Spring 5-29-2021

The Role Of Privacy And Security Threats In The Adoption Of A Blockchain

Davit Marikyan
Newcastle University Business School, d.marikyan2@newcastle.ac.uk

Savvas Papagiannidis
Newcastle University Business School, savvas.papagiannidis@ncl.ac.uk

Omer Rana
Cardiff University, ranaof@cardiff.ac.uk

Rajiv Ranjan
Newcastle University, raj.ranjan@newcastle.ac.uk

Recommended Citation

Marikyan, Davit; Papagiannidis, Savvas; Rana, Omer; and Ranjan, Rajiv, "The Role Of Privacy And Security Threats In The Adoption Of A Blockchain" (2021). *UK Academy for Information Systems Conference Proceedings 2021*. 16.
https://aisel.aisnet.org/ukais2021/16

THE ROLE OF PRIVACY AND SECURITY THREATS IN THE ADOPTION OF A BLOCKCHAIN

Davit Marikyan
D.Marikyan2@newcastle.ac.uk
Newcastle University Business School, 5 Barrack Road, Newcastle Upon Tyne, UK, NE14SE

Savvas Papagiannidis
Savvas.Papagiannidis@ncl.ac.uk
Newcastle University Business School, 5 Barrack Road, Newcastle Upon Tyne, UK, NE14SE

Omer Rana
School of Computer Science and Informatics, Cardiff University, Cardiff CF24 3AA, UK
ranaof@cardiff.ac.uk

Rajiv Ranjan
Newcastle University, School of Computing, 1, Urban Sciences Building, Science Square, Newcastle Upon Tyne, NE4 5TG, UK
raj.ranjan@newcastle.ac.uk

Abstract: *The main focus of the blockchain literature has been on the technical capabilities of the technology in terms of data privacy and security enhancement. Such an approach has disregarded the individual's perception of potential threats in data exchange and the capabilities of a blockchain to eliminate them. To fill this gap this study aims to examine the cognitive factors determining the users' motivation to utilise blockchains as a means to protect oneself from privacy and security issues. This paper adopts the Protection Motivation Theory, which makes it possible to assess the role of threat and coping appraisal in relation to the adoption of the blockchain. We examined the effect of the factors using a sample of 506 respondents. The findings showed that threat vulnerability, response efficacy, response cost and self-efficacy determine adoption intention. Compared to threat appraisal, coping appraisal has a stronger effect on intention to use. The findings contribute to the understanding of the individual's perspective on blockchain adoption by focusing on cognitive factors. They can inform blockchain developers and marketers about aspects of individuals' behaviour that should be considered when developing and promoting the technology.*

Keywords: Protection Motivation Theory, Technology Adoption, Blockchain

1.0. Introduction

In adoption and acceptance studies, the underlying technologies considered are typically “black boxes”. For example, when it comes to electronic banking, users do not need to fully understand how security works. They are focused on the benefits and what the technology does as opposed to how it does it. There are often cases, though, where the underlying technologies form a significant part of the overall product or service offering. As a result, these technologies come to the foreground and are used as a differentiating factor that aims to encourage adoption. The blockchain is such a case. A blockchain is *“a technology which made it possible to build an immutable, distributed, always available, secure and publicly assessable repository of data (ledgers), which relies on a distributed consensus protocol to manage this repository (e.g., to decide what valid new data to include) in a distributed manner”* (Sankar et al., 2017). It is not a unified technology with predefined services, but an underlying technological block that enhances the security and privacy of digital transactions irrespective of the area of application (Hughes et al., 2019). The primary advantage of enhanced privacy and security characterises the blockchain as a privacy-preserving technology (Bauer et al., 2019). However, the technological complexity of blockchains raises challenges for users' understanding (de Leon et al., 2017). Typical users find it difficult to grasp its use cases, services and benefits, let alone the functionality of its infrastructural layer (Liu, 2021).

