

# ScholarWorks@GSU

## The Impact of Blockchain Technology on Financial Transactions

Authors	Tilooby, Al
Citation	Tilooby, Al. "The Impact of Blockchain Technology on Financial Transactions." 2018. Dissertation, Georgia State University <a href="https://doi.org/10.57709/12552634">https://doi.org/10.57709/12552634</a>
DOI	<a href="https://doi.org/10.57709/12552634">https://doi.org/10.57709/12552634</a>
Download date	2026-06-09 18:18:30
Link to Item	<a href="https://hdl.handle.net/20.500.14694/2398">https://hdl.handle.net/20.500.14694/2398</a>

## **PERMISSION TO BORROW**

In presenting this dissertation as a partial fulfillment of the requirements for an advanced degree from Georgia State University, I agree that the Library of the University shall make it available for inspection and circulation in accordance with its regulations governing materials of this type. I agree that permission to quote from, copy from, or publish this dissertation may be granted by the author or, in her absence, the professor under whose direction it was written or, in his absence, by the Dean of the Robinson College of Business. Such quoting, copying, or publishing must be solely for scholarly purposes and must not involve potential financial gain. It is understood that any copying from or publication of this dissertation that involves potential gain will not be allowed without written permission of the author.

*Al Tilooby*

## **NOTICE TO BORROWERS**

All dissertations deposited in the Georgia State University Library must be used only in accordance with the stipulations prescribed by the author in the preceding statement.

The author of this dissertation is:

Al Tilooby

J. Mack Robinson College of Business

Georgia State University

Atlanta, GA 30302-4015

The director of this dissertation is:

Lars Mathiassen

J. Mack Robinson College of Business

Georgia State University

Atlanta, GA 30302-4015

The Impact of Blockchain Technology on Financial Transactions

by

Al Tilooby

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree

Of

Executive Doctorate in Business

In the Robinson College of Business

Of

Georgia State University

GEORGIA STATE UNIVERSITY

ROBINSON COLLEGE OF BUSINESS

2018

Copyright by  
Al Tilooby  
2018

## ACCEPTANCE

This dissertation was prepared under the direction of the *AL TILOOBY* Dissertation Committee. It has been approved and accepted by all members of that committee, and it has been accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business Administration in the J. Mack Robinson College of Business of Georgia State University.

Richard Phillips, Dean

## DISSERTATION COMMITTEE

*Dr. Lars Mathiassen (Chair)*

*Dr. Conrad Ciccotello*

*Dr. Harold Weston*

## **ACKNOWLEDGEMENTS**

To my wife Rawia and my daughter Alma who provided me with ultimate support and accommodation all along. To my mother and father who instilled in me the quest for knowledge. To my sisters, brother, extended family, and friends for their encouragement.

To my supervisor Dr. Lars Mathiassen, whose knowledge, guidance, care, and patience were indispensable. To my committee members, Dr. Conrad Ciccotello, and Dr. Harold Weston for this vital input. To the participants whose input was essential to this dissertation. To my professors, colleagues, and staff for their teachings, help, and for making the journey fruitful and fun.

## TABLE OF CONTENTS

<b>ACKNOWLEDGEMENTS .....</b>	<b>iv</b>
<b>LIST OF TABLES .....</b>	<b>viii</b>
<b>LIST OF FIGURES .....</b>	<b>ix</b>
<b>LIST OF ABBREVIATIONS .....</b>	<b>x</b>
<b>I INTRODUCTION .....</b>	<b>1</b>
<b>I.1 Financial Transactions .....</b>	<b>1</b>
<b>I.2 Blockchain Technology.....</b>	<b>3</b>
<b>I.3 State of Adoption.....</b>	<b>4</b>
<b>I.4 Research Approach.....</b>	<b>6</b>
<b>I.5 The Role of Theory .....</b>	<b>8</b>
<b>II TECHNOLOGY: BLOCKCHAINS.....</b>	<b>13</b>
<b>II.1 Blockchain Explained .....</b>	<b>13</b>
<b>II.2 Authentication .....</b>	<b>15</b>
<b>II.3 Content and Verification.....</b>	<b>16</b>
<b>II.4 Network Operation .....</b>	<b>17</b>
<b>II.5 Chain of Blocks .....</b>	<b>19</b>
<b>II.6 Blockchain Categories .....</b>	<b>20</b>
<b>III APPLICATION: FINANCIAL TRANSACTIONS.....</b>	<b>23</b>
<b>III.1 Asset Verification .....</b>	<b>24</b>
<b>III.2 Record Keeping .....</b>	<b>26</b>
<b>III.3 Data Privacy .....</b>	<b>29</b>
<b>III.4 Transaction Costs.....</b>	<b>32</b>
<b>IV PERSPECTIVE: STAKEHOLDER VIEWS.....</b>	<b>36</b>

<b>IV.1</b>	<b>Transaction Issues</b> .....	<b>36</b>
<b>IV.2</b>	<b>Technological Issues</b> .....	<b>43</b>
<b>IV.3</b>	<b>Regulatory Issues</b> .....	<b>49</b>
<b>IV.4</b>	<b>Adoption Issues</b> .....	<b>55</b>
<b>V</b>	<b>THEORY: TRANSACTION COST ANALYSIS</b> .....	<b>62</b>
<b>V.1</b>	<b>Searching</b> .....	<b>64</b>
<b>V.2</b>	<b>Bargaining</b> .....	<b>69</b>
<b>V.3</b>	<b>Controlling</b> .....	<b>73</b>
<b>VI</b>	<b>DISCUSSION</b> .....	<b>79</b>
<b>VI.1</b>	<b>Blockchain Technology Can Enable Asset Verification, Record Keeping, and Data Privacy</b> .....	<b>79</b>
<b>VI.2</b>	<b>On Balance, Blockchain Technology Can Lower Financial Transaction Costs</b> ... 81	
<b>VI.3</b>	<b>Blockchain Technology Furnishes a Reporting Platform for Financial Transactions</b> .....	<b>82</b>
<b>VI.4</b>	<b>Blockchain Technology Requires Approaching Financial Transactions Differently</b> .....	<b>83</b>
<b>VI.5</b>	<b>Adoption of Blockchain Technology for Financial Transactions is Uncertain and Complex</b> .....	<b>85</b>
<b>VII</b>	<b>REFLECTIONS</b> .....	<b>88</b>
<b>VII.1</b>	<b>Understanding the Complexity of Designing Blockchains</b> .....	<b>88</b>
<b>VII.2</b>	<b>Applying Transaction Cost to Blockchain Design</b> .....	<b>90</b>
<b>VII.3</b>	<b>Appreciating the Blockchain Ecosystem</b> .....	<b>91</b>
<b>VII.4</b>	<b>Creating Value with Blockchains</b> .....	<b>92</b>
<b>VII.5</b>	<b>Considering Blockchain Applications</b> .....	<b>93</b>
<b>VIII</b>	<b>CONCLUDING REMARKS</b> .....	<b>95</b>

<b>APPENDICES .....</b>	<b>96</b>
<b>Appendix A: Pluralist Methodology .....</b>	<b>96</b>
<i>Appendix A.1: The Literature Review Method.....</i>	<i>99</i>
<i>Appendix A.2: The Perception Analysis Method .....</i>	<i>101</i>
<i>Appendix A.3: The Theoretical Interpretations Method .....</i>	<i>103</i>
<b>Appendix B: General Blockchain Applications.....</b>	<b>108</b>
<i>Appendix B.1: Programmable Assets and Programmable Ownership .....</i>	<i>109</i>
<i>Appendix B.2: Programmable Trust.....</i>	<i>111</i>
<i>Appendix B.3: Programable Identity .....</i>	<i>113</i>
<i>Appendix B.4: Programable Contracts.....</i>	<i>114</i>
<i>Appendix B.5: Programable Money .....</i>	<i>117</i>
<b>Appendix C: Actual blockchain structure .....</b>	<b>119</b>
<b>Appendix D: Classes of Blockchain technology Non-Cryptocurrency Applications.....</b>	<b>120</b>
<b>Appendix E: Market Cap of Top 10 Cryptocurrencies .....</b>	<b>121</b>
<b>Appendix F: Major Research Paradigms .....</b>	<b>122</b>
<b>Appendix G: Recruitment E-mail.....</b>	<b>124</b>
<b>Appendix H: Informed Consent From.....</b>	<b>126</b>
<b>Appendix I: Interview Protocol .....</b>	<b>129</b>
<b>REFERENCES.....</b>	<b>132</b>
<b>VITA.....</b>	<b>147</b>

**LIST OF TABLES**

<b>Table 1: Financial Transaction Phases and Areas of Research Focus.....</b>	<b>2</b>
<b>Table 2: State of Enterprise Blockchain Technology .....</b>	<b>6</b>
<b>Table 3: Research Design Summary .....</b>	<b>11</b>
<b>Table 4: Bitcoin Blockchain Terms .....</b>	<b>14</b>
<b>Table 5: Categories of Blockchains .....</b>	<b>22</b>
<b>Table 6: Industry Perceptions of Transaction Issues .....</b>	<b>43</b>
<b>Table 7: Industry Perceptions of Technological Issues .....</b>	<b>49</b>
<b>Table 8: Industry Perceptions of Regulatory Issues.....</b>	<b>55</b>
<b>Table 9: Industry Perceptions of Adoption Issues .....</b>	<b>61</b>
<b>Table 10: Searching Transaction Costs .....</b>	<b>69</b>
<b>Table 11: Bargaining Transaction Costs .....</b>	<b>73</b>
<b>Table 12: Controlling Transaction Costs.....</b>	<b>78</b>

**LIST OF FIGURES**

<b>Figure 1: A Simplified Blockchain-based Transaction.....</b>	<b>13</b>
<b>Figure 2: Authentication Using Digital Signature .....</b>	<b>16</b>
<b>Figure 3: Transaction from Alice to Bob.....</b>	<b>17</b>
<b>Figure 4: Alice Transacting with Bob through Blockchain Network .....</b>	<b>17</b>
<b>Figure 5: A Traditional Credit Card Transaction (MasterCard, n.d.).....</b>	<b>18</b>
<b>Figure 6: Chain of Blocks in a Bitcoin Blockchain .....</b>	<b>20</b>
<b>Figure 7: Simplified Blocks of Transaction .....</b>	<b>20</b>
<b>Figure 8: Records Reconciliation .....</b>	<b>28</b>
<b>Figure 9: Dimensions of Blockchain.....</b>	<b>89</b>
<b>Figure 10: Blockchain Gestalt.....</b>	<b>92</b>

## LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AML	Anti-Money Laundering
BIS	Bank of International Settlement
CPU	Central Processing Units
CSD	Central Securities Depository
DAO	Distributed Autonomous Organization
DLT	Distributed Ledger Technology
DNS	Domain Name System
DTCC	Depository Trust & Clearing Corporation
EEA	Enterprise Ethereum Alliance
EU	European Union
EVM	Ethereum Virtual Machine
FINRA	Financial Industry Regulatory Authority
FinTech	Financial Technology
KYC	Know Your Customer
HTML	Hypertext Markup Language
ICO	Initial Coin Offering
IoT	Internet of Things
IS	Information Systems
IT	Information Technology
NYSE	New York Stock Exchange
PoC	Proof of Concept
PwC	PricewaterhouseCoopers
R&D	Research and Development
SWIFT	Society for the Worldwide Interbank Financial Telecommunication
UK	United Kingdom
USA	United States of America

**ABSTRACT****The Impact of Blockchain Technology on Financial Transactions**

by

**Al Tilooby****August 2018****Chair: Lars Mathiasen****Major Academic Unit: Executive Doctorate in Business**

Blockchain technology could emerge as a disruptive innovation that streamlines financial transactions and attenuates their cost. Therefore, the financial industry must assess the opportunities and challenges presented by the technology. As a grand breakthrough, it could transform financial transactions and introduce new possibilities for established financial institutions as well as for new entrants. At the same time, incumbents and startups need to overcome technological, regulatory, and adoption challenges before blockchain technology can become a mainstream reality. Despite its potential, the literature on its impact on financial transactions is still fragmented, with weak empirical insights and limited theoretical explanations. Therefore, financial industry managers lack guidance on how to plan and prepare for the impact of blockchain technology on the operation of financial transactions.

Against that backdrop, this dissertation explores the asserted and potential impacts on financial transactions with emphasis on asset verification, record keeping, data privacy, and transaction costs. The dissertation adopts a pluralist approach to examine the subject matter based on three approaches: analysis of the extant literature about blockchain technology concerning financial transactions; perception analysis based on interviews with financial executives, subject matter experts, and researchers; and a theoretical interpretation using

transaction cost theory. Therefore, the dissertation synthesizes insights from the three approaches to offer managers of financial institutions guidance concerning the opportunities and challenges of blockchain technology.

**INDEX WORDS:** Blockchain and Distributed Ledger Technology, Financial Transactions, Asset Verification, Record Keeping, Data Privacy, Transaction Cost Theory

## I INTRODUCTION

### I.1 Financial Transactions

Financial transactions are foundational to the national and global economy. The global financial systems transact trillions of dollars daily and serve billions of customers (Tapscott & Tapscott, 2016). Taking the USA as an example, the Automated Clearing House system processes more than forty trillion dollars' worth of annual transactions—and that only represents about 20 percent of the electronic payments in the nation (Kiviat, 2015). With many competitors seeking a share of this huge market, to remain competitively efficient, financial institutions must frequently disrupt their operations and processes driven by new technologies such as blockchain (PwC, 2017).

Workie and Jain (2017) distinguish three phases of a blockchain-based financial transaction: 1) the initiation phase, where a client accesses the blockchain network to buy or sell financial assets, 2) the verification of financial assets in the blockchain ledger by involved stakeholders, and 3) the recording of the information into the blockchain ledger. In alignment with these three phases, this dissertation focuses on four areas of financial transactions: asset verification, record keeping, data privacy, and transaction costs. Table 1 illustrates the mapping between the four areas of dissertation focus and the three phases of a blockchain-based financial transaction. Asset verification and record keeping map directly to the first and second phases respectively. However, users and financial institutions are concerned about data privacy and transaction costs during all phases of financial transactions. To cover the four areas of focus methodically, the dissertation explores the opportunities, challenges, and recommendations from technological, regulatory and adoption perspectives.

**Table 1: Financial Transaction Phases and Areas of Research Focus**

<i>Financial Transaction Phases</i>		<i>Area of Research Focus</i>
Transaction initiation	Data privacy	Overall transaction cost
Verification of asset	Asset verification Data privacy	
Recording information	Record keeping Data privacy	

At present, financial transaction costs involve many layers of fees that are collected by intermediaries. Digital payments and currency transfers require heavy consumption of human and infrastructural assets of financial institutions that act as intermediaries to conduct, clear, and settle transactions (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). Transaction fees are significant—McKinsey states that the global payment industry enjoyed a 1.8 trillion dollar revenue in 2015 (Bansal, Bruno, Istace, & Niederkorn, 2016). Moreover, it takes several days to settle transactions—transactions such as money transfers require nearly three days to settle (Guo & Liang, 2016; Kiviat, 2015). Although profitable to the intermediaries, these costs burden the parties making the transaction. Blockchain technology might make these transactions faster and less costly by eliminating several layers of intermediaries. The decentralized nature of blockchain could imply costly layers of redundancy, infrastructural costs, and delays. Nonetheless, the reverse could be true because the technology could provide its own cost-efficiencies—as will be described later. Efficiencies could be gained in the same way that double-entry accounting has improved security and reliability despite its redundancy, and analogous to how computer technology has improved security and reliability—until cyber risks evolved. Blockchain technology could, therefore, be the next step in security and reliability. Nonetheless, many challenges and issues would need to be resolved before getting there.

## **I.2 Blockchain Technology**

Blockchain technology was introduced by Nakamoto (2008) to bypass middleman actors such as financial institutions by allowing direct peer-to-peer transactions. To achieve this goal, Nakamoto suggested a peer-to-peer distributed ledger. In this way, payer and payee can exchange directly over the network, utilizing encryption and consensus mechanisms (Guo & Liang, 2016; Tsai, Blower, Zhu, & Yu, 2016; Zhu & Zhou, 2016) to make transactions tamperproof since any modification to the historical data record is detectable by participating blockchain network nodes (B. Lee & Lee, 2017; Tapscott & Tapscott, 2017).

One of the fundamental objectives of any payment system is to guard against double spending. In other words, the system should be able to track who owns the money and should only allow the person who owns the money to spend it once and not more than once. Blockchain technology solves the double spending issue through a consensus mechanism (Nakamoto, 2008; Pazaitis, De Filippi, & Kostakis) that will be detailed later in this dissertation.

Blockchain technology comprises several technological and non-technological concepts and ideas. The integration of these concepts and ideas allows value exchanges without a trusted central institution (Kiviat, 2015). As a result, there is a growing interest in the technology because it provides security, anonymity, and data integrity without third-party organizations in control of the transactions (Yli-Huumo et al., 2016). Although it could theoretically disintermediate, in reality, blockchain networks re-intermediate trust away from the center (Mougayar, 2016) and form ‘multi-center, weakly intermediated’ schemes (Guo & Liang, 2016). The decentralized nature of blockchain technology could also make the data more transparent when compared to centralized transactions (Yli-Huumo et al., 2016). However, since public blockchain network users could opt to act anonymously, a high level of privacy could diminish

the degree of transparency from the perspective of entities that need to know more about end users.

Initially, blockchain technology emerged as the underpinning platform for the Bitcoin cryptocurrency. However, for the reasons outlined, banks expect it will help them streamline and reduce the costs of activities such as international payments and trading settlement (Irrera & Shumaker, 2017). This expectation opens the door for a potentially disruptive technology that could have broad implications for the financial sector. Zhao, Fan, and Yan (2016) and Mougayar (2016) predict that the transformational effect of blockchain technology on enabling trustworthy transactions globally will parallel the paradigmatic influence of the Internet on accessibility to information. Zhao et al. (2016) further elaborate that decentralized trust—arising from blockchain technology—will attenuate costs of transactions that are due to non-technical aspects of centralization. Similarly, Guo and Liang (2016) posit that applying blockchain technology can resolve many of the efficiency bottlenecks, delays, fraud, and operational risks they assert infest the financial industry. Nonetheless, blockchain networks are inherently slow since 1) getting a whole network to a consensus on a single truth is time-consuming and 2) peer-to-peer nodes have to act both as a client and a server (Tsai et al., 2016).

### **I.3 State of Adoption**

Since blockchain technology could offer opportunities to reduce cost and improve the speed of transaction settlements, exchanges, banks, and the whole securities industry are increasingly interested in the technology (de Meijer, 2016). Moreover, international institutions including the International Monetary Fund, and nations, such as the USA, the UK, Japan, China, Russia, India, and South Africa have initiated research on blockchain technology applications targeting many fields (Guo & Liang, 2016).

Recently, international institutions, including the United Nations and the International Monetary Fund (Guo & Liang, 2016), as well as central banks in the U.K., China, the USA, Korea, Singapore, Japan, Russia, India, Netherlands, and South Africa have recently announced blockchain technology plans (Mori, 2016; Tsai et al., 2016). National stock exchanges such as Nasdaq; banking titans such as J.P. Morgan; and financial bodies such as the USA Depository Trust & Clearing Corporation and the People's Bank of China have all started their blockchain technology research laboratories (Guo & Liang, 2016; Mori, 2016). Most financial institutions have pilot programs for blockchain technology. For instance, R3—founded in 2015 as a blockchain technology consortium—has partnered with over eighty financial institutions and bodies (R3, n.d.). China Financial Blockchain Consortium (Guo & Liang, 2016) is another alliance. Traditional companies have jumped on the blockchain technology bandwagon with a variety of offerings. For instance, IBM has built a supply chain blockchain with a mission statement to lubricate exchange, enhance trust, increase accountability, and elevate transparency. IBM CEO Ginni Rometty stated: “*What the Internet did for communications, blockchain will do for trusted transactions*” (IBM, n.d.). Startups such as Blockstream and Digital Asset Holdings already offer financial institutions services that facilitate digital asset dealing (Pilkington, 2015). According to Coindesk (2017a), enterprise-oriented blockchain-based projects grew in size, and pilot projects continued in partnership with major groups and corporations as summarized in Table 2.

**Table 2: State of Enterprise Blockchain Technology (Coindesk, 2017a)**

<p><b>Hyperledger expands projects and members:</b></p> <p>4 top level frameworks including EVM code, 130 members, PoCs in finance, and working groups in healthcare</p>	<p><b>Enterprise Ethereum Alliance is born:</b></p> <p>EEA launches with major membership list, focused on permissioned Ethereum with interoperability with public blockchains</p>
<p><b>Corporates expand staffing, R&amp;D labs:</b></p> <p>Enterprises, consortia, and working groups continue launching pilots, PoCs and tests</p>	<p><b>Ripple expands to Japan, completes pilot:</b></p> <p>Mitsubishi joins board, 47 bank consortia implements cloud-based payment pilot</p>
<p><b>R3 continues diverse tests:</b></p> <p>Demos Ethereum applications, and commercial paper programs</p>	<p><b>DTCC (Depository Trust &amp; Clearing Corporation) expands DLT settlement trials:</b></p> <p>Eying REPO market, working with startups including Digital Asset and R3</p>

#### **I.4 Research Approach**

Even though blockchain technology could impact many aspects of our lives, thus far, there are only a few published academic papers that treat the technology from a business perspective. Over Research on blockchain technology has been mainly attentive to technical and legal topics (Lindman, Tuunainen, & Rossi, 2017) primarily published in practitioner-oriented journals and on websites that are targeting Bitcoin evangelists and hobbyists. Over 80 percent of the extant literature focuses on Bitcoin systems, and less than 20 percent deals with other blockchain technology applications (Yli-Huumo et al., 2016) with most of that focused on technological (Beck, Czepluch, Lollike, & Malone, 2016; Lindman et al., 2017; Teigland, Yetis, & Larsson, 2013) and legal problems (Bollen, 2013; Ingram & Morisse, 2016; Lindman et al., 2017). Hence, as blockchain technology permeates, further research in the domains of information systems (IS) and management is called for (Giaglis & Kyriotaki, 2014; Lindman et

al., 2017; Van Alstyne, 2014). This dissertation contributes to the efforts of bridging this gap in knowledge.

To explore the impact of blockchain technology on financial transactions, this dissertation uses a pluralistic method that combines a review of the literature, an analysis of the perspectives of key industry players and observers, and a theoretical interpretation through the lens of transaction cost theory (Coase, 1937; Ouchi, 1980; Williamson, 1975). A pluralist approach that compares and contrasts multiple plausible perspectives on reality is crucial to the emergence of rigorous scientific knowledge (Azevedo, 1997; Van de Ven, 2007) as it can provide complementary insights and possible synthesis of them to study an emerging business phenomenon. Furthermore, using multiple perspectives on a complex business problem decreases the likelihood of unintended bias in interpretations (Van de Ven, 2007).

When utilizing a pluralist methodology, the researcher moves iteratively between data and theory (A. S. Lee & Baskerville, 2003) contrasting perspectives and synthesizing findings into a holistic account. Consistent with the approach, this dissertation moves between description and theory by drawing on a) the intersection of literature about blockchain technology and financial transactions, b) interviews with financial industry executives and subject matter experts about the impact of blockchain technology on financial transactions, and c) transaction cost theory (Coase, 1937; Ouchi, 1980; Williamson, 1975) as a particularly thought-provoking theoretical framework that promises insights into the potentially disruptive effects of the technology. When applying the first and second methods, we adopt a broad view of the phenomenon exploring various types of blockchain technology impacts on financial transactions. In this way, we report findings such as technical, regulatory, and adoption issues. Moreover, in this case, the term ‘transaction cost’ has a broader meaning to engulf ‘transaction theory’ costs,

production costs (Dyer, 1997; Zajac & Olsen, 1993), and transition costs that are related to deploying blockchain technology. Nevertheless, when we look through the prism of transaction cost theory, we zoom in to solely focus on ‘transaction theory’ costs.

A detailed account of how the dissertation has applied the pluralist methodology is found in appendix A.

## **I.5 The Role of Theory**

The field of IS is concerned with studying phenomena that emerge from the interaction between technological systems and social systems (Gregor, 2006; A. S. Lee, 2001). As such, the use of blockchain technology in any industry satisfies the definition of IS and could be explored targeting the four central goals of IS theory (Gregor, 2006). The second goal is to explain how, why, and when things occur based on causality and methods of argumentation (Gregor, 2006). The third goal is to probabilistically predict what will transpire in the future if certain preconditions obtain (Gregor, 2006). Finally, the fourth goal is future-oriented like prediction with theory offering a prescription of normative methods and structures for the development of artifacts to attain desired outcomes (Gregor, 2006).

This dissertation provides descriptive accounts and examines opportunities and risks from business and societal perspectives (Lindman et al., 2017) to uncover new explanations underlying the blockchain technology phenomenon by invoking transaction cost theory to explicate the interaction of the financial sector with blockchain technology (Gregor, 2006). In part, the goal here is a response to the assessment of Zhao et al. (2016) that research in the economic and social validity of blockchain technology applications is lagging because it takes more effort to uncover. Additionally, there is a lack of a deep understanding regarding how blockchain technology decentralized services are designed, developed, and organized to

revolutionize trust (Lindman et al., 2017). In addition, this research seeks to foresee (Gregor, 2006) the impact of blockchain technology on financial transactions by enlisting perceptions by key industry players and observers and by adopting theoretical interpretations. Hence, the final integrative goal of this research is to prescriptively (Gregor, 2006) outline insights into how financial organizations can prepare for blockchain technology opportunities and threats.

The transaction cost theory is a fitting theoretical framework for understanding and explicating the impact of blockchain technology on financial transactions because blockchains could impact how transactions are conducted. Transaction cost theory is interdisciplinary by virtue of joining economic perspectives with aspects of organization theory and contract law (Williamson, 1979). The theory is concerned with minimizing the cost of transactional activities that are not directly attributed to the production of goods and services, and are instead related to the cost of searching, bargaining, monitoring, and enforcement activities that are associated with the transaction of goods and services (Husted & Folger, 2004). Consequently, a persistent goal of transaction cost theory is concerned with organizational boundaries around the decision of whether a transaction is more efficiently performed within a firm or outside a firm's boundaries (Coase, 1937; Geyskens, Steenkamp, & Kumar, 2006).

Ouchi (1980) defines a 'transaction cost' as any activity that is conducted to satisfy the expectations of participants in an exchange. Usually such costs are attributed to the difficulty of redeploying assets to their next best use—the asset specificity challenge (Husted & Folger, 2004; Klein, Crawford, & Alchian, 1978; Williamson, 1985, 1991)—or to the difficulties in measuring individual contributions to team effort—the metering problem which is also referred to as performance ambiguity (Alchian & Demsetz, 1972; Husted & Folger, 2004; Milgrom & Roberts, 1992; Ouchi, 1980). Another problem with perceiving equity is contingent goal incongruence—

the degree to which exchange participants have incompatible objectives (Husted & Folger, 2004; Ouchi, 1980).

There are two primitives in transaction cost theory that are closely related to the aforementioned notions. First, bounded rationality—the individual’s limitation on receiving, sustaining, retrieving, and processing information (Simon, 1955; Williamson, 1973). The second is opportunism—exemplified by dodging duties, breaching agreements, and stealing (Alchian & Demsetz, 1972; Husted & Folger, 2004) as each participant endeavors to maximize their advantages in transactions through dishonesty and lack of transparency (Williamson, 1973). Moreover, Williamson also specific two more transaction costs determinants: frequency, meaning how often a contract is invoked (Milgrom & Roberts, 1992; Williamson, 1979) and uncertainty, comprising ex ante difficulties of anticipating all future scenarios, language equivocality, and ex post performance ambiguity.

Accordingly, Table 3 summarizes the research design for this dissertation based on Mathiassen (2017). The table defines the problem setting, the area of concern, the analytical framing, the method, the research question, and the expected contribution to the body of knowledge.

**Table 3: Research Design Summary—Adapted from Mathiassen (2017)**

<i>Component</i>	<i>Definition</i>	<i>Details</i>
P	The problem setting represents people's concerns in a real-world problematic situation.	Blockchain technology could offer opportunities concerning financial transactions. On the other hand, to implement blockchain technology there are many technological, regulatory, and adoption challenges.
A	The area of concern represents a body of knowledge within the literature that relates to the problem setting.	The impact of blockchain technology on financial transactions with specific focus on asset verification, record keeping, data privacy, and transaction costs
F	The conceptual framing helps structuring the analysis of data to answer the research question. $F_A$ draws on concepts from the areas of concern, whereas $F_I$ is independent of area of concern.	The study will leverage transaction cost theory as an independent conceptual framing $F_I$ .
M	The adopted methods of empirical inquiry.	The study adopts a pluralist approach by combining three different methods of inquiry: Method 1: Extant literature analysis. Method 2: Perception analysis based on interviews with financial executives, subject matter experts, and blockchain technology researchers. Method 3: Theoretical interpretation of insights from Methods 1 and 2 based on transaction cost theory.
RQ	The research question relates to the problem setting; it opens the research into the area of concern and helps ensure the research design is coherent and consistent.	What is the impact of blockchain technology on financial transactions?
C	The contributions to the problem setting and area of concern and possibly to conceptual framework and method.	This study contributes to the existing body of knowledge as follows: Contribution to practitioners: Insights into how financial organizations can prepare for blockchain technology opportunities and threats $C_P$ .

