Advances in Social Science, Education and Humanities Research, volume 359
4th International Conference on Social, Business, and Academic Leadership (ICSBAL 2019)

Management and economic security of blockchain technology for achieving leadership in the conditions of improved information

Ekaterina Butenko
Institute of economics and management
North-Caucasus Federal University
Pushkin str. 1, 35500 Stavropol
Russian Federation
e-mail: edbutenko@gmail.com

Ivan Chernikov
Institute of economics and management
North-Caucasus Federal University
Pushkin str. 1, 35500 Stavropol
Russian Federation
e-mail: ivanmonolit1@gmail.com

Anna Sherstobitova
Togliatti State University
Belorusskaya str. 14, 445020 Togliatti
Russian Federation
e-mail: ya_anya@mail.ru

Abstract Most experts predict that more than 10 % of global GDP will be stored in blockchains. This technology is usually associated only with the world of cryptocurrency, but it has deeper roots and appears in the areas of health care, the production of goods and services, and also stores various secret data and information. After all, when in the information society, the main resource is information, influence and money, the security of data and their confidentiality should come first. All of these ensures leadership and dominant position. And many people think that it is precisely for the blockchain that we are waiting for the "stone wall" from our problems. But very few people think about how safe it really is.
This study focuses on the management and the use of blockchain technology, types of threats to the system and its consequences on our world for achieving a leading position. In the process of studying the problem of using the blockchain technology and determining security threats, we employed the methods of logical, deductive, interrogative and statistical analysis.
Our results show that the use of blockchain technology can significantly ease the life of the government, companies and people. The use of smart contracts can significantly change the usual understanding of secure transactions, however, with the growth of this technology, hacking techniques are also being improved, as well as old ones that adapt to modern security protocols. This technology has not yet penetrated the masses, so it is necessary to highlight the main methods of preventing privacy and security for users and new companies in the market. Therefore, the main results of this work were focused both on the general structure of understanding of this technology, and on the general prevention of threats from intruders.

1 Introduction

The history of the blockchain, despite the still young age, is quite rich in events and incidents. This technology is gaining more and more popularity and attracts the attention of various states, organizations, ordinary people, and also not law-abiding citizens (see e.g. Zielinska 2016; Jun 2018; or Galvez et al. 2018). Thanks to this technology, it became possible to conduct business on the Dark Web in all possible spheres of business, education, and social life with relative confidentiality of transactions (see e.g. Strielkowski 2018). Special attention should be paid to what a blockchain is, how it is possible to conduct a shadow business using this technology, and whether this technology is safe and resistant to various types of attacks.

Blockchain serves as a database for storing all information about cryptocurrency transactions. Cryptocurrency is a digital currency, the creation and control of which is based on cryptographic methods

(Butenko 2014). This encrypted currency can be used by a person with a special decryption code (Yuan and Wang 2018).

All data is stored in a decentralized network, which serves as the central bank for transfers of all transactions. It contains records of the amount of each transaction, the address of the sender and recipient. The blockchain is not controlled by people or is regulated by financial institutions. This is done using open source software that is distributed throughout the world through computer networks.

The blockchain technology owes its rapid development Bitcoin cryptocurrency. This digital currency was positioned as the achievement of a new century, because it is completely "anonymous", "safe" and with an "ever-increasing exchange rate". However, over time, it turned out a lot of unpleasant details (Penkova et al. 2019).

First, to argue with the fact that this currency is a very stupid achievement, but in the matter of anonymity and security, things are different. A striking example is the comparison of the new digital currency with the paper ones. Unlike cash, where their user is responsible for a specific episode of their use, in the event of an offense. Those who were caught in the dark affairs with Bitcoin, reveal all their transactions that were stored in the blockchain network. However, they also disclose all intermediaries with whom they had business relations.

On top of that, Bitcoin is tied to a static wallet number. For example, knowing the "WebMoney" wallet number will not be able to see transactions for a regular user, but knowing the Bitcoin wallet number makes this possible. It is enough to find out the number and go to the official website of the blockchain, and anyone can view various information about the wallet. To which purse were the funds transferred, from where they were received, what was the amount on the balance sheet and much more. This problem began to be solved, the emergence of other types of cryptocurrency and Bitcoin-mixer, but the very fact of the threat of confidentiality of user data remains in the world of digital payment transactions (Butenko and Isakhaev 2018a).

