IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 8 May 2022, accepted 7 June 2022, date of publication 27 June 2022, date of current version 6 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3186786

How Perceptions of Information Privacy and Security Impact Consumer Trust in Crypto-Payment: An Empirical Study

ATEFEH MASHATAN[1], MOHAMAD SADEGH SANGARI[1], AND MILAD DEHGHANI[2]

[1]Cybersecurity Research Laboratory, Ted Rogers School of Management, Toronto Metropolitan University (formerly Ryerson University), Toronto, ON M5B 2K3, Canada

[2]Cork University Business School, University College Cork, Cork 21, T12 CY82 Ireland

Corresponding author: Atefeh Mashatan (amashatan@ryerson.ca)

This work was supported in part by the Social Sciences and Humanities Research Council (SSHRC) of Canada and in part by the Ted Rogers School of Management Research Development Grant.

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Research Ethics Board (REB) at Toronto Metropolitan University (formerly Ryerson University) under the REB in accordance with the requirements of Canada's Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2).

ABSTRACT The ever-increasing acceptance of cryptocurrencies has fueled applications beyond investment purposes. Crypto-payment is one such application that can bring radical changes to financial transactions in many industries, particularly e-commerce and online retail. However, characteristics of the technology such as transaction disintermediation, lack of central authority, and lack of adequate regulations may introduce new privacy and security concerns among the users. This coincides with another trend of rising individuals' concerns pertaining to information privacy and security issues in online transactions. The current paper investigates how consumer trust in crypto-payment, a key determinant of consumer intentions and relational exchanges over the long-term, is formed based on their perceptions towards privacy and security aspects of the technology. Using data from 327 survey participants, the study found that perceived information privacy risk, perceived anonymity, and perceived traceability of transactions are significant determinants of consumer trust in crypto-payment; but their perceptions of information security fraud risk have no significant effect. It also provided support for the hypothesis that perceived trust contributes to consumers' intention to adopt crypto-payment. The findings highlight the need to enhance consumer understanding and awareness of information privacy and potential security issues in crypto-payment as well as what needs to be done to address consumer concerns in this regard. The paper creates novel insights into the requirements of trust in crypto-payment services and the consequences of consumers' perceptions of privacy and security in this domain.

INDEX TERMS Adoption intentions, consumer trust, crypto-payment, e-commerce, information security, partial least squares structural equation modeling (PLS-SEM), privacy.

I. INTRODUCTION

The field of cryptocurrency has been attracting substantial attention over the past few years, with a growing number of cryptocurrencies that have emerged and are being traded in the global market. Today, consumer adoption of cryptocurrencies is not just an investment craze, but evidence of a stable and long-term interest. Cryptocurrency transactions do not require financial intermediaries. They have shorter processing times and impose lower or no fees. Also, their quantity of supply cannot be manipulated, unlike fiat currencies that are inflationary in nature [1]. In addition, cryptocurrencies possess the required features of regular currencies, such as storing value, providing a unit of account, and measure of

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

value [2], [3]. Such attributes further motivate the adoption of cryptocurrencies as a means of exchange or money transfer beyond only investment purposes.

Crypto-payment is one such application that refers to the use of cryptocurrencies as a method of payment by consumers when buying goods or services, for example, in e-commerce or online retail [4]. The use of crypto-payment by individual consumers is associated with the business adoption of cryptocurrencies in many industries. In particular, crypto-payment use in retail purchase is a precursor to mainstream cryptocurrency adoption [5]. Several major companies such as AT&T, Overstock, and Gyft have recently begun to accept cryptocurrencies, directly or indirectly, as a method of payment so that they provide their customers with the crypto-payment option when purchasing goods or services. However, the lack of demand from consumers is the most serious barrier to the wider acceptance of crypto-payment in this context [6]. In addition, the benefits of using crypto-payment come with risks that may hinder the mainstream use of the technology, including privacy risks, transaction risks, market risks, counterparty risks, operational risks, and regulatory and legal risks [7]. It causes crypto-payment to remain mostly as a fringe tool and move towards mainstream use slower than anticipated. To capture the full benefits of using cryptocurrencies for payment purposes, there is a pressing need to understand the drivers of consumer adoption and their perceptions of the technology. However, academic research on cryptocurrencies has largely neglected the user perspective connecting existing markets with technological infrastructure. This extends to the expected impact on society resulting from the technology.

When it comes to the public users, there has been a recent trend of growing concerns with respect to information privacy and security issues. This has resulted from several reasons such as increasing the number of breaches that occurred as well as the number and complexity of emerging privacy and security threats in online environments [8]–[10]. Such concerns can even be more critical in the context of online payment services and technologies [11]. Therefore, the way individuals perceive privacy and security aspects of a specific payment technology may become more relevant to the acceptance of that technology. Compared to traditional currencies, cryptocurrencies have some unique characteristics such as the elimination of intermediaries. There is also a lack of central authority and adequate legal and regulatory support for the use of cryptocurrencies. These may entail new sources of privacy and security concerns on the user side. Such unique characteristics raise the problem of understanding how people perceive privacy and security aspects of using cryptocurrencies for making payment transactions. In particular, it necessitates understanding the consequences of such perceptions and their impact on long-term acceptance and willingness to use the technology.

This research aims to examine the formation of consumers' trust in crypto-payment based on their perceptions about privacy and security aspects of the cryptocurrency technology. Trust is a key determinant of consumer intentions and behavior [12]. It serves as a significant predictor of consumer loyalty to a system and relational exchanges over the long-term [13], [14], particularly in the context of digital possession, where verifiability and trustworthiness are even greater concerns. More specifically, the research addresses the following research questions:

RQ1: How is consumers' trust in crypto-payment formed with respect to their perceptions of information privacy risk, anonymity, information security fraud risk, and traceability of payment transactions?

RQ2: How does consumers' perceptions of trust in crypto-payment influence their intention to use it?

The remainder of this paper is organized as follows: Section II provides a brief overview of the research background and related literature. Section III develops the research hypotheses. Section IV describes the methodology and data collection. Section V presents results of data analysis and testing the proposed hypotheses. Section VI discusses the findings and key research implications. Finally, Section VII concludes the paper with research limitations and recommendations for future research.

II. BACKGROUND AND LITERATURE REVIEW

A. PRIVACY AND SECURITY OF CRYPTOCURRENCIES

Over the last few years, a large part of blockchain technology research has centered around cryptocurrencies, including research with respect to privacy and security aspects (e.g., [15], [16]). Several studies have identified major threats to the Bitcoin system, such as double-spending attacks, mining pool attacks, network attacks, client-side security threats pertaining to Bitcoin storage wallets, and attacks to the privacy of Bitcoin data. They have also discussed solutions to deal with these issues and proposals for security enhancement of the Bitcoin system (e.g., [17]–[19]). A large amount of research has also investigated privacy and security issues of blockchain as the underlying technology for cryptocurrencies (e.g., [20], [21]). Zhang *et al.* [22] discussed privacy and security requirements of blockchain and identified several aspects that need to be improved including confidentiality, unlinkability of transactions, and resistance to the 51% attack. Related research involves the analysis and development of consensus protocols as a key component of maintaining blockchain security and preventing attacks (e.g. [23], [24]). It also involves the development of privacy-preserving solutions to address existing privacy challenges and enhance confidentiality, anonymity, and user privacy control in blockchain [25].

Although the privacy and security of cryptocurrencies have been extensively investigated from the technical perspective, there is limited understanding of the end-user perspectives and attitudes towards these aspects. Research showed that user perceptions of Bitcoin security and usability are associated with each other [26]. However, cryptocurrency users take varying privacy and security practices depending on their

perceptions of risk with an intended usage [27]. A survey of Bitcoin users indicated that there exist significant misunderstandings on privacy and anonymity protection in the network while many of the users do not adequately use the security capabilities of Bitcoin management tools [28]. Such observations further highlight the need to understand user perceptions of privacy and security of cryptocurrencies and the way these perceptions may influence intentions towards adoption of the technology for specific use-cases.

B. CONSUMER ADOPTION OF CRYPTOCURRENCIES

Several literature reviews have been published on cryptocurrencies (e.g., [29]), but not much research has been carried out to adequately understand the determinants of intention to adopt cryptocurrency by individuals, particularly beyond using it as an investment tool. Among the available cryptocurrencies, Bitcoin has particularly gained more mainstream awareness and sparked an interest in the drivers and barriers behind adoption. An early study by Folkinshteyn and Lennon [30] identified different risk factors that may contribute to the acceptance of Bitcoin as a currency by developers and end-users. Presthus and O'Malley [31] found that Bitcoin users are predominantly motivated by their technological curiosity. On the other hand, non-adopters prefer not to use it before others do, because they are more doubtful about the benefits and security aspects of the technology. Previous research also posited that the users' behavioral intention to use Bitcoin as a method of payment is influenced by their perceptions towards self-efficacy, trust, transaction processing, and security and control [32].

