Blockchain Technology as a Means for Brand Trust Repair – Empirical Evidence from a Digital Transgression

Martin Fleischmann
University of Southern California
mf_949@usc.edu

Bjoern S. Ivens
University of Bamberg
bjoern.ivens@uni-bamberg.de

Bhaskar Krishnamachari
University of Southern California
bkrishna@usc.edu

Abstract

Though much discussion in the realm of blockchain revolves around the concept of trust, research examining blockchain technology as a means for brand trust repair is still at an initial stage. This study conducts an experiment that analyzes blockchain technology as a substantive response to a data breach within a global business-to-consumer information systems application. Thereby, the present study expands trust repair theories to the context of blockchain and branding. Research results indicate that the use of blockchain technology as a reaction to a digital transgression may be able to reinstate brand trust, having a superior impact compared to an approach that uses a centrally managed information systems platform to restore brand trust. Overall, study results suggest that the use of blockchain technology can be an effective component of brand trust repair strategies in the digital space.

1. Introduction

Trust is touted to be one of the main benefits offered by blockchain technology [1] [2] [3], being identified as a likely key driver for user adoption of blockchain applications [4]. Though it may not yet fully live up to its promises [5], blockchain technology is attributed the potential to facilitate the generation of trust-free systems in which the underlying technology itself serves as a guarantee of trust [6] [7]. Therefore, blockchain technology may offer brands and businesses the possibility to enhance existing organizational information systems (IS) with a new, fortified level of trust [1].

Finding innovative, superior approaches to improving the trustworthiness of organizations is critical as numerous brands and companies are publicly under fire for transgressions [8]. Scandals within businesses can be witnessed worldwide, encompassing many industries such as media, manufacturing, or banking [9]. Many organizational transgressions occur with regard to digital IS platforms and applications, e.g. in the form of data breaches in which personal user data is compromised and data privacy is violated [10]. IS platforms and applications of global brands such as Equifax, Facebook or Marriott have fallen victim to attacks [11] [12] [13], resulting in the theft, exposure and processing of sensitive personal data from centralized storage systems without the consent of users [10]. As a result, trust in the companies and organizations managing the compromised platforms/ applications subsides [14]. Finally, digital platforms and applications are likely to suffer user defection after an organizational transgression such as a data breach occurs [14].

As a response to a transgression in the digital space, blockchain technology may be an auspicious solution to effectively address prevailing vulnerabilities of existing digital platforms/ applications. By adding an improved level of trust [1], the use of blockchain technology in afflicted IS platforms and applications may be a suitable response to the looming negative effects of digital scandals [15], potentially helping to reinstate trust in a brand or business. To date, however, there is a dearth of empirical evidence how users exposed to an organizational transgression in the digital space perceive the use of blockchain technology as a remedy. Consequently, it is crucial to understand if the implementation of a blockchain solution as a response to a digital transgression may be able to help reestablish trust in the affected brands, companies, organizations, platforms and applications, which may finally help to reduce the churn rate of users after a digital scandal.

Therefore, this research paper contributes to the existing body of literature by investigating whether blockchain technology is a means for brand trust repair, and to what extent blockchain technology can assist in reinstating brand trust of organizations, companies, platforms and applications affected by a scandal in the digital space. In this regard, the empirical investigation is driven by the following two research questions:

URI: https://hdl.handle.net/10125/64396
978-0-9981331-3-3

1. Can the use of blockchain technology repair brand trust that users have in a company/ organization/ platform/ application after a digital transgression occurs?
2. Following a digital transgression, how does the impact of a decentralized blockchain solution on brand trust compare to the more common approach that aims to reinstate trust via a centrally managed IS platform?

To answer these research questions, this study uses a critical incident that is based on a true, worldwide data breach within a globally operating digital business-to-consumer application. In a quantitative online experiment among affected users, brand trust is used to assess trust perceptions towards the afflicted application. The employed analysis extends existing theory around trust repair [8] [16] to the context of blockchain technology and branding.

With these objectives and the applied methodology in mind, the contribution of present research is threefold: First, this research creates new insights at the highly relevant intersection of blockchain technology and trust, complementing extant literature with an empirical research angle. Second, this study expands trust repair theories to the context of blockchain technology, analyzing the restoration of trust with regard to a technology that itself posits to stand for a system where trust concerns are non-existent. And third, this research complements the yet limited body of knowledge on trust repair in IS and marketing research [8] [17], generating a novel perspective on brand trust repair in the digital space.

2. Theoretical background

2.1. Trust and brand trust

Trust is a construct that has been studied from the most diverse angles by many disciplines, such as psychology, sociology, brand, and IS research. Rousseau and colleagues synthesize common understandings from these different fields. Taking their cross discipline angle, trust can be defined as a "psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" [18]. Though, the psychological state of trust may change over time and, hence, is of dynamic nature [18]. Trust plays a key role in interactions between two parties, serving as a promoter of social exchange if present, but representing a barrier within social interactions if absent [19]. In that regard, a party does not necessarily need to be of human nature, but can also represent e.g. an IS technology.