Many adhere to the point of view that if the user is careful, then his wallet number will never be known. But the history of the Dark Web site - "Silk Road" proved that there is always a threat. After all, when the FBI managed to hack this site, all user data, including their wallet numbers, were threatened (Chertoff 2017).

Nowadays, sites have become more competent in the issue of security, and are trying to store user data scattered, encrypt them with various methods, and constantly transfer the database. However, no site guarantees the security of anyone's data 100%. After all, security problems may exist long before your entry into the site.

The main thing that a user has to do on his own is to provide anonymous Internet traffic, because in case of leakage of traffic outside the secure network, it can be intercepted by third parties, and any of your activity will be registered. Therefore, at the very beginning, it is necessary to limit all programs that have access to the Internet. After all, when using any kind of confidentiality and anonymity, it is very important that all Internet traffic is transmitted through an anonymous network (Butenko and Isakhaev 2018b).

The next step is to secure the transaction itself by using mixers, or at the very least a personal wallet. But do not use different exchange points for payment, as there is a risk that your data will go further than the exchange point. Separately, it is worth mentioning that each cryptocurrency has its own blockchain, and each of them has its own methods of protecting the privacy of users. And that does not work well with one cryptocurrency, it can work well with another, it all depends on the competence of developers.

After considering the main threats to confidentiality, it is worth paying special attention to the threat to the security of the funds themselves. There are a lot of them, and according to the security report on the blockchain technology in 2018, only from exchange hacks, 51 % attack, lack of software and other threats was lost in the amount of $ 1,060,898,000 (Zheng et al. 2018)

The majority of blockchain users agree that such a technology can only be cracked with the help of quantum computers that will appear in decades. And then, immediately another quantum computer will stand guard over its protection. But there may also be counterarguments to this. By itself, information security cannot be static. During the Second World War, with the help of the Enigma machine, it was possible to encrypt German messages using a method not previously known, and after Alan Turing was able to find a method for decrypting them (Christensen 2007). The German command had no doubt about the capabilities of this vehicle. However, it could not find the source of the information leak until the end of the war. But if they had found out about the hacking of the Enigma machine code, they would have just slightly changed the encryption, and mathematicians with engineers would again have to look for key numbers to decrypt.

2 Attacks on blockchain technology

Unfortunately, blockchain threats exist not in the distant future, but in our present. Despite the fact that security systems are integrated into all blockchain technologies, there are still opportunities to attack directly and indirectly. Of course, the blockchain may well resist the usual cyber-attacks, but, as in any system, it reveals security holes that hackers enjoy using. In the second part of this work will be dismantled the main types of attacks (Meng et al. 2018; Watanabe and Fan 2019). One of the most common types of attacks are network type:

- DDoS attack

The first to be considered will be a very famous DDoS attack in hacker circles. Which decrypts as a denial of service, and a technology such as blockchain is completely susceptible to such an attack. Given that the blockchain is a chain of blocks, then by damaging several of them, it is quite possible to disable the entire system.

The basic principle of this attack is that with a DDoS attack, incoming victim-oriented traffic comes from many different IP addresses, from a few to hundreds of thousands. It is almost impossible to stop such an attack, because by blocking one IP address, others will remain. In addition, it is rather difficult to determine which traffic comes from real users and which does not. But there are problems in implementation, firstly, it will take a lot of resources to attack the blockchain. Normal attacks on traffic will not be enough. It will be necessary to automate thousands, millions, hundreds of millions of small cryptocurrency transfers in the blockchain to overload the network. However, the commission exists everywhere, and the loss may exceed the profit.

Therefore, one of the most important questions - who can this be useful? Thinking about this, there are three main versions: The first is to hide some very important transactions. Blockchain is a database, it is impossible to cross out any transactions, because they remain there forever. At the time of the attack, there are millions of new transactions, and there is a chance that your transaction could be lost among them.

The second is an attack from competitors, for example, in one of the versions of the attack on Bitcoin in the summer of 2017, a bitcoin cache was launched to promote cryptocurrency (Bartoletti and Pompianu 2017).

The third is the artificial destruction of any cryptocurrency. It is impossible to completely destroy it, but it is possible to disable it for an indefinite amount of time. Therefore, if a cryptocurrency banned by the government appears, it can be removed from mass use in this way.

