European Journal of Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tjis20

Becoming a blockchain user: understanding consumers' benefits realisation to use blockchain-based applications

Nirmalee Raddatz, Joshua Coyne, Philip Menard & Robert E Crossler

To cite this article: Nirmalee Raddatz, Joshua Coyne, Philip Menard & Robert E Crossler (2021): Becoming a blockchain user: understanding consumers' benefits realisation to use blockchain-based applications, European Journal of Information Systems, DOI: 10.1080/0960085X.2021.1944823

To link to this article: https://doi.org/10.1080/0960085X.2021.1944823

Published online: 08 Jul 2021.

EUROPEAN JOURNAL OF INFORMATION SYSTEMS
https://doi.org/10.1080/0960085X.2021.1944823

Becoming a blockchain user: understanding consumers' benefits realisation to use blockchain-based applications

Nirmalee Raddatz[a], Joshua Coyne[a], Philip Menard[b] and Robert E Crossler[c]

[a]University of Memphis, Crews School of Accountancy, Memphis, United States; [b]University of Texas at San Antonio, Department of Information Systems and Cyber Security, San Antonio, United States; [c]Washington State University, Management, Information Systems & Entrepreneurship Department, , Pullman, United States

ABSTRACT

Data breaches and cyber incidents are on the rise, and companies continually research new technologies to defend against attacks and protect customer data. The blockchain is a data store designed to promote data privacy, as well as transaction integrity. Enterprises in several industries, especially banking, have investigated the implementation of blockchain-based databases to replace centralised databases as one mechanism for protecting customers' data by separating transactional data from personally identifiable information. Despite the blockchain's privacy protections, consumers remain largely unaware of these benefits. Building on the Health Belief Model (HBM), we include privacy concerns and inertia as critical factors that influence consumers' perceptions of blockchain-based databases' benefits. Using a sample of 304 respondents, we test a theoretical model incorporating these factors. Our study results indicate threat severity, threat susceptibility, awareness, and inertia significantly influence the perceived benefits of blockchain, which has a significant positive influence on consumers' intention to switch to blockchain-based applications. Although consumers' comfort with the status quo of traditional banking mechanisms is a significant barrier to the realisation of blockchain banking applications benefits, additional awareness of consumer privacy protections can persuade customers to use the blockchain-based applications, especially if they exhibit heightened privacy concerns.

ARTICLE HISTORY
Received 20 August 2019
Accepted 9 June 2021

KEYWORDS
Blockchain; privacy concerns; perceived benefits; health belief model; inertia; banking

1. Introduction

The frequency of cyber incidents has risen dramatically in recent years. In 2014, a successful cyber-attack against JPMorgan Chase leaked the personal information of 83 million account holders (Weise, 2014). In 2017, an attack against Equifax leaked the personal information of over 140 million individuals (Yurieff, 2017). In 2018, the same group infiltrated both British Airways', TicketMaster UK's, and Newegg's payment systems and obtained the credit card numbers of as many as 50 million customers (Mihalcik & Zhou, 2018). These examples are only a few of the more dramatic breaches in recent history. Although the attack methods differ, what these cyber incidents have in common is that unauthorised entities accessed personal information. According to IBM, the average cost for each lost or stolen record containing sensitive and confidential personal information is 148, USD and the average cost of a data breach is 3.86 USD million.[1]

One key factor in enabling the leakage of personal information in a cyber-attack is that businesses obtain this personal information from their customers in the first place and then store it. It follows that if businesses did not store personal information, cyber-attacks that compromise personal information would be less successful. However, because businesses use this personal information to identify customers and conduct financial transactions, the decision to refrain from collecting and storing personal information would need to be accompanied by the adoption of data stores that enable organisations to conduct business without it. Businesses' use of consumer personal information and the consumer's disclosure (or privacy) decision provides an opportunity for an organisation to be the victim of a security attack.

Blockchain-based databases,[2] such as those that form the backbone for cryptocurrencies, are data stores that enable both customer identification and financial transactions without the use of personal information. The banking industry has significantly latched on to the idea that the blockchain will improve confidentiality. The Head of Global Innovation at BNY Mellon has stated that the banking sector will continue to face an increase in cyber-attacks and that distributed blockchain-based databases can protect against data theft better than centralised banking databases (FinTech Network, 2017). The blockchain co-lead at Rabobank has proposed a blockchain

CONTACT Nirmalee Raddatz nirmaleer@gmail.com

This article has been republished with minor changes. These changes do not impact the academic content of the article.

implementation that satisfies "Know Your Customer" (KYC) requirements without storing personal information (FinTech Network, 2017). According to Goldman Sachs, operational savings associated with KYC compliance will be anywhere from 160 USD million to 4 USD billion (FinTech Network, 2017).

Although banking *professionals* perceive benefits from blockchain adoption, it is unclear whether their *customers* experience the same perceptions. The purpose of this study is to investigate the forces that can influence banking customers to perceive benefits from having their banks replace their current traditional databases that store account holders' personal information with blockchain-based databases that would not. We are motivated to conduct this study by a desire to better understand how the consumer base perceives the benefits of the blockchain. We concentrate on the perception of benefits for two primary reasons. First, since most banking customers have not experienced a transition from traditional databases to blockchain-based databases, we cannot investigate realised behaviours. Instead, we take advantage of this gap between potential and realised technological innovation to inform the banking industry regarding the extent to which customers would recognise blockchain-based databases as providing them with value-added benefits. We believe that banks will incorporate benefits to customers in their cost-benefit analyses when weighing the decision to transition to blockchain-based databases. Second, consumer realisation of increased benefits can ultimately influence their intention to switch to a blockchain-based database. This intention is necessary to realise wider scale blockchain implementation once perceived benefits by banks and perceived benefits by customers align.

This study is especially timely as there is a lack of research that focuses on blockchain application, governance, and value creation (Yli-Huumo et al., 2016). Beck et al. (2018) propose an IT governance framework and research agenda for governance in the blockchain economy and maintain that future research involving blockchain needs to explore individual human behaviour and individuals' willingness to engage and transact on the blockchain. This study attempts to bridge this gap by understanding the factors that play a role in consumers' benefits realisation to use blockchain-based applications. By looking at consumers' perceptions, we can begin to identify whether consumers even care about the blockchain benefits that banking professionals promote. Through our investigation, we endeavour to see how these benefits will lead to future switching behaviour. Thus, the following research question drives our study.

RQ: What factors influence consumers' perceptions of the benefits of blockchain implementation by their banks that will lead to eventual switching to blockchain-based databases?

Our research question regarding the benefits of blockchain implementations is distinct from the research questions in recent, related literature investigating consumer perspectives on Bitcoin because of the differences in business use cases, risk factors, and potential benefits between blockchain usage, in general, and Bitcoin as a primary blockchain implementation. According to existing behavioural studies, consumer perceptions of Bitcoin as an investment or a means of payment are determined by profit expectancy (Glaser et al., 2014), loss aversion (Abramova & Böhme, 2016), awareness (Henry et al., 2018), status quo bias (Mattke et al., 2018), community sentiment (Mai et al., 2018), regret (Mattke, Maier, Reis et al., 2020) and whether cryptocurrency satisfies the definition of money (Mattke, Maier, Reis et al., 2020).

We build on prior literature and incorporate the relevant constructs from earlier behavioural studies into our model framework. Because blockchain technology is not specifically about money, we do not include constructs for whether cryptocurrency is money nor for investor profit expectancy or regret. Instead, we include constructs of perceived benefits of blockchain adoption and privacy risks associated with the use of traditional databases. To these, we add measures of loss aversion (as it pertains to the potential for personal information to be compromised), awareness, community sentiment, and status quo bias to view our research question through a comparable lens as has been used in prior studies. Despite these similarities, our study represents a novel contribution to the literature in two major ways. Our work examines the inherent differences between cryptocurrency and the blockchain that underlies it. Our study also addresses repeated declarations by authors of prior behavioural studies that behavioural findings regarding one cryptocurrency do not extend to others (Mattke, Maier, Reis et al., 2020, 2020).

We integrate the Health Belief Model (HBM), the Antecedents – Privacy Concerns – Outcomes Model (APCO), and inertia to develop a theoretical framework for explaining the factors that influence banking customers' benefit perceptions when their banks switch to blockchain-based databases. In exploring consumer perceptions of blockchain technology's benefits, we administer a scenario-based survey instrument to a general sample population of 304 bank account users. The study results indicate that

perceived threat severity, perceived threat susceptibility, awareness, and inertia significantly influence the perceived benefits of blockchain, which has a significant positive influence on a consumer's intention to switch to a blockchain-based application. Furthermore, privacy concerns have a significant influence on perceived threat severity and perceived threat susceptibility.

Our research has both theoretical and practical implications. We have developed a theoretical framework to better understand consumer concerns surrounding their existing banking systems. Our theoretical integration allows us to analyse these concerns in conjunction with consumer perceptions of blockchain systems as a means of exploring the factors that influence banking customers to perceive higher benefits of blockchain-based databases. Our findings contribute to the extant literature by indicating that threat is the focal point in the consumer decision-making process. Individuals' increased concerns about the privacy of their personal information lead to higher threat perceptions, which impacts their realised benefits and, ultimately, their intention to use blockchain.

We organise the rest of the paper as follows. The next section presents a brief review of the relevant literature. We then discuss the research model and develop the hypotheses to be tested. The subsequent section describes the sample, measures, and the data, followed by our discussion of the findings, their implications, and future research directions.

2. Theoretical development of research model

2.1. Adapting theory to the blockchain research context

Hong et al. (2014) contended that, through thoughtful contextualisation, IS research could be broadened to new contexts for establishing cross-context construct validity, thereby strengthening and improving theories adapted in the IS field. Further, they offered six specific guidelines on appropriately contextualising existing theory, which we followed in our study. We grounded our work in a general theory (guideline 1) by selecting HBM as our primary theoretical lens. HBM explains, from a healthcare perspective, why people engage in a risky behaviour despite the availability of a safer alternative. HBM theorises that for individuals to engage in healthy behaviour, they must (1) perceive that a threat is severe and probable, (2) be aware of healthier alternatives, and (3) recognise sufficient benefits of healthy behaviour (Rosenstock, 1974).

IS researchers have previously contextualised and refined HBM to information security adaptations (guideline 2), which aligns with our conceptual adaptation of HBM. Our examination of HBM, based on its foundational conceptualisation in healthcare, its established adaptations in information security research, and its applicability to the blockchain context, provided evidence that our contextualisation was valid in the blockchain domain. In our context, the "healthy" behaviour is adopting a blockchain-based database, which facilitates personal information protection and the promotion of data privacy.

Next, we examined the blockchain context to determine context-specific factors (see Appendix A for summary of prior work in IS), leading to our identification of privacy concerns and inertia as potentially meaningful factors (guideline 3). Because privacy protection is core to the design of blockchain-based databases, the APCO model provides a context for investigating the specific role that data privacy plays in the decision-making process (Smith et al., 2011). At the organisational level, banking consumers continuously face threats to their personal information, influencing their privacy concerns. Consequently, individuals may perceive the risks faced by the organisation as a potential risk to the disclosure of their personal information with third parties. Risk is "the possibility of loss" (Yates & Stone, 1992, p. 4), where a consumer who is concerned about the possible threats to their personal information in the hands of third parties will perceive increased risks to their information. As antecedents of HBM, perceived threat severity and perceived threat susceptibility capture an individual's perception of risk of the possibility of other entities' opportunistic acquisition and use of a consumer's personal information. Thus, we classify HBM's perceived severity and susceptibility constructs as components of privacy risk. Based on extant literature, we believe that the relationship between privacy concerns and perceived risk will also be significant when integrating HBM into the APCO framework.

Furthermore, according to HBM, an individual's likelihood of engaging in a specific behaviour is dependent on an evaluation of the perceived benefits and barriers associated with the behaviour along with cues from various sources (e.g., social media, news outlets and other websites, friends, TV, radio, and podcasts) that promote awareness. The longstanding prevalence of centralised banking represents the status quo in personal banking. The principle of inertia highlights the importance of considering the effect of status quo bias as a barrier to benefits realisation of any technology solution, regardless of current concerns or potential future benefits. In the context of this study, inertia provides a framework for investigating perceived barriers (i.e., negative aspects of a cause of action that instigate conflicting motives for the avoidance of the behaviour (Rosenstock, 1974)) proposed by HBM. An individual's refusal to change the status quo or inertia can explain a banking consumer's

unwillingness to realise the blockchain's benefits. Prior research has also identified inertia, or status quo bias, in consumer willingness to purchase cryptocurrency, which also relies on the blockchain (Mattke et al., 2018).

In our joint use of HBM, along with privacy concerns and inertia to measure hypothesised determinants of eventual behaviours, we recognise the perception of (net) benefits as the precursor of planned actions. Thus, we integrate constructs from HBM, APCO, and inertia to explore the motivations influencing individuals' perceptions of the blockchain's benefits. In the following subsections, we hypothesise how we model the relationships among our contextualised factors (guideline 4), including the incorporation of mediation to examine the interplay between these factors and the blockchain artefact (guideline 5). Finally, we also examine a post hoc model to test a theoretically based alternative to our hypothesised relationships (guideline 6).

