Computers in Human Behavior 131 (2022) 107207

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Blockchain adoption: A study of cognitive factors underpinning decision making[☆]

Davit Marikyan [a,*], Savvas Papagiannidis [b], Omer F. Rana [c], Rajiv Ranjan [d]

[a] School of Management, University of Bristol, Queens Road Bristol, BS8 1QU, UK
[b] Newcastle University Business School, 5 Barrack Road, Newcastle Upon Tyne, NE1 4SE, United Kingdom
[c] School of Computer Science and Informatics, Cardiff University, Cardiff, CF24 3AA, UK
[d] Newcastle University, School of Computing, 1, Urban Sciences Building, Science Square, Newcastle Upon Tyne, NE4 5TG, UK

ARTICLE INFO

Keywords:
Blockchain
Technology adoption
Protection motivation theory

ABSTRACT

The literature so far has been focused on technological sophistication rather than the aspects of blockchain adoption that can hinder or facilitate the use of the technology. To address this gap this paper aims to study the cognitive factors underpinning adoption decision-making moderated by user characteristics. Using a cross-sectional research design, the study recruited 506 respondents to participate and test the relationships hypothesised in the research model. The results of the analysis demonstrated that perceived threat vulnerability, response cost, response efficacy and self-efficacy determine adoption intention. These factors have varying effects on intention depending on users' subjective knowledge, objective knowledge and innovativeness. This evidence contributes to the understanding of users' perspectives on blockchain adoption, which has been under-researched so far. The findings shed light on the cognitive factors motivating blockchain-based technology use and the individual characteristics of users who are likely to adopt the technology in the context of data privacy and security. In turn, these findings can inform practitioners about the aspects of user behaviour that should be considered while developing and marketing the technology.

1. 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; Kavanagh & Ennis, 2020). The primary advantage of enhanced privacy and security characterise the blockchain as a privacy-preserving technology (Centobelli et al., 2021; Mora et al., 2021; Warkentin & Orgeron, 2020). However, the technological complexity of the blockchain raises challenges for users' understanding (De Leon et al., 2017; Sahebi et al., 2020). Typical users find it difficult to grasp its use cases, services and benefits, let alone the functionality of its infrastructural layer (Ingold & Langer, 2021; Liu, 2021; Pleger et al., 2021).

Given the above, there is a gap in the current literature focusing on blockchain utilisation. Specifically, there is a lack of insight into the factors explaining users' perceptions of the services and applications enabled by blockchains. 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). Only a few papers have adopted a user-centric approach, such as users' perception of cryptocurrency (Albayati et al., 2020; Salcedo & Gupta, 2021), the traceability feature (Asfarian et al., 2020), privacy and trust (Kowalski et al., 2021; Shin, 2019). There is, as yet, no evidence about the

[☆] The intention to use blockchain-enabled services are moderated by subjective knowledge, objective knowledge and innovativeness.

[*] Corresponding author. School of Management, University of Bristol, Queens Road Bristol, BS8 1QU, UK.
E-mail address: davit.marikyan@bristol.ac.uk (D. Marikyan).

https://doi.org/10.1016/j.chb.2022.107207
Received 16 October 2021; Received in revised form 12 January 2022; Accepted 20 January 2022
Available online 24 January 2022

psychological and cognitive factors underpinning users' decision making when it comes to the use of the technology preserving users' data privacy. The lack of individuals' understanding as to how blockchain-based applications and services can ensure personal data privacy and security reduces their perceived benefits and the public's willingness to adopt them. Hence, it is important to gain an insight into the cognitive factors underpinning the adoption of such technological "black boxes". This is especially true considering that blockchain technology as a building block has been increasingly utilised to enable technologies in different domains (Hughes et al., 2019; Kavanagh & Ennis, 2020). Due to 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 data exchange. In such use cases, threat-related cognitions, associated with the evaluation of the benefits and costs of adopting technology, could potentially play a pivotal role in protection motivation (Culnan & Armstrong, 1999; Floyd et al., 2000). When it comes to the evaluation of risks and personal capabilities, individuals' knowledge and predisposition to adopt new technologies could explain the variance in behavioural intention (Newell et al., 2000; Rogers, 2010). Knowledge is especially important when assessing the rationale for switching to protective behaviour, which is dependent on weighing privacy risks against the benefits of existing behaviour (Awad & Krishnan, 2006; Culnan & Armstrong, 1999; Dinev & Hart, 2006). This assumption about the significant role of knowledge originates from prior studies. These suggested that knowledge and awareness of the consequences of security protection measures significantly affect the perception of the coping and threat appraisal factors, facilitating or inhibiting the motivation to engage in adaptive behaviour (Liang & Xue, 2010; Torten et al., 2018). Therefore, to understand potential differences related to the effect of cognitive appraisal factors among people, their knowledge and innovativeness need to be taken into consideration.

In order to make a contribution towards addressing the above gaps, this study sets out to examine blockchain adoption from the users' perspective. As a first step, the study aims to explore the motivational role of cognitive factors, such as coping and threat appraisal, in the intention to adopt a blockchain. For that purpose, the study adopts the Protection Motivation Theory (PMT), which has been confirmed to be robust in explaining switching behaviour in online and technology-mediated environments as a measure to protect oneself from unfavourable consequences (Elhai et al., 2017; Jansen & Van Schaik, 2018; Menard et al., 2017). PMT helps explore the belief as to whether security/privacy threats can affect individuals' decision making and whether users perceive blockchain-enabled applications as being able to help avoid those threats. As a second step, the study tests the moderating role of knowledge and innovativeness in technology adoption. This approach helps explore the variance in the effects of PMT variables on behavioural intention depending on the degree of users' objective and subjective knowledge and innovativeness.

The paper is structured as follows. First, the paper presents a literature review on blockchain technological factors, benefits and risks. The next two sections present theoretical frameworks 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 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. Literature review and hypothesis development

2.1. Blockchain adoption

A blockchain is based on a distributed ledger, a cryptographic security protocol and a consensus mechanism (Aujla et al., 2020; 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 continually copied and distributed to different nodes across the network, making it accessible and traceable by the participants of the network (Cuccuru, 2017; Lu & Xu, 2017). Data forms a chain of sequentially created blocks, which are cryptographically protected, thus making data immutable. That means that once the user has agreed to proceed with a transaction, the record of it can never be altered (Atlam & Wills, 2019; Lu & Xu, 2017). The data is controlled and validated by a centralised or decentralised consensus mechanism (Tönnissen & Teuteberg, 2020). The data immutability and the validation mechanism of the distributed system increase the trustworthiness of transactions and eliminate the need for intermediaries (De Filippi et al., 2020; 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; Marikyan et al., 2021; Morkunas 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 lowers the degree of data immutability. The networks are centralised or partially decentralised, which gives a central authority to control transactions (Zheng et al., 2017).