The technology acceptance model (TAM) has been the mostly cited theory in studying antecedents of cryptocurrency adoption (e.g., [33], [34]). Other well-known adoption theories, such as the theory of planned behavior (TPB), have also been applied in this domain (e.g., [35], [36]). These studies highlighted relevant factors to cryptocurrency adoption such as individuals' perceptions about usefulness and ease of using the technology as well as their subjective norms. More recent research indicated that technology readiness is also a significant predictor of cryptocurrency adoption by individuals [37], [38]. In the context of tourism and travel industry, Treiblmaier *et al.* [39] posited that continuous use of crypto-payment by travellers is motivated by their satisfaction with the use of the technology, which is associated with a range of perceptual antecedents including trust, safety, novelty, usability, and security.

There are several gaps in the existing body of knowledge on cryptocurrency adoption. First, the research on drivers and barriers of end-user adoption of cryptocurrency beyond a financial instrument is far from maturity. In particular, determinants of consumers' intention to adopt cryptocurrencies for payment purposes are largely unexplored. The cryptocurrency domain and its applications are rapidly evolving over time that leads to changes in the adoption landscape. This further underscores the need to continually revisit and refine current understanding of the dynamics behind end-user adoption. It also puts emphasis on the exploration of factors that contribute to adoption intentions based on empirical data, rather than previous research. Second, although trust has been identified as a predictor of cryptocurrency adoption by end-users, research is lacking on how consumer trust in crypto-payment is formed based on their perceptions towards properties of the technology pertaining to privacy and security aspects. More specifically, the impacts of perceived anonymity, information privacy risks, security fraud risks, and traceability have not been examined in this context. Third, studies on individuals' perceptions towards cryptocurrencies have yielded inconsistent results. The existing literature reports contradicting empirical findings on whether, or the extent to which, perceived trust contributes to individuals' intention to adopt cryptocurrencies. This is also the case with the role of security risks. In addition, the literature does not delineate user perceptions towards different aspects of security (e.g., end-point security versus security against protocol or server hacks).

C. CONSUMER TRUST IN E-COMMERCE AND E-PAYMENT

The antecedents and consequences of consumer trust in e-commerce and e-payment systems have been the subject of research for many years. Several previous studies demonstrated positive associations between trust and behavioral intentions of individual consumers with respect to new payment technologies. Consumer trust is a significant determinant of adoption and use of e-payment systems [40], [41]. Gao *et al.* [42] indicated that initial trust drives individuals' intention to use mobile payment services as well as their perceptions of benefits and convenience of using the service. The formation of initial trust is positively influenced by perceptions towards the quality of the system, information, and service itself, while negatively influenced by perceived uncertainty. Patil *et al.* [43] found a positive association between consumer trust and attitude towards mobile payment.

Trust is also a significant predictor of consumers' behavioral intentions in the e-commerce environment. Consumers' trust in e-commerce can be driven by their trusting beliefs as well as their perceptions of usefulness and ease of use of the platform [44]. Sullivan and Kim [45] demonstrated that trust has a positive impact on consumers' perceived usefulness and repurchase intention in e-commerce. In addition, their perceptions of risk, value, and reputation determine how they trust in e-commerce. Consumers' perception of e-commerce trustworthiness is further motivated by their disposition to trust [46]. Such empirical findings highlight the significance of trust and the factors that may promote or impede trust formation in the process of consumer acceptance of new technologies in this domain.

Information privacy and security have long been recognized among the major determinants of user trust in online environments [47]. However, relevant research is still fragmented in e-commerce and e-payment domains and needs to be revisited, particularly when it comes to consumer perceptions towards emerging dimensions of information privacy

and security concerns with specific technologies. In general, the violation of privacy results in reduced online trust [48]. On the other hand, clear privacy statements and procedures enhance user trust in online services [49]. Dinev and Hart [50] suggested that dealing with privacy risks and concerns is important for consumers performing online transactions. The relationship between user concerns towards privacy and the way they build trust is more significant in the context of business-to-consumer (B2C) e-commerce [51]. Perceptions of information privacy risk could even be a more important consideration than the economic risk for consumers when choosing to carry out an e-commerce transaction [50].

Apart from privacy, perceived security has also been identified as a determinant of consumer trust in a range of online trading systems such as online banking [52], mobile payment [53], and online purchase [54]. Consumers' perceived security as well as technical protections in place to ensure secure payment transactions have both significant influences on their trust in e-payment systems [40]. Perceived security in mobile payment is dependent on other security measures such as security rules and policies [55]. Previous research also found anonymity as another relevant factor in consumers' decision to participate in e-commerce, where a lack of discretion may discourage them from continuance usage [56]. More positive beliefs about anonymity encourage online trust [57] and make trust issues less relevant [47]. In addition, traceability creates positive trust perceptions in e-commerce due to enhanced transaction auditability when consumers find elements of their transactions traceable from origin to the destination [58], [59].

The fundamental differences between cryptocurrencies and fiat currencies may affect consumer trust towards their use as a means of payment. In particular, regulatory issues, lack of central authority, and disintermediation of transactions with cryptocurrencies potentially make privacy and security more relevant considerations for consumer trust. This is further emphasized by a general trend of increasing privacy and security concerns among public users. The use of crypto-payment in e-commerce is at the early stages and has not been widely accepted yet. Research is needed to investigate individuals' perceptions towards privacy and security aspects of using this emerging technology and to revisit the consequences of such perceptions in terms of consumer trust.

III. HYPOTHESES DEVELOPMENT

A. CONSUMER TRUST IN CRYPTO-PAYMENT AND ADOPTION INTENTIONS

Trust in crypto-payment can be described as ''the willingness to take risks based on the belief, expectation, competence, and integrity of electronic payments made with cryptocurrencies'' [5]. Trust is a crucial factor for consumers when participating in payment transactions, especially using cryptocurrency [30]. If consumers were to use a currency for e-commerce, they would have to trust the system it is based on and the currency itself [60].

The cryptocurrency ecosystem is not mature enough and has potential trust issues pertaining to technology providers, users, and also governments, such as the risk of information privacy and security attacks and issues with transparency, reputation systems, and the shadow economy, that may negatively influence trustworthiness and adoption of cryptocurrencies. Some cryptocurrencies available in the market have less of some of these issues, but they do not differ so much due to the nature and properties of the underlying technology [61]. Also, cryptocurrencies do not have the universal trust that real-world currencies have built up over centuries [32].

Previous research indicated that perceived trust influences consumers' intention to use cryptocurrencies [32], [33], [36], [39], [62]. However, Mendoza-Tello *et al.* [5] found that trust is not among strong predictors of cryptocurrency use, possibly due to a lack of adequate understanding at early stages of disruptive technologies. Since people are becoming more inclined to adopt and more informed about cryptocurrencies, it is then reasonable to infer that trust will most likely have a strong positive impact on their intention to use them for payment purposes. In light of these arguments, the following hypothesis is put forth:

H1: Consumers' perception of trust in crypto-payment is positively associated with their intention to use it.

B. PERCEIVED PRIVACY RISK

Perceived privacy risk represents an individual's perception of ''potential loss of control over personal information'' [63]. In line with this definition, consumers' perception of information privacy risk can be inferred as how likely it is for them to lose their personal information while making transactions using cryptocurrencies. It is important for consumers to preserve their privacy when using crypto-payment because their perception of privacy risk can prevent them from partaking in the transaction [64]. Consumers' concerns for information privacy are growing [8], and it is essential for crypto-payment systems to reduce relevant risks to entice potential customers to use their services. Many e-commerce consumers rely on legal systems to protect their privacy; however, because cryptocurrencies are currently unregulated, it would be their function to provide consumers with sufficient privacy protection.

The risk of privacy compromise is identified among trust-related issues of cryptocurrency [61]. Potential privacy loss when using cryptocurrencies is becoming a more prevalent concern with the introduction of more regulations, such as those pertaining to knowing your customer (KYC) and anti-money laundry, that require disclosure of personal information [30]. In addition, perceived privacy in a blockchain-based service, influenced by the distributed ledger function of the technology, has a positive impact on users' trust in that service [65]. Hence, the following hypothesis is advanced regarding the impact of consumers' perceptions towards privacy risks in using crypto-payment:

H2: Consumers' perception of information privacy risk is negatively associated with their perceived trust in crypto-payment.

C. PERCEIVED ANONYMITY

Anonymity is defined as the ''non-coordinate ability of traits in a given respect'' and can be described as a ''form of non-identifiability'' [66]. Cryptocurrencies like Bitcoin have been reputed as a means of anonymous payment [67]. However, they only provide pseudo-anonymity, which is limited compared to full anonymity [68]. Bitcoin and similar cryptocurrencies suffer from significant anonymity vulnerabilities that make them a subject of deanonymization attacks [69]. Cryptocurrency users employ pseudonyms when participating in transactions on the Bitcoin network, but it is still possible to track transactions back to the user with well-known network analysis techniques [70]. Cryptocurrency users can also be identified through the analysis of transaction records on the blockchain [71]. However, there are ways for users to become more anonymous when transacting with cryptocurrencies, such as using The Onion Router (TOR) network. Krombholz *et al.* [28] found that 25% of Bitcoin users preserve their anonymity by using Bitcoin over TOR. Despite this, the effort required from users to gain this extra bit of anonymity is significant, and the reduction in the ease of usability is not worth it for most regular users [72]. The pseudo-anonymity of cryptocurrencies, on the other hand, may limit companies' ability to gather consumer information for target marketing and other purposes [73].