It is important to note that our study explores consumers' perceptions of existing banking systems (centralised databases) and analyzes them in conjunction with their perceptions of blockchain systems (decentralised databases). Thus, our model's threat severity and threat susceptibility constructs relate to consumer security provided by non-blockchain-based (i.e., centralised) systems, and the privacy construct measures consumer privacy concerns, and awareness and perceived benefits pertain to a consumer's likelihood of action regarding blockchain-based systems. Inertia and intention involve perceptions related to switching from non-blockchain-based systems to the blockchain.

The integration of disparate research streams (i.e., HBM, APCO, and inertia) allows us to develop a more comprehensive theoretical framework in understanding banking consumer perceptions of using blockchain databases. The blockchain offers powerful advantages for data security and privacy (Yli-Huumo et al., 2016), but consumers may not recognise these benefits (Popper, 2017). When consumers exchange personal information with service providers, such as banks that use centralised databases, these service providers assume the responsibility for preserving the privacy of that personal information. This exchange eliminates consumers' ability to control the privacy of their personal information and exposes consumers to risks associated with cyber-attacks against the service provider's database. Unauthorised access to an individual's personal information can result in various unintended adverse consequences to an individual. Karwatzki et al. (2017) categorises these adverse consequences into seven factors: psychological, social, career-related, physical, resource-related, prosecution-related, and freedom-related. Blockchain-based databases rely on the principles of public-key cryptography. Public and private keys use anonymous identifiers and digital signatures to uniquely identify users and authenticate user transactions, removing consumers' need to share personal information with service providers. As a result, an individual concerned about security and privacy may be more inclined to prefer blockchain-based databases because they remove the need for the individual to reveal or share any personally identifying information.

anony trans

2.2. Application of the health belief model to blockchain benefits realisation

As an expectancy-value theory, HBM offers a socio-cognitive perspective of undertaking various protective behaviours (Lee, 2011). "Expectancy" can be defined as an individual's belief of their confidence in successfully completing a task, whereas "value" is the motivation to perform the task based on its perceived usefulness, importance, and enjoyment (Eccles, 1983). Regardless of whether it is related to healthcare or information, individuals face threats. Threats exist as external stimuli, regardless of whether individuals are cognisant of their existence. In some instances, individuals are confronted with threats through repeated prompting by cues from internal or external sources, which in turn lead them to engage in behaviours to protect themselves (Rosenstock, 1974).

The HBM was initially developed to explain individuals' health-related behaviours while attempting to predict their engagement in specific preventive measures (Rosenstock, 1974). The HBM postulates that the intention to engage in various kinds of health behaviours may be dependent on an individual's perceptions of the inherent risk of the disease and the benefits of and their capacity to engage in an appropriate responsive behaviour to mitigate the threat. Consequently, the behavioural intention is, in turn, dependent on two key determinants: "(1) the value placed by an individual on a particular goal; and (2) the individual's estimate of the likelihood that a given action will achieve that goal" (Janz & Becker, 1984, p. 2).

Before engaging in a specific behavioural response in preventing disease, individuals follow a rational thought process (Rosenstock, 1974). First, individuals form beliefs regarding their susceptibility to disease. Then, they predict the impact of the occurrence of the disease on their lives. Finally, they evaluate the chosen response's effectiveness in mitigating or preventing the condition while assessing the potential benefits of the chosen response. Since its inception, HBM has been used successfully in addressing preventive behaviours such as seat belt use, health screenings, medical

compliance, and the use of vaccinations (Janz & Becker, 1984).

In the fields of healthcare and information security, "parallels can be drawn between preventive healthcare behavior (such as observing a healthy diet to avoid heart diseases) and information protective behaviors (such as using a strong password to prevent unauthorized use of one's account) " (Ng et al., 2009, p. 817). A disease adversely affects the body; likewise, a cyber-attack adversely affects the information system and its data. Ultimately, the success of healthcare countermeasures depends on the prevention of a disease, whereas the success of security countermeasures depends on the non-occurrence of threats to organisational information (Ng et al., 2009). In our study, at the organisational level, individuals face risks to their personal information because of security threats against the organisation. Assessing these organisational threats and how banks secure personal information determines whether individuals will make an information disclosure decision consistent with their desire for information privacy.

Table 1 highlights within our study's context some similarities that exist between behaviours undertaken by individuals in protecting their health and those behaviours involved in protecting their digital information. In the context of this study, the preventive behaviour is to utilise a blockchain-based database for banking transactions to protect personal information. The core HBM assumptions can be explained in terms of an individual's perceptions of a threat (i.e., perceived severity and perceived susceptibility), perceptions of the solution (i.e., perceived benefits), and modifying factors related to those perceptions (i.e., awareness).

Table 1. Mapping of core assumptions of the HBM to information privacy related behaviour (National Cancer Institute, 2005).

An individual will engage in a health-related behaviour (i.e., use sunscreen), if that individual	An individual will engage in an information privacy related behaviour (i. e., adopt a blockchain-based database) if that individual
1. feels the disease (i.e., skin cancer) can be prevented.	1. feels the privacy risk (i.e., a threat to their personal information) can be prevented.
2. has a positive expectation that engaging in the recommended behaviour will avoid negative outcomes associated with the disease (i.e., using sunscreen will prevent skin cancer).	2. has a positive expectation that engaging in the recommended behaviour will avoid negative outcomes associated with the privacy risk (i.e., using a blockchain-based database will prevent unauthorised access to personal information).
3. can successfully engage in the recommended behaviour (i.e., use sunscreen).	3. can successfully engage in the recommended behaviour (i.e., use a blockchain-based database).

2.3. Perceived benefits of blockchain-based databases

According to the HBM, an individual will evaluate the availability and effectiveness of potential benefits among the various alternatives in preventing a particular disease. Within the underlying premise of this expectancy-value theory, individuals tend to prefer behaviours with favourable outcomes while eliminating behaviours with unfavourable outcomes. Thus, the actions an individual takes to mitigate a threat depend on the benefits achieved by undertaking those actions. During the rational decision-making process, individuals will conduct a cost-benefit analysis before choosing a particular course of action (Paternoster & Pogarsky, 2009). These individuals are more likely to choose outcomes with higher net benefits than alternatives with lower net benefits.

Similarly, several studies in information systems literature have highlighted the importance of the perception of countermeasures' benefits in encouraging information-protecting behaviours desirable to the organisation (e.g., Bulgurcu et al., 2010; Hu et al., 2012; Ng et al., 2009; Warkentin et al., 2017). The final chosen action depends on a belief in the effectiveness of the solution in mitigating the threat.

In our study context, we draw upon the numerous benefits offered by blockchain technology as an effective solution in protecting consumers' personal information stored by third parties. Essentially, the blockchain can be considered a more secure system than other record-keeping systems based on centralised database platforms. Additionally, blockchain provides a wealth of other benefits such as information privacy, transaction traceability, avoidance of intermediaries, and reduction of transaction costs to customers (Marr, 2017). In this study context, the perceived benefit of blockchain-based databases is the protection of personal information from a cyber-attack through an inherent separation of transactional data and personal information. Thus, the consumers' realisation of the benefits of blockchain technology will result in their development of favourable attitudes towards the technology. As a result, we investigate the forces within the HBM framework that influence customers' perception of the benefits of blockchain-based databases.

2.3.1. Effect of perceived benefits of blockchain-based databases on behavioural intention to switch to blockchain-based databases

Because the HBM includes individuals' consideration of benefits as an antecedent to the performance of protective behaviours, the HBM inherently assumes that individuals are cognitively rationalising whether to perform the behaviour, rather than relying on

automatic processes such as habituated maladaptive behaviours. As a component of the rational cognitive process, an increase in the perceived benefits of following a particular course of action would increase an individual's likelihood of selecting that course of action as the best alternative (Willison & Backhouse, 2006). Relating this process to an information privacy context, if an individual has an elevated perception of the benefits associated with protecting personal information, the individual should be more likely to form intentions to perform actions that maintain information privacy (Warkentin et al., 2017). A blockchain-based database provides privacy protection as a critical element of its functionality. If an individual rationalises that a blockchain-based database is beneficial due to its privacy protection mechanisms, the individual would be more likely to intend to switch from using centralised banking to blockchain-based banking when given the option. Although many researchers have called for an increased operationalising of actual behaviour as the dependent variable of behavioural studies, there are instances where measuring intention is appropriate (Ajzen et al., 2009). Because most banks have not adopted blockchain-based systems and have not given their customers the option to switch, actual behavioural data is not available at this time. Thus, understanding consumer intentions is of increased importance for centralised banks to better understand the various factors that may persuade their customers to opt into a blockchain system. Hence,

H1: Perceived benefits of blockchain-based databases are positively associated with behavioural intention to switch to blockchain-based databases.

2.3.2. Effect of perceived threat severity of storing information in a centralised database on perceived benefits of blockchain-based databases

Perceived severity refers to an individual's perception of the seriousness or magnitude of a threat, an illness, or condition (Rosenstock, 1974). An individual will evaluate the severity of a particular threat through the emotions evoked by the thought of experiencing the particular condition or the perceived adversities created by the condition (Boss et al., 2015; Menard et al., 2017). When individuals perceive the particular condition to be severe, they are more likely to conclude that a proffered solution may mitigate the risk of developing the condition (Summers & Marett, 2016).

Like threats to health, threats to information motivate individuals to engage in a protective behaviour through invoking fear within the individual. Individuals are more likely to perceive the benefits of security-related behaviours to protect their information when they perceive a higher threat to their informational assets when they perceive the loss from unauthorised access to their personal information to be severe (Boss et al., 2015; Menard et al., 2017). In this study context, individuals should consider a higher degree of threats from unauthorised access to their personal information stored in a bank's centralised database. In contrast, blockchain-based databases allow users to store personal information exclusively on their own devices, separate from other transactional data (McKinsey & Company, 2016). The ability to divorce the storage of (anonymised) banking transactions from the storage of private personal information reduces the likelihood of a customer's exposure to cyber-attacks against banking databases. Consequently, customers who consider severe threats to their personal information stored by third parties (i.e., banks) are more likely to prefer blockchain-based databases. Thus, we predict that a consumer's perception of threats to their personal information and the privacy-preserving mechanisms inherent in blockchain technology will increase the consumer's realisation of the personal benefits associated with blockchain-based databases. Hence,

H2: Perceived threat severity of unauthorised access to personal information stored in centralised databases is positively associated with perceived benefits of blockchain-based databases.

2.3.3. Effect of perceived threat susceptibility of storing information in a centralised database on perceived benefits of blockchain-based databases

Perceived susceptibility is an individual's belief in the likelihood of experiencing a particular condition (Janz & Becker, 1984). An individual will evaluate the susceptibility of a particular threat through the emotions evoked by the thought of experiencing the particular condition or the perceived adversities created by the condition (Boss et al., 2015; Menard et al., 2017). According to the HBM, when individuals believe that they are susceptible to a particular condition or disease, they are more likely to adopt a behavioural response to mitigate the risk of developing the condition (Summers & Marett, 2016).

Individuals are more likely to perceive the benefits of protecting their information when they consider themselves more susceptible to a cyber-incident (Boss et al., 2015; Menard et al., 2017). Blockchain technology can help organisations enhance their cyber-defences by preventing unauthorised access to consumer information through consensus mechanisms, data encryption, transparency, immutability, and the ability to detect data tampering. The distributed nature of blockchain technology eliminates a central point of failure, thus providing more safeguards and privacy benefits than the present centralised database-driven transactional structures used by banks and other third parties (Infosecurity, 2018).

Thus, we predict that when individuals perceive that their personal information is susceptible to cyber attacks in the hands of third parties that use conventional systems, they are more likely to perceive greater benefits of blockchain-based databases. Hence,

H3: Perceived threat susceptibility of unauthorised access to personal information stored in centralised databases is positively associated with perceived benefits of blockchain-based databases.

2.3.4. Effect of awareness on perceived benefits of blockchain-based databases

Perceptions of threats and benefits alone are insufficient to prompt appropriate action without an "instigating event [that] occurred to set the process in motion" (Rosenstock, 1974, p. 101). Cues, which increase an individual's awareness of either a threat or a solution, provide such an instigating event. Within the context of the HBM, individuals do not achieve awareness through a general knowledge of the existence of the problem or solution, but rather through contemporaneous or repeated prompting by cues from internal (e.g., pain caused by a disease) or external (e.g., reminders for doctor's office visits or reminders to take medication) sources (Janz & Becker, 1984). Cues can promote awareness of the benefits of a particular solution, thus, changing the perceptions of an individual's ability to take appropriate action. For example, during the H1N1 flu outbreak in 2009, the Indiana State Department of Health (ISDH) successfully launched an aggressive vaccination campaign through radio and television that emphasised the benefits of vaccination as a means of increasing people's perceptions of their own ability to get vaccinated (Jones, et al., 2015).

