Trusting the Trust Machine: Evaluating Trust Signals of Blockchain Applications

Fabiane Völter[1,2,3,*], Nils Urbach[1,2,4], Julian Padget[5]

[1]Project Group Business and Information Systems Engineering of the Fraunhofer FIT
[2]FIM Research Center
[3]University of Bayreuth
[4]Frankfurt University of Applied Sciences
[5]University of Bath

*Corresponding author: fabiane.voelter@uni-bayreuth.de

Abstract

Information systems research emphasizes that blockchain requires trust in the technology itself. However, we lack knowledge on the applicability of established trust cues to blockchain technology. Thus, this paper's objective is to empirically evaluate the effectiveness of several established IS trust formation factors on end user trust. We do so by conducting a between-groups experiment. While we can validate the applicability of previous IS trust research for blockchain technology to some extent, we find that trust signals emphasizing the technology's underlying trust-building characteristics are most effective. Hence, we highlight the need for contextualization of trust research on blockchain technology. We provide both researchers and practitioners with insights for building trustworthy blockchain applications that enable trust-less interactions not only in theory but in practice.
Keywords: Blockchain Technology, Trust Signals, End Users' Trust, Trustworthiness, Distributed Ledger

1. Introduction

Initially proposed by Nakamoto (2008) as the underlying technology of Bitcoin, blockchain technology aims to forgo control authorities. In essence, each node within a network holds a copy of transaction data. Instead of needing a controlling authority, blockchain's inherent characteristics regulate interactions, providing immutability and decentralization. Accordingly, blockchain technology can create an environment for trust-less interactions that allows each participant to directly engage with any other participant in a value exchange (Zheng et al., 2017). The literature on blockchain technology emphasizes this capability to enable trust-less transactions as the essential value proposition (Frizzo-Barker et al., 2020; Locher et al., 2018), but blockchain technology does not eliminate the need for trust at its core. Instead, using blockchain technology shifts the need for interpersonal trust to trust in the technology itself (Marella et al., 2020; Ostern, 2018). Specifically, users do not need to trust a control authority to oversee transactions but trust in implementations of algorithms regulating the transactions between users (Janssen et al., 2020). IS research also refers to this form of trust as "algorithmic trust" (Hawlitschek et al., 2018,

p. 55). Hence, for successful adoption of the technology, users' trust in blockchain technology is decisive. If users are unable to trust in the technology, its value proposition of creating an environment for trustless interactions will remain unfulfilled.

However, while IS research acknowledges the importance of trust in the technology, the sources of user trust in the technology remain unclear. Blockchain technology differentiates itself from other technologies by creating trustworthy ecosystems for untrusted interactions generated by itself. Accordingly, there is no intermediary or central party liable for faults in contrast to traditional platform ecosystems. Furthermore, blockchain is significantly less limited by ecosystem-based boundaries than conventional technologies. It is usually created by multiple, sometimes unknown, or untrusted actors and used by a heterogeneous group of users. As a result, trust in blockchain technology becomes less tangible than trust in traditional technology creating a single, distinct product.

Due to these differences between blockchain technology and conventional technologies, researchers have investigated which and how blockchain technology characteristics create trust (Marella et al., 2020; Ostern, 2018; Wallbach et al., 2020), mainly focusing on Bitcoin. However, IS research has observed underlying characteristics as well as extensively discussed strategies to stimulate trust in IT. For example, signals, which are signs or phenomena advocating the property of trustworthiness (O'Hara, 2012), have been established to foster user trust in autonomous agents and online environments at the application level (Benlian & Hess, 2011). Nevertheless, we lack investigations into whether the difference of blockchain technology compared to conventional IT affect not only underlying trust-stimulating characteristics but also the applicability of prevailing IS trust strategies. Only if established trust-building strategies also apply to blockchain technology, researchers and practitioners may build upon existing theoretical models as a basis for future research regarding trust and blockchain technology. Accordingly, our research objective is to examine whether signals stemming from the IS domain also engender trustworthiness in the context of blockchain technology. To do so, we pose the following research question:

To what extent are established IS trust signals also effective in enhancing a user's trust level in blockchain applications?

To answer this research question, we analyze the effectiveness of three signals by conducting a between-groups experiment. Specifically, we test the effectiveness of signals addressing familiarity, information, and reliability in combination with social effects. We do so by letting user groups interact with blockchain interfaces, which vary in the presence or absence of the aforementioned signals. We capture their level of trustworthiness using a questionnaire on the trustworthiness of IT artifacts developed by Jian et al. (2000). This approach allows us to empirically validate the impact of the presented signals on the level of trustworthiness.

We contribute to the literature on blockchain technology by building an empirical foundation for the currently solely theoretical discussion on trust in blockchain technology. By delivering empirical data about the applicability of IS trust research in the context of blockchain technology, we contribute to the academic discourse on trust formation in blockchain technology. Our findings can be used both in research for the motivation of using and contextualizing IS trust formation models to blockchain technology and in practice for the creation of meaningful blockchain implementations.

The structure of the remainder of the paper is as follows. In Section 2, we review the existing literature on trust in technology. We also present different concepts and evaluate their applicability for the underlying context. In Section 3, we lay out the conceptual development, which allows us to form hypotheses as a basis for the experiment that follows. In Section 4, we outline the experimental setup and justify the design choice of the application interface used. In Section 5, we present our results. Finally, we discuss our findings in Section 6, before we draw overall conclusions in Section 7.

2. Background

Trust has been widely examined from a psychological and organizational perspective. Also, in information systems (IS) research, trust became a central research objective (Benbasat et al., 2010) as the notion of a "human-to-technology trust relationship" was developed (Lankton et al., 2015, p. 882). In the following, we lay a theoretical foundation by reviewing different approaches to trust in technology and its creation before we address trust in the context of blockchain technology.

Trust in Information Systems Research

The exponential growth in complexity and a surge in user reliance on technology justifies the acknowledgment of IT artifacts as objects of human trust (Kelton et al., 2008; Nickel, 2013) as the individual is exposed to uncertainty, vulnerability, and dependence when interacting with an IT artifact (Söllner, 2015). Researchers have extensively studied trust in online environments, specifically trust in e-commerce (Liu & Goodhue, 2012; McKnight et al., 2002a; Pavlou & Gefen, 2004), in the matters of the disposition to trust, institution-based trust, trusting beliefs, intentions, and behaviors (Gefen & Pavlou, 2012; McKnight et al., 2002a). Furthermore, regarding the emergence of more complex technological artifacts, different trust constructs evolved (Lankton et al., 2015; Söllner et al., 2016). For example, trust may depend on the users' perception of social actors ("Computer-As-A-Social Actor"). Also, an approach stemming from Human-Computer-Interaction (HCI) research was derived to describe the formation of trust in IT artifacts.

The "computers-as-a-social actor" (CSA) paradigm is based on the observation that people view computers as teammates and assign them personality traits like helpfulness or dominance (Reeves & Nass, 1996). Similarly, Benbasat and Wang (2005) showed that users perceive IT artifacts as "social actors" in terms of virtual providers possessing human character traits. Therefore, IS trust research acknowledges that a human treats a computer as a social actor (Fussell et al., 2008; Nass et al., 1995; Reeves & Nass, 1996). This trust construct is also called human-like trust in technology (Lankton et al., 2015). Thus, IS research adopted the character traits of *ability*, *benevolence,* and *integrity* to describe the trustworthiness of IT artifacts (Benbasat & Wang, 2005; Gefen et al., 2003; McKnight et al., 2002a, 2002b; Pavlou, 2004). The traits originally have been established for describing the trust formation between people or in organizations (Castelfranchi & Falcone, 2010; Lankton et al., 2015; Mayer et al., 1995). The trait ability addresses the technology's necessary skills, competencies, and characteristics to fulfill its aims. Benevolence represents the absence of egocentric motivation, while integrity reflects the IT artifact's adherence to

acceptable principles (Lankton et al., 2015). The construct was used extensively for studying user trust in e-commerce and recommendation agents (Benbasat & Wang, 2005; Vance et al., 2008).

However, some researchers argue against the general applicability of the CSA paradigm because a concept designed for interpersonal relationships may not serve as an appropriate theoretical foundation for studying trust in IT artifacts (Söllner, Hoffmann, Hoffmann, et al., 2012). Accordingly, factors like benevolence can only be applied to humans while technologies may not have volition or follow ethical decision-making (Lankton et al., 2015). A "benevolent" IT artifact would have to be "able to actively decide whether to keep the interests of the trustor – its user – in mind or not" (Söllner, Hoffmann, Hoffmann, et al., 2012, p. 5). Consequently, the HCI approach was developed, which does not require technologies to have volition (Lankton et al., 2015). The HCI approach relies on various similar dimensions to describe the system-like trust in technology. For example, Lee and See (2004) and Söllner, Hoffmann, Hoffmann, et al. (2012) suggest that humans use the dimensions of *performance, process,* and *purpose* to evaluate the trustworthiness of IT artifacts. Performance represents the system's ability to support the user in reaching his or her goals. The process dimension reflects the user's judgement about the system's appropriateness. Lastly, the purpose dimension addresses the perceived intentions of the system's designer and its future value (Söllner, Hoffmann, Hoffmann, et al., 2012). These system-like trust dimensions are also sometimes termed as *reliability, functionality,* and *helpfulness* (McKnight et al., 2011) or *reliability, utility,* and *predictiveness* (Lippert & Swiercz, 2005).