		<p>Contribution to the literature: A synthesis of the extant financial literature related to blockchain technology, coupled with empirical accounts of industry perceptions of the impact of blockchain technology <math>C_A</math> on financial transactions.</p> <p>Contribution to the theory: A theoretical interpretation of the phenomenon through the lens of transaction cost theory <math>C_F</math>.</p>
--	--	--

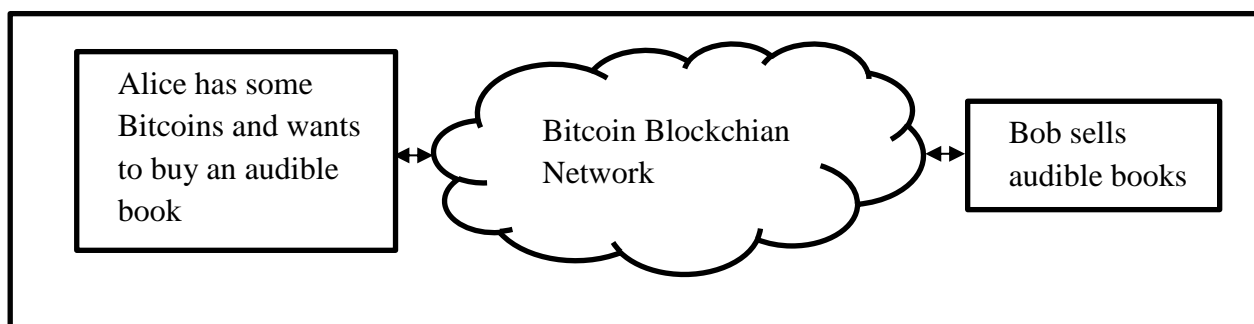
## II TECHNOLOGY: BLOCKCHAINS

Blockchain technology is both an economic innovation—a new architecture for enabling humans or machines exchanges without the need of full trust—and a technological innovation—a novel decentralized ledger that engenders trust (Liebenau & Elaluf-Calderwood, 2016; Lindman et al., 2017) because the technology could provide the platform to record transactions and share data between participating parties in a more efficient, transparent, and verifiable manner (Workie & Jain, 2017). However, disruptive innovations usually surpass the internal absorption and usurpation capabilities of established institutions (Mougayar, 2016) and both established institutions and startups will have to navigate the regulatory and adoption turbulences and technological hurdles as will be detailed later in this dissertation.

### II.1 Blockchain Explained

To explain how blockchain technology works, we start with a simple scenario based on Bitcoin blockchain. In our scenario, Alice wants to use some of her Bitcoins to buy an audible book from Bob through the Bitcoin blockchain—Figure 1.

**Figure 1: A Simplified Blockchain-based Transaction**



Alice initiates the exchange by sending a broadcast message to the blockchain network. The message contains the electronic address of Bob and the amount required to pay for the audiobook. Next, the blockchain network assembles Alice’s transaction information and adds it to its public ledger. Then, seeing the payment from Alice, Bob sends Alice the electronic keys to

download the audible book. Based on this scenario, we present the underpinning blockchain concepts that explain how the transaction in the scenario works.

To support the ensuing elaboration of the above scenario, we describe in Table 4 the relevant Bitcoin blockchain terms.

**Table 4: Bitcoin Blockchain Terms**

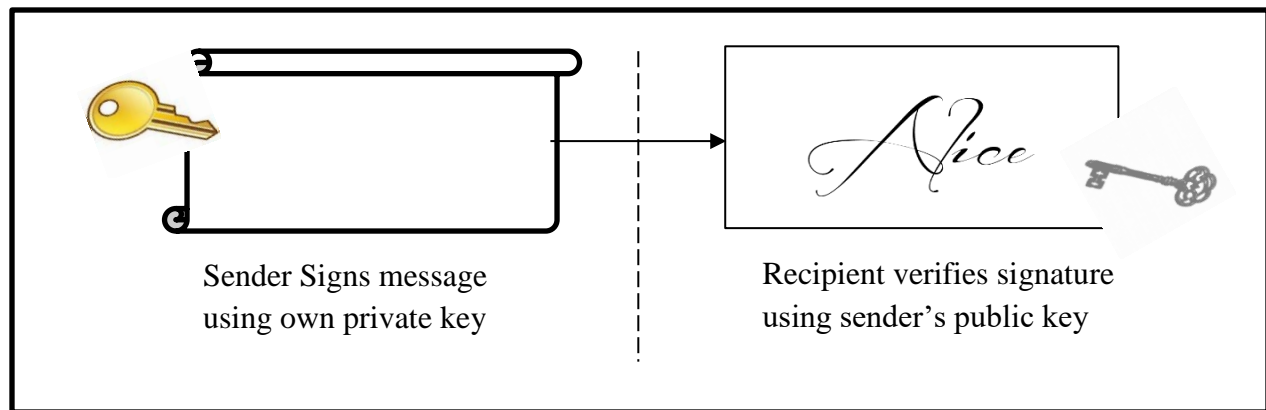
<i>Term</i>	<i>Description</i>
Transaction	<p>According to (BitcoinWiki, n.d.) a Bitcoin transaction is</p> <ol style="list-style-type: none"> <li>1. A transfer of value that is broadcasted to the network and recorded by the network into a block.</li> <li>2. Typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs.</li> <li>3. Not encrypted, so it is possible to browse and view every transaction ever recorded into a block.</li> <li>4. Once buried under enough confirmations it can be considered irreversible.</li> </ol>
Block	<p>A unit of data in the blockchain that includes a hash of itself, the hash of the prior block, and multiple transactions (Narayanan, Bonneau, Felten, Miller, &amp; Goldfeder, 2016).</p> <p>Bitcoin blockchain reached <a href="#">510188</a> blocks as of 2018 Feb 20<sup>th</sup> (Blockchain, n.d.).</p>
Blockchain	<p>Is a chain of blocks where each block is cryptographically linked to the prior one (Mattila, 2016).</p>
Blockchain Network	<p>A peer-to-peer arbitrarily connected network with no hierarchy, no centralization, and no master nodes; where each full node stores a replica of the blockchain and relays info to its connected neighbors (Narayanan et al., 2016).</p>
Node	<p>Any computer that connects to the Bitcoin network (BitcoinWiki, n.d.).</p>
Full node	<p>A special type of node that fully validates transactions and blocks; almost all full nodes also support the network by accepting transactions and blocks from other full nodes, validating those</p>

	<p>transactions and blocks, and then further relaying them to neighboring nodes (BitcoinCore, n.d.).</p> <p>The number of full nodes is unknown. (Bitnodes, 2018) asserts that there are 11389 reachable full nodes as of 2018 Feb 20th, but estimates by different sources vary significantly.</p>
Miner	<p>A full node that competes to build the next block (Tapscott &amp; Tapscott, 2016).</p> <p>Estimates vary, but they are thousands Bitcoin miners.</p>

## II.2 Authentication

How does the Bitcoin blockchain network and Bob know that Alice authenticated the transaction? The answer is digital signature. Alice initiates the transaction by using her private key—a password that only Alice knows—to digitally sign, and therefore, authenticate the transaction. Paralleling the objectives of a traditional hand-written signature, a digital signature is a cryptographic mechanism that utilizes pairs of private and public keys to satisfy four objectives (Badev & Chen, 2014). First, only the signatory can sign with her specific signature. Second, it is not possible to append the signature to other than the signed documents. Third, the signatory cannot deny her signature. Fourth, the recipient can validate that the document has the authentic signature of the signatory. Narayanan et al. (2016) explain how the public and private keys are generated using a mathematical algorithm such that if Alice signs a message with her private key, and Bob knows her public key, then Bob can verify that Alice has indeed signed the message and that the message has not been tampered with. Figure 2 depicts this authentication scenario.

**Figure 2: Authentication Using Digital Signature—Adapted from Badev and Chen (2014)**



### II.3 Content and Verification

What is in the transaction initiated by Alice? Narayanan et al. (2016) explain how transactions are constructed in a Bitcoin blockchain network, in the scenario where Alice intends to send some Bitcoins to Bob. The transaction comprises a pointer to where Alice acquired the Bitcoins in the historical record of the blockchain, the amount she wants to transfer to Bob, the public key of Bob which is the payee's digital address, Alice's digital signature for the whole transaction, and a small transaction fee as an optional incentive for the node that assembles her transaction. Figure 3 illustrates the content of the transaction broadcasted by Alice to the blockchain network.

Upon receiving Alice's transaction, the blockchain network verifies a few items such as Alice's digital signature and her claim of ownership of the Bitcoins. Following the verification of the veracity of the transaction, one of the nodes in the blockchain network assembles Alice's transaction into a block of data alongside hundreds of other transactions, and hence, the block becomes part of the chain or ledger. The network is now aware that the Bitcoins spent by Alice are owned by Bob. By virtue of Alice's transaction being part of the public ledger, Bob may confidently send Alice the keys to the audiobook she bought from him.

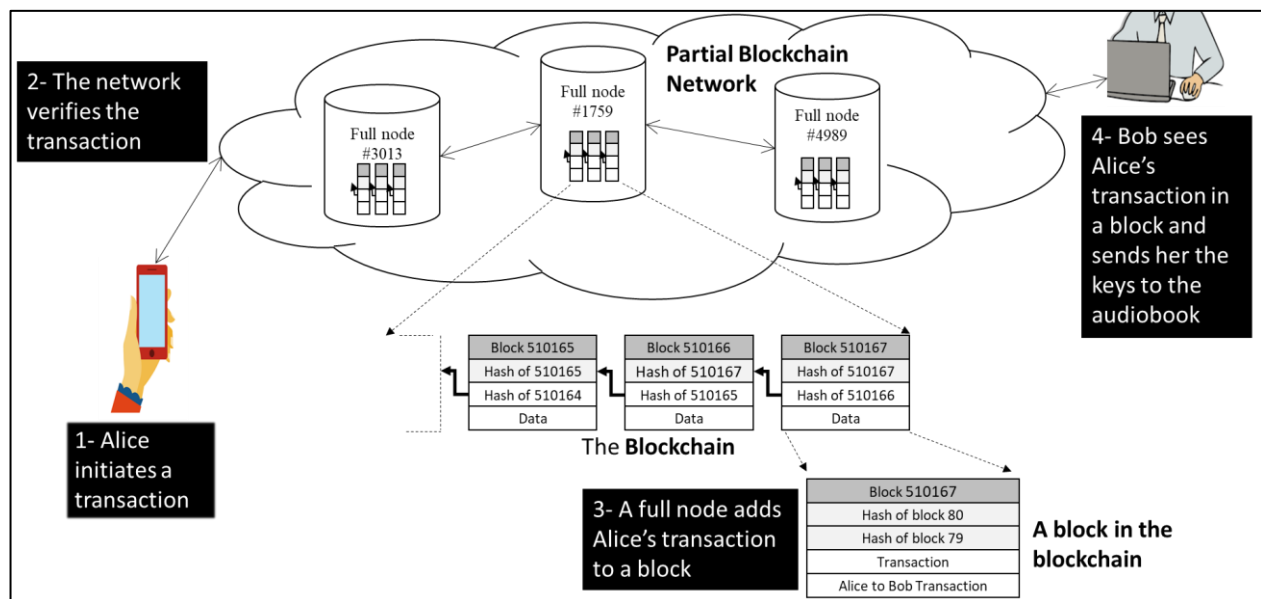
**Figure 3: Transaction from Alice to Bob—Adapted from Narayanan et al. (2016)**

Input: Pointers to where Alice acquired the Bitcoins
Output 1: Bitcoins to be transferred to Bob and his public key
Output 2: Change address—Alice’s public key and change amount
Signature: Alice’s digital signature of the whole transaction
Notes: <ul style="list-style-type: none"> <li>• The total of inputs should be equal or greater than the total of outputs</li> <li>• When total of inputs is greater than total of outputs, the difference is considered as a transaction fee</li> </ul>

## II.4 Network Operation

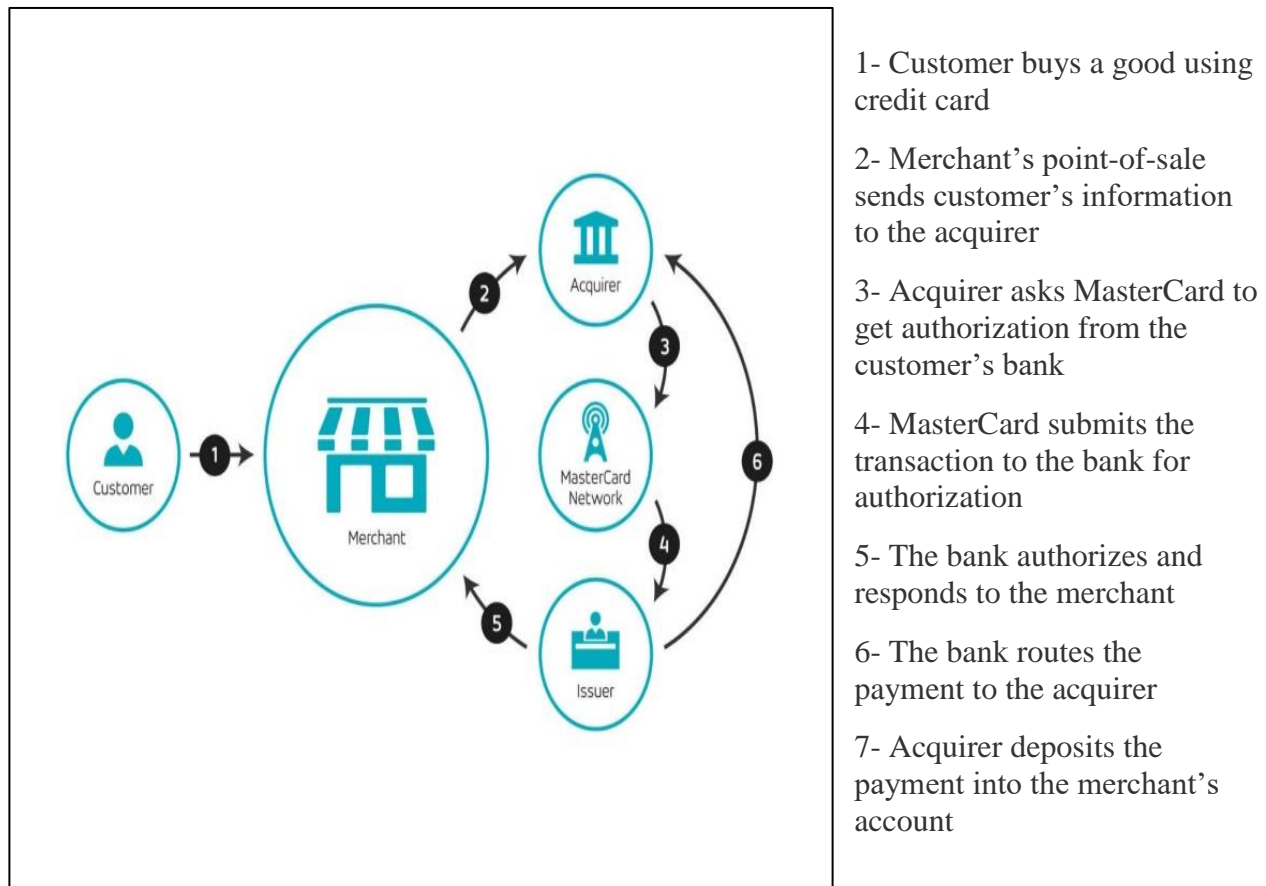
How does the Bitcoin blockchain network operate? Our scenario is based on the Bitcoin blockchain network. Figure 4 depicts the steps of our scenario in more details.

**Figure 4: Alice Transacting with Bob through Blockchain Network**



To contrast and, therefore, appreciate the simplification blockchain technology brings to the table, Figure 5 depicts a traditional credit card transaction.

**Figure 5: A Traditional Credit Card Transaction (MasterCard, n.d.)**



Bitcoin is a cryptocurrency operating over a public blockchain network. According to Narayanan et al. (2016), the Bitcoin blockchain network comprises many nodes that are arbitrarily and partially connected to relay information to each other using the blockchain protocol. The Bitcoin blockchain network is a peer-to-peer network that has no hierarchy, no centralization, and no master nodes.

Some full nodes participate in the tasks of validating and relaying transactions in the Bitcoin blockchain network (Swan, 2015). Such full nodes are called 'miners'—a metaphor for their quest to compete with each other to build new blocks. Since the Bitcoin protocol allows full nodes to share their knowledge about transactions with their neighbors, the network guards

against double-spending by validating each new transaction against the list of unspent transactions in the ledger (Bjerg, 2016). ‘Miners’ are motivated by two monetary incentives described by Narayanan et al. (2016). First, each new valid block conceives a set amount of new bitcoins that will belong to the builder of that block. Second, the block builder collects the transaction fees of all the transactions included in the block.

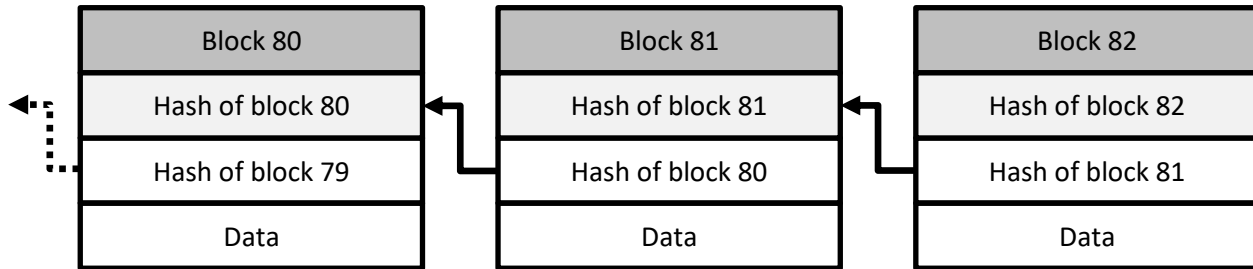
Narayanan et al. (2016) go on to explain this operation of a blockchain network. Before a ‘miner’ builds a new block, she must find a solution for a hard-to-solve mathematical puzzle. This endeavor is referred to as proof of work since it requires spending a significant amount of computational power to solve the puzzle. That is the reason, on average, it takes nine minutes to generate a new block in the Bitcoin blockchain network. Next, other ‘miners’ verify the integrity of the newly-built block and append it to the longest chain. The longest valid chain is considered the operational blockchain that the network nodes honor and extend. Honoring and extending the longest valid chain is another significant component of the consensus mechanism that allows the network to function without a central authority.

## **II.5 Chain of Blocks**

How are blocks structured? From a database perspective, the blockchain is a series of data blocks that are cryptographically chained together (Mattila, 2016) as each block contains the ‘hash’—a unique short encryption of the message—of the preceding block, and therefore, it is a chain of blocks or a ‘blockchain’. A hash function produces an easy to compute, but extremely hard to invert fixed-length compact ‘hash’ from a message of arbitrary length (Gilbert & Handschuh, 2003). Figure 6 illustrates a high-level schematic of a blockchain ledger or database. Since the header of the block contains a ‘hash’ of the data of the current block, and the current block contains the hash from the previous block, back to the genesis block, the history of every

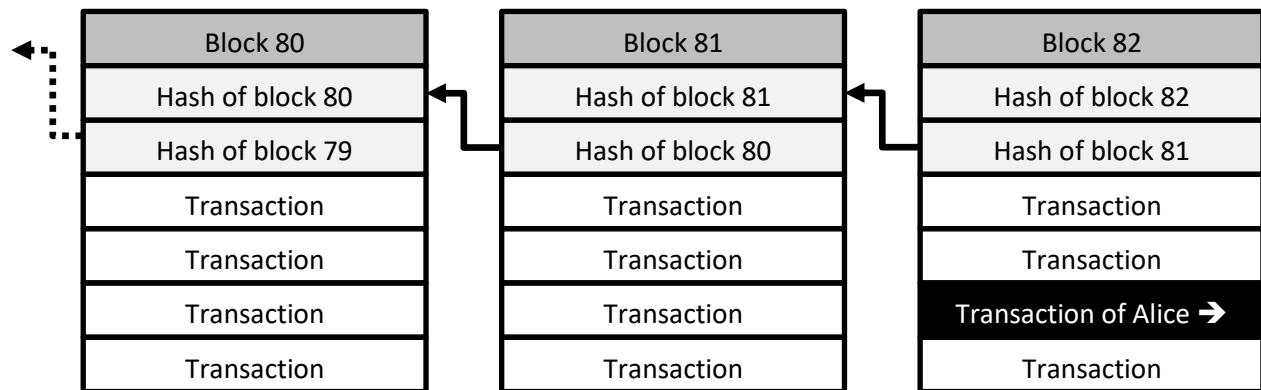
past block predicates the latest block. The ‘hash-chaining’ of blocks makes it extremely difficult to hack a blockchain—as we mentioned earlier, it is hard to solve the mathematical puzzle for a single block, let alone to work backward to rebuild many blocks that satisfy the required solutions.

**Figure 6: Chain of Blocks in a Bitcoin Blockchain (Narayanan et al., 2016)**



Each Bitcoin block is a collection of transactions in the range of 2000 transactions per block. Figure 7 depicts a simplified representation of the Bitcoin blockchain ledger.

**Figure 7: Simplified Blocks of Transaction (Narayanan et al., 2016)**



## II.6 Blockchain Categories

This dissertation adopts the definition of blockchain by Mougayar (2016) as “*a technology that permanently records transactions in a way that cannot be later erased but can only be sequentially updated, in essence keeping a never-ending historical trail.*” As such, immutability is the defining attribute of blockchains. Therefore, except for immutability, which must be present in every blockchain, the rest of the attributes exist at varying degrees (Coletti,

2015; DeRose, 2015; Pilkington, 2015). The key attributes of blockchain technology are distributed ledgers, cryptography, consensus mechanisms, and peer-to-peer transmission (Guo & Liang, 2016; Tsai et al., 2016). It is, therefore, a meta-technology that integrates several technologies to form a gestalt—greater than the sum of its parts (Mougayar, 2016).

There are different flavors of blockchains with diverse sets of attributes (Pilkington, 2015) and varying levels of control that define categories of blockchains. Table 5 illustrates a typological distinction between the main categories. These different categories provide flexible trust-based services (Lindman et al., 2017) as will be further elaborated later. Each blockchain is a standalone database with varying levels of access and control. Public blockchains are unconditionally accessible by every Internet user (Buterin, 2015; Pilkington, 2015). At the other end of the spectrum, access to an entirely private blockchain is controlled by a central locus of governance (Buterin, 2015; Pilkington, 2015). In between the public and private dichotomy, there is a continuum (Allison, 2015; Brown, 2014; Pilkington, 2015) of permissioned, hybrid, or partially decentralized blockchains (Buterin, 2015; Pilkington, 2015).

**Table 5: Categories of Blockchains—Adapted from (Guo & Liang, 2016)**

	<i>Public Blockchain</i>	<i>Consortium Blockchain</i>	<i>Private</i>
Participants	Anyone	Specific groups	Centrally controlled
Credit mechanism	Consensus Mechanisms	Collective endorsement	Self-endorsement
Bookkeeper	All participants	Participants decide	Self-determined
Incentive	Needed	Optional	Not needed
Prominent advantage	Self-established credit	Efficiency and cost optimization	Transparency and traceability
Prominent advantage	Self-established credit	Efficiency and cost optimization	Transparency and traceability
Typical application	Bitcoin	Clearing	Audits
Load capacity	30-20 times/second	1000-10000 times/second	Varies

### III APPLICATION: FINANCIAL TRANSACTIONS

Analogous to how the digital wave disrupted the telecommunication industry, blockchain technology is emerging as a FinTech paradigm shift (Guo & Liang, 2016) that promises to enhance the efficiency of financial transactions and to transform the global financial network altogether (de Meijer, 2015). Leaders of the financial industry expect the technology to disrupt the sector. A 2016 survey conducted by McKinsey unveils that approximately 50 percent of the executives in the financial industry are confident that blockchain technology will have a significant impact within three years (Guo & Liang, 2016; McKinsey, 2016). IBM pronounced that 66 percent of banks will have a scalable blockchain-based deployment by the year 2020 (Fortune, 2016; Guo & Liang, 2016; Zhao et al., 2016). Such predictions demonstrate that change is imminent and may materialize within the next few years. Furthermore, the financial industry has already begun to undergo a technological revolution (Accenture, 2015; Kiviat, 2015). To move from general notions of the impact of blockchain technology on financial transactions, we focus on four specific issues that play indispensable roles across financial transactions. These are asset verification, record keeping, data privacy, and transaction costs. The relevance was explained earlier in Table 1 in relation to the three phases of any transaction described by Workie and Jain (2017): 1) the initiation phase, where a client accesses the blockchain network to buy or sell financial assets 2) the verification of financial assets in the blockchain database by involved intermediaries and stakeholders, and 3) the recording of the information into the blockchain ledger.

In this chapter, ‘transaction costs’ have a broader meaning to include transaction costs from Transaction Cost Theory as well as production costs (Dyer, 1997) (Dyer, 1997; Zajac & Olsen, 1993). In addition, we touch upon transition costs of moving from current technologies in financial transactions to a blockchain-enabled environment.

### **III.1 Asset Verification**

The first activity in trading a financial asset on a blockchain network is to verify specific attributes of the asset (Workie & Jain, 2017). The asset verification involves confirming that the parties who seek to exchange are the legitimate owners of the corresponding assets (FINRA, 2017). Ownership according to Stephen Pair, CEO of BitPay, is established when some entity recognizes, documents, and defends the rights of someone over an asset (Tapscott & Tapscott, 2016). As such, blockchain technology can facilitate direct ownership verification by virtue of a consensus mechanism (Workie & Jain, 2017) that is already agreed upon by all participants. The confirmation of the ownership of the asset in the blockchain network is carried by a single full node that constructs the block that encompasses the asset information and is also corroborated by other full nodes in the network which continuously verify the validity of every new block and the overall veracity of the whole ledger. The strength of the blockchain stems from that fact that no single custodian—full node—has control over the entire ledger at any time (Rechtman, 2017). Instead, it is akin to a majority rule. The apparent risk here is when a single entity controls over 50 percent of the custodians of the network (Rechtman, 2017). Whether that is likely or not depends on the operational environment.

The immutability attribute of blockchain data makes it possible to store information indefinitely in its database. Subsequently, this elevates the level of trust in the veracity of assets information on a blockchain. Furthermore, immutability leads to traceability (Mori, 2016) because blockchain contains verifiable timestamped records of every asset ever transacted in blockchain (Crosby, Pattanayak, Verma, & Kalyanaraman, 2016). Therefore, by virtue of its built-in native audit trail, blockchain technology is readily available to verify assets (Rechtman, 2017). As such, asset verification becomes viable and possibly more reliable using blockchain technology. On the other hand, immutability means that it is not possible—especially in a public

blockchain—to fix a mistake pertaining to an asset by editing the database. Instead, one must append the corrected representation of the asset in a new block. Therefore, immutability affords traceability and reliability; nonetheless, it makes it difficult to fix mistakes and human errors.

Due to the nature of its distributed ledger, it is arguable that blockchain built-in redundancy is helpful in significantly reducing the risk of losing assets information (Rechtman, 2017). Hence, compared to centralized databases, blockchain is more reliable and fault-tolerant because clones of the database—chain or ledger—are maintained by multiple network nodes (Mori, 2016). If most of the network nodes go down, the network will continue to verify records uninterrupted since the database is available in many other nodes and the consensus mechanism is independent of the number of operational full nodes. Nevertheless, redundancy comes with the price of taxing resources in terms of storage and processing requirement.

In any case, a decentralized consensus mechanism requires significant infrastructural and operational expenses in areas of communication networks, computation, and storage to operate a chatty transactional financial system (Tsai et al., 2016; Yli-Huumo et al., 2016; Zhao et al., 2016). Moreover, it requires effort to integrate blockchain-based asset verification, at scale, with the financial legacy platforms and processes; and to enhance the capabilities of blockchain technology to meet the requirements of the financial industry (Tsai et al., 2016). Financial systems, for the most part, require high throughput and speed—stock exchanges execute over 100K transactions per second that may require asset verification; hence, blockchain technology must be able to handle these types of loads. Moreover, Tsai et al. (2016) state that since the blockchain protocols are executed sequentially, it is difficult to meet the financial industry requirements no matter how much computational power is added, especially that blockchain network is inherently slow because it is peer-to-peer, which means that each node needs to act

both as a client and a server. However, some people such as Mougayar (2016) argue that scalability is a moving target that has, historically speaking, been met by technological innovations and by the pressure of imminent demand.

From a compliance point of view, before deploying a blockchain-based network, there are several regulatory rules concerning asset verification that broker-dealers need to devise ways to comply with. Some of these asset verification requirements are established by FINRA and Exchange Act Rules (FINRA, 2017). Furthermore, for a global blockchain covered by heterogeneous jurisdictions, the task of asset verification from a regulatory framework is further complicated (Mori, 2016).

### **III.2 Record Keeping**

Record keeping is to resiliently and accurately preserve past information through time in a manner that satisfies involved parties (Witte, 2016)—precisely what blockchain technology does by design, and as such, blockchain technology is capable of keeping records (DuPont & Maurer, 2015). Furthermore, the technology could have a significant impact on record keeping (Kiviat, 2015) since it alters centrality and reshapes governance (Guo & Liang, 2016). Currently, financial institutions keep records across disparate databases, unlike a shared blockchain ledger which affords a central repository where records are accessible by all participating institutions.

