Bitcoin adoption: Scams and anonymity may not matter but trust into Bitcoin security does

Aleksander Murko
aleksander.murko@student.um.si
University of Maribor
Ljubljana, Slovenia

Simon L. R. Vrhovec
simon.vrhovec@um.si
University of Maribor
Ljubljana, Slovenia

ABSTRACT

Bitcoin is the most successful cryptocurrency with more than half of the market capitalization of all more than 2,000 currently existing cryptocurrencies. In recent years, there have been several high-profile hacks and scams that resulted in billions of stolen funds. In this paper, we focus on the impact of Bitcoin cybersecurity and privacy characteristics on its adoption. A survey (N = 152) has been conducted among users and non-users of Bitcoin in Slovenia to test the proposed research model. The results suggest that in addition to known factors (i.e., usefulness, ease of use and subjective norm) trust into Bitcoin security also influences Bitcoin adoption. The results however show no support for the influence of perceived threat of Bitcoin scams or Bitcoin anonymity on Bitcoin adoption.

CCS CONCEPTS

• **Social and professional topics → Computer crime**; • **Security and privacy → Pseudonymity, anonymity and untraceability**; • **Networks → Network privacy and anonymity**;

KEYWORDS

scam, anonymity, trust, adoption, Bitcoin, cryptocurrency

ACM Reference Format:
Aleksander Murko and Simon L. R. Vrhovec. 2019. Bitcoin adoption: Scams and anonymity may not matter but trust into Bitcoin security does. In *Central European Cybersecurity Conference (CECC 2019), November 14–15, 2019, Munich, Germany.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3360664.3360679

1 INTRODUCTION

In roughly ten years of their existence, cryptocurrencies became a major industry [37]. Media attention has pushed the adoption of cryptocurrencies around the world and many businesses are increasingly adopting them as an alternative payment method [31]. When they first appeared, cryptocurrencies were associated with their use for criminal transactions on the darknet and cybercrime in general [10]. However, this no longer seems to be true in 2019 as cryptocurrencies are valid payment methods for purchasing various goods and services on platforms, such as Overstock.com, eGifter, Newegg, Shopify stores, Dish, Roadway Moving Company, Microsoft, CheapAir and many individual merchants worldwide [30]. Currently, 2,202 different cryptocurrencies exist with a market capitalization of $261,838,304,350 [3, 12]. Bitcoin is considered as the most successful cryptocurrency of all time with a market capitalization of $179,060,450,159 [5, 12].

High market capitalization and the use of cyberspace make cryptocurrencies an attractive target for cybercriminals. For years, the media has been filled with news of high-profile hacks, such as Mt. Gox (2014, $460 million) [15, 25], NiceHash (2017, $78 million) [33], Coincheck (2018, $530 million) [22], BitGrail (2018, $195 million) [22], Zaif (2018, $60 million) [22], Coinrail (2018, $40 million) [22], Bithumb (2018, $30 million) [22], and most recently Binance (2019, $40.7 million) [14]. Threats to cryptocurrency users are complemented by scams, such as Ponzi schemes, wallet and exchange scams. The number of scams appears to be rising [3, 11] although they do not seem to receive as much media attention as hacks. Also, the amounts seem to be much lower (e.g., $11 million from 192 studied scams [41]).

The adoption of new technologies, such as cryptocurrencies, is influenced by both their characteristics and the social influence on the adopting individual [13, 44]. There is however a gap in research on how cybersecurity and privacy-related characteristics of new technologies, such as anonymity and trust, may influence their adoption. This paper aims to address this gap by studying factors that may influence Bitcoin adoption (i.e., behavioral intention to use Bitcoin for paying) in addition to the three key adoption factors, namely usefulness, ease of use and subjective norm [13, 44]. To achieve this, we focused on studying the associations between trust into Bitcoin security, perceived Bitcoin anonymity and perceived threat of Bitcoin scams, and behavioral intention for paying with Bitcoin.