Although we can adopt the CSA paradigm and the HCI approach as a basis for studying blockchain technology (Ostern, 2018), it is questionable whether the known trust-building strategies apply to blockchain technology. Signals are an established method to deliver the trustworthiness of a technology (Benlian et al., 2020; Nickel, 2011; O'Hara, 2012). They are evidential cues, which indicate to users that their predictive and normative expectations are met (O'Hara, 2012). Also, Nickel (2011) suggests that the perception of technology being trustworthy can be achieved via signals. He defines evidence for trustworthiness as "some available sign or phenomenon that makes it more likely that a desired performance is worth counting on and may be expected" (Nickel, 2011, p. 359). However, cues are often not present in online environments (Jøsang et al., 2007). Moreover, no consensus prevails regarding what those signals should be as they may take various forms and vary widely depending on the technology (O'Hara, 2012). Due to this context-dependence, it remains unclear what are the most effective ways to convey trustworthiness to the end users and what is "the right [..] kind of evidence for users to rely on technology" (Nickel, 2015, p. 564).

Creating Trustworthy Blockchain Technology

Originally developed as the underlying technology of Bitcoin (Nakamoto, 2008), blockchain can be described as a distributed data structure containing blocks of information about transactions or events. The blocks are linked using cryptographic hashes, which ensures relative tamper-proofness of information. Accordingly, by design, blockchain encompasses the features of decentralization, data integrity and transparency, and auditability. Further design parameters represent access restriction (private versus public) and read/write permissions (permissioned versus permissionless) (Fridgen et al., 2018). Researchers and practitioners have identified use cases in a variety

of industries, including financial services (Ali et al., 2020; Garg et al., 2021), supply chain and logistics (Dubey et al., 2020; Guggenberger et al., 2020; Pournader et al., 2020; Wamba & Queiroz, 2020), manufacturing (Hughes et al., 2020), and the energy (Djamali et al., 2021)as well as the public sector (Amend et al., 2021; Rieger et al., 2019).

As the original conception of blockchain was to enable trust-less transactions (Abbas et al., 2020; Hughes et al., 2019; Nakamoto, 2008; Upadhyay, 2020), research acknowledges that this promise is accompanied by a shift to trust in the technology itself (Ostern, 2018). Moreover, Schuetz and Venkatesh (2020) consider trust in the technology as a driver of blockchain adoption, highlighting the need to study the effects of IT features on end user trust. Also, Mattke et al. (2020) acknowledge that trust in blockchain technology motivates Bitcoin investment. However, little attention has been paid to the formation of trust in blockchain technology at its core. For example, Ostern (2018) found that only eight papers explicitly address trust in blockchain technology in the IS domain. All of those focus either specifically on Bitcoin or on cryptocurrencies. Additionally, Marella et al. (2020) investigated which attributes facilitate the creation of trust in the Bitcoin ecosystem. While the papers provide insights on trust-creating attributes inherent to blockchain technology, the question of how those attributes can be used to convey trustworthiness to the end user remains unanswered.

Regarding the end user's perspective, we could identify one research paper addressing the creation of trustworthy blockchain technology. Zavolokina et al. (2019) show how design science may be applied in the blockchain domain and highlight the need for IS research to more intensively address trust at the application level of the technology. While the researchers provide valuable insights for how trust signals may be derived, their sample size of nine participants does "not allow for generalizable conclusions about which [signals] are the most effective in building trust" (Zavolokina et al., 2019, p. 14).

Consequently, while it is of high relevance whether end users place their trust in blockchain technology and the interactions it enables, we lack insights on how to create trustworthy blockchain applications. It remains unclear to what extent established findings on trust in IS also apply to blockchain technology, too. Hence, we develop signals for trustworthiness based on the theoretical constructs and empirically evaluate them in a user study.

3. Conceptual Development

In this section, we develop signals for trustworthiness based on the finding that both the CSA paradigm and the HCI approach are valid constructs to describe the formation of trust in blockchain technology (Ostern, 2018). We followed a four-step procedure for the development of signals. First, we screened IS literature on trust in IT artifacts and identified signals increasing end user trust. Second, we screened the literature on blockchain technology and cryptocurrencies that address trust and identified factors as well as attributes of the technology that impede or foster trust. In a third step, we matched those attributes with established signals of trustworthiness to create only signals which are relevant for interacting with blockchain technology. Hence, the signals address either overcoming impeding factors or leveraging trust-fostering attributes of the technology. Lastly, for inclusion in our experiment, each signal must align either with the HCI approach or the CSA paradigm. This step ensures that the created

signals reflect fundamental trust formation processes. As a result, we identified familiarity, transparency, and interaction history in combination with network effects as relevant signals in the context of blockchain technology.

Signaling Familiarity

Ostern (2018) found that the need to rely on the trustworthiness of an unknown developer team impedes the formation of trust in blockchain technology. Also, Mathivathanan et al. (2021) highlight the role of familiarity on blockchain adoption in the context of supply chains. These findings are in line with the observation that interactions with strangers have been internalized to be inappropriate or even dangerous. In contrast, familiarity may serve as a signal for trustworthiness (Einwiller et al., 2000). It is defined as "an understanding often based on previous interactions, experiences, and learning of what, why, where and when others do what they do" (Gefen, 2000, p. 727). Logos serve as a means to signal respective familiarity (Lowry et al., 2007). Interacting with an IT artifact that is associated with a familiar company due to the presentation of a logo feels less perilous. Correspondingly, a requirement for trustworthy software is that users are familiar with the brand of the system and are aware of the designer's positive orientation towards the user (Söllner, Hoffmann, & Hoffmann, 2012). Applying this to the context of blockchain implementations implies that presenting a user with a familiar logo leads to higher trust in the implementation than with an unfamiliar logo. The signal also adheres to the last criterion for inclusion. It represents the dimensions of benevolence (CSA paradigm) and purpose (HCI approach). On the basis that previous research on both IT artifacts and blockchain technology attributes importance to the role of familiarity in trust formation, we form the first hypothesis.

> ***Hypothesis 1:*** *Equipping a blockchain implementation with a logo of an established and familiar brand will stimulate user trust in contrast to an unfamiliar logo.*

Signaling Transparency

The effect of transparency on trust has also been widely investigated, mainly in the domain of autonomous agents. For example, Wang and Benbasat (2007) showed that explanations enhance trust in recommendation agents as they make the performance of a system more transparent. Also, Verberne et al. (2012) found that providing information is beneficial for judgments of trustworthiness in the context of autonomous vehicles. Similarly, examining the trustworthiness of autonomous flight planners in planes, Sadler et al. (2016) concluded that systems' advice was trusted more often if the recommendation was accompanied by an explanation. Accordingly, information decreases uncertainty and risk associated with the usage of a system while in turn, transparency through information increases trust. It allows the user to feel he or she is given back control and the ability to monitor the "inner workings" of the system (Verberne et al., 2012, p. 807). Thus, information from explanation facilities allows to make predictions about the behavior of the system and develop expectations (Verberne et al., 2012). Consequently, the user can validate whether their expectations match system performance.

In contrast, Sas and Khairuddin (2015) found that insufficient knowledge about the underlying technology hinders user trust in the Bitcoin blockchain. Ostern (2018) also concludes that the technology's complexity impedes user trust. These observations relate well to the findings made by IS researchers in the context of autonomous systems.

Thus, we adopt the approach of IS trust researchers and use transparency to enhance the understanding of the system to increase trust. We contend that transparency through information supports blockchain users in making predictions about the artifact's behavior and develop expectations about its performance. As the signal of transparency was identified in the context of autonomous agents, it predominantly reflects the HCI approach. Specifically, transparency addresses the dimension of the "process of the IT artifact" (Söllner, Hoffmann, Hoffmann, et al., 2012). Regarding the specific type of explanation facility, we can rely on the finding that explanations which address the logical processes of a system are more effective compared to explanations addressing the reasons behind the actions taken by a system (Wang & Benbasat, 2007). This theoretical background allows us to form the second hypothesis:

> ***Hypothesis 2:*** *Accompanying a blockchain implementation with information explaining the underlying process of the system will lead to a higher level of trust than without the corresponding information.*

Signaling Past Credible Commitment

Functional requirements also support users in placing their trust in technology (Nickel, 2015). The CSA approach categorizes this aspect as ability, defined as "the trustor's perception that the trustee has the necessary skills, competencies, and characteristics" (Söllner, Hoffmann, & Hoffmann, 2012, p. 4) while the HCI approach's performance dimension addresses "the capability of the automated system in helping the user to achieve his goals" (Söllner, Hoffmann, & Hoffmann, 2012, p. 4). The fact that functional requirements are emphasized by both approaches highlights this factor's importance in the trust formation process. Considering Ostern's (2018) finding that accountability is central for blockchain users, this also applies to the underlying technology. Also, Marella et al. (2020) found that functional attributes including the technology's ease of transactions, decentralization, immutability, and openness foster trust among its users. Accordingly, the dimension of functionality should be addressed when designing trustworthiness signals for blockchain implementations.