The features of the technology, namely disintermediation, accessibility, immutability and control over the blockchain, enable benefits but also create risks revolving around data transparency, privacy, security and system usage. Due to the accessibility of blockchains to the public, the transactions become transparent and traceable. This gives the public an opportunity to see the history of data exchange, control transactions by lowering the possibility of data misuse and boosts confidence in the quality of the services provided. The immutability, enhanced transparency and traceability of data bring benefits in terms of system security and the capability to preserve actors' privacy (Cuccuru, 2017; Janssen et al., 2020). Specifically, the distributed data exchange increases a system's ability to withstand any potential cyber-attack by allocating information to other nodes if one has been attacked, thus strengthening security (Atlam et al., 2018; Dubey et al., 2020). The use of a blockchain in e-government services can eliminate potential fraud, data manipulation and corruption (Kshetri, 2017). On the other hand, the traceability and transparency of transactions could raise concerns, as 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). Also, the deployment of blockchain technologies can result in overhead costs required to maintain operational complexity enabling anonymous participation for users (Anderson et al., 2016; Kiayias et al., 2017; Notheisen et al., 2017). The operational complexity, in turn, may cause a decrease in transaction throughput and latency (Notheisen et al., 2017).

From the privacy calculus perspective, the decision to adopt such a technology can be the result of the evaluation of the trade-off between risks and benefits. Such a perspective suggests that privacy decisions are inhibited by perceived risks and facilitated by perceived benefits (Awad & Krishnan, 2006; Culnan & Armstrong, 1999; Dinev & Hart, 2006). The evaluation of the consequences of technology use requires a knowledge of the system, which may bring benefits or cause privacy risks (Liang & Xue, 2010; Torten et al., 2018). For example, the decision to adopt blockchain-based applications can be dependent on whether the risk of personal data mistreatment outweighs the financial and operational costs associated with the use of technology. However, due to the technical complexity of blockchains, 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.

Drawing on the technology adoption literature, a number of theoretical frameworks have been used to explain the perceived antecedents of motivation when it comes to technology in relation to security and privacy risks. Researchers tested the factors that were pertinent to individual-specific constraints or facilitators of behavioural motivation (Herath & Rao, 2009; Ifinedo, 2012; Menard et al., 2017). For example, the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB) and Self-determination Theory have been used to study the role of personal capabilities and needs (e.g. competence, behavioural control, relatedness) that are important for engaging in security-compliant behaviour (Herath & Rao, 2009; Ifinedo, 2012; Menard et al., 2017). Other studies drew on the factors that matter in strengthening security compliance, such as appeals to fear and concerns that can trigger individuals' withdrawal from the threat-inducing behaviour (Mcleod & Dolezel, 2021; Featherman & Pavlou, 2003). For example, Security Capitulation Theory considers the feeling of threat inevitability triggered by privacy, vulnerability and security issues, leading to behavioural withdrawal (Mcleod & Dolezel, 2020; Mcleod & Dolezel, 2021). Perceived Risk Theory distinguishes the facets of the risks, such as psychological, financial, performance, privacy and time, that hinder technology adoption (Featherman & Pavlou, 2003). Although the above theories are robust in predicting the risks, associated emotions and individual needs and abilities, they do not explain the cognitive mechanisms that underpin individuals' approach behaviour. The understanding of coping and threat appraisal is important when examining motivations to undertake certain actions, as motivations can result from the evaluation of the perceived benefits of actions relative to the costs of carrying out such actions.

The research on protective behaviour from the cognitive perspective shows the application of the theory on coping mechanisms developed by Lazarus and Folkman (1984). The theory made it possible to study the role of emotions and cognitive techniques that downplay or strengthen the perception of threat underpinning security compliance (D'Arcy et al., 2009). Also, researchers used Technology Threat Avoidance Theory (TTAT), which stems from PMT and focuses on cognitive appraisal factors that facilitate behavioural avoidance (Liang and Xue, 2009, 2010). However, TTAT was developed to investigate the cognitive mechanisms underpinning the avoidance of malicious technology rather than the adoption of security safeguarding systems. The cognitive mechanisms underpinning approach and avoidance behaviour are different in relation to the goal direction. Approach cognition implies that individuals undertake behaviour pushing them towards the desired end state. Avoidance cognition means that individuals move away from the harmful present state without a clear understanding of a desired end state (Liang & Xue, 2009). In contrast, Protection Motivation Theory (PMT) has been used to examine individuals' approach motivation resulting from the evaluation of privacy security threats and the activities required to cope with them (Elhai et al., 2017; Jansen & Van Schaik, 2018; Menard et al., 2017). Rather than focusing on the triggers and enablers of behaviour (i.e. emotions, perceived risks, individual abilities), the use of PMT can shed light on the mechanisms of the assessment of risks, costs and benefits. Such knowledge can help address the gap in the literature related to the lack of research on the appraisal factors motivating the adoption of blockchains as a measure to avoid security and privacy issues.

The next section of the paper discusses the principles and the core factors of PMT, underpinning the research model developed in this study. The section provides the justification for hypothesising the relationships between the cognitive factors and the motivations to adopt services enabled by blockchains as an adaptive behaviour directed at ensuring the privacy and security of personal data.

2.2. Research model and hypothesis development

2.2.1. Cognitive factors

PMT is rooted in the expectancy-value paradigm, which maintains 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 to avert a threat (Rogers & 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).

The first cognitive factor related to threat appraisal is perceived threat vulnerability. This refers to the individuals' 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 information systems security behaviour, such as compliance with policies and the adoption of anti-spyware software (Chenoweth et al., 2009; Ifinedo, 2012; Lee, 2011). However, the significance of the effect was not consistent across different studies (Menard et al., 2017; Tsai et al., 2016; Vance et al., 2012). A potential explanation of the contradictory findings could be the context of the research. The studies mostly focus on the threats resulting from the use of technology that can be partly controlled by users (Menard et al., 2017; Tsai et al., 2016; Vance et al., 2012). Individuals may think that particular types of threats are not likely to happen, even though they potentially exist (Vance et al., 2012). When it comes to the current study, the threat is associated with the misuse of data by third parties, who can be difficult or impossible to control unless privacy-preservation technology, such as a blockchain, is used. Given the seriousness of the threats that blockchain technology is designed to tackle and evidence of frequent cyber-hacking cases, we expect perceived vulnerability to have 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 & Prentice-Dunn, 1997). In information systems 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 security policies, and the adoption of antiplagiarism software (Ifinedo, 2012; Lee, 2011). Consequently, we assume that when it comes to blockchain adoption, the role of threat severity will be significant in motivating adoption. This may be especially the case considering that the use of privacy-preserving technology is induced by the risk that third parties may get hold of personal data and treat it inappropriately. Such consequences are beyond one's own control. In contrast, when individuals have a high degree of control over the behaviour and are aware of the threats and personal efficacy in relation to protective measures, the effect of threat severity may play a relatively less important role (Hanus & Wu, 2016; Menard et al., 2017; Tsai et al., 2016). In such situations, the perception of the coping efficiency could attenuate the effect of threat severity on the intention to undertake security measures (Tsai et al., 2016). 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). Prior studies have confirmed the role of response efficacy in technology use by demonstrating the positive relationship between the evaluation of the effectiveness of protective measures and intention to switch behaviour (Chenoweth et al., 2009; Menard et al., 2017). Given such findings and the 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. 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 & 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 literature (Chenoweth et al., 2009; Menard et al., 2017; Tsai et al., 2016). Self-efficacy directly and indirectly affects intention to engage in activities, such as email authentication, the use of software and fake-website detection systems (Herath & Rao, 2009; Johnston & Warkentin, 2010). Therefore, it is expected that personal capability of carrying out protective behaviours will correlate with the intention to adopt blockchain-based applications.

