EXPLORING TECHNOLOGY TRUST IN BITCOIN: THE BLOCKCHAIN EXEMPLAR

Research paper

Sadhya, Vikram, Louisiana State University, Louisiana, USA, vsadhy1@lsu.edu

Sadhya, Harshali, Louisiana State University, Louisiana, USA, hsadhy1@lsu.edu

Hirschheim, Rudy, Louisiana State University, Louisiana, USA, rudy@lsu.edu

Watson, Edward, Louisiana State University, Louisiana, USA, ewatson@lsu.edu

Abstract

The acceptance of Bitcoin as an electronic currency is steadily on the rise. This implies there is a surge in the diffusion and adoption of the blockchain technology introduced by Bitcoin as well. Moreover, the potential of this novel disruptive technology has been acknowledged by academic researchers and practitioners alike. IS research has shown that trust is a significant antecedent enabling the adoption of a novel technology and attenuating the apprehensions of risk and uncertainty among consumers. Trust in a technology is formed by the trusting beliefs of a trustor regarding the trustworthiness of the IT artifact. The blockchain technology, the trustee, has features like cryptography, decentralization, hash functions, digital signature, consensus mechanism, which embody trust in the technology. We present an extensive description of Bitcoin as an instantiation of the blockchain technology, while offering a detailed account of the literature on trust in a technology. We conceptually present, through the use of knowledge mapping, how blockchain ensures trust in the technology. We propose future research directions for trust research in the blockchain context and urge IS academics to explore trust in this novel context.

Keywords: Bitcoin, Blockchain, Trust, Technology Trust, Trust in IS, Trust in Information Systems, Digital Ledger Technology, DLT, Argument Mapping, Knowledge Mapping.

1 Introduction

With a market capitalization of over $100 billion, average daily transaction value and number of regular active users in the millions along with a market price of over $10,000 (as of December 2017) (Worldcoinindex, 2017), it is clear that Bitcoin has become quite the phenomenon. Consequently, it draws the attention of diverse audiences. Bitcoin is the most widely adopted peer to peer form of electronic currency. It functions as a decentralized payment system enabling the transfer of funds without relying on any financial intermediaries (Nakamoto, 2008). The primary motive of this invention was to eliminate the need for a trusted third party in an economic exchange and enable fast micro transactions. But the contribution of Bitcoin is twofold. First, it created awareness about the idea and the need for a decentralized electronic currency system (Zohar, 2015). Secondly, it introduced a novel technology that now forms the foundation for a diverse range of applications being proposed and developed (Brenig et al., 2016). This new technology is most widely acknowledged as the blockchain technology, although other terms like distributed ledger technology are also being used. The blockchain technology is a novel information technology that combines cryptography, peer-to-peer computing and incentives to enable systems with networked trust where system wide consensus among the peers is achieved by different mechanisms (Wörner et al., 2016). Cryptography plays a major role in the design of this new technology. Hence a monetary application like Bitcoin, is often referred to as a "cryptocurrency" or more generally as

a "virtual currency" (Brenig et al., 2016). Another diverse range of applications named "decentralized consensus systems" (DCS) are being proposed and envisioned to have far-reaching consequences beyond the financial spheres of industries and societies (Brenig et al., 2016). Researchers have accredited trust for the diffusion, adoption and acceptance of technologies and proposed various conceptualizations of trust in different contexts. In this study, we speculate that the blockchain technology in Bitcoin is a manifestation of almost all the dimensions of trust in a technology identified by IS scholars. We adopt the idea of knowledge mapping, specifically the concept of argument mapping, to present and support our claims.

1.1 Motivation

The internet introduced different online technologies that transformed numerous industries and several aspects of societies; Likewise, the blockchain technology and the ensuing applications like DCS's have the potential to completely remodel entire businesses and other information-based industries as well (Tilson et al., 2010). In fact, cryptocurrencies are often considered the most conservative applications of the technology (Brenig et al., 2016). New concepts, applications, systems and organizations leveraging the capabilities of this novel technology are being proposed and developed almost every day (Glaser and Bezzenberger, 2015). More specifically, applications that require a network and rely on some form of ownership management to an underlying valuable asset are being redesigned as decentralized applications employing smart contracts (Fairfield, 2014); as for example decentralized digital content streaming and decentralized cloud storage. A new form of organization which operates without any human intervention and relies solely on a set of programmed, immutable rules in order to "orchestrate human and non-human interaction in intelligent ways" is being proposed (Buterin, 2014). These new organizations exist only virtually and are being coined as decentralized autonomous organizations (DAO) or companies (DAC). Although most of these early conceptualizations might not survive the test of time in their original envisioned form, those that do survive may have the chance to become the pioneers of the future. Thus, the underlying technology centered on the concept of decentralization may have significant implications for the future (Glaser and Bezzenberger, 2015).

Information systems (IS) research has recognized trust as a significant factor for the diffusion of innovations and the adoption of new technologies or online services, thereby reducing consumers' perceptions of risk and uncertainty regarding the new technology (Gefen et al., 2003). The rapid technological changes in today's digital world offer novel challenges with respect to trust. Also, the increasing adoption of digital services has made security of information and privacy of users important social issues (Öksüz et al., 2016). Moreover, concerns pertaining to trust, privacy and security have often been cited as the primary reasons for the limited adoption or sometimes even total repudiation of a new technology (Hoffman et al., 1999).

The blockchain technology has been labelled as a "trust - free technology" because it eliminates the need for implementing mechanisms to convey trust (Beck et al., 2016). While research has shown that Bitcoin users have primarily adopted the technology due to its perceived usefulness although inherently it is not easy to use in its current form, users are also apprehensive of the latent risk in the technology (Abramova and Böhme, 2016). Indeed, the blockchain technology is still emerging and not clearly understood by many. There is a high degree of uncertainty regarding this novel technology and the possible consequences of its adoption. A stream of IS research on Bitcoin and blockchain technology in general has focused on understanding the risk as perceived in the Bitcoin ecosystem (Glaser et al., 2014). It is known that trust is critical in a situation where there is high uncertainty and risk, as well as the possibility of undesirable outcomes (Fukuyama, 1995). IS research has explored trust in various forms and applications in different technologies and the research stream continues to evolve as new technologies are developed due to rapid innovation. But there is very limited IS research on understanding trust in the blockchain technology or Bitcoin (Glaser and Bezzenberger, 2015). Thus, the claim that blockchain is the "trust machine" (Economist, 2015) has not yet been contested extensively by the IS research community. The

blockchain technology presents a new context and plausible trust research stream for IS researchers to explore and in the process, contribute to the trust literature of the field.

