Using blockchain Technology for Boost Cyber Security

Antonina Farion
Economic Security and Financial Investigations Department
Ternopil National Economic University
Ternopil, Ukraine
ORCID 0000-0002-0485-9563
Secretmail_antonina@ukr.net

Oleksandr Dluhopolskyi
Economic Theory Department
Ternopil National Economic University
Ternopil, Ukraine
ORCID 0000-0002-2040-8762
dlugopolsky77@gmail.com

Serhiy Banakh
Criminal Law and Process Department
Ternopil National Economic University
Ternopil, Ukraine
ORCID ID: 0000-0002-2300-1220
s.v.banakh@tneu.edu.ua

Nadiia Moskaliuk
Economic Security and Financial Investigations Department
Ternopil National Economic University
Ternopil, Ukraine
ORCID ID: 0000-0003-2972-3352
moscaluc_nadiya@ukr.net

Mykhailyna Farion
Economic Theory Department
Ternopil National Economic University
Ternopil, Ukraine
ORCID ID: 0000-0001-7456-2864
mishelle1@ukr.net

Yuryi Ivashuk
Economic Theory Department
Ternopil National Economic University
Ternopil, Ukraine
ORCID 0000-0002-8459-4744
ivashuk@email.ua

***Abstract* – The article discusses the main possibilities of the blockchain technology for boosting cyber security. It is wide known that cyber criminals are able to break any computer system and accounts; simultaneously available for nowadays protecting technologies could not protect high secret informational dates and bank accounts reliably with guarantee. So, technologies based on cryptography are becoming more demanding by companies and organizations as well as scientists and researchers.**

Keywords - information technology, blockchain, cyberspace, cyber criminals, cyber security, and protection.

I. Introduction

The high level of the internet using nowadays has resulted on various organizations and companies and on all communication and date and make opportunities for cyber attackers. If several years ago cyber criminals stole only information and valuable dates now they try to steal even intellectual property. There is a possibility that in the near future they will join in groups.

II. Theoretical Basis

The biggest threat for Internet network and all users is cybercriminal activity that is becoming the biggest challenge that humanity faced nowadays. There are many types of software that protect computers but it becomes hardly to get full and professional protection against cyber criminals.

Blockchain is a powerful innovation that brings substantial positive change to the financial services industry. There are two types of blockchains: public and permissioned blockchains. Dylan Yaga and others [1] prove that blockchain technologies become more popular during last few years and blockchain implementations are often designed with a specific purpose or function – cryptocurrencies, smart contracts and distributed ledger systems between businesses.

III. Literature Review

Scientists from all countries summarize their research results towards cyber crimes activities and seek solution to prevent increasing numbers of cyber attacks around the world and many of them overgo from theoretical framework and investigations to practical implementation.

VI. Practice

Cyber criminals more than ever before have organized their operations to take advantage of stolen dates and information from the world Internet network. 2018 year showed the continued increasing of cyber crime globally. The last year also became the scene for the rapid rise of cryptojacking as a means of making money for cyber criminals. Dr. Michael McGuire [2] indicated that the cybercrime economy has grown to $1.5 trillion dollars in 2018, equal to the GDP of Russia. The research showed impressed figures (fig. 1).

The reasonable explanation for it could be a growing interconnectedness and interdependence between both the illegitimate and legitimate economies. Platform for cyber criminals is commercial area not only personal information and personal computers as it was several years ago.

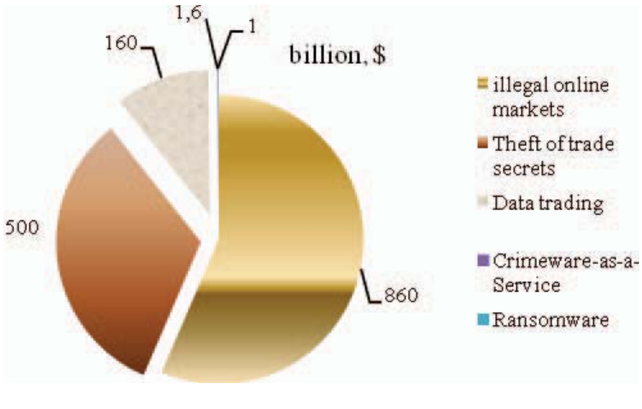


Fig. 1 Cybercriminal revenue generation in the hyper-connected web of profit, 2018 [2]

We consider that here should be given the list of the most spread types of cybercrimes around the world (fig. 2). Cyber theft of intellectual property is the most dangerous for almost all types of business as cyber crooks work to exploit every opportunity they find.