This aspect of reliability of the technology is also indirectly reflected by social effects. Social effects cause trust due to the positive recommendation from trusted individuals. Credible individuals serve as a reputation for the network's reliability (Sas & Khairuddin, 2017). Also, Khiabani et al. (2010) find that the "most relevant sources of information to calculate trustworthiness of an entity are the previous transactions of that entity with other parties" (p.831). This effect was also observed in the context of blockchain technology. When it comes to trusting the technology, participants "mimic the behavior of their friends or acquaintances" (Ostern, 2018, p. 13). Bitcoin users joined the network because they heard from their friends or on social networks (Sas & Khairuddin, 2017). Hence, we argue that seeing other users engage with an implementation in real-time enhances trust. Ostern (2018) classifies this observation as the human tendency to anthropomorphize technology, which corresponds to the CSA paradigm. On this basis, we form our third hypothesis:

> ***Hypothesis 3:*** *Seeing both current users and the entire history of past interactions is more conducive towards trust in the blockchain implementation than without said elements.*

4. Method

We validate the effectiveness of the identified trust signals based on a between-groups experiment, an acknowledged research method for IS research (Jenkins, 1985). Experiments aim to determine the relationship among variables and subjects by manipulation and controls (Palvia et al., 2004) and are especially suitable for user-systems interface studies as experiments allow to test hypotheses on the utility of an artifact (Jarvinen, 2000; Jenkins, 1985).

Experimental Design and Participants

Our study aims to examine whether the signals identified in Section 3 effectively enhance end users' level of trust in blockchain implementations. Thus, we aim to measure the difference of trust between implementations containing the signals and implementations without respective signals, resulting in four test conditions. We choose a between-groups experimental design to test the impact of the manipulations. This setting allows controlling for learning effects because participants interact with only one condition rather than several (Lazar et al., 2017). As a consequence, individual differences have to be accounted for by comparatively larger sample sizes. We chose the sample size based on research conducting similar experiments. Verberne et al. (2012) tested six conditions of automated cruise control systems with 59 participants. Lazar et al. (2017) suggest 15-20 participants for each group. Thus, to maximize the accuracy of our results, we aimed for 20 participants per condition, resulting in a total of 80 participants.

We chose to recruit students as participants for our experiment owing to our direct access to these participants and their everyday interaction with technology. Thus, we expect that individual biases towards technology are less likely to impact our results compared to conducting the study with an older cohort. Besides, we made sure that the groups are as similar as possible demographically to mitigate potential confounding factors (MacKenzie, 2012). Hence, all participants were students recruited at two universities in Great Britain. Half the students were enrolled in Computer Science departments and the other half in other departments, which allowed us to balance out different levels of experience with technology. A major fraction of 87.5% of participants were completing their post-graduate degree, while 12.5% are undergraduate students. Participants' ages varied between 21 and 35 years ($M = 24.07$, $SD = 2.685$), and comprised a close to equal mix of males and females, with 55% and 45%, respectively (see also Appendix D).

Data Collection

Regarding the use case underlying our experimental setting, we adapt the conflict example proposed by Weber et al. (2016). Accordingly, disputes about errors and delays in collaborative processes in supply chains represent a major challenge for business processes, which a blockchain-based solution may overcome. Thus, our experimental setting describes two parties, who aim to resolve their conflicts with an immutable audit trail documented in a distributed manner on a blockchain. Consequently, we address the trustworthiness within a permissioned blockchain implementation.

We briefed participants on the scenario (see Appendix A) and gave them basic information about blockchain technology to ensure common understanding of the technology. Afterwards, participants completed a task to interact with the interface by adding four orders to the ledger. Thereafter, they filled out a questionnaire to capture their level of trust. Additionally, qualitative interviews were conducted with three participants from each group.

Implementation Interface: The participants were presented one of four interfaces. The control condition contains all signals, while the three treatment conditions withhold them, respectively. The concrete signals were designed based on the hypotheses developed in Section 3. The first signal addresses familiarity through the display of a logo. We tested the presence of a familiar logo against an unfamiliar logo instead of testing presence versus absence. This allows measurement of the difference in trust of familiarity versus unfamiliarity rather than the difference between familiarity versus no association with any entity. Based on a pilot study prior to the experiment, we included the logo of IBM as the most familiar brand in the control condition and substituted it by the logo of Devvio as a likely unfamiliar brand in the respective treatment group (see Appendix B).

To test the second hypothesis that information about how the ledger works increases trust, an information box (see feature 2 in Figure 1) was included in the implementation. The respective treatment condition did not contain the information box (see Figure 3). The information aims at educating the user about the inner workings of the system. Our pilot study conducted prior to the experiment ensured that we achieved the signal identified in Section 3 (see Appendix B).

A list of entries represents the third hypothesis (see feature 3 Figure 1). To show real-time interaction of other users, we implemented a script adding randomized entries every second. The table also listed the name of the person adding the entry. This element aimed at evoking the feeling that other users are using the implementation at the same time. Again, in the respective treatment condition, the entry list was eliminated (see Figure 4). However, both the box "order detail" and the information box are out of context without the list of entries. To prevent that confusion negatively affects user trust, these two elements were also excluded in the treatment condition. To account for this design, we measure both the differences in group assignment and the single effect of the signals on user trust (see Results).

Trustworthiness: The level of trustworthiness was measured by twelve questions (see Appendix B) on a 7-point Likert scale (*1 = Not at all, 7 = Extremely*). We used the questions proposed by Jian et al. (2000) who developed the questionnaire for measuring the trustworthiness of automation technology. As trust in blockchain technology is affected by similar characteristics as trust in autonomous systems (Ostern, 2018), we argue that it can also be used in the underlying context, too. Additionally, we collected demographic details including the participants' age, gender, educational level, and their degree to validate consistency across the groups.

