ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/328465252

Blockchain and Trust: Refuting Some Widely-held Misconceptions

Conference Paper · December 2018

CITATIONS
0

READS
175

2 authors:

Andreas Auinger
Fachhochschule Oberösterreich
77 PUBLICATIONS **513** CITATIONS
SEE PROFILE

René Riedl
Fachhochschule Oberösterreich
134 PUBLICATIONS **1,369** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Medical Statistics View project

Project SCIM 2.0 - Effective Supply Chain Information Management using Enterprise 2.0 View project

All content following this page was uploaded by Andreas Auinger on 13 December 2018.

The user has requested enhancement of the downloaded file.

Blockchain and Trust: Refuting Some Widely-held Misconceptions

Short Paper

Andreas Auinger
University of Applied Sciences
Upper Austria
Wehrgrabengasse 1-3, 4400 Steyr
andreas.auinger@fh-steyr.at

René Riedl
University of Applied Sciences
Upper Austria & University of Linz
Wehrgrabengasse 1-3, 4400 Steyr
rene.riedl@fh-steyr.at

Abstract

In this paper, we discuss a fundamental question: What is the nature of trust in the blockchain context? Thereby, we critically examine widely-held assumptions on blockchain and trust. In particular, we examine the assumption that the blockchain is trust-free. Based on a comprehensive review of the Information Systems (IS) literature on blockchain, we identified and analyzed all text passages related to trust (N = 452 text passages, distributed across 61 papers out of a total of 85 blockchain papers). This analysis revealed that "Trust in algorithms," "Technological mechanisms and trust," and "Substitution of intermediaries and trust" constitute the top-3 research themes in the current IS blockchain literature. We discuss these themes based on a simple conceptual trust framework in the Bitcoin context, and thereby reveal the misconceptions that participation in a blockchain ecosystem (here Bitcoin) only implies trust in algorithms and consensus mechanisms, and that the blockchain makes intermediaries dispensable and thereby trust in them irrelevant. Rather, we argue that trust only shifts from specific market players in the blockchain ecosystem to others. Against this background, we conclude that trust issues have not changed fundamentally. Rather, traditional determinants of trustworthiness (i.e., ability, benevolence, integrity), along with known mechanisms to establish trust in online settings (e.g., third-party institutional mechanisms), will remain critical in blockchain settings. We also discuss limitations of the study and outline potential avenues for future examination.

Keywords: Bitcoin, Blockchain, Literature Review, Trust, Trustworthiness, Trust-free

Introduction

Beck et al. (2017) define the blockchain as "a distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism" (p. 381). While modification of validated blockchain transactions is theoretically possible, it is highly unlikely to happen in reality. A technology that guarantees resistance to modification of its records has enormous business potential, predominantly because such a technology assures both traceability and confirmability of transactions between different parties. The probably most prominent application of the blockchain technology is Bitcoin, a cryptocurrency which serves as a worldwide payment system that does *not* involve a central authority (i.e., a bank as an intermediary). Rather, it is argued (e.g., Jarvenpaa and Teigland 2017) that it is the blockchain's (and hence the Bitcoin's) decentralized nature which distinguishes this technology and its corresponding applications from prior technologies related to human interaction and business transactions (however, note that there is an ongoing discussion whether the blockchain and its applications such as Bitcoin are of a truly decentralized nature; see, for example, Bonpay 2017).

In the Information Systems (IS) literature, and also beyond the boundaries of the IS discipline, the blockchain and its applications in various industries (e.g., finance, logistics, or public administration) and

scenarios (e.g., Internet-of-Things) have become an important research domain (see, for example, a 2017 BISE special issue, Vol. 59/6). In the present paper, we address the blockchain topic from a trust perspective. We raise the following research question: *What is the nature of trust in the blockchain context?* Raising this question is critical. *First*, statements in the scientific literature on blockchain and trust are contradictory. Several authors indicate "trust-free" as an inherent property of the blockchain, either by drawing upon the blockchain's technological foundations or by citing related work. Thus, according to this perspective, the blockchain is something that is trust-free. For example, Notheisen et al. (2017a) already indicate in the title of their paper that trading real-world assets on blockchain is "an application of trust-free transaction systems". To state another example, Schweizer et al. (2017) write that "[b]lockchain systems are generally considered to operate as closed trust-free ecosystems" (p. 15). In sharp contrast to this perspective, other statements in the literature suggest that the blockchain is not trust-free. For example, Siira et al. (2017) write that "utilising blockchain technology … would offer … *possibly more trustworthiness*" (p. 539, italics added). As another example, Cao et al. (2017) write that "the blockchain technology has great influence on *reducing the risk of trust*" (p. 112, italics added). It follows that opposing views exist in the scientific literature on whether the blockchain is a trust-free technology or not. *Second*, statements in the scientific literature suggest that the relationship between blockchain and trust is unclear today, and hence several researchers have made calls for research on the relationship between blockchain and trust. For example, Niederman et al. (2017) recently wrote that "[t]rust has been a major factor in many kinds of IS," and they raised fundamental questions, such as "Is it possible to create trust-free transactions using blockchain?" and "What are trust-free transactions?" (p. 86). Risius and Spohrer (2017), to state another example, argue that "it is not even clear whether blockchain transactions are actually perceived as trust-free since they may still require a certain amount of trust in the blockchain providers" (p. 391). In a similar vein, Avital et al. (2016), in an ICIS panel paper on blockchain technology, indicate that "the nature of trust [is] an issue that people agree is important but that has not been carefully studied" (p. 4).