Response cost refers to the evaluation of the costs that users will have to bear if they choose to engage in adaptive behaviour (Tsai et al., 2016). 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). For example, it was found that the perception of the costs associated with the installation of anti-spyware software lowered the intention to use the software (Chenoweth et al., 2009). Similarly, the strengthened perception of monetary, time and effort input into the use of anti-plagiarism software diminishes the intention to adopt the software (Lee, 2011). Despite the above (Chenoweth et al., 2009; Lee, 2011), the inhibiting role of response cost on behaviour may vary depending on the context (Hanus & Wu, 2016; Ifinedo, 2012; Menard et al., 2017). For example, in the workplace, the adoption of technology by employees may not be affected by the consideration of the amount of resources that they expected to spend on the behaviour (Ifinedo, 2012). Employees may not care much about costs, as organisations deal with financial expenses and have professionals who can implement technologies for employees (Ifinedo, 2012). For employees, it might be difficult to objectively quantify the costs that adaptive behaviour might entail, because security and privacy-preserving features are often built into technology (e.g. firewalls, data back-up solutions, spyware software) and are available at low or no cost (Hanus & Wu, 2016). However, compared to workplace settings, the adoption of a blockchain implies costs borne by individuals. Also, when security compliant behaviour implies explicit costs (e.g. price for software, time spent on installation), the behaviour may be perceived as less time and effort-consuming (Hanus & Wu, 2016; Menard et al., 2017). However, when it comes to blockchain-based applications, due to the novelty and the functional complexity of the technology (Ingold & Langer, 2021; Liu, 2021; Pleger et al., 2021), the understanding of what it takes to preserve personal data may require a lot of mental effort and time. As such, the effect of response cost is likely to be negative in the context of this study.

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.

2.2.2. *Moderating effects*

Drawing on prior empirical research investigating the role of knowledge in attitude formation, intention and behaviour (Friestad & Wright, 1994; Manika et al., 2018), in this study we assume that the appraisal of threat and coping depends on the knowledge that a user has about the system. Individuals' knowledge can be measured both subjectively and objectively. While objective measures can give a more accurate representation of the information about the subject, subjective knowledge reflects individuals' perception about the degree of knowledge that they have (Packard & Wooten, 2013; Park et al., 1994). The latter is more associated with users' self-concept and experience driving consumer behaviour (Packard & Wooten, 2013). The rationale for assuming a moderating effect of objective and subjective knowledge on consumer decision making comes from the findings of research confirming an effect of knowledge/awareness on coping and threat appraisal, underpinning intention (Chen et al., 2020; Torten et al., 2018). The individual's awareness of security protection measures increases the perception of the negative consequences of maladaptive behaviour (D'Arcy et al., 2009), the effectiveness of coping measures (self-efficacy, response efficacy) and decreases the perception of the response cost (Liang & Xue, 2010; Torten et al., 2018). An understanding of the avoidability of the threat, in turn, increases the motivation to engage in adaptive behaviour (Liang & Xue, 2010). Based on these findings, it is expected that the knowledge of blockchain technology increases the effect of threat vulnerability, threat severity, self-efficacy and response efficacy and lowers the effect of response cost.

Individuals who scored high on the innovativeness scale tend to accept new technologies earlier than others (Agarwal & Prasad, 1998). There are several ways in which innovativeness is associated with behavioural intention. Innovativeness can be a direct and an indirect predictor of intention (Ramos-De-Luna et al., 2016; Liébana-Cabanillas et al., 2015; Mun et al., 2006). For example, when examining intention to use phone payments and QR codes, personal innovativeness was found to have a direct positive influence on the outcome variable (Ramos-de-Luna et al., 2016; Liébana-Cabanillas et al., 2015). Innovative people are inclined to use technology as they think that it is easy to use, they are knowledgeable about it and in control of technology utilisation (Mun et al., 2006). However, the moderating effect of innovativeness in the domain of technology acceptance has been under-researched. The hypothesis that innovativeness moderates the effect of cognitive factors is based on the assumption that innovative people are tech-savvy since they are early adopters of technology (Agarwal & Prasad, 1998). Tech-savviness enables them to react towards the potential threat and cope more effectively compared to people who scored low on the innovativeness scale. Give the aforementioned statements, the third hypothesis of the research states that:

Hypothesis 3. a) Subjective knowledge, b) objective knowledge and c) innovativeness moderate the effect of coping appraisal and threat appraisal on intention to adopt blockchain-enabled services. They increase the effect of threat appraisal, response efficacy and self-efficacy and decrease the effect of response cost.

Fig. 1 illustrates the research model, which aims to examine individuals' cognitive factors motivating them to adopt a blockchain, measured by the perception of threat vulnerability, threat severity, response efficacy, self-efficacy and response cost. The effect of the predictors is moderated by knowledge and innovativeness.

3. Methodology

3.1. *Data collection*

For the collection of data, we adopted a purposeful sampling strategy, recruiting participants through an independent research platform.

