

*Trust and Its Antecedents in Semi-
Autonomous Information Systems: The Case
of Bitcoin*

By Ahmed Mohamadean

**A Thesis Submitted to the School of Graduate Studies in Partial Fulfilment of the
Requirements for the Degree Doctor of Philosophy in Business Administration**

PhD in Business Administration (2024)

Information Systems

McMaster University, Hamilton, Ontario, Canada

TITLE: Trust and Its Antecedents in Semi-Autonomous
Information Systems: The Case of Bitcoin

AUTHOR: Ahmed Mohamadean

SUPERVISOR: Dr. Khaled Hassanein

NUMBER OF PAGES: 182

Abstract

Since its inception in 2009, Blockchain (i.e., the underlying technology of cryptocurrencies) has sparked new potential to question the fundamental nature of things such as money and intermediaries. At the very core of this technology is a new type of trust embedded in the design of the information system that enables its functionality. Public Blockchain applications (e.g., Bitcoin) are examples of Semi-Autonomous Information Systems. Semi-Autonomous Information Systems are information systems that humans and algorithms jointly control. Trust in public Blockchain applications is produced through a decentralized network of actors transacting under an algorithmic authority – a new type of trust in Semi-Autonomous Information Systems.

This study followed the information systems design method to develop a design theory that explains the process of designing trustworthy Semi-Autonomous Information Systems. The proposed design theory includes decentralization and algorithmic authority as new factors in building users' trust in Semi-Autonomous Information Systems. As the IS literature lacks scales for these two factors, new decentralization and algorithmic authority scales were developed and validated following established guidelines. Following an extensive literature review, ten inductive interviews with subject-matter experts were conducted during the conceptualization phase. The initial measurement items list for these scales was evaluated and refined through 12 more interviews with qualified raters and a subsequent survey study of 126 MBA students to establish content validity for the proposed new items. Two independent samples, 200 participants each, were used during the exploratory and confirmatory analyses to validate the new scales.

Then, the two new scales of decentralization and algorithmic authority were tested as part of a new trust model. The proposed model includes decentralization and algorithmic authority as two new cognitive-based trust factors. The model also includes perceived control and sense of community as two types of emotional-based trust. The pre-established factors of structural assurance, users' trust beliefs in actors, and calculative-based trust are also included in the model. The model was empirically validated through a quantitative survey study of 450 Bitcoin users. The proposed design theory, two new scales, and the new trust model provide significant implications for theory and practice in this area.

Acknowledgment

This work would not have been possible without many people's tremendous guidance, support, and help throughout this Ph.D. journey.

Thank you, Dr. Khaled Hassanein, for being my supervisor. It was a great honor and pleasure to receive your valuable guidance and support throughout this process. Despite your busy schedule, you were always there whenever and wherever you were needed with fast and understanding responses. You will always be my role model in research and beyond. Thank you for believing in me, especially when I told you I wanted to develop scales. I will always remember your feedback on everything, even the spaces I forgot at the beginning of some sentences. Your way of thinking and supervision style shaped me as a scholar.

Thank you, Dr. Brian Detlor, for being on my supervisory committee. I appreciated your continued feedback during the different stages of this research. Completing your qualitative course was a great opportunity as you instilled in me the love and appreciation of qualitative research. This knowledge helped me during the interview part of the scale development phase of my thesis. I benefited greatly from your invaluable and detailed feedback in improving the flow and writing of my thesis.

Thank you, Dr. Melina Head, for being on my supervisory committee. I appreciated your continued feedback during the different stages of this research. You also helped me during the critical step of scale development by helping me promote the study to participants through your LinkedIn profile. Your guidance and support is very much appreciated.

Thank you, Dr. Baba, for chairing my defense committee. It was especially meaningful as my first course in the program was your course, “Management Theory.” It shaped my general understanding of theorizing and helped me in the design theory part of my thesis. Thank you so much for encouraging PhD student and calling us scholars in your course.

I sincerely thank Nour El-Shamy for promoting my study on his LinkedIn profile.

To my beloved parents, your tireless encouragement has been the bedrock of my academic pursuits. I am forever indebted to your love and support.

To my wife, Dr. Esraa Abdelhalim. Thank you for being a true partner in my personal and academic life. Your unconditional love, support, encouragement, and determination were instrumental throughout this journey. I am so grateful for you and everything you sacrificed to help me get to where I am now. Thank you for believing in me.

To my daughter, Lareen, and my son, Yaseen. Thank you for being the joy of this journey. Your smiles made it easy for your mom and dad to bear the sleepless nights and stress.

To my dear sisters, Asmaa and Alyaa, and brother, Mohamad, thank you for being on my side and supporting me during my Ph.D. journey. Your support and encouragement helped me navigate many critical moments in this journey. Alyaa, your support and advice, especially during COVID, are unforgettable.

To all those who have influenced and guided me along this academic journey, your unwavering support, encouragement, and belief in my abilities have been the wind underneath my wings. Thank you for being so instrumental in this milestone achievement.

Table of Contents

Abstract	i
List of Tables	viii
List of Figures	x
List of Key Terms	xi
Chapter 1. Introduction	1
1.1. Outline of The Thesis	8
Chapter 2. Literature Review	10
2.1. Bitcoin	10
2.2. Trust as a Social Construct	13
2.3. Trust in the IS Literature	16
2.4. Trust in Bitcoin	19
Chapter 3. A Proposed Design Theory for SAIS	25
3.1. Kernel Theory for SAIS	27
3.2. Design Principles for SAIS.....	28
3.3. Meta-Design for SAIS	29
3.3.1. Algorithmic Authority.....	31
3.3.2. Decentralized Structure for SAIS.....	33
3.3.3. Decisions.....	36
3.3.4. Security and Privacy Lead to Trust	37
Chapter 4. Research Model and Hypotheses	41
4.1. Established Factors	43
4.1.1. Users' Trust Beliefs in Actors.....	44
4.1.2. Calculative-based Trust.....	46
4.1.3. Structural Assurance.....	46
4.2. Cognitive-Based Trust	47
4.2.1. Decentralization	47
4.2.2. Algorithmic Authority	50
4.3. Emotional-Based Trust	52
4.3.1. Perceived Control.....	52

4.3.2.	Sense of Community.....	53
4.4.	Control Variables.....	55
4.4.1.	Users’ Knowledge of Bitcoin	55
4.4.2.	Gender	56
4.4.3.	Risk Tolerance	56
4.4.4.	Community Membership.....	57
Chapter 5. Scale Development		58
5.1.	Scale Development in the IS Literature.....	58
5.2.	Scale Development Process for Decentralization and Algorithmic Authority.....	60
5.2.1	Conceptualization (Step 1)	62
5.2.2.	Items Generation (Step 2).....	73
5.2.3.	Content Validity Assessment (Step 3)	74
5.2.4.	Model Specification (Step 4).....	82
5.2.5.	Scales Development Initial Reliability Analysis (Pilot Study)	83
5.2.6.	Exploratory Factor Analysis (EFA) (Step 5 & 6)	84
5.2.7.	Confirmatory Factor Analysis (CFA) (Steps 7 & 8)	90
Chapter 6. Methodology and Results		95
6.1.	Main Study Analysis	96
6.1.1.	Pilot Phase	96
6.1.2.	Main Phase	97
6.1.3.	Data Cleansing	98
6.1.4.	Measurement Scales.....	99
6.1.5.	Structural Equation Modelling (SEM)	102
Chapter 7. Discussion, Contributions, and Limitations		114
7.1.	Discussion of the Proposed SAIS Design Theory.....	114
7.2.	Discussion of Scale Development Results	117
7.2.1.	Dimensionality Issue for Constructs.....	117
7.2.2.	Conceptualization, Operationalization, and Contextualization	119
7.2.3.	Further Considerations for Future Scale Development Research	121
7.3.	Discussion of the Proposed New Model for Trust in SAIS.....	122
7.3.1.	Contributions to Theory	126
7.3.2.	Contributions to Practice.....	128

7.3.3. Limitations and Future Research	129
References	131
Appendix A. Early Scale Development Attempts in the IS Literature	145
Appendix A.1 Davis's Approach, MISQ 1989:.....	147
Appendix A.2 Moore and Benbasat's Approach, ISR 1991:	148
Appendix A.3 Chin et al. Approach, ISR 1997 / Salisbury et al. Approach, ISR 2002:	150
Appendix B. Participants' quotes on the newly developed definitions of the constructs (Step 3: Scale Validation in the Scale Development Process)	152
Appendix C. Main Study Survey	154
1. Welcome Message.....	154
2. Screening Question 1	154
3. Screening Question 2	155
4. Years of Experience Question.....	155
5. Demographic Question	156
6. Age Question	156
7. Education Question.....	157
8. Online Community Membership Question	157
9. Self-Reported Knowledge Question.....	158
10. Consent Letter	159
Appendix D. Outlier Analysis	160
Round 1 (N=475)	160
Round 2 (N=458)	165

List of Tables

Table 1: Main Types of Trust in Extant Literature	15
Table 2: A comparison between trust in previous IS research and trust in Semi-Autonomous IS	23
Table 3: Conceptualization for the new scales of decentralization and Algorithmic Authority	62
Table 4: Interviews' Themes	67
Table 5: Initial Definitions and Measurement Items	73
Table 6: Scale Development Content Validity Assessment.....	75
Table 7: Constructs Definitions and Corresponding Measurement Items	77
Table 8: One-Way Repeated ANOVA Test Results	81
Table 9: Measurement Items Adjustment.....	82
Table 10: Reliability analysis of the initial measurement items.....	83
Table 11: Pearson correlation coefficients	84
Table 12: Sample's Descriptive Statistics for the Exploratory Factor Analysis.....	85
Table 13: Exploratory Factor Analysis Items List.....	88
Table 14: Reliabilities and Validities Measures for the Exploratory Factor Analysis (EFA).....	89
Table 15: Weights, Path Coefficients, Significance Level, and R ² for EFA Stage 2 Model.....	90
Table 16: Sample's Descriptive Statistics for the Confirmatory Factor Analysis	91
Table 17: Confirmatory Factor Analysis Items List	92
Table 18: Reliabilities and Validities Measures for the Confirmatory Factor Analysis (CFA).....	93
Table 19: Weights, Path Coefficients, Significance Level, and R ² for CFA Stage 2 Model	93
Table 20: Main Study Sample's Demographics	99
Table 21: Measurement Scales	100
Table 22: Items Loading and Cross-Loading.....	103
Table 23: Cronbach's Alpha, Composite Reliability, and AVE for Reflective Constructs	104

Table 24: Formative Latent Constructs Items Analysis.....	105
Table 25: Fornell-Larcker Criterion for Discriminant Validity	105
Table 26: Correlation Values among Latent Constructs	106
Table 27: Principal Component Analysis for Harman’s Single Factor Test	107
Table 28: Comparison of Path Coefficients by CLC Approach and Original PLS Models	108
Table 29: Comparison of R ² Values by CLC Approach and Original PLS Models	108
Table 30: Validation of the Study Hypotheses	109
Table 31: PLS Effect Size Analysis	111
Table 32: Perceived Control Mediation Effect	112
Table 33: Correlation Results for Control Variables	113
Table 34: Control Variables Analysis PLS Results	113
Table 35. Summary of Some Early IS Scale Development Research and Guidelines	145
Table 36: Participants' Quotes on the New Definitions	152

List of Figures

Figure 1: Different Types of Information Systems Designs.....	4
Figure 2: Thesis Outline	9
Figure 3: Simple Bitcoin Ecosystem of Four Users	12
Figure 4: SAIS' Meta-Design Properties in a Process Flow	30
Figure 5: Proposed Research Model.....	42
Figure 6: Scale Development Steps (Source: Mackenzie et al. 2011).....	59
Figure 7. Scale Development for Decentralization and Algorithmic Authority Following the Mackenzie et al.'s Approach (2011).....	61
Figure 8: Sample's Age Distribution	79
Figure 9: Definitions Agreement Statistics	80
Figure 10: The Two-Stage EFA Model.....	87
Figure 11: Pilot Sample Age Distribution	96
Figure 12: Final PLS Model Results.....	109
Figure 13: Bias Impact on the Scale Development Process	120

List of Key Terms

Term	Definition	Adapted From
Algorithmic Authority	- Algorithmic authority is the legitimate level of control an algorithm has to enforce specific actions based on its programmable logic.	Self-developed
Algorithms	- “Algorithms are simultaneously a set of abstract instructions (logic) and possibilities for action (control).”	(Lustig and Nardi 2015, p.744)
Artifact	- “Artifact describes anything that is artificial or has been constructed by humans.”	(Hevner and Chatterjee 2010, p.5)
Bitcoin	- Bitcoin is the first known public cryptocurrency application developed using Blockchain technology.	Self-developed
Block	- A block is a virtual concept that represents information about transactions. It is a "container" of transaction information.	(Antonopoulos 2017)
Blockchain	- Blockchain is a Distributed Ledger Technology (DLT) that records information that is accessible, transparent, verifiable, immutable, and agreed upon among all nodes in its network.	Self-developed

	- Blockchain is a chain of connected blocks.	
Cryptocurrencies	- Cryptocurrencies are those Blockchain digital currencies that use cryptography to validate and record transactions.	Self-developed
Decentralized IS	- A decentralized IS is an IS that is collaboratively managed and accessible to humans and algorithms in a network where participating entities share inputs (i.e., computing resources, data/information) and influence the system’s outputs, with no single entity playing a dominant role in the operation of the system.	Self-developed
Design Theory	- “A design theory answers the question of how to design something” to achieve specific goals.”	(Gregor 2006, p.628)
Hash Algorithm	- An encryption algorithm that is used to transform plain messages into encrypted messages.	Self-developed
Miners	- Miners are nodes in the Blockchain that verify and record information.	Self-developed
Node	- In computer science, nodes are devices or data points on a	https://www.cbronline.com/what-is/what-is-a-node-4927877/ .

	network; devices such as PCs, phones, or printers are considered nodes.	
Semi-Autonomous Information Systems (SAIS)	- SAIS refer to information systems that cannot operate independently and require human involvement to complete tasks.	(Zilberstein 2015)

Chapter 1. Introduction

Since its inception in 2009, Blockchain has sparked a new potential to revolutionize lives by re-inventing financial services, re-architecting the firm, creating the ledger of things, and rebuilding government and democracy (Namasudra et al. 2021; Tapscott and Tapscott 2016). Indeed, it has cultivated a questioning of the fundamental nature of things, such as what money is (Maurer et al. 2013), the value of intermediaries in economic transactions (Tapscott and Tapscott 2016), or the need to rewrite a new social contract (Tapscott 2017).

Blockchain is a distributed ledger technology that records information that is accessible, transparent, verifiable, immutable, and agreed upon among all nodes¹ in its network. From a technical perspective, Blockchain is a combination of a public-key infrastructure to assure authenticity and nonrepudiation, a hash algorithm to encrypt the data to establish confidentiality and integrity, and a consensus algorithm to create agreement among all nodes (e.g., Bitcoin² uses the proof-of-work (PoW) as a consensus algorithm). In other words, Blockchain is a "*distributed database stored by parties in a decentralized network*" (Tapscott and Vinod 2019, p.7). Amongst its numerous transformative ideas is that Blockchain enables us to realize, probably for the first time, the possibility of designing a decentralized system that can operate without a central entity.

Cryptocurrencies (aka digital currencies) such as bitcoin, ether, and ripple are the first applications of Blockchain in the financial sector. The underlying design features of Blockchain

¹ In computer science, nodes are devices or data points on a network; devices such a PC, phone, or printer are considered nodes, <https://www.cbronline.com/what-is/what-is-a-node-4927877/>.

² Capitalized **Bitcoin** refers to the system whereas **bitcoin, ether, and ripple** refer to the digital currency unit.

have also enabled different applications in other sectors, including healthcare (e.g., MedRec³ by MIT Media Lab) and supply chain (e.g., TREUM⁴). As much as Blockchain holds tremendous opportunities for the private sector, it also prompts new possibilities for the public sector, specifically for redesigning sovereign currencies.

The first survey conducted by the Central Bank Digital Currency (CBDC) initiative, which tracks the developments of CBDC as national sovereign currencies, in February 2020 reported that 65% of central bank respondents were researching the potential of CBDC, with 23% of those respondents having already taken their research into the proof-of-concept stage (King 2020). Recently, this percentage has risen to 93% of central banks engaged in some form of CBDC (Kosse and Mattei 2023). Indeed, the Bank of Canada is already researching issuing its digital crypto dollar (Dube 2023). This growing interest can be attributed to the commercial interests of technology companies such as the Meta (previously known as Facebook) digital currency initiative (i.e., the Libra project) and the rolling out of digital currencies in China, India, Australia, Sweden, and the United States. One of the critical factors for such interest is trust (Wladawsky-Berger 2017), which is at the very core of Blockchain (Tapscott and Tapscott 2016).

Trust is the glue among all societal entities (Botsman and House. 2018). It has been shown to be a critical factor in all social interactions, including personal relationships (e.g., (Rempel et al. 1985)), dyadic relationships within organizations (Mayer et al. 1995), and inter-organizational relationships (Zaheer et al. 1998). Historically, institutions have created a safe environment for individuals to transact safely through societal structures at the level of individuals (e.g., individual qualifications), firms (e.g., firm reputation), and intermediaries (e.g., third-party assurance)

³ MedRec Project: <https://www.media.mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis/>.

⁴ Kaleido's TREUM platform for Enterprise Blockchain Apps, <https://www.kaleido.io/blockchain-platform/treum>.

(Zucker 1986). Subsequently, all different types of trust have been conceptualized because of this institutional-based trust and have been validated in various contexts, including eCommerce (e.g., (Gefen et al. 2003; McKnight et al. 2002a; Pavlou 2003)), mobile payments (m-payments) (e.g., (Chandra et al. 2010)), and even peer-to-peer lending platforms (Burtch et al. 2014). However, Blockchain has enabled individuals to transact freely without the two means of institutional-based trust (i.e., central entity and intermediaries). In turn, since Blockchain could operate without institutional trust, its nature of trust may differ from other types of information systems and, most importantly, how each information system's design influences trust.

Blockchain has created a system to generate trust that is accessible to everyone (Berkeley 2015). In essence, the Blockchain's first application (i.e., Bitcoin) was designed as a network protocol where the underlying algorithms and the networked actors share the responsibility of running the system without a central entity or a trusted third party. As such, trust in Bitcoin could be defined as an overall assessment of the system's reliability, similar to early attempts in the IS trust literature (Gefen 2000).

Previous IS trust research was developed and tested in centralized human-managed systems. As a result, the factors investigated combined interpersonal trust factors (e.g., trust beliefs about the web vendors) and institutional-based trust elements (i.e., structural assurance and situational normality). Moreover, earlier research also distinguished between trusting an online vendor (e.g., Amazon) and trusting the communication medium (i.e., Amazon's IT infrastructure) (Grabner-Kräuter and Kaluscha 2003; Pavlou 2003). However, the latter was assumed to be an "implicit" factor that affects trust (Pavlou 2003) or an "exogenous" factor (Grabner-Kräuter and Kaluscha 2003). Trust in Bitcoin is embedded in the system design. In other words, trust is an

“intrinsic design feature” and not an extrinsic factor (Tapscott and Tapscott 2016). This aspect, in particular, has been neglected in previous attempts to study trust in cryptocurrencies.

Because of the underlying information system design of Bitcoin, the system is managed by algorithms and humans where no one party controls the other or can affect the system's continuity. As such, it could be perceived as an example of a Semi-Autonomous Information System (SAIS). SAIS refer to information systems that cannot operate independently and require human involvement to complete tasks (Zilberstein 2015). Figure 1 below shows the different types of information systems designs.

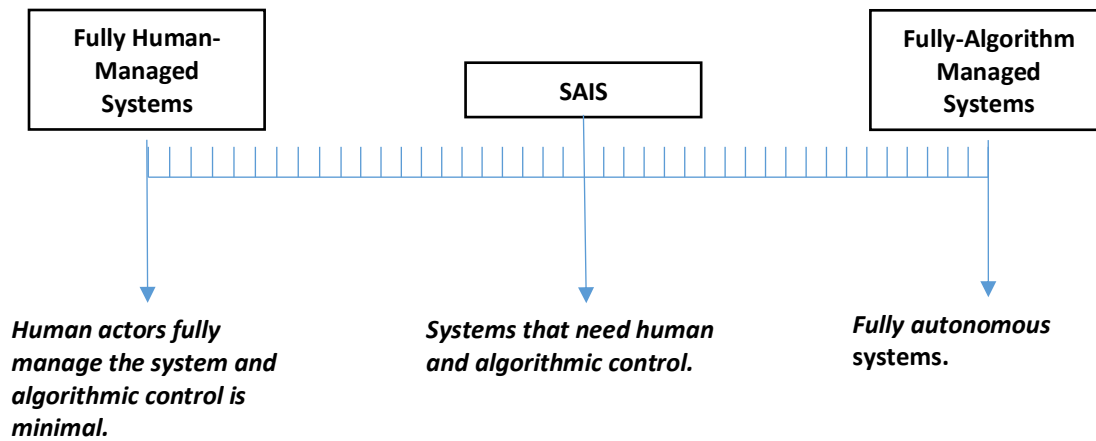


Figure 1: Different Types of Information Systems Designs

As shown in Figure 1 above, information systems designs could be classified into three groups: fully human-managed, SAIS, and autonomous. In fully human-managed systems, algorithmic control is minimal. In comparison, autonomous systems operate without any human intervention. SAIS requires both human intervention and algorithmic control to operate. On this spectrum, we can place Bitcoin as a SAIS closer to the fully autonomous systems end of the scale as the system has four functions where algorithms control the amount of money supply in the system, create consensus in the network, and give recommendations for all nodes to verify the

authenticity of each transaction. The human nodes (i.e., mining nodes) in the Bitcoin control the amount of computing resources that could be dedicated to supporting the systems based on a particular reward scheme.

Several attempts have been made to conceptualize users' trust beliefs in Bitcoin, mainly through qualitative research (Sas and Khairuddin 2017; Zarifis et al. 2014) and other conceptual frameworks (Auinger and Riedl 2018; Ostern 2018; Sas and Khairuddin 2015). Even though these previous attempts inform our understanding, they are insufficient for four reasons. First, the conceptualization process was based on interpersonal trust and trust in IT artifacts⁵ without considering the unique design features of Bitcoin as a SAIS. Second, these models did not distinguish between what constitutes trust as components and what affects trust as antecedents. Third, no consideration has been made to clarify the dynamic process of users' interactions with the system and how these interactions influence their cognitive and emotional perceptions to build trust. Finally, no relevant models or empirical results are available to guide the future design of "trustworthy" similar SAIS in other contexts such as financial services, eCommerce applications, supply chains, and healthcare sectors. What drives users' trust in SAIS are some unique factors embedded within the system's design, such as in the case of Bitcoin. Thus, a design theory was needed to explain the nature of these new factors. A design theory for an information system defines how an information system can be designed to be as effective and efficient as feasibly possible (Walls et al. 1992).

Bitcoin's users believe in its underlying algorithms instead of any central authority (Maurer et al. 2013; Simser 2015). What makes Bitcoin operate successfully is its algorithmic authority,

⁵ While the system's design provides guidelines of how to design a system, the system's artifact refers to the tangible product of actualizing the design.

where users are transacting under the authority of some computer algorithms and a network of actors who enable these algorithms to run smoothly (Lustig and Nardi 2015). It is an open and decentralized network where algorithms can enforce networked actors to behave according to the users' expectations and best interests. That is, the decentralized enabling structure of the technology allows for meaningful collaboration between the networked actors and the underlying cryptographic algorithms. These features can be understood from the collaborative control theory (CCT) (Nof 2007; Nof et al. 2015).

Collaborative control theory is a recent theory developed to describe the nature of interactions in any "collaborative, computer-supported and communication-enabled productive activities in highly distributed organizations of humans and robots and autonomous systems" (Nof 2007, p.281). The theory recognizes humans' and algorithms' capabilities to augment the systems' outcomes and achieve effective collaborations (Nof 2007; Nof et al. 2015). In this regard, collaboration is an effective tool to enable "all involved entities of decentralized e-systems to share their resources, information, and responsibilities, such that mutual benefits are obtained" (Nof et al. 2015, p.33). Such a definition precisely describes public Blockchain applications (e.g., Bitcoin) where all nodes in the network are connected in a decentralized manner and share resources, information, and responsibilities of running the system.

Additionally, the system enables users to have a sense of control over their financial transactions, and the system is supported by some online communities devoted to enhancing users' knowledge. Through these online communities, Bitcoin users enjoy communicating with each other about matters that are important to their learning about the system and any proposed role of the Bitcoin community to protect the future of the system (Lustig and Nardi 2015), which makes the system more predictable and, thus, more trustworthy. While these factors have their scales in

the IS literature so that they can be validated, the IS literature lacks scales for decentralization and algorithmic authority. Hence, these new factors need scales to be validated as new factors in building users' trust in SAIS.

The underlying philosophy of this work goes against the frequent description of Blockchain as a trustless technology (e.g., (Shermin 2017; Werbach 2018)) to claim that the nature of trust has shifted and a new conceptualization process is needed. Indeed, when there is no need to trust anyone, trust does not dissipate. Trust was, is, and will always be an essential concept in our consciousness as humans, even when dealing with fully autonomous information systems. Still, to study it, we will have to develop new theories, scales, and models. I consider my thesis to be an attempt in this direction. Thus, the objectives of this research is to propose and empirically validate a new theoretical research model for users' trust in Bitcoin as an example of SAIS.

The proposed design theory for SAIS acknowledges the symbiotic relationship between humans and algorithms, which is the core of effective human-algorithm integration (Stephanidis et al. 2019). Thus, the proposed design theory is well-positioned to inform future designs of trustworthy SAIS. Moreover, developing new scales for decentralization and algorithmic authority would be of value to further validate scale development practices in the IS literature (MacKenzie et al. 2011), as scales are the bridge between theory and practice. Finally, the proposed new trust model emphasizes the importance of decentralization and algorithmic authority in building users' trust in SAIS and further validates established factors in the IS trust literature.

In summary, following an information systems design method, this research proposes a design theory to explain how such new systems of SAIS could be perceived as trustworthy. The proposed theory identifies algorithmic authority and decentralization as critical new factors driving users' perception of trust in SAIS. The new theory encompasses four propositions and hypotheses

related to algorithmic authority, decentralization, a sense of control for human participants, and security and privacy protection to ensure SAIS trustworthiness. As security and privacy protections have already been validated in the IS literature (Chandra et al. 2010; Xin et al. 2013) to build users' trust in information systems, the three hypotheses of decentralization, algorithmic authority, and sense of control were validated as part of a larger trust model in SAIS. The new trust model includes self-developed scales for decentralization and algorithmic authority, as the IS literature lacks scales for decentralization and algorithmic authority. The model was validated in Bitcoin as an example of SAIS.

1.1. Outline of The Thesis

The remainder of this thesis is organized as follows: Chapter 2 gives a literature review of the main concepts of this research and shows how trust has been constructed and studied so far and how the uniqueness of Bitcoin as an example of SAIS could drive new factors in building users' trust in SAIS. Chapter 3 presents a proposed design theory to explain the properties that build trustworthy semi-autonomous information systems. The proposed design theory's new factors are further developed as part of a larger proposed trust model for Bitcoin and presented in Chapter 4. Chapter 5 discusses the scale development for decentralization and algorithmic authority. Chapter 6 shows the research methodology and results of the hypotheses testing. Finally, Chapter 7 discusses the study's contributions, limitations, and future research. Figure 2 below shows the thesis outline.

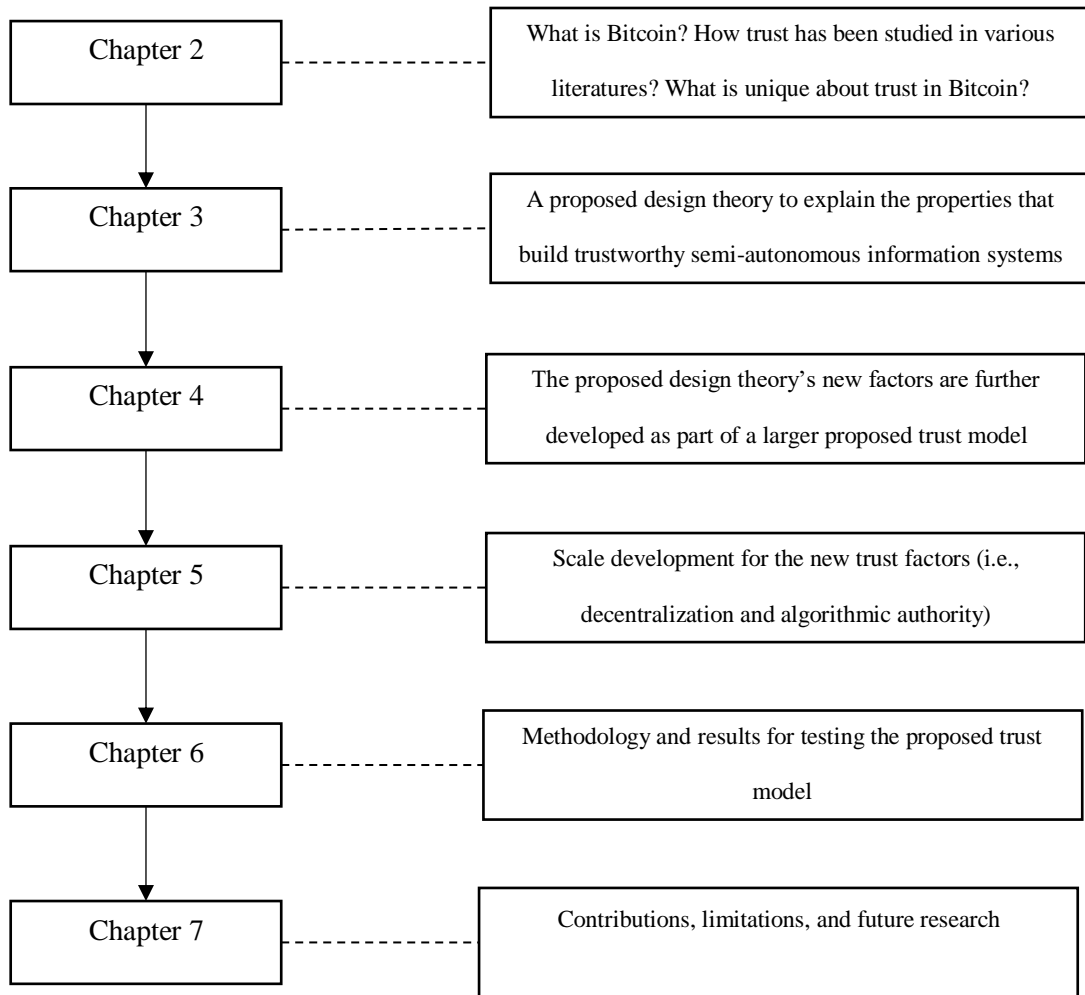


Figure 2: Thesis Outline

Chapter 2. Literature Review

This chapter first explains the Bitcoin system so the reader can understand what Bitcoin is. Then, an extensive discussion of trust as a social construct in the various literature is presented so that the reader is familiar with fundamental concepts of trust that have been used to inform the IS trust literature. After that, a closer look into the IS trust literature is presented so the reader knows how trust has been constructed and studied. Finally, previous attempts to study trust in Bitcoin are explained to show how the uniqueness of Bitcoin as an example of SAIS could drive new factors in building users' trust in SAIS.

2.1. Bitcoin

Bitcoin was introduced to satisfy people's need to conduct financial transactions directly without any central interference. As a peer-to-peer network, it is the first digital platform to create a truly decentralized and secure environment to exchange value, and it is the first e-payment system to solve the "double spending" problem (Nakamoto 2008) when users can spend the digital coin more than once. At an abstract level, Bitcoin comprises a group of mathematical algorithms that operate across a network of actors. The system operates like a universal network where users (also called nodes) can submit their transactions to the network to be validated and recorded. The validation and the recording processes are done by those users who opted to be miners. Miners are the nodes responsible for validating and recording transactions. Each node in the network has the right to mine transactions.

Miners compete against each other for who first will verify and record valid transactions in the public ledger (i.e., Blockchain), where all transactions are anonymous, immutable, persistent, and secure (Zheng et al. 2017). Whoever mines transactions first is rewarded in two

ways. One is through a transaction fee in the form of a fraction of existing bitcoins that are being recorded in the Blockchain, and the second is in the form of earning newly generated bitcoins, currently set at 3.125 bitcoins for adding a new block.

A block is a virtual concept that represents information about transactions. It is a "*container*" of transaction information (Antonopoulos 2017). It consists of a header, which is used to create a unique digital fingerprint for each block, and a body, which is utilized to hold information about transactions (Antonopoulos 2017; Zheng et al. 2017). When miners want to add a new block of transactions, they must include the fingerprint of the previous, most recently added block in the header of the new block. This is how the blocks are all connected in a chain of blocks or Blockchain.

The underlying mathematical algorithms of Bitcoin are a public-key infrastructure to assure authenticity and nonrepudiation, a hash algorithm to encrypt the data and establish confidentiality and integrity, and a proof-of-work algorithm to create consensus among nodes. Even though the public-key infrastructure and the hash algorithm were suggested by Tsiakis and Stephanides (2005) as integrated mechanisms to create secure e-payments, Bitcoin was the first system to leverage these two algorithms in developing the new concepts of Blockchain and proof-of-work. The proof-of-work is the mathematical operation that builds consensus in the network. The combined impact of these algorithms with a decentralized network of actors has made Bitcoin a unique e-payment system.

Users can join the system through a "wallet" application. These wallet applications generate two unique alphanumeric numbers – private and public keys. While the private key creates a digital signature for transactions to enforce nonrepudiation, the public key creates the digital identity for each user to guarantee authenticity. Moreover, each user can be a miner and

hold a copy of the ledger, updated with each new block added every ten minutes. Figure 2 illustrates a simple example of Bitcoin consisting of only four users (U1, U2, U3, and U4). U1 and U2 are two "Light Users" who use the system to make transactions without holding a copy of the ledger or mining transactions (Antonopoulos 2017). U3 and U4 are miners, each storing a copy of the ledger.

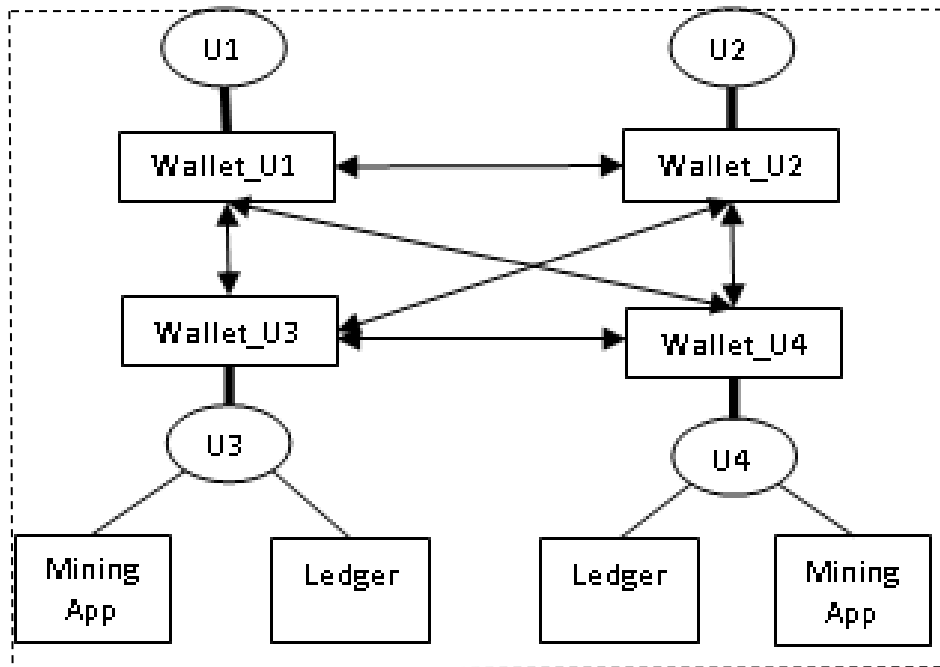


Figure 3: Simple Bitcoin Ecosystem of Four Users

Although the Blockchain is a public ledger, users' transaction information is encrypted. To some extent, their privacy is protected as users' transactions are represented only by their digital identities (i.e., public keys). Additionally, once transactions' information is added to a block, these records are "immutable" since the affordance of computing power to change the entire Blockchain is highly unlikely (Nakamoto 2008). Miners are doing the two main processes of verifying and recording transactions into blocks. While the verification process is based on checking the

relationship between users' public key and their digital signatures, the recording process is based on the concept of proof-of-work⁶ (Antonopoulos 2017). As a result, Bitcoin has created a trusted environment for users to make online transactions without the need for a central authority or even a third-party assurance. Therefore, trust in Bitcoin differs from previous types of trust, which were developed and tested where a central authority and a third-party assurance exist. Trust in Bitcoin is based on a new kind of trust in Semi-Autonomous Information Systems. This unique design has enabled the underlying cryptographic algorithms to operate across a decentralized network of users. In the following section, I discuss the nature of trust as a social construct.

2.2. Trust as a Social Construct

The need for trust arises in risky situations (Mayer et al. 1995), uncertainty (Mayer et al. 1995; Pavlou 2003), or when the trustor might be "*vulnerable*" to the trustee's actions (Doney and Cannon 1997; Mayer et al. 1995; Rempel et al. 1985). Trust has not been defined as an absolute concept, but rather it was socially constructed. Trust holds different meanings in different contexts, such as personal relationships (e.g., (Rempel et al. 1985)), dyadic relationships within organizations (i.e., in sociology, dyad means a group of two people) (Mayer et al. 1995), and in inter-organizational relationships (Zaheer et al. 1998). Mainly, the concept has been examined through interpersonal and institutional-based trust lenses. Interpersonal trust is based on assessing familiarity and similarity among individuals (Pavlou 2002). Whereas institutional-based trust is derived from the facilitating conditions in terms of formal societal structures at the level of individuals (e.g., individual qualifications), firms (e.g., firm reputation), and intermediaries (e.g., third-party assurance) (Zucker 1986).

⁶ For more information on the technical details of the Bitcoin, readers are referred to (Antonopoulos 2017).

Interpersonal trust refers to "*an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon*" (Rotter 1967, p.651). In personal relationships, trust has been operationalized to include benevolence (i.e., is the partner motivated individually or cooperatively with good intention towards the relationship?) and honesty (i.e., the extent to which one thinks that the partner is telling the truth) (Larzelere and Huston 1980). Similarly, Rempel et al. (1985) used predictability, dependability, and faith as components of interpersonal trust, and the authors provided *higher relative importance* for faith in personal relationships.

Inter-organizational trust was explained from different perspectives. For instance, Zaheer et al. (1998) describe this type of trust as inherently "relational" (i.e., just like trust in a dyad which is derived from interactions and experiences between individuals) rather than "dispositional" (i.e., a propensity to trust others in general (Rotter 1971)). They conceptualize it to include the three components of reliability, predictability, and fairness in negotiations. However, Doney and Cannon (1997) explain inter-organizational trust as "*a governance mechanism through which opportunism behaviors are mitigated in the exchange*" p.35. The authors operationalized it in terms of credibility (i.e., an expectancy that the partner's word or written statement can be relied on, the exact definition that was provided by Rotter (1967)), and benevolence. Most importantly, Doney and Cannon (1997) described five different cognitive processes through which trust is formed. These processes are *calculative, prediction, capability, intentionality, and transference*. The *calculative* process is an assessment of the cost/benefit analysis of the trustee's untrustworthy behaviours, the *prediction* process is the predictability of the trustee's behaviours, the *capability* process is the trustee's ability to fulfill their promises, the *intentionality* process is an evaluation of the trustee's motives, and *transference* process is any trust type that was transferred to the trustee

through a trustworthy third-party (e.g., reputation, firm size, or the trustor previous experiences with similar trustees) (Doney and Cannon 1997). Table 1 summarizes the main types of trust in extant literature.

Table 1: Main Types of Trust in Extant Literature

Trust Types	Definitions (contextual)	Dimensions
Interpersonal Trust	Interpersonal trust is " <i>an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon</i> " (Rotter 1967, p.651).	In personal relationships, interpersonal trust includes benevolence and honesty (Larzelere and Huston 1980). Similarly, Rempel et al. (1985) used predictability, dependability, and faith as components of interpersonal trust.
Inter-organizational Trust	Inter-organizational trust is " <i>the extent of trust placed in the partner organization by the members of a focal organization</i> " (Zaheer et al. 1998, p.142).	Inter-organizational trust includes reliability, predictability, and negotiation fairness (Zaheer et al. 1998).
Institutional-Based Trust	Institutional-based trust is derived from the facilitating conditions in terms of formal societal structures at the level of individuals (e.g., individual qualifications), firms (e.g., firm reputation), and intermediaries (e.g., third-party assurance) (Zucker 1986).	In the IS trust literature, institutional-based trust has been operationalized to include structural assurance and situational normality (McKnight et al. 1998, 2002a).
Disposition to Trust (aka propensity to trust)	Disposition to trust is the propensity to trust others (Rotter 1967).	In the IS trust literature, disposition to trust includes the two dimensions of trusting stance and faith in humanity (McKnight et al. 1998, 2002a).

