# Digital Transformation Challenges: The Cyber Security Threats of Cryptocurrency Technology Use

Sabina Baraković[1], Jasmina Baraković Husić[2]

[1]University of Sarajevo, Faculty of Transport and Communication, 71000 Sarajevo, B&H

[2]University of Sarajevo, Faculty of Electrical Engineering, 71000 Sarajevo, B&H

## Abstract

Digital transformation is unstoppable and ongoing process that affects all segments of our everyday lives such as healthcare, banking and finance systems, public administration, or postal and logistics systems. One of the main engines of this process, among many, is the use of cryptocurrencies. Both of these concepts are usually addressed from the firm perspective, but they should be considered from the individual's perspective as well. Cryptocurrencies recently face increased cyber security threats, thereby affecting the digital transformation and posing additional challenges to it. Therefore, this paper gives a brief overview of security threats and challenges characteristic for cryptocurrency technology today and discusses what can be expected tomorrow. We provide insight how these challenges can affect digital transformation process and propose ways to increase the level of protection for both individuals and organizations.

***Keywords**: Cryptocurrency, Cyber, Digital Transformation, Logistics, Security, Threats*

## 1 Introduction

Digital transformation has become an imperative for most organizations worldwide, but the term is broadly (mis)used and it leads to confusion. There are many definitions of digital transformation [1] and one defines it as "a process that aims to improve an entity by triggering significant changes to its properties through combinations of information, computing, communication, and connectivity technologies" [2]. Digital transformation is omnipresent trend in all business branches: banking and financial systems, healthcare, public administration, power systems, postal and logistic systems, and many more. However, so far it has been investigated primarily from the point of view of firms and less from the perspective of individual non-firm practices that drive the transformative digital phenomenon more broadly [3]. In this process it is important to consider both, firm and non-firm actors.

Nowadays the most prominent digital technology fueling the rise of digital transformation is cryptocurrency, since through its versions, such as Bitcoin, Ethereum, etc., it has a massive global market capitalization. A cryptocurrency is an encrypted, decentralized digital currency that allows people to exchange value and pay services by exchanging crypto tokens and it is used to buy and sell goods and services [4]. This technology is also mostly considered from the business perspective and less from customer's point of view, i.e., assuming that non-firm actors remain passive when faced to new digital technologies and processes [3]. However, cryptocurrencies also need to be addressed from both perspectives, business and customer.

As stated earlier, digital transformation process has a significant impact on logistics [5], while cryptocurrency technology in this domain is mostly mentioned in terms of blockchain usage [6]-[8]. However, the evolution of new technologies, financial innovations, and the dramatic evolution of digital currencies transforms the way we use money in general, but in terms of logistics services as well [9]. Therefore, cryptocurrencies, as well as the technologies supporting it, will become the basis of logistics systems functioning in both aspects: organizational and customer. With that in mind, one has to consider broadly the impact of usage of cryptocurrency technologies in digital transformation of these systems.

At the same time while the abovementioned trends are developing, the number of cyber security threats and challenges in the digital world is constantly on the rise [10]. Cyberattacks are the 5th top rated risk in 2020, while only in 2021, cybercrime, including everything from theft or embezzlement to data hacking and destruction, is up to 600% as a result of pandemic [11]. Given that the cryptocurrency money is being increasingly used and a lot of cybercrime acts will be related to this technology [12], the security challenges it introduces must be seriously addressed.

Taking into account the importance of security of cryptocurrency technology used in logistics systems, from both business and customer's point of view, this paper aims to give a brief overview of security challenges and threats that cryptocurrencies face today and they will face tomorrow. The paper is organized in the following way: Section 2 gives short overview and explanation of cryptocurrency basics in terms of functioning and main notions. Section 3 discusses and analyses the current security threats and attacks targeting cryptocurrencies, while Section 4 gives future trends in cryptocurrency security one needs to pay attention to. Protection measures and conclusion is given in Section 5.

## 2 Cryptocurrency Basics

Cryptocurrencies are based on cryptography, peer-to-peer networks, and open-source concept (Fig. 1). They are primarily a software – logs within program installed on interconnected computers. The first component, i.e., cryptography, is a multidisciplinary science based on mathematics and computer science for more efficient data coding and decoding. It is defined also as an art of solving codes [13]. Cryptography is done to protect the communication between two or more ends. The second component, peer-to-peer networks are networks of personal computers, each of which acts as both client and server. Each computer can access any of the others, although access can be restricted to those files that a computer's user chooses to make available [14]. The third component, open-source software represents software whose original source code is available and it can be distributed and modified [15].