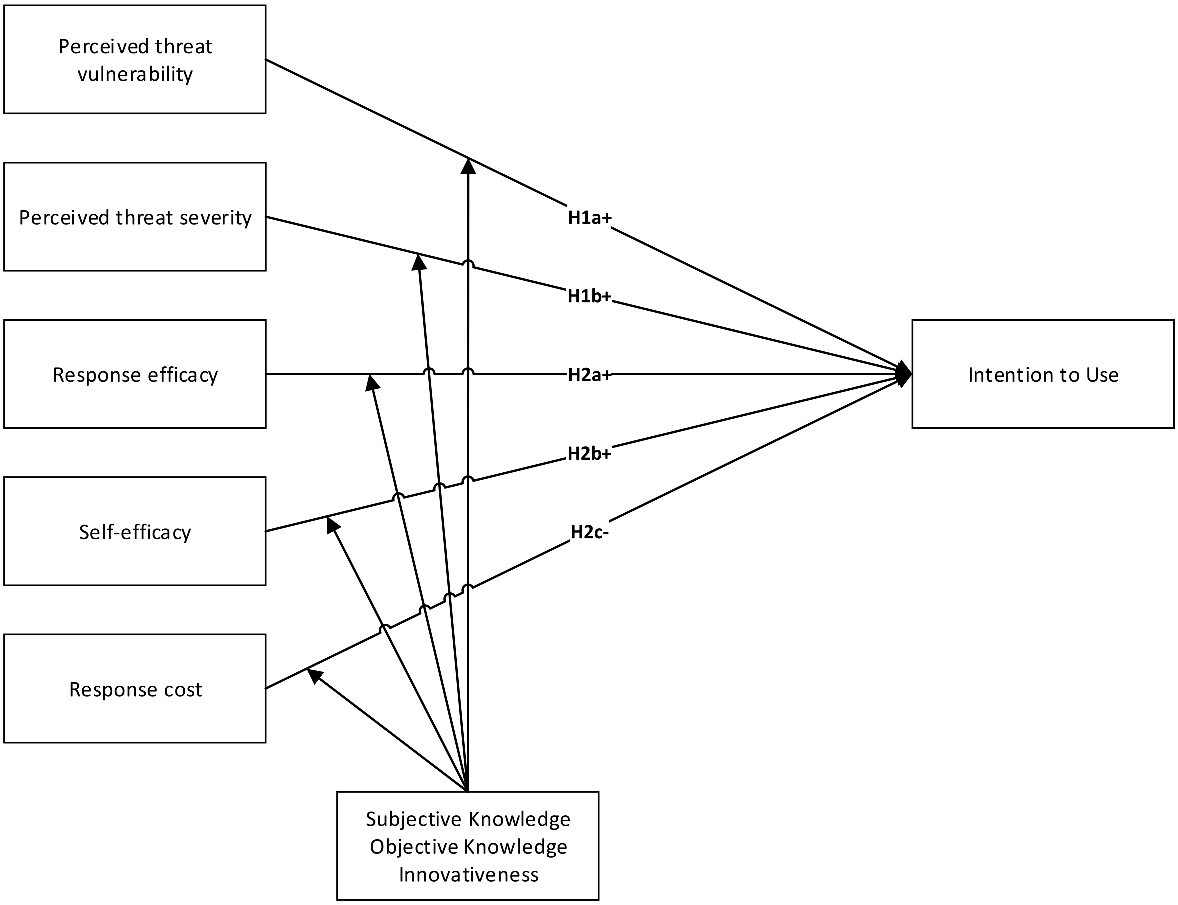

Fig. 1. Research model.

As the study was aimed at investigating the moderating effect of knowledge and innovativeness, we did not filter respondents based on their understanding of blockchain technology. As a result, 506 respondents were recruited for the study (Table 1). When it came to the data collection instrument, we developed an online questionnaire with three parts, which could be accessed through a URL distributed by the data collection platform. The first part briefly outlined the objective of the research study and asked the respondents to complete a consent form. Then, they were given the textual vignette with a hypothetical scenario about the potential use case and the services of a blockchain-based application in the context of shopping (Appendix 1). That scenario enabled respondents to relate a 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 blockchain technology could enable with regards to personal data storage and usage. The second part contained questions about the coping and threat appraisal factors predicting the motivation for protective behaviour. The questions referred to the potential security and privacy-preservation benefits enabled by a blockchain, and not to the services of the digital wallet app (examples provided in Table 2). The last section of the survey included questions about socio-demographic characteristics and technology usage patterns. Prior to collecting the data, a pilot test with 30 respondents was carried out. The pilot test made it possible to validate the comprehensiveness of the questions.

3.2. *Measurements*

All measurements were adopted from prior studies (Table 2). The objective knowledge scale was developed specifically for this study in line with the approach used by other scholars (Manika et al., 2018). The list of items and multiple-choice answers was drawn from the literature on blockchain technologies, and then reviewed by 3 domain experts. The final list of questions for testing objective knowledge is in Appendi×2. Two of the 15 questions measuring objective knowledge were touched upon while defining the services and applications of blockchain technology in the vignette. The innovativeness scale was developed by Agarwal and Prasad (1998). All the items, except the objective knowledge scale, were measured using a 7-point Likert scale.

3.3. *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 testing the relationships between the independent and dependent variables using multiple linear regression analysis in SPSS, 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 & Wright, 2015). To test for multicollinearity between the independent variables, we checked variance inflation factor (VIF) and tolerance coefficients. Tolerance values were above 0.10 ($0.64 \geq 0.91$), while VIF coefficients were below 10 ($1.09 \geq 1.82$), which enabled us to reject the possibility of collinearity (Thompson et al., 2017). We also checked for validity issues by conducting factor analysis. Table 3 demonstrates that the items of each scale

Table 1
The Profile of the respondents.

Demographic Characteristics	Type	Frequency (n = 506)	Percentage
Age	18–24 years	91	18
	25–34 years	164	32.4
	35–44 years	163	32.2
	45–54 years	49	9.7
	55–64 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
Marital Status	Single (never married)	372	73.4
	Married or in civil partnership	128	25.2
	Separated	1	0.2
	Widowed	1	0.2
	Divorced	4	0.8
Internet Use by Year	1–5 years	1	0.2
	5–10 years	4	0.8
	10–15 years	70	13.8
	15–20 years	214	42.2
	More than 20 years	217	42.8

do not have high loadings on other factors.

In addition, to exclude the possibility of spurious variance between the variables attributed to the measurement method, Harman's single-factor test was conducted. The results showed that the variance extracted by a single factor was 32.7%, which is significantly lower than the acceptable cut-off point of 50%. Table 4 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. The effects of independent variables were controlled for by sociodemographic factors, such as age, gender, income and education. However, their inclusion has not resulted in significant changes in the effects of the predictors. The effect of the proposed moderators on the relationships between the predictors and intention was tested using the PROCESS macro for SPSS (Hayes, 2015). This tool enabled us to probe the significance of the effects of the predictors interacting with subjective/objective knowledge and innovativeness.

4. Results

The results of the multiple regression and moderation analyses are provided in Tables 5a and 5b. The research model explained 41% of the variance ($R^2 = 0.412$) for intention to use. Four out of five hypothesised paths were found to be significant. Although the relationship between perceived threat severity and intention to use was non-significant (H3b), the positive effect of threat vulnerability on intention was confirmed (H3a). Response efficacy and self-efficacy were found to have a positive influence on intention (H4a, H4b), while the effect of response cost on intention to use was confirmed to be negative (H4c).

Table 2
Measurement items of constructs.