There does not exist much evidence on consumer perceptions towards anonymity of cryptocurrencies and their consequences. A survey of experts by Ermakova *et al.* [74] found anonymity to be an adoption driver on the user side, but it impedes governmental adoption [33]. Not only does inadequate anonymity raise user concerns about leakage of their identity, it may also have negative impacts on the fungibility and efficacy of the cryptocurrency to be used as a currency in payment transactions [75]. These imply the consequences of negative perceptions towards anonymity in terms of reduced consumer trust. It agrees with Rehman *et al.* [61] who identified weak anonymity as one of the trust issues with the cryptocurrency ecosystem. Recent research also posited that anonymity is an important consideration for privacy enhancing technologies. The more the users perceive they can retain their anonymity, the more they tend to trust in the technology [76]. These arguments motivate our third hypothesis:

H3: Consumers' perception of anonymity is positively associated with their perceived trust in crypto-payment.

D. PERCEIVED SECURITY FRAUD RISK

When using payment tools, consumers expect them to be secure and free from fraud. Information security fraud in cryptocurrency occurs when an attacker manages to issue transactions on behalf of a user (by gaining access to their private key or hacking the system) and takes their money, or gains unauthorized access to their data. Security becomes paramount in services that handle cryptocurrencies, considering that the transactions are disintermediated [30]. An impressive market expansion together with the lack of adequate regulations make cryptocurrencies more prone to frauds, hacks, and Ponzi schemes [77]. Also, the lack of consumer protection and financial loss due to system flaws increase the level of risk that consumers perceive regarding Bitcoin use [78]. A large number of information security fraud instances is reported every year, causing cryptocurrency owners to lose millions of dollars. In line with prior research on perceived security risk [79], the perception that using crypto-payment is associated with information security fraud issues is referred to as perceived security fraud risk.

According to Abramova and Böhme [78], perceived security positively influences cryptocurrency usage behavior. Presthus and O'Malley [31] and Ermakova *et al.* [74] identified negative perceptions of security as an impediment to Bitcoin adoption. Also, Treiblmaier *et al.* [39] posited that perceived security drives user satisfaction with cryptocurrencies. Other studies indicate that trustworthiness of cryptocurrency systems depends on the users' perceived security, which reflects the level of security that they feel when using the system [61], [80]. Consumer perceptions about information security contribute to their level of trust in FinTech innovations as well [81]. Therefore, the following hypothesis is proposed:

H4: Consumers' perception of information security fraud risk is negatively associated with their perceived trust in crypto-payment.

E. PERCEIVED TRACEABILITY

According to Wilson and Clarke [82], traceability denotes the information required to describe the transaction history of purchases and any subsequent changes. The benefits of traceability are visible at the levels of industry, involved technology providers, and end-consumers. Traceability helps locate where a system crashed and what is responsible for the problem. It helps with detection and resolution of problems without causing irreversible costs throughout the chain [83]. A recent study of blockchain-based food traceability indicated that it increases consumer trust in the retailer [12].

The role of traceability of systems has gained a great interest in supply chain management research. However, its significance has not been well discussed or explored in the cryptocurrency domain and there is a lack of understanding about consumer perceptions of traceability in using cryptocurrencies for payment transactions. Traceability in blockchain is the ability for someone to follow their information exchanges over the network and see the status of transactions they have made. Although traceability of payment transactions comes with the cost of losing some degree of anonymity on the user side, it provides benefits to the payment system in terms of payment verifiability, auditability, and integrity. In addition, it assists with protection of the payment system against illegal activities and financial crime [67]. Therefore, perceived traceability may, in turn, stimulate more positive consumer perceptions towards building trust in crypto-payment. This leads to the last hypothesis as follows:

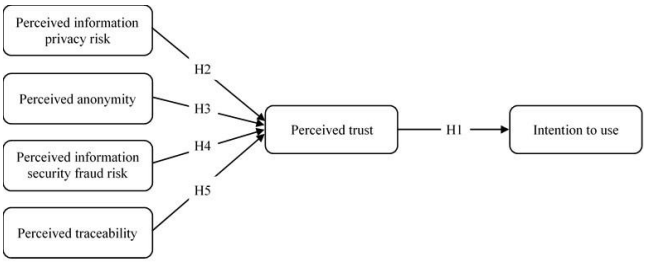

FIGURE 1. Research model.

H5: Consumers' perception of traceability is positively associated with their perceived trust in crypto-payment.

Figure 1 shows the proposed model and research hypotheses.

IV. METHODOLOGY

A. MEASUREMENT INSTRUMENT

To measure the model constructs, we developed a survey instrument, involving items adapted from relevant established studies as well as self-developed scales. The complete list of measurement items is presented in the Table 1. All the items were measured using a seven-point Likert-type scale (1 = strongly disagree; 7 = strongly agree). The four-item scale proposed by Shahzad *et al.* [33] was used to measure consumer intention to use (ITU). The scales developed by Dinev and Hart [50] and Shareef *et al.* [84] were adapted to measure perceived information privacy risk (PPR) and perceived trust (PT), respectively. To measure perceived anonymity (PA), three items were formulated based on the scale developed by Hite *et al.* [85]. Since there were no previously validated measurement instruments for the constructs of perceived traceability (PRT) and perceived information security fraud risk (PFR), we developed measurement items based on existing research on traceability, existing scales for perceived information security, and interviews with eight subject matter experts in blockchain technology in the financial industry. This resulted in four measurement items for perceived information security fraud risk and two items for perceived traceability. We followed the guidelines proposed by Carpenter [86] to ensure the accuracy of newly-developed scales. To ensure the clarity, quality, and validity of the measurement items and the whole survey, a pretest was conducted with 17 participants recruited through convenience sampling. The feedback received from participants indicated that the survey questionnaire was well understood and clear for the target respondents.

B. DATA COLLECTION

An online questionnaire managed with Qualtrics was employed to gather the data needed for the study. The sample consisted of undergraduate university students. Due to being more technology-savvy, university students have been commonly chosen as survey participants in technology adoption studies [87]. Research also found that those who have college or university education are much more aware of Bitcoin compared to other people [88]. In addition, university students come from different districts, backgrounds, and social and economic groups [89], so that they provide a reasonably representative sample of different socio-economic groups. In our survey, the students were recruited via a Canadian university sanctioned participant pool and received 0.25% bonus course credit in lieu of taking part in the study. The survey obtained approval from the research ethics board (REB) of the university.

On the opening page of the questionnaire, participants were briefed about the survey and asked to give their consent prior to answering the questions. The questionnaire was designed in two parts. In the first part, respondents were asked about their demographic details including age and gender as well as their familiarity with cryptocurrencies. They were also asked to specify if and how frequently they use crypto-payment for e-commerce or other types of online purchase activities. The second part of the questionnaire comprised the measurement items. Based on the self-assessed ratings given in the first part, data from 80 participants was excluded as they reported they were not familiar with cryptocurrencies. Overall, a total of 327 responses were considered as the sample for data analysis.

A non-response bias test was conducted to ensure representativeness of the responses and generalizability of the results. The analysis was performed based on a comparison between the early and late respondents [90]. The results of t-test indicated that there was no significant statistical difference between the two groups regarding each scale item in the individual constructs. Therefore, non-response bias did not pose a major effect on the results. Also, Harman's one-factor test was conducted to check for potential common method bias (CMB) [91]. Results confirmed that the measurement instrument did not introduce biases in the relationships among variables. Hence, the CMB was unlikely a serious concern in our study.

V. RESULTS

The mean age of the sample profile was 21.52 with 63.0% female versus 37.0% male respondents. Of the whole sample, 14.1% identified themselves as actual users of some types of cryptocurrencies. Of these respondents, 56.5% indicated that they use crypto-payment for e-commerce. They also reported that they use it in other applications such as online gaming (41.3%), gambling (39.1%), and education (32.6%). More than one third of the users indicated that they use crypto-payment frequently or more. In the initial model, gender and usage were included as control variables. Results showed that eliminating these variables had marginal, if any, influence on the variance described in the endogenous constructs (t-values ranged from 0.20 to 1.33). Therefore, there were no significant patterns between males versus females and between the results for users versus non-users, indicating the generalizability of study findings.

TABLE 1. Measurement items.

Code	Items
Consumer intention to use	
ITU1	I intend to use a cryptocurrency as an alternative source of currency to buy or sell products in the future.
ITU2	I believe using a cryptocurrency is very helpful in a timely manner to fulfill my obligations.
ITU3	I intend to use a cryptocurrency on a regular basis.
ITU4	I will encourage others to use a cryptocurrency as a mode of exchange.
Perceived trust	
PT1	Transaction through a cryptocurrency is guaranteed.
PT2	The service takes full responsibility for any type of insecurity during operation by a cryptocurrency.
PT3	Technological policies of a cryptocurrency adequately protect me from problems on financial service channel.
PT4	Cryptocurrencies are overall reliable.
Perceived information privacy risk	
PPR1	Private/personal information can be sold to third parties when using a cryptocurrency.
PPR2	Private/personal information submitted on a cryptocurrency can be misused.
PPR3	Private/personal information in a cryptocurrency can be made available to unauthorized entities without your knowledge.
PPR4	Private/personal information in a cryptocurrency can be made available to government agencies.
Perceived anonymity	
PA1	While using a cryptocurrency, I can keep my identity anonymous.
PA2	While using a cryptocurrency, personal identity is unknown to others or that they are unidentifiable as an individual.
PA3	Overall, my action in using cryptocurrencies cannot be trackback to my personal identity.
Perceived information security fraud risk	
PFR1	An attacker can steal and use my private information if I use a cryptocurrency.
PFR2	An attacker can steal the private key and issue transactions on behalf if I use a cryptocurrency.
PFR3	An attacker can steal the private key and get unauthorized access to data if I use a cryptocurrency.
PFR4	While using a cryptocurrency, I cannot prevent a security fraud (later dropped).
Perceived traceability	
PTR1	While using a cryptocurrency, I can trace my transaction easily.
PTR2	While using a cryptocurrency, I can identify which exchange has been done.