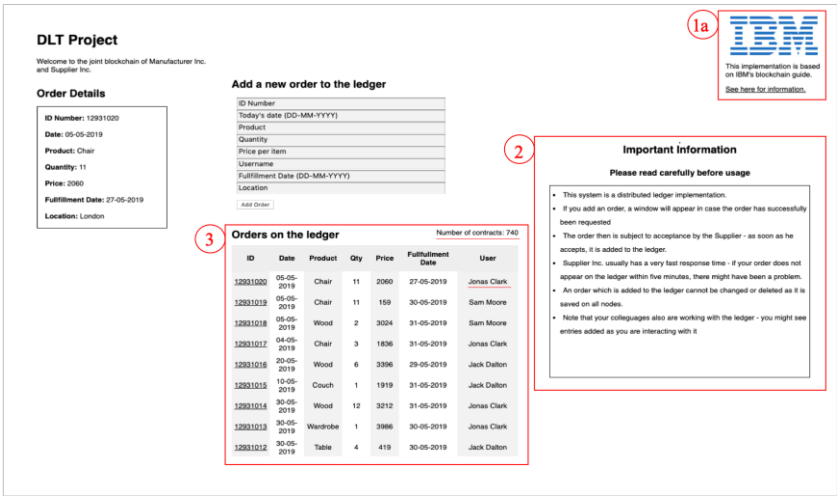

Figure 1: Interface Control Group

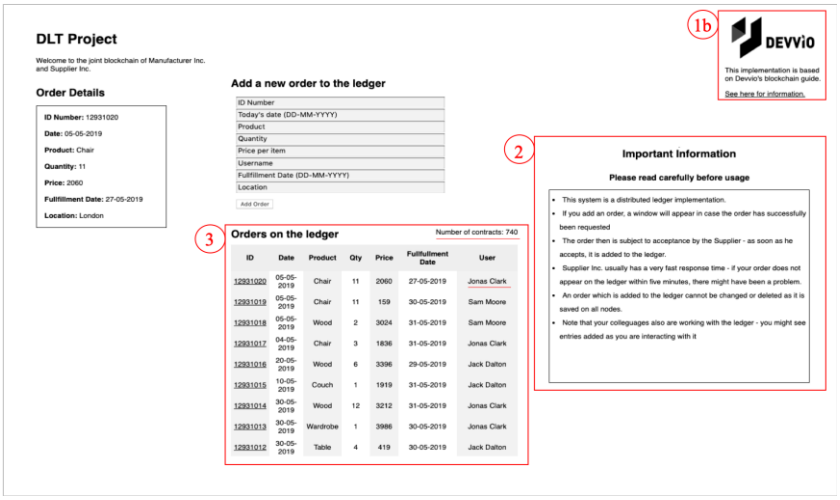

Figure 2: Interface Group 1

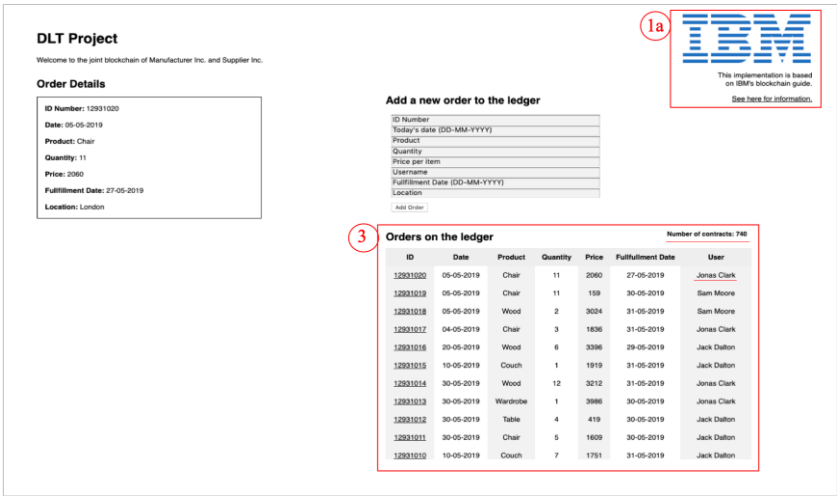

Figure 3. Interface Group 2

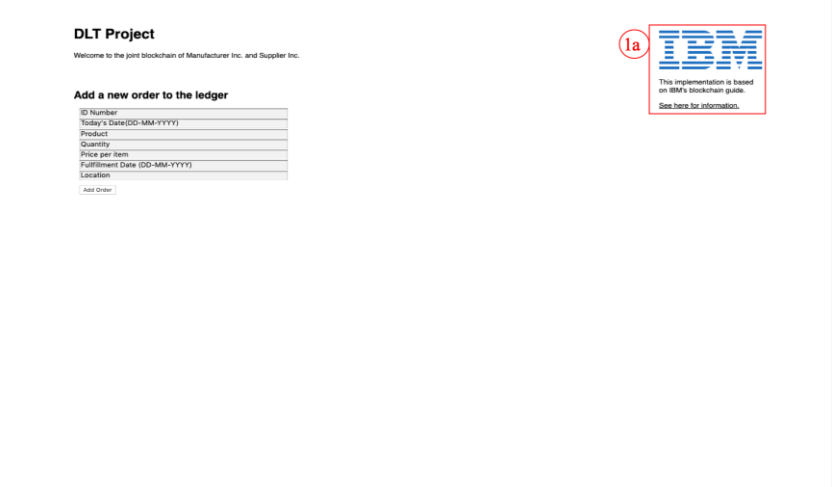

Figure 4: Interface Group 3

Qualitative Interviews: Interviews were conducted with a dozen participants from all experimental groups to gain a deeper understanding of the users' perspectives. We aimed to identify whether they desired further aspects of trustworthiness that we did not consider so far, in a semi-formal setting, to ensure participants freely expressed their opinions. We carried out the interviews after the questionnaire had been filled out to ensure that we did not bias participants with insights on the aim of the study.

5. Results

In the analysis, responses were coded such that higher scores indicate a higher level of trustworthiness. The scale was found to have a large Cronbach's alpha ($\alpha = .92$) indicating internal consistency. A chi-square test of goodness-of-fit reveals that all characteristics are equally distributed across the groups except for the educational status (see Appendix D). However, we argue that the difference between being enrolled in an undergraduate compared to a postgraduate degree has little impact as all participants were on track for higher education.

Quantitative Results

The quantitative data collected from the questionnaire (Appendix B) was analyzed in two ways. First, the difference between the four groups was observed, then we tested for the signals. In the following, the term "Trustworthiness Score" (TS) refers to the average score out of all survey items.

Testing for Group Assignment

As can be observed in Figure 5, the mean score in Group 1, 2 and 3 is lower than in the Control Group. A Fisher's test (ANOVA) reveals that the difference in variance of the TS between the groups is statistically significant and hence can be attributed to the test condition ($F_{(3, 76)} = 13.5$, $p < 0.001$). Furthermore, a Tukey's range post-hoc test determines which groups specifically deviate. Table 1 shows that the score of Group 3 differs significantly from all other conditions. The results of the Control Group do not differ significantly from Group 1 ($p = 0.867$), but from Group 2 at a 10% confidence level ($p = 0.055$). No effect can be found between Group 1 and 2.

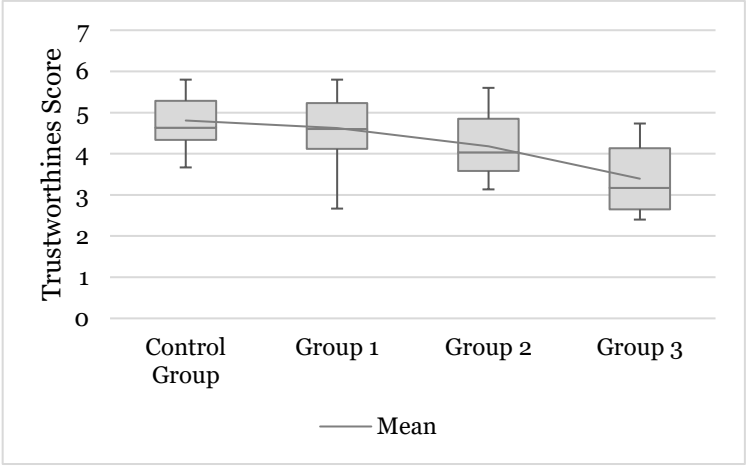

Figure 5: Group Allocation on Trustworthiness Score

An analysis of variance including the covariances (ANOCOVA) rules out any of the demographic details being a significant covariate (age: $F = 0.004$, $p = 0.951$; gender: $F = 0.091$, $p = 0.764$; enrollment: $F = 0.190$, $p = 0.664$; education: $F = 0.102$, $p = 0.75$). The assumptions of the test are met (independent samples by random distribution; Levene's test for Equality of Variance: $F_{(3, 76)} = 5.98$, $p = 0.619$; Shapiro-Wilk test of Normality: $W = 9.973$, $p = 0.085$).

		Control Gr.	*Group 1*	*Group 2*	*Group 3*
Control Group	Mean difference	—	0.187	0.627	1,413
	p-value	—	0.867	0.055	**< .001**
Group 1	Mean difference		—	0.44	1,227
	p-value		—	0.274	**< .001**
Group 2	Mean difference			—	0.787
	p-value			—	**0.009**
Group 3	Mean difference				—
	p-value				—

Table 1: Results of Turkey Post-Hoc Test

Additionally, we analyzed the effect of group assignment on the scores of the individual trust items. As the values are not normally distributed ($W = 0.846$, $p < 0.00$), we conducted a Kruskal-Wallis test, which is considered a non-parametric analogue for MANOVA. Accordingly, all 12 items differ significantly across the four experimental groups (see Table 2). A pairwise comparison allows attribution of the difference to specific groups. All results are adjusted by the Bonferroni correction. In most cases, the effect is due to the differences between the Control Group and Group 3, and Group 1 and 3. In contrast, the difference for the terms "deceptiveness" and "underhandedness" was significant for the Control Group and Group 2 ($p = 0.002$; $p = 0.009$, respectively). Deceptiveness was also rated differently in Group 1 in comparison to Group 2. In line with the observation that there is no significant difference between the Control Group and 1 on the average score, no difference between the single items on the scale is apparent for those conditions either.

Item	χ^2	*df*	*p*
Trust	26.30	3	**< 0.001**
Reliability	17.15	3	**< 0.001**
Integrity	20.74	3	**< 0.001**
Security	15.41	3	**0.001**
Suspicion	15.28	3	**0.002**
Confidence	14.72	3	**0.002**
Dependability	13.88	3	**0.003**
Deceptiveness	13.90	3	**0.003**
Underhandedness	12.31	3	**0.006**
Familiarity	12.29	3	**0.006**
Harmfulness	10.02	3	**0.018**
Wariness	9.09	3	**0.028**

Table 2: Difference in Rating of the Single Items Between the Groups (Kruskal-Wallis-Test)

Testing for Signals

As the groups contain mixed signals on trustworthiness, we also measured their single effect on the recorded trustworthiness. For example, Group 3 contains neither the signal for information nor the list of entries. Analyzing the effect of the single signals allows drawing precise conclusions. As a Shapiro-Wilk test for normality revealed that the errors might not be normally distributed under Signal 3 ($W = 0.895$, $p = 0.033$), we conduct a non-parametric test rather than a parametric analysis of variance (see Table 3).