Against the background of (i) the contradicting trust statements in the blockchain literature and (ii) the fact that several scholars have already made explicit calls for studying the nature of trust in the blockchain context, a systematic review of what we know about the blockchain and trust, along with a critical discussion of that knowledge, is essential. Thus, the primary contribution of this short paper, which is part of a larger ongoing research project on the blockchain and trust, is to shed light on the widely-held notion that the blockchain is trust-free. The relevance of the present paper goes beyond the IS discipline (e.g., we also consider the insight presented in this paper relevant to economics), because trust has been identified as one of the strongest predictors of economic welfare in human society (e.g., Zak and Knack 2001).

The remainder of this paper is structured as follows: Section 2 presents the methodology of our literature review. In Section 3, we focus our discussion on the top research themes which we identified in our literature review, namely "Trust in algorithms," "Technological mechanisms and trust," and "Substitution of intermediaries and trust"; we use Bitcoin as our blockchain application context. Section 4, finally, summarizes this paper's contribution, outlines its limitations, and provides some thoughts on possible directions for future research.

Methodology of the Literature Review

Our methodological approach followed guidelines by Webster and Watson (2002). In order to identify publications on blockchain in the IS literature, we conducted a literature search and considered peer-reviewed journal and conference publications. Specifically, we conducted a full coverage literature search using the keyword "blockchain" in the Association for Information Systems (AIS) eLibrary and in all AIS Senior Scholar's Basket of Eight Journals (EJIS, ISJ, ISR, JAIS, JIT, JMIS, JSIS, MISQ). This search process was conducted in February 2018. Hence, our review comprises publications from 2014, when the term was used by Glaser et al. (2014) in an IS publication the first time, to 2018. In total, we identified 85 blockchain publications in the IS literature (64 conference publications, 21 journal publications). A list of all 85 publications may be obtained in electronic form by request from the authors. We observed the following publication numbers per year: 2014/1 paper (= 2014/1), 2015/5, 2016/19, 2017/57, 2018/3 (note that our review of 2018 papers only covers the first two months). With respect to publication outlets, we observed the following distribution: ICIS/15 papers (= ICIS/15), AMCIS/13, BISE/10, ECIS/10, HICSS/9, MCIS/7, JIT/4, BLED/2, CAIS/2, ISJ/2, ISR/2, PACIS/2, SCAND/2, WIN/2, GLOBDEV/1,

JMIS/1, and WHICEB/1. Details on publication outlets can be found in the AIS eLibrary (for details, see http://aisel.aisnet.org/).