Overall, trust continues to constitute a contemporary, highly relevant matter of research. Also in the IS field, researchers have recognized the elevated importance of trust and called for investigating the concept of trust more in-depth [20] [21], especially when it comes to novel, yet scarcely researched IS contexts [22], such as blockchain technology. For purposes of present research, we unite the trust perspectives from extant IS literature that study trust-based relationships between people and organizations as well as between people and technology [21].

Trust at the brand level is attributed a high importance for long-term business success as it plays a critical role in establishing brand admiration, brand loyalty behaviors, and brand advocacy behaviors [23]. In line with the formulated definition of trust and based on the research of Delgado-Ballester and colleagues, brand trust can be characterized as "the confident expectations of the brand's reliability and intentions in situations entailing risk to the consumer" [24]. In this context, a brand represents a "value-generating entity (name) relevant to both customers and the brand owner" [23]. By being an entity, a brand may holistically stand for various services and products offered by a company as well as the organization behind it, especially if products, services and brand carry the same name. As brand trust is a decisive, long-term success factor for businesses that captures the trust perceptions users may have towards digital IS platforms and applications as well as towards the companies and organizations managing them in a holistic way, present research study focusses on trust at the brand level.

2.2. Trust repair theories

Trust repair describes the enhancement of a trustor's trust following a transgression in which the trustee is perceived as behaving in an untrustworthy manner [8] [16] [25]. In order to restore trust, a trustee can apply different trust repair strategies [8], whereby the nature of the transgression has a strong influence on how trust can be repaired [26]. Depending on industry and type of transgression, some strategies proved to reinstate trust better and in a different way than others [9] [16] [27].

Verbal response strategies, such as apology, denial, promise, or explanation [8], represent non-substantive responses that do not contain a tangible element and may often be perceived as 'cheap talk' by trustors [16]. Of these verbal responses, apologies have been investigated most frequently by extant literature, most likely because it is the most commonly used strategy in business practice [8] [10] [28].

Offering a more tangible response, substantive trust repair strategies involve some kind of action or change that is undertaken by the trustee [16]. Organizational

restructuring describes widely-used, substantive responses in which changes are made to how an organization operates. This can involve the introduction, adjustment or elimination of structures, systems, processes or policies within an organization [8]. With the aim to guarantee that the trustee will behave in a trustworthy manner in the future [16], the main goal of organizational restructuring is to convey to the trustee that preventive measures are put in place that preclude another transgression in the future [16].

Another substantive response that can often be found in business practice is penance, i.e. the voluntary offer of some kind of financial compensation or remedy to the trustor [9] [27]. Penance is used to send a signal of repentance that pursues to provide a credible proof that the trustee can be relied upon again in the future [16].

In summary, by employing one or various trust repair strategies as a response to a transgression, trustees are able to solve negative emotions a trustor may have, create more transparency and thereby more understanding of the transgression, generate assurance for the future, and generally shift the feelings of trustors into a more positive direction [8].

While the existing body of research around trust repair is generally vast, there is still limited research in some specific areas of IS and marketing literature. First, research on trust violations and especially trust repair in the IS field remains scarce [17]. In particular, a major gap can be identified for the areas of digital data privacy and data breaches [17]. The same is true for trust repair research in marketing where particularly research investigating the restoration of trust from the user/consumer perspective is still at an initial stage – hence, requiring more attention from scholars [8]. The present study analyzes brand trust repair in the digital space.

2.3. Blockchain technology and brand trust repair

The blockchain concept, in its generic form, describes a distributed ledger that is governed and maintained autonomously in the digital space without any central authority [29]. The term blockchain stands for a distributed database that is shared within a peer-to-peer network and comprises a sequence of interconnected blocks. These blocks contain cryptographically secured, immutable, and tamper-free information around transactions that is verified within the distributed network via a de-centralized consensus mechanism [30].

The creation of trust is claimed to be one of the most central benefits of blockchain technology [1] [2] [31]. Trust, moreover, is identified as one of the key drivers for user acceptance of blockchain applications [4]. In line with extant literature, user trust in blockchain technology can be defined as the belief that lets users "willingly rely and become vulnerable to businesses offering blockchain applications after having assessed the application's characteristics" [4]. Blockchain technology is attributed the ability to facilitate the design and construction of trust-free systems in the digital space [6]. In a trust-free setting, there is no need for trust concerns with regard to another party as the underlying blockchain technology securely guarantees that everyone plays by the rules [3] [6]. Therefore, blockchain technology is set to establish a new, yet unattained level of trust within IS platforms [1].

Though promising to create superior levels of trust, blockchain technology has yet to give proof of its trust generating capabilities and overcome its prevailing vulnerabilities [5]. Currently, some researchers still advocate that trust concerns may continue to exist in blockchain ecosystems [32]. In fact, there are several limitations that prevent blockchain technology from delivering on the trust promise [33], such as a lack of a guarantee that the data stored on a blockchain is reliable [34], the technological complexity that generates feelings of insecurity and distrust on the user side [35], or missing expertise with the blockchain topic [33]. Of these barriers to trust, blockchain expertise appears to be a critical aspect as a more profound knowledge of the topic would also reduce perceived complexity and, hence, ease distrust and insecurity with users. Consequently, trust perceptions of blockchain technology may likely get stronger among users as expertise with the technology increases.