Based on the descriptive statistics reported in Table 2, the sample showed higher-than-average levels of concern towards both information privacy and security fraud risks (mean scores = 4.84 & 4.75). The respondents also had relatively positive attitudes about traceability of their transactions (mean score = 4.37) and preserving their anonymity (mean score = 4.24) in using crypto-payment. However, they reported relatively lower degrees of trust (mean score = 3.71) and intention to use crypto-payment (mean score = 3.17). The standard deviations (SD) given in Table 2 indicated the highest variation in respondents' views on the intention to use among other research constructs (SD = 1.36). On the other hand, the minimum dispersion in responses was pertained to perceived trust (SD = 1.14).

TABLE 2. Descriptive statistics, reliability, and validity of the measurement scales.

Constructs/ Items	Mean	SD	Item loading	Cronbach's α	CR	AVE
ITU	3.17	1.36		0.892	0.925	0.755
ITU1	3.50	1.70	0.853			
ITU2	3.63	1.50	0.863			
ITU3	2.56	1.48	0.884			
ITU4	3.00	1.55	0.876			
PT	3.71	1.14		0.807	0.873	0.632
PT1	3.70	1.44	0.802			
PT2	3.82	1.40	0.745			
PT3	3.61	1.34	0.840			
PT4	3.70	1.54	0.789			
PPR	4.84	1.27		0.904	0.929	0.767
PPR1	4.72	1.47	0.900			
PPR2	4.89	1.43	0.920			
PPR3	4.88	1.43	0.939			
PPR4	4.88	1.45	0.728			
PA	4.24	1.26		0.886	0.925	0.805
PA1	4.24	1.43	0.892			
PA2	4.21	1.38	0.882			
PA3	4.26	1.36	0.917			
PFR	4.75	1.30		0.903	0.933	0.823
PFR1	4.80	1.46	0.930			
PFR2	4.74	1.39	0.888			
PFR3	4.70	1.39	0.903			
PTR	4.37	1.17		0.767	0.895	0.810
PTR1	4.44	1.29	0.913			
PTR2	4.29	1.32	0.887			

A. RELIABILITY AND VALIDITY ANALYSIS

To analyze the proposed model, partial least squares structural equation modeling (PLS-SEM) using SmartPLS 3 [92] was employed. PLS-SEM is particularly useful when the theoretical foundation describing the research model is not well-formed [93] and the focus is mainly on identifying determinants of a target variable [94], which is the case in this study. Table 2 presents results of testing the measurement model, including information regarding reliability and validity of the model constructs and indicators. The factor loadings for the measurement items were higher than 0.6 as recommended by Chen and Myagmarsuren [95], except for one item of the self-developed scale for perceived information security fraud risk which was then dropped from the model (indicated in Table 1). The values obtained for Cronbach's α were all above 0.7, indicating satisfactory reliability and internal consistency of the latent constructs. Construct reliability was also assessed using the composite reliability (CR) measure which was greater than the threshold of 0.7 in all cases. In addition, Table 2 indicates that the average variance extracted (AVE) for all latent variables was above the 0.5 cut-off, thus providing evidence of good convergent validity of the measurement model [96].

The discriminant validity of model constructs was tested in three ways. First, correlations among the constructs were compared against the square roots of their AVEs [97]. As presented in Table 3, the square roots of AVE values were greater than the inter-correlations for all the latent constructs. The discriminant validity was also confirmed by an assessment of the Heterotrait-Monotrait (HTMT) criterion reported in

TABLE 3. Results of testing the Fornell-Larcker criterion.

Constructs	PFR	ITU	PA	PPR	PTR	PT
PFR	0.907					
ITU	– 0.154	0.869				
PA	– 0.155	0.267	0.897			
PPR	0.626	– 0.156	– 0.247	0.876		
PTR	– 0.067	0.409	0.306	– 0.064	0.900	
PT	– 0.156	0.483	0.319	– 0.240	0.443	0.795

TABLE 4. Results of testing the HTMT criterion.

Constructs	PFR	ITU	PA	PPR	PTR
ITU	0.175				
PA	0.144	0.290			
PPR	0.684	0.163	0.284		
PTR	0.082	0.494	0.359	0.081	
PT	0.157	0.555	0.343	0.240	0.553

TABLE 5. Cross-loadings.

Indicators	ITU	PT	PPR	PA	PFR	PTR
ITU1	*0.853*	0.399	– 0.146	0.262	– 0.163	0.364
ITU2	*0.863*	0.443	– 0.070	0.235	– 0.069	0.406
ITU3	*0.884*	0.401	– 0.161	0.197	– 0.133	0.336
ITU4	*0.876*	0.431	– 0.170	0.233	– 0.175	0.315
PT1	0.450	*0.802*	– 0.210	0.252	– 0.135	0.417
PT2	0.268	*0.745*	– 0.164	0.172	– 0.065	0.293
PT3	0.350	*0.840*	– 0.245	0.340	– 0.166	0.347
PT4	0.435	*0.789*	– 0.136	0.232	– 0.116	0.332
PPR1	– 0.158	– 0.201	*0.900*	– 0.257	0.524	– 0.089
PPR2	– 0.155	– 0.205	*0.920*	– 0.220	0.565	– 0.058
PPR3	– 0.140	– 0.271	*0.939*	– 0.203	0.593	– 0.051
PPR4	– 0.037	– 0.053	*0.728*	– 0.218	0.617	0.021
PA1	0.178	0.218	– 0.197	*0.892*	– 0.063	0.259
PA2	0.247	0.213	– 0.233	*0.882*	– 0.147	0.233
PA3	0.274	0.371	– 0.231	*0.917*	– 0.180	0.311
PFR1	– 0.133	– 0.190	0.662	– 0.184	*0.930*	– 0.075
PFR2	– 0.146	– 0.084	0.470	– 0.105	*0.888*	– 0.068
PFR3	– 0.151	– 0.106	0.491	– 0.093	*0.903*	– 0.031
PTR1	0.356	0.372	– 0.031	0.260	– 0.010	*0.887*
PTR2	0.380	0.423	– 0.081	0.291	– 0.105	*0.913*

Table 4, indicating that all the ratios satisfied the condition of being less than the recommended threshold of 0.90 [98]. In addition, the cross-loadings of the measurement items were examined as given in Table 5. The results showed that all items loaded higher on their corresponding construct than on other constructs in the model, providing further evidence to establish discriminant validity [96].

B. TESTING THE PROPOSED MODEL

The variance inflation factor (VIF) was used to test for any potential collinearity. The highest VIF value for predictor constructs was 1.711, which was far less than the threshold of 5 [99]. Thus, collinearity was not an issue for the proposed model. Also, the standardized root mean square residual (SRMR) was measured to check if there is any potential concern regarding the model fit. The resulting SRMR was 0.074, which was below the conservative value of 0.08 as the recommended threshold for covariance-based SEM [100]. This indicated a good fit for the proposed model.

TABLE 6. Results of hypothesis testing.

Hypothesis/ Path	Path coefficient	*t*-value	Result	Effect size (f^2)
H1: PT >> ITU	0.483 ***	9.458	Supported	0.304
H2: PPR >> PT	– 0.180 **	2.735	Supported	0.026
H3: PA >> PT	0.158 **	2.582	Supported	0.029
H4: PFR >> PT	0.007 ^{ns}	0.099	Not supported	0.000
H5: PTR >> PT	0.384 ***	6.957	Supported	0.180

Significance level: *** 0.001; ** 0.01; * 0.05; ^{ns} non-significant

A bootstrapping procedure was performed to generate *t*-statistics and standard errors for the structural model. The path coefficients and statistical findings on the significance of the hypothesized relationships are reported in Table 6. The results indicated that perceived trust in crypto-payment was significantly and positively associated with consumers' intention to use it ($\beta = 0.483$). Thus, *H1* was supported. It also indicated that perceived information privacy risk had a negative relationship with perceived trust ($\beta = -0.180$). This provided support for *H2*. In addition, the results of path analysis confirmed *H3* and *H5* on perceived anonymity and perceived traceability to be significant predictors of perceived trust in crypto-payment ($\beta = 0.158$ & 0.384). On the other hand, *H4* was rejected as no significant relationship was found between perceived information security fraud risk and perceived trust.