Trust Category	*Example Statement in the Category*	*Total*	*%*
Categories with a Focus on Technology			
Trust in algorithms	"[H]uman users are required to trust in algorithms instead of traditional institutions." (Notheisen et al. 2017b, p. 1069)	74	16%
Technological mechanisms and trust	"If there is consensus among the majority of computers that the transaction is valid, a new block of data is added to the chain and shared by all on the network. Transactions are secure, trusted, auditable, and immutable." (Clemons et al. 2017, p. 434)	72	16%
Substitution of intermediaries and trust	"Blockchain technology will make these payments 'faster and cheaper', i.e. faster by providing a solid, common infrastructure across borders for transactions, and cheaper by removing expensive intermediaries, thus overcoming today's 'lack of trust'." (Holotiuk et al. 2017, p. 920)	72	16%
Trust and Internet-of-Things (IoT) and other technologies	"Another important factor that can influence the wide acceptance of IoT in personal as well as organizational activities is trust … the lack of trust in the IoT and their applications can also be an inhibitor of IoT adoption. Thus, it is necessary to ensure that any IoT application can be trusted by the intended users." (Papadopoulou et al. 2017, p. 7)	30	7%
Trust and smart contracts	"As current blockchain technology can not only process monetary transactions but can also ensure that transactions comply with programmable rules in the form of 'smart contracts' … it allows even parties who do not fully trust each other to conduct and reliably control mutual transactions without relying on the services of any trusted middlemen." (Risius and Spohrer 2017, p. 386)	24	5%
Categories with No Focus on Technology			
Non-technological trust factors	"[M]ajor drawback of using a non-Bitcoin blockchain is that the service no longer benefits from the trustworthiness that comes with its widespread use …" (Gipp et al. 2016, p. 8)	38	8%
Trust and behavior of market participants	"The global economic system depends on that individuals and organizations trust other entities to create, store, and distribute essential records." (Beck et al. 2017, p. 381)	34	8%
Trust in economic transactions lost	"[T]he financial crisis of 2008 has shown once more that our established, centralized financial and political systems are far from being invulnerable to trust issues and systemic risks that potentially emerge with increased centralization." (Glaser and Bezzenberger 2015, p. 1)	21	5%
Trust in face-to-face transactions	"The face-to-face transactions improve 'knowledge acquisition, trust and friendship' since buying physically in local shops offers opportunities for sociable interactions in local communities …" (Diniz et al. 2016, p. 10)	4	1%
Courts, their verdicts, and trust	"Currently, precedence has yet to be established regarding the obligation of courts to recognize trusted timestamping using the blockchain of a cryptocurrency as evidence in court proceedings." (Gipp et al. 2016, p. 8)	2	0%
Miscellaneous	"Trust is one of the most complex concepts and has been researched extensively across disciplines." (Leidner et al. 2017, p. 1)	81	18%
Total		452	100%

Table 1. Twelve Trust Categories and Assignment of N = 452 Statements to the Categories

We used the analysis software tool MaxQDA Pro 2018 (https://www.maxqda.com) for semi-automatic analysis of all 85 papers. Specifically, we used the tool to search for and code *all* text passages with the term "trust". The tool automatically marked all sentences in which the term "trust" appeared (note that searching for the term "trust" implies identification of related terms such as "trustworthy", "trustworthiness", "distrust", etc.). In total, we identified 452 relevant text passages (cleaned by titles, keywords, and references) with the term "trust" (in 61 out of the 85 publications). It is possible that a text passage (i.e., a composite of sentences which form a conclusive statement, a definition developed by the authors in the context of this study) contains the term "trust" more than one time. This explains why we identified the term "trust" 656 times in our sample (= rank 102 out of all words used in the 85 publications). The tool has a function to export relevant text passages (here the trust text passages) in a

separate file. In the next step, the two authors of this paper independently read the exported file containing all 452 text passages with the objective to develop more abstract categories. Next, the authors met and discussed their ideas on categories in a half-day workshop. This discussion process resulted in the specification of 12 categories. Thus, the approach used to develop the categories was fully inductive. In the workshop, based on joint assignment of 25 selected statements (i.e., circa 5% of the entire coding material), the authors developed and discussed coding rules. Specifically, a coding scheme was developed which included coding rules and several representative example statements in each category. As an example, a rule was defined that all papers comprising the terms "algorithm" or "mathematics" have to be assigned to the category "Trust in algorithms", while papers with more detailed technical blockchain descriptions (including terms such as "cryptograph*", "timestamp*", "distributed ledger", or "peer-to-peer network") have to be assigned to the category "Technological mechanisms and trust". The objective of this procedure was to secure a maximum of common understanding of the twelve categories in order to lay the foundations for coding reliability.

Next, the classification was carried out by the two authors who independently conducted the assignment of the text passages to the categories; that is, each text passage (N = 452) was assigned to exactly one category. In 44 out of 452 cases there was no consensus. To determine the inter-rater reliability we used Cohen's Kappa coefficient (Cohen 2016). This value indicates the degree of consistency of coding between two persons, while the possibility of random match ($pc=1/12\times1/12$) is already taken into account. According to (Landis and Koch 1977) values for the Cohen's Kappa coefficients are "substantial" between 0.61 and 0.80 and values above are "almost perfect". The value of Cohen's Kappa coefficient for the 452 classified text passages was 0.90 [$po=1-(44/452)$ and $pc=1/144$; see Cohen (2016, p. 40), for further methodological details]. Thus, the result of the coding is highly reliable. Consensus was ultimately reached on all classifications through discussion.

