupPlus. (2019). Prototype faster, smarter and easier with mockplus. Retrieved April 2, 2019, from <https://www.mockplus.com/>
- Moorman, C., Deshpandé, R., & Zaltman, G. (1993). Factors affecting trust in market research relationships. *Source: Journal of Marketing*, 57(1), 81–101. Retrieved from <https://faculty.fuqua.duke.edu/~moorman/Publications/JM1993.pdf>
- Morrow, J. (2014). The history of bitcoin mining. Retrieved April 7, 2019, from <https://blog.cex.io/cryptonews/evolution-of-Bitcoin-mining-12312>
- Möser, M. (2013). Anonymity of bitcoin transactions an analysis of mixing services. Retrieved from <https://www.torproject.org/>
- Muller, M. J., & Druin, A. (2002). Participatory design: the third space in hci. Retrieved from [http://www.watson.ibm.com/cambridge/Technical\\_Reports/2010/TR2010.10 Participatory Design The Third Space in HCI.pdf](http://www.watson.ibm.com/cambridge/Technical_Reports/2010/TR2010.10%20Participatory%20Design%20The%20Third%20Space%20in%20HCI.pdf)

- MultiChain. (n.d.). Multisignature transactions. Retrieved April 7, 2019, from <https://www.multichain.com/developers/multisignature-transactions/>
- Muszynska, M., Michels, D., & Zezschwitz, V., E. (2018). Not on my phone. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (pp. 1–6). New York, New York, USA: ACM Press. <https://doi.org/10.1145/3170427.3188625>
- Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Retrieved January 15, 2019, from [www.Bitcoin.org](http://www.Bitcoin.org)
- Neumann, C., Prigent, N., Varvello, M., & Suh, K. (2007). Challenges in peer-to-peer gaming. *ACM SIGCOMM Computer Communication Review*, 37(1), 79. <https://doi.org/10.1145/1198255.1198269>
- Nielsen, J. (2000). Designing web usability. *New Riders Indianapolis Indiana*.
- Nielsen, J. (1994). Usability inspection methods. In *Conference companion on Human factors in computing systems - CHI '94* (pp. 413–414). New York, New York, USA: ACM Press. <https://doi.org/10.1145/259963.260531>
- Nielsen, J. (1998). Introduction to web design. In *CHI 98 Conference Summary on Human factors in computing systems - CHI '98* (pp. 107–108). New York, New York, USA: ACM Press. <https://doi.org/10.1145/286498.286557>
- Nielsen, J., & Mack, R. L. (1994). *Usability Inspection Methods*. Wiley. Retrieved from <https://www.nngroup.com/books/usability-inspection-methods/>
- Nissen, B., Pschetz, L., Murray-Rust, D., Mehrpouya, H., Oosthuizen, S., & Speed, C. (2018). GeoCoin. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (pp. 1–10). New York, New York, USA: ACM Press. <https://doi.org/10.1145/3173574.3173737>
- Norman, D. A. (1990). *Psychology of Everyday Things*. Basic Books.
- Norman, D. A., & Draper, S. W. (1986). *User Centered System Design : New Perspectives on Human-computer Interaction*. L. Erlbaum Associates. Retrieved from <https://dl.acm.org/citation.cfm?id=576915>
- Ogono, U. (2018). Ether reward slashed to 2 eth by ethereum developers. Retrieved April 5, 2019, from <https://smartereum.com/31866/ether-reward-reduced-from-3-eth-per-block-to-2-eth-per-block-ether-reward-slashed-to-2-eth-by-ethereum-developers-ether-bomb-difficulty-ethereum-developers-ether-mining-ether-news-today/>
- Öksüz, A. (2014). Turning dark into white clouds-a framework on trust building in cloud providers via websites. Retrieved April 7, 2019, from <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1143&context=amcis2014>
- Omni Layer. (2017). Omni layer. Retrieved April 7, 2019, from <https://www.omnilayer.org/>
- Open Bazaar. (2015). Decentralized reputation in open bazaar. Retrieved April 1, 2019, from <https://openbazaar.org/blog/decentralized-reputation-in-openbazaar/>
- Orsini, L. (2013). GitHub for beginners: don't get scared, get started. Retrieved April 3, 2019, from

- <https://readwrite.com/2013/09/30/understanding-github-a-journey-for-beginners-part-1/>
- Patton, M Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Services Research, 34*(5 Pt 2), 1189–1208. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/10591279>
- Patton, M. Q. (1990). *Qualitative Evaluation and Research Methods*. Sage Publications.
- PayPal. (2015). Fees for sending money to friends and family. Retrieved April 7, 2019, from <https://www.paypal.com/uk/webapps/mpp/paypal-fees>
- Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In *2nd IEEE International Conference on Cloud Computing Technology and Science*. <https://doi.org/10.1109/CloudCom.2010.66>
- Pierce, J., & Paulos, E. (2012a). Designing everyday technologies with human-power and interactive microgeneration. In *Proceedings of the Designing Interactive Systems Conference on - DIS '12* (p. 602). New York, New York, USA: ACM Press. <https://doi.org/10.1145/2317956.2318047>
- Pierce, J., & Paulos, E. (2012b). The local energy indicator: designing for wind and solar energy systems in the home. In *Designing Interactive System*. Retrieved from [http://www.paulos.net/papers/2012/LocalEnergyIndicator \(DIS 2012\).pdf](http://www.paulos.net/papers/2012/LocalEnergyIndicator%20(DIS%202012).pdf)
- Pinelle, D., Wong, N., & Stach, T. (2008). Heuristic evaluation for games. In *Proceeding of the twenty-sixth annual CHI conference on Human factors in computing systems - CHI '08* (p. 1453). New York, New York, USA: ACM Press. <https://doi.org/10.1145/1357054.1357282>
- Ping Z., Small, R. V., Von, D. G. M., & Barcellos, S. (1999) Websites that satisfy users: a theoretical framework for Web user interface design and evaluation. In *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers* (p. 8). IEEE Comput. Soc. <https://doi.org/10.1109/HICSS.1999.772668>
- Pizam, A., Chon, K. S., & Mansfeld, Y. (1999). *Consumer Behavior in Travel and Tourism*. Haworth Hospitality Press. Retrieved from [https://books.google.co.uk/books?hl=en&lr=&id=Z4iA12CpQpQC&oi=fnd&pg=PA5&dq=consumer+r+behavior+in+travel+and+tourism+pdf+pizam+and+mansfeld&ots=leP\\_aeA256&sig=9XCaFHOhMFvJOEEUNzcFwCaV-8A#v=onepage&q=consumer%2520behavior%2520in%2520travel%2520and%2520tourism%2520pdf%252](https://books.google.co.uk/books?hl=en&lr=&id=Z4iA12CpQpQC&oi=fnd&pg=PA5&dq=consumer+behavior+in+travel+and+tourism+pdf+pizam+and+mansfeld&ots=leP_aeA256&sig=9XCaFHOhMFvJOEEUNzcFwCaV-8A#v=onepage&q=consumer%20behavior%20in%20travel%20and%20tourism%20pdf%252)
- Polit, D. F., & Beck, C. T. (2016). *Nursing Research : Generating and Assessing Evidence for Nursing Practice*. Lippincott Williams and Wilkins.
- Popper, K. (1959). *Karl Popper: The logic of Scientific Discovery*. Vienna, Austria: Taylor & Francis Group. Retrieved from <http://s-f-walker.org.uk/pubsebooks/pdfs/popper-logic-scientific-discovery.pdf>
- Purser, S. (2001). A simple graphical tool for modeling trust. *Journal of Computers Security, 20*(6), 479–484.
- Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting &*

- Management*, 8(3), 238–264. <https://doi.org/10.1108/11766091111162070>
- Rahimi, H., & Bakkali, H. EL. (2014). A new trust reputation system for e-commerce applications. *International Journal of Computer Science Issues*. Retrieved from <http://arxiv.org/abs/1405.3199>
- Ray, A., Ventresca, M., & Wan, H. (2018). A mechanism design approach to blockchain protocols. In *IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics*. [https://doi.org/10.1109/Cybermatics\\_2018.2018.00268](https://doi.org/10.1109/Cybermatics_2018.2018.00268)
- Redman, J. (2016). HashOcean: another cloud mining scam? Retrieved April 7, 2019, from <https://news.Bitcoin.com/hashocean-cloud-mining-scam/>
- Remy, J. C. (2017). *Incorporating sustainable hci research into design practice*. University of Zurich. Retrieved from [http://christianremy.com/\\_publications/2017\\_phd-thesis.pdf](http://christianremy.com/_publications/2017_phd-thesis.pdf)
- Resnick, P., Zeckhauser, R., Swanson, J., & Lockwood, K. (2006). The value of reputation on eBay: A controlled experiment. *Experimental Economics*, 9(2), 79–101. <https://doi.org/10.1007/s10683-006-4309-2>
- Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. *International Journal of Human Computer Studies*, 62(3), 381–422. <https://doi.org/10.1016/j.ijhcs.2005.01.001>
- Rogojanu, A., & Badea, L. (2014). The issues of competing currencies, Case study-Bitcoin. *Theoretical and Economics Journal* 103, 21(1).
- Rolnick, A. J., & Weber, W. E. (1997). Money, inflation, and output under fiat and commodity standards. *Journal of Political Economy*, 105(6), 1308–1321. <https://doi.org/10.1086/516394>
- Salomaa, A. (1996). *Public-Key Cryptography*. Springer Berlin Heidelberg. Retrieved from <https://books.google.co.uk/books?hl=en&lr=&id=0ceqCAAQBAJ&oi=fnd&pg=PA1&dq=public+cryptography&ots=E7V3yb9IqY&sig=vYdWaBwIDGj4V0SBKwgM4KfuaIo#v=onepage&q=public cryptography&f=false>
- Salovaara, A, Höök, K. Cheverst, K., Twidale, M. Chalmers, M and Sas, C. (2011). Appropriation and creative use linking user studies and design. In *Extended Abstracts on Human Factors in Computing Systems CHI EA 11 ACM* (pp. 37–40). New York, New York, USA: ACM Press.
- Santibáñez, F. (2002). The object image-schema and other dependent schemas. In *Jstor*, 24(2). Retrieved from [https://www.jstor.org/stable/41055078?seq=1#metadata\\_info\\_tab\\_contents](https://www.jstor.org/stable/41055078?seq=1#metadata_info_tab_contents)
- Sapirshstein, A., Sompolinsky, Y., & Zohar, A. (2015). Optimal selfish mining strategies in bitcoin. Retrieved April 7, 2019, from <http://arxiv.org/abs/1507.06183>
- Sas, C., & Khairuddin, I. E. (2015). Exploring Trust in Bitcoin technology: a framework for hci research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction* (pp. 338–342). <https://doi.org/10.1145/2838739.2838821>
- Sas, C., & Khairuddin, I. E. (2017). Design for trust: an exploration of the challenges and opportunities of Bitcoin users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*

- (pp. 6499--6510). Retrieved from <http://dl.acm.org/citation.cfm?id=3025886>
- Sas, C., & Neustaedter, C. (2017). Exploring diy practices of complex home technologies. *ACM Transactions on Computer-Human Interaction*, 24(2), 1–29. <https://doi.org/10.1145/3057863>
- Sas, C., Whittaker, S., Dow, S., Forlizzi, J., & Zimmerman, J. (2014). Generating implications for design through design research. In *In Proceedings of the 32nd Annual ACM Conference on Human factors in computing systems CHI 14 ACM* (pp. 1971–1980).
- Schuler, D., & Namioka, A. (1993). *Participatory Design : Principles and Practices*. L. Erlbaum Associates.
- Schwandt, T. A. (2001). *Dictionary of Qualitative Inquiry*. Sage Publications.
- Schweikart, L. (1991). U.S. commercial banking: a historiographical survey. *Business History Review*, 65(03), 606–661. <https://doi.org/10.2307/3116769>
- Seckler, M., Heinz, S., F., Tuch, A. N., & Opwis, K. (2015). Trust and distrust on the web : user experiences and website characteristics. Retrieved from <https://edoc.unibas.ch/35602/>
- Shaer, O., & Jacob, R. J. K. (2009). A specification paradigm for the design and implementation of tangible user interfaces. *ACM Transactions on Computer-Human Interaction*, 16(4), 1–39. <https://doi.org/10.1145/1614390.1614395>
- Sharma, T. K. (2017). List of best open source blockchain platforms and their features. Retrieved April 7, 2019, from <https://www.blockchain-council.org/blockchain/list-of-best-open-source-blockchain-platforms/>
- Sharma, V., Simpson, R. C., LoPresti, E. F., Mostowy, C., Olson, J., Puhlman, J., Kerley, B. (2008). Participatory design in the development of the wheelchair convoy system. *Journal of Neuroengineering and Rehabilitation*, 5, 1. <https://doi.org/10.1186/1743-0003-5-1>
- Shcherbak, S. (2014). How should Bitcoin be regulated? In *European Journal of Legal Studies.*, 7(1), 46–91.
- Shneiderman, B., & Ben. (2000). Creating creativity: user interfaces for supporting innovation. *ACM Transactions on Computer-Human Interaction*, 7(1), 114–138. <https://doi.org/10.1145/344949.345077>
- Shoaib, M., Ilyas, M., & Hayat Khiyal, M. S. (2013). Official digital currency. In *Eighth International Conference on Digital Information Management (ICDIM 2013)* (pp. 346–352). IEEE. <https://doi.org/10.1109/ICDIM.2013.6693982>
- Sillence, E., Briggs, P., Harris, P., & Fishwick, L. (2006). A framework for understanding trust factors in web-based health advice. *International Journal of Human-Computer Studies*, 64(8), 697–713. <https://doi.org/10.1016/J.IJHCS.2006.02.007>
- Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 463–467). IEEE. <https://doi.org/10.1109/IC3I.2016.7918009>