Measurement item - Protection motivation theory	Loading	α
Perceived threat severity (Ifinedo, 2012; Johnston & Warkentin, 2010)		0.895
Having someone hacking my digital wallet is harmful	0.808	
Threats to the security of my personal data when using a digital wallet are harmful	0.867	
I view data security attacks on my digital wallet as harmful	0.908	
Security attacks on my digital wallet are harmful	0.905	
Perceived threat vulnerability (Ifinedo, 2012; Johnston & Warkentin, 2010)		0.855
I know my personal data could be vulnerable to security breaches if I do not use a digital wallet	0.846	
I could fall victim to a malicious attack if I do not use a digital wallet	0.872	
I believe that trying to protect my personal data using a digital wallet would reduce illegal access to it	0.750	
My personal data and resources may be compromised if I do not use a digital wallet	0.868	
Response efficacy (Vance et al., 2012)		0.933
Using a blockchain-enabled digital wallet to protect my personal data would enable me to reduce the likelihood of security breaches	0.859	
If I use a blockchain-enabled digital wallet, the instances of security breaches will be fewer	0.851	
The regular usage of a blockchain-enabled digital wallet would help avoid security problems	0.860	
Using a blockchain-enabled digital wallet would be an effective way of deterring hacker attacks	0.859	
Using a blockchain-enabled digital wallet would prevent hackers from gaining important personal or financial data	0.877	
Using a blockchain-enabled digital wallet would prevent hackers from stealing my personal data	0.872	
Self-efficacy (Woon et al., 2005)		0.854
It would be easy for me to switch to the usage of a blockchain-enabled digital wallet	0.832	
I could protect my personal data by using a blockchain-enabled digital wallet if there was no-one around to tell me what to do	0.820	
It would not be difficult for me to switch to the usage of a blockchain-enabled digital wallet	0.854	
I could comply with information security policies by myself when using a blockchain-enabled digital wallet	0.820	
Response cost (Woon et al., 2005)		0.813
The cost of protecting my personal data using a blockchain-enabled digital wallet decreases the convenience of its use	0.709	
There are too many overheads associated with trying to protect my personal data using a blockchain-enabled digital wallet	0.813	
Protecting my personal data using a blockchain-enabled digital wallet would require a considerable investment of effort.	0.847	
Protecting my personal data using a blockchain-enabled digital wallet would be time-consuming.	0.826	
Intention to Use (Venkatesh et al., 2012)		0.936
I intend to use the blockchain-enabled digital wallet in the future	0.940	
I will try to use the blockchain-enabled digital wallet in daily life	0.944	
I plan to use the blockchain-enabled digital wallet frequently	0.941	
Subjective knowledge Flynn and Goldsmith (1999)		0.940
I know quite a lot about blockchain technologies	0.851	
I feel very knowledgeable about blockchain technologies	0.837	
Among my circle of friends, I'm one of the "experts" on blockchain technologies	0.781	
Compared to most other people, I know more about blockchain technologies	0.727	
When it comes to blockchain technologies, I know a lot	0.834	
Innovativeness Agarwal and Prasad (1998)		0.905
If I heard about new information technologies, I would look for ways to experiment with them	0.865	
Among my peers, I am usually the first to try out new information technologies	0.848	
In general, I am eager to try out new information technologies	0.918	
I like to experiment with new information technologies	0.898	

When it comes to the moderation effects of subjective knowledge, objective knowledge and personal innovativeness (H5a, b and c), their effects on the relationships between self-efficacy and the outcome variable were negative.

Table 3
Cross loadings of measurement items.

Scale	Items	Component					
		1	2	3	4	5	6
Response Efficacy (1)	1	**0.843**	0.123	0.172	0.176	−0.030	0.067
	2	**0.839**	0.160	0.153	0.151	−0.027	0.064
	3	**0.800**	0.177	0.162	0.210	−0.085	0.029
	4	**0.769**	0.236	0.215	0.154	−0.029	0.113
	5	**0.759**	0.236	0.195	0.137	−0.037	0.168
	6	**0.734**	0.265	0.273	0.135	−0.049	0.180
Self-efficacy (2)	1	0.179	**0.825**	0.197	0.061	−0.041	0.047
	2	0.218	**0.752**	0.096	0.152	−0.154	−0.026
	3	0.297	**0.750**	0.047	0.126	−0.095	0.074
	4	0.237	**0.708**	0.313	0.166	−0.143	0.068
Intention (3)	1	0.306	0.160	**0.843**	0.129	−0.117	0.091
	2	0.336	0.190	**0.827**	0.140	−0.107	−0.001
	3	0.320	0.232	**0.825**	0.131	−0.088	−0.022
Perceived threat vulnerability (4)	1	0.196	0.127	0.024	**0.864**	0.050	−0.033
	2	0.101	0.115	0.137	**0.849**	−0.013	0.051
	3	0.291	0.142	0.113	**0.797**	0.017	−0.025
	4	0.470	0.094	0.262	**0.558**	−0.054	0.044
Response Cost (5)	1	−0.080	−0.142	−0.065	0.014	**0.823**	0.029
	2	−0.084	−0.064	−0.074	0.021	**0.807**	−0.018
	3	−0.138	−0.264	−0.093	0.016	**0.771**	−0.068
	4	0.109	0.071	−0.033	−0.028	**0.753**	0.088
Perceived Threat Severity (6)	1	0.101	−0.010	0.011	−0.018	0.034	**0.874**
	2	0.068	0.020	0.001	−0.005	0.029	**0.863**
	3	0.121	0.065	0.012	−0.006	0.012	**0.832**
	4	0.138	0.109	0.460	0.113	−0.063	**0.512**

Table 4
Mean, standard deviation and correlation coefficients.

Constructs	Mean	S.D.	Correlations					
			1	2	3	4	5	6
1 Intention	4.615	1.424	1					
2 Perceived threat severity	6.214	0.844	.230**	1				
3 Perceived threat vulnerability	4.529	1.186	.406**	.120**	1			
4 Response efficacy	5.109	1.115	.590**	.301**	.528**	1		
5 Self-efficacy	4.792	1.196	.497**	.186**	-.390**	.548**	1	
6 Response cost	4.262	1.093	-.230 **	-.022	-.044	-.151**	-.277**	1

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

Table 5a
Regression results.