Guo and Liang (2016) asserts that many of the financial sectors' problems stem from a) poor quality of records needed for assessing individual credit, b) inability to share records, c) lack of utilization of external sources of records such as the Internet data, and d) difficulties of meeting compliance requirements related to customers' records such as know your customer (KYC). According to Moyano and Ross (2017), the annual costs of KYC due diligence per bank is up to 500 million dollars. They further conclude that financial institutions should collaborate

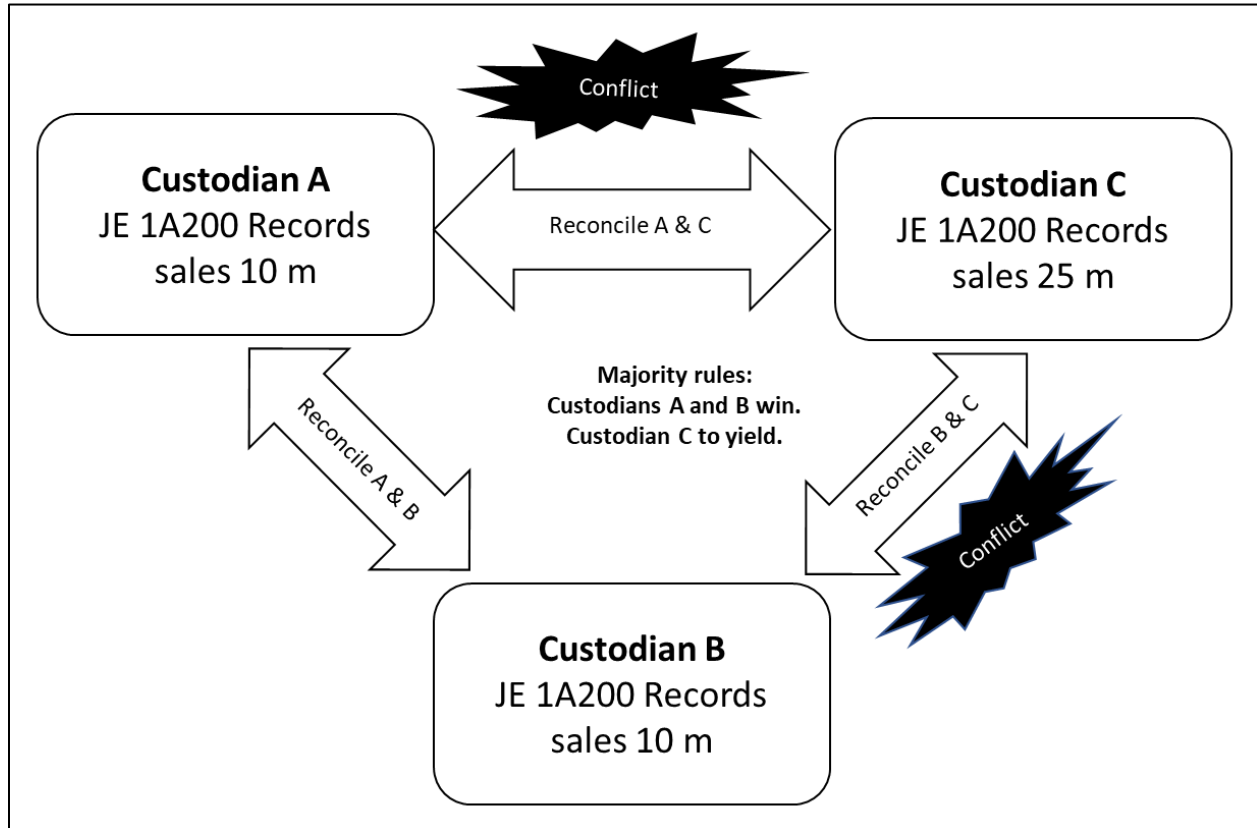
among themselves, and other stakeholders, to develop blockchain-based record keeping systems to address these weaknesses. Such blockchain networks could be permissioned (private with appropriate access control) to allow financial institutions (exchanges, central banks, banks, and insurance firms) to enhance reputability, accountability, and controllability (de Meijer, 2015) by computationally, efficiently, and seamlessly keep records across the financial value chain (Kiviat, 2015). Nonetheless, to achieve this desired vision for record keeping, financial institutions need to agree on what records to share, how to contribute to the cost of building and maintaining the network, and how to manage access control.

A record of information stored on a blockchain ledger attains further veracity over time, and as such, blockchain technology is well positioned to be the source of truth, the provider of accurate records, and ultimately, the platform for trust and record keeping due to its immutability attribute and consensus mechanisms (DuPont & Maurer, 2015; Mori, 2016). Consequently, blockchain technology can natively, seamlessly, and more transparently afford robust audit trails of records of dividend disbursements, ownership details, stock split terms, stock transactions timestamps, taxes reports, and compliance reporting requirements (Rechtman, 2017). Therefore, blockchain technology is a readily available reporting infrastructure (Workie & Jain, 2017) and is impactful to auditing and monitoring (Kiviat, 2015) requirements and practices desired by financial institutions and regulatory bodies. To attain this collaborative record keeping interface, it would require building the appropriate tools and processes. Additionally, inasmuch as blockchain data is immutable and irreversible, the industry must innovate solutions for how to address issues that may arise from erroneous human or platform record entries (de Meijer, 2015). Furthermore, there need to be considerations of computational resources for maintaining a blockchain's growing ledger (Workie & Jain, 2017) that is redundantly stored in multiple nodes.

However, the risk here is likely insignificant grounded on Moore’s law that computing storage and Central Processing Units (CPUs) tends to get cheaper and faster, thus allowing cheaper record keeping and faster record retrieval. Furthermore, if we envision a future permeated by machine-to-machine type of transactions, then when pushing the blockchain technology towards the internet of things (IoT) periphery, the current blockchain techniques are generally not appropriate since IoT devices work with low computational power and are limited to tiny amounts of energy consumption (Atzori, 2016; Zhao et al., 2016).

According to Rechtman (2017), to guard against fraud and errors, financial custodians keep records independently, and if a conflict arises between records during reconciliation, then the majority win—Figure 8 illustrates the reconciliation process. It is arguable that blockchain’s single truth can afford seamless records reconciliation.

**Figure 8: Records Reconciliation (Rechtman, 2017)**



In late 2015, Nasdaq finalized the first-ever private security record keeping over its blockchain, thus leading to a significant reduction of settlement time and the elimination of paper stock certification records (Nasdaq, 2015). Some of the financial sectors that could seek to utilize blockchain technology to enhance their record keeping practices are a) equity markets, where the current process require a slow and manual tracking of records of shares ownership, b) debt markets, where the current settlement time is long and involves multiparty, c) repurchase agreements, where currently there is risk of settlement failures and lengthy settlement time, d) corporate bonds, where blockchain technology could digitize the records of assets and codify the necessary calculations, e) derivative market, where records transparency could aid both regulators and participants currently struggling to conduct and monitor the intricate post-trade records and activities, and f) customer identity management, where a shared blockchain records could provide a centralized repository to ease the task (Workie & Jain, 2017).

Again, there are regulatory requirements that need to be met by a blockchain-based deployment vis-à-vis record keeping. For instance, broker-dealers have to comply with recordkeeping compliance requirements such as Exchange Act and FINRA rules that mandate the minimum length of time for keeping the record, establish the required type of records, and detail accessibility to attestations (FINRA, 2017).

### **III.3 Data Privacy**

Data privacy is an essential aspect in financial transactions because customers care about their data privacy, and consequently, businesses must care as well since it makes good business sense to care about the wants of the customers. Besides, financial institutions must comply with regulatory mandates around data privacy. We could think about data here to mean two things: a) content data that pertains to transactions and the like and b) identity data that provides

information about the users of a blockchain network. Furthermore, privacy and transparency are two desired outcomes, but sometimes they conflict. While individuals usually care more about their privacy than transparency, the collective typically cares more about transparency.

Blockchain technology can paradoxically and flexibly swing between a continuum of high degree of transparency—decentralization of a public blockchain ledger makes the data more accessible (Yli-Huumo et al., 2016)—and high level of privacy (Narayanan et al., 2016)—pseudonymity of users of Bitcoin and similar blockchains is made possible by a lack of a central authority that governs the network users as well as by its built-in cryptography. The level of data privacy and transparency depends on whether the blockchain network is public, private, or a hybrid, in addition to other operational architecture issues—see Table 5. Furthermore, the level of transparency is also a function of the how the data is stored in the network since it is possible to encrypt the data before sending it to the network. However, if access control is not managed well, it can lead to dire consequences (Rechtman, 2017). Besides, although blockchain technology could reduce security and privacy risk, it could introduce new issues because of the decentralized nature of blockchain network (Workie & Jain, 2017). For example, safeguarding private keys is of amplified importance in a public blockchain network. Although stealing private keys from a blockchain network user is akin to stealing passwords from users of non-blockchain users, the subtle difference is that if a password is forgotten, in decentralized blockchain network, it is impossible to retrieve private keys due to the absence of a central authority.

Some people express concerns that bitcoin and similar blockchains could be used for illegal activities encouraged by the anonymity of the users. However, as detailed by Narayanan et al. (2016), Bitcoin blockchain is pseudonymous—network identities could be traced to real-world identities. Also, the culpability of cryptocurrency to criminal activities is not more than

cash. Furthermore, since blockchain data is immutable, the fact that there is a permanent trace of activities on the ledger could be discouraging to criminals (Tapscott & Tapscott, 2016).

Workie and Jain (2017) aver that innovative technologies, when operating in alignment with the goal of achieving market integrity and protecting investors, could enhance access, efficiency, and transparency. However, they go on to state the need to augment blockchain technology with policies that address privacy objectives such as a safeguarding “*personally identifiable information and trade strategies*.” Moreover, they assert that private blockchain networks could exclude non-network participants from access to data and, therefore, reduce the level of transparency.

In the views of Guo and Liang (2016), one of the problems facing the financial sector stems from the lack of definition of privacy and security terms vis-à-vis ownership of user data. It is arguable that the design philosophy of blockchain technology is founded on enabling users to control their transactions and their data. Therefore, many blockchain technology advocates such as Tapscott and Tapscott (2016) call for shifting towards a society where users are in full control of their data. It is not clear if financial institutions will tilt towards the direction of less centrality in controlling users’ data.

The area of user data is further complicated due to regulatory requirements such as KYC, Anti-Money Laundering (AML), and customer data protection (FINRA, 2017). Nonetheless, the lack of clarity of regulatory and compliance requirements create uncertainty for financial institutions when assessing blockchain technology with consideration of privacy and transparency requirements. Moreover, since a blockchain network could cross the boundaries of multiple jurisdictions, financial institutions must contemplate how to satisfy privacy and transparency regulatory requirements in these different jurisdictions. Besides, financial

regulators are still comprehending the implications of blockchain technology (Kiviat, 2015). For example, the definition of finality in current settlements is radically different from the protocol-based consensus mechanism in blockchain networks (Mori, 2016).

#### **III.4 Transaction Costs**

Past technological advancements had conceived substitutes that consequently intensified the degree of competition. For instance, Internet financial products have encroached upon the market share of traditional financial institutions (Guo & Liang, 2016). In order to survive and meet ever-increasing customer's demands, the financial sector must continuously innovate (Guo & Liang, 2016; Zhao et al., 2016) and attenuate transaction costs (Zhao et al., 2016) through the deployment of new technologies. Hence, blockchain technology has been touted as the innovation engine for financial areas such as clearing and settlement, payment systems, operational risks, and insurance (de Meijer, 2015; Kakavand & Kost De Sevres, 2016; Peters & Panayi, 2016; Zhao et al., 2016).

Currently, interbank payments often pass through intermediary clearing houses where they get scrutinized through complicated, time-consuming, and expensive processes (Guo & Liang, 2016). The technology, according to de Meijer (2015) may reduce the cost of transactions and increase their speed in the areas of business-to-business payments and peer-to-peer remittance market; and could help in reducing the cost of the securities sector embodied by exchanges and traditional banks. Nonetheless, from an implementation perspective, Workie and Jain (2017) state that blockchain technology players, rightfully, focus on discrete applications that target current pain points of significant inefficiencies with a vision of implement the solutions gradually rather than adopting wholesale changes. A somewhat related point is made

by Mougayar (2016) who avers that it is easier to adopt decentralization from scratch versus from centralized systems.

Although blockchain technology could allow long-term cost reduction, in the short term some upfront expenditure is required to develop a blockchain-based infrastructure. Taking the payment sector as a major candidate for innovation through blockchain technology, in the year 2013 and 2014, 5.4 billion dollars was invested in FinTech innovation (Kiviat, 2015) with the anticipation that blockchain technology could revolutionize the infrastructure and lead to new business models (de Meijer, 2015; Lindman et al., 2017) that could consequently generate more value and save cost. According to a 2016 World Economic Forum report, the investment in exploring financial applications of blockchain technology exceeded 1.5 billion dollars (Workie & Jain, 2017).

In addition to the payment and clearing area, the technology could decrease transaction costs related to credit information (Guo & Liang, 2016) and significantly reduce the amount of time of settlement (Tapscott & Tapscott, 2016) enabling near real-time settlement due to its network-based consensus mechanism, resulting in saving days of delay. However, the adoption of blockchain real-time settlement would require a departure from established procedures for lending and borrowing securities and the practice of conducting trades when the market is open during specific hours of the day (Mori, 2016). Blockchain technology could automate the back office operations in the area of clearing and settlement, and decrease the transaction costs related to authentication of trading records by making them transparent to all participating parties (de Meijer, 2015). Another target area of transaction costs reduction through the deployment of blockchain technology is private equity exchange. To exemplify, NASDAQ established a startup called chain.com to furnish a blockchain-based platform for private equity exchanges (Crosby et

al., 2016; Zhao et al., 2016). One of IBM's goals is to utilize blockchain technology in order to reduce coordination costs in capital markets and to streamline settlements in derivatives markets (Coindesk, 2017b). In supply-chain finance, blockchain technology could reduce costs of financing by automating manual processes and attenuating legal risks through smart contracts (Guo & Liang, 2016).

McKinsey estimates that blockchain technology could a) reduce the cost of a cross-border transaction from 26 dollars to 15 dollars, b) lower the annual operational costs by as much as 15 billion dollars, and c) reduce the annual cost of risk by as much as 1.6 billion dollars (Guo & Liang, 2016). A FinTech report estimates that blockchain technology will allow banks to save as much as twenty billion dollars in areas of cross-border payments, securities trading, and regulatory compliance (Mori, 2016; Oliver Wyman, Anthemis Group, & Santander Innoventures, 2015).

Some researchers suggest that the deployment of blockchain technology alone will not lead to significant reduction in transaction costs. For instance, Mori (2016) asserts that 80 percent of the challenges in the financial industry are attributed to business models and processes, and only 20 percent are attributable to technological hurdles. That means introducing blockchain technology alone is not enough. To be effective, such efforts must be coupled with fundamental changes of established process and business models.

Blockchain technology could potentially permeate all sectors of the financial industry. Its impact will include private securities, insurance, Internet finance, and other financial sectors (Wang, Chen, & Xu, 2016). However, in accordance with systems development best practices, Tsai et al. (2016) suggest deploying blockchain features in modular and insular forms, with each module targeting a specific functionality such as accounting, or trading, but not both.

Furthermore, the value of centralization itself should be carefully assessed as stressed by Auctus\_Team (2017) who warns against forcing blockchain technology as a substitute for addressing problems that traditional centralized databases can solve sufficiently well.

## IV PERSPECTIVE: STAKEHOLDER VIEWS

As one of the three pillars of the dissertation pluralist methodology, we have interviewed sixteen participants with expertise in blockchain technology and the financial industry. The views of the stakeholders augment the literature review presented above, and both chapters will be analyzed later through the lens of transaction cost theory. Six of the participants held executive roles in financial institutions, five were researchers, and five were subject matter experts. The diversity of views provided a number of opportunities, challenges, and recommendations regarding blockchain technology and its impact on financial transactions. In this chapter, we synthesize the participants' perspectives with a focus on asset verification, record keeping, data privacy, and transaction costs. The views are grouped into four areas: transaction issue, technological issues, regulatory issues, and adoption issues. As mentioned earlier, in this chapter 'transaction costs' have a broader meaning to include transaction costs in the sense of Transaction Cost Theory as well as production costs (Dyer, 1997; Zajac & Olsen, 1993); in addition, we touch upon transition costs of moving from current technologies to a blockchain-enabled environment.

### IV.1 Transaction Issues

Participants agreed that financial services are based on trust. Hence, when a transaction transpires between two parties, the financial intermediary verifies the asset, records the transaction, and ensures that both parties are served satisfactorily: "*When buying shares, financial institutions guarantee delivery of those shares and the agreed upon payment to the corresponding parties. Even if one party defaults, financial institutions absorb that risk by delivering to the other party.*" Consequently, the intermediary financial institution charges a commission for the service. The above scenario exemplifies the type of trust-based service

blockchain technology will have to deliver if it were to play a role in asset verification and record keeping.

*“Visa today takes 3% of the transaction fee if you pay at a Walmart. Inherently, Walmart will include that in the price since most of the transactions are credit card based,”* said one of the participants. Financial institutions also incur high costs when they go through intermediaries: *“Clearinghouses trade trillions of dollars daily. They charge a commission for each transaction. Although it is an extremely tiny commission, with millions and millions of transactions, banks have to pay substantial amounts.”* Blockchain technology could afford opportunities to attenuate these types of costs. Current financial institutions have been closely linked to central banks, partially for regulatory purposes. Stock exchanges, brokers, and banks participate in assets verification and record keeping in a manner that is inefficient as it takes a long time and uses significant human resources. Some participants believed that blockchain technology would reduce transaction costs: *“You have to stitch so many different things and pour millions of dollars. If you have blockchain architecture, this cost will drastically reduce, because everything is connected.”* Another participant advocated using blockchain technology as a means *“to support transactions across geographical distances without a very heavyweight institutional arrangement.”* Nevertheless, others see the phenomenon as *“full of hype and euphoria with real potential for only a few use cases.”* Along similar lines, a financial executive participant stated that *“blockchain technology opportunities are limited because of the way the whole asset industry is structured right now. Change is not happening, it would require quite a bit.”* Nonetheless, the majority of participants believed that blockchain technology will further elevate that level of network-based trust and furnish a better platform for verifying assets, keeping records, protecting data privacy, and reducing transaction costs: *“Blockchain technology can*

*codify something of value and assign it a proof of authorship or a proof of ownership, and that becomes a digitally codified asset. Which when put on the blockchain will be immutable, meaning everybody can publicly verify it via a search and authenticate who owns it, at a specific timestamp.” Given that it could be shared publicly, at a much lower transaction cost than we do today.”* Another participant expressed the current issue with transaction costs as follows: *“Today in banking for example, if you own a credit card, if you pay merchandise from Walmart, the payment has to process through a number of channels, first of all, the card issuer: e.g., Bank of America. Also, the transaction has to pass through different payment networks such as Master Card.”*

A few of the participants pointed out that, in some regards, we now trust computers more than people as exemplified by Uber: *“I will get in a car with somebody in the middle of the night that I have never met before. Still, I completely trust that the Uber driver has been vetted well enough by the network.”* Blockchain exemplifies such networks that are capable of asset verification and record keeping concerning reputational data. However, like every newly introduced technology, blockchain is not fully charted waters as expressed by one of the participants: *“It is so fascinating, and we still do not understand it. We still do not understand some of the negative.”*

Some participants compared the inevitability of the permeation of blockchain-based financial transactions to what some countries in Africa and South-East Asia have done regarding cellular technologies as *“they leapfrogged western economies such as the USA or Canada. I could send money from one person to another person, in Kenya five years back. The USA is now trying it out. Now all the banks are doing it.”* Hence, it is quite possible to leapfrog with blockchain technology, not hindered by all the regulations or all the legacy technologies. For that

reason, “*some of the venture capitalists think the next Apple or Google will come from the blockchain world.*” Nonetheless, some participants posited that just like the Internet promised to decentralize and ended up moving in a different direction, blockchain technology will not deliver on all its promises. For example, the current transaction fee structure in a Bitcoin and similar blockchains has not fulfilled its promises of allowing microtransactions at low cost. Moreover, the quest of decentralization itself could prove to be elusive “*It is frequently the case in human history that people think that anarchy is a good idea, but it turns out that every time that power is put in the hands of people, we end up coalescing into some centralization.*” Blockchain mining pools is an example of how we are trending towards centralization as time passes.

Many participants saw inadequacy in the number of transactions per second—throughput—despite some promising consensus-based mechanisms. Therefore, they suggested that the technology is not ready for prime time for financial transactions. In the USA some banks have 35 million customers or more. In China or India, some banks have over 100 million customers. It is a daunting task for a blockchain to handle that type of volume in real or semi-real-time: “*Imagine, you are at a cashier, and instead of only Visa approving your transaction, every participant has to approve it, verify its authenticity, and get to unanimity.*” Those are the type of challenges that need to be overcome computationally before blockchain technology could be adopted widely. Developers have to come up with algorithms that meets current processing standards because “*when customers go to Walmart, they have expectations that their cards will be approved in less than 30 secs.*” Contrarily, one of the participants pointed out that although instantaneously processed, Visa and similar settlements take several days in the backend.

Payments fall into two buckets. The first bucket is consumer payments which are person to person, person to commercial, commercial to commercial, and commercial to person. The

second bucket is treasury payments, and that is bank to bank. The payment sector uses the SWIFT (Society for the Worldwide Interbank Financial Telecommunication) platform to carry interbank payment instructions. In the SWIFT network one bank could connect directly to another bank, or the case could be it must go through an intermediate bank to exchange the payment information with another bank. No one bank is connected to all the banks. Those intermediaries collect transaction fees. Going through the SWIFT hub is essential since regulations mandate banks to know who is on the other end of the transaction. Nevertheless, treasury payments are not slow because of the speed of SWIFT. The speed issue could be due to banks holding on payments to check certain things. To resolve these issues, SWIFT is being replaced by a new platform called SWIFT GPI (Global Payment Innovation). SWIFT GPI is an improvement over SWIFT since it mandates filling some of the payment fields such as the tax rates. Moreover, participating SWIFT GPI banks must meet certain service level agreements. Against this backdrop, participants in payments sector had no high anticipations from blockchain technology in the treasury payments area since SWIFT GPI is resolving speed and transparency issues. Additionally, the issue with speed concerning treasury payments is not technological but a liquidity issue: *“It is bit of a falsehood to think money is flowing all the time, because unless value passes from one place to another”* via central banks, *“it does not really happen. The limitation is business days and time zones. Commercial banks are governed by their central banks and central banks close. That is a critical component to how fast you can go when you go around to the other side of the planet.”*

It is not straightforward to compare the costs of transactions that are blockchain-based versus those that are not. For example, factors that contribute to a transaction costs stemming from a Visa payment are radically different compared to a cryptocurrency payment—

computational energy, fees, and so on. Therefore, *“transaction costs should be viewed on a use case basis and cannot be generalized.”* Moreover, use cases differ. For example, *“if it takes me X amount of dollars to send one bitcoin from one party to the other, that is different from transacting a bond. When you start looking at it that way, you also have to look at matching architectures.”* Asset verification and record reconciliation are not simple, and according to a participating financial executive, this is where blockchain technology could make a difference: *“Let us take Apple shares for example. At any point in time, we need to know who has assets or equity in Apple because we need to have the correct info to be able to pay dividends, taxes, tax rates, etc. Keeping track of that is very tricky. Therefore, reconciliation is very complex, and something takes long. That is where blockchain technology might make a difference.”*

Some participants advocated using blockchain technology for internal operations concerning record keeping, asset verification, and data privacy protection: *“It does not have to be a public or peer-to-peer in the consumer sense. They can use blockchain technology just within their ecosystem and start using distributed computing as the way to securely store private information.”* For example, record keeping, and asset verification processes could indeed take advantage of blockchain technology: *“hedge funds try to verify assets. They use excel sheets. Many things are messed up.”* On the other hand, some participants argued that blockchain technology is more effective in attenuation transaction costs in large multiparty context: *“Blockchain technology brings down transaction costs for large multiparty transactions where many institutions and people come together such as stock exchanges and the DTCC. For internal system concerned with record keeping, inventory management, and the like, there has not been much blockchain-based application development.”*

Potentially, blockchain technology could introduce a massive change regarding how we would interact with capital markets: *“The way to raise capital today is either you through investment banks as a company or through private placements with institutional investors. Tomorrow it is going to be a blockchain environment.”* Another participant echoed views along the same lines: *“In the USA alone, only 55% of the people have access to the stock market, and these types of new technologies are going to socialize finance.”*

Before applying blockchain technology to enhance asset verification, record keeping, data privacy, or transaction costs, it must prove its advantage over established technologies: *“You use blockchain technology in a use case that is very centralized. Besides, if your system does not require any trust because it is a single company, then you probably do not need blockchain technology.”* Finally, one of the participants stressed the need to objectively contemplate the dichotomy of centralization versus decentralization without taking sides. *“I listened to Vitalic Buterin—the founder of Ethereum—and he realizes that there is just as many good people and just as many bad people in both the cryptocurrency world and the banking industry.”* Table 6 highlights the summary of this section.

**Table 6: Industry Perceptions of Transaction Issues**

<i>Opportunities</i>	<i>Challenges</i>	<i>Recommendations</i>
Blockchain technology can reduce transaction costs and improve asset verification and record keeping	Blockchain technology is uncharted waters in the area of financial transactions	Deploy blockchain technology only when it adds value relative to established transaction technologies
Blockchain technology can improve efficiency of record reconciliation	Current capabilities of blockchain platforms do not meet all financial transaction requirements	Deploy blockchain technology for large multiparty transactions
Blockchain technology can increase access to finance and capital markets	Financial institutions find it difficult to understand the impact of blockchain technology for financial transactions	Compare blockchain versus non-blockchain transaction costs on a use case basis
Blockchain technology can enable leapfrogging, especially in developing economies	It is difficult to compare costs of blockchain transactions to non-blockchain transactions	

## IV.2 Technological Issues

*“Most processes are semi-manual, and therefore the sector is looking for ways to optimize, automate, streamline, and make transactions faster while maintaining the same level of security,”* said one of the financial executives while stressing that it is becoming increasingly difficult to generate satisfactory profit. Most participants believed that blockchain technology could play a major role in improving the processing of financial transactions. According to one of the participants, some studies show if blockchain technology is used as an infrastructure, transaction cost will decrease anywhere between 25 and 75 percent. However, a few participants stated that blockchain technology is meager as architecture or that *“it is hype more than better technology.”* Moreover, financial transaction systems are not just a single system that could be

simply replaced by a blockchain-based system. They are multiple interconnected systems. Consequently, one of the participants posited that *“there would not be a chance for a disrupter to come and change the way things are set up. Few people would even understand what we do.”*

An executive from the insurance sector described a use case which illustrates how blockchain technology is being implemented to enable asset verification, record keeping, data privacy and transaction costs attenuation: Today when two people get into an auto accident with each other, their proof of insurance is paper insurance cards. The coverage could have been canceled. To improve the process of proof of insurance, *“we developed a plugin that goes into Geico’s or Allstate’s mobile APP.”* To exchange insurance information, the two people tap their phones together to access *“the policy blockchain to get verification of current coverages.”* Moreover, in the future, authorities could get a feed from the state department of motor vehicles of licensed motorist and compare that to that policy blockchain and be able to identify uninsured motorist proactively. The policy blockchain is a private blockchain *“accessible by participating insurance carriers, insurance distribution firms, and brokers.”* It uses ‘proof of authority’ as a consensus mechanism—the level of access is based on the user’s identity. When the two drivers tap their phones together, they get a temporary access to each other’s data. Although the ledger is distributed, some of the data is hashed such that participating institutions can only see what they want each other to see. Blockchain technology allows different degrees of so-called zero-knowledge proof, whereby one can, for instance, prove she had a private data at an earlier time without revealing its content. For instance, *“if I want to confidentially prove that I have the idea on a certain date, I would hash it and put the hash on the blockchain. Later, if someone says I have the idea, I can prove that I had the idea by showing its timestamped hash on the blockchain, and ‘unhash’ it with my public key.”*

There will always be cryptography researchers working on developing better encryption methods. Contrarily, there will always be cryptography researchers looking for ways to break encryption. Part of that is driven by the tension between privacy and transparency where, for instance, the government believes that it has good intentions when finding ways to break the current methods of encryption: *“Government wants to have more visibility, and citizens often want more privacy. That ongoing is not just related to blockchain technology.”* Additionally, hackers also play a role in breaking cryptography, and consequently, push researchers to find stronger cryptography schemes: *“There is no model that humans can build that has perfect encryption. Also, in the next 50-100 years, we might see quantum computers that will break all methods of encryption we currently have. With the advent of AI (Artificial Intelligence), there might be better encryption built with AI. Nevertheless, there could also be better ways to break the cryptography by AI.”* When someone breaks a hash function, we stop using it and come up with a stronger one. Breaking a hash function does not mean that hashed data could be inverted. Even after a hash function is ‘broken’ it is still useful for checking data integrity. It is almost not possible to recreate the original piece of data. Hence, breaking a hash function is not a danger to privacy or the data integrity. However, *“we run the risk of the hash losing its proof of prior knowledge of something”* as we have explained above.