978-1-7281-0450-8/19/$31.00 ©2019 IEEE

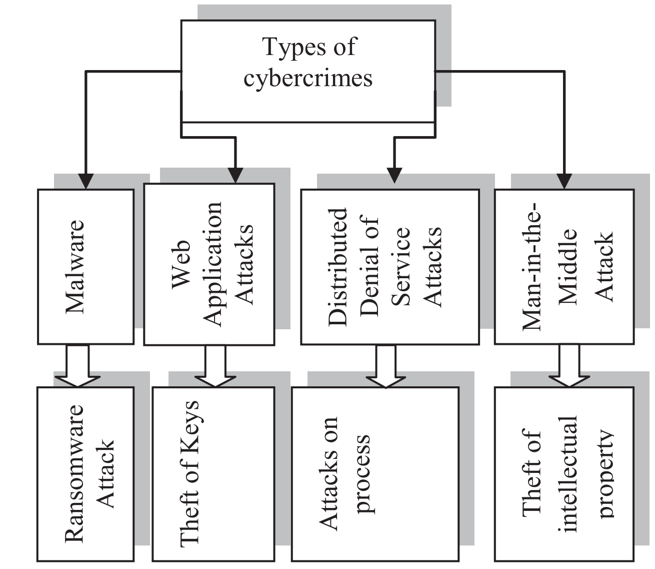


Fig. 2. The most spread types of cybercrime in the world, 2018 [3]

Most cyber crimes are connected through a lack of protection or not effective programs or software. But even with a high protected combination of different software everyone could not be safe totally. Intellectual property crimes are committed when someone makes such procedures as: manufactures, distributes or sells the counterfeit or pirated goods – patents, literary, trademarks, industrial designs or artistic works with commercial goal. The main method of cybercrime is committing crimes by targeting computer networks or devices. With so much attention given to acquiring the newest and most sophisticated types of cyber security software, safeguarding the security of company hardware is often overlooked but the loss or theft of devices is a real threat to be aware of [4].

There were appeared not only the new types of cybercrimes but various tools of their execution (fig. 3).

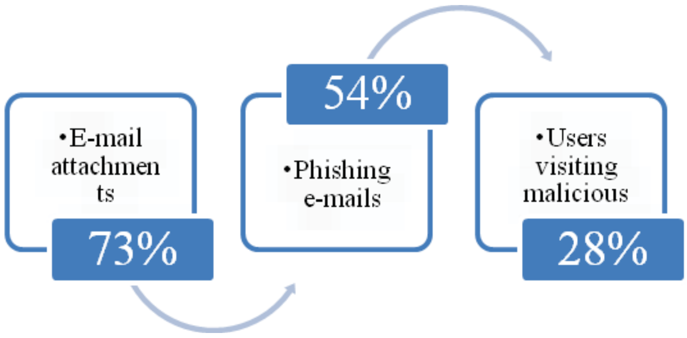


Fig. 3. Ways of entering organizations by cyber criminals [5]

V. Companies Protection Methods

All countries take the harsh actions to protect own properties from cyber attacks. Many companies also establish

precautions to protect own information, dates and intellectual properties:

- strong passwords;
- strong firewall;
- antivirus protection;
- updating programs regularly;
- laptops secure;
- mobile phones secure;
- backup regularly;
- monitoring diligently:
- own attention with e-mails, IM, the web pages;
- employees education and trainings.

But is it possible to guarantee security and privacy? Internet security is a great concern to the governments of all countries. In Deloitte research was admitted: "As cybercrime is increasing in frequency, size and sophistication, it is clear that technological defences alone are no longer sufficient to protect a business from attacks.

Cybercrime has evolved from being a vertically integrated, individualistic activity, to an extremely sophisticated and well-organised, distributed operation, where stolen data is traded and matched on exchanges, and highly specialized professionals are coming in on the action" [6]. In this research also were given the most valuable advices to safe companies from cyber criminals (fig. 4).

Richard Clarke gave such quote to cyber activity increasing: "Corporations need to figure out what their crown jewels are. You can't protect everything and defend your entire corporate network equally. It's not all equally important, either" [6].