In the context of information systems, studies have found a significant impact of awareness on engaging in information privacy-preserving behaviours, as well as cryptocurrency transactions (e.g., Henry et al., 2018; Mai et al., 2018; Ng et al., 2009). External cues that create awareness of blockchain technology come from social media, news outlets, and other websites, friends, TV, radio, and podcasts. References to blockchain technology by these outlets can prompt awareness of the added privacy benefits of this storage solution, thus increasing the consumers' confidence in transacting online through blockchain-based platforms. Consequently, its inherent positive aspects can increase the mainstream implementation of blockchain that has revolutionised many business sectors. Hence,

H4: Awareness is positively associated with perceived benefits of blockchain-based databases.

2.4. Application of the antecedents – privacy concerns – outcomes model to benefits realisation of blockchain-based databases

In their quest to define and understand privacy, researchers have attempted to combine various perspectives of the concept from numerous fields. As a result, over the years, several definitions of the privacy concept have emerged. Westin (1967) defines privacy as a "voluntary and temporary withdrawal of a person from the general society" (p. 7). In the context of information, Clark et al. (2009) define privacy as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves." Both definitions indicate that privacy involves the desire to remove access to one's own self or one's data from the larger population. In reviewing the role that privacy concerns play on individual behaviours, Smith et al. (2011) developed the APCO model. The initial APCO model was then extended with the enhanced APCO Model (Dinev et al., 2015). The enhanced APCO model posits that awareness influences privacy concerns and that privacy concerns, in turn, influence perceptions or threat risks and solution benefits (Dinev et al., 2015).

2.4.1. Effect of awareness on privacy concerns

Multiple studies have confirmed the relation between awareness and privacy concerns (e.g., Dinev et al., 2015; Smith et al., 2011). Blockchain awareness can increase individuals' perceptions of blockchain technology's added privacy benefits. However, it can also inform them about privacy-related risks associated with conventional systems based on centralised database-driven transactional structures used by most banks and other third parties. The more aware individuals become of the privacy-related risks associated with current behaviours, the more their privacy concerns increase (Sheehan & Hoy, 2000). Prior research in information privacy has demonstrated that awareness affects privacy concerns related to social media usage (Zlatolas et al., 2015) and mobile devices (Gerber et al., 2018). Zlatolas et al. (2015) surveyed Facebook users and discovered that increased awareness of privacy implications increased privacy concerns and, in turn, decreased self-disclosure behaviour. Gerber et al. (2018) used gamification to study privacy concerns by developing a mobile game that educated users on various privacy issues. They found that after playing the privacy game, users possessed significantly more knowledge and awareness; these users subsequently exhibited greater concerns and enacted behaviours to protect their privacy. Therefore, in our study, we expect blockchain awareness to increase individuals' privacy concerns over storing their information in centralised databases. Hence,

H5: Awareness is positively associated with privacy concerns over unauthorised access to personal information stored in centralised databases.

2.4.2. Effects of privacy concerns on perceived threats of storing information in a centralised database

The APCO Model also posits that privacy concerns lead to perceptions of risks (Dinev et al., 2015). According to the information security literature, privacy concerns positively determine perceived privacy risks related to sharing personal information (Bélanger et al., 2002; Dinev & Hart, 2006; Li et al., 2010) and location-based information (Keith et al., 2013). Studies have mainly found these results in the context of online transactions via e-business platforms where an individual will consider the positive and negative utility of disclosing personal information with third-party vendors before the information disclosure. When there is a negative utility (i.e., high risk or threat of possible misuse of personal information by the vendor) coupled with privacy concerns, individuals are less likely to disclose their personal information with third-party vendors (Bélanger et al., 2002; Dinev et al., 2015; Eastlick et al., 2006; Pavlou et al., 2007; Van Slyke et al., 2006). Based on prior work, we believe that the relationship between privacy concerns and perceived risk will also be significant when integrating HBM into the APCO framework. According to Smith et al. (2011), "an individual's calculation of risk involves an assessment of the likelihood of negative consequences as well as the perceived severity of those consequences" (p. 1001). Thus, we identify HBM's perceived severity and susceptibility constructs as components of privacy risk.

When consumers perceive increased concerns over their information's privacy, their perceptions of the seriousness or magnitude of the perceived adversities created by the condition tend to increase. Thus, in the context of this study, when individuals are concerned about storing personal information on centralised databases maintained by third parties such as banks, these concerns result in heightened perceptions of threat severity. Combining assumptions and elements from HBM and APCO, we predict that individuals with privacy concerns over storing personal information in centralised databases have stronger perceptions of the severity of unauthorised access to their personal information. Hence,

H6: Privacy concerns of unauthorised access to personal information are positively associated with perceived severity of unauthorised access to personal information stored in centralised databases.

Extant literature indicates that privacy concerns are a primary reason that discourages individuals from conducting online transactions and surrendering personal information to third parties (Dinev & Hart, 2006). The reluctance to share personal information can result from the individuals feeling susceptible to the possibility of unauthorised entities accessing their personal information in the hands of third parties. Thus, we predict that individuals with privacy concerns over storing personal information in centralised databases have stronger perceptions of the susceptibility of unauthorised access to their personal information. Hence,

H7: Privacy concerns of unauthorised access to personal information are positively associated with perceived susceptibility of unauthorised access to personal information stored in centralised databases.

2.4.3. Effects of privacy concerns on perceived benefits of using blockchain-based databases

According to the view of libertarian political scientists, privacy is subject to the economic principle of cost-benefit analysis where an individual will engage in a self-surveillance (i.e., sharing information online willingly) process (Smith et al., 2011). Hence, the consumer will perceive privacy as a right or a commodity they can exchange as a means of receiving benefits (Campbell & Carlson, 2002; Smith et al., 2011). Furthermore, according to the APCO model, an individual will consider the potential benefits received by disclosing information in conjunction with the risks. Thus, when the potential benefits of disclosure are higher than the costs, individuals are more likely to share their information with a third-party vendor. In the context of our study, consumers perceive higher net benefits from vendors using blockchain-based databases compared to centralised databases for data storage. When individuals exchange personal information with service providers such as banks that use centralised databases, these service providers are responsible for keeping the individual's personal information private. However, compared to blockchain-based databases, centralised databases inherently pose more risks towards information privacy. Since keeping this information private and secure is solely dependent on the service provider, the information stored in these centralised databases is subject to a single point of failure. The housing of information in a single location further eliminates individuals' ability to control their data privacy or decide on how the data is used and shared among third parties (Marr, 2017). As a result, unauthorised access to personal information stored by third-party service providers is sometimes unreported to the data owners or undetected by the service provider.

With cryptography, hashing, and smart contracts, blockchain can keep individual information private by enabling anonymity. Blockchain technology also can transact with non-blockchain-based platforms

through a reference hash to the specific transaction. This feature results in a blockchain database being able to conduct a transaction off the blockchain without releasing an individual's private information to third parties while maintaining anonymity and confidentially of information (Nakamoto, 2008). Consumers who exhibit elevated concerns towards their information privacy will be cognisant of the inherent risks to their personal information in the hands of third parties and gravitate towards solutions that alleviate their concerns. These individuals will likely recognise the benefits that blockchain-based databases provide regarding increased privacy protection. Hence,

H8: Privacy concerns of unauthorised access to personal information are positively associated with the perceived benefits of using blockchain-based databases.

2.5. Inertia in switching to blockchain-based databases

Inertia, defined as an entity's resistance to change, has been investigated in various behavioural (Polites & Karahanna, 2012), social (Keen, 1981), cultural (Zárate et al., 2012), organisational (Rumelt, 1995) and individual contexts (Bawa, 1990; Chen & Hitt, 2002; Greenfield, 2005; Kim, 2009; Kim & Kankanhalli, 2009). While social, cultural, and organisational inertia are mainly associated with resistance to change in groups and societies, individual inertia is based on the "attachment to, and persistence of, existing behavioral patterns (i.e., the status quo)" at the individual level (Polites & Karahanna, 2012, p. 24). Samuelson and Zeckhauser (1988) identify status quo bias as a contributor to individuals' preference for their current situation. According to Polites and Karahanna (2012):

> [I]nertia reflects unwillingness to abandon the status quo irrespective of present alternatives or alternatives that may potentially become available in the future. However, inertia is perhaps most easily recognized when present alternatives are ignored or incentives fail. (p. 24)

Research shows that, in such situations, individuals prefer the *status quo ante* or the "way things were before", over the potential benefits of new alternatives (Samuelson & Zeckhauser, 1988). Research has identified multiple potential causes for status quo maintenance, such as (1) an individual's more frequent encounters with the current state, (2) longevity or a length existence of the current state, (3) cognitive limitations, and (4) informational limitations of decision outcomes.

Extant information systems literature includes research into inertia and status quo bias concerning switching costs and brand loyalty in Internet-enabled businesses (Chen & Hitt, 2002), online customer retention based on customers' resistance to change (Gupta et al., 2007), user resistance before new system implementation (Hirschheim & Newman, 1988; Kim & Kankanhalli, 2009), user acceptance of a new system (Polites & Karahanna, 2012), user resistance to information security policy changes (Malimage et al., 2019) and individual decisions and behaviours related to technology adoption (Lending & Straub, 1997). Kim and Kankanhalli (2009) use the principles of status quo bias and technology acceptance to develop a model to explain user resistance to new enterprise system implementation. They find that switching costs significantly increase user resistance, while perceived value and organisational support diminish user resistance. Crossler and Posey (2017) find that inertia is a significant factor in influencing consumer preference for new security-enhancing technology. Polites and Karahanna (2012) investigate the impact of an individual's incumbent system usage behaviour on using a newly implemented system. Their results reveal several factors that drive an individual's resistance to a new system, such as habitual use of the old system, psychological commitment related to sunk costs, and rationalisation related to transition costs.

Prior research in inertia may be associated with the blockchain context, either through direct studies of inertia in the blockchain context (Chong et al., 2019; Vial, 2019) or examinations of inertia in explaining the adoption of similarly disruptive technologies (Baiyere et al., 2020; Carlo et al., 2014; Treiblmaier & Strebinger, 2008; Walther et al., 2018). Chong et al. (2019) reported observing organisational inertia in their case study of blockchain-inspired business models. In his review of digital transformation research, Vial (2019) specifically included blockchain research and identified inertia as an ongoing barrier to acceptance for blockchain technologies and other technologies. Like many prior disruptive technologies, inertia may provide a similar barrier to blockchain-based systems' widespread adoption.

When individuals believe that it might be too cumbersome to switch to a blockchain-based database, they will continue to prefer the current centralised database of their service provider. The use of a blockchain-based database can require end-users to store their personal information on their own devices instead of having a service provider store this information. This personal storage results in a transfer of responsibility to the individual in keeping personal information secure. The added responsibility may reduce the perception of benefits associated with blockchain-based databases. Polites and Karahanna (2012) identify this as affective-based inertia, one of the three components of inertia along with behavioural-based and cognitive-based. In the presence of

behavioural-based inertia, an individual will remain in the existing state because this is what the individual has always done, and because the individual has developed a familiarity with the behaviour. In the presence of cognitive-based inertia, an individual will simply remain in the existing state despite the presence of a better alternative. We predict end-users may prefer to have their personal information stored in the centralised databases of their service providers (1) because of an aversion to accepting responsibility for keeping personal information private, (2) because of the preference to maintain the status quo concerning service providers' data stores, and (3) despite the existence of a data storage solution that can better preserve the privacy of personal information. Consequently, due to retaining the *status quo ante*, consumers may fail to recognise the potential benefits of a new alternative, such as blockchain-based technology. Hence,

H9: Inertia is negatively associated with the perceived benefits of blockchain-based databases.

3. Research methodology

3.1. Scenario-based Survey

Figure 1 displays our research model. We use a scenario-based survey instrument to test our hypotheses. The first part of the survey presents a scenario followed by measures to capture perceptions of threat severity, threat susceptibility, and privacy concerns associated with personal information stored on a centralised database, affective-based, behavioural-based, and cognitive-based inertia associated with continued reliance on centralised databases, as well as awareness, perceived benefits, and behavioural intention to switch to blockchain-based databases.

It is important to note that our study explores consumers' perceptions of their existing banking systems (which are centralised) and analyzes them in conjunction with their perceptions of blockchain systems (which are decentralised) by presenting a scenario. The scenario presents the respondents with a situation where their current bank has offered to move their existing bank account number and transaction history to a decentralised blockchain database. (Refer to Appendix B for the scenario and survey items.) Figure 2 further illustrates the flow of our survey instrument.

We select a banking scenario because of the strong current focus on adapting blockchain technology specifically to the banking industry. We also believe that bank accounts are an appropriate domain to ensure respondents would perceive the scenarios as realistic and to increase internal validity. According to an FDIC survey on the banking habits of individuals in the United States, only 7% of households were unbanked (FDIC, 2015), indicating the plausibility of a bank scenario to the survey sample. Immediately after presenting the scenario to the study participants, we asked them to rate the scenario's realism based on a scale of 100. Results indicate a realism score of 73.2 for the scenario, thus indicating our respondents to perceive our scenario to be highly realistic.

3.2. Item development and sample population

Table 2 displays the constructs depicted in the research model, along with their types and sources.