Another integrative model for trust was proposed by Mayer et al. (1995), where trust was defined as the *"willingness of a party 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"* p.712. The authors identified two types of antecedents for trust: one related to the trustee (i.e., competence, benevolence, and integrity) and another concerned with the trustor (i.e., the propensity to trust). This previous research formed the basis for studying trust in the IS literature, as explained below.

2.3. Trust in the IS Literature

Trust has been identified as an essential concept in the IS literature (Söllner et al. 2016). It has been shown to be a critical factor in different contexts, including eCommerce (e.g., (Gefen et al. 2003; McKnight et al. 2002b; Pavlou 2003)), recommendation agents (Komiak and Benbasat 2004, 2006), virtual communities (Kanawattanachai and Yoo 2007; Ridings et al. 2002; Srivastava and Chandra 2018), mobile-payment (m-payment) (e.g., (Chandra et al. 2010)), peer-to-peer lending platforms (Burtch et al. 2014), and social networks (Bapna et al. 2017). The construct has been operationalized as a group of trust beliefs (e.g., (Gefen et al. 2003; McKnight et al. 2002b)) or an overall trust intention (e.g., (Cyr et al. 2007, 2009; Gefen 2000; Hassanein and Head 2007)). Moreover, different classifications have been developed as cognitive-based trust and emotional-based trust (Komiak and Benbasat 2004, 2006), and interpersonal trust and trust in IT artifacts (Lankton et al. 2014; Lankton and McKnight 2011; Paravastu et al. 2014; Pavlou 2003; Söllner et al. 2012). Additionally, various trust antecedents were identified to fit the nature of the different contexts.

In the context of eCommerce and drawing on the theory of reasoned actions (Fishbein and Ajzen 1977), McKnight et al. (2002a) conceptualized trust as a group of *Beliefs* that lead to an overall trust intention, which is the willingness to depend on an eCommerce website's vendor. These trust beliefs include benevolence, competence, honesty, and predictability. In subsequent research, the conceptualization was further adjusted to include only the three beliefs of competence, benevolence, and integrity (McKnight et al. 2002a). These beliefs were conceptualized to capture the users' initial trust (McKnight et al. 1998, 2002a). Users' initial trust is formed before interacting with eCommerce websites (i.e., in the pre-adoption phase). This type of trust has been shown to be influenced by users' traits (e.g., dispositional trust), institutional-based trust (i.e., situational normality and structural assurance), and some cognitive processes, including categorization processes and the illusion of control (McKnight et al. 1998). Moreover, when users start interacting with eCommerce websites, their initial trust will be updated based on their interaction experience and any perceivable clues they might get. As a result, calculative-based trust, institutional-based trust (i.e., situational normality and structural assurance), and knowledge-based trust (e.g., familiarity with the website) were empirically validated to influence users' trust beliefs after their interactions (i.e., in the post-adoption phase) (Gefen et al. 2003).

In the context of recommendation agents, a distinction was made between cognitive-based trust and emotional-based trust (Komiak and Benbasat 2004, 2006). Cognitive-based trust is "*a consumer's rational expectation that a trustee will have the necessary competence, benevolence, and integrity to be relied upon,*" emotional-based trust is "*the extent that a trustor feels secure and comfortable about relying on a trustee*" (Komiak and Benbasat 2004, p.187). Personalization and familiarity were found to be the two antecedents for both types of trust when interacting with a recommendation agent. While the study was the first to offer such classification, these definitions

are limited in the sense that they only encompass the established trust beliefs (i.e., competence, benevolence, and integrity) about the trustee for cognitive-based trust and only the feelings of security and comfortability of relying on that trustee for the emotional-based trust. However, some other rational expectations and feelings can also be drawn from the system's design and can influence users' trust in the system. For example, adding a sense of social presence to an eCommerce website is positively associated with users' trust (Hassanein and Head 2007).

While interpersonal trust is considered a dominant type of trust in the IS literature, several other attempts have been made to explain the nature of trust in IT artifacts. Unlike interpersonal trust, which is based on human-to-human interaction, trust in IT artifacts is based on human-to-technology interaction. For example, trust in IT artifacts might include functionality, reliability, and helpfulness when using social networks such as Facebook or general desktop applications such as Microsoft Excel (Lankton et al. 2014; Lankton and McKnight 2011), predictability and performance when using antiviral software (Paravastu et al. 2014) or performance, process, and purpose when using mobile apps (Söllner et al. 2012).

Recent studies took a different approach to quantifying the effect of trust on intention. For instance, trust was found to be a moderator in peer-to-peer lending platforms, which attenuates the propensity to lend to others when there is a high level of cultural differences between peers (Burtch et al. 2014). Bapna et al. (2017) also provide evidence that social ties (e.g., the number of common friends and peers who are tagged in a photo together and shared posts) in social platforms can drive trust behaviour, which was quantified in terms of the amount that was sent to friends in the platform. Similarly, other measures of informational quality trust are essential in affecting students' propensity to comply with the campus emergency notification systems (Han et al. 2015). In this

context, informational quality trust encompasses the three dimensions of information relevance trust, information actionability trust, and information criticality trust.

Building on the previous discussion, I argue that most IS trust literature was about interpersonal trust and institutional-based trust based on the theory of reasoned action. Moreover, even though some earlier attempts have been made to study knowledge-based trust (Gefen et al. 2003; Gefen 2000), no subsequent work has been done to directly examine the critical role of knowledge in deriving trust beliefs. Earlier research also distinguished between trusting an online vendor and trusting the communication medium (i.e., the underlying IT infrastructure) (Grabner-Kräuter and Kaluscha 2003; Pavlou 2003). However, the latter was assumed to be an "*implicit*" factor that affects trust (Pavlou 2003) or an "*exogenous*" factor (Grabner-Kräuter and Kaluscha 2003). I argue that the uniqueness of each information system design might have different implications for trust. Although various types of trust have been considered, as shown in the above discussion, in many contexts, no precise classification is available to differentiate among them based on the uniqueness of each information system's design. The subsequent trust models were modified based on contextualized factors not necessarily core to the information system's design. In the next section, I elaborate on this idea in the context of Blockchain and explain why trust in Blockchain is a new type of trust in Semi-Autonomous Information Systems.

2.4. Trust in Bitcoin

Blockchain was first introduced as a purely "peer-to-peer" online system that can operate without any central institution (Nakamoto 2008). This unique architecture represents a significant challenge to the status quo of how information systems work and what builds trust in them. The embedded design features shift the power from current information systems that operate in a centralized design to a semi-autonomous decentralized peer-to-peer network interacting under an

“algorithmic authority” (Lustig and Nardi 2015). In this new decentralized paradigm, there is no need for any central entity or even a third-party assurance (Antonopoulos 2014). Historically, and as shown in the earlier discussion, these two elements have been identified as the basis for Structural Assurance, which builds users' trust (e.g., (Gefen et al. 2003; McKnight et al. 2002a)). However, decentralized semi-autonomous Blockchain applications run without these elements (i.e., central authority and third-party protection). Accordingly, trust in semi-autonomous information systems is distinct from interpersonal trust or trust in IT artifacts. Most importantly, the factors building this new type of trust differ indeed.

Bitcoin was introduced as the first application of Blockchain and an e-payment network. In the case of e-payment platforms, previous research shows that the most commonly identified trust antecedents are the vendor's reputation, perceived security protection, and structural assurance (Chandra et al. 2010; Xin et al. 2013). The most noticeable feature of Bitcoin is its underlying algorithms' ability to replace the vendor's role in the e-payment platform as a central entity and to ensure the network of actors involved will act according to users' expectations and best interests. Therefore, vendor reputation is not a factor in this system when considering user trust. However, since Bitcoin is an open system, some illegitimate users have exploited the system to make illicit transactions, creating a bad reputation for the system. Nonetheless, some researchers interviewed some Bitcoin users and reported that users believe that criminals' access to the system might play a higher role for non-users (i.e., the pre-adoption phase) who are considering adopting the system but have less impact on the system's current users (i.e., in the post-adoption phase) (Lustig and Nardi 2015) or the system's credibility (Sas and Khairuddin 2017). Additionally, the actors and the algorithms have created a secure environment for the users to transact their bitcoins. Indeed, in a recent study, Bitcoin users agreed that the insecurity of transactions, in general, is a

user-related error rather than a technology-related error, and they did not express any concern about either the actors (i.e., miners) or the underlying algorithms of Bitcoin as a cause of insecurity (Sas and Khairuddin 2017). Finally, structural assurance is still assumed to be a critical factor affecting users' trust in Bitcoin or any other information system. However, I argue that it stems from the system's unique architecture as a type of semi-autonomous information system. In other words, it is mainly a technological-driven factor and not based on legal protection provided.

As one component of institutional-based trust, structural assurance refers to the legal and technological safeguards that create a secure environment for users (McKnight et al. 2002a, 2002b). The protection provided to the users of Bitcoin is technological. It stems only from the underlying algorithms and not from legal protection for two reasons. First, the global user base of Bitcoin makes it difficult to enforce any regulations developed within any jurisdiction. Second, suppose, arguably, some universal regulations was created; still, no one will have the power to enforce them in a way to revoke or rewrite the history of the ledger. In other words, those regulations will not give a sense of protection to the users. In fact, some Bitcoin users stated that escaping from overregulated online platforms was one reason for them to use the system in the first place (Sas and Khairuddin 2017). As a result, I argue that structural assurance is embedded in the system design and not in the surrounding legal protection.

Several attempts have been made to conceptualize users' trust beliefs in Bitcoin, mainly through qualitative research. Zarifis et al. (2014) interviewed 41 users and non-users of Bitcoin to explore how users trust transacting in this system. They found evidence supporting the importance of the same kind of previous constructs in eCommerce, such as disposition to trust, institutional-based trust, and users' prior experiences using e-payments. Most importantly, they found evidence that more explanation about the system would influence user trust. Still, users' opinions during the

interviews were mixed regarding whether this explanation would negatively or positively influence trust. Likewise, Sas and Khairuddin (2017) interviewed 20 Bitcoin users to explore participants' motivations and experiences in perceiving Bitcoin as trustworthy. The authors identified two Bitcoin characteristics that drive users' trust beliefs: system-related and transaction-related characteristics. System-related characteristics are decentralization, lack of regulation, embedded competencies of miners, and reputation. Transaction-related characteristics are transparency, low cost, ease of use, and secure transactions. Moreover, an early theoretical model proposed by the same authors (Sas and Khairuddin 2015) conceptualized three different layers of trust in Bitcoin: technological, social, and institutional. Similarly, two other conceptual frameworks were developed to describe trust in the Blockchain (Auinger and Riedl 2018; Ostern 2018).

Even though these previous attempts inform our understanding, they are insufficient for four reasons. First, the conceptualization process was based on interpersonal trust and trust in IT artifacts without considering the unique nature of trust in Bitcoin as a type of trust in a Semi-Autonomous Information System. Second, these models did not distinguish between what constitutes trust as components and what affects trust as antecedents. Third, no consideration has been made to clarify the dynamic process of users' interactions with the system and how these interactions influence their cognitive and emotional perceptions to build their trust. Finally, no relevant models or empirical results are available to guide the future design of "trustworthy" similar semi-autonomous information systems in other contexts such as financial services, eCommerce applications, supply chains, and healthcare sectors. What drives users' trust in semi-autonomous information systems are some unique factors embedded within the design of the system, such as Bitcoin.

Bitcoin's users believe in its underlying algorithms instead of any central authority (Maurer et al. 2013; Simser 2015). What makes Bitcoin work is the algorithmic authority, where users transact under the authority of some computer algorithms and a network of actors (i.e., miners) who enable these algorithms to run smoothly (Lustig and Nardi 2015). It is an open network where algorithms can enforce networked actors to behave according to the users' expectations and best interests. Based on the preceding discussion, Table 2 below compares trust in previous information systems research and the uniqueness of trust in Semi-Autonomous Information Systems in the context of Blockchain.

Table 2: A comparison between trust in previous IS research and trust in Semi-Autonomous IS

Factors	Trust in previous IS research	Trust in Semi-Autonomous IS
Cognitive-Based Trust	It is derived from users' rational expectations about the actors involved in the system (i.e., users' trust beliefs of competency, benevolence, and integrity about those actors) (Komiak and Benbasat 2004).	It is derived from users' rational expectations of the system's design.
Emotional-Based Trust	It encompasses users' feelings of security and comfort when using the system (Komiak and Benbasat 2004).	It encompasses all the users' feelings about the system (e.g., perceived control and sense of community).
Interpersonal Trust	It is derived from dyadic seller-buyer relationships.	Not applicable.
Institutional-Based Trust	It is enabled through structural assurance and situational normality	It is assumed to be embedded in the system's design.

	(McKnight et al. 1998, 2002a, 2002b).	
Users' Knowledge	Has been tested only as familiarity (Gefen et al. 2003).	It is expected to influence many trust antecedents.
System's Design	Considered at the interface level by adding a sense of social presence (Hassanein and Head 2007).	It is assumed to drive many trust antecedents (e.g., decentralization and algorithmic authority)
Power / Control	Power is concentrated in a centralized structure.	Power is shared between humans and algorithms.
Algorithmic Authority	It is assumed to be at a minimal level.	It is recognized as a legitimate integral part of the system's design.

Trust in Bitcoin comes from the unique design and the nature of the interactions between humans and algorithms. This particular design of a SAIS is explained in the next chapter through a proposed design theory for trustworthy SAIS.

Chapter 3. A Proposed Design Theory for SAIS

The rise of platform technologies (e.g., Airbnb (Cheng and Foley 2019), Uber (Möhlmann et al. 2021), and Amazon (Delfanti 2021)) has enabled the development of algorithmic control where algorithms, along with humans, control tasks. Within organizational boundaries, this new type of algorithmic control reshapes organizational practices in three areas through the automation process of directing humans (i.e., algorithms tell humans what they can do), the evaluation process (i.e., algorithms evaluate outcomes), and in achieving discipline (algorithms monitor and enforce the rewards and the punishments) (Kellogg et al. 2020; Wood 2021). However, the advent of Blockchain as a distributed ledger technology (e.g., Bitcoin and Smart Contracts) changed the nature of this algorithmic control to be embedded in a decentralized structure. In this structure, the system is accessible, and all entities (i.e., humans and algorithms) can share resources, with no one entity controlling the system or affecting its continuity. As such, a decentralized structure recognizes the capabilities of both humans and algorithms to create meaningful collaboration and, thus, optimal system performance.

While previous studies have informed us about such a phenomenon (e.g., (Bucher et al. 2021; Möhlmann et al. 2021) or discussing its harmful and ethical impacts (Gal et al. 2020; Galiere 2020), not enough explanation has been provided for the underlying enabling information system design of this phenomenon. Indeed, because of the unique underlying information system design, humans and algorithms jointly control tasks. We describe these information systems as Semi-autonomous. On a spectrum, these information systems fall between fully human-managed systems and fully autonomous systems on both ends. In fully human-managed information systems, the level of algorithmic control in the system's design is minimal. Algorithms are used

and act based on predefined rules, and they are mere tools that can be used to carry out specific tasks based on humans' directions and will. For example, Enterprise Resource Planning (ERP) information systems are fully human-managed systems where the mere function of the system is to process inputs received from humans (i.e., manual data entry) or machines (i.e., sensor data) and produce outputs based on a human' or algorithm' request. In contrast, human control in fully autonomous systems is minimal. An example of these systems would be an autonomous network of smart vehicles connected through a peer-to-peer autonomous vehicle leasing system (Miryneck 2019). In this system, vehicles act with a high level of autonomy to share information with other autonomous cars participating in the network. Smart vehicles can engage in economic transactions to be leased to different users based on their pre-recorded availability and price-matching algorithms. Algorithms control all of these activities and tasks. As such, the critical point in distinguishing among these systems is the algorithmic control or algorithmic authority. Algorithmic authority is *the legitimate level of control an algorithm has to enforce specific actions based on its programmable logic*.

The need for SAIS comes from the fact that algorithms are now capable of carrying out some tasks more efficiently than humans (e.g., the matching process between riders and users when using Uber) or other tasks that humans cannot do (e.g., creating consensus in a distributed network when using the Bitcoin system). The defining characteristics of these new designs come from the fact that we would not imagine such systems without both parties (i.e., algorithms and humans). Such systems opened new possibilities for us as humans that we would not have had before. For instance, we can now think about future decentralized systems where algorithmic authority interacts dynamically with human participants to achieve optimality in the system's use of resources. As such, I argue that a design theory for SAIS is needed to explain the nature of such

systems, as the absence of a theory will hinder our ability to achieve synergy in human-computer collaboration (Stephanidis et al. 2019). A good understanding of such design would uncover the nature of each component in the system to benefit theory and generate new evaluation criteria to inform practice. In addition, the findings of previous studies could apply only to fully centralized human-managed systems such as Uber and Amazon with little implications for semi-autonomous decentralized systems. Thus, a design theory is necessary to explain the nature of these new SAIS.

A design theory for an information system defines how it can be designed to be as effective and efficient as feasibly possible (Walls et al. 1992). A design theory for an information system includes a kernel theory, an established theory or theories from natural or social sciences to guide the design theory (Walls et al. 1992, 2004), design principles (Aken 2004; Gregor and Jones 2007), meta-design, which is the evaluation measurement(s) (i.e., propositions/hypotheses) that can be used to assess how well the design theory achieves its goals (Gregor and Jones 2007).

The rest of this chapter is organized as follows: collaborative control theory as the kernel theory for SAIS is first explained (Nof 2007; Nof et al. 2015). Then, three proposed SAIS design principles are discussed per established guidelines (Aken 2004; Gregor and Jones 2007). Afterward, meta-design is described with four propositions (Walls et al. 1992, 2004). Finally, the proposed propositions are articulated as measurable research hypotheses.

3.1. Kernel Theory for SAIS

Collaborative Control Theory (CCT) (Nof 2007; Nof et al. 2015) describes the collaboration among humans, robots, or autonomous systems in completing production tasks. Usually, these systems are enabled through computer-supported and communication-enabled production activities in highly distributed structures (Nof 2007). The theory provides the principles

for designing successful collaborative e-work, e-production, or e-service systems (Nof et al. 2015). The theory principles have been used in developing decision support systems (Nof 2017; Seok et al. 2012) and collaborative factories of the future (Moghaddam and Nof 2017). CCT recognizes human and algorithm capabilities to augment system outcomes through collaboration (Nof 2007; Nof et al. 2015). Unlike traditional centralized system designs, the optimality of the system is achieved through a decentralized structure where participating entities share their resources, information, and responsibilities for mutual benefits (Nof et al. 2015). Thus, human-machine collaboration is the central prevailing topic of the theory.

3.2. Design Principles for SAIS

Human-machine collaboration ensures effective integration between humans and algorithms (Stephanidis et al. 2019), the hallmark of SAIS. Such collaboration adds value to both parties as algorithms can be used to carry out repetitive and automatic tasks. On the other hand, humans can focus more on the tasks that require human judgment and the use of their cognitive abilities. This collaboration is necessary to broaden the scope of tasks that would be otherwise impossible for both parties to do autonomously.

Meaningful collaboration first depends on the idea that all stakeholders recognize algorithms as a legitimate part of the system. Additionally, crafting a successful human-machine integration requires a defined level of autonomy for both parties (Stephanidis et al. 2019) so that each party can work independently and effectively. Finally, SAIS's enabling technology/technologies should protect human participants' privacy and the system's security to be perceived as trustworthy. Indeed, such features should be intrinsic to the design (Tapscott and Tapscott 2016) and not dependent on extrinsic factors. In essence, the three design principles of the proposed new design theory for SAIS are as follows:

1. Collaboration between humans and algorithms in SAIS must be logically and economically justifiable and legitimately accepted by all stakeholders.
2. Humans and algorithms should have autonomy in the system through a decentralized structure.
3. The underlying enabling technologies of SAIS must protect human participants' privacy and the system's security to be perceived as trustworthy.

In what follows, these three principles are operationalized as meta-design for SAIS.

3.3. Meta-Design for SAIS

Figure 4 provides the proposed meta-design properties of SAIS as a process flow. At the very core of the meta-design is human-algorithm collaboration. The starting point is that algorithmic authority must be defined and perceived as a legitimate part of the system. This algorithmic authority needs a decentralized structure to function properly. A decentralized structure defines all the decision points. Then, all decisions need access to relevant data, information, and appropriate resources to make effective and efficient decisions. When using data, information, or any system resource, privacy and security protection should be ensured so that humans can perceive the entire system design as trustworthy. Each of these points is discussed in the following sections.

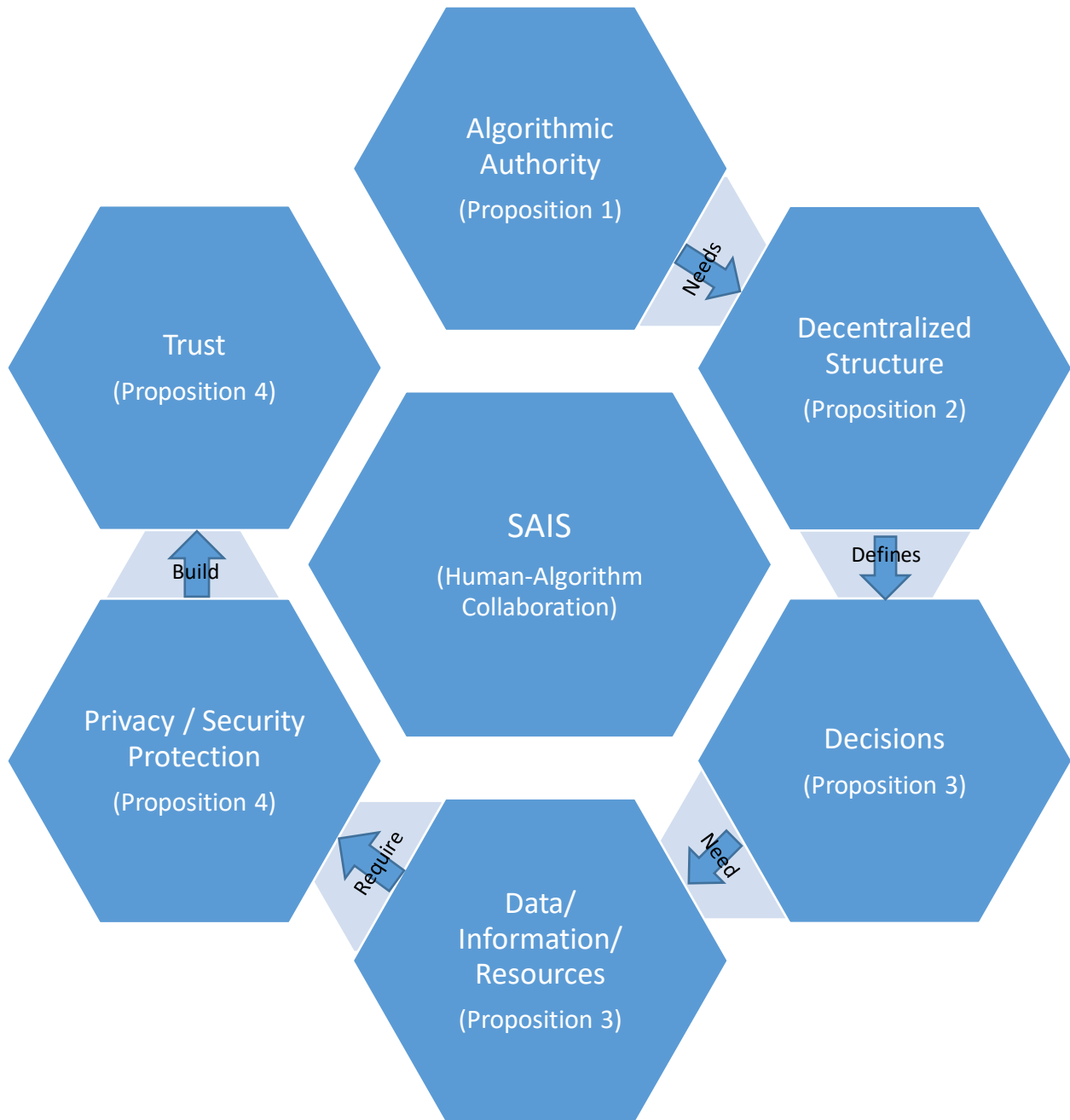


Figure 4: SAIS' Meta-Design Properties in a Process Flow

3.3.1. Algorithmic Authority

Effective Human-Computer integration (Stephanidis et al. 2019) is based on the idea that algorithms and humans need some autonomy. Additionally, and based on CCT, both parties need this level of authority/independence when designing collaborative systems to ensure the system's success (Nof 2007; Nof et al. 2015). Some scholars define Algorithmic Authority as "the legitimate power of algorithms to direct human action and to impact which information is considered true" (Lustig and Nardi 2015, p.743). However, this definition limits the scope of this authority in some aspects. First, the defined scope only includes directing human actions without considering it as a required part of the system design in the first place. Thus, such algorithms should have the power to direct human actions and be an integral part of the system. Additionally, human autonomy should also be recognized so that humans will come to decide what to do, not based on the direction of the algorithm but based on their own judgment, rationale, and choice.

Second, the scope of algorithmic direction should not be restricted to humans only, as we might need the algorithm to direct the work of other algorithms that are part of the system. As such, the scope of this algorithmic authority should include any party subject to such authority, including algorithms and humans. Finally, the ultimate goal of this algorithmic authority is to control some tasks when designing a SAIS, not to impact the trueness of the information. Algorithms work by following programmable logic and always generate true results following this logic. The logic is the pre-defined rules for the algorithm to take certain actions once specific criteria are met. Thus, I define algorithmic authority as *the legitimate independent level of control that allows an algorithm to take and enforce specific actions based on its programmable logic.*

In this definition, I use the word control to represent this authority, as there must be parts in the process that the algorithm can control. For instance, the Bitcoin cryptographic algorithms

are responsible for managing the verification process of transactions and the money supply in the system (Antonopoulos 2017). It should be noted that, in the case of the Bitcoin system, these algorithmic tasks are beyond the capabilities of allocating them to humans to carry them out efficiently. As such, it is crucial to justify why the algorithm(s) and not humans should control this part. Thus, algorithmic authority over this part is justifiable. Besides, this level of algorithmic control is embedded in the system's design and protocol to ensure algorithmic independence. Thus, users know this authority's scope, limits, and ways to modify it.

Even though the mechanical or mathematical characteristics of these algorithms might not be clearly understood by all users, such as in the case of the cryptographic algorithms in the Bitcoin system, their functionality should always be understood in creating consensus among all participating entities and ensuring the system's security. Human interactions with the algorithms and their perception of the underlying algorithmic logic will constitute its legitimacy. The source of this legitimacy is always humans, regardless of who designed the algorithm in the first place, whether one individual or an organization. Thus, humans will perceive algorithmic control as a legitimate part of the system.

Additionally, while the justification of algorithmic authority to control specific tasks efficiently is apparent in the initial design, it has to be enabled through an appropriate alignment structure and enforcement mechanisms. One enforcement mechanism could be when gains from misbehaviours are not justifiable economically. For instance, no economic gains could be realized for any entity to afford the computing resources required to change the history of transactions recorded in Bitcoin. Another way is through punishment techniques such as fines or penalties with harmful consequences to deter disobedience of such authority.

Algorithmic authority in SAIS can be conceptualized at two levels: the system level and the node level. An algorithm can control parts of the system's operations at the system level. For instance, the consensus process and the money supply in Bitcoin are governed by algorithms (Antonopoulos 2017). Similarly, the matching process in Uber is controlled through the underlying algorithm of the Uber platform (Möhlmann et al. 2021). At the node level, an algorithm could be assigned to take specific actions for the human participant(s). For example, a smart contract could control the leasing activity of participating vehicles for human users in a peer-to-peer network (Mirynech 2019). Both levels must be recognizable and appropriately defined when designing a successful SAIS.

Overall, and based on the above discussion, the practical design of SAIS requires an appropriate definition of algorithmic authority as part of the design. This is enabled by recognizing algorithms as a legitimate system part based on their functionality. Algorithmic authority requires appropriate mechanisms to ensure its enforcement power in the system. As such, I propose the following proposition:

P1: *SAIS allows algorithmic authority to be perceived as a legitimate part of the system and supports it with appropriate enforcement mechanisms.*

3.3.2. Decentralized Structure for SAIS

Historically, organizations have gained efficiencies from their centralized organizational structure (Lundy 2016). However, centralized structures have not effectively served some unique local requirements of the business units or achieved organizational agility by responding quickly to customers (Fan et al. 2003). An organizational structure defines the allocation of decision rights, the incentive system, and the monitoring system used to measure organizational actions and outcomes (Jensen and Meckling 1992). Centralized structures have decision rights at the top levels

of the hierarchical structure. In contrast, decentralized structures allocate decision rights to levels where information and expertise lie for optimal decisions. In centralized structures, the incentive and the monitoring systems are designed and managed by a single authority. However, decentralized structures distribute this authority at appropriate levels so that resources are justifiable from an economic perspective at corresponding levels of authority.

In addition, while the incentive structure in a decentralized structure is ensured at different sub-levels, system optimality is also guaranteed through an effective alignment/coordination function design. For instance, through the Bitcoin protocol, participating parties' separate interests are aligned/coordinated to serve the system's optimal performance. It is done through the economic incentive system embedded in the system's design, where all participants are motivated from a monetary standpoint to act according to the system's best interest, not to the best self-interest. It happens when the optimization of the self-interest needs of parties intersects with the system's optimization function. According to Shermin (2017), that was done by the invention of the "token," where a "token to humans is like code to algorithms." That is, while algorithms follow some pre-defined rules to optimize their gains in the systems, the structure also optimizes humans' gains with value tokens from an economic perspective. Thus, while both parties reap benefits from engaging in economic activity, system optimization happens when the system's outcomes transcend the individual units' bilateral cost/benefit analysis and maximize the system's performance. For example, while the mining nodes in Bitcoin are motivated by gaining some transaction fees and a pre-defined reward of newly issued digital coins (i.e., tokens), with more transactions and more new nodes added to the system, the level of security is also increased as it will be harder and harder to compete against more computing resources devoted in the system.

Decentralization promotes “resilience” in data storage and “freedom from concentrated power” (Walch 2019). Decentralization, as a design feature in information systems, facilitates the system’s resilience because data can be stored in different geographical places (i.e., data redundancy), and no one node has a dominant power in the network. Furthermore, and based on CCT (Nof 2007; Nof et al. 2015), designing a successful decentralized e-system (e.g., human-managed system, semi-autonomous, or autonomous system) requires a design where all participating entities (i.e., human and algorithm) can exercise power in affecting the system’s outcomes. A decentralized system requires every node to affect the system’s outcome based on power-sharing and available resources. In essence, a decentralized SAIS is *a system that is collaboratively managed and accessible to humans/algorithms in a network where participating entities share inputs (i.e., resources, data/information) and influence the system’s outputs with no single entity playing a dominant role in the operation of the system.*

This definition recognizes that collaboration between humans and algorithms is needed for a decentralized structure to work. This definition also acknowledges that both parties must have autonomy in decision-making by recognizing them as decision-makers. A decentralized structure operates in a collaborative network of entities with a need and a purpose for having such collaboration. Further, the above definition emphasizes accessibility to resources and data/information for all entities to ensure efficient and effective decision-making. Thus, information flow and resource allocation are optimized at the level of each decision-maker. Finally, no single entity plays a dominant role in operating the system (i.e., no single point of failure) to protect the system’s continuity and survivability. As such, and based on the above discussion, I propose the following proposition:

P2: *A decentralized structure of SAIS ensures effective and efficient human-algorithm collaboration.*

3.3.3. Decisions

The design of an information system mirrors the organizational structure and the types of information flow required to support all the different organizational functions (Fan et al. 2003). From a technical perspective, information technology structures can be classified into five types: centralized computing structure (i.e., low decentralized processing, low network connectivity, and no shared data and applications); decentralized computing structure (i.e., high decentralized processing, low network connectivity, and no shared data and applications); hub-and-spoke structure (i.e., low decentralized processing, high network connectivity, and no shared data and applications); distributed computing structure (i.e., high decentralized processing, high network connectivity, and no shared data and applications); and cooperative computing structure (i.e., high decentralized processing, high network connectivity, and high in shared data and applications) (Fiedler et al. 1996).

Effective information systems' design for organizations calls for decision-makers to have timely access to required information (Brynjolfsson and Mendelson 1993). Every single decision point in the underlying structure should first be identified and equipped with the relevant information and the required resources to ensure effective and efficient decisions. While previous centralized structures were sufficient in matching the flow of information with the needs of every decision point, the speed and the complexity of decisions could now be hindered by centralized structures in two ways. First, centralized structures were built to match only human-decision markers' needs. However, information systems now include algorithms as decision markers. Unlike human decisions, algorithms require different inputs for their decisions. These inputs are

usually complex and beyond the capabilities and the speed of humans' capacities. For instance, in a distributed network to manage solar power tokens for users using smart contracts, the instructions for triggering certain decisions by the smart contract will be based on some inputs from sensors associated with the solar power cell and the requests received from the network. Thus, a decentralized structure meets the need for human and algorithm decisions. Second, to ensure flexibility in the decision-making process, the nature of decisions at each node could be modified to include more (less) decisions by algorithms (humans). For example, a user could implement new programs to sell digital tokens in the previous solar power decentralized system. A central structure cannot manage such inputs, but a decentralized structure is required to ensure the flow of new relevant decision inputs at all levels. A decentralized structure allows for such flexibility where the needs of the decisions could be modified at the node level without central approval. Thus, I argue that a decentralized structure recognizes algorithms as decision-makers with humans. It also ensures accessibility to relevant information and resources for all decision-makers. Therefore, decisions are assumed to be efficient, effective, and flexible. As such, I argue for the following proposition:

P3: *A decentralized structure of a SAIS should facilitate accessibility to relevant data, information, and resources to match the needs of each decision-maker in the system.*

3.3.4. Security and Privacy Lead to Trust

Trust is critical in all social interactions, including personal relationships (e.g., (Rempel et al. 1985), interpersonal relationships (Mayer et al. 1995), and inter-organizational relationships (Zaheer et al. 1998). Historically, institutions have created environments for individuals to transact safely through societal structures at the level of individuals (e.g., individual qualifications), firms (e.g., firm reputation), and intermediaries (e.g., third-party assurance) (Zucker 1986).

Subsequently, different types of trust have been conceptualized and validated in various contexts, including eCommerce (e.g., (Gefen et al. 2003; McKnight et al. 2002a; Pavlou 2003)), mobile-payments (m-payments) (e.g., (Chandra et al. 2010)), and even peer-to-peer lending platforms (e.g., (Burtch et al. 2014)).

In eCommerce, previous IS trust research was developed and tested in centralized human-managed systems. As a result, the factors that usually drive trust include a combination of interpersonal trust factors. For example, initial trust research focused on the three users' trust beliefs of integrity, competency, and benevolence toward web vendors (McKnight et al. 2002a). In addition, some other institutional-based factors were shown to be relevant in driving users' trust feelings, such as structural assurance (e.g., where the interaction environment with any online vendor is perceived safe) and situational normality (e.g., where users feel the online environment is somehow similar to what they used to see offline) (McKnight et al. 2002a, 2002b). Moreover, earlier research also distinguished between trusting an online vendor like Amazon and the communication medium, such as the IT infrastructure enabling Amazon to function (Grabner-Kräuter and Kaluscha 2003; Pavlou 2003). However, the latter was assumed to be an "implicit" (Pavlou 2003) or an "exogenous" (Grabner-Kräuter and Kaluscha 2003) factor in affecting users' trust feelings. In a fully human-managed system, all the factors that could drive users' trust feelings are anchored on humans (e.g., trust feelings about online vendors), and the underlying enabling technology design was not proven relevant. In other words, feelings toward the human online vendors subsumed feelings related to technological design and its ability to drive users' trust beliefs. However, Blockchain has enabled a new type of trust.

Blockchain has created a system to generate trust (Berkeley 2015) that is accessible to all entities (i.e., humans and algorithms). Blockchain has enabled individuals to transact freely

without needing a central entity or intermediaries to ensure trust. For example, Bitcoin was designed as a network protocol that enables cryptographic algorithms, and the networked actors share the responsibility of running the system without a central entity or a trusted third party. I argue that this new type of trust comes from the unique system architecture of Bitcoin, which is an example of SAIS.

Trust in Bitcoin is embedded in the system design. In other words, trust is "intrinsic" and not extrinsic to the platform or the application (Tapscott and Tapscott 2016). First, user privacy is a by-design feature in the system. For instance, the anonymity feature in Bitcoin has enabled privacy protection for the users as they are identified in the system only by their digital identities and not through their real identities (Antonopoulos 2017; Nakamoto 2008). Second, security is also enabled as a by-design feature in the system. For instance, the cryptographic algorithms in Bitcoin verify the authenticity of all transactions (Antonopoulos 2017). They also create consensus among all participants when adding transactions to the ledger records. This ledger is also distributed across the network to create data redundancy. As such, security is enhanced as it is harder for an entity to mathematically afford to change the history of transactions across all nodes, significantly when this history is consistently updated automatically once a new block of transactions has been added every ten minutes (Antonopoulos 2014, 2017). As such, because of the unique design of a system like Bitcoin as a SAIS, where privacy and security are ensured as by-design features, users perceive the system as trustworthy. Hence, I posit the following proposition:

P4: *SAIS design ensures the privacy of human participants and the system's security so that it can be perceived as trustworthy.*

The next chapter presents a proposed model for trust in Bitcoin as an example of SAIS that is informed by the above design theory.

Chapter 4. Research Model and Hypotheses

The extant IS literature has investigated trust in centralized human-managed information systems. Trust was usually conceptualized as a combination of interpersonal trust (i.e., trust beliefs of benevolence, competence, and integrity) and institutional-based trust (i.e., structural assurance and situational normality). However, Blockchain has allowed us to create SAIS, which is where humans and algorithms are responsible for running the information system. These new systems are decentralized, and there is a meaningful human-computer integration where human actors and algorithms have autonomy. Thus, the nature of trust in these new systems differs from previous types of trust investigated in the IS literature. Notably, the factors that drive each type of trust are indeed different.

