Advances in Social Science, Education and Humanities Research, volume 441
6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019)

Leading Opportunities for Fighting Cyberterrorism Using Blockchain Technology

Olga Vorobyova*
Togliatti State University
Belorusskaya str.14, 445020 Togliatti
Russian Federation
e-mail: olga80_tlt@mail.ru

Julia Polyakova
Togliatti State University
Belorusskaya str.14, 445020 Togliatti
Russian Federation
e-mail: ua.polyakova@yandex.ru

Olga Borzenkova
Samara State Social and Pedagogical University
Gorky str. 65/67, 443099 Samara
Russian Federation
e-mail: olga80_tlt@mail.ru

Abstract This paper focuses on the leading opportunities of applying the blockchain technology for tackling cyberterrorism. Originally developed for the digital currency called Bitcoin, blockchain technology created a platform for a new segment of Internet, influenced the decentralization of the network by the principle of a distributed registry, and began to be used in all kinds of combinations and combinations for various purposes, including cybersecurity.
The use of blockchain technology for ensuring cybersecurity and its leading potential in that is unlimited, thanks to such unique properties as reliability, accessibility, high adaptability, economic efficiency, and profitability.
Our results show that the use of blockchain technologies in combating cybercrime, including cyber terrorism, can extend to the control of financial services, transport, or any other industry. However, the growth of criminal activity using blockchain technologies will also intensify if law enforcement agencies cannot technologically competently, at a faster pace, detect these developing centres, determine their actions, and destroy illegal plans.

Keywords: *leading opportunities, cyberterrorism, blockchain technology, Bitcoin, digital technologies*

1 Introduction

Today's rapidly globalising world is marked by the development of computer technology, the massive increase in the number of Internet users, and overall cyber integration (Kshetri 2017). The digital transformation embraced such fundamental areas of activity as public administration, economics, politics, legislation, justice, business, management, as well as education and science. Communication, training, banking operations, purchases, information storage and much more have moved into the virtual space. One of the main roles in these processes belongs to blockchain technology in its various varieties and combinations (Hinings et al. 2018).

Innovative blockchain use is particularly useful for enhancing cybersecurity and has already become a component in other areas besides cryptocurrencies. Blockchain technology might help to protect companies, individuals, and governments from the threat of cyber-attacks such as ransomware, phishing, or ransomware attacks (Wilner et al. 2020).

Although few of the capabilities underlying the blockchain offer data availability, integrity, and confidentiality, companies and their technical infrastructure must follow cybersecurity standards and controls to protect themselves from external attacks. Blockchain, a distributed ledger technology (DLT), focuses on building trust in an untrusted ecosystem and making it a decentralized ledger system. All information is transparently available to members of a blockchain, and members' nodes can view, record, share or record transaction data encrypted on their blockchain (Siano et al. 2019). This registry technology has many advantages, such as the ability to encrypt messages and secure transactions. But there is much more, such as accounts with personal information and digital financial data spread across multiple accounts, protected only by weak passwords, and just waiting to be exploited. Blockchain technology is at the heart of this ecosystem - a system as a viable way to improve

cybersecurity, protect valuable assets from the myriad cyber-attacks that afflict organizations and the economy as a whole, and create a safer environment for digital assets and financial transactions.