Another intriguing area related to privacy is identity. There are personal identity data and user-generated data. Many participating subject matter experts believed that blockchain technology allows users to control the use of their data: *“Self- sovereign identity means if it is my identity, I should be empowered to share it with whomever I want, whenever I want, but only limited to whomever I want. The government can attest to my identity and can authenticate it but at the end of the day it is my identity.”*

Especially with public blockchains, another security issue is *“the risk of losing passwords”* or private keys since no central authority exists to allow retrieval of private keys. As such, backing up and storing private keys is crucial. Doing so, however, might compromise these private keys. When implementing blockchain technology, in addition to the costs of building up the blockchain network and employing blockchain technology experts, there are also security costs. It is not clear if blockchain technology security costs are higher than with current systems: *“Currently they have to safeguard the database. So, they are facing similar issues. However, with blockchain technology, cybersecurity may be of a different nature. People cannot take over the blockchain, but if they can steal your keys, they can wreak havoc.”* Blockchain by itself is phenomenally secure, is hard to hack, and even if someone manages to get closer to that, the system can upgrade to a different cryptographic protocol and keep it more secure: *“Breaking in the blockchain is very remote. I do not foresee that happening in the near future. All the stories about someone stealing Bitcoins or hacking Ethereum are because of bad coding or bad ways of saving private keys.”*

All participants agreed that scalability is a significant technical challenge. Therefore, although we have touched on scalability in previous sections, we will treat it here for further details. Blockchain is *“centralized and fully decentralized at the same time. Therefore, it takes long to validate transactions since it has to be one truth and it has to be distributed so that everybody has access to it at the same time.”* It is not easy for an entire large network, through a consensus mechanism, to agree to a single record. That is one of the reasons it is difficult to achieve high throughput. Nonetheless, *“there are several proposals to increase that.”* For example, Bitcoin is testing a proposal called ‘lightning’ where transactions could be verified on ‘sidechains’ and bundled together then pushed to the main blockchain as a single record. In

addition to the speed issue, blockchain networks that use proof of work type of consensus mechanisms require much energy consumption. Nevertheless, *“there are many other mechanisms such as ‘proof of stake’ that are faster and more energy friendly.”* For private blockchains, scalability is less of an issue since the networks are smaller. Another challenge with scalability is the sheer size of the blockchain. Blockchain is sequential: *“When you have a huge number of transactions every second, then the size of blockchain can grow to become unmanageable.”* That also results in *“fewer people being willing to store the entire blockchain,”* thereby weakening some of the advantages of decentralization. Ethereum has a proposal called ‘Plasma’ with the idea of storing only part of the blockchain. Of course, there must be a way to access the full history when needed. Furthermore, some of the participants reasoned that space is *“not a big issue because we have already seen solutions in the past such as light nodes that do not need to store the full blockchain.”* Besides, *“memory and hard disk space are cheap these days.”* From a strategic scalability perspective, *“it is hard to be aware of all the different flavors of blockchains in an arms race to see who can provide better features.”*

The blockchain ledger could accept unstructured data which could pose a technical challenge since bad data could go in without governing rules. In a structured database, *“there are some rules codified in the database, which make sure that the data that goes in is pure and pristine. Blockchain has no such rules.”* The issue is especially concerning when considering the immutability nature of blockchain records: *“In a public blockchain it is hard to go back and modify the record because one has to get agreement from everyone.”* That is precisely what happened when Ethereum had to split into ‘Ethereum Classic’ and ‘Ethereum’ since people could not agree on whether to rectify the record or not after a hacking incident. In a permissioned blockchain, it could be manageable for participating parties to agree to modify the record.

Notwithstanding that challenge, this dissertation adopts the core definition of blockchain as being immutable. Immutability, on the one hand, is an advantage because nothing is ever lost. On the other hand, as we mentioned earlier, it taxes the network computational resources. Many of the participants advocated storing data into the blockchain ledger only when there is a need for immutability and keeping the rest in a different database that could be accessible by the blockchain network. Some of the participants went further to express reservations regarding using blockchain as a database: *“Many people try to turn it into a database. Blockchain should not be used as a database, is not made to be one, and is not very good one if you try to use it that way.”* Using blockchain as a database is *“basically wasting space.”*

A best practice adopted by a consortium led by one of the participants was to build a reusable blockchain framework that can *“accelerate the building of applications on top of this framework.”* Leaders of a consultancy recommended staying platform agnostic: *“We see advantages in being platform agnostic and have the choice between all different platforms. We believe that there are use cases for every one of them.”* Each blockchain platform has its technical advantages and disadvantages. For example, Ethereum is suitable for smart contracts while Ripple is a better fit for payments. As such, a participant who led a consortium averred that building an interoperability layer is vital: *“One of the things that we have built into our blockchain framework, and again this is very bleeding edge, is an interoperability layer.”*

Table 7 highlights the technical opportunities, challenges, and recommendations related to blockchain technology in the space of financial asset verification, record keeping, data privacy, and transaction costs.

**Table 7: Industry Perceptions of Technological Issues**

<i>Opportunities</i>	<i>Challenges</i>	<i>Recommendations</i>
Blockchain technology could further automate many financial transactions processes	It is hard to keep up with the technical features of different blockchain platforms	The need for immutability qualifies if the data should go into blockchain or not
Blockchain records are stored redundantly and cryptographically secure, making it hard to lose or hack	Provisioning access in a permissioned blockchain is complicated	Access provisioning schemes are critical for competing entities to be comfortable with having data in a common blockchain
Blockchain affords a central collaborative repository for record keeping	Hash functions are almost guaranteed to be broken in the future	Build the blockchain framework in a manner that is extendable to broad use cases
Blockchain can fit the desired shades of privacy and transparency	Blockchain throughput is currently not adequate for some financial applications	Remain blockchain platform agnostic
Blockchain enables users to control their private data	It is not possible to retrieve lost private keys in blockchain	Device secure practices for storing blockchain private keys

### IV.3 Regulatory Issues

Since it deals with public money, the financial sector is “*one of the most regulated industries in the USA.*” Regulations are essential to protect the public from being subject to misguidance, robbery, “*Ponzi schemes,*” and other types of mischiefs. Although blockchain can be used to bypass regulations and intermediary financial institutions, participants argued that no matter how the technology is developed, it “*will end up landing somewhere in a jurisdiction*”

Some laws will be federal, and others will be state laws: *“In the European Union (EU), there will be federal laws at the EU level, and there will be laws specific to each country.”* As such, blockchain technology will be regulated like other financial services technologies where regulations vary greatly from country to country with *“some common denominators to account for global concerns such as KYC and AML.”* Regulating blockchain technology could, therefore, be challenging and *“confusing because the beauty of decentralized networks is not having borders, although we still have borders and live in physical places. There are rules and taxes that we cannot just end on a dime.”* In any way, some of the participants cautioned against overregulation: *“Overregulation is not good because it stifles innovation.”*

The technology is still new and evolving making it difficult for the regulators to have a good grasp of how it works: *“The problem is that the regulators themselves do not understand how cryptocurrencies or blockchain technology works. This is a new and evolving technology.”* From a regulatory point of view, there are two schools of thoughts: the first advocates pushing new laws right now; the second advocates waiting and monitoring patiently to see what type of new laws will be required. Which school of thought prevails *“depends on what the technology ends up facilitating.”* It also depends on if ‘catastrophic’ events transpire as exemplified by one of the participants: *“It is only a matter of time. In 2008 banks went bankrupt. The regulations were missing certain areas that caused the collapse of the banks. Then the government bailed out the banks causing a massive loss for the economy. It took more than ten years to recover.”* Hence, right now the regulators ought to start thinking how to regulate blockchain technology and in what form without crippling innovation. A US-based participant argued that the state of regulatory uncertainty is hurting the growth of blockchain technology: *“The largest problem is the regulatory framework. The USA is behind. Uncertainty is hurting blockchain technology.”*

*Only 12% to 18% ICO (Initial Coin Offering) is based in the USA. The country waited for too long.*” Nonetheless, some participants expected regulations to solidify in the coming one or two years: *“In the range of a one or two-year timeframe we could expect to see some regulatory guidance and control in place.”*

Current regulations have been tailored for a *“financial ecosystem that we have developed over the past 100 to 200 years.”* The regulatory framework will have to adapt to the new financial practices we are creating. Regulations typically lag innovation: *“Regulations are always two phases lagging behind the maturity of the technology.”* Moreover, regulations take time: *“There are many approvals required, notices of proposed rule meeting—meaning making regulations based on feedback from the industry—or passing bills such as the Dodd-Frank Act.”* Still, in some blockchain-related areas, we already have some regulations: *“There are pockets of cryptocurrency or blockchain technology where there are regulations right now.”* For instance, Bitcoin futures are now listed on Chicago Mercantile Exchange and Chicago Board of Exchange—both are well respected financial institutions that are regulated by the Commodity Future Trading Commission.

When asked whether incumbents or startups will spearhead blockchain technology, executives in the financial industry answered in favor of the former. They reasoned based on regulations: *“Regulatory requirements are the biggest hurdle for a blockchain-based alternative provider to be a disruptor and start offering services as we do.”* Incumbents already adhere to a comprehensive set of regulatory and compliance requirements. As such, their answer implicitly averred that blockchain-based services would be heavily regulated. One of the participants illustrated the challenge facing new entrants as follows: *“Google or Amazon tried to develop their own bank. Their CEO admitted that it was more complicated than they thought it would be.”*

*That was just plain vanilla capital banking or commercial banking. I do not think they could venture into corporate banking, investment banking, the whole payment industry, or securities.”*

Financial institutions spend a large part of their budget on compliance. Some participants stated that compliance costs are by far the primary cost factor: *“We spend more money and time on people who look after compliance than we spend on people who serve clients.”* As such, blockchain technology could potentially attenuate the compliance-related processes, and therefore, significantly reduce financial transaction costs. The idea is to store customer’s information into a shared blockchain ledger instead of each financial institution vetting every customer on their own: *“Blockchain technology is a fantastic way to comply with KYC. All you have to do is to put the data on the blockchain, and anyone can use an App to verify.”* Of course, this should be done in compliance with regulations governing customer data privacy.

Blockchain technology can be used for positive and negative purposes. Some participants expressed concerns about using its cryptocurrency for illicit activities such as *“drug trafficking, arms smuggling, or any illegal activity such as requesting ransom payments.”* At some point in time *“China banned Bitcoin. Banning is not a solution, but you need to have effective controls to avoid illegal activities.”* North Korea, given the type of scrutiny put on its transactions, is allegedly channeling money through Bitcoin and other cryptocurrencies. Hence, the recent appreciation of cryptocurrency is partially attributed to higher demand generated by North Korea and the like.

When computers and the Internet sprung into existence, there was a need for some regulatory arrangements to allow authorities to snoop on suspects’ hard disks and online activities to check for illicit activities such as child pornography and terrorism. There might be *“a need for some extra sort of blockchain sensors”* to achieve similar objectives. In any case, the

nature of privacy-related regulations “*will vary greatly from country to country, from Estonia where everything is on blockchain, to countries where they will take many years before doing anything.*”

Blockchain technology could challenge some of the established data privacy norms. For instance, today, in the USA, three credit bureaus have the oligopoly on credit scores of people: Equifax, Experian, and TransUnion. If the USA has something like Lithuania’s identity management blockchain, anybody can check out credit scores and other details. That will be a significant change to how asset and record verification are conducted. Furthermore, the presence of blockchain technology could surface some renewed regulatory questions: “*Who authorized Equifax to collect data on me?*” Equifax, Experian, and TransUnion are not governmental entities; they are private companies. What are the users’ rights “*regarding Equifax securing their identity?*” “*Who authorized Equifax to share their data?*” and “*What do they gain from Equifax sharing their data?*” Users may gain access to services by virtue of their identity information being shared. However, there are no direct monetary benefits to the user. Hence, blockchain technology can alter the landscape of credit rating agencies: “*People can even obtain a return from their data. That would affect the business model of credit rating agencies and may reduce their profits. They might even cease to exist.*”

One of the participants explained the regulatory framework surrounding blockchain-based financial transactions as follows: “*Mycelium is a smartphone App that taps into Bitcoin blockchain.*” A person could be living anywhere in the world and be able to send and receive money to anyone anywhere. Having Mycelium is akin to having a global bank account “*without having to go to a place and give my photo ID or registration. I just downloaded the app.*” That puts a different burden on regulators since today, “*regulators are used to work through the*

*banks.*” As such, regulators have shifted the burden of enforcing the prohibition of activities such as money laundering to the banks. The authorities just audit the bank’s ledger. With the presence of Mycelium, the regulators must pivot, change, and adapt to a different way of looking at transactions. Hence, KYC is no more like a person going into a place giving her identification card. KYC in the future *“will mean who is downloading the information? What is the serial number of the device? To whom is the device registered?”* There will be an expanded network of things coupled with a rich web of activities that the authorities could tap into to know the customer. The authorities will have to crawl these different pieces of information and stitch them together to get a reasonable picture of the customer.

Nivaura, a UK-based company, *“just a few weeks ago issued the first regulated bond in collaboration with the British regulator.”* Nivaura resolved the technical aspects and engaged the regulator to agree to two things: 1) this is a financial instrument that lives in a public blockchain, and 2) it is a legal instrument, meaning that parties involved in the transaction have legal obligations they must adhere to (if not, one party could drag the other into the court of law). This is an illustrative *“example of innovative companies engaging with regulators to expand the regulations in a way that makes sense in this blockchain real world”* related to asset verification, and record keeping. A different example refers to the ‘proof of insurance’ example detailed earlier. In this case, the road had already been paved from a regulatory standpoint since every state in the USA had already agreed to honor electronic verification of proof of insurance. Notwithstanding other use cases could summon more restrictive requirements from regulators, especially with regards to data privacy, asset verification, and record keeping.

Finally, blockchain technology could offer a collaborative platform that is also helpful to authorities in terms of streamlining the reports required by the regulators from financial

institutions: *“It is a big arduous task for them to gather that information across various back office systems. If you have the information on the blockchain, you could very easily create a use case to do all that regulatory reporting very quickly and cut out many working hours required for that.”* Table 8 summarizes the perceptions of the industry stakeholders on regulatory issues concerning the impact of blockchain technology on financial transactions.

**Table 8: Industry Perceptions of Regulatory Issues**

<i>Opportunities</i>	<i>Challenges</i>	<i>Recommendations</i>
Blockchain technology can reduce financial transaction costs related to compliance	Blockchain technology is new and evolving, making it hard for regulators to grasp	Regulators should guard against overregulation so as not to stifle innovation
Blockchain offers an immutable trail of records to authorized auditors	The state of regulatory uncertainty is hurting the growth of blockchain technology	Regulators should adapt to emerging paradigm shifts in financial transactions
Blockchain-based platforms can furnish a streamlined and collaborative reporting infrastructure	Blockchain-related regulations will vary across jurisdictions, challenging the borderless nature of blockchain	Innovators should collaborate with regulators to back their products with authoritative power

#### **IV.4 Adoption Issues**

The current financial ecosystem operates based on well-established processes and methods of transaction. With the introduction of blockchain technology, we can transact, verify assets, keep records, and protect data in a decentralized fashion with fewer intermediaries and fewer loci of control, thus, enabling a consumer-to-consumer web of transactions. Nonetheless, some participants questioned some of the core value propositions of blockchain: *“To say you have a private blockchain, why even have a blockchain? Why not just have encrypted hard drives?”* Other participants countered: *“Who will maintain the common central database? You*

*have several banks, and each has its own interests. A central party, such as a stock exchange, will have monopoly power and will charge other parties. Blockchain technology allows decentralized environment management without relying on a central party.”* Depending on how compelling the new technology is, the availability of resolutions of some of the challenges, and the degree of willingness to embrace, the financial transactions ecosystem might adopt the emerging technology at varying rates and degrees or might reject it all together. One of the participants averred: *“The current ecosystem is not sophisticated enough to fully disintermediate. It may take 10 to 20 years to get there. Will there be a pure peer-to-peer transaction? That depends on the use cases and the relative value it creates.”*

The RiskBlock is an insurance consortium. They use a social concept called ‘proof of collaboration’ to encourage and monitor the effectiveness of blockchains shared among a number of highly competitive insurance companies that are typically cautious about how much information they share with each other and how much they work together: *“One of the first hurdles that we had was to be able to prove that these competitors could come together on these various solutions and work together.”* Regardless of the quality of the underlying solution, a shared blockchain would not be useful if participating parties are not willing to work together: *“It does not matter how good the proof of insurance is if it is one-sided.”* From a data privacy perspective, the starting point is public blockchain where everyone can see all the data records, although they may not see the identities of who are conducting the transactions. However, financial institutions do not want all their data to be public: *“Some of them are legally bound from disclosing all their data.”* Even if the data is encrypted, there is a risk that *“someone could break the cryptography or reverse engineer the data.”* The successful adoption of the RiskBlock for asset verification, record keeping, and data privacy protection is driven by the demonstration

of immediate benefits to the participating parties such as “*reduced cost, enhanced efficiencies, customer service improvement, and greater revenue.*” As such, consortiums must focus on bringing true production value to their members: “*Our motto is 'no science experiments' such as proof of concepts and standalone projects that never make it into production.*”

“*No organization wants to be a dinosaur when significant changes transpire,*” said one of the participants. Large financial service providers are, therefore, exploring blockchain technology by typically building pilot projects on top of the Ethereum public blockchain platform where implementations may be private, or may utilize some other framework such as Hyperledger—an open source blockchain technology development consortium. Many financial institutions have their in-house research teams. For instance, Bank of America, one of the biggest banks in the USA, has already filed for more than twenty-five patents in the area of blockchain technology. A participating financial executive stated that incubating blockchain technology projects is inevitable because “*I fear that something might come along with blockchain technology that I did not see, and I lose positioning.*” Another participant echoed views along marketing lines: “*Every bank in London has blockchain technology projects, mostly so they can just say they have one.*” Even technology giants such as IBM, Microsoft, and Oracle offer various implementations of the technology. However, many of the implementations are exploratory in nature: “*Blockchain technology projects are fairly small-scale operations, and for the most part it is more about trying to figure it out.*” Financial institutions are hesitant to spend heavily or build their own new private network within their organizations since: “*CTOs, CIOs, and CFOs are waiting until blockchain technology is mature before they spend the money.*” Nevertheless, there are high anticipations of growth: “*I envision that in the next couple of years,*

*the growth will speed up, and people who initially doubted blockchain technology will realize its potential.”*

Some sectors are more advanced in their roadmap than others: *“The Australian stock exchange is going to move all their settlement on blockchain making it much more efficient. The verification will depend on cryptography. The transaction will ensue instantly.”* The participant continued: *“Traditional financial transactions such as stocks and bonds will still take place on established stock exchanges such as Nasdaq or NYSE (New York Stock Exchange), but they might move their settlement to a blockchain.”* Senegal and Tunisia already have their currencies on blockchain. Singapore and China are thinking about coming up with national digital currencies *“because of the transaction cost. It will boost the GDP by 3 to 4 percent just by replacing 30 to 40 percent of the national currency with cryptocurrency due to the reduction of friction.”*

Blockchain-based startups will force incumbents to reduce transaction costs: *“Visa and MasterCard are now a duopoly in the payment sector. If we have many other options then, especially internationally, they have to reduce their fees drastically to remain competitive.”* In essence, startups are innovating. However, established financial institutions are not sitting still. As such, *“blockchain technology will disrupt many businesses like how Apple changed the Newsweek.”* Overall, *“the winner might be the customers because they will enjoy better service, faster transactions, more transparency, and to some extent they will be more in charge of their own data and their own assets.”* Nonetheless, it is difficult to realize the possibilities of a new technology as exemplified by one of the participants: *“In my daily routine, when I ask operation people: Can blockchain technology apply to this or that? The answer is always no.”*

As an adoption roadblock, the dichotomy between privacy and transparency is not a technical issue but a business choice concerning the balance between confidentiality and verifiability: *“If you encrypt data, then you increase privacy and confidentiality, but you lose transparency and verifiability. This tradeoff will always be there. There is no technical solution to that. It is a business decision.”* Public blockchain networks allow high degrees of anonymity but *“we cannot have a system where people do things completely anonymously.”* There are different blockchain networks with different objectives from a privacy perspective. ‘Zcash’ and ‘Monero’ are the type of blockchain networks that claim to offer full privacy protection. However, participants believed that no blockchain is fully anonymous because one could track transactions back to a user’s activities and patterns. Concerning asset verification and privacy, all participants believed that it is easier to track blockchain-based transactions than tracking cash transactions.

A general challenge is how to maneuver the idea of blockchain technology *“in an aligned way of using it within the existing system and then in a radically new way of pulling things apart so you can do things in new ways.”* Overall, adoption is more concerned with desired business outcome than with technology: *“I would be more interested in getting a technology that helps me measure and manage liquidity. If a specific technology makes that possible, I will buy.”* The fate and rate of adoption, therefore, hinges on creating relative value out of the technology. Consequently, viable ecosystems emerge around the technology: *“Without the ecosystem, the technology itself is just sitting in a lab.”*

Another significant challenge is how to settle around standards that all the industry players will adopt. There are consortiums such as the R3 consortium and the Ethereum alliance. They sometimes call themselves a financial institution or a standard, but the adoption of which is

not unanimous. For example, *“Goldman Sachs used to be part of R3, then they left later probably because they have different goals.”*

There are several adoption challenges related to maintenance and governance: *“In a private blockchain network, who should be an admin?” “If any dispute occurs, who resolves it?” “Who manages the blockchain infrastructure?” “If a new version is out, who is responsible for release management?”* These are the type of challenges financial executives must think about when planning to adopt blockchain technology.

A participant explained a framework for adopting blockchain smart contracts in which blockchain technologies could be used for two types of smart contracts. The first type is a simple encounter smart contract that is evoked repetitively. The second type is relationship smart contract that attempts to solve ongoing equivocal problems that might need intermittent human interaction. As such, the adoption of blockchain smart contracts becomes more accessible by thinking about them as partially automated: *“Enabling them to get on with the job as much as possible and to only interact with them when needed.”* As such, smart contracts could be adopted faster by making a conscious decision to *“codify more into the automatic part and less into the human part. To solve an equivocal problem, it might need more human assistance.”*

A participant recommended adopting blockchain technology in a controlled way: *“As a banker, rather than jump in, which could bring numerous problems I could not think of, I would cautiously watch the technology as it matures, then adopt it in a controlled way. Banks deal with billions of dollars. The accountability and penalties are extremely high.”* Some participating consultants offer a strategic path for adoption: *“The technology is evolving and improving so fast. So, it is a strategic decision to invest now while it is still developing to gain a head start.”*

The summary of this section is found in Table 9.

**Table 9: Industry Perceptions of Adoption Issues**

<i>Opportunities</i>	<i>Challenges</i>	<i>Recommendations</i>
Adopting blockchain technology reduces reliance on central authorities that may charge service fees	It is hard for financial institutions to adapt to collaborating and sharing information with competitors	Invest early while blockchain technology is still developing to gain competitive edge
The growth of blockchain-based startups forces incumbents to innovate and reduce transaction costs	Financial institutions will unlikely invest heavily in blockchain technology before it is mature	Demonstrate tangible relative value of blockchain technology projects and consortiums
Adopting blockchain technology reduces opacity, increase speed, and democratizes users' data	It is hard to settle on standards for blockchain transactions that all industry players will adopt	Align blockchain technology with established systems while exploring radical innovative ways
Partial adoption of cryptocurrency reduces friction and increases a nation's GDP	The benefits of adopting blockchain for internal transactions are not clear	Adopt blockchain technology in a controlled way
The dichotomy between privacy and transparency is a business decision, not a technical limitation		Device sound plans for governance and maintenance of the blockchain

## V THEORY: TRANSACTION COST ANALYSIS

In this chapter, we add a theoretical perspective on the impact of blockchain technology on financial transactions by applying transaction cost theory to analyze the insights from our literature review and stakeholder perceptions. Tapscott and Tapscott (2016) provide a general transaction cost analysis of blockchain technology independent of industry. We build on and extend their work by presenting a transaction cost analysis for financial transactions. Specifically, we explore the transaction cost theory activities comprising searching, bargaining, and controlling (monitoring and enforcement) (Hennart, 1993; Husted & Folger, 2004; Williamson, 1985) to shed light on how the adoption of blockchain technology will affect the transaction costs related to asset verification, record keeping, and data privacy. We also go beyond the analysis of Tapscott and Tapscott (2016) by examining not only where blockchain technology attenuates transaction cost but also where it increases transaction cost. Finally, to compare transaction costs between traditional technologies and blockchain technology, we assume that the blockchain network is already up and running. This assumption allows us to avoid the complications in comparing sunk costs that are related to established technologies with implementation costs that are related to deploying blockchain technology.

Transaction cost theory is concerned with the costs of transactional activities that are not directly attributed to the production of goods and services but are instead associated with the cost of searching, bargaining, and controlling activities that accompany the transaction of goods and services (Husted & Folger, 2004). Owing to the benefit of competition, transaction cost theory assumes a priori that markets are more efficient than hierarchies (Geyskens et al., 2006) and then moves on to define when hierarchies are better. Coase (1937), the founder of transaction cost theory, established that vertical integration into hierarchies applies when transaction costs are lower compared to the forces of free markets. The theory was further developed by Williamson

(1985) specifying contracting between the firm and its stakeholders—customers, employees, partners, creditors, and suppliers—as the focus of analysis (Milgrom & Roberts, 1992).

According to Ouchi (1980), transaction costs appear primarily due to the difficulty of evaluating the goods or services that are transacted. As such, transaction costs in Ouchi's view are due to activities that advance the goal of guaranteeing the expectations of the exchange participants. He further posits that the difficulty in achieving such a goal may be attributed to lack of trust between the parties. Williamson posits that transaction costs are determined by:

- 1) Frequency, meaning how often a contract is invoked (Milgrom & Roberts, 1992; Williamson, 1979).
- 2) Asset specificity, referring to whether the asset could be deployed to a different purpose (Husted & Folger, 2004; Klein et al., 1978; Williamson, 1979), and therefore, raising the concern of goal incongruence (Ouchi, 1980) which is defined as the degree to which parties to an exchange have incompatible objectives (Husted & Folger, 2004).
- 3) Uncertainty, comprising *ex ante* difficulties of anticipating all future scenarios, language equivocality (Milgrom & Roberts, 1992; Williamson, 1975), and *ex post* performance ambiguity concerning the difficulty of measuring performance (Ouchi, 1980) or in other words, the metering problem related to the intricacy of assessing the level of contribution of each individual or entity to a joint effort (Alchian & Demsetz, 1972; Husted & Folger, 2004; Milgrom & Roberts, 1992).
- 4) Bounded rationality, positing that people have limited ability to store, process, and retrieve information (Simon, 1955; Williamson, 1973).
- 5) Opportunism, exemplified by dodging duties, breaching agreements, and stealing (Alchian & Demsetz, 1972; Husted & Folger, 2004; Williamson, 1979).

## V.1 Searching

Searching costs involve ex-ante activities (Husted & Folger, 2004) that are related to gathering information to support transactions such as identifying counter partners (Dyer, 1997), verifying assets, searching for information related to KYC, and gathering reputation data to assess credibility. Tapscott and Tapscott (2016) list three distinctive characteristics concerning blockchain technology search: 1) in a blockchain realm, the user can control the level of their privacy, 2) unlike the Internet which tends to present information that is unreliable, perishable, and abundant, blockchain information is tamperproof, permanent, and not as abundant, and 3) information on a blockchain is not just a snapshot at a specific time, it is a chronological account or a state machine in the words of Mougayar (2016). As such, we proceed to cover how each of the above blockchain technology attributes affects the searching cost in financial transactions.

First, from a data privacy perspective, by virtue of blockchain technology empowering customers to control their data, customers can enter their correct expansive identity record elements, hence, arguably increasing its veracity and richness. Consequently, credit reporting agencies would not need to extensively search multiple data sources to draw an accurate view of the customer's profile. In this way, the cost of searching blockchain is lower in terms of human power and effort since credit reporting agencies do not have to search disparate data sources that might have a lower quality of records or conflicting records of information. As such, it is helpful to service providers who according to Guo and Liang (2016) suffer from poor quality of records needed for assessing individual credit. Hence, Guo and Liang posit blockchain technology could decrease 'searching' transaction costs related to credit information. On the other hand, it is also arguable that due to opportunism, users being in charge of presenting their own data may falsify their records or be less transparent about them. Consequently, searching risk costs could increase by requiring more expenditure in searching multiple reputational elements to arrive at

appropriate user risk profile assessments. Since users of a blockchain, especially a public one, could be pseudonymous, the cost for searching users' private data could also increase in this case. Moreover, some of the data entered by the users could be encrypted making it impossible to search or use without the permission of the user, thus, incurring additional searching costs. In a blockchain, the data is phenomenally secure and conserved; however, if someone loses their private keys, then there is not a way to retrieve the password. Consequently, it is plausible that users who lose their private keys would create new identifications, and therefore, generate multiple profiles, resulting in increased costs of searching due to duplications and fragmentation of their data. Searching costs could also increase if people, empowered by blockchain technology, choose to monetize their identity data and their content data. In any case, Workie and Jain (2017) posit that blockchain technology eases customer identity management due to its shared, centralized repository.