Despite the weaknesses that still surface with regard to the concept of trust, yet nascent blockchain technology, if further developed and matured, may be able to strengthen the trust level of existing IS platforms and applications in the future [1].

Summarizing and considering the findings from extant research and theories, this research puts forward the following hypotheses:

Hypothesis 1. The use of blockchain technology as a substantive response to a data breach helps repair brand trust that an affected user puts in an IS application and the company managing it.

Hypothesis 2. Responding to a data breach with the implementation of a decentralized blockchain solution has a higher impact on brand trust repair than the more common deployment of a centrally managed IS solution.

Hypothesis 3. The level of expertise with the blockchain technology concept has a positive influence on the brand trust repair effect of a substantive response to a data breach that uses blockchain technology.

3. Research methodology

To answer the formulated research questions via a theory testing, deductive analysis approach, the present study conducts an experiment that is facilitated via a quantitative online survey [36] [37].

3.1. Sample and data collection

Data was collected via an online survey among college students at a major research university in the United States. A student sample was selected for three main reasons:

First, college students are the part of the population that most actively uses the internet and digital applications [17]. Hence, the employed student sample promises to yield a high overlap with the examined IS application's user base, especially when considering the age profile published for the users of the IS platform that is analyzed in this study. This makes students a relevant and important segment for the studied IS application and this research [38].

Second, college students have an advanced education and represent a demographic group that adopts technological innovations, such as smartphones or tablet PCs, earlier than other subgroups of the population [39]. This is also true for the adoption of cryptocurrencies as people with a high education, such as college students, are more likely to be cryptocurrency owners than individuals with a low education [40]. Consequently, a student sample is convenient to examine the formulated research questions and hypotheses of this study, especially when it comes to analyzing the role of blockchain expertise in the trust repair process (see hypothesis 3). As the student sample is likely to include a comparably high early adopter share of already available blockchain applications, such as cryptocurrencies, the blockchain expertise among students is also expected to be more advanced than in other demographic subgroups.

Third, the use of a student sample is well-suited for present study due to its homogeneity [38] which offers important advantages for the employed theory testing research strategy [41]. The sample comprises a set of homogenous individuals who promise to carry a combination of the most relevant characteristics relevant for this study, i.e. they most likely use the analyzed IS platform and may have at least some expertise with the blockchain topic. Thus, college students provide an ideal environment for a rigorous test of trust repair theories in the context of blockchain technology [41], facilitating theory application that involves all relevant aspects and excludes any extraneous factors that may potentially decrease validity of results. Hence, the homogenous sample adds rigor to the analysis and enhances the statistical validity of conclusions [41].

Students were invited to participate in the study via email or in-class learning management systems. The invitation included a link to the online survey that contained the experiment involving the critical incident. A short screener made sure that only currently enrolled students who were users of the affected, digital business-to-consumer application were allowed to participate in the study. The online survey (median length: 22 min) was conducted in April 2019 using the data collection software Qualtrics. The obtained sample included n=121 participating students. Table 1 visualizes the main demographic characteristics of the sample. Student respondents have a median age of 23 years. 60.3% are citizens of the United States. The sample, moreover, is characterized by an almost equal gender split. 41.3% of the respondents pursue undergraduate studies, 58.7% study at the graduate level.

Table 1. Demographic sample profile

	n	%
Gender		
Female	58	47.9%
Male	63	52.1%
Other	0	0.0%
Age		
23 years old or younger	68	56.2%
24 years old or older	53	43.8%
Nationality		
United States	73	60.3%
Other	48	39.7%
Level of studies		
Undergraduate	50	41.3%
Graduate	71	58.7%

3.2. Experimental setup

This study carries out an experiment that involves a true data breach within a well-known digital business-to-consumer application that operates on a global scale. More specifically, the critical incident comprises a transgression in which the IS application fell victim to a hacker attack and had sensitive personal user data illicitly harvested and commercialized without the consent of users. In this particular context, the affected application and the company managing it both carry the same name.

A true, real-world data breach was purposely selected for the present study with the goal to generate findings that are closely tied to empirical reality.

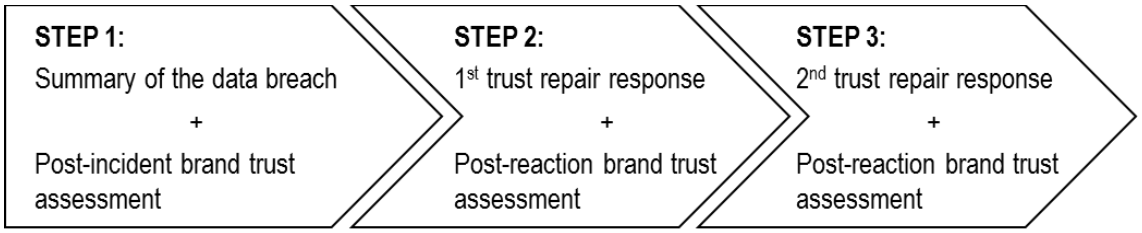

Figure 1. Three-step experimental process

Being close to business practice was deemed as more important for this study than assessing brand trust perceptions prior to the transgression, which would have required to design a purely fictional experiment. The use of an experiment, for purposes of this study, is commensurate with extant empirical trust repair research strategies [16] [17] [25].