Table 1 indicates (i) the 12 trust categories, (ii) an example statement from each category, (iii) the total number of text passage assignments per category, and (iv) corresponding percentages (rounded). The categories are listed in descending order of total number of assignments, except the category "Miscellaneous" which is listed at the very end. Moreover, we grouped the 12 categories into two more abstract categories, namely categories with a focus on technology (60%: 272 out of 452) and categories with no focus on technology (40%: 180 out of 452). Based on this categorization, it becomes evident that the current IS literature on blockchain and trust is focused on technology-related themes. Note that a relatively large number of statements had to be assigned to the "Miscellaneous" category because the analyzed papers included a number of general statements which are not Blockchain-specific, such as the example in Table 2. Moreover, we assigned all trust definitions in the papers to this category, such as the following example (Jarvenpaa and Teigland 2017): "Trust can be seen as a measure of confidence or belief that the other party will refrain from opportunistic behavior and behave in an expected manner … thereby fulfilling the trusting party's expectations without exploiting its vulnerabilities" (p. 5812).

Critical Reflection on the Top-3 Themes: The Example of Bitcoin

In this section, we focus our discussion on the top-3 research themes which we identified in our literature review, namely "Trust in algorithms," "Technological mechanisms and trust," and "Substitution of intermediaries and trust". In order to establish a context for this discussion, it is essential to briefly summarize the traditional notion of trust in online settings; specifically, we refer to trust in e-commerce settings (e.g., Gefen et al. 2008). The analysis of such a trust situation is focused on situations involving two specific parties: a trusting party (trustor) and a party to be trusted (trustee). Once a trustor (online buyer) and a trustee (online seller) begin to interact via the Internet (i.e., a seller puts a product on the Internet and a buyer views the offer), the trustor can perceive this information (e.g., a product for sale on eBay or Amazon). A trustor typically processes the online information to learn more about the product for sale. However, the information is also used to infer the trustee's characteristics, because this makes possible predictions of the seller's trustworthiness. From a seller's perspective, information provision on a website serves the purpose of deliberately signaling trustworthiness. Major characteristics of a trustee, which together constitute a trustee's trustworthiness, are ability, benevolence, and integrity (Mayer et al. 1995). If a trustor believes in the trustworthiness of a trustee, he/she believes that the trustee (i) has skills and competencies that are important for the relationship (ability), (ii) wants to do good to the trustor, aside from an egocentric profit motive (benevolence), and (iii) adheres to a set of principles that the

trustor finds acceptable (integrity). Importantly, trust perceptions in traditional online settings such as e-commerce are not only influenced by a trustor's perceptions of the trustee's trustworthiness, but also by buyers' perceptions of the effectiveness of third-party institutional mechanisms, such as feedback mechanisms, third-party escrow services, and credit card guarantees (e.g., Pavlou and Gefen 2004). Consistent with this perspective, McKnight et al. (2011) argue trust in a specific technology is strongly affected by structural assurance (because such an assurance influences a user's "belief that success is likely because contextual conditions like promises, contracts, regulations and guarantees are in place").

Our literature review revealed that "trust in algorithms" is the dominant trust topic in the current IS literature on blockchain, followed by "Technological mechanisms and trust" and "Substitution of intermediaries and trust". However, identification of these topics does not mean that these topics are well-understood today. Rather, in our review we identified a number of text passages related to trust in these three domains; yet, these passages mainly contain relatively abstract statements rather than a detailed discussion of the topics. The following quote may serve as a good example for the kind of statements that we observed (Notheisen et al. 2017b, p. 1069): "The concept of being trust-free, however remains unclear, since one could argue that trust will not be replaced but rather shift from central institutions or market authorities towards algorithms."

According to Merriam-Webster, an algorithm is "a procedure for solving a mathematical problem" or, more broadly, "a step-by-step procedure for solving a problem or accomplishing some end especially by a computer". In the blockchain context, this "step-by-step procedure" refers to the interplay of technological components (i.e., software, hardware, consensus rules) which make possible the functioning as a distributed transactional database, secured by cryptography, and governed by a consensus mechanism (Beck et al. 2017); the "end" is the execution of a secure and transparent transaction (note that radical transparency is not per se and not in all situations a desirable characteristic, e.g., Brin 1999).