- Attack on time

This type of attack exploits a vulnerability in time. For example, during an attack, a hacker would have to change the node's time counter, thereby causing the system to accept an alternative block chain. This is achieved at the moment when several peers with inaccuracies in time will be added to the network. The problem is that if you limit the time ranges of decision making to the maximum possible, then this approach loses its relevance.

- Attack of the Sybil

This type of attack is the most effective at the moment among the network. This attack is often observed in peer-to-peer networks, in which a network node simultaneously uses several identifiers. Blockchain networks do not have trusted nodes; therefore, each request is sent by several nodes.

Most networks, particularly peer-to-peer, rely on user identification, where each computer represents one person. The Sybil attack occurs when several computers are hacked and are under the control of a hacker for a network attack.

One example of this type of attack is falsification of polls. For example, an online election survey can be falsified using a variety of infected computers. Or, a company can raise its rating in various applications; there are many ways to use this type of attack. The advantage of this method of attack is that to external observers, these fake identities seem to be unique users.

It is very dangerous if the attack of pseudo-unique users will function successfully in the blockchain network, thereby gradually taking control over it. In addition to the ability to influence polls, the Sybil attack is also capable of interrupting the flow of information over the network. After all, Sybil nodes can surround and try to influence information coming from the nodes of another network, gradually influencing it, and even try to transfer it to their network.

3 Digital security and protection

There are several ways to protect the blockchain from the Sybil attack (Efanov and Roschin 2018. Each has its own advantages and disadvantages, mainly used hybrid options. The first method, probably the most unpleasant for new users, is the complication of creating a new personality on the network. Here the main thing is to keep a balance, because the creation of a unique personality should not severely restrict real users from joining the network. The blockchains try to balance this point as much as possible in order to defend themselves against the Sybil when mining. To test the algorithms when creating a new user who wants to participate in the mining of cryptocurrency, you will need a computer with good computational power and much more. This helps get rid of thousands of pseudo-nodes that can affect the overall network.

The second method is very controversial. It is associated with a system of trust, as in closed clubs, where a member's guarantee is required to obtain membership. Another option is to trust the system itself, i.e. the user must confirm his activity for a certain amount of time, but this option is easy to fake.

However, in recent times, it has become easy to defend the network with two-factor authentication from a Sybil attack. She suggests the following. To enter the system, you need to enter a special code that will be sent

to your mail, however, this can be automated. Therefore, among the two-factor authentication method, they began to use the scanner system of a unique QR code using a telephone. This method is almost impossible to fake. The last way is not equality of voice. Those. new users will have no impact on the network, polls and even voting rights. Users with an average reputation will have a small voting right, and users with a large reputation will have a full voting right. Security threat to users' wallets:

Surprisingly, not only the blockchain can be to blame for the theft of your funds, but also the luck of the hacker, as well as your overconfidence. In this section, various security issues of digital and hardware users' wallets will be considered:

- Brutfors

Attack on wallets using the password database, or as this type of attack is called - “brute force”. Brutus is a brute force password. Hackers when attacking a specific user wallet can use various password databases, which can have millions, if not billions of options (Volety et al. 2019). And gradually, each of the passwords will be checked for "validity", i.e. the truth. Most users do not think about their security and can enter as a password "qwerty123" or their date of birth, which is one of the first passwords in the hacker database.

The easiest way to protect yourself from this is to come up with the most original and complex password, consisting of several characters and numbers, with various capital letters. And most importantly, your password must be unique, otherwise, if the site in which you left your password is hacked using SQL injection, the password has every chance to get into the common database of the brut.

- Attacks on online and offline wallets with cryptocurrency

Many people wonder where and how to store their cryptocurrency. The simplest solutions are hardware wallet (offline) and online wallet (application or website). However, they both have their advantages and disadvantages.

Online wallets are subject to DDoS attack, if they are downloaded to the phone and your phone is infected with a virus, then the virus also poses a threat. As for offline wallets, then things are rosier. The hardware wallet "Ledges Nano S" is devoid of many of the drawbacks of the online version. It takes over the function of storing, generating keys and confirming transactions. Externally, is a regular accessory. However, like any other application, the wallet is not without flaws, and it can be quite a hack to itself.

He is quite vulnerable to the attack of the "evil Virgin". An “evil maiden” attack is an attack on a device that was left unattended, where an attacker, having direct access to the device, can change it at the software and technical level, in such a way that he will be able to gain access to his data. After all, even a closed system, like IOS, has flaws that allowed the FBI to get a password from the device with the help of specialists.