As discussed in Chapter 2 and as part of the literature review, some established factors can still be relevant in building users' trust in Bitcoin. These factors are users' trust beliefs in actors (i.e., miners), calculative-based trust, and structural assurance. Hence, established factors in the IS trust literature are included in the model but not hypothesized. Then, Chapter 3 showed a proposed design theory for trustworthy SAIS and identified four new hypotheses for algorithmic authority, decentralization, sense of control, and privacy and security protection to build users' trust in SAIS. Since security and privacy protection have already been proven to be positively associated with users' trust in information systems (Chandra et al. 2010; Xin et al. 2013), they are not included in the proposed model. Thus, only the three factors of decentralization (H1a), algorithmic authority (H2a), and perceived control (H3) were hypothesized in the model. In addition, the model includes decentralization (H1b) and algorithmic authority (H2b) to be positively associated with perceived control, as discussed in Chapter 3. Figure 5 below shows the proposed new model

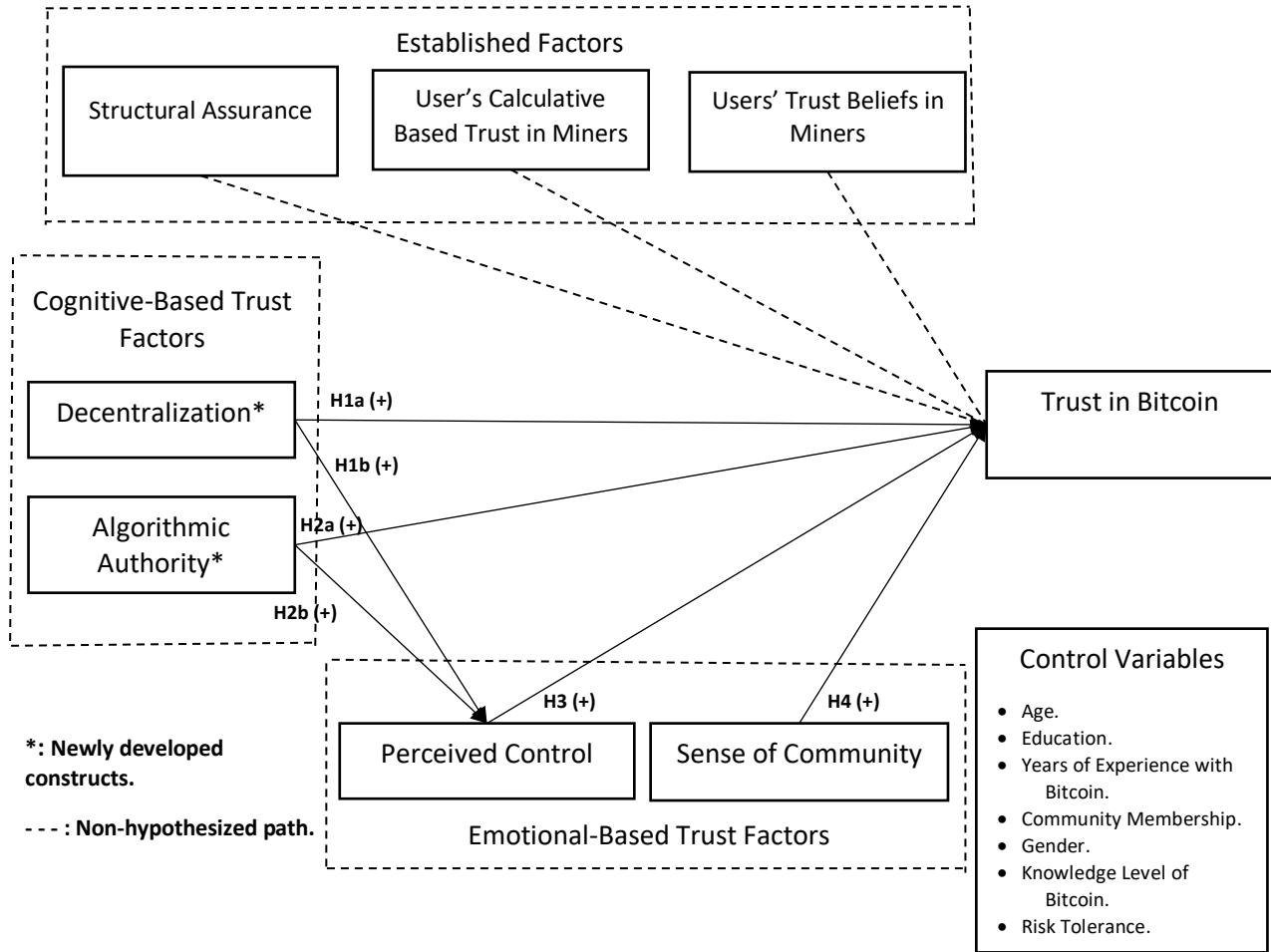


Figure 5: Proposed Research Model

In the proposed model, decentralization and algorithmic authority are proposed as new cognitive-based trust constructs to reflect users' "rational expectations" about the system's operation. The model also includes perceived control and sense of community as two types of emotional-based trust to capture users' "feelings" when interacting with the system and its online communities. In the model, trust is conceptualized as an overall assessment of the system's reliability and trustworthiness (Gefen 2000). This approach tends to be parsimonious (Schlosser et al. 2006) and has been utilized and validated in several previous research studies (e.g., (Cyr et al. 2007, 2009; Gefen et al. 2003; Hassanein and Head 2007)). I chose Bitcoin as the context of

this research to develop and validate this new model of trust in SAIS. As a SAIS, Bitcoin is managed by human actors (miners) and algorithms (i.e., cryptographic algorithms). In addition, the underlying decentralized structure of the system enables both users to have control (i.e., perceived control) and algorithms (i.e., algorithmic authority). The system is also supported by online open communities for all users and nonusers. The following sections cover hypothesis development for the model.

4.1. Established Factors⁷

Bitcoin was introduced as the first cryptocurrency e-payment application based on Blockchain. In the context of e-payment platforms, previous research showed that the most commonly identified trust antecedents are the vendor's reputation, perceived security protection, and structural assurance (Chandra et al. 2010; Xin et al. 2013). Bitcoin does not have a vendor, so users can utilize its reputation to build their trust in the system. This user-vendor relationship has been replaced with two other relationships in Bitcoin: user-actor and user-algorithm relationships. Therefore, I argue that users' trust in Bitcoin is a combination of established trust beliefs (i.e., integrity, competency, and benevolence) about those actors (i.e., miners) and the underlying algorithms of the system.

The underlying cryptographic algorithms govern the interaction with those actors. Thus, the security protection comes from the system's design. Indeed, in a recent study, Bitcoin users agreed that the insecurity of transactions, in general, is a user-related error rather than a system-related error, and they did not express any concern about the actors (i.e., miners) or the underlying

⁷ Please note that as these relationships have been empirically validated in many previous research studies as discussed in Chapter 3, the purpose here is to provide the rationale to examine them in the context of this research without developing hypotheses.

algorithms of the Bitcoin as a cause of insecurity (Sas and Khairuddin 2017). Similarly, structural assurance is still assumed to be a critical factor affecting users' trust in Bitcoin, as we cannot imagine any interaction between users and an information system without some level of protection. Bitcoin protection, however, comes from its unique technological design as a semi-autonomous information system based on its technological architecture without the need for any legal protection.

As such, I propose that users' trust beliefs in actors, calculative-based trust, and structure assurance are still established factors that affect users' trust in Bitcoin. In the following sections, I discuss these factors in more detail.

4.1.1. Users' Trust Beliefs in Actors

A fundamental concept in Bitcoin is replacing the central vendor with a network of actors interacting under the algorithmic authority (Lustig and Nardi 2015). This unique design has enabled both the actors and the underlying algorithms of cryptography to form the system as a semi-autonomous information system. Indeed, the system would not be possible without the role of the two parties. As such, users' trust in the system would be affected by the actors involved. Actors in Bitcoin are other users who opted to be miners. It must be noted that trust in other users (i.e., non-miners) is thought not to affect trust in Bitcoin (Antonopoulos 2014; Werbach 2018) and, as such, is not considered here as part of the users' trust beliefs in actors. Indeed, whether other users are competent, have integrity, or are benevolent does not bear on the users' trust in the system because these users' beliefs have no impact on the users' interaction experience or the expected outcomes of using the system.

In the context of this research, users' trust beliefs are conceptualized to include the three beliefs of competency, integrity, and benevolence (McKnight et al. 1998, 2002b). These beliefs

are established and have been proven to be the building blocks of trust when users interact with different IT artifacts (e.g., eCommerce websites (McKnight et al. 2002a)). However, these trust beliefs have always been related to the central party who provides the service (e.g., an online vendor in the case of eCommerce). This has been the case as this central party holds all the responsibilities towards the end-users and usually aims to provide users with a trustworthy service or product. In Bitcoin, miners are part of the system but are not the entire system. As such, users must trust these actors to have trust in Bitcoin. Indeed, without miners being competent in carrying out their respective roles, users would not trust the system.

Similarly, if users do not believe in the integrity of those actors, they will not trust the system. However, the benevolence of those miners might not be a factor in forming these beliefs. This is the case as Bitcoin is designed in a way that does not allow the actors to behave in ways that are not in line with the users' best interests. Nevertheless, given that people have associated trust in different situations with their perceptions of the benevolence of the other parties involved throughout human history, it is probably the case that many Bitcoin users will continue to do the same when assessing their trust in the Bitcoin actors. This will especially be the case for users who do not fully understand the intricacies of the system's design and operations. Therefore, users' perceptions of benevolence will likely continue to play a role in forming their trust beliefs in Miners, consequently influencing their trust in the system. Additionally, there has been a call to check the relative importance of these three beliefs (Schoorman et al. 2007), and to the best of my knowledge, no previous research has investigated this relative importance as embedded in the context at hand.

4.1.2. Calculative-based Trust

From an economic cost-benefit analysis, calculative-based trust implies that engaging in opportunistic behaviours that might harm trustees is not justifiable to the trustors (Doney et al. 1998). In the context of eCommerce, this factor has been positively associated with users' trust (Gefen et al. 2003). That is, when users believe that the trustor will gain no economic benefits by not being trustworthy, users will trust that trustor more. Similarly, in the context of Bitcoin, the system's users are expected to form some expectations about those actors involved in the system as miners. Miners are motivated to behave in a trustworthy manner, as once the users lose their trust in the system, the entire system will be worthless. That is, what makes Bitcoin valuable is the users' trust in it.

Miners are also system users and are rewarded with newly generated bitcoins. Thus, they are directly affected by any adverse consequences of misbehaviour, just like any other user. Furthermore, it is not a rational economic decision for miners to use a gigantic amount of resources to change the history of transactions. Thus, users will lose their trust in the system. Therefore, the system's value will diminish. Consequently, such calculations about miners could positively affect the perceived system's trust level. As such, Calculative-based trust is also included as another established factor in the proposed model.

4.1.3. Structural Assurance

As a component of institutional-based trust, structural assurance refers to the legal and technological safeguards that create a secure environment for users (McKnight et al. 2002a, 2002b). Structural assurance has been proven essential to building users' trust in information systems (Gefen et al. 2003; McKnight et al. 1998, 2002a, 2002b). This is the case as users cannot trust an information system they feel unsafe about or lack protection within. In Bitcoin, the

protection provided to the users is technological and stems only from the underlying algorithms and not from any legal protection. In other words, the unique design features of Bitcoin give the users this sense of protection. Traditional legal protection, in this context, is assumed to be a less important factor as it lacks the enforcement power to revoke transactions and cannot enforce a change in the system unless it has been approved by at least 51% of the entire global network of the system. Accordingly, the existence of those regulations might not be an essential factor in giving a sense of protection to the users. Some Bitcoin users stated that escaping from overregulated online platforms was one of the reasons they used the system in the first place (Sas and Khairuddin 2017). As a result, I argue that structural assurance is embedded in the system design and not in the surrounding legal protection and will still play a positive role in affecting users' trust in the system.

4.2. Cognitive-Based Trust

Cognitive-based trust refers to the users' "*rational expectations*" that the trustee is competent, benevolent, and has integrity (Komiak and Benbasat 2004). Privacy protection, security protection, system reliability, and information quality in eCommerce have been identified as cognitive-based trust factors (Kim 2005; Kim et al. 2008). These factors are essential in building users' trust in any information system, including a semi-autonomous one such as Bitcoin. As such, I propose decentralization and algorithmic authority as two new types of cognitive-based trust, as these two features are embedded in the system's design of Bitcoin and might influence users' trust in the system.

4.2.1. Decentralization

Larger organizations can gain more efficiency and reduce costs from their centralized organizational structures (Lundy 2016). Decentralization, on the other hand, enables organizations

to be more innovative and respond quickly to the market (Fan et al. 2003). The design of an information system mirrors the organizational structure and the types of information flow required to support all the different organizational functions (Fan et al. 2003). An organizational structure defines the allocation of decision rights, the incentive system, and the monitoring system used to measure the outcomes of organizational actions (Jensen and Meckling 1992). Centralized structures have the decision rights at the top levels of the hierarchical structure, while decentralized structures allocate some decision rights to the lower levels.

Effective information system design for organizations requires co-locating the information flow with the decision rights (Brynjolfsson and Mendelson 1993). From an information technology perspective, information technology structures can be classified into *centralized computing structure* (i.e., low decentralized processing, low network connectivity, and no shared data and applications), *decentralized computing structure* (i.e., high decentralized processing, low network connectivity, and no shared data and applications), *hub-and-spoke structure* (i.e., low decentralized processing, high network connectivity, and no shared data and applications), *distributed computing structure* (i.e., high decentralized processing, high network connectivity, and no shared data and applications), and *cooperative computing structure* (i.e., high decentralized processing, high network connectivity, and high in shared data and applications) (Fiedler et al. 1996).

Blockchain was born as a network, and decentralization is one of its core concepts (Scott et al. 2017; Shermin 2017; Walch 2019). Several attempts have been made to conceptualize decentralization in the context of cryptocurrencies (e.g., (Shermin 2017; Walch 2019)). From the information technology perspective, the current structure of Bitcoin can be classified as a cooperative computing structure. Decentralization in the context of Bitcoin is based on the two

dimensions of resilience in data storage and freedom from concentrated power (Walch 2019). As a design feature in an information system, it enables the system's resilience because data can be stored in different nodes in the network, and no node has a dominant power in the system. Based on Collaborative Control Theory (Nof 2007; Nof et al. 2015), designing a successful decentralized e-system (e.g., human-managed system, semi-autonomous, or autonomous system) requires a design where all nodes *have* and *can* experience power in affecting the system's outcomes. A decentralized system also requires every node to affect the system's outcome. As a decentralized system, Bitcoin gives each node (i.e., user) in the network equal power to verify, record, and store the ledger of transactions. Indeed, no single node has an overall power in the system or can threaten the system's continuity. In the context of this research, I define decentralization as *is the extent to which an information system is collaboratively managed and accessible by entities (e.g., humans or algorithms) where all participating entities share inputs (e.g., computing resources, data/information) and affect the system's outputs with no single entity playing a dominant role in the operation of the system.*

Traditionally, centralization was a driving means to build users' trust since there was always someone accountable in control (i.e., someone who held the responsibility by law) if things went wrong at any time. However, this centralized design allows unauthorized access to the users' data (Pureswaran and Brody 2015). Decentralization, on the other hand, eliminates the need for participants to be "trusted," and there is "*no single point of failure*" (Pureswaran and Brody 2015). That is, users trust decentralized information systems because there is no single point of failure in the system's design, and there is no need to trust other involved parties as they do not have power over the users. Additionally, decentralization restricts power abuse over individual users and thus is associated with trust (Sas and Khairuddin 2017). As such, the higher the perception of the

decentralization of a semi-autonomous information system, the higher the users' trust in the system will be. Thus, I hypothesize that:

H1a: Decentralization, as a design feature in Bitcoin as a semi-autonomous information system, will be positively associated with users' trust in Bitcoin.

Bitcoin users also believe decentralization diminishes the need to trust anyone, even third parties, when making online transactions (Sas and Khairuddin 2017). That is, decentralization as a design feature distributes the power structure among users, allowing them to impact the system outcome and thus feel more in control. As a result, the higher the perception of decentralization, the higher the perception of perceived control. Hence, I hypothesize that:

H1b: Decentralization, as a design feature in Bitcoin as a semi-autonomous information system, will be positively associated with users' perceived control.

4.2.2. Algorithmic Authority

Human-computer integration is based on the idea that both algorithms and humans need autonomy (Stephanidis et al. 2019). This autonomy requires assigning a defined level of authority to each party in the system's design. Additionally, the underlying philosophy of collaborative control theory recognizes the need to assign some authority to algorithms or autonomous systems to ensure the success of any collaborative e-systems (Nof 2007; Nof et al. 2015). In the context of this research, I define Algorithmic Authority as *the legitimate independent level of control an algorithm has to take and enforce specific actions based on its logic.*

Bitcoin is designed in a way that gives its underlying algorithms authority in directing human actions. The underlying proof-of-work algorithm can create consensus among nodes on

which transactions are valid⁸ and thus should be recorded in the ledger. It also adjusts the difficulty of the mining challenge⁹ according to the available computing power in the network so that a block of transactions is added precisely every ten minutes. As a result, it controls the supply of the coins in the system.

Unlike human beings' actions, algorithms' outcomes are predictable. This predictability has always been associated with a higher perceived level of trust (Lustig and Nardi 2015). However, a certain level of authority has to be guaranteed in the system's design to ensure predictability. As a design feature in semi-autonomous systems, algorithmic authority can provide some user protection. For instance, the underlying algorithms in Bitcoin control the number of bitcoins produced, making Bitcoin an anti-inflationary system that can restore users' trust in money (Simser 2015). As such, the higher the perception of algorithmic authority, the higher the perception of trust in the system. Thus, I hypothesize that:

H2a: *Algorithmic Authority, as a design feature in Bitcoin as a semi-autonomous information system, will be positively associated with users' trust in Bitcoin.*

Algorithmic authority, on the other hand, reduces the vulnerability of the users to humans' actions as algorithms are designed to enforce specific actions that are in the best interest of all users. This makes users perceive that they are empowered in the system. The system's design also gives them a unique digital key to sign and control their wealth. Hence, users feel in control and decide when and how to spend their money. The higher the perception of algorithmic authority, the higher the perception of perceived control. Thus, I hypothesize that:

⁸ Each node in the network can check the validity of transactions by checking the mathematical relationship between the public and the private key of submitted transactions (Antonopoulos 2017).

⁹ The mining challenge is that miners have to produce a hash outcome of the proposed block's header that is mathematically less than the challenge number which is known as "nonce" and is part in the new added block's header so that all node can check that immediately and add the new block (Antonopoulos 2017).

H2b: *Algorithmic Authority, as a design feature in Bitcoin as a semi-autonomous information system, will be positively associated with users' perceived control.*

4.3. Emotional-Based Trust

Originating from interpersonal relationships, emotional-based trust is about the users' "feelings" of security and the comfortability of relying on a trustee (Komiak and Benbasat 2004). In the context of eCommerce, reputation, presence of third-party seals, referral, recommendation, buyers' feedback, and word-of-mouth have been identified as emotional-based trust factors (Kim 2005; Kim et al. 2008). These factors have always been about the vendor, the third party, or other social actors without considering the underlying IS design and how it might affect trust. In this research, I am focusing on new emotional-based trust factors that can be derived from the unique IS design of Bitcoin. These new factors include perceived control and a sense of community, two types of emotional-based trust.

4.3.1. Perceived Control

Interacting with eCommerce platforms generally implies some levels of uncertainty, complexity, dependency, and vulnerability (Gefen 2000; McKnight et al. 1998; Pavlou 2003) that are usually out of the users' control. Users' perception of some level of control when interacting with the technology is assumed to mitigate such complexity, as users can predict the outcomes based on how much control they perceive. Perceived control refers to a "belief in one's ability to command and exert power over the process and the outcome" of the interaction with the technology (Collier and Sherrell 2010, p.492). Bitcoin is designed to give users control over their bitcoins by locking all their coins with the user's private key. Without this private key, no one can have control over these coins. This is why when users lose their private key, the coins are considered to be lost forever. When users want to send their coins to others at any time, they use

that private key to sign their transactions, and all other nodes in the network will approve such transactions because of the attached private key (Antonopoulos 2017). Once transactions are validated, they are recorded in the ledger and become immutable. It is practically impossible for anyone to revoke these transactions by affording an enormous amount of computing power to change the entire ledger. As a result, Bitcoin users have control over making transactions, and they can predict the outcome of these transactions upfront.

Perceived control will boost users' trust in the technology as the outcomes of their interactions with the technology depend, even if partially, on their own actions. Users with little experience with the technology rely on some measures, such as their perceived level of control, to determine their level of trust in the technology (Lee and Turban 2001). Additionally, Bart et al. (2005) found evidence that perceived control significantly impacts users' trust in 25 different websites. Indeed, perceived control positively influences the users' trust even when they must share their personal information online (Eastlick et al. 2006). As embedded in the system's design, Bitcoin users feel complete freedom and control over their bitcoins (Sas and Khairuddin 2015). Indeed, Bitcoin is the "*financial freedom*" for its users (Lustig and Nardi 2015). Accordingly, the higher the perception of perceived control, the higher the level of trust in the system. Thus, I hypothesize that:

H3: Perceived control, as a design feature in Bitcoin as a semi-autonomous information system, will be positively associated with users' trust in Bitcoin.

4.3.2. Sense of Community

As a distributed universal network of users, Bitcoin is built on collaboration among the users in sharing resources and information about the system (Fares and Hassanein 2019). This collaboration is not only enabled through the technical protocol but also through online social

communities that are devoted to the system. We cannot think about Bitcoin without its online communities (Antonopoulos 2017). Generally, users join online communities to fulfill their needs for “*belongingness*,” for being “*socially connected and recognized*,” or to interact with “*like-minded*” individuals (Laroche et al. 2012). Online communities can be classified as communities for interest (i.e., shared interest and expertise), for relationship (i.e., forming meaningful personal relationships), for fantasy (i.e., fantasy and entertainment), or transaction (i.e., information sharing among the members) (Armstrong and Hagel 1997). For the context of this research, a sense of community refers to a “*feeling that the members of a community have in relation to their belonging to a community, a feeling that members worry about each other and that the group is concerned about them, and a shared faith that the needs of the members will be satisfied through their commitment of being together*” (McMillan and Chavis 1986, p.9).

Bitcoin communities include users, crypto enthusiasts, tech developers, media, financial institutions, and various startups (Bitcoin.org 2020). The essential role of these communities is to disseminate knowledge about the system in different aspects, including general discussion, technical issues, and mining (Bitcointalk.com 2019). Moreover, these communities are offered in many other languages to be accessible to almost everyone without any language barrier. These communities can be classified into two types: for shared interest and for sharing knowledge. Bitcoin users enjoy communicating with each other about matters important to their learning and any proposed role of the Bitcoin community to protect the system's future (Lustig and Nardi 2015). Information sharing often reduces uncertainty and information asymmetry and increases predictability (Laroche et al. 2012).

Furthermore, Bitcoin users can also share any matter deemed to be relevant to the community. Accordingly, Bitcoin users, as part of this community, obtain knowledge about the

system and can have a say in any aspect related to the system. Thus, having a sense of community would reduce uncertainty and information asymmetry and make the system more predictable, reliable, and trustworthy. Therefore, I hypothesize that:

H4: *The sense of community, as an essential feature of Bitcoin as a semi-autonomous information system, will be positively associated with users' trust in Bitcoin.*

4.4. Control Variables

As per established norms in the IS research, some control variables will be examined in the context of this research. In particular, I suggest that the four variables of Knowledge, Gender, Risk Tendency, and Community Membership might impact the tested relationships as discussed below.

4.4.1. Users' Knowledge of Bitcoin

Users form their trust beliefs based on their knowledge about an information system, and then, after gaining experience, this knowledge creates familiarity with the system (Gefen 2000). Therefore, knowledge is the underlying concept of any trust belief. In the context of Bitcoin, I define users' knowledge as their level of understanding of how Bitcoin works, including the role of actors (i.e., miners) and the characteristics of the underlying algorithms. Based on the level of user knowledge, they can assess whether the system is reliable and trustworthy. Most importantly, users can assign relative importance to the factors that might influence their level of trust in the system. Zarifis et al. (2014) interviewed 41 users and non-users of cryptocurrency to explore users' trust in the system. The authors found evidence that more explanation about the system would influence the level of users' trust. Still, opinions were mixed on whether it would negatively or positively influence trust. I argue that since Bitcoin is a newly developed unique system and given

its complex nature, knowledgeable users might assign more importance to its features, such as decentralization and algorithmic authority over the established factors of the users' trust beliefs in the involved actors. This is the case as the system was designed in a way to enable those algorithms to ensure that the actors will behave following the users' expectations and best interests. On the other hand, less knowledgeable users may resort to the traditional assignment of trust in the human actors involved. As such, the role of users' knowledge in affecting the proposed relationships in the research model will be explored.

4.4.2. Gender

Users' gender choices have been shown to affect the factors contributing to their overall trust level when interacting with eCommerce platforms (Awad and Ragowsky 2008). This has also been corroborated by some neuro-IS evidence (Riedl et al. 2010). Given the fact that there are two groups of factors in this proposal (i.e., cognitive-based and emotional-based trust), gender might have an impact on the importance of these factors. Thus, Gender will be examined in the context of this research.

4.4.3. Risk Tolerance

Technology-perceived risks are those potential threats associated with using a particular technology and are negatively related to the perception of trust in the technology (Pavlou 2003). It has been proven that perceived risks also have a negative impact on adopting information systems (Featherman and Pavlou 2003; Luo et al. 2010; Marriott and Williams 2018; Pavlou 2003). Surprisingly, however, perceived risks have not been shown to negatively affect Bitcoin users' adoption of the technology (Arias-Oliva et al. 2019; Mendoza-Tello et al. 2018; Walton and Johnston 2018). An interesting explanation is that Bitcoin users might hold a high-risk tolerance (i.e., the propensity to take a risk) toward the system. Therefore, they do not perceive any risks

associated with the technology. However, given that this new technology has caused a shift in the nature of trust, it might be risky for some people to trust it without traditional established trust factors and to put their trust in the technology only without any legal protection. Hence, I argue that risk tolerance might also affect some of the proposed research model's proposed relationships.

4.4.4. Community Membership

Bitcoin users who are members of any online community about Bitcoin might see the value of such membership and might have different evaluations of the underlying suggested factors to influence their level of trust in the system. Importantly, having such membership is expected to increase the suggested benefit of feeling more about the sense of community and thus trusting the system more. Likewise, members of online communities might have a higher sense of control as they see this community membership as a way to have a say and influence the system and, therefore, put more trust in the system. Thus, I added community membership as an additional control variable to be tested in the model.

As decentralization and algorithmic authority are both new constructs, Chapter 5 discusses a scale development process that was carried out for the two constructs. Chapter 6 then presents the research methodology to validate the suggested model empirically. Finally, Chapter 7 discusses the thesis' contributions, limitations, and future research.

Chapter 5. Scale Development

Chapter 3 of this thesis presented a new proposed design theory. The two unique factors of decentralization and algorithmic authority have been identified as critical elements in designing trustworthy SAIS. These two new factors have been further developed as hypotheses in Chapter 4 as part of a larger trust model. However, the IS literature lacks scales for these new factors. Thus, this chapter discusses scale development for perceived decentralization and perceived algorithmic authority following Mackenzie et al.'s approach (2011). The two new scales were tested as new trust antecedents.

5.1. Scale Development in the IS Literature

Early IS scale development research did not follow specific guidelines to carry out the scale development process (Readers are referred to *Appendix A* for a detailed discussion about some of the early IS scale development research). It was not until 2011 that the seminal work of Mackenzie et al. (2011) gave complete guidelines, recommendations, and specifications for the process. Figure 6 below depicts these six phases and their corresponding ten steps.

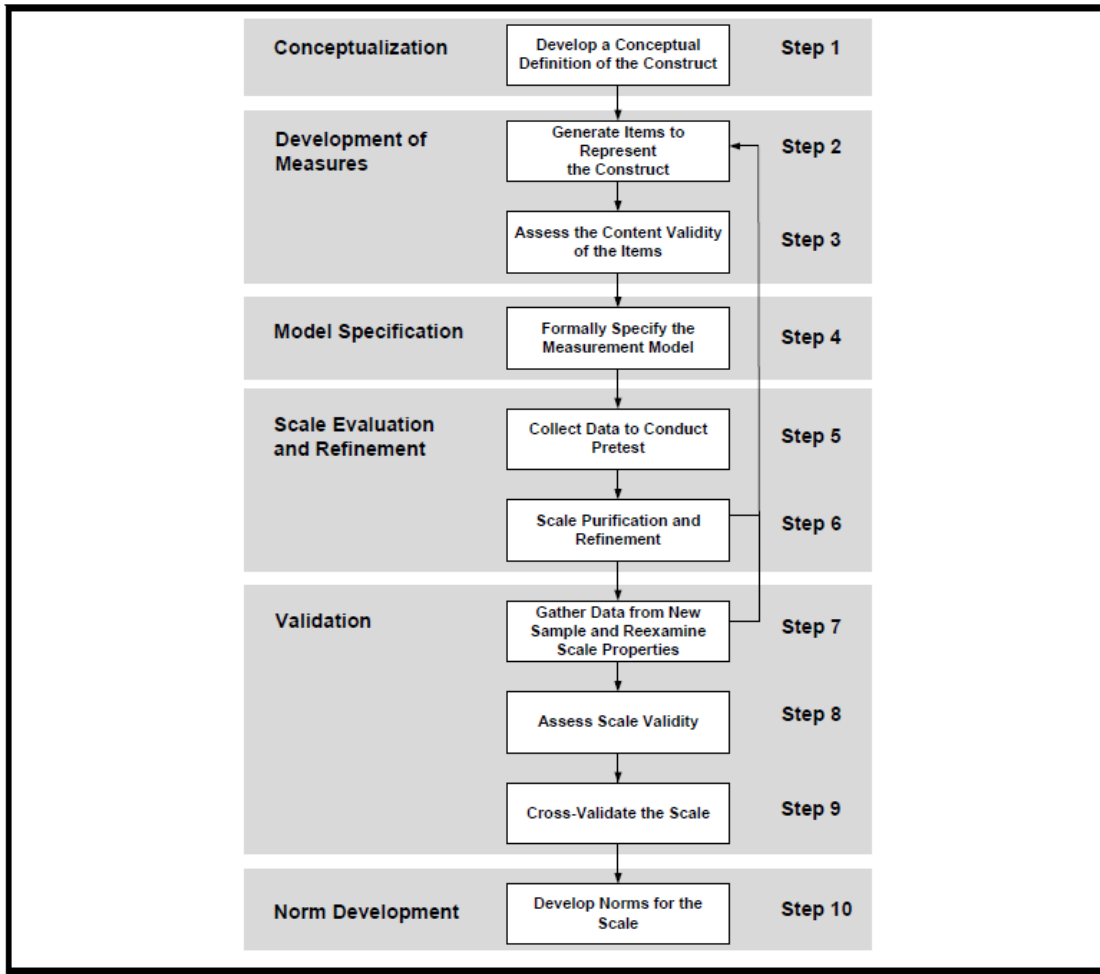


Figure 6: Scale Development Steps (Source: Mackenzie et al. 2011)

Thus far, and to the best of my knowledge, this approach, with all its steps, has been partially adopted only once (Jabagi et al. 2021). The authors tried to develop a scale for Gig Workers’ Perceived Algorithmic-Autonomy Support (PAAS). The authors carried out the first eight steps. However, as recommended, they did not conduct interviews during the conceptualization phase (MacKenzie et al. 2011). Furthermore, the authors ran two rounds of evaluations with raters to assess the content validity of the newly generated items using the Q-sort score without utilizing the one-way repeated ANOVA test recommended by Mackenzie et al. (2011). This test has been suggested as an appropriate way to adjust for any error term due to any

missing aspect that has not been captured by the measurement items (MacKenzie et al. 2011). These two shortcomings were covered in this research, where I followed Mackenzie et al.'s recommendations closely.

It is worth mentioning that the cross-validation and the norm development of the new scale in Steps 9 and 10 in Figure 6 were not completed because they require more resources and are considered to be a nontrivial path as the distributional properties of the new scale have to be validated in another population on which the new scale is expected to be applied (MacKenzie et al. 2011). Besides, the new scale's norms could vary as time changes (e.g., the Scholastic Aptitude Test (SET) is known to be changing over time (MacKenzie et al. 2011) and, thus, requires periodical re-evaluation and re-assessment. Hence, completing the last two steps in this approach goes beyond the scope of one manuscript and needs collaborative work in the field. In the next section, I will describe my attempt at a scale development process for perceived decentralization and perceived algorithmic authority in the context of Bitcoin as an example of a semi-autonomous information system using the first 8 steps of the Mackenzie et al.'s approach (2011).

5.2. Scale Development Process for Decentralization and Algorithmic Authority

Following Mackenzie et al.'s approach (2011), the two scales for perceived decentralization and perceived algorithmic authority were developed in eight steps, as shown in Figure 7 below. The left side of the figure shows each step of Mackenzie's guidelines, and the right side illustrates how it was executed and the aim of each step. Each of these steps is discussed in the following sections.

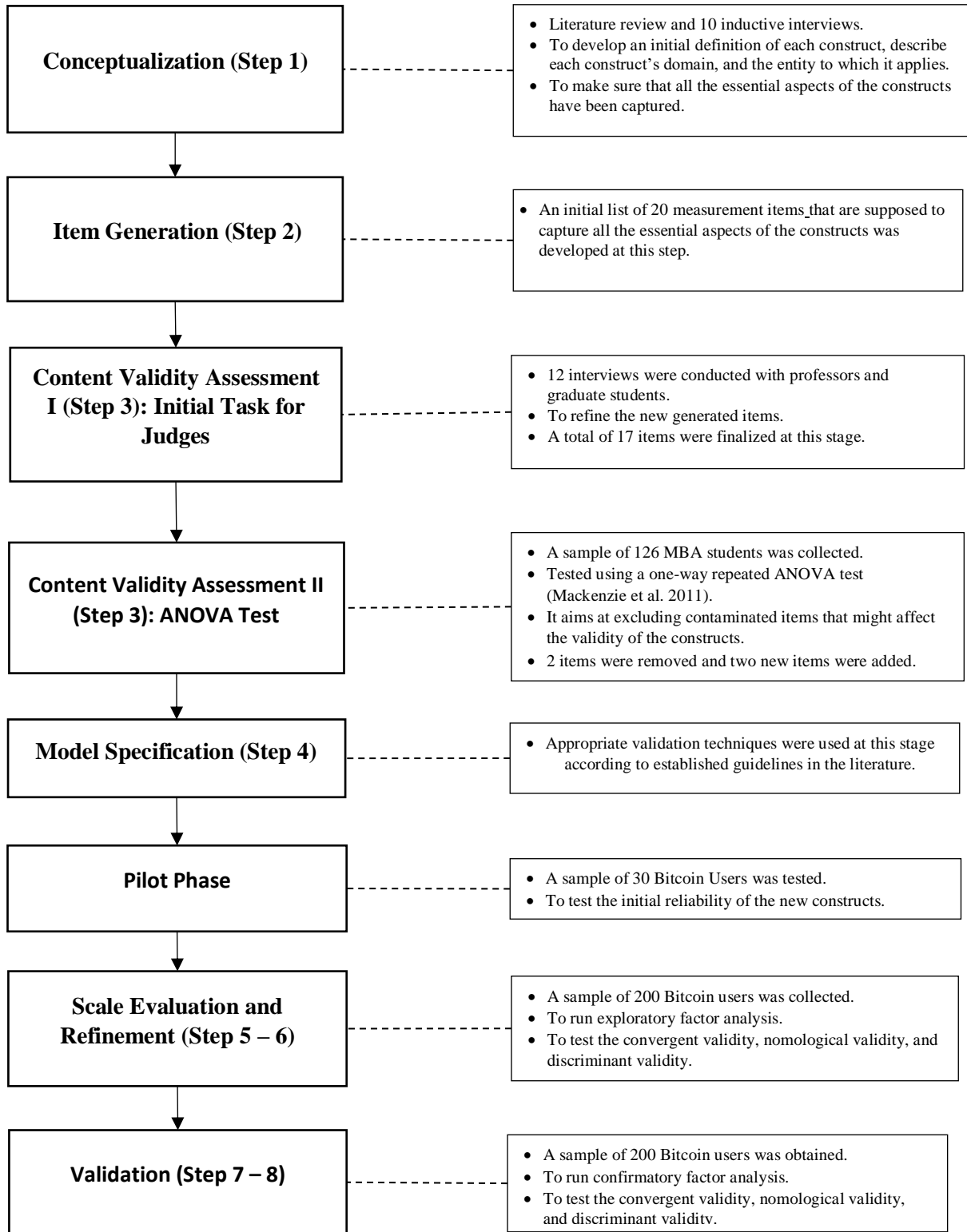


Figure 7. Scale Development for Decentralization and Algorithmic Authority Following the Mackenzie et al.'s

Approach (2011)

5.2.1 Conceptualization (Step 1)

The intent at this stage is to examine the meaning of the construct and other related constructs so that a better unambiguous definition can be developed. It is essential to check all relevant literature to see how the focal construct has been used in prior research or by practitioners (MacKenzie et al. 2011). Table 3 below summarizes the complete list of guidelines and describes the procedures followed for the two new constructs of perceived decentralization and algorithmic authority.

Table 3: Conceptualization for the new scales of decentralization and Algorithmic Authority

<u>Guidelines</u>	<u>Decentralization</u>	<u>Algorithmic Authority</u>
<p><u>Step 1:</u> Examine how the focal construct has been used in prior research or by conducting qualitative research using practitioners. The guidelines are:</p> <ul style="list-style-type: none"> • Literature review of previous theoretical and empirical research on the focal construct; • Review of literature on the meaning of related constructs; • Conduct preliminary research using an inductive approach with subject matter experts or practitioners. 	<p><u>Step 1:</u></p> <ul style="list-style-type: none"> • In the context of Blockchain, decentralization is defined as the system’s resilience and freedom from concentrated power (Walch 2019). • A related concept to decentralization is distributed systems. While all decentralized systems require distributed architecture, not all distributed systems are decentralized, as we might design a distributed system, but data can be meaningful only at the higher central point, and a central entity controls the ultimate decision. • No scale development was found in the literature. 	<p><u>Step 1:</u></p> <ul style="list-style-type: none"> • In the context of Blockchain, algorithmic authority can be defined as "<i>the legitimate power of algorithms to direct human action and to impact which information is considered true</i>" (Lustig and Nardi 2015, p.743). • Some related constructs are Algorithmic Management and Algorithmic Autonomy. Both constructs focus on the control level of the algorithm. While algorithmic management is associated with organizational structure control (Kellogg et al. 2020; Wood 2021), algorithmic autonomy focuses on the control in the human-computer-interaction context (André et al. 2018; Ye and Kankanhalli 2018). • No scale development was found in the literature.
<p><u>Step 2:</u> Specify the nature of the construct’s conceptual domain by identifying the entity to which it applies and the type of property the construct represents.</p>	<p><u>Step 2:</u></p> <ul style="list-style-type: none"> • Entity: end-user. • General Property: a perceived feature of the information system’s design. 	<p><u>Step 2:</u></p> <ul style="list-style-type: none"> • Entity: end-user. • General Property: a perceived feature of the underlying algorithms of an information system.

<p>Step 3: Specifying the conceptual theme of the construct through:</p> <ul style="list-style-type: none"> • Describe the necessary and sufficient attributes/characteristics as narrowly as possible as common attributes/characteristics, the uniqueness of the attributes/characteristics, the breadth, and inclusiveness. • Dimensionality: Unidimensional vs. Multidimensional • Stability: Over time and across situations and cases. 	<p>Step 3:</p> <ul style="list-style-type: none"> • Necessary and sufficient attributes/characteristics: physical distribution, logical distribution, and resource sharing. • Dimensionality: Decentralization is a <i>multidimensional formative</i> construct because decentralization does not exist without its defining sub-dimensions, and a change in any of its defining sub-dimensions is expected to be associated with a change in decentralization. • Stability: decentralization is expected to be a dynamic concept as it is a system design feature, and humans can adjust the extent to which a system can be decentralized over time. 	<p>Step 3:</p> <ul style="list-style-type: none"> • Necessary and sufficient attributes/characteristics: control/enforcement, legitimacy, independence. • Dimensionality: Algorithmic authority is a <i>unidimensional reflective</i> construct as it exists based on the one dimension of giving an algorithm some legitimate and independent level of control in the system design. • Stability: algorithmic authority is expected to be a dynamic concept as it is a system design feature, and humans can adjust the extent to which a system could have this type of authority over time.
<p>Step 4: Defining the construct in unambiguous terms. The guidelines are:</p> <ul style="list-style-type: none"> • Provide a clear, concise conceptual definition of the construct. • It should not be subject to multiple interpretations. • It should not be overly technical (technical terms with narrow meanings). • Should define construct positively, not by denying other things; negating one thing does not imply the affirmation of something else. • It should not be circular, tautological, or self-referential. 	<p>Step 4: Decentralization is <i>the extent to which all participating nodes in a system have the power to affect the system's outcomes, with no single entity having a dominant role in data storing, running, or even impacting the continuity of the system.</i></p>	<p>Step 4: Algorithmic Authority refers to <i>the legitimate independent level of control embedded in an algorithm by design, which allows it to take and enforce specific actions based on its logic.</i></p>

As shown in Table 3 above, the first step is conducting a literature review to ensure the researcher’s familiarity with how the focal constructs have been conceptualized thus far. Additionally, all related constructs have to be examined at this stage to better inform the researcher about the nature of each construct and how it might relate or differ from other similar constructs. Notably, the researcher must confirm that no scale development effort has been conducted so far for the focal construct and that the perceived differences with other related constructs are distinct enough to justify efforts and the resources that will be used for the scale development process.

To identify other related constructs, I relied on various fields, including technology and information systems, and other fields that would be relevant to these constructs, such as political science and management theory. Thus, I obtained a good understanding of the conceptual domain

of each construct at this stage. I found a conceptual definition for each construct, as shown in Table 3 above. Importantly, no scale development attempt was found for the two constructs.

In the context of Blockchain, decentralization was defined as the system's resilience and freedom from concentrated power (Walch 2019). Even though this definition captures essential characteristics, the causes of this resilience and the uniqueness of this resilience as a defining characteristic of decentralization are not clear. In fact, we can have a centralized system with some level of resilience because it has a distributed and centrally managed structure. Thus, a related concept to decentralization is distributed systems. While all decentralized systems require distributed architecture, not all distributed systems are decentralized, as we might design a distributed system, but data can only be made meaningful at a higher central point, and a central entity could control the ultimate decision power.