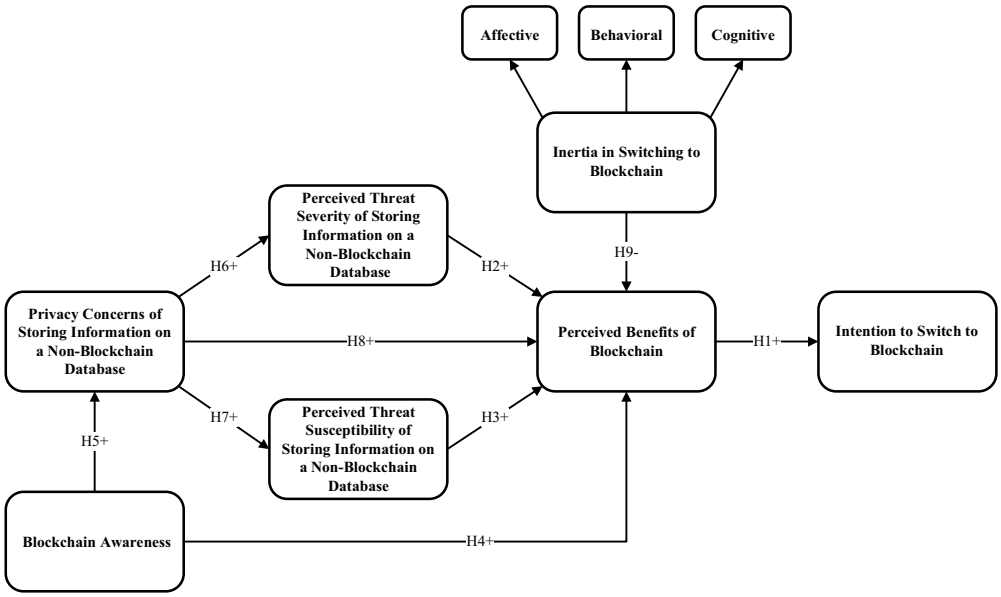

Figure 1. Research model.

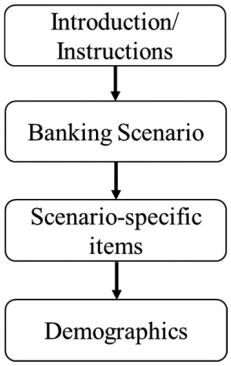

Figure 2. Instrument Flow.

Table 2. Sources of Measurement Items.

Construct	Type	Source	Items
Perceived Threat Severity	Reflective	Johnston & Warkentin, 2010	4
Perceived Threat Susceptibility	Reflective	Johnston & Warkentin, 2010	3
Awareness	Reflective	Ng et al., 2009	5
Privacy Concerns	Reflective	Dinev & Hart, 2006	4
Inertia	Reflective	Polites & Karahanna, 2012	9
Perceived Benefits	Reflective	Ng et al., 2009	4
Behavioural Intention	Reflective	D'Arcy et al., 2009	3

All measurement items use a 5-point Likert scale anchored from strongly disagree to strongly agree. We base each construct in our study on previously validated scales. As indicated by Straub (1989), the use of previously validated items increases the instrument's validity and reliability. We adapted the items measuring perceived severity and susceptibility from Johnston and Warkentin (2010). Because we focused our banking scenario on the blockchain's enhanced privacy protections in thwarting unauthorised access to personal information, we adapted these scales to be specifically related to the threat of unauthorised access. We adapted awareness items from Ng et al. (2009) and Dinev and Hu (2007). We adapted the items for privacy concerns from Dinev and Hart (2006), inertia from Polites and Karahanna (2012), perceived benefits from Ng et al. (2009), and behavioural intention from D'Arcy et al. (2009). Based on the criteria indicated by inertia's native origins in applied psychology (Oreg, 2003), we model inertia as a second-order reflective and first-order reflective construct, with first-order scales measuring affective, behavioural, and cognitive inertia. We model all other measures utilised in the study reflectively.

An expert panel of information systems Ph.D. students experienced in scale development and survey research methods conducted a review of our survey instrument, and we revised the survey content according to their feedback. Qualtrics hosted and administered the final survey. Before the main data collection, we conducted two pilot tests: (1) 129 undergraduate students from a large Mid-South university and (2) 300 MTurk respondents. We retained a final sample of 83 responses for the pilot test analysis of the student sample after discarding 46 responses due to incompleteness (a respondent has abandoned the survey before completing it), failing attention checks, and missing values (a respondent has skipped some of the survey's mandatory fields). We retained a final sample of 267 responses for the MTurk pilot test sample after discarding 33 responses using the same criteria as for the student sample. In overcoming some of the validity concerns associated with the MTurk pilot sample, we added an additional item for privacy, awareness, and benefits for the main data collection. Due to the low item loading, we removed one of the susceptibility items and substituted it with another item for the main data collection. Apart from these changes, based on the pilot study results and the feedback obtained from the study participants, we deemed the survey items appropriate for our main investigation.

To determine the minimum sample size needed based on a priori criteria, we conducted a power analysis for structural equation models using G*Power, which accounts for both observable measures and latent constructs (Faul et al., 2007). Assuming a medium effect size of 0.3, a power level of 0.8, and an alpha level of 0.05, a minimum of 200 observations were needed to ensure sufficient power. We collected a sample of 330 observations through Amazon Mechanical Turk (MTurk) from individuals in the

United States who own any of the following bank accounts: checking account, savings account, money market account, certificate of deposit (CD), or individual retirement accounts (IRAs). A general sample population of bank account users is appropriate for the study because the survey measures individuals' perceptions of switching bank accounts due to the potential benefits of a new alternative such as blockchain-based databases for banking. Bank account ownership applies to individuals from all facets regardless of their occupational, technical, or educational background. Furthermore, to ensure that the respondents understood the information pertaining to blockchain within the scenario, we included a blockchain comprehension question (Appendix B). 67.1% of the respondents indicated that they were either confident or very confident in explaining blockchain after reading the scenario. Thus, indicating that most of the respondents fully comprehend the material presented within the scenario.

We do not report a response rate for the MTurk sample because individuals were not selected randomly and had the option to self-select into the study. To ensure that our respondents read the scenario and the survey items, we embedded attention check questions throughout the survey. An example attention check item includes "Based on the scenario, if a blockchain database is decentralized, select Strongly Agree. Otherwise, mark Strongly Disagree for this statement". We further examined our data for incomplete responses and missing values. We removed 26 respondents who did not answer the attention check questions correctly, which yielded 304 complete usable responses for our final dataset. As illustrated in Table 3, the survey population is 52.3% percent male, with an average age of 39.6. Of the participants, a total of 92.7% indicated that they have an average, high, or very high knowledge of computers and IT. Table 4 provides descriptive statistics for our measures. According to Brown (2006), for structural equation modelling (SEM) analysis, acceptable skewness values are within ± 3, and acceptable kurtosis values are within ±10. Therefore, our skewness and kurtosis values are well below the recommended guidelines for the proceeding SEM analysis.

4. Data analysis and results

4.1. Confirmatory factor analysis

In Confirmatory Factor Analysis (CFA), a measurement model containing latent constructs constrains observable measurement items to their respective unobservable constructs. During CFA, we identify items that did not demonstrate a loading of 0.7 or greater on their construct. After removing the problematic items from the measurement model, we examine model fit based on χ^2 index, goodness of fit

Table 3. Demographics.

n = 304			
Gender (% Male)	52.3%	Age	Average: 39.6
Education:		IT and computer knowledge:	
Less than high school	0.0%	Low	2.0%
High school degree	13.5%	Slightly low	5.3%
Undergraduate degree	43.4%	Average	34.2%
Graduate degree	43.1%	High	42.1%
Other	0.0%	Very high	16.4%
Employment Status:		Years of computer usage	Average: 25.6
Employed full-time	80.3%	Hours of computer usage per day	Average: 10.8
Employed part-time	5.0%	Years of Internet usage	Average: 24.2
Self-employed	8.9%	Hours of Internet usage per day	Average: 11.0
Retired	1.0%		
Student	1.3%		
Not employed	3.6%		

Table 4. Descriptive Statistics.

Variable	Mean	Std. Dev	Skewness	Kurtosis
Perceived Threat Severity	4.001	.695	−.499	−.124
Perceived Threat Susceptibility	3.905	.749	−.935	1.212
Awareness	3.326	1.041	−.653	−.451
Privacy Concerns	3.626	.742	−.652	.543
Inertia-Affective Based	2.692	1.129	.098	−1.183
Inertia-Behavioural Based	2.968	1.046	−.285	−.812
Inertia-Cognitive Based	2.724	1.134	−.025	−1.153
Perceived Benefits	3.895	.708	−.891	.714
Intention to Switch to Blockchain	3.734	.861	−.905	.852

n = 304
Item min = 1; Item max = 5

Table 5. Measurement Model Fit Statistics.

Goodness of Fit Statistic	Recommended Value	Calculated Value
χ^2	–	547.042
Degrees of Freedom (df)	–	428
χ^2 statistical significance (p-value)	–	.000
χ^2 index (Chi-square/df)	< 3	1.278
Standardised Root Mean square Residual (SRMR)	≤ .09	.041
Comparative Fit Index (CFI)	≥ .90	.976
Tucker–Lewis Index (TLI)	≥ .90	.972
Incremental Fit Index (IFI)	≥ .90	.976
Root Mean Square Error of Approximation (RMSEA)	≤ .08	.030

(IFI, CFI, and TLI), root mean square error of approximation (RMSEA), and standardised root mean square residual (SRMR). The χ^2 index for the main study (1.278) is below the recommended threshold. The remainder of the analysis indicates that the model fits the data well (IFI = .976; TLI = .972; CFI = .976; RMSEA = .030; SRMR = .041). Table 5 shows the model fit statistics for the main study.

Next, we assessed our items' convergent and discriminant validity (Churchill, 1979; Peter, 1981), following Fornell and Larcker (1981) guidelines. Based on these recommendations, constructs must exhibit average variance extracted (AVE) measures above 0.5 to demonstrate convergent validity, and latent correlations between constructs must not exceed the corresponding constructs' square root AVEs to show evidence of discriminant validity. Our analysis indicates that our measurement items demonstrate convergent validity. All standardised item loadings on their respective constructs are above or very close to 0.7 (Hair et al., 2002; Nunnally, 1978). The composite reliability for each of the latent constructs is above the recommended 0.7 threshold, and all AVEs are above 0.5 (Hair et al., 2017). These values provide sufficient evidence of convergent validity for our measurement items. Table 6 further illustrates these values.

Table 6. Summary Results for Reflective Measurement Models.

Constructs	Indicators	Loadings >0.7	AVE >0.5	CR >0.7	VIF < 3	R^2
SEV	**SEV1**	.719	.564	.838	1.775	.330
	SEV2	.758			1.926	
	SEV3	.748			1.815	
	SEV4	.777			1.900	
SUS	**SUS1**	.753	.593	.814	1.721	.520
	SUS2	.800			1.852	
	SUS3	.756			1.805	
AWR	**AWR1**	.860	.647	.901	2.844	–
	AWR2	.838			2.721	
	AWR3	.769			2.231	
	AWR4	.786			2.372	
	AWR5	.764			2.078	
PVC	**PVC1**	.748	.564	.838	1.832	.030
	PVC2	.757			1.932	
	PVC3	.714			1.775	
	PVC4	.784			1.830	
IAB	**IAB1**	.802	.686	.867	2.145	–
	IAB2	.868			2.541	
	IAB3	.813			2.177	
IBB	**IBB1**	.750	.593	.814	1.747	–
	IBB2	.781			1.804	
	IBB3	.779			1.825	
ICB	**ICB1**	.804	.639	.841	2.040	–
	ICB2	.856			2.228	
	ICB3	.733			1.805	
BEN	**BEN1**	.756	.584	.849	1.760	.830
	BEN2	.793			2.100	
	BEN3	.745			1.843	
	BEN4	.761			1.922	
INT	**INT1**	.872	.645	.845	2.340	.280
	INT2	.750			1.826	
	INT3	.783			2.026	

n = 304

AVE = Average variance extracted; CR = Composite (Rho) reliability. SEV = Perceived Threat Severity of Storing Information on a Non-Blockchain Database; SUS = Perceived Threat Susceptibility of Storing Information on a Non-Blockchain Database; AWR = Blockchain Awareness; PVC = Privacy Concerns of Storing Information on a Non-Blockchain Database; IAB = Inertia-Affective Based; IBB = Inertia-Behavioural Based; ICB = Inertia-Cognitive Based; BEN = Perceived Benefits of Blockchain; INT = Intention to Switch to Blockchain

Table 7. Inter-Construct correlations for Reflective Measures (Fornell-Larcker Criterion).

Construct	SEV	SUS	AWR	PVC	IAB	IBB	ICB	BEN	INT
SEV	**.751**								
SUS	.550	**.770**							
AWR	.079	.150	**.804**						
PVC	.541	.698	.185	**.751**					
IAB	−.350	−.428	−.015	−.346	**.828**				
IBB	−.284	−.191	.116	−.195	.419	**.770**			
ICB	−.264	−.219	.111	−.169	.547	.365	**.799**		
BEN	.655	.758	.238	.602	−.572	−.426	−.432	**.764**	
INT	.338	.481	.448	.509	−.299	−.237	−.209	.500	**.803**

n = 304

SEV = Perceived Threat Severity of Storing Information on a Non-Blockchain Database; SUS = Perceived Threat Susceptibility of Storing Information on a Non-Blockchain Database; AWR = Blockchain Awareness; PVC = Privacy Concerns of Storing Information on a Non-Blockchain Database; IAB = Inertia-Affective Based; IBB = Inertia-Behavioural Based; ICB = Inertia-Cognitive Based; BEN = Perceived Benefits of Blockchain; INT = Intention to Switch to Blockchain.