The *R*-squared (R^2) values for perceived trust and intention to use constructs were 0.262 and 0.233, respectively. Both values were significant with *p*-value of 0.000 and considered high in consumer behavior research [94], [101]. Table 6 also reports the effect size (f^2) for the predictor variables. Based on the suggested guidelines of 0.02, 0.15, and 0.35 for small, medium, and large effects [102], the results indicated small effects for perceived privacy risk and perceived anonymity. In contrast, a medium effect was observed for perceived traceability and perceived trust. In addition, the Stone-Geisser's Q^2 statistics was employed to assess the out-of-sample predictive power of the proposed model. Following the blindfolding procedure, Q^2 values greater than zero were obtained for both of the endogenous constructs (0.155 for perceived trust and 0.173 for intention to use), confirming the predictive relevance of the model [101], [103].

The importance-performance map analysis (IPMA) was conducted to enrich the results of structural model analysis. The IPMA further examines the significance of the predecessor variables in describing target variables based on their total effect (importance) and their average latent variable scores (performance) [104]. As reported in Figure 2 and Table 7, perceived trust had a relatively low performance (44.963) but high importance in intention to use. The results indicated that one unit increase in the performance of perceived trust causes 0.572 increase in the performance of intention to use. Among the independent variables, perceived traceability had the highest importance in shaping perceived trust and intention to use. It was also found that a one-unit decrease

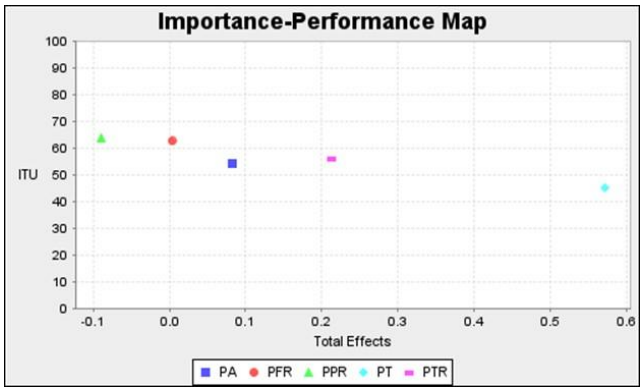

FIGURE 2. IPMA for ITU.

TABLE 7. IPMA results.

Construct	Importance in PT	Importance in ITU	Performance
PPR	– 0.157	– 0.090	63.973
PA	0.144	0.082	54.038
PFR	0.006	0.003	62.655
PTR	0.372	0.213	56.077
PT	-	0.572	44.963

in perceived privacy risk leads to 0.157 and 0.090 units of increase in the performance of perceived trust and intention to use, respectively. The IPMA results provided additional support for the hypothesis testing results obtained from the structural model analysis where *H1* and *H5* had the highest path coefficients.

VI. DISCUSSION AND IMPLICATIONS

According to the findings, consumers' perceptions about information privacy risks, anonymity, and traceability are significant predictors of trust in crypto-payment, which in turn predicts their intention to use it. However, their perception about the risks of information security fraud does not have a significant impact on how trustworthy they perceive crypto-payment to be. With regard to the positive association between trust perceptions and intention to use crypto-payment, the findings from testing *H1* agree with previous studies on cryptocurrency adoption (e.g., [33], [39]) and adoption of new payment technologies (e.g., [42], [43]). Also, in line with the arguments raised by Mendoza-Tello *et al.* [5], the empirical results for university students as a more technology-savvy group of consumers provide evidence on the role of technology understanding in consumers' decision to use cryptocurrencies based on their perceptions of trust. The findings reveal that consumers have concerns about both privacy and security risks of using cryptocurrencies for payment purposes, but only privacy concerns contribute to their level of trust in the technology as proposed in *H2*. The findings in this regard comply with those reported in other relevant domains (e.g., [48], [65]). In fact, there are no safeguards against privacy loss when using cryptocurrencies as they are inherently decentralized and highly unregulated.

On the other hand, the non-significant *H4* for the relationship between trust and perceived information security fraud risk is interesting since it contradicts previous findings on security – trust association in online payment systems (e.g., [52], [53]). Such a result, however, supports those obtained by Walton and Johnston [35], who found security to be neither a predictor of attitudes towards cryptocurrencies nor a significant barrier to its adoption. Undergraduate students have frequently used cyber technologies and, hence, likely perceive a higher sense of self-efficacy that may cause increased confidence in their own abilities to deal with information security issues. Such perceptions may become more critical since they have not been generally provided with formal cybersecurity training [89]. Another possible reason is that consumers might be desensitized to information security breaches happening all the time and covered in the news extensively. Even big corporations that possess abundant resources to deal with cybersecurity issues suffer from such breaches. Hence, it might be perceived as the cost of doing business and accepted as a reality by consumers.

From *H3*, we can infer that consumers consider anonymity preservation as a significant driver of trust in crypto-payment services. The empirical evidence in this regard provides support for the exploratory findings of Rehman *et al.* [61] on trust issues of weak anonymity with cryptocurrencies. Practically speaking, this means that enhancing the positive effect of anonymity, which may come from an external source such as government regulations, should be a key consideration for users. Regulation might make consumers feel much safer about the anonymous environment, while allowing for some of the benefits of controlled anonymity or pseudo-anonymity. Another option to allow for the benefit of anonymity without encouraging criminal practice could be the creation of a new regulation system based on cryptocurrencies that can only be spent on specific products or services. This would allow anonymity to be preserved without the negatives of criminals. For example, a merchant could increase anonymity by accepting cryptocurrency using services such as Bitcoin mixer. This could be an in-house or third-party method for anonymizing transactional data and increasing perceived anonymity in the consumer side. Apart from that, many consumers place great value on anonymity for specific purchases. In addition, existing evidence of criminal or questionably legal transactions via crypto-payment suggests that this could be a driver for some people. Most consumers, however, are likely driven by anonymity because they do not wish to be trackable by large companies or government agencies. Although most cryptocurrencies only provide pseudo-anonymity, a misunderstanding by non-technical consumers could influence their likelihood of trust.

With regards to anonymity, it is also relevant to remark that governments can benefit from publicly available transactions by using them in unprecedented circumstances (e.g., cyberterrorism or ransomware). The perception of anonymity when using cryptocurrencies remains an open debate with some uncertainty of the real significance. While many governments

have started exploiting this convenient affordance by developing systems that record transaction data and take private data into a single database, most have just started moving in this direction. However, there are still approaches to continue anonymity in cryptocurrencies for those who want to avoid drawing attention, despite the best attempts of governments in Russia, US, and elsewhere.

The findings from testing *H5* and the IPMA show that among the significant trust enhancers, perceived traceability has the largest magnitude of effect for consumers. It is an unexplored concept in existing literature regarding cryptocurrencies. Although traceability relates and performs similarly to anonymity and privacy, it is more concerned with specific transactions. Most cryptocurrencies have publicly verified records of transactions, which is in contrast to traditional payment schemes that merely involve the buyer, seller, and verifier. Having multiple nodes holding records that can trace transactions back to a single wallet could be alarming to people used to traditional payment schemes. Therefore, the lack of technical understanding among non-technical users and their inability to correctly perceive how blockchain traceability works may cause a stronger traceability – trust relationship.

The results obtained from this empirical investigation indicate the lack of adequate understanding towards privacy and security aspects of crypto-payment. In particular, younger consumers generally feel more confident about their online skills and know-how [105], [106], which may in turn encourage risk-taking behaviors and make them more vulnerable to privacy and security threats. More specifically, the non-significant impact of perceived information security fraud risk on perceived trust highlights the need for enhancing consumers' awareness of potential information security issues that may come with crypto-payment services and how they can be avoided. Again, this is an important consideration for younger consumers in view of previous findings that demonstrated lower levels of information security awareness [107] and higher likelihood of adopting poorer security practices among this group of individuals [108]. In the literature, there also exists evidence that they feel more confident and less concerned about how to protect their privacy [109], [110]. This, combined with potential misperceptions about privacy in using cryptocurrencies, underlines the need for increasing consumer privacy awareness in the context of crypto-payment.

The exploratory model presented in this paper contributes to the limited scholarly knowledge on how consumers build trust in using cryptocurrencies as a payment method. It takes a step towards a theory of user trust for cryptocurrencies based on perceptions about characteristics of the underlying technology. The findings provide insights into perceptions of consumers towards privacy and security aspects of cryptocurrencies and the way it may shape their behavioral intentions to use crypto-payment. The research also responds to the need for revisiting current understanding of elements of consumer trust in the context of e-commerce and online retail considering possible major shifts due to the ever-increasing penetration of cryptocurrencies.

From the practical point of view, this study sheds light on the features of cryptocurrencies that need to be further developed to be effectively used as a method of payment. In this regard, it characterizes important prerequisites stemming from end-user attitudes and perceptions. The findings demonstrate that users expect high degrees of privacy, anonymity, and traceability from cryptocurrencies to rely on them as a trustworthy means for payment purposes. More importantly, the findings reveal that consumers may have misperceptions about cryptocurrencies and their features. Such misperceptions may result in major discrepancies between user expectations and experiences at the early stages of adoption, which may in turn negatively influence intentions towards continuous use. The concerns related to user misunderstanding become more serious with regards to privacy and security aspects. Therefore, enhancing privacy and security awareness about the technology needs to be a priority for the consumer side. Other important considerations pertain to user expectations of anonymity and traceability in crypto-payment as well as impacts of government regulations on their attitudes. These are particularly relevant in view of how a cryptocurrency works and what possibilities it offers as a blockchain-based system.