Similarly, algorithmic authority has been defined as "*the legitimate power of algorithms to direct human action and to impact which information is considered true*" (Lustig and Nardi 2015, p.743). While the definition captures the essence of the legitimate control that an algorithm could have, it is not clear why the domain of this authority is only applicable to direct human actions without other entities (i.e., algorithms). Notably, the trueness of information is a human perception and not a factual outcome of implementing the algorithm's logic. Other related constructs are Algorithmic Management and algorithmic autonomy. Both constructs focus on the control level of the algorithm. While algorithmic management is associated with algorithmic control within the organizational structure (Kellogg et al. 2020; Wood 2021), algorithmic autonomy focuses on algorithmic control in the human-computer-interaction context (André et al. 2018; Ye and Kankanhalli 2018). Algorithmic management can be described as the automation process of directing human participants (i.e., where algorithms tell humans what to do), the evaluation process

(i.e., where algorithms evaluate humans' outputs), and achieving discipline (i.e., where the rewards/punishments are monitored and enforced by algorithms) (Kellogg et al. 2020; Wood 2021).

Besides the literature review that was carried out at this stage, I conducted nine interviews with subject matter experts to complement my understanding of any differences between how the focal constructs have been conceptualized in the literature and the perception of these constructs in practice. Interviews are considered the most prominent data collection method for qualitative research (Myers 2019). A researcher can pick one of the three types of interviews in this research: structured, semi-structured, and unstructured (Myers 2019). Among them, the semi-structured interview is considered to be the most effective method as it has the advantages of the other two methods in having flexibility in directing the discussion around some main questions, just like structured interviews, and also allows the researcher to add some follow-up questions to any emerging theme or discussion point (Babbie 2020; Myers 2019).

Before running the semi-structured interviews, ethical approval was obtained as part of the study's ethics application approval (MREB#5268). The sample consisted of nine participants. Participants were recruited through a LinkedIn post that the researcher put in his public LinkedIn profile, and all invited participants were also asked to refer the researcher to some other potential participants who might be interested in participating using a snowball sampling technique. All the interviews were conducted online using Zoom and on a one-on-one basis. Interviews took 25-30 minutes and were recorded and transcribed for the data analysis.

Each participant was compensated with a \$25 gift card. Before their participation, each participant got an electronic copy of the letter of information for the study, the consent form, and

a copy of the interview questions. I used the following interview questions to guide my discussion with the interviewees:

- *How do you describe decentralization in an information system? Could you please give me some examples of a decentralized information system?*
- *What are the essential/important aspects of a decentralized information system so that without them, we cannot call an information system a decentralized system?*
- *Is there anything else you would like to add, or is there something important we should know about decentralization in general?*
- *How do you describe an algorithmic authority in an information system?*
- *What are the essential/important aspects of the algorithmic authority in an information system so that without them, there is no algorithmic authority?*
- *Is there anything else you would like to add, or is there something important we should know about algorithmic authority?*

All the questions were open-ended (not just “yes or no” answers). Additionally, I sometimes used other short questions to make sure I understood what the participant told me, “*So, you are saying that ...?*” Or if I needed more information when they were talking, “*Please tell me more?*” Or to learn further clarification, “*Why do you think that is...?*”

Transcribed data were analyzed using the content analysis method. Content analysis systematically summarizes a body of text into fewer categories and themes (Elo and Kyngäs 2008; Stemler 2000) and generates new insights (Krippendorff 2018). As the researcher was familiar with previous definitions of algorithmic authority and decentralization, the data analysis's main aim was to develop new themes and test how these new themes could corroborate or contradict

established themes, as identified in the conceptualization phase. Table 4 summarizes the results of the content analysis.

Table 4: Interviews' Themes

Concept	Themes	Supporting Quotes
Decentralization	Distributed Structure (i.e., concerned with the physical and logical Structure of an information system)	<p>“Decentralization, that's network decentralization. Like physical or material decentralization, you can have logical decentralization, which is about power sharing and decision-making rights,” Participant 1.</p> <p>“Decentralization is to take the essential dependence of trust on a single party out of the equation. Instead of using centralized servers, you can use massive amounts of decentralized servers. By doing so, you've taken single points of failure and distributed them across millions and millions of points,” Participant 3.</p> <p>“Decentralized has no single authority or single owner,” Participant 4.</p> <p>“Decentralization ensures that enough parties validate the legitimacy of every transaction or information that moves through a network. Essentially, it is getting past these centralized points of failure in large systems,” Participant 5.</p> <p>“No one individual can insert, change, modify, or reverse a transaction without many people seeing it and preventing it from happening. No one person could impact what you're doing or cheat because there are so many people looking over your shoulder. The entire intent in the integrity of the transaction is insured by having many distributed authorities supervising that transaction when it occurs,” Participant 6.</p> <p>“The more diffuse the power, the more decentralized the system is. We're looking at two kinds of power here: pure technology power, like what someone malicious could or couldn't do in the back-end. Then, the other kind of power is the empowerment of participants,” Participant 7.</p>
	Information Sharing (i.e., the ability of the underlying decentralized structure of an information system to support information sharing)	<p>“Decentralization is the sharing of information, and everybody in the system should have the same copy of the information, and everybody should have equal rights in making some decisions,” Participant 2.</p>
	Resources Sharing (i.e., the ability of the underlying decentralized structure of an information system to support resources)	<p>“They [The System Users] were as concerned about resource sharing as they were about survivability. Survivability means having some percentage of the network go down and still have communications,” Participant 1.</p>

	sharing among nodes)	
Algorithmic Authority	Programmable Control / Power (i.e., algorithmic control to work according to programmed rules.)	<p>“Algorithmic authority definitely has something to do with power, but then you have to ask yourself, kind of okay, what on earth is power ... Power is about controlling people,” Participant 1.</p> <p>“The programmatic management of power,” Participant 3.</p> <p>“So the algorithm or the authority allows those transactions to happen and get validated,” Participant 4.</p> <p>“This protocol is a set of rules that if you're going to participate in the Bitcoin network, you have to abide by—the kind of authority of the protocol where you can't do anything outside the rules' scope. So I think it is controlling in one way, but I think that controlling provides the groundwork for the expression and creative limits,” Participant 5.</p>
	Legitimacy (i.e., algorithmic control to be perceived as a legitimate part of the system.)	<p>“As long as we understand that the algorithmic authority is a consensus-driven model that is community enhanced and modified and the community gets to vote and thereby ensure that the code that now enhances this algorithmic authority,” Participant 3.</p> <p>“But I don't believe it has authority until that algorithm is distributed, widely used, and scrutinized. So, the authority doesn't come from the algorithm or the quality of the algorithm. It comes from the trust many people put into using that algorithm. So, its authority comes from our ability to trust it like a paper bill or piece of currency with no merit and no value until enough people trust it. The only reason it works is that people trust it and are willing to accept the algorithm's integrity, so in itself, the algorithm is not valuable, but it's the perception in the community,” Participant 6.</p> <p>“The other piece is the world's readiness to accept and act on that algorithm's outcomes,” Participant 7.</p>
	Independence (i.e., algorithmic control to work independently without human intervention.)	<p>“The ability to prevent human tampering. Algorithms only have authority if these algorithms produce the information independently, so I guess independence would be one piece of it,” Participant 7.</p>
	Altering Human Behaviour (i.e., algorithmic control ability to alter human behaviour.)	<p>“Authority is a meta concept that allows the holder of that authority to alter the conduct or the behaviour of those subject to that authority,” Participant 1.</p> <p>“When using other systems like recommendation systems, the algorithm influences your decision-making at a level you're unaware of. And that's one definition of this process, but I don't know that Bitcoin and cryptocurrencies follow the same idea of influencing people's decisions. It isn't going to change where you spend the money, and it isn't going to change who you do the transaction with,” Participant 6.</p>

As shown in Table 4 above, while the previous literature review for the conceptual definition of each construct was informative, the interviews were instrumental in generating interesting insights and discussions about the predefined themes in the literature. For decentralization, the two dimensions that were already identified, the system's resilience and the freedom from concentrated power, were combined. Participants viewed the system's resilience as a result of a distributed power structure where the system is "physically distributed" in its computing resources (i.e., servers and operations) and "logically distributed" in its decision-making rights. The following participants' quotes support that,

- *"Like physical or material decentralization, you can have logical decentralization, which is about power sharing and decision-making rights,"* **Participant 1,**
- *"Decentralization is to take the essential dependence of trust on a single party out of the equation. Instead of using centralized servers, you can use massive amounts of decentralized servers. By doing so, you've taken single points of failure and distributed them across millions and millions of points,"* **Participant 3.**

In addition, the importance of each node in the system is to be able to share resources so that the system's survivability is guaranteed;

- *"They [The System Users] were as concerned about resource sharing as they were about survivability. Survivability means having some percentage of the network go down and still have communications,"* **Participant 1.**

Moreover, participants emphasized the aspect of information sharing,

- *“Decentralization is the sharing of information, and everybody in the system should have the same copy of the information, and everybody should have equal rights in making some decisions,”* **Participant 2.**

As such, and based on the above insights, I defined decentralization at this stage as *the extent to which all participating nodes can share computing resources, information, and affect the system’s outcomes with no single entity playing a dominant role in the data storage, operation, or the continuity of the system.*

Like decentralization, participants perceived algorithmic authority as a form of *programmable control,*

- *“The programmatic management of power,”* **Participant 3.**

Where the algorithm can enforce specific actions,

- *“This protocol is a set of rules that if you're going to participate in the Bitcoin network, you have to abide by these rules,”* **Participant 5.**

This enforcement comes as a legitimate part of the system as perceived by the users,

- *“As long as we understand that the algorithmic authority is a consensus-driven model that is community enhanced and modified and the community gets to vote and thereby ensure that the code that now enhances this algorithmic authority,”* **Participant 3.**

Indeed, and regardless of any merits that an algorithm might have, the enabler of such authority comes from the users' trust and acceptance, and thus a legitimate part of the system,

- *“But I don't believe it has authority until that algorithm is distributed, widely used, and scrutinized. So, the authority doesn't come from the algorithm or the quality of the*

algorithm. It comes from the trust many people put into using that algorithm. So, its authority comes from our ability to trust it like a paper bill or piece of currency with no merit and no value until enough people trust it,” **Participant 6.**

Additionally, to maintain such authority, some level of independence must be assured in the system design so that it will be hard for human participants to tamper with,

- *“The ability to prevent human tampering. Algorithms only have authority if these algorithms produce the information independently, so I guess independence would be one piece of it,”* **Participant 7.**

The existing definition of an information system’s algorithmic authority in the literature, *the legitimate power of algorithms to direct human action and to impact which information is considered true* (Lustig and Nardi 2015, p.743), emphasizes the authority to be exercised over other people in directing their actions. However, all parts of a fully autonomous system could be algorithms. Thus, we might be in a situation where no human is involved, but algorithmic authority still exists. In another case, algorithmic authority could be exercised over algorithms and humans who voluntarily accepted to be subject to this authority. As such, the ultimate goal of this authority is to affect the actions of those subject to it, including algorithms and humans, as reflected in this quote;

- *“Authority is a meta concept that allows the holder of that authority to alter the conduct or the behaviour of those subject to that authority.”* **Participant 1**

In addition, the emphasis should be on the outcome of this authority in ensuring consistent outcomes based on its algorithmic logic. Similarly, the idea of which information is true is a human perception. It should not be part of the authority as it is a *risky* idea when considering the capability

of an algorithm to evolve and learn while having the ability to affect the trueness of information. Therefore, the main focus should be on how an algorithm works based on its logic and whether users perceive its authority as a legitimate type of authority. As such, algorithmic authority is defined as *the legitimate independent level of control embedded in an algorithm by design, which allows it to take and enforce specific actions based on its logic.*

To ensure the validity of the qualitative interview findings (Venkatesh et al. 2013), another researcher familiar with the IS literature and qualitative interview research was invited to conduct an independent content analysis of the data. The other researcher was provided with a copy of the transcribed data, the video recordings, and the initial definitions. The initial definitions included the categories that were identified in the conceptualization phase, as shown in Table 3 above. These categories were the basis for the independent content analysis conducted by each researcher. After that, we met to discuss some differences in the emerging themes, especially concepts of power, algorithmic logic, and legitimacy. The discussion increased the Cohen's Kappa (K) inter-coder reliability measure from an initial score of 0.75 to 1. This was not surprising, given the small number of categories that emerged.

In articulating the conceptual domain of each construct, and as shown in Table 3 above, both constructs define *end-user(s)* as the focal entity to obtain *measures/perceptions* about the two constructs as *design features* in an information system. Decentralization is assumed to be a *multidimensional formative* construct because decentralization does not exist without its defining sub-dimensions. With any change in any of its sub-dimensions, a change is expected to happen with the latent construct of decentralization. However, algorithmic authority is anticipated to be a *unidimensional* construct as it exists based on the one dimension of giving an algorithm some legitimate and independent level of control in the system design. Both constructs are expected to

be *dynamic*. Since they are both system design features, humans can adjust them at any time. Next, the measurement items for the two constructs were generated.

5.2.2. Items Generation (Step 2)

After developing a definition for each construct, the next step of the scale development process is to generate a list of items to represent the scope of this definition. This is a crucial step as it is the bridge between conceptualizing a construct and operationalizing it. The guidelines for completing this step provided by Mackenzie et al. 2011 are as follows:

- Literature review;
- Deduction from the theoretical definition of the construct;
- Suggestions from experts in the field;
- Interviews or focus group discussions with representatives from the population(s) to which the focal construct is expected to be generalized.

In this research, the initial pool of items was developed based on the literature review conducted for each construct and the subsequent interviews with subject-matter experts during the previous conceptualization step. Table 5 below provides an initial pool of 19 measurement items and the two corresponding definitions.

Table 5: Initial Definitions and Measurement Items

Construct Definition	Initial Measurement Items
<p>Decentralization <i>is the extent to which all participating nodes can share computing resources, information, and affect the system’s outcomes, with no single entity playing a dominant role in the data storage, operation, or the continuity of the system.</i></p>	<ol style="list-style-type: none"> 1. The system is decentralized. 2. In the system, computing resources are shared. 3. In the system, information is shared. 4. I feel that I can play a role in determining the system’s outcomes. 5. In the system, there is no one dominant entity. 6. In the system, no single entity is storing all data.

	<ol style="list-style-type: none"> 7. In the system, no single entity is operating the system. 8. In the system, no single entity is affecting the system’s continuity. 9. In the system, there is no single point of failure.
<p>Algorithmic Authority is the legitimate independent level of control embedded in an algorithm by design, allowing it to take and enforce specific actions based on its logic.</p>	<ol style="list-style-type: none"> 10. In the system, the underlying algorithms have authority. 11. In the system, the underlying algorithms are legitimate. 12. The underlying algorithms are embedded in the system. 13. In the system, the underlying algorithms have control. 14. In the system, the underlying algorithms have enforcement ability. 15. In the system, the underlying algorithms can enforce certain actions. 16. In the system, the underlying algorithms can take certain actions. 17. In the system, the underlying algorithms have logic. 18. In the system, the underlying algorithms follow logic. 19. The features of the underlying algorithms of the system are there by design.

The development of this initial list followed established guidelines of having some positive and negative worded items as recommended (MacKenzie et al. 2011; Spector 1992), as well as avoiding the double-barrelled items (i.e., only one idea for each item) as advised (Churchill 1979). Readers are referred to a complete discussion of these guidelines in Diamantopoulos and Winklhofer 2001, MacKenzie et al. 2011, and Spector 1992.

5.2.3. Content Validity Assessment (Step 3)

The next step was to ensure the content validity of the newly generated measurement items. Content validity refers to the degree to which items in an instrument are *relevant* and *represent* the construct’s domain for a particular purpose (Haynes et al. 1995; MacKenzie et al. 2011). While content validity focuses on both the relevance and the representation of the measurement items,

face validity is considered to be part of content validity and refers to the degree to which a judge/respondent agrees on the appropriateness of the measurement items to the targeted construct (Allen and Yen 2001; Nevo 1985). At this stage, it is critical to minimize any potential error variance with the measurement items (Haynes et al. 1995).

The consideration of content validity starts with appropriately conceptualizing the targeted construct and subsequent assessments of the measurement items using qualitative and quantitative methods (Haynes et al. 1995). To complete this step, I conducted a qualitative study with a group of Information Systems (IS) and Organizational Theory (OT) professors and graduate students of IS and a quantitative study with a group of MBA students to represent the targeted population of the constructs. Both samples are considered convenient and have the merits of scale development skills in the expert group and representativeness of the targeted population in the MBA student group. Table 6 provides the details for this step.

Table 6: Scale Development Content Validity Assessment

Steps	Objectives	Procedures	Evaluation
Step 3-1: Scale development/domain expert rater's analysis (n=12)	<ol style="list-style-type: none"> 1. To determine the extent to which the proposed definition of each construct is comprehensive. 2. To determine the extent to which the proposed definition of each construct is comprehensible. 3. To determine the extent to which the proposed measurement items properly represent the conceptual domain of the underlying construct. 	<p>Judges were first asked to think about a definition for the focal construct in their own words. Then, each definition was shown to them, and they were asked the following three questions:</p> <ul style="list-style-type: none"> • To what extent do you think the proposed definition of each construct is comprehensive? • To what extent do you think the proposed definition of each construct is comprehensible? • To what extent do you think the proposed items capture the conceptual domain of the underlying construct? 	<ol style="list-style-type: none"> 1. Qualitative analysis. 2. Rater's agreement score.

		After answering these three questions, judges were also asked to give a qualitative opinion about any aspect they thought might be missing or confusing in the definition and the measurement items. This process continued until there was no confusion in the construct's definition, and the proposed items captured all the conceptual aspects of the constructs.	
Step 3-2: Targeted population representatives' assessment (n=126)	1. To assess the <i>face validity</i> of the newly developed items.	Participants were provided with a pool of measurement items and were asked to give a score from 1 – 5 on their assessment of the belongingness of each item to each corresponding provided definition.	1. One-way repeated ANOVA test.

5.2.3.1 Professors and Graduate Students Qualitative Interviews Study

Twelve semi-structured interviews (n=12) were conducted with a sample of Information Systems (IS) professors (n=4), Organizational Theory (OT) professors (n=3), and graduate students of IS (n=5) until the theoretical saturation was achieved (Myers 2019). Each interview lasted between 45 - 50 minutes. To minimize the potential impact of interpretational confounding bias (Moore and Benbasat 1991), participants were asked to give their understanding and definition of each construct. Then, participants were shown the proposed definitions and requested to assess their agreement/disagreement with a rationale for each choice. After that, participants were shown the measurement items and asked to assess whether they agree or disagree with the measurement items' representation of the constructs. Finally, participants were asked to express their opinion about anything that is still missing or confusing on both the definition and the measurement items.

The interviews were conducted in two rounds so that I could reflect and add any potential modifications required at that stage. Round 1 consisted of 7 participants, while Round 2 included

5 participants. For decentralization, five of the participants emphasized the role of explicitly adding the *system’s accessibility*, as users can get *access* to the system in the first place. Then, they will be able to share resources and information collaboratively. As such, the definition of decentralization was slightly modified to be *the extent to which an information system is collaboratively managed and accessible by entities (e.g., humans or algorithms) where all participating entities share inputs (e.g., computing resources, data/information) and affect the system’s outputs with no single entity playing a dominant role in the operation of the system.* Following the two rounds of interviews, the definition of algorithmic authority became more precise as *the legitimate independent level of control an algorithm has to take and enforce certain actions based on its logic.* Table 7 below shows the two definitions and their corresponding measurement items at that stage.

Table 7: Constructs Definitions and Corresponding Measurement Items

Construct Definition	Initial Measurement Items
<p>Decentralization <i>is the extent to which an information system is collaboratively managed and accessible by entities (e.g., humans or algorithms) where all participating entities share inputs (e.g., computing resources, data/information) and affect the system’s outputs with no single entity playing a dominant role in the operation of the system.</i></p>	<ol style="list-style-type: none"> 1. The system is collaboratively managed. 2. The system is accessible. 3. I have access to data/information. 4. Computing resources are shared. 5. I feel that I play/can play a role in determining the system’s outputs 6. There is no single point of failure in the system. 7. There is no one dominant entity controlling the system. 8. No single entity is affecting the system’s continuity. 9. No single entity is storing all system data. 10. No single entity is operating the system.
<p>Algorithmic Authority <i>is the legitimate independent level of control an algorithm has to take and enforce certain actions based on its logic.</i></p>	<ol style="list-style-type: none"> 1. Algorithms are legitimate. 2. Algorithms are independent. 3. Algorithms can enforce certain actions. 4. Algorithms have control. 5. Algorithms can take action. 6. Algorithms work without intervention. 7. Algorithms follow a specific logic.

The inter-judge agreement score for the 12 participants was 0.83 for decentralization and 1 for algorithmic authority in round 1. Meanwhile, in round 2, as shown in Table 7 above, the two definitions and the inter-judge agreement scores were 1 for the two constructs. Both rounds indicated a strong level of agreement among participants (Landis and Koch 1977). As such, the two constructs have shown an acceptable level of validity, which will be further assessed in the next step of the repeated one-way ANOVA test as recommended in the IS literature (MacKenzie et al. 2011).

5.2.3.2 MBA Students Quantitative Study

The primary purpose of this step is to ensure the face validity of the new items (Allen and Yen 2001; Nevo 1985) through a one-way repeated ANOVA test that was recommended in the literature (Hinkin and Tracey 1999; MacKenzie et al. 2011; Yao et al. 2008). I chose a sample of 126 participants from an MBA program at a North American university. All participants completed a required MBA introductory Management Information Systems (MIS) course. As such, some basic understanding of the nature of Information Systems was ensured. Besides, the sample's demographic characteristics, such as biological sex (72 male, 52 female, 2 prefer not to say) and age distribution as shown in Figure 8 below, are similar to the potential targeted population of the Bitcoin users where both decentralization and algorithmic authority are assumed to prevail as system's design features. Hence, the representation of the sample was ensured as recommended in the literature (MacKenzie et al. 2011).

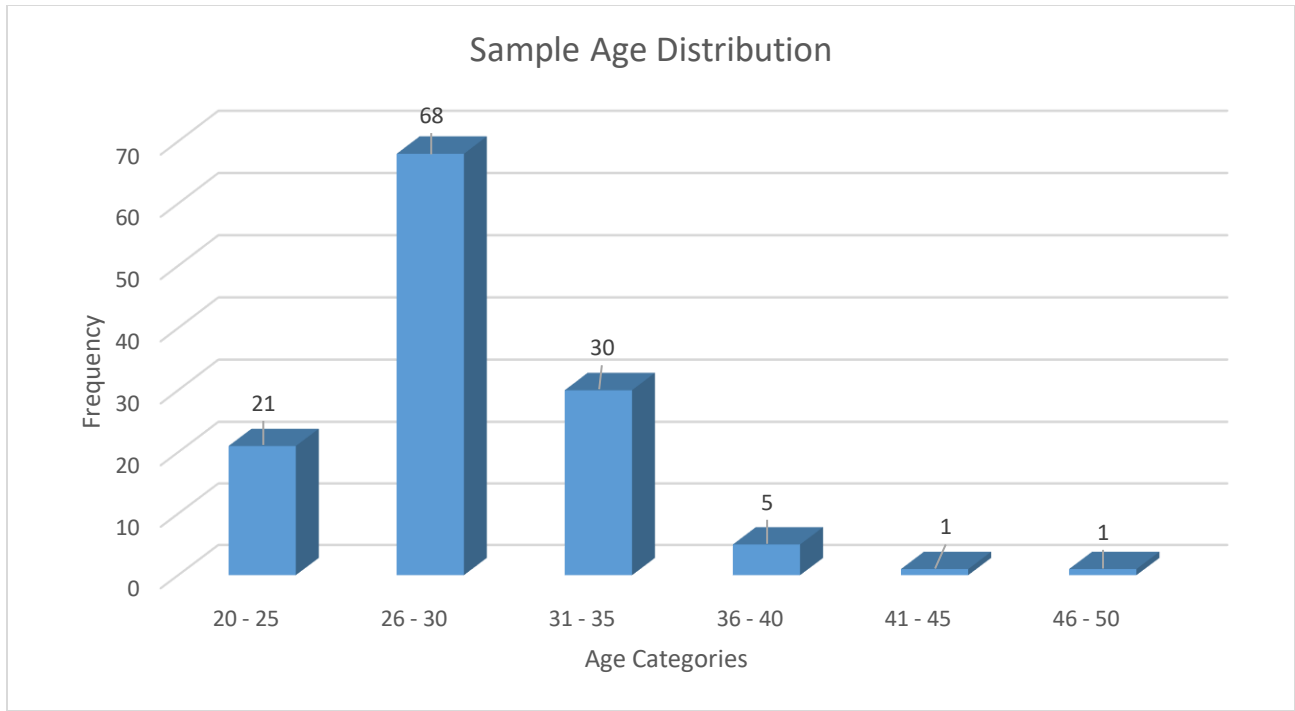


Figure 8: Sample's Age Distribution

To ensure data quality, I asked participants to send out an email request from their official university email indicating their interest in participating in the study after reviewing the letter of information that was publicized in the school. The researcher then created a unique survey link for each participant via the researcher's Qualtrics account. All participants consented before their participation and were compensated with a \$10 gift card for their time.

To further minimize any potential interpretational confounding bias (Moore and Benbasat 1991), participants were shown the definitions of the two constructs and were asked in the first question to give their agreement on the definition with a chance to provide any feedback they might have in a follow-up open-ended question asking them to justify their agreement/disagreement with each definition. For decentralization, 115 participants agreed on the definition, 10 participants partially agreed on it, and only 1 participant did not agree on the

definition. Similarly, for algorithmic authority, 113 participants agreed on the definition, and 13 participants partially agreed on it. Figure 8 below shows percentages of agreement on the two definitions of the constructs.

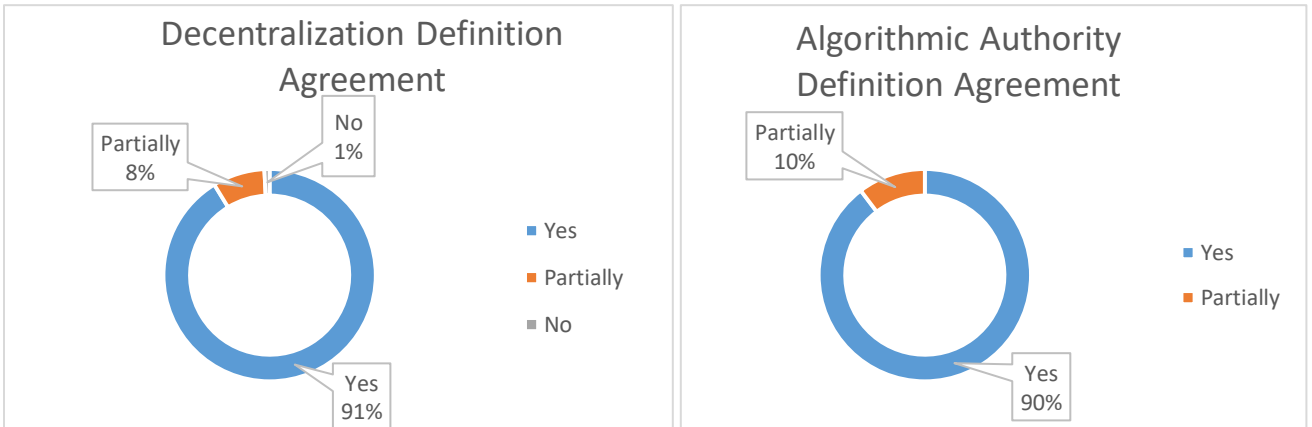


Figure 9: Definitions Agreement Statistics

As shown in Figure 9 above, both definitions have a strong level of agreement among the 126 participants, with a percentage above 90%. This indicates a high level of the face validity of the two new constructs (Landis and Koch 1977). *Appendix B* provides all the quotes from the participants in the follow-up open-ended question.

In the second set of questions, participants were shown the 17 measurement items and were asked to assign a value between 1 and 5 (i.e., 1: strongly disagree to 5: strongly agree) for the extent each item was a good measure of the two corresponding constructs definitions. I randomized the measurement items to minimize any tendency to rank an item based on its position in the survey. Additionally, I split the 17 items into two pages to reduce the cognitive load issue when ranking the items (MacKenzie et al. 2011). Table 8 below shows the measurement items' repeated one-way ANOVA test results.

Table 8: One-Way Repeated ANOVA Test Results

Item	Mean (D)	SD (D)	Mean (AA)	SD (AA)	ANOVA F Statistics	Significant Level
I feel that I play/can play a role in determining the system’s outputs. (Code 1D)	<u>3.48</u>	1.319	2.48	1.25	31.686	<0.001
No single entity is operating the system. (Code 2D)	<u>4.19</u>	1.171	2.39	1.29	117.777	<0.001
There is no one dominant entity controlling the system. (Code 3D)	<u>4.09</u>	1.386	2.25	1.258	211.750	<0.001
Computing resources are shared. (Code 4D)	<u>4.29</u>	1.011	2.70	1.316	98.093	<0.001
No single point of failure in the system. (Code 5D)	<u>3.28</u>	1.462	2.40	1.322	22.231	<0.001
No single entity is affecting the system’s continuity. (Code 6D)	<u>3.82</u>	2.35	2.35	1.241	135.813	<0.001
I have access to data/information. (Code 7D)	<u>4.07</u>	1.097	2.83	1.276	96.571	<0.001
No single entity is storing all system data. (Code 8D)	<u>3.89</u>	1.346	2.48	1.218	67.222	<0.001
The system is accessible. (Code 9D)	<u>3.89</u>	1.285	2.79	1.250	57.105	<0.001
The system is collaboratively managed. (Code 10D)	<u>4.34</u>	1.067	2.28	1.191	194.110	<0.001
Algorithms can enforce certain actions. (Code 1A)	2.74	1.352	<u>4.42</u>	1.053	95.825	<0.001
Algorithms have control. (Code 2A)	2.48	1.250	<u>4.14</u>	1.093	105.676	<0.001
Algorithms can take action. (Code 3A)	2.69	1.214	<u>4.27</u>	1.207	96.176	<0.001
Algorithms work without intervention. (Code 4A)	2.46	1.256	<u>3.83</u>	1.284	68.063	<0.001
Algorithms are legitimate. (Code 5A)	2.98	1.242	<u>3.92</u>	1.217	56.194	<0.001
Algorithms follow a specific logic. (Code 6A)	2.94	1.401	<u>4.29</u>	1.080	114.683	<0.001
Algorithms are independent. (Code 7A)	2.52	1.355	<u>4.00</u>	1.226	84.723	<0.001

As shown in Table 8 above, all items were assigned the expected belongingness value for the corresponding construct with significant differences from the other construct. Thus, all the proposed measurement items indicated a strong *face validity* at that stage.

Reflecting on the results and in an attempt to prepare the items to fit the nature of the selected testing context of Bitcoin, four items were reworded for clarity, and two items were

replaced, as presented in Table 9 below. Notably, the two dimensions of decentralization have become more apparent at this stage, which are the *system’s neutrality and distributed structure*. The system’s neutrality as a design feature and a sub-dimension of decentralization allows users to access and share information and computing resources. It also ensures that users/nodes are treated neutrally and equally by expecting the same output based on the same input. All the proposed measurement items were validated in an exploratory and confirmatory analysis in the next step.

Table 9: Measurement Items Adjustment

Old Measurement Items	New Measurement Items
I feel that I play/can play a role in determining the system’s outputs. (Code 1D: Reworded)	The system’s outputs are the same for all users. (Code 1D: Reworded)
No single entity is operating the system. (Code 2D)	No single entity is operating the system. (Code 2D)
Algorithms can enforce certain actions. (Code 1A)	Algorithms can enforce certain actions. (Code 1A)
There is no one dominant entity controlling the system. (Code 3D)	There is no one dominant entity controlling the system. (Code 3D)
Computing resources are shared. (Code 4D)	Computing resources are shared. (Code 4D)
There is no single point of failure in the system. (Code 5D)	There is no single point of failure in the system. (Code 5D)
Algorithms have control. (Code 2A)	Algorithms have control. (Code 2A)
No single entity is affecting the system’s continuity. (Code 6D)	No single entity is affecting the system’s continuity. (Code 6D)
Algorithms can take action. (Code 3A: Removed)	Algorithms work without intervention. (Code 3A)
Algorithms work without intervention. (Code 4A)	I have access to data/information. (Code 7D)
I have access to data/information. (Code 7D)	No single entity is storing all system data. (Code 8D)
No single entity is storing all system data. (Code 8D)	Algorithms’ control in the system is legitimate. (Code 4A: Reworded)
Algorithms are legitimate. (Code 5A: Reworded)	All users have equal access to the system. (Code 9D: Reworded)
The system is accessible. (Code 9D: Reworded)	The system is collaboratively managed. (Code 10D)
The system is collaboratively managed. (Code 10D)	Algorithms follow a specific programmable logic. (Code 5A: Reworded)
Algorithms follow a specific logic. (Code 6A: Reworded)	The system’s data is distributed. (Newly added item: code 11D)
Algorithms are independent. (Code 7A: Removed)	All users can share data. (New Added Item: code 12D)

5.2.4. Model Specification (Step 4)

The relationship between the measurement items and their focal latent construct should be identified to specify the model formally (MacKenzie et al. 2011). As argued before, and as shown

in Table 3, and based on the previous steps, decentralization is conceptualized as a second-order formative construct, which has two reflective first-order constructs: the system’s neutrality and distributed structure. Algorithmic authority, on the other hand, is conceptualized as a first-order reflective construct. The measurement items were assessed based on the established recommendations and appropriate validation techniques in the IS literature that fit the nature of the two constructs (e.g., (Chin 1998; Fornell and Larcker 1981; Hair et al. 2013; MacKenzie et al. 2011; Petter et al. 2007), as they will be explained in the following steps.

5.2.5. Scales Development Initial Reliability Analysis (Pilot Study)

As the primary purpose of this stage is to test the initial reliability of the proposed two scales, a sample of 30 Bitcoin users was collected through Qualtrics, <https://www.qualtrics.com/>. Qualtrics is a software company specializing in scientific data collection. The targeted population was Bitcoin users in the USA and Canada. Participants were compensated through their accounts with the company. Based on the proposed research model in Chapter 4, I chose trust as a test construct in the nomological network to have a positive relationship with decentralization and algorithmic authority. Cronbach reliability tests were conducted for the two new scales, and the results are shown in Table 10 below.

Table 10: Reliability analysis of the initial measurement items

Item	Scale Reliability
Decentralization _ Neutrality 1	0.912
Decentralization _ Neutrality 2	
Decentralization _ Neutrality 3	
Decentralization _ Neutrality 4	
Decentralization _ Neutrality 5	
Decentralization _ Neutrality 6	
Decentralization _ Dis. Structure 1	0.884
Decentralization _ Dis. Structure 2	
Decentralization _ Dis. Structure 3	
Decentralization _ Dis. Structure 4	
Decentralization _ Dis. Structure 5	

Decentralization _ Dis. Structure 6	
Algorithmic Authority 1	0.831
Algorithmic Authority 2	
Algorithmic Authority 3	
Algorithmic Authority 4	
Algorithmic Authority 5	

As shown in Table 10 above, all the two new constructs have an acceptable Cronbach Alpha value greater than 0.7 (Fornell and Larcker 1981). Additionally, the two new constructs showed the expected positive correlation with trust, as shown in Table 11 below. Thus, I proceed with the next stage using the 17 items.

Table 11: Pearson correlation coefficients

Correlation Coefficient (Significance level)	(1)	(2)	(3)
Decentralization (1)	--		
Algorithmic Authority (2)	0.442* (0.015)	--	
Trust (3)	0.373* (0.042)	0.217 (0.250)	--

5.2.6. Exploratory Factor Analysis (EFA) (Step 5 & 6)

This phase aims to test the reliability of the newly developed scales and uncover the underlying dimensionality structure to support the proposed theoretical structure developed in the previous phases of the scale development process. A sample of 209 Bitcoin users was used in this phase. The proposed sample size satisfies the guidelines provided by (MacKenzie et al. 2011), where at least ten subjects are required for each measurement item, and also accommodating any spoiled responses that were eliminated for any data quality issue. In addition, a sample size of 200 is considered acceptable for a moderately complicated model (Howard 2016). All respondents were recruited through an online survey through Qualtrics.

The data collected were subject to several screening quality measures before being included in the final dataset. First, no missing data points were accepted. Second, all completed responses in less than five minutes were also removed from the dataset. Third, straight-lining responses were also eliminated (Payne et al. 2018). Finally, respondents have also passed two attention check questions, *Q1: I am answering this question with full attention* (answer should be 7) and *Q2: I am answering this question without full attention* (answer should be 1), on a scale from 1 to 7 that were used in different part of the survey. Qualtrics dealt with any problematic data points related to these issues.

The final dataset (N=209) was also checked against the statistical quality measures to ensure its suitability for the structural equation modeling using SPSS 28. Six data points were removed as outliers when using Cook’s D values (Moussawi and Koufaris 2019), and three more data points were also eliminated so that all items scored within the acceptable range of Skewness and Kurtosis values (i.e., within the -2 and 2), which suggests no severe violation of the normality assumption. Finally, the required two tests for Kaiser-Meyer-Olkin Measure of Sampling Adequacy (0.826) and Bartlett’s test of Sphericity ($P < 0.001$) justified the applicability of the exploratory factor analysis test. Table 12 provides the descriptive statistics for the final sample used in the analysis (N=200).

Table 12: Sample's Descriptive Statistics for the Exploratory Factor Analysis

	Variable	Count	Percentage
Gender	Man	103	51.5%
	Woman	97	48.5%
	Non-gender-binary, two-spirit, or similar	0	0%
	Others	0	0%
	Total	200	
Age	20-30	47	23.5%
	31-40	97	48.5%
	41-50	42	21%
	51-60	8	4%

	61-70	6	3%
	> 70	0	0%
	Total	200	
Education Level	High school diploma	33	16.5%
	Some college degree	45	22.5%
	Bachelors	91	45.5%
	Master's	21	10.5%
	Ph.D.	5	2.5%
	Other	5	2.5%
	Total	200	
Bitcoin Experience	1 - 3 year	96	48%
	4 - 7 years	93	46.5%
	>7 years	11	5.5%
	Total	200	

As decentralization is conceptualized as a second-order formative construct consisting of two reflective first-order constructs, the two-stage (Ringle et al. 2012) model was followed for an exploratory factor analysis using the guidelines of (Hair et al. 2021). This two-stage model effectively addresses the artificially correlated residuals that might lead to inaccurate conclusions about the relationship among constructs (Hair et al. 2013; Van Riel et al. 2017). In the first stage, both decentralization and algorithmic authority are modeled as three reflective constructs, two constructs for decentralization and one construct for algorithmic authority, to have a positive relationship with trust as an endogenous variable, as shown in Figure 10 below. In the second stage, the two dimensions of decentralization are modeled to form decentralization, and the model tests the direct relationship between decentralization and trust, as shown in Figure 10 below.