- Attack with developer incompetence

We can often notice that some company releases updates for its devices, programs or systems that are much worse than previous versions. Or new defects appear in them, unfortunately, the blockchain technology is no exception. After all, like any other online technology, it is being developed and improved; as a result of a minor error in the code, there is a risk that a hacker will gain access to the entire system.

The vulnerability of smart contracts:

The concept of smart contracts has become spread along with the Ethereum cryptocurrency. The distinctive side of "Ethereum" is the advanced technology of smart contacts. Her task is to verify the transaction between the sender and the recipient. It is believed that this type of contract cannot be circumvented.

Unlike Bitcoin, where smart contacts are capable of performing simple tasks, because of the programming language Script, smart Ethereum contracts use JavaScript. Due to this, the system can confirm the operation immediately after receiving the notification. Smart contacts allow you to implement an automation mechanism by analyzing all the conditions for each transaction. There are many uses for them. For example, use Ethereum when issuing loans, which will allow the lender to prescribe all the necessary conditions and implement them.

However, if there are threats in written contracts, it is logical to assume that they can also be electronic. These types of threats present a risk to both parties who sign a smart contract. Thus, as a result of detecting errors in the Ethereum cryptocurrency contract in 2016, losses for the company cost $ 80 million (Giancaspro 2017).

Here it is important to understand that the security of the blockchain of a given cryptocurrency and the security of the smart contracts themselves are of a different nature, and most of the vulnerabilities occur precisely in the environment of smart contracts. Smart contracts themselves are a special kind of computer protocol designed for digital facilitation, enforcement, and compliance with the terms of a negotiation or fulfillment of a contract. In the role of intermediary serves only blockchain, without the participation of third parties, which will allow ordinary citizens to save on notaries. Many problems of smart contracts originate from its code.

First of all, there are a lot of people responsible for mistakes and writing code, and there is a risk that one of them could make a mistake and create a security hole. By their nature, the smart contract is not changeable and complete, and can be updated only by concluding a new contract, provided that the old one has been

executed. And if the old contract was concluded with errors in the code, they also will not be possible to fix, and they will become an easy victim for the hacker.

In addition, the large requirements for those who enter into a contract. After all, if there is a broadcast transmission to an address that is not registered in the contract or does not exist, then all transferred funds will disappear from the system. Thus, users and companies to improve smart contracts should treat their content with even greater caution than usual. After all, they can be compromised by applying the previously mentioned network hacking methods, for example DDoS.

Attack on the block check system:

In this section of the types of attacks on the blockchain technology, time plays an important role. Basically, an attack is made when the generated block is checked for authenticity by other network participants, and while the check is in progress, a hacker can apply various hacking techniques to the blockchain.

- Double attack

This type of attack looks more like a coin on a rope. Where using this method you could buy something several times in one coin before. The main focus here is on the elasticity of cryptocurrency, where the hacker will try to copy the spent bitcoin and use it again. This type of attack is useless to such a cryptocurrency as Bitcoin, because each operation is checked separately, however various weaker blockchains appear quite often, and this type of attack can successfully approach some of them.

- One-way attack

This type of attack is better known under the name "Vector76". Basically, this type of attack has a short amount of time, approximately 10 minutes, and is possible, provided that the function of withdrawing funds from the victim's wallet is automated. Its mechanism is rather complicated for understanding at first glance. From the hacker it will be necessary to create two transactions of high and low cost. After adding a high cost transaction to the exchanger, it must wait until the transaction is confirmed, and quickly send the unit with a low cost to the network to replace the original one. This method of implementation is possible only if the victim gets into the infected nodes that will be controlled by the hacker.

- Attack half power

The attack of 51 % is quite famous. The main point is in the theory of the blockchain itself, for its implementation a group of miners are needed who control more than 50% of the computing power of the network. This is more like a joint stock company, where with a controlling stake a person can dictate their terms to the company. Similarly, if attackers get more than 50% of the blockchain's network capacity, they can easily prevent confirmation of new transactions, cancel transactions that have been completed, and much more.

In addition, they also have the ability to change mining costs. In spite of the fact that theoretically the final control of capacities to get an incredibly expensive pleasure, this remains possible. This type of attack will not be able to destroy the cryptocurrency, create new blocks out of nothing, or take control of old blocks, but it remains possible to capture the entire new transaction system.