2 THEORETICAL BACKGROUND

2.1 Bitcoin in a nutshell

Bitcoin is well-known for being the first cryptocurrency [37]. It was introduced in an anonymous paper in 2008 under the pseudonym Satoshi Nakamoto [26, 32]. It was developed to be a kind of electronic cash that would allow people to send it from one party to another without any brokers in between [32]. Bitcoin works on cryptographic protocols in distributed network of users which are mining, storing and transferring digital currency [7, 32]. Bitcoin is operating in an open and fully decentralized system and Bitcoins can be considered as digital coins which are not issued by any government or state regulatory organization [2, 7]. To achieve this, Bitcoin works on a data structure called the blockchain [40]. First

CECC 2019, November 14–15, 2019, Munich, Germany

ACM ISBN 978-1-4503-7296-1/19/11…$15.00
https://doi.org/10.1145/3360664.3360679

application of blockchain was introduced with Bitcoin [19]. As the name implies, blockchain allows the creation of blocks of data on top of existing ones and connecting them into a chain [32]. It is a platform that supports peer-to-peer transactions, tracking and more [32].

As the first cryptocurrency, Bitcoin was adopted in a very short time and raised its economic value to substantial amounts and today it is considered as the most successful cryptocurrency in all history currently holding a 68 percent revenue market share [5, 12]. At first, Bitcoin was adopted without any thorough analysis of the structure and design of its system [2]. Bitcoin and other cryptocurrencies received a lot of media attention that significantly contributed to the popularity of cryptocurrencies today [1, 7]. However, popularity and high value make Bitcoin an attractive target for cybercriminals looking for naive and undereducated users [2]. Additionally, the risk of Bitcoin scams and other related threats is increased by the irreversibility of Bitcoin transactions and decentralization which impedes effective law enforcement countermeasures [28, 41].

2.2 Bitcoin scams

Bitcoin scams can be categorized into four groups: Ponzi schemes (also high-yield investment programs), mining investment scams, scam wallet services, and fraudulent exchanges [41]. *Ponzi schemes* are fraudulent investment schemes which repay existing investors with contributions of new investors joining the scheme [4, 41]. They implode when it is no longer possible to find new investors therefore they rely on advertising to stay in business [4, 42]. When these schemes collapse, they are replaced by new ones often run by the same cybercriminals [41]. *Mining investment scams* are exploiting people's interest in Bitcoin mining by offering profitability without a large up-front investment in expensive mining hardware [41]. These scams take payments however never deliver the promised product [41]. *Scam wallet services* offer similar features to online wallets and sought-after services, such as mixing that enhance transaction anonymity for customers [41]. The key difference is however that its operators siphon some or all incoming transfers [41]. Typically, scam wallets transfer the money into their own wallet only if it is above a certain threshold and keep it in the customers' wallet if it is not [41]. Mining investment scams and scam wallets may be rather considered as Ponzi schemes if they have promise high profits for investments (e.g., offer daily return on savings) [41]. *Fraudulent exchanges* are pretending to be Bitcoin exchanges [41]. They attract customers by offering features that other exchanges do not offer, such as PayPal or credit card processing or an attractive exchange rate [41].

2.3 Bitcoin adoption

In adoption, there are five major categories of adopters: innovators (approx. 2.5 percent), early adopters (approx. 13.5 percent), early majority (approx. 34 percent), late majority (approx. 34 percent) and laggards (approx. 16 percent) [6, 45]. *Innovators* are typically adventurous technology experts who are willing to take the risks and potential failure when adopting new technology [45]. The *early majority* are typically trying to weigh out whether to adopt new technology or not. *Late majority* are average members in a social system and must be very highly convinced or pressured by the society and surrounding people to adopt new technology. *Laggards* are taking new technology with suspicion and are adopting new technology at that point when innovators are already taking steps towards adopting the next new technology [45].

According to adoption research, there are three key factors driving adoption of new technologies, such as Bitcoin and other cryptocurrencies: usefulness, ease of use and subjective norm [13, 44]. First, individuals are more likely to adopt new technology if they perceive it as useful (e.g., it helps them to perform better their everyday tasks) [13, 43]. Next, if new technology is too hard for usage, it will not be adopted because its benefits will not outweigh the effort to use it [13, 43]. Finally, an individual's behavior is influenced by the way they believe others will see them as a result of having used new technology [44].