Because Bitcoin is the most prominent application context that we identified in our literature review, we use this cryptocurrency as the basis for our analyses. Antonopoulos (2014) argues that Bitcoin "implements a trust model of trust by computation", and he explains this argument as follows: "Trust in the network is ensured by requiring participants to demonstrate proof-of-work, by solving a computationally difficult problem. The cumulative computing power of thousands of participants, accumulated over time in a chain of increasing-difficulty proofs, ensures that no actor or even collection of actors can cheat, as they lack the computation to override the trust. As proof-of-work accumulates on the chain of highest difficulty (the blockchain), it becomes harder and harder to dispute … new trust model of trust-by-computation: no one actor is trusted, and no one needs to be trusted. There is no central authority or trusted third party in a distributed consensus network." It follows that the blockchain and its underlying transactions, by design, are trustworthy. This fact has led *The Economist* to title in 2015 that the blockchain is a "trust machine" (Berkely 2015) and it also resulted in the widely-held notion that the blockchain is trust-free (e.g., Notheisen et al. 2017a or Schweizer et al. 2017). However, this notion is only correct from a purely mathematical stance (i.e., formal verification of an algorithm). However, the blockchain and its applications such as Bitcoin are not pure technical systems; rather, they are *socio-technical systems*. It follows that the trust issue is more complex than outlined by Antonopoulos (2014) and in purely technical papers (see, for example, a paper by Bhargavan et al. (2016) on formal verification of smart contracts).

In the context of Bitcoin, Lustig and Nardi (2015) coined the concept of "algorithmic authority," defined as "the trust in algorithms to direct human action and to verify information, in place of trusting or preferring human authority" (p. 743). Based on a multi-method research approach drawing upon a multicultural sample (online survey: N = 510; interviews: N = 22; document analysis: blogs, forums, and articles), they found "tensions and complexities of algorithmic authority" (p. 746). In other words, their study revealed that trust in algorithms can neither completely substitute trust in humans nor trust in institutions, as exemplified in the following statement: "Participants preferred algorithms to institutions, but they argued that Bitcoin itself and third party Bitcoin services require human oversight … the judgment of individuals is a necessary supplement to algorithmic authority" (p. 748). Furthermore, they tellingly write that "Bitcoins need to be able to be transacted without fear of criminal exploitation. This requires an empowered authority to prosecute fraudsters and other financial criminals. Anarchists will dispute any government intervention, but without established trust, no market can succeed. Bitcoin cannot continue to be 'the Wild West currency' and also succeed in the long-term" (p. 750).

What is the implication of these research findings? The Bitcoin ecosystem, as well as blockchain ecosystems in general, typically involve a number of stakeholders such as (i) people (e.g., people who would like to buy Bitcoins, bloggers who write about Bitcoin, experts who talk about Bitcoin), (ii) communities (particularly the open source community behind Bitcoin), and (iii) institutions (e.g., Bitcoin trading platforms or legislative bodies in different countries which develop laws that regulate Bitcoin). All these stakeholders have to be trusted to some extent in order to establish a functioning market. The kind of trust necessary is significantly influenced by the "traditional" trustworthiness components, namely ability, benevolence, and integrity (Mayer et al. 1995). Moreover, perceptions of the effectiveness of third-party institutional mechanisms also influence trust behavior.

To substantiate our reasoning and to formalize our theorizing, we developed a simplified conceptual framework for trust in the Bitcoin context (note that we define a conceptual framework as an analytical tool which helps to organize ideas, this distinguishes it from more advanced theoretical frameworks which comprise constructs and relationships among constructs). Specifically, our framework documents fundamental trust questions from the perspective of a potential Bitcoin user and distinguishes four phases: motivation, information, buying, and using or selling (see Figure 1, the framework is read clockwise). As shown in Figure 1, in addition to the fundamental trust question whether a user trusts the algorithms and consensus mechanisms, which are frequently said (see results of our review) to substitute trust in intermediaries and therefore make the blockchain a trust-free technology, a number of further trust questions are relevant. Next, we discuss such trust questions.

Imagine a person who wants to use Bitcoins. In the *first phase*, a fundamental question which is relevant from a trust perspective concerns the user's motivation to use Bitcoin. Evidence (e.g., Lustig and Nardi 2015) indicates that people interested in using Bitcoin, as well as Bitcoin miners, typically have less trust in the traditional monetary system than less interested people (except those people who were only attracted by the sharply increasing Bitcoin price at the end of the year 2017, in this case the motivation to buy Bitcoins was likely more guided by short-term investment motives). Marella (2017), in one of the papers that we reviewed, indicates that the 2008 collapse of Lehman Brothers, at that time one of the largest investment banks in the United States, led to a loss of trust of many people in the traditional monetary system. In the *second phase*, once a person has decided to eventually buy Bitcoins, information acquisition is critical in order to make a final decision. A fundamental question in this phase is: Do I trust the people and institutions that provide information on Bitcoin? Relevant information sources are, among others: the Bitcoin community and miners, general governments, central banks and financial institutions, Bitcoin-related start-ups, and experts. Imagine that the person has made the decision to buy Bitcoins, a further trust question becomes relevant in the *third phase*: Do I trust the digital currency exchanges (e.g., Coinbase or Kraken) and other distribution channels (e.g., since July 2017 Austrian post office, in a cooperation with the platform Bitpanda, has been selling vouchers for cryptocurrencies such as Bitcoin in its stores; see news on coinfox.info). Once the user has bought Bitcoins, further trust questions become relevant in the *fourth phase*. In case of currency use, the question of whether the companies accepting Bitcoins (typically online businesses) can be trusted arises. Moreover, if a user has bought Bitcoins to speculate on increasing prices (investment motive), the question arises whether the trading platforms can be trusted with respect to selling.

