KUNGLIGA TEKNISKA HÖGSKOLAN, RESEARCH METHODOLOGIES

Project Plan

Title:
Identity Management In The Blockchain

Riccardo Sibani
email: riccardo.sibani@gmail.com

Filippo Boiani
email: filippo.boiani2@gmail.com

October 3, 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 held accountable of the final version of the paper as well as the project development and the evaluation part. The evaluation part will consists of results presentation and further discussions.

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, distributes directory system called *GSLS* (Global Social Lookup System) [2]. The GSLS executes a single task: mapping a GlobalID to to corresponding user's social profile.

4 Problem statement

The aim of our 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 wants to investigate the possibility to improve the identity management system implemented by Sebastian Göndör et al.[2]. This system relies on a distributed hash table 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someone can spawn a malicious node in the DHT network containing validated - meaning signed by the real user - but outdated data that can override the correct ones without leaving any trace.

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 if this data is the most recent one. We want to overcome this and other problems by exploiting the security provided by the blockchain.

5 Problem

Keeping security and consistency of data is of paramount importance for every system. It is even more important for the GSLS in that it handles personal user's data. The distributed hash table 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 aforementioned solution can be employed to solve some of the security issues of the GSLS. There are at least a couple of different ways to achieve transactions based on cold walles [3] [5] and we will probably stress more on this type of solutions.

7 Purpose

The purpose is to: first research the state of the art regarding to identity management and blockchains; then conceptualize and design a service to manage self-asserted identities in a blockchain. The serivice derives and evolves from the current GSLS implementation. The final 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

The aim is to briefly illustrate the main security flaws of the current GSLS implementation. After having done that, we want illustrate some of the frameworks, systems that can be employed to solve the issues. Then, we want to describe the solution we decided to implement along with its evaluation in terms of security and performances. 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.

Then an implementation part is needed where the team develop a viable solution demonstrating its effectiveness.
It is priority of the task and the team to guarantee that the solution will be as less invasive as possible to the users in order to reach the majority of the people registered on social networks.
Finally an evaluation part is needed: analyzing 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 respect 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 and impacting on the users' device as less as possible 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: basing on the studies carried out over the past month, we should have assessed different possible solutions in terms of security and performances. Each and every 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 working system is implemented and ready to be tested. The test 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, can they scale to a large number of entries? How is the response time? The evaluation will lead us to some discussion about drawbacks and possible trade-offs.

15 December: the paper is written and ready for proof of 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`.