Given the above there is a research gap in the blockchain adoption literature. This concerns the lack of user insight into the utilisation of the technology, as the focus of the predominant stream of research is on technical components creating value in the digital exchange of data (Yang et al., 2019, Zheng et al., 2017). Given the security and privacy features of blockchains, the adoption of the technology can be regarded as a behaviour protecting oneself from the consequences of the privacy and security issues in digital transactions. Prior research has not examined the threat-related cognitions that play a pivotal role in protection motivation (Floyd et al., 2000). Given this gap, the objective of this paper is to explore cognitive factors, such as coping and threat appraisal, in line with the Protection Motivation Theory (PMT) to understand the role of privacy and security concerns in the adoption of blockchains. This theory helps explore the belief as to whether security/privacy threats might affect users and whether the use of blockchain-enabled applications can help avoid them.

The paper is structured as follows. First, the paper presents a literature review on blockchain technological factors, benefits and risks. The next section presents the theoretical background followed by the development of hypotheses, justifying the proposed relationship in the model. Then, the paper explains the methodology of the study, and proceeds with the results of the path analysis and a discussion of the findings. The paper concludes with a short summary of the study, it outlines limitations and makes suggestions for future research.

2.0. Literature review and Hypothesis Development

2.1. Blockchain

A blockchain is based on a distributed ledger, a cryptographic security protocol and a consensus mechanism (Beck et al., 2016). The distributed ledger ensures that the entry of new data creates a block that is not stored in a single location, but is continually copied and distributed to different nodes across the network, making it accessible and traceable by the participants of the network (Cuccuru, 2017, Lu and Xu, 2017, Aujla et al., 2020). Data forms a chain of sequentially created blocks, which are cryptographically protected, thus making the data immutable. That means that once the user has agreed to proceed with a transaction the record of it can never be altered (Lu and Xu, 2017). The data is controlled and validated by a centralised or decentralised consensus mechanism (Tönnissen and Teuteberg, 2020). The data immutability and the validation mechanism of the distributed system increase the trustworthiness of transactions and eliminate the need for intermediaries (Ying et al., 2018).

The degree of data accessibility, immutability, control and the openness of the blockchain for participants varies depending on the type of blockchain network, which can be public, private and consortium ones (Bauer et al., 2019, Zheng et al., 2017). A public blockchain is free for participation, making the network large in terms of the number of nodes. A large number of participants makes any attempt at data tampering more difficult. Data in the network is accessible for all actors and completely decentralised, which makes it uncontrollable by the organisation (Bauer et al., 2019, Zheng et al., 2017). Private and consortium blockchains are permissioned and can imply restrictions on data accessibility. The limited number of participants decreases the degree of data immutability. The networks are centralised or partially decentralised, which results in a central authority to control transactions (Zheng et al., 2017).

The features of the technology, namely disintermediation, accessibility, immutability, control and the openness of the blockchain, enable four types of benefits and risks, revolving around data transparency, privacy, security and system usage. The transparency and traceability inherent to blockchains give the public an opportunity to see the history of transactions, diminish the possibility of data misuse and boost the confidence in the quality of the services provided. For instance, the use of a blockchain in e-government services can eliminate potential fraud, data manipulation and corruption (Kshetri, 2017). The immutability, enhanced transparency and traceability of data have an equivocal effect on system security and the capability to preserve actors' privacy (Cuccuru, 2017, Janssen et al., 2020). On one hand, the distributed data exchange increases a system's resilience to withstand any potential cyber-attacks by allocating information to other nodes if one has been attacked, thus strengthening security (Atlam et al., 2018). On the other hand, blockchain technologies can be subjected to attacks, which can potentially lower the users' perception of privacy and the security of blockchain technologies (Yli-Huumo et al., 2016). In addition, blockchain networks enable users to see all records of transactions (Ahram et al., 2017). Although the actors are anonymous, some scholars argue that the transactions can be traced back to the users' IP address (Yli-Huumo et al., 2016).