The diagonal axis contains the square root AVE values.

In establishing the constructs' discriminant validity, we examine the inter-construct correlations, including the second-order reflective factor for inertia, as illustrated in Table 7 and the heterotrait-monotrait ratio of correlations (HTMT) as illustrated in Table 8. In line with established theoretical rationale for determining whether a second-order factor is reflective (D'Arcy et al., 2014), each inertia dimension alone can create inertia. One does not need to perceive the existence of all three dimensions to perceive inertia. Because our data demonstrate that inertia's first-order constructs exhibit values that indicate a reflective, rather than causal, relationship with the second-order factor, we model inertia as a first-order reflective, second-order reflective construct.

Consistent with the premise of the Fornell and Larcker (1981) framework, the square root of AVE values for each construct should be greater than the corresponding off-diagonal correlations of other constructs. The heterotrait-monotrait ratio of correlations is a measure of similarity between latent variables. An HTMT value of less than .85 between a pair of latent variables indicates discriminant validity (Henseler et al., 2015). As illustrated in Table 8, all correlations are less than .85, establishing discriminant validity. Since all our items depict a good model fit, convergent validity, and internal consistency reliability, we retained all items for the structural model analysis.

When researchers collect data using a single method and do not acquire the dependent and independent variables from different sources, common method variance (CMV) is a potential threat (Buckley et al., 1990). To minimise CMV's threat, we relied on an expert panel review, a pilot test, random assignment of scenarios to participants, randomisation of items within the survey, and anonymity of study participants (Malhotra et al., 2006). We further assessed the extent of CMV using the marker variable technique (Lindell & Whitney, 2001). A marker variable is a theoretically unrelated construct that should not correlate with any other latent construct in a model. In untabulated results, the squared latent correlation between our marker variable and all other survey constructs is less than 0.05.

4.2. Structural model testing

We tested the structural model and its associated hypotheses using AMOS version 26, a covariance-based statistical tool for assessing structural equation models. Before analysing individual relationships within the model, we assessed the structural model's fit statistics. The χ^2 index (χ^2 = 685.822; df = 451; χ^2

Table 8. HTMT Analysis.

	SEV	SUS	PVC	AWR	BEN	IAB	IBB	ICB	INT
SEV									
SUS	0.550								
PVC	0.532	0.690							
AWR	0.077	0.152	0.193						
BEN	0.657	0.758	0.604	0.238					
IAB	0.359	0.434	0.346	0.015	0.579				
IBB	0.285	0.184	0.195	0.114	0.423	0.422			
ICB	0.264	0.208	0.162	0.115	0.433	0.545	0.372		
INT	0.348	0.491	0.511	0.430	0.518	0.310	0.256	0.221	

n = 304

SEV = Perceived Threat Severity of Storing Information on a Non-Blockchain Database; SUS = Perceived Threat Susceptibility of Storing Information on a Non-Blockchain Database; AWR = Blockchain Awareness; PVC = Privacy Concerns of Storing Information on a Non-Blockchain Database; IAB = Inertia-Affective Based; IBB = Inertia-Behavioural Based; ICB = Inertia-Cognitive Based; BEN = Perceived Benefits of Blockchain; INT = Intention to Switch to Blockchain.

index = 1.521) for the structural model is below the recommended threshold. Our SRMR for the structural model was above the recommended threshold, but a variance inflation factor (VIF) analysis revealed all items were below 3 (see Table 6), indicating that multicollinearity was likely not causing a rise in SRMR (Hair et al., 2017). The remainder of the analysis indicates that the model adequately fits the data (IFI = .953; TLI = .948; CFI = .953; RMSEA = .041) and that we can proceed to examine the individual relationships within the model. Fit statistics for the structural model are in Table 9. Table 10 and Figure 3 report standardised path coefficients, t-values, and coefficient of determination (R^2) values for our model. Except for H8, the remaining hypotheses are significant at $p < 0.01$ or better.

4.3. Post hoc analysis

Contextualisation requires researchers to examine where existing theories are applicable, as well as where they differ, in new research contexts (Hong et al., 2014). Based on our results, it appears that privacy concerns do not influence the perceived benefits of blockchain. Due to the novelty of blockchain research related to consumer perceptions, there is limited empirical research into the perceived benefits of blockchain and intention to switch to blockchain. Thus, to complete our application of HBM to blockchain research contexts, we conducted a post-hoc analysis by re-specifying our research model. Our initial model hypothesised that privacy concerns would influence the perceived benefits of blockchain directly. However, based on our findings, privacy concerns failed to have a significant influence on benefits. Therefore, we removed the relationship between privacy concerns and perceived benefits and added a path from awareness to intention to switch.

As illustrated in the post hoc model (Figure 4), the reformulation did not result in substantial differences in the model. With the post hoc revisions, the model explains 77% of the variance in perceived benefits (R^2 = 83% in the original model – see Figure 3) and 36% of the variance in intention (R^2 = 28% in the original model – see Figure 3). The strongest influence on benefits comes from threat susceptibility (.447), followed by inertia (total effect of –.334), and threat severity (.329). The total effect of awareness on intention is .361.

As in the prior test of the model, threat susceptibility, severity, inertia, and awareness are all factors that influence consumer perception of the benefits of blockchain-based databases and their intention to switch. Furthermore, privacy concerns influence perceived benefits through threat susceptibility, severity, and awareness. To that end, the post-hoc model may be a more parsimonious and pragmatically intuitive model of explaining the benefits realisation of blockchain databases. Additionally, the post hoc model substantially improves the amount of variance explained for intention to switch.

Table 9. Structural Model Fit Statistics.

Goodness of Fit Statistic	Recommended Value	Calculated Value
χ^2	–	685.822
Degrees of Freedom (df)	–	451
χ^2 statistical significance (*p* value)	–	.000
χ^2 index (Chi-square/df)	< 3	1.521
Standardised Root Mean square Residual (SRMR)	≤ .09	.104
Comparative Fit Index (CFI)	≥ .90	.953
Tucker–Lewis Index (TLI)	≥ .90	.948
Incremental Fit Index (IFI)	≥ .90	.953
Root Mean Square Error of Approximation (RMSEA)	≤ .08	.041

Table 10. Significance Analysis of the Direct Effects.

Hypothesis	Path (Predicted Sign)	Path Coefficient	t Value	Significance (one-tailed)	Supported $p < 0.05$
H1	Perceived Benefits of Blockchain → Intention to Switch to Blockchain (+)	.773	7.573	$p < .001$	**Supported**
H2	Perceived Threat Severity of Non-Blockchain → Perceived Benefits of Blockchain (+)	.315	4.650	$p < .001$	**Supported**
H3	Perceived Threat Susceptibility of Non-Blockchain → Perceived Benefits of Blockchain (+)	.442	5.794	$p < .001$	**Supported**
H4	Blockchain Awareness→ Perceived Benefits of Blockchain (+)	.156	4.892	$p < .001$	**Supported**
H5	Blockchain Awareness → Privacy Concerns of Non-Blockchain (+)	.144	2.793	$p < .01$	**Supported**
H6	Privacy Concerns of Non-Blockchain → Perceived Threat Severity of Non-Blockchain (+)	.440	7.830	$p < .001$	**Supported**
H7	Privacy Concerns of Non-Blockchain → Perceived Threat Susceptibility of Non-Blockchain (+)	.678	9.634	$p < .001$	**Supported**
H8	Privacy Concerns of Non-Blockchain → Perceived Benefits of Blockchain (+)	.002	.032	n.s.	**Not Supported**
H9	Inertia in Switching to Blockchain → Perceived Benefits of Blockchain (-)	–.369	–6.553	$p < .001$	**Supported**

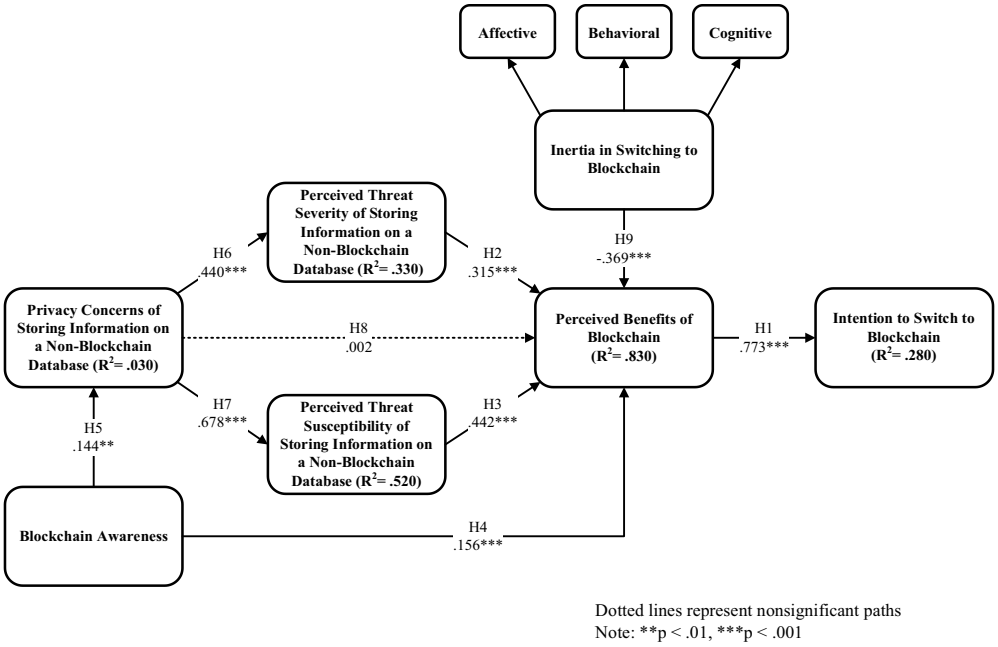

Figure 3. Results of Structural Model Analysis.

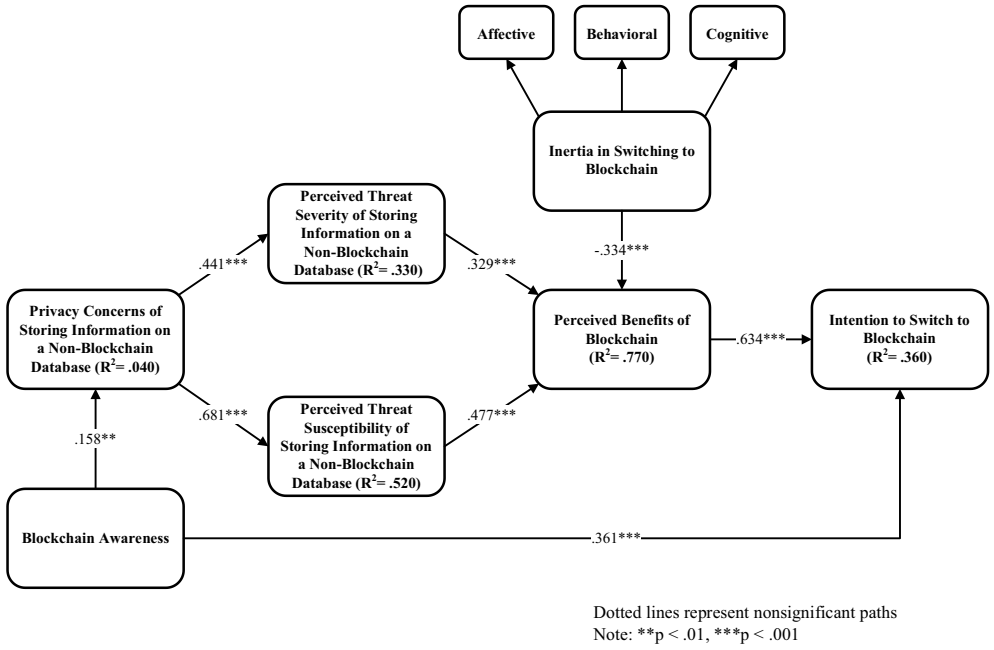

Figure 4. Post hoc Model.

5. Discussion

Our study examines various factors influencing customers' perception of the benefits of blockchain-based databases and how these perceived benefits lead to intention to switch to a blockchain-based database for banking purposes. The analysis of our research model yields several interesting findings. First, we assess the direct influence of HBM factors, along with privacy concerns and inertia, on the perception of benefits. Second, we assess the impact of perceived benefits on consumer intention to switch to blockchain-based applications. Finally, we discuss the impacts on research and practice.