- Skarlatidou, A., Cheng, T., & Haklay, M. (2013). Guidelines for trust interface design for public engagement Web GIS. *International Journal of Geographical Information Science*, 27(8), 1668–1687. <https://doi.org/10.1080/13658816.2013.766336>
- Slush Pool. (2017). Hash Proof Rate. Retrieved April 7, 2019, from <https://slushpool.com/help/hashrate-proof/>
- Staggers, N., & Norcio, A. F. (1993). Mental models: concepts for human-computer interaction research. *International Journal of Man-Machine Studies*, 38(4), 587–605. <https://doi.org/10.1006/IMMS.1993.1028>
- Steemit. (2017). Decentralized free voice calls, video calls and messages over a blockchain, do you want to be part of it? Retrieved April 3, 2019, from <https://steemit.com/blockchain/@interpreter/decentralized-free-voice-calls-video-calls-and-messages-over-a-blockchain-do-you-want-to-be-part-of-it>
- Steinbrück, U., Schaumburg, H., Duda, S., & Krüger, T. (2002). A picture says more than a thousand words. In *CHI '02 extended abstracts on Human factors in computing systems - CHI '02* (p. 748). New York, New York, USA: ACM Press. <https://doi.org/10.1145/506443.506578>
- Stevens, A. (2018). Distributed ledger consensus explained. Retrieved April 5, 2019, from <https://hackernoon.com/distributed-ledger-consensus-explained-b0968d1ba087>
- Strauss, A. L., Schatzman, L., Bucher, R., Ehrlich, D., & Sabshin, M. (1964). *Psychiatric Ideologies and Institutions*. New York: Free Press.
- Subramanian, R., & Chino, T. (2015). The state of cryptocurrencies, their issues and policy interactions. *Journal of International Technology and Information Management*, 24. Retrieved from <http://scholarworks.lib.csusb.edu/jitimhttp://scholarworks.lib.csusb.edu/jitim/vol24/iss3/2>
- Swan, M. (2015). *Blockchain: blueprint for a new economy*. California: O'Reilly.
- Sward, A., Vecna, I., & Forrest, S. (2018). Data insertion in bitcoin's blockchain. *Ledger Journal*, 3(0). Retrieved from <https://ledgerjournal.org/ojs/index.php/ledger/article/view/101/93>
- Sykes, E. (1905). *Banking and currency*. London: Butterworth & Co., Crane Court E.C. Retrieved from <https://archive.org/details/bankingcurrency00sykerich/page/n5>
- Talk, B. (2010). Anonymity. Retrieved April 5, 2019, from <https://Bitcointalk.org/index.php?topic=241.msg8874 #msg8874>
- Tasca, P. (2015a). Digital currencies: principles, trends, opportunities, and risks. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2657598>
- Tasca, P. (2015b). Digital currencies: principles, trends, opportunities, and risks. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2657598>
- Tashakkori, A., & Teddlie, C. (1998). *Mixed Methodology: Combining Qualitative and Quantitative Approaches*. - *PsycNET*. CA, USA: Sage Publications, Inc. Retrieved from <https://psycnet.apa.org/record/1998-08132-000>

- Tether. (n.d.). Tether: fiat currencies on the bitcoin blockchain. Retrieved September 19, 2016, from <https://www.weusecoins.com/assets/pdf/library/Tether20Whitepaper.pdf>
- Tharakan, K. (2006). Methodology of social sciences: positivism, anti-positivism and the phenomenological mediation. *Indian Journal of Social Work, 1*, 16–31. Retrieved from <https://philpapers.org/rec/THAMOS-2>
- The Guardian. (2014). Bitcoin explained and made simple. Retrieved April 5, 2019, from <https://www.youtube.com/watch?v=s4g1XFU8Gto>
- Thornburg, E. G. (2012). Going private: technology, due process and internet dispute resolution: The Federal Arbitration Act., *9*, 1–16.
- Torpey, K. (2015). What is selfish bitcoin mining and is it a threat? Retrieved April 5, 2019, from <https://coinjournal.net/what-is-selfish-mining-and-is-it-a-threat-to-Bitcoin/>
- Trivedi, M. (2018). Bitcoin in india: a deep down scenario. *Journal of Management Science, Operations & Strategies (e ISSN 2456-9305)*, *2*(1), 21–26. Retrieved from <http://management.nrjp.co.in/index.php/JMSOS/article/view/214>
- Truong, K. N. (2006). Storyboarding: an empirical determination of best practices and effective guidelines. In *Proceedings of DIS 2006*, 12--21. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.110.6354>
- Tyler, T. R., & DeGoey, P. (1996). Trust in organizational authorities: the influence of motive attributions on willingness to accept decisions. In *Trust in Organizations: Frontiers of Theory and Research* (pp. 331–356). 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc. <https://doi.org/10.4135/9781452243610.n16>
- Vanian, J. (2018). Bitcoin: microsoft welcomes back cryptocurrency after halt fortune. Retrieved April 1, 2019, from <http://fortune.com/2018/01/10/microsoft-Bitcoin-temporary-halt/>
- Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, bitcoin, and ethereum: a brief overview. In *2018 17th International Symposium Infoteh-Jahorina (Infoteh)* (pp. 1–6). IEEE. <https://doi.org/10.1109/INFOTEH.2018.8345547>
- Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: concepts, elements, and implications. *Computers in Human Behavior, 21*(1), 105–125. <https://doi.org/10.1016/J.CHB.2003.11.008>
- WeiDex. (n.d.). WeiDex - decetralized exchange. Retrieved April 7, 2019, from <https://weidex.market/welcome>
- White, L. H. (2014). The troubling suppression of competition from alternative monies: the cases of the liberty dollar and e-gold. *Cato Journal, 34*. Retrieved from <https://heinonline.org/HOL/Page?handle=hein.journals/catoj34&id=297&div=24&collection=journals>
- Wiberg, M., & Mikael. (2014). Methodology for materiality: interaction design research through a material lens. *Personal and Ubiquitous Computing, 18*(3), 625–636. <https://doi.org/10.1007/s00779->

- Wikipedia. (n.d.). Sifteo cubes. Retrieved April 7, 2019, from [https://en.wikipedia.org/wiki/Sifteo\\_Cubes](https://en.wikipedia.org/wiki/Sifteo_Cubes)
- Wilson, L. (2016). The average price of electricity, country by country. Retrieved April 7, 2019, from <https://www.energycentral.com/c/ec/average-price-electricity-country-country>
- Wirdum, A. Van. (2016a). A primer on bitcoin governance, or why developers aren't in charge of the protocol. Retrieved April 7, 2019, from <https://Bitcoinmagazine.com/articles/a-primer-on-Bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427/>
- Wirdum, A. Van. (2016b). Slush pool introduces provably fair bitcoin mining. Retrieved April 7, 2019, from <https://Bitcoinmagazine.com/articles/slush-pool-introduces-provably-fair-Bitcoin-mining-1455217308/>
- Wray, L. R. (2012). Introduction to an alternative history of money. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2050427>
- Wright, A. (1988). *The Beginner's Guide to Colour Psychology*. London: Colour Affects Ltd.
- Yermack, D. (2013). Is bitcoin a real currency? an economic appraisal. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. <https://doi.org/10.1016/B978-0-12-802117-0.00002-3>
- Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: epistemological, theoretical, and methodological differences. *European Journal of Education, 48*(2). Retrieved from <https://pdfs.semanticscholar.org/f45f/993702833849749b3ddd83e1673728d569eb.pdf>
- Young M. R., (1981). The machine inside the machine: user's models of pocket calculators. *International Journal of Man-Machine Studies, 15*, 15–83.
- Young, J. (2016). Remittance-demanding countries dominate bitcoin searches in 2016. Retrieved April 5, 2019, from <https://news.Bitcoin.com/remittance-countries-Bitcoin-searches/>
- Young, J. (2017). Exponential growth: number of bitcoin users to reach 200 million by 2024. Retrieved April 1, 2019, from <https://www.ccn.com/exponential-growth-number-Bitcoin-users-reach-200-million-2024>
- Zanjani, A. V. (2004). Bitcoin exchanges as payment institutions testing the ground with an “indirect” form of regulation. Retrieved April 5, 2019, from <http://www.neopay.co.uk/wp-content/uploads/Diacle-Bitcoin-Regulation.pdf>
- Zhang, M., Sas, C., Lambert, Z. F., & Ahmad, M. (2019). Designing for the infrastructure of the supply chain of malay handwoven songket in terengganu. In *CHI Proceedings 2019*. ACM. Retrieved from <http://eprints.lancs.ac.uk/129626/>
- Zhe, K. S. K., Noordin, K. A., & Yong, M. (2016). How have they performed? Retrieved April 7, 2019, from <https://www.theedgemarkets.com/article/how-have-they-performed-part-1>

# Appendix A

The following are the ethics documentations for Study 1 and 2 (Chapter 4 and 5).

## INTERVIEW GUIDE 1 (Study 1 – Chapter 4)

### Exploring People's Attitudes and Use of Bitcoin Technology

**Interviewees** : Bitcoin Users

#### **INTRODUCTION**

1. Bitcoin activities are your hobby or it is your fulltime or part time income?
2. How did you learn about Bitcoin?
3. Did you attend any training on Bitcoin?
4. How long have you been using Bitcoin?
5. Why are you interested in Bitcoin? Which benefits did you experience or are expecting to experience?

#### **BITCOIN**

1. Can you please describe your understanding about Bitcoin technology?
2. Do you know how does the price of Bitcoins is controlled? Why?
3. Who is responsible to manage the price of Bitcoin?
4. In your opinion, are there any mechanisms to control the price of Bitcoin?
5. What are the challenges that you face when using or engaging with Bitcoin technology?
  - a. How secured do you perceive Bitcoin transaction to be? Why? Why not?
  - b. What do you think about the anonymity aspect of using Bitcoin? Why?
  - c. How much trust do you have in Bitcoin technology? Why? Why not?
  - d. Literature suggested that there is still people reluctance to use Bitcoin, what is your opinion?
  - e. Have you experienced any fraud in Bitcoin? If yes can you please describe?

#### **USER**

1. Do you have any IT background? If yes please describe.
2. Do you have any experience in financial or economic field? If yes please describe.
3. Do you have any experience in property/forex/others investment? If yes please describe.
4. What are the differences between Bitcoin and other forms of investment?
5. Do you think Bitcoin is a good investment? Why? Why not?
6. What are the motivational aspects that make you start to invest in or collect Bitcoins?
7. Have you connected with other Bitcoin users? If yes please describe.
8. Do you monitor the Bitcoins price? How?
9. When do you normally buy/sell your Bitcoins?
10. Can you describe your process of buying and selling Bitcoins?
11. How much trust you have in the exchange or personal seller? Why? Why not?

12. Do ever you verify their wallet id/account? How?
13. Have you encountered any fraud or problem while buying or selling Bitcoins?
14. How do you think the selling/buying process can be improved? How the Bitcoin technology can be improved to better support this process?

#### **WALLET**

1. How you create your wallet?
2. How do you manage it?
3. How secure you perceive your Bitcoins are secured in your wallet to be? Why? Why not?
4. Can the Bitcoins be stolen from your wallet? How?
5. How do you transfer your Bitcoins to local cash?
6. Do you verify your buyer's or seller's the wallet ID? How do you verify?
7. Have you experienced any loss of BTC from your wallet? If yes how did it happen? How could have been prevented?