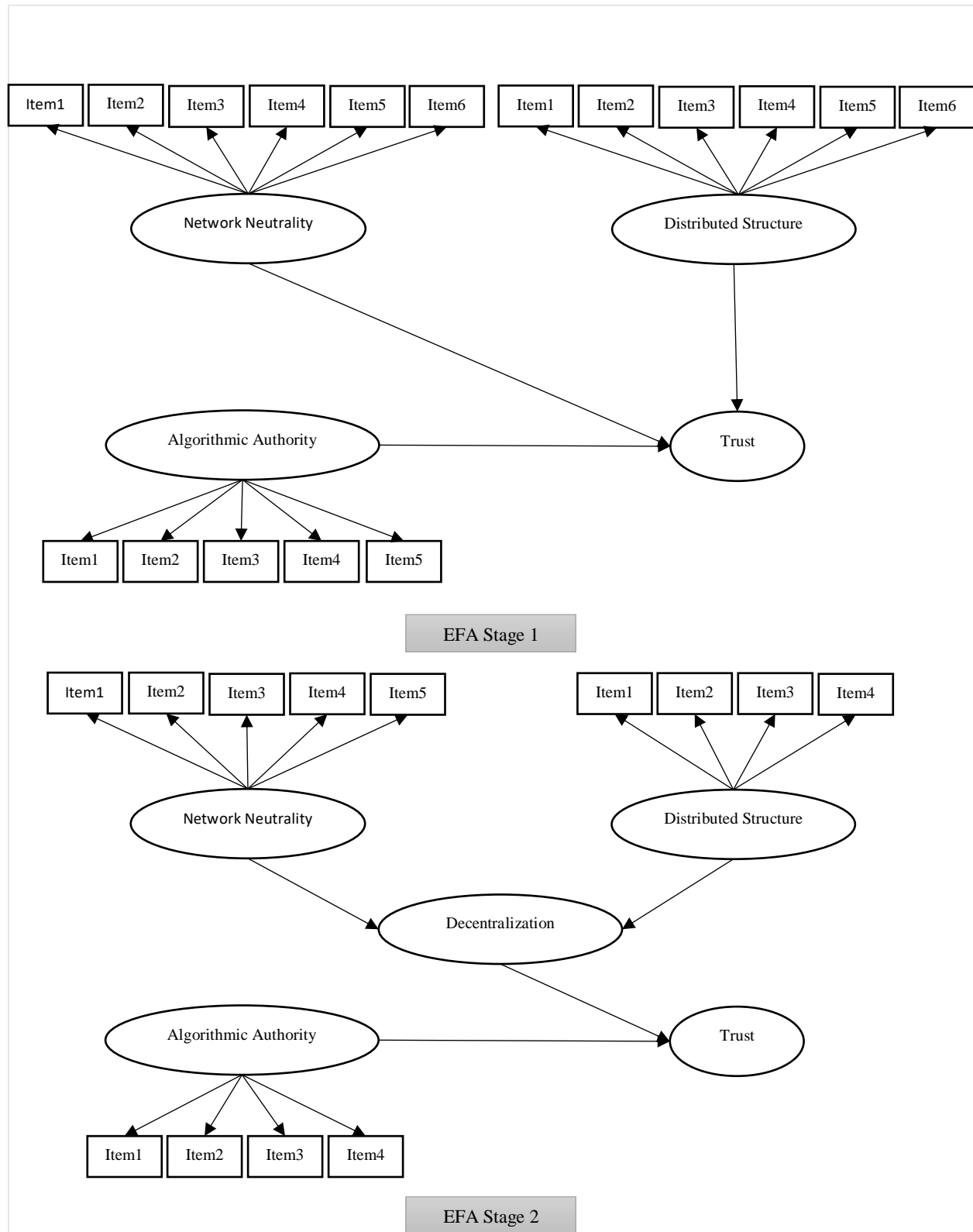


Figure 10: The Two-Stage EFA Model

Through an iterative process, all items were analyzed one at a time, where model fit, reliability, and validity measures were continuously observed (Hair et al. 2010). In addition, each construct should have at least three measurement items (Hair et al. 2010). Table 13 provides the final list of the measurement items.

Table 13: Exploratory Factor Analysis Items List

Items	Factor Loading	Construct's Sub-dimension	Construct
1. All users have equal access to the system.	0.767	System's Neutrality	Decentralization
2. All users have the same access to data.	0.718		
3. The system's outputs are the same for all users.	0.732		
4. All users can share data.	0.722		
5. All users can share resources.	0.774		
1. No one dominant entity is controlling the system.	0.779	Distributed Structure	
2. No single entity is operating the system.	0.803		
3. No single entity is affecting the continuity of the system.	0.820		
4. The system is collaboratively managed.	0.825		
1. The underlying algorithms can enforce certain actions.	0.761	N/A	
2. The underlying algorithms have control.	0.627		
3. The underlying algorithms' control in the system is legitimate.	0.834		
4. The underlying algorithms follow a specific programmable logic.	0.837		

As shown in Table 13 above, all factor loading values passed the threshold of 0.7 (Hair et al. 2011) except for one item with a factor loading of 0.627, above the threshold of 0.6 identified by (Chin 1998). In addition, all items loaded on their intended construct with a difference greater than 0.2 to any other latent construct in the model (Howard 2016). Furthermore, the model fit was assessed using the Standardized Root Mean Square Residual (SRMR) measure, which measures the match between the proposed structural model and the best model to fit the data. The SRMR

value for the model is *0.091*, which is considered to be a good fit as it is less than *0.1* (Henseler and Sarstedt 2013). Table 14 provides the measures used to assess the constructs’ reliability and validities.

Table 14: Reliabilities and Validities Measures for the Exploratory Factor Analysis (EFA)

Construct	α	CR	AVE	VIF	Square Root of AVE			
					1	2	3	4
Neutrality (1)	0.800	0.823	0.552	1.349	0.743			
Dis. Structure (2)	0.838	0.931	0.652	1.483	0.463	0.807		
Algo. Authority (3)	0.777	0.818	0.592	1.403	0.412	0.495	0.770	
Trust (4)	0.801	0.821	0.714	N/A	0.351	0.352	0.380	0.845

As shown in Table 14 above, all constructs achieved acceptable measures for reliability and validity. The reliability values for all constructs are above *0.7* using the Cronbach Alpha (α) measure, which indicates the strong covariance among the items (Fornell and Larcker 1981). In addition, all Composite Reliability (CR) values are above *0.7*, supporting a high convergent validity value for each construct (Hair et al. 2021). Furthermore, all Average Variance Extracted (AVE) values for all constructs were above *0.5*, supporting convergent validity (Fornell and Larcker 1981). Fornell-Larcker’s criterion was used to assess the discriminant validity of each construct as the square root of the AVE of each construct was above the correlation values with all other constructs in the model. Finally, multicollinearity was tested using Variance-Inflation-Factor (VIF). All VIF values were below 3.3, which suggests that common method bias is not a problem in the estimated model (MacKenzie et al. 2011; Petter et al. 2007; Podsakoff et al. 2003).

In addition, the model achieved satisfactory performance in the second stage as the paths from decentralization’s two sub-dimensions are significant with values above 0.5, and all the path coefficients on the model were also significant (Chin 1998), as shown in Table 15.

Table 15: Weights, Path Coefficients, Significance Level, and R² for EFA Stage 2 Model

Outer Model	Weight	P value	
System Neutrality → Decentralization	0.599	0.000	
Distributed Structure → Decentralization	0.574	0.000	
Inner Model	Path Coefficient	P value	R²
Decentralization → Trust	0.248	0.000	0.191
Algorithmic Authority → Trust	0.257	0.000	

5.2.7. Confirmatory Factor Analysis (CFA) (Steps 7 & 8)

The next step was to conduct a confirmatory factor analysis on a new sample to check the consistency of the new sample in confirming the results of the exploratory sample. Another sample of 207 Bitcoin users was collected for that purpose. All participants were recruited through an online survey using Qualtrics. The targeted population was Bitcoin users in the USA and Canada. Participants were compensated through Qualtrics.

The new data was scrutinized using the previously discussed methods in the EFA phase, where all missing data points were removed, the completion time should be above five minutes, and all straight-lining responses were also extracted (Payne et al. 2018). Finally, two attention check questions, **Q1: I am answering this question with full attention** and **Q2: I am answering this question without full attention**) were used in different parts of the survey, and participants were required to answer them correctly, Q1=7 and Q2=1, on a scale from 1 to 7. Qualtrics dealt with any problematic data points related to these issues.

The final dataset (N=207) was also checked against the statistical quality measures to ensure its suitability for the structural equation modeling using SPSS 28. Four data points were removed as outliers when using Cook’s D values (Moussawi and Koufaris 2019), and three more data points were also eliminated so that all items scored within the acceptable range of Skewness and Kurtosis values (i.e., within the -2 and 2), which suggests no severe violation of the normality assumption. Finally, the required two tests for Kaiser-Meyer-Olkin Measure of Sampling Adequacy (0.834) and Bartlett’s test of Sphericity ($P < 0.001$) justified the applicability of the exploratory factor analysis test. Table 16 provides the descriptive statistics for the final sample used in the analysis (N=200).

Table 16: Sample's Descriptive Statistics for the Confirmatory Factor Analysis

	Variable	Count	Percentage
Gender	Man	110	55%
	Woman	89	44.5%
	Non-gender-binary, two-spirit, or similar	0	0%
	Others	1	0.5%
	Total	200	
Age	20-30	40	20%
	31-40	94	47%
	41-50	44	22%
	51-60	18	9%
	61-70	2	1%
	> 70	2	1%
	Total	200	
Education Level	High school diploma	39	19.5%
	Some college degree	50	25%
	Bachelors	75	37.5%
	Master’s	29	14.5%
	Ph.D.	4	2%
	Other	3	1.5%
	Total	200	
Bitcoin Experience	1 - 3 year	94	47%
	4 - 7 years	94	47%
	>7 years	12	6%
	Total	200	

Similar to the exploratory factor analysis phase, the two-stage (Ringle et al. 2012) model was followed for a confirmatory factor analysis using the guidelines of (Hair et al. 2021). All the previously identified items were confirmed at this stage with an acceptable level of factor loading above 0.7 (Hair et al. 2011) except for one item with a factor loading of 0.645, above the threshold of 0.6 (Chin 1998). In addition, all items were loaded in their intended construct with a difference greater than 0.2 to any other latent construct in the model (Howard 2016). Table 17 below provides the loading values for all the measurement items in the model. Furthermore, the model fit was assessed using the SRMR measure, which measures the match between the proposed structural model and the best model to fit the data. The SRMR value for the model is 0.080, which is considered to be a good fit as it is less than 0.1 (Henseler and Sarstedt 2013).

Table 17: Confirmatory Factor Analysis Items List

Items	Factor Loading	Construct's Sub-dimension	Construct
1. All users have equal access to the system.	0.799	System's Neutrality	Decentralization
2. All users have the same access to data.	0.839		
3. The system's outputs are the same for all users.	0.742		
4. All users can share data.	0.645		
5. All users can share resources.	0.757		
1. No one dominant entity is controlling the system.	0.827	Distributed Structure	
2. No single entity is operating the system.	0.827		
3. No single entity is affecting the continuity of the system.	0.815		
4. The system is collaboratively managed.	0.762		
1. The underlying algorithms can enforce certain actions.	0.733	N/A	
2. The underlying algorithms have control.	0.706		
3. The underlying algorithms' control in the system is legitimate.	0.852		
4. The underlying algorithms follow a specific programmable logic.	0.753		

In addition, all constructs achieved acceptable measures for reliability and validity. The reliability values for all constructs are above 0.7 using the α measure, which indicates the strong covariance among the items (Fornell and Larcker 1981). In addition, all CR values are also above 0.7, which supports convergent validity for each construct (Hair et al. 2021). Furthermore, AVE values for all constructs were above 0.5, which further supports convergent validity (Fornell and Larcker 1981). Fornell-Larcker’s criterion was also supported as the square root of AVE for each construct was above the correlation values with all other constructs in the model. Finally, multicollinearity was tested using VIF. All VIF values were below 3.3, which suggests that common method bias is not a problem in the estimated model (MacKenzie et al. 2011; Petter et al. 2007; Podsakoff et al. 2003). Table 18 provides these values.

Table 18: Reliabilities and Validities Measures for the Confirmatory Factor Analysis (CFA)

Construct	α	CR	AVE	VIF	Square Root of AVE			
					1	2	3	4
Neutrality (1)	0.816	0.832	0.577	1.772	0.759			
Dis. Structure (2)	0.827	0.840	0.653	1.291	0.451	0.808		
Algo. Authority (3)	0.765	0.815	0.582	1.672	0.621	0.395	0.763	
Trust (4)	0.826	0.831	0.742	N/A	0.466	0.407	0.427	0.861

Finally, the model also achieved satisfactory performance in the second stage as decentralization’s two sub-dimensions are significantly correlated with values above 0.5, and all the model’s path coefficients are significant (Chin 1998), as shown in Table 19.

Table 19: Weights, Path Coefficients, Significance Level, and R² for CFA Stage 2 Model

Outer Model	Weight	P value	
System Neutrality → Decentralization	0.631	0.000	
Distributed Structure → Decentralization	0.548	0.000	
Inner Model	Path Coefficient	P value	R ²
Decentralization → Trust	0.389	0.000	0.280
Algorithmic Authority → Trust	0.196	0.000	

In conclusion, the newly developed scales for perceived decentralization and perceived algorithmic authority with their psychometric properties are reliable and valid. Indeed, similar characteristics have been confirmed through an exploratory and confirmatory factor analysis from two equivalent samples belonging to the same context (i.e., Bitcoin), characterized by a high level of perceived Decentralization and perceived Algorithmic Authority. However, the observed positive association of the new scales is not always the case, as we might have a centralized system with high algorithmic authority. As such, the cross-validation (*Step 9*) of the new scales requires various contexts with various distributional properties of each scale, which is beyond the scope and the resources available for this research and has been recognized as a “*nontrivial*” path and needs collaboration within the field (MacKenzie et al. 2011). Besides, the two new scales are conceived as the system’s design features and, thus, can vary from time to time. Hence, establishing scale norms (*Step 10*) requires periodical assessment for an extended time for the desired population where the construct will be generalized. In the next section, the two established scales are tested as part of a proposed model for trust’s antecedents in Bitcoin, an example of a semi-autonomous information system.

Chapter 6. Methodology and Results

An IS research design encompasses defining the philosophical assumptions, research method, data collection technique(s), research approach, writing up, and, if applicable, a plan for publication (Myers 2019). Philosophical assumptions are general ideas about the three components of scientific inquiry of ontology (i.e., assumptions about reality and the physical world), epistemology (i.e., assumptions about knowledge and the method of knowing), and methodology (i.e., assumptions about data collection and the validity of the research findings) (Orlikowski and Baroudi 1991). These three philosophical assumptions are embedded in the researcher(s)'s choice of the positivist, interpretive, or critical approach (Myers 2019).

The positivist approach assumes that reality can objectively be measured in terms of some measurable properties and exists independent of the observer(s)'s view. It aims to test a theory in the form of research hypotheses. As such, its goal is to predict pattern(s) based on some statistical assumptions by analyzing the unit of analysis (e.g., individual, group of people, or organization) to formulate a finding about the tested hypotheses. The interpretive approach, on the other hand, is based on the idea that reality is a “subjective concept” that is socially constructed. As a result, it is subject to different interpretations and recognizes the researcher(s)'s view in building these interpretations. Thus, there are no hypotheses to be tested. Most importantly, this approach values the “context” of each research and how it might shape different meanings and variations of the research phenomena. As such, it aims to develop some insights and customized recommendations. However, these insights usually lack statistical generalizability. Finally, the critical approach challenges the assumptions taken for granted and the imposed reality on people (Orlikowski and Baroudi 1991). In this research, I follow a positivist approach as the aim is to test the hypotheses

presented in Chapter 4 empirically. Additionally, the two new scales for decentralization and algorithmic authority developed and validated in Chapter 5 are further validated.

6.1. Main Study Analysis

This section details the methodology followed to test the proposed research model for trust in semi-autonomous information systems, as shown in Chapter 4 above. Recall that Bitcoin was chosen as the context of this research study.

6.1.1. Pilot Phase

The study started with a pilot phase to test the recruitment strategy, the survey platform, and the proposed measures for initial reliability assessment. Furthermore, to ensure that the survey is free from problematic or unclear statements. Participants were recruited through Qualtrics to participate in the study's pilot phase. The pilot sample includes 30 Bitcoin users. The sample consisted of 20 men, nine women, and one non-gender participant. The age distribution was concentrated on the categories 31 – 40 and 41 – 50, which makes sense given the technology is widely used among these two age categories. Figure 11 shows the age distribution of the sample.

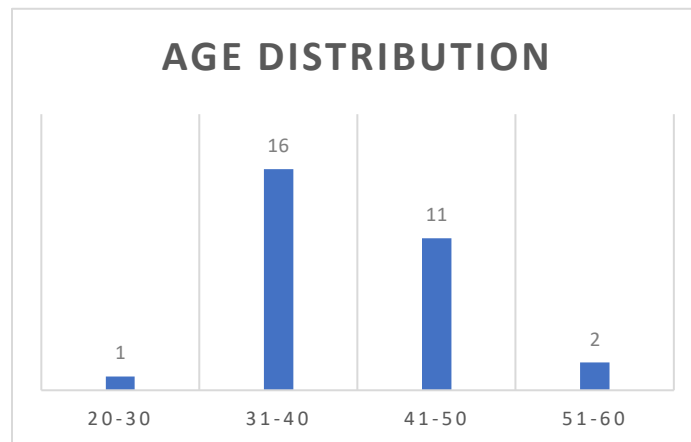


Figure 11: Pilot Sample Age Distribution

Importantly, no issues have been found with the recruitment strategy, the survey platform, or the measurement items' initial reliability assessment. Thus, I proceeded with the main phase of the study.

6.1.2. Main Phase

Bitcoin users were recruited and compensated through Qualtrics to participate in the study's main phase. Before filling out the survey, participants were prompted with two screening questions to make sure that we have the targeted Bitcoin users as follows:

Screening Question 1: What is your preferred system when making online transactions?

(Check All That Apply)

- Credit Card
- PayPal
- ***Cryptocurrencies***
- Interac
- Other
- I do not use online transactions

Screening Question 2: What is your preferred cryptocurrency?

(Check Only One)

- XRP
- Ethereum (ETH)
- ***Bitcoin (BTC)***
- Tether
- Other

To be eligible to participate in the study, participants must choose “*Cryptocurrencies*” as one of their options in the first screening question and “***Bitcoin (BTC)***” in the second screening question.

After that, qualified participants were prompted with all the survey questions outlined in *Appendix C*. A total of 475 qualified responses were obtained at this stage.

6.1.3. Data Cleansing

Before running any analysis using the data, several procedures were put in place to ensure the quality of the data collected. First, the platform-embedded algorithm examined the completion time against a predicted time threshold determined during the pilot phase. The estimated minimum time to complete the survey was 4.85 minutes. However, I agreed with the company to set the minimum time at 5 minutes to ensure we have good responses. The dataset was also examined against straight-lining responses (Payne et al. 2018). Finally, two attention check questions, *Q1: I am answering this question with full attention* and *Q2: I am answering this question without full attention*, were used in different places in the survey, and participants were required to answer them both correctly; Q1=7 and Q2=1, on a scale from 1 to 7. The initial sample of 475 responses satisfied all these conditions.

After that, an outlier analysis was also carried out on the initial dataset (N=475) to remove out-of-range values using the Boxplot method (Cohen 2008). The analysis was conducted at the item level to ensure all items were free of any outliers before using them. In addition, the two measures of skewness and kurtosis were monitored so that the value for all items should fall within the acceptable range of -2 and +2. Four items were found to have values outside of that range. Additionally, 11 items were discovered to have outliers, as shown in *Appendix D*. Upon further checking these 15 items, problems with 17 data points were noted and thus were removed before rerunning the analysis. Following the same process, eight more data points were deleted in the second round of the analysis, as shown in *Appendix D*. The remaining dataset (N=450) satisfies all the conditions for skewness and kurtosis without any outliers. Additionally, the sample size is

appropriate for the analysis as it exceeds the requirement of having at least ten times the number of items in the most complicated construct (i.e., Decentralization with nine measurement items) (Gefen et al. 2000). Table 20 below provides the sample demographics.

Table 20: Main Study Sample's Demographics

	Variable	Count	Percentage
Gender	Man	276	61.3%
	Woman	174	38.7%
	Total	450	
Age	20-30	70	15.6%
	31-40	230	51.1%
	41-50	123	27.3%
	51-60	21	4.7%
	61-70	5	1.1%
	> 70	1	0.2%
	Total	450	
Education Level	High school diploma	35	7.8%
	Some college degree	108	24%
	Bachelors	222	49.3%
	Master's	66	14.7%
	Ph.D.	13	2.9%
	Other	6	1.3%
	Total	450	
Bitcoin Experience	1 - 3 year	159	35.4%
	4 - 7 years	266	59.1%
	>7 years	25	5.5%
	Total	450	

6.1.4. Measurement Scales

A seven-point Likert scale was used to measure the variables, with 1: strongly disagree and 7: strongly agree as the two endpoints. All the model's constructs were measured using established scales in the literature except the two newly self-developed scales of decentralization and algorithmic authority, as detailed in the previous section. All scales were adapted to fit the context of this research. Trust in Bitcoin was measured using a 3-item scale (Gefen 2000). Perceived control was measured using a 4-item scale (Collier and Sherrell 2010). The sense of community was measured using a 4-item scale (Peterson et al. 2008). Users' trust beliefs in miners were

measured using a 3-item scale (Pavlou 2003). Calculative-based trust was measured using a 3-item scale (Gefen et al. 2003). Structural assurance was measured using a 3-item reflective scale (McKnight et al. 2002b, 2002a). Table 21 provides a complete description of the study’s instrument.

Table 21: Measurement Scales

Construct	Conceptualization	Operationalization
Trust	Trust is an overall feeling about the reliability and the trustworthiness of the system (Gefen 2000).	Generally speaking, <ul style="list-style-type: none"> - I trust the Bitcoin system to be reliable. - I believe the Bitcoin system to be trustworthy. - I trust the Bitcoin system.
Decentralization (newly developed construct)	Decentralization is the extent to which an information system is collaboratively managed and accessible by entities (e.g., humans or algorithms) where all participating entities share inputs (e.g., computing resources, data/information) and affect the system’s outputs with no single entity playing a dominant role in the operation of the system.	In the Bitcoin system, <ul style="list-style-type: none"> - All users have an equal access to the system. - All users have the same access to data. - The system’s outputs are the same for all users. - All users can share data. - All users can share resources. - No one dominant entity is controlling the system. - No single entity is operating the system. - No single entity is affecting the continuity of the system. - The system is collaboratively managed.
Algorithmic Authority (newly developed construct)	Algorithmic Authority is the legitimate independent level of control an algorithm has to take and enforce certain actions based on its programmable logic.	In the Bitcoin system, <ul style="list-style-type: none"> - The underlying algorithms can enforce certain actions. - The underlying algorithms have control. - The underlying algorithms' control in the system is legitimate. - The underlying algorithms follow a specific programmable logic.
Perceived Control	Perceived control refers to “ <i>a belief in one’s ability to command and exert power over the process and the outcome</i> ” of the interaction with the technology (Collier and Sherrell 2010, p.492).	When using the Bitcoin system, <ul style="list-style-type: none"> - I feel in control. - I feel decisive. - I feel I am in charge of my digital coins. - I feel in control over my digital coins.
Sense of Community*	Sense of community refers to a “ <i>feeling that the members of a community have in relation to their belonging to a community, a feeling that members worry about each other and that the group is concerned about them, and a shared faith that the needs of the members will be satisfied through their</i>	Interacting with the Bitcoin community members, <ul style="list-style-type: none"> - Provides me with the information I need about the Bitcoin system (information needs fulfillment). - Gives me a sense of belongingness to the Bitcoin community (membership). - Makes me feel I have a say about what goes on in the community (Influence).

	<i>commitment of being together</i> ” (Peterson et al. 2008, p.9).	- Provides me with a good bond with other Bitcoin users (emotional connection).
Users' Trust Beliefs in Actors**	Users’ trust beliefs in actors include the beliefs of benevolence, competency, and integrity of the miners who are involved in the Bitcoin system (Pavlou 2003).	Thinking about the miners involved in the Bitcoin system, - I feel they are competent. - I feel they keep their promises and commitments toward the system. - I feel they keep my best interest in mind.
Calculative Based Trust.	Calculative-based trust (Gefen et al. 2003).	Thinking about the miners involved in the Bitcoin system, - I feel they have nothing to gain by being dishonest when interacting with the system. - The miners have nothing to gain by not caring about users. - The miners have nothing to gain by not being knowledgeable about the system.
Structural Assurance***	Structural assurance refers to the legal and technological safeguards that create a secure environment for users (McKnight et al. 2002b, 2002a).	When using the Bitcoin system, - I feel the system has enough safeguards to make me feel comfortable using it. - I feel assured that the <i>legal</i> structures imposed by the government are there to protect me from any problems. - I feel confident that <i>encryption and other protection technologies</i> make it safe for me to make financial transactions.
Risk Tolerance	Financial risk tolerance scale (Kannadhasan et al. 2016).	In general, - I am more comfortable putting my money in a bank account than in the stock market. - When I think of the word “risk,” the term “loss” comes to mind immediately. - In terms of investing, safety is more important than returns.
<p>*: This scale has been adapted from previous research (Peterson et al. 2008) by modifying the first dimension of the construct to include information need fulfillment instead of the general need fulfillment. **: This scale has been adapted from previous research (Pavlou 2003) by modifying only the first item for the web provider’s trustworthiness to include competency instead. ***: This scale has been adapted from previous research (McKnight et al. 2002b, 2002a) by separating perceived legal structures from perceived technological protection to test each one individually.</p>		

In addition to the primary measurement items, the survey collects data for the control variables. Risk tolerance is measured using the 3-item scale (Kannadhasan et al. 2016). Gender was measured through a 4-category question of “*Male,*” “*Female,*” “*Non-binary,*” or “*Prefer not to say.*” Users’ knowledge about the system was measured through a self-reported question: ***How would you describe your knowledge level of Bitcoin?***

- None.
- Very Basic.
- Medium.
- Very Good.
- Excellent.

6.1.5. Structural Equation Modelling (SEM)

Structural Equation Modelling (SEM) was used to test the proposed model. SEM generates a measurement model to assess how much variance of the measurement item is shared with the latent construct and a structural model to estimate the linear relationship between dependent construct(s) and its predictors (Boudreau et al. 2001). Partial Least Square (PLS) (i.e., SmartPLS 4) was used for the analysis. PLS analysis was chosen because of (i) the level of complexity in the proposed model to have both reflective and formative constructs (Gefen et al. 2000); (ii) it suits exploratory models that are tested for the first time (Gefen et al. 2000); (iii) it estimates how much variance in the endogenous construct(s) can be attributed to exogenous constructs (Chin et al. 2003).

6.1.5.1. Measurement Model

The measurement model was analyzed by testing the validity and reliability of the measurement variables in the model (Chin et al. 2003).

Discriminant validity refers to the idea that the measurement items that are “*believed to make up*” a construct differ from those items that “*are not believed to make up*” the same construct (Straub et al. 2004). For the model’s reflective constructs, the factor loading of each item and the AVE were first examined (Gefen and Straub 2005). As per established guidelines, the minimum threshold for factor loading is 0.6 in the intended construct (Chin 1998), with a demonstrated

difference of 0.2 with loading on any other construct (Howard 2016). Table 22 below shows the items' loadings and cross-loading in all reflective constructs included in the model.

Table 22: Items Loading and Cross-Loading

	Algo. Authority	Dis. Structure	Calculative Based Trust	Neutrality	Perceived Control	Structural Assurance	Trust
Algo.Auth_1	0.762	0.288	0.222	0.358	0.343	0.295	0.254
Algo.Auth_2	0.651	0.262	0.166	0.315	0.222	0.197	0.148
Algo.Auth_3	0.795	0.322	0.219	0.405	0.374	0.324	0.315
Algo.Auth_4	0.747	0.372	0.24	0.395	0.321	0.344	0.309
Dis.Struc_1	0.311	0.782	0.179	0.318	0.175	0.22	0.214
Dis.Struc_2	0.299	0.792	0.233	0.33	0.188	0.186	0.203
Dis.Struc_3	0.281	0.818	0.235	0.296	0.231	0.229	0.215
Dis.Struc_4	0.386	0.740	0.188	0.403	0.33	0.376	0.344
Cal. Based_1	0.238	0.249	0.868	0.275	0.212	0.191	0.147
Cal. Based_2	0.247	0.23	0.893	0.226	0.194	0.208	0.147
Cal. Based_3	0.264	0.179	0.753	0.247	0.152	0.152	0.080
Neutrality_1	0.261	0.321	0.171	0.665	0.282	0.283	0.272
Neutrality_2	0.315	0.324	0.15	0.667	0.255	0.296	0.219
Neutrality_3	0.313	0.233	0.274	0.682	0.267	0.281	0.239
Neutrality_4	0.369	0.293	0.152	0.670	0.237	0.307	0.198
Neutrality_5	0.447	0.341	0.242	0.730	0.302	0.348	0.288
Perceived_Control_1	0.365	0.275	0.138	0.333	0.768	0.427	0.460
Perceived_Control_2	0.24	0.137	0.194	0.247	0.431	0.264	0.201
Perceived_Control_3	0.304	0.213	0.145	0.241	0.776	0.398	0.460
Perceived_Control_4	0.321	0.25	0.19	0.307	0.805	0.469	0.466
Str.Assurance_1	0.33	0.271	0.165	0.358	0.507	0.816	0.546
Str.Assurance_2	0.25	0.167	0.13	0.251	0.284	0.536	0.326
Str.Assurance_3	0.292	0.297	0.184	0.346	0.395	0.786	0.552
Trust_1	0.286	0.236	0.090	0.303	0.483	0.549	0.821
Trust_2	0.262	0.260	0.132	0.284	0.434	0.464	0.708
Trust_3	0.283	0.275	0.143	0.243	0.416	0.538	0.788

As shown in Table 22 above, all the measurement items passed the threshold of 0.6 except for two items. Perceived control's second item loading value was 0.429, and the second measurement item in structural assurance (i.e., the legal protection) had a loading value of 0.536. Thus, the two

items were removed. Table 23 provides the Cronbach alpha reliability test, composite reliability, and AVE for all reflective constructs after removing the two items.

Table 23: Cronbach's Alpha, Composite Reliability, and AVE for Reflective Constructs

Variable	Cronbach's Alpha (α)	Composite Reliability	Average Variance Extracted (AVE)
Neutrality	0.719	0.814	0.466
Distributed Structure	0.800	0.864	0.613
Algorithmic Authority	0.730	0.828	0.548
Perceived Control	0.721	0.843	0.642
Calculative Based Trust	0.798	0.878	0.706
Structural Assurance	0.580	0.826	0.704
Trust	0.655	0.814	0.594

As shown in Table 23 above, all the latent constructs achieved an acceptable level of Cronbach alpha's reliability above 0.6 (Nunnally 1967) except structural assurance with the value of 0.580. Additionally, composite reliability values for all constructs were above 0.6 (Bagozzi and Yi 1988), and AVE values for all constructs were above 0.5 (Fornell and Larcker 1981) except for neutrality, which had a value of 0.466. Thus, structural assurance was dropped from the model due to the reliability issue. However, this does not mean structural assurance is not essential in building users' trust in the system. Still, because legal protection is not present in the context of Bitcoin, users are rightly aware of that, as shown in the previous step in Table 22. neutrality, however, was kept as the AVE could be acceptable with a value above 0.4 when composite reliability is higher than 0.6 (Fornell and Larcker 1981).

For formative constructs, measurement items were evaluated per established guidelines to have strong and significant shared variance with the latent constructs (MacKenzie et al. 2011). Table 24 shows the results for all the model’s formative constructs.

Table 24: Formative Latent Constructs Items Analysis

Latent Constructs	Dimension / Items	Shared Variance	P-value
Decentralization (Second-Order)	Neutrality	0.570	0.000
	Distributed Structure	0.616	0.000
Trust Beliefs in Miners (First-Order)	Competency	0.372	0.000
	Integrity	0.507	0.000
	Benevolence	0.434	0.000
Sense of Community (First-Order)	Information Need	0.683	0.000
	Membership	0.298	0.005
	Influence	(0.022)	0.848
	Emotional Connection	0.272	0.020

As shown in Table 24 above, all items have strong and significant shared variance with the latent constructs except the influence item in the sense of community. Hence, it was removed from the construct.

To further validate the model against all established methods, the Fornell-Larcker criterion was also examined, where all reflective constructs should meet the criterion, as the square root of AVE should be higher than any correlation value with any other construct. The results are reported in Table 25 below, indicating that this criterion was met.

Table 25: Fornell-Larcker Criterion for Discriminant Validity

	Algorithmic Authority	Distributed Structure	Calculative Based Trust	Neutrality	Perceived Control	Trust
Algorithmic Authority	0.741					
Distributed Structure	0.422	0.783				
Calculative Based Trust	0.290	0.265	0.840			
Neutrality	0.498	0.445	0.292	0.683		
Perceived Control	0.415	0.310	0.196	0.370	0.801	
Trust	0.361	0.332	0.155	0.361	0.577	0.770

6.1.5.1.1. Multicollinearity and Common Method Bias

Multicollinearity occurs when two or more constructs are highly correlated, usually above 0.8 (Meyers et al. 2016), as it leads to erroneous conclusions about the relationship among the variables. Table 26 provides the correlation values among all constructs, and no violation has been found, as the highest value reported is 0.574 between trust and perceived control.

Table 26: Correlation Values among Latent Constructs

	<i>Neutrality</i>	<i>Distribute Structure</i>	<i>Algorithmic Authority</i>	<i>Perceived Control</i>	<i>Sense of Community</i>	<i>Trust Beliefs in Miners</i>	<i>Calculative Based Trust</i>	<i>Trust</i>
<i>Neutrality</i>	1.00							
<i>Distribute Structure</i>	0.408**	1.00						
<i>Algorithmic Authority</i>	0.493**	0.387**	1.00					
<i>Perceived Control</i>	0.358**	0.271**	0.395**	1.00				
<i>Sense of Community</i>	0.428**	0.278**	0.404**	0.447**	1.00			
<i>Trust Beliefs in Miners</i>	0.441**	0.226**	0.453**	0.448**	0.442**	1.00		
<i>Calculative Based Trust</i>	0.293**	0.254**	0.288**	0.190**	0.116**	0.316**	1.00	
<i>Trust</i>	0.349**	0.299**	0.339**	0.574**	0.493**	0.484**	0.152**	1.00

** : correlation is significant at the 0.01 level (2-tailed).

As respondents are the source of measurement for independent and dependent variables, the study must be examined against any potential common method bias issue (Podsakoff et al. 2003). Several tests and methods have been recommended in the literature. First, the Variance Inflation Factor (VIF) has to be checked for all the items with a threshold of 3.3 (MacKenzie et al. 2011; Petter et al. 2007; Podsakoff et al. 2003), and all items exceeded that threshold. Moreover, a one-factor test using Harman’s Single-factor analysis was carried out, and no one factor was

found to explain more than 50% of the variance (Podsakoff et al. 2003), as shown in Table 27 below.

Table 27: Principal Component Analysis for Harman’s Single Factor Test

Total Variance Explained						
Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.736	25.598	25.598	9.736	<u>25.598</u>	25.598
2	4.237	11.141	36.739			
3	3.785	9.952	46.691			
4	1.884	4.953	51.644			
5	1.475	3.878	55.523			
.	.	.	.			
.	.	.	.			
30	0.232	0.609	100.000			

Finally, a more recent technique was also conducted by adding a marker variable analysis to the model. In this technique, researchers choose a marker variable that is theoretically unrelated to the variables of interest to the model, and it has to be exposed to the same sources of biases as the variables of interest (Lindell and Whitney 2001; Simmering et al. 2015; Williams et al. 2010). As such, attitude toward the color blue was chosen as a marker variable in the model. The Construct Level Correction (CLC) approach was carried out to test the marker variable (Chin et al. 2013). In this technique, all paths’ coefficients in the model are estimated twice when the marker is present and when it is absent, and the significant differences are tested for all the model’s predictors. Any change in the R² value for the model’s two dependent constructs was also examined when adding the marker variable as one of its predictors. Tables 28 and 29 provide the marker variable test results.

Table 28: Comparison of Path Coefficients by CLC Approach and Original PLS Models

Relationships	CLC Estimation (Path Coefficients)	Original PLS Estimates (Path Coefficient)
Decentralization → Trust	0.130	0.130
Algorithmic Authority → Trust	(0.017)	(0.018)
Perceived Control → Trust	0.371	0.371
Sense of Community → Trust	0.173	0.172
Trust beliefs in Miners → Trust	0.210	0.211
Calculative-based Trust in Miners → Trust	(0.039)	(0.038)
Decentralization → Perceived Control	0.229	0.229
Algorithmic Authority → Perceived Control	0.292	0.292

Table 29: Comparison of R² Values by CLC Approach and Original PLS Models

Endogenous Constructs	CLC Estimation (R²)	Original PLS Estimate (R²)
Trust	0.435	0.435
Perceived Control	0.209	0.209

As shown in the two tables above, no differences have been found on all the paths estimated in the model, and the calculated two R² values did not change after adding the marker variable. Hence, common method bias is not an issue for the estimated model.

6.1.5.2. Structural Model

The two-stage model (Ringle et al. 2012) was followed using the guidelines of (Hair et al. 2021) to assess the structural model. In addition to all the criteria that were checked for the measurement model, the model fit was evaluated using the SRMR measure, which measures the match between the proposed structural model and the best model to fit the data. The SRMR value

for the model is 0.071, which is considered a good fit as it is less than 0.1 (Henseler and Sarstedt 2013). Figure 12 below depicts the model results, and Table 30 summarizes them.

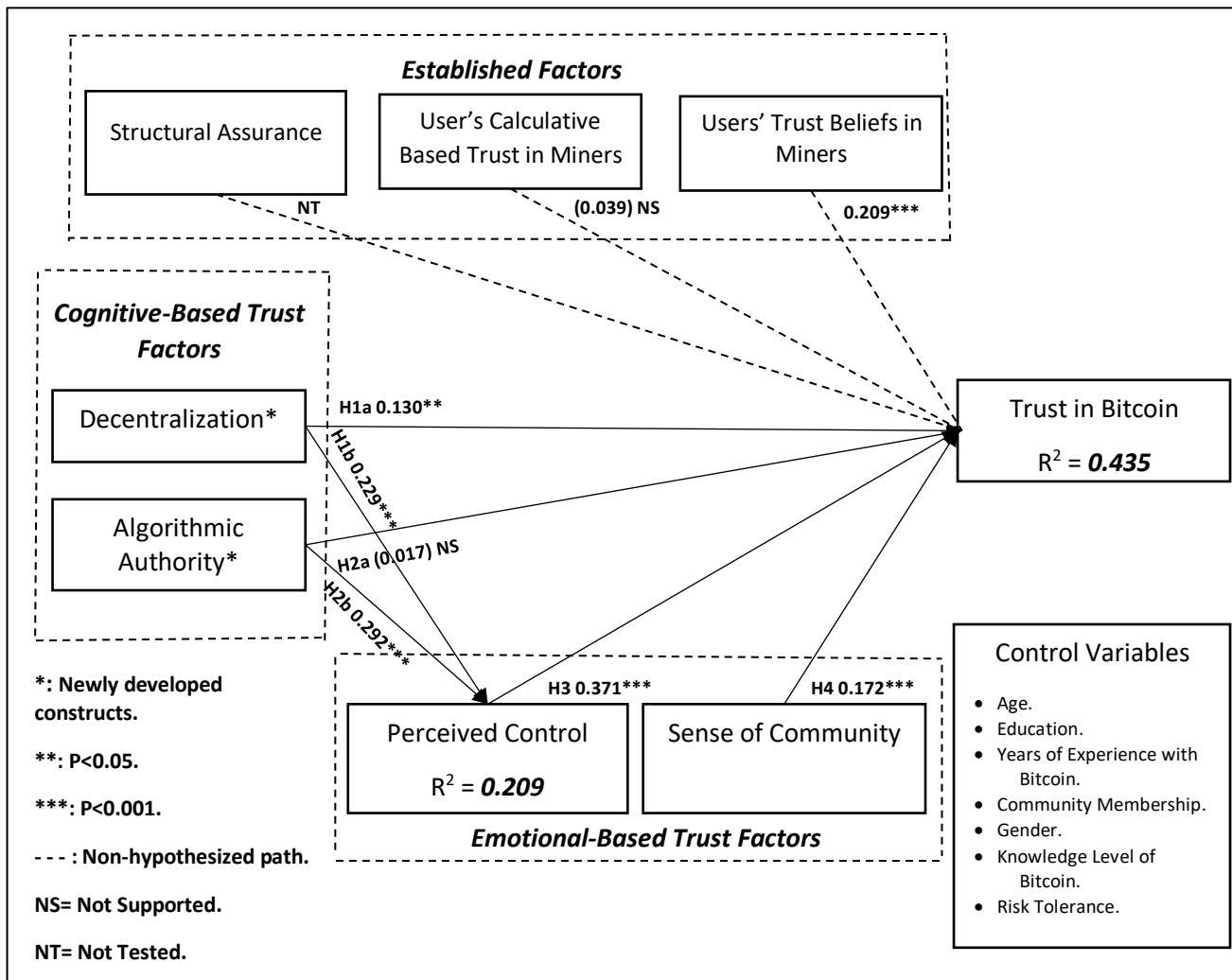


Figure 12: Final PLS Model Results

Table 30: Validation of the Study Hypotheses

Hypotheses	Path Coefficient (β)	P-value	Supported?
H1a (+): Decentralization → Trust	0.130	0.012	Yes
H1b (+): Decentralization → Perceived Control	0.229	0.000	Yes
H2a (+): Algorithmic Authority → Trust	(0.017)	0.566	No
H2b (+): Algorithmic Authority → Perceived Control	0.292	0.000	Yes
H3 (+): Perceived Control → Trust	0.371	0.000	Yes
H4 (+): Sense of Community → Trust	0.172	0.000	Yes

As shown in Table 30 above, all the hypothesized paths were supported except the path between algorithmic authority and trust. Decentralization ($\beta = 0.130$, P-value = 0.012), sense of community ($\beta = 0.172$, P-value = 0.000), and perceived control ($\beta = 0.371$, P-value = 0.000) have significant positive relationships with trust. In addition, decentralization ($\beta = 0.229$, P-value = 0.000) and algorithmic authority ($\beta = 0.292$, P-value = 0.000) have significant positive relationships with perceived control. Moreover, when testing out the two non-hypothesized established relationships (i.e., calculative-based trust and users' trust beliefs in miners), only users' trust beliefs in miners construct ($\beta = 0.209$, P-value = 0.000) has a significant positive relationship with trust.