In order to assess brand trust repair among users, the experiment was designed as a three-step process, visualized in figure 1: In step 1, participants were presented with a summary of the true data breach, followed by the first brand trust assessment: the post-incident measurement (PIM). Afterwards, step 2 and step 3 presented respondents with two different, fictional trust repair responses to the data breach, again complemented by a brand trust evaluation for each response: the post-reaction measurements. With the aim to avoid any response bias, the order of the two trust repair strategies was rotated in a way that each repair strategy was rated before the other by approximately half of the respondents.

The first trust repair response described a fictional trust repair strategy of the company managing the compromised IS application. This response was developed based on actual actions to a data breach that were taken in the past by other companies within the same industry.

In this reaction, the company first offered a non-substantive response in form of an apology and a promise [8] [10] [16], followed by a substantive response that outlined an organizational restructuring [8] [16]. The organizational restructuring proposed the introduction of an enhanced, centrally managed storage system for sensitive personal data within the company. This storage system would be kept within and administered by the company. Additionally, the company promised to enable users to control their data privacy configurations within the new system, facilitating an easy, transparent access to personal privacy settings. For purposes of this study, the brand trust assessment with regard to the first response is labeled as the post-reaction measurement based on actual actions (PRM-A).

Opposed to the response that is based on actual actions taken within the industry in similar data breaches, the second fictional trust repair strategy involved the use of blockchain technology. In this reaction, the non-substantive repair efforts were the same as in the response that is based on actual actions, hence including the same apology and promise.

With regard to the substantive repair strategy that involved organizational restructuring, major changes were implemented compared to the first response: instead of a centrally managed storage system within the company (central, internal data base), the second response introduced a decentralized blockchain system for storing sensitive personal data with users of the application (decentralized, distributed data base). Opposed to being maintained by the company (administration by the company), the underlying blockchain technology would automatically manage the data base in the second case (automatic administration by blockchain technology). And, instead of the company granting access to data privacy control settings (data privacy control provided by the company), the response using blockchain technology would allow users to decide collectively on the data privacy control configurations of the system, i.e. on how the application was able to use and share sensitive personal data (data privacy control determined by the user base).

With these characteristics, the substantive response in the second repair scenario encompasses some of the central benefits that extant literature attributes to blockchain technology: decentralization, automation, participation, and control [4] [30]. In this research study, the brand trust assessment with regard to the second response is described as the post-reaction measurement based on the use of blockchain (PRM-B).

Figure 2 provides a compact comparison of the different substantive responses used in the two brand trust repair strategies that are finally evaluated in PRM-A as well as PRM-B.

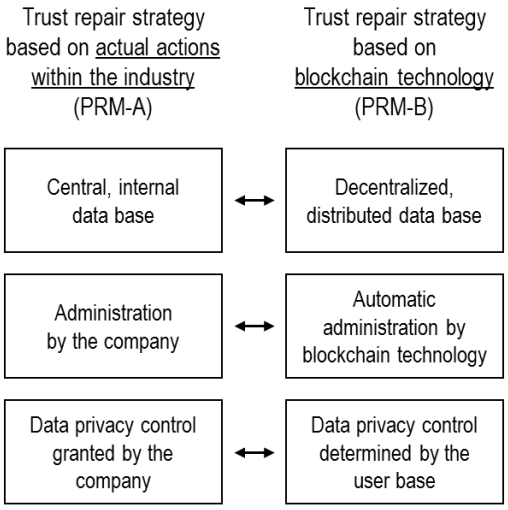

Figure 2. Trust repair strategies and their substantive responses

3.3. Measures

This study measured brand trust using the scale developed by Delgado-Ballester and colleagues [24] [42]. All brand trust items were assessed on a 7-point scale that ranged from 1 "very strongly disagree" to 7 "very strongly agree". The scale measuring blockchain expertise of respondents was derived from the work of Mishra and colleagues [43] and the work of Sichtmann and Diamantopoulos [44]. The items were measured on 7-point scales ranging from 1 "uninformed" to 7 "informed, 1 "know very little" to 7 "know very much", and 1 "unfamiliar" to 7 "familiar", depending on the item. Table 2 gives an overview of the employed items to measure brand trust and blockchain expertise.

Table 2. Items to measure brand trust and blockchain expertise

Brand trust
BT1: This brand meets my expectations
BT2: I feel confidence in this brand
BT3: This brand never disappoints me
BT4: This brand guarantees satisfaction
BT5: This brand would be honest and sincere in addressing my concerns
BT6: I could rely on this brand to solve any problem I have with the platform
BT7: This brand would make any effort to satisfy me
Blockchain expertise
BE1: How knowledgeable do you feel about blockchain?
BE2: How informed do you feel about blockchain?
BE3: How familiar are you with blockchain?

