Iryna DMYTRIEVA[1]

Opiekun naukowy: Oleksandr OKSIIUK[2]

TECHNOLOGIA BLOCKCHAIN W ZADANIACH ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI

Streszczenie: Technologia Blockchain pomaga chronić zarówno osoby fizyczne, jak i firmy. Oprócz kryptowaluty jest ona już wykorzystywana jako komponent w innych obszarach, w szczególności w celu zwiększenia bezpieczeństwa cybernetycznego i bezpieczeństwa informacji.

Słowa kluczowe: Blockchain, cyberbezpieczeństwo, bezpieczeństwo informacji, zagrożenia bezpieczeństwa, kryptowaluta

BLOCKCHAIN TECHNOLOGY IN INFORMATION SECURITY TASKS

Summary: Blockchain technology helps protect both individuals and companies. In addition to cryptocurrency, it is already being used as a component in other areas, in particular, to increase cybersecurity and information security.

Keywords: Blockchain, cybersecurity, information security, security threats, cryptocurrency

1. Blockchain and security issues

Blockchain is decentralized transaction and data management technology. After the publication of data, a stable technique for setting time and a complex link to the previous block is used, so it becomes impossible to make any changes to the record or roll it back.

Blockchain has become an almost ideal tool for ensuring security, storage, and confirmation of data. This technology is the result of many years of achievements in cryptography and information security. The already implemented use of the blockchain is its use in cryptography since this technology allows you to transfer

[1] Taras Shevchenko National University of Kyiv, Faculty of information security, Cybersecurity, email: dmitrieva.die@gmail.com

[2] Doctor of Science, Taras Shevchenko National University of Kyiv, Faculty of information security, email: o.oksiuk@gmail.com

information in a safe way. Blockchain is also used to prevent data manipulation, because the nature of the blocks is unchanged, using sequential hashing along with cryptography in a decentralized structure, it becomes possible to build a system that is almost impossible to manipulate.

Information security is also not standing aside and in the near future will be fully adapted to blockchain technology. The fundamental difference in the technological approach allows us to go beyond the end devices, including the security of information transfer, the digital "identity" of the user, as well as the protection of critical infrastructure. Despite the fact that such transformations are quite complicated, today they can already be observed.

Blockchain is a solid rock, being a distributed and interdependent database. However, not all blocks are equally integrated. There is a big difference between public and private blockchains. If public blockchains do not have restrictions on who can access data or carry out transactions, then in private blockchains these operations are limited to a certain circle of people. Public blockchains provide transparency, while private blockchains provide higher levels of control, but only from specific administrators.

However, blockchain technology isn't all sunshine and rainbows, as you'll soon see, the young industry is chock-full of potential security threats.

Total money lost in blockchain-related hacks in 2018 - $1,064,176,000. Where;

- Exchange hacks - $907,500,00 total lost;
- Software flaws (wallets and dApps) - $24,098,000 total lost;
- Phishing & social engineering - $2,728,000 total lost;
- 51% Attacks - $20,800,000 total lost;
- Other threats - $88,500,000 total lost.

2. Exchange hacks

Exchanges were one of the most popular targets for cybercriminals in 2018, and that doesn't appear to be changing in 2019. One of the largest cybersecurity heists of all time was due to a cryptocurrency exchange breach. Most cryptocurrency exchanges don't have the security rigor, so when trading on an exchange, you should keep the minimum amount of funds you need to actively trade on the platform and the rest of your money should be kept in a hardware wallet.

3. Software flaws (wallets and dApps)

Even if an underlying protocol (e.g. Bitcoin) is a temper-proof, the products built on top of it may have flaws. Software is bound to have bugs, and blockchain products are no exception.

Due to common security flaws, hackers heavily target decentralized applications (dApps) as well. Simply put, dApps are applications and programs that run on a blockchain instead of a central database.

Unfortunately, there's only so much vetting you can do on a wallet and dApps. When researching your choices, it's paramount to read numerous user reviews, checking for any negative reports of bugs or lost funds. Additionally, any wallet or dApp that you decide on should have gone through at least one third-party security audit. Additionally, if the developers open-source their code then the entire community can audit it. Even with third-party audits and community review, some bugs are bound to slip through the cracks. And because blockchain is such a nascent industry, you should always use extreme caution no matter the dApp you operate.

4. Phishing and social engineering

Phishing and social engineering scams are one of the most widespread attacks in cryptocurrency today. In these attacks, malicious parties use a variety of tricks to dupe unsuspecting victims into sending over their private keys or login information.

