Proceedings of the 27th International Symposium Nuclear Electronics and Computing (NEC'2019)
Budva, Becici, Montenegro, September 30 – October 4, 2019

ZERO-KNOWLEDGE PROOF IN SELF-SOVEREIGN IDENTITY

N.V. Kulabukhova[1,a]

[1] *Faculty of Applied Mathematics and Control Processes, Saint Petersburg State University, 13B Universitetskaya Emb., St Petersburg 199034, Russia*

E-mail: [a] n.kulabukhova@spbu.ru

This article provides an overview of the currently existing technologies in the field of Self-Sovereign Identity. Special attention is paid to the zero-knowledge proof and how it can be used in distributed ledgers technologies. The work shows how to make a new user anonymous, but at the same time provide him with all the features without decreasing the level of trust to him. It will be the same as if he was fully known to the system. Particular attention is paid to the ability of users to provide access to each other's resources without losing security. The algorithms of how it is done is presented.

Keywords: Self-Sovereign Identity, Zero-Knowledge Proof, Blockchain, Distributed Ledgers, IoT, Knowledge Base

Nataliia Kulabukhova

1. Introduction

The idea of building a digital passport for every person in the world is not unique, but with the growing interest and progress of distributed ledgers, a new way to solve existing problems has appeared. The concept of digital identity ((Self-Sovereign Identity, SSI)) has been around for more than 30 years [1, 2, 3, 4]. The main task of this technology is to ensure the sovereignty of a particular entity. In this case, the entity can be understood as a person, organization, IoT device, etc.On the other hand, from our point of view, many development groups are working on similar topics in parallel, but it is not yet clear what is happening inside. In order to understand the diversity of existing technologies, it was necessary to study them, compare them and identify the main pros and cons of each of them. We took into account developments with the currently existing prototypes of mobile applications: Connect.Me from Hyperledger Indy [5, 6], Jolocom Smart Wallet [7], uPort [8] and some others. In addition, we will consider the idea of using SSI not through a mobile phone application, but the very idea of a person's sovereign identity in some expert system based on zero-knowledge proof principles.

First of all, it should be said that the concept of SSI was originally based not on the blockchain, but on a certain protocol that defines the rules for the interaction of independent identification agents representing the end user with his identifier. But, as mentioned earlier, there was a question of trust, in particular, there was no way to find out whether the counterparty was compromised or not. For example, if someone can replace public keys in an agent's vault, they can make claims on behalf of the state's identity. So, at this stage, a problem with the trust store was identified.

The concept of a distributed ledger is based on a decentralized root of trust that cannot be compromised and that everyone can rely on. Obviously, with the advent of distributed ledgers, the idea arose of transferring responsibility from the centralized root of trust.

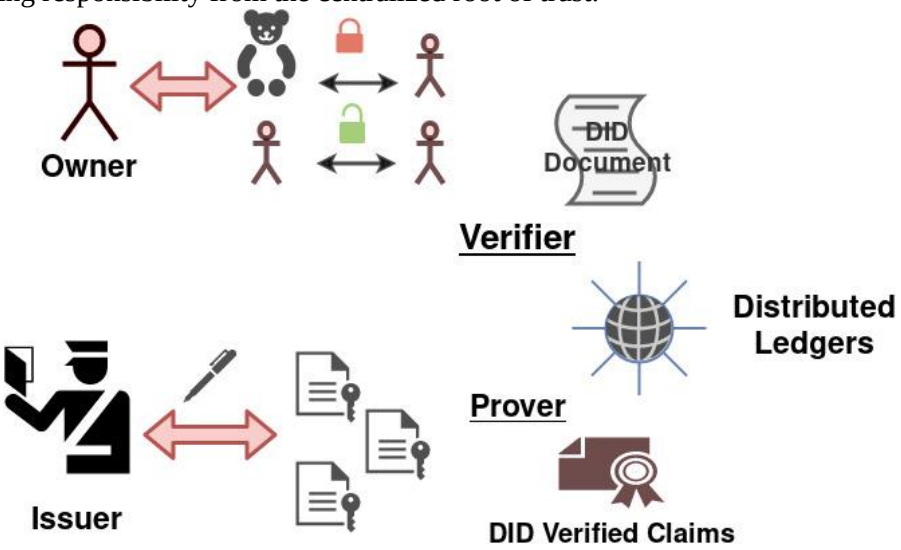


Figure 1. General scheme of DID mechanism

The second problem is to use hash tables to store and manage key pairs (public keys, private keys) of users. The fact is that they are not safe enough, although they have a lot of advantages. The developers worked on a solution for this, and as a result, the W3C community team is now working on the specification of Decentralized Identifiers (DID). The general scheme of interaction between the distributed ledger and the components of the DID concept is shown on figure 1.