The extended technology adoption model proposed by Gefen et al. (2003), established that trust is a significant antecedent for adoption along with the perceived usefulness and ease of use of the technology itself. We propose that because Bitcoin users realize the usefulness of this innovative technology and also recognize the inherent risks involved (Abramova and Böhme, 2016), they rely on trust to overcome the apprehensions of risks and adopt the technology. In this work, we draw on the most prominent IS research literature on IT artifact trust to conceptually assess trust in the blockchain technology as implemented in Bitcoin. Bitcoin is the first and most widely adopted application of the technology, hence we consider it as an archetype of the technology. An adequate understanding of the mechanisms of the technology is essential to comprehend how trust is ensured by the innovation. Additionally, the academic literature discussing the technology is largely inconsistent and does not present a congruent and complete picture. Thus, we construct a detailed description of the technology as implemented in Bitcoin to articulate the critical blockchain characteristics such as decentralization, cryptography, hash functions, consensus mechanism, anonymity, etc. and point out their contribution to trust in the technology. We present an overview of the trust literature in the IS discipline and primarily focus on the trust in the technology stream of the research. A systematic review of the trust literature was undertaken to identify the relevant constructs developed to measure trust in a specific technology. The dimensions of the identified constructs were mapped to the blockchain technology features to justify how the technology ensures trust in the present form. Whilst this conceptual work is not supported by empirical evaluation, it forms the foundational basis for our future planned empirical studies. The potential of the blockchain technology is undeniable and majority of the potential applications have not been anticipated yet. Thus, to realize and appropriate the potential of this innovation, it is imperative to understand the notion of trust in this context. In this paper, we explore the notion of trust and propose future research directions in this context.

In the following section, we present a technical description of the technology followed by the current state of IS research on the topic in section 3. Section 4 outlines the trust literature relevant to our study followed by a succinct description of the research methodology adopted and our proposed claims in section 5. The article concludes with a discussion and suggestions for future research in section 6, and we offer some conclusions in section 7.

2 Bitcoin: The Blockchain Technology Overview

Bitcoin, introduced as a peer-to-peer electronic currency system by the pseudonymous entity, Satoshi Nakamoto in early 2009, has expanded to a global network of thousands of computers. It was proposed as an alternative to the traditional fiat currencies to enable pseudonymous transfers between untrusted parties over the internet and to prevent double spending (Wörner et al., 2016). It is open source, decentralized and the transactions are recorded on a publicly available distributed ledger-like data structure called the blockchain (Nakamoto, 2008). The blockchain is literally what the name implies, a chain of blocks, and a block contains all the transaction records for a specific period of time (Beck et al., 2016); which at present is 10 minutes for Bitcoin (Bitcoin Wiki, 2017). Any user can access the entire history of transactions ever made by scanning the blockchain, all the way back to the first transaction of the first block on the open ledger (called the genesis block in Bitcoin). The blockchain is not stored centrally but rather available for download freely and thus distributed and replicated throughout the network (Bitcoin Wiki, 2017).

2.1 Nodes and Miners

The Bitcoin payment network is sustained by two important stakeholders, namely nodes and miners. Any user on the network can volunteer to serve as a node by executing the Bitcoin Core, which is a software available for free download. Nodes require some computational power to validate transactions but

substantial storage and are not rewarded any economic incentives for their participation. Nodes are the computers on the network which investigate the validity of the transactions and propagate them (Zohar, 2015). They only forward valid transactions to their immediate neighboring nodes until they reach the miners. If a node circulates an invalid transaction, the surrounding nodes abandon it for a specific time. But if the dishonest node continues its unethical behavior, it may be abandoned from the network permanently. Nodes are required to download either a full copy of the current blockchain or a truncated version of it and store it locally to participate in the transaction validation activity. The storage requirements for the nodes increase parallely as the size of the blockchain grows.

Miners are a class of unique workstations on the network requiring significant computational power and energy resources. They are responsible for the creation of blocks and the inclusion of valid transactions in them. In return, the miners are awarded bitcoins and they also receive the transaction fees of all those transactions included in the created block. Miners compete with each other in a race to be the first to create a block and claim the corresponding reward. Once a block is created, a message is broadcasted to the network of miners and nodes who verify the validity of the block. If found valid the nodes will incorporate that block into their copy of the blockchain and the miners will also. The miners will abandon their work on the current set of transactions and start working on creating the next block with transactions from the pool, waiting to be incorporated into a block (Antonopoulos, 2014).

2.2 Bitcoin Transaction

A transaction in the Bitcoin system is triggered by a wallet software and requires a public address and a private key (Sas and Khairuddin, 2017). There are no actual coins in the Bitcoin system but rather only transactions (Wörner et al., 2016). Bitcoin does not require any identifiable personal information of a user to allow participation in a transaction (Sas and Khairuddin, 2017). The wallet software runs on either the user's personal computer, or any mobile device or can be web based and generates wallet addresses which are public and visible to every participant on the network. Although the wallet addresses are public the identity of the owner is not and unless the owner of a public address claims its authority publically, it is very intricate to associate a real-world identity with the address (Sas and Khairuddin, 2017). These public wallet addresses are the pseudonymous identities of the users on the network and are representative of the account numbers in a traditional banking system (Zohar, 2015). But there is no restriction on the number of such addresses a user can generate; The creator, Nakamoto suggested the use of a new address for each new transaction for additional security and privacy (Nakamoto, 2008). Every public address has a corresponding private key that is stored by the wallet application. Thus, wallets store the public and private keys of a user and not the bitcoins (Antonopoulos, 2014). Bitcoins are transferred between two public addresses and the private key is used to prove ownership of the bitcoins for the particular public address initiating the transaction. The owner of the bitcoins digitally signs a transaction with the private key to indicate ownership of the cryptocurrency and can initiate a transfer to any other public address on the network. This digital signing (Table 1) is done by the wallet software implicitly and does not require the users' cognizance. But the security of the wallet, more specifically of the private keys, is the responsibility of the users. The public address can be used by any participant of the network to decrypt a digitally signed transaction to verify the legitimacy of the transaction. A transaction is broadcasted by the wallet software to its immediate neighboring nodes in the Bitcoin network, to be tested for validity and subsequently included in the blockchain (Sas and Khairuddin, 2017).