Second, blockchain records are tamperproof, permanent, and less abundant. Being tamperproof attenuates the likelihood of opportunistic behavior exemplified by participating entities attempting to falsify records, therefore, increasing the cost of searching for data elements to verify assets and keep records. When the information is less abundant it decreases the effect of bounded rationality, and consequently, reduces searching cost for asset verification and record keeping, as well as the search of users' private data—a similar conclusion reached by Williamson (1975) who avers that the ease of verification is critical to the operation of capital markets. One of the reasons blockchain records and private data are permanent is immutability. Immutability of the blockchain records increases the fidelity of the information on the blockchain. Once a search for a particular record at a specific timestamp is run, the results will always be valid. Therefore, no costly repetitive search is needed. In addition to immutability, the

permanence of blockchain data is also guaranteed by the nature of its distributed ledger, since, compared to centralized databases, blockchain ledger is more reliable and fault-tolerant owed to the clones of its ledger that is maintained by multiple network nodes (Mori, 2016). If most of the network nodes go down, the network will continue to verify records uninterrupted since the database is available in many other nodes and the consensus mechanism is independent of the number of operational full nodes. Therefore, the built-in redundancy could significantly reduce the risk of losing records and private data (Rechtman, 2017). As such, the cost of inability to search records is reduced owed to lack of risks of downtime due to failure or congestion.

Third and finally, blockchain is a state machine, meaning that events or records are chronologically and immutably documented on the blockchain ledger. In this context, immutability means it is impossible to correct past records on the blockchain. As such, the immutability of records and private data could increase searching cost since one has to search for the latest update of the record, which could have multiple versions of it. This is especially true in a public blockchain where a high degree of goal incongruence could make editing a past blockchain record extremely difficult since it requires the consensus of many participants. In private blockchains, goal incongruence is arguably less, hence, it might be easier for participating entities to align around a protocol on how to edit or purge records.

To illustrate searching transaction costs analysis, we turn our attention to two financial transaction activities: record reconciliation and KYC. Blockchain technology could significantly help record reconciliation—a combination of asset verification and record keeping. The savings in searching costs associated with reconciliations are significant as corroborated by the stakeholders perspective asserting that blockchain technology would help reconciliation: *“Let us take Apple shares for example. At any point in time, we need to know who has assets or equity in*

*Apple because we need to have the correct info to be able to pay dividends, taxes, tax rates, etc. Keeping track of that is very tricky. Therefore, reconciliation is very complex, and something takes long. That is where blockchain technology might make a difference.*” According to Rechtman (2017), to guard against fraud and errors, financial custodians keep records independently (Figure 8). Therefore, it is necessary to search the records of all custodians and compare them to make a manual judgment call concerning a reconciliation decision. Assuming individuals and parties are opportunistic, have different goals, and act with bounded rationality, searching for reconciliation is costly. Contrarily, the veracity of the data on a blockchain is automatically corroborated by all nodes of the network and is shared as a single truth across the whole network. When recording an asset, the whole blockchain network automatically corroborates the new entry. Consequently, record reconciliation becomes a seamless activity. Therefore, blockchain technology significantly attenuates searching activities vis-à-vis record reconciliation.

As a second illustration, the annual costs of KYC due diligence per bank are up to 500 million dollars (Moyano & Ross, 2017) and Guo and Liang (2016) stress the difficulties faced by financial institutions in meeting KYC compliance requirements. Along the same lines, our participants suggested that blockchain technology could significantly reduce searching costs related to KYC: *“Blockchain technology is a fantastic way to comply with KYC. All you have to do is to put the data on the blockchain, and anyone can use an App to verify.”* However, some of the participants argued that blockchain technology will change the nature of searching where KYC in the future *“will mean who is downloading the information, what is the serial number of the device, to who is the device registered, and so on.”* In this case, financial institutions would have to crawl these different pieces of information to stitch them together to get a reasonable

picture of the customer, arguably increasing searching costs. Some participants suggested blockchain technology might even shift the KYC burdens from financial institutions to government authorities. If this prediction transpires, it would mean increased searching costs for the authorities, but reduced searching costs for the institutions. It is unclear whether the KYC due diligence will remain with the banks or shift to the authorities; however, it is likely that the nature of searching for KYC information will change with blockchain technology. Further searching costs could be incurred due to pseudonymous behavior by some customers as we have explained earlier in this section. Table 10 summarizes searching transaction costs related to blockchain-enabled financial transactions.

**Table 10: Searching Transaction Costs**

<i>Effect</i>	<i>Cause</i>
Attenuated transaction costs	Immutability of the blockchain records increases the fidelity of its information
	Blockchain technology allows users to enter their own correct expansive identity data elements allowing credit agencies to reduce the need to corroborate data from multiple sources
	Blockchain data is less abundant resulting in reducing the effect of bounded rationality
	With blockchain technology, searching and verifying assets are redundantly reliable and accessible
	Blockchain technology eliminates the need for searching to reconcile records
	Blockchain technology could significantly reduce searching costs related to the current KYC process
Increased transaction costs	Immutability of blockchain data makes it difficult to correct past records
	Users in charge of their own data may opportunistically falsify their records or be less transparent about them
	Users of a blockchain, especially a public one, could be pseudonymous
	Some of the data entered by the users could be encrypted
	Users of a blockchain could choose to monetize their identity and content data
	Blockchain is more prone to the duplications and fragmentation of users' profiles when users lose their private keys
	If the nature of KYC changes by blockchain technology, financial institutions or authorities would have to crawl more pieces of information

## V.2 Bargaining

Bargaining transaction costs are related to negotiating, contracting, determining, devising, and arranging the steps to be taken and the terms of exchange when conducting business with others (Dyer, 1997; Husted & Folger, 2004; Milgrom & Roberts, 1990). As such,

in a blockchain-based financial transaction realm, bargaining takes place with customers concerning matters of access to private data and services and with partners when cooperating on a shared blockchain—partners could be collaborators or competitors. Accordingly, we proceed to cover three areas to examine the differences between bargaining costs with or without blockchain technology. The areas are bargaining with partners, bargaining with customers, and smart contract as a prominent blockchain native feature that is specially related to bargaining.

First, we examine partnering bargaining costs. Workie and Jain (2017) suggest that blockchain technology is helpful where financial transactions involve multiparty in areas such as repurchase agreements when there are risks of settlement failure—an assessment corroborated by participants: *“Blockchain technology brings down transaction costs for large multiparty transactions where many institutions and people come together such as stock exchanges and the DTCC.”* In a blockchain realm, partners share a ledger with predefined consensus mechanism, agreed upon shared records, and code-based asset verification process. Consequently, the blockchain environment has reduced frequency, higher goal congruence, lower performance ambiguity, and less effect of bounded rationality. Therefore, parties sharing a blockchain enjoy attenuated bargaining costs of negotiation and renegotiations: A participant aver that the technology *“supports transactions across geographical distances without a very heavyweight institutional arrangement.”* Moreover, if the shared ledger was designed with high level of transparency, the result is further reduced performance ambiguity and opportunism since negotiations between partners are anchored on accurate records and realistic expectations. Arguably, the reverse holds true—a blockchain that emphasizes privacy results in higher performance ambiguity and opportunism. Therefore, we conclude that the higher degree of transparency of a blockchain, the less the transaction bargaining costs. To illustrate, we revisit

our ‘proof of insurance’ earlier example. The policy blockchain is a private blockchain “*accessible by participating insurance carriers, insurance distribution firms, and brokers.*” It uses ‘proof of authority’ as a consensus mechanism—the level of access is based on the user’s identity. In this case, insurance carriers require significantly less bargaining effort to be able to settle an accident between two of their policyholders.

Second, we examine bargaining with customers. Inasmuch as blockchain users are able to control their data, additional bargaining costs between the customers and the financial institutions are expected so as to be able to convince customers to share their information, or even buy the information in the case of some customers desiring to monetize their identity information: “*Self-sovereign identity means if it is my identity, I should be empowered to share it with whomever I want, whenever I want, but only limited to whomever I want.*” Since we have concluded earlier that the ability of the users to control their information will improve the veracity, richness, and access to their private identity data, it is arguable that due to decreased uncertainty, bargaining costs between customers and financial institutions will decrease. For example, credit and insurance rates are easy to bargain provided accurate, rich, semi-real-time telemetry data based on accurate user profile data or drivers record. It is also plausible that the richness of private data and the flexibility to share which type of private data elements will result in a decreased asset specificity of the user’s identity data elements a product in itself. Therefore, bargaining transaction costs will decrease.

Finally, smart contracts is a prominent native feature of blockchain technology—digitally drafting and automatically enforcing transactions instead of arduous human interventions (de Meijer, 2015; Yli-Huumo et al., 2016; Zhao et al., 2016). A contract is “*a framework that is a highly adjustable and almost never accurately indicative of real working relations, but a guide in*

*cases of doubt or conflict*” (Llewellyn, 1931; Williamson, 2008). Williamson posits that contracts are never complete due to 1) environmental uncertainty owed to the unpredictability of future contingencies (Geyskens et al., 2006), 1) behavioral uncertainty stemming from performance ambiguity ex-post (Milgrom & Roberts, 1990), 3) language equivocality where the more detailed the contract, the more likely it contains ambiguous clauses (Milgrom & Roberts, 1990), and 4) bounded rationality (Simon, 1955; Williamson, 1973). Compared to traditional contracts, when constructing a smart contract, heftier negotiation costs obtain since smart contracts are code-based with less room for future flexibility needed to accommodate for future uncertainty, bounded rationality, and challenges concerning the conversion of equivocal language into algorithms (Simon, 1955; Williamson, 1973). Therefore, with a smart contract people might be more reluctant to commit to a code-based that is perceived to be a rigid contract, and if they do, it will take significant effort to agree to the terms and the translation of the terms into an algorithm. Furthermore, since a smart contract has to account for every scenario, it is arguable that more burdensome upfront negotiations costs obtain. Nonetheless, once a smart contract is deployed, no future renegotiations costs are expected, and therefore, not costs of renegotiations are incurred. To summarize, Table 11 illustrates the bargaining transaction costs as they relate to the impact of blockchain technology on asset verification, record keeping, and data privacy.

**Table 11: Bargaining Transaction Costs**

<i>Effect</i>	<i>Cause</i>
Attenuated transaction costs	In a blockchain realm, partners share a ledger with predefined consensus mechanism, agreed upon shared records, and code-based asset verification process
	It is possible to design a blockchain with a high level of transparency
	The ability of the users to control their information improves the veracity, richness, and access to their private identity data, leading to a decreased uncertainty
	The richness of blockchain users' private data and the flexibility to share which type of private data elements results in a decreased asset specificity of the user's identity data elements
	Blockchain smart contracts require no future adjustments
Increased transaction costs	It is possible to design a blockchain with a high level of privacy
	Inasmuch as blockchain users are able to control their data, financial institutions need to convince customers to share their information or even offer to buy
	Preparing a smart contract requires heavy bargaining costs

### V.3 Controlling

Control costs are ex-post transaction costs related to monitoring and enforcing predetermined obligations to ensure their fair fulfillment or to respond to the breach thereof by any party (Husted & Folger, 2004; Milgrom & Roberts, 1992). In a blockchain-based financial transaction ecosystem, control costs comprise costs such as tracking assets, monitoring records, ensuring the protection of private data, enforcing AML laws, and policing the execution of financial contracts.

We first explicate the reasons blockchain technology could be designed as a readily transparent control platform (Workie & Jain, 2017; Yli-Huumo et al., 2016), hence affecting the controlling costs of auditing, monitoring (Kiviat, 2015), and enforcement requirements and

practices desired by financial institutions, government authorities, and regulatory bodies. First, as we have explained earlier, blockchain timestamps events and records (Crosby et al., 2016). As such, owing to the dimension of chronology, it impacts controlling costs due to the effects on performance ambiguity, opportunism, and bounded rationality. Second, by design, blockchain transactions are immutable and tamperproof (Mougayar, 2016; Wang et al., 2016), thereby, affecting opportunism. Third, blockchain ledger is “*centralized and fully decentralized at the same time*,” thus, impacting goal incongruence and asset specificity. Fourth, blockchain technology employs code-based consensus mechanisms (DuPont & Maurer, 2015; Mori, 2016), and consequently, impacting controlling costs determinants of frequency, goal incongruence, and performance ambiguity. Finally, blockchain technology has smart contracts as a native feature (Auctus\_Team, 2017; Mougayar, 2016), therefore, impacting the effects of frequency, uncertainty, bounded rationality, and opportunism. Next, we cover each one of the above attributes in relation to financial transactions controlling costs.

First, the impact of timestamping on transaction controlling costs could be explicated by a scenario where a customer initiates a transaction to buy a specific financial asset. Owing to the timestamp of the event and the timestamp of the value of the asset, it would be possible to cross-verify the value of the asset at that exact timestamp, and therefore, less transaction controlling costs are incurred due to the reduction of opportunism—where, for example, the seller could opportunistically claim an asset value at a different timestamp—or bounded rationality behavior. Likewise, user private data is readily available to be visualized as time series, hence, reducing the costs of monitoring activities stemming from performance ambiguity.

Second, by design, blockchain transactions are immutable and tamperproof. Any opportunistic modification of the historical data record is detectable by participating blockchain

network nodes (B. Lee & Lee, 2017; Tapscott & Tapscott, 2017). Evidence that is tamperproof reduces litigation transaction costs incurred by parties that are involved in a dispute.

Furthermore, immutability leads to traceability (Mori, 2016) due to the verifiability of every record ever transacted on a blockchain (Crosby et al., 2016). Contrarily, in blockchains with a high level of privacy such as Monero, and Zcash, pseudonymous behavior by users could raise the costs for authorities to control illicit activities such as AML. On the other hand, blockchain being immutable, it is arguable that controlling costs associated with blockchain exchanges are less than cash exchanges since a permanent trace of activities on the ledger could be discouraging to criminals (Tapscott & Tapscott, 2016). From the regulators perspective, they are “*used to work through the banks.*” In a blockchain world, regulators might absorb the burden of enforcing the prohibition of activities such as money laundering. In such cases, financial institutions would enjoy less controlling transaction costs while the authorities would incur additional transaction controlling costs.

Third, blockchain ledger is “*centralized and fully decentralized at the same time.*” As such, it has built-in redundancy leading to less transaction controlling costs attributed to the loss of access due to network downtime or congestion. Moreover, a blockchain ledger is a single source of truth (Pilkington, 2015) that is shared across the whole network. Therefore, monitoring costs are reduced owed to a reduced asset specificity of its data that is accessible by all authorized participants. However, in a blockchain environment, sharing data between partners, and sometimes competitors, is essential. For instance, “*it does not matter how good the proof of insurance is if it is one-sided.*” Hence, further transaction controlling is needed to monitor the ‘proof of collaboration’ meta-records: “*One of the first hurdles that we had was to be able to prove that these competitors could come together on these various solutions and work together.*”

Fourth, blockchain technology employs code-based consensus mechanisms (DuPont & Maurer, 2015; Mori, 2016). As such, less transaction controlling is needed due to the attenuation of the effects of bounded rationality and language equivocality. Furthermore, the blockchain records are also corroborated by other full nodes in the network continuously verifying the validity of every new block and the overall integrity of the whole ledger. As such, the built-in and code-based automation reduce manual efforts to achieve the same with traditional setups. Moreover, if ‘monitoring’ is considered as a skill, the generality of blockchain code-based capability reduces the asset specificity compared to more traditional monitoring procedures. Similarly, the current processes of digital payments and currency transfers require heavy consumption of human and infrastructural assets of financial institutions that act as intermediaries to conduct, clear, and settle transactions (Yli-Huumo et al., 2016). With a public blockchain, parties can exchange directly over the network, utilizing encryption and consensus mechanisms (Guo & Liang, 2016; Tsai et al., 2016; Zhu & Zhou, 2016) with thinner layers of intermediaries and less involvement of external judicial systems to monitor and enforce the fairness of value exchanges. To illustrate, blockchain technology can enforce ownership by virtue of a consensus mechanism (Workie & Jain, 2017) that is already agreed upon by all participants, and therefore, reducing the transaction enforcement costs.

Fifth and lastly, we examine controlling costs for smart contracts. In the ‘Bargaining’ section we have examined smart contracts ex-ante bargaining costs provided environmental uncertainty and the difficulties vis-à-vis the translation of equivocal language to code. If we assume a smart contract is already appropriately coded and deployed, it is arguable that the smart contract would significantly attenuate the monitoring, enforcement, and litigation controlling transaction costs. In general, contractual disputes represent a significant share of litigations in the

US and the UK—44 percent and 57 percent of the cases respectively (Swan, 2015; Swanson, 2014). Accordingly, Tapscott and Tapscott (2016) assert that smart contracts could disintermediate the law profession.

The current financial transaction controlling process is slow and semi-manual. If replaced by blockchain technology, the ensuing elevated transparency could aid both regulators and participants currently struggling to conduct and monitor the intricate post-trade records and activities (Workie & Jain, 2017). Blockchain technology can natively, seamlessly, and more transparently afford robust audit trails of records of dividend disbursements, ownership details, stock split terms, stock transactions timestamps, taxes reports, and compliance reporting requirements (Rechtman, 2017). Therefore, financial institutions and regulators could build collaborative platforms that would reduce the transaction controlling costs required by the regulators from financial institutions: *“It is a big arduous task for them to gather that information across various back office systems. If you have the information on the blockchain, you could very easily create a use case to do all that regulatory reporting very quickly and cut out many working hours required for that.”*

Finally, a blockchain could traverse multiple jurisdictions which could be *“confusing because the beauty of decentralized networks is not having borders, although we still have borders and live in physical places. There are rules and taxes that we cannot just end on a dime.”* Therefore, applying these multijurisdictional laws contributes to the transaction enforcement costs. For instance, the nature of privacy-related regulations *“varies greatly from country to country, from Estonia where everything is on blockchain, to countries where they will take many years before doing anything.”* Table 12 summarizes the financial transactions controlling costs.

**Table 12: Controlling Transaction Costs**

<i>Effect</i>	<i>Cause</i>
Attenuated transaction costs	Blockchain timestamps attenuate the effects of bounded rationality, opportunism, and performance ambiguity
	Blockchain immutability affords evidence that is tamperproof
	Blockchain immutability increases traceability and verifiability
	In a blockchain world, financial institutions might get rid of the burden of being required to enforce the prohibition of activities such as money laundering
	Blockchain has built-in redundancy
	Blockchain shared ledger has a reduced asset specificity
	Blockchain code-based consensus mechanism attenuates the effects of bounded rationality and language equivocality
	In a blockchain environment, monitoring records validity and network integrity are built-in, code-based, and less asset specific
	Blockchain technology affords thinner layers of intermediaries and less involvement of external judicial systems to monitor and enforce the fairness of value exchanges
	Smart contracts significantly attenuate the monitoring, enforcement, and litigation controlling
Blockchain can natively, seamlessly, and more transparently afford robust audit trails of records	
Increased transaction costs	A blockchain with a high level of privacy raises the cost for controlling illicit activities
	In a blockchain world, government authorities might absorb the burden of prohibiting things such as money laundering
	In a blockchain environment, there is a need to share data between partners, and sometimes competitors
	For a blockchain crossing multiple jurisdictions, there is a need to enforce all global laws covered

## VI DISCUSSION

Blockchain is an integrative meta-technology characterized by a decentralized and distributed single truth ledger, immutable and tamperproof data records, code-based consensus mechanisms, time-stamped records, peer-to-peer transmission, built-in cryptography, and native applications such as smart contracts (Mougayar, 2016; Wang et al., 2016). Motivated by its potential to reduce the costs and improve the performance of financial transactions, the technology has been touted as the innovation engine for the financial industry (de Meijer, 2015; Guo & Liang, 2016; Zhao et al., 2016). With its introduction, it is possible to verify assets, keep records, and protect data in a decentralized fashion with less friction and fewer loci of control (Yli-Huumo et al., 2016). As such, financial institutions are increasingly interested in the technology (de Meijer, 2016).

Against this backdrop, this dissertation contributes to the body of knowledge concerning the impact of this emerging phenomenon on asset verification, record keeping, data privacy, and transaction costs. To achieve our goal, we have employed a pluralist methodology that develops and contrasts a review of the literature, an analysis of the perspectives of key industry players and observers, and a theoretical interpretation through the lens of transaction cost theory (Coase, 1937; Ouchi, 1980; Williamson, 1975). By discussing and synthesizing these different perspectives in the following, this dissertation offers a number of specific contributions to the body of knowledge related to the impact of blockchain technology on financial transactions.

### **VI.1 Blockchain Technology Can Enable Asset Verification, Record Keeping, and Data Privacy**

Enabled by the characteristics of its ledger, network, and protocol, blockchain technology can facilitate asset verification and records keeping (Workie & Jain, 2017) in a manner agreed upon by all participants. The network has a high level of goal congruence engendered by its

nodes corroborating to verify the validity of new information and the overall veracity of existing records (Mougayar, 2016). No single custodian can exercise opportunistic control over the blockchain ledger at any time (Rechtman, 2017). The ledger is, therefore, a single truth that is redundantly distributed across the network enabling asset verification and record keeping with high integrity and accessibility. As such, blockchain technology eliminates the need for the current semi-manual processes where multiple custodians keep records in disparate databases and where each financial institution verifies assets on its own. Consequently, for blockchain participants, asset reconciliation becomes automatic since the ledger has a single shared pre-agreed upon truth at any particular timestamp. This is of significant value because asset verification and record reconciliation consume much of the financial institutions' resources: *“We need to have the correct info to be able to pay dividends, taxes, tax rates, etc. Keeping track of that is very tricky. Therefore, reconciliation is very complex, and something that takes long. That is where blockchain technology might make a difference.”*

Data privacy and transparency are two desired outcomes, but sometimes they conflict. The tradeoff between privacy and transparency is a business decision concerning the balance between confidentiality and verifiability. A blockchain network could be designed to enable the desired balance between transparency and privacy (Narayanan et al., 2016; Yli-Huumo et al., 2016). The level of data privacy and transparency depends on factors such as the agreed upon policy regarding the pseudonymity of the users, whether the data is stored using encryption, the access control scheme, and whether the blockchain network is public, private, hybrid, or permissioned. Moreover, blockchain users could control their *“Self-sovereign identity”* data (Tapscott & Tapscott, 2016) leading to the improvement of its veracity and richness, and therefore, reducing its asset specificity.

These insights were corroborated by our literature review and empirical data and were further supported by our theoretical analysis.

## **VI.2 On Balance, Blockchain Technology Can Lower Financial Transaction Costs**

In alignment with our theoretical analysis we focus on ‘transaction theory’ costs and further support our argument pluralistically with our literature review and empirical data where transaction costs takes a broader meaning of ‘transaction theory’ costs and production costs (Dyer, 1997; Zajac & Olsen, 1993), in addition to transition costs. As such, we proceed to discern the impact of blockchain technology on searching, bargaining, and controlling costs.

First, considering searching costs, the ability of blockchain users to enter their own identity data increases the integrity and richness of the ledger. Therefore, significantly reducing searching costs for credit reporting data. Contrarily, pseudonymity behavior, encrypting records, and falsifying own records increase searching costs. However, it is less significant assuming users’ reputational data is important to them to receive financial transaction services. Furthermore, blockchain searching attributes increase the fidelity of the information and significantly reduces searching costs. On the other hand, the need to search for multiple versions due to immutability could be solved technologically. Our pluralistic findings detailed KYC and asset reconciliation as two major exemplars where blockchain technology positively attenuates transaction searching costs.

Second, related to bargaining costs, blockchain tenants share a pre-agreed upon code-based and transparent ecosystem. This significantly reduces the negotiation and renegotiation costs since bargainers are anchored on correct information. We argue that blockchains with more focus on privacy will be less profuse since the quest for transparency drives the value proposition of building a blockchain network. The ‘proof of insurance’ example drawn from our empirical

data supports this conclusion. Indeed, there is a possibility that some users might try to monetize their identify data, therefore increasing bargaining cost. Nevertheless, it is less likely there will be many such users for reasons explained above. Certainly, negotiating smart contracts could significantly increase bargaining costs. Nonetheless, these bargaining costs are less significant compared to the savings on the controlling costs.

Third and finally, we consider controlling costs. The ability to design a blockchain as a readily transparent controlling platform (Workie & Jain, 2017; Yli-Huumo et al., 2016) significantly reduces controlling costs (Kiviat, 2015) as shown by the long list of where blockchain technology attenuates controlling costs—Table 12. The few areas where blockchain technology increases cost are of less significance based on the following argument: a) we have already addressed private blockchains above b) the scenario of the authorities absorbing KYC and AML compliance requirements is merely a matter of shifting costs away from financial institutions, c) the need for monitoring the sharing of data between partners could reduce over time as goal congruency increases, and d) enforcing all global laws covered by a blockchain network might be of significance, but not too different compared to traditional technologies.

Therefore, we conclude that, on balance, blockchain technology attenuates transaction costs.

### **VI.3 Blockchain Technology Furnishes a Reporting Platform for Financial Transactions**

The findings from our pluralistic method concur that blockchain technology could potentially be the platform for reporting activities for financial transactions. Owing to immutability and decentralization, the permanence of blockchain data (Narayanan et al., 2016) makes it a reliable platform to keep important records indefinitely. The events are verifiable and traceable due to their timestamps (Crosby et al., 2016; Tapscott & Tapscott, 2016). Furthermore,

corroborated by the whole network (Rechtman, 2017), data on a blockchain ledger attains a high level of integrity and veracity. With its built-in cryptography, data privacy and access control are built-in capabilities. Besides, its native applications such as smart contracts (Mougayar, 2016; Wang et al., 2016) could enable process automation. As such, blockchain technology can natively, seamlessly, and more transparently afford robust audit trails of records of financial transactions (Rechtman, 2017) with minimal transaction costs.

As a readily available reporting infrastructure (Workie & Jain, 2017), blockchain technology is impactful to auditing and monitoring (Kiviat, 2015) requirements and practices desired by financial institutions and regulatory bodies. The platform could enable financial institutions to exchange reports among themselves, as well as with authorities in compliance with regulatory requirements: *“It is a big arduous task for them to gather that information across various back office systems. If you have the information on the blockchain, you could very easily create a use case to do all that regulatory reporting very quickly and cut out many working hours required for that.”*

#### **VI.4 Blockchain Technology Requires Approaching Financial Transactions Differently**

Blockchain technology is greater than the sum of its parts (Mougayar, 2016). Thus, it is both a technological and economic innovation that offers a platform to record transactions and share data between participating parties in a more efficient, transparent, and verifiable manner (Liebenau & Elaluf-Calderwood, 2016; Lindman et al., 2017; Workie & Jain, 2017). The technology reshapes centrality and reshapes governance (Guo & Liang, 2016). Synthesizing the perspectives of our literature review, empirical data, and theoretical analysis, we found the following six aspects about blockchain-based financial transactions that behoove managers to approach financial transactions differently when considering blockchain technology.

First, a blockchain network is a multitenant environment. Its value proposition obtains when the ecosystem is a decentralized multiparty that would benefit from an engendered trust. To be successful, blockchain participants should do away with isolated data records and share information on the blockchain ledger to enhance reputability, accountability, and controllability (de Meijer, 2015) by computationally, efficiently, and seamlessly keeping records across the financial value chain (Kiviat, 2015). In this way, blockchain participants are enabled to work with high level of goal congruence and low level of performance ambiguity.

Second, blockchain records alter the nature of financial transactions and their transaction costs since they a) attain further veracity over time (Narayanan et al., 2016), therefore, redefining traditional concepts such as the finality of settlements (Mori, 2016), b) are immutably corroborated by the whole network, c) are secure, but could raise security issues of different nature, d) could be made accessible to only the intended audience, and e) are chronological accounts of events (Tapscott & Tapscott, 2016).

Third, the technology could expand the richness and reach of financial transaction services (de Meijer, 2015). Nonetheless, much of the gain would not be owed to the automation of current processes, but to the development of new business models (Mori, 2016; Workie & Jain, 2017). An extreme exemplar could be the emergence of DAOs—organizations with self-governed operations and user-produced value creation and rewards (Mougayar, 2016).

Fourth, blockchain technology enables individuals to assume controls of their privacy aspects (Nakamoto, 2008). Tapscott and Tapscott (2016) further posit that not only would blockchain technology furnish a flexible means for individuals to control and protect their data, but also to monetize their identities and personal information. The implications were

demonstrated in our empirical and theoretical analysis, and are exemplified by the potentially significant impact on credit reporting industry.

Fifth, the current financial transaction regulations that have been tailored for a “*financial ecosystem that we have developed in the past 100 to 200 years*” will have to adapt to a different world. There might be “*a need for some extra sort of blockchain sensors*” to enable monitoring financial activities. The nature of compliance requirements such as KYC and AML could become different. As such, KYC and AML could be expanded to searching and monitoring a network of vibrant online activities. Moreover, the transaction costs of KYC and AML due diligence might shift from financial institutions to government authorities.

Sixth and finally, blockchain-based startups will force incumbents to reduce transaction costs: “*Visa and MasterCard are now a duopoly in the payment sector. If we have many other options then, especially internationally, they have to reduce their fees drastically to remain competitive.*” Therefore, incumbents must invest in exploring blockchain technology since it is “*a strategic decision to invest now while it is still developing to gain a head start.*” Moreover, potentially, blockchain technology could introduce a massive change regarding how we would interact with capital markets in the form of ICOs.