3 RESEARCH MODEL

The proposed research model is presented in Figure 1. The constructs and developed hypotheses are described below.

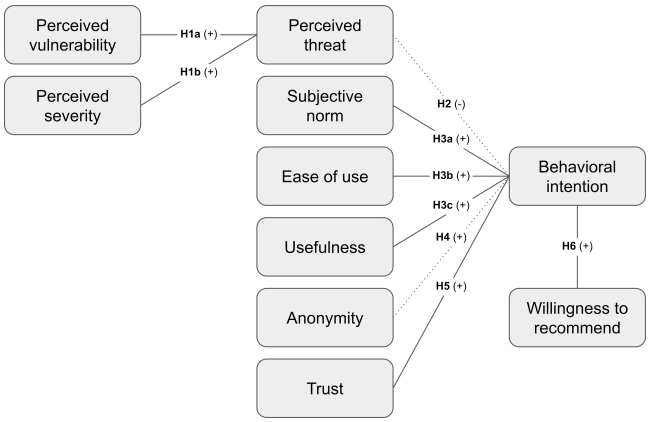

Figure 1: Research model.

Due to their increasing presence and media attention [1], Bitcoin scams may affect the use of Bitcoin. People who feel threatened by Bitcoin scams may not adopt Bitcoin or existing Bitcoin users may use it less likely [9, 23]. Individuals however need to first detect and evaluate Bitcoin scams as a threat to them [17, 27]. Perceived threat is associated with perceived vulnerability (i.e., the likelihood of becoming a victim of a Bitcoin scam) and perceived severity (i.e., the consequences of becoming a victim of a Bitcoin scam) in existing research [16, 24]. We therefore propose the following hypotheses:

H1a: Perceived vulnerability to Bitcoin scams is positively correlated with perceived threat of Bitcoin scams.

H1b: Perceived severity of falling victim to Bitcoin scams is positively correlated with perceived threat of Bitcoin scams.

H2: Perceived threat of Bitcoin scams is negatively correlated with behavioral intention to use Bitcoin for paying.

According to research on the adoption of new technologies, there are three key factors influencing the acceptance of a new technology, namely ease of use (i.e., how easy it is to use new technology), usefulness (i.e., how much does new technology benefit a user's performance), and subjective norm [13, 44]. If new technology is too hard to use, it will not be adopted because its benefits will be outweighed by the effort to use it [13, 29, 34]. Similarly, new technology will not be adopted if it does not provide enough added value for the user [13, 29, 34]. Finally, the opinion of friends and other people someone considers as important to them may influence most his or her adoption of new technology [39, 44]. We therefore suggest the following hypotheses:

H3a: Subjective norm is positively correlated with behavioral intention to use Bitcoin for paying.

H3b: Ease of paying with Bitcoin is positively correlated with behavioral intention to use Bitcoin for paying.

H3c: Usefulness of paying with Bitcoin is positively correlated with behavioral intention to use Bitcoin for paying.

Anonymity is an important implied feature of cash as opposed to money (e.g., on banking accounts) and cryptocurrencies were developed to mimic cash [32]. Bitcoin is a pseudo anonymous cryptocurrency [42] which may also influence the adoption of new technology [35]. Based on these assumptions, we propose the following hypotheses:

H4: Perceived anonymity of Bitcoin users is positively correlated with behavioral intention to use Bitcoin for paying.

Trust is the degree to which individuals perceive Bitcoin to be safe to use either due to the characteristics of its design (e.g., implemented measures for securing transactions) and existing regulation protecting Bitcoin users. Trust into new technology may be an important determinant of its adoption [8, 18, 34, 38] therefore we suggest the following hypothesis:

H5: Trust into the security of using Bitcoin is positively correlated with behavioral intention to use Bitcoin for paying.

Adoption of new technology does not end with the decision of an individual to adopt it. It is a social process in which adopters may influence others, e.g., by recommending new technology to others. Since more satisfied adopters of new technology are more likely to recommend it to others [36], we suggest our final hypothesis:

H6: Behavioral intention to use Bitcoin for paying is positively correlated with the willingness to recommend it to others.