The findings from the IPMA provide insights on the prioritization of practical activities pertaining to privacy and security aspects of using cryptocurrencies by individual consumers in e-commerce and online retail. In particular, the analysis indicates that traceability of payment transactions should be given the highest priority among other factors. It also suggests that mitigation of consumer privacy risks is one of the top considerations. The findings further emphasize building consumer trust in crypto-payment as a key antecedent of its public acceptance.

VII. CONCLUSION

The field of cryptocurrency is becoming more vibrant and moving to the mainstream by being used in a growing number of applications. This calls for a more nuanced understanding of user perceptions, preferences, and attitudes towards cryptocurrencies, particularly when it comes to new frontiers of application such as crypto-payment. Users may fail to determine the kind of direct peer-to-peer transactions in an anonymous setting and the basic requirements of real-time transactions. Such issues may hinder utilitarian adoption of cryptocurrencies for payment purposes. Given how fragmented the current state of crypto-payment standards and regulations is, potential users need trustworthy solutions that offer them higher anonymity and traceability along with lower privacy and security risks. These highlight technical aspects of crypto-payment services that need further development to address consumer concerns and promote wider acceptance of the technology. In addition to that, there is a need for an enhancement of consumer understanding

of privacy and security features of crypto-payment to avoid misperceptions in this regard. Increasing awareness of potential information security fraud risks and vulnerabilities in this context is of particular importance for consumers.

All in all, the findings from this research provide evidence regarding the significance of incorporating information privacy and security considerations for cryptocurrencies to achieve greater acceptance and be brought into the mainstream use beyond the investment purposes. These considerations should not only be reflected in technical requirements and specifications of cryptocurrencies, but should also involve raising awareness and rectifying misperceptions on the end-user side. The findings in this regard add to the scant literature on determinants of crypto-payment adoption by providing new empirical insights into the facilitators and barriers to consumer trust pertaining to privacy and security aspects. At a higher level, the research also advances scholarly knowledge on the implications and impacts of consumers' privacy and security perceptions of new technologies in the context of B2C e-commerce and e-payment. In terms of practical contributions, the research identifies important prerequisites of crypto-payment success. Moreover, the results have implications on cryptocurrencies that can better meet user expectations, so that they can gain more acceptance to be used for crypto-payment.

This study has limitations that are associated with the nature of empirical research settings. The sample was restricted to undergraduate students from a single Canadian university. Although statistical analysis provided evidence for external validity and generalizability of the findings, the resulting inferences should be applied to other settings with caution. This study did not address the impact of consumer age, education, and other potentially relevant considerations such as technology readiness or contextual factors. This necessitates future investigations that look over such considerations, for instance through comparative analyses among different consumer groups.

The research on cryptocurrency adoption is still at the early stages, particularly in view of immaturity and rapid changes in the landscape. For future research, it is imperative to examine other aspects of user trust in cryptocurrencies, including those that go beyond the features of the technology itself. Price manipulation and volatility are examples of such aspects. More frequent and potentially drastic market fluctuations may pose a significant challenge to the use of cryptocurrencies for payment purposes as consumers may find it more reasonable not to spend cryptocurrencies for purchasing goods or services but hold them as an investment. Further research involving a longitudinal study is also needed to unfold how perceptions of non-users towards crypto-payment may change after actual use. In addition to understanding consumer perceptions towards crypto-payment, providing more nuanced insights into drivers and barriers of adoption at the organizational level is an important topic for future research.

ACKNOWLEDGMENT

Toronto Metropolitan University (formerly Ryerson University) is in the "Dish With One Spoon Territory," which is a treaty between the Anishinaabe, Mississaugas, and Haudenosaunee that bound them to share the territory and protect the land. Subsequent Indigenous Nations and people, Europeans and all newcomers, have been invited into this treaty in the spirit of peace, friendship, and respect. The authors thank them for allowing them to conduct research on their land.

REFERENCES

[1] M. H. Joo, Y. Nishikawa, and K. Dandapani, "Cryptocurrency, a successful application of blockchain technology," *Managerial Finance*, vol. 46, no. 6, pp. 715–733, Aug. 2019.

[2] E. D. Zamani and G. M. Giaglis, "With a little help from the miners: Distributed ledger technology and market disintermediation," *Ind. Manage. Data Syst.*, vol. 118, no. 3, pp. 637–652, Apr. 2018.

[3] J. H. Yu, J. Kang, and S. Park, "Information availability and return volatility in the bitcoin market: Analyzing differences of user opinion and interest," *Inf. Process. Manage.*, vol. 56, no. 3, pp. 721–732, May 2019.

[4] B. E. Mykulyak, "Facilitating online crypto-payments now and in the future," in *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries*. U.K.: Wiley, 2019, pp. 132–133.

[5] J. C. Mendoza-Tello, H. Mora, F. A. Pujol-Lopez, and M. D. Lytras, "Social commerce as a driver to enhance trust and intention to use cryptocurrencies for electronic payments," *IEEE Access*, vol. 6, pp. 50737–50751, 2018.

[6] N. Jonker, "What drives the adoption of crypto-payments by online retailers?" *Electron. Commerce Res. Appl.*, vol. 35, May 2019, Art. no. 100848.

[7] H. B. B. Doyduk, "Impact of digital technology and the use of blockchain technology from the consumer perspective," in *Blockchain Economics and Financial Market Innovation*. Cham, Switzerland: Springer, 2019, pp. 271–292.

[8] H. Yun, G. Lee, and D. J. Kim, "A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs," *Inf. Manage.*, vol. 56, no. 4, pp. 570–601, Jun. 2019.

[9] R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102376.

[10] Y. Jung and J. Park, "An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services," *Int. J. Inf. Manage.*, vol. 43, pp. 15–24, Dec. 2018.

[11] C. Mombeuil and H. Uhde, "Relative convenience, relative advantage, perceived security, perceived privacy, and continuous use intention of China's WeChat pay: A mixed-method two-phase design study," *J. Retailing Consum. Services*, vol. 59, Mar. 2021, Art. no. 102384.

[12] M. Garaus and H. Treiblmaier, "The influence of blockchain-based food traceability on retailer choice: The mediating role of trust," *Food Control*, vol. 129, Nov. 2021, Art. no. 108082.

[13] D. Sirdeshmukh, J. Singh, and B. Sabol, "Consumer trust, value, and loyalty in relational exchanges," *J. Marketing*, vol. 66, no. 1, pp. 15–37, Jan. 2002.

[14] C. F. Herrera and C. F. Blanco, "Consequences of consumer trust in PDO food products: The role of familiarity," *J. Product Brand Manage.*, vol. 20, no. 4, pp. 282–296, Jul. 2011.

[15] L. Herskind, P. Katsikouli, and N. Dragoni, "Privacy and cryptocurrencies—A systematic literature review," *IEEE Access*, vol. 8, pp. 54044–54059, 2020.

[16] E. Badawi and G.-V. Jourdan, "Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review," *IEEE Access*, vol. 8, pp. 200021–200037, 2020.

[17] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[18] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and blockchain: Security and privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10288–10313, Oct. 2020.

[19] L.-H. Zhu, B.-K. Zheng, M. Shen, F. Gao, H.-Y. Li, and K.-X. Shi, "Data security and privacy in bitcoin system: A survey," *J. Comput. Sci. Technol.*, vol. 35, no. 4, pp. 843–862, Jul. 2020.

[20] T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, Jul. 2019, pp. 362–367.

[21] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, p. 121, 2018.

[22] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, 2019.

[23] N. Verma, S. Jain, and R. Doriya, "Review on consensus protocols for blockchain," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, Feb. 2021, pp. 281–286.

[24] R. Longo, A. S. Podda, and R. Saia, "Analysis of a consensus protocol for extending consistent subchains on the bitcoin blockchain," *Computation*, vol. 8, no. 3, p. 67, Jul. 2020.

[25] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[26] A. Alshamsi and P. P. Andras, "User perception of bitcoin usability and security across novice users," *Int. J. Hum.-Comput. Stud.*, vol. 126, pp. 94–110, Jun. 2019.

[27] M. Fröhlich, F. Gutjahr, and F. Alt, "Don't lose your coin! Investigating security practices of cryptocurrency users," in *Proc. ACM Designing Interact. Syst. Conf.*, Jul. 2020, pp. 1751–1763.

[28] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl, "The other side of the coin: User experiences with bitcoin security and privacy," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Berlin, Germany, 2016, pp. 555–580.

[29] A. Manimuthu, G. Rejikumar, and D. Marwaha, "A literature review on bitcoin: Transformation of crypto currency into a global phenomenon," *IEEE Eng. Manage. Rev.*, vol. 47, no. 1, pp. 28–35, Mar. 2019.

[30] D. Folkinshteyn and M. Lennon, "Braving bitcoin: A technology acceptance model (TAM) analysis," *J. Inf. Technol. Case Appl. Res.*, vol. 18, no. 4, pp. 220–249, 2016.

[31] W. Presthus and N. O'Malley, "Motivations and barriers for end-user adoption of bitcoin as digital currency," *Proc. Comput. Sci.*, vol. 121, pp. 89–97, Jan. 2017.