4. Analysis and results

In order to comprehensively test the formulated hypotheses, analyses were performed using the statistical analysis software SPSS (v.24). With regard to assessing whether and to what extent brand trust levels were different between PIM, PRM-A and PRM-B, a set of group comparing analyses [45], namely paired-samples t tests and Wilcoxon signed-rank tests, was performed.

The results of the paired-samples t-test show that brand trust improves significantly for PRM-B compared to PIM ($MEAN_{PRM\text{-}B}$ = 3.556; $MEAN_{PIM}$ = 3.069; t = 5.298; $p < 0.001$), while for PRM-A no significant change in brand trust can be observed in comparison to PIM ($MEAN_{PRM\text{-}A}$ = 3.143; $MEAN_{PIM}$ = 3.069; t = 1.235; $p > 0.05$). The same is true for the Wilcoxon signed-rank tests: brand trust enhances for PRM-B in comparison to PIM ($MEDIAN_{PRM\text{-}B}$ = 3.571; $MEDIAN_{PIM}$ = 3.000; Z = -5.146; $p < 0.001$), but not for PRM-A compared to PIM ($MEDIAN_{PRM\text{-}A}$ = 3.000; $MEDIAN_{PIM}$ = 3.000; Z = -1.028; $p > 0.05$). When comparing the brand trust levels attained after implementing the trust repair responses, PRM-B outperforms PRM-A, reaching a significantly higher brand trust level. This is evidenced by the results of the paired-samples t-test ($MEAN_{PRM\text{-}B}$ = 3.556; $MEAN_{PRM\text{-}A}$ = 3.143; t = 5.078; $p < 0.001$) as well as the Wilcoxon signed-rank test ($MEDIAN_{PRM\text{-}B}$ = 3.571; $MEDIAN_{PRM\text{-}A}$ = 3.000; Z = -4.687; $p < 0.001$). In summary, the results of the paired-samples t tests and Wilcoxon signed-rank tests, visualized in table 3, support both hypotheses 1 and 2.

Table 3. Results of paired-samples t tests and Wilcoxon signed-rank tests

Paired-samples t tests			
$MEAN_{PRM\text{-}B}$ =3.556	$MEAN_{PIM}$ =3.069	t = 5.298	$p < 0.001$
$MEAN_{PRM\text{-}A}$ =3.143	$MEAN_{PIM}$ =3.069	t = 1.235	$p > 0.05$
$MEAN_{PRM\text{-}B}$ =3.556	$MEAN_{PRM\text{-}A}$ =3.143	t = 5.078	$p < 0.001$
Wilcoxon signed-rank tests			
$MEDIAN_{PRM\text{-}B}$ =3.571	$MEDIAN_{PIM}$ =3.000	Z = -5.146	$p < 0.001$
$MEDIAN_{PRM\text{-}A}$ =3.000	$MEDIAN_{PIM}$ =3.000	Z = -1.028	$p > 0.05$
$MEDIAN_{PRM\text{-}B}$ =3.571	$MEDIAN_{PRM\text{-}A}$ =3.000	Z = -4.687	$p < 0.001$

In order to analyze whether the level of blockchain expertise has an influence on the trust repair effect of a substantive response, this study undertook a series of independent samples t tests [45]. For the analyses, the post-incident brand trust measurement (PIM), the brand trust assessment of the repair strategy involving the use of blockchain technology (PRM-B) as well as the difference in brand trust between PRM-B and PIM (DELTA) were designated as being the independent variables, the level of blockchain expertise served as the dependent variable.

For purposes of the independent samples t test, respondents with some level of blockchain expertise (ratings ≥ 2) were contrasted to participants with no expertise around blockchain technology (ratings < 2). Results of the performed analyses, visualized in table 4, show no significant differences in brand trust between the two groups for PRM-B ($MEAN_{PRM\text{-}B/some\ expertise} = 3.738$; $MEAN_{PRM\text{-}B/no\ expertise} = 3.331$; $t = 1.778$; $p > 0.05$), for PIM ($MEAN_{PIM/some\ expertise} = 3.107$; $MEAN_{PIM/no\ expertise} = 3.021$; $t = 0.384$; $p > 0.05$), as well as for DELTA ($MEAN_{DELTA/some\ expertise} = 0.631$; $MEAN_{DELTA/no\ expertise} = 0.310$; $t = 1.752$; $p > 0.05$). Thus, the results obtained in the independent samples t tests do not support hypothesis 3.

Table 4. Results of independent samples t tests

Independent samples t tests			
Some expertise	No expertise		
$MEAN_{PRM\text{-}B} = 3.738$	$MEAN_{PRM\text{-}B} = 3.331$	$t = 1.778$	$p > 0.05$
$MEAN_{PIM} = 3.107$	$MEAN_{PIM} = 3.021$	$t = 0.384$	$p > 0.05$
$MEAN_{DELTA} = 0.631$	$MEAN_{DELTA} = 0.310$	$t = 1.752$	$p > 0.05$

5. Discussion

Blockchain is a yet nascent, emerging technology that strives to add a new level of trust to IS applications and platforms. More specifically, blockchain technology may yield the potential to facilitate the generation of trust-free systems in which the underlying technology itself serves as a guarantee of trust to users. Therefore, the use of blockchain technology may also improve trust perceptions that users have towards brands, organizations and businesses. With this, the use of blockchain technology as a substantive response to a transgression in the digital space may offer brands and businesses the possibility to effectively address prevailing vulnerabilities of existing digital platforms and applications. This may finally help to repair trust after an occurred scandal and reduce churn among users. Therefore, the present study investigates whether and to what extent blockchain technology can be a means for brand trust repair, conducting an online experiment among affected users of a real-world business-to-consumer IS application struck by a true, major data breach.