4 METHODS

We conducted an exploratory study by an online survey among members of a Facebook group, a Facebook group chat and a mailing list of University of Maribor students:

- *Kriptovalute - Slovenska Blockchain Skupnost - Bitcoin.si* (14,156 Facebook group members, topic: cryptocurrencies)
- *Active association members of Klub ptujskih študentov* (44 Facebook group chat participants, topic: student association)
- *Faculty of Criminal Justice and Security students* (981 mailing list entries, topic: student mailing list)

The survey was carried out between December 2018 and March 2019. A total of 152 respondents completed the survey (N_{S1} = 83, N_{S2} = 7, N_{S3} = 62). The response rate was 1 percent overall which is low due to a high number of Facebook group members that most likely did not see the post. The response rate of individuals that accessed the introductory survey page was 37.9 percent suggesting a satisfactory response rate of individuals that saw the invitation to complete the survey. The age of respondents was from 16 to 83 years (M = 27.18, SD = 8.96). Other demographic characteristics of respondents are presented in Table 1.

Table 1: Demographic characteristics

Characteristic	N	Percent
Gender		
Male	69	45.4
Female	69	45.4
Not specified	14	9.2
Status		
Student	73	48.0
Employed	60	39.5
Unemployed	5	3.3
Not specified	14	9.2
Education		
Less than bachelor's degree	52	34.2
Bachelor's degree	55	36.2
Master's degree	28	18.4
PhD	3	2.0
Not specified	14	9.2

The questionnaire was designed to measure 10 constructs: perceived vulnerability, perceived severity, perceived threat, subjective norm, ease of use, usefulness, anonymity, trust, behavioral intention, and willingness to recommend. We adapted to the context of our study all survey items from previously validated items. Items for perceived threat, perceived vulnerability and perceived severity were adapted from [24], [21], and [20], respectively. Next, items for subjective norm were adapted from [43]. Items for ease of use and usefulness were adapted from [13]. Survey items for anonymity and trust were adapted from [35] and [38], respectively. Finally, items for behavioral intention were adapted from [9]. Willingness to recommend is a single-item construct adapted from [36]. All items except willingness to recommend were measured using a seven-point Likert scale from 1 (I strongly disagree) to 7 (I strongly agree). Willingness to recommend was measured using an 11-point scale from 0 (very unlikely) to 10 (very likely).

5 RESULTS

To assess the reliability of our questionnaire, we evaluated Cronbach's alpha (CA) of individual constructs. CA values above 0.8 indicate high reliability and CA values above 0.6 are deemed acceptable although CA values above 0.7 are preferred. In our study, CA ranged from 0.629 (anonymity) to 0.954 (behavioral intention) indicating at least acceptable reliability of all constructs. We deemed this adequate for exploratory research such as ours.

To test the research hypotheses, we first aggregated the items for each multi-item construct and then calculated Pearson's correlation coefficients between constructs. The results of hypothesis testing are presented in Figure 2.

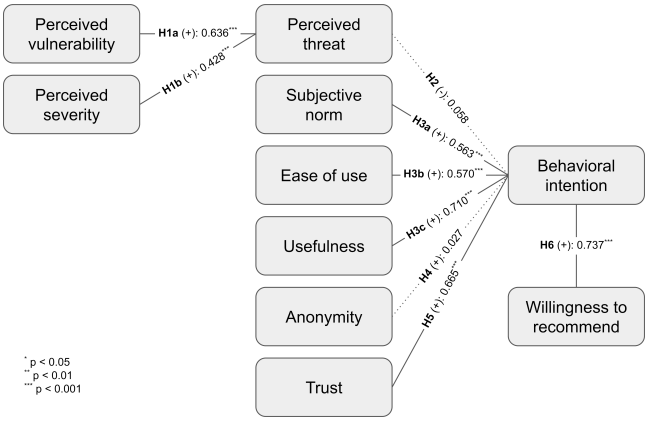

Figure 2: Hypotheses testing results (Pearson's correlation coefficients).

