The 9th International Conference on Business Information Security (BISEC-2017), 18th October 2017, Belgrade, Serbia

BISEC BUSINESS INFORMATION SECURITY CONFERENCE

BLOCKCHAIN/CRYPTOCURRENCIES AND CYBERSECURITY, THREATS AND OPPORTUNITIES

ALEKSANDAR MATANOVIĆ
Master in Digital Currency, Founder of ecd.rs – Serbian Cryptocurrency Exchange, alex@ecd.rs

Abstract: *The document gives the short introduction of cryptocurrencies and blockchain technology and then aims to give an overview of how it relates to some of the cybersecurity challenges. The role of bitcoin in the recent ransomware plague is analysed, having in mind that it has been the currency of choice in most of the ransomware attacks that took place in the last couple of years. It is followed by the brief description of what valuable lessons we might learn from cryptocurrencies and apply elsewhere. Finally, the document analyses the potential of applying the blockchain technology for data storage, the benefits it can bring and the limitations it has, with examples of some projects focused specifically on that area.*

Keywords: *Cryptocurrencies, Bitcoin, Blockchain, Ransomware*

1. INTRODUCTION

Cryptocurrencies are digital, decentralized currencies that use cryptography to secure the transactions and control the creation of additional units of a currency. They exist only in digital form and they function independently of a central bank or any other central authority. Unlike traditional currencies, their supply is usually limited, predefined by the mathematical algorithm.

The oldest and the most famous cryptocurrency is bitcoin. Bitcoin was first presented, as *peer-to-peer electronic cash system*, in a white paper [1] published by Satoshi Nakamoto[1] on October 31st, 2008 and the first bitcoins were created on January 3rd, 2009. Bitcoin attracted little attention at the beginning as it took almost a year and a half until some value was attributed to it. The first time it was used as a payment method was on May 22nd, 2010, when 2 pizzas were bought for 10.000 bitcoins, valuing bitcoin at around $0.003. Bitcoin price has risen significantly since then, reaching all-time-high on Septembet 1st, 2017, when bitcoin was traded for slightly over $5000. Bitcoin price is very volatile and, although the price has mostly been rising since bitcoin was created, there have been some very sharps drops in its value. The last one happened at the beginning of this month, when the price fell around 40%, right after reaching $5000.

Although bitcoin code is open source, which makes it easy for anyone to create a similar cryprocurrency, no such thing happened until late 2011, when Litecoin[2] was created. It would soon be followed by other projects, with number of cryptocurrencies increasing rapidly and now exceeding 1.000.

Cryptocurrencies use Blockchain as the underlying technology. According to [2], *a blockchain is a distributed database that maintains a set of information bundles called blocks*. Blockchain applied in cryptocurrency represents a public ledger of all the transactions of a certain cryptocurrency that ever happened. There are some significant differences between blockchain and the other ways of storing the data.

As the name implies, data is packed in blocks and blocks are connected in a chain. Each block contains the hash of the previous one, as shown in Figure 1[3], making it impossible to change the data within a single block without changing all the blocks that come after it. Ledger is shared between thousands of independent participants (nodes), connected in a peer-to-peer network, with every single one of them having the full copy of the ledger, and they all verify every transaction and every block that is added to the blockchain.

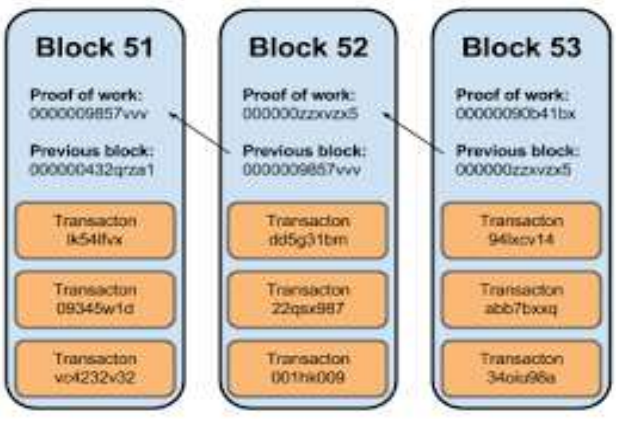

Figure 1: Connecting blocks in the blockchain

[1] Satoshi Nakamoto's true identity still remains a mystery. There were several attempts to reveal his/her true identity but they were unsuccessful and it is still unknown who is hidden behind the name.

[2] Cryptocurrency which resembles bitcoin in many ways, with slightly different mining algorithm, and blocks created every 2.5 minutes instead 10 minutes, which is the case with bitcoin.