Given the promised benefits and potential risks, the adoption of blockchain technologies could be a double-edged sword. It can make the transaction process automated, which eliminates the potential for human error (Cai and Zhu, 2016). It can also raise complexity due to the scalability challenge. With the increasing use of blockchain technologies, scalability becomes a big issue as the system faces difficulties coping with the increasing workload (Yli-Huumo et al., 2016). Hence, an understanding of blockchain functions requires sufficient technical knowledge. However, the general public has little awareness about the technology and how it works (Atlam et al., 2018). This does not help encourage adoption as users may not fully appreciate the benefits that such a technology can bring.

Given the lack of understanding of the users' perception of blockchain benefits and limited research on its adoption, further sections of this paper develop a research model aiming to explore whether individuals are willing to use a blockchain to protect themselves from privacy and security issues.

2.2. Research Models and Hypothesis Development

Utilising Protection Motivation Theory (PMT) can help address the gap in the literature related to the cognitive factors underpinning users' motivation to adopt the blockchain as a measure to avoid security and privacy issues. PMT has been used to examine individuals' motivation to switch behaviour as a means to protect oneself (Menard et al., 2017). The theory is rooted in the expectancy-value paradigm, which explains that individuals' behaviour change is driven by the expectancy that it will result in consequences. Fear of a potential threat incurred by the behaviour is the stimulus for actions that people undertake to avert a threat (Rogers and Prentice-Dunn, 1997, Rogers, 1983). Behaviour change reflects individuals' maladaptive and adaptive behaviour when facing threats. Adaptive behaviour refers to recommended activities that one should take to eliminate the threat, while maladaptive behaviour refers to the tendency to avoid the recommended activities (Menard et al., 2017). There are two sets of cognitive processes that predict maladaptive or adaptive behaviour, namely threat appraisal (threat severity and threat vulnerability) and coping appraisal (response efficacy, self-efficacy and response cost) (Rogers, 1983). When individuals face a threat, they cognitively evaluate the severity of that threat and their capability of confronting it (Menard et al., 2017). In this study, the use of Protection Motivation Theory makes it possible to examine the motivations to use blockchain-based services, representing a protective behaviour directed at ensuring the security and privacy of data.

The first construct related to threat appraisal is perceived threat vulnerability. This refers to the individual's assessment of the likelihood that threatening events might occur (Ifinedo, 2012). When it comes to the use of technology, threat may refer to financial losses, private data misuse or identity exposure in online transactions. PMT posits that there is a direct relationship between perceived vulnerability and behaviour (Chenoweth et al., 2009). The relationship has been confirmed empirically when examining IS security behaviour, such as compliance with IS security policies and the adoption of anti-spyware software (Ifinedo, 2012, Chenoweth et al., 2009, Lee, 2011). However, the significance of the effect was not consistent across different studies (Vance et al., 2012, Menard et al., 2017, Tsai et al., 2016). A potential explanation of the contradictory findings could be the context of the research. Users may think that particular types of threats are not likely to happen, even though they potentially exist (Vance et al., 2012). However, given the seriousness of the threats that blockchain technology is designed to tackle and evidence of frequent cyber-hacking cases, we assume that perceived vulnerability has a significant effect on intention to adopt blockchain-enabled services.