#### **LEGISLATION**

1. Is Bitcoin technology legal? Which aspects are grey areas?
2. Have you heard any feedback from local banks about Bitcoin technology?
3. In your view, is mining a legal procedure?
4. Could the local banks or governments take any legal action against miners?
5. Based on literature, there are still government and policy makers who don't accept Bitcoin technology. Why do you think this is the case? What is your opinion on this view? Why?
6. Can you think of ways in which Bitcoin technology can become widely legal and accepted?

#### **SOCIAL & ECONOMY**

1. What are the impacts of Bitcoin technology on the world economy? Major benefits? Major risks?
2. What makes Bitcoin technology different from other local currencies?
3. What are the main challenges associated with Bitcoin technology? Can you think of ways of overcoming these challenges?
4. What are your future predictions towards this technology?

#### **DEMOGRAPHIC**

1. How old are you?
2. What is your highest level of education?
3. What is your current job?
4. For how long you have been a user?

## **INTERVIEW GUIDE 2 (Study 2 – Chapter 8)**

**Interviewees** : Bitcoin Miners

### **INTRODUCTION**

1. Bitcoin activities are your hobby or it is your fulltime or part time income?
2. How did you learn about Bitcoin?
3. Did you attend any training on Bitcoin?
4. How long have you been using Bitcoin?
5. Why are you interested in Bitcoin? Which benefits did you experience or are expecting to experience?

### **BITCOIN**

1. Can you please describe your understanding about Bitcoin technology?
2. Do you know how does the price of Bitcoins is controlled? Why?
3. Who is responsible to manage the price of Bitcoin?
4. In your opinion, are there any mechanisms to control the price of Bitcoin?
5. What are the challenges that you face when using or engaging with Bitcoin technology?
  - a. How secured do you perceive Bitcoin transaction to be? Why? Why not?
  - b. What do you think about the anonymity aspect of using Bitcoin? Why?
  - c. How much trust do you have in Bitcoin technology? Why? Why not?
  - d. Literature suggested that there is still people reluctance to use Bitcoin, what is your opinion?
  - e. Have you experienced any fraud in Bitcoin? If yes can you please describe?

### **MINER**

1. Did you invest any resources in becoming a miner? How much money? Time?
2. Why did you make this investment? Do you think it was a good investment? Why? Why not?
3. Is there any equipment need for mining? Can you describe?
  - a. If so, what is the cost of equipment?
  - b. What is the cost of its maintenance?
4. Can you please explain the mining process?
5. Do you monitor the mining process? How?
6. Do you have benefits or returns from each mining transactions? If so, what are they?
7. In average, within one day how much Bitcoins you earn from mining?
8. What are the motivational aspects for you to continue mining? Why?
9. Have you encountered any problem while mining? If yes, which ones it?
10. How do you think the mining process can be improved or better supported How the Bitcoin technology can be improved to better support this Process?
11. How do you estimate your trust in other miners and in the Bitcoin technology as a whole?
12. What is your opinion about selfish mining? What are the solutions?

### **LEGISLATION**

1. Is Bitcoin technology legal? Which aspects are grey areas?

2. Have you heard any feedback from local banks about Bitcoin technology?
3. In your view, is mining a legal procedure?
4. Could the local banks or governments take any legal action against miners?
5. Based on literature, there are still government and policy makers who do not accept Bitcoin technology. Why do you think this is the case? What is your opinion on this view? Why?
6. Can you think of ways in which Bitcoin technology can become widely legal and accepted?

### **SOCIAL & ECONOMY**

1. What are the impacts of Bitcoin technology on the world economy? Major benefits? Major risks?
2. What makes Bitcoin technology different from other local currencies?
3. What are the main challenges associated with Bitcoin technology? Can you think of ways of overcoming these challenges?
4. What are your future predictions towards this technology?

### **DEMOGRAPHIC**

1. How old are you?
2. What is your highest level of education?
3. What is your current job?
4. For how long you have been a miner?

# Research Ethics Approval for Study 1 and 2 from Universiti Teknologi MARA,

## Malaysia

www.utm.edu.my

**Fakulti Pengurusan Maklumat**  
Faculty of Information Management  
www.fpm.utm.edu.my

**Universiti Teknologi MARA**  
Kampus Puncak Perdana  
No.1, Jalan Pualau Angsa A U10/A  
Seksyen U10, 40150 Shah Alam  
Selangor, MALAYSIA  
Tel : (+603)-79622002/2020/2021/2023  
Fax : (+603)-79622007/2058



**Dekan**  
Prof Madya Dr Mohd Sazli Shahibi  
Tel : 03-79622001  
Emel : mohdsazli@salam.utm.edu.my

**Timbalan Dekan (Akademik)**  
Prof Madya Dr Norasiah Hj Harun  
Tel : 03-79622003  
E-mel : norasiah@salam.utm.edu.my

**Timbalan Dekan (Pelajar)**  
Prof Madya Dr Wan Ab Kadir Wan Dillah  
Tel : 03-79622004  
E-mel : wkadir@salam.utm.edu.my

**Timbalan Dekan  
(Jaringan Industri, Masyarakat & Alumni)**  
Tel : 03-79622047

#### KETUA PUSAT PENGAJIAN

**Pengurusan Perpustakaan**  
Dr Che Zanah Hj Abdullah  
Tel : 03-79622014  
Emel : cheza347@salam.utm.edu.my

**Pengurusan Pusat Sumber**  
Dr Shamila Mohamed Shubdan  
Tel : 03-79622012  
Emel : shamila@salam.utm.edu.my

**Pengurusan Sistem Maklumat**  
Enik Zaharudin Ibrahim  
Tel : 03-79622013  
E-mel : zahar347@salam.utm.edu.my

**Pengurusan Rekod**  
Dr Irwan Kamaruddin Abd Kadir  
Tel : 03-79622010  
E-mel : irwan@salam.utm.edu.my

**InED (e-PJ) & PLK**  
Enik Husain Hashim  
Tel : 03-55225311  
E-mel : husainha@salam.utm.edu.my

**Program Pasca Siwazah**  
Dr Dang Merdawati Hj Hashim  
Tel : 03-79622126  
Emel : dang@salam.utm.edu.my

#### KOORDINATOR PROGRAM SISWAZAH

**Sarjana Penyelidikan & Doktor Falsafah**  
Enik Ahmad Nazri Mansor  
Tel : 03-79622138  
E-mel : anazri@salam.utm.edu.my

**Sarjana Sains Kerja Kursus**  
Puan Masitah Ahmad  
Tel : 03-79622148  
E-mel : masitah@salam.utm.edu.my

**Sarjana Sains Pengurusan Maklumat  
(Kerja Kursus) (IM770-FLP)**  
Dr Mohd Razlan Abdul Kadir  
Tel : 03-79622011  
E-mel : mrazlan@salam.utm.edu.my

**Penolong Pendaftar (Pentadbiran)**  
Enik Mohd Kamal Mohamed Ner  
Tel : 03-79622005  
E-mel : kamal@salam.utm.edu.my

**Penolong Pendaftar (Akademik)**  
Enik Mohamad Zahid Ahmad  
Tel : 03-79622050  
E-mel : zahid@salam.utm.edu.my

Faculty of Information Management  
Universiti Teknologi MARA  
Research Ethics Committee  
Puncak Perdana Campus  
No 1 Jalan Pualau Angsa AU 10/A  
40150 Shah Alam Selangor  
MALAYSIA

#### Memorandum

**To:** Irni Eliana Binti Khairuddin  
**Cc:** Dr. Corina Sas  
School of Computing and Communication  
Lancaster University,  
Bailrigg, Lancaster LA1 4YW, United Kingdom  
**From:** Faculty of Information Management  
Universiti Teknologi MARA  
Research Ethics Committee  
**Date:** 1 September 2015  
**Subject:** 2015-1  
Development of Human Trust Information Architecture  
Model for Bitcoin Technology

The application for this project was considered and approved at the Faculty of Information Management, Research Ethics Committee meeting held on 16<sup>th</sup> June 2015.

Approval has been given for Mrs Irni Eliana Binti Khairuddin, under supervision of Dr Corina Sas, School of Computing and Communication, Lancaster University, United Kingdom to undertake this project from 1 September 2015 to 31 December 2015.

The approval given by the Faculty of Information Management, Research Ethics Committee is only for the project and the period stated. It is your responsibility to contact the Faculty of Information Management, Research Ethics Committee immediately should any of the following occur

- Serious or unexpected adverse effects on the participants
- Any proposed changes in the protocol, including extensions of time
- Any events which might affect the continuing ethical acceptability of the project
- The project is discontinued before the expected date of completion

- Modifications are requested by other than Faculty of Information Management, Research Ethics Committee

In addition you will be required to report on the progress of your project at least once at the conclusion of the project. Failure to report as required will result in suspension of your approval to proceed with this project.

Faculty of Information Management, Research Ethics Committee  
Universiti Teknologi MARA  
Telephone : +603-79622002/2020/2023

## **Research Ethics Approval for Study 1 and 2 from Lancaster University, UK**

19/07/2019

Stage 1 self assessment approval UREC reference RS2015-144 - Khairuddin, Irni

### Stage 1 self assessment approval UREC reference RS2015-144

#### Ethics (RSO) Enquiries

Tue 4/19/2016 1:13 PM

To: Khairuddin, Irni <i.khairuddin@lancaster.ac.uk>;

Cc: Sas, Corina <c.sas@lancaster.ac.uk>;

Dear Irni

Thank you for submitting your completed stage 1 self assessment form for **Exploring People's Attitudes and Use of Bitcoin Technology**. The Part B information has been reviewed by members of the University Research Ethics Committee and I can confirm that approval has been granted for this project.

*To note, as your project questionnaire indicates this project will involve making a prototype please can you contact Gavin Smith, Enterprise Services Division, phone 01524 593298 about this if you haven't already done so.*

As principal investigator your responsibilities include:

- ensuring that (where applicable) all the necessary legal and regulatory requirements in order to conduct the research are met, and the necessary licenses and approvals have been obtained;
- reporting any ethics-related issues that occur during the course of the research or arising from the research (e.g. unforeseen ethical issues, complaints about the conduct of the research, adverse reactions such as extreme distress) to the Research Ethics Officer;
- submitting details of proposed substantive amendments to the protocol to the Research Ethics Officer for approval.

Please contact the Research Ethics Officer, Debbie Knight ([ethics@lancaster.ac.uk](mailto:ethics@lancaster.ac.uk) 01542 592605 if you have any queries or require further information.

Kind regards,

*Debbie*

Debbie Knight | Research Ethics Officer | Email: [ethics@lancaster.ac.uk](mailto:ethics@lancaster.ac.uk) | Phone (01524) 592605 | Research Support Office, B58 Bowland Main, Lancaster University, LA1 4YT

Web: Ethical Research at Lancaster: <http://www.lancaster.ac.uk/depts/research/ethics.html>



[www.lancaster.ac.uk/50](http://www.lancaster.ac.uk/50)

*This e-mail and any attachment is for authorised use by the intended recipient(s) only. It may contain proprietary material, confidential information and/or be subject to legal privilege. It should not be copied, disclosed to, retained or used by, any other party. If you are not an intended recipient then please promptly delete this e-mail and any attachment and all copies and inform the sender. Thank you.*

# Appendix B

The following are the workshop guide for Study 3 and 4 (Chapter 7 and 8).