We designed our study to determine the factors that influence consumers' perceptions of the benefits of blockchain implementation by their banks, particularly those lead to eventual switching to blockchain-based databases. Perceived threat severity, threat susceptibility, and awareness each demonstrate a significantly positive effect on consumers' perceived benefits of blockchain technology, which in turn have a significant positive impact on their intention to switch to the blockchain. Awareness has a significant

positive effect on both privacy concerns and perceived benefits, indicating that privacy concerns partially mediate the indirect effect of awareness on benefits. This finding highlights the importance of both privacy concerns and awareness in the research model. Awareness comes from a diverse range of triggers that motivate a consumer to take a particular action by informing the individual of both the costs and benefits of the behaviour (Rosenstock, 1974). Additionally, our post hoc model reveals that awareness significantly affects intention to switch, highlighting the importance of promoting awareness to influence users to adopt blockchain-based solutions. Inertia, which we conceptualise as a relevant barrier towards benefits realisation of blockchain technology, has a significant negative impact on customers' perception of blockchain benefits.

Surprisingly, the hypothesised relationship between privacy concerns and perceived benefits (H8) is not supported. Extant literature supports the notion that a consumer's intention to surrender personal information is highly dependent on their perceptions of privacy concerns (Culnan & Armstrong, 1999; Dinev & Hart, 2006). However, to the best of our knowledge, there is a lack of studies investigating the impact of privacy concerns on consumers' realisation of benefits related to disclosing personal information to third-party service providers. Thus, our study may provide novel insights into why consumers continue to engage with third-party service providers despite heightened privacy concerns. As indicated by Culnan and Armstrong (1999), consumers are more comfortable disclosing personal information with third parties in instances where they knew who would have access to the information. In the context of our study, our respondents consisted of banking consumers who have already realised the benefits offered to them by their bank and have shared their personal information with the bank in exchange for obtaining these benefits. Thus, while banking consumers are concerned about the privacy of their information and believe that blockchain may be able to safeguard their information, these privacy concerns alone may not necessarily motivate consumers to realise the benefits offered by their bank. Furthermore, even though most banking consumers are concerned about privacy, research finds banks to be trusted data security providers, and customers expect banks to safeguard their personal information (The Clearing House, 2018).

According to our results, threat severity and threat susceptibility fully mediate the indirect effect of privacy concerns on benefits, indicating that privacy concerns may not fully manifest without the presence of a threat to personal information. This finding was corroborated in our post hoc model as well. Thus, we can infer that threat is a focal point in the consumer decision-making process. A consumer concerned about the privacy of their personal information in the hands of third parties will perceive increased threats to their information, impacting their realised benefits of blockchain. Dinev and Hart (2006) call for research investigating the perceived benefits associated with distanciation from the Internet as a means of reducing consumer privacy concerns and risk perceptions. In contrast, our study results indicate that blockchain databases may alleviate privacy risks and concerns and provide consumers with a secure means of transacting online without consideration for distanciation from the Internet.

Inertia is also especially powerful in predicting consumers' perception of blockchain benefits. Even in the presence of known benefits of the technology, perceptions of inertia may lead consumers not to realise the privacy-related benefits offered by blockchain. Thus, organisations should consider inertia as an essential mechanism in which the perceptions of switching costs and status quo bias can impact the ultimate acceptance of blockchain technology. These findings are important because, while many of our model's factors were consistent across contexts, blockchain implementations are highly contextual. Researchers and practitioners should treat them as such moving forward. Therefore, in the context of adoption decisions related to blockchain technology, our findings support our adaptation of HBM.

5.1. Implications for research

Our study contributes to research streams related to HBM, information privacy, blockchain adoption, and inertia. By integrating disparate research streams within the blockchain context, we have added crucial knowledge to each of these theories' research streams by testing their applicability within a unique context and examining how they interact with each other and with the external factors provided by the context. Because the blockchain offers inherently strong privacy protections, examining these varying theories together within this specific context is both timely and relevant, considering the rapid adoption of blockchain-based systems and their relevancy to ongoing research on the interplay between privacy concerns and disruptive technology. Our work may also be generalisable to other contexts featuring longstanding systems poised to be replaced by systems that, like the blockchain, offer more privacy or security protections. Future work may build on our study by testing the applicability of our model in related contexts.

Our work extends the adaptation of HBM to the context of consumer's perceptions of blockchain privacy benefits. Our results show that individuals conduct the core cognitive appraisals described in HBM when

evaluating the benefits of blockchain, which in turn leads to their intention to switch to blockchain-based applications. Inertia represents a considerable hurdle to a consumers' realisation of blockchain benefits. Our inclusion of privacy concerns in the HBM model is novel but necessary, given that the blockchain has critical benefits for information privacy. Our results demonstrate that an individual's concern for privacy is a critical factor in explaining the customers' perception of blockchain-based privacy benefits. This finding expands our understanding of the APCO model (Dinev et al., 2015; Smith et al., 2011). We show that when including privacy concerns with HBM constructs and inertia, the relationship between privacy concerns and risk and privacy concerns and behavioural outcomes remain. As future work considers the role of privacy in understanding the adoption of new technologies, studies should continue to consider these factors. Our findings also suggest that as the APCO model merges with other theoretical-based understandings of behavioural outcomes, these other theoretical-based constructs may play a more substantial role in determining behaviours than those central to the APCO model.

Our work also extends existing knowledge on factors motivating consumers to use new technology by investigating consumers' willingness to use blockchain applications through customers' understanding of the benefits of blockchain-based databases, which ultimately influence their intention to use blockchain. Although traditional Technology Acceptance Model (TAM)-based constructs such as usefulness and ease of use have effectively explained technology adoption for prior systems, different factors emerge when potential users do not understand the given system well. With blockchain technology, individuals lack the understanding of the blockchain's decentralised nature or public-key cryptography that makes anonymously posting to the ledger possible. Perceived usefulness is irrelevant if the system's utility is not comprehensible, and the status quo of well-established existing systems severely impacts perceived ease of use. Our research demonstrates that for transformative technologies that upend widely used systems by trusted institutions (e.g., banks), individuals conduct a more in-depth cognitive evaluation when considering whether to use the new technology.

Because we focus on consumers' perception of the benefits of blockchain-based databases as replacements to centralised databases in banking, our study provides an ideal context for further validating inertia concerning a currently emerging technology. For centuries, people have relied on centralised data stores for banking, establishing a contextual status quo ideal for testing inertia's applicability. We show that demonstrate acts as a significant barrier for blockchain application use, further validating its applicability to emerging technologies such as the blockchain.

5.2. Implications for practice

The findings of our study have several practical implications, as well. First, managers should be aware that consumer inertia is a significant barrier to convincing customers to buy into blockchain technology. Consumers are typically resistant to switching from a system they perceive as sufficiently effective. However, consumers will consider other factors and can be convinced to use blockchain-based databases if they recognise the technology's many benefits. One key benefit that companies may want to emphasise is the inherent anonymity provided by blockchain technology. For consumers who are especially concerned about their privacy, this can be a powerful way for companies to frame information related to blockchain promotion. To counteract the status quo, companies must increase consumer awareness of blockchain technology while highlighting its benefits related to privacy protection and promoting its overall effectiveness and efficiency compared to existing centralised databases.

Practitioners should also be encouraged by the impact that awareness can have on several consumer perceptions. Our findings indicated that awareness affects privacy concerns, perceived benefits, and intention to switch. Thus, organisations may need to craft blockchain awareness campaigns highlighting the various reasons to be concerned about information privacy while also providing information about the blockchain's benefits in alleviating privacy issues. Such a campaign should be an effective means to convince users of the various ways in which the blockchain is useful and represents a substantial upgrade over their current system.

5.3. Limitations and future research

A key limitation of our work is the scope of blockchain implementations described in our scenario. Although cryptocurrency comprises most blockchain technologies currently in use, developers continually adapt the blockchain for different industries (e.g., healthcare, supply chain). While this limitation impacts the generalisability of our findings, future research can explore these other emerging avenues. Blockchain implementations are expanding as industries investigate novel ways to utilise the technology, which should be a fertile research stream for the near future.

Another limitation is our use of customers' perception of the benefits of blockchain-based databases related to the banking industry rather than the actual

benefits reaped from blockchain by banking consumers. Although measuring actual benefits is preferable, measuring perceptions of benefits is a suitable alternative for emerging technologies that experience low adoption rates or low general awareness (Menard et al., 2017). However, future research may further test our adaptation of HBM and APCO to determine whether to use behaviours through perceptions of benefits to validate theoretical linkages. A potential avenue for future work in this area would be to replicate the current study when blockchain usage is closer to a tipping point.

Apart from the HBM constructs, privacy concerns, and inertia regarding using technology such as blockchain, other persuading factors might build consumer confidence while minimising their privacy concerns. For instance, extant research has identified trust as an essential condition for an individual to engage in various information security behaviours (Pavlou & Gefen, 2004; Pavlou et al., 2007; Srivastava & Chandra, 2018) and share their personal information with third parties (Dinev & Hart, 2006). Consequently, future research should investigate the impact of trust on increasing the acceptance of blockchain technology into the current organisational infrastructure.

Another limitation pertains to the Standardised Root Mean Square Residual (SRMR) value for our structural model (.104), which is above the recommended threshold (.09). SRMR is an absolute measure of fit that indicates the standardised difference between the observed and the predicted correlation. The SRMR for our measurement model was low (.041), suggesting that the rise in SRMR for the structural model may be attributable to the addition of structural paths, rather than a lack of construct validity. Kenny (2020) provides one explanation for our SRMR score by observing that SRMR "is a positively biased measure and that bias is greater for small N and for low df studies". Although our sample is large enough to achieve adequate statistical power, future researchers with larger sample sizes can mitigate SRMR bias in similar studies. Another explanation for our SRMR score is the potential complexity and depth of individual motivation towards blockchain adoption. While a low RMSEA (0.30 from Table 5) demonstrates that our structural model is parsimonious, a high SRMR may indicate that our model does not capture all associations among variables. For example, the variance explained in privacy concerns is low, and the variance explained in intention to switch is modest. These results indicate that other variables outside of our research scope may influence these constructs. Our study attempts to discover what forces can influence blockchain adoption behaviour, and our findings coupled with the indication that additional forces come into play reinforce the importance of our investigation, as well as future investigations, in developing an understanding of consumer intentions towards blockchain technologies to inform both academia and the business community.

Finally, in the context of this study, we used inertia to investigate perceived barriers (i.e., negative aspects of a cause of action that instigate conflicting motives for the avoidance of the behaviour (Rosenstock, 1974)) proposed by HBM. However, since most banks are currently in the pilot phase of implementing blockchain into their banking infrastructure, we could not find an existing financial institution or application that might have provided quantitative data in measuring individuals' inertia in switching to the blockchain. Therefore, we measured our respondents' perceptions of their existing banking systems in conjunction with their perceptions of blockchain systems by presenting a hypothetical blockchain-based banking system scenario. Thus, our study may have failed to capture consumers' actual behaviour relative to their resistance to change and their unwillingness to realise the blockchain's benefits. Future studies should use this current study as a foundation to explore inertia in an actual blockchain banking context. Future studies should further investigate the potential barriers to switching in terms of other costs unexplored in this study (e.g., lack of standards and regulation surrounding blockchain, difficulty and complexity in understanding the technology as barriers to switching). Future research should most importantly investigate mechanisms to overcome consumer inertia related to new technologies such as blockchain to increase user acceptance.

6. Conclusion

The blockchain is one of the most recent IS innovations but remains confusing and mostly misunderstood by a general audience. Although the blockchain began strictly as a cryptocurrency mechanism and has been mostly a curiosity for many users, more opportunities for blockchain use have emerged as various industries explore blockchain implementations for core functions. While many users may not see the need to switch from well-established and reliable centralised forms of trusted third-party verification, an increase in general awareness that highlights enhanced information privacy protection can convince them of the blockchain's utility. As users continue to use blockchain for various purposes, and as

blockchain developers find novel ways to implement the technology, researchers should continue examining users' decisions to use blockchain-based applications in differing contexts.

Notes

1. https://www.ibm.com/security/data-breach
2. Throughout this paper, we use the term "blockchain" to represent the technological construct and "blockchain-based database" to represent that construct's implementation

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Nirmalee Raddatz http://orcid.org/0000-0001-7641-1314
Joshua Coyne http://orcid.org/0000-0001-7661-8382
Philip Menard http://orcid.org/0000-0001-8696-3198
Robert E Crossler http://orcid.org/0000-0002-8179-9138

References

Abramova, S., & Böhme, R. (2016) Perceived benefit and risk as multidimensional determinants of bitcoin use: A quantitative exploratory study. In Proceedings of the Thirty Seventh International Conference on Information Systems (ICIS), Dublin, Ireland. https://doi.org/10.17705/4ICIS.00001 .

Ajzen, I., Czasch, C., & Flood, M. G. (2009). From intentions to behavior: Implementation intention, commitment, and conscientiousness. *Journal of Applied Social Psychology*, *39*(6), 1356–1372. https://doi.org/10.1111/j.1559-1816.2009.00485.x

Baiyere, A., Salmela, H., & Tapanainen, T. (2020). Digital transformation and the new logics of business process management. *European Journal of Information Systems*, *29*(3), 238–259. https://doi.org/10.1080/0960085X.2020.1718007

Bawa, K. (1990). Modeling inertia and variety seeking tendencies in brand choice behavior. *Marketing Science*, *9*(3), 263–278. https://doi.org/10.1287/mksc.9.3.263

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, *19*(10), 1020–1034. https://doi.org/10.17705/1jais.00518

Bélanger, F., Hiller, J., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, *11*(3–4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Brown, T. A. (2006). *Confirmatory factor analysis for applied research*. The Guilford Press.