	Sum of Squares	*df*	*p*	*ε2*
Signal 1: Familiarity	2.86	1	0.091	0.0362
Signal 2: Transparency	19.90	1	**< .001**	0.252
Signal 3: Entry List	19.87	1	**< .001**	0.252

Table 3: The Effect of Cues on the TS (Kruskal-Wallis-Test)

The test results confirm that both the signal of information and commitments have a significant effect on the TS while the familiar logo does not. The test statistic of Signal 2 and Signal 3 differs only slightly (~ 0.003), while the effect size (ε^2) of both is given with 0.252, which suggests that both the information box and the list of entries explain 25.2% of the variance of the TS. In contrast to the parametric test, Signal 1 is significant at a confidence level of 10% only. Its ε^2 value suggests a rather small effect size of 3.62%.

Furthermore, we measured the effects of the signals on the items of the trustworthiness scale. As the test for normality suggests normality cannot be assumed, we have to rely on non-parametric tests. While there is no prevailing consensus about the most appropriate method for a non-parametric alternative to MANOVA, we chose Ordinal Logistic Regression as this method can handle data-like ranks and is readily extendable to multiple factors (Kikvidze & Moya-Laraño, 2008; Oja, 2010). A Pearson Square test confirms that the model fits the data well as all tests lead to a non-significant result ($p > 0.05$). Also, its assumptions are met (Thompson, 2017).

Regarding the Control Group and Group 1, our findings are analogous with our previous results: the signal of a familiar logo in contrast to an unfamiliar one had no significant effect on any single item on the trustworthiness scale as no p-value is lower than 0.05. We observe significant effects of the second signal, information on the perceived deceptiveness, underhandedness and trust are significant at a 5% confidence level ($p < 0.001$, $p = 0.001$, $p = 0.046$, respectively). Furthermore, Signal 2 also has affected the participant's suspicion of the system ($p = 0.085$). However, considering a confidence level of 10%, we study the effect with precautions. Moreover, Signal 3 affects all items except for the perceived underhandedness and wariness ($p = 0.511$ and $p = 0.197$, respectively). We list a summary of the results and the validation of hypotheses in Table 4.

Signal	*Effect on trustworthiness score*	*Effect on single items*	*Support of hypothesis*
Signal 1: Familiarity	None ($p = 0.091$)	None	None
Signal 2: Information	Strong ($p < .001$)	Perceived deceptiveness, Underhandedness, Trust, (Suspicion)	Hypothesis 2
Signal 3: Interaction history & network effects	Strong ($p < .001$)	Deceptiveness, Suspicion, Harmfulness, Confidence, Security, Integrity, Dependability, Reliability, Trustworthiness, Familiarity	Hypothesis 3

Table 4: Summary of Signals' Effects

Qualitative Results

The collected qualitative data provides additional information about why participants gave specific answers. All three control group participants answered that seeing the entry immediately appearing helped place trust in the system. One participant responded that it "seems infallible because I cannot edit it after adding it". Another participant said that "because it is there, it must be saved somewhere". The participants also answered that they are reasonably confident in their answers. Concerning the information box, it helped a participant to "get with it" in the beginning as it described what is happening. However, "it was more the table that made [him] trust the system". Two participants said they did not notice the logo, while one did. For example, one participant emphasized that the IBM visual "helped [her] to base [her] trust in the system". In contrast, another participant stated that it did not negatively affect him, but he "didn't notice it actually". Similarly, one participant stated that he "saw that, but did not really pay attention to [the logo]".

Participants of Group 1, which included another logo, gave similar answers. One participant added that she mainly based her trust on the information that it is a blockchain-based system and its "legitimate looks". This was further strengthened by the fact that there was "nothing suspicious" about the system. However, she noted that she could not assess the degree of connection between the interface and the technology in the backend.

For Group 2, the interviewed participants seemed still to base their trust on the list of entries. However, a participant noted that because "it popped up there, I figured that's how it's supposed to work". Concerning the confidence in their answers, an interviewee also mentioned that she was not "super sure about it".

Regarding Group 3, interviewees agreed that the lack of information on what is going on hindered their reliability and trust judgments. One participant noted that "I don't know what is going on in the backend; I mean, there could be a lot of things actually going wrong that I don't know about." Another one noted that "there was nothing that I could base my judgment on, so I really couldn't trust [the system]."

In summary, our qualitative data suggest that the unobtrusiveness of Signal 1 may be the cause of its ineffectiveness. Further, the data support our quantitative result that information helps users base their trust in the system while the lack of an interaction history hinders trust formation.

6. Discussion

While trust in blockchain technology is crucial for researchers and practitioners to create implementations that fulfill its value proposition, we lack knowledge in the means to stimulate trustworthiness. Specifically, we do not know to what extent existing IS research on trust applies to blockchain technology. Accordingly, on the basis of the CSA and the HCI approach, we extend the trust literature on blockchain technology by an empirical evaluation of trust signals. Our expectation that formerly developed signals are not necessarily applicable to the context of blockchain technology holds true. Thus, established IS trust signals are effective in enhancing a user's trust level in blockchain applications to a limited extend only. In the following, we evaluate the hypotheses derived in Section 3 and discuss the resulting implications for theory and practice. We also outline the limitations of our research and highlight future research opportunities.

Theoretical Implications

In contrast to Zavolokina et al. (2019), who found that information about providers enhances trust in blockchain implementations, our results show that the users' level of trust in blockchain technology is not affected by association with a familiar organization. Based on our qualitative results, we infer that the association with a developer team or company does not affect all users generally but is at least to some degree user-dependent. This, in turn, aligns with Ostern's (2018) finding that the reliance on the trustworthiness of an unknown developer team does encourage distrust among some Bitcoin users, but only a small proportion. Furthermore, this finding aligns with the underlying motive and philosophy of using blockchain technology as it represents a technology independent of a central service provider or intermediary (Mattke et al., 2020). As a consequence, we find that institutional trust is of little relevance in the context of blockchain technology.

Moreover, our study confirms the expectation of Schuetz and Venkatesh (2020) regarding a positive effect of environmental variables like explanations as users significantly more often stated that they "trust the system" when information was provided. Furthermore, users rated the characteristics "deceptiveness" and "underhandedness" considerably different. Thus, we conclude that information supported users in predicting how the system worked. This result is consistent with previous research stating that complexity is one of the main factors negatively influencing user trust in Bitcoin (Ostern, 2018; Sas & Khairuddin, 2017; Zavolokina et al., 2019), while transparency and comprehensibility increase trust in the system (Lustig & Nardi, 2015).

Similarly, our study confirms that displaying previous and concurrent transactions of other users increases perceptions of trust, reliability, and integrity. This observation corresponds to the argument that a history of past interactions and social effects enable users to form and confirm their expectations about functionalities and characteristics. Also, previous research found that the attributes immutability and decentralization positively influence users' trust (Marella et al., 2020; Ostern, 2018; Sas & Khairuddin, 2017). Thus, we show that highlighting trust-stimulating attributes of the technology enable user trust.

Regarding our theoretical contribution, we follow previous researchers' recommendations to investigate trust elements of blockchain implementations (Zavolokina et al., 2019). Current research on blockchain technology and

trust typically observes fundamental characteristics of the Bitcoin blockchain, which help users form trust in the technology. While we can use foundational research for developing trust signals, we conducted a user-centric study focusing on the application level. Thus, we observed trust in blockchain technology from a different perspective.

Furthermore, while we acknowledge Ostern's (2018) finding that both the CSA paradigm and the HCI approach serve to describe trust in blockchain technology, our findings deliver less evidence for the applicability of the CSA paradigm than the HCI approach. Accordingly, we find that trust in blockchain technology has limited parallels to trust in a social actor. Rather, the HCI's approach dimensions process, performance, and purpose (Söllner, 2015) are more applicable to describing trust in blockchain technology. Thus, we recommend future researchers to rely on the notion stemming from HCI rather than the CSA paradigm to describe trust in blockchain applications. This observation also provides insights regarding the future development of trust signals: while the effective signals were drawn from previous research on autonomous agents, the ineffective signal was drawn from research on interactions in online environments. This finding is surprising as blockchain technology provides an infrastructure for interactions, and users do not directly face the IT artifact. In contrast, relying on autonomous systems calls for direct interactions with the IT artifact (Verberne et al., 2012). Thus, as our results show similarities to findings stemming from user-facing technologies, we highlight that investigating user-related aspects of blockchain technology is highly relevant, although it represents a non-user facing technology (Ostern, 2018).

Furthermore, our findings that familiarity with the service provider is ineffective in stimulating trust, while explanations of the application's features and observations from the community are highly effective have further implications for theory. In specific, our results emphasize the entanglement of the underlying observation object: signals, which represent features relevant in the context of interacting with blockchain technology were effective, while the other was not. This observation implies that only features inherent to the blockchain ecosystem allow the stimulation of trust. Specifically, we suggest that researchers must adapt theories on trust in IS to the context of interacting with blockchain technology to be effective (Burton-Jones & Volkoff, 2017). This theoretical observation may not apply only to trust research but also other prominent IS research topics. Thus, we motivate the contextualization of further IS concepts onto the context of blockchain, too – similar to the current reorganization of research on IT governance on blockchain technology.