## WORKSHOP GUIDE (Study 3 –Chapter 7)

### Evaluating and Designing for Trust with BlocKit

**Participants** : Bitcoin Blockchain Experienced Users

<b>Session 1: Build up a Bitcoin Blockchain design kit</b>	
<b>Ice breaking</b>	<b>5 Mins</b>
<b>Task 1</b>	
Pretending that I am a novice Bitcoin user, verbally, can you explain a can you please explain a complete process of Bitcoins transaction. ( <i>i.e; wallet, miner, Blockchain, public key, private key and Bitcoin nodes</i> )	
<b>Follow up questions</b>	<b>10 Mins</b>
	<ol style="list-style-type: none"> <li>1. What object that you are trying to explain?</li> <li>2. How does it look like?</li> <li>3. How does it link from the previous object that you mentioned earlier?</li> </ol>
<b>Task 2</b>	
Pretending that I am a novice Bitcoin user, By using objects provided, can you please explain a complete process of Bitcoins transaction. ( <i>i.e; wallet, miner, Blockchain, public key, private key and Bitcoin nodes</i> )	
<b>Follow up questions</b>	<b>15 Mins</b>
	<ol style="list-style-type: none"> <li>1. Why you choose that object to represent the property?</li> <li>2. What are the characteristics of the property?</li> <li>3. What are the functions of the property?</li> <li>4. How does it work?</li> <li>5. Who are responsible to manage this property?</li> <li>6. Who else can view the property?</li> </ol>
<b>Assisting questions</b>	<p>Situation 1 – If the object is not the same as they imagined</p> <ol style="list-style-type: none"> <li>1. What type of object did you try to find?</li> <li>2. Can you see the object on the table?</li> <li>3. If no, how would you represent it?</li> <li>4. Why do you think this object is not working for you?</li> <li>5. What should be add or remove on this object</li> </ol> <p>Situation 2 – If the object is not exists</p> <ol style="list-style-type: none"> <li>1. What type of object did you try to find?</li> <li>2. Can you see the object on the table?</li> <li>3. If no, how would you represent it?</li> </ol>

	4. How does it work?	
<b>Wrapping up questions</b>	<ol style="list-style-type: none"> <li>1. In your opinion, in between this two methods, which method that you prefer to explain on the Bitcoin Blockchain activity? Why?</li> <li>2. Do you think that this design kit will help better understanding on Bitcoin Blockchain activity? Why?</li> <li>3. What are the advantages of this design kit?</li> <li>4. What are the disadvantages of this design kit?</li> <li>5. How to overcome the disadvantages?</li> </ol>	<b>5 Mins</b>

<b>Session 2: Bitcoin Blockchain Reputation Management System</b>		
<b>Task 1</b>		
<i>“Alice and Bob are both strangers. Alice requested for Bob to send her 1Btc to her Bitcoin’s wallet, and as a return, she will send £2000 to Bob’s bank account”</i>		
<b>Instruction 1</b>	Please complete the task by using the design kit from the previous session.	<b>5 Mins</b>
<b>Questions: Privacy</b>	<ol style="list-style-type: none"> <li>a. What is the best way for Alice to transfer the £2000 to Bob’s bank account? <ol style="list-style-type: none"> <li>a. How can she ensure that her identity is protected if she does it that way?</li> <li>b. Are there any way that she can protect her identity? How?</li> </ol> </li> <li>b. Should Alice generate a new wallet address to allow Bob to transfer the Bitcoin to her? <ol style="list-style-type: none"> <li>a. Reason for yes or no.</li> </ol> </li> </ol>	
<b>Instruction 2</b>	<p>These are the two types of token of trust. The green token is the sign trust, while red is for distrust. If I want to implement this token in this design kit:-</p> <ol style="list-style-type: none"> <li>1. Where should we place those tokens?</li> <li>2. How should it be used?</li> <li>3. Who should use the token?</li> <li>4. Who should manage the token?</li> <li>5. How to calculate the tokens?</li> <li>6. How the token can resembles the trust?</li> </ol>	<b>15 Mins</b>
<b>Task 2</b>		
<i>“John and Lisa are both strangers. John wants to purchase a notebook from Lisa. Lisa agrees to sell the notebook for 0.5Btc”</i>		
<b>Instruction 1</b>	Please complete the task by using the design kit from the previous session.	<b>10 Mins</b>
<b>Token of trust</b>	<ol style="list-style-type: none"> <li>1. How should the token of trust be placed in the following situations <ol style="list-style-type: none"> <li>a. John received and satisfied with the notebook. Lisa received the agreed amount of Bitcoins from John.</li> <li>b. John received and satisfied with the notebook. Lisa does not receive the correct amount of Bitcoins from John</li> <li>c. John received and satisfied with the notebook but Lisa does not receive any Bitcoins from John.</li> <li>d. John received but not satisfied with the notebook that he</li> </ol> </li> </ol>	

	received. Lisa received the agreed amount of Bitcoins from John e. John does not receive the notebook from Lisa but he already sends the agreed amount of Bitcoins to Lisa.	
<b>Wrapping up questions</b>	<ol style="list-style-type: none"> <li>1. Do you think that the token of trust can help to build the trust among the Bitcoin community?</li> <li>2. What are the advantages of this token system to the Bitcoin community?</li> <li>3. What are the disadvantages of this token to the Bitcoin community?</li> <li>4. Technically, do you think that it can be implemented? How?</li> </ol>	<b>5 Mins</b>
<b>Demographic Questions</b>	<ol style="list-style-type: none"> <li>1. How old are you?</li> <li>2. What is your highest level of education?</li> <li>3. What is your current job?</li> <li>4. For how long you have been engaging with Bitcoins?</li> </ol>	

**VALIDATION GUIDE (Study 4 – Chapter 8)**

**Validation for Trust Algorithms Design for Peer-to-Peer Bitcoins Transactions**

**Participants** : Bitcoin Blockchain Experienced Users

<b>Presentation of the algorithms (Chapter 8)</b>		<b>15 Mins</b>
<b>Follow up questions</b>	<ol style="list-style-type: none"> <li>1. What do you think about the algorithms?</li> <li>2. Are any parts of the algorithms that need to be revised? Why?</li> <li>3. What is your suggestion for the revise work?</li> <li>4. What are the requirements for the revise work?</li> </ol>	<b>15 Mins</b>

## **Research Ethics Approval for Study 3 and 4 from Lancaster University, UK**

19/07/2019

Ethics approval FSTREC ref: FST16153 - Khairuddin, Irni

Ethics approval FSTREC ref: FST16153

FST Ethics

Mon 6/5/2017 10:13 AM

To: Khairuddin, Irni <i.khairuddin@lancaster.ac.uk>;

Cc: Sas, Corina <c.sas@lancaster.ac.uk>;

Dear Irni,

Thank you for submitting your research ethics application for the project '**Towards Building a Trusted Bitcoin Technology Community**' for review. The application has been reviewed by members of the FST Research Ethics Committee and I can confirm that approval has been granted for this project.

As principal investigator your responsibilities include:

- ensuring that (where applicable) all the necessary legal and regulatory requirements in order to conduct the research are met, and the necessary licenses and approvals have been obtained;
- reporting any ethics-related issues that occur during the course of the research or arising from the research (e.g. unforeseen ethical issues, complaints about the conduct of the research, adverse reactions such as extreme distress) to the Research Ethics Officer;
- submitting details of proposed substantive amendments to the protocol to the Research Ethics Officer for approval.

Please contact the Research Ethics Officer, Becky Case ([fst-ethics@lancaster.ac.uk](mailto:fst-ethics@lancaster.ac.uk) 01542 593987) if you have any queries or require further information.

Kind regards,

Becky Case.

### **Becky Case**

Research Ethics Officer  
B33, Faculty of Science and Technology  
Lancaster University  
Lancaster  
LA1 4YR  
Tel: 01524 (5)93987  
E-mail: [fst-ethics@lancaster.ac.uk](mailto:fst-ethics@lancaster.ac.uk)

**Next FSTREC deadline 12 noon on Wednesday 28<sup>th</sup> June for the meeting on Thursday 13<sup>th</sup> July. There will be no committee meeting in August.**

<http://www.lancaster.ac.uk/sci-tech/research/ethics/>

 [Follow us on Twitter](#)

 [Find us on Facebook](#)



[www.lancaster.ac.uk](http://www.lancaster.ac.uk)

<https://outlook.office.com/owa/?ItemID=AAMkADhIN2kZDYzLWUzOTMINDdiZS1iNmFILTBjNW11NzY4ZTE3MQBGAAAAAABG8GZE31o5SYoP...> 1/1

# Appendix C

The following are the validation guide for the trust algorithms design for peer-to-peer Bitcoins transactions in Study 5 (Chapter 10).

## Trust Evaluation for Interface of BitXFps Bitcoin Mobile Wallet App (Study 5 – Chapter 10)

### EVALUATION GUIDE

**Participants** : Bitcoin Users

<b>Ice breaking</b>	<b>5 Mins</b>
Each of you needs to choose a role as a seller, buyer or witness.	<b>10 Mins</b>
<p><b>Explanations on the app</b></p> <ol style="list-style-type: none"> <li>1. Create the wallet account</li> <li>2. Getting around the app             <ol style="list-style-type: none"> <li>a. My BitXFps</li> <li>b. Reputation</li> <li>c. Send/receive Bitcoins</li> <li>d. Trade</li> <li>e. Scan QR</li> <li>f. Preference</li> <li>g. Help</li> <li>h. About</li> </ol> </li> <li>3. Buying             <ol style="list-style-type: none"> <li>a. List of Bitcoins to sell</li> </ol> </li> <li>4. Selling             <ol style="list-style-type: none"> <li>a. List of Bitcoins to buy</li> </ol> </li> <li>5. Merchant             <ol style="list-style-type: none"> <li>a. List of items to sell</li> </ol> </li> </ol>	
<b>Task 1</b>	
<p>By using BitXFps app, create an honest Bitcoins transactions by selling the 0.0779 BTC for the price of 500USD</p> <ol style="list-style-type: none"> <li>1. Buyer (Request a trade)</li> <li>2. Seller (Create a contract)</li> <li>3. Witness (Receive invitation)</li> </ol>	<b>5 Mins</b>

<b>Task 2</b>		<b>5 Mins</b>
<p>By using BitXFps app, create a dishonest Bitcoins transactions (Buyer did not make the fiat money payment through the bank) by selling the 0.0779 BTC for the price of 500USD</p> <ol style="list-style-type: none"> <li>1. Buyer (Request a trade)</li> <li>2. Seller (Create a contract)</li> <li>3. Witness (Receive invitation &amp; manage dispute)</li> </ol>		
<b>Task 3</b>		<b>5 Mins</b>
<p>By using BitXFps app, create an honest transactions to purchase a laptop with the price of BTC 0.0161</p> <ol style="list-style-type: none"> <li>1. Buyer (Request a trade)</li> <li>2. Seller (Create a contract)</li> <li>3. Witness (Receive invitation)</li> </ol>		
<b>Task 4</b>		<b>5 Mins</b>
<p>By using BitXFps app, create a dishonest transactions (buyer receives a broken laptop) to purchase a laptop with the price of BTC 0.0161</p> <ol style="list-style-type: none"> <li>1. Buyer (Request a trade)</li> <li>2. Seller (Create a contract)</li> <li>3. Witness (Receive invitation &amp; manage dispute)</li> </ol>		
<b>Filling up the heuristic evaluation forms</b>		<b>5 Mins</b>
<b>Follow-up Questions</b>	<p>Graphic design</p> <ol style="list-style-type: none"> <li>1. What choice of colors that can boost the trust?</li> <li>2. What do you think about the arrangement of the app’s layout</li> <li>3. What type of photos should be include in the app increase the trust?”</li> </ol> <p>Structure design</p> <ol style="list-style-type: none"> <li>1. Are there any important functions that are not included in the app?</li> <li>2. Do you find any difficulties to navigate the functions within the app?</li> </ol> <p>Content design</p> <ol style="list-style-type: none"> <li>1. Do you think that security signs are good for trust?</li> <li>2. What else can help to increase trust through the image and branding for the app?</li> <li>3. What additional contents are relevant to encourage trust that needs to be include in the app?</li> </ol> <p>Personal and social proof</p> <ol style="list-style-type: none"> <li>1. Do you think the social media pages could help to increase the personal and social proofs?</li> </ol> <p>Social-cue design</p>	<b>20 Mins</b>

	<ol style="list-style-type: none"> <li>1. Do you have any suggestions to improve the social-cue for the app?</li> </ol> <p>Peer-to-peer transactions cue design</p> <ol style="list-style-type: none"> <li>1. Do you think that the transparency of the transaction could improve the trust?</li> <li>2. Do you agree that the agreements between buyer and seller should be include in a contract will facilitate the trust?”,</li> <li>3. Do you think the witness is a good mediator to mitigate the trust of the transaction?</li> <li>4. Do you agree that the user’s reputation design could assist the trust of the transaction?</li> </ol>	
<b>Demographic Questions</b>	<ol style="list-style-type: none"> <li>1. How old are you?</li> <li>2. What is your highest level of education?</li> <li>3. What is your current job?</li> </ol>	

## Research Ethics Approval for Study 5 from Lancaster University, UK

19/07/2019

Ethics approval FSTREC ref: FST17163 - Khairuddin, Irni

Ethics approval FSTREC ref: FST17163

FST Ethics

Wed 9/19/2018 9:51 AM

To: Khairuddin, Irni <i.khairuddin@lancaster.ac.uk>;

Cc: Sas, Corina <c.sas@lancaster.ac.uk>;

Dear Irni,

Thank you for submitting your research ethics application for the project '**Towards Building a Trusted Bitcoin Technology Community**' for review. The application has been reviewed by members of the FST Research Ethics Committee and I can confirm that approval has been granted for this project.