The second threat appraisal construct is perceived threat severity. This is defined as "*the degree of physical harm, psychological harm, social threats, economic harm, dangers to others rather than oneself, and even threats to other species which refers to the severity of the outcome or consequence of the event*" (Rogers and Prentice-Dunn, 1997). In IS management, the construct reflects the seriousness of the consequences of events, such as hackers' attacks and financial fraud. Perceived threat severity was found to have a significant role in motivating practices, such as energy-conservation, compliance with IS security policies, the adoption of antiplagiarism software (Lee, 2011, Ifinedo, 2012). The effect of the construct was not confirmed in some prior studies (Vance et al., 2012, Menard et al., 2017, Tsai et al., 2016), putting it down to methodological limitations (Vance et al., 2012) and the difference in settings (Tsai et al., 2016). It was suggested that in the organisational context, the losses that might potentially result from the use of technologies are borne by firms, rather than employees (Tsai et al., 2016). That is why individuals experience mild consequences. However, the refusal to use privacy-preserving technology entails personal threats, such as personal data misuse and the exposure of financial data. Hence, we assume that the relationship between perceived threat severity and adoption intention is significant. Given the above, we hypothesise:

Hypothesis 1: *a) Perceived threat vulnerability and b) perceived threat severity have a positive effect on intention to adopt blockchain-enabled services.*

Coping appraisal processes are dependent on response efficacy, self-efficacy and response cost. Response efficacy refers to the individual's belief that adaptive behaviour will avert a threat (Lee, 2011). Given prior studies in the IS domain confirming the role of response efficacy in technology use (Chenoweth et al., 2009, Menard et al., 2017) and evidence about the security and privacy benefits of blockchains (Cuccuru, 2017, Janssen et al., 2020), we expect that individuals consider the technology to be helpful in protecting personal data from unauthorised use by other parties. Having evaluated potential threat, individuals perform a cognitive assessment of available opportunities to deal with the threat. If they think that adaptive behaviour will increase their chances of confronting the threat, the intention to adopt will also increase. Self-efficacy refers to individuals' belief that they are capable of undertaking effective measures intended to cope with the threat (Woon et al., 2005). The confidence in personal capabilities increases the intention to embark on adaptive behaviour (Rogers and Prentice-Dunn, 1997), such as the adoption of blockchain-enabled services. The correlation between self-efficacy and behaviour change has been examined in research on psychology (Bandura et al., 1980) and confirmed in the IS stream (Chenoweth et al., 2009, Menard et al., 2017, Tsai et al., 2016). Self-efficacy indirectly and directly affects intention to engage in activities, such as email authentication, the use of software and fake-website detection systems (Johnston and Warkentin, 2010). Response cost refers to the individuals' evaluation of the costs that they bear if they choose to engage in adaptive behaviour (Tsai et al., 2016). The costs can be financial investments or mental efforts that one might need to put in to operate blockchain-enabled services. The higher the response cost the lower is the intention to engage in the behaviour (Menard et al., 2017). Despite the theoretical foundation and supporting results of prior studies (Chenoweth et al., 2009, Lee, 2011), a negative effect of response cost on intention was not always the case (Ifinedo, 2012, Vance et al., 2012, Menard et al., 2017). An insignificant effect was mostly found in the research exploring the utilisation of technology in workplace settings. Drawing on this observation, the role of the construct could be non-significant when organisations deal with financial costs and assign specialised units to implement technologies for employees (Ifinedo, 2012, Vance et al., 2012, Menard et al., 2017). Therefore, individuals cannot objectively quantify the costs that adaptive behaviour might entail. However, when it comes to blockchain-based applications, the consequences of maladaptive behaviour have a direct impact on users, which outweighs the costs. That means that in the context of this study the effect of response cost is most likely to be negative. Given the above arguments, we suggest that:

Hypothesis 2: *a) Perceived response efficacy and b) perceived self-efficacy have a positive effect, while c) perceived response cost has a negative effect on intention to adopt blockchain-enabled services.*

3.0. Methodology

3.1. Data collection and Measurements

A survey was used as a data collection tool. The first part of the questionnaire introduced the aim of this study and included the consent form. In the second part of the questionnaire, the respondents were given the scenario of the potential use case and services of a blockchain-based application in the context of shopping. That scenario enabled respondents to relate personal experience to the particular hypothetical case. The respondents were asked to consider a case in which they were the users of a free digital wallet app. The services that the app provides and the ways in which personal data processed through the app is treated were outlined. Then, they were introduced to an alternative version of the app that was based on a blockchain. Respondents were informed about additional services that the blockchain technology could enable with regards to personal data storage and usage. The third part contained questions about coping and threat appraisal factors predicting the motivation for a protective behaviour. The last section of the survey included questions about socio-demographic characteristics and technology usage patterns. Using an independent research company, we collected 506 valid responses (Table 1).