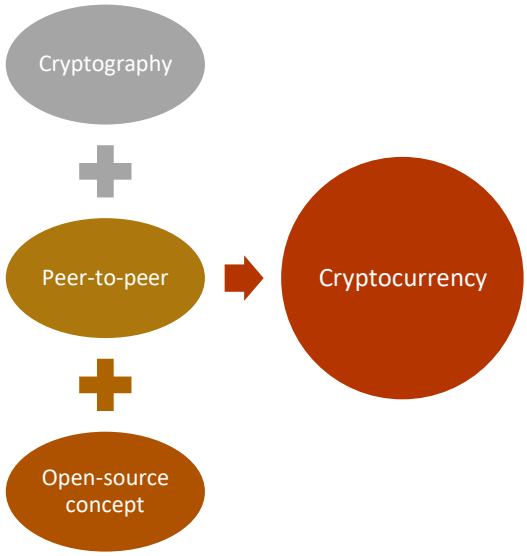


**Fig. 1.** Basic concept of cryptocurrency

Basic terms in cryptocurrencies are: transaction, wallet, blockchain, private and public key, and mining. Cryptocurrency **transaction** is transfer of value between two digital wallets registered in blockchain [16]. This transaction via Internet is based on cryptographic system of two keys: **private and public key** and cryptographic signature. This concept is used by many online applications for safe communications via Internet. In order to have cryptocurrency transaction, one needs to have a wallet. **Cryptocurrency wallet** is a software solution that can be installed on user device or smartphone, used on Internet as online web wallet or as specialized device, i.e., hardware wallet. Obtaining the wallet is informal process that requires no institution and it can be done completely anonymously [17].

The sender of crypto money sends the transaction in the network and waits for it to be confirmed. The network that verifies the transaction is consisted of computers that can gain reward in crypto money for doing the math. This concept is called mining. **Cryptocurrency mining** has several roles: creates new crypto money, creates trust by ensuring the confirmation of transactions, and makes cryptocurrencies special, decentralized, and secure mechanism [18].

Each transaction the miners confirm go to the main book, i.e., blockchain [19]. **Blockchain** is a data block connected into one-way chain in which each block depends on the value of older block. It is based on cryptography due to importance of security and privacy. Also, it can be considered as decentralized book of events

which cannot be edited once the data is inserted. Blockchain contains classified logs related to each transaction ever made, while each transaction in blockchain is confirmed by the consensus of the majority of the participants in the system. This technology has enabled for the first time transparent transactions that do not require trust among the participants [20]. Working principle consists of the following: (i) anyone can request a transaction; (ii) the requested transaction is broadcasted to a peer-to-peer connection to nodes; (iii) the nodes validate the transaction and user's status using the existing known algorithms, (iv) a validated transaction can exhibit cryptocurrency records, contracts, and other important information; (v) the transaction is merged to form a new block with other transactions; (vi) the new block is combined to the existing blockchain in permanent and unchangeable manner; and (vii) the transaction ends [21][22].

## 3 Cyber Security of Cryptocurrency Technology: Today

Given that is current and attractive technology, one of the main drive engines of the digital transformation, and often in public perceived as the money of the future, the use of cryptocurrency technology is on the rise. However, on rise is not the knowledge related to its functioning as well as risks and challenges it presents in security terms which is consequently used by cybercriminals. Cybercrimes are more rampant in 2022 and their rate is increasing every year. Furthermore, it is said that cybercrime affects the security of more than 80% of businesses worldwide today [23].

Some interesting statistics related to security challenges that cryptocurrencies face are as follows [24]: the biggest cryptocurrency heist was Coincheck hack in 2018 with $532 million stolen; John McAfee, accused in a $13 million fraud "pump and dump" scheme was found dead; 2021 saw a 23% year-on-year increase in cryptojacking attack, while 2020 cryptojacking attacks on healthcare rose almost 1400%; cryptocurrency hack and thefts increased almost 40% in 2020; losses from cryptocrime rose 79%; over half of billion dollars in cryptocurrency was stolen in 86 attacks in 2020, while around $4 billion in 2021, etc. As one can see, the lack of knowledge has left the door opened for cybercriminals to scam, steal, and otherwise exploit the concept. Thus, cryptocurrencies are used in darknet scams and business, drug, alcohol, weapons, and human trafficking, financing terrorist activities, ransomware, organized crime, and money laundering.