## **VI.5 Adoption of Blockchain Technology for Financial Transactions is Uncertain and Complex**

Like all newly introduced technologies, blockchain technology is far from fully charted waters: “*It is so fascinating, and we still do not understand it. We still do not understand some of the negative.*” Disruptive innovations usually surpass the internal absorption and usurpation capabilities of established institutions (Mougayar, 2016). To successfully transition to blockchain technology, incumbents and startups will have to resolve the technological, regulatory, adoption,

and transaction hurdles as we found in our literature review, empirical data, and theoretical analysis.

First, blockchain technology is not yet mature, and therefore, several technological issues arise. Many financial systems require high throughput, thus, presenting a challenge for blockchain technology provided its sequential ledger, consensus mechanism, and the need for its nodes to operate in server-client dual mode (Tsai et al., 2016). Storage requirements are also high given its ever-growing ledger (Yli-Huumo et al., 2016; Zhao et al., 2016). There are also security risks such as the 50% attack (Narayanan et al., 2016) and *“the risk of losing passwords.”* Immutability makes it *“hard to go back and modify the record because one has to get agreement from everyone.”* Moreover, its built-in redundancy comes with the price of taxing computational and networking resources. Therefore, the financial industry leaders *“are waiting until blockchain technology is mature before they spend the money.”*

Second, the regulatory framework is still evolving, therefore, adding to the uncertainty surrounding a relatively new technology: *“The largest problem is the regulatory framework.”* Besides, *“the regulators themselves do not understand how cryptocurrencies or blockchain technology works.”* Thus far, there are a few compliance requirements concerning asset verification, record keeping, and data privacy (FINRA, 2017). Furthermore, for a global blockchain covered by heterogeneous jurisdictions, compliance is further complicated (Mori, 2016).

Third and finally, there are several general adoption issues. For instance, not all stakeholders appreciate the value proposition of blockchain technology, but some see it as *“full of hype and euphoria with real potential for only a few use cases.”* Some believe blockchain technology will not deliver on all its promises. Many stakeholders, therefore, advocate gradual

adoption: *“Rather than jump in, which could bring numerous problems I could not think of, I would cautiously watch the technology as it matures, then adopt it in a controlled way.”* The decision of when to use blockchain technology versus traditional ones is complex (Auctus\_Team, 2017) and *“it is hard to be aware of all the different flavors of blockchains in an arms race to see who can provide better features.”* Sharing a blockchain network requires participating parties to agree on governance and operational aspects and probably settling around standards that all the industry players will adopt. It requires effort to integrate the current multiple interconnected financial systems or replace with blockchain technology. Besides, although, on balance, blockchain technology attenuates transaction costs, it also increases some of them—Tables 10-12.

## VII REFLECTIONS

Based on our pluralistic methodology, we have uncovered specific areas that pertain to the impact of blockchain on financial transactions. In this section, we reflect on some general themes that have emerged through this dissertation.

### VII.1 Understanding the Complexity of Designing Blockchains

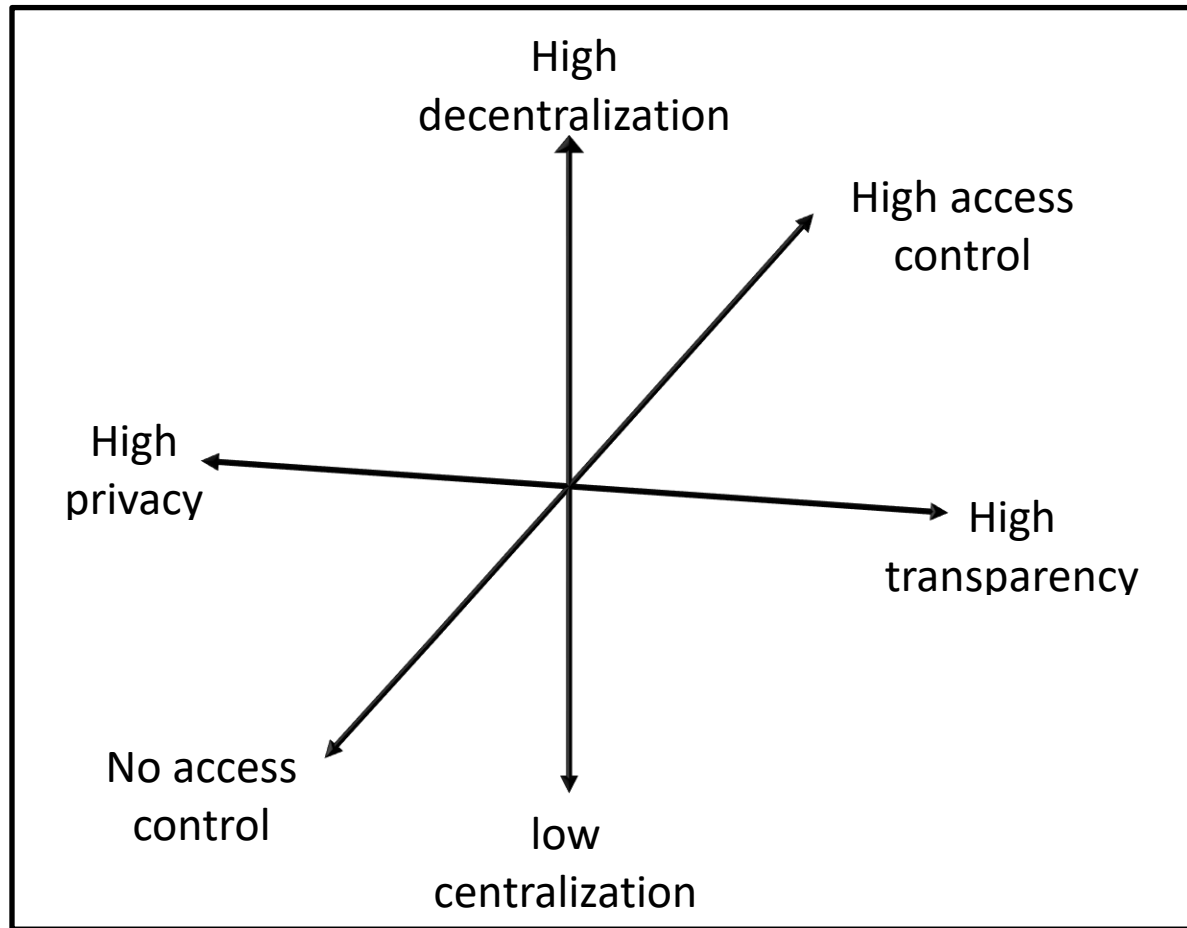
We have detailed how complex blockchain technology is. As such, the industry needs guidance to simplify how to design, develop, and organize blockchain-based financial transaction services (Lindman et al., 2017). To assist with this goal, we emphasize the key dimensions of blockchains.

Table 5 illustrates a few major categories of blockchains. However, the characteristics of blockchain technology allow financial institutions to conduct and operate a wide array of financial transaction services at any point in three-dimensional octants as shown in Figure 9. The figure shows the three operational axes.

The first axis measures the degree of access control. Access refers to who can write and read which data on a blockchain. At the lowest end, a blockchain can be unconditionally accessible by every Internet user (Buterin, 2015; Pilkington, 2015). At the opposite end, access to an entirely private blockchain is controlled by a central locus of governance (Buterin, 2015; Pilkington, 2015). The second axis is the degree of privacy. Privacy refers to aspects of level of encryption and degree of user anonymity (Narayanan et al., 2016; Yli-Huumo et al., 2016). A blockchain can be designed with a high degree of privacy, a high degree of transparency, or anywhere in between. The third axis is concerned with the degree of decentralization. Decentralization refers to several things including the type of consensus mechanism used, the ownership and distribution of the network nodes, and who participates in coding and

development. Similar to the other dimensions, decentralization is not an ‘all or nothing’ (Narayanan et al., 2016).

**Figure 9: Dimensions of Blockchain**



Choosing levels of a blockchain access control, privacy, or centralization should be based on the suitability of the configuration to the business needs rather than on technological limitations. However, according to Ethereum founder Vitalik Buterin, these choices are subject to what is called the “blockchain trilemma.” The trilemma states that between security, privacy, and decentralization, , one can only achieve optimal solutions in two of the three dimensions.

## VII.2 Applying Transaction Cost to Blockchain Design

We have analyzed blockchain transaction costs related to the activities of searching, bargaining, and controlling. This exercise proved useful, and there are additional opportunities to apply transaction cost theory to interpret the blockchain technology phenomenon. As we have discussed, transaction cost theory assumes a priori that markets are generally more efficient than hierarchies (Geyskens et al., 2006) and also defines when hierarchies perform better (Coase, 1937). The determinants of the boundaries are frequency, asset specificity, goal incongruence, uncertainty, bounded rationality, and opportunism (Klein et al., 1978; Milgrom & Roberts, 1992; Ouchi, 1980; Williamson, 1979).

Akin to the market versus hierarchy dichotomy, the choices of the type of access control, level of privacy, the degree of decentralization could be analyzed using the above transaction cost determinants. A typical blockchain is decentralized with multiparty sharing information on the ledger to enhance reputability, accountability, and controllability (de Meijer, 2015) by computationally, efficiently, and seamlessly keeping records across the financial value chain (Kiviat, 2015). However, other configurations are possible, and sometimes desirable.

A highly accessible and decentralized blockchain is extremely immutable, and therefore, it is not possible to fix a mistake. In this sense, immutability affords traceability and reliability; nonetheless, it makes it difficult to fix mistakes and human errors. The choice of this configuration is arguably needed when there are high levels of opportunism and goal incongruence. A blockchain with high privacy could be the choice of users whose primary concern is opportunism. A transparent, decentralized, and accessible blockchain could be the choice when transactions are frequent with a low level of asset specificity.

### VII.3 Appreciating the Blockchain Ecosystem

For blockchain innovation to permeate, a surrounding and integrated ecosystem needs to flourish. Blockchain technology alone will not lead to a significant transformation of financial transactions. For instance, Mori (2016) asserts that 80 percent of the challenges in the financial industry are associated with business models and processes, and only 20 percent are attributable to technological hurdles. As such, redesigning processes and coming up with innovative business models are vital to the success of a blockchain technology paradigm shift. Doing so is not easy by any means as stated by one of the participants: *“Blockchain technology opportunities are limited because of the way the whole asset industry is structured right now. Change is not happening, it would require quite a bit.”*

The ecosystem comprises a) blockchain-based new entrants to the financial transaction sector, b) incumbent financial services providers, c) interconnectors between different entities exemplified by cryptocurrency exchanges, d) technology innovators—incumbents and entrepreneurs—to supply the market with blockchain-based solutions, and e) regulators to guarantee compliance and to build the required regulatory framework. In addition, the ecosystem includes new types of consumers with new aspirations, passion, and demands. In this way, collaboration and convergent interests are essential to unleashing the power of blockchain technology.

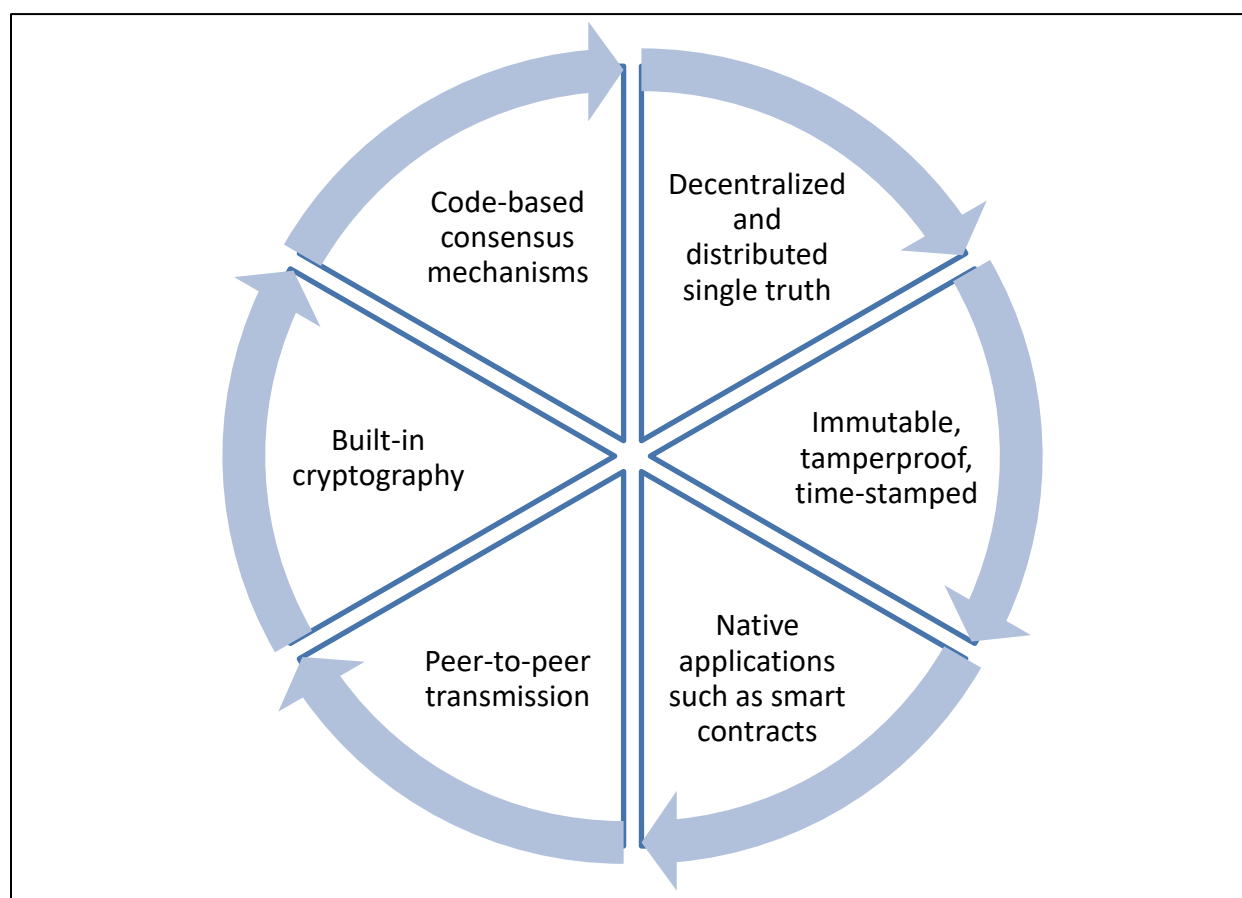
From a technology stack ecosystem point of view, we envision a future permeated by machine-to-machine type of transactions pushing the blockchain technology towards the internet of things (IoT) periphery. Besides, AI is expected to play an important role in adding analytical capability to blockchain technology. That is especially important for blockchain smart contracts to become smarter, more dynamic, and more flexible (machine learning type of AI), and more

integrated with big data. The integration of these three technologies could lead to unprecedented, innovative waves of development.

#### VII.4 Creating Value with Blockchains

To understand the value creation options owed to blockchain technology, it is worth revisiting blockchain as a meta-technology that integrates several technologies to form a gestalt (Kiviat, 2015; Mougayar, 2016)—see Figure 10 which illustrates the main characteristics of blockchains that we have covered in this dissertation.

**Figure 10: Blockchain Gestalt**



The original promise of blockchain technology introduced by Nakamoto (2008) was to bypass middleman actors and allowing direct peer-to-peer transactions, a vision celebrated by anarchists and alarming to institutionalists. Ten years passed since, and the technology adoption

is shaping in a way that is rather different. Instead of disintermediating, we see the reintermediation of trust away from the center (Mougayar, 2016) and the formation of ‘multi-center, weakly intermediated’ schemes (Guo & Liang, 2016) exemplified by cryptocurrency exchanges and blockchain-based escrow services. Many businesses were established to enable financial transactions and to exchange value. As such, blockchain technology permits the displacement of older and thicker layers of intermediation with newer and thinner ones. In doing so, the technology surpasses equivalence in terms of speed of financial transactions and their cost, level of trust, degree of flexibility, and broadening business models (de Meijer, 2015; Guo & Liang, 2016; Kiviat, 2015)—not only from a business side, but also from consumer and regulator sides.

## **VII.5 Considering Blockchain Applications**

Blockchain applications can be categorized in many ways as we have seen in Appendix B, and Appendix D. We have uncovered three broad areas that are being actively pursued by financial transactions providers.

The first area of applications is payments. Blockchain technology can reduce the cost of cross-border transactions, lower annual operational costs, and reduce annual cost of risk (Guo & Liang, 2016). Besides, the phenomenon of cryptocurrency in itself is destined for more adoption as exemplified by some countries augmenting their fiat currencies by cryptocurrency. The payment sector gave rise to new models of financial transaction services such as cryptocurrency exchanges, digital asset escrow service providers, and different type of cryptocurrency minters. The exchanges allow end users to swap cryptocurrencies with each other or with fiat currency. The concern of cryptocurrency being used for illicit activities is countered by blockchain

traceability and the concept of pseudonymity (Tapscott & Tapscott, 2016). In this context, pseudonymity could be considered as a balance between privacy and transparency.

Second, immutability and timestamps of blockchain data make the technology suitable for tracking assets and activities with an elevated level of trust in the veracity of assets information (Crosby et al., 2016; Mori, 2016; Rechtman, 2017). As such, blockchain technology affords a suitable platform for asset reconciliation (Rechtman, 2017). It is also a suitable system to achieve compliance auditing services required by regulators (Kiviat, 2015; Workie & Jain, 2017). Moreover, supply chain financial transactions are another major field for blockchain technology as exemplified by IBM Hyperledger.

The third area is identity management. The capabilities of blockchain in managing identity are exemplified by its implementation in the country of Georgia. Moreover, the technology allows “*self- sovereign identity*” where users have more control over their identity and their content. Blockchain technology can challenge some of the established identity privacy norms where individual and the collective—instead of central entities—are in control of reputational information.

## VIII CONCLUDING REMARKS

Asset verification, record keeping, data privacy, and transaction costs are but some few areas of the financial transaction domain. Moreover, our theoretical framework is but one of many lenses to explore the impact of blockchain technology on financial transactions. Future research should, therefore, examine different theoretical frameworks and additional financial transaction areas to shed more light on the phenomenon.

Although we have utilized transaction cost theory, we have focused on the impact on searching, bargaining, and controlling costs. However, we have left out a central transaction cost theory goal concerning organizational boundaries around the decision of ‘make, buy, or ally’ (Coase, 1937; Ouchi, 1980; Williamson, 1979). As such, future research should consider extending this dissertation to examine the governance aspect.

Compared to our theoretical analysis where we solely focused on ‘transaction theory’ costs, while collecting and synthesizing the literature and the empirical data, we broadly examined various aspects of blockchain technology impact on financial transactions. Moreover, in this case, the term ‘transaction cost’ took a broader meaning to engulf ‘transaction theory’ costs and production costs (Dyer, 1997; Zajac & Olsen, 1993), in addition to transition costs—blockchain technology enablement costs. As such, future research should look deeper into these broader areas of costs related to transitioning to and operating blockchain-enabled financial transactions.

## APPENDICES

### Appendix A: Pluralist Methodology

Mingers and Brocklesby (1997) define a methodology as a structured set of guidelines or activities to undertake a study. They further posit that a methodology will develop implicitly or explicitly within a particular paradigm embodying its philosophical assumptions in terms of ontology—the types and nature of entities—epistemology—the possibilities of, and limitations on, our knowledge—and praxeology—the nature of our actions. For further details about the characteristics of the main paradigm families the reader may refer to Appendix F.

This dissertation employs a pluralist approach, where all situations are viewed as inherently complex and multidimensional, therefore, would benefit from multimethodology (Mingers, 2001). The real-world is ontologically stratified and differentiated (Bhaskar, 1994), and therefore, pluralism is essential to portray the richness and multidimensionality of the real world. Mingers (2001) avers that research methods are instruments for provoking a response from a complex multidimensional world, and in this respect, different methods may produce useful information about various aspects of the world. Hence, to construct a rich view of a phenomenon, it is both desirable and feasible to use pluralist methodology to gain richer and more reliable representation of reality. From an engaged scholarship standpoint, pluralist methodology is sensible because practitioners are already ahead of academia in combining methodologies in practice (Mingers & Brocklesby, 1997).

Furthermore, Mingers and Brocklesby (1997) advocate that a study comprises several phases where each phase has different tasks and requirements, and therefore, could be embarked upon more effectively with a different methodology or a diversity of methodologies. Additionally, Mingers and Brocklesby (1997) align with the view of postmodernists where

methods or parts of methods may be removed from their theoretical and philosophical base and pressed into the service of different, even competing, logics.

To the common argument that research methods are bound to particular paradigms that are incommensurable, Mingers (2001) reiterates that the world is almost certainly more complex than we could ever know, therefore, this argument is an epistemic fallacy—limiting what may exist to our current knowledge—and an anthropic fallacy—defining existence as centered around human being (Bhaskar, 1978). Hence, it is both ontologically desirable and possible to approach a phenomenon pluralistically. Mingers (2001) goes further to affirm the feasibility of detaching research methods from a paradigm and using them within a context that proposes different assumptions.

Tashakkori and Teddlie (1998) list additional benefits of pluralist methodology. First, triangulation allows the researcher to validate data and results by blending a range of data sources, methods, or observers. Second, pluralist methodology aids creativity through the discovery of fresh or paradoxical factors that stimulate further research. Finally, pluralist methodology permits the expansion of the scope of the research to draw broader conclusions from situations (Mingers, 2001).

Triangulating multiple perspectives or methods on a complex business problem or challenge attenuates the likelihood of unintended bias in interpretations (Van de Ven, 2007). Furthermore, a pluralist methodology that compares and contrasts multiple plausible models of reality is crucial to the emergence of rigorous scientific knowledge (Azevedo, 1997; Van de Ven, 2007). Most importantly, a pluralist methodology can help to study a business phenomenon that is emerging and not well researched, by providing complementary types of insights. The essence

of pluralist methodology is to combine perspectives and parts of methodologies (Mingers & Brocklesby, 1997).

Against this backdrop, this dissertation iteratively traverses multiple perspectives by drawing on three methods. First, is exploring the literature on blockchain technology as it relates to the financial industry. The second method of this research is a number of interviews on blockchain technology with financial sector executives, subject matter experts, and academics to enhance the understanding of a complex phenomenon by engaging the perspectives of diverse scholars and stakeholders (Bechara & Van de Ven, 2007). Third, transaction cost theory (Coase, 1937; Ouchi, 1980; Williamson, 1975) as a particularly stimulating theoretical framework that promises insights into the potentially disruptive effects of the blockchain technology. This dissertation will employ an iterative juxtaposing and analysis of these three perspectives and methods. While collecting and synthesizing the literature and the empirical data, we broadly examined various aspects of blockchain technology impacts on financial transactions. Moreover, in this case, the term ‘transaction cost’ took a broader meaning to engulf ‘transaction theory’ costs and production costs (Dyer, 1997; Zajac & Olsen, 1993), in addition to transition costs—blockchain technology enablement costs. However, during the theoretical analysis, we zoomed in to solely focus on ‘transaction theory’ costs.

Underlying this qualitative dissertation, the researcher espouses, at the paradigm level, a critical realist stance that adopts a combination of an objective ontology and a subjective epistemology (Bechara & Van de Ven, 2007). This paradigm sits well with the context of the inquiry at hand as well as with the pluralist methodology because of five major assumptions made by Bechara and Van de Ven (2007). First there is a real world; however, we are limited in our ability to understand it. Second, all facts and data are theory-laden. Third, even though some

methods are better than others in a given context, no form of inquiry can be value-free and unbiased. Fourth, triangulation produces more rigorous knowledge. Finally, the fit of a methodology is context specific.

### ***Appendix A.1: The Literature Review Method***

The first side of the triangular pluralistic methodology is the literature review. The literature review situates the research contextually and builds on prior research (Myers, 2013). The literature review is the foundation (Webster & Watson, 2002) that forms the empirical basis for conducting the research (Trochim, Donnelly, & Arora, 2015). A major purpose of the literature review is to recognize what is covered by the extant literature and to validate the originality of the intended contribution as inspired by the research question.

According to Webster and Watson (2002), two forms of literature reviews exist. First, when treating a mature subject matter that is well covered by the extant literature. Second, when exploring an emerging topic that has a dearth of coverage by the extant research. Inasmuch as blockchain technology is emerging, the approach of research adopted here aligns with the second from where it is beneficial to augment with potential theoretical foundations (Webster & Watson, 2002) as explicated by the subsequent theoretical interpretation section. Moreover, the triangulation with the perception analysis method helps in tightening the inherent looseness in extant body of knowledge of such an emerging field as in the case of the topic of this dissertation.

Based on the research question concerning the impact of blockchain technology on financial transactions, the first step taken was to identify the intersection of the literature streams comprising the overlap of blockchain technology with the financial industry. Although a few technological articles were covered, the focus was on the business-related literature streams. To

fully comprehend the underlying business aspects and technological schemes of blockchain technology, the researcher took notes from attending a virtual class offered by Princeton University (Princeton University, 2014) as well as reading five books on the topic. The effort was followed by a systematic literature review—a relatively broad survey of relevant literature that is considered complete when no new concepts emerge in the article set (Trochim et al., 2015). Accordingly, a systematic review of related literature began by searching for articles covering the intersection of literature on blockchain technology and the intersection with the financial industry. The search of the extant literature yielded four hundred and twenty related articles.

The next step was to examine the summaries of the articles mentioned above with two goals in mind. The first goal was to identify which articles are strongly related to this dissertation subject matter. The second goal was to group the concepts into subcategories. Following this winnowing effort, the articles were read, and related passages were identified. Furthermore, additional related articles—referenced in the set—were discovered. Next, the supplementary articles were read, and related passages were identified. The overall effort resulted in a) fifty-seven articles of general nature detailing blockchain-related business and technological aspects; b) forty-three articles concerning the intersection of blockchain technology with the financial industry—inclusive of current and potential future blockchain-based financial applications; c) thirty articles covering various non-financial applications of blockchain technology; and d) seven articles related to legal and legislative areas of blockchain technology. In addition to the five books mentioned earlier, the literature set comprised academic papers, white papers, industry blogs, and videos. The deviation from the reliance on only academic articles is due to the newness and emergence of the blockchain technology phenomenon.

Next, a systematic data analysis of the passages was conducted to identify and categorize text passages in relation to the corresponding ‘literature review’ sections in the manuscript. Open coding was employed to identify passages in the texts that describe relevant phenomena (Myers, 2013). Later, axial coding was utilized to conceptualize and group the passages into categories in order to triangulate with the perception analysis data. Axial coding specifies each category’s properties and dimensions (Charmaz, 2014). Finally, selective coding (Strauss & Corbin, 1990) was employed to select core categories and relate them to corresponding concepts from transaction cost theory—the theoretical framework.

In addition, the literature review supports the systematic compilation and synthesis of all of the extant literature related to a research subject matter (Trochim et al., 2015) and concisely explicates what has been learned (Webster & Watson, 2002). Accordingly, to enable the synthesis of uncovered concepts, the literature review was organized into three chapters: 1) Introduction, 2) Technology: Blockchains, and 3) Application: Financial Transactions.

### ***Appendix A.2: The Perception Analysis Method***

The second pillar of the triangular pluralist mythology is the perception analysis. Interviews are like night vision goggles that permit the researcher a vivid view of the scattered objects in the field (Myers, 2013; Rubin & Rubin, 2011). The inclusion of the perception analysis of blockchain technology practitioners, experts, and researchers increases the rigor of the research because it fills the contextual gaps typically present in the extant literature concerning emerging fields such as the one being examined by this dissertation. Furthermore, a significant benefit for augmenting the literature review method with the perception data is to bridge the temporal lag where there is two to three-year between conducting studies and their publication in academic journals (Myers, 2013). Additionally, the perception analysis serves to

validate insights from the theoretical interpretation method. Finally, interviews are primary data—collected by the researcher—that adds richness and credibility to qualitative research (Myers, 2013).

The first step was to decide on how many people to interview in order to gain their perception. Inasmuch as this is a qualitative research, sample size has no significance. A more critical concern than the number of interviews is to make sure that the pool of participants embodies a variety of voices (Myers, 2013; Myers & Newman, 2007). As such, we believed that sixteen participants provided enough variety of voices. Our confidence level in reaching rigorous conclusions is further elevated by virtue of triangulating the data from the interviews with both the literature review and the theoretical perspective. To further ensure diversity of views, target participants were selected as follows: a) six financial industry blockchain technology executives, b) five senior blockchain technology subject matter experts, and c) five blockchain researchers.

A semi-structured interview was devised with prepared questions; however, at times, we deviated from the script and improvised new questions depending on the conversation (Myers, 2013). The reader may refer to Appendix I for details regarding structure of the interviews. According to Myers (2013), semi-structured interviews enable the interviewees to provide more rich insights and to offer valuable information. Contrasted with structured interviews where the researcher sticks to prepared questions, and unstructured interviews where no prepared questions are preformulated, semi-structured interviews allow flexibility while sustaining a reasonable level of focus. As such, each participant was separately interviewed once for a duration of sixty minutes by telephone. The researcher took notes during each interview. Additionally, each interview was recorded digitally and transcribed later.