As principal investigator your responsibilities include:

- ensuring that (where applicable) all the necessary legal and regulatory requirements in order to conduct the research are met, and the necessary licenses and approvals have been obtained;
- reporting any ethics-related issues that occur during the course of the research or arising from the research (e.g. unforeseen ethical issues, complaints about the conduct of the research, adverse reactions such as extreme distress) to the Research Ethics Officer;
- submitting details of proposed substantive amendments to the protocol to the Research Ethics Officer for approval.

Please contact the Research Ethics Officer, Becky Case ([fst-ethics@lancaster.ac.uk](mailto:fst-ethics@lancaster.ac.uk) 01542 593987) if you have any queries or require further information.

Kind regards,

Becky Case

### **Becky Case**

Research Ethics Officer – FST & FHM  
B14, Faculty of Health and Medicine, Mon&Tue  
B33, Faculty of Science and Technology, Wed,Thur&Fri  
Lancaster University  
Lancaster  
LA1 4YR  
Tel: 01524 (5)93987  
E-mail: [fhmresearchsupport@lancaster.ac.uk](mailto:fhmresearchsupport@lancaster.ac.uk), [fst-ethics@lancaster.ac.uk](mailto:fst-ethics@lancaster.ac.uk)

<http://www.lancaster.ac.uk/fhm/research/research-ethics/>

<http://www.lancaster.ac.uk/sci-tech/research/ethics/>



[Follow us on Twitter](#)



[Find us on Facebook](#)

<https://outlook.office.com/owa/?ItemID=AAMkADhIN2ZkZDYzLWUzOTMNDdIZS1INmFILTBJNW11NzY4ZTE3MQBGAAAAAABG8GZE31o5SYoP...> 1/2

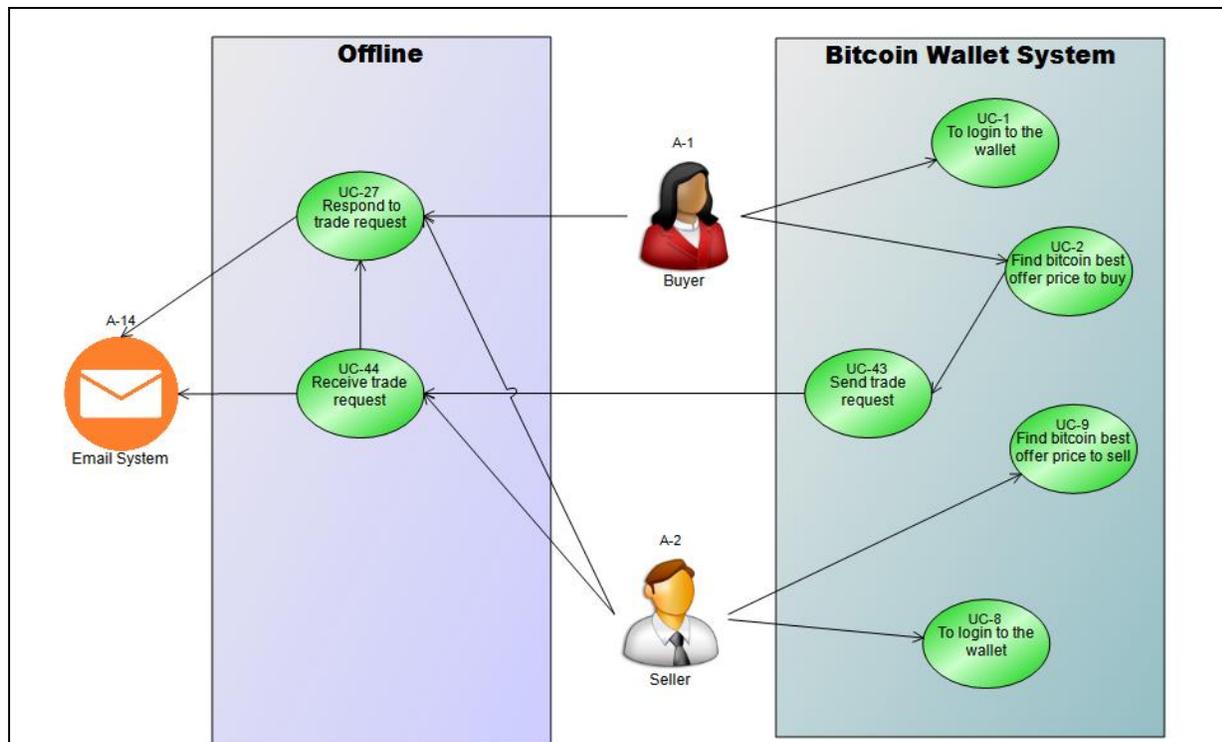
# Appendix D

The following are the detailed trust algorithms for Bitcoin peer-to-peer transactions.

## a. Step 1: Pre Transaction between Buyer and Seller

The first step is explaining on the preliminary interactions between seller and buyer through the system. At this stage, buyer and seller are required to create a Bitcoin wallet in order to allow them to interact with the system. The buyer and seller may begin to initiate a transaction by finding a suitable trader to either sell or buy Bitcoins from the system. They may browse the Bitcoin price, including the details of the traders, such as reputation tokens. If they found a suitable trader, they may send a trade request and make further discussions and negotiations for the transaction through email. The processes involved are further described in the Use Case Diagram in **Table and Figure A.**

<b>Primary Actor:</b>	{A-1- Buyer}; {A-2-Seller}
<b>Secondary Actor</b>	{A-14-Email System}
<b>Use Cases:</b>	<p><i>Valid wallet account:</i> {UC-1 - To login the wallet (Buyer)}; { UC-8 - To login the wallet (Seller)}</p> <p><i>Browsing the Bitcoin price advertisements:</i> {UC-2 – Find the best offer price to buy}; {UC-9 – Find the best offer price to sell}</p> <p><i>Initiate pre Bitcoin transaction:</i> {UC-43-Send trade request};{UC-44-Receive trade request};{UC-27-Respond to trade request};</p>



**Figure A: Case Diagram for Pre Transaction between Buyer and Seller**

<b>Valid wallet account</b>	
<b>UC-1 - To login to the wallet (Buyer)</b>	
<b>Pre-conditions</b>	The Buyer must have a valid wallet ID
<b>Success Guarantee</b>	The Buyer's wallet ID is successfully verified
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Buyer chooses to log in to the wallet</li> <li>2. System asks Buyer valid passcode</li> <li>3. Buyer tells the system her passcode <i>*to refer extensions 3.a and 3.b</i></li> <li>4. System verifies Buyer's passcode</li> <li>5. System tells Buyer her passcode is valid <i>*to refer extensions 5.a</i></li> <li>6. Buyer says OK to the system</li> <li>7. System shows the Buyer the main screen</li> <li>8. Use case continues at UC-2</li> </ol>
<b>Extensions</b>	<ol style="list-style-type: none"> <li>3.a Buyer chooses to create a new wallet account               <ol style="list-style-type: none"> <li>1. System gives 12-word phrases and asks Buyer to write down those words and keep for future wallet recovery</li> <li>2. System asks Buyer to enter the 12 words</li> <li>3. Buyer keys in all the 12 words</li> <li>4. System tells the buyer the 12 words are correct                   <ol style="list-style-type: none"> <li>4.1. If the system tells the buyer the 12 words are incorrect</li> <li>4.2. Use case repeats at step 3.a.2</li> </ol> </li> <li>5. System asks Buyer to create 6 digit passcode</li> <li>6. Buyer creates 6-digit passcode</li> <li>7. System asks Buyer to re-enter the passcode</li> <li>8. Buyer re-enters the passcode</li> <li>9. System verifies the passcode</li> <li>10. system tells Buyer the passcode is valid</li> </ol> </li> </ol>

	<p>10.1. If the passcode is invalid  10.2. Use case repeats at step 3.a.6  11. Buyer says OK to the system  12. Use case continues as step 7</p>
	<p>3.b Buyer chooses to restore her wallet  1. Use case continues at 3.a.2</p>
	<p>5.a System tells Buyer her passcode is invalid  1. System tells Buyer to re-enter the passcode  2. Buyer re-enters the passcode  3. System verifies the passcode  3.1. If the passcode is valid, use case continues at step 5  3.2. If the passcode is invalid, use case repeats step 5.a</p>
<p><b>Valid wallet account</b>  <b>UC-8 - To login to the wallet (Seller)</b></p>	
<b>Pre-conditions</b>	The Seller must have a valid wallet ID
<b>Success Guarantee</b>	The Seller's wallet ID is successfully verified
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Seller chooses to log in to the wallet</li> <li>2. System asks the Seller valid passcode</li> <li>3. Seller tells the system his passcode <i>*to refer extensions 3.a and 3.b</i></li> <li>4. System verifies the Seller passcode</li> <li>5. System tells the Seller his passcode is valid <i>*to refer extensions 5.a</i></li> <li>6. Seller says OK to the system</li> <li>7. System shows the Seller the main screen</li> <li>8. Use case continues at step UC-9</li> </ol>
<b>Extensions</b>	<p>3.a Seller chooses to create new wallet account</p> <ol style="list-style-type: none"> <li>1. System gives 12-word phrases and asks Seller to write down those words and keep for future wallet recovery</li> <li>2. System asks Seller to enter the 12 words</li> <li>3. Seller keys in all 12 words</li> <li>4. System tells Seller the 12 words are correct <ol style="list-style-type: none"> <li>4.1. If System tells Seller the 12 words are incorrect</li> <li>4.2. Use case repeats step 3.a.2</li> </ol> </li> <li>5. System asks Seller to create 6 digit passcode</li> <li>6. Seller creates a 6-digit passcode</li> <li>7. System asks Seller to re-enter the passcode</li> <li>8. Seller re-enters the passcode</li> <li>9. System verifies the passcode</li> <li>10. System tells Seller the passcode is valid <ol style="list-style-type: none"> <li>10.1. If passcode invalid,</li> <li>10.2. Use case repeats step 3.a.6</li> </ol> </li> <li>11. Seller says OK to the system</li> <li>12. Use case continues as step 7.</li> </ol> <p>3.b Seller chooses to restore her wallet  1. Use case continues at 3.a.2</p> <p>5.a System tells Seller his passcode is invalid</p> <ol style="list-style-type: none"> <li>1. System tells Seller to re-enter the passcode</li> <li>2. Seller re-enters the passcode</li> <li>3. System verifies the passcode</li> </ol>

	<p>3.1. If passcode valid, use case continues at step 5</p> <p>3.2. If passcode invalid, use case repeats step 5.a</p>
<p><b>Browsing the Bitcoin Price Advertisement</b></p> <p><b>UC-2 – Find Bitcoin best offer price to buy</b></p>	
<b>Pre-conditions</b>	Buyer must log in to the wallet
<b>Success Guarantee</b>	Buyer's wallet ID is verified
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Buyer chooses to enter the options for Buyer</li> <li>2. System shows a list of Bitcoin price to sell by Sellers</li> <li>3. Buyer chooses the best offer price and click Buy</li> <li>4. System shows the details of the Seller <ol style="list-style-type: none"> <li>4.1. reputation score</li> <li>4.2. Bitcoin selling price</li> <li>4.3. payment method</li> <li>4.4. trade limit</li> <li>4.5. payment window</li> <li>4.6. Additional description</li> </ol> </li> <li>5. System asks Buyer the amount of Bitcoin to buy</li> <li>6. Buyer enters the amount of Bitcoin to buy</li> <li>7. Buyer chooses to send the trade request to Seller</li> <li>8. System send the trade request to Seller</li> <li>9. Use case continues at UC-43</li> </ol>
<b>Extensions</b>	NIL
<p><b>Browsing the Bitcoin Price Advertisement</b></p> <p><b>UC-9 – Find Bitcoin best offer price to sell</b></p>	
<b>Pre-conditions</b>	Seller must log in to the wallet
<b>Success Guarantee</b>	Seller's wallet ID is verified
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Seller chooses to enter the options for Seller</li> <li>2. System shows a list of Bitcoin price to buy by Buyers</li> <li>3. Seller choose the best offer price and click sell</li> <li>4. System shows the details of the Seller <ol style="list-style-type: none"> <li>4.1. reputation score</li> <li>4.2. Bitcoin selling price</li> <li>4.3. payment method</li> <li>4.4. trade limit</li> <li>4.5. payment window</li> <li>4.6. Additional description</li> </ol> </li> <li>5. System asks Seller the amount of Bitcoin to sell</li> <li>6. Seller enters the amount of Bitcoin to sell</li> <li>7. Seller chooses to send the trade request to Buyer</li> <li>8. System send the trade request to Buyer</li> <li>9. Use case continues at UC-43</li> </ol>
<b>Extensions</b>	NIL
<p><b>Initiate Pre Bitcoin Transaction</b></p> <p><b>UC-43-Send trade request</b></p> <p><i>(e.g. Buyer initiates a request trade with Seller)</i></p>	
<b>Pre-conditions</b>	Buyer sends the trade request to Seller
<b>Success Guarantee</b>	Seller must receive the trade request in his Email System
<b>Main Success</b>	<ol style="list-style-type: none"> <li>1. System asks Buyer the amount of Bitcoin to buy</li> </ol>