Vectors of attack in terms of cryptocurrencies, i.e., the ways one can become a victim, are countless. Also, there are many context-oriented classifications of those vectors, but the main ones can be in general grouped in: (i) unintelligent activity, (ii) manipulation; (iii) attacks on technology, and (iv) greater force. In accordance with the proposed taxonomy, unintelligent activity means that one does something and consequently becomes a victim of an attack. This can include clicking on a malicious link, or opening an e-mail message attachment which can result in malware infection, or one can become a victim of a phishing attack. Also, one can give remote access to his/her computer or smartphone to potential attacker which can lead to loss. Therefore, this attack vector is solely the result of individual's irresponsible and unintelligent behavior. Further, one can become a victim if he or she is manipulated to reveal the true identity or give away sensitive information. This is usually done through form of social engineering. Third group are attacks on technology that individual cryptocurrency user cannot prevent. Some of the most prominent examples of such attacks are blockchain network attacks, attacks on technology of user wallets, smart contract attacks, transaction verification mechanism attacks, or mining pool attacks [25]. More details on security issues that can be exploited in terms of blockchain is given in [22]. Finally, greater force is an event for which no party can be held accountable such as hurricane, foods, etc.

The most common crypto attack vectors that are discussed nowadays are given in Table 1. It is important to note that even cybercriminals become victims of crypto attacks. Therefore, it is important to individually stay updated with the current and new angles of attack vectors, while the organizations need to update their security policies and practices.

**Table 1.** Cryptocurrency attack vectors for 2021 [26][27]

| Attack vector | Description | Mitigation measures |
|---|---|---|
| Reverse proxy engineering (session hijacking) | Using phishing techniques to steal money from crypto wallet | Using two-factor authentication<br>Skepticism to e-mails with clickable links<br>Double checking the correctness of sender's email address and URL |
| Cryptojacking | Stealing the processing power to mine<br>Infecting the victim with malware and including the machine into a mining botnet | Updated antivirus and antimalware software<br>Awareness regarding e-mail link from unknown senders<br>Installing browser plugins<br>Avoiding public Wi-Fi |
| Cryptocurrency dusting | Putting the small amount of cryptocurrencies (dust) on addresses and analyzing them in an attempt to identify the individual or company standing behind the wallet | Generate a new wallet address for every transaction |
| Cryptocurrency clipping | Clippers (malware) secretly substituting the wallet addresses of the intended recipient with that of the attacker | Double-checking the inserted address<br>No downloading of suspicious applications and revising their permissions |
| Ransomware | Malware locking electronic files on devices and attacker asking for payment to decrypt them | Using antivirus and antimalware software<br>Monitoring of applications<br>Frequent backups<br>User training<br>Nomoreransomware.org |

Legend: URL (Uniform Resource Locator), Wi-Fi (Wireless Fidelity).

## 4 Tomorrow's Cryptocurrency Cyber Security

It is hard to predict what to expect in terms of cryptocurrency security in the upcoming period given that this technology is rapidly developing and the number of users is accelerating. This motivates cybercriminals to invent new ways to attack the technology and users. However, according to the pool of experts in security [28]-[31], the upcoming period could bring the following challenges which will reflect on digital transformation and all the sectors where it is present.

Information stealers will additionally rise and consolidate in the future and continue to monetize attacks. They will be used against financial assets due to their simplicity and effectiveness in attacks. Stolen information is very useful in several ways. Namely, it can be sold in the illegal market and used to profile the victim for further attack. Those attacks can be ransomware or the traditional ones, and they can include cryptocurrency, but the regular money as well.

Targeted cryptocurrency attacks will be on the rise since the cryptocurrency business continues to grow, and individuals as well as firms continue to invest their money in this market because it is a digital asset and all transactions occur online. In addition, it also offers anonymity to users which is an important feature for cybercriminals and state-sponsored attackers. Furthermore, there will be more cryptocurrency-related threats such as fake hardware wallets, smart contract attacks, DeFi (Decentralized Finance) hacks, etc. In this context, cybercriminals will exploit devices with various malwares (ransomware, Trojan, virus, backdoor, etc.), use social engineering, or other methods to steal the financial assets. What is sure is that when money becomes purely software, cybersecurity will change in ways we cannot predict and expect.