Path	*Std. Beta*	t-value	p-value
Perceived Threat Vulnerability → Intention to use	0.135	2.742	*
Perceived Threat Severity → Intention to use	0.103	1.687	ns
Response Efficacy → Intention to use	0.494	8.348	***
Self-efficacy → Intention to use	0.238	4.671	***
Response Cost → Intention to use	−0.143	−3.071	**

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

5. Discussion

5.1. Cognitive factors

Most of the hypothesised paths between cognitive factors and intention to adopt blockchain-based applications were supported, confirming the applicability of PMT when it comes explaining approach motivation to engage in a security-preserving behaviour. The positive effect of threat vulnerability on intention is in line with the Protection Motivation Theory (Rogers & Prentice-Dunn, 1997; Rogers & Mewborn, 1976). The significance of the tested relationship confirms that individuals' fear of being affected by cyber-security issues increases the likelihood of them using blockchain-based services to avoid such threats. This result offers an additional piece of evidence to the literature, which has provided inconsistent conclusions about the role of this factor in motivating protective behaviour in different contexts (Menard et al., 2017; Tsai et al., 2016; Vance et al., 2012). While it was assumed that users may perceive some types of threats as unlikely (Vance et al., 2012), this study confirmed that individuals consider privacy and security issues as highly probable in the context of digital data exchange. The non-supported hypothesised relationship between perceived threat severity and intention contradicts PMT (Rogers & Prentice-Dunn, 1997; Rogers & 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). 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 relatively small amount of money passing through digital wallets, the risk of financial loss 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 comes to the coping appraisal factors, response efficacy was found to have a positive effect. Response efficacy had the strongest effect compared to other predictors. This indicates the existence of strong beliefs that blockchain-based services will help avoid cyber-threats, as promised by the developers of the technology (Barati & Rana, 2019; Gai et al., 2019; Osmani et al., 2020; Wan et al., 2019). The juxtaposition of

Table 5b
Moderation results.

Moderator	Path	Std. Beta	t-value	p-value
Subjective knowledge	Perceived threat vulnerability → Intention to use	−0.024	−0.685	ns
	Response efficacy → Intention to use	0.021	0.675	ns
	Self-efficacy → Intention to use	−0.107	−3.041	**
	Response cost → Intention to use	0.027	0.631	ns
Objective knowledge	Perceived threat vulnerability → Intention to use	−0.038	−0.964	ns
	Response efficacy → Intention to use	−0.030	−0.836	ns
	Self-efficacy → Intention to use	−0.080	−2.131	*
	Response cost → Intention to use	0.004	0.090	ns
Innovativeness	Perceived threat vulnerability → Intention to use	0.001	0.034	ns
	Response efficacy → Intention to use	−0.022	−0.614	ns
	Self-efficacy → Intention to use	−0.100	−2.590	*
	Response cost → Intention to use	0.045	1.090	ns

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

potential threats of unauthorised data use against the capabilities of blockchain-based services to avoid them leads to the idea that the use of such services represents an opportunity to confront security/privacy threats. The dependence of intention on self-efficacy is in line with what was 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 the technology and realise its potential. The negative effect of the 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 outweigh the values of the application, thus inhibiting its adoption. However, compared to response efficacy, the negative effect of response cost on motivation is weaker. This may indicate that adoption decision-making is mostly determined by the belief that using a blockchain-enabled technology to protect personal data would enable individuals to reduce the likelihood of security breaches.

5.2. Moderation effects

Among the examined moderation paths involving subjective knowledge, objective knowledge and personal innovativeness, three were found to be significant, namely those involving self-efficacy and intention. The significant result is in line with prior research postulating that personal predisposition and knowledge enhance self-efficacy perception (Maertz et al., 2005; Latham & Budworth, 2006; Gist & Mitchell, 1992), which, in turn, can facilitate approach behaviour (Lewis et al., 2003). More specifically the three moderations operated in a similar manner. Those with low self-efficacy and also low scores on the moderators had significantly lower intentions to use the blockchain enabled app compared to those with low self-efficacy, but high scores on the moderators. In the case of high self-efficacy, the moderators did not have a significant impact on intentions.

The moderating effects of objective knowledge, subjective knowledge and innovativeness on the paths between perceived threat vulnerability, response efficacy, response cost and intention were statistically insignificant. Such insignificant results do not agree with the prior research on the role of individual traits in coping behaviour and technology adoption (Badii et al., 2020; Wilson et al., 2017; Balapour et al., 2020; D'Arcy et al., 2009; Torten et al., 2018).

Overall, the results of the moderation analysis could potentially reflect the fact that the moderators are more of a personal nature and hence more likely to impact on self-efficacy and less on factors that are more out of people's control, or that the participants have sufficient knowledge to assess the threat and implications at the application level. Further research could focus more on these findings in the context of different applications and explore the impact of other moderators.

5.3. Theoretical and practical contributions

This study contributes to the blockchain and technology acceptance literature in two ways. Firstly, the existing blockchain literature mostly focuses on technical aspects of the technology (Barati & Rana, 2019; Lu & Xu, 2017; Zheng et al., 2017), and lacks 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 & Andras, 2019), the traceability function of blockchain-based supply systems in Indonesia (Asfarian et al., 2020), privacy and trust (Shin, 2019) and organisational adoption of blockchains for supply chain management (Kamble et al., 2021). In contrast to prior research, the findings in this paper advance the literature by exploring the cognitive factors that correlate with the intention to use the technology and represent the first empirical evidence about the potential predictors of the adoption of blockchain-based services. For example, given that the strongest cognitive factor underpinning intention was found to be response efficacy, it is important for users to believe that blockchain-based services will be effective in coping with cyber-threats, as promised. Secondly, the evidence provided in this paper enriches the understanding of the utilisation of innovative technology with an inherently high degree of technical complexity by investigating individual-specific conditions affecting the perception of technology. It was found that the effect of coping appraisal factors can vary among users with different levels of knowledge and innovativeness. While prior research proposed that knowledge and awareness can significantly affect the perception of the coping and threat appraisal factors (Liang & Xue, 2010; Torten et al., 2018), this study helps understand the individual characteristics of users, who are likely to adopt the technology in the context of data privacy and security. This understanding, in turn, can facilitate the diffusion of such technology in different sectors. These findings are important given the fast pace at which similar technologies are being introduced on the market (Hughes et al., 2019; Kavanagh & Ennis, 2020).

From the practical viewpoint, the findings of this paper provide implications for the user-centric development and promotion of a blockchain vs. a more technically oriented one. They provide evidence about the perception of privacy and security threats that conflict with the existing literature presenting the developers' view on blockchain utilisation (Kshetri, 2017; Wan et al., 2019). Specifically, the results suggest 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, users may not pay the expected attention to how these are achieved. Such a finding has implications for marketers, suggesting that they need to embrace more effective channels to convey the long-term consequences of security and privacy errors. The evidence about the significant effects of the coping appraisal factors (response efficacy, self-efficacy and response cost) and the role of knowledge in moderating the paths has a practical value too. To attenuate the effect of the response cost on the intention to use blockchain-enabled services, the investment in blockchain adoption should be justified. In addition, individuals need evidence-based knowledge of the benefits of a blockchain for protecting personal data. Users' understanding of the technology's functionality can be improved by demonstrating how a blockchain works in action.

6. Conclusion and future research suggestions

This paper has addressed the objective rooted in the lack of research on the technology adoption from the user perspective. The study examined cognitive factors, in line with the Protection Motivation Theory and 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. The moderating effects of personal innovativeness, subjective knowledge and objective knowledge on the strength of the predictors were also tested. Three out of twelve hypothesised moderation effects were significant.