The Bitcoin system presents a unique way of representing and tracking of changes to the ownership of funds (Zohar, 2015). Every Bitcoin transaction is a reassignment of the ownership of the fund and consists of inputs as well as outputs (Zohar, 2015), and ideally the sum of the inputs should be equivalent to the sum of the outputs. If it is not equal, the unclaimed bitcoins are returned as change to the initiating user while the miners claim the ownership of the bitcoins specified as transaction fees. Also, each input has to refer to an output of a previous transaction to confirm its source. Cryptographic hash functions (Table 1)

are used to encrypt the transaction data for secure transmission over the network and subsequent storage in blocks. There are different algorithms that can be used for this function.

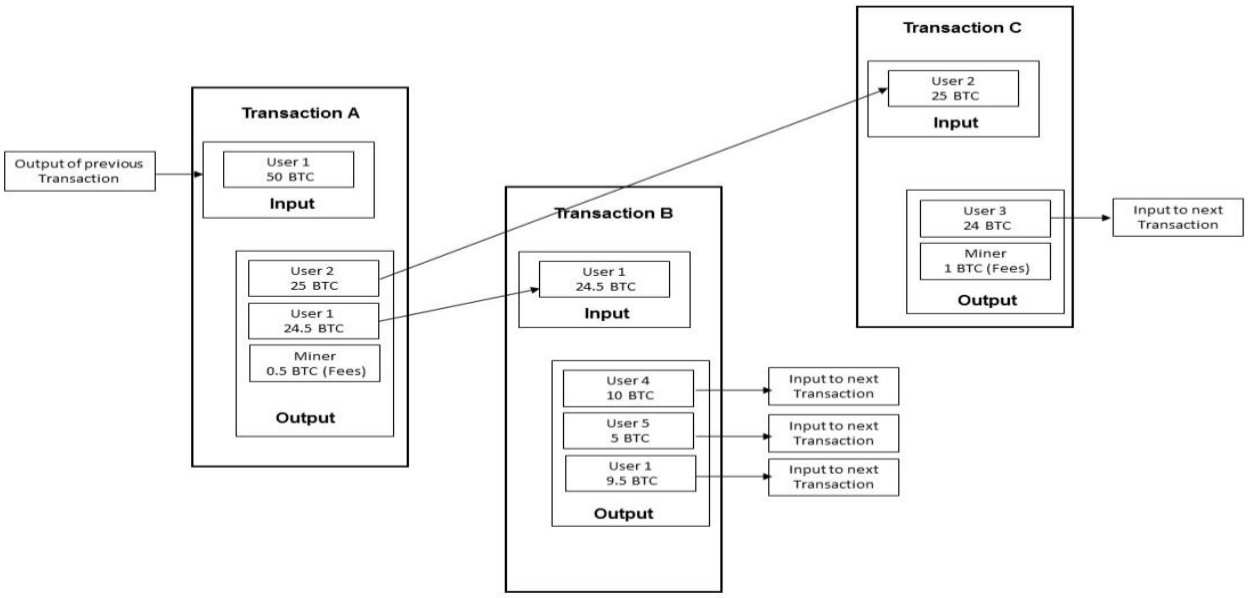

Figure 1. This figure shows three Bitcoin transactions comprised of inputs, outputs and miner fees.

Cryptography: The study of mathematical techniques related to information security aspects such as confidentiality, data integrity, entity authentication, and data origin authentication. It is a means or set of techniques for providing information security (Menezes et al., 1996).
Hash Function: A function that can transform an input of any size to an output of a fixed size called hash or digest. The function has the following properties – • It is deterministic, that is the same input always produces the same output • It is computationally quick and efficient to produce the hash for a given input • It is collision resistant implying that it is infeasible to find two inputs producing the same hash output • The input and the corresponding output are uncorrelated and thus ensures information hiding • The transformation is irreversible • A small change in the input changes the output entirely (Coron et al., 2005; Krawczyk et al., 1997).
Digital Signature: A user, A's digital signature is a value that depends on a message, M and a private key PK which is kept secret, such that anyone can verify the validity of A's signature using A's public key P. Thus, each user has two keys, one public key used for validating signatures and another private key, kept secret, used for producing the signatures. Digital signatures are used to prove ownership of digital assets (Goldwasser et al., 1988).

Table 1. Definitions of cryptography, hash function and digital signature.

2.3 Bitcoin Blocks

In the Bitcoin system, each block contains a special transaction called the coinbase transaction which is added by the miners competing to create a block. The coinbase transaction is always the first transaction in a block and it records the transfer of the bitcoins for the block reward to a public address claimed by the miner. However, it does not refer to the output of a previous transaction. Thus, Bitcoins are created out of thin air as rewards for creating blocks and transferred to public addresses of the miners. In a block, pairs of transactions are hashed and these hashes are hashed successively until a single hash is produced to

represent the set of transactions. This hash is called the merkle root (see Figure 2) of the transactions and the corresponding representation of the set of transactions in a tree like form is the merkle tree. The merkle root is distinct for each miner even for the same set of transactions because the first transaction in the set is always the coinbase transaction to the public address claimed by the miner; and, due to the collision resistant property of the hash function, the output of the hash is radically different by virtue of the different public address in the coinbase transaction.

A block header contains this merkle root, the hash of the previous block header, a unique string called the nonce and some other fields required for version control and time stamping (Bitcoin, 2017). The hash of all these fields in the block header is required to meet a criterion, a target that is specified by the Bitcoin protocol (Zohar, 2015). This criterion is usually a specific number of leading zeros in the hash of the block header being created. Thus, the miners compete to determine the nonce which is unique for each miner. The miners employ a brute force approach repetitively hashing the merkle root, hash of the previous block header and the other fields with a new random number every time to produce a hash that meets the requirement specified by the protocol. Therefore, the miners have to expend exponential amounts of computational power and energy resources to iterate swiftly to compete for the rewards. Once an acceptable random number, the nonce, is found which meets the criterion, the accountable miner broadcasts a message containing the nonce and its merkle root to the network for validation. The miners and nodes can hash the message to verify if it satisfies the requirement set by the protocol. Thus, verification is relatively much easier than the extensive computation required to determine the nonce and so even the nodes can participate in this verification. This mechanism of establishing consensus among the participants of a network is labelled as the proof of work, implying the miner had to expend considerable amount of computational power and energy resources to mine the block. Mining is this process of creating blocks and appending them to the blockchain by demonstrating proof of work, and thus the name miners.