To sum up, the simplified trust framework in Figure 1 summarizes a number of critical trust questions from the perspective of a potential Bitcoin user, and the framework is organized along four phases (motivation, information, buying, using/selling). Moreover, as indicated in Figure 1, the general trust question regarding a person's trust in the legislative system and justice is critical as well, because the decision to use Bitcoins is also influenced by the belief of whether potential issues can be clarified in a reasonable way by courts. Importantly, in reality the trust situation is even more complex, because further trust questions become relevant, such as whether users trust manufacturers of hardware wallets, because their correct functioning is critical to securely store Bitcoins (if not completely stored online).

However, our framework serves the purpose to illustrate the *misconceptions* that participation in a blockchain ecosystem (here Bitcoin) only implies trust in algorithms and consensus mechanisms, and that the blockchain makes intermediaries dispensable. Rather, our analyses indicate that while trust in algorithms and consensus mechanisms are relevant to develop trust in Bitcoin (and the blockchain in general), it is incorrect to assume that trust in intermediaries (or other institutions and people) becomes irrelevant in the blockchain context. What we observe is that *trust shifts* from specific types of

intermediaries (e.g., banks in the Bitcoin context) to other types of intermediaries (e.g., digital currency exchanges in the Bitcoin context). Against this background, we conclude as follows:

> *It is a massive exaggeration to claim that the blockchain is trust-free or that trust in intermediaries is not needed any more in the blockchain context. Trust only shifts from specific market players in the blockchain ecosystem to others. However, this does not mean that trust issues have changed fundamentally. Rather, traditional determinants of trustworthiness (i.e., ability, benevolence, integrity), along with known mechanisms to establish trust in online settings (e.g., third-party institutional mechanisms), will remain critical in blockchain settings.*

This conclusion along with our argumentation is consistent with recent work by Soellner et al. (2016). They showed (i) that trust from a user's perspective has different targets, namely information system, provider, Internet, and community of Internet users, and (ii) that trust in these targets may significantly affect usage intention (mediated by a system's perceived usefulness and perceived ease of use). Moreover, Soellner et al. (2012) found that a user's trust in an IT artifact is influenced by performance of the IT artifact (e.g., reliability), process of the IT artifact (e.g., understandability), and purpose of the IT artifact (e.g., authorized data usage). The blockchain is an IT artifact. Hence, the evidence by Soellner et al. (2012, 2016) substantiates our conclusion that the blockchain and its applications are not trust-free technologies.

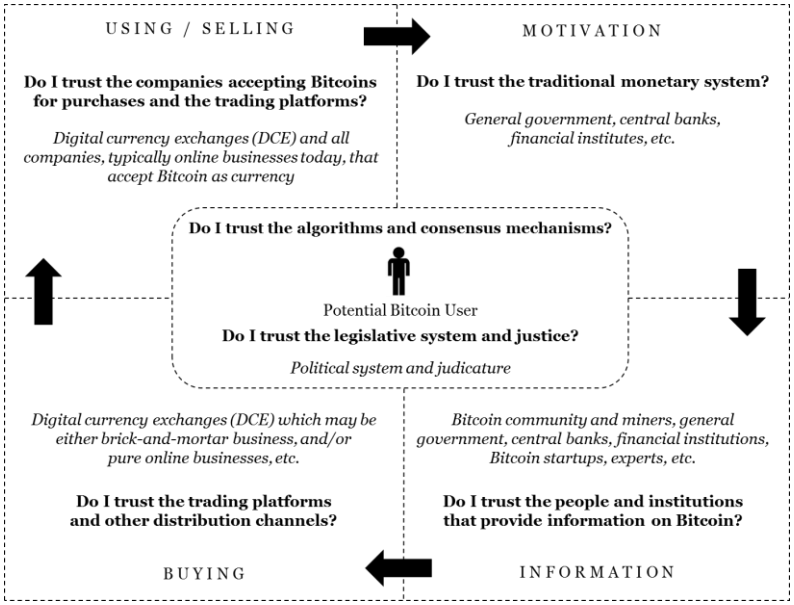

Figure 1. Simplified Trust Framework and Trust Questions from the Perspective of a Potential Bitcoin User