[3] Source: https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/

Since there is no central authority that governs the system, there also isn't any central server where the system is run. Instead, the system is maintained by so called "miners", people who dedicate their resources to maintaining the network and are being awarded for that with newly generated units of a cryptocurrency. There are different types of mining algorithms, with most dominant being proof-of-work[4] and proof-of-stake[5]. There are also cryptocurrencies that use combination of two different mining algorithms.

Networks of the top cryptocurrencies are being maintained by at least thousands of nodes and changing the data that has already been added to the blockchain would require consensus of the majority of nodes. It is a very unlikely event and it is probably safe to say that blockchain technology brings us an unprecedented level of data integrity. Changing the history is not, however, totally impossible. The most famous rollback, which caused a lot of controversy, is the one done on Ethereum[6] Blockchain on July 20th, 2016, when transaction history was rewriten in order to delete transactions connected with the DAO hack[7].

Blockchains can be public (e.g. Bitcoin, Ethereum, Litecoin...) and private (or permissioned). Public blockchain are accessible to everyone and they have their native cryptocurrency, most of all because miners need to be incentivized for their contribution to the network. Private blockchains are accessible only with a permission. They are newer type of blockchains and usually don't have a native currency or a token attached to it. Some argue that private blockchains are useless and that true power of blockchain technology lies in decentralization, transparency and accessibility for all.

Potential applications of the blockchain technology go far beyond cryptocurrency and even far beyond the whole financial industry. They include industries such as: insurance, media, healthcare, government, identity, asset titles, supply chain and many more. It is still a young technology and most of those applications are still in experimental phase.

2. BITCOIN AND RANSOMWARE

Because of its pseudo-anonimous[8] nature, bitcoin has often been linked to different illegal activities. In most cases, its supposed use in such activities was highly exacurated. However, it is hard to deny the link between ransomware and bitcoin, the currency that has been used lot of those attacks. Acording to [3], 75% of attackers demanded the ransom to be paid in bitcoins.

The most common pattern is:

- Hackers send the ransomware, usually as an e-mail attachment.
- When attachment is opened, the ransomware starts encrypting files on the computer and also on other computers that might be connected to the infected one through the internal network. More advanced ones target the recently used files in order to maximize the damage by making sure the most important files are encrypted first. In that case, even if the encryption is interupted at some moment, the most important files are already encrypted.
- In the Windows Desktop and in each folder that contains infected files, ransom notes are created. Notes provide a step-by-step guide on how to set up a bitcoin wallet, where and how to purchase bitcoins and where to send them in order to acquire a file decrypter.
- Amount of bitcoins that is required is usually doubled after certain time intervals (e.g. every week) urging the victim to pay as soon as possible, also threatening that every chance for data recovery will be lost forever if the payment is not completed until the deadline.
- After the payment is made, victims are given the link they could use to download the decrypter which decrypts the infected files.

While most fo the hackers do provide file decrypter after being paid for, there is no guarantee that they would actually do so. Some just collect the payment and never deliver anything. Others ask for additional payment after receiving the initial one. The problem in predicting hacker's behavior is the fact that the barrier to entry for hackers is extremely low. One can literally send the ransomware to potential victims without having any knowledge about hacking or even coding. On Dark Web[9], it is possible to purchase a ransomware kit and have your own ransomware within minutes.

Depending on the type of ransomware, in some cases it is possible to exchange messages with the hacker. In those cases, if the payment is the only solution, victim should try to negotiate the price because there were cases when attackers were willing to lower the price significantly. However, payment should always be the last option. Unfortunately, statistics [4] shows that corporate victims pay the ransom in 70% of the cases, with half of those paying over $10000. Table 1 shows the posibilities for bargaining depending on the type of the ransomware.

[4] Rewards that miners are getting are proportional to the processing power of the hardware they use to help maintain the network.

[5] Rewards that miners are getting are proportional to the amount of a currency they already hold.

[6] The second biggest cryptocurrency in terms of market capitalization

[7] The DAO was Decentralized Autonomous Organization run on Ethereum blockchain network. On June 17th, 2016, the vulnerability in DAO code was exploited and about $50M was stolen

[8] All the bitcoin transactions there ever happened are visible to everyone. However, names and other personal data of the participants in transactions are not exposed.