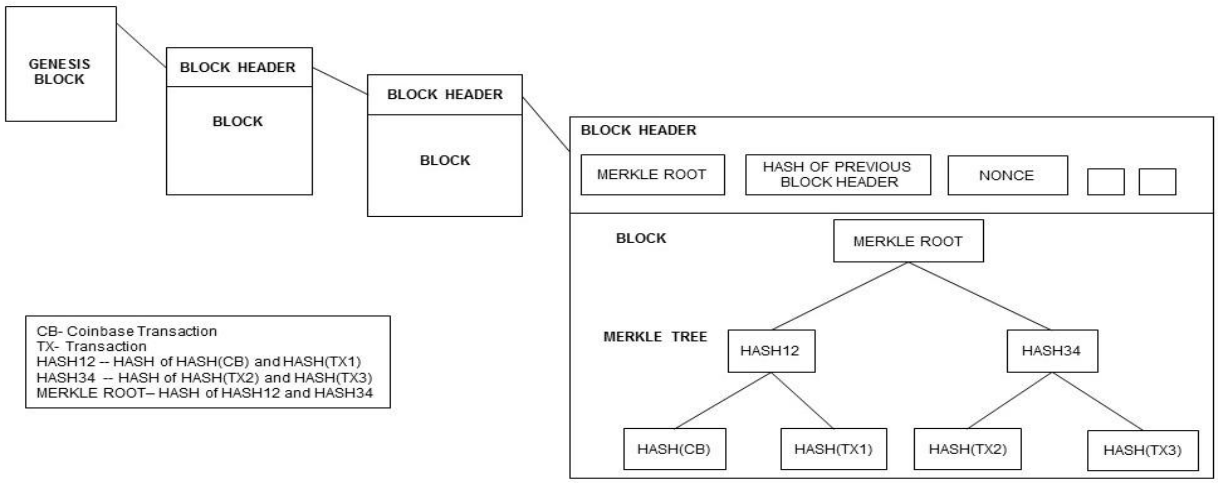

Figure 2. This figure shows a block containing transactions arranged in a merkle tree structure, its block header and the Bitcoin blockchain.

The reward value in the Bitcoin system is halved after every 210,000 blocks are mined which is approximately every four years. At the outset in 2009, the reward was 50 bitcoins for each block created. But the current reward is 12.5 bitcoins and this reduction will continue till the year 2140 when the reward will reduce to 1 Satoshi (1 Bitcoin = 100,000,000 Satoshis) (Blockchain, 2017). The total number of bitcoins to be mined is fixed at 21 million and by the year 2140 all those bitcoins will be mined and added to circulation. The protocol examines the network once every 2016 blocks are mined, which is

approximately every 2 weeks. The protocol adjusts the mining difficulty by altering the requirement of the nonce to ensure that the speed of mining is maintained to mine a block on an average every 10 minutes.

Bitcoin Statistics
A block is mined every: 10 minutes (on an average)
Number of blocks mined in a day: (60 / 10) * 24 = 144 (approximately)
Number of blocks mined in 2 weeks: 144 * 7 * 2 = 2016 (approximately)
Bitcoin mining difficulty level adjusted every: 2016 blocks
Number of blocks mined in 4 years (approximately): 210,000
Block reward halved every: 210,000 blocks

Table 2. Statistics representing Bitcoin mining.

The blockchain technology is secure because of the immutability it ensures by the hashing algorithms employed on a decentralized open network and it is transparent (Beck et al., 2016) as any user can read through the incremental log of transactions recorded on the blockchain and thus verify any transaction ever recorded or compute the balance of any public address by following the transfer of funds (Zohar, 2015). This unique combination of security, transparency and the absence of a central point of failure is the value proposition of this novel technology and the primary reason for its nomination as a trust-free technology (Beck et al., 2016). The transparency echoes the technology's credibility and honesty. Consequently, the technology enables the resolution of conflicts among the network participants and attenuates information asymmetries without the need of a trusted central authority (Notheisen et al., 2017).

3 Research on Blockchain

While most of the early academic research on blockchain technology can be attributed to the computer science discipline pertaining to the areas of cybersecurity and cryptography (Sas and Khairuddin, 2015), IS research has primarily focused on use case analyses and design science studies of proof of concepts and prototypes (Notheisen et al., 2017). Additionally, IS researchers have been more involved in exploring the implications of the financial applications of the technology like cryptocurrencies, especially their role in illegal activities. Theoretical issues like adoption have been scrutinized to some extent (Abramova and Böhme, 2016), but the significance of trust in the blockchain context is yet to be significantly explored either conceptually or empirically. Within the human-computer interaction (HCI) discipline, there has been some interest in studying the technology and trust in this context. For example, HCI research has shown that Bitcoin users' trust the technology and value its secure cryptographic protocol but they are apprehensive of insecure transactions and the presence of untrustworthy entities in the network (Sas and Khairuddin, 2015). The insecurity of transactions is largely attributed to human errors or malice like the users' risk of losing wallet passwords, inadequate protection measures and ignorance of personal responsibility for the security of the private keys. Moreover, hackers' threat to wallets, failure to recover passwords, dishonest transaction partners and the irreversibility of a transaction are also noted concerns of Bitcoin users (Sas and Khairuddin, 2015). But most of these concerns can be blamed on the users' incompetence except for the inability to reverse a transaction. This irreversibility of a transaction and the fixed number of bitcoins are design principles of the Bitcoin system by choice to enforce the exclusion of a central authority which is usually required to trace stolen funds and settle disputes by reversing the transactions or to authorize the issuance of currency in a traditional monetary system (Zohar, 2015). Furthermore, trust enables people to participate in risky activities which are not under their control and there is also a likelihood of disappointment by the actions of the others (Lewis and Weigert, 1985). We assert that trust plays a critical role in stimulating adoption for Bitcoin and its contribution in the nomological network of the blockchain technology in general needs conceptual and empirical evaluation.

4 Trust Overview

The notion of trust is broad and multifaceted and has captivated IS researchers for quite some time. Trust is most commonly defined as "the willingness of a party to be vulnerable to the actions of another based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al., 1995). The party who grants trust in such a situation is called the trustor, while the trust receiving entity is the trustee (Mayer et al., 1995). The attributes and actions of the trustee that ensures trust, is the trustworthiness of the trustee. This trustworthiness is perceived diversely by the trustors. The different perceptions regarding the trustworthiness of the trustee are the trusting beliefs that form the trust (Gefen et al., 2003). Therefore, trust is formed by the trusting beliefs of a trustor regarding the trustworthiness of a trustee.

Trust researchers of the IS discipline initially focused on technology enabled interpersonal relations where the trustee is an individual; like trust in virtual teams which facilitates trust among team members separated by temporal and spatial boundaries and consumers trust in e-vendors enabled by ecommerce websites (Li et al., 2008). Besides this, the influence of trust on consumers that results in individual decisions to use a technology was also one of the primary research streams of the discipline (McKnight et al., 2011). The technology mediated trust is based on the trustworthiness of a human trustee and usually evaluated by the trusting beliefs related to the human. IS researchers have developed numerous constructs to measure this trustworthiness, but integrity, competence, and benevolence are the three most commonly adopted dimensions used to evaluate interpersonal trust as per the literature (Wang and Benbasat, 2005).