To further explain the impact of each predictor in the model, an effect size analysis (Cohen 2013) was carried out as follows:

1. The value of R^2 per each independent construct was calculated twice, one time when one predictor was present and another time when the same predictor was dropped from the model.
2. Any change in R^2 was assessed, and any values between 0.02 and < 0.15 were considered to have a small effect, any values between 0.15 and < 0.35 were considered to have a medium effect, and any values equal to 0.35 or above were considered to have a large effect (Henseler and Sarstedt 2013; Roldán and Sánchez-Franco 2012).

Table 31 below shows the results of the effect size analysis.

Table 31: PLS Effect Size Analysis

Dependent Construct	Independents	R ²		ΔR ²	Effect Size
		Included	Excluded		
Trust	Decentralization	0.435	0.424	0.011	Very Small
	Trust Beliefs in Miners		0.408	0.027	Small
	Perceived Control		0.341	0.094	Small
	Sense of Community		0.412	0.013	Very Small
Perceived Control	Decentralization	0.209	0.171	0.038	Small
	Algorithmic Authority		0.149	0.060	Small

As shown above, all the model’s predictors have small or very small effect sizes on the dependent constructs. Having such a small effect aligns with the nature of social science research, as predictors usually have a small effect size on dependent constructs (Ferguson 2016; Rosnow and Rosenthal 2003).

6.1.5.3. Post-Hoc Analysis

In addition to testing the relationships in the proposed research model, a post hoc analysis was conducted to test the mediating effect of perceived control on the proposed positive relationships between decentralization → trust and algorithmic authority → trust. The analysis was performed using the four steps outlined by Baron and Kenny (1986). First, perceived control regressed on trust. Second, decentralization and algorithmic authority were regressed on trust one at a time while perceived control was absent. Third, decentralization and algorithmic authority were regressed on trust and perceived control one at a time. Fourth, the path coefficients from previous steps were examined, as shown in Table 32 below.

Table 32: Perceived Control Mediation Effect

Steps	Decentralization				Algorithmic Authority			
	Path	Coefficient	P-value	R ²	Path	Coefficient	P-value	R ²
Step 1	Per. Con → Trust	0.581	0.000	0.338	Per. Con → Trust	0.581	0.000	0.338
Step 2	Decen. → Trust	0.393	0.000	0.155	AA → Trust	0.364	0.000	0.133
Step 3	Decen. → Trust	0.200	0.000	0.372	AA → Trust	0.142	0.001	0.355
	Per. Con → Trust	0.504	0.000		Per. Con → Trust	0.523	0.000	
	Decen. → Per. Con	0.386	0.000	0.149	AA → Per. Con	0.414	0.000	0.171

As shown in Table 32 above, when testing the model with the two constructs of decentralization and algorithmic authority alone without any other predictors in the model (i.e., perceived control, sense of community, and users’ trust beliefs in miners), both constructs have a significant positive relationship with trust as shown in Step 2 above. Still, after adding perceived control as a mediator to the model, decentralization and algorithmic authority also had significant positive relationships with trust and perceived control, as reported in Step 3. Hence, the relationships between decentralization and algorithmic authority as predictors and trust as a dependent are partially mediated by perceived control.

6.1.5.4. Control Variables Analysis

Besides the model’s constructs, seven control variables (i.e., age, gender, risk tendency, community membership, education level, knowledge level of Bitcoin, and years of experience with Bitcoin) were also examined. The analysis was conducted in two steps. The correlation between these control variables and the model’s constructs was checked in step one. Only three variables (i.e., education level, knowledge, and years of experience) had significant correlations with some of the model’s constructs, as shown in Table 33 below. Thus, these three control variables were tested in step two, where they were added as predictors for the model’s two endogenous constructs

(i.e., trust and perceived control). Among the tested six paths, only the knowledge level and perceived control path was significant with a positive coefficient value of 0.118, P=0.014, as shown in Table 34 below. This indicates that with a higher level of knowledge about the system, users’ perception of perceived control will be increased.

Table 33: Correlation Results for Control Variables

<i>Control Variable</i>	Neutrality	Dis. Structure	Algorithmic Authority	Perceived Control	Sense of Community	Trust Beliefs in Miners	Trust
Age	0.002	0.045	-0.048	-0.063	-0.016	-.095	0.023
Gender	-0.074	-0.056	0.018	-0.021	0.007	0.023	-0.056
Risk Tendency	0.058	.153	0.050	0.023	0.083	0.021	.119
Community Membership	0.089	0.054	.116	-.122	0.063	0.088	-0.048
Education Level	.186**	-0.034	.150**	0.081	.116*	.205**	.112*
Knowledge Level	.219**	0.077	.255**	.225**	.224**	.303**	.169**
Years of Experience	.255**	0.077	.239**	.094*	.147**	.221**	.119*
**: Correlation is significant at the 0.01 level. *: Correlation is significant at the 0.05 level.							

Table 34: Control Variables Analysis PLS Results

<i>Control Variable</i>	Endogenous Constructs	Path Coefficient	Significance
Education Level	Trust	0.021	Not Significant
	Perceived Control	0.020	Not Significant
Knowledge Level	Trust	(0.022)	Not Significant
	Perceived Control	0.118	0.014
Years of Experience	Trust	0.008	Not Significant
	Perceived Control	(0.024)	Not Significant

Chapter 7. Discussion, Contributions, and Limitations

This research aims to explain the nature of a new emerging class of information systems - SAIS. In SAIS, both humans and algorithms have control. Following a design theory approach, this research proposed a design theory to explain how such new systems could be perceived as trustworthy. The proposed theory identifies algorithmic authority and decentralization as critical new factors driving users' perception of trust in SAIS. The new theory encompasses four propositions and hypotheses related to algorithmic authority, decentralization, a sense of control for human participants, and security and privacy protection to ensure SAIS trustworthiness. As security and privacy protections have already been validated in the IS literature (Chandra et al. 2010; Xin et al. 2013) to build users' trust in information systems, three hypotheses were validated as part of a larger trust model in SAIS. The new trust model included self-developed scales for decentralization and algorithmic authority. The model was validated in the context of Bitcoin as an example of SAIS. The following sections discuss the findings, contributions, limitations, and future research.

7.1. Discussion of the Proposed SAIS Design Theory

In information systems, there are five types of theories: theories for analyzing, theories for explaining, theories for predicting, theories for explaining and predicting, and theories for design and action (Gregor 2006). Among them, design theories answer the question of “*how to do something*” (Gregor 2006, p.628). Design theories in IS usually depend on existing theories, kernel theories, to inform the proposed design (Walls et al. 1992, 2004). Design theories are the operationalization of existing theories as they include empirical hypotheses that can be used to validate theories (Goldkuhl 2004).

In this research, a proposed design theory for SAIS was developed. At the very core of this new theory is human-algorithm collaboration and how to design a SAIS where humans collaborate with algorithms, which is perceived as a trustworthy information system. The starting point in the proposed SAIS theory is acknowledging algorithms with the authority to collaborate meaningfully with human counterparties. Such collaboration exists based on a need and a purpose so that it can be justifiable logically and economically. The logical aspect is based on the fact that algorithms can do tasks beyond humans' capabilities, such as complex computations; therefore, only algorithms should be assigned such tasks. Likewise, there are other tasks only humans can do, such as tasks that require judgment, involvement, and creativity in developing new insights and conclusions. Additionally, the economic rationale comes from the fact that it is efficient to have collaboration between algorithms and humans, where the productivity of each party is augmented because of such collaboration. As far as the design of SAIS allows for this collaboration to be justifiable, it will be perceived as legitimate.

By recognizing algorithms with authority, this authority will have a defined scope. This scope establishes the extent to which algorithms can affect human actions by enforcing specific actions and deterring undesirable actions. Thus, a critical ethical question might arise about allowing these algorithms to direct and control human actions. Addressing this question should be based on a meaningful discussion among all stakeholders so that the shared benefit can be achieved by augmenting existing systems or creating new ones. Importantly, algorithmic authority and control in SAIS should be treated as a system capability, not a threat. As such, SAIS designers should be aware of this issue and keen on having active communication channels with all involved stakeholders.

While established theories such as Actor-network theory explain the motivations and actions of humans and nonhumans in collaborative networks (Walsham 1997), the proposed design theory operationalizes what it means for such collaborative work to be perceived as trustworthy. Through leveraging collaborative control theory, humans and algorithms should have authority in the design of SAIS. Indeed, the proposed new theory recognizes humans with a sense of control and algorithms with algorithmic authority. The proposed theory argues for a decentralized structure as the means for autonomy to all parties through appropriate alignment and enforcement mechanisms. This autonomy is the core of human-computer integration (Stephanidis et al. 2019).

A decentralized structure for SAIS facilitates efficient and effective decisions for humans and algorithms where every decision point is appropriately supported with relevant data, information, and resources. With any use of data, information, and resources, the underlying enabling technologies must ensure privacy protection for human participants and the system's security, thus being perceived as trustworthy. The underlying decentralized structure should also reflect the growing capabilities of algorithms to learn (i.e., machine learning tools and AI) and the growing computing resources that humans can utilize to tweak algorithmic authority. Thus, any proposed SAIS will constantly evolve through internal feedback loops, assessment for SAIS self-governance and enforcement mechanisms, and periodic external assessment. Consequently, we can now think about future decentralized systems where algorithmic authority interacts dynamically with human participants to achieve optimality in the system's operation and use of resources.

Given the recent significant developments in AI models, especially Generative AI models (e.g., ChatGPT), this theory has provided an alternative view for the future of human-algorithm collaboration. While these developments in the AI models pose an essential question about the

value of human work when algorithms could be working autonomously to complete tasks and whether the future will be fully autonomous and controlled by algorithms, this research takes a different stand by envisioning a semi-autonomous future where algorithms collaborate with humans. A future that is “Human + AI” (Daugherty and Wilson 2018), not “Human vs. AI.” A future where we recognize algorithms' capabilities, augment our productivity and never undermine our creativity and innovation. As such, a design theory for SAIS was needed to explain the nature of such systems, as the absence of a theory hinders our ability to achieve synergy in human-computer collaboration (Stephanidis et al. 2019).

7.2. Discussion of Scale Development Results

Scales bridge theoretical ideas about constructs and empirical observations of testing them in specific contexts. Indeed, scales are the toolkit to test theories; thus, they are the building blocks of our knowledge base. Only a few studies have been dedicated to scale development in the IS literature, even though it has been more than a decade since the seminal work of Mackenzie et al. 2011 which provides guidelines for scale development. Still, the guidelines have been followed partially only in one paper thus far (Jabagi et al. 2021). To the best of my knowledge, this is the only research that followed the guidelines thoroughly. In developing the two scales, I encountered issues worthy of further discussion and other considerations for future research, as shown below.

7.2.1. Dimensionality Issue for Constructs

Even though the guidelines were apparent in explaining the dimensionality issue of the new constructs as formative vs. reflective and the appropriate assessment techniques, the guidelines left the door open for different interpretations where, for example, the same construct could be conceptualized both ways (e.g., Job Satisfaction). I argue that this is an important

question, and it has to be adequately addressed not only in the early stage of conceptualization, as recommended, but throughout the process's steps.

The starting point is that researchers have to start with an open mindset when exploring the dimensionality issue of the construct and provide an appropriate rationale for their “initial expectation” about whether a construct has different dimensions and how these dimensions relate to each other. The next step in validating this expectation has to be driven from the critically recommended inductive qualitative phase before imposing any conceptualization bias on informants. At this stage, the main task of the researcher(s) is to explain any differences between how a construct's dimensionality issue could be conceptualized as theory-driven versus data-driven from interviews. For example, the initial conceptualization of Decentralization based on the literature includes the two dimensions of the system's resilience and freedom from concentrated power (Walch 2019). However, the interviews were helpful in refining these two dimensions to be conceptualized as the system's neutrality and distributed power structure. Likewise, Algorithmic Authority is conceptualized as a multidimensional construct that includes the ability of an algorithm to direct human actions and identify which information is true (Lustig and Nardi 2015). Nonetheless, based on the interviews conducted, the construct is conceptualized as a unidimensional construct that includes the ability of an algorithm to control specific tasks based on its logic.

Next, the measurement items generation phase has to depend on the result of the previous analysis, which it has to be aligned with conceptualizing the construct as either formative or reflective. For reflective measurement items, the expectations are that each dimension has to be measured through only one set of items, and these items have to be similar to each other in reflecting the same idea and to be distinct enough not to mix the dimensions. This step, in

particular, has not been discussed enough in the guidelines (MacKenzie et al. 2011). This will also significantly impact the recommended one-way ANOVA test to be fully utilized in establishing proper content validity, not just face validity, as suggested by (MacKenzie et al. 2011).

In summary, the construct dimensionality issue has to be approached with flexibility so that researchers are open to modifying their initial understanding of the construct dimensions while going through the various steps of the scale development process. In other words, the initial conceptualization is expected to be affected by the initial literature review, which will constitute a particular understanding of the construct's dimensions. Then, inductive interviews could provide an opposing or confirming stance on those dimensions. Additionally, the raters phase could contribute to this discussion with some insights. The critical aspect is for the researchers to be receptive and open to emerging differences and, most importantly, explain and report such differences. Lastly, the selected context for validating the new construct might have some unique characteristics that might cause the dimensions to behave in a specific way that is not as expected. As such, it might be a data-driven decision, not just a theory-driven decision like what was conveyed in the guidelines (MacKenzie et al. 2011). Hence, researchers should be mindful of this relativity issue.

7.2.2. Conceptualization, Operationalization, and Contextualization

In the scale development process, a clear distinction has to be made between conceptualization (i.e., conceptual definition), operationalization (i.e., the measurement items), and contextualization (i.e., how users perceive the construct). Notably the role of context in shaping the process. In fact, it is okay to deal with some potential differences between the conceptual definition of the construct (i.e., how the researcher(s) and experts think about the construct qualitatively), the operationalization process of the construct (i.e., how the construct is

measured quantitatively), and the contextualization of the construct (i.e., how users collectively perceive the construct based on both qualitative and quantitative analyses). In doing so, the chosen context might have a higher or a lower level of the new construct or even be missing some characteristics/dimensions entirely. Thus, the definition and the measurement items might require going through an adaptation process to convey the “relative” meaning of the new construct based on the uniqueness of each context. Hence, it ensures each construct's “relevant” meaning, not absolute. As such, the important decisions that the researchers will come up with during these different phases will craft the construct in a certain way and thus could bias the scale. Figure 13 below shows the impact of each of the three phases of conceptualization, operationalization, and contextualization in biasing the scale.

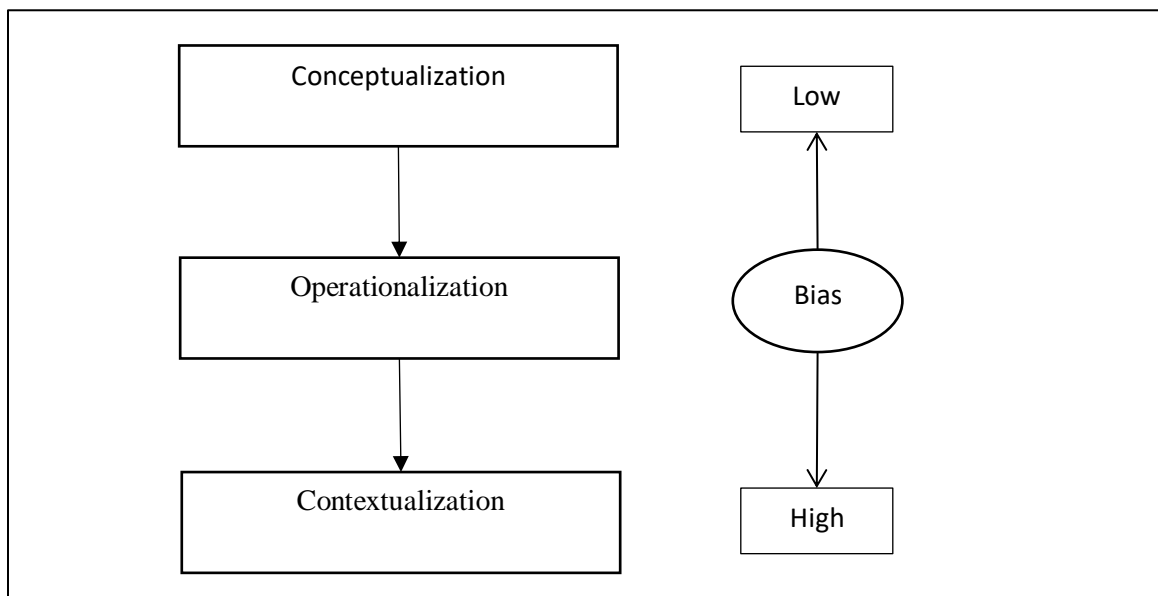


Figure 13: Bias Impact on the Scale Development Process

As shown in Figure 12 above, the conceptualization process is expected to have a low bias on the scale. This is because researchers have many safeguards to utilize as they are supposed to use a diverse body of literature in many related fields. Mainly, they must consider similar and

different constructs to explain why the focal construct is expected to have similar characteristics and other unique ones that make them distinct. In addition, conducting inductive interviews with subject matter experts could lower the possibility of the researchers imposing biases on the initial conceptualization step of the construct.

Next, the operationalization phase is expected to have a moderate bias on the construct's scale. In this phase, the researchers must generate the measurement items in alignment with how the focal construct was defined as either reflective or formative. Therefore, the choice of certain words or even the improper definition of the dimensionality issue will bias the measurement items. Finally, the chosen context where the measurement items will be tested will strongly influence the scale, as each context's unique characteristics could drive the measurement items to behave in specific ways. As such, it is essential to distinguish between the construct's context-free and context-unique characteristics.

It has to be noted that while the call in the IS literature was about considering “context” when developing relevant theories in IS (Hong et al. 2014), I urge the need for proper consideration of the context at the scale level so that our interpretation of phenomena are accurately representative and thus predictable as theoretical imperatives. Likewise, implementing the cross-validation and construct norms as recommended in the guidelines (MacKenzie et al. 2011) should not be only about new constructs but also about established constructs to understand and assess the role of any potential biases imposed on the constructs.

7.2.3. Further Considerations for Future Scale Development Research

The guidelines (MacKenzie et al. 2011) clearly describe the quantitative cut-off points to be used in assessing the model's performance. However, some of the recommended techniques have been scrutinized recently, such as the Cronbach Alpha cut-off point of 0.7 (Cho and Kim

2015; Peterson 1994), Fornell & Larcker criterion, and Heterotrait-Monotrait ratio assessment of discriminant validity (Henseler et al. 2015). Importantly, it is crucial to explain the rationale behind these cut-off points so that some practical guidelines can be followed to remedy any issue with the constructs, especially since reaching this point of the data collection comes after going through a long path that entails a significant amount of time and resources before testing the items. Knowing these options before collecting the data will be very helpful in providing some precautions to be considered during the conceptualization and operationalization phases. Thus, a review of the recommended quantitative cut-off points is needed to reassess their validities and, most importantly, explain their rationale in the scale development process. This, in particular, provides exciting avenues for future research to enrich, update, and further improve the applicability of the guidelines in the IS literature.

7.3. Discussion of the Proposed New Model for Trust in SAIS

SAIS, such as Bitcoin, are widely described as “*Trustless*” or “*Trust-free*” systems (Ostern 2018; Werbach 2018). However, this research shows that trust is still an essential part of these systems, but it requires a different conceptualization. The origins of trust in these systems come from technology-related features and other human-related features. To that end, this research builds the case for a new type of trust rooted in the information system’s design features, where trust is generated because of the meaningful human-computer integration embedded in the system’s design.

Results from the structural model reveal that decentralization, as a technology-related feature, has a positive association with trust ($\beta = 0.130$; $p < 0.012$). As such, an increase in users’ perception of the system’s neutrality and the distributed power structure is associated with increased trust in the system. This aspect, in particular, is also supported by several statements in

the open-ended question in the survey when respondents were asked to explain why they trust Bitcoin. Below are some examples:

- *“The Bitcoin system is trustworthy because it is decentralized.”*
- *“I like that the system is decentralized, which makes me feel good about it.”*
- *“ I trust the system because it is decentralized and secure, and no central institution manages everything.”*
- *“Because the system is not centralized and controlled by one entity.”*
- *“The characteristic of decentralization is that by removing the control of centralized institutions, the system becomes more secure and reliable.”*
- *“The Bitcoin system removes the centralized management system and decentralizes control of the system to nodes in the network.”*
- *“The foundation of the trust in the Bitcoin system differs from traditional payment systems because Bitcoin is a decentralized cryptocurrency.”*
- *“The Bitcoin system is different as payments are made through network nodes that are not dependent on any central authorities.”*
- *“Because all users have access to the system.”*
- *“There is no third party involved in the system.”*
- *“The system operates in a secure decentralized manner, and trust is created based on the consensus of the user network.”*
- *“Because the system is a decentralized digital currency maintained by a network of users.”*
- *“What is different about the Bitcoin system is that it is decentralized, and all users can participate.”*

- *“The Bitcoin system is more secure as there is no single point of failure.”*
- *“No one entity controls it, and users have access to it; it is decentralized.”*
- *“The system is free from third party .”*
- *“The system is decentralized that the government does not back.”*
- *“It is transparent and decentralized, and most importantly, it does not allow the government to print to the point of worthlessness.”*
- *“Because there is no one authority that can crash the entire system.”*

While it might seem counter-intuitive to see people trusting a decentralized system, this decentralization feature allows users to feel that they are in control. This perceived users’ control is supported in the SEM with a significant association with trust ($\beta= 0.371$; $p<0.000$) and with some quotes from participants as follows:

- *“When using the system, I feel confident in myself instead of anything. Decentralized finance takes central power away and balances it among the users.”*
- *“Users can control the system.”*
- *“In a decentralized system like Bitcoin, you are practically in control of your money, unlike online banking.”*
- *“It is different because every user owns and controls the system.”*
- *“The system is decentralized, so I feel more control over my funds.”*
- *“I can control my digital coins.”*
- *“I can make transactions any place with my cryptocurrencies.”*

This finding has also been supported where decentralization ($\beta= 0.229$; $p<0.000$) and algorithmic authority ($\beta= 0.292$; $p<0.000$) are significantly associated with perceived control, as reported in the SEM results. Additionally, as the post-hoc analysis shows, perceived control

partially mediates the relationship between decentralization and trust and algorithmic authority and trust. However, the direct path between algorithmic authority and trust has not been supported ($\beta = -0.017$; $p < 0.566$). This leads to an interesting finding that users are not ready to associate their trust in the system directly with algorithmic authority but accept it as long as it enables them to feel that they are also in control. Hence, it further supports SAIS's first proposition that the successful design of SAIS recognizes algorithms and humans with control.

Additionally, the model includes the sense of community construct and is shown to have a significant positive relationship with Trust ($\beta = -0.172$; $p < 0.000$). This indicates that even though the system is safe enough with appropriate safeguards and advanced technologies, users still base their trust level on some emotional connection from belonging to a specific community. Importantly, information needs (**Loading Value = 0.683**; $p < 0.000$), Membership (**Loading Value = 0.298**; $p < 0.000$), and emotional connection (**Loading Value = 0.272**; $p < 0.000$) are the drivers of this feeling as subdimensions. However, the need to influence others (**Loading Value = -0.022**; $p < 0.848$) who belong to the community is not supported in the context of the Bitcoin community as a subdimension of the sense of community. This can be explained by the fact that the system is now mature enough, and there is no need to influence other users to make important decisions about the system. Nonetheless, reevaluating this subdimension, in particular, could be relevant when there might be a need to change the Bitcoin protocol as a community-driven initiative.

The findings report on three other non-hypothesized paths of users' trust beliefs in miners, structural assurance, and calculative-based trust to positively influence trust. Users' trust beliefs in miners have a positive relationship with trust ($\beta = 0.209$; $p < 0.000$). As such, users' trust beliefs in actors are still important factors in building the users' overall trust in the system. No support

was obtained for calculative-based trust in miners ($\beta = -0.039$; $p < 0.680$), and structural assurance was not tested due to the reliability issue (Cronbach's Alpha (α) = 0.580) after removing the legal protection item included in the original scale. However, this does not mean structural assurance is irrelevant; instead, it emphasizes that technological protection alone ensures the users' sense of protection without the need for any governmental assurance. Participants' quotes further support this finding, as follows:

- *“Encryption and its protection technology allow me to conduct financial transactions safely.”*
- *“More advanced technology and features than traditional ones that make the system secure and trustworthy.”*
- *“The system has enough security mechanisms to make me comfortable using it.”*
- *“I trust the Bitcoin system to be much safer.”*
- *“The Bitcoin system is much more secure than any other system.”*

Finally, among the tested control variables (i.e., age, gender, risk tendency, community membership, education level, knowledge level of Bitcoin, and years of experience with Bitcoin), only users' knowledge level of Bitcoin positively impacts algorithmic authority in the model ($\beta = 0.118$; $p < 0.000$). This finding indicates the critical role of knowledge in perceiving algorithmic authority as a positive factor in any SAIS.

7.3.1. Contributions to Theory

This research contributes to the theory with a newly proposed trust model to explain the basis of trust as an IS design-driven factor. While previous research studied the information system's design as an exogenous or external factor (Grabner-Kräuter and Kaluscha 2003; Pavlou 2003), this research shows that new design features such as decentralization can drive users' trust

toward the system. However, this does not mean that established trust factors, such as trust beliefs in miners (McKnight et al. 2002b), are irrelevant. Indeed, both factors are significant in forming users' trust in SAIS. In turn, this corroborates the study's initial propositions in the newly proposed theory for SAIS, which is that a decentralized structure should ensure users' trust.

Additionally, and as argued before, we cannot understand trust without the users' perception of the safety of the transacting environment, which is known as structural assurance (McKnight et al. 1998). In previous studies, this structural assurance was derived from technological and legal protection. Nonetheless, this research shows that technological protection alone can elicit such feelings in users without any legal protection, as in the case of Bitcoin. Notably, Bitcoin users are aware of that fact, as shown in the lower loading of the legal protection item in the latent construct of structural assurance. Even though this construct was not tested due to the reliability issue after dropping the legal protection item, in future studies, this construct should be contextualized based on mere technological protection.

Moreover, other emotional factors, namely perceived control and the sense of community, are also considered here to drive users' trust. Further, the two technological factors of decentralization and algorithmic authority have also been positively associated with users' perceived control. This leads to an exciting finding that humans are ready to accept this algorithmic authority as much as they perceive it as an enabling factor of their control when interacting with any system. As a result, viewing this algorithmic authority as an enabler for human autonomy, not a substitute, has proven to be an excellent path to promote successful human-algorithm collaboration in SAIS, as proposed in the new SAIS design theory. Notably, users' knowledge has been shown to affect the positive perception of algorithmic authority and its ability to influence

users' trust in the system. This corroborates early research findings about how familiarity with the system positively affects users' trust (Gefen 2000).

7.3.2. Contributions to Practice

Explaining the nature of trust in semi-autonomous information systems such as Bitcoin has numerous implications for practice. First, this research builds the case for public awareness to imagine a trustworthy human-algorithm collaboration as the essence of any SAIS where algorithms are recognized with authority to carry out some tasks. This will lead to significant benefits when implementing this idea to enhance the system's efficiency when allocating repetitive tasks to algorithms, reduce risks that are associated with human errors, handle complex tasks that involve analyzing complex computational factors for instant decisions, save more human lives for not doing risky tasks, and overall improve the system accessibility, scalability, and adaptability.

Second, the proposed research model tested the two unique and essential factors of decentralization and algorithmic authority and showed their importance in building users' trust in cryptocurrencies. The suggested factors can inform stakeholders (e.g., central banks, designers, and developers) about the importance of these design features to build users' trust in any proposed similar applications such as CBDC and semi-autonomous information systems in general (e.g., global semi-autonomous supply chain networks, global semi-autonomous security networks, global semi-autonomous financial services networks, global semi-autonomous eCommerce platforms). Designers of these new systems should strike and craft a delicate and fine balance between the tasks that algorithms should control and the other tasks that humans should control to optimize the system's overall performance and, most importantly, make it trustworthy. Designing a decentralized system is also expected to reinforce the system's security by driving technological protection and the diffused power structure so that the system does not rely on a single point of

failure, third-party assurance, or legal protection to be trustworthy. A decentralized structure of SAIS allows nodes to have power and thus perceive themselves as active actors, not passive. Hence, decentralization improves the overall trustworthiness of the system because of this perceived level of control. Moreover, decentralization ensures a sustainable future for SAIS by facilitating system interoperability, as it allows nodes to communicate and collaborate on shared system objectives and enables adaptive governance through collective decision-making and evolution over time.

Finally, SAIS would benefit from associated communities so that users can access required information about the system and feel a sense of membership and connection to build trust. It is crucial to provide all users with the necessary knowledge about the system in general and explain the nature of algorithmic authority, in particular, so that their level of trust in the system can be higher. Thus, this emphasizes the importance of these elements in any new SAIS initiatives.

7.3.3. Limitations and Future Research

Even though this research argues for a new basis for trust in semi-autonomous information systems, some limitations could be raised. First, the proposed research model is not comprehensive because it does not include all the variables that can explain trust with 100% accuracy. However, this research tests the new and relevant technology features of decentralization and algorithmic authority to assess their role in explaining users' trust in the system. Along with all the other included variables, as reported in the SEM's R^2 value, these variables account for only 43.5% percent of the variance explained in trust. As such, other non-included variables could be tested in future research, such as privacy protection, perceived anonymity, and transparency. Another variable could be structural assurance, which was not tested due to reliability issues.

Second, the research model was validated through a survey study. Even though the generalizability of the study findings is ensured through external validity, the internal validity of the proposed relationships could be criticized due to the lack of experimental manipulation. Thus, future research could be done in an experimental setting by manipulating variables, such as algorithmic authority and perceived control, and testing their impacts on trust. Moreover, Bitcoin is a SAIS with a higher level of algorithmic authority, and the role of human intervention is mainly through providing computing resources. Hence, the results of the trust model are generalizable to similar types of SAIS. Future research could consider other SAIS with a higher level of human control.

Third, this research applies only to any public Blockchain applications, but it needs to be tested/refined before generalizing it to any private or hybrid Blockchain applications. Testing the proposed model in other contexts, such as algorithmic platforms like Uber, also provides interesting future avenues for this research.

Finally, this work focuses only on the factors that might influence trust in the post-adoption stage, as driven by the system's underlying infrastructure and architecture, which might drive this trust without considering any transaction-related factors. As a result, the factors that drive pre-adoption trust are out of the scope of this research. Hence, the factors that might lead to the users' initial trust or distrust in the system and any transaction-related factors, such as traceability and speed, give excellent opportunities for future research.

References

- Aken, J. E. van. 2004. "Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-tested and Grounded Technological Rules," *Journal of Management Studies* (41:2), Wiley Online Library, pp. 219–246.
- Allen, M. J., and Yen, W. M. 2001. *Introduction to Measurement Theory*, Waveland Press.
- André, Q., Carmon, Z., Wertenbroch, K., Crum, A., Frank, D., Goldstein, W., Huber, J., Van Boven, L., Weber, B., and Yang, H. 2018. "Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data," *Customer Needs and Solutions* (5), Springer, pp. 28–37.
- Antonopoulos, A. 2014. "Bitcoin Security Model: Trust by Computation." (<http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html>).
- Antonopoulos, A. 2017. *Mastering Bitcoin: Programming the Open Blockchain*, O'Reilly Media, Inc.
- Arias-Oliva, M., Pelegrín-Borondo, J., and Matías-Clavero, G. 2019. "Variables Influencing Cryptocurrency Use: A Technology Acceptance Model in Spain," *Frontiers in Psychology*. (<https://doi.org/10.3389/fpsyg.2019.00475>).
- Armstrong, A., and Hagel, J. 1997. *Net Gain: Expanding Markets through Virtual Communities*, Harvard Business School.
- Auinger, A., and Riedl, R. 2018. "Blockchain and Trust: Refuting Some Widely-Held Misconceptions," in *International Conference on Information Systems 2018, ICIS 2018*.
- Awad, N. F., and Ragowsky, A. 2008. "Establishing Trust in Electronic Commerce through Online Word of Mouth: An Examination across Genders," *Journal of Management Information Systems* (24:4), Taylor & Francis, pp. 101–121.
- Babbie, E. R. 2020. *The Practice of Social Research*, Cengage AU.
- Bagozzi, R. P., and Yi, Y. 1988. "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science* (16:1), Springer, pp. 74–94.
- Bapna, R., Gupta, A., Rice, S., and Sundararajan, A. 2017. "Trust and the Strength of Ties in Online Social Networks: An Exploratory Field Experiment," *MIS Quarterly: Management Information Systems* (41:1). (<https://doi.org/10.25300/MISQ/2017/41.1.06>).
- Baron, R. M., and Kenny, D. A. 1986. "The Moderator–Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations.," *Journal of Personality and Social Psychology* (51:6), American Psychological Association, p. 1173.

- Bart, Y., Shankar, V., Sultan, F., and Urban, G. L. 2005. "Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study," *Journal of Marketing* (69:4), SAGE Publications Sage CA: Los Angeles, CA, pp. 133–152.
- Berkeley, J. 2015. "The Trust Machine - The Technology behind Bitcoin Could Transform How the Economy Works," *The Economist*.
- Bitcoin.org. 2020. "Bitcoin Community." (<https://bitcoin.org/en/community>).
- Bitcointalk.com. 2019. "Bitcoin Forum - Statistics Center," *Web*. (<https://bitcointalk.org/index.php?action=stats>).
- Botsman, R., and House, P. R. 2018. *Who Can You Trust? : How Technology Brought Us Together - and Why It Could Drive Us Apart*, p. 323. (https://books.google.co.uk/books/about/Who_Can_You_Trust.html?id=7cGWDgAAQBAJ&redir_esc=y).
- Boudreau, M.-C., Gefen, D., and Straub, D. W. 2001. "Validation in Information Systems Research: A State-of-the-Art Assessment," *MIS Quarterly*. (<https://doi.org/10.2307/3250956>).
- Brynjolfsson, E., and Mendelson, H. 1993. "Information Systems and the Organization of Modern Enterprise," *Journal of Organizational Computing and Electronic Commerce* (3:3), Taylor & Francis, pp. 245–255.
- Bucher, E. L., Schou, P. K., and Waldkirch, M. 2021. "Pacifying the Algorithm—Anticipatory Compliance in the Face of Algorithmic Management in the Gig Economy," *Organization* (28:1), SAGE Publications Sage UK: London, England, pp. 44–67.
- Burt, R. S. 1976. "Interpretational Confounding of Unobserved Variables in Structural Equation Models," *Sociological Methods & Research* (5:1), Sage Publications Sage CA: Thousand Oaks, CA, pp. 3–52.
- Burtch, G., Ghose, A., and Wattal, S. 2014. "Cultural Differences and Geography as Determinants of Online Prosocial Lending," *MIS Quarterly: Management Information Systems* (38:3), pp. 773–794. (<https://doi.org/10.25300/MISQ/2014/38.3.07>).
- Chandra, S., Srivastava, S. C., and Theng, Y.-L. 2010. "Evaluating the Role of Trust in Consumer Adoption of Mobile Payment Systems: An Empirical Analysis," *Communications of the Association for Information Systems*.
- Cheng, M., and Foley, C. 2019. "Algorithmic Management: The Case of Airbnb," *International Journal of Hospitality Management* (83), Elsevier, pp. 33–36.
- Chin, W. W. 1998. "Commentary: Issues and Opinion on Structural Equation Modeling," *MIS Quarterly*, JSTOR, vii–xvi.

- Chin, W. W., Gopal, A., and Salisbury, W. D. 1997. “Advancing the Theory of Adaptive Structuration: The Development of a Scale to Measure Faithfulness of Appropriation,” *Information Systems Research* (8:4), INFORMS, pp. 342–367.
- Chin, W. W., Marcolin, B. L., and Newsted, P. R. 2003. “A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study,” *Information Systems Research* (14:2), INFORMS, pp. 189–217.
- Chin, W. W., Thatcher, J. B., Wright, R. T., and Steel, D. 2013. “Controlling for Common Method Variance in PLS Analysis: The Measured Latent Marker Variable Approach,” in *New Perspectives in Partial Least Squares and Related Methods*, Springer, pp. 231–239.
- Cho, E., and Kim, S. 2015. “Cronbach’s Coefficient Alpha: Well Known but Poorly Understood,” *Organizational Research Methods* (18:2), Sage Publications Sage CA: Los Angeles, CA, pp. 207–230.
- Churchill, G. A. 1979. “A Paradigm for Developing Better Measures of Marketing Constructs,” *Journal of Marketing Research* (16:1), SAGE Publications Sage CA: Los Angeles, CA, pp. 64–73.
- Cohen, B. H. 2008. *Explaining Psychological Statistics*, John Wiley & Sons.
- Cohen, J. 2013. *Statistical Power Analysis for the Behavioral Sciences*, Academic press.
- Collier, J. E., and Sherrell, D. L. 2010. “Examining the Influence of Control and Convenience in a Self-Service Setting,” *Journal of the Academy of Marketing Science* (38:4), Springer, pp. 490–509.
- Cyr, D., Hassanein, K., Head, M., and Ivanov, A. 2007. “The Role of Social Presence in Establishing Loyalty in E-Service Environments,” *Interacting with Computers* (19:1), Oxford University Press, pp. 43–56.
- Cyr, D., Head, M., Larios, H., and Pan, B. 2009. “Exploring Human Images in Website Design: A Multi-Method Approach,” *MIS Quarterly: Management Information Systems* (33:3). (<https://doi.org/10.2307/20650308>).
- Daugherty, P. R., and Wilson, H. J. 2018. *Human+ Machine: Reimagining Work in the Age of AI*, Harvard Business Press.
- Davis, F. D. 1989. “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology,” *MIS Quarterly*. (<https://doi.org/10.2307/249008>).
- Delfanti, A. 2021. “Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse,” *New Media & Society* (23:1), SAGE Publications Sage UK: London, England, pp. 39–55.
- Diamantopoulos, A., and Winklhofer, H. M. 2001. “Index Construction with Formative

- Indicators: An Alternative to Scale Development,” *Journal of Marketing Research* (38:2), SAGE Publications Sage CA: Los Angeles, CA, pp. 269–277.
- Doney, P. M., and Cannon, J. P. 1997. “An Examination of the Nature of Trust in Buyer-Seller Relationships,” *Journal of Marketing* (61:2). (<https://doi.org/10.2307/1251829>).
- Doney, P. M., Cannon, J. P., and Mullen, M. R. 1998. “Understanding the Influence of National Culture on the Development of Trust,” *Academy of Management Review* (23:3). (<https://doi.org/10.5465/AMR.1998.926629>).
- Dube, J. 2023. “The Bank of Canada Is Researching a Digital Version of Cash. Here’s What That Could Mean for You,” *THE GLOBAL AND MAIL*. (<https://www.theglobeandmail.com/business/article-digital-currency-canada-cbdc/>).
- Eastlick, M. A., Lotz, S. L., and Warrington, P. 2006. “Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment,” *Journal of Business Research* (59:8), Elsevier, pp. 877–886.
- Elo, S., and Kyngäs, H. 2008. “The Qualitative Content Analysis Process,” *Journal of Advanced Nursing* (62:1), Wiley Online Library, pp. 107–115.
- Fan, M., Stallaert, J., and Whinston, A. B. 2003. “Decentralized Mechanism Design for Supply Chain Organizations Using an Auction Market,” *Information Systems Research* (14:1), INFORMS, pp. 1–22.
- Fares, A., and Hassanein, K. 2019. “What Drives Decentralized Cryptocurrencies Users’ Continuance Intention? The Case of Bitcoin,” in *PROCEEDINGS OF Pre-ICIS SIGBPS 2019 Workshop on Blockchain and Smart Contract*, Munchen, Germany.
- Featherman, M. S., and Pavlou, P. A. 2003. “Predicting E-Services Adoption: A Perceived Risk Facets Perspective,” *International Journal of Human Computer Studies*. ([https://doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/10.1016/S1071-5819(03)00111-3)).
- Ferguson, C. J. 2016. *An Effect Size Primer: A Guide for Clinicians and Researchers.*, American Psychological Association.
- Fiedler, K. D., Grover, V., and Teng, J. T. C. 1996. “An Empirically Derived Taxonomy of Information Technology Structure and Its Relationship to Organizational Structure,” *Journal of Management Information Systems* (13:1), Taylor & Francis, pp. 9–34.
- Fishbein, M., and Ajzen, I. 1977. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*.
- Fornell, C., and Larcker, D. F. 1981. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” *Journal of Marketing Research* (18:1), Sage Publications Sage CA: Los Angeles, CA, pp. 39–50.
- Gal, U., Jensen, T. B., and Stein, M.-K. 2020. “Breaking the Vicious Cycle of Algorithmic

Management: A Virtue Ethics Approach to People Analytics,” *Information and Organization* (30:2), Elsevier, p. 100301.