Demographic Characteristics	**Type**	**Frequency (n = 506)**	**Percentage**
Age	18 to 24 years	91	18
	25 to 34 years	164	32.4
	35 to 44 years	163	32.2
	45 to 54 years	49	9.7
	55 to 64 years	24	4.7
	65 or above	15	3
Gender	Male	313	61.7
	Female	195	38.3
Education	Completed some high school	122	24.1
	Completed some college (GSCE/AS/A-Level)	122	24.1
	Bachelor's degree	183	36.1
	Master's degree	64	12.6
	Ph.D.	11	2.2

	Other degree beyond a Master's degree	4	0.8
Income	Less than £25,000	180	35.5
	£25,000 to £34,999	115	22.7
	£35,000 to £49,999	82	16.2
	£50,000 to £74,999	61	12
	£75,000 to £99,999	36	7.1
	£100,000 to £149,999	17	3.4
	£150,000 to £199,999	10	2
	£200,000 or more	5	1

Table 1: The profile of the respondents

All measurements were adopted from prior studies (Tables 2). All the items were measured using a 7-point Likert scale.

Measurement item - Protection motivation theory	**α**
Perceived threat severity (Johnston and Warkentin, 2010, Ifinedo, 2012)	0.895
Perceived threat vulnerability (Johnston and Warkentin, 2010, Ifinedo, 2012)	0.860
Response efficacy (Vance et al., 2012)	0.933
Self-efficacy (Woon et al., 2005)	0.854
Response cost (Woon et al., 2005)	0.813
Intention to Use (Venkatesh et al., 2012)	0.937

Table 2: Measurement items

3.2. Data Analysis

SPSS statistical software was employed for analysing the collected data. A descriptive statistical analysis was performed to summarise the demographic profile of the respondents. Prior to embarking on the analysis of the relationships between the independent and dependent variables, we tested the reliability of the scales using Cronbach Alpha coefficients and factor loadings (Table 2). All the scales had satisfactory reliability with factors loadings above 0.4, which is the required cut-off criterion (Bonett and Wright, 2015). Table 3 presents the mean, standard deviation and correlation coefficients for the research model. To analyse the association of the predictors with the intention to adopt technology, multiple linear regression analysis was employed.

Constructs	**Mean**	**S.D.**	**Correlations**					
			1	**2**	**3**	**4**	**5**	**6**
1 Perceived threat severity	6.213	0.844	1					
2 Perceived threat vulnerability	4.325	1.057	0.057	1				
3 Response efficacy	5.108	1.114	.301**	.591**	1			
4 Self-efficacy	4.792	1.196	.186**	.467**	.548**	1		
5 Response cost	4.262	1.093	-0.022	-0.054	-.151**	-.277**	1	
6 Intention to use	4.615	1.424	.230**	.425**	.590**	.497**	-.230**	1

Note: The significance of the results is at the levels of p=0.05 (*), p=0.01 (**) and p=0.001 (***).

Table 3: Mean, Standard Deviation and Correlation Coefficients

4.0. Results and Discussion

The results of the multiple regressions are provided in Table 4. The research model explained 40% of the variance (R^2=0.402) for intention to use. Four out of the five hypothesised paths were found to be significant. Although the relationship between perceived threat severity and intention to use was non-significant (H1b), the positive effect of threat vulnerability on intention was confirmed (H1a). Response efficacy and self-efficacy were found to have a positive influence on intention (H1a, H1b), while the effect of response cost on intention to use was confirmed to be negative (H1c).