Blockchain technology and distributed ledger technology are decentralized, decentralized ledgers that capture the origin of a digital asset and make the history of that asset immutable and transparent. Simply put, blockchain technology enables distributed access to digital assets, the ability to copy and transfer assets, and creates a transparent recorded history and change that preserves the integrity of the document. The use of blockchain technology in cryptocurrencies is diverse, but the use case of blockchain identity is likely to gain the most traction among technology enthusiasts and enthusiasts worldwide, because the ability to securitize data and store personal data securely is one of the original purposes of blockchain technologies. In industries ranging from health-care digital identity to politics and digital voting, smart contracts come into play, as do decentralized notaries. Today, blockchain technology can be used to identify individuals, companies, organizations, and even governments such as the United States government. Blockchain has become one of the most disruptive technologies, reducing the prevailing security issues surrounding financial transactions. With the discovery of further practical implementations of this technology, blockchain becomes a powerful tool to address a range of cybersecurity challenges and provide security to global institutions. Blockchain technology has been used to improve IT security through cyber security, but there is now progress in using blockchain technology in other areas such as digital identity, digital coordination, and smart contracts. Blockchains can be stored in a single place without the need to make exact redundant copies, making them more secure and reliable than traditional databases. A clear distinction must be made between the use of blockchains for cyber security and the serious vulnerabilities reported by hackers who have been able to steal from cryptocurrency exchanges. The fallacy of cryptocurrency exchanges is that blockchain security is not strong enough to protect transactions that need to decrypt the data before they can be processed.

Nowadays, blockchain is most in demand in the financial sector, for example for the creation of digital currencies, transactions, exchange, and storage of financial information (Ciaian and Rajcaniova 2018). It is used in other areas, such as smart contracts, registration of public records (registration of ownership of real estate, licensing, creation and liquidation of organizations, civil registration, issuance of digital identification cards, driver's licenses, or the electronic medical records).

Our paper focuses on the leading opportunities for fighting cyberterrorism using blockchain technology that might help to extend to the control over the financial services, transport, or any other industry and any part of the social and economic life.

2. Blockchain and cryptocurrencies

By the simplest definition, a cryptocurrency is a digital currency that operates independently of a central authority or central bank (Lansky 2018). With a holistic definition, many argue that cryptocurrencies such as Bitcoin, Ethereum, and other distributed ledgers are capable of radically transforming and transforming the fundamental economic pillars of society. However, the technology is new and subject to change, and certain headwinds related to scalability and security still need to be addressed. In recent years, tens of millions of cryptocurrencies - assets - have been lost in cyberattacks carried out by sophisticated hackers using a variety of techniques, including phishing and other forms of cyber-attacks. Despite efforts to strengthen cryptocurrency custody security and the infrastructure needed to maintain it, attackers continue to innovate, even surpassing the current state of cybersecurity technology. A total of 125 exchanges were looted by cyber criminals in the second quarter of 2019, and suspected fraud has emerged in recent months, blaming Bitcoin, Litecoin, Monero and Ethereum, as well as other cryptocurrencies. In the same month, researchers from the Palo Alto Network published a report on a new form of malware that can "steal" bitcoin, Litecoin, Monero, or Ethereum by replacing the addresses of cryptocurrency transactions with those in a wallet controlled by the attacker (ZDNET 2018).

Cryptocurrency exchanges are often the target of attacks. On the one hand, the exchange acts as an intermediary between buyers and sellers of cryptocurrencies, but on the other it still uses centralized server technology to store user information and transactions (Sun Yin et al. 2019). Moreover, blockchain companies tend to prioritize the development of technological infrastructure over corporate and human resources, and this often leaves cybersecurity problems open.

A digital currency like Bitcoin ensures that money in the network cannot be duplicated. However, any Bitcoin transaction can only be verified by using the Bitcoin blockchain, not by the user's computer. The recipient returns the Bitcoin to the sender, but only after a certain time, usually after a few seconds. If a duplication attempt is made, the transaction is rejected by the blockchain as faulty or as a forge due to a faulty forge. Bitcoin and other services that build services on Bitcoin had some problems but have taken security measures to ensure there is no loss of funds in network disruptions. Bitcoin withdrawal services such as Coinbase and Bitfinex have stopped processing Bitcoin withdrawals due to conflicting results reported by the BitCoind wallet, caused by a denial-of-service attack that used the Malleable transaction to temporarily disrupt the balance sheet audit (Cryptoslate 2019). However, according to a report by the United States Department of Justice, it is unlikely that governments will

accept bitcoin payments if they are obtained by a criminal enterprise or a ransomware attack. Since cryptocurrencies are banned in Iran, owners of Bitcoins do not appear to have any legal recourse in either Iran or the United States. Federal agents seized 500 bitcoins, which were worth just $5.7 million at the time (Dion-Schwarz et al. 2019).