Next, we engaged in systematic data analysis of the interview transcripts. First, open coding was applied to uncover relevant concepts (Myers, 2013). 286 passages were captured. The second step was to use axial coding to conceptualize and group the passages into higher-level concepts (Charmaz, 2014) resulting into 9 distinct codes. Third and finally, selective coding was employed to select core categories and relate them to other categories (Strauss & Corbin, 1990) being our four arear areas of financial transaction in the case: asset verification, record keeping, data privacy, and transaction costs. The perception analysis was iteratively juxtaposed to the data generated with the literature review method. Moreover, data from both the interviews and the literature review was iteratively related to the insights from the theoretical interpretation method as will be explicated in the next section.

During all phases of the interview process precautionary measures were taken to protect the privacy of the participants' personal information and their organizational data. The tools used for conducting the interviews are listed in Appendices F, G, and H.

On the one hand, the goal of practical knowledge is concerned with situations in a particular case. On the other hand, the purpose of scientific knowledge is to seek a generalization that can be used to explain and understand things (Van de Ven, 2007). As such, the perception analysis method covers the former, while the next method covers the latter.

### ***Appendix A.3: The Theoretical Interpretations Method***

The third and final leg of the pluralistic methodology is the theoretical interpretation. Theoretical frameworks provide abstract, conceptual understandings of the phenomenon under investigation (Charmaz, 2014). The approach adopted by the pluralistic methodology of this dissertation aligns with the way Yin (2013) advocates triangulating multiple sources of empirical data with theoretical schemes (Myers, 2013). As such, this dissertation embarked upon

iteratively triangulating transaction cost theory concepts, as a theoretical framework, with the literature review and the interviews data. The endeavor provided more profound insights supported by: a) practical knowledge that aided the understanding of a particular practical situation and b) theoretical knowledge that helped in describing the fundamental nature of things (Van de Ven, 2007).

This dissertation started by applying the literature review method as detailed in the 'Literature Review Method' section. Next, the perception analysis method was applied as explained in the 'Perception Analysis Method' section. Lastly, transaction cost theory was invoked to understand and explain findings from the two preceding methods. This sequential approach aligns with Lawrence (1992) who advocates problem-oriented approaches rather than theory-oriented approaches (Van de Ven, 2007). Lawrence suggests to start by surveying the field to inspect the problem and make an initial assessment of significant parameters; and then explore relevant theory for promising conceptualizations (Van de Ven, 2007). Furthermore, this dissertation summoned transaction cost theory in a fashion aligned with the view of Locke and Latham (2004) who aver that extant frameworks are likely inspirational resource for making sense of data since theory can be used to open up new possibilities (Van de Ven, 2007). As such, the intended approach of this dissertation of exposing the tension between data and concepts of transaction cost theory led to an interaction of observations that refined research foci and generated possibilities to uncover new interpretations that, at times, conflicted with prevailing views or advanced different perspectives (Van de Ven, 2007).

Drawing on the literature review and the perception analysis, we obtained perspicacity to identify transaction cost theory concepts with potential explanatory power of interpreting the blockchain technology phenomenon in the financial industry. To achieve that, we thoroughly

studied research papers detailing the fundamentals of transaction cost theory as exemplified by (Coase, 1937, 2013; Commons, 1931, 1932; Ouchi, 1980; Williamson, 1973, 1975, 1979, 1985, 1988, 1994, 2008, 2010a, 2010b, 2014). Next, to acquire expertise with the analytical utility of transaction cost theory concepts, we read studies that engage transaction cost theory as a framework for analyzing different phenomena as exemplified by (Anderson & Gatignon, 1986; Cheung, 1969; Pollak, 1985).

Transaction cost theory is interdisciplinary as it joins economics with aspects of organization theory and contract law (Williamson, 1979). The kernel question of transaction cost theory is concerned with organizational boundaries around the decision of ‘make, buy, or ally;’ in other words, whether a transaction is more efficiently performed within a firm—vertical integration—or outside the firm—market governance—(Coase, 1937; Geyskens et al., 2006). As such, the goal of minimizing transaction costs determines the governance mechanisms (Husted & Folger, 2004). Transaction costs consist of searching, bargaining, monitoring, enforcement, and other costs that are not directly related to the production of goods or services (Husted & Folger, 2004). Accordingly, the industry perception data and the literature review data were analyzed to examine impact of blockchain technology on transaction costs. The transaction costs approach allows identifying the circumstances—comprising goal incongruence and performance ambiguity in Ouchi’s view—which produce the costs of mediating exchanges between participants (Ouchi, 1980). In Williamson’s views, transaction costs are determined by: a) frequency, meaning how often a contract is invoked (Milgrom & Roberts, 1992; Williamson, 1979), b) asset specificity, referring to whether the asset could be deployed to a different purpose (Husted & Folger, 2004; Klein et al., 1978; Williamson, 1979), and therefore, raising the concern of goal incongruence (Ouchi, 1980) which is defined as the degree to which parties to an

exchange have incompatible objectives (Husted & Folger, 2004), c) uncertainty, comprising ex ante difficulties of anticipating all future scenarios, language equivocality (Milgrom & Roberts, 1992; Williamson, 1975), and ex post performance ambiguity concerning the difficulty of measuring performance, (Ouchi, 1980) or in other words, the metering problem related to the intricacy of assessing the level of contribution of each individual or entity to a joint effort (Alchian & Demsetz, 1972; Husted & Folger, 2004; Milgrom & Roberts, 1992), d) bounded rationality, positing that people have limited ability to store, process, and retrieve information (Simon, 1955; Williamson, 1973), and e) opportunism, exemplified by dodging duties, breaching agreements, and stealing (Alchian & Demsetz, 1972; Husted & Folger, 2004; Williamson, 1979).

Accordingly, we examine the aforementioned transaction costs determinants to contrast traditional technologies with blockchain technology. Therefore, we stress the differentiating characteristics of blockchain technology. First, blockchain timestamps events and records (Crosby et al., 2016). Second, by design, blockchain transactions are immutable and tamperproof (Mougayar, 2016; Wang et al., 2016). Third, blockchain ledger is “*centralized and fully decentralized at the same time.*” Fourth, blockchain employs code-based consensus mechanisms (DuPont & Maurer, 2015; Mori, 2016). Fifth and finally, blockchain has smart contracts as a native feature (Auctus\_Team, 2017; Mougayar, 2016)—digitally drafting and automatically enforcing transactions instead of burdensome human interventions (de Meijer, 2015; Yli-Huomo et al., 2016; Zhao et al., 2016).

Tapscott and Tapscott (2016) provided a general transaction cost analysis of blockchain technology independent of industry. We build on and extend their work by presenting a transaction cost analysis specific to financial transactions. Specifically, we explore the transaction cost theory activities comprising searching, bargaining, and controlling (monitoring

and enforcement) (Hennart, 1993; Husted & Folger, 2004; Williamson, 1985) to shed light on how the adoption of blockchain technology will affect the transaction costs related to asset verification, record keeping and data privacy. We also go beyond the analysis of Tapscott and Tapscott (2016) by examining not only where blockchain technology attenuates transaction cost but also where it increases transaction cost. Finally, to objectively compare transaction costs between traditional technologies and blockchain technology, we assume that the blockchain network is already up and running. The assumption allows us to avoid the complications in comparing sunk costs that are related to established technologies with enablement costs that are related to deploying blockchain technology.

In this way, this dissertation sought to employ transaction cost theory to make sense of blockchain technology phenomenon in the financial industry. The approach is analogous to past analysis conducted by researchers such as the study by Cheung (1969) that utilizes the transaction cost theory concepts of uncertainty and contracts to examine contractual records in Chinese agricultural communities. Another example is the analysis of entry mode decision into international markets through the lens of transaction cost theory by Anderson and Gatignon (1986). A final and third example is the work of Pollak (1985) who examines the economic activity and behavior of the family through the lens of transaction cost theory.

In summary, the employment of transaction cost theory enriched the insights of the findings because according to Van de Ven (2007) scientific inquiry involves a repetitive contrast between theoretical ideas and empirical data that aids in making sense of the observations.

## **Appendix B: General Blockchain Applications**

Blockchain technology use beyond cryptocurrency is being tried in many industries where some forms of exchange is conducted (Yli-Huumo et al., 2016). Zhao et al. (2016) posit that the evolution of blockchain technology runs through blockchain 1.0 with a focus on digital currency, then blockchain 2.0 concerning digital finance, to blockchain 3.0 encompassing a digital society. Zhao et al. discern that despite the burgeoning of many experimental projects, blockchain 2.0 and 3.0 will need many years to flourish and bring about significant economic impacts. Mougayar (2016) concurs and anticipates blockchain technology adoption and evolution to parallel the Web's, which formed initially over seven years after the launch of the Internet in 1983, but then required additional efforts over three years (1994-1997) for most business to understand its potential. Therefore, Mougayar expects that blockchain technology will persist as a semi-complex phenomenon for the period 2015–2018, analogous to how it took Bitcoin three years (2009–2012) before it started to permeate into the main fabric of the economy.

To establish a reference for understanding current and potential blockchain-based offerings, this dissertation will invoke the utilitarian framework of Mougayar (2016) which lists blockchain technology touch-points as programmable assets, programmable trust, programmable ownership, programmable money, programmable identity, and programmable contracts. Swan (2015) provides other classifications for applications —see Appendix D. The details of each of Mougayar's six concepts will follow. Because blockchain technology applications may overlap with more than one touch-point, the examples offered under each are not necessarily mutually exclusive. Furthermore, because the concepts of programable assets and programable ownership are intricately conjoined, they will be combined in a single section.

### ***Appendix B.1: Programmable Assets and Programmable Ownership***

According to Swan (2015), blockchain technology allows registry, inventory, and exchange of hard assets such as houses and computers; intangible assets such as shares, reservations, and health data; and copyrights such as music albums, audible books, and digitized fine art. The exchange of assets is possible because blockchain immutably stores information about every transaction and ensures its legitimacy (Pilkington, 2015). In other words, the blockchain time-stamps documents signifying rights or ownership, therefore providing indisputable certifications that are cryptographically secure and enabling seamless verification capabilities (Mougayar, 2016) (Swan, 2015). As such, in a blockchain database, anything can be treated as a ‘smart property’ (Swan, 2015). Smart property is the notion of assigning a unique identifier such that an asset can be traced, administered, and exchanged (Swan, 2015). Mougayar (2016) considers smart property a native unit requirement for blockchain operations defined as a digitized version of an item that includes specific rights to use and typically has a value associated with it. Elaborating further, Mougayar states that smart property extends the concept of a digital asset by associating it to a blockchain such that it can never be double-spent, double-owned, or double-sent. As such, a smart property is "*an asset or thing that knows who owns it*" and, as such, it enables more possibilities, flexibility, and discoverability to facilitate frictionless decentralized peer-to-peer exchanges (Mougayar, 2016). However, that does not imply that related contracts concerning the exchanges are not subject to existing laws (Swan, 2015).

In this way, smart property enables things like domain name systems (DNS) as embodied by Namecoin—an open-source organization that seeks to heighten decentralization, security, censorship resistance, privacy, and speed of certain apparatuses of the Internet exemplified by DNS (Namecoin, n.d.)—and digital content distribution and anti-counterfeit—enabled by the immutability attribute which prevents double-spending, double-owning, or double-sending

(Mougayar, 2016; Wang et al., 2016). Another example listed by Swan (2015) is a pre-established smart contract that would automatically transfer a title deed of an automobile from the financing firm to the individual owner upon receiving the final payment. In this sense, blockchain becomes a single source of truth (Pilkington, 2015) for the latest status of ownership of assets. The absence of central human intervention to enforce verifiability is a fundamental blockchain technology novelty (Swan, 2015).

Blockchain technology enables irrefutable proofs that are cryptographically secure through the time-stamping of documents representing rights or ownership (Mougayar, 2016). As such, blockchain technology allows exact ownership and chain of custody to be ascertained (de Meijer, 2015). Consequently, for the legal sector, this facilitates efficient digital asset exchange concerning document and authorship verification, title transfers, and contract enforcement (Kiviat, 2015). Two of the established blockchain-based enterprises are Viacoin (VIAcoin, n.d.) which offers notarizing services through the timestamping, transfer, and verification of ownership of documents (Kiviat, 2015); and Libra (Libra, n.d.) which supplies business customers with reports, audits, and digital asset transactions analysis in any blockchain database (Pilkington, 2015).

Blockchain technology could furnish a transactional platform for sharing economy services (Mainelli & Smith, 2015), as it naturally allows trusted documentation of large-scale peer-to-peer activities (Lindman et al., 2017). Contrary to the misconception of considering Airbnb, Uber, and the like as sharing economy, these businesses do not share but rather aggregate, and in the process, they collect data for commercial exploitation (Tapscott & Tapscott, 2016). Moreover, Uber and Airbnb exemplify oligopolistic intermediaries according to Mougayar (2016). Swan (2015) expects the emergence of decentralized models of Airbnb—for

lodging, Getaround—for vehicles rentals, and LaZooz—for peer-based ride sharing. Backfeed is a leader in the sharing economy space. On its homepage, Backfeed mission statement is to develop a distributed governance system for blockchain-based applications that allows collaborative creation and distribution of value in spontaneously emerging networks of peers (Backfeed, n.d.). Toyota Research Institute has a vision to use blockchain technology to allow car owners to monetize seats, trunk space and other unused resources (Coindesk, 2017g). Vitalik Buterin, founder of the Ethereum blockchain said: “*Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly*” (Tapscott & Tapscott, 2016).

### ***Appendix B.2: Programmable Trust***

Joichi Ito, Director, MIT Media Lab said: “*Blockchain is to trust as the Internet is to information*” (Tapscott & Tapscott, 2016). Blockchain technology embeds trust as an intrinsic attribute of transactions by implanting rules that represent trust, making blockchain a platform for validating transactions via logic in the network, not via a protected database entry or central authority (Mougayar, 2016). Swan (2015) describes blockchain as trustless in the sense that users do not need to trust each other or a central intermediary, but only need to trust the system. She further explicates that the blockchains immutability, transparency, access, and reach enable global trust.

From executive stock exercises to online lottery to patenting—through time binding commitments with proof of knowledge—the blockchain trust fabric can transform any form of transaction. Democratic system could be strengthened by blockchain because the technology can elevate the level of trust in voting (de Meijer, 2015; Lindman et al., 2017) where transparency

(Zhao et al., 2016) and immutability attributes are the primary blockchain technology enablers. The technology could also be used for the creation of smart property where blockchain becomes an inventory, tracking, and an exchange mechanism for hard assets like diamonds, and for tracing the authenticity and origin of goods for socially responsible consumers and businesses (Lindman et al., 2017).

Blockchain technology can transform trust in supply chain management by exacting provenance (Kim & Laskowski, 2016; Zhao et al., 2016) because it furnishes a shared, consensus-based public ledger that can track the process from source to destination (Crosby et al., 2016; Zhao et al., 2016). According to Arvind Krishna, the director of research at IBM (Coindesk, 2017b), the technology could save billions of dollars spent in coordination costs in both capital markets and the shipping industry; a typical shipment gets scrutinized by about thirty administrations before reaching its final destination; blockchain technology is ideal to aggregate and transmit the certifications required during the process, and therefore could save 20 percent of the cost.

There has always been tension between transparency and privacy. Transparency enhances the collective trust—increased transparency provides increased levels of trust (Mougayar, 2016). Nevertheless, at users' level, trust is also concerned with privacy. In a public blockchain network, selective transparency and privacy are achieved via cryptographic technologies, where transactions can be verified without revealing all aspects of the identity of their user (Mougayar, 2016).

Another application of the trust feature in blockchain technology is prediction markets, where the platform could furnish a system for increased trust and confidence in the outcome of the process. For example, Predictious—enabling crowd predictions from the presidential

elections to the Oscars (Predictionous, n.d.)—and Fairlay—enables users to bet on sport events like horse races and popular events like elections (Fairlay, n.d.)—offer betting venues for the typical real-world outcomes (Swan, 2015). A distinct flavor of trust-based blockchain technology applications is distributed cloud storage—exemplified by Storj (Storj, n.d.) which allows users to store data securely, economically, and privately without a centralized authority (Kiviat, 2015; Tapscott & Tapscott, 2016). Storj uses peer-to-peer protocols to provide secure, and private cloud storage (Swan, 2015) that enables users to monetize their extra space in a manner that provides more trust and privacy, compared to regular clouds, because the data is encrypted and fragmented. Mougayar (2016) affirms that blockchain networks do not replace cloud computing, but rather unbundle and democratize parts of it.

Blockchain technology enables new business models and resolves the trust issue more efficiently via code-based networks (Zhao et al., 2016). A distinct and foundational blockchain technology application is an emerging business model called distributed autonomous organization—organizations with self-governed operations and user-produced value creation and rewards (Mougayar, 2016). The distributed autonomous organization is a transformational concept that could radically alter the architecture of trust, and subsequently, the structure of businesses.

### ***Appendix B.3: Programmable Identity***

Tapscott and Tapscott (2016) posit that blockchain technology will allow ‘the virtual you—your avatar’ be owned by you, hence, empowering you to reveal only what you needed to, depending on the situation, while whisking up your data crumbs when navigating the digital sphere. Moreover, the blockchain technology concept of zero-knowledge—ability to proof something without revealing information—protects the confidentiality of transactions and the

privacy of individuals where one can prove something without revealing any information about one's identity or the content of the transaction (Narayanan et al., 2016).

According to a Coindesk (2017c) article, about 2.4 billion individuals do not have a government-issued identity?, and for those who do, the current centralized systems that manage those identities are cumbersome at best. The article goes on to suggest that blockchain technology could aggregate fragmented identities and reputation systems that are spread out across numerous forms such as passports and birth certificates; and platforms like LinkedIn and Uber. Drummond Reed, chief trust officer of Evernym—a company building an identity network on a permissioned blockchain—argued that fear about privacy is unjustified, stating: "*You do not put private data on the chain. You put public data on the chain*" (Coindesk, 2017c). Put in a slightly different way, in a blockchain database, one can reveal their public elements of identity, while securely encrypt their private elements. Identity and reputation go together hand in hand. Identify reputation in the physical world is local according to Tapscott and Tapscott (2016)—shopkeepers, employers, friends—however, in the blockchain digital economy, reputations is globally portable, allowing a resident of Africa to establish the reputation required to borrow money from America. Ultimately, the technology enables an open, democratic, and scalable digital economy (Wang et al., 2016).

#### ***Appendix B.4: Programable Contracts***

Smart contracts are contracts that are digitally drafted and automatically enforced with the goal of attenuating human interventions (de Meijer, 2015; Yli-Huumo et al., 2016; Zhao et al., 2016), and hence, reduce transaction costs. Smart contracts are potentially a groundbreaking application of blockchain technology. Mougayar (2016) argues that smart contracts are a vital underpinning of blockchain technology and their role in blockchain technology is analogous to

how HTML allowed information to be openly publishable and linkable on the Web. The possibilities for programmable contracts were implanted into the blockchain protocol at its contrivance (Swan, 2015). Smart contracts potentially could substitute some of the functions currently executed by expensive and slow legacy intermediaries (Mougayar, 2016).

There are three elements of smart contracts that make them distinct: 1) autonomy—ensuing its launch the code acts on its own, 2) self-sufficiency—ability to direct resources on its own, and 3) decentralization—distributed over multiple servers where a smart contract is self-executing across the network (De Filippi, 2014; Swan, 2015). Therefore, a smart contract embodies ‘code is law’ because it will execute ‘no matter what’ in a fashion that could introduce a new paradigm that requires hefty absorption by the society for smart contracts to become common (Swan, 2015). However, Lindman et al. (2017) contend that the standing of smart contracts will upsurge by virtue of the broader adoption of the Internet of things.

A traditional contract is a promise between two or more parties to exchange commitments (Swan, 2015). She further posits that while trust plays a central role in traditional contracts, smart contracts minimize trust requirements because they are defined and executed by the code (Swan, 2015). Smart contracts do not change the expected outcome, they only lessen the role of human judgment (Swan, 2015). Steve Omohundro, president of think tank Self-Aware Systems, said: "*That intersection of legal descriptions and software is fundamental, and the smart contracts are the first step in that direction*" (Tapscott & Tapscott, 2016). Smart contracts will potentially attenuate court litigations (de Meijer, 2015) and enable frictionless transactions.

Since the launch of Ethereum in 2015, smart contracts enjoyed increased cognizance. Ethereum actualizes the possibilities of smart contracts by furnishing an open source platform (Ethereum, n.d.) that is foundational to its mission (Mougayar, 2016). Smart contracts stimulate

autonomous economic agents and decentralized autonomous organizations where code displaces human management and traditional corporations (Tapscott & Tapscott, 2016) because coupled with the underlying blockchain platform, smart contracts enable innovative business models and settle the trust conundrum more profoundly (Zhao et al., 2016). As such, “*smart contract also provides a means for owners of assets to pool their resources and create a corporation on the blockchain, where the articles of incorporation are coded into the contract, clearly spelling out and enforcing the rights of those owners*” (Tapscott & Tapscott, 2016).

For example, a smart contract-based mortgage could reset automatically upon checking a prespecified agreement-encoded website (Swan, 2015) or could enable renting hotel rooms without human intervention (Zhao et al., 2016). Other simple examples listed by (Swan, 2015) are a smart contract that enacts a gift upon a grandchild’s eighteenth birthday, or a pre-established smart contract that automatically transfers the ownership of a car title to individual owner upon completion of payments. A final smart contract example is envisioned by Toyota Research Institute where vehicle's sensors could store driving data on a blockchain, hence, allowing owners to be eligible for lower insurance rates by virtue of increased transparency, reduce fraud, and access to driving data that measures safety habits (Coindesk, 2017d).

To interconnect smart contracts on the blockchain to off-chain databases, smart oracles are required. Smart oracles hold real-world information, such as an identity, a certificate, or any data element and could behave in an agent-like fashion to direct the smart contracts (Mougayar, 2016). Therefore, one could envisage a world of interconnections and interactions between smart contracts, smart oracles, Internet of Things, and artificial intelligence that would open a wide range of possibilities.

### ***Appendix B.5: Programmable Money***

As a continuation of the earlier chapter ‘General applications’, this section will discuss programmable money as the sixth and final chapter touch-point of blockchain technology according to the framework of Mougayar (2016). Although Bitcoin will be the focus of the discussion, the argument applies to any brand of cryptocurrency. Bitcoin is chosen because it is the first and the one with largest share in the cryptocurrency market, where numerous brands of cryptocurrency have emerged. One example is Litecoin—a platform similar to Bitcoin but faster (Kiviat, 2015).

Money is defined as a medium of exchange, a store of value, and a unit of account (Greeley, 2013; Van Alstyne, 2014). Although Bitcoins have no physical existence, no government sponsorship, and operate with mostly technical regulation, Bitcoin has all the of the three above mentioned attributes of money (Van Alstyne, 2014). Alternatively, according to Bjerg (2016) money could be conceptualized through any of three major theories: commodity theory, fiat theory, and credit theory; and “*it is arguable that Bitcoin is commodity money without gold, fiat money without a state, and credit money without debt.*” To the question of whether Bitcoin has value, Van Alstyne (2014) answers affirmatively that it already has. He further posits that, in the future, countries will establish their own cryptocurrency. Bitcoin adoption has increased rapidly, and today Bitcoin is honored as a unit of payment for various goods and services (Bjerg, 2016).

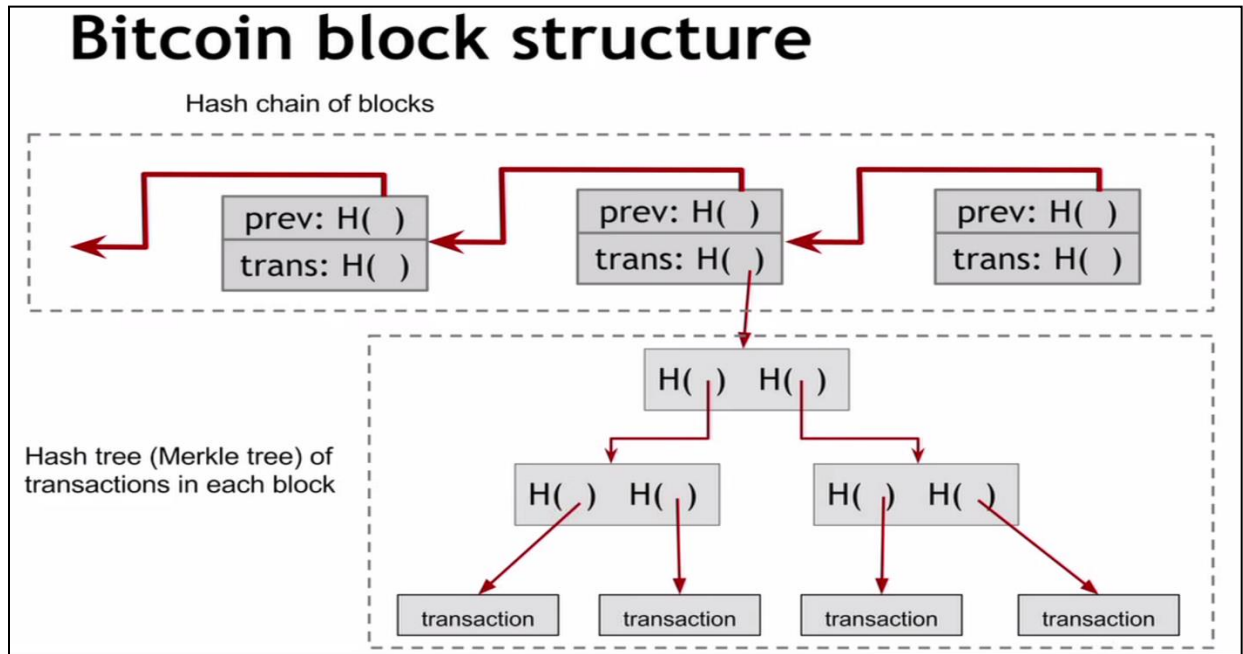
As explained earlier, new Bitcoins are produced by ‘miners’ as a reward for their computational participation in the bitcoin network. The cryptocurrency is then circulated in the blockchain user’s network and is thereafter exchanged with goods, services or traditional fiat currencies. Van Alstyne (2014) argues for Bitcoin over conventional exchange methods stating that a) the Bitcoin network furnishes a near frictionless commerce platform that enables less

expensive transactions (Andreessen, 2014), b) transcends credit cards at detecting fraud since Bitcoin transactions require public authentication, and c) the Bitcoin protocol guarantees that only authorized parties can spend from a specific account with a guaranteed desired level of privacy and pseudonymity. Nonetheless, the pseudonymity feature led some critics to raise concerns related to the misuse of cryptocurrency for unlawful activities (de Meijer, 2015; Van Alstyne, 2014). However, conventional payment methods are hardly any different in that respect. To the contrary, Van Alstyne (2014) argues that the preferred method of exchange for criminals is cash. Moreover, he avers that the immutability and traceability of the blockchain ledger make it possible for legal authorities to identify and track lawless activities.

Bitcoin presents a conceptual departure from conventional forms of money (Bjerg, 2016) and, therefore, is a fundamental change to some foundational basics in the financial industry. Consequently, it could existentially threaten traditional financial institutions because it radically alters the way transactions are conducted. Subsequently, the financial industry must explore how to benefit from cryptocurrency while adjusting for consequences that may not be advantageous. Consequently, de Meijer (2015) avers that financial institutions may benefit from collaborating with the ecosystem around crypto technology. Furthermore, a) cryptocurrencies are increasingly adopted by users, b) more salespoints are accepting cryptocurrency as a method for exchange, and c) the market cap of cryptocurrencies continues to increase—The reader may refer to Appendix E to appreciate the growth of market cap of cryptocurrency. Therefore, the financial industry cannot ignore the cryptocurrency growing phenomenon.