The results of this research study provide clear answers to the formulated research questions.

1. Can the use of blockchain technology repair brand trust that users have in a company/ organization/ platform/ application after a digital transgression occurs? The obtained results indicate that blockchain technology as a substantive response to a data breach may be able to repair brand trust that an affected user puts in an IS application and the company managing it. These findings support hypothesis 1.

2. Following a digital transgression, how does the impact of a decentralized blockchain solution on brand trust compare to the more common approach that aims to reinstate trust via a centrally managed IS platform? The study results provide evidence that the implementation of a decentralized blockchain solution as a response to a data breach outperforms a response that is more commonly used in business practice and involves the deployment of a centrally managed IS solution. These findings provide support for hypothesis 2.

As the substantive, blockchain-based response focusses on the benefits of decentralization, automation, participation, and control [4] [30], the obtained results suggest that those aspects may in fact be enticing and important benefits to users and consumers. Hence, focusing on these four aspects when developing and designing a blockchain-based data privacy application may help practitioners to establish trust with users and may finally help to promote the application's technology acceptance among them.

Additionally, results suggest that the most commonly used substantive response to a data breach, i.e. the introduction of an enhanced, centrally managed storage system that is administered by the affected company and provides users data privacy control (granted by the company), has only limited impact on the restoration of trust. This outcome supports the assumption that it is crucial to find innovative, superior approaches to improving the trustworthiness of organizations that are hit by a transgression.

Another finding of this study is that the level of expertise that users have with the blockchain technology concept does not seem to influence the brand trust repair effect of a blockchain-based, substantive response to a data breach. Hence, the study findings do not support hypothesis 3. This result may be explained by the fact that blockchain is still a relatively new, yet nascent technology [1] that is far from being mainstreamed. With this, the general level of knowledge about blockchain technology is still relatively low. This is also true for this research study: the mean level of blockchain

expertise reaches a relatively low score of 2.52, the median level a score of 2.00 (on a 7-point scale where 1 stands for "no expertise" and 7 stands for "very high expertise"). As a result, this study found no support for hypothesis 3 by contrasting trust perceptions of respondents with some level of blockchain expertise (ratings ≥ 2) to participants with no expertise around blockchain technology (ratings < 2). Once blockchain technology matures and blockchain-based applications are used in a more widespread manner, the general level of expertise with the blockchain topic may become stronger. With this, differences in the respondents' levels of expertise may become more pronounced and noticeable. Thereby, the greater differentiation may facilitate a more granular and refined analysis of the relationship between blockchain expertise and the trust repair effect a substantive, blockchain-based response to a data breach. Therefore, blockchain expertise may unveil as a promoter of brand trust in the future as knowledge of and familiarity with the blockchain topic increase, resulting in more pronounced differences when it comes to the level of expertise with the blockchain topic.

6. Limitations and future research

While present research complements and enriches extant literature, it certainly is not without limitations. These identified limitations can serve scholars as fruitful avenues for future research:

First, this study performs an online experiment and investigates brand trust repair based on a true data breach within a global business-to-consumer IS application. With this, the research stays close to business practice and mirrors real-world reactions of businesses and users. Contrary to that, using a purely fictional transgression may offer some opportunities for future research. On one hand, a purely fictional scandal facilitates the pre-incident measurement of brand trust, serving as an additional point of comparison to unveil shifts in brand trust from before the incident all the way until the implementation of the brand trust repair strategy. The additional pre-incident measurement could lead to an even more comprehensive understanding of the use of blockchain technology as a response to a transgression in the digital space and its implications for brand trust.

On the other hand, a fictional transgression allows researchers to induce manipulations and reactions in an isolated way, facilitating the investigation of single aspects that a blockchain technology solution may offer to a brand trust repair strategy, such as control over personal data following a data breach. Despite being further away from business practice, an isolated view, as successfully performed in organizational literature [16] [28], could more specifically assess the role of different blockchain characteristics in the brand trust repair process. This could promote an even better understanding of the importance that aspects of blockchain technology, such as decentralization, automation, participation, and control have, when designing a substantive response to a data breach.

A second limitation of this research is the sample. Of course, the student sample offers important advantages for purposes of this study, such as the provision of a relatively homogenous sample that is deemed as being ideal for a deductive, theory testing research strategy. That said, the sample comprises a highly relevant user group for the examined IS application and yields all important characteristics needed to expand trust repair theories to the context of this study and to test the formulated hypotheses. With this, the choice of the sample adds rigor to the analyses and increases validity of results [41]. Nonetheless, opening up the research to a target group that better represents the demographics of the population may help to generate more generalizable insights. The findings outlined in this paper provide an ideal foundation to replicate the research study among a broader audience and, thereby, to create an even closer connection between the research setup and empirical reality.