Phishing scams attempt to duplicate authentic organization online identities to trick you into thinking you're receiving information from an official entity. Scammers usually deceive users by developing replica identities that mimic cryptocurrency-related companies. They'll copy a company's entire identity including an email signature, social media handle, URL design, website design. Often, phishing emails include an official-looking message describing a fictitious issue or chance to receive free tokens. These emails usually contain a call-to-action with a sense of urgency as well.

So when dealing with social media or company communications, it's okay to have a healthy dose of paranoia. Before taking any action, check to make sure every aspect of what you're reading makes sense. Do the names, pictures, branding, handles, and URLs match exactly what they should be? Is the communication free of any spelling or grammar mistakes? If your answer is "no" to either of these questions, don't hesitate to reach out to the other party directly or contact customer support to ask for more information.

1. Conclusion

Another blockchain threat is the 51% Attack. While previous vulnerabilities have focused on the user, this one is an attack on a blockchain itself. They've drastically affected many different blockchains/coins in 2018 and continue to pose an existential threat to many cryptocurrencies, specifically ones using a Proof-of-Work consensus.

A 51% Attack is when a single entity controls the majority of a blockchain's hash rate, "potentially causing a network disruption". Such an attack allows that malicious entity to effectively reverse transactions, leading to the potential of coins to be spent twice. To explain further, a double-spend enables the attacker to obtain coins they just spent and return them to their wallets. Ultimately, the attacker spends coins without actually losing possession, allowing them to pad their wallets with free crypto.

As an individual, there's not so much you can do to protect yourself against 51% attacks. If you're working with a blockchain, it should be one with a significant hash rate, like Bitcoin, or one that uses a consensus method other than Proof-of-Work.

This list of blockchain security issues is just a shortlist of threats. With the development of security strategies, more and more tactics to circumvent it appear.

Therefore, in order to protect yourself, it is very important to keep abreast of the latest blockchain security issues, as well as preventive security measures.

REFERENCES

1. YLI-HUUMO J., KO D., CHOI S., PARK S., SMOLANDER K.: Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE, 11(2016)10, 1– 27. Retrieved from *http://10.0.5.91/journal.pone.0163477.*
2. BENTON M. C., RADZIWILL N. M., PURRITANO A. W., GERHART, C. J.: Blockchain for Supply Chain: Improving Transparency and Efficiency Simultaneously. Software Quality Professional, 20(2018)3, 28–38. Retrieved from *http://search.ebscohost.com/login.aspxdirect=true&db=aps&AN=130510381&site=ehost-live.*
3. CARLOZO L.: What is blockchain? Journal of Accountancy, 224(2017)1, 1–2. https://doi.org/10.1089/glr2.2017.2174
4. OGBU J. O., OKSIUK A.: Information protection of data processing center against cyber attacks,&quot; 2016 Third International Scientific- Practical Conference Problems of Infocommunications Science and Technology (PIC S&amp;T), Kharkiv, 2016, pp. 132-134. doi: 10.1109/INFOCOMMST.2016.7905358
5. KUZNETSOV A., YU. I., GORBENKO D. I., PROKOPOVYCH-TKACHENKO M. S., LUTSENKO M., PASTUKHOV V.: NIST PQC: Code-Based Cryptosystems. Telecommunications and Radio Engineering, Volume 78, 2019, Issue 5, pp. 429-441. DOI: 10.1615/TelecomRadEng.v78.i5.50
6. ENSIGN D.: COPYRIGHT CORNER: Blockchain and Copyright. Kentucky Libraries, 82(2018)3, 4–5. Retrieved from *http://search.ebscohost.com/login.aspxdirect=true&db=llf&AN=131290801&site=ehost-live*
7. NAKAMOTO S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from *https://bitcoin.org/bitcoin.pdf*
8. WOODSIDE J. M., AUGUSTINE JR. F.K., GIBERSON W.: Blockchain technology adoption status and strategies. Journal of International Technology & Information Management, 26(2017)2, 65–93. Retrieved from *http://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=128220219&site=ehost-live*
9. OKSIIUK O., CHAIKOVSKA V.: Development of authentication process when accessing cloud services, 2017 4th International Scientific- Practical Conference Problems of Infocommunications. Science and Technology (PIC S&amp;T), Kharkov, 2017, pp. 604-607. doi: 10.1109/INFOCOMMST.2017.8246473
10. KUZNETSOV A., GORBENKO Y., ANDRUSHKEVYCH A., BELOZERSEV I.: Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2, 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&amp;T), Kharkov, 2017, pp. 203-206. DOI: 10.1109/INFOCOMMST.2017.8246380