Galiere, S. 2020. “When Food-delivery Platform Workers Consent to Algorithmic Management: A Foucauldian Perspective,” *New Technology, Work and Employment* (35:3), Wiley Online Library, pp. 357–370.

Gefen, D. 2000. “E-Commerce: The Role of Familiarity and Trust,” *Omega* (28:6), pp. 725–737. ([https://doi.org/10.1016/S0305-0483\(00\)00021-9](https://doi.org/10.1016/S0305-0483(00)00021-9)).

Gefen, D., and Straub, D. 2005. “A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example,” *Communications of the Association for Information Systems* (16:1), p. 5.

Gefen, D., Straub, D. W., and Boudreau, M.-C. 2000. “Structural Equation Modeling and Regression : Guidelines for Research Practice,” *Communications of the Association for Information Systems*. (<https://doi.org/10.1.1.25.781>).

Gefen, Karahanna, and Straub. 2003. “Trust and TAM in Online Shopping: An Integrated Model,” *MIS Quarterly*. (<https://doi.org/10.2307/30036519>).

Goldkuhl, G. 2004. “Design Theories in Information Systems-a Need for Multi-Grounding,” *Journal of Information Technology Theory and Application (JITTA)* (6:2), p. 7.

Grabner-Kräuter, S., and Kaluscha, E. 2003. “Empirical Research in On-Line Trust: A Review and Critical Assessment,” *International Journal of Human-Computer Studies*. ([https://doi.org/10.1016/S1071-5819\(03\)00043-0](https://doi.org/10.1016/S1071-5819(03)00043-0)).

Gregor, S. 2006. “The Nature of Theory in Information Systems,” *MIS Quarterly*, JSTOR, pp. 611–642.

Gregor, S., and Jones, D. 2007. *The Anatomy of a Design Theory*, Association for Information Systems.

Hair, J. F., Anderson, R. E., Babin, B. J., and Black, W. C. 2010. *Multivariate Data Analysis: A Global Perspective (Vol. 7)*, Upper Saddle River, NJ: Pearson.

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. “PLS-SEM: Indeed a Silver Bullet,” *Journal of Marketing Theory and Practice* (19:2), Taylor & Francis, pp. 139–152.

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2013. “Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance,” *Long Range Planning* (46:1–2), pp. 1–12.

Hair, Joe F, Hair, Joseph F, Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2021. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Sage publications.

Han, W., Ada, S., Sharman, R., and Rao, H. R. 2015. “Campus Emergency Notification Systems:

An Examination of Factors Affecting Compliance with Alerts,” *Mis Quarterly* (39:4), Society for Information Management and The Management Information Systems ..., pp. 909–930.

Hassanein, K., and Head, M. 2007. “Manipulating Perceived Social Presence through the Web Interface and Its Impact on Attitude towards Online Shopping,” *International Journal of Human-Computer Studies* (65:8), Elsevier, pp. 689–708.

Haynes, S. N., Richard, D., and Kubany, E. S. 1995. “Content Validity in Psychological Assessment: A Functional Approach to Concepts and Methods.,” *Psychological Assessment* (7:3), American Psychological Association, p. 238.

Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. “A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling,” *Journal of the Academy of Marketing Science* (43), Springer, pp. 115–135.

Henseler, J., and Sarstedt, M. 2013. “Goodness-of-Fit Indices for Partial Least Squares Path Modeling,” *Computational Statistics* (28), Springer, pp. 565–580.

Hevner, A., and Chatterjee, S. 2010. *Design Research in Information Systems: Theory and Practice*, (Vol. 22), Springer Science & Business Media.

Hinkin, T. R., and Tracey, J. B. 1999. “An Analysis of Variance Approach to Content Validation,” *Organizational Research Methods* (2:2), Sage Publications Sage CA: Thousand Oaks, CA, pp. 175–186.

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., and Dhillon, G. 2014. “A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research,” *Information Systems Research*. (<https://doi.org/10.1287/isre.2013.0501>).

Howard, M. C. 2016. “A Review of Exploratory Factor Analysis Decisions and Overview of Current Practices: What We Are Doing and How Can We Improve?,” *International Journal of Human-Computer Interaction* (32:1), Taylor & Francis, pp. 51–62.

Jabagi, N., Croteau, A.-M., Audebrand, L. K., and Marsan, J. 2021. *Who’s the Boss? Measuring Gig-Workers’ Perceived Algorithmic Autonomy-Support*.

Jensen, M., and Meckling, W. 1992. “Knowledge, Control and Organizational Structure: Parts I and II,” *Contract Economics*, Basil Blackwell, Cambridge, MA, pp. 251–274.

Kanawattanachai, P., and Yoo, Y. 2007. “The Impact of Knowledge Coordination on Virtual Team Performance over Time,” *MIS Quarterly: Management Information Systems* (31:4). (<https://doi.org/10.2307/25148820>).

Kannadhasan, M., Aramvalathan, S., Mitra, S. K., and Goyal, V. 2016. “Relationship between Biopsychosocial Factors and Financial Risk Tolerance: An Empirical Study,” *Vikalpa* (41:2), SAGE Publications Sage India: New Delhi, India, pp. 117–131.

- Kellogg, K. C., Valentine, M. A., and Christin, A. 2020. “Algorithms at Work: The New Contested Terrain of Control,” *Academy of Management Annals* (14:1), Briarcliff Manor, NY, pp. 366–410.
- Kim, D. 2005. “Cognition-Based Versus Affect-Based Trust Determinants in E-Commerce: Cross-Cultural Comparison Study,” *ICIS 2005 Proceedings*, p. 59.
- Kim, D. J., Ferrin, D. L., and Rao, H. R. 2008. “A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents,” *Decision Support Systems*. (<https://doi.org/10.1016/j.dss.2007.07.001>).
- King, R. 2020. “The Central Bank Digital Currency Survey 2020 – Debunking Some Myths.” (<https://www.centralbanking.com/fintech/cbdc/7540951/the-central-bank-digital-currency-survey-2020-debunking-some-myths>).
- Komiak, S. X., and Benbasat, I. 2004. “Understanding Customer Trust in Agent-Mediated Electronic Commerce, Web-Mediated Electronic Commerce, and Traditional Commerce,” *Information Technology and Management* (5:1–2), Springer, pp. 181–207.
- Komiak, S. Y. X., and Benbasat, I. 2006. “The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents,” *MIS Quarterly: Management Information Systems* (30:4). (<https://doi.org/10.2307/25148760>).
- Kosse, A., and Mattei, I. 2023. “Making Headway-Results of the 2022 BIS Survey on Central Bank Digital Currencies and Crypto,” *BIS Papers*, Bank for International Settlements.
- Krippendorff, K. 2018. *Content Analysis: An Introduction to Its Methodology*, Sage publications.
- Landis, J. R., and Koch, G. G. 1977. “The Measurement of Observer Agreement for Categorical Data,” *Biometrics*, JSTOR, pp. 159–174.
- Lankton, N. K., and McKnight, D. H. 2011. “What Does It Mean to Trust Facebook?,” *ACM SIGMIS Database*. (<https://doi.org/10.1145/1989098.1989101>).
- Lankton, N., McKnight, D. H., and Thatcher, J. B. 2014. “Incorporating Trust-in-Technology into Expectation Disconfirmation Theory,” *Journal of Strategic Information Systems*. (<https://doi.org/10.1016/j.jsis.2013.09.001>).
- Laroche, M., Habibi, M. R., Richard, M.-O., and Sankaranarayanan, R. 2012. “The Effects of Social Media Based Brand Communities on Brand Community Markers, Value Creation Practices, Brand Trust and Brand Loyalty,” *Computers in Human Behavior* (28:5), Elsevier, pp. 1755–1767.
- Larzelere, R. E., and Huston, T. L. 1980. “The Dyadic Trust Scale: Toward Understanding Interpersonal Trust in Close Relationships,” *Journal of Marriage and the Family*, JSTOR, pp. 595–604.
- Lee, M. K. O., and Turban, E. 2001. “A Trust Model for Consumer Internet Shopping,”

International Journal of Electronic Commerce (6:1), Taylor & Francis, pp. 75–91.

- Lindell, M. K., and Whitney, D. J. 2001. “Accounting for Common Method Variance in Cross-Sectional Research Designs,” *Journal of Applied Psychology* (86:1), American Psychological Association, p. 114.
- Lundy, L. 2016. “Blockchain and the Sharing Economy 2.0: The Real Potential of Blockchain for Developers,” *Last Accessed <https://www.ibm.com/developerworks/library/lot-blockchain-sharingeconomy/index.html>*.
- Luo, X., Li, H., Zhang, J., and Shim, J. P. 2010. “Examining Multi-Dimensional Trust and Multi-Faceted Risk in Initial Acceptance of Emerging Technologies: An Empirical Study of Mobile Banking Services,” *Decision Support Systems*. (<https://doi.org/10.1016/j.dss.2010.02.008>).
- Lustig, C., and Nardi, B. 2015. “Algorithmic Authority: The Case of Bitcoin,” *Proceedings of the Annual Hawaii International Conference on System Sciences* (2015-March), pp. 743–752. (<https://doi.org/10.1109/HICSS.2015.95>).
- MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. “Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques,” *MIS Quarterly* (35:2), Society for Information Management and The Management Information Systems ..., pp. 293–334.
- Marriott, H. R., and Williams, M. D. 2018. “Exploring Consumers Perceived Risk and Trust for Mobile Shopping: A Theoretical Framework and Empirical Study,” *Journal of Retailing and Consumer Services*. (<https://doi.org/10.1016/j.jretconser.2018.01.017>).
- Maurer, B., Nelms, T. C., and Swartz, L. 2013. “‘When Perhaps the Real Problem Is Money Itself’: The Practical Materiality of Bitcoin,” *Social Semiotics* (23:2), pp. 261–277. (<https://doi.org/10.1080/10350330.2013.777594>).
- Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. “An Integrative Model of Organizational Trust,” *Academy of Management Review* (20:3), Academy of Management Briarcliff Manor, NY 10510, pp. 709–734.
- McKnight, H., Choudhury, V., and Kacmar, C. 2002a. “The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model,” *Elsevier* (11:3–4), pp. 297–323. (<https://www.sciencedirect.com/science/article/pii/S0963868702000203>).
- McKnight, H., Choudhury, V., and Kacmar, C. 2002b. “Developing and Validating Trust Measures for E-Commerce: An Integrative Typology,” *Information Systems Research*. (<https://doi.org/10.1287/isre.13.3.334.81>).
- McKnight, H., Cummings, L. L., and Chervany, N. L. 1998. “Initial Trust Formation in New Organizational Relationships,” *Academy of Management Review*. (<https://doi.org/10.5465/AMR.1998.926622>).

- McMillan, D. W., and Chavis, D. M. 1986. "Sense of Community: A Definition and Theory," *Journal of Community Psychology* (14:1), Wiley Online Library, pp. 6–23.
- Mendoza-Tello, J. C., Mora, H., Pujol-López, F. A., and Lytras, M. D. 2018. "Social Commerce as a Driver to Enhance Trust and Intention to Use Cryptocurrencies for Electronic Payments," *IEEE Access*. (<https://doi.org/10.1109/ACCESS.2018.2869359>).
- Meyers, L. S., Gamst, G., and Guarino, A. J. 2016. *Applied Multivariate Research: Design and Interpretation*, Sage publications.
- Mirynech, D. 2019. "AUTONOMOUS VEHICLES AND BLOCKCHAIN How a Distributed Ledger System Could Fund the Next Generation of Transportation Infrastructure."
- Moghaddam, M., and Nof, S. Y. 2017. "The Collaborative Factory of the Future," *International Journal of Computer Integrated Manufacturing* (30:1), Taylor & Francis, pp. 23–43.
- Möhlmann, M., Zalmanson, L., Henfridsson, O., and Gregory, R. W. 2021. "ALGORITHMIC MANAGEMENT OF WORK ON ONLINE LABOR PLATFORMS: WHEN MATCHING MEETS CONTROL.," *MIS Quarterly* (45:4).
- Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), INFORMS, pp. 192–222.
- Moussawi, S., and Koufaris, M. 2019. *Perceived Intelligence and Perceived Anthropomorphism of Personal Intelligent Agents: Scale Development and Validation*.
- Myers, M. D. 2019. "Qualitative Research in Business and Management," *Qualitative Research in Business and Management*, SAGE publications Ltd, pp. 1–364.
- Nakamoto, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. (http://www.academia.edu/download/32413652/BitCoin_P2P_electronic_cash_system.pdf).
- Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., and Gandomi, A. H. 2021. "The Revolution of Blockchain: State-of-the-Art and Research Challenges," *Archives of Computational Methods in Engineering* (28), Springer, pp. 1497–1515.
- Nevo, B. 1985. "Face Validity Revisited," *Journal of Educational Measurement* (22:4), Wiley Online Library, pp. 287–293.
- Nof, S. Y. 2007. "Collaborative Control Theory for E-Work, e-Production, and e-Service," *Annual Reviews in Control* (31:2), Elsevier, pp. 281–292.
- Nof, S. Y. 2017. "Collaborative Control Theory and Decision Support Systems.," *Computer Science Journal of Moldova* (25:2).
- Nof, S. Y., Ceroni, J., Jeong, W., and Moghaddam, M. 2015. *Revolutionizing Collaboration through E-Work, e-Business, and e-Service*, (Vol. 2), Springer.

Nunnally, J. C. 1967. *Psychometric Theory*, McGraw Hill.

Orlikowski, W. J., and Baroudi, J. J. 1991. “Studying Information Technology in Organizations: Research Approaches and Assumptions,” *Information Systems Research* (2:1), INFORMS, pp. 1–28.

Ostern, N. 2018. “Do You Trust a Trust-Free Technology? Toward a Trust Framework Model for Blockchain Technology,” in *International Conference on Information Systems 2018, ICIS 2018*.

Paravastu, N., Gefen, D., and Creason, S. 2014. “Understanding Trust in IT Artifacts- An Evaluation of the Impact of Trustworthiness and Trust on Satisfaction with Antiviral Software,” *Advances in Information Systems*. (<https://doi.org/10.1007/BF01089753>).

Pavlou, P. A. 2002. “Institution-Based Trust in Interorganizational Exchange Relationships: The Role of Online B2B Marketplaces on Trust Formation,” *Journal of Strategic Information Systems* (11:3–4). ([https://doi.org/10.1016/S0963-8687\(02\)00017-3](https://doi.org/10.1016/S0963-8687(02)00017-3)).

Pavlou, P. A. 2003. “Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model,” *International Journal of Electronic Commerce* (7:3). (<https://doi.org/10.1080/10864415.2003.11044275>).

Payne, K. C., J Keith, M., Babb, J., and N Spruill, A. 2018. *Development and Validation of the Information Systems Creative-Self-Efficacy Scale*.

Peterson, N. A., Speer, P. W., and McMillan, D. W. 2008. “Validation of a Brief Sense of Community Scale: Confirmation of the Principal Theory of Sense of Community,” *Journal of Community Psychology* (36:1), Wiley Online Library, pp. 61–73.

Peterson, R. A. 1994. “A Meta-Analysis of Cronbach’s Coefficient Alpha,” *Journal of Consumer Research* (21:2), The University of Chicago Press, pp. 381–391.

Petter, Straub, and Rai. 2007. “Specifying Formative Constructs in Information Systems Research,” *MIS Quarterly*. (<https://doi.org/10.2307/25148814>).

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. “Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies,” *The Journal of Applied Psychology*. (<https://doi.org/10.1037/0021-9010.88.5.879>).

Pureswaran, V., and Brody, P. 2015. “Device Democracy: Saving the Future of the Internet of Things,” *IBM Corporation*.

Rempel, J. K., Holmes, J. G., and Zanna, M. P. 1985. “Trust in Close Relationships,” *Journal of Personality and Social Psychology* (49:1). (<https://doi.org/10.1037/0022-3514.49.1.95>).

Ridings, C. M., Gefen, D., and Arinze, B. 2002. “Some Antecedents and Effects of Trust in Virtual Communities,” *The Journal of Strategic Information Systems* (11:3–4), Elsevier, pp.

271–295.

- Riedl, R., Hubert, M., and Kenning, P. 2010. “Are There Neural Gender Differences in Online Trust? An fMRI Study on the Perceived Trustworthiness of eBay Offers,” *MIS Quarterly* (34:2), Society for Information Management and The Management Information Systems ..., pp. 397–428.
- Van Riel, A. C. R., Henseler, J., Kemény, I., and Sasovova, Z. 2017. “Estimating Hierarchical Constructs Using Consistent Partial Least Squares: The Case of Second-Order Composites of Common Factors,” *Industrial Management & Data Systems* (117:3), Emerald Publishing Limited, pp. 459–477.
- Ringle, C. M., Sarstedt, M., and Straub, D. W. 2012. “A Critical Look at the Use of PLS-SEM in MIS Quarterly. MIS Q. Manag.,” *Inf. Syst* (36:1).
- Roldán, J. L., and Sánchez-Franco, M. J. 2012. “Variance-Based Structural Equation Modeling: Guidelines for Using Partial Least Squares in Information Systems Research,” in *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems*, IGI global, pp. 193–221.
- Rosnow, R. L., and Rosenthal, R. 2003. “Effect Sizes for Experimenting Psychologists.,” *Canadian Journal of Experimental Psychology/Revue Canadienne de Psychologie Expérimentale* (57:3), Canadian Psychological Association, p. 221.
- Rotter, J. B. 1967. “A New Scale for the Measurement of Interpersonal Trust,” *Journal of Personality* (35:4). (<https://doi.org/10.1111/j.1467-6494.1967.tb01454.x>).
- Rotter, J. B. 1971. “Generalized Expectancies for Interpersonal Trust.,” *American Psychologist* (26:5), American Psychological Association, p. 443.
- Salisbury, W. D., Chin, W. W., Gopal, A., and Newsted, P. R. 2002. “Better Theory through Measurement—Developing a Scale to Capture Consensus on Appropriation,” *Information Systems Research* (13:1), INFORMS, pp. 91–103.
- Sas, C., and Khairuddin, I. 2017. “Design for Trust an Exploration of the Challenges and Opportunities of Bitcoin Users,” *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 6499–6510. (<https://doi.org/10.1145/3025453.3025886>).
- Sas, C., and Khairuddin, I. E. 2015. “Exploring Trust in Bitcoin Technology,” *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction on - OzCHI '15* (October), pp. 338–342. (<https://doi.org/10.1145/2838739.2838821>).
- Schlosser, A. E., White, T. B., and Lloyd, S. M. 2006. “Converting Web Site Visitors into Buyers: How Web Site Investment Increases Consumer Trusting Beliefs and Online Purchase Intentions,” *Journal of Marketing* (70:2), SAGE Publications Sage CA: Los Angeles, CA, pp. 133–148.
- Schoorman, F. D., Mayer, R. C., and Davis, J. H. 2007. “An Integrative Model of Organizational

- Trust: Past, Present, and Future,” *Academy of Management Review*.
(<https://doi.org/10.5465/AMR.2007.24348410>).
- Scott, B., Loonam, J., and Kumar, V. 2017. “Exploring the Rise of Blockchain Technology: Towards Distributed Collaborative Organizations,” *Strategic Change* (26:5), Wiley Online Library, pp. 423–428.
- Seok, H., Nof, S. Y., and Filip, F. G. 2012. “Sustainability Decision Support System Based on Collaborative Control Theory,” *Annual Reviews in Control* (36:1), Elsevier, pp. 85–100.
- Shermin, V. 2017. “Disrupting Governance with Blockchains and Smart Contracts,” *Strategic Change* (26:5), Wiley Online Library, pp. 499–509.
- Simmering, M. J., Fuller, C. M., Richardson, H. A., Ocal, Y., and Atinc, G. M. 2015. “Marker Variable Choice, Reporting, and Interpretation in the Detection of Common Method Variance: A Review and Demonstration,” *Organizational Research Methods* (18:3), Sage Publications Sage CA: Los Angeles, CA, pp. 473–511.
- Simser, J. 2015. “Bitcoin and Modern Alchemy: In Code We Trust,” *Journal of Financial Crime*. (<https://doi.org/10.1108/JFC-11-2013-0067>).
- Söllner, M., Gefen, D., Leimeister, J. M., and Pavlou, P. A. 2016. “Trust: An MIS Quarterly Research Curation,” *MIS Quarterly* (October), pp. 1–9.
(https://static1.squarespace.com/static/5887a660b3db2b05bd09cf36/t/5956582c9f745673dae7df53/1498830893024/trust-research-curation_oct-31-20161.pdf).
- Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A., and Leimeister, J. M. 2012. “Understanding The Formation of Trust in IT Artifacts,” in *Thirty Third International Conference on Information Systems, Orlando*.
- Spector, P. E. 1992. *Summated Rating Scale Construction: An Introduction*, (Vol. 82), Sage.
- Srivastava, S. C., and Chandra, S. 2018. “Social Presence in Virtual World Collaboration: An Uncertainty Reduction Perspective Using a Mixed Methods Approach,” *MIS Quarterly* (42:3), Society for Information Management and The Management Information Systems ..., pp. 779–804.
- Stemler, S. 2000. “An Overview of Content Analysis,” *Practical Assessment, Research, and Evaluation* (7:1), p. 17.
- Stephanidis, C., Salvendy, G., Antona, M., Chen, J. Y. C., Dong, J., Duffy, V. G., Fang, X., Fidopiastis, C., Fragomeni, G., and Fu, L. P. 2019. “Seven HCI Grand Challenges,” *International Journal of Human–Computer Interaction* (35:14), Taylor & Francis, pp. 1229–1269.
- Straub, D., Boudreau, M.-C., and Gefen, D. 2004. “Validation Guidelines for IS Positivist Research,” *Communications of the Association for Information Systems* (13:1), p. 24.

- Tapscott, D. 2017. *A Declaration of Interdependence Towards*.
- Tapscott, D., and Tapscott, A. 2016. *Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World*, Penguin.
- Tapscott, D., and Vinod, A. 2019. "DISTRIBUTED ARTIFICIAL INTELLIGENCE Blockchain as an Operating Platform for AI."
- Tsiakis, T., and Sthephanides, G. 2005. "The Concept of Security and Trust in Electronic Payments," *Computers and Security*. (<https://doi.org/10.1016/j.cose.2004.11.001>).
- Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly*, JSTOR, pp. 21–54.
- Walch, A. 2019. "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems," *Crypto Assets: Legal and Monetary Perspectives (OUP, Forthcoming 2019)*.
- Walls, J. G., Widmeyer, G. R., and El Sawy, O. A. 2004. "Assessing Information System Design Theory in Perspective: How Useful Was Our 1992 Initial Rendition?," *Journal of Information Technology Theory and Application (JITTA)* (6:2), p. 6.
- Walls, J. G., Widmeyer, G. R., and El Sawy, O. A. 1992. "Building an Information System Design Theory for Vigilant EIS," *Information Systems Research* (3:1), INFORMS, pp. 36–59.
- Walsham, G. 1997. "Actor-Network Theory and IS Research: Current Status and Future Prospects," in *Information Systems and Qualitative Research: Proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research, 31st May–3rd June 1997, Philadelphia, Pennsylvania, USA*, Springer, pp. 466–480.
- Walton, A., and Johnston, K. 2018. "Exploring Perceptions of Bitcoin Adoption: The South African Virtual Community Perspective," *Interdisciplinary Journal of Information, Knowledge, and Management*. (<https://doi.org/10.28945/4080>).
- Werbach, K. 2018. "Trust, but Verify: Why the Blockchain Needs the Law," *Berkeley Technology Law Journal* (33:2). (<https://doi.org/10.2139/ssrn.2844409>).
- Williams, L. J., Hartman, N., and Cavazotte, F. 2010. "Method Variance and Marker Variables: A Review and Comprehensive CFA Marker Technique," *Organizational Research Methods* (13:3), Sage Publications Sage CA: Los Angeles, CA, pp. 477–514.
- Wladawsky-Berger, I. 2017. "Building a Framework for Blockchain Adoption: What CEOs Should Know," *Blockchain Research Institute (BRI)*.
- Wood, A. J. 2021. "Algorithmic Management Consequences for Work Organisation and Working Conditions," JRC Working Papers Series on Labour, Education and Technology.

- Xin, H., Techatassanasoontorn, A. A., and Tan, F. B. 2013. “Exploring the Influence of Trust on Mobile Payment Adoption,” *PACIS 2013 Proceedings*.
- Yao, G., Wu, C., and Yang, C. 2008. “Examining the Content Validity of the WHOQOL-BREF from Respondents’ Perspective by Quantitative Methods,” *Social Indicators Research* (85), Springer, pp. 483–498.
- Ye, H. J., and Kankanhalli, A. 2018. “User Service Innovation on Mobile Phone Platforms: Investigating Impacts of Lead Userness, Toolkit Support, and Design Autonomy,” *MIS Quarterly* (42:1), Society for Information Management and The Management Information Systems ..., pp. 165–188.
- Zaheer, A., McEvily, B., and Perrone, V. 1998. “Does Trust Matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance,” *Organization Science* (9:2). (<https://doi.org/10.1287/orsc.9.2.141>).
- Zarifis, A., Efthymiou, L., Cheng, X., and Demetriou, S. 2014. “Consumer Trust in Digital Currency Enabled Transactions,” *Lecture Notes in Business Information Processing*. (https://doi.org/10.1007/978-3-319-11460-6_21).
- Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. 2017. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*. (<https://doi.org/10.1109/BigDataCongress.2017.85>).
- Zilberstein, S. 2015. “Building Strong Semi-Autonomous Systems,” in *Twenty-Ninth AAAI Conference on Artificial Intelligence*.
- Zucker, L. G. 1986. “Production of Trust: Institutional Sources of Economic Structure, 1840-1920,” *Research in Organizational Behavior* (8), pp. 53–111.

Appendix A. Early Scale Development Attempts in the IS Literature

Table 35. Summary of Some Early IS Scale Development Research and Guidelines

<u>Phases</u>	(Davis 1989) (MISQ)	(Moore and Benbasat 1991) (ISR)	(Chin et al. 1997; Salisbury et al. 2002) (ISR)*	(MacKenzie et al. 2011) (MISQ: Guidelines)
<u>Conceptual definition</u>	<p>Construct(s): <i>Easy of use and usefulness</i></p> <p>Source: Literature Review</p>	<p>Construct(s): <i>Users' perceptions of adopting an information technology innovation.</i></p> <p>Source: Literature Review</p>	<p>Construct(s): <i>Faithfulness of Appropriation (FOA) & Consensus on Appropriation (COA)</i></p> <p>Source: Literature Review</p>	<p>Guidelines: Literature review and interviews with professional and IS scholars.</p>
<u>Items generation</u>	<p>Based on the literature review, fourteen items were generated for each construct.</p>	<p>Existing instruments were identified in the literature, and at least ten items were generated for each of the seven dimensions specified in the literature. A list of 94 items was developed for the seven characteristics.</p>	<p>The self-developed items list was based on the previous literature review.</p> <p>FOA: 11 items. COA: 10 items.</p>	<p>Guidelines: Initial items should be generated based on the previous literature review and interviews.</p>
<u>Initial Raters (pre-test)</u>	<p>Initial pre-test interviews were conducted, and the proposed fourteen items were reduced to ten items for each construct.</p> <p>Fifteen users with good computer backgrounds, staff, and secretaries were used to group similar items together.</p> <p>Items and definitions were presented to the raters. The first</p>	<p>A group of four judges (i.e., professor, graduate student, administrative clerk, and secretaries) were used for four rounds. In each round, items with definitions in the first task were presented, and items without definitions in the second task were given.</p> <p>The initial 94 items were reduced to 75 items.</p>	<p>FOA: Three experienced personnel were invited to assess the content validities of the initial 11 items.</p> <p>COA: This step was not completed.</p>	<p>Guidelines: It is essential to have raters representing the instrument's intended population.</p> <p>Then, items with the definitions can be tested through another one-way repeated ANOVA test to ensure their initial content validity.</p>

	task was prioritization with the given definition, and the second task was categorization.			
<u>Pre-test and scale purification</u>	N/A	<p>Twenty users and non-users were used to test the initial reliability test. Respondents were allowed to comment on the items in terms of their length, wording, and instructions. Here, the authors reduced the total number of items from 75 to 43 items.</p> <p>In addition, they then ran a second study of 66 users and non-users similar to the target population.</p>	This step was not completed for either FOA or COA.	
<u>Data collection (Wave I)</u>	<p>Study 1 (112 IBM users in two different systems email and file editor).</p> <p>The two scales were refined to 6 items per construct.</p>	<p>Here, the authors collected data from 540 respondents and split them into two samples, 270 each. After running the factor analysis, the items were reduced to 25 items in eight dimensions.</p>	<p>Two consecutive exploratory studies were used for FOA (Study 1: sample size 114 and Study 2: sample size 284). Three factors were developed in the first study and then were reduced to two factors in the second study.</p> <p>One exploratory study was used for COA (Study 1 sample size 236). Two factors were</p>	<p>Guidelines:</p> <p>The recommendation for EFA sample size is from 100 – 500, and the recommendation for the item-sample ratio is 3:1 – 10-1.</p> <p>There might be some variability based on the level of commonality of the construct and determinations of the factor such that a small sample (60-100) is sufficient with a high level of commonality and substantial factors' determination. In contrast, a large sample is necessary with a low commonality</p>

			developed at this stage for COA.	level and weak underlying factors' determination. Other variables must be measured at this stage to evaluate the convergent, nomological, and discriminant validities.
<u>Confirmation / Cross-validation (Wave 2)</u>	Study 2 (40 MBA students in an experimental study where two IBM systems were tested, one for chart master and one for Pen Drawing.	It can be assumed that was done on the previous data collection as the first half of the dataset was used for an exploratory factor analysis while the second part was used for confirmatory factor analysis. In addition, the authors found significant differences between the user group (size 418) and non-user group (size 122)	Two other studies (Study 1: Sample size 90 and Study 2: Sample size 228) were used as a confirmatory analysis for FOA. One confirmatory study of 298 participants was conducted for COA. In this phase, FOA and COA had a final list of five items loaded in one factor.	Guidelines: The recommendation for CFA sample size is from 100 – 500, and the recommendation for the item-sample ratio is 3:1 – 10-1. Other variables must be measured at this stage to evaluate the convergent, nomological, and discriminant validities.

*: These two papers were combined in the analysis as they are about the same concept of appropriation but from two different angles (i.e., faithfulness and consensus on appropriation), are developed by the same researchers, and use the same steps for the scale development process.

Appendix A.1 Davis's Approach, MISQ 1989:

1. Davis reviewed published research and came up with the initial definition for ease of use and usefulness.
2. Fourteen items were then generated for each construct.
3. He then interviewed fifteen participants (i.e., five graduate professional computer users, five professional staff, and five secretaries). Both the definition of each construct and the measurement items were given to the participants, and the task was to *prioritize* the items and then *cluster* similar items in groups (i.e., between 3 and 5 items per

group). From the initial 14 items developed for each construct, the author had ten items for each construct in this phase.

4. The pre-test phase included two studies. The first study included 120 IBM users testing two systems. The analysis was done using the multi-traits multimethod analysis (i.e., a correlation analysis to check the discriminant and the convergent validity) and principal component analysis. This step resulted in 6 items for each construct. The second study was an experimental study for 40 MBA students, where he tested two hypothetical systems for prospective users with an emphasis on ease of use and usefulness.

What is unique about this approach is that the study used users in the initial items test and the following two examinations to represent the intended population where the new measurements were supposed to be generalized. However, the approach was criticized in the early phase as presenting both the definitions and items to the participants and asking them to do the rating task made the study exposed to the “*Interpretational Confounding*” issue where the theoretical meaning of the construct differs from the measurement items (Burt 1976; MacKenzie et al. 2011; Moore and Benbasat 1991). In addition, asking the participants to group the items implies the enforcement of an implicit logic on the participants, as this has to be justified based on the construct's dimensionality identification.

Appendix A.2 Moore and Benbasat’s Approach, ISR 1991:

1. A literature review was conducted about the perceived characteristics of technological innovation. Seven different dimensions were identified from the literature, named voluntariness, image, relative advantage, compatibility, easy of use, observability, and trial-ability.

2. Initial items were generated based on the literature review. Then, the authors added items to any dimension with less than ten items. A total list of 94 items was developed during this phase.
3. Like Davis's 1989 approach, they asked an initial set of judges to rank these items against each dimension's definition in the first round. They then extended Davis's work by testing the sorting of these items into groups by judges without giving them the definition of each construct. The purpose was to control the "interpretational confounding" issue that might reduce the new construct's validities. This step was done in four rounds. Each round included four judges, a secretary, an administrative clerk, a student, and a professor. The initial 94 items were reduced to 75 after these four rounds.
4. In the pre-test phase, the authors purified the items through an initial pilot of 20 users and non-users and a subsequent sample of 66 users and non-users. Participants were also asked to express any issue with the items (e.g., wording and instructions). The 75 items were reduced to 43 items after this phase.
5. Only one wave of data collection was conducted where a sample of 540 respondents was used (i.e., 418 users and 122 non-users). The sample was randomly split into two halves of 270 each, where the first half was used for exploratory analysis, and the second half was used to run a confirmatory factor analysis. The new measures exhibited significantly different levels for the users than non-users.

Like the first approach, this approach is rigorous in considering users and non-users and the use of factor analysis to validate the new measurements. However, this approach might have also been exposed to the same "interpretational confounding" as an inherited issue because the initial dimensions were based on what has been published in the literature, and the subsequent rounds

did not reflect on the nature of these sub-dimensions and how they are related to the focal construct. As such, there was not enough discussion about the dimensionality issue (i.e., formative vs. reflective) and how it might affect the relationship between these dimensions. In addition, some dimensions had only two items, while the recommended number has to be at least three items for each dimension (Hair et al. 2010). Finally, only the measurement model was considered in the analysis without testing the structure model in a nomological network of other related measurements.

Appendix A.3 Chin et al. Approach, ISR 1997 / Salisbury et al. Approach, ISR 2002:

1. A literature review was conducted to capture the definition of the variables “Faithfulness of Appropriation (FOA)” in Chin et al. (1997) and “Consensus on Appropriation (COA)” in Salisbury et al. 2002.
2. Initial eleven items were generated for FOA, and ten items were developed for COA.
3. Three experienced personnel were used to assess the content validity of the new eleven items for FOA, whereas no raters have been used for COA.
4. In two consecutive experiments (Study 1: sample size 114 and Study 2: sample size 284), the 11 items were explored and reworded for clarification in FOA. Three factors were identified in Study 1, whereas two factors were generated in Study 2. In contrast, only one study was used in the COA exploratory phase, consisting of 236 participants.
5. In another two studies (Testing: Sample size 90 and Confirmation: Sample size 228), a final list of five items was captured in the confirmatory Structural Equation Modeling (SEM) for FOA, and all the different types of validities (i.e., discriminant, convergent, and nomological) were tested. In comparison, one confirmatory study of 298 participants was

used for COA. In this phase, FOA and COA had a final list of five items loaded in one factor.

Unlike the previous two approaches, the authors in this approach utilize the SEM technique in the confirmatory phase of the analysis and systematically evaluate the three different validities (i.e., discriminant, convergent, and nomological). However, this approach can be criticized for starting with three factors in the first experiment, then being reduced to two factors, and finally, the study ending up with only one factor in the confirmatory phase without considering the dimensionality issue. In addition, all the participants were students, which might have threatened the scale's validity when tested with actual users.

Based on the above discussion, the IS literature lacks a systematic approach to the scale development process and clearly explains the rationale for each step. Most importantly, there was a need for some guidelines and recommendations about carrying out each step and remedies for some potential issues. This need was addressed in Mackenzie et al. (2011) approach.

Appendix B. Participants’ quotes on the newly developed definitions of the constructs (Step 3: Scale Validation in the Scale Development Process)

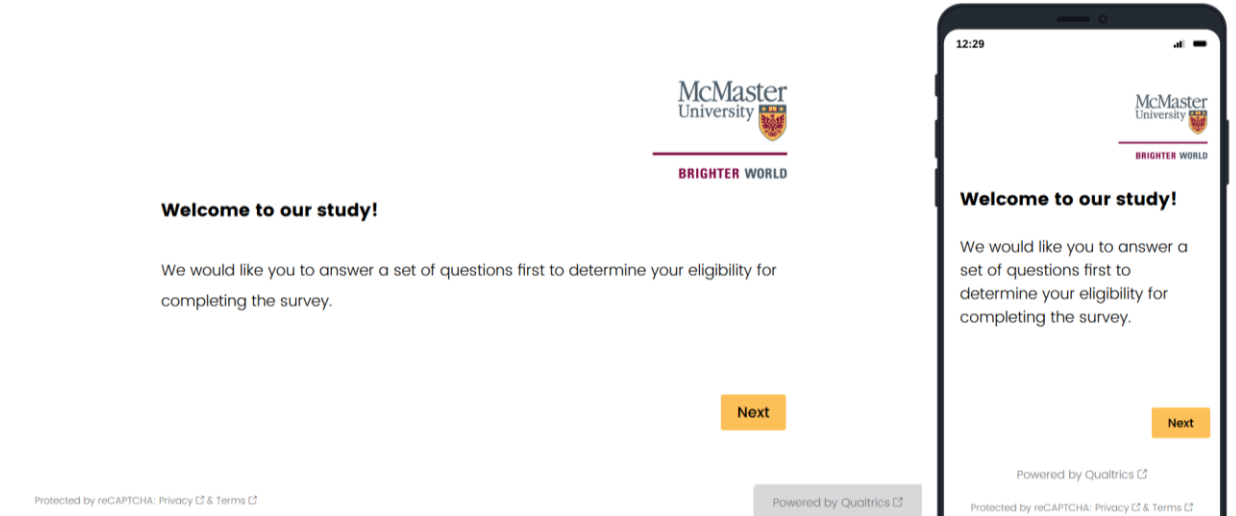
Table 36: Participants' Quotes on the New Definitions

Construct Definition	Initial Measurement Items
<p>Decentralization is the extent to which an information system is collaboratively managed and accessible by entities (e.g., humans or algorithms) where all participating entities share inputs (e.g., computing resources, data/information) and affect the system’s outputs with no single entity playing a dominant role in the operation of the system.</p>	<ul style="list-style-type: none"> • It's more like the transfer of control, Participant 5. • Because if there is no consensus, then someone should have the authority to override everyone and decide. For instance, if there is a malfunction, then you may need to override the protocols. However, this authority must be used in emergency situations where it is justifiable without question, Participant 9. • Decentralization means distributing roles of authorities to avoid anyone having a dominant role, Participant 28. • A decentralized system is a distributed system whereby the inputs may come from various sources (human interaction or through automation from a set of processors), and the processing is done elsewhere. Nowhere in the definition does it say anything about the information assessment to assess how relationships and outcomes are generated, Participant 46. • There may be a high likelihood that a particular group of individual entities as a collective dominate or have a major influence on outcomes in some systems, even if all parties contribute to inputs, Participant 48. • Computing resources are not located in one space (server, data center, or vendor) but spread across several places to minimize risk, Participant 49. • Lack of definition of accurate decentralization approach, Participant 59. • I think there could also be a physical location component where the system is managed from different locations, Participant 83. • I think the first part of the definition, specifically with "accessible by entities," is a bit doubtful. Still, the second part, where the effects of decentralization are discussed, makes sense, Participant 99.