Implications for Practice

Besides our theoretical contribution, our research has strong managerial implications. Specifically, our insights on suitable trust signals can assist developers in utilizing blockchain technology's full potential to design trustworthy applications. Building trusted implementations is particularly crucial for blockchain technology as it mediates interactions between untrusted users. Hence, the technology may fulfill its purpose only if its users trust it. Thus, our results support designers and application builders in integrating trustworthy signals to stimulate end user trust, which allows fully leveraging the technology's inherent trust-building characteristics.

Regarding development cycles, our findings enable specifying design goals and the formation of requirements during the developmental stages of blockchain applications. Furthermore, practitioners may use our findings as a

basis for the evaluation of prototypes and pilots. Because we found that signals differ in their level of trustworthiness, developers may use our results as a foundation for benchmarking blockchain application prototypes regarding their trustworthiness during piloting stages.

We also make specific recommendations for practitioners. First, our results show that familiarity with the provider plays an insignificant role in trust formation. This implies that unfamiliar organizations and institutions may deliver trusted blockchain implementations, which may motivate the emergence of new creators in the blockchain implementation field.

Second, we suggest that transparency by providing information about the system is the primary factor attention should be paid to when designing blockchain interfaces as information allows users to form expectations about system functionalities. Thus, in line with previous literature, we encourage practitioners to minimize system complexity to avoid adverse effects on user trust (Lustig & Nardi, 2015; Ostern, 2018). However, textual information boxes may not be the only option for creating a transparent environment and supporting the user in building mental models about the system's behavior. There may as well be other means to achieve this goal. For example, tooltips, FAQs, or chatbots may represent alternative textual information tools (Zavolokina et al., 2019). Information may also be transmitted in audio or visual form by explanation tracks or videos. Hence, we suggest future researchers to address the effectiveness of different explanation forms, which may differ depending on situational constraints.

Third, in consequence of confirming our third hypothesis, we suggest that trust signals should leverage the inherent trust-building characteristics of the technology and acknowledge the social effects of trust formation. Thus, according to our theoretical implications, we motivate researchers to contextualize theory and emphasize the need for practitioners to contextualize signals used in blockchain implementations. Trust signals should highlight and leverage the underlying trust-stimulating characteristics of the technology.

Last, while signals are supportive in highlighting the technology**'**s trust-stimulating characteristics, they also allow generating trust in untrustworthy environments. Thus, besides supporting researchers in underscoring the technology's trust features, our findings also allow deriving insights on how to create trusted blockchain applications in untrustworthy environments. Accordingly, trust mechanisms can be misused to create trusted but untrustworthy blockchain implementations. For this reason, we encourage practitioners to also enable users to validate the trustworthiness of the underlying blockchain implementation itself. For example, this may include showing that blockchain's underlying characteristics like immutability are fulfilled. Against this backdrop, conveying the dimensions of performance and process of the system becomes even more important for the creation of trusted and trustworthy blockchain implementations.

Limitations and Future Research

Despite following a rigorous research approach, our study is subject to limitations. First, as we observe organizational blockchain implementations, we do not claim the generalizability of our findings to all architectural configurations. Although our findings provide insights regarding the creation of trustworthy private blockchain imple-

mentations in an inter-organizational context, we encourage further research on trust in blockchain implementations in diverse domains and of different architectural types. Second, our sample is young and highly educated meaning that participants might be more technology-savvy than the broader population. While our sample characteristics prevented biased results due to individual biases towards technology, a replication of the study with a different cohort would allow determinating the wider applicability of our results. Third, our experimental setup allows for future research. We encourage future research to separately observe the effect of an interaction history and social effects to draw a precise conclusion about which of those is more effective. Furthermore, as information increased trust in blockchain technology implementations, future researchers should specify and investigate various ways of displaying information to solicit the most effective way to build trust.

7. Conclusion

Our research is motivated by the observation that "trust-less interactions" enabled by blockchain technology are preceded by a shift to trust in the technology itself. However, we lack insights into the formation thereof, as due to its different nature, the applicability of established trust-building strategies from IS research onto blockchain technology remains unclear. Thus, we build on previous research on fundamental trust-building characteristics of blockchain technology and validate the effects of three signals on end user trust embedded in the established CSA paradigm and HCI approach. We chose an experimental research approach to measure the impact of the signals' presence and absence on trust.

Our findings extend the trust literature on blockchain technology by an empirical evaluation of trust signals, revealing that not all insights from previous IS research on trust in IT artifacts apply to blockchain technology. Consequently, we highlight the importance of contextualizing and validating the applicability of prior research on IT artifacts for blockchain technology. In line with our theoretical contribution, we highlight the need for practitioners to design trust signals at the application level, emphasizing and leveraging the underlying trust-stimulating characteristics of the technology. Furthermore, we suggest that applications prioritize transparency by informing the user about how the system works and what they will experience. Practitioners may also use past interactions to convey the fulfillment of functionality by the implementation. Integrating former users into those past interactions leverages social effects. Finally, we hope that future research relies on our results to discuss users' trust in blockchain technology to advance meaningful application development further and drive widespread adoption. We also motivate future researchers to extend IS research's applicability to blockchain technology by contextualizing prevailing IS concepts onto blockchain technology.

8. References

Abbas, Y., Martinetti, A., Moerman, J.-J., Hamberg, T., & van Dongen, L. A. (2020). Do You Have Confidence in How Your Rolling Stock Has Been Maintained? A Blockchain-Led Knowledge-Sharing Platform for Building Trust Between Stakeholders. *International Journal of Information Management*, *55*(102228), 1–10. https://doi.org/10.1016/j.ijinfomgt.2020.102228

Ali, O., Ally, M., Clutterbuck, & Dwivedi, Y. (2020). The State of Play of Blockchain Technology in the Financial Services Sector: A Systematic Literature Review. *International Journal of Information Management*, *54*(102199), 1–19. https://doi.org/10.1016/j.ijinfomgt.2020.102199

Amend, J., Kaiser, J., Uhlig, L., Urbach, N., & Völter, F. (2021). What Do We Really Need? A Systematic Literature Review of the Requirements for Blockchain-Based E-Government Services. In *Proceedings of the 16th International Conference on Wirtschaftsinformatik (WI21)* (pp. 1–16). AIS.

Benbasat, I., Gefen, D., & Pavlou, P. (2010). Introduction to the Special Issue on Novel Perspectives on Trust in Information Systems. *MIS Quarterly*, *34*(2), 367–371. https://doi.org/10.2307/20721432

Benbasat, I., & Wang, W. (2005). Trust in and Adoption of Online Recommendation Agents. *Journal of the Association for Information Systems*, *6*(3), 72–101. https://doi.org/10.17705/1jais.00065

Benlian, A., & Hess, T. (2011). The Signaling Role of IT Features in Influencing Trust and Participation in Online Communities. *International Journal of Electronic Commerce*, *15*(4), 7–56. https://doi.org/10.2753/JEC1086-4415150401

Benlian, A., Klumpe, J., & Hinz, O. (2020). Mitigating the Intrusive Effects of Smart Home Assistants by Using Anthropomorphic Design Features: A Multimethod Investigation. *Information Systems Journal*, *30*(6), 1010–1042. https://doi.org/10.1111/isj.12243

Burton-Jones, A., & Volkoff, O. (2017). How Can We Develop Contextualized Theories of Effective Use? A Demonstration in the Context of Community-Care Electronic Health Records. *Information Systems Research*, *28*(3), 468–489. https://doi.org/10.1287/isre.2017.0702

Castelfranchi, C., & Falcone, R. (2010). *Trust Theory: A Socio-Cognitive and Computational Model*. John Wiley & Sons. https://doi.org/10.1002/9780470519851

Djamali, A., Dossow, P., Hinterstocker, M., Schellinger, B., Sedlmeir, J., Völter, F., & Willburger, L. (2021). Asset Logging in the Energy Sector: A Scalable Blockchain-Based Data Platform. In *Proceedings of the 10th DACH+ Conference on Energy Informatics.* Springer.

Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K., & Papadopoulos, T. (2020). Blockchain Technology for Enhancing Swift-Trust, Collaboration and Resilience Within a Humanitarian Supply Chain Setting. *International Journal of Production Research*, *58*(11), 3381–3398. https://doi.org/10.1080/00207543.2020.1722860

Einwiller, S., Geissler, U., & Will, M. (2000). Engendering Trust in Internet Business Using Elements of Corporate Branding. In *Proceedings of the 6th Americas Conference on Information Systems (AMCIS)* (pp. 733–739). AIS.