There are positive statistically significant correlations between perceived threat, and perceived vulnerability ($p < 0.001$) and perceived severity ($p < 0.001$). However, the correlation between perceived threat and behavioral intention is not statistically significant. These results show support for hypotheses **H1a** and **H1b** however there is no support for hypothesis **H2**. A positive correlation between subjective norm and behavioral intention is also statistically significant ($p < 0.001$) indicating support for hypothesis **H3a**. Correlations between behavioral intention, and ease of use ($p < 0.001$) and usefulness ($p < 0.001$) are positive and statistically significant supporting both hypotheses **H3b** and **H3c**. The correlation between anonymity and behavioral intention is not statistically significant therefore we cannot neither accept nor reject hypothesis **H4**. There are positive statistically significant correlations between both trust and behavioral intention ($p < 0.001$), and behavioral intention and willingness to recommend ($p < 0.001$) supporting hypotheses **H5** and **H6**, respectively.

6 DISCUSSION

This study provides several implications. First, we build on well-established research on adoption by including factors related to cybersecurity and privacy to improve our understanding of adoption of new technologies that depend on cyberspace, such as cryptocurrencies. Existing research strongly supports the existence of relations between usefulness, ease of use and subjective norm, and behavioral intention to use new technology. In addition, our results however suggest that trust into the security of new technology may also play an important role. Trust into Bitcoin security reflects the belief of Bitcoin adopters that it is safe to use Bitcoin (i.e., that they would be adequately protected from hacks by security mechanisms found in the Bitcoin ecosystem).

Next, the results of this study suggest that Bitcoin adopters do not consider scams to be a key issue. This could be attributed to less media attention received by Bitcoin scams compared to hacks and to the lower amounts involved. Another reason could be that individuals may have more control over falling victims to Bitcoin scams than being victims of hacks. However, more research directly comparing perceived threats of Bitcoin scams and perceived threats of Bitcoin hacks would be highly beneficial to better understand the relationship between perceived threats and behavioral intention to use Bitcoin for paying.

Finally, perceived anonymity of Bitcoin does not appear to be related to its adoption. This could be because individuals do not consider anonymity as an important characteristic of Bitcoin. Alternatively, individuals may be aware that Bitcoin is only pseudo anonymous and therefore cannot provide full anonymity for its users. To better understand the relation between anonymity and adoption of Bitcoin and other new technologies based in cyberspace, studying the relationships between anonymity and adoption of technologies would be welcome.

6.1 Limitations and future work

This paper reports on an exploratory study and has certain limitations that the readers should note. First, the study may have a considerable sampling bias due to opportunity sampling therefore generalizing its findings needs the utmost caution. Most respondents come from a cryptocurrency community (54.6 percent) who may be more cryptocurrency savvy than an average person. A significant share of respondents also has a background in cybersecurity or security in general (40.8 percent). Further studies employing a more random sampling would be needed to validate the results of this study. Second, the study does not distinguish between people who already use Bitcoin and those who do not. Future studies may break down the respondents into users and potential users of cryptocurrencies to determine if there are any significant differences between the two. Furthermore, it would be beneficial to consider the context of transactions. For example, whether the respondents would be more willing to adopt cryptocurrencies for some of the payments (e.g., depending on the transaction partner, the nature of exchanged goods or services, transaction amount).

7 CONCLUSION

This paper adds some exploratory empirical findings to the current literature on Bitcoin adoption and new technologies based in cyberspace, in general. It provides empirical support for the influence of trust into Bitcoin security on Bitcoin adoption. There was however no support for either perceived threat of Bitcoin scams or anonymity of Bitcoin use. Although these results suggest no influence of these factors on adoption of Bitcoin, further studies would be needed to confirm this and broaden these conclusions on adoption of new technologies based in cyberspace.

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for helping to improve this paper with their insightful comments. This paper is partially based on a research project *Human factors in cybersecurity and digital forensics* funded by University of Maribor, Faculty of Criminal Justice and Security.