Some studies argue that 25% of Bitcoin users are associated with illegal activities, whole other studies suggest that less than $1 of all Bitcoins exchanged for currencies such as the dollar and the euro come from illegal sources (Corbet et al. 2019). Regardless of the proportion of illegal transactions, criminal organisations use virtual currencies (VC) as a means of payment for organisations that still prefer cash that remains completely anonymous. This is fuelled by the fact that terrorist organisations also use VCs and terrorists are increasingly adept at using the Internet to support their terrorist activities, such as buying weapons online. The use of anonymisation services for access to the darknet, combined with money transfers and cryptocurrencies such as Bitcoin, leaves little trace and makes them more attractive to criminals and terrorists than traditional transfer methods. They offer encrypted chats to avoid interception of communications by law enforcement agencies, as well as access to a wide range of financial services.

While the growth of ransomware attacks may have slowed, such attacks persist and increasingly appear to be launched by nation states. But ransomware is not the only malware game in town. As individuals and businesses use digital technologies, the risk of cybercrime threats increases, according to the report. One can see targeted threats that often use a variety of clever techniques to infect systems. The growth of ransomware in recent years was significant, with the report claiming that ransomware was be the top 5 malware activity in the U.S. for the first time identified in 2016, compared to the top 3 the previous year (Hull et al. 2019). This is mainly because hackers can block access to important files and use bitcoin payment methods. This shows how damaging a cyberattack can be to a city, and increases the potential for cyberterrorism, a phenomenon that has been largely avoided. Cyberterrorism is not necessarily planned, orchestrated, or orchestrated with a specific political motivation, but it is not necessarily a direct threat any country or its citizens.

The virtual currency also faces growing vulnerabilities and orchestrated attacks on bitcoin exchanges, rogue miners who selfishly mine, and the threat of a hard fork. These concerns, which can be destructive to Bitcoin, are real, but they are not the only ones. There are also real vulnerabilities in Bitcoin wallets when it comes to hacks, attacks, and thefts. There is also the possibility that hackers use ransomware attacks on targets as targets. The developers of such Ransomware want you to pay a ransom in the form of Bitcoins to release the hacked computer files. Cryptocurrency traders are a soft target, as some of them are the first - time traders lured by the massive price increase offered by the cryptocurrency market. Bitcoin wallets are targeted because of a lack of security to curb wallet thefts, and because blockchain is essential to the formation of bitcoin. Blockchain has its flaws and is not easy to find and overtake, giving hackers multiple opportunities to attack. Sometimes these attacks are so successful that cryptocurrency exchanges are hacked, sometimes not. The cyber criminals of the new age are now using phishing techniques to steal cryptocurrencies, such as "crypto jacking." In the new age of crime, crypto jacking is essentially when a website is injected with malicious code to harness the processing power (CPU) of website visitors. We are publishing a new report entitled "Crypto - Jacking and Cryptocurrency Threats" which shows that hackers do indeed pose a risk to both holders of cryptocurrencies and depositors of cryptocurrencies (Lamba and Garg 2019). It is estimated that almost $2 billion has been lost since the rise of the asset class through the large cryptocurrency hacks (Makarov and Schoar 2020). In the face of such security threats discussed in this article, the original thesis that the valuation of digital assets is rapidly increasing has been solidified. As the market transcends the manic hype and begins to understand the most important fundamental issues of digital wealth, digital preservation (centralized vs. decentralized) will be an important issue.