	<ul style="list-style-type: none"> • <i>The definition does not include the transfer of control or power from dominant players to the less dominant players. (Participant 110)</i> • <i>When I think of "collaboratively," I believe that all parties are communicating with each other, but that might not be the case in this context. Each party might be managing their own piece within a silo, Participant 117.</i>
<ul style="list-style-type: none"> • Algorithmic Authority is the legitimate independent level of control an algorithm has to take and enforce certain actions based on its logic. 	<ul style="list-style-type: none"> • <i>In essence, algorithmic authority involves the legitimate ability of algorithms to direct human actions and impact what information is accepted as accurate, Participant 10.</i> • <i>While the definition has correct elements related to Algorithmic Authority, I believe it should also dictate human actions since Algorithmic Authority directly influences what information is available to users. Bitcoin is a familiar example of this, as users tend to trust algorithmic authority instead of conventional institutions since they believe that AA [Algorithmic Authority] enforces and "corrects" human judgment, Participant 27.</i> • <i>This [Algorithmic Authority] could have an additional reference to ethical actions, not just "certain" actions, Participant 31.</i> • <i>Given the word authority, we need information on regulation in the definition, Participant 43.</i> • <i>I'm just wondering if the level of control has to be independent. I believe an algorithm could still depend on other inputs for decision-making, so its logic might not be entirely independent, Participant 51.</i> • <i>Unsure how the actions will be utilized, Participant 60.</i> • <i>The definition makes sense, but I'm uncertain what algorithmic authority is as I've never heard the term, Participant 69.</i> • <i>If the definition has been expounded a bit longer, especially with what makes its level of control "legitimately independent," that probably would sound clearer, Participant 99.</i> • <i>It could be expanded to say, which types of activities in specific contexts are all human activities? Participant 101.</i> • <i>The power of algorithms to manage human action and influence what information is accessible to users, Participant 112.</i> • <i>Based on this logic - it would be beneficial to expressly state its programming, as it is human-made unless some of its logic is black-box or independently derived, Participant 115.</i>

Appendix C. Main Study Survey

1. Welcome Message




2. Screening Question 1



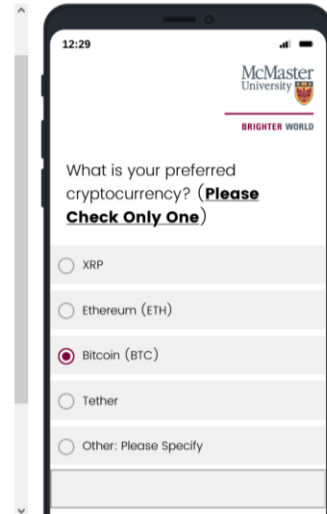
Please note that participants had to choose “Cryptocurrencies” as one of their options to be prompted to the second screening question below.

3. Screening Question 2


BRIGHTER WORLD

What is your preferred cryptocurrency? (**Please Check Only One**)

- XRP
- Ethereum (ETH)
- Bitcoin (BTC)
- Tether
- Other: Please Specify



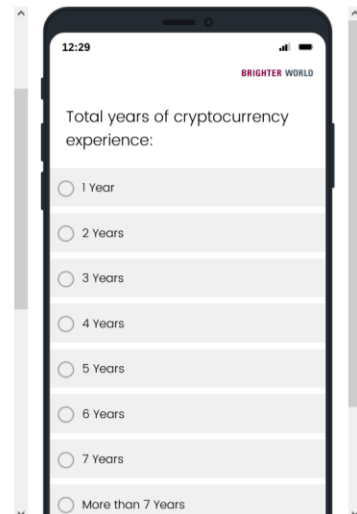
Participants have to choose “Bitcoin” to be able to participate in the study.

4. Years of Experience Question


BRIGHTER WORLD

Total years of cryptocurrency experience:

- 1 Year
- 2 Years
- 3 Years
- 4 Years
- 5 Years
- 6 Years
- 7 Years
- More than 7 Years



5. Demographic Question

I identify as (Check one):

- Man
- Woman
- Non-gender-binary, two-spirit, or others
- Prefer not to say

Next

A screenshot of the mobile version of the survey question. The text 'I identify as (Check one):' is at the top. Below it are four radio button options: 'Man' (selected), 'Woman', 'Non-gender-binary, two-spirit, or others', and 'Prefer not to say'. The mobile interface includes a status bar at the top showing the time 12:29 and the McMaster University logo with the slogan 'BRIGHTER WORLD'.

6. Age Question

I am (Check one):

- 20-30
- 31-40
- 41-50
- 51-60
- 61-70
- >70
- Prefer not to answer

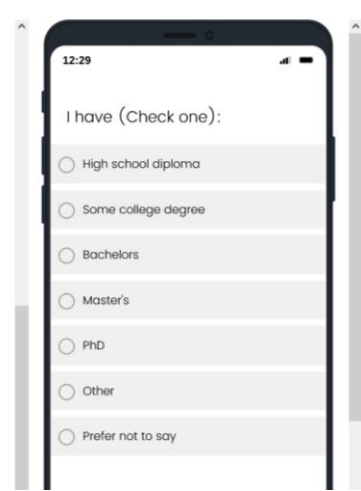


A screenshot of the mobile version of the age question. The text 'I am (Check one):' is at the top. Below it are seven radio button options: '20-30', '31-40', '41-50', '51-60', '61-70', '>70', and 'Prefer not to answer'. The mobile interface includes a status bar at the top showing the time 12:29 and the McMaster University logo with the slogan 'BRIGHTER WORLD'.


7. Education Question

I have (Check one):

- High school diploma
- Some college degree
- Bachelors
- Master's
- PhD
- Other
- Prefer not to say

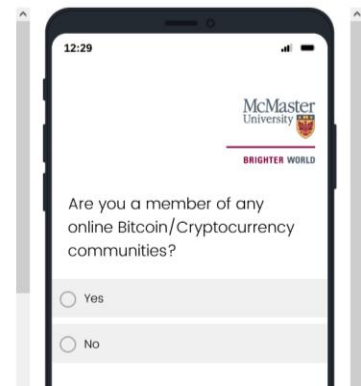


8. Online Community Membership Question


BRIGHTER WORLD

Are you a member of any online Bitcoin/Cryptocurrency communities?

- Yes
- No

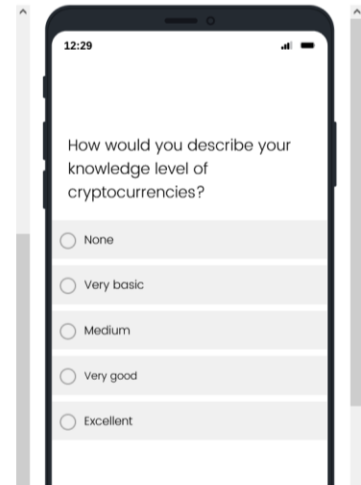


9. Self-Reported Knowledge Question

How would you describe your knowledge level of cryptocurrencies?

- None
- Very basic
- Medium
- Very good
- Excellent

Next



10. Consent Letter



BRIGHTER WORLD

Letter of Consent A Study about Using Cryptocurrencies

- This research seeks to understand Cryptocurrencies users' experience.

Potential Harms, Risks or Discomforts: We do not foresee any significant risk or discomfort from your participation in this research.

However, this study will collect data through an online survey, which is an externally hosted cloud-based service. Please note that whilst this service is approved for collecting data in this study by the McMaster Research Ethics Board, there is a small risk with any platform such as this of data that is collected on external servers falling outside the control of the research team.

Potential Benefits: This study will not benefit you directly. However, by participating in this study, you will help to provide understanding of some factors to affect trust and risks to benefit academics and professional about the nature of these cryptocurrencies systems.

Payment or Reimbursement: if you agree to participate in this study, you will be compensated according to the scheme you agreed to with Qualtrics before you entered into the survey.

Confidentiality: Every effort will be made to protect (guarantee) your confidentiality and privacy. All information you supply during the research will be held in confidence. No personally-identifying information (e.g., name, social insurance number) will be required or collected before, during, or after the study, and therefore, your name will not appear in any report or publication of the research. The data will be collected through an online survey without the need to record any audios or videos. Your data will be safely stored on a password protected computer and only the student researcher and the supervisors will have access to this information. Data will be kept for approximately 4 years, after which the data will be completely deleted from any computer or storage drive. Confidentiality will be provided to the fullest extent possible by law.

Participation and Withdrawal: Your participation in this study is voluntary. It is your choice to be part of the study or not. If you decide to be part of the study, you can stop (withdraw) from whatever reason, even after giving consent or part-way through the study. Once you have submitted your responses for this anonymous survey, your answers will be put into a database and will not be identifiable. This means that once you have submitted your survey, your responses cannot be withdrawn from the study because it will not be possible for us to identify which responses are yours. Your decision whether or not to be part of the study will not affect your continuing access to services from Qualtrics.

This study has been reviewed by the McMaster University Research Ethics Board and received ethics clearance. If you have concerns or questions about your rights as a participant or about the way the study is conducted, please contact: McMaster Research Ethics Secretariat Telephone: (905) 525-9140 ext. 23142 C/o Research Office for Administrative Development and Support E-mail: ethicsoffice@mcmaster.ca.

Next

Protected by reCAPTCHA: Privacy & Terms

Powered by Qualtrics



BRIGHTER WORLD

Letter of Consent A Study about Using Cryptocurrencies

- This research seeks to understand Cryptocurrencies users' experience.

Potential Harms, Risks or Discomforts: We do not foresee any significant risk or discomfort from your participation in this research. However, this study will collect data through an online survey, which is an externally hosted cloud-based service. Please note that whilst this service is approved for

12:29
irectly however, by participating in this study, you will help to provide understanding of some factors to affect trust and risks to benefit academics and professional about the nature of these cryptocurrencies systems.

Payment or Reimbursement: if you agree to participate in this study, you will be compensated according to the scheme you agreed to with Qualtrics before you entered into the survey.

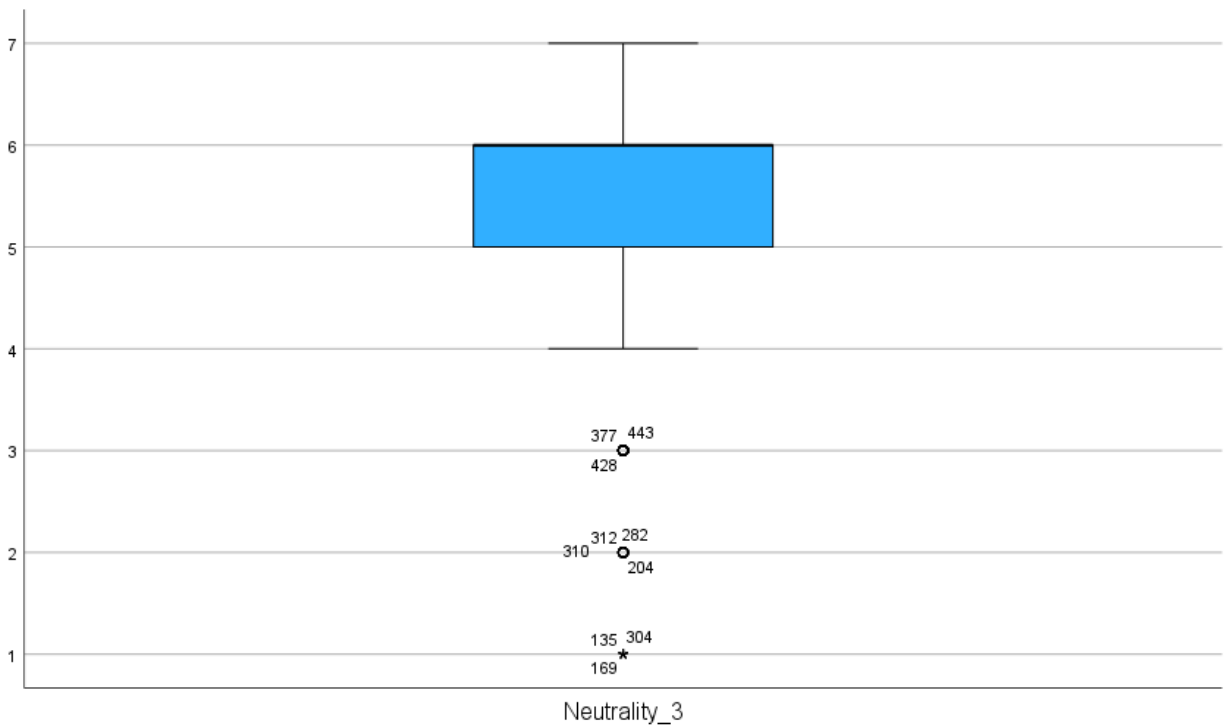
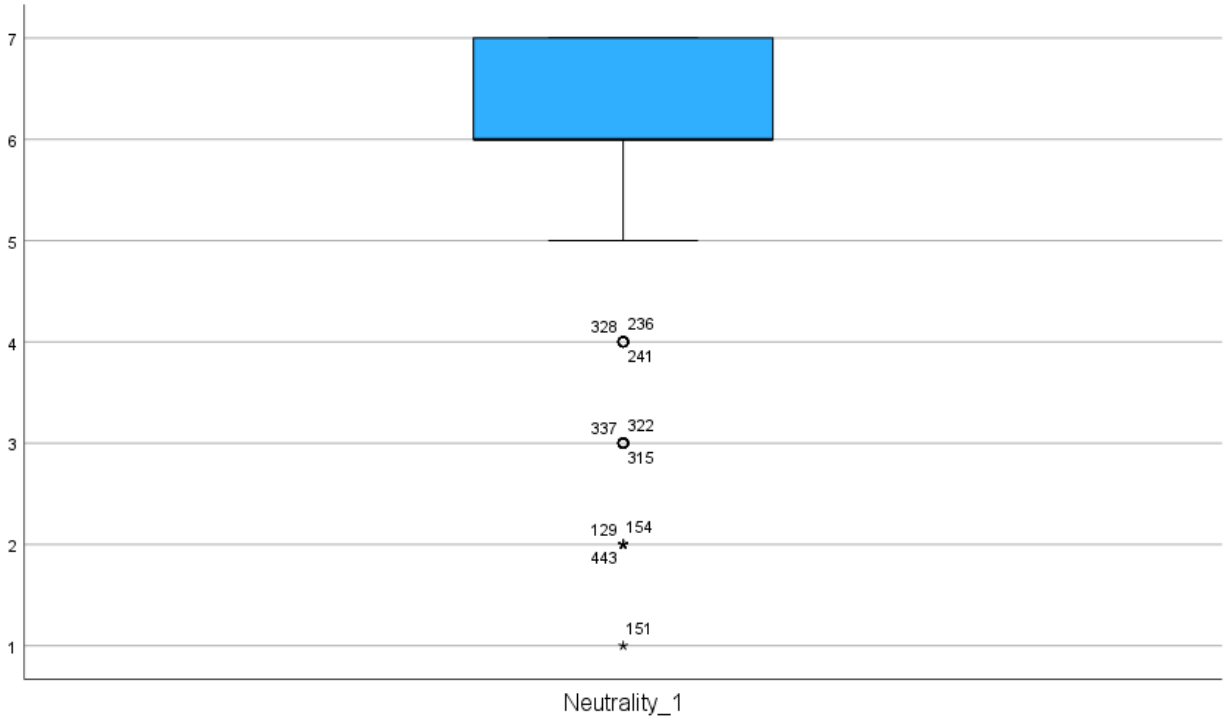
Confidentiality: Every effort will be made to protect (guarantee) your confidentiality and privacy. All information you supply during the research will be held in confidence. No personally-identifying information (e.g., name, social insurance number) will be required or collected before, during, or after the study and therefore your name will not appear

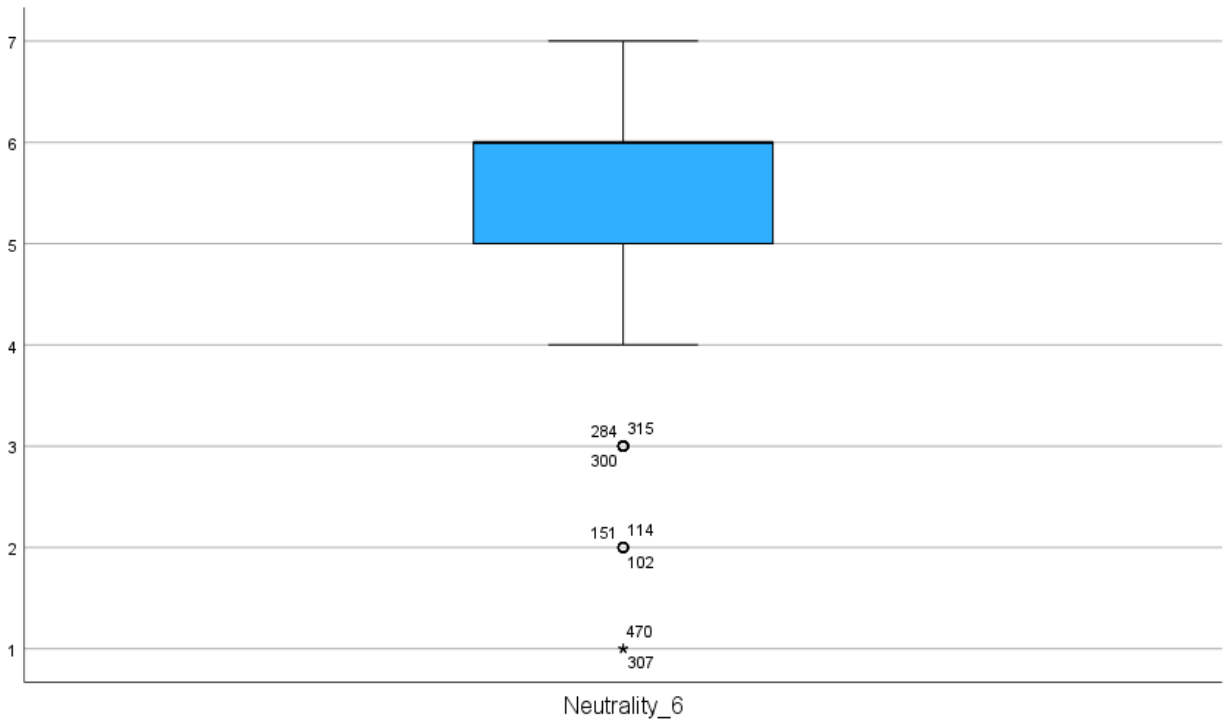
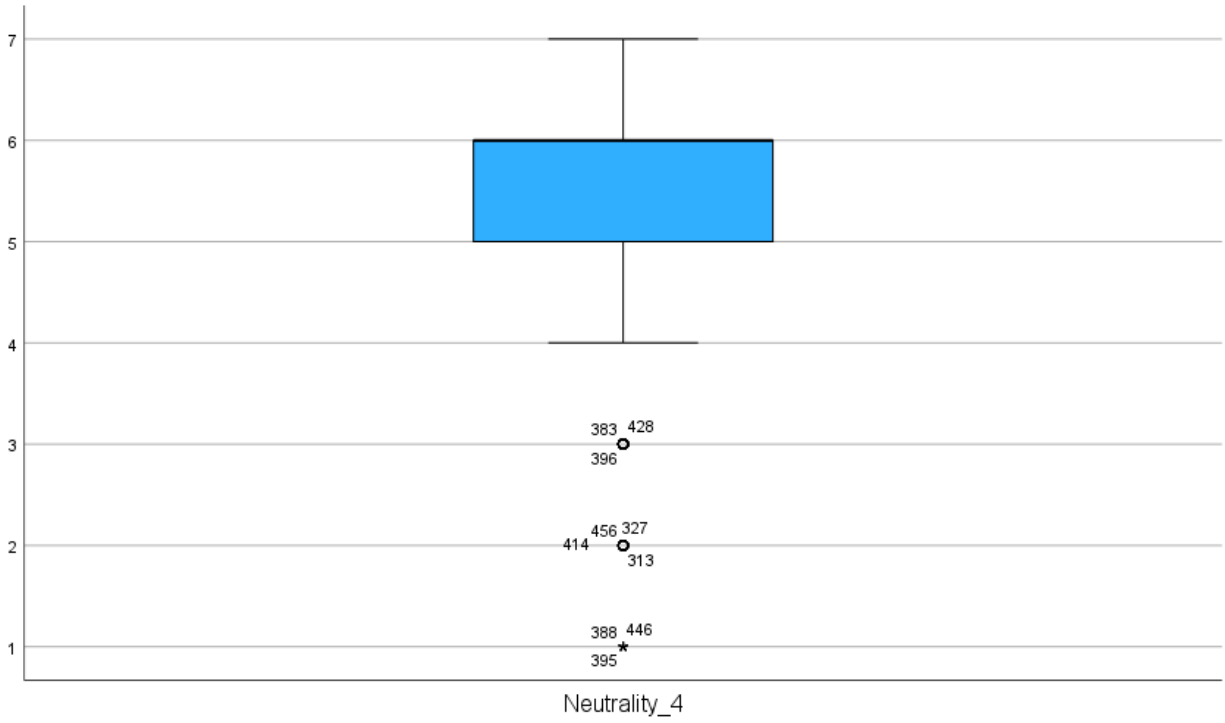
12:29
Participation and Withdrawal: Your participation in this study is voluntary. It is your choice to be part of the study or not. If you decide to be part of the study, you can stop (withdraw) from whatever reason, even after giving consent or part-way through the study. Once you have submitted your responses for this anonymous survey, your answers will be put into a database and will not be identifiable. This means that once you have submitted your survey, your responses cannot be withdrawn from the study because it will not be possible for us to identify which responses are yours. Your decision whether or not to be part of the study will not affect your continuing access to services from Qualtrics.

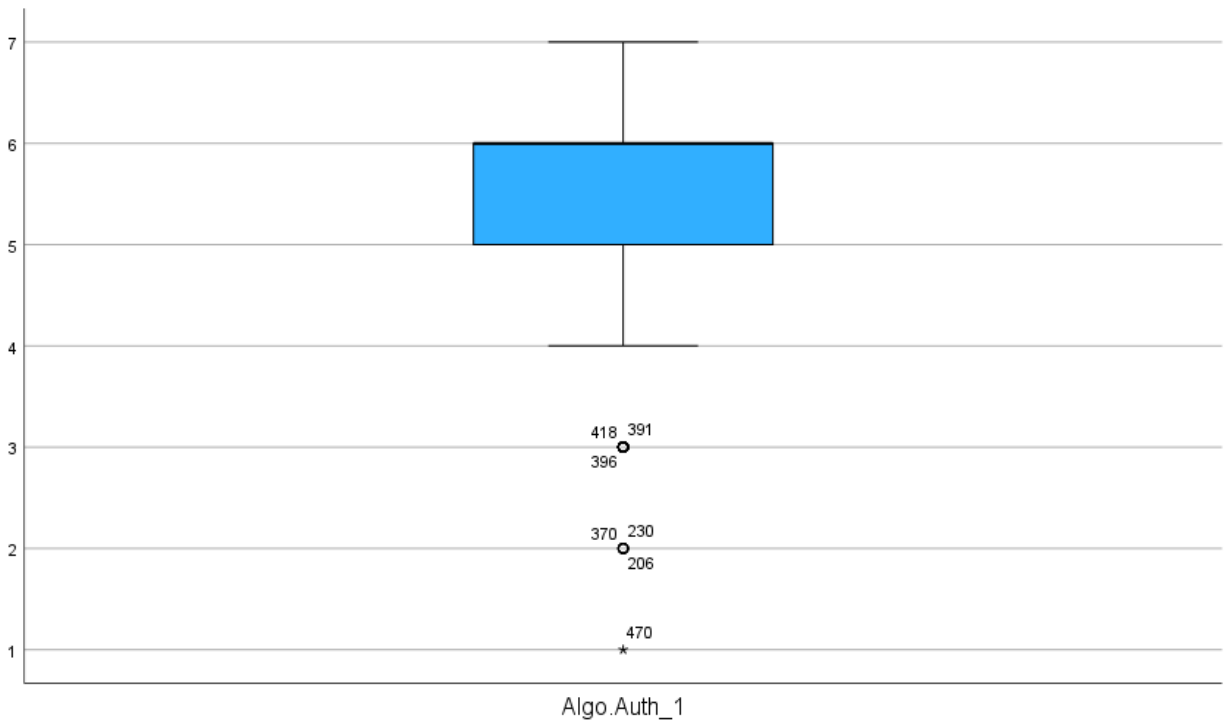
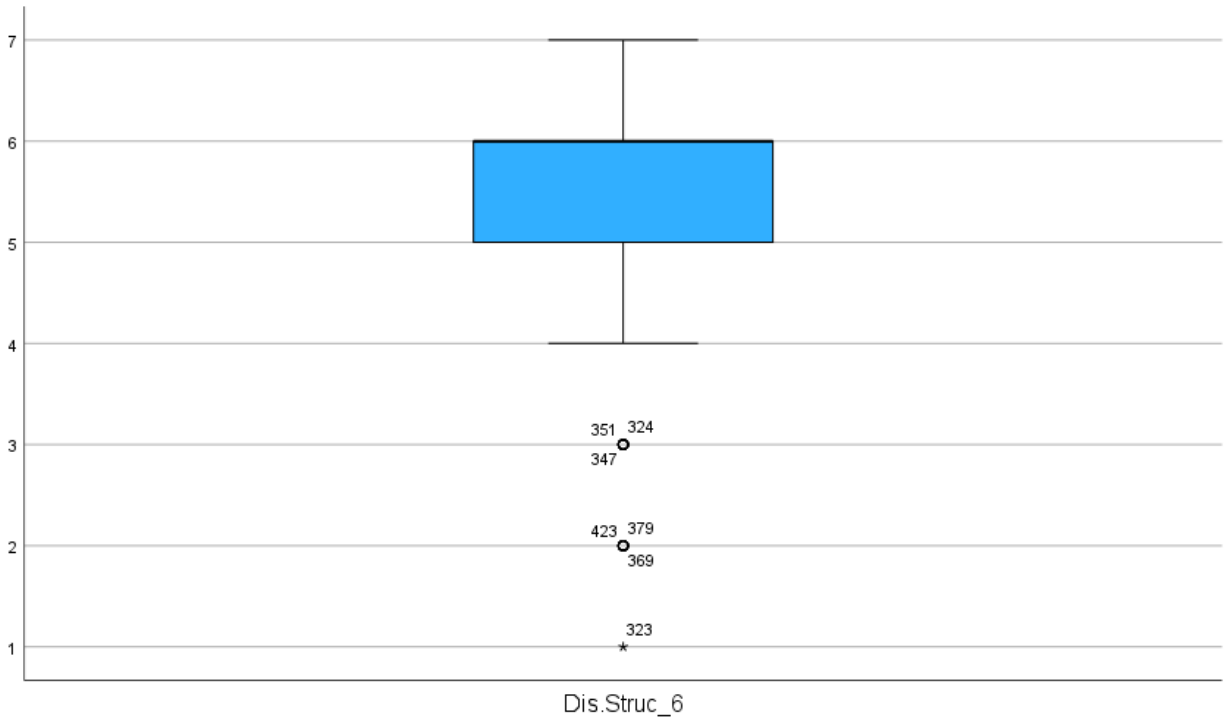
This study has been reviewed by the McMaster University Research Ethics Board and received

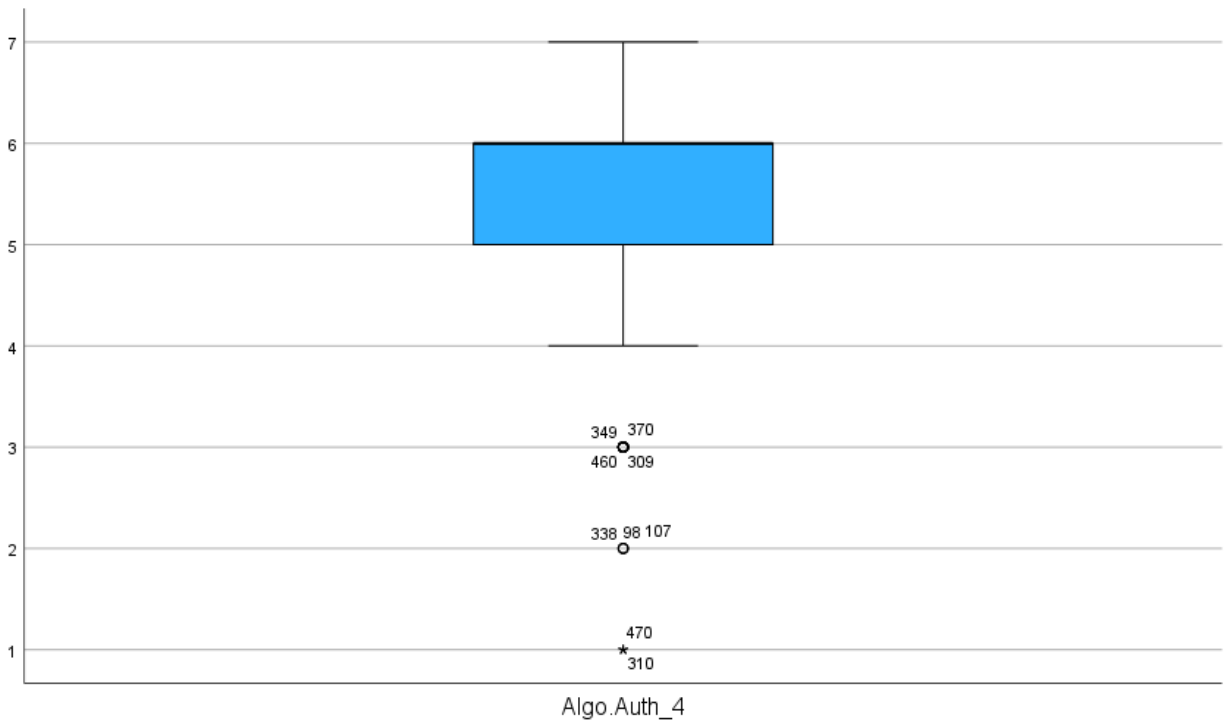
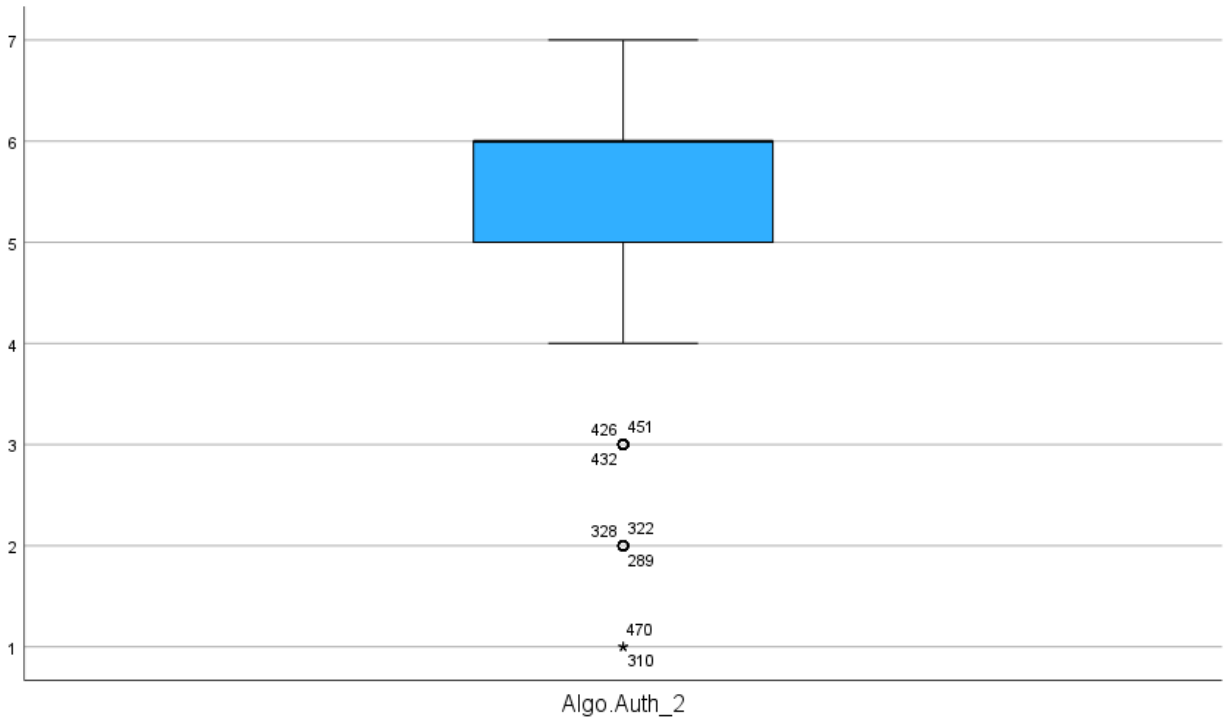
Appendix D. Outlier Analysis

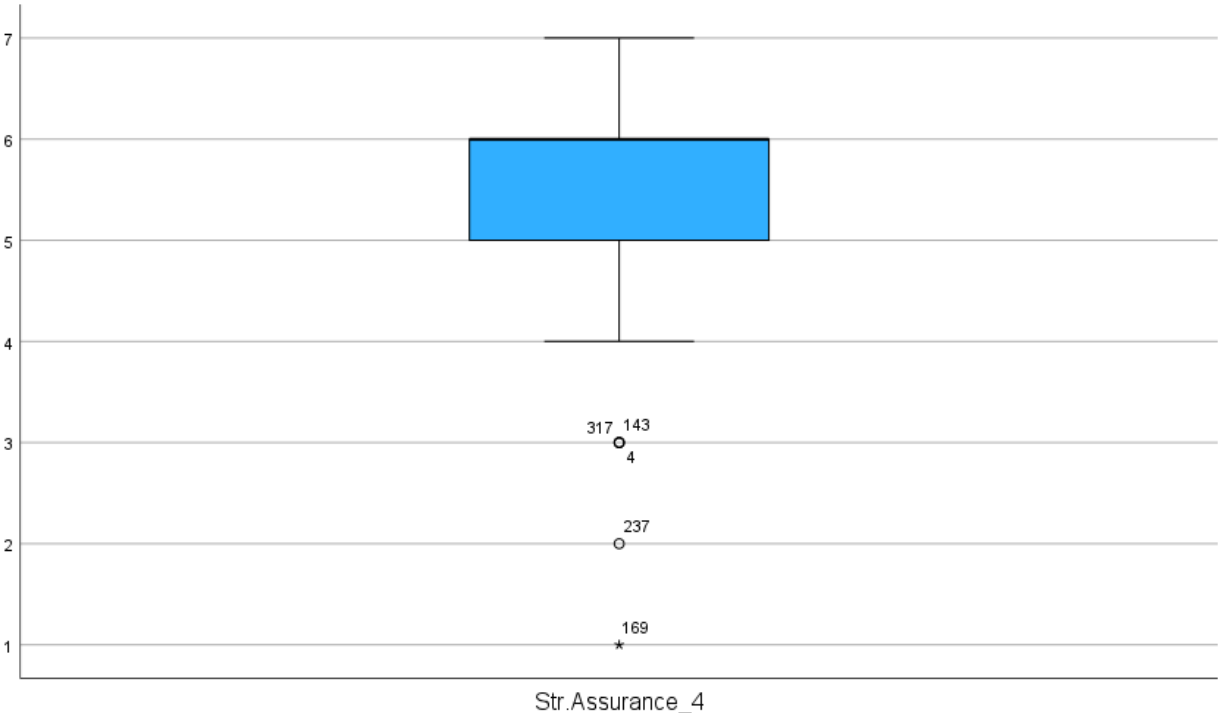
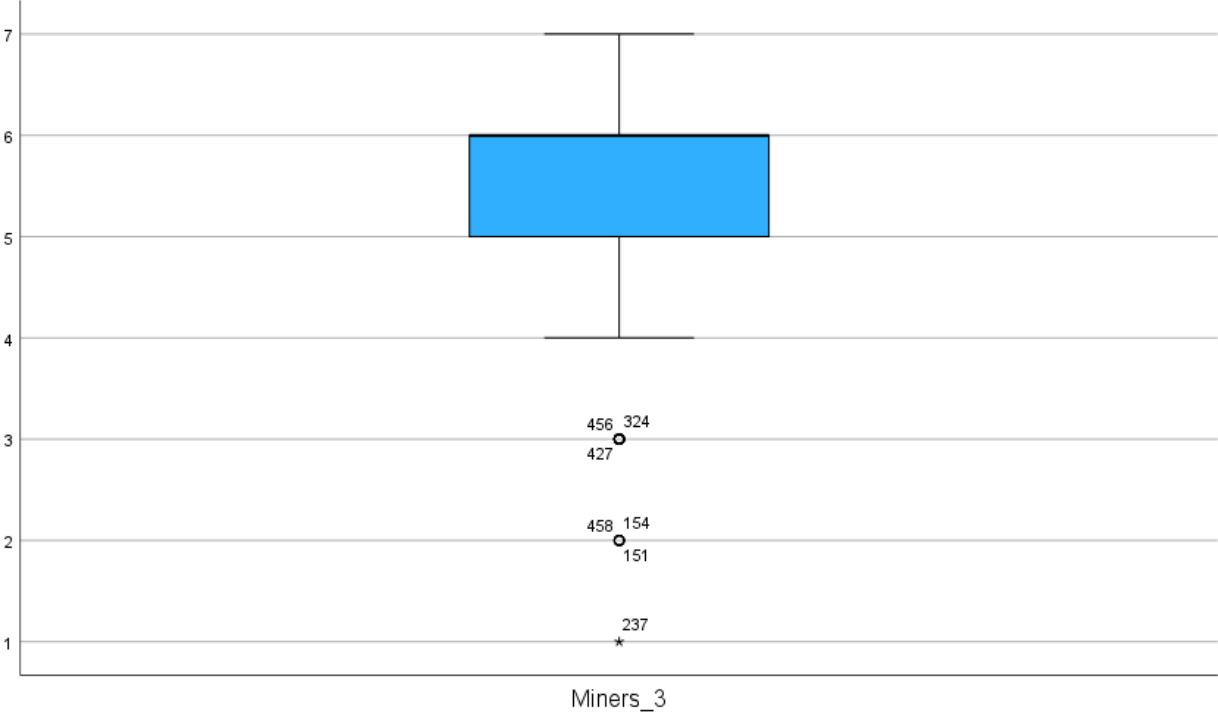
Round 1 (N=475)

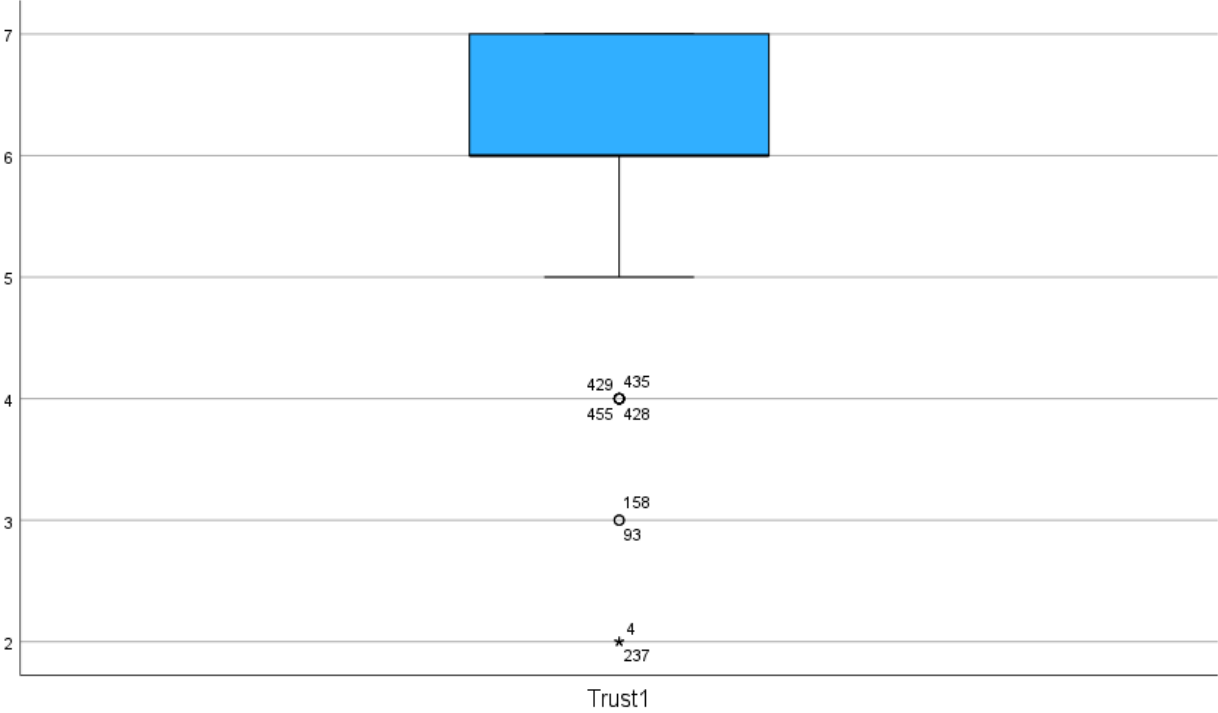












Round 2 (N=458)

