Cryptocurrencies as facilitators of cybercrime

Julija Lapuh Bele[1]*

[1]Visoka šola za poslovne vede, Tržaška cesta 42, Ljubljana, Slovenija

Abstract. The aim of the article is to show cryptocurrencies as facilitators of crime, especially cybercrime. While investing in cryptocurrencies is publicly discussed, their role in the criminal world is more hidden from the public, however, causes a lot of problems for law enforcement and regulatory authorities around the world. Criminals are interested in cryptocurrencies as targets for of their attacks, means of payment and as a method of money laundering. In this article, we discuss why cryptocurrencies have become a means of payment for the criminal underworld, what benefits they have from them, and what major challenges law enforcement is facing in that regard. The survey was conducted based on reports from authorities involved in the prosecution of cybercrime. We can conclude that the organized criminal underworld has a strong interest in cryptocurrencies and their popularity among ordinary, honest citizens, as in this way it is much easier for the criminals to conceal their activities and the origin of their assets.

1 Introduction

There are a myriad questions and unknowns regarding cryptocurrencies. Developments in the cryptocurrency market from its inception to the present day confirm that investments in cryptocurrencies are highly speculative. They allowed for substantial earnings as well as significant losses at times of sudden crashes.

Since the emergence of the first cryptocurrency bitcoin (BTC) we have been wondering whether the duration of this phenomenon will be limited in time, whether cryptocurrencies would remain a part of society and affect the world's economy? As it turns out, cryptocurrencies are a factor that we will surely be facing in the future, unless the regulatory authorities of individual countries decide to actively intervene in this area.

Cryptocurrencies have both changed cybercrime and are closely related to it, as they are e.g. a means of payment, a target of attack, or a bait for phishing data [6].

We conducted this survey based on reports from authorities dealing with the prosecution of cybercrime. Based on that survey, we conclude that the organized criminal underworld is strongly interested in cryptocurrencies and their popularity among ordinary, honest citizens, as in this way they can much more easily conceal their criminal activities and the origin of their assets.

* Corresponding author: julija.bele@vspv.si

2 Cryptocurrencies

If we try to understand the phenomenon of cryptocurrencies, we must first understand how they differ from ordinary (fiat) currencies.

Cryptocurrencies are digital currencies. They exist only on computer systems, not in material form. The best known and by market capitalization the largest currency of this type is bitcoin [1].

In computer terms, cryptocurrencies are based on blockchain technology. Transactions are confirmed in batches called blocks. Because transactions cannot be changed retrospectively, blockchain technology solves the problem of uncontrolled reproduction and unauthorized modification of digital content [9]. Bitcoins and other digital currencies designed in a similar way cannot be copied and assets cannot be acquired in this way. It is also impossible to pay with them without reducing the account balance accordingly.

2.1 Reasons for the emergence of cryptocurrencies

Normally, money transactions take place through trusted intermediaries between clients. These are banks or companies such as e.g. credit/payment card issuers or PayPal. Transfers between customers are mostly made through banks' payment systems.

Intermediaries are legally obliged to report any suspicious transactions to the regulatory authorities and to cooperate in the fight against money laundering. Under pressure from influential countries, they can block accounts and deny users access to money. This happened in the case of WikiLeaks, whose account, which was used to collect donations, was blocked by PayPal [2]. Criminal organizations are also afraid, because financial institutions can deny them access to all their bank accounts if they are identified.

The main reason for the emergence of the most important of the cryptocurrencies was the desire to invent a trusted digital currency that does not need intermediaries to facilitate its payment system [9].

2.2 Blockchain technology

In late 2008, an unknown developer (or a group) nicknamed Satoshi Nakamoto announced that they had developed a digital money system that did not require an intermediary or a central bank to operate. He described his discovery in detail in his article [9]. He also set up the bitcoin.org website. He supposedly left the project in 2010 and we still don't know today who he was or whether he really stopped working on blockchain technology.

Experts and researchers found great potential in blockchain technology, so it has experienced rapid growth and a lot of interest from both the professional public and researchers, as well as potential users.

The benefits perceived by users are:

- The payment system operates without intermediaries, so there is no fear of regulatory authorities or denial of access to funds.
- All users of the system are equal.
- Although there is no central institution to resolve disputes, the system is very likely to be trustworthy.

Bookkeeping is dispersed among all users, and the payment information exchange algorithm ensures that all users always agree on who owns how much electronic money [2]. An individual transaction is based on an encrypted and digitally signed message saying that someone is transferring a certain number of e-coins to another user. Nevertheless, the system does not operate entirely without intermediaries. Transactions are confirmed by computer experts called miners. They are remunerated for their work with a commission.

2.3 Trading with cryptocurrencies

Apart from the miners, one more intermediary is needed, namely exchanges that convert real money into cryptocurrencies or vice versa.