Path	*Std. Beta*	t-value	p-value
Perceived Threat Vulnerability → Intention to use	0.093	2.096	*
Perceived Threat Severity → Intention to use	0.068	1.869	ns
Response Efficacy → Intention to use	0.39	8.08	***
Self-efficacy → Intention to use	0.196	4.508	***
Response Cost → Intention to use	-0.11	-3.057	**

Note: The significance of the results is at the levels of p=0.05 (*), p=0.01 (**) and p=0.001 (***).

Table 4: Regression results

4.1. Elaboration of Findings

The positive effect of threat vulnerability on intuition is in line with the Protection Motivation Theory (Rogers and Prentice-Dunn, 1997, Rogers and Mewborn, 1976). The significance of the tested relationship confirms that individuals' fear of being affected by cyber-security issues increases the likelihood of using blockchain-based services to avoid such threats. The non-supported hypothesised relationship between perceived threat severity and intention contradicts the principles of PMT (Rogers and Prentice-Dunn, 1997, Rogers and Mewborn, 1976). However, it is consistent with prior studies that found that threat severity did not play a role in motivating people towards security compliance (Menard et al., 2017, Tsai et al., 2016, Ifinedo, 2012). The potential interpretation of the effects of the two appraisal factors offers evidence that while the security/privacy threat may have a direct impact on technology users, the consequences of the threat can be easily eliminated or experienced to a small extent. For instance, users may think that due to the limit on the relatively small amount of money passing through digital wallets, the risk of financial losses is low. Also, they may think that in the case of cyber-attacks incurring financial losses, service providers or banks can refund any losses.

When it came to the coping appraisal factors, response efficacy was found to have a positive effect. This finding indicates the existence of strong beliefs that blockchain-based services will help avoid cyber-threats as promised by the developers of the technology (Osmani et al., 2020, Barati and Rana, 2019). The dependence of intention on self-efficacy is expected, given the evidence of prior research (Chenoweth et al., 2009, Lee, 2011, Woon et al., 2005). Since technology is embedded in all aspects of life people believe that they have enough skills to operate technology and realise its potential. The negative effect of response cost was also in line with the research confirming that people are not ready to embark on the usage of technology if they bear any costs (Chenoweth et al., 2009, Lee, 2011, Rogers, 1983). In the context of this research, the finding suggests that the potential monetary losses, physical effort and time that individuals might spend switching to blockchain-based services overshadow the values of the application, thus inhibiting its adoption.

4.2. Theoretical and Practical Contributions

This study contributes to the blockchain and technology acceptance literature. Firstly, the existing blockchain literature mostly focuses on technical aspects of the technology (Lu and Xu, 2017, Barati and Rana, 2019, Zheng et al., 2017), lacking insight into the user perspective on technology utilisation and adoption. While the benefits of blockchains for users have triggered a massive interest in the technology (Atlam et al., 2018, Janssen et al., 2020), the psychological and cognitive factors underlying the use have been under-researched. Few papers examining users' attitudes to blockchains provide contextual insight. For example, researchers have explored the users' perception of Bitcoin (Alshamsi and Andras, 2019), the traceability function of blockchain-based supply systems in Indonesia (Asfarian et al., 2020), and privacy and trust (Shin, 2019). Secondly, the findings move forward the research on the adoption of blockchains by exploring the cognitive factors that correlate with the intention to use technology. The strongest cognitive factor underpinning intention was found to be response efficacy, indicating the importance of the belief that blockchain-based services will be effective in coping with cyber-threats, as promised. The findings represent the first empirical evidence on the potential predictors of the adoption of blockchain-based services.