[9] A part of the internet only accessible using special software. That software helps website operators and users to remain anonymous and untrecable

FAMILY	STARTING DEMAND	LOWEST DEMAND	%DISCOUNT
CERBER	530	530	0%
CRYPTOMIX	1900	635	67%
JIGSAW	150	125	17%
SHADE	400	280	30%
			AVERAGE: 29%

Table 1: Bargaining opportunities for several types of ransomware[10]

After suffering a ransomware attack, victims' attitude towards bitcoin is usually negative, some even go as far as blaming bitcoin for the attack. It is important to know that ransomware existed well before bitcoin and will continue to exist after hackers stop using bitcoin as a payment method. It is just the most convenient payment method for them at the moment with the right blend of anonymity and accessability for the victims. There are other cryptocurrencies (e.g. Monero[11]) that have advanced anonymity features, but they are more difficult to acquire[12] than bitcoin, which is probably why they still havent't replaced bitcoin as a preferred payment method for ransomware. However, since the number of users and the availability of those currencies is rising, it is just a matter of time when bitcoin will be replaced by more anonymous cryptocurrencies. It has already happened on Dark Web illegal markets, where bitcoin has lost ground to Monero.

Bitcoin is generally much better understood than it was before. It is not nearly as anonymous as some might think. All the transactions are recorded forever in a public ledger and visible to everyone. Although the names of the participants in a transaction are not shown, it is possible to discover the names behind almost every bitcoin transaction. The current problem is that the procedure is relatively complicated and time-consuming so it is not feasible to track every single transaction. Instead, those who track them are mostly focused on larger suspicious transactions. Besides, there is still a lack of personel skilled enough to conduct blockchain research and tools that would facilitate blockchain analysis. Once those obstacles are overcome, it is logical to expect that bitcoin will be avoided by most of the hackers and others that currently use it in their illegal activities.

3. WHAT CAN BE LEARNED FROM CRYPTOCURRENCIES?

With traditional currencies, people trust banks or other financial institutions to conduct the payments on their behalf and store money for them. The convenience of having some institution taking care of one's money is paid for with limited freedom in using of using that money.

The approach that cryptocurrencies offer is completely different. One of the main reasons for their relatively slow adoption is in fact their nature, which requires people to change the mindset and change the perception of money as a concept. For the first time, we have unlimited freedom to use our money and unlimited control over our funds. However, that comes with a price – unlimited responsibility and that is something people are having hard time getting used to.

Embracing cryptocurrencies is about embracing both the freedom in using the money and the responsibility that comes with it. The one who holds a private key to a cryptocurrency wallet has a total control over whatever is on that wallet. On the other hand, if the private key is lost and no backup has been done prior to that, the funds on the wallet are lost forever. That is the lesson many have learned the hard way.

Living in a highly centralized world, we have learned to trust different centralized organizations and trade freedom for convenience. What cryptocurrencies teach is that freedom can be great, but can also be very expensive if not handled approached properly. It is something that can be applied to the area of cybersecurity. The freedom of using the internet can be very dangerous and expensive if there is a lack of responsibility. It is important to always remember that we are the ones holding the "private key" and that the whole responsibility is always on us.

4. SHOULD BLOCKCHAIN BE USED TO STORE IMPORTANT DATA?

Whenever there is an important piece of data, it has to be stored in a secure way and it needs to have a backup. However, backups are sometimes not done often enough or even not done at all. Blockchain has an inherent backup mechanism within itself. As explained earlier, blockchain-based systems have a big number of nodes who hold the complete copy of the ledger. Those nodes communicate with each other and update their respective copies of the ledger in real-time. Having thousands of automatically updated copies of the database looks like a perfect way to store any kind of data. Is it really so?

[10] Source: "F-Secure State of Cybersecurity", https://www.f-secure.com/documents/996508/1030743/cyber-security-report-2017

[11] Monero uses ring signatures to make the transactions untraceable. Besides the names of the participants in a transaction, Monero addresses and the amounts are also invisible.

[12] Number of cryptocurrency exchanges and similar services that are listing Monero is still very limited.

If we are talking about public blockchains, they have higher number of nodes, they are more secure, more robust, they have a longer track record, but they also have one serious limitation – capacity. Those systems are maintained by individuals and are designed to attract as many of those individuals as possible. Therefore, designers of those systems had to be mindful about users' bandwidth and hard drive capacity. As a consequence of that, the rate of adding new data to the blockchain is relatively low. In bitcoin, up to 1MB of data is added to the ledger every 10 minutes[13]. Some public blockchains have bigger capacity, but not big enough.

What public blockchains do provide is the very high level of data integrity. Blockchains are almost immutable as changing the history requires a huge effort that can't be unnoticed. So, when we have some piece of information and it is critically important that the information cannot be altered, storing it in the blockchain makes a lot of sense, as long as the size of the data is relatively small.