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. The 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 beliefs were formed. Third, scholars could gather data about users' experiences while utilising blockchain-based services in different contexts. Such an approach would produce knowledge that can be applied for the adoption of blockchains in specific industries. On the other hand, the findings of this paper guide future studies with regards to the exploration of the services and the benefits of blockchains. Scholars need to demystify the practical usefulness of complex technologies by explaining the implementation of services rather than describing their underpinning technical mechanisms. Such insights will facilitate the users' knowledge of technology applications, increase their perceived value and the perceived capability of implementing them in daily life.

Credit author statement

Davit Marikyan: Conceptualisation, Methodology, Formal analysis, Writing – original draft, Writing – review & editing, Visualisation. **Savvas Papagiannidis**: Conceptualisation Methodology, Formal analysis, Writing – original draft, Writing – review & editing, Funding acquisition, Visualisation. **Omer Rana**: Formal analysis, Writing – review & editing, Visualisation. **Rajiv Ranjan**: Formal analysis, Writing – review & editing, Visualisation.

Funding details

This project has been funded by the Engineering and Physical Sciences Research Council (EPSRC): PACE: Privacy-Aware Cloud Ecosystems (Project Reference: EP/R033293/1).

Declaration of competing interest

There is no conflict of interest.

Appendix 1. Blockchain-app scenario

When going out to a shopping mall, you prefer using a free digital wallet app that stores your credit/debit card information for your day-to-day cashless transactions. This makes it possible to keep all transactions in one place and not have to carry the cards with you. The app can keep records of the transactions. It can potentially share data with third parties who can offer you services accordingly. When carrying out transactions, third parties can potentially have access to your personal details including your shopping behaviour, details of your payments cards and invoices.

To make sure that data is not misused and your privacy rights are not violated, prior to conducting the transaction, you are given:

- the choice of accepting or rejecting the consent to use their private data
- explicit information about the purposes of the use of the data
- explicit information about the parties accessing the data
- the opportunity to easily withdraw the consent

Now imagine that the app developers have announced that they are going to launch a premium version of the app.

This time, the above application has an extra layer of security and privacy. If you have concerns about the violation of privacy rights, the application can facilitate the protection of rights by providing the history of the data use by other parties, including the purpose of data processing, the type of data processed and the parties to whom the data is disclosed. These services are enabled by blockchain technologies upon which this new security and privacy layer is built.

Blockchain is a technology which made it possible to build an immutable, distributed, always available, secure and publicly accessible 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. The distributed manner of data recording and storing in blocks across multiple locations ensures the immutability and traceability of data. The inclusion of a new piece of data (i.e. block) is controlled by the consensus mechanism (i.e. the consent of all participants across the network). The conditions of transactions are written in smart contracts that automatically control the implementation of the rules of transactions, thus eliminating the need for a trusted intermediary to oversee the transaction. Given the traceability and irreversibility of data, blockchain technology provides the opportunity to receive evidence about the conditions upon which personal data is collected and stored by the providers.

In principle, blockchain promises to provide the following advantages for the users:

- Greater Transparency - Users can get hold of the following data: 1) the purpose of data processing, 2) the categories of personal data concerned, 3) the recipients or categories of recipients to whom the personal data have been or will be disclosed, 4) when possible, the period for which the personal data will be stored.

- Increased Efficiency - The disintermediation of data exchange due to a consensus mechanism increases the speed at which transactions are carried out. The retrieval of the transaction data is a very quick and cost-efficient process for the provider, which enables users to resolve any privacy-related concern efficiently.
- Better Security - All data entry is cryptographically protected, which ensures the protection of the system and significantly reduces the risk of data tampering and cyber-attacks.
- Improved Traceability - Users can trace their data usage being confident that records have not been tampered with.

Appendix 2. Objective knowledge Scale

Please read and select the options below that apply to the statements, based on your knowledge of blockchain technology:

Statements	True	False	I do not know
Blockchain is a distributed ledger that enables the creation and storage of data at multiple computers in the network.			
Blocks in the blockchain store information about transactions like the date, time, amount of money, users, etc.			
A smart contract is a part of a blockchain that enables the performance of credible transactions without third parties			
Public blockchain is a decentralised system			
The use of blockchain makes digital transactions more secure			
The use of blockchain ensures users' anonymity			
Blockchain is used only for cryptocurrency			
The immutability of records ensures data security			
Proof of Work (PoW) is a consensus algorithm			
The chronological order of blocks in the system ensures data mutability			
Tendermint is the name of the developer of bitcoins			
The transactions conducted through blockchain are verified			
Blockchain can be used in finance, medical services and insurance			

What types of blockchain exist?

- Public
- Public, consortium
- Public, private, consortium
- I do not know

What types of consensus process exist in a blockchain network?

- permissioned
- permissionless
- both
- neither

References

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research, 9*, 204–215.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)* (pp. 137–141). IEEE.

Albayati, H., Kim, S. K., & Rho, J. J. (2020). Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach. *Technology in Society, 62*, 101320.

Alshamsi, A., & Andras, P. (2019). User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies, 126*, 94–110.

Anderson, L., Holz, R., Ponomarev, A., Rimba, P., & Weber, I. (2016). *New kids on the block: An analysis of modern blockchains*. arXiv preprint, 1606.06530.

Asfarian, A., Hilmi, K. I., & Hermadi, I. (2020). Preliminary user studies on consumer perception towards blockchain-based livestock traceability platform in Indonesia: An implication to design. In *2020 international conference on computer science and its application in agriculture (ICOSICA)* (pp. 1–6). IEEE.

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.

Atlam, H. F., & Wills, G. B. (2019). *Technical aspects of blockchain and IoT. Advances in computers*. Elsevier.

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.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13–28.

Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. *IEEE Access, 8*, 23601–23623.

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management, 52*, 102063.

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. (2019). Enhancing user privacy in IoT: Integration of GDPR and blockchain. In *International conference on blockchain and trustworthy systems* (pp. 322–335). Springer.

Bauer, I., Zavolokina, L., Leisibach, F., & Schwabe, G. (2019). Exploring blockchain value creation: The case of the car ecosystem. In *Proceedings of the 52nd Hawaii international conference on system Sciences*.

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.

Centobelli, P., Cerchione, R., Esposito, E., & Oropallo, E. (2021). Surfing blockchain wave, or drowning? Shaping the future of distributed ledgers and decentralized technologies. *Technological Forecasting and Social Change, 165*, 120463.

Chen, F., Dai, S., Zhu, Y., & Xu, H. (2020). Will concerns for ski tourism promote pro-environmental behaviour? An implication of protection motivation theory. *International Journal of Tourism Research, 22*, 303–313.