2. Zero-Knowledge Proof in SSI

In the Privacy-ABC concept [9], each user can generate a secret key. However, in comparison with the traditional publice-private key pair scheme in the authentication process, in Privacy-ABC there can be many public keys for one secret, as the user wants. These public keys are called aliases. They are based on two very important functions related to privacy. Firstly, this lack of traceability, which ensures that the submission of credentials cannot be associated with their issuance. In other words, this means that, given two different aliases, it cannot be said whether they were created from the same or from different secret keys. Another major feature is non-connectivity, which ensures that the verifier cannot link various presentations of a given user. Thus, by creating different aliases for each verifier, users can be known by different unrelated aliases on different sites, but use the same secret key for authentication on all of them. In some literary sources, they are called the Issuer-non-connectivity and the verifier-non-connectivity [10, 11]. Today there are two technologies implementing Privacy-ABC concept: Identity Mixer by IBM and U-Prove by Microsoft.

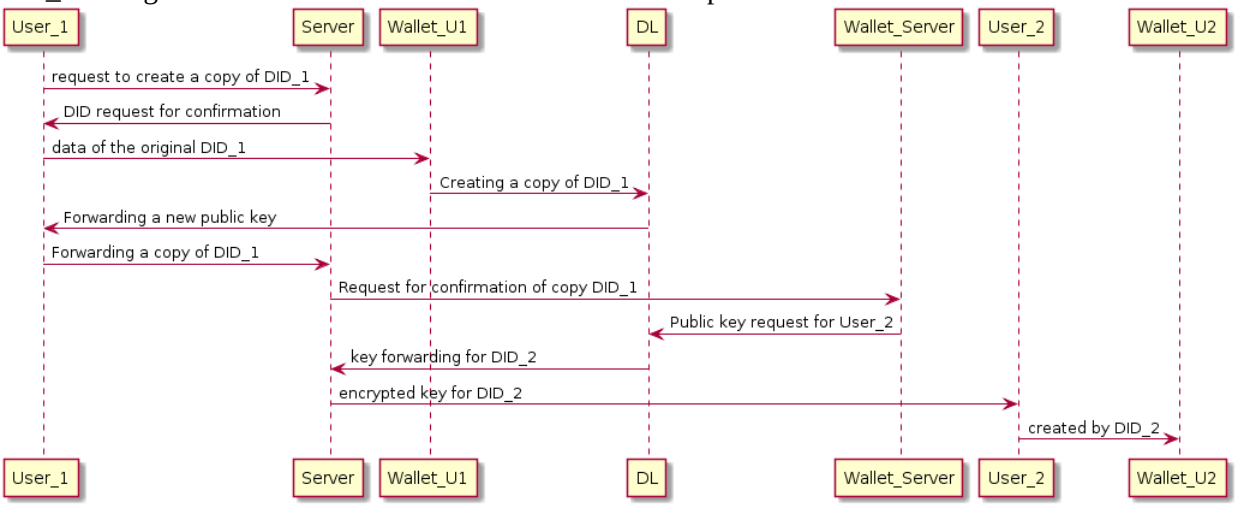
There is an independent implementation of ZKP from ZCash - ZK-SNARK [12]. This is the initial version, subsequently finalized by the ZKP implementation for anonymous user identification in distributed ZK-STARK registries [13, 14]. ZK-STARK significantly speeds up the time it takes to create records, process and verify both the verifier and the verifier. Theoretical studies indicate that ZK-STARK does not need to use high-performance computing for calculations, and it is cryptographically robust even for cracking by quantum computers [15].

Currently, the following system components are being developed on the basis of DID and ZKP technologies:

User Authentication;
User authorization;
Transfer of limited rights of one user to another;
Nested user anonymization.

The authentication protocol was described in a previous work [16].

The DIDs interaction mechanism allows you to provide limited access for one user to the resources of another. In this case, User 1 creates a new DID, which is a copy of his own verified DID_1 for a certain operation with limited functionality and transfers it to User 2. The simplest example of such a restriction can be a time period after which User 2 can no longer Use your copy of DID_1. The general mechanism of interaction in this case is presented in Scheme 1.



Scheme 1. Mechanism of providing limited access from one user to another

3. ZKP in IoT case

Quite a lot of development is now underway in applying SSI to IoT devices. On the one hand, a person has a mobile phone with an application installed with a set of DID documents, on the other hand, there is an IoT device with a built-in so-called wallet and its own verified DIDs for interaction.

In our case, we consider the logistic chain of movement of some cargo on which a smart device is connected. This device has a standard set of sensors for monitoring the state of the cargo during transportation. In addition, it is equipped with a simplified version of the mobile wallet, in which DIDs are protected, which allow to provide information about the cargo only to those who, for their part, present the same confirming DID. At the stage of cargo verification, a smart device allows you to confirm that the condition of the cargo is normal, it is not prohibited for transportation and the owner of the cargo has all the permissions. However, the device does not disclose information about what the cargo is and who its owner is. In this case, Zero-Knowledge Proof is used.