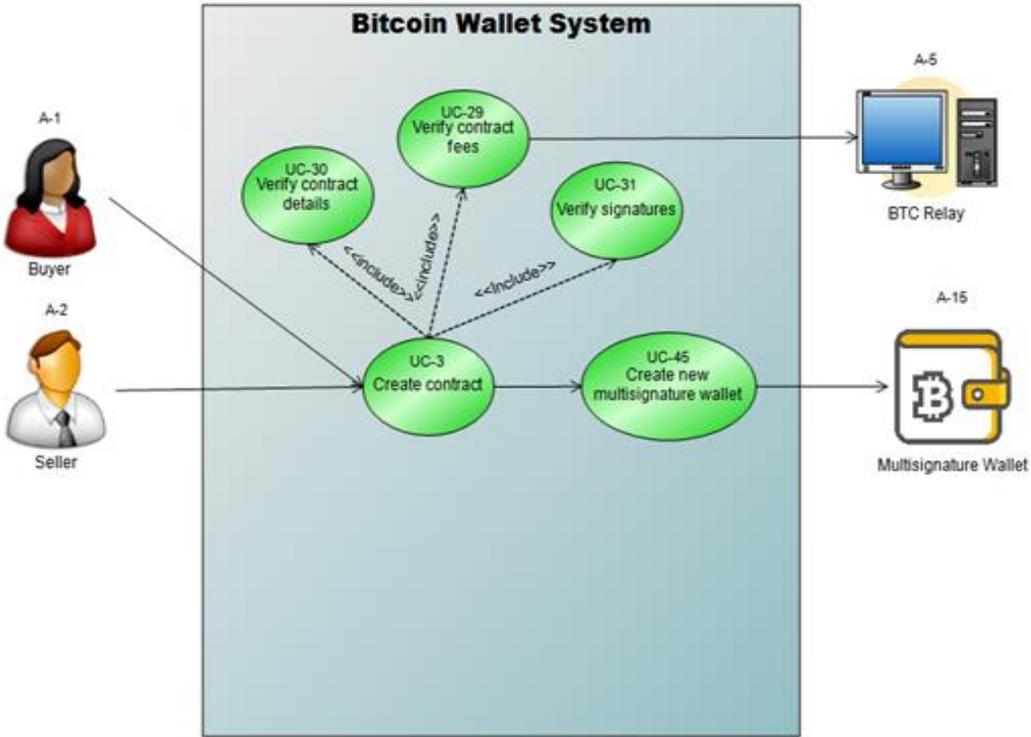
<b>Scenario</b>	<ol style="list-style-type: none"> <li>2. Buyer enters the amount of Bitcoin to buy</li> <li>3. System asks if Buyer want to request the trade to the Seller</li> <li>4. Buyer tells the system that she agrees to send the request to trade</li> <li>5. The system sends the trade request to Seller's registered email system</li> <li>6. Use case continues at UC-44</li> </ol>
<b>Extensions</b>	NIL
<b>Initiate Pre Bitcoin Transaction</b> <b>UC-44-Receive trade request</b> <i>(e.g. Buyer initiates a request trade with Seller)</i>	
<b>Pre-conditions</b>	NIL
<b>Success Guarantee</b>	NIL
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Seller receives email for trade request from Buyer</li> <li>2. Use case continues at UC-27</li> </ol>
<b>Extensions</b>	NIL
<b>Initiate Pre Bitcoin Transaction</b> <b>UC-27 – Respond to trade request</b> <i>(e.g. Buyer initiates a request trade with Seller)</i>	
<b>Pre-conditions</b>	Trade request is sent to Seller's email
<b>Success Guarantee</b>	Seller must receive the trade request email from buyer
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Seller receives trade request from Buyer</li> <li>2. Seller sends email to Buyer about the details of the transaction <i>(payment time, offline payment method, type of offline proof, multisignature wallet, contract fee, Trust token fee, Witness for the transactions and Witness token fee for Witness)</i></li> <li>3. Buyer replies to Seller email to agree with the details * to refer extensions 3.a</li> <li>4. Use case continues at <b>Step 2: Create a Valid Contract for the Transaction</b></li> </ol>
<b>Extensions</b>	3.a Buyer reply to Seller email to negotiate on some of the details for the transaction <ol style="list-style-type: none"> <li>1. Seller replies to Buyer's email to agree with the negotiations <ol style="list-style-type: none"> <li>1.1. If Seller replies to Buyer email to not agree with the negotiations the transaction is void.</li> <li>1.2. Use case End</li> </ol> </li> <li>2. Use case continues at step 4</li> </ol>
	Buyer reply to Seller's email to not agree with the details <ol style="list-style-type: none"> <li>1. Transaction is void</li> <li>2. Use case End</li> </ol>

**Table A: Use Cases Details for Pre-Transaction between Seller and Buyer**

**b. Step 2: Create a Valid Contract for the Transaction**

The second step describes the algorithms to create a valid agreement between buyer and seller in a smart contract. The agreements details are including the Bitcoin price, method for offline payment, types of evidence for the offline payment, contract fee, witness, multisignature wallet, trust token fee, and witness token fee. They write the contract based on those agreed details. The processes involved are further described in the Use Case Diagram in **Table and Figure B**.

<b>Primary Actor:</b>	{A-1- Buyer}; {A-2-Seller}
<b>Secondary Actor</b>	{A-5-BTC Relay}
<b>Use Cases:</b>	<p><i>Creating contract:</i></p> <p>{UC-3 – Verifying Create contract}; {UC-30 – Verifying Contract details}; {UC-31 – Verifying Signature}; {UC-29- Verifying Contract fee}</p> <p><i>Contract output:</i></p> <p>{UC-45- Create New Multisignature wallet}</p>



**Figure B: Case Diagram for Creating a Valid Contract between Buyer and Seller**

<b>Creating a contract</b>	
<b>UC-3 – Create a contract</b>	
<b>Pre-conditions</b>	Write details of the contract agreed by Seller and Buyer
<b>Success Guarantee</b>	Signed by Seller and Buyer and paid contract fee
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Seller chooses the option from the main screen to create multisignature wallet</li> <li>2. System asks Seller to give a name for the wallet</li> <li>3. Seller tells the system the name of the wallet</li> <li>4. System tells the Seller the name and the address of the wallet</li> <li>5. Seller says OK</li> <li>6. System asks Seller to write the contract</li> <li>7. Seller writes the Contract details (UC-30) as previously agreed by Buyer</li> <li>8. Seller confirms the Contract details (UC-30) to the system</li> <li>9. Seller sends the multisignature wallet address to Buyer’s email</li> <li>10. Buyer joins the contract * to refer extensions 10.a</li> <li>11. System shows Buyer the Contract details (UC-30) written by Seller</li> </ol>

	12. Buyer tells the system that she agrees with the contract * <i>to refer extensions 12.a</i> 13. System asks Buyer and Seller to pay Contract fee (UC-29) 14. Buyer and Seller pay the Contract fee (UC-29) in Bitcoin 15. System asks Buyer and Seller to sign the contract 16. Buyer and Seller sign the contract (UC-30) 17. Use case continues at UC-45
<b>Extensions</b>	10.a Buyer decline to join the contract 1. Use case Ends
	12.a Buyer did not agree with the contract 1. Buyer makes changes on the Contract details (UC-30) 2. Buyer confirms the changes to the system 3. System asks the seller about the changes made by Buyer 4. Seller tells the system that he agrees with the changes 4.1. If the seller tells the system that he does not agree with the changes 4.2. Contract is void 4.3. Use case Ends 5. Use case continues at step 14
<b>Creating a Contract</b> <b>UC-30 – Verifying Contract Details</b>	
<b>Pre-conditions</b>	Mutual agreement between Buyer and Seller as discussed through email
<b>Success Guarantee</b>	Includes all the details of the agreement in the contract
<b>Main Success Scenario</b>	1. Verify the contract details 2. Use case continues at UC-3
<b>Extensions</b>	<i>NIL</i>
<b>Creating a Contract</b> <b>UC-31 – Verifying Signature</b>	
<b>Pre-conditions</b>	Buyer and Seller must both agree with the contract details
<b>Success Guarantee</b>	Buyer and Seller signed the contract
<b>Main Success Scenario</b>	1. System verifies Buyer and Seller's signature 2. Use case continues at UC-3
<b>Extensions</b>	<i>NIL</i>
<b>Creating a Contract</b> <b>UC-29 – Verifying Contract Fees</b>	
<b>Pre-conditions</b>	Buyer and Seller agree to bear the contract fee
<b>Success Guarantee</b>	Paid the contract fee
<b>Main Success Scenario</b>	1. Verify the contract details 2. Use case continues at UC-3 3.
<b>Extensions</b>	<i>NIL</i>

<b>Contract Output</b> <b>UC-45 – Create New Multisignature Wallet</b>	
<b>Pre-conditions</b>	Multisignature wallet must be specified as an output of the contract
<b>Success Guarantee</b>	The contract must be created and verified
<b>Main Success Scenario</b>	<i>NIL</i>
<b>Extensions</b>	<i>NIL</i>

**Table B: Use Cases Details for Creating Valid Contract for the Transaction between Seller and Buyer**

**c. Step 3: Enacting the Bitcoin Transactions**

The third step describes the processes of buyer sends Bitcoin to the multisignature wallet. The buyer and seller also send the token fees as stated in the contract to the same wallet. Those Bitcoin payments will be verified by BTC Relay to ensure that the Bitcoin payments are support the Ethereum smart contract. An independent user is also randomly invited to join the contract as a witness for the transaction. The processes involved are further described in the Use Case Diagram in **Table and Figure C.**

<b>Primary Actor:</b>	{ A-1- Buyer}; { A-2-Seller}
<b>Secondary Actor:</b>	{ A-3 – Witness}; { A-5 – BTC-Relay};{ A-15 – Multisignature wallet}
<b>Use Cases:</b>	<p><i>Sending Bitcoins:</i> { UC-32 – Send Trust and Witness token fees}; { UC-11 – Send Bitcoin for buyer }</p> <p><i>Bridging Bitcoin with ethereum smart contract:</i> { UC-47 – To verify the Bitcoins }</p> <p><i>Updating Multisignature Wallet:</i> { UC-46– Contract receives the Bitcoins}; { UC-50– Update signature for multisignature wallet }</p> <p><i>Witnessing the transaction</i> { UC-49 – Invite user as a witness}; { UC-16 – Respond to the invitation }</p>