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. In *2009 42nd Hawaii international conference on system Sciences* (pp. 1–10). IEEE.

Cuccuru, P. (2017). Beyond bitcoin: An early overview on smart contracts. *International Journal of Law and Info Technology, 25*, 179–195.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*, 104–115.

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*, 79–98.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society, 62*, 101284.

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*.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*, 61–80.

Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K., & Papadopoulos, T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *International Journal of Production Research*, 1–18.

Elhai, J. D., Levine, J. C., & Hall, B. J. (2017). Anxiety about electronic data hacking: Predictors and relations with digital privacy protection behavior. *Internet Research*.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*, 451–474.

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.

Flynn, L. R., & Goldsmith, R. E. (1999). A short, reliable measure of subjective knowledge. *Journal of Business Research, 46*, 57–66.

Friestad, M., & Wright, P. (1994). The persuasion knowledge model: How people cope with persuasion attempts. *Journal of Consumer Research, 21*, 1–31.

Gai, K., Wu, Y., Zhu, L., Zhang, Z., & Qiu, M. (2019). Differential privacy-based blockchain for industrial internet-of-things. *IEEE Transactions on Industrial Informatics, 16*, 4156–4165.

Gist, M. E., & Mitchell, T. R. (1992). Self-efficacy: A theoretical analysis of its determinants and malleability. *Academy of Management Review, 17*, 183–211.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*, 2–16.

Hayes, A. F. (2015). An index and test of linear moderated mediation. *Multivariate Behavioral Research, 50*, 1–22.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*, 106–125.

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.

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.

Jansen, J., & Van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior, 87*, 371–383.

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.

Kamble, S. S., Gunasekaran, A., Kumar, V., Belhadi, A., & Foropon, C. (2021). A machine learning based approach for predicting blockchain adoption in supply Chain. *Technological Forecasting and Social Change, 163*, 120465.

Kavanagh, D., & Ennis, P. J. (2020). Cryptocurrencies and the emergence of blockocracy. *The Information Society, 36*, 290–300.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual international cryptology conference* (pp. 357–388). Springer.

Kowalski, M., Lee, Z. W., & Chan, T. K. (2021). Blockchain technology and trust relationships in trade finance. *Technological Forecasting and Social Change, 166*, 120641.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*, 1027–1038.

Latham, G. P., & Budworth, M.-H. (2006). The effect of training in verbal self-guidance on the self-efficacy and performance of Native North Americans in the selection interview. *Journal of Vocational Behavior, 68*, 516–523.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer publishing company.

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

Lewis, W., Agarwal, R., & Sambamurthy, V. (2003). Sources of influence on beliefs about information technology use: An empirical study of knowledge workers. *MIS Quarterly*, 657–678.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 71–90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*, 394.

Liébana-Cabanillas, F., Ramos De Luna, I., & Montoro-Ríos, F. J. (2015). User behaviour in QR mobile payment system: The QR payment acceptance model. *Technology Analysis & Strategic Management, 27*, 1031–1049.

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 28 October 2021).

Lu, Q., & Xu, X. (2017). Adaptable blockchain-based systems: A case study for product traceability. *IEEE Software, 34*, 21–27.

Maertz, C. P., Jr., Bauer, T. N., Mosley, D. C., Jr., Posthuma, R. A., & Campion, M. A. (2005). Predictors of self-efficacy for cognitive ability employment testing. *Journal of Business Research, 58*, 160–167.

Manika, D., Gregory-Smith, D., & Papagiannidis, S. (2018). The influence of prior knowledge structures on website attitudes and behavioral intentions. *Computers in Human Behavior, 78*, 44–58.

Marikyan, D., Papagiannidis, S., Rana, O., & Ranjan, R. (2021). Blockchain in a business model: Exploring benefits and risks. In *Conference on e-Business, e-Services and e-Society* (pp. 555–566). Springer.

Mcleod, A., & Dolezel, D. (2020). *Toward security capitulation theory*.

Mcleod, A., & Dolezel, D. (2021). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security*, 102526.

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.

Mora, H., Mendoza-Tello, J. C., Varela-Guzmán, E. G., & Szymanski, J. (2021). Blockchain technologies to address smart city and society challenges. *Computers in Human Behavior, 122*, 106854.

Morkunas, V. J., Paschen, J., & Boon, E. (2019). How blockchain technologies impact your business model. *Business Horizons, 62*, 295–306.

Mun, Y. Y., Jackson, J. D., Park, J. S., & Probst, J. C. (2006). Understanding information technology acceptance by individual professionals: Toward an integrative view. *Information & Management, 43*, 350–363.

Newell, S., Swan, J., & Galliers, R. D. (2000). A knowledge-focused perspective on the diffusion and adoption of complex information technologies: The BPR example. *Information Systems Journal, 10*, 239–259.

Notheisen, B., Cholewa, J. B., & Shanmugam, A. P. (2017). Trading real-world assets on blockchain. *Business & Information Systems Engineering, 59*, 425–440.

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*.

Packard, G., & Wooten, D. B. (2013). Compensatory knowledge signaling in consumer word-of-mouth. *Journal of Consumer Psychology, 23*, 434–450.

Park, C. W., Mothersbaugh, D. L., & Feick, L. (1994). Consumer knowledge assessment. *Journal of Consumer Research, 21*, 71–82.

Pleger, L. E., Guirguis, K., & Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behavior, 122*, 106830.

Ramos-De-Luna, I., Montoro-Ríos, F., & Liébana-Cabanillas, F. (2016). Determinants of the intention to use NFC technology as a payment system: An acceptance model approach. *Information Systems and E-Business Management, 14*, 293–314.

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, E. M. (2010). *Diffusion of innovations*. Simon and Schuster.

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*.

Sahebi, I. G., Masoomi, B., & Ghorbani, S. (2020). Expert oriented approach for analyzing the blockchain adoption barriers in humanitarian supply chain. *Technology in Society*, 101427.

Salcedo, E., & Gupta, M. (2021). The effects of individual-level espoused national cultural values on the willingness to use Bitcoin-like blockchain currencies. *International Journal of Information Management, 60*, 102388.

Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. In *2017 4th international conference on advanced computing and communication systems (ICACCS)* (pp. 1–5). IEEE.

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

Thompson, C. G., Kim, R. S., Aloe, A. M., & Becker, B. J. (2017). Extracting the variance inflation factor and other multicollinearity diagnostics from typical regression results. *Basic and Applied Social Psychology, 39*, 81–90.

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.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security, 79*, 68–79.

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.

Wan, J., Li, J., Imran, M., & Li, D. (2019). A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Transactions on Industrial Informatics, 15*, 3652–3660.

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management, 52*, 102090.

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy Policy, 103*, 72–83.

Woon, I., Tan, G.-W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *ICIS 2005 proceedings* (p. 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*, Article e0163477.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557–564). IEEE.