From the practical viewpoint, the findings of this paper provide implications for the user-centric development and promotion of a blockchain. The results demonstrated that individuals perceive the consequences of the threat to be non-severe. This could potentially be the case as they take the security and privacy aspects for granted. Hence, they may not pay the expected attention to how these are achieved. The evidence about the significant effects of the coping appraisal factors (response efficacy, self-efficacy and response cost) also have a practical value. To attenuate the effect of response cost on the intention to use blockchain-enabled services, the investment in blockchain adoption should be justified. Hence, marketers could convey the long-term consequences of security and privacy errors.

5.0. Conclusion and Future Research Suggestions

The objective of this paper was to examine cognitive factors, in line with the Protection Motivation Theory. The results showed that four out of five factors have significant effects on use intention. The coping factors explain the greater variance for the dependent variable, with response efficacy and self-efficacy having the strongest effects on the intention to use.

This study provides directions for future research. On one hand, due to the selected research design, this study has limitations that future research could build upon. First, respondents were provided with the hypothetical scenario of using a blockchain-enabled application while shopping. The context of the study may create boundary conditions. Therefore, future research needs to examine adoption intention using other types of blockchain-based applications to compare the strength of the predictors. Second, while this study provides quantitative evidence about the determinants of adoption, future research could qualitatively explore users' experiences and perceptions in relation to blockchain utilisation. A qualitative approach could move the blockchain adoption research in several ways. Although this study statistically confirmed the significant role of the factors in adoption intention, future studies could provide a richer insight into the reasons as to why certain attitudes and beliefs were formed.

Reference List

AHRAM, T., SARGOLZAEI, A., SARGOLZAEI, S., DANIELS, J. & AMABA, B. Blockchain technology innovations. 2017 IEEE technology & engineering management conference (TEMSCON), 2017. IEEE, 137-141.

ALSHAMSI, A. & ANDRAS, P. 2019. User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies,* 126**,** 94-110.

ASFARIAN, A., HILMI, K. I. & HERMADI, I. Preliminary User Studies on Consumer Perception Towards Blockchain-Based Livestock Traceability Platform in Indonesia: An Implication to Design. 2020 International Conference on Computer Science and Its Application in Agriculture (ICOSICA), 2020. IEEE, 1-6.

ATLAM, H. F., ALENEZI, A., ALASSAFI, M. O. & WILLS, G. 2018. Blockchain with internet of things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems and Applications,* 10**,** 40-48.

AUJLA, G. S., BARATI, M., RANA, O., DUSTDAR, S., NOOR, A., LLANOS, J. T., CARR, M., MARIKYAN, D., PAPAGIANNIDIS, S. & RANJAN, R. 2020. COM-PACE: Compliance-Aware Cloud Application Engineering Using Blockchain. *IEEE Internet Computing,* 24**,** 45-53.

BANDURA, A., ADAMS, N. E., HARDY, A. B. & HOWELLS, G. N. 1980. Tests of the generality of self-efficacy theory. *Cognitive Therapy and Research,* 4**,** 39-66.

BARATI, M. & RANA, O. Enhancing User Privacy in IoT: Integration of GDPR and Blockchain. International Conference on Blockchain and Trustworthy Systems, 2019. Springer, 322-335.

BAUER, I., ZAVOLOKINA, L., LEISIBACH, F. & SCHWABE, G. Exploring blockchain value creation: the case of the car ecosystem. Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019.

BECK, R., STENUM CZEPLUCH, J., LOLLIKE, N. & MALONE, S. 2016. Blockchain–the gateway to trust-free cryptographic transactions.

BONETT, D. G. & WRIGHT, T. A. 2015. Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior,* 36**,** 3-15.

CAI, Y. & ZHU, D. 2016. Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation,* 2**,** 20.

CHENOWETH, T., MINCH, R. & GATTIKER, T. Application of protection motivation theory to adoption of protective technologies. 2009 42nd Hawaii International Conference on System Sciences, 2009. IEEE, 1-10.

CUCCURU, P. 2017. Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology,* 25**,** 179-195.