This type of attack can make mining a useless exercise for the remaining percentages of power. Power over half the power makes it possible to completely and completely control the recording of new blocks, destroy the mining, reducing the reward to the lowest possible threshold, even to zero. But the problem lies elsewhere, with an attack of 51 %, the doors to the blockchain open up for the previously described attacks as widely as possible, for example, a double attack cannot be perfect under normal conditions, as network users will reject it, but with 51 % control many illegal operations can become legal.

For such giants as Bitcoin, this attack is almost not feasible, but not large blockchains are completely susceptible to this attack, it will suffice to rent several powerful servers, and you will have the whole opportunity to attack.

In addition, the main threat to the blockchain is the people themselves. Indeed, many painful violations for users and companies occurred due to the fault of the people responsible for security, and not because of failures in the blockchain technology. For example, as a result of their incompetence, some exchanges could sell keys, passwords, or any other confidential information to third parties. In addition, those responsible for the access key to the system can do almost anything with the data. And most importantly, it is almost impossible to check their actions due to the fact that there are not so many key holders, otherwise the technology will lose its significance.

The second problem caused by people is more global and is the weak link of any blockchain. In this case, the attack will be made not on the technology, but on the organization or the user. Three major threats have been identified in this study.

- Direct virus infection

This method is traditional. And it requires from a hacker only charisma and excellent skills for manipulating people. It is enough for him to influence the employee of the cryptocurrency exchange or to settle on it himself, after which, independently or through an intermediary, infect the server with a virus. That will allow access to the blockchain.

- Not a direct virus infection

This problem has recently become increasingly relevant. Regular Internet users who download various programs from questionable sources, most often using “uTorrent”, “MediaGet” programs or using an “EXE archiver”, risk infecting your computer with various viruses, including “styler” and “virus- miner.

In the first case, there is a risk of instantly transferring all your saved documents and browser caches to hackers, who can easily recognize your numbers and passwords if they were registered on a computer somewhere. If your computer is infected with a “miner-virus”, then almost all computer resources will go to provide the attacker with a cryptocurrency. Now went more advanced viruses that skillfully know how to hide their existence. So, on “Windows 10” when launching Task Manager, the virus will automatically be turned off, so that the user cannot trace unplanned expenses of his computer resources. Therefore, it is recommended to use analogues, for example, "AIDA64".

In addition, there is another type of virus called "WinLocker". Which translates as "window lock", it involves the closure of access to the operating system. In order to remove it, you need either advanced user skills to combat the virus, or pay for a password, and most often the bitcoin wallet is indicated. This item refers to the error of people, since these viruses cannot get onto your computer on their own, most often this happens when a user with antivirus turned off visits prohibited sites, downloads hacked programs that cannot be installed with antivirus turned on. But even if one is always careful, there is a risk of facing social engineering. This is one of the big security problems of the blockchain. It presupposes that you voluntarily, even if not consciously, provide all your data, including the numbers and necessary information to receive your cryptocurrency.

The easiest way for a hacker to achieve this is “phishing”. Most often it is distributed via emails or social networks. In them you are most often sent to a popular, but fake site, which is not significantly different domain name. On the site you are asked to enter your details to get something tempting. And as practice shows, some users believe in it, and willingly send their data.

To defend against this kind of attack is simple. You need to be vigilant and never send your credentials or keys to cryptocurrency wallets.

- Doubtful exchange

This method is similar to financial pyramids. It is enough to create your own cryptocurrency exchange or a website on the Dark Web network, wait for investments and leave with all means.

As can be understood from the article, there are many security problems with the blockchain, which positions itself as one of the safest inventions of mankind. In addition to social engineering, direct virus injection, fraudulent schemes, and other types of system fraud, there are also more formidable security opponents, such as the 51% attack or DDoS. And even if the traditional power of hacker attacks is not enough, cybercrime develops with cybersecurity, and vice versa. In addition, blockchains are being improved, and not standing still. The factor of reforms plays here, they happen all the time, but not all of them are good and positive by nature, because in a place with a good, like a Trojan horse, they are able to carry various kinds of mistakes. Thereby opening the door for hackers in their system.