REFERENCES

[1] Ane Alexandre. 2018. Study: Crypto Coverage in Media Peaked Following Market Slump. https://cointelegraph.com/news/study-crypto-coverage-in-media-peaked-following-market-slump

[2] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. 2017. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, 375–392. https://doi.org/10.1109/SP.2017.29

[3] Paul Barnes. 2018. Cryptocurrency and its susceptibility to speculative bubbles, manipulation, scams and fraud. *Journal of Advanced Studies in Finance* 9, 2 (2018), 60–77. https://doi.org/10.14505//jasf.v9.2(18).03

[4] Massimo Bartoletti, Barbara Pes, and Sergio Serusi. 2018. Data mining for detecting Bitcoin Ponzi schemes. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, Zug, Switzerland, 75–84. https://doi.org/10.1109/CVCBT.2018.00014

[5] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy*. IEEE, San Jose, CA, 104–121. https://doi.org/10.1109/SP.2015.14

[6] Giangiacomo Bravo, Mikko Laitinen, Magnus Levin, Welf Löwe, and Göran Petersson. 2017. Big data in cross-disciplinary research. *Journal of Universal Computer Science* 23, 11 (2017), 1035–1037. https://doi.org/10.3217/jucs-023-11-1035

[7] Stephen Chan, Jeffrey Chu, Saralees Nadarajah, and Joerg Osterrieder. 2017. A Statistical Analysis of Cryptocurrencies. *Journal of Risk and Financial Management* 10, 2 (may 2017), 12. https://doi.org/10.3390/jrfm10020012

[8] Ankur Chattopadhyay, Michael J. Schulz, Katie L. Turkiewicz, and Eli Hughes. 2018. A Novel Visual Recognition-based Authentication Model Using a Hybrid Trust Theme to Verify Provider Profiles for Enhancing Information Assurance in Online Healthcare. *Journal of Cyber Security and Mobility* 7, 3 (2018), 1–46. https://doi.org/10.13052/jcsm2245-1439.733

[9] T.C. Edwin Cheng, David Y.C. Lam, and Andy C.L. Yeung. 2006. Adoption of internet banking: An empirical study in Hong Kong. *Decision Support Systems* 42, 3 (2006), 1558–1572. https://doi.org/10.1016/j.dss.2006.01.002

[10] Nicolas Christin. 2013. Traveling the silk road. In *Proceedings of the 22nd international conference on World Wide Web - WWW '13*. ACM Press, Rio de Janeiro, Brazil, 213–224. https://doi.org/10.1145/2488388.2488408

[11] CipherTrace. 2019. *Cryptocurrency Anti-Money Laundering Report, 2018 Q4*. Technical Report January. CipherTrace.

[12] CoinMarketCap. 2019. CoinMarketCap. https://coinmarketcap.com/

[13] Fred D. Davis. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly* 13, 3 (1989), 319. https://doi.org/10.2307/249008

[14] Nikhilesh De. 2019. Hackers Steal $40.7 Million in Bitcoin From Crypto Exchange Binance.

[15] Peter D. DeVries. 2016. An Analysis of Cryptocurrency, Bitcoin, and the Future. *International Journal of Business Management and Commerce* 1, 2 (2016), 1–9.

[16] Damjan Fujs, Anže Mihelič, and Simon L. R. Vrhovec. 2019. Social Network Self-Protection Model: What Motivates Users to Self-Protect? *Journal of Cyber Security and Mobility* 8, 4 (2019), 467–492. https://doi.org/10.13052/jcsm2245-1439.844

[17] Damjan Fujs, Simon Vrhovec, and Anže Mihelič. 2018. What drives the motivation to self-protect on social networks? The role of privacy concerns and perceived threats. In *Proceedings of the Central European Cybersecurity Conference 2018 - CECC 2018*. ACM, New York, NY, USA, a11. https://doi.org/10.1145/3277570.3277581

[18] Christos K. Georgiadis, Nikolaos Polatidis, Haralambos Mouratidis, and Elias Pimenidis. 2017. A Method for Privacy-preserving Collaborative Filtering Recommendations. *Journal of Universal Computer Science* 23, 2 (2017), 146–166. https://doi.org/10.3217/jucs-023-02-0146

[19] Swati Goyal. 2018. The History of Blockchain Technology: Must Know Timeline. https://101blockchains.com/history-of-blockchain-timeline/

[20] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2012), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