[32] I. Almarashdeh, H. M. Bouzkraoui, A. Azoui, H. Youssef, L. Niharmine, A. A. Rahman, and N. P. Jagini, "An overview of technology evolution: Investigating the factors influencing non-bitcoins users to adopt bitcoins as online payment transaction method," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 13, pp. 3984–3993, 2018.

[33] F. Shahzad, G. Xiu, J. Wang, and M. Shahbaz, "An empirical investigation on the adoption of cryptocurrencies among the people of mainland China," *Technol. Soc.*, vol. 55, pp. 33–40, Nov. 2018.

[34] M. Arias-Oliva, J. Pelegrín-Borondo, and G. Matías-Clavero, "Variables influencing cryptocurrency use: A technology acceptance model in Spain," *Frontiers Psychol.*, vol. 10, p. 475, Mar. 2019.

[35] A. J. Walton and K. A. Johnston, "Exploring perceptions of bitcoin adoption: The South African virtual community perspective," *Interdiscipl. J. Inf., Knowl., Manage.*, vol. 13, pp. 165–182, 2018.

[36] B. A. Soomro, N. Shah, and N. A. A. Abdelwahed, "Intention to adopt cryptocurrency: A robust contribution of trust and the theory of planned behavior," *J. Econ. Administ. Sci.*, Jan. 2022.

[37] O. Sohaib, W. Hussain, M. Asif, M. Ahmad, and M. Mazzara, "A PLS-SEM neural network approach for understanding cryptocurrency adoption," *IEEE Access*, vol. 8, pp. 13138–13150, 2019.

[38] A. Alharbi and O. Sohaib, "Technology readiness and cryptocurrency adoption: PLS-SEM and deep learning neural network analysis," *IEEE Access*, vol. 9, pp. 21388–21394, 2021.

[39] H. Treiblmaier, D. Leung, A. O. J. Kwok, and A. Tham, "Cryptocurrency adoption in travel and tourism—An exploratory study of Asia Pacific travellers," *Current Issues Tourism*, vol. 24, no. 22, pp. 3165–3181, Nov. 2021.

[40] C. Kim, W. Tao, N. Shin, and K.-S. Kim, "An empirical study of customers' perceptions of security and trust in e-payment systems," *Electron. Commerce Res. Appl.*, vol. 9, no. 1, pp. 84–95, Jan. 2010.

[41] S. A. Salloum and M. Al-Emran, "Factors affecting the adoption of e-payment systems by University students: Extending the TAM with trust," *Int. J. Electron. Bus.*, vol. 14, no. 4, pp. 371–390, 2018.

[42] L. Gao and K. A. Waechter, "Examining the role of initial trust in user adoption of mobile payment services: An empirical investigation," *Inf. Syst. Frontiers*, vol. 19, no. 3, pp. 525–548, Jun. 2017.

[43] P. Patil, K. Tamilmani, N. P. Rana, and V. Raghavan, "Understanding consumer adoption of mobile payment in India: Extending meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal," *Int. J. Inf. Manage.*, vol. 54, Oct. 2020, Art. no. 102144.

[44] J. Benamati, M. A. Fuller, M. A. Serva, and J. Baroudi, "Clarifying the integration of trust and TAM in e-commerce environments: Implications for systems design and management," *IEEE Trans. Eng. Manag.*, vol. 57, no. 3, pp. 380–393, Aug. 2009.

[45] Y. W. Sullivan and D. J. Kim, "Assessing the effects of consumers' product evaluations and trust on repurchase intention in e-commerce environments," *Int. J. Inf. Manage.*, vol. 39, pp. 199–219, Apr. 2018.

[46] H. Hallikainen and T. Laukkanen, "National culture and consumer trust in e-commerce," *Int. J. Inf. Manage.*, vol. 38, no. 1, pp. 97–106, Feb. 2018.

[47] A. Joinson, U.-D. Reips, T. Buchanan, and C. B. P. Schofield, "Privacy, trust, and self-disclosure online," *Hum. Comput. Interact.*, vol. 25, no. 1, pp. 1–24, Jan. 2010.

[48] K. Martin, "The penalty for privacy violations: How privacy violations impact trust online," *J. Bus. Res.*, vol. 82, pp. 103–116, Jan. 2018.

[49] U. Klinger and J. Svensson, "The end of media logics? On algorithms and agency," *New Media Soc.*, vol. 20, no. 12, pp. 4653–4670, Dec. 2018.

[50] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, Mar. 2006.

[51] C. Liu, J. T. Marchewka, J. Lu, and C. S. Yu, "Beyond concern—A privacy-trust-behavioral intention model of electronic commerce," *Inf. Manage.*, vol. 42, no. 2, pp. 289–304, Jan. 2005.

[52] H. Damghanian, A. Zarei, and M. A. S. Kojuri, "Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran," *J. Internet Commerce*, vol. 15, no. 3, pp. 214–238, Jul. 2016.

[53] J. Khalilzadeh, A. B. Ozturk, and A. Bilgihan, "Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry," *Comput. Hum. Behav.*, vol. 70, pp. 460–474, May 2017.

[54] E. B. Ponte, E. Carvajal-Trujillo, and T. Escobar-Rodríguez, "Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents," *Tourism Manage.*, vol. 47, pp. 286–302, Apr. 2015.

[55] J. Fan, M. Shao, Y. Li, and X. Huang, "Understanding users' attitude toward mobile payment use: A comparative study between China and the USA," *Ind. Manage. Data Syst.*, vol. 118, no. 3, pp. 524–540, Apr. 2018.

[56] J. Woo, "The right not to be identified: Privacy and anonymity in the interactive media environment," *New Media Soc.*, vol. 8, no. 6, pp. 949–967, Dec. 2006.

[57] S. C. Robinson, "Self-disclosure and managing privacy: Implications for interpersonal and online communication for consumers and marketers," *J. Internet Commerce*, vol. 16, no. 4, pp. 385–404, Oct. 2017.

[58] D. D. Steinauer, S. A. Wakid, and S. Rasberry, "Trust and traceability in electronic commerce," *StandardView*, vol. 5, no. 3, pp. 118–124, Sep. 1997.

[59] N. Jailani, N. F. M. Yatim, Y. Yahya, A. Patel, and M. Othman, "Secure and auditable agent-based e-marketplace framework for mobile users," *Comput. Standards Interface*, vol. 30, no. 4, pp. 237–252, May 2008.

[60] Y. Lu, S. Yang, P. Y. K. Chau, and Y. Cao, "Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective," *Inf. Manage.*, vol. 48, no. 8, pp. 393–403, 2011.

[61] M. H. U. Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1196–1212, Nov. 2019.

[62] J. Koroma, Z. Rongting, S. Muhideen, T. Y. Akintunde, T. S. Amosun, S. J. Dauda, and I. A. Sawaneh, "Assessing citizens' behavior towards blockchain cryptocurrency adoption in the Mano River Union States: Mediation, moderation role of trust and ethical issues," *Technol. Soc.*, vol. 68, Feb. 2022, Art. no. 101885.

[63] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quart.*, vol. 35, no. 4, pp. 989–1016, Dec. 2011.

[64] A. Bergström, "Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses," *Comput. Hum. Behav.*, vol. 53, pp. 419–426, Dec. 2015.

[65] D. D. H. Shin, "Blockchain: The emerging technology of digital trust," *Telematics Informat.*, vol. 45, Dec. 2019, Art. no. 101278.

[66] K. A. Wallace, "Anonymity," *Ethics Inf. Technol.*, vol. 1, no. 1, pp. 21–31, 1999.

[67] R. Werner, S. Lawrenz, and A. Rausch, "Blockchain analysis tool of a cryptocurrency," in *Proc. 2nd Int. Conf. Blockchain Technol.*, Mar. 2020, pp. 80–84.