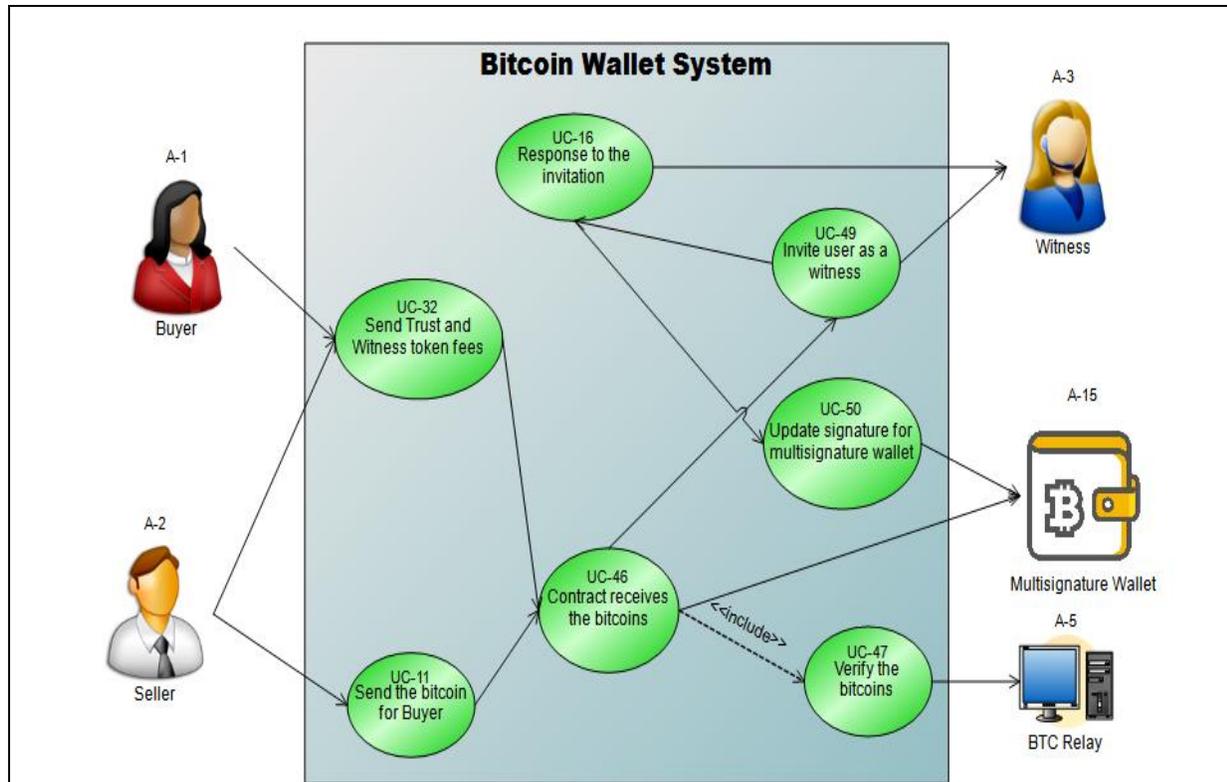


Figure C: Case Diagram for Enacting Bitcoin Transactions

<b>Sending Bitcoin</b>	
<b>UC-32 – Send Trust and Witness token fees</b>	
<b>Pre-conditions</b>	Buyer and seller send the token fees
<b>Success Guarantee</b>	The amount of token fees must be received as stated in the contract in the multisignature wallet.
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Seller and Buyer send the fee for the tokens as stated in the contract to the system</li> <li>2. Seller and buyer sign their personal wallet to proceed with the actions</li> <li>3. Use case continues at UC-46</li> </ol>
<b>Extensions</b>	<i>NIL</i>
<b>Sending Bitcoin</b>	
<b>UC-11 – Send Bitcoins for the buyer</b>	
<b>Pre-conditions</b>	Seller sends Bitcoins for the buyer to the multisignature wallet
<b>Success Guarantee</b>	The number of Bitcoins received in the multisignature wallet must be matched with the amount stated in the contract
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Seller sends the amount of Bitcoin to sell as stated in the contract to the system</li> <li>2. Seller signs his personal wallet to proceed with the action</li> <li>3. Use case continues at UC-46</li> </ol>
<b>Extensions</b>	<i>NIL</i>
<b>Bridging Bitcoin with Ethereum Smart Contract:</b>	
<b>UC-47 – To verify the Bitcoin</b>	
<b>Pre-conditions</b>	System send Bitcoin to BTC Relay
<b>Success Guarantee</b>	BTC relay must receive Bitcoin from system

<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. System sends the payment details to BTC Relay to verify the Bitcoin</li> <li>2. System receives a notification from BTC Relay that the Bitcoin is verified</li> <li>3. Use case continues at UC-46</li> </ol>
<b>Extensions</b>	<i>NIL</i>
<b>Updating Multisignature Wallet</b> <b>UC-46– Contract receives the Bitcoins</b>	
<b>Pre-conditions</b>	Seller and Buyer sends the Bitcoins, and token fees as agreed in the contract
<b>Success Guarantee</b>	Multisignature Wallet must receive all Bitcoins and token fees as agreed in the contract
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. System verifies the number of Bitcoins received based on the contract</li> <li>2. System confirms the amount of Bitcoins send by seller are accurate * <i>to refer extensions 2.a</i></li> <li>3. System confirms the amount of token fees send by the seller are accurate * <i>to refer extensions 3.a</i></li> <li>4. System confirms the amount of token fees send by the buyer are accurate * <i>to refer extensions 4.a</i></li> <li>5. System stores the verified Bitcoins and token fees in the Multisignature Wallet</li> <li>6. Use case continues at UC-49</li> </ol>
<b>Extensions</b>	<ol style="list-style-type: none"> <li>2.a If the amount of Bitcoin sent by the seller are inaccurate <ol style="list-style-type: none"> <li>1. System asks the seller to make an additional payment</li> <li>2. Seller says OK to the system <ol style="list-style-type: none"> <li>2.1. If Seller does not agree</li> <li>2.2. The remaining Bitcoins will be returned to the respective sender</li> <li>2.3. Contract end</li> </ol> </li> <li>3. Use case continues at UC-11</li> </ol> </li> <li>3.a If the amount of token fees send by Seller are inaccurate <ol style="list-style-type: none"> <li>1. System asks the seller to make an additional payment</li> <li>2. Seller says OK to the system <ol style="list-style-type: none"> <li>2.1. If Seller does not agree</li> <li>2.2. The remaining Bitcoins will be returned to the respective sender</li> <li>2.3. Contract end</li> </ol> </li> <li>3. Use case continues at UC-32</li> </ol> </li> <li>4.a If the amount of token fees sent by Buyer is inaccurate <ol style="list-style-type: none"> <li>1. System asks Buyer to make an additional payment</li> <li>2. Buyer says OK to the system <ol style="list-style-type: none"> <li>2.1. If Buyer does not agree</li> <li>2.2. The remaining Bitcoins will be returned to the respective sender</li> <li>2.3. Contract end</li> </ol> </li> <li>3. Use case continues at UC-32</li> </ol> </li> </ol>
<b>Updating Multisignature Wallet</b> <b>UC-50– Update signature for multisignature wallet</b>	
<b>Pre-conditions</b>	An independent valid user willing to be a witness
<b>Success Guarantee</b>	The valid user must sign the contract
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. System updates the witness signature to be associated with the multisignature wallet</li> <li>2. System changes the Multisignature Wallet signature requirements from 2 of 2 to 2 of 3.</li> <li>3. System shows Witness the complete pseudoanonymous contract between seller and buyer</li> <li>4. Use case continues at <i>Step 4: Enacting Offline Transaction</i></li> </ol>
<b>Extensions</b>	<i>NIL</i>

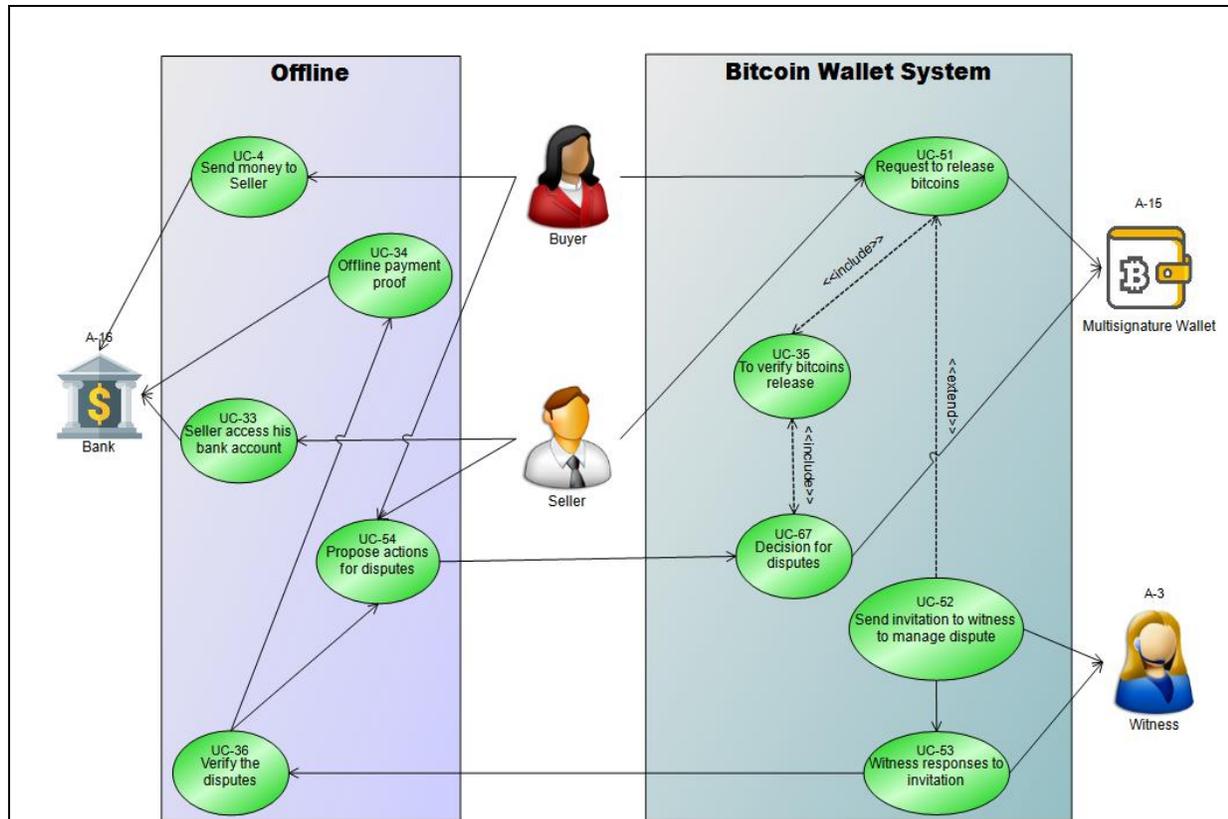
<b>Witnessing the transaction UC-49 – Invite user as a witness</b>	
<b>Pre-conditions</b>	Seller and Buyer must send the Bitcoins and the tokens fees
<b>Success Guarantee</b>	Bitcoins and fees are available in the multisignature wallet
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. System randomly sends an invitation to a user that has a valid wallet ID to join the multisignature wallet as the witness for the transaction</li> <li>2. The system shows the summary of the contract (UC-30) between Seller and Buyer anonymously (including the buyer and seller wallet ID)</li> <li>3. Use case continues at UC-16</li> </ol>
<b>Extensions</b>	<i>NIL</i>
<b>Witnessing the transaction UC-16 – Response to the Invitation</b>	
<b>Pre-conditions</b>	Agree with the conditions stated in the contract
<b>Success Guarantee</b>	Signed the contract
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. The system receives a notification of acceptance from the invited wallet ID as the witness * to refer extensions 1.a</li> <li>2. System asks the wallet ID to sign the contract as a witness</li> <li>3. The wallet ID signs the contract</li> <li>4. Use case continues at UC-50</li> </ol>
<b>Extensions</b>	<ol style="list-style-type: none"> <li>1.a If system receives a notification of decline from the invited wallet ID as the witness <ol style="list-style-type: none"> <li>1. Use case continues at UC-49</li> </ol> </li> </ol>

**Table C: Use Cases Details for Enacting the Bitcoin Transaction**

**d. Step 4: Enacting Offline Transaction**

The fourth step describes the process of buyer sending the fiat money to the seller’s bank account. The proof of offline payment is essential evidence for the transaction. Once the offline payment is made, the buyer will request to release the Bitcoins from the multisignature wallet as well as the seller will also sign to release the Bitcoins to the buyer. However, if one of the signatures is not received on the multisignature wallet, the witness will be invited to facilitate and make a decision for the dispute based on the proofs for the transactions. The processes involved are further described in the Use Case Diagram in **Figure and Table D.**

<b>Primary Actor:</b>	{A-1- Buyer}; {A-2-Seller}
<b>Secondary Actor:</b>	{A-3- Witness}; {A-5 – BTC-Relay};{A-15 – Multisignature wallet}
<b>Use Cases:</b>	<p><i>Sending money:</i> {UC-4 – Send money to seller}; { UC-33 – Seller bank account}; { UC-34 – Offline payment proof}</p> <p><i>Updating Multisignature Wallet:</i> {UC-54 – Request to release Bitcoins};{UC-35- To verify Bitcoins release}; {UC-67 – Decision for disputes}</p> <p><i>Managing disputes</i> {UC-52 – Send invitations to witness to manage disputes}; {UC-53 – Witness responses to the invitations}; {UC-36- Verify the disputes}</p>



**Figure D: Case Diagram for Enacting Offline Transaction**

<b>Sending Money</b>	
<b>UC-4 – Send money to the seller</b>	
<b>Pre-conditions</b>	The amount of money sent must be accurate as stated in the contract to the correct bank account number
<b>Success Guarantee</b>	The money must be received in the Seller’s bank account
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Buyer sends the amount of agreed fiat money as stated in the contract (UC-30)</li> <li>2. Buyer sends the money to the bank account number as stated in the contract (UC-30)</li> <li>3. Use case continues at step UC-33</li> </ol>
<b>Extensions</b>	<i>NIL</i>
<b>Sending Money</b>	
<b>UC-33 – Seller bank account</b>	
<b>Pre-conditions</b>	The amount of money sent must be accurate as stated in the contract to the correct bank account number
<b>Success Guarantee</b>	The money must be received in the Seller’s bank account
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Seller access his Bank account to check the amount of money send by Buyer</li> <li>2. The amount of money in Seller's bank account matched with the amount stated in the contract * to refer extensions 2.a</li> <li>3. Use case continues at UC-56</li> <li>4. Reverse Bitcoins (UC-56)</li> </ol>
<b>Extensions</b>	2.a If the amount of money in Seller's bank account did not match the amount stated in the contract