Buckley, M., Cote, J., & Comstock, S. (1990). Measurement errors in behavioral sciences: The case of personality/attitude research. *Educational Psychology*, *50*(3), 447–474. https://doi.org/10.1177%2F0013164490503001

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

ones, C. L., Jensen, J. D., Scherr, C. L., Brown, N. R., Christy, K., & Weaver, J. (2015) The health belief model as an explanatory framework in communication research: exploring parallel, serial, and moderated mediation. *Health Communication*,*30*(6): 566–576. https://doi.org/10.1080/10410236.2013

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606. https://doi.org/10.1207/s15506878jobem4604_6

Carlo, J. L., Gaskin, J., Lyytinen, K., & Rose, G. M. (2014). Early vs. late adoption of radical information technology innovations across software development organizations: An extension of the disruptive information technology innovation model. *Information Systems Journal*, *24*(6), 537–569. https://doi.org/10.1111/isj.12039

Chen, P., & Hitt, L. M. (2002). Measuring switching costs and the determinants of customer retention in internet-enabled businesses: A study of the online brokerage industry. *Information Systems Research*, *13*(3), 255–274. https://doi.org/10.1287/isre.13.3.255.78

Chong, A. Y. L., Lim, E. T., Hua, X., Zheng, S., & Tan, C. W. (2019). Business on chain: A comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems*, *20*(9), 1310–1339. https://doi.org/10.17705/1jais.00568

Churchill, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, *16*(February), 64–73. https://doi.org/10.1177/002224377901600110

Clark, J. G., Beebe, N., Williams, K., & Shepherd, L. (2009). The privacy advocates: Resisting the spread of surveillance. *Journal of Information Privacy & Security*, *5*(4), 3–30. http://dx.doi.org/10.3233/IP-2011-0256

Crossler, R., & Posey, C. (2017). Robbing peter to pay paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of AssJournal of the Association for Information Systems*, *18*(7), 487–515. https://doi.org/10.17705/1jais.00463

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information*

Systems Research, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. https://doi.org/10.17705/1jais.00133

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "apco" box. *Research Commentary—Informing Privacy Research through Information Systems, Psychology, and Behavioral Economics: Thinking outside the "APCO" Box*, *26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online b-to-c relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, *59*(8), 877–886. https://doi.org/10.1016/j.jbusres.2006.02.006

Eccles, J. (1983). Expectancies, values, and academic behaviors. In J. T. Spen (Ed.), *Achievement and Achievement Motives: Psychological and Sociological Approaches*. W. H. Freeman, 75–119.

Faul, F., Erdfelder, E., Lang, A., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175–191. https://doi.org/10.3758/bf03193146

FDIC. (2015). *2015 fdic national survey of unbanked and underbanked households*. Retrieved from https://www.fdic.gov/householdsurvey

FinTech Network. (2017). *Four blockchain use cases for banks*. Retrieved from https://blockchainapac.fintecnet.com/uploads/2/4/3/8/24384857/fintech_blockchain_report_v3.pdf

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Gerber, N., Gerber, P., Drews, H., Kirchner, E., Schlegel, N., Schmidt, T., & Scholz, L. (2018). FoxIT: Enhancing mobile users' privacy behavior by increasing knowledge and awareness. *In Proceedings of STAST2017: 7th International Workshop on Socio-Technical Aspects in Security and Trust*. Orlando, USA, (pp. 53–63). https://doi.org/10.1145/3167996.3167999

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014). Bitcoin-asset or currency? revealing users' hidden intentions. In Proceedings of the 22th European Conference on Information Systems (ECIS). Tel Aviv.

Greenfield, H. I. (2005). Consumer inertia: A missing link? *American Journal of Economics and Sociology*, *64*(4), 1085–1089. https://doi.org/10.1111/j.1536-7150.2005.00427.x

Gupta, S., Ng, E. H., & Kim, H.-W. (2007). Online customer retention: The resistance to change perspective. In Proceedings of the 28th International Conference on Information Systems (ICIS). Montreal, Quebec, Canada.

Hair, J., Hult, T., Ringle, C., & Sarstedt, M. (2017). *A primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (2nd ed.). SAGE Publications.

Hair, J., Tatham, R., & Anderson, R. (2002). *Multivariate data analysis*. Prentice-Hall.

Henry, C. S., Huynh, K. P., & Nicholls, G. (2018). *Bitcoin awareness and usage in canada: An update*. The *Journal of Investing Cryptocurrency Special Issue, 28*(3), 21-31. https://doi.org/10.3905/joi.2019.28.3.021

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–13. https://doi.org/10.1007/s11747-014-0403-8

Hirschheim, R., & Newman, M. (1988). Information systems and user resistance: Theory and practice. *The Computer Journal*, *31*(5), 398–408. https://doi.org/10.1093/comjnl/31.5.398

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *25*(1), 111–136. https://doi.org/10.1287/isre.2013.0501

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Infosecurity. (2018). *The role of blockchain in cybersecurity*. Retrieved from https://www.infosecurity-magazine.com/next-gen-infosec/blockchain-cybersecurity

Janz, N., & Becker, M. (1984). The health belief model: A decade later. *Health Education Quarterly*, *11*(1), 1–47. https://doi.org/10.1177/109019818401100101

Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. https://doi.org/10.2307/25750691

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, *26*(6), 688–715. https://doi.org/10.1057/s41303-017-0064-z

Keen, P. G. W. (1981). Information systems and organizational change. *Communications of the ACM*, *24*(1), 24–33. https://doi.org/10.1145/358527.358543

Keith, M. J., Thompson, S. C., Hale, J., Benjamin Lowry, P., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Kenny, D. A. (2020). *Measuring model fit*. David A. Kenny. Retrieved from http://www.davidakenny.net/cm/fit.htm

Kim, H., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS Quarterly*, *33*(3), 567–582. https://doi.org/10.2307/20650309

Kim, S. (2009). The integrative framework of technology use: An extension and test. *MIS Quarterly*, *33*(3), 513–537. https://doi.org/10.2307/20650307

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, *50*(2), 361–369. https://doi.org/10.1016/j.dss.2010.07.009

Lending, D., & Straub, D. (1997). Impacts of an integrated information center on faculty end-users: A qualitative assessment. *Journal of the American Society for Information Science*, *48*(5), 466–471. https://doi.org/10.1002/(SICI)1097-4571(199705)48:5<466::AID-ASI12>3.0.CO;2-X

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62–71. https://doi.org/10.1080/08874417.2010.11645450

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114–121. https://doi.org/10.1037/0021-9010.86.1.114

Mai, F., Shan, Z., Bai, Q., Wang, X., & Chiang, R. H. L. (2018). How does social media impact bitcoin value? a test of the silent majority hypothesis. *Journal of Management Information Systems*, *35*(1), 19–52. https://doi.org/10.1080/07421222.2018.1440774

Malhotra, N., Kim, S., & Patil, A. (2006). Common method variance in is research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, *52*(12), 1865–1883. https://doi.org/10.1287/mnsc.1060.0597

Malimage, K., Raddatz, N., Trinkle, B. S., Crossler, R. E., & Baaske, R. (2019). Impact of deterrence and inertia on information security policy changes. *Journal of Information Systems*. *34*(1), 123–134. http://dx.doi.org/10.2308/isys-52400

Marr, B. (2017). *Practical examples of how blockchains are used in banking and the financial services sector*. Forbes. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/08/10/practical-examples-of-how-blockchains-are-used-in-banking-and-the-financial-services-sector/#29f5a58b1a11

Mattke, J., Maier, C., Müller, L., & Weitzel, T. (2018). Bitcoin resistance behavior: A qca study explaining why individuals resist bitcoin as a means of payment. In Proceedings of the 39th International Conference on Information Systems (ICIS). San Francisco, USA.

Mattke, J., Maier, C., & Reis, L. (2020). Is cryptocurrency money? three empirical studies analyzing medium of exchange, store of value and unit of account. SIGMIS-CPR'20: Proceedings of the 2020 on Computers and People Research Conference. https://doi.org/10.1145/3378539.3393859

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): 261–285. https://doi.org/10.1080/0960085X.2020.1787109

McKinsey & Company. (2016). *Blockchain in insurance – Opportunity or threat?* Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Mihalcik, C., & Zhou, M. (2018). *Newegg data breach exposed customer credit card info, says report*. Cnet. Retrieved from https://www.cnet.com/news/newegg-data-breach-exposed-customer-credit-card-info-says-report

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin.org. Retrieved from https://bitcoin.org/bitcoin.pdf

National Cancer Institute. (2005). *Theory at a glance-a guide for health promotion and practice*. Retrieved from https://www.sbccimplementationkits.org/demandrmnch/wp-content/uploads/2014/02/Theory-at-a-Glance-A-Guide-For-Health-Promotion-Practice.pdf

Ng, B.-Y., Kankanhalli, A., & Xu, Y., (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Nunnally, J. (1978). *Psychometric Theory*. McGraw-Hill.

Oreg, S. (2003). Resistance to change: Developing an individual differences measure. *Journal of Applied Psychology*, *88*(4), 680–693. https://doi.org/10.1037/0021-9010.88.4.680

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology*, *25*(2), 103–127. https://doi.org/10.1007/s10940-009-9065-y

Pavlou, P. A., & 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

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal–agent perspective. *MIS Quarterly*, *31*(1), 105–136. https://doi.org/10.2307/25148783

Peter, J. P. (1981). Construct validity: A review of basic issues and marketing practices. *Journal of Marketing Research*, *18*(2), 133–145. https://doi.org/10.1177/002224378101800201

Polites, G. L., & Karahanna, E. (2012). Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly*, *36*(1), 21–42. https://doi.org/10.2307/41410404

Popper, N. (2017, October 1). What is bitcoin, and how does it work? *The New York Times*. https://www.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.html

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs*, *2*(4), 328–335. https://doi.org/10.1177/109019817400200403

Rumelt, R. P. (1995). Precis of inertia and transformation. In *Resources in an evolutionary perspective: Towards a synthesis of evolutionary and resource-based approaches to strategy*,101-132. Norwell, Mass: Kluwer Academic Publishers.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty*, *1*(1), 7–59. https://doi.org/10.1007/BF00055564

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, *19*(1), 62–73. https://doi.org/10.1509/jppm.19.1.62.16949

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Srivastava, S. C., & Chandra, S. (2018). Social presence in virtual world collaboration: An uncertainty reduction perspective using a mixed methods approach. *MIS Quarterly*, *42*(3), 779–803. https://doi.org/10.25300/MISQ/2018/11914

Straub, D. (1989). Validating instruments in mis research. *MIS Quarterly*, *13*(2), 147–169. https://doi.org/10.2307/248922

Summers, N., & Marett, K. (2016). An image of information security: Examining the coping process by internet users. *Journal of Information System Security*, *12*(1), 3–25.

The Clearing House. (2018). *Fintech apps and data privacy: New insights from consumer research*. Retrieved from https://iapp.org/media/pdf/resource_center/fintech_apps_data_privacy.pdf

Treiblmaier, H., & Strebinger, A. (2008). The effect of e-commerce on the integration of it structure and brand architecture. *Information Systems Journal*, *18*(5), 479–498. https://doi.org/10.1111/j.1365-2575.2007.00288.x

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 415–444. https://doi.org/10.17705/1jais.00092

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Walther, S., Sedera, D., Urbach, N., Eymann, T., Otto, B., & Sarker, S. (2018). Should we stay, or should we go? analyzing continuance of cloud enterprise systems. *Journal of Information Technology Theory and Application (JITTA)*, *19*(2), 57–88.