The pandemic caused moving of many companies' systems to digital and online

environment. People had to rely on online markets and payment systems as well as cryptocurrencies. However, the rapid shift is not followed by the appropriate security measures which lures cybercriminals. This issue is particularly severe in developing countries. Also, a lot of personal data is stored in our devices because of payment systems and other types of applications which are used from the same devices that we use for cryptocurrency affairs. Therefore, cybercriminals will continue to attack personal information with innovative and complex strategies (deep fake technology, advanced malware, artificial intelligence, etc.). Again, as in information stealer case, this data can be monetized in several ways.

Also due to the pandemic, many employees had to work from their homes. Now, around two thirds of them state they would not return to an office if they do not have to. Working from home brought us additional challenges in terms of security. Namely, a lot of employees conducted their personal and private affairs via their work devices, i.e., they have inadequately used their business devices. Seemingly, those are innocent activities such as music listening, movie watching, reading books, learning, gaming, etc. However, inadequate activities can lead to cybercriminals and their activities of spreading malware and stealing logins, personal and payment information, business information, etc. Once infected, employees as individuals but their companies as well are susceptible to blackmailing, sabotage, reputation destruction, and many other things which can be monetized in cryptocurrencies. This trend is not a temporary phenomenon, but something that is here to stay and affect the security of our online and digital affairs and lives.

## 5 Protection Measures and Conclusion

This paper gives a brief overview of cyber security threats and challenges characteristic for cryptocurrency technology today and discusses what can be expected tomorrow. We provide insight how these challenges can affect digital transformation process for both individuals and organizations in any business branch (public administration, logistics systems, etc.).

In order to protect themselves in the context of cryptocurrency technology usage in the process of digital transition, individuals and organizations should practice the basic principles of cyber hygiene thereby improving their knowledge, awareness, and behavior [32]. This includes at least the basic knowledge on used digital devices, who access them and where they are; the usage of antivirus and antimalware software together with enabling the security features on devices; better password management and controlled personal information and data sharing policies; regular software updates; and finally repeating all said. Furthermore, these basic activities should be strengthened in the context of cryptocurrency technology by the following five principles [33]: (i) set and use strong and unique passwords, (ii) use secure two-factor authentication, (iii) do not give remote access to accounts, (iv) protect private keys, and (v) do not make yourself a target.

From organizations perspective, protection measures should include adoption, regular update, and enforcement of security policies and practices addressing all aspects of cryptocurrency technology usage. This includes acceptable use, security awareness, incident response, network security, change management, password creation and management, access control, and remote access policy. More funds should be allocated for security management and staff should be regularly educated and trained.

When it comes to future work regarding the impact of cyber security of cryptocurrency technology on digital transformation in logistics should cover examination and quantification of the effects, creation of specialized trainings in order to raise awareness and knowledge of individuals and within organizations, invention, application, and regular update of protection measures, as well as novel legal regulation of this concept.

## References


[1] C. Gong and V. Ribiere, “Developing a Unified Definition of Digital Transformation,” *Technovation*, vol. 102. April, 2021.

[2] G. Vial, “Understanding Digital Transformation: A Review and Research Agenda,” *The Journal of Strategic Information Systems*, vol. 28, no. 2, pp. 118-144. June, 2019.

[3] S. Tana and C.F. Breidbach, “Institutionalizing Digital Transformation Through Cryptocurrency

Use,” *European Conference on Information Systems (ECIS 2021): Human Values Crisis in a Digitizing World*, Marrakech, Morocoo, June, 2021.

[4] I. Faheem, “Application of Cryptocurrency in Industrial Field: Storing and Recording,” *International Journal of Research in Circuits, Devices and Systems*, vol. 3, no. 1, pp. 92-97. 2022.

[5] D. Egorov, A. Levina, S. Kalyazina, P. Schuur, and B. Gerrits, “The Challenges of the Logistics Industry in the Era of Digital Transformation,” *Technological Transformation: A New Role for Human, Machines, and Management, Lecture Notes in Networks and Systems*, vol. 157, pp. 201-209. 2020.