3. Blockchain and Darknet

The term "darknet" first appeared in the 1970s and refers to private networks with a high degree of secrecy (Mirea et al. 2019). It is a large online marketplace that began as an experiment and turned into a network for buying drugs, selling drugs and counterfeit documents, and operating things with Bitcoin as the main currency. Onion routing is most used, where IP addresses are hidden, and data is transmitted in encrypted form. Darknet runs on the anonymous software The Onion Router (TOR) which constitutes a system of proxies that secretly enter the Internet, maintain anonymity when visiting sites, instant messaging, working with applications, etc. Although the anonymous Internet initially meant nothing dangerous, it began to go underground and became a means of communication for illegal activities and crimes. The shady corners of the deep web are like the usual Internet in that it is impossible to get to the other side without a Google search.

Analysts say criminals are ditching Bitcoin in favour of other digital currencies which are easier for law enforcement to use to track criminals in the anonymous corner of the internet known as the darknet. While the exact number of illicit bitcoin transactions in 2015 and 2016 is hard to pin down, illegal transactions have fallen from 20 percent last year to about half of the total, according to the United States Justice Department (Popper 2020). While anonymity is untouchable in the deepest reaches of the Internet, transactions can be made with

cryptocurrencies such as Bitcoin and Ethereum.

People shopping on dark web markets are understandably concerned about privacy, as they often use a number of methods to transfer money. A conventional equivalent would be to move funds through a bank in the United States, Canada, Australia, New Zealand, or other countries. Some even claim that Bitcoin was originally created to facilitate the transfer of money from one person to another, not the other way around. However, one of the main objectives of cryptocurrencies and the blockchain technology that enables them is to empower individuals through truly disintermediated peer-to-peer networks.

It is likely that some people are using Bitcoin for some extremely dubious purposes. These events are helping to make Bitcoin's status as a haven for illegal activity even more questionable. In addition to other illegal applications of cryptocurrencies, including ransomware, smuggling sales have also shifted to new digital currencies such as Moneros and Zcash, which by default promise much more privacy. As global regulators and enforcement agencies do their best to shut down darknet markets that operate with cryptocurrencies, new arrests and reports keep coming. It is interesting to note that since early January 2020, United States citizens have been held responsible for the illegal distribution of narcotics and the exchange of bitcoin.

4. Threats of cyberterrorism

Cyberterrorism is often understood to mean cybercrime, but the obvious difference between cyberterrorism is a political (and/or ideological, religious-ethnic, social) motive (Steiger et al. 2018). Cybercrime is aimed solely at financial gain. Based on the analysis and synthesis of Russian and foreign sources, it can be concluded that cyber terrorism is a deliberate, ideologically and politically motivated criminal activity carried out in cyberspace through digital technology and directed against information, computer systems, computer programs and databases, as well as critical information objects infrastructure that poses a threat to life or health of people or the onset of other serious consequences, if such actions were committed with the purpose of violating public security, intimidating the population and authorities, achieve criminal intent, provoking military conflict. At the same time, terrorist cyber-attacks can be aimed at objects of both a virtual environment and reality

In addition to providing obvious advantages and a new quality of life, total digitalization entailed not only a large-scale dependence of society on information technology, but also the emergence of cybercrime, as well as its most destructive forms - cyber terrorism and cyber extremism. The Internet has been realized in the creation of cyberspace in which terrorists and extremists can quickly and anonymously carry out an extensive exchange of information, seamlessly make communications and launch attacks on objects of value to them.

Today, terrorist groups such as Hamas, Hezbollah, Egyptian Al-Gamaa al-Islamiya, the Kurdish Workers Party, Al Qaeda, the Islamic State of Iraq and the Levant (ISIS), as well as hundreds of others, are actively working on the World Wide Web. Militant radical organizations see the Internet as an ideal arena for illegal activities due to the extremely inadequate legislative regulation of relations in the cyber network, the unhindered distribution of the flow of free information, and easy access to online space from almost anywhere in the world.