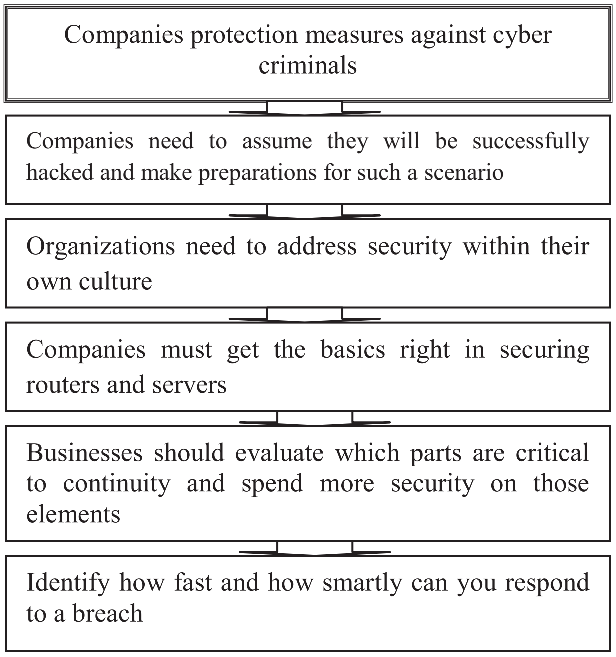
Why people are under so huge risk to be attacked by cyber criminals. Symantec research shows that social networks increase the risk to be affected by criminals and use personal dates. Shortened URLs hide malicious links, increasing infections. Not so many people know that social networks have a dark side. More than 41% of people join the new friends in the social networks and even do not know them [8].

VI. Blockchain Technologies as a Challenge for Boosting Cyber Security

Nowadays blockchain technologies become a challenge for boosting the cyber security. Blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer1 (P2P) basis. Structurally, blockchain data can be consulted, shared and secured thanks to consensus-based algorithms. It is used in a decentralized manner and removes the need for intermediaries, or "trusted third parties" [9].

On October 31, 2008, Satoshi Nakamoto released the Bitcoin White Paper outlining a purely peer to peer electronic cash/digital asset transfer system. This is the first popular implementation of Blockchain and is attributed as birthing today's Blockchain industry. Blockchain is a historical archive of decisions and actions taken.

Nowadays more than 50 largest public companies exploring blockchain and most of them agree to use it on the stable basics and 10 companies have already adopted blockchain – FedEx, Burger King Russia, KIK, IBM, Walmart, Microsoft, Overstock, MasterCard, Huawei Technologies and Bank of America.


Companies protection measures against cyber criminals

Companies need to assume they will be successfully hacked and make preparations for such a scenario

Organizations need to address security within their own culture

Companies must get the basics right in securing routers and servers

Businesses should evaluate which parts are critical to continuity and spend more security on those elements

Identify how fast and how smartly can you respond to a breach

Fig. 4 Companies measures to protect their properties from cyber criminals [6]

With its help, operations can be recorded in blocks; with each block containing the signature of the previous block, which bind them together in a special chain. This technology allows storing and share data based on a “peer-to-peer”[1] computer network that is the combination of asymmetric cryptography and P2P. The general process could be described in follow way (fig. 5).

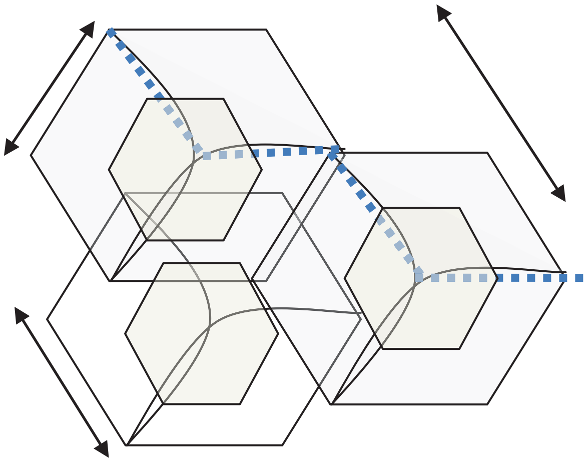


Fig. 5 Blockchain networks system

Blockchain was made from two concepts (fig. 6).