Third, this study measures expertise with the blockchain topic based on how knowledgeable, familiar, and informed respondents feel to be with the topic. By complementing this measurement with contentual aspects such as personal experiences and perceptions or know-how with regard to specific use cases such as cryptocurrencies, the construct of blockchain expertise would get richer.

A richer, more differentiated conceptualization of blockchain expertise could offer the opportunity for an even deeper understanding of relationships between expertise and brand trust repair. Especially as blockchain applications and the use of blockchain technology in IS platforms are still nascent and far from being mainstreamed, infusing additional information on the blockchain expertise and experience of users may add value to future empirical research by allowing to induce more demographic and psychographic respondent data into the analytic process.

7. Conclusion

This research paper adds new empirical insights to the existing body of literature at the intersection of blockchain technology, trust, and branding. More specifically, the present study expands trust repair theories to the contexts of blockchain technology,

digital IS applications and branding – three areas in which research on this topic is yet scarce. The research study generates evidence that the deployment of blockchain technology in a substantial response to a digital transgression has the potential to restore brand trust that users put into an IS application and the organization managing it. Therefore, present research advocates that the use of blockchain technology appears to be an effective means of brand trust repair in the digital space.

8. References

[1] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain Technology in Business and Information Systems Research", Business & Information Systems Engineering 59(1), 2017, pp. 381–384.

[2] B. Notheisen, J. B. Cholewa, and A. P. Shanmugam, "Trading Real-World Assets on Blockchain", Business & Information Systems Engineering 59(1), 2017, pp. 425–440.

[3] P. Mehrwald, T. Treffers, M. Titze, and I. M. Welpe, "Application of Blockchain Technology in the Sharing Economy: A Model of Trust and Intermediation", in Proceedings of the 52nd Hawaii International Conference on System Sciences, Wailea, HI, USA, 2019, pp. 4585–4594.

[4] M. Fleischmann and B. Ivens, "Exploring the Role of Trust in Blockchain Adoption: An Inductive Approach", in Proceedings of the 52nd Hawaii International Conference on System Sciences, Wailea, HI, USA, 2019, pp. 6845–6854.

[5] M. Avital, R. Beck, J. L. King, M. Rossi, and R. Teigland, "Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future", in Proceedings of the 37th International Conference on Information Systems, Dublin, Ireland, 2016, pp. 1-6.

[6] R. Beck, J. Stenum Czepluch, N. Lollike, and S. Malone, "Blockchain - The Gateway to trust-free cryptographic transactions", Research Papers 153, 2016.

[7] L. Wang, X. Luo, Y. Hua, and J. Wang, "Exploring How Blockchain Impacts Loyalty Program Participation Behaviors: An Exploratory Case Study", in Proceedings of the 52nd Hawaii International Conference on System Sciences, Wailea, HI, USA, 2019, pp. 4565–4574.

[8] B. Bozic, "Consumer trust repair: A critical literature review", European Management Journal 35(4), 2017, pp. 538–547.

[9] N. Gillespie, G. Dietz, and S. Lockey, "Organizational Reintegration and Trust Repair after an Integrity Violation: A Case Study", Business Ethics Quarterly 24(3), 2014, pp. 371–410.

[10] L. Wan and C. Zhang, "Responses to trust repair after privacy breach incidents", Journal of Service Science Research 6(2), 2014, pp. 193–224.

[11] L. H. Newman, "The WIRED Guide to Data Breaches", 2018. [Online]. Available: https://www.wired.com/story/wired-guide-to-data-breaches. [Accessed 23 May 2019].

[12] J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection", Computer 51(8), 2018, pp. 56–59.

[13] N. Vemprela and G. Dietrich, "A Social Network Analysis (SNA) Study On Data Breach Concerns Over Social Media", in Proceedings of the 52nd Hawaii International Conference on System Sciences, Wailea, HI, USA, 2019, pp. 7186–7193.

[14] A. Malhotra and C. Kubowicz Malhotra, "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach", Journal of Service Research 14(1), 2011, pp. 44–59.

[15] B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS: A Blockchain-based Personal Data and Identity Management System", in Proceedings of the 52nd Hawaii International Conference on System Sciences, Wailea, HI, USA, 2019, pp. 6855–6864.

[16] K. T. Dirks, P. H. Kim, D. L. Ferrin, and C. D. Cooper, "Understanding the effects of substantive responses on trust following a transgression", Organizational Behavior and Human Decision Processes 114(2), 2011, pp. 87–103.

[17] G. Bansal and F. M. Zahedi, "Trust violation and repair: The information privacy perspective", Decision Support Systems 71, 2015, pp. 62–77.

[18] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not So Different After All: A Cross-Discipline View Of Trust", Academy of Management Review 23(3), 1998, pp. 393–404.

[19] D. Gefen and P. A. Pavlou, "The Boundaries of Trust and Risk", Information Systems Research 23(3), 2012, pp. 940–959.

[20] I. Benbasat, D. Gefen, and P.A. Pavlou, "Introduction to the Special Issue on Novel Perspectives on Trust in Information Systems", MIS Quarterly 34(2), 2010, pp. 367-371.