Superpower for cyberterrorists created a darknet, as well as fiscal-uncontrolled digital computing, virtual logistics, instant messaging, and transaction anonymity. Cybercriminals use the decentralized organization of the shadow Internet to conduct illegal transactions, to receive payments from victims of extortion and to launder proceeds. In order to carry out criminal intentions, terrorist organizations are actively using digital technologies - blockchain, artificial intelligence (AI), big data, augmented and virtual reality, robotics, 3D printing, and others. The Internet is used by them for safe communication, gathering information, disseminating propaganda, applying cyberattacks to databases and critical information infrastructures, conducting psychological and unleashing a real war, recruiting, recruiting fighters and sympathizers (Van Niekerk 2018).

The use of blockchain technology and products based on it in the fight against cyber terrorism is carried out, as a rule, in a complex with other super technologies. So, the blockchain in combination with artificial intelligence is used to filter and identify important information, to search in huge data arrays.

Based on the blockchain, software is being developed that can identify and remove terrorist content before it becomes mass distributed. Elements of blockchain technology are present in face recognition and recognition software, in explosive detection systems in vehicles, For example, there are robots that can penetrate an extremely dangerous environment for humans, and even in high-tech elevators that instantly deliver people from the upper floors of skyscrapers to the lobby.

The scope of blockchain technology in cybersecurity is unlimited due to its unique properties such as reliability, accessibility, high adaptability, economic efficiency and profitability. Using the blockchain to fight cybercrime can be extended to financial services, legislation, the transport industry, or any other industry that requires third-party verification.

5. Conclusions and implications

All in all, it becomes clear that Blockchain technology can contribute to improved data allocation, better data

security and more efficient data management in industrial IoT applications such as smart contracts, smart grids, as well as smart cities. Even though blockchain is still considered an emerging technology, but many global organizations have already begun to make significant investments in blockchain - application-based development. Blockchain is the fundamental technology on which the popular Bitcoin platform is built and is a technology that organizes and secures data in such a way that it can greatly reduce the cost and complexity of transactions. The technology is being trialled to ensure that transactions are carried out by applications developed to use it, such as smart contracts and smart grids. The global banking industry is fully committed to the adoption of blockchain technology. In particular, the world's largest banks, including Bank of America, Goldman Sachs, JPMorgan Chase, and Citigroup, have adopted them as part of their business models.

It goes without saying that the basis of all these developments and the mechanism for their application in law enforcement should be appropriate legislation that responds to new risks and threats in a timely manner, as well as legalizing the use of digital technologies. It seems necessary to introduce into the legal field the activities of digital currency exchange providers, as well as the sale and purchase of not only tokens, but also cryptocurrencies, which will solve a number of primary tasks, such as countering the financing of terrorist activities and money laundering. It should be noted that the practical implementation of the requirements for the identification of traders is difficult due to the lack of direct contact with the user and the lack of proven identification mechanisms in relation to cryptocurrencies.

Blockchain-based Bitcoins which can be used to transfer money without a centralized, trusted entity, have made it possible to decentralize untraceable marketplaces. Regulators are weighing and fearful about how common cryptocurrencies are allegedly used for dark web transactions, and drug trafficking is the subject of intense scrutiny by the legislators and law enforcement agencies worldwide. In fact, Bitcoin and other digital assets have been used to buy contraband from illegal websites. Nonetheless, misinformation about regulators ability to track bitcoin or other crypto transactions suggests that their capabilities still leave much to be desired.

In addition, legislation should continuously improve the criminal law assessment (qualification) of cybercrime and cyber offenses, introduce new types of them, and strengthen the system of punishments for cyber terrorism. Set administrative fines for such offenses in a virtual environment, such as repeatedly viewing streaming terrorist video content or sending files of a terrorist and extremist nature.

