Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 75 – 79 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

BLOCKCHAIN TECHNOLOGY AND PERSONAL PRIVACY ISSUES

Iryna Dmytrieva[1], Oleksandr Oksiiuk[2]
[1]Taras Shevchenko University of Kyiv, Faculty of Information Technology, [2]Taras Shevchenko University of Kyiv, Faculty of Information Technology

ABSTRACT: Blockchain technology has gone from prominence in a narrow circle of enthusiasts to mass insanity and frustration. The time has come to take a look at the trends in the development of technology and soberly assess the capabilities of the blockchain after the hype has stopped. Now blockchain finds application in areas such as financial transactions, user identification, or the creation of cybersecurity technologies. Despite the fact that blockchain technology is reliable and supportive, the privacy issues and challenges of this technology cannot be left out.

KEYWORDS*: privacy, blockchain technology, data security, zk-SNARK, online threats*

1. The brief introduction to blockchain

Back in 1991, research scientists S. Haber and W. Scott Stornett described blockchain technologies for solving the security of digital documents with a timestamp so that they could not be faked or framed retroactively.

The system used a cryptographically secured chain of blocks to store documents with a time stamp, and in 1992 Merkle trees were included, and thus, this made the chain of blocks more efficient. However, this technology was not used, and the patent was lost in 2004 [1].

Nevertheless, in 2009, the concept of blockchain again made itself felt, not only as a bitcoin but also expanding its use in other areas. Blockchain, as a distributed database, turned out to be not only an excellent platform for cryptocurrency management, but also interested specialists from other fields, and especially the information security sphere, since this technology allows for more secure transactions, eliminates certain hacker attacks, and in some cases even eliminates the need for passwords [2].

2. Positive side of blockchain technology

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 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 [3].

Among the undeniable advantages of this technology stands out:

- resolving an intermediary attack,
- immunity to data manipulation,
- immunity to DDoS attacks.

2.1 Resolving an intermediary attack

Intermediary attack (Man-in-the-Middle (MITM)) is the name of the attack when users are fraudulently offered through the certification authority (CA) fake public keys, the use of which can lead to the disclosure of confidential data. One solution to this problem is the ability to put the

public key in the published block, which will make the key unchanged. As a result, it will be very difficult for potential attackers to publish fake keys and prove their authenticity. In addition, the certification authority will also be distributed, and disabling the service will become virtually impossible.

2.2 Immunity to data manipulation

Each blockchain-based transaction is distributed between nodes. In other words, each node that confirms the transaction receives a copy of the confirmed information. This means that no one can change the data and go unnoticed.

This prevents many problems, including data manipulation, which can be crucial in some industries, such as healthcare. Using the blockchain, it became almost impossible to engage in fraud in medical insurance or fake records.

2.3 Immunity to DDoS attacks

In recent years, DDoS attacks have become one of the largest online threats from which numerous websites and systems have suffered. However, if domain name systems (DNS) were based on blockchain technology, it would be much more difficult to carry out such attacks. The system would receive additional protection, become more transparent, and the DNS infrastructure would be distributed.

3. Blockchain technology and personal privacy issues

One of the main distinguishing features of blockchain technology is transparency. It is necessary for conducting online transactions without hiding any details, for which crypto aesthetes praise this technology. However, as soon as alternative options for using the blockchain appeared, it became clear that transparency was not always useful, especially when exchanging data.

Transactions on the blockchain are conducted publicly, everyone can view them at any time. This means that the data is not encrypted and accessible to everyone. This is not always convenient - in particular when it comes to confidentiality, be it financial information or medical records.

Of course, such solutions as storing exclusively encrypted data were proposed, but there are drawbacks. For example, the loss of a decryption key can lead to a complete loss of data. Finding it is also a problem: data can again be made available to everyone if the key is published on the Internet.

Confidentiality in blockchain technology is an aspect that still needs a lot of refinement. Despite the fact that the security of the blockchain is significantly improved compared to other systems, with respect to confidentiality, it is significantly lame. However, there is a solution. One of them - zk-SNARK (evidence with zero disclosure), which has already been used by Ethereum and Zcash - gives users the ability to make anonymous payments, vote anonymously, and also has a number of other advantages.

3.1 zk-SNARK technology

When people in the cryptocurrency sphere say “evidence of zero knowledge”, they usually refer to a certain type of evidence - zk-SNARKs. With it you can completely hide all the data: from

which address the payment went, where it came from and how much money was transferred. It also allows you to prove that the transaction has really passed and that the correct amount is on the account of the recipient [4].

When you hear about zero-knowledge proofs, most likely, we are talking about their one specific kind - zk-SNARKs. The basis of these protocols is a complex mathematical apparatus, but you cannot go into it if you do not implement this solution yourself.

Zk stands for zero-knowledge. SNARK – succinct non-interactive adaptive argument of knowledge [5].

Succinct means effective enough to be calculated in a short period of time. This is extremely important when conducting verification.