	<ol style="list-style-type: none"> <li>1. Seller emails the buyer to inform the insufficient amount of money</li> <li>2. Buyer respond positively to Seller email <ol style="list-style-type: none"> <li>2.1. If Buyer did not agree with Seller's email and does not send the remaining balance</li> <li>2.2. Use case continues at step 3</li> </ol> </li> <li>3. Use case continues at UC-4</li> </ol>
<b>Sending Money</b> <b>UC-34 – Offline payment proof</b>	
<b>Pre-conditions</b>	Produce proof for the bank transaction
<b>Success Guarantee</b>	Receive money in the bank account
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Bank receives money from Buyer * <i>to refer extensions 1.a</i></li> <li>2. Bank produce the proof of transaction made by the buyer</li> <li>3. The proof of Bank transaction is sent to Seller and Buyer</li> <li>4. End of offline transaction</li> </ol>
<b>Extensions</b>	<ol style="list-style-type: none"> <li>1.a If seller's bank did receive any money <ol style="list-style-type: none"> <li>1. No proof of transaction produced</li> <li>2. Use case continues at step 1</li> </ol> </li> </ol>
<b>Updating Multisignature Wallet:</b> <b>UC-51 – Request to release Bitcoins</b>	
<b>Pre-conditions</b>	Two signatures request to release the Bitcoins
<b>Success Guarantee</b>	Both signatures are valid and verified
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. The system receives a signature from Buyer to request Bitcoin from multisignature wallet</li> <li>2. System receives a signature from Seller to release Bitcoin from multisignature wallet * <i>to refer extensions 2.a</i></li> <li>3. System releases the Bitcoins from Multisignature Wallet to Buyer</li> <li>4. Use case continues at <b>Step 5: Sending Reputation Token</b></li> </ol>
<b>Extensions</b>	<ol style="list-style-type: none"> <li>2.a If the system did not receive the signature from Seller <ol style="list-style-type: none"> <li>1. Use case continues at UC-52</li> </ol> </li> </ol>
<b>Updating Multisignature Wallet:</b> <b>UC-35- To verify Bitcoins release</b>	
<b>Pre-conditions</b>	Any of two signatures from either seller, buyer or Witness signs on the multisignature wallet
<b>Success Guarantee</b>	Received two signatures on multisignature wallet
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. System verifies both signatures to ensure it full fill the requirements for 2 of 3 signatures</li> </ol>
<b>Extensions</b>	<i>NIL</i>
<b>Updating Multisignature Wallet:</b> <b>UC-67 – Decision for disputes</b>	
<b>Pre-conditions</b>	Witness had examined the proof and proposed the actions to solve the disputes
<b>Success Guarantee</b>	Seller and buyer had received the proposed actions to solve the disputes and decided either to take the corrective actions or not
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. The system receives the dispute report from Witness</li> <li>2. The system asks the witness to choose the preference either seller or buyer to receive the Bitcoins from the Multisignature Wallet</li> <li>3. Witness tells system that her preference is Buyer * <i>to refer extensions 3.a</i></li> </ol>

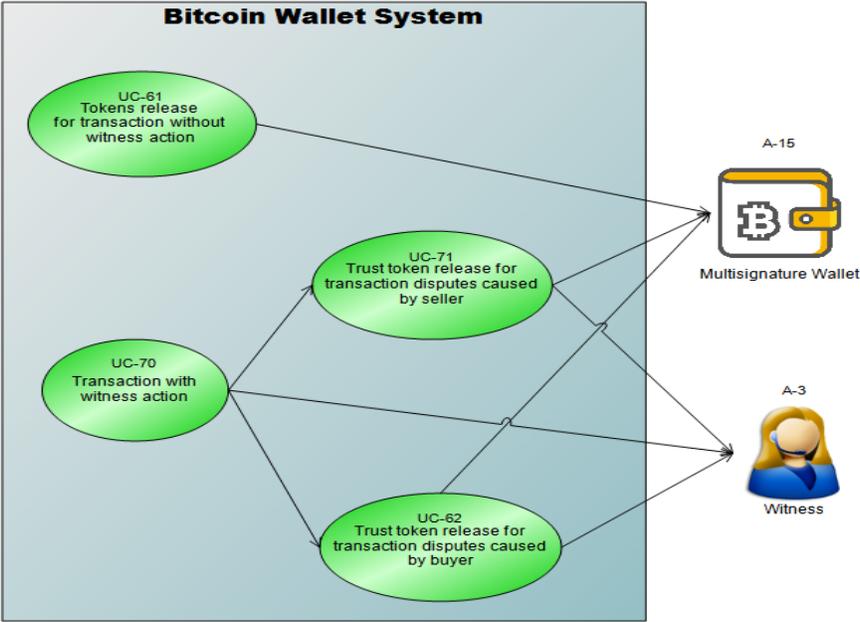
	<ol style="list-style-type: none"> <li>4. System asks Witness to sign the wallet</li> <li>5. Witness signs the wallet</li> <li>6. The system releases the Bitcoins from the Multisignature Wallet to Buyer's wallet</li> <li>7. Use case continues at <i>Step 5: Sending Reputation Token</i></li> </ol>
<b>Extensions</b>	<ol style="list-style-type: none"> <li>3.a Witness tells the system that her preference is Seller <ol style="list-style-type: none"> <li>1. System asks Witness to sign the wallet</li> <li>2. Witness signs the wallet</li> <li>3. The system releases the Bitcoins from the Multisignature Wallet to Seller's wallet</li> <li>4. Use case continues at step 7</li> </ol> </li> </ol>
<b>Managing Disputes</b> <b>UC-52 – Send invitations to witness to manage disputes</b>	
<b>Pre-conditions</b>	Only one signature requested to release the Bitcoins from multisignature wallet
<b>Success Guarantee</b>	Only 1 valid signature received within the agreed time frame as stated in the contract
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. System asks witness to manage the disputes</li> <li>2. System shows witness the contract between seller and buyer</li> <li>3. Use case continues at UC-53</li> </ol>
<b>Extensions</b>	NIL
<b>Managing Disputes</b> <b>UC-53 – Witness responses to the invitations</b>	
<b>Pre-conditions</b>	Witness manage the dispute
<b>Success Guarantee</b>	Witness received and accepted the notification from the system to manage the disputes
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Witness tells the system that she will manage the dispute based on the contract * to refer extensions 1.a</li> <li>2. Use case continues at UC-36</li> </ol>
<b>Extensions</b>	<ol style="list-style-type: none"> <li>1.a If the witness did not respond to the invitation for the dispute <ol style="list-style-type: none"> <li>1. System makes the witness status as idle until the contract end</li> <li>2. System appoints new Witness</li> <li>3. Use case continue at UC-49 (<i>Step 3: Enacting the Bitcoin Transactions</i>)</li> </ol> </li> </ol>
<b>Managing Disputes</b> <b>UC-36- Verify the disputes</b>	
<b>Pre-conditions</b>	Witness handle disputes based on evidence provided by Seller and Buyer
<b>Success Guarantee</b>	The witness is granted with access to the contract
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. Witness accesses the email address of seller and buyer from the contract UC-30</li> <li>2. Witness contacts Seller and Buyer ask for proof for the offline transaction (UC-34) made and other supportive evidence</li> <li>3. Witness compares the evidence with the contract (UC-30)</li> <li>4. Use case continues at UC-53</li> </ol>
<b>Extensions</b>	NIL

**Table D: Use Case Details for Enacting Offline Transaction**

**e. Step 5: Sending Reputation Tokens**

At the fifth step, describes the processes in contract to release either trust or distrust tokens to the seller and buyer. If there are no disputes between them, both will receive the trust tokens in their wallet. However, if there was a dispute reported then the type of tokens to be received by seller and buyer are depending on the witness decision. The witness also receives the witness token from the multisignature wallet. The processes involved are further described in the Use Case Diagram in **Figure and Table E**.

<b>Primary Actor:</b>	NIL
<b>Secondary Actor</b>	{A-3 – Witness}; {A-15 – Multisignature wallet}
<b>Use Cases:</b>	<i>Updating Multisignature Wallet:</i> {UC-61- Tokens release for the transaction without witness action}; {UC-70-Transaction with witness actions}; {UC-71 – Trust token release for transaction disputes caused by seller}; {UC-62 – Trust token release for transaction disputes caused by buyer}



**Figure E: Case Diagram for Sending the Reputation Token**

<b>Updating Multisignature Wallet:</b>	
<b>UC-61- Tokens release for the transaction without witness action</b>	
<b>Pre-conditions</b>	Seller and Buyer had signed to release Bitcoins from multisignature wallet
<b>Success Guarantee</b>	The Bitcoins in the multisignature wallet were sent to the Buyer’s wallet
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>System releases trust tokens for Buyer and Seller from Multisignature Wallet</li> <li>System releases witness tokens to Witness from Multisignature Wallet * <i>to refer extensions 2.a</i></li> <li>System dismisses the contract</li> <li>Use Case End</li> </ol>
<b>Extensions</b>	2.a If there are 2 Witnesses <ol style="list-style-type: none"> <li>The first Witness who did not respond to the invitation of the dispute will receive the irresponsible witness token</li> <li>Use case continues at step 2</li> </ol>
<b>Updating Multisignature Wallet:</b>	
<b>UC-70-Transaction with witness actions</b>	
<b>Pre-conditions</b>	Witness and either Buyer or seller had signed to release Bitcoins from multisignature wallet
<b>Success Guarantee</b>	The Bitcoins in the multisignature wallet were sent to the Buyer or Seller’s wallet
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>System asks the witness to choose the preference either seller or buyer or offline technical error that causes the dispute *<i>to refer extensions 1.a</i></li> <li>Witness tells system the dispute is caused by Seller</li> <li>Use case continues at UC-71</li> </ol>

<b>Extensions</b>	1.a If Witness tells the system the dispute is caused by Buyer 1. Use case continues at UC-62
<b>Updating Multisignature Wallet: UC-71- Trust tokens release for transaction disputes caused by seller</b>	
<b>Pre-conditions</b>	Witness and either Buyer or seller had signed to release Bitcoins from multisignature wallet
<b>Success Guarantee</b>	The Bitcoins in the multisignature wallet were sent to the Buyer or Seller's wallet
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. System asks witness whether Seller has taken the corrective action as propose to solve the dispute or not.</li> <li>2. Witness tells the system that Seller did not take any corrective action for the dispute <i>*to refer extensions 2.a</i></li> <li>3. System sends the distrust token to Seller's wallet</li> <li>4. System sends the trust token to Buyer's wallet</li> <li>5. System sends the witness token to Witness wallet</li> <li>6. System dismisses the contract</li> <li>7. Use Case End</li> </ol>
<b>Extensions</b>	2.a If Witness tells system that Seller did not take corrective action for the dispute <ol style="list-style-type: none"> <li>1. System sends the trust token to Seller's wallet</li> <li>2. Use case continues at step 4</li> </ol>
<b>Updating Multisignature Wallet: UC-62- Trust tokens release for transaction disputes caused by buyer</b>	
<b>Pre-conditions</b>	Witness and either Buyer or seller had signed to release Bitcoins from multisignature wallet
<b>Success Guarantee</b>	The Bitcoins in the multisignature wallet were sent to the Buyer or Seller's wallet
<b>Main Success Scenario</b>	<ol style="list-style-type: none"> <li>1. System asks the witness whether the buyer has taken the corrective action as propose to solve the dispute or not.</li> <li>2. Witness tells the system that buyer did not take any corrective action for the dispute <i>*to refer extensions 2.a</i></li> <li>3. System sends the distrust token to buyer wallet</li> <li>4. System sends the trust token to Seller's wallet</li> <li>5. System sends the witness token to Witness wallet</li> <li>6. System dismisses the contract</li> <li>7. Use Case End</li> </ol>
<b>Extensions</b>	2.a If Witness tells the system that buyer did take any corrective action for the dispute <ol style="list-style-type: none"> <li>1. System sends the trust token to buyer wallet</li> <li>2. System sends the trust token to Seller's wallet</li> <li>3. System sends the witness token to Witness wallet</li> <li>4. Use case continues at step 4</li> </ol>

**Table E: Use Case Details for Sending Reputations Token**