Thus, we can conclude that the development of high-tech digital mechanisms to counter cyber terrorism and the unification of efforts by states around the world is a priority at the present stage. The international community should develop uniform rules for the game in the field of digital technologies for all countries, a universal and common international standard for all that will consider the interests of each country to the maximum. The cross-border cyber threat data sharing system should be improved. However, security measures should not be taken to the detriment of technological progress and innovation. Freedom of communication and communication, as well as the unhindered exchange of experience and ideas in the digital age, should be guaranteed by law.

References

Ciaian P, Rajcaniova M (2018) Virtual relationships: Short-and long-run evidence from Bitcoin and altcoin markets. Journal of International Financial Markets. Institutions and Money 52:173-195. doi: 10.1016/j.intfin.2017.11.001

Corbet S, Lucey B, Urquhart A, Yarovaya L (2019) Cryptocurrencies as a financial asset: A systematic analysis. International Review of Financial Analysis 62:182-199. doi: 10.1016/j.irfa.2018.09.003

Cryptoslate (2019) Bitfinex users unable to withdraw funds, $430 million drained from exchange cold wallets. https://cryptoslate.com/bitfinex-users-unable-withdraw-funds-430-million-drained-exchange/ Accessed 19 Apr 2020

Dion-Schwarz C, Manheim D, Johnson P (2019) Terrorist use of cryptocurrencies. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf Accessed on 29 Mar 2020

Hinings B, Gegenhuber T, Greenwood R (2018) Digital innovation and transformation: An institutional perspective. Information and Organization 28(1):52-61. doi: 10.1016/j.infoandorg.2018.02.004

Hull G, John H, Arief B (2019) Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science 8(1):2. doi: 10.1186/s40163-019-0097-9

Kshetri N (2017) The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply. Telecommunications Polic 41(1):49-67. doi: 10.1016/j.telpol.2016.11.002

Lamba T, Garg A (2019) Cyber: Threats in social networking websites and physical system security. IITM Journal of Management and IT 10(1):46-54

Lansky J (2018) Possible state approaches to cryptocurrencies. Journal of Systems Integration 9(1):19-31. doi: 10.20470/jsi.v9i1.335

Makarov I, Schoar A (2020) Trading and arbitrage in cryptocurrency markets. Journal of Financial Economics 135(2):293-319. doi: 10.1016/j.jfineco.2019.07.001

Mirea M, Wang V, Jung J (2019) The not so dark side of the darknet: a qualitative study. Security Journal 32(2):102-118. doi: 10.1057/s41284-018-0150-5

Popper N (2020) Bitcoin Has Lost Steam. But Criminals Still Love It. https://www.nytimes.com/2020/01/28/technology/bitcoin-black-market.html Accessed 02 Apr 2020

Siano P, De Marco G, Rolán A, Loia V (2019) A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. IEEE Systems Journal 13(3):3454-3466. doi: 10.1109/JSYST.2019.2903172

Steiger S, Harnisch S, Zettl K, Lohmann J (2018) Conceptualising conflicts in cyberspace. Journal of Cyber Policy 3(1):77-95. doi: 10.1080/23738871.2018.1453526

Sun Yin HH, Langenheldt K, Harlev M, Mukkamala RR, Vatrapu R (2019). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. Journal of Management Information Systems 36(1):37-73. doi: 10.1080/07421222.2018.1550550

Van Niekerk B (2018) The Cybersecurity Dilemma: considerations for investigations in the Dark Web. Acta Criminologica: Southern African Journal of Criminology 31(3):132-148

Wilner A, Jeffery A, Lalor J, Matthews K, Robinson K, Rosolska A, Yorgoro C (2019) On the social science of ransomware: Technology, security, and society. Comparative Strategy 38(4):347-370. doi: 10.1080/01495933.2019.1633187

ZDNET (2018) 2018's most high-profile cryptocurrency catastrophes and cyberattacks. https://www.zdnet.com/article/2018s-most-high-profile-cryptocurrency-catastrophes-ico-failures-and-cyberattacks Accessed 22 Mar 2020