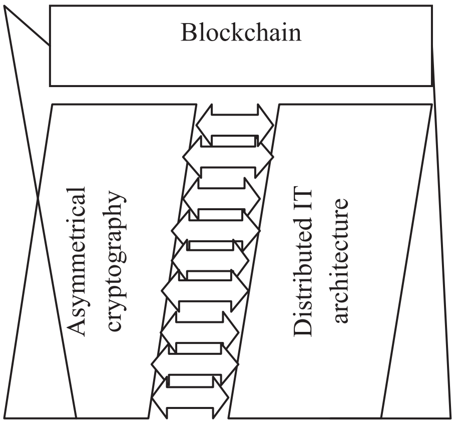


Fig. 6 Blockchain structure [9]

Anonymity – is the main aspect of blockchain technology. Many scientists proof that it is impossible to break codes and stole dates from blockchain technologies. Asymmetrical cryptography enables users who do not know each other to exchange encrypted information. The system is based on a public key that can be made available to all, and allows encrypted data to be sent to a third party. The third party accesses the encrypted data via a paired private key. The public key is similar to a bank account number, which can be provided to anyone. The private key, which remains secret, acts as the password to the same bank account. The blockchain is open-ended and operates in a decentralized, ongoing manner thanks to the activity of its users who can store information, and to consensus algorithms – notably “proof-of-work”[2] and “proof-of-stake”[3].

Blockchain technologies have several advantages. After the invention of the blockchain which is a decentralized database that contains united blocks of information and is limited to modification, many studies have been carried out to study the blockchain technology and many alternative designs have been created and implemented. In summary, it could be emphasize that the blockchain protocol contains several miners that receive data from users (transactions) and store the received information in discrete fragments, which are called blocks, which in turn are combined by hashing for the formation of blockchain. Blockchain technologies are used mainly for mining cryptocurrencies. Yulia Horbenko proves that: “Even though hackers are getting better at hacking, the ways to combat them are also improving very fast. In fact, we already have a nearly impenetrable technology, known as blockchain, which can be used to protect our data from cyber attacks and improve cybersecurity across industries” [10].

[1] Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Materials of Wikipedia. Available at: https://en.wikipedia.org/wiki/Peer-to-peer

[2] A Proof-of-Work (PoW) system (or protocol, or function) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. The concept was invented by Cynthia Dwork and Moni Naor as presented in a 1993 journal article.

[3] Proof of stake (PoS) is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. In PoS-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and wealth or age (*i.e.,* the stake). In contrast, the algorithm of proof-of-work-based cryptocurrencies such as bitcoinuses mining; that is, the solving of computationally intensive puzzles to validate transactions and create new blocks.

We agree with scientific approach that blockchain technology provides one of the best tools we currently have got to protect data and information from hackers, preventing potential fraud and decreasing the chance of data being stolen or compromised. If theft wants to destroy or corrupt a blockchain, this person need to destroy the data stored on every users' computers around the global network where are counted millions of computers, owners of them store copies of all the data.

Hacker could break codes if he will simultaneously bring down an entire network. This task is impossible. Bigger blockchain networks with more users have an infinitely lower risk of getting attacked by hackers because of the complexity required to penetrate such a network.

Authoritative group of subject experts and enthusiasts who are evangelizing the Blockchain Research and Development indicates: "Blockchain technology can be used to prevent any type of data breaches, identity thefts, cyber-attacks or foul play in transactions. This ensures that data remains private and secure" [11]. Many scientists prove that blockchain will transform cyber security (fig. 7).

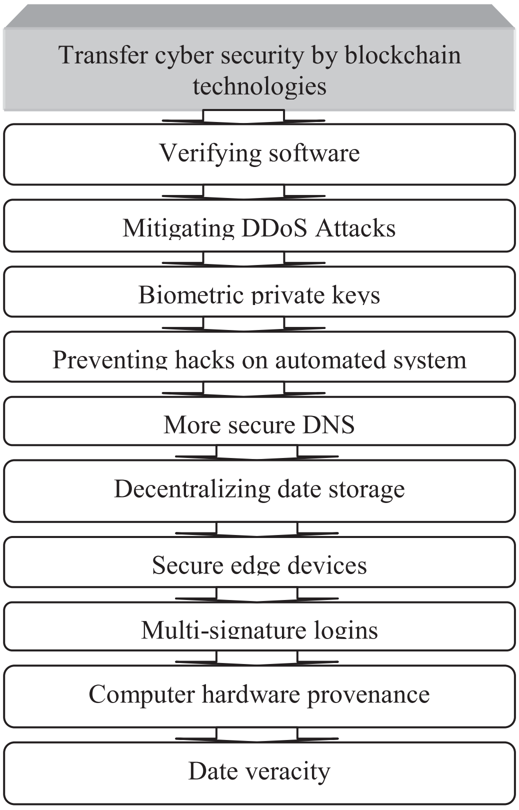

Transfer cyber security by blockchain technologies
Verifying software
Mitigating DDoS Attacks
Biometric private keys
Preventing hacks on automated system
More secure DNS
Decentralizing date storage
Secure edge devices
Multi-signature logins
Computer hardware provenance
Date veracity