## Appendix C: Actual blockchain structure

Actual blockchain structure (Narayanan et al., 2016)



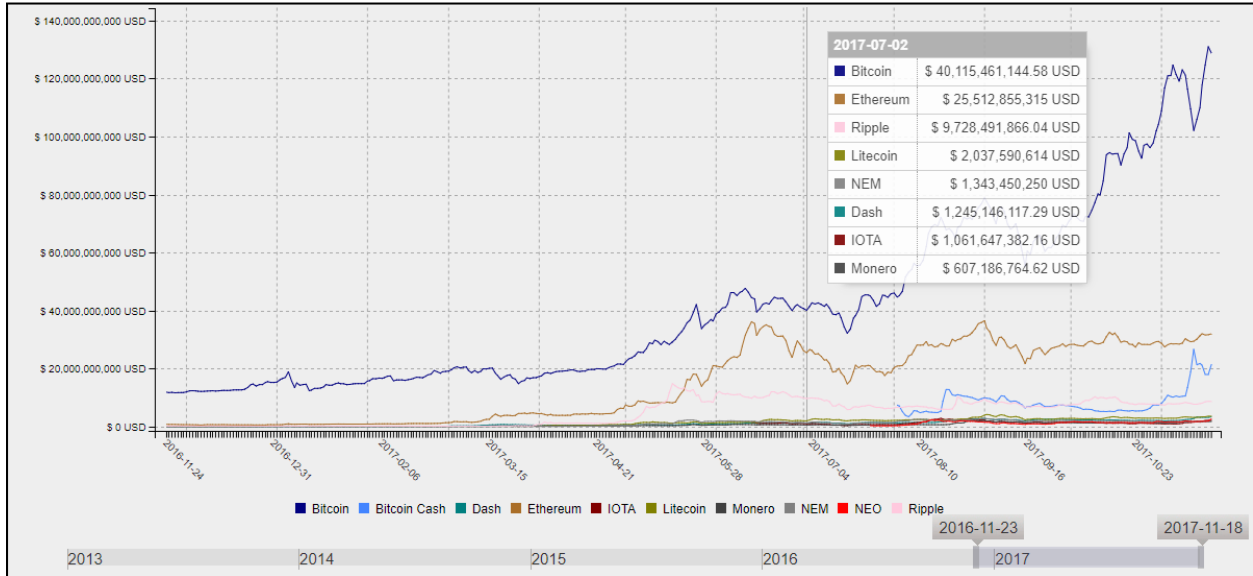
## Appendix D: Classes of Blockchain technology Non-Cryptocurrency Applications

### Blockchain Technology Applications Beyond Cryptocurrency (Swan, 2015)

Class	Examples
General	Escrow transactions, bonded contracts, third-party arbitration, multiparty signature transactions
Financial transactions	Stock, private equity, crowdfunding, bonds, mutual funds, derivatives, annuities, pensions
Public records	Land and property titles, vehicle registrations, business licenses, marriage certificates, death certificates
Identification	Driver's licenses, identity cards, passports, voter registrations
Private records	IOUs, loans, contracts, bets, signatures, wills, trusts, escrows
Attestation	Proof of insurance, proof of ownership, notarized documents
Physical asset keys	Home, hotel rooms, rental cars, automobile access
Intangible assets	Patents, trademarks, copyrights, reservations, domain names

## Appendix E: Market Cap of Top 10 Cryptocurrencies

### Market Cap of Top 10 Cryptocurrencies (cryptocurrencychart, n.d.).



## Appendix F: Major Research Paradigms

### Positivist, Interpretive, & Critical Paradigms (Myers, 2013)

<i>Positivism</i>	<i>Interpretivism</i>	<i>Critical Systems</i>
The dominant form of research in most business and management disciplines	Not as common but has gained ground over the past two decades	Much less common. However, there are signs of growth
Reality is objectively given and can be described by measurable properties, which are independent of the observer and their instruments	Access to reality is only through social constructions such as language, consciousness, shared meanings, and instruments. The observer is part of the reality constructed	Social reality is historically constituted and is produced and reproduced by people. Although people can consciously act to change their reality, they are constrained by forms of social, cultural, and political domination.
Aligns with the tools of the natural science.	The tools of the natural sciences are inappropriate for the study of social and organizational phenomena	Similar to interpretive
The language of science can be exact. Meanings are separate from facts.	Human science Languages is irreducibly equivocal and evolving. Meanings are the facts.	Similar to interpretive
Attempts to increase the predictive understanding of phenomena	Attempts to understand phenomena through the meanings that people assign to them	Challenges prevailing beliefs, values, and assumptions that might be taken for granted by the subjects.
Empirical data are assumed to be objective	The correct meaning of data is determined by the context	Different interpretations are given different weight or preference—sometimes imposed by some upon others.
Assumes value-free data and facts	Tries to be value-free, though acknowledging the	Explicit ethical basis that motivates the researcher

	difficulty	work
Propositions in terms of independent, dependent variables, and relationships	Focus instead on the complexity of human sense making as the situation emerges	Similar to Interpretive

## Appendix G: Recruitment E-mail

The following email was sent to each prospective participant in the study:

Request to Participate in a Georgia State University Research Regarding the Impact of

Blockchain **Subject:** Technology on the Financial Industry

### **Email Text:**

Dear <Name of candidate participant>,

As a subject matter expert on blockchain technology, you are cordially invited to participate in a research study. The purpose of the study is to investigate the impact of blockchain technology on the financial sector.

Please feel free to read exact details in the ‘informed consent form’ attached. If you agree to participate, we will contact you to arrange for a time slot convenient to you.

Participation in the research is voluntary and consists of a single interview over the phone, lasting no more than 1 hour. You may skip questions or stop participating at any time.

Your name and other facts that might point to you will not appear when the researchers present this study or publish its results. The findings will be summarized and reported in a synthesized form. You will not be identified personally. Nor will your organization be identified.

### **Summary:**

**Name and contact information of the interviewer:** Al Tilooby at 510-770-4599 or [aali38@student.gsu.edu](mailto:aali38@student.gsu.edu)

**Where the research will be conducted:** Over the phone from Georgia State University

**Purpose of research:** To investigate the impact of blockchain technology on the financial sector

**A summary of the criteria that will be used to determine eligibility:** Financial industry blockchain technology executives, senior blockchain technology subject matter experts, and blockchain technology researchers.

**A brief list of participation benefits:** There are no direct benefits to you personally.

Overall, the research team hope to contribute the following to the existing body of knowledge:

- Contribution to practitioners: How financial institutions can prepare for blockchain technology opportunities and threats.
- Contribution to the literature: A synthesis of the extant financial literature related to blockchain technology, coupled with empirical accounts of industry perception of the future impact of blockchain technology.

- Contribution to the theory: A theoretical interpretation of blockchain technology as a disruptive technology in terms of transaction cost theory.

**The number of participants to be enrolled:** 16 participants.

**Time or other commitment required:** 1-hour interview conducted in a single session.

**Compensation, if any:** You will not receive compensation for participating in this research.

Thank you and Best Regards,

Name: Al Tilooby

Candidate – Doctorate in Business

J. Mack Robinson College of Business

Georgia State University

35 Broad Street, NW, Suite 427

Atlanta GA 30303

e-mail: [aali38@student.gsu.edu](mailto:aali38@student.gsu.edu)

phone: +1-510-770-4599

## **Appendix H: Informed Consent From**

The following form was sent to and discussed with and accepted by all participants before the interviews.

**Georgia State University  
Department of Computer Information Systems**

### **Informed Consent**

**Title:** The impact of blockchain technology on financial transactions

**Investigators:** Lars Mathiassen and Al Tilooby

#### **I.Purpose:**

You are invited to participate in a research study. The purpose of the study is to investigate the impact of blockchain technology on financial transactions with focus on **asset verification, record keeping, data privacy, and transaction costs**. You are invited to participate because you are a subject matter expert. Sixteen participants will participate in this study. Each participant will individually be interviewed over the phone for a maximum of one hour at a time slot of their convenience.

#### **II.Procedures:**

If you decide to participate, one of the investigators will contact you to arrange for a time slot convenient to you, then call you at the time to conduct and record the interview. The audio recordings will be captured on the investigator's smart phone that is password-protected. The recording will be destroyed after the completion of the transcriptions to protect the confidentiality of the data. Only one investigator will conduct your interview.

#### **III.Risks:**

In this study, you will not have any more risks than you would in a normal day of life.

#### **IV.Benefits:**

Participation in this study may not benefit you personally. Overall, we hope that the society will benefit from the contributions of this study to the existing body of knowledge as follows:

- a) Contribution to practitioners: How the financial organizations can prepare for blockchain technology opportunities and threats.
- b) Contribution to the literature: A synthesis of the extant financial literature related to blockchain technology, coupled with empirical accounts of industry perception of the future impact of blockchain.
- c) Contribution to the theory: A theoretical interpretation of blockchain as a disruptive technology in terms of transaction cost theory.

#### **V. Voluntary Participation and Withdrawal:**

Participation in research is voluntary. You do not have to be in this study. If you decide to be in the study and change your mind, you have the right to drop out at any time. You may skip questions or stop participating at any time. Whatever you decide, you will not lose any benefits to which you are otherwise entitled to.

#### **VI. Confidentiality:**

The investigators will keep your records private to the extent allowed by law. Dr. Lars Mathiassen, and Al Tilooby will have access to the information you provide. Information may also be shared with those who make sure the study is done correctly—GSU Institutional Review Board, the Office for Human Research Protection (OHRP). The investigators will use your initials instead of your name on the study records. The information you provide will be stored on a password-protected smartphone for audio, and password-protected computer for taking notes and transcribing. The audio recording will be stored for no more than two weeks and then destroyed after the completion of the transcriptions to protect the confidentiality of the data. Your name and other facts that might point to you or the institution you work for will not appear when the researchers present this study or publish its results. The findings will be summarized and reported in a synthesized form. You will not be identified personally. Nor will your organization be identified.

#### **VII. Contact Persons:**

Contact Lars Mathiassen at 404-413-7855 or [lars.mathiassen@ceprin.org](mailto:lars.mathiassen@ceprin.org); or Al Tilooby at 510-770-4599 or [aali38@student.gsu.edu](mailto:aali38@student.gsu.edu) if you have questions, concerns, or complaints about this study. You can also call if you think you have been harmed by the study. Call Susan Vogtner in the Georgia State University Office of Research Integrity at 404-413-3513 or [svogtner1@gsu.edu](mailto:svogtner1@gsu.edu) if you want to talk to someone who is not part of the study team. You can talk about questions, concerns, offer input, obtain information, or suggestions about the study. You can also call Susan Vogtner if you have questions or concerns about your rights in this study.

#### **VIII. Copy of Consent Form to Participant:**

Please save a copy of this consent form for your records.

If you are willing to volunteer for this research and be audio recorded, please continue with the interview.

## Appendix I: Interview Protocol

The following semi-structured interview protocol was conducted with each of the study participants:

### Interview Metadata

Date	
Initials of the interviewee	
Category of the interviewee: 1. Financial industry executive 2. Senior blockchain technology subject matter experts 3. Blockchain technology researcher	
Length of Interview	

### Introductory script:

*Hi <participant's name>. Thanks for accepting to participate in this study. My name is Al Tilooby. I am a candidate for a doctoral degree in business at Georgia State University. Please let me know if you have questions about the informed consent form, or other general questions.*

*Thank you <participant's name>. If you are willing to volunteer for this research and be audio recorded, please continue with the interview. And With your permission, I am going to start the recording and take notes as well.*

*Just to make sure I ask the right questions, please tell me a bit about you and your background.*

*Thank you <participant's name>. The purpose of our interview today is to gather your perspective as input to our research study. The study is to understand the impact of blockchain technology on financial transactions with emphasis on **asset verification, record keeping, data***

*privacy, and transaction costs. You have been selected to participate in this study because you are a subject matter expert.*

### Semi-Structured Interview Questions

How could blockchain technology enhance asset verification in financial transactions?	What are some of the challenges and issues the financial industry could face with blockchain technology regarding asset verification in financial transactions?	Any regulatory aspects to watch out for in relation to blockchain technology and asset verification in financial transactions?
How could blockchain technology enhance record keeping in financial transactions?	What are some of the challenges and issues the financial industry could face with blockchain technology regarding record keeping in financial transactions?	Any regulatory aspects to watch out for in relation to blockchain technology and record keeping in financial transactions?
How could blockchain technology strengthen data privacy in financial transactions?	What are some of the challenges and issues the financial industry could face with blockchain technology related to data privacy protection in financial transactions?	Any regulatory aspects to watch out for in relation to blockchain technology and data privacy in financial transactions?
Could blockchain technology decrease financial transaction costs?	What are some of the challenges and issues the financial industry could face with transaction costs in relation to blockchain technology?	Any regulatory aspects to watch out for in relation to blockchain technology and transaction costs in financial transactions?
Any use cases for blockchain technology you could think of in financial transactions with regards to	Challenges and issues that arise from these use cases?	Regulatory impacts due to these use cases?

asset verification, record keeping, data privacy, or transaction costs.		
What is the likelihood that the financial industry will implement blockchain technology with regards to asset verification, record keeping, data privacy, or transaction costs.	Roadblocks?	Regulatory concerns
Any further concluding insights and thoughts?		

## REFERENCES

- Accenture. (2015). THE FUTURE OF FINTECH AND BANKING: DIGITALLY DISRUPTED OR REIMAGINED? Retrieved from [https://www.accenture.com/t20150707T195228\\_w\\_lven/acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub\\_11/Accenture-Future-Fintech-Banking.pdf](https://www.accenture.com/t20150707T195228_w_lven/acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Future-Fintech-Banking.pdf)
- Alchian, A. A., & Demsetz, H. (1972). Production, information costs, and economic organization. *The American economic review*, 62(5), 777-795.
- Allison, I. (2015). Bank of England: Central banks looking at 'hybrid systems' using Bitcoin's blockchain technology. Retrieved from <http://www.ibtimes.co.uk/bank-england-central-banks-looking-hybrid-systems-using-bitcoins-blockchain-technology-1511195>
- Anderson, E., & Gatignon, H. (1986). Modes of foreign entry: A transaction cost analysis and propositions. *Journal of international business studies*, 17(3), 1-26.
- Andreessen, M. (2014). Why Bitcoin Matters. *The New York Times*, 21.
- Atzori, M. (2016). Blockchain-based architectures for the internet of things: a survey.
- Auctus\_Team. (2017). Smart Contracts Ideal Use Cases. Retrieved from <https://medium.com/auctus/smart-contracts-ideal-uses-cases-930a9ca6a02f>
- Azevedo, J. (1997). Mapping reality. *An Evolutionary Realist Methodology for the Natural and Social Sciences*.
- Backfeed. (n.d.). Backfeed Website. Retrieved from <http://backfeed.cc/>

- Badev, A. I., & Chen, M. (2014). Bitcoin: Technical background and data analysis.
- Bansal, S., Bruno, P., Istace, F., & Niederkorn, M. (2016). A mixed year for the global payments industry. Retrieved from <http://www.mckinsey.com/industries/financial-services/our-insights/a-mixed-year-for-the-global-payments-industry>
- Bechara, J., & Van de Ven, A. (2007). Philosophy of science underlying engaged scholarship. *Engaged Scholarship*, 12(2), 233-239.
- Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). *Blockchain-the Gateway to Trust-Free Cryptographic Transactions*. Paper presented at the ECIS.
- Bhaskar, R. (1978). A Realist Theory of Science, Brighton. *Google Scholar*.
- Bhaskar, R. (1994). Plato y otros. *The problems of Philosophy and their resolution*.
- BitcoinCore. (n.d.). Running A Full Node. Retrieved from <https://bitcoin.org/en/full-node#what-is-a-full-node>
- BitcoinWiki. (n.d.). Full node. Retrieved from [https://en.bitcoin.it/wiki/Full\\_node](https://en.bitcoin.it/wiki/Full_node)
- Bitnodes. (2018). Reachable nodes as of Tue Feb 20 2018 22:44:24 GMT-0500 (Eastern Standard Time). Retrieved from <https://bitnodes.earn.com/>
- Bjerg, O. (2016). How is Bitcoin Money? *Theory, Culture & Society*, 33(1), 53.
- Blockchain**. (n.d.). Latest Blocks. Retrieved from <https://blockchain.info/>
- Bollen, R. (2013). The legal status of online currencies: are bitcoins the future? *Browser Download This Paper*.

Brown, R. G. (2014). THE “UNBUNDLING OF TRUST”: HOW TO IDENTIFY GOOD CRYPTOCURRENCY OPPORTUNITIES? Retrieved from

<http://gandal.me/2014/11/14/the-unbundling-of-trust-how-to-identify-good-cryptocurrency-opportunities/>

Buterin, V. (2015). On Public and Private Blockchains. Retrieved from

<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>

Charmaz, K. (2014). *Constructing grounded theory*: Sage.

Cheung, S. N. S. (1969). Transaction Costs, Risk Aversion, and the Choice of Contractual Arrangements. *Journal of Law and Economics*, 12(1), 23-42.

doi:<http://www.jstor.org/action/showPublication?journalCode=jlaweconomics>

Coase, R. H. (1937). The Nature of the Firm. *Economica*, 4(16), 386.

Coase, R. H. (2013). The Problem of Social Cost. *JOURNAL OF LAW & ECONOMICS*, 56(4), 837-877.

Coindesk. (2017a). Blockchain Q1 Report. Retrieved from <http://www.coindesk.com/coindesk-releases-state-of-blockchain-q1-2017-research-report/>

Coindesk. (2017b). IBM Thinks Blockchain Could Save Shipping Industry 'Billions'. Retrieved from <https://www.coindesk.com/consensus-2017-ibm-thinks-blockchain-save-shipping-industry-billions/>

- Coindesk. (2017c). People and Machine Problems – Solved with Blockchain? Retrieved from <https://www.coindesk.com/consensus-2017-people-and-machine-problems-solved-with-blockchain/>
- Coindesk. (2017d). Toyota's R&D Division is Building a Blockchain Consortium. Retrieved from <https://www.coindesk.com/toyota-consortium-research-blockchain/>
- Coletti, P. (2015). Bitcoin's baby: Blockchain's 'tamper-proof' revolution. Retrieved from <http://www.bbc.com/news/technology-32781244>
- Commons, J. R. (1931). Institutional Economics, 648.
- Commons, J. R. (1932). The problem of correlating law economics and ethics. *Wis. L. Rev.*, 8, 3.
- Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2, 6-10.
- cryptocurrencychart. (n.d.). cryptocurrencychart. Retrieved from <http://www.cryptocurrencychart.com/>
- De Filippi, P. (2014). Primavera De Filippi on Ethereum: Freenet or Skynet? The Berkman Center for Internet and Society at Harvard University. Retrieved from <https://www.youtube.com/watch?v=slhuidzccpI>
- de Meijer, C. R. W. (2015). The UK and Blockchain technology: A balanced approach. *Journal of Payments Strategy & Systems*, 9(4), 220-229.
- de Meijer, C. R. W. (2016). Blockchain and the securities industry: Towards a new ecosystem. *Journal of Securities Operations & Custody*, 8(4), 322-329.

- DeRose, C. (2015). BankThink Behind the Ingenious Security Feature that Powers the Blockchain. Retrieved from <https://www.americanbanker.com/opinion/behind-the-ingenious-security-feature-that-powers-the-blockchain>
- DuPont, Q., & Maurer, B. (2015). Ledgers and Law in the Blockchain. *Kings Review* (23 June 2015) <http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain>.
- Dyer, J. H. (1997). Effective interfirm collaboration: how firms minimize transaction costs and maximize transaction value. *Strategic Management Journal*, 535-556.
- Ethereum. (n.d.). Ethereum website. Retrieved from <https://ethereum.org/>
- Fairlay. (n.d.). Retrieved from <https://fairlay.com/>
- FINRA. (2017). *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*. Retrieved from [http://www.finra.org/sites/default/files/FINRA\\_Blockchain\\_Report.pdf](http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf)
- Fortune. (2016). Blockchain Will Be Used by 15% of Big Banks By 2017. Retrieved from <http://fortune.com/2016/09/28/blockchain-banks-2017>
- Geyskens, I., Steenkamp, J.-B. E. M., & Kumar, N. (2006). MAKE, BUY, OR ALLY: A TRANSACTION COST THEORY META-ANALYSIS. *Academy of Management Journal*, 49(3), 519-543. doi:10.5465/AMJ.2006.21794670

- Giaglis, G. M., & Kypriotaki, K. N. (2014). *Towards an Agenda for Information Systems Research on Digital Currencies and Bitcoin*. Paper presented at the International Conference on Business Information Systems.
- Gilbert, H., & Handschuh, H. (2003). *Security analysis of SHA-256 and sisters*. Paper presented at the International workshop on selected areas in cryptography.
- Greeley, B. (2013). The Dollar Will Never Fall to Bitcoin. *Bloomberg Businessweek*.
- Gregor, S. (2006). The nature of theory in information systems. *MIS quarterly*, 611-642.
- Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, 2(1), 24.
- Hennart, J.-F. (1993). Explaining the swollen middle: Why most transactions are a mix of “market” and “hierarchy”. *Organization science*, 4(4), 529-547.
- Husted, B. W., & Folger, R. (2004). Fairness and Transaction Costs: The Contribution of Organizational Justice Theory to an Integrative Model of Economic Organization, 719.
- IBM. (n.d.). IBM Blockchain. Retrieved from <https://www.ibm.com/blockchain/what-is-blockchain.html>
- Ingram, C., & Morisse, M. (2016). *Almost an MNC: Bitcoin Entrepreneurs' Use of Collective Resources and Decoupling to Build Legitimacy*. Paper presented at the System Sciences (HICSS), 2016 49th Hawaii International Conference on.

- Irrera, A., & Shumaker, L. (2017). UPDATE 3-JPMorgan Chase & Co leaves blockchain consortium R3. Retrieved from <http://www.cnbc.com/2017/04/27/reuters-america-update-3-jpmorgan-chase-co-leaves-blockchain-consortium-r3.html>
- Kakavand, H., & Kost De Sevres, N. (2016). *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies.*
- Kim, H. M., & Laskowski, M. (2016). Towards an ontology-driven blockchain design for supply chain provenance.
- Kiviat, T. I. (2015). BEYOND BITCOIN: ISSUES IN REGULATING BLOCKCHAIN TRANSACTIONS. *Duke Law Journal*, 65(3), 569-608.
- Klein, B., Crawford, R. G., & Alchian, A. A. (1978). Vertical integration, appropriable rents, and the competitive contracting process. *The journal of Law and Economics*, 21(2), 297-326.
- Lawrence, P. R. (1992). The challenge of problem-oriented research. *Journal of Management Inquiry*, 1(2), 139-142.
- Lee, A. S. (2001). MIS quarterly's editorial policies and practices. *MIS quarterly*, 25(1), iii-vii.
- Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information systems research*, 14(3), 221-243.
- Lee, B., & Lee, J.-H. (2017). Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *The Journal of Supercomputing*, 73(3), 1152-1167.
- Libra. (n.d.). Libra Blockchain. Retrieved from <http://www.libra.tech/home-business/blockchain/>

- Liebenau, J., & Elaluf-Calderwood, S. M. (2016). Blockchain Innovation Beyond Bitcoin and Banking.
- Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). Opportunities and Risks of Blockchain Technologies—A Research Agenda.
- Llewellyn, K. N. (1931). What price contract?. An essay in perspective. *The Yale Law Journal*, 40(5), 704-751.
- Locke, E. A., & Latham, G. P. (2004). What should we do about motivation theory? Six recommendations for the twenty-first century. *Academy of management review*, 29(3), 388-403.
- Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *The Journal of Financial Perspectives*, 3(3), 38-69.
- MasterCard. (n.d.). How the payment process works. Retrieved from <https://www.mastercard.us/en-us/merchants/start-accepting/payment-process.html>
- Mathiassen, L. (2017). Designing Engaged Scholarship: From Real-World Problems to Research Publications. *Engaged Management ReView*, 1(1), 2.
- Mattila, J. (2016). The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures.
- McKinsey. (2016). Blockchain—Disrupting the Rules of the Banking Industry.

Milgrom, P., & Roberts, J. (1990). Bargaining costs, influence costs, and the organization of economic activity. *Perspectives on positive political economy*, 57, 60.

Milgrom, P., & Roberts, J. (1992). Economics, organization and management.

Mingers, J. (2001). Combining IS research methods: towards a pluralist methodology. *Information systems research*, 12(3), 240-259.

Mingers, J., & Brocklesby, J. (1997). Multimethodology: towards a framework for mixing methodologies. *Omega*, 25(5), 489-509.

Mori, T. (2016). Financial technology: Blockchain and securities settlement. *Journal of Securities Operations & Custody*, 8(3), 208-217.

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*: John Wiley & Sons.

Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, 59(6), 411-423.

Myers, M. D. (2013). *Qualitative research in business and management*: Sage.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, 17(1), 2-26.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Namecoin. (n.d.). Namecoin. Retrieved from <https://namecoin.org/>

- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*: Princeton University Press.
- Nasdaq. (2015). NASDAQ LINQ ENABLES FIRST-EVER PRIVATE SECURITIES ISSUANCE DOCUMENTED WITH BLOCKCHAIN TECHNOLOGY. Retrieved from <http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326>
- Oliver Wyman, Anthemis Group, & Santander Innoventures. (2015). The Fintech 2.0 Paper: rebooting financial services. Retrieved from <http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf>
- Ouchi, W. G. (1980). Markets, bureaucracies, and clans. *Administrative science quarterly*, 129-141.
- Pazaitis, A., De Filippi, P., & Kostakis, V. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. *Technological Forecasting and Social Change*. doi:<https://doi.org/10.1016/j.techfore.2017.05.025>
- Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money* (pp. 239-278): Springer.
- Pilkington, M. (2015). Blockchain technology: principles and applications. *Browser Download This Paper*.

- Pollak, R. A. (1985). A transaction cost approach to families and households. *Journal of economic Literature*, 23(2), 581-608.
- Predictious. (n.d.). Retrieved from <https://www.predictious.com/>
- Princeton University. (2014). Bitcoin and Cryptocurrency Technologies. Retrieved from <https://www.coursera.org/learn/cryptocurrency>
- PwC. (2017). FinTech Report. Retrieved from <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2017.pdf>
- R3. (n.d.). R3 website. Retrieved from <https://www.r3.com/>
- Rechtman, Y. (2017). Blockchain: The Making of a Simple, Secure Recording Concept. *CPA Journal*, 87(6), 15-17.
- Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data*: Sage.
- Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics*, 69(1), 99-118.
- Storj. (n.d.). Retrieved from <https://storj.io/>
- Strauss, A. L., & Corbin, J. (1990). Basics of qualitative research (Vol. 15). In: Newbury Park, CA: Sage.
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc."
- Swanson, T. (2014). Great chain of numbers: A guide to smart contracts, smart property and trustless asset management. *Amazon Digital Services*.

- Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world*: Penguin.
- Tapscott, D., & Tapscott, A. (2017). How Blockchain Will Change Organizations. *MIT Sloan Management Review*, 58(2), 10-13.
- Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46): Sage.
- Tejgland, R., Yetis, Z., & Larsson, T. O. (2013). Breaking out of the bank in Europe-exploring collective emergent institutional entrepreneurship through bitcoin.
- Trochim, W., Donnelly, J. P., & Arora, K. (2015). *Research methods: The essential knowledge base*: Nelson Education.
- Tsai, W.-T., Blower, R., Zhu, Y., & Yu, L. (2016). A System View of Financial Blockchains. *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 450.
- Van Alstyne, M. (2014). Why Bitcoin has value. *Communications of the ACM*, 57(5), 30-32.
- Van de Ven, A. H. (2007). *Engaged scholarship: A guide for organizational and social research*: Oxford University Press on Demand.
- VIAcoin. (n.d.). Retrieved from <http://viacoin.org>
- Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation*, 2(1), 1.

- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.
- Williamson, O. E. (1973). Markets and Hierarchies: Some Elementary Considerations, 316.
- Williamson, O. E. (1975). *Markets and hierarchies, analysis and antitrust implications : a study in the economics of internal organization*: New York : Free Press, [1975].
- Williamson, O. E. (1979). Transaction-Cost Economics: The Governance of Contractual Relations, 233.
- Williamson, O. E. (1985). *The economic institutions of capitalism: firms, markets, relational contracting*: Free Press.
- Williamson, O. E. (1988). Technology and transaction cost economics. A reply. *Journal of Economic Behavior and Organization*, 10, 355-363. doi:10.1016/0167-2681(88)90055-8
- Williamson, O. E. (1991). Comparative economic organization: The analysis of discrete structural alternatives. *Administrative science quarterly*, 269-296.
- Williamson, O. E. (1994, 02//). Research needs and opportunities in transaction cost economics, Editorial. *Journal of the Economics of Business*, p. 45. Retrieved from <http://ezproxy.gsu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9705301163&site=eds-live>
- Williamson, O. E. (2008). TRANSACTION COST ECONOMICS: THE PRECURSORS. *Economic Affairs*, 28(3), 7-14. doi:10.1111/j.1468-0270.2008.00838.x

- Williamson, O. E. (2010a). Transaction Cost Economics: The Natural Progression. *Journal of Retailing*. doi:10.1016/j.jretai.2010.07.005
- Williamson, O. E. (2010b). Transaction Cost Economics: The Origins. *Journal of Retailing*, 86(3), 227-231. doi:10.1016/j.jretai.2010.07.006
- Williamson, O. E. (2014). THE TRANSACTION COST ECONOMICS PROJECT. *Montenegrin Journal of Economics*, 10(1), 7.
- Witte, J. H. (2016). The Blockchain: A Gentle Four Page Introduction. *arXiv preprint arXiv:1612.06244*.
- Workie, H., & Jain, K. (2017). Distributed ledger technology: Implications of blockchain for the securities industry. *Journal of Securities Operations & Custody*, 9(4), 347-355.
- Yin, R. K. (2013). *Case study research: Design and methods*: Sage publications.
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?-A Systematic Review. *Plos One*, 11(10), e0163477-e0163477. doi:10.1371/journal.pone.0163477
- Zajac, E. J., & Olsen, C. P. (1993). From transaction cost to transactional value analysis: Implications for the study of interorganizational strategies. *JOURNAL OF MANAGEMENT STUDIES*, 30(1), 131-145.
- Zhao, J., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, 2(1), 1.

Zhu, H., & Zhou, Z. (2016). Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. *Financial Innovation*, 2(1), 1.

## VITA

Al Tilooby is a consultant on strategy formulation, business transformation, business technology enablement, organization management, blockchain and distributed ledger, finTech, support and professional services.

Led high-impact large-scale programs to expand business outcomes. Fluent with innovative development frameworks, processes optimization methodologies, change management, and leadership influencing skills.

Research interest comprises blockchain, finTech, information systems, organization management, emerging markets, and executive decision making.

Doctorate in Business: Georgia State University

MS, Interdisciplinary Telecom: University of Colorado at Boulder

BS, Electrical Engineering: University of Khartoum