[21] M. Söllner, I. Benbasat, D. Gefen, J. M. Leimeister, and P. A. Pavlou, "Trust", in MIS Quarterly Research Curations, A. Bush and A. Rai, Eds., 2016, pp. 1-9.

[22] I. Benbasat, D. Gefen, and P. A. Pavlou, "Call for Papers: Special Issue on Novel Perspectives of Trust in Information Systems," MIS Quarterly 32(2), 2008, pp. 465-466.

[23] C. W. Park, D. J. MacInnis, and A. B. Eisingerich, Brand Admiration: Building A Business People Love, Wiley, Hoboken, NJ, USA, 2016.

[24] E. Delgado-Ballester, J. L. Munuera-Alemán, and M. J. Yagüe-Guillén, „Development and validation of a brand trust scale", International Journal of Market Research 45(1), 2003, pp. 35–54.

[25] P. H. Kim, C. D. Cooper, K. T. Dirks, and D. L. Ferrin, "Repairing trust with individuals vs. groups", Organizational Behavior and Human Decision Processes 120(1), 2013, pp. 1–14.

[26] R. J. Lewicki and C. Brinsfield, "Trust Repair", Annual Review of Organizational Psychology and Organizational Behavior 4(1), 2017, pp. 287–313.

[27] E. C. Tomlinson and R. C. Mayer, "The Role Of Causal Attribution Dimensions In Trust Repair", The Academy of Management Review 34(1), 2009, pp. 85–104.

[28] P. H. Kim, K. T. Dirks, C. D. Cooper, and D. L. Ferrin, "When more blame is better than less: The implications of internal vs. external attributions for the repair of trust after a competence- vs. integrity-based trust violation", Organizational Behavior and Human Decision Processes 99(1), 2006, pp. 49–65.

[29] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 27 January 2018].

[30] S. Seebacher and R. Schüritz, "Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review," in Exploring Services Science: 8th International Conference, IESS 2017, Rome, Italy, Proceedings, S. Za, M. Drăgoicea, and M. Cavallari, Eds. Springer International Publishing, Cham, Germany, 2017, pp. 12–23.

[31] M. Friedlmaier, A. Tumasjan, and I. M. Welpe, "Disrupting Industries with Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures", in Proceedings of the 52nd Hawaii International Conference on System Sciences, Waikoloa Village, HI, USA, 2018, pp. 3517-3526.

[32] A. Auinger and R. Riedl, "Blockchain and Trust: Refuting Some Widely-held Misconceptions", in Proceedings of the 39th International Conference on Information Systems, San Francisco, CA, USA, 2018, pp. 1-9.

[33] L. Zavolokina, N. Zani, and G. Schwabe, "Why Should I Trust a Blockchain Platform? Designing for Trust in the Digital Car Dossier", in Extending the Boundaries of Design Science Theory and Practice, DESRIST 2019, Lecture Notes in Computer Science 11491, B. Tulu, S. Djamasbi, G. Leroy, Eds. Springer International Publishing, Cham, Germany, 2019, pp. 269-283.

[34] V. L. Lemieux, "Trusting records: is Blockchain technology the answer?", Records Management Journal 26(2), 2016, pp. 110–139.

[35] N. Ostern, "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, San Francisco, CA, USA, 2018, pp. 1-17.

[36] J. Recker, Scientific research in information systems, Springer, Berlin, Germany, 2013.

[37] W. Creswell, Research design: Qualitative, quantitative, and mixed methods approaches, Sage, Los Angeles, CA, USA, 2014.

[38] B. Yoo, N. Donthu, and S. Lee, "An Examination of Selected Marketing Mix Elements and Brand Equity", Journal of the Academy of Marketing Science 28(2), 2000, pp. 195–211.

[39] S. Y. Lee, "Examining the factors that influence early adopters' smartphone adoption: The case of college students", Telematics and Informatics, 31(2), 2014, pp. 308-318.

[40] R. Jakubauskas. "How Many People Actually Own Cryptocurrency?", 2018. [Online]. Available: daliaresearch.com/how-many-people-actually-own-cryptocurrency. [Accessed 22 August 2019].

[41] B. J. Calder, L. W. Phillips, and A. M. Tybout, "Designing Research for Application", Journal of Consumer Research 8(2), 1981, pp. 197–207.

[42] E. Delgado-Ballester and J. L. Munuera-Alemán, "Does brand trust matter to brand equity?", Journal of Product & Brand Management 14(3), 2005, pp. 187–196.

[43] S. Mishra, U. N. Umesh, and D. E. Stem, "Antecedents of the Attraction Effect: An Information-Processing Approach", Journal of Marketing Research 30(3), 1993, pp. 331-349.

[44] C. Sichtmann and A. Diamantopoulos, "The impact of perceived brand globalness, brand origin image, and brand origin–extension fit on brand extension success", Journal of the Academy of Marketing Science 41(5), 2013, pp. 567–585.

[45] W. Mertens, A. Pugliese, and J. Recker, Quantitative Data Analysis: A Companion for Accounting and Information Systems Research, Springer International Publishing, Cham, Germany, 2017.