Fig. 7. Blockchain will transform cyber security [12]

VII. Conclusion

The using of blockchain technologies by companies and organizations will help secure Internet data, information, devices, and services from cyber attacks. The main advantage of blockchain technologies is impossible to break codes and keys as it combines many computers and users, dates which are anonymous. With blockchain technologies business can authenticate users and devices without the need for giving special information. It could protect all information, dates, transfers and financial operations. Blockchain takes the responsibilities for strong protection from attacks.

References

[1] D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain Technology Overview". NIST, U.S. Department of Commerce," October 12. [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf. [Accessed Jan. 20, 2019].

[2] Bromium, "Hyper-connected web of profit emerges, as global cybercriminal revenues hit $1.5 trillion annually," Bromium, Research by doctor Michael McGuire, April 20, 2018. [Online]. Available at: https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually. [Accessed Jan. 27, 2019].

[3] E. English, A. D. Kim, M. Nonaka, "Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry", Microsoft. 2018. [Online]. Available at: file:///D:/Documents/Downloads/Blockchain-Cyber-Security_WhitePaper_Single-Page_Linked%20(1).pdf. [Accessed Jan. 27, 2019].

[4] A. Popat, "Five Ways To Protect Your Company Against Cyber Attacks," Entrepreneur. July 19, 2018. [Online]. Available at: https://www.entrepreneur.com/article/316886. [Accessed Jan. 29, 2019].

[5] A. Javed, "Cybercrime Trends 2018: Seven misconceptions that can expose companies to a risk of cybercrime," Xorlogics. 1 Jan. 2018. [Online]. Available at: http://www.xorlogics.com/2018/01/01/cybercrime-trends-2018-seven-misconceptions-that-can-expose-companies-to-a-risk-of-cybercrime. [Accessed Jan. 29, 2019].

[6] Deloitte, "Cybercrime is not just a tech problem," Deloitte. [Online]. Available at: https://www2.deloitte.com/au/en/pages/risk/articles/cybercrime-tech-problem.html. [Accessed Jan. 30, 2019].

[7] K. S. Nash, "Richard Clarke: Your company is a front in a future cyberwar," CIO. 27 August. [Online]. Available at: https://www.cio.com/article/2415670/richard-clarke--your-company-is-a-front-in-a-future-cyberwar.html. [Accessed Jan. 30, 2019].

[8] K. K. Ng, "Technology Solutions to Fight Cybercrime," Symantec. 2011. [Online]. Available at: https://www.unodc.org/documents/southeastasiaandpacific/2011/09/cybercrime-workshop/ppt/SYMC_UNODC_ITU_Cybercrime_Workshop.pdf. [Accessed Jan. 30, 2019].

[9] P. Adam-Kalfon, S. El Moutaouakil, "Blockchain, a catalyst for new approaches in insurance," PWC. [Online]. Available at: https://www.pwc.com/gx/en/insurance/assets/blockchain-a-catalyst.pdf. [Accessed Jan. 30, 2019].

[10] Yu. Horbenko, "Using Blockchain Technology to Boost Cyber Security," Steel Kiwi. [Online]. Available at: https://steelkiwi.com/blog/using-blockchain-technology-to-boost-cybersecurity/. [Accessed Jan. 30, 2019].

[11] T. K. Sharma, "The future of cyber security: blockchain technology," Blockchain Council. 25 Sep. 2018. [Online]. Available at: https://www.blockchain-council.org/blockchain/the-future-of-cyber-security-blockchain-technology/. [Accessed Jan. 30, 2019].

[12] S. Mire, "Blockchain In Cyber Security: 10 Possible Use Cases," Disruptor. 26 Nov. 2018. [Online]. Available at: https://www.disruptordaily.com/blockchain-use-cases-cyber-security. [Accessed Jan. 30, 2019].