Summary of Contribution, Limitations, and Future Research

We conducted a systematic literature review to identify all published blockchain papers in the IS literature (85 papers), and we automatically searched for all trust text passages in these papers (we found 452 passages distributed across 61 papers). Based on this empirical foundation, we identified widely-held assumptions (i.e., the blockchain is trust-free, and trust in intermediaries is not needed any more). Based on a narrative discussion (with reference to Bitcoin as example) we showed that these assumptions are wrong. We argue that trust in the blockchain context is not so different at all compared to the more traditional online contexts such as e-commerce. To the best of our knowledge, this review is the most comprehensive study of the IS literature from a trust perspective that is currently available. Yet, the present review has limitations. *First*, the present study focused on IS journals and proceedings. It follows that our review does not include studies published in outlets from other fields, such as economics or computer science. Therefore, we make a call for future research which also analyzes literature in other scientific fields. *Second*, our critical reflection on the top-3 research themes focused on Bitcoin as an

example. However, while we have deliberately chosen Bitcoin as our study context, and despite the fact that we are currently not aware of arguments why our conclusions should not be generally applicable to other blockchain applications, it has yet to be shown whether generalization is possible. The devil lies in the detail, as the proverb says, and therefore future investigations have to discuss our insights in other blockchain contexts (for example, a recent BISE special issue on blockchain, Vol. 59/6, outlines several interesting contexts). *Third*, apart from the fact that the papers which were analyzed in our review constitute an empirical basis, our discussion of the top-3 research themes is conceptual in nature (despite the fact that we substantiate our argumentation by evidence presented in related work, e.g., Lustig and Nardi 2015). What follows is that future research should empirically study the questions indicated in our conceptual framework (see Figure 1).

Determining whom to trust and whom not to trust has been important since the early days of ancient civilizations. Trust in individuals who turned out not to be trustworthy led to death in many situations from the Stone Age to the Middle Ages. Moreover, it is argued that trust was a critical precondition for the prosperous development of early human societies, such as the ancient Greek society (Johnstone 2011). However, although in today's digital world the consequences of trusting untrustworthy people and firms are typically not as directly related to survival as they were in former times, broken trust, or blind trust, may result in severe economic consequences. Claiming that the blockchain is a trust-free technology is simply wrong. Anyone who doubts this fact could ask the people who invested in Bitcoins via intermediaries such as Mt.Gox and lost their money. Thus, a distinguishing factor among investors and users of Bitcoin (and other blockchain applications) is how they develop their trust in the people and firms behind the technological systems, and the technologies themselves (e.g., security mechanisms). As long as people develop and manage technologies, it is difficult to imagine that the fundamental trust principles will not be applicable any more.

References

Antonopoulos, A. 2014. *Bitcoin security model: trust by computation*: *A shift from trusting people to trusting math*. http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html.

Avital, M., Beck, R., King, John, L. Rossi, Matti, and Teigland, R. 2016. "Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future," in *Proceedings of the Thirty Seventh International Conference on Information Systems, Dublin, Ireland*.

Beck, R., Avital, M., Rossi, M., and Thatcher, J. B. 2017. "Blockchain Technology in Business and Information Systems Research," *Business & Information Systems Engineering* (59:6), pp. 381–384.

Berkely, J. Oct. 31st 2015. "The trust machine: The promise of the blockchain," *The Economist*.

Bhargavan, K., Swamy, N., Zanella-Béguelin, S., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., Kulatova, N., Rastogi, A., and Sibut-Pinote, T. 2016. "Formal Verification of Smart Contracts," in *Proceeding of the 2016 ACM Workshop on Programming Languages and Analysis for Security*, T. Murray and D. Stefan (eds.), Vienna, Austria, pp. 91–96.

Bonpay, Nov. 24th 2017. "Is Decentralized Bitcoin Really Decentralized?" https://medium.com/@bonpay/is-decentralized-bitcoin-really-decentralized-a3215467e1d5

Brin, D. 1999. "The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?" Basic Books.

Cao, S., Cao, Y., Wang, X., and Lu, Y. 2017. "A Review of Researches on Blockchain," in *Proceedings of Wuhan International Conference on e-Business 2017*, pp. 108–117.

Clemons, E. K., Dewan, R. M., Kauffman, R. J., and Weber, T. A. 2017. "Understanding the Information-Based Transformation of Strategy and Society," *Journal of Management Information Systems* (34:2), pp. 425–456.

Cohen, J. 2016. "A Coefficient of Agreement for Nominal Scales," *Educational and Psychological Measurement* (20:1), pp. 37–46.