Dimension	Definition	Reference
Benevolence	"The belief that a trustee will want to do good to a trustor, aside from an egocentric profit motive."	Mayer et al., 1995
Competence	"The belief that a trustee has the ability to do what a trustor needs to have done."	Mayer et al., 1995
Integrity	"The belief that a trustee adheres to a set of principles that a trustor finds acceptable."	Mayer et al., 1995

Table 3. Definitions of interpersonal trust dimensions - benevolence, competence and integrity.

4.1 Technology Trust

Recent IS trust research has shifted its focus to the IT artifact itself to recognize the concept of trust in a technology. Researchers acknowledged the fact that many trustors also place trust in the technological artifact itself and this trust is significantly different from the traditional interpersonal trust studied in IS (Lankton et al., 2015). The IT artifact itself that is the technology is the recipient of the trust, the trustee. With information technology increasingly becoming prevalent in personal, social as well as professional lives, the role of technology trust has become even more significant in users' decisions (Gefen et al., 2003). Trust in a technology represents people's trusting beliefs regarding the trustworthiness of the specific information technology to perform a particular task (McKnight et al., 2011). Researchers often used existing trust theories to study trust in a specific technology and empirical research also established the significance of technology trust in the broader context of the nomological network of trust theories (Wang and Benbasat, 2005).The initial studies of technology trust were based on the theories of social response towards computing; This conception claims that "people treat computers and computer based technologies as social actors and apply social rules to them" (Nass and Moon, 2000). This conceptualization was primarily used for research on recommendation agents in an ecommerce context,

where the IT artifact represented an incarnation of a human agent and thus the dimensions of benevolence, competence, and integrity were appropriate (Wang and Benbasat, 2005). However, it is often inappropriate to personify technological artifacts as humane objects warranting a distinction between the dimensions of trust for the interpersonal context and the inanimate IT artifact (Li et al. 2012). This differentiation is primarily based on the argument that interpersonal technology mediated trust assumes that the human trustees have volition that is the ability to make choices and can make ethical decisions (Lankton et al., 2015). Thus, IS researchers studying trust in a technology envisioned the IT artifact as an artificial object lacking volition and proposed numerous distinct sets of dimensions to measure trust based on the features of the underlying technical artifact solely.

5 Research Methodology

The concept of knowledge mapping has been frequently adopted by IS academics primarily for qualitative studies. Different techniques like mind mapping, concept mapping and argument mapping have been employed for conceptually deciphering a phenomenon, while sometimes presenting a framework based on existing theories. For this study, we adopt the argument mapping technique which is appropriate for understanding a novel phenomenon in the early stages when there are inadequate sources of empirical evidences (Hirschheim et al., 2012). The argument mapping technique is based on the philosophies of Toulmin (1958). The technique builds on the theory of informal logic and treats arguments as rhetorical acts proposed to persuade others (Hirschheim et al., 2012). Arguments are comprised of claims, grounds and warrants as primary components while qualifiers and rebuttals are considered secondary and hence not necessary (Kim and Watson, 2017). Claims are the statements presented for an audience to believe, grounds are the evidence used to formulate the claims while the warrants show the logical connections between the claims and the grounds (Toulmin 1958; Hirschheim et al., 2012). Warrants are often implicit and unstated and based on ethos, logos and pathos (Edwards and Nicoll, 2006). Moreover, the efficiency of the technique depends on the quality of the data applied. The literature on trust in a technology and the technical features of Bitcoin form our grounds and we make claims based on our understanding of the technology and trust dimensions supplemented by the knowledge of the research and the phenomena surrounding Bitcoin and blockchain.

5.1 Technology Trust Dimensions as Grounds

We adopted the structured literature review process outlined by Webster and Watson (2002) to identify the technology trust constructs. Table 4 is a summary of the prominent works recognized as studies of trust in a technology. We only included those studies which developed distinct dimensions for measuring technology trust and excluded the ones which measured trust in an IT artifact like a recommendation agent using dimensions of interpersonal trust such as benevolence, competence and integrity. We conducted frequent forward and backward searches iteratively until no new dimensions or constructs measuring technology trust were encountered. Among the dimensions identified, technical competence, medium understanding and privacy pertain to the trustworthiness of a human trustee. Similarly, website attractiveness and web seal value refer to attributes of a specific class of artifacts, websites, while "best business practices" does not refer to attributes of an IT artifact at all. So, we exclude them for our study. McKnight et al. (2011) distinguished between interpersonal trust and trust in technology and proposed reliability, functionality and helpfulness as parsimonious dimensions to measure trust in a specific technology. But the authors also proposed that the nature and the specific form of the IT and the meaning of the dimensions in the particular context should also be considered while applying the dimensions to measure trust (McKnight et al., 2011). Thus, we also include the dimensions proposed by Ratnasingam and Pavlou (2004) for our assessment. They proposed a unique set of dimensions to measure technology trust in a B2B ecommerce context. These dimensions pertain to the attributes of the underlying technological platform that enables technology trust to mitigate the uncertainties of online transactions.

The Bitcoin system essentially enables entities to participate in transactions and the aim of our study is to explore trust in the technology of the Bitcoin system. Therefore, we exclude the aforementioned dimensions for our study and consider only the dimensions and their interpretations as presented in Table 5 as the grounds for our claims.

Technology Trust Dimensions	Latent Construct	Study and Context
Technical competence, reliability and medium understanding	Trustworthiness of internet shopping medium	Lee and Turban (2001) - Online Shopping
Reliability, security and privacy	Perceived technical trustworthiness	Corbitt et al. (2003) - Ecommerce
Confidentiality, integrity, authentication, access controls, availability, non-repudiation and best business practices	Technology trust	Ratnasingam and Pavlou (2004) - Organizations using ecommerce
Website attractiveness, web seal value	Trust in a website	Wakefield et al. (2004) - Online auction for cameras
Confidentiality, integrity, authentication, access controls, availability, non-repudiation and best business practices	Technology trust	Ratnasingam (2005) - Inter Organization trust relations in B2B ecommerce
Reliability, functionality and helpfulness	Trust in IT artifact	McKnight et al. (2011) - Adoption of MS Excel
Reliability and capability	Trust in IT artifact	Li et al. (2012) - Online shopping (store lacking physical presence)

Table 4. Summary of technology trust constructs and dimensions from IS literature.