Non-interactive means that SNARKs do not require Verifier to directly poll Prover. The last one can publish his evidence in advance, and the verifier will verify its authenticity. Imagine that your teacher is asking you an arithmetic problem. After you have solved it, you do not submit the work. Instead, zk-SNARKs prove to the teacher that your result is correct. So far, everything looks very simple, but it's worth a couple of reservations [9].

SNARKs require large computing power. Often they lack the resources of mobile devices. Recently, however, some promising advances have been observed in this regard.

There is also the problem of losing access to the hash function, on the basis of which authentication is verified. SNARK technology allows the user to prove that he has access to a certain secret, but that must ensure its safety and accessibility.

The biggest drawback of SNARKs is the so-called installation phase.

3.2 Installation phase

This step is a necessary part of introducing SNARK protocols into any task. The authenticity of the calculation is fixed on it (the so-called circuit), the result of which you want to prove. Due to this limitation, SNARK protocols are poorly suited for arbitrary Turing-complete smart contracts - each new contract will require a new installation. Each of the tasks set by your teacher will require its own installation phase [6]. For example, one phase will be required for the operation of addition or multiplication.

The installation phase has another important aspect. It is at this stage that a secret is created, the existence of which allows the publication of fake proofs. In a system with two participants (teacher-student) this is permissible - the verifier (your teacher) creates a secret, and security is ensured until he shares the secret with you.

If you want to use some circuit publicly, that is, with more than one verifier, you must have a "trusted setup". In this case, the secret will be generated not by one person (which, incidentally, is obliged to destroy it immediately), but by a group of users. If all members of the group adhere to the rules (delete sensitive data), the security of the exchange is guaranteed [10].

3.3 How does it work?

The math underlying zk-SNARKs is hard to understand. Only a couple hundred people actually understand how this protocol works, but let's try to give analogies to understand how this system works.

Imagine that you meet someone on the street, and he claims to know your cat - she is stuck in a tree yard, and you need to urgently go with him to save her. You worry about your cat, but at the

same time you feel some kind of distrust. You need to make sure that this stranger is, in fact, a neighbor whom you can trust. Therefore, you ask questions to which he must know the answer, if you really saw your cat. Assuming you are asking the right questions, the protocol you just came up with is an example of proof of zero knowledge. You, the verifier, verify that the stranger or prover really saw your cat. You do this interactively, coming up with questions that are difficult to prepare in advance, and as much as is necessary to confirm the event. That's all. The proof of zero knowledge is when the prover convinces the verifier that he has secret knowledge without revealing this knowledge directly to the verifier.

3.4 Anonymity and Authenticity Elections

The decision-making process has always been one of the most important components of the development of any community. One form of finding an option that suits everyone is voting. It is acceptable to most people under the following basic conditions: votes must be counted impartially. Most often, uninterested parties are involved for this, or it is possible to check the correctness of the calculation on individual samples [7]. Another important characteristic of voting is the anonymity of the participants.

At first glance, it seems that these are conflicting concepts. There is some truth to this: compliance with anonymity complicates the provision of verification. This is where Zero Knowledge Proof will help us [8]. It allows you to verify the correctness of the calculation without disclosing personal information.

Conclusions

Now that online threats continue to emerge almost daily, it’s important to develop a strong and secure system, such as blockchain. Of course, the blockchain will not become a panacea, since there is no universal solution. Especially if you consider this technology from the side of personal safety.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] G. Zyskind, O. Nathan et al., Decentralizing privacy: Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, IEEE, 2015, 180–184.

[3] O. J. Onyigwang, Y. Shestak and A. Oksiuk, "Information protection of data processing center against cyber attacks," *2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP)*, Lviv, 2016, pp. 397-400. doi: 10.1109/DSMP.2016.7583586

[4] Jens Groth. “Short pairing-based non-interactive zero-knowledge arguments”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2010, pp. 321–340.

[5] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza. *Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture*. Cryptology ePrint Archive, Report 2013/879. https://eprint.iacr.org/2013/879. 2013.

[6] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. *Quadratic Span Programs and Succinct NIZKs without PCPs*. Cryptology ePrint Archive, Report 2012/215. https://eprint.iacr.org/2012/215. 2012.

[7] Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn, and Ian Miers. *Updatable and Universal Common Reference Strings with Applications to zk-SNARKs*. Cryptology ePrint Archive, Report 2018/280. https://eprint.iacr.org/2018/280. 2018.

[8] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. *Scalable, transparent, and post-quantum secure computational integrity*. Cryptology ePrint Archive, Report 2018/046. https://eprint.iacr.org/2018/046. 2018.

[9] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. *Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updateable Structured Reference Strings*. Cryptology ePrint Archive, Report 2019/099. https://eprint.iacr.org/2019/099. 2019.

[10] O. Oksiiuk, L. Tereikovska and I. Tereikovskiy, "Adaptation of the neural network model to the identification of the cyberattacks type "denial of service"," *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, 2018, pp. 502-505. doi: 10.1109/TCSET.2018.8336251