Warkentin, M., Goel, S., & Menard, P. (2017). Shared benefits and information privacy: What determines smart meter technology adoption? *Journal of the Association for Information Systems*, *18*(11), 758–786. https://doi.org/10.17705/1jais.00474

Weise, E. (2014). *JP morgan reveals data breach affected 76 million households*. USA Today. Retrieved from https://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403–414. https://doi.org/10.1057/palgrave.ejis.3000592

Yates, J. F., & Stone, E. R. (1992). Risk appraisal. In J. F. Yates (Ed.), *Risk-Taking behavior*. (pp. 49–85). New York: John Wiley.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., & Song, H. (2016). Where is current research on blockchain technology?—a systematic review. *PLoS ONE*, *11*(10), e0163477. Retrieved from. https://doi.org/10.1371/journal.pone.0163477

Yurieff, K. (2017). *Equifax data breach: What you need to know*. CNN Business. Retrieved from https://money.cnn.com/2017/09/08/technology/equifax-hack-qa/index.html

Zárate, M. A., Shaw, M., Marquez, J. A., & Biagas, D. (2012). Cultural inertia: The effects of cultural change on intergroup relations and the self-concept. *Journal of Experimental Social Psychology*, *48*(3), 634–645. https://doi.org/10.1016/j.jesp.2011.12.014

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for sns self-disclosure: The case of facebook. *Computers in Human Behavior*, *45*, 158–167. https://doi.org/10.1016/j.chb.2014.12.012

Appendix A: Summary of Prior Blockchain Research in IS

	Context	Method/Sample	Results
Ingold & Langer, (2021)	Comparing classical, social media, and blockchain resumes to determine if fraud is more prevalent in resume types	Between-subjects experiment; Senior and graduate students (n = 324)	Resume format had negligible effects on fraud, but novel formats made organisations less attractive to applicants
Mattke et al., (2021)	Motivations of Bitcoin investors	Qualitative (interviews) and quantitative (MTurk survey) analysis	Individuals are motivated by bitcoin ideology more than profit expectancy
Toufaily et al., (2021)	Developing an adoption framework borrowing concepts from DOI, TOE, Network externalities, adoption under uncertainty, institutional isomorphism	46 semi-structured qualitative interviews with private sector, public sector, and experts/entrepreneurs	Conceptual framework for blockchain adoption, including challenges and expected value across multiple sectors
Drummer & Neumann, (2020)	Examining the legal and technical adoption issues regarding smart contracts	Qualitative interviews w/ 30 domain experts	Identification of current shortcomings of smart contracts w/ potential remedies suggested
Renwick & Gleasure, (2020)	Boundary object perspective	Case study; interviews w/ users, developers, cryptographic researchers, corporate architects, and government regulators	Observed the tension between privacy protection and methods for overseeing typical transactions
Xie et al., (2020)	Network cohesion in social media discussion of Bitcoin	Web scraping of discussion content from Bitcointalk.org	Less cohesive social media discussion networks are better at predicting next-day returns than more cohesive networks
Ziolkowski et al., (2020)	Blockchain governance	Semi-structured interviews with representatives from organisations using blockchain systems; content analysis of grey literature	Identification of 4 key problems with governing blockchain-based systems
Andersen & Bogusz, (2019)	Forking into Self-Organised Blockchain Infrastructures originating from Bitcoin	Longitudinal multimethod design using forum data	Identification of self-organising forking patterns
Chanson et al., (2019)	Blockchain for privacy preservation in IoT	Proof of concept	Design theory for a blockchain-based sensor data protection system
Chong et al. (2019)	Using digital business models and value configuration to compare blockchain pioneers	Comparative case study of 5 business models in China	Typology of five blockchain-inspired business models
Du et al., (2019)	Affordance-Actualisation Theory	Case Study in Chinese conglomerate; structured interviews w/ employees	Insights into blockchain implementation in an organisation
Rossi et al., (2019)	Provides a framework for blockchain research in IS	multi-paradigmatic IS research agenda	Identifies issues of blockchain governance, human and material agency, blockchain affordances and constraints, as well as the consequences of its use
Yin et al., (2019)	Testing the actual anonymity provided by blockchain-based cryptocurrencies	Supervised ML analysing the transactions of 957 revealed entities (encompassing 385 million transactions)	ML model that can de-identify entity types by analysing blockchain transactions
Beck et al. (2018)	Decision rights, accountability, and incentives for decentralised autonomous organisations (DAOs)	Case study of a DAO	Governance for blockchain economy differs from traditional notions of governance; Proposal of novel framework for IT governance focused on blockchain
Bogusz & Morisse, (2018)	Open entrepreneurship and stigma associated with cryptocurrency	Case study using forum data, archival data, and interviews with Bitcoin entrepreneurs	Process model depicting ideologically-influenced stigma responses by open entrepreneurs
Gomber et al., (2018)	Fintech start-ups and their potential business models	Literature review	New mapping to identify how Fintech Innovation has affected four traditional financial areas
Gozman et al., (2018)	How information pathways influence the operation of financial services and markets	Cluster analysis of 402 fintech start-ups to determine representative fintech cases	Cluster classifications of fintech characteristics, identification of information flows in fintech markets, identification of value creation strategies
Kazan et al., (2018)	Strategic groups/Mobile payment platforms	Interpretive multiple case study of mobile payment market in UK	Taxonomy of mobile platform profiles based on value creation and value delivery dimensions
Mai et al. (2018)	The influence of social media discourse on Bitcoin value	Web scraping of discussion content from Bitcointalk.org	Social media effects on Bitcoin value are mostly driven by the 95% of users who are less active; messages on a forum have more impact than tweets

References

Andersen, J. V., & Bogusz, C. I. (2019). Self-Organiszing in blockchain infrastructures: generativity through shifting objectives and forking. *Journal of the Association for Information Systems, 20(9)*, 1242–1273. http://dx.doi.org/10.17705/1jais.00566

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: a framework and research agenda. *Journal of the Association for Information Systems, 19(10)*, 1020–1034. http://dx.doi.org/10.17705/1jais.00518

Bogusz, I. C., & Morisse, M. (2018). How infrastructures anchor open entrepreneurship: the case of bitcoin and stigma. *Information Systems Journal, 28(6)*, 1176–1212. https://doi.org/10.1111/isj.12204

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the iot: privacy-preserving protection of sensor data. *Journal of the Association for Information Systems, 20(9)*, 1271–1307. http://dx.doi.org/10.17705/1jais.00567

Chong, A. Y. L., Lim, E. T., Hua, X., Zheng, S., & Tan, C. W. (2019). Business on chain: a comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems, 20(9)*, 1310–1339. http://dx.doi.org/10.17705/1jais.00568

Drummer, D., & Neumann, D. (2020). Is code law? current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. *Journal of Information Technology, 35(4)*, 337–360. https://doi.org/10.1177%2F0268396220924669

Du, W. D., Pan, S. L., Leidner, D. E., & Ying, W. (2019). Affordances, experimentation and actualisation of fintech: a blockchain implementation study. *The Journal of Strategic Information Systems, 28(1)*, 50–65. https://doi.org/10.1016/j.jsis.2018.10.002

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems, 35(1)*, 220–265. http://dx.doi.org/10.1080/07421222.2018.1440766

Gozman, D., Liebenau, J., & Mangan, J. (2018). The innovation mechanisms of fintech start-ups: insights from swift's innotribe competition. *Journal of Management Information Systems, 35(1)*, 145–179. https://doi.org/10.1080/07421222.2018.1440768

Ingold, P. V, & Langer, M. (2021). Resume = resume? the effects of blockchain, social media, and classical resumes on resume fraud and applicant reactions to resumes. *Computers in Human Behavior, 114, 106573*. https://doi.org/10.1016/j.chb.2020.106573

Kazan, E., Tan, C.-W., Lim, E. T., & Sørensen, Carsten Damsgaard, J. (2018). Disentangling digital platform competition: the case of uk mobile payment platforms. *Journal of Management Information Systems, 35(1)*, 180–219. https://doi.org/10.1080/07421222.2018.1440772

Mai, F., Shan, Z., Bai, Q., Wang, X., & Chiang, R. H. (2018). How does social media impact bitcoin value? a test of the silent majority hypothesis. *Journal of Management Information Systems, 35(1)*, 19–52. https://doi.org/10.1080/07421222.2018.1440774

Mattke, J., Maier, C., Reis, L., & Weitzel, T. (2021). Bitcoin investment: a mixed methods study of investment motivations. *European Journal of Information Systems*, 30(3), 261–285. https://doi.org/10.1080/0960085X.2020.1787109

Renwick, R., & Gleasure, R. (2020). Those who control the code control the rules: how different perspectives of privacy are being written into the code of blockchain systems. *Journal of Information Technology, 36(1)*, 16–38. https://doi.org/10.1177%2F0268396220944406

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain research in information systems: current trends and an inclusive future research agenda. *Journal of the Association for Information Systems, 20(9)*. http://dx.doi.org/10.17705/1jais.00571

Toufaily, E., Zalan, T., & Dhaou, S. Ben. (2021). A framework of blockchain technology adoption: an investigation of challenges and expected value. *Information & Management, 58(3)*, 103444. https://doi.org/10.1016/j.im.2021.103444

Xie, P., Chen, H., & Hu, Y. J. (2020). Signal or noise in social media discussions: the role of network cohesion in predicting the bitcoin market. *Journal of Management Information Systems, 37(4)*, 933–956. https://doi.org/10.1080/07421222.2020.1831762

Yin, H. H. S., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrapu, R. (2019). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. Journal of Management Information Systems, 36(1), 37–73. https://doi.org/10.1080/07421222.2018.1550550

Ziolkowski, R., Miscione, G., & Schwabe, G.(2020). Decision problems in blockchain governance: old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems,37(2)*, 316–348. https://doi.org/10.1080/07421222.2020.1759974

Appendix B: Survey Instrument

Filter Question

Do you currently own any following of the following bank accounts? (Select all that apply).

Checking Account
Savings Account
Money Market Account
Certificate of Deposit (CD)
Individual Retirment Accounts (IRAs)
Other banking account not listed:
Do not own a bank account

Scenario

Your bank stores your bank account number and transaction history in a centralised database along with your personal information, such as name and social security number. Your bank is responsible for keeping the information in this centralised database private. Since the information in a centralised database is located, stored, and maintained in a single location, it is often a target for data breaches. Unauthorised access to your name and bank account number can result in fraudulent financial transactions.

Your bank has offered to move your bank account number and transaction history to a decentralised blockchain database. In a blockchain database, account holders are responsible for keeping their own personal information private. Your account number and transaction history are stored separately from your personal information. Account holders store their personal information, including a digital key necessary to initiate and authorise any financial transactions, on their own devices that are only accessible by the device owner. Account holders are identified in the blockchain only by account number that does not contain any personally identifying information. If anyone acquires a copy of the database and views the account numbers and account transactions stored in it, they cannot see any of your personal information. Without the digital key, unauthorised access to an account number cannot result in fraudulent financial transactions, thus reducing the likelihood that the blockchain will be a target for data breaches.

Survey Items

Construct	Adapted Item
Perceived Severity	SEV1: If my personal information were accessed by unauthorised entities, it would be significant. SEV2: If my personal information were accessed by unauthorised entities, it would be severe. SEV3: If my personal information were accessed by unauthorised entities, it would be serious. SEV4: If my personal information were compromised, it would be serious.
Perceived Susceptibility	SUS1: It is possible that my personal information stored by my bank will be accessed by unauthorised entities. SUS2: My personal information that is stored by my bank is at risk of being accessed by unauthorised entities. SUS3: My personal information that is stored by my bank is vulnerable to unauthorised access.
Inertia	**Inertia-Affective Based** IAB1: I will continue to have my bank account information stored on my bank's existing centralised database because it would be stressful to change. IAB2: I will continue to have my bank account information stored on my bank's existing centralised database because I am more comfortable doing so. IAB3: I will continue to have my bank account information stored on my bank's existing centralised database because I enjoy doing so. **Inertia-Behavioural Based** IBB1: I will continue to have my bank account information stored on my bank's existing centralised database simply because it is what I have always done. IBB2 I will continue to have my bank account information stored on my bank's existing centralised database simply because it is part of my normal routine. IBB3: I will continue to have my bank account information stored on my bank's existing centralised database simply because I've done so regularly in the past. **Inertia-Cognitive Based** ICB1: I will continue to have my bank account information stored on my bank's existing centralised database even though I know it is not the best way of doing things. ICB2: I will continue to have my bank account information stored on my bank's existing centralised database even though I know it is not the most efficient way of doing things. ICB2: I will continue to have my bank account information stored on my bank's existing centralised database even though I know it is not the most effective way to do things.
Privacy Concerns	PC1: I am concerned that the personal information I store on my bank's existing centralised database could be misused. PC2: I am concerned that a person can find private information about me on my bank's existing centralised database. PC3: I am concerned about storing personal information on my bank's existing centralised database, because of what others might do with it. PC4: I am concerned about storing personal information on my bank's existing centralised database, because it could be used in a way I did not foresee.
Awareness	AWR1: I follow news and developments about blockchain databases. AWR2: I discuss with friends and people around me about blockchain databases. AWR3: I read about blockchain databases in newsletters or articles. AWR4: I learn about blockchain databases on social media outlets or other websites. AWR5: I hear about blockchain databases on TV, podcasts or the radio.
Perceived Benefits	BEN1: Storing my bank account information in a blockchain database is effective in preventing unauthorised entities from tampering with my personal information. BEN2: Storing my bank account information in a blockchain database is effective in preventing unauthorised entities from accessing my personal information. BEN3: Storing my bank account information in a blockchain database eliminates the need for me to rely on my bank to protect my information. BEN4: Storing my bank account information in a blockchain database is effective in preventing unauthorised entities from using my personal information.
Intention	INT1: I am likely to switch to the blockchain-based bank account offered by my bank in order to protect my personal information. INT2: I could see myself switching to the blockchain-based bank account offered by my bank in order to protect my personal information. INT3: I intend to switch to the blockchain-based bank account offered by my bank in order to protect my personal information.
Blockchain Comprehension	After reading the scenario, how confident are you in explaining blockchain to someone who doesn't know about it? *Very Confident* *Confident* *Neither Confident nor Not Confident* *Not Confident* *Not at All Confident*