5.2 Claims About Technology Trust in Bitcoin

Technology trust may replace interpersonal trust where human presence is completely substituted by an IT artifact because it is difficult and almost impossible to trust human actors when they are not visible or physically existent in a trust relation (Li et al., 2012). In situations where there is little or no human presence in a technology mediated phenomenon, the identification of the trusted party is highly uncertain, technology trust becomes a significant enabler of trust a relation (Li et al., 2012). Bitcoin and its technology inherently enables phenomena where human interventions are either very limited or totally absent, thus magnifying the need for trust in the technology.

Researchers have differentiated trust along the course of a technology's adoption, specifically the initial trust building stage and the later knowledge based or experiential stage, and technology trust may exist at both (McKnight et al., 1998). The perceptions of initial trust are attributable to a trustor's cost and benefit assessment of extending trust while the knowledge based experiential trust is enabled by a socio-psychological evaluation of the trustee's attributes (McKnight et al., 2011). Knowledge based trust often induces commitment towards a specific technology which makes it appear more attractive than reasonable alternatives even where the alternative seems more useful and easy to use; thus the widely acknowledged notions of perceived usefulness and ease of use may be subdued by experiential knowledge based trust over time (McKnight et al., 2011). Bitcoin and other blockchain applications have to demonstrate

substantial benefits over existing counterparts to allure users initially and prove their merits over time to sustain the adoption.

Additionally, the notion of institution based trust implies security in terms of technical safety, it conveys that regulations, legal recourse, guarantees and similar procedures exist to ensure benefits and also the environment is in proper order to guarantee success because the situation is normal or favorable (McKnight et al, 2002). However, trust research in the context of ecommerce demonstrated that institution based trust is not application specific, but rather the trusting beliefs are (McKnight et al, 2002). Also, institutional trust does not influence the intended behavior but rather it affects interpersonal and technology trust (Li et al., 2012). When users have more confidence in knowledge based trust, they tend to rely less on institutional beliefs and their decisions are motivated by the trusting beliefs about the features of the technology itself (McKnight et al., 2011). Thus, we conclude that knowledge based trust about the technology of Bitcoin is more significant in the context than institutional beliefs.

The ecosystem surrounding the Bitcoin phenomenon has developed and expanded considerably. It now includes sophisticated online exchanges and ATM's for converting local currencies into bitcoins, electronic wallet providers featuring exceptional customer service and point-of-sale systems enabling businesses to accept payments in bitcoins (Zohar, 2015). Because the technology of Bitcoin and its stakeholders like the exchanges, wallet providers, etc. play different roles, it is important to explore trust in these two independently. The stakeholders provide additional benefits like customer service to alleviate users' apprehensions, which are not offered by the technology itself and thus may have critical influence on the adoption. The literature on trust conveys the relative significance of technology trust with respect to interpersonal trust. We adopt the trust in technology perspective, and on the grounds of our comprehension of the features of the technology and the interpretation of the identified technology trust dimensions we propose the following claims.

Ground: *Reliability* - "The belief that a specific technology will consistently operate properly." (McKnight et al., 2011) **Claim:** The decentralization and the distributed nature of the technology ensures reliability. The blockchain is replicated at several nodes on the network which ensures that at least a copy of the log of transactions is always present. Also, the abundance of nodes and miners, the decentralized verification and validation of the transactions ensures that there is no single point of failure and the transparency of the blockchain also establishes reliability.
Ground: *Functionality* - "The belief that a specific technology has the capability, functionality or features to do for one what one needs to be done." (McKnight et al., 2011) **Claim:** Similar to a traditional monetary system the objective of the Bitcoin system is to enable transfer of funds between two parties and maintain a log of all the transactions. In the Bitcoin system, the technology facilitates transactions between untrusted entities over a network without a central authority. The public addresses generated via the wallet software, analogous to the account numbers in a banking system, can be created by a user at will and there is no restriction on the number of such addresses a user can generate. A user is not required to depend on a central authority like a financial institution to begin transacting in the Bitcoin system. Although the technology does not support reversibility of a payment, this feature is essential to eliminate the need of an authoritative body and ensure the trustworthiness of the participating entities. Additionally, the blockchain maintains a record of all the validated transactions ever conducted on the network.
Ground: *Helpfulness* - "The belief that a specific technology provides adequate and responsive help for users." (McKnight et al., 2011) **Claim:** The Bitcoin system does not offer the traditional help functionalities observed in the conventional technologies studied in IS like an ecommerce system, online banking system, reputation management system, etc. Thus, for a new user the learning curve is quite steep and the risks of committing mistakes are high.

Ground: *Security* - The belief that a specific technology provides protection for trustor's information against threats that may cause economic hardship to data in the form of destruction, disclosure, modification, denial of service, fraud, waste, or abuse. (Kalakota and Whinston, 1996; Belanger et al., 2002) **Claim**: Cryptographic hash functions ensure that the pseudonymous public addresses cannot be linked to identifiable information of the users. Additionally, only the users possessing the required private keys can initiate a transaction utilizing the funds associated with the corresponding public key. The transparent transmission of the transactions and the tamper proof record of the validated transactions all contribute to security.
Ground: *Confidentiality* - "Confidentiality mechanisms aim to protect transactions and message content against unauthorized reading, copying, or disclosure using encryption mechanisms." (Ratnasingam and Pavlou, 2004) **Claim:** The anonymity of the entities on the network ensures confidentiality. The public wallet addresses are the pseudonymous identities of the users in the Bitcoin system. Although these addresses and the transaction details are publically disclosed on the network, any personal information is not unless the user desires to do so.
Ground: *Integrity* - "Integrity mechanisms provide transaction accuracy and assurance that the transactions have not been altered or deleted." (Ratnasingam and Pavlou, 2004) **Claim:** The immutability of the transparent blockchain ledger accounts for integrity in the Bitcoin system. The creation of each block and its addition to the ledger adds further confirmation to the transactions in the preceding blocks and the transparency of the blockchain guarantees the blockchain is tamper proof as every activity in the network is recorded publically.
Ground: *Authentication* - "Authentication mechanisms provide transaction quality of being authoritative, valid, true, genuine, worthy of acceptance or belief by reason of conformity to the fact that reality is present." (Ratnasingam and Pavlou, 2004) **Claim**: Digital signatures, private key encryption and cryptographic hash functions all ensure that transactions in the Bitcoin system are authentic and attributable to the responsible public address owners.
Ground: *Non-repudiation* - "Non-repudiation mechanisms protect the originator of transactions and uses acknowledgement procedures applying digital signatures." (Ratnasingam and Pavlou, 2004) **Claim**: The originator has to digitally sign a transaction using the appropriate private key to initiate a transaction. Only the private key owner can access the funds associated with a public key, while any participant on the network can verify the digital signature by using the corresponding public key. This ensures non-repudiation.
Ground: *Availability* - "Availability mechanisms protect transactions against weaknesses in the transmission media and protect the sender against internal fraud or manipulation by using authorization mechanisms such as User IDs and passwords." (Ratnasingam and Pavlou, 2004) **Claim:** The decentralized and distributed nature of the blockchain protocol eliminates the threat to a central point of failure and assures availability. Because there are no barriers to entry, nodes can enter and leave the network at will and thus the consensus mechanism is maintained by the active nodes in the network. Also, there are no limitations enforced by the protocol on the number of nodes required by the network, although the speed of transaction processing may suffer greatly due to a reduction in their number. The transmission of transactions is never interrupted and the digital signature mechanism ensures security to the senders against frauds.
Ground: *Access control* - "Access control mechanisms provide authorization mechanisms thereby assuring that transactions are sent and received without interruption." (Ratnasingam and Pavlou, 2004) **Claim:** Access control is ensured by the private key signature requirement to initiate a transaction. Only users possessing the private key to a public address can access the bitcoins associated with an address and indulge in utilization of the funds. Although the security of the private keys is a liability of the users.