[21] Jurjen Jansen and Paul van Schaik. 2018. Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior* 87 (2018), 371–383. https://doi.org/10.1016/j.chb.2018.05.010

[22] Yogita Khatri. 2018. Nearly $1 Billion Stolen In Crypto Hacks So Far This Year: Research. https://www.coindesk.com/nearly-1-billion-stolen-in-crypto-hacks-so-far-this-year-research

[23] Dac-Nhuong Le, Bijeta Seth, and Surjeet Dalal. 2018. A Hybrid Approach of Secret Sharingwith Fragmentation and Encryptionin Cloud Environment for Securing Outsourced Medical Database: A Revolutionary Approach. *Journal of Cyber Security and Mobility* 7, 4 (2018), 379–408. https://doi.org/10.13052/jcsm2245-1439.742

[24] H. Liang and Y. Xue. 2010. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Jurnal of the Association for Information Systems* 11, 7 (2010), 394–413.

[25] Robert McMillan. 2014. The Inside Story of Mt. Gox, BitcoinâĂ§s $460 Million Disaster. https://www.wired.com/2014/03/bitcoin-exchange/

[26] Rok Meden and Anton Kos. 2017. Rudarjenje bitcoinov s podatkovno pretokovnimi računalniki Maxeler. *Elektrotehniški vestnik / Electrotechnical Review* 84, 5 (2017), 253–258.

[27] Anže Mihelič and Simon Vrhovec. 2018. A model of self-protection in the cyberspace / Model samozaščite v kibernetskem prostoru. *Elektrotehniški vestnik / Electrotechnical Review* 85, 1-2 (2018), 13–22.

[28] Tyler Moore, Nicolas Christin, and Janos Szurdi. 2018. Revisiting the Risks of Bitcoin Currency Exchange Closure. *ACM Transactions on Internet Technology* 18, 4 (2018), 1–18. https://doi.org/10.1145/3155808

[29] Miguel Morales Chan, Roberto Barchino Plata, Jose Amelio Medina, Carlos Alario-Hoyos, Rocael Hernández Rizzardini, and Mónica de la Roca. 2018. Analysis of Behavioral Intention to Use Cloud-Based Tools in a MOOC: A Technology Acceptance Model Approach. *Journal of Universal Computer Science* 24, 8 (2018), 1072–1089.

[30] Elise Moreau. 2019. 13 Major Retailers and Services That Accept Bitcoin. https://www.lifewire.com/big-sites-that-accept-bitcoin-payments-3485965

[31] Saad B. Murtaza. 2019. Cryptocurrency and Bitcoin mass adoption is increasing in 2019; data report. https://www.cryptopolitan.com/cryptocurrency-and-bitcoin-mass-adoption-is-increasing-in-2019-data-report/

[32] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. (2008). https://doi.org/10.1007/s10838-008-9062-0

[33] Danny Paez. 2017. Bitcoin Stolen: How NiceHash Was Robbed Of $78 Million and What's Next. https://www.inverse.com/article/39221-nicehash-robbed-of-78-million-worth-of-bitcoin

[34] Umberto Panniello, Lorenzo Ardito, and Antonio Messeni Petruzzelli. 2017. Does the Users' Tendency to Seek Information Affect Recommender Systems' Performance? *Journal of Universal Computer Science* 23, 2 (2017), 187–207. https://doi.org/10.3217/jucs-023-02-0187

[35] Alain Pinsonneault and Nelson Heppel. 1997. Anonymity in group support systems research: new conceptualization and measure. In *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*. IEEE, Wailea, HI, 134–145. https://doi.org/10.1109/HICSS.1997.665469

[36] Frederick F. Reichheld. 2003. The one number you need to grow. *Harvard Business Review* December, 4 (2003), 46–54.

[37] Kate Rooney. 2018. Bitcoin turns 10 - how it went from an abstract idea to a $100 billion market in a decade. https://www.cnbc.com/2018/10/31/bitcoin-turns-10-years-old.html

[38] Amit Shankar and Biplab Datta. 2018. Factors Affecting Mobile Payment Adoption Intention: An Indian Perspective. *Global Business Review* 19, 3_suppl (2018), S72–S89. https://doi.org/10.1177/0972150918757870

[39] Hardwin Spenkelink. 2014. *The Adoption Process of cryptocurrencies*. Ph.D. Dissertation. University of Twente.