DE LEON, D. C., STALICK, A. Q., JILLEPALLI, A. A., HANEY, M. A. & SHELDON, F. T. 2017. Blockchain: properties and misconceptions. *Asia Pacific Journal of Innovation and Entrepreneurship*.

FLOYD, D. L., PRENTICE-DUNN, S. & ROGERS, R. W. 2000. A meta-analysis of research on protection motivation theory. *Journal of applied social psychology,* 30**,** 407-429.

HUGHES, L., DWIVEDI, Y. K., MISRA, S. K., RANA, N. P., RAGHAVAN, V. & AKELLA, V. 2019. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management,* 49**,** 114-129.

IFINEDO, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security,* 31**,** 83-95.

JANSSEN, M., WEERAKKODY, V., ISMAGILOVA, E., SIVARAJAH, U. & IRANI, Z. 2020. A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management,* 50**,** 302-309.

JOHNSTON, A. C. & WARKENTIN, M. 2010. Fear appeals and information security behaviors: an empirical study. *MIS quarterly***,** 549-566.

KSHETRI, N. 2017. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy,* 41**,** 1027-1038.

LEE, Y. 2011. Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems,* 50**,** 361-369.

LIU, S. 2021. *Share of individuals who have heard about blockchain in Italy 2019, by context* [Online]. Statista. Available: https://www.statista.com/statistics/1065809/awareness-of-blockchain-population-in-italy/ [Accessed].

LU, Q. & XU, X. 2017. Adaptable blockchain-based systems: A case study for product traceability. *IEEE Software,* 34**,** 21-27.

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**,** 1203-1230.

OSMANI, M., EL-HADDADEH, R., HINDI, N., JANSSEN, M. & WEERAKKODY, V. 2020. Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. *Journal of Enterprise Information Management*.

ROGERS, R. W. 1983. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook***,** 153-176.

ROGERS, R. W. & MEWBORN, C. R. 1976. Fear appeals and attitude change: effects of a threat's noxiousness, probability of occurrence, and the efficacy of coping responses. *Journal of personality and social psychology,* 34**,** 54.

ROGERS, R. W. & PRENTICE-DUNN, S. 1997. Protection motivation theory.

SANKAR, L. S., SINDHU, M. & SETHUMADHAVAN, M. Survey of consensus protocols on blockchain applications. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017. IEEE, 1-5.

SHIN, D. D. 2019. Blockchain: The emerging technology of digital trust. *Telematics and Informatics,* 45**,** 101278.

TÖNNISSEN, S. & TEUTEBERG, F. 2020. Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies. *International Journal of Information Management,* 52**,** 101953.

TSAI, H.-Y. S., JIANG, M., ALHABASH, S., LAROSE, R., RIFON, N. J. & COTTEN, S. R. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security,* 59**,** 138-150.

VANCE, A., SIPONEN, M. & PAHNILA, S. 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management,* 49**,** 190-198.

VENKATESH, V., THONG, J. Y. & XU, X. 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly***,** 157-178.

WOON, I., TAN, G.-W. & LOW, R. 2005. A protection motivation theory approach to home wireless security. *ICIS 2005 proceedings***,** 31.

YANG, W., AGHASIAN, E., GARG, S., HERBERT, D., DISIUTA, L. & KANG, B. 2019. A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future. *IEEE Access,* 7**,** 75845-75872.

YING, W., JIA, S. & DU, W. 2018. Digital enablement of blockchain: Evidence from HNA group. *International Journal of Information Management,* 39**,** 1-4.

YLI-HUUMO, J., KO, D., CHOI, S., PARK, S. & SMOLANDER, K. 2016. Where is current research on blockchain technology?—a systematic review. *PloS one,* 11**,** e0163477.

ZHENG, Z., XIE, S., DAI, H., CHEN, X. & WANG, H. An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE international congress on big data (BigData congress), 2017. IEEE, 557-564.