Table 5. Definitions of technology trust dimensions as grounds and proposed claims.

We believe that the identified dimensions of technology trust can be used to study trust in the technology of Bitcoin without representing the conceptual difficulties of anthropomorphism (Li et al. 2012). We mapped the dimensions to the technical features of Bitcoin, although the realization of some of them may

be confounding. Cryptography inherently mitigates the issues of information security like security, confidentiality, availability, authentication, non-repudiation, integrity and access control (Menezes et al., 1996) and these same dimensions are also used to measure trust in a technology (Ratnasingam and Pavlou, 2004). However, empirical research is required to conclude if these dimensions along with functionality, reliability and helpfulness are adequate to study trust in the context of blockchain technology and Bitcoin. We plan to conduct survey research based on these dimensions supplemented by open ended questions. We also propose to conduct interviews with blockchain and Bitcoin experts to supplement this conceptual assessment with quantitative as well as qualitative data and analysis.

6 Discussion and Future Research Directions

Interpersonal trust and technology trust can coexist (Li et al., 2012; Ratnasingam and Pavlou, 2004; Corbitt et al., 2003). In fact, technology trust is not a substitute for interpersonal trust rather it complements it while the latter has more influence on the intended behavior induced by a technology (Li et al., 2012). The steady expansion of the ecosystem surrounding Bitcoin is offering more avenues for nurturing interpersonal trust. Therefore, the significance and influence of interpersonal and technology trust in the Bitcoin context needs empirical investigation. Social media research has shown that users may trust a platform as a technology but not the other users on it, while ecommerce research established that users trust a service provider and the offered services due to trust in the IT artifact enabling the experience (Lankton and McKnight, 2011; Karimov et al., 2011). Therefore, technology trust mediates interpersonal trust but the former does not guarantee interpersonal trust.

The literature on trust and our conceptual justification by argument mapping highlights the significance of technology trust in the Bitcoin and blockchain context. IS researchers can formulate specific propositions and hypotheses and design experiments to evaluate our proposed claims. Also, the applicability of the traditional notion of institutional trust, and the distinction between initial and knowledge based trust presents avenues for future academic research. Moreover, whether Bitcoin or the blockchain technology presents a novel context which challenges the traditional conceptualizations of trust might also be an intriguing research topic to pursue. Additionally, Bitcoin being a monetary application, trust theories based on economic perspectives might also be relevant in the context. For practitioners involved in the domain, they may consider applying the identified dimensions of trust and the presented claims as guidelines in their endeavors to ensure trust. The applications and the technology itself can be refined to address the lack of adequate mechanisms to offer helpfulness. Practitioners may also develop their blockchain projects to minimize the repercussions of the irreversibility of transactions.

7 Conclusion

The concepts of decentralization, consensus mechanisms, cryptography and digital signatures have existed for quite some time. But the novelty of the Bitcoin technology is the particular assembly of those to offer a unique solution which is complex and not yet understood widely. The fundamental contribution of trust is to serve as a mechanism to reduce perceived social complexity (Luhmann, 1979). This becomes important for many disciplines because of the increasing complexity of organizations and technology (Gefen et al., 2003). Additionally, trust aids in the adoption of a new technology and reduces apprehensions of risk and uncertainty for users (Gefen et al., 2003). In this work, we presented an overview of the literature on trust and identified the dimensions established to measure trust in a technology. We supplemented it with an intricate description of the Bitcoin technology to articulate the features of the technology. We adopted the argument mapping technique to present claims about trust in the Bitcoin technology linking the identified trust dimensions to the features of the technology. This work introduces a new research perspective and lays the foundation for more concrete propositions requiring empirical justification, which is necessary for mainstream adoption of Bitcoin and the blockchain technology.

References

Abramova, S., and Böhme, R. (2016). "Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study." In: *ICIS 2016 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc.

Beck, R., Czepluch, J. S., Lollike, N., and Malone, S. (2016). "Blockchain-the Gateway to Trust-Free Cryptographic Transactions." In: *ECIS 2016 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Belanger, F., Hiller, J. S., and Smith, W. J. (2002). "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes." *Journal of Strategic Information Systems*, 11(3), 245-270.

Bitcoin. (2017). URL: https://bitcoin.org/en/ (visited on 11/03/2017).

Bitcoin Wiki. (2017). URL: https://en.bitcoin.it/wiki/Block/ (visited on 11/01/2017).

Blockchain. (2017). URL: https://blockchain.info/ (visited on 11/01/2017).

Brenig, C., Schwarz, J., and Rückeshäuser, N. (2016, June). "Value of Decentralized Consensus Systems-Evaluation Framework." In: *ECIS 2016 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Buterin, V. (2014). DAOs, DACs, DAs and More: An Incomplete Terminology Guide. URL: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ (visited on 10/20/2017).

Corbitt, B. J., Thanasankit, T., and Yi, H. (2003). "Trust and e-commerce: a study of consumer perceptions." *Electronic Commerce Research and Applications*, 2(3), 203-215.

Coron, J. S., Dodis, Y., Malinaud, C., and Puniya, P. (2005). "Merkle-Damgård revisited: How to construct a hash function." In: *Advances in Cryptology–CRYPTO 2005* (pp. 430-448). Springer Berlin/Heidelberg.