Payments with cryptocurrencies are made using crypto wallets, where users store crypto coins. When they make the payment, the corresponding amount is moved from their own to the recipient's crypto wallet. The system is set up so reliably that fraud is virtually impossible and that transactions made only in cryptocurrencies are anonymous.

It soon became apparent that having miners validate transactions was time-consuming and expensive. The commission is calculated from the transaction. In January 2021, the average tariff per transaction was $11.42. However, the price fluctuates a lot every day [15]. Therefore, bitcoins and other digital currencies operating on blockchain technology are not suitable for the payment of goods and services of lower value. Researchers are trying to solve this problem. A good attempt in this direction is the Lightening network, which allows transactions between clients where trust has already been established to be conducted without confirmation. Therefore, they run faster and with lower costs [10].

Today, many believe in the profitability of investing in bitcoins. Although these investments are among the highly speculative ones, it seems that the system will probably not break down any time soon. Cryptocurrencies are a means of payment for the criminal underworld and facilitate the business of cybercriminals [4].

Traditional crime traded in cash and tried to legalize it for further use, which we call money laundering. National regulatory authorities have introduced anti-money laundering legislation and made it very difficult to deal with illegally obtained cash. With the advent of cybercrime, cash has become useless. Cryptocurrencies are ideal for the criminal underworld because of all the features we have mentioned above. The data show that bitcoin has become the currency used by cybercriminals, making it very difficult for law enforcement to track illegal payments. Blockchain technology increases privacy, e.g., with the Wasabi and Samurai crypto wallets, posing an even greater challenge for law enforcement [4].

It is undoubtedly in the interest of criminal organizations that bitcoins are not just their currency, as it is easier to hide among a crowd of anonymous investors from around the world.

Currently, the greatest threat to the existence of cryptocurrencies appears to be law enforcement and national regulatory authorities, as they do not look favourably upon an accelerator of criminal activities that can lead to uncontrolled individual wealth.

3 Cryptocurrencies and cybercrime

For cybercrime, cryptocurrencies are both targets of attacks and a means of payment in criminal activities where the victim must pay, e.g., for various forms of extortion, Ponzi schemes, and other investment scams [8].

In addition, cryptocurrencies are used for payments on the dark web, where trading with tools, data and services used for conducting cybercrime takes place. The criminal underworld uses a form of cloud computing called Crime-as-a-service. Cybercrime has been growing year by year. The main motive is money. According to Verizon [14], one of the world's leading providers of communications and information services, in 2020, of all successful cyberattacks on their customers, as many as 86% were aimed at obtaining financial gain.

3.1 Cyber blackmail

Cyber blackmail takes many forms. However, as a rule, payments in cryptocurrencies are required.

Attempts at mass blackmail take place via e-mail. Criminals obtain stolen data and try to extort money from victims.

After having user data stolen on the network LinkedIn [13], many of us have been receiving extortion letters for years. The blackmailers claimed to know our password and our activities on the internet. If we did not pay the ransom, they would make public our inappropriate activities and publish the recordings they have. Most of these are empty threats. They assume that there is probably someone among the contacted persons who may be afraid of disclosure. Unfortunately, many people get caught in this trap and end up paying.

Experts advise that we should never pay blackmailers. We do not rid ourselves of them by making payments; on the contrary, the pressures only increase.

Ransomware is a major challenge to the global economy. Both small and large businesses are at risk. These are viruses that encrypt victims' data. This makes the data unreadable to both computers and humans. The blackmailer demands a ransom in BTC to recover the useful data. As many organizations are prepared for such cyberattack and have their data archived, criminal organizations have upgraded their threats; if the victim does not pay the ransom, their data will be publicly disclosed or sold on the dark web [4].

Both the FBI and Europol report that cryptocurrency blackmail is the greatest threat to cybersecurity [4, 5]. There is no exact data on the amount of such illegally obtained money. The FBI claims that, since 2016, there have been at least 4,000 such attacks per day in the U.S. and that there is a noticeable growth trend. The average damage to an organization is estimated at $233,000, and the average cost of repairing the damage increases that amount to $761,000 [11]. In Slovenia, the largest known individual ransom so far was EUR 2,400,000, paid in 2019 [12].

3.2 Theft of cryptocurrencies

Since cryptocurrencies are purchased through cryptocurrency exchanges, such exchanges are quite interesting for criminals.

Every year, there are quite a few publicly confirmed intrusions into exchanges, where hundreds of millions of euros in crypto assets are stolen per year. In 2018, cryptocurrencies worth EUR 500 million were stolen from the Japanese exchange Coincheck alone [4].

3.3 Third-party mining

Validating transactions (mining) is wasteful. It requires a lot of processing power and consumes a lot of electricity. The cyber underground creates networks of subordinated computers. Without the knowledge of the owners, those computers perform the tasks assigned to them by the criminal command server. These tasks can be different, e.g., sending malicious mail or mining cryptocurrencies.

