A. Beshchuk, Master student
L. Kovalchuk, PhD in Math., Prof., research advisor
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

ZK-SNARK ZERO KNOWLEDGE PROOFS: BASIC PRINCIPLES

A goal of this study is analysis of vulnerabilities of zk-SNARK type zero knowledge protocol “GRO-16” and conditions, in which those vulnerabilities are critical.

zk-SNARK stands for zero-knowledge succinct non-interactive argument of knowledge. Let us for simplicity say that it means that a person is able to prove that s/he has something without showing it to verifier. Let us look at the next example that describes the main idea of such zero-knowledge proof.

The greatest warrior Victor and the smartest wizard Peggy had their adventure, but an accident happened to Peggy. Victor asks the blind god to resurrect her, but he was answered, “I will fulfill your will, but if you prove me that there are another colors but darkness”. Victor took two apples, one is green and another is red, and gave it to the blind god and said to him, “Take these apples and hide them behind the back. Switch them or don’t and then show them to me and I will say you switched them or you didn’t”. Of course, Victor could guess, but if they do the procedure even for a ten times, then the possibility of fraud (that Victor could guess ten times in a row) would be equal to 0.00098, so they perform this ‘data exchange protocol’ for a hundred times that the blind god could be sure that there is no way Victor could just guess every time. The blind god resurrected Peggy and they continued their adventure.

So, what did we see? A person was able to prove a knowledge of something without actually showing it to verifier. This type of zero-knowledge proofs found itself the most in blockchain where a person is able to prove having a coin.

“Non-interactive” means that a verifier does not have to be “online”. A prover can just post his or her proof and then every person is able to verify that proof. That is really matters when we talk about blockchain with a big amount of users.

“Succinct” means that creation and validation of a proof are fast. However, we could achieve this only if we create something that is called as “SETUP” – a number of parameters that are known to every participants of blockchain and used to create and verify proofs of having a coin. Creation of SETUP set is the hardest and the longest part of zk-SNARK type proofs, because it requires that every user participate in its creation. In addition, SETUP set contains some secret parameters and their exposure would allow creating fake and valid proofs, so an algorithm of creation of SETUP should be strong.

The object of my research is process of protection personal data while performing transactions in the blockchain. The subject of this research is attacks on personal data protection protocol in blockchain subject to reuse setup.

The SETUP stage of zero knowledge prove protocols zk-SNARK type was considered step by step and we developed SETUP constricting algorithm. Vulnerabilities of generation setup parallelization were analyzed and five types of attack on protocol GRO-16 were developed. They are based on the human factor and

the conspiracy of several participants. In addition, strategies have been developed to protect against the attacks described in this work, both algorithmic and using third-party devices.

REFERENCES

1. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] / Satoshi Nakamoto — Access mode: https://bitcoin.org/bitcoin.pdf

2. Биткоин-миксеры топ: обзор лучших миксеров для перемешивания криптовалюты Bitcoin. Принцип работы, список сайтов, нюансы, преимущества и недостатки [Електронний ресурс] / Редакция Profinvestment.com — 2020. — Access mode: http://profinvestment.com/bitcoin-mixer/

3. Аналіз загроз при повторному використанні налаштування у snark-доведенні за протоколом GRO-16 [Електронний ресурс] / Бещук Андрій — 2020. — Access mode: https://drive.google.com/file/d/1WYvUZCFoT9YuhyBvd4Ke-Q8X4ZjJwV4G/view

4. On the Size of Pairing-based Non-interactive Argument [Електронний ресурс] / Jens Groth — 2016. — Access mode: https://ia.cr/2016/260

5. Deleting Secret Data with Public Verifiability [Електронний ресурс] / Feng Hao and Dylan Clarke and Avelino Francisco Zorzo — 2015. — Access mode: https://ia.cr/2014/364