Economist (2015). Blockchain - The next big thing. URL: http://www.economist.com/news/special-report/21650295-orit-next-big-thing/ (visited on 10/20/2017).

Edwards, R., and Nicoll, K. (2006). "Expertise, competence and reflection in the rhetoric of professional development." *British Educational Research Journal*, 32(1), 115-131.

Fairfield, J. (2014). "Smart contracts, Bitcoin bots, and consumer protection." *Wash. & Lee L. Rev. Online*, 71, 35-299.

Fukuyama, F. (1995). "Trust: The social virtues and the creation of prosperity." *New York: Free Press*.

Gefen, D., Karahanna, E., and Straub, D. W. (2003). "Trust and TAM in online shopping: An integrated model." *MIS Quarterly*, 27(1), 51-90.

Glaser, F., and Bezzenberger, L. (2015). "Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems." In: *ECIS 2015 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., and Siering, M. (2014). "Bitcoin-asset or currency? revealing users' hidden intentions." In: *ECIS 2014 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Goldwasser, S., Micali, S., and Rivest, R. L. (1988). "A digital signature scheme secure against adaptive chosen-message attacks." *SIAM Journal on Computing*, 17(2), 281-308.

Hirschheim, R., Murungi, D. M., and Peña, S. (2012). "Witty invention or dubious fad? Using argument mapping to examine the contours of management fashion." *Information and Organization*, 22(1), 60-84.

Hoffman, D. L., Novak, T. P., and Peralta, M. (1999). "Building consumer trust online." *Communications of the ACM*, 42(4), 80-85.

Kalakota, R. and Whinston, A.B., (1996). *Frontiers of Electronic Commerce*, Addison-Wesley, Reading, MA.

Karimov, F. P., Brengman, M., and Van Hove, L. (2011). "The effect of website design dimensions on initial trust: a synthesis of the empirical literature." *Journal of Electronic Commerce Research*, 12(4), 272.

Kim, J. B., and Watson, E. (2017). "Exploring practical potentials of business simulation games." In: *HICSS 2017 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Krawczyk, H., Canetti, R., and Bellare, M. (1997). "HMAC: Keyed-hashing for message authentication."

Lankton, N.K. and McKnight, D.H. (2011). "What does it mean to trust Facebook? Examining technology and interpersonal trust beliefs." *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 42*(2), pp.32-54.

Lankton, N. K., McKnight, D. H., and Tripp, J. (2015). "Technology, humanness, and trust: Rethinking trust in technology." *Journal of the Association for Information Systems*, 16(10), 880.

Lee, M. K., and Turban, E. (2001). "A trust model for consumer internet shopping." *International Journal of Electronic Commerce*, 6(1), 75-91.

Lewis, J. D., and Weigert, A. (1985). "Trust as a social reality." *Social Forces* 63.4: 967-985.

Li, X., Hess, T. J., and Valacich, J. S. (2008). "Why do we trust new technology? A study of initial trust formation with organizational information systems." *Journal of Strategic Information Systems*, 17(1), 39-71.

Li, X., Rong, G., and Thatcher, J. B. (2012). "Does Technology Trust Substitute Interpersonal Trust? Examining Technology Trust's Influence on Individual Decision-Making." *Journal of Organizational and End User Computing* (JOEUC), 24(2), 18-38.

Luhmann, N. (1979). "Trust and power." *John Willey & Sons*.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). "An integrative model of organizational trust." *Academy of Management Review*, 20(3), 709-734.

McKnight, D. H., Cummings, L. L., and Chervany, N. L. (1998). "Initial trust formation in new organizational relationships." *Academy of Management Review*, 23(3), 473-490.

McKnight, D. H., Choudhury, V., and Kacmar, C. (2002). "Developing and validating trust measures for e-commerce: An integrative typology." *Information Systems Research*, 13(3), 334-359.

McKnight, D. H., Carter, M., Thatcher, J. B., and Clay, P. F. (2011). "Trust in a specific technology: An investigation of its components and measures." *ACM Transactions on Management Information Systems* (TMIS), 2(2), 12.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nass, C., and Moon, Y. (2000). "Machines and mindlessness: Social responses to computers." *Journal of Social Issues*, 56(1), 81-103.

Notheisen, B., Hawlitschek, F., and Weinhardt, C. (2017). "Breaking Down the Blockchain Hype– Towards a Blockchain Market Engineering Approach." In: *ECIS 2017 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Öksüz, A., Walter, N., Distel, B., Räckers, M., and Becker, J. (2016). "Trust in the Information Systems Discipline." In: *Trust and Communication in a Digitized World* (pp. 205-223). Springer International Publishing.

Ratnasingam, P., and Pavlou, P. A. (2004). "Technology trust in internet-based inter organizational electronic commerce." *The Social and Cognitive Impacts of E-commerce on Modern Organizations*, 311.

Ratnasingam, P. (2005). "Trust in inter-organizational exchanges: a case study in business to business electronic commerce." *Decision Support Systems*, 39(3), 525-544.

Sas, C., and Khairuddin, I. E. (2015). Exploring trust in Bitcoin technology: a framework for HCI research. In: *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction* (pp. 338-342). ACM.

Sas, C., and Khairuddin, I. E. (2017). "Design for Trust: An exploration of the challenges and opportunities of bitcoin users.: In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6499-6510). ACM.

Tilson, D., Lyytinen, K., and Sørensen, C. (2010). Research commentary - "Digital infrastructures: The missing IS research agenda." *Information Systems Research*, 21(4), 748-759.

Toulmin, S. (1958). *The Uses of Argument*. Cambridge: Cambridge UP.

Wakefield, R. L., Stocks, M. H., and Wilder, W. M. (2004). "The role of web site characteristics in initial trust formation." *Journal of Computer Information Systems*, 45(1), 94-103.

Wang, W., and Benbasat, I. (2005). "Trust in and adoption of online recommendation agents." *Journal of the Association for Information Systems*, 6(3), 4.

Webster, J., and Watson, R. T. (2002) "Analyzing the past to prepare for the future: Writing a literature review." *MIS Quarterly*: xiii-xxiii.

Worldcoinindex (2017). Bitcoin Charts. URL: https://www.worldcoinindex.com/coin/bitcoin/ (visited on 11/02/2017).

Wörner, D., Von Bomhard, T., Schreier, Y. P., and Bilgeri, D. (2016). "The Bitcoin Ecosystem: Disruption Beyond Financial Services?" In: *ECIS 2016 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Zohar, A. (2015). "Bitcoin: under the hood." *Communications of the ACM*, 58(9), 104-113.