Another issue with public blockchain is the transparency. If blockchain contains the data of interest to the public, it is a great feature. However, if the data is sensitive and shouldn't be revealed to third parties, public blockchain is far from perfect solution.

There is a way benefit from blockchain's immutability even when we have larger chunks of important data. We would have to store the data outside of the blockchain, then apply cryptographic hash function to the data and store only the hash of that data on the blockchain. If the data changes, the hash of that data changes too and it doesn't match the hash stored on the blockchain anymore.

Private blockchains don't have issues with the capacity. They are usually maintained by an organization or a group of organizations that can have full nodes hosted on big servers with high bandwidths. They are, however, less secure than the public ones, because they usually have significantly lower number of nodes.

Running a private blockchain within a single company, with a purpose of having the data stored in a more secure way doesn't make much sense. It could only benefit huge organizations that spread across different countries. Even then, there are cheaper and easier way to handle data security.

Having a private blockchain for a group of organizations, especially within the same industry, is something that has grabbed the attention of many companies and institutions all over the world. A simple example could be the group of insurance companies sharing the database of fraudulent customers to reduce the risk of frauds or banks sharing KYC data between themselves and saving a lot of time. It is still very questionable whether the blockchain-based solution is the more efficient one at this stage of the development of blockchain technology.

There are some blockchain-based projects specifically focused on storage. The idea behind most of those projects is to store the data on unused hard drive space of other users in the network instead on a centralized server. The latest big one that appeared and attracted a lot of attention was Filecoin. It has raised an astonishing $200M in only 1 hour through its ICO[14]. Other significant projects are Storj and Sia.

5. CONCLUSION

Cryptocurrencies and blockchain present a very significant innovation. Cryptocurrencies not only change the way we use money but also the way we think about money. By taking away the control over money from central banks and cutting off the intermediaries, cryptocurrencies manage to speed up the transaction, lower the transaction fees and make money accessible to anyone.

Blockchain technology revolutionizes the way data is sent and stored. It introduces the trust into a distributed system without central authority. Cryptocurrencies are the first application of the blockchain technology, but blockchain might be applied to many other different areas.

Ransomware has been an increasing threat in the recent years. Barrier for entry for hackers has been significantly lowered since ransomware-as-a-service is being offered on Dark Web. Besides, bitcoin has made it easier for hackers to collect their ransoms and stay relatively anonymous. Three out of four hackers use bitcoin as the payment method for ransomware. Around 70% of all the corporate victims end up paying the ransom. It implies that most of them probably don't do backups regularly. If payment is in fact the only option, bargaining should be tried whenever possible, because the ransom can be lowered as much as 67%.

Since bitcoin is not nearly as anonymous as many may think and tools for blockchain analysis are getting better and better, it is reasonable to expect that bitcoin will be replaced as a "ransomware currency" in the near future by one of the cryptocurrencies with advanced anonymity features. Judging by its penetration on Dark Web markets, Monero is probably the strongest candidate.

Blockchains as databases are almost immutable and have a big number of updated copies at any given moment. It is natural to think they would be ideal for storing data. However, not every type of data can take advantage of the blockchain technology. Public blockchains mostly suffer from limited bandwidth and limited storage capacity. They are also relatively transparent and accessible to anyone which makes storing sensitive data unfeasible.

Private blockchains are more flexible and don't have issues with the capacity. However, they are not as secure as public ones and, as young as the blockchain technology is, private blockchain as a concept is even younger. There is a lot of testing done in that area, but the number of usable solutions

[13] Maximum size of a block of data is 1MB, although some blocks are smaller. Blocks are not added exactly every 10 minutes, but in average. Time between 2 blocks may vary from 1 minute to couple of hours

[14] ICO is the short of Initial Coin Offering. It is a new method of raising the money for the project which has been heavily used (and abused) in 2017, with over 2 billion dollars raised since the beginning of the year.

is still very limited. There are blockchain-based projects focused specifically on data storage. Although some of them have attracted a lot of interest and investments, we are yet to see them being widely adopted.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008

[2] D. Verma, N. Desai, A. Preece, A. Taylor, “A blockchain based architecture for asset management in coalition operations”, 2017

[3] Dr. L. Hadlington, “Exploring the Psychological Mechanisms used in Ransomware Splash Screens”, 2017, De Montfort University, Leicester

[4] IBM Study, “Businesses More likely to Pay Ransomware than Consumers”, 2016