KUNGLIGA TEKNISKA HÖGSKOLAN, RESEARCH METHODOLOGIES

Project Plan

Identity Management in Blockchain

Riccardo Sibani
riccardo.sibani@gmail.com

Filippo Boiani
filippo.boiani2@gmail.com

October 4, 2017

1 ALLOCATION OF REPONSIBILITIES

Riccardo Sibani is in charge of: writing the first draft; composing the structure of the paper; setting the research questions and hypotheses and explaining the employed method.

Filippo Boiani is in charge of writing the first sections including introduction and background. The latter will be explained in terms of theoretical framework and literature study.

Both are working on the final version of the report as well as the project development and the evaluation. The evaluation will present the results and further discussion.

2 ORGANIZATION

The project will be organized as a two-person project, building upon previously develop solution at TU Berlin. Once the theoretical process is defined and the implementation ready, there will be an evaluation work.

3 Background

This project is based on another project regarding identity management [4] [2], developed at TU Berlin in collaboration with Deutsche Telekom. This domain *independent ID management architecture*, meant for Distributed Online Social Networks (DOSN) [1], is based on an open source, distributed directory system called *GSLS* (Global Social Lookup System) [2]. The GSLS executes a single task: mapping a GlobalID to the corresponding user's social profile.

4 Problem statement

The aim of the project is to build a blockchain-based, distributed system for self-asserted identities between DOSN [6] by modifying the current GSLS implementation. In order to do so, it is necessary to investigate different possible approaches – mainly storage and validation systems – taking advantage of the secutiry privided by blockchain [7].

In other words, the project investigats the possibility to improve the identity management system implemented by Sebastian Göndör et al.[2]. This system relies on a distributed hash table (DHT) to map the GlobalIDs to the corresponding user data. However, there are different security issues with this implementation; for example, someone can spawn a malicious node in the DHT network containing data signed by the user (validated) but outdated. This uncorrect data can override the correct one.

In the current implementation, data is checked against the user's public key and it is considered valid if the signature is correct, but the system cannot be sure wether the data is the most recent. We want to overcome this and other problems by exploiting the security, provided by the blockchain.

5 Problem

Keeping secure and consitent is of paramount importance for many systems. It is even more important for the GSLS since it handles personal data. The DHT implementation alone is no longer enough to meet the security requirements. In this particular case, the blockchain consensus and its timestamps can be employed to provide the additional security that is needed.

6 Hypothesis

With certain blockchain implementations, it is possible to create a transactions [8] on one device, sign them with a private key, and, either send them directly to the network of blockchain nodes or to a service that does this on the user's behalf.

Since a transaction is nothing but a modification of the state in the blockchain, the aformentioned solution can be employed to solve some of the security issues of the GSLS. There are different ways to achieve transactions based on cold wallets [3] [5] and we will probably focus on this type of solution.

7 Purpose

Research the state of the art regarding identity management and blockchains. Conceptualize and design a service to manage self-asserted identities in a blockchain starting from the current GSLS implementation. The aim is to increase the level of security of the users who want to have the possibility to move their profiles from one social network to another.

8 Goal

Briefly illustrate the main security flaws of the current GSLS implementation. After having done that, we illustrate some of the frameworks that can be employed to solve these issues. Then, we describe the implemented solution and the evaluation in terms of security and performance. The final outcome should be a qualitative analysis of the implemented identity management system based on blockchain.

9 Tasks

Investigate different implementations of the GSLS: the system is composed of a client side and a number of servers connected to one another through the blockchain network.
The implementation of a vaible and effective solution needs to be investigates by the team. The priority is to guarantee that the solution will be not invasive for the users. This is done in order to reach the majority of the people registered on federated social networks.
Analyze the security of the proposed solution, the advantages and the disadvantages of such a system.

10 METHOD

The project will use the analytic method since it must follow the GSLS and the selected blockchain specifications in order to create a reliable and consistent transaction. The transaction should be created and sent without loss of data impact on the users' device as well as be safe and secure.

11 MILESTONE CHART

The project development part started on Saturday the 16th of September with the literature and general industry study.

13 October: with on the studies carried out over the past month, we have assessed solutions in terms of: security and performances. Each solution should be based on existing frameworks and blockchain implementations.

25 October: define the final approach and start designing the system. The introduction part of the report should be written and reviewed.

15 November: a basic implementation ready to be tested. The tests are meant to find implementation flaws.

25 November: perform the evaluation in terms of scalability of the server, transaction costs and response times. If part of the solution is based on smart contracts: could they scale to a large number of entries? What is the response time? The evaluation will lead to a discussion about drawbacks and possible trade-offs.

15 December: the report is written and ready for proof read.

30 December: submit the report.

REFERENCES

[1] Sebastian Göndör and Hussam Hebbo. "SONIC: Towards seamless interaction in heterogeneous distributed OSN ecosystems". In: *Wireless and Mobile Computing, Networking*

and Communications (WiMob), 2014 IEEE 10th International Conference on. IEEE. 2014, pp. 407–412.

[2] Sebastian Göndör et al. "Distributed and Domain-Independent Identity Management for User Profiles in the SONIC Online Social Network Federation". In: *International Conference on Computational Social Networks*. Springer International Publishing. 2016, pp. 226–238.

[3] *Icebox: lightwallet-powered cold storage solution*. 2017. URL: https://github.com/ConsenSys/icebox.

[4] Spencer C. Lee. *Introduction to Identity Mangement*. 2003. URL: https://www.sans.org/reading-room/whitepapers/authentication/introduction-identity-management-852.

[5] *Lightwallet: lightweight JS Wallet for Node and the browser*. 2017. URL: https://github.com/ConsenSys/eth-lightwallet.

[6] Elena Mesropyan. *Blockchain for Identity Management*. 13-2-2017. URL: https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/.

[7] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2008.

[8] Gavin Wood. *A Next-Generation Smart Contract and Decentralized Application Platform*. 2014. URL: https://github.com/ethereum/wiki/wiki/White-Paper.