Computers are most often infected with a malicious code that victims install themselves by clicking on infected links. The Monero cryptocurrency was most often associated with this type of attack, as no special applications, such as exist e.g., for Bitcoin, are necessary. However, not only are computers at risk, but also smartphones.

Google Play, for example, was found to have applications with malicious codes for mining cryptocurrency [6].

3.4 Cryptocurrencies used by the criminal underworld

Initially, dark web markets exclusively used cryptocurrencies.

Although Bitcoin is still the most popular means of payment, mainly due to its widespread use, its reputation, and ease of use, the use of cryptocurrencies with enhanced privacy is increasing. Monero is becoming increasingly popular, followed by Zcash and Dash. These currencies are an even harder nut to crack for law enforcement [4].

3.5 Cryptocurrencies and money laundering

Cryptocurrencies are of interest for money laundering due to the lack of regulations in this regard, and because it is possible to transfer money across national borders without detection. Therefore, they are becoming an important detergent in the money laundering process. In 2018, EUR 4.6 billion is assumed to have been laundered in Europe via cryptocurrencies alone. Consequently, governments around the world have called for the introduction of anti-money laundering regulations with cryptocurrencies [7].

The anonymity of cryptocurrency holders, however, is not only a problem for regulators, but also a security risk for some other stakeholders.

The data show that cryptocurrency exchanges are vulnerable and are frequent targets of cyberattacks. Knowing your clients (KYC) is in their own and in the broader social interest. This gives them both the opportunity to identify fraudulent parties and allows them to meet ever-growing legislative pressures. In the EU, the 5th Money Laundering Directive stipulates that cryptocurrency exchanges and crypto wallet providers are required to identify their customers [3]. Some other countries also require greater control and traceability when purchasing cryptocurrencies. In any case, this does not apply to the whole world. In addition, cryptocurrencies can also be purchased through cryptocurrency ATMs, which provide more privacy, and providers often do not require customer identification, or their verification methods are insufficient. Cybercriminals try to avoid obstacles by using marketplaces that support decentralized transactions or by employing direct transactions between the payer and the recipient of funds [4].

Cybercriminals also use the dark web to exchange information on how to use cryptocurrencies to launder money.

4 Conclusion

Cryptocurrencies are attractive to both risk-averse investors and the criminal underworld. They are interesting to criminals as a target of attack, as a means of payment, and as a way of laundering money. Regulators are aware that cryptocurrencies empower criminals and offer them many opportunities to develop new cybercrimes. According to one study, both sides are making progress. Law enforcement is gradually enforcing new measures, and criminals are taking advantage of new opportunities to evade control and are developing new cybercrime services. The year 2021 will be especially interesting for further research in this field due to the large growth in the price of cryptocurrencies in the recent period and the public's increased interest in them.

References

1. Cryptocurrency statistics (prices, charts, correlations) (Bitinfocharts, 2021), https://bitinfocharts.com. Accessed 8 Feb 2021

2. S. Dolenc, Kaj je blockchain? (2016), https://kvarkadabra.net/2016/10/kaj-je-blockchain. Accessed 22 Jan 2020.
3. European Commission, Anti-money laundering and counter terrorist financing (European Commission, 2018)
4. Internet organised crime threat assessment (IOCTA) 2020 (European Cybercrime Centre, 2020), https://www.europol.europa.eu/iocta-report. Accessed 1 Feb 2021
5. FBI Internet Crime Complaint Center (IC3), 2020 Internet Crime Report (FBI, 2021) https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. Accessed 11 May 2021.
6. A. Higbee, The role of cryptocurrency in cybercrime (Computer fraud&security. Elsevier, 2018)
7. V. Marria How Cryptocurrencies Are Empowering Cybercriminals (Forbes, 2019)
8. A. Minnaar, E. Reddy Cryptocurrency: a tool and target for cybercrime. Acta Criminologica: Southern African Journal of Criminology **31(3)** (2018)
9. S. Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
10. J. Poon, T. Dryja The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments (2016)
11. Safeatlast, 22 Shocking Ransomware Statistics for Cybersecurity in 2021 (Safeatlast, 2021), https://safeatlast.co/blog/ransomware-statistics. Accessed 3 Feb 2021.
12. SI-CERT, Poročilo o kibernetski varnosti za leto 2019 (2020) Accessed 30 Dec 2020. https://www.cert.si. Accessed 30 Dec 2020
13. V. Silveira An Update on LinkedIn Mem ber Passwords Compromised (2012)
14. Verizon, Data breach investigations report 2020 (2020), https://enterprise.verizon.com. Accessed 30 Dec 2020.
15. Ycharts, Bitcoin Average Transaction Fee (2021), https://ycharts.com