Fridgen, G., Radszuwill, S., Urbach, N., & Utz, L. (2018). Cross-Organizational Workflow Management Using Blockchain Technology-Towards Applicability, Auditability, and Automation. In *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS)* (pp. 1–10). IEEE. https://doi.org/10.24251/HICSS.2018.444

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a Disruptive Technology for Business: A Systematic Review. *International Journal of Information Management*, *51*(102029), 1–14. https://doi.org/10.1016/j.ijinfomgt.2019.10.014

Fussell, S. R., Kiesler, S., Setlock, L. D., & Yew, V. (2008). How People Anthropomorphize Robots. In *Proceedings of the 3rd ACM/IEEE International Conference on Human Robot Interaction* (pp. 145–152). Association for Computing Machinery. https://doi.org/10.1145/1349822.1349842

Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the Perceived Benefits of Implementing Blockchain Technology in the Banking Sector. *Technological Forecasting and Social Change*, *163*(120407), 1–18. https://doi.org/10.1016/j.techfore.2020.120407

Gefen, D. (2000). E-Commerce: The Role of Familiarity and Trust. *Omega*, *28*(6), 725–737.

Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, *27*(1), 51–90.

Gefen, D., & Pavlou, P. A. (2012). The Boundaries of Trust and Risk: The Quadratic Moderating Role of Institutional Structures. *Information Systems Research*, *23*(3), 940–959. https://doi.org/10.1287/isre.1110.0395

Guggenberger, T., Schweizer, A., & Urbach, N. (2020). Improving Interorganizational Information Sharing for Vendor Managed Inventory: Toward a Decentralized Information Hub Using Blockchain Technology. *IEEE Transactions on Engineering Management*, *67*(4), 1074–1085. https://doi.org/10.1109/TEM.2020.2978628

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The Limits of Trust-Free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy. *Electronic Commerce Research and Applications*, *29*(3), 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain Research, Practice and Policy: Applications, Benefits, Limitations, Emerging Research Themes and Research Agenda. *International Journal of Information Management*, *49*, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

Hughes, L., Dwivedi, Y. K., Rana, N. P., Williams, M. D., & Raghavan, V. (2020). Perspectives on the Future of Manufacturing Within the Industry 4.0 Era. *Production Planning & Control*, 1–21. https://doi.org/10.1080/09537287.2020.1810762

Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A Framework for Analysing Blockchain Technology Adoption: Integrating Institutional, Market and Technical Factors. *International Journal of Information Management*, *50*, 302–309. https://doi.org/10.1016/j.ijinfomgt.2019.08.012

Jarvinen, P. H. (2000). Research Questions Guiding Selection of an Appropriate Research Method. In *Proceedings of the 8th European Conference on Information Systems (ECIS)* (pp. 124–131). AIS.

Jenkins, A. M. (1985). Research Methodologies and MIS Research. *Research Methods in Information Systems*, *2*(1), 103-117.

Jian, J.-Y., Bisantz, A., & Drury, C. (2000). Foundations for an Empirically Determined Scale of Trust in Automated Systems. *International Journal of Cognitive Ergonomics*, *4*(1), 53–71. https://doi.org/10.1207/S15327566IJCE0401_04

Jøsang, A., Ismail, R., & Boyd, C. (2007). A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, *43*(2), 618–644. https://doi.org/10.1016/j.dss.2005.05.019

Kelton, K., Fleischmann, K. R., & Wallace, W. A. (2008). Trust in Digital Information. *Journal of the American Society for Information Science and Technology*, *59*(3), 363–374. https://doi.org/10.1002/asi.20722

Khiabani, H., Sidek, Z. M., & Manan, J.-L. A. (2010). Towards a Unified Trust Model in Pervasive Systems. In *Proceedings of the 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (pp. 831–835). IEEE. https://doi.org/10.1109/WAINA.2010.144.

Kikvidze, Z., & Moya-Laraño, J. (2008). Unexpected Failures of Recommended Tests in Basic Statistical Analyses of Ecological Data. *Web Ecology*, *8*(1), 67–73.

Lankton, N., McKnight, D. H., & Tripp, J. (2015). Technology, Humanness, and Trust: Rethinking Trust in Technology. *Journal of the Association for Information Systems*, *16*(10), 880–918. https://doi.org/10.17705/1jais.00411

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research Methods in Human Computer Interaction*. Morgan Kaufmann. https://doi.org/10.1017/cbo9780511814570

Lee, J. D., & See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors*, *46*(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392

Lippert, S. K., & Swiercz, M. P. (2005). Human Resource Information Systems and Technology Trust. *Journal of Information Science*, *31*(5), 340–353. https://doi.org/10.1177/0165551505055399

Liu, B. Q., & Goodhue, D. L. (2012). Two Worlds of Trust for Potential E-Commerce Users: Humans as Cognitive Misers. *Information Systems Research*, *23*(4), 1246–1262. https://doi.org/10.1287/isre.1120.0424

Locher, T., Obermeier, S., & Pignolet, Y.-A. (2018). When Can a Distributed Ledger Replace a Trusted Third Party? In *Proceedings of the 11th IEEE International Conference on Internet of Things* (pp. 1069–1077). IEEE. https://doi.org/10.1109/Cybermatics_2018.2018.00197

Lowry, P. B., Roberts, T. L., & Higbee, T. (2007). First Impressions with Websites: The Effect of the Familiarity and Credibility of Corporate Logos on Perceived Consumer Swift Trust of Websites. In *Proceedings of the 12th International Conference on Human-Computer Interaction: HCI Applications and Services* (pp. 77–85). Springer.

Lowry, P. B., Wilson, D. W., & Haig, W. L. (2014). A Picture Is Worth a Thousand Words: Source Credibility Theory Applied to Logo and Website Design for Heightened Credibility and Consumer Trust. *International Journal of Human-Computer Interaction*, *30*(1), 63–93. https://doi.org/10.1080/10447318.2013.839899

Lustig, C., & Nardi, B. (2015). Algorithmic Authority: The Case of Bitcoin. In *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)* (pp. 743–752). IEEE. https://doi.org/10.1109/HICSS.2015.95

MacKenzie, I. S. (2012). *Human-Computer Interaction: An Empirical Research Perspective*. Morgan Kaufmann.

Marella, V., Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the Creation of Trust in Cryptocurrencies: The Case of Bitcoin. *Electronic Markets*(30), 259–271. https://doi.org/10.1007/s12525-019-00392-5

Mathivathanan, D., Mathiyazhagan, K., Rana, N. P., Khorana, S., & Dwivedi, Y. K. (2021). Barriers to the Adoption of Blockchain Technology in Business Supply Chains: A Total Interpretive Structural Modelling (TISM) Approach. *International Journal of Production Research*, *59*(11), 1–22. https://doi.org/10.1080/00207543.2020.1868597

Mattke, J., Maier, C., Reis, L., & Weitzel, T. (2020). Bitcoin Investment: A Mixed Methods Study of Investment Motivations. *European Journal of Information Systems*, *30*(3), 1–25. https://doi.org/10.1080/0960085X.2020.1787109

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a Specific Technology. *ACM Transactions on Management Information Systems*, *2*(2), 1–25. https://doi.org/10.1145/1985347.1985353

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002a). Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. *Information Systems Research*, *13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002b). The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model. *The Journal of Strategic Information Systems*, *11*(3), 297–323. https://doi.org/10.1016/S0963-8687(02)00020-3

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Nass, C., Moon, Y., Fogg, B. J., Reeves, B., & Dryer, C. (1995). Can Computer Personalities Be Human Personalities? *International Journal of Human-Computer Studies*, *10*(2), 228–229. https://doi.org/10.1006/ijhc.1995.1042

Nickel, P. J. (2011). Ethics in E-Trust and E-Trustworthiness: The Case of Direct Computer-Patient Interfaces. *Ethics and Information Technology*, *13*(4), 355–363. https://doi.org/10.1007/s10676-011-9271-9

Nickel, P. J. (2013). Trust in Technological Systems. In M. J. de Vries, S. O. Hansson, & A. W. M. Meijers (Eds.), *Norms in Technology: Philosophy of Engineering and Technology* (Vol. 9, pp. 223–237). Springer. https://doi.org/10.1007/978-94-007-5243-6_14

Nickel, P. J. (2015). Design for the Value of Trust. In J. van den Hoven, P. E. Vermaas, & I. van de Poel (Eds.), *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains* (pp. 551–567). Springer. https://doi.org/10.1007/978-94-007-6970-0_21

O'Hara, K. (2012). Trust in Social Machines: The Challenges. In *Proceedings of the AISB/IACAP World Congress on Social Computing, Social Cognition, Social Networks and Multiagent Systems* (1-6). AISB/IACAP.

Oja, H. (2010). *Multivariate Nonparametric Methods with R: An Approach Based on Spatial Signs and Ranks*. Springer.

Ostern, N. (2018). Do You Trust a Trust-Free Technology? Toward a Trust Framework Model for Blockchain Technology. In *Proceedings of the 39th International Conference on Information Systems (ICIS)* (1- 17). AIS.