4. ZKP in knowledge base systems

The second project involves the use of a trusting environment for a number of examinations, including confirmation of the competencies of the participants in the system. This system is a knowledge base about specialists in different fields, which has the following features:

1. Find individual specialists by keywords;
2. Find groups of specialists;
3. Confirm the competencies of specialists, information about which is in the system;
3. Give an expert assessment of the work carried out by a specialist or group thereof.

In this project, ZKP is used to anonymize expert reviews (Fig. 2). But if we already have a confirmed DID that contains information that the user of the system has the right to leave feedback on the expert's work, then the system can trust the accuracy of the data received from this user.

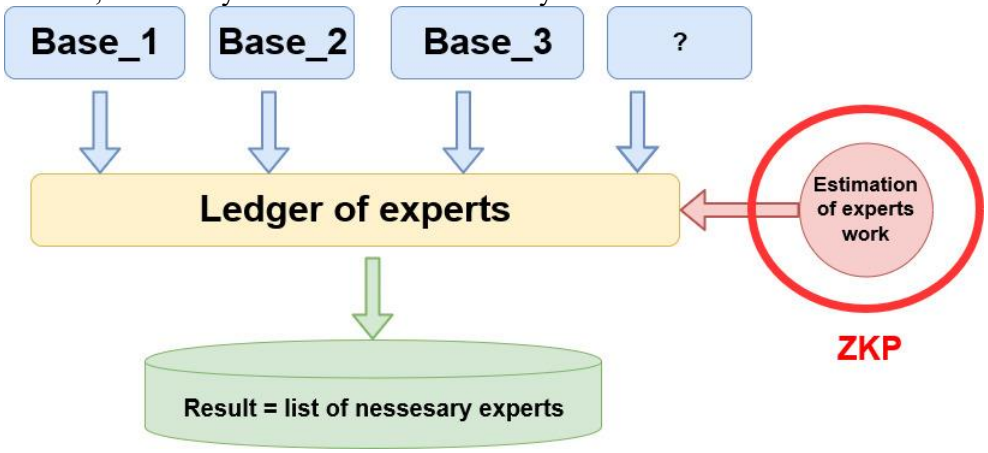


Figure 2. The scheme of the knowledge base of the expert system

4. Conclusion

In the future, it is planned to conduct tests of the interaction schemes presented in the work. Since there are currently no sources of information on how to use DID if we do not have a wallet deployed on a mobile device. Is it possible to deploy an analogue of such a wallet in the system to confirm the reliability of user data. The study of all these issues is planned at the next stages of system development.

5. Acknowledgement

The author wants to thank Vladimir Korkhov and Oleg Yakushkin for constructive criticism and useful advice during the development of the concept for this project.

References

[1] Jan Camenisch, Maria Dubovitskaya, Anja Lehmann, Gregory Neven, Christian Paquin, and Franz-Stefan Preiss, Concepts and Languages for Privacy-Preserving Attribute-Based Authentication, 2013

[2] Kai Wagner, Balázs Némethi, Elizabeth Renieris, Philipp Lang, Elliott Brunet, Eric Holst, Self-sovereign Identity. A position paper on blockchain enabled identity and the road ahead, 2018, p.57

[3] Kai Rannenberg, Jan Camenisch, Ahmad Sabouri, Attribute-based Credentials for Trust, Springer International Publishing, 2015, p.395

[4] Camenisch, J., Dubovitskaya, M., Lehmann, A., Neven, G., Paquin, C., Preiss,F.-S.: Concepts and languages for privacy-preserving attribute-based authentication. In: Fischer-H¨ubner, S., de Leeuw, E., Mitchell, C. (eds.) IDMAN 2013. IAICT,vol. 396, pp. 34–52. Springer, Heidelberg (2013).https://doi.org/10.1007/978-3-642-37282-74

[5] https://try.connect.me/

[6] https://github.com/hyperledger/indy-plenum/

[7] https://www.uport.me

[8] https://jolocom.io/

[9] Ernie Brickell, Jan Camenisch, Liqun Chen, Direct Anonymous Attestation, 2004, p.24

[10] Jan Camenisch, Manu Drijvers, and Anja Lehmann, Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited, 2016, p.65

[11] Christina Garman, Matthew Green, Ian Miers, Decentralized Anonymous Credentials, 2013, p.21

[12] https://medium.com/coinmonks/introduction-to-zero-knowledge-proofs-8e8261b4a48a

[13] https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b

[14] https://coincentral.com/zk-starks/

[15] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev, Scalable, transparent, and post-quantum secure computational integrity, ZK-STARK White Paper, March 6, 2018, https://eprint.iacr.org/2018/046.pdf