[6] A. Rajeb, K. Rejeb, S. Simske, and H. Treiblmaier, “Blockchain Technologies in Logistics and Supply Chain Management: A Bibliometric Review,” *Logistics*, vol. 5, no. 4. October, 2021.

[7] L. Koh, A. Dolgui, and J. Sarkis, “Blockchain in Transport and Logistics – Paradigms and Transitions,” *International Journal of Production Research*, vol. 58, no. 7. April, 2020.

[8] D. H., Alahmadi, F. A. Baothman, M.M. Alrajhi, F. S. Alshahrani, and H Z. Albalawi, “Comparative Analysis of Blockchain Technology to Support Digital Transformation in Ports and Shipping,” *Journal of Intelligent Systems*. December, 2021.

[9] M. Wojno, “The Future of Money: Where Blockchain and Cryptocurrency Will Take Us Next,” *ZDNet*. January, 2022.

[10] S. Morgan, “Top 6 Cybersecurity Predictions and Statistics for 2021 to 2025,” *Cyber Security Ventures*. December, 2021. [online] https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ .

[11] 2022 Must-Know Cyber Attack Statistics and Trends. *Embroker*. March, 2022. [online] https://www.embroker.com/blog/cyber-attack-statistics/ .

[12] Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity. *Chainalysis*. January, 2022. [online] https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/ .

[13] Cryptography. Oxford Dictionary. 2022.

[14] Peer-to-peer networks. Oxford Dictionary. 2022.

[15] Open-source software. Oxford Dictionary. 2022.

[16] N. Abu Bakar, S. Rosbi, and K. Uzaki, “Cryptocurrency Framework Diagnostics from Islamic Finance Perspective: A New Insight of Bitcoin System Transaction,” *International Journal of Management Science and Business Administration*, vol. 4, no. 1, pp. 19-28. 2017.

[17] What is cryptocurrency wallet? 2022. [online] https://bankrate.com .

[18] How does Bitcoin mining work? 2022. [online] https://investopedia.com .

[19] Bitcoin, cryptocurrency, blockchain...so what does it all mean? 2022. [online] https://pwc.com.

[20] B. Dević, “Kriptovalute,” *University in Split*. 2018.

[21] D. Gountia, “Towards Scalability Trade-off and Security Issues in State-of-the-Art Blockchain,” *EAI endorsed Transactions on Security and Safety*, vol. 5, no. 18. 2019.

[22] S. Baraković and J. Baraković Husić, “Cyber Security Perspective of Top Future Technologies,” in *NATO IOS Press Series – D: Information and Communication Security*, 2022.

[23] R. Geetha, “The Rise of Cybercrime – An Overview,” *Security Boulevard*. March, 2022. [online] https://securityboulevard.com/2022/03/the-rise-of-cybercrime-an-overview/ .

[24] A. O’Driscoll, “Bitcoin fraud, Theft, and Security Statistics,” *Comparitech*. February, 2022. [online] https://www.comparitech.com/crypto/bitcoin-statistics-security/ .

[25] A. Katrenko and S. Mihail, “Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology,” *Apriorit*. 2022. [online] https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors .

[26] Cryptocurrency Attacks to Be Aware of in 2021. June, 2021. [online] https://www.digitalshadows.com/blog-and-research/cryptocurrency-attacks-to-be-aware-of-2021/ .

[27] No More Ransom. 2022. [online] https://nomoreransom.org.

[28] Deepfakes, Cryptocurrencies and Misinformation: Cybercriminals Find New Opportunities in 2022. *Checkpoint*. 2021. [online] https://checkpoint.com.

[29] Cyberthreats to Financial Organizations in 2022. *Secureleist*. 2021. [online] https://securelist.com/cyberthreats-to-financial-organizations-in-2022/104974/.

[30] C. Brooks, "Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats," *Forbes*. January, 2022. [online] https://www.forbes.com.

[31] Financial Systems Jeopardized, Infostealers on the Rise and More Cryptocurrency Attacks: A Look at Financial Threats in 2022. *Kaspersky*. November, 2021. [online] https://www.kaspersky.com.

[32] S. Baraković and J. Baraković Husić, "Cyber Hygiene Knowledge, Awareness, and Behavioral Practices of University Students," Under review.

[33] Top 5 Cryptocurrency Security Tips from Coinbase. *Coinbase*. October, 2021. [online] https://www.youtube.com/watch?v=1Ct-OkiodKQ.