4 Conclusions

In conclusion, it can be said that the blockchain is a relatively new revolutionary and leading technology that is able to completely reconsider the issues of data storage and the use of digital currency. The only problem with this technology is its errors and vulnerabilities, most of which have not yet been eliminated. Our results demonstrated a possibility of various types of attacks on the technology and provided many examples and cases that show its vulnerability. This is an aspect that should be tackled via technological but also the legal means that are lacking today.

Nevertheless, we should admit that the technology might ensure leadership for business entities, individuals and even national governments in the spheres of business and finance, information technology and science, as well as cybersecurity. The technology is getting popular virtually in all spheres of economic and public life, so it becomes a centre of attention of media, governments, and people.

Along with the popularity and proliferation of blockchain technology, a growing number of cyber-attacks against it are also increasing. New vulnerabilities are discovered, new hacking methods are being developed, and old ones are being improved. A huge number of technical problems are solved very quickly and efficiently, however, such technology should be more strongly promoted to the general public and masses, along with ways

of dealing with vulnerabilities, to ensure the confidentiality of users, and most importantly, to save them from their own mistakes and careless decisions.

References

Bartoletti M, Pompianu, (2017) An analysis of Bitcoin OP_RETURN metadata. In International Conference on Financial Cryptography and Data Security. Springer, Cham, pp. 218-230

Butenko ED (2014) Bitcoin The state and prospects for the development of cryptocurrency. Finance and credit 23(599):44-47.

Butenko ED, Isakhaev NR (2018a) Contours of blockchain technology in a financial institution. Finance and credit 24(774):1420-1431.

Butenko ED, Isakhaev NR (2018b) Electronic money and cryptocurrencies: contradictions and pitfalls. National interests: priorities and security 6(363):1092-1108.

Chertoff M (2017) A public policy perspective of the Dark Web. Journal of Cyber Policy 2(1):26-38. doi: 10.1080/23738871.2017.1298643

Christensen C (2007) Polish mathematicians finding patterns in Enigma messages. Mathematics Magazine 80(4):47-273. doi: 10.1080/0025570X.2007.11953492

Efanov D, Roschin P (2018) The all-pervasiveness of the blockchain technology. Procedia Computer Science 123:116-121. doi: 10.1016/j.procs.2018.01.019

Galvez JF, Mejuto JC, Simal-Gandara J (2018) Future challenges on the use of blockchain for food traceability analysis. TrAC Trends in Analytical Chemistry 107:222-232. doi: 10.1016/j.trac.2018.08.011

Giancaspro M (2017) Is a 'smart contract' really a smart idea? Insights from a legal perspective. Computer Law & Security Review 33(6):825-835. doi: 10.1016/j.clsr.2017.05.007

Jun M (2018) Blockchain government-a next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity 4(1):7. doi: 10.1186/s40852-018-0086-3

Meng W, Tischhauser EW, Wang Q, Wang Y, Han J (2018) When intrusion detection meets blockchain technology: a review. IEEE Access 6:10179-10188. doi: 10.1109/ACCESS.2018.2799854

Penkova IV, Korolev VA, Butenko ED, Glazkova IY, Eldarov SK (2019) Crypto currencies as a modern financial tool of digital economy: global experience of state regulation Advances in Intelligent Systems and Computing 726:326-334. doi: 10.1007/978-3-319-90835-9_38

Strielkowski W (2017) Will the rise of Sci-Hub pave the road for the subscription-based access to publishing databases? Information Development 33(5):540-542. doi: 10.1177/0266666917728674

Volety T, Saini S, McGhin T, Liu CZ, Choo KKR (2019) Cracking Bitcoin wallets: I want what you have in the wallets. Future Generation Computer Systems 91:136-143. doi: 10.1016/j.future.2018.08.029

Watanabe H, Fan H (2019) A Novel Chip-Level Blockchain Security Solution for the Internet of Things Networks. Technologies 7(1):28. doi: 10.3390/technologies7010028

Yuan Y, Wang FY (2018) Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems 48(9):1421-1428. doi: 10.1109/TSMC.2018.2854904

Zielinska A (2016) Information is a market products and information markets. Czech Journal of Social Sciences, Business and Economics 5(4):31-38. doi: 10.24984/cjssbe.2016.5.4.4

Zheng Z, Xie S, Dai HN, Chen X, Wang H (2018) Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services 14(4):352-375. doi: 10.1504/IJWGS.2018.095647