[68] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and Privacy in Social Networks*. New York, NY, USA: Springer, 2013, pp. 197–223.
[69] G. Fanti, S. B. Venkatakrishnan, S. Bakshi, B. Denby, S. Bhargava, A. Miller, and P. Viswanath, "Dandelion++ lightweight cryptocurrency networking with formal anonymity guarantees," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 2, no. 2, pp. 1–35, 2018.
[70] C. Remy, B. Rym, and L. Matthieu, "Tracking bitcoin users activity using community detection on a network of weak signals," in *Proc. Int. Conf. Complex Netw. Appl.* Cham, Switzerland: Springer, 2017, pp. 166–177.
[71] G. Kanwalinderjit, "Traceability of cryptocurrency transactions using blockchain analytics," *Int. J. Comput. Digit. Syst.*, vol. 9, no. 2, pp. 159–165, Jan. 2020.
[72] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names," in *Proc. Conf. Internet Meas. Conf.*, Oct. 2013, pp. 127–140.
[73] M. Polasik, A. I. Piotrowska, T. P. Wisniewski, R. Kotkowski, and G. Lightfoot, "Price fluctuations and the use of bitcoin: An empirical inquiry," *Int. J. Electron. Commerce*, vol. 20, no. 1, pp. 9–49, Sep. 2015.
[74] T. Ermakova, B. Fabian, A. Baumann, M. Izmailov, and H. Krasnova, "Bitcoin: Drivers and impediments," SSRN, Rochester, NY, USA, Tech. Rep. 3017190, 2017.
[75] N. Alsalami and B. Zhang, "SoK: A systematic study of anonymity in cryptocurrencies," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Nov. 2019, pp. 1–9.
[76] D. Harborth, S. Pape, and K. Rannenberg, "Explaining the technology use behavior of privacy-enhancing technologies: The case of Tor and JonDonym," *Proc. Privacy Enhancing Technol.*, vol. 2020, no. 2, pp. 111–128, Apr. 2020.
[77] M. Linton, E. G. S. Teo, E. Bommes, C. Y. Chen, and W. K. Härdle, "Dynamic topic modelling for cryptocurrency community forums," in *Applied Quantitative Finance*. Berlin, Germany: Springer, 2017, pp. 355–372.
[78] S. Abramova and R. Böhme, "Perceived benefit and risk as multidimensional determinants of bitcoin use: A quantitative exploratory study," in *Proc. 37th Int. Conf. Inf. Syst.*, Dublin, Republic of Ireland, 2016, pp. 1–20.
[79] J. E. Klobas, T. McGill, and X. Wang, "How perceived security risk affects intention to use smart home devices: A reasoned action explanation," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101571.
[80] S. K. Ooi, C. A. Ooi, J. A. L. Yeap, and T. H. Goh, "Embracing bitcoin: Users' perceived security and trust," *Qual. Quantity*, vol. 55, no. 4, pp. 1219–1237, Aug. 2021.
[81] H. Stewart and J. Jürjens, "Data security and consumer trust in FinTech innovation in Germany," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 109–128, Mar. 2018.
[82] T. P. Wilson and W. R. Clarke, "Food safety and traceability in the agricultural supply chain: Using the Internet to deliver traceability," *Supply Chain Manage., Int. J.*, vol. 3, no. 3, pp. 127–133, Sep. 1998.
[83] X. Gellynck and W. Verbeke, "Consumer perception of traceability in the meat chain," *German J. Agricult. Econ.*, vol. 50, no. 6, pp. 368–374, 2001.
[84] M. A. Shareef, A. Baabdullah, S. Dutta, V. Kumar, and Y. K. Dwivedi, "Consumer adoption of mobile banking services: An empirical examination of factors according to adoption stages," *J. Retailing Consum. Services*, vol. 43, pp. 54–67, Jul. 2018.
[85] A. Robertson, "Measuring perceived anonymity: The development of a context independent instrument," *J. Methods Meas. Social Sci.*, vol. 5, no. 1, pp. 22–39, Sep. 2014.
[86] S. Carpenter, "Ten steps in scale development and reporting: A guide for researchers," *Commun. Methods Measures*, vol. 12, no. 1, pp. 25–44, Jan. 2018.
[87] M. Z. Alam, W. Hu, M. A. Kaium, M. R. Hoque, and M. M. D. Alam, "Understanding the determinants of mHealth apps adoption in Bangladesh: A SEM-neural network approach," *Technol. Soc.*, vol. 61, May 2020, Art. no. 101255.
[88] C. S. Henry, K. P. Huynh, and G. Nicholls, "Bitcoin awareness and usage in Canada," *J. Digit. Banking*, vol. 2, no. 4, pp. 311–337, 2018.
[89] Z. Yan, T. Robertson, R. Yan, S. Y. Park, S. Bordoff, Q. Chen, and E. Sprissler, "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?" *Comput. Hum. Behav.*, vol. 84, pp. 375–382, Jul. 2018.
[90] J. S. Armstrong and T. S. Overton, "Estimating nonresponse bias in mail surveys," *J. Marking Res.*, vol. 14, no. 3, pp. 396–402, Aug. 1977.
[91] P. M. Podsakoff and D. W. Organ, "Self-reports in organizational research: Problems and prospects," *J. Manage.*, vol. 12, no. 4, pp. 531–544, 1986.
[92] C. M. Ringle, S. Wende, and J.-M. Becker. (2015). SmartPLS 3, SmartPLS. GmbH. Bönningstedt, Germany. [Online]. Available: http://www.smartpls.com
[93] W. W. Chin, B. L. Marcolin, and P. R. Newsted, "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study," *Inf. Syst. Res.*, vol. 14, no. 2, pp. 189–217, 2003.
[94] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a silver bullet," *J. Marketing Theory Pract.*, vol. 19, no. 2, pp. 139–152, 2011.
[95] C.-F. Chen and O. Myagmarsuren, "Exploring relationships between Mongolian destination brand equity, satisfaction and destination loyalty," *Tourism Econ.*, vol. 16, no. 4, pp. 981–994, Dec. 2010.
[96] J. F. Hair, Jr., G. T. M. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Berkeley, CA, USA: Sage, 2016.
[97] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. Marketing Res.*, vol. 18, no. 1, pp. 39–50, Feb. 1981.
[98] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Marketing Sci.*, vol. 43, no. 1, pp. 115–135, 2015.
[99] J. Fox, *Applied Regression Analysis and Generalized Linear Models*. Berkeley, CA, USA: Sage, 2015.
[100] L.-T. Hu and P. M. Bentler, "Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification," *Psychol. Methods*, vol. 3, no. 4, p. 424, 1998.
[101] J. Henseler, C. M. Ringle, and R. R. Sinkovics, "The use of partial least squares path modeling in international marketing," *Adv. Int. Marketing*, vol. 20, pp. 277–320, Mar. 2009.
[102] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*. New York, NY, USA: Academic, 2013.
[103] M. Tenehaus, V. E. Vinzi, Y.-M. Chatelin, and C. Lauro, "PLS path modeling," *Comput. Statist. Data Anal.*, vol. 48, no. 1, pp. 159–205, 2005.
[104] C. M. Ringle and M. Sarstedt, "Gain more insight from your PLS-SEM results: The importance-performance map analysis," *Ind. Manage. Data Syst.*, vol. 116, no. 9, pp. 1865–1886, Oct. 2016.
[105] C. Jones, R. Ramanau, S. Cross, and G. Healing, "Net generation or digital natives: Is there a distinct new generation entering university?" *Comput. Educ.*, vol. 54, no. 3, pp. 722–732, Apr. 2010.
[106] A. Malik, K. Hiekkanen, and M. Nieminen, "Privacy and trust in Facebook photo sharing: Age and gender differences," *Program*, vol. 50, no. 4, pp. 462–480, Sep. 2016.
[107] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Comput. Hum. Behav.*, vol. 69, pp. 151–156, Apr. 2017.
[108] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, Mar. 2018.
[109] I. D. Anic, V. Škare, and I. K. Milaković, "The determinants and effects of online privacy concerns in the context of e-commerce," *Electron. Commerce Res. Appl.*, vol. 36, Jul. 2019, Art. no. 100868.
[110] C. L. Miltgen and D. Peyrat-Guillard, "Cultural and generational influences on privacy concerns: A qualitative study in seven European countries," *Eur. J. Inf. Syst.*, vol. 23, no. 2, pp. 103–125, Mar. 2014.

ATEFEH MASHATAN is an Associate Professor with the Ted Rogers School of Information Technology Management. She is a Canada Research Chair (Tier II) with Quality of Security Framework for the Internet of Things. Her research interests include development of novel cybersecurity designs based on emerging technologies, such as the IoT, blockchain, and quantum computing. Her expertise at the frontlines of the global cybersecurity field was recognized by SC Magazine, in 2019, when she was named one of the top five Women of Influence in Security. She was recognized as one of Canada's Top 19 of 2019 Tech Titans at IBM CASCON Evoke Conference. In 2020, she received the Enterprise Blockchain Award in the category of New Frontiers at Blockchain Academic Research, Blockchain Research Institute. She received the recognition of Top 20 Women in Cybersecurity, Canada, for her efforts in advancing cybersecurity research.

MOHAMAD SADEGH SANGARI received the B.Sc., M.Sc., and Ph.D. degrees in industrial engineering from University of Tehran, Iran. He is a Postdoctoral Researcher with the Cybersecurity Research Laboratory (CRL), Ted Rogers School of Management. He conducts research on adoption and impacts of emerging information technologies and systems (IT/IS), particularly beyond the organizational boundaries, to address business challenges and requirements to realize the potentials of IT/IS at strategic and operational levels. His main expertise lies in the areas of supply chain management as well as customer and user relations. Recently, he has also been conducting research on human aspects of cybersecurity by focusing on users' security and privacy concerns, decisions, and behaviors. His research interests include application of multivariate data analysis, machine learning, and optimization and decision analysis methods. His previous works have been published in several outlets, such as *The International Journal of Logistics Management*, *Advances in Engineering Software*, *Annals of Operations Research*, *International Journal of Production Economics*, and *The Service Industries Journal*.

MILAD DEHGHANI received the Ph.D. degree in technology management and industrial engineering from the Sapienza University of Rome, Italy, in 2017. He held several academic positions as a Postdoctoral Fellow and a Research Associate in Canada and Hong Kong, respectively. He is a Research Fellow and a Lecturer with the University College Cork (UCC), Ireland. He is also a Research Advisor in related IPs with Fexco Company—part of a multi-million-euro co-funded project called FINTECHNEXT. He primarily investigates digital innovation, ICT adoption, and technology analysis and forecasting. He has a proven track record of research in top-tier journals and actively engages as a guest editor and an ad-hoc reviewer in more than 12 technological and innovation journals.