Diniz, E. H., Siqueira, E. S., and van Heck, E. 2016. "Taxonomy for Understanding Digital Community Currencies: Digital Payment Platforms and Virtual Community Feelings," *Annual Workshop of the AIS SIG for ICT in Global Development*.

Gefen, D., Benbasat, I., and Pavlou, P. 2008. "A Research Agenda for Trust in Online Environments," *Journal of Management Information Systems* (24:4), pp. 275–286.

Gipp, B., Kosti, J., and Breitinger, C. 2016. "Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain," in *Proceedings of the Mediterranean Conference on Information Systems, Paphos, Cyprus*.

Glaser, F., and Bezzenberger, L. 2015. "Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems," in *Proceedings of the European Conference on Information Systems, Münster, Germany*.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., and Siering, M. 2014. "Bitcoin: Asset or Currency? Revealing Users' Hidden Intentions," in *Proceedings of the European Conference on Information Systems*, Tel Aviv, Israel.

Holotiuk, F., Pisani, F., and Moormann, J. 2017. "The Impact of Blockchain Technology on Business Models in the Pay," in *Proceedings of 13th International Conference on Wirtschaftsinformatik*.

Jarvenpaa, S., and Teigland, R. 2017. "Trust in Digital Environments: From the Sharing Economy to Decentralized Autonomous Organizations," in *Proceedings of the Hawaii International Conference on System Sciences*.

Johnstone, S. 2011. "A History of Trust in Ancient Greece," University Of Chicago Press.

Landis, J. R., and Koch, G. G. 1977. "The Measurement of Observer Agreement for Categorical Data," *Biometrics* (33:1), p. 159.

Leidner, D. E., Kettinger, B., Gonzalez, E., and Milovich, M. 2017. "Introduction to the HICSS-50 Minitrack on Practice-based IS Research," in *Proceedings of the Hawaii International Conference on System Sciences*.

Lustig, C., and Nardi, B. 2015. "Algorithmic Authority: The Case of Bitcoin," in *Proceedings of the Hawaii International Conference on System Sciences*, pp. 743–752.

Marella, V. 2017. "Bitcoin: A Social Movement Under Attack," *Scandinavian IRIS Association*.

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

McKnight, H. D., 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* (2:2), pp. 12-32.

Niederman, F., Clarke, R., Applegate, L., King, J. L., Beck, R., and Majchrzak, A. 2017. "IS Research and Policy: Notes From the 2015 ICIS Senior Scholar's Forum," *Communications of the Association for Information Systems* (40), pp. 82–92.

Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. 2017. "Blockchain," *Business & Information Systems Engineering* (59:3), pp. 183–187.

Notheisen, B., Cholewa, J. B., and Shanmugam, A. P. 2017a. "Trading Real-World Assets on Blockchain," *Business & Information Systems Engineering* (59:6), pp. 425–440.

Notheisen, B., Hawlitschek, F., and Weinhardt, C. 2017b. "Breaking down the Blockchain Hype - Towards a Blockchain Market Engineering, Appraoch," in *Proceedings of the European Conference on Information Systems*.

Papadopoulou, P., Kolomvatsos, K., Panagidi, K., and Hadjiefthymiades, S. 2017. "Investigating The Business Potential Of Internet Of Things," in *Proceedings of the Mediterranean Conference on Information Systems*.

Pavlou, P. A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1), pp. 37–59.

Risius, M., and Spohrer, K. 2017. "A Blockchain Research Framework," *Business & Information Systems Engineering* (59:6), pp. 385–409.

Schweizer, A., and et al. 2017. "Unchaining Social Businesses: Blockchain as the Basic Technology of a Crowdlending Platform," *in Proceedings of the Thirty Eight International Conference on Information Systems, Seoul, South Korea*.

Siira, E., Annanpera, E., Simola, O., Heinonen, S., Yli-Kantola, J., and Jarvinen, J. 2017. "Designing and Implementing Common Market for Cross-Game Purchases between Mobile Games," in *Proceedings of BLED eConference, Bled, Slovenia*, pp. 531–543.

Soellner, M., Hoffmann, A., Hoffmann, H., Wacker, A., and Leimeister, J. M. 2012. „Understanding the Formation of Trust in IT Artifacts," in *Proceedings of the Thirty Third International Conference on Information Systems, Orlando, FL*.

Soellner, M., Hoffmann, A., Leimeister, J. M. 2016. Why Different Trust Relationships Matter for Information Systems Users," European Journal of Information Systems (25:3), pp. 274-287.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. xiii-xxiii.

Zak, P. J., and Knack, S. 2001. "Trust and Growth," *The Economic Journal* (111:470), pp. 295–321.

View publication stats