[40] N.S. Tinu. 2018. A Survey on Blockchain Technology- Taxonomy, Consensus Algorithms and Applications. *International Journal of Computer Sciences and Engineering* 6, 5 (2018), 691–696. https://doi.org/10.26438/ijcse/v6i5.691696

[41] Marie Vasek and Tyler Moore. 2015. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In *Financial Cryptography and Data Security (FC 2015)*. Springer, San Juan, Puerto Rico, 44–61. https://doi.org/10.1007/978-3-662-47854-7_4

[42] Marie Vasek and Tyler Moore. 2018. Analyzing the Bitcoin Ponzi Scheme Ecosystem. In *International Conference on Financial Cryptography and Data Security*. Springer, Nieuwpoort, Curaçao, 101–112. https://doi.org/10.1007/978-3-662-58820-8_8

[43] Viswanath Venkatesh and Hillol Bala. 2008. Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences* 39, 2 (2008), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

[44] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly* 27, 3 (2003), 425–478. https://doi.org/10.2307/30036540

[45] Joseph M Woodside, Fred K Augustine Jr, Will Giberson, Fred K Jr Augustine, and Will Giberson. 2017. Blockchain Technology Adoption Status and Strategies. *Journal of International Technology and Information Management* 26, 2 (2017), 65–93.

A SURVEY INSTRUMENT

Construct	Items	
Perceived vulnerability	PV1	I am at risk of being victimized by a Bitcoin scam.
(M=3.24, SD=1.42, CA=0.864)	PV2	It is likely that I will become victim of a Bitcoin scam.
	PV3	It is possible that I will become victim of a Bitcoin scam.
Perceived severity	PS1	Being a victim of a Bitcoin scam would be harmful for me.
(M=4.97, SD=1.40, CA=0.673)	PS2	I view being a victim of Bitcoin scam as harmless for me. (**reverse**)
	PS3	Being a victim of a Bitcoin scam would be a serious problem for me.
Perceived threat	PT1	Bitcoin scams pose a threat to me.
(M=3.69, SD=1.61, CA=0.902)	PT2	The trouble caused by Bitcoin scams threatens me.
	PT3	Bitcoin scams are a danger to my financial well-being.
Subjective norm	SN1	People who influence my behavior think that I should pay with Bitcoin.
(M=3.45, SD=1.41, CA=0.846)	SN2	People who are important to me think that I should pay with Bitcoin.
	SN3	In general, my friends support paying with Bitcoin.
Ease of use	EoU1	Learning to pay with Bitcoin would be easy for me.
(M=4.39, SD=1.45, CA=0.898)	EoU2	It would be easy for me to become skillful at paying with Bitcoin.
	EoU3	I would find Bitcoin easy to use.
Usefulness	U1	Using Bitcoin would enable me to pay more quickly.
(M=4.04, SD=1.56, CA=0.871)	U2	Using Bitcoin would make it easier to pay.
	U3	I would find Bitcoin useful when paying.
Anonymity	A1	I believe Bitcoin malfunction could help identify me. (**reverse**)
(M=3.59, SD=1.26, CA=0.629)	A2	I believe it is possible to identify me using Bitcoin. (**reverse**)
	A3	I believe that I cannot be identified by other Bitcoin users.
Trust	T1	I believe that legal frameworks for paying with Bitcoin are sufficiently robust to protect users.
(M=3.84, SD=1.39, CA=0.842)	T2	I am confident in the security of Bitcoin.
	T3	I believe that Bitcoin implements adequate security measures to secure my paying.
Behavioral intention	BI1	I would use Bitcoin for my paying needs.
(M=3.92, SD=1.77, CA=0.954)	BI2	Paying with Bitcoin is something I would do.
	BI3	I would see myself paying with Bitcoin.
Willingness to recommend	WtR	How likely is that you would recommend paying with Bitcoin to a friend or a colleague?
(M=4.16, SD=3.02)		

M – mean; SD – standard deviation; CA – Cronbach's alpha