Palvia, P., Leary, D., Mao, E., Midha, V., Pinjani, P., & Salam, A. F. (2004). Research Methodologies in MIS: An Update. *The Communications of the Association for Information Systems*, *14*(1), 58. https://doi.org/10.17705/1CAIS.01424

Pavlou, P. (2004). Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research*, *15*(1), 37–60. https://doi.org/10.1287/isre.1040.0015

Pavlou, P., & Gefen, D. (2004). Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research*, *15*(1), 37–59. https://doi.org/10.1287/isre.1040.0015

Pournader, M., Shi, Y., Seuring, S., & Koh, S. L. (2020). Blockchain Applications in Supply Chains, Transport and Logistics: A Systematic Review of the Literature. *International Journal of Production Research*, *58*(7), 2063–2081. https://doi.org/10.1080/00207543.2019.1650976

Reeves, B., & Nass, C. (1996). *The Media Equation: How People Treat Computers, Television, and New Media Like Real People and Places*. Cambridge University Press.

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., & Urbach, N. (2019). Building a Blockchain Application That Complies with the EU General Data Protection Regulation. *MIS Quarterly Executive*, *18*(4), Article 7, 263–279. https://doi.org/10.17705/2msqe.00020

Sadler, G., Battiste, H., Ho, N., Hoffmann, L., Johnson, W., Shively, R., Lyons, J., & Smith, D. (2016). Effects of Transparency on Pilot Trust and Agreement in the Autonomous Constrained Flight Planner. In *Proceedings of the IEEE/AIAA Digital Avionics Systems Conference (DASC)* (pp. 1–9). IEEE. https://doi.org/10.1109/DASC.2016.7777998

Sas, C., & Khairuddin, I. (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. https://doi.org/10.1145/2838739.2838821

Sas, C., & Khairuddin, I. (2017). Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI)* (pp. 6499–6510). ACM. https://doi.org/10.1145/3025453.3025886

Schuetz, S., & Venkatesh, V. (2020). Blockchain, Adoption, and Financial Inclusion in India: Research Opportunities. *International Journal of Information Management*, *52*, 101936. https://doi.org/10.1016/j.ijinfomgt.2019.04.009

Söllner, M. (2015). Understanding Trust in Information Systems - the Impact of Trust in the System and in the Provider. In *Proceedings of the 75th Annual Meeting of the Academy of Management.* AOM. https://doi.org/10.5465/AMBPP.2015.10159abstract

Söllner, M., Hoffmann, A., & Hoffmann, H. (2012). Twenty Software Requirement Patterns to Specify Recommender Systems That Users Will Trust. In *Proceedings of the 20th European Conference on Information Systems (ECIS)* (1-13). AIS. https://doi.org/10.2139/ssrn.2484462

Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A., & Leimeister, J. (2012). Understanding the Formation of Trust in IT Artifacts. In *Proceedings of the 33rd International Conference on Information Systems (ICIS)* (1-18). AIS. https://doi.org/10.1007/978-3-319-05044-7__3

Thompson, C. G. (2017). Extracting the Variance Inflation Factor and Other Multicollinearity Diagnostics from Typical Regression Results. *Basic & Applied Social Psychology*, *39*(2), 81–91. https://doi.org/10.1080/01973533.2016.1277529

Upadhyay, N. (2020). Demystifying Blockchain: A Critical Analysis of Challenges, Applications and Opportunities. *International Journal of Information Management*, *54*(102120), 1–26. https://doi.org/10.1016/j.ijinfomgt.2020.102120

Valet, V. The World's Most Reputable Companies 2019. *Forbes*. https://www.forbes.com/sites/vickyvalet/2019/03/07/the-worlds-most-reputable-companies-2019/

Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture. *Journal of Management Information Systems*, *24*(4), 73–100. https://doi.org/10.2753/MIS0742-1222240403

Verberne, F. M. F., Ham, J., & Midden, C. J. H. (2012). Trust in Smart Systems: Sharing Driving Goals and Giving Information to Increase Trustworthiness and Acceptability of Smart Systems in Cars. *Human Factors*, *54*(5), 799–810. https://doi.org/10.1177/0018720812443825

Wallbach, S., Lehner, R., Roethke, K., Elbert, R., & Benlian, A. (2020). Trust-Building Effects of Blockchain Features–An Empirical Analysis of Immutability, Traceability and Anonymity. In *Proceedings of the 28th European Conference on Information Systems (ECIS).* AIS.

Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the Operations and Supply Chain Management: Benefits, Challenges and Future Research Opportunities. *International Journal of Information Management*, *52*(102064), 1–9. https://doi.org/10.1016/j.ijinfomgt.2019.102064

Wang, W., & Benbasat, I. (2007). Recommendation Agents for Electronic Commerce: Effects of Explanation Facilities on Trusting Beliefs. *Journal of Management Information Systems*, *23*(4), 217–246. https://doi.org/10.2753/MIS0742-1222230410

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted Business Process Monitoring and Execution Using Blockchain. In *Proceedings of the International Conference on Business Process Management (BPM)* (pp. 329–347). Springer. https://doi.org/10.1007/978-3-319-45348-4_19

Zavolokina, L., Zani, N., & Schwabe, G. (2019). Why Should I Trust a Blockchain Platform? Designing for Trust in the Digital Car Dossier. In *Proceedings of the 14th International Conference on Design Science Research in Information Systems and Technology* (pp. 269–283). Springer. https://doi.org/10.1007/978-3-030-19504-5_18

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In *Proceedings of the 2017 IEEE International Congress on Big Data* (pp. 557–564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85

9. Appendices

A. Participants Briefing

Scenario:

You are working in the purchasing department for Manufacturing Inc. Your job is to set up contracts for ordering supplies from Supplier Inc. necessary for production. In the past, conflicts with the supplier challenged Manufacturing Inc.'s productivity: Supplies weren't delivered on time or in full. It was impossible to track whether the details of the order have been communicated incorrectly to Supplier Inc. or whether Supplier Inc. did not meet the contract requirements. In order to prevent incidents as such in future, a new system has been set up between you and Supplier Inc: A blockchain which documents all contract details.

Blockchain:

A blockchain is a decentralized ledger – you can imagine it like a distributed database. It has the following characteristics:

- It serves as storage for all order details
- Any entry is immutable: Once added and accepted, it is practically impossible to change or delete
- The entries are transparent: They can be viewed by both parties
- The only parties involved in adding order contracts is you and Supplier Inc. No third party governs the network

The purpose of the blockchain is to establish an audit trail to be able to resolve disputes quickly.

Your task:

A customer has made an order. You are given the following overview of supplies needed:

ID Number	Product	Quantity	Price per item (in £ / piece)	Fulfillment date
10092	Wood	200 pieces	6	04 August 2019
17782	Screws	40 pieces	0.05	12 August 2019
19732	Paint	2 liters	8	16 August 2019
17293	Handles	4 pieces	4	17 August 2019

Your task is to add the supplies needed to the ledger. You can use today's date and your current location.

After completion, you will be asked to fill out a survey.

B. Pilot Study

Prior to the experiment, we conducted a pilot study to ensure that the first two signals achieve their intended manipulation. Participants rated the familiarity of a set of presented logos, which contained the five most reputable brands (Valet) offering blockchain-as-a-service (BAAS) and five start-ups offering BAAS. To prevent that negative brand reputation affects the level of trust during the experiment (Lowry et al., 2014), participants also rated the logos' credibility. IBM scored the highest on average while the start-up Devvio scored the lowest. Consequently, we included IBM's logo in the control condition and substituted it by Devvio's in the respective treatment group (see Figure 1 and Figure 2, respectively).

Furthermore, our pilot study also asked the participants to classify an informative text into "how" or "why" to ensure that we achieved the signal identified in Section 3. All participants of the pilot study classified the presented information as describing "how" the system works.

C. Questionnaire on Trustworthiness

Items Measuring the level of the artefact's trustworthiness adapted from Jian, Bisantz and Drury (2000):

1. The system is deceptive
2. The system behaves in an underhanded manner
3. I am suspicious of the system's intent, action or outputs
4. I am wary of the system
5. The system's actions will have a harmful or injurious outcome
6. I am confident in the system
7. The system provides security
8. The system has integrity
9. The system is dependable
10. The system is reliable
11. I can trust the system
12. I am familiar with the system

Demographic Questions:

1. What is your age?
2. Gender
3. Are you a Computer Science Student?
4. What is your highest educational degree?

D. Participant Demographics

Variable	*Control Gr.*	*Group 1*	*Group 2*	*Group 3*	*X (3)*	*p*
Total Participants	20	20	20	20		
					7.273	0.064
Gender Male	12	12	6	6		
Gender Female	8	8	14	14		
					2.264	0.894
20-25 years	14	14	14	15		
25-30 years	4	5	5	4		
30-35 years	2	1	1	0		
					26.057	**0.000**
Undergraduate Degree	1	0	0	9		
Postgraduate Degree	19	20	20	11		
					0.0	1.0
Computer Science Student	10	10	10	10		
Other Degree	10	10	10	10		

Table 5: Participant Demographics