KUNGLIGA TEKNISKA HÖGSKOLAN, RESEARCH METHODOLOGIES

Project Plan

Title:
Ethereum offline transaction

Riccardo Sibani
email: riccardo.sibani@gmail.com

Filippo Boiani
email: filippo.boiani2@gmail.com

September 19, 2017

1 ALLOCATION OF REPONSIBILITIES

Riccardo Sibani is in charge of writing the first draft, composing the structure of the paper and explaining the process, demonstrating on a theoretical basis how to achieve the offline transaction.
Filippo Boiani is in charge of developing the script in order to test the presented assumptions as well as testing the performance and developing the suggested solution.

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 paper is based on a project for TU Berlin in collaboration with Deutsche Telekom regarding identity management through blockchain. The offline solution was developed in order to give the users the possibility to update their social records (stored into the Ethereum public blockchain) without the constraint of downloading the entire blockchain node or use a third party node (which can be malicius and steal the blockchain credentials).

4 PROBLEM STATEMENT

The project wants to investigate the possibility to create and sign an Ethereum transaction offline and then upload it through a different device or medium, increasing the security of the wallet.

5 PROBLEM

Access to the network in extreme situations or among poor communities is not always possible. The cryptocurrencies are becoming one of the main tool for exchange assets in part of the world where there is not a legitimate government, a weak bank sistem or simply illegal markets.
In this situation access to network is not always possible or simply the player are not able to host an entire blockchain node.

Another part of the population instead, might be required to make a transaction to proceed with a payment or to transfer the property of an asset (as is happening in Sweden, India and so on [**references**]).

6 HYPOTHESIS

It is possible to create a transaction on one computer or any sort of computational device, sign it and be able to transfer it in a serializable way to another device.

The security and the integrity of the transaction must be prevented, preserving it from malicius attacks or lost of information.

7 PURPOSE

The purpose is to present a new approach in order to create a transaction whenever the conditions are contrary or simply the creator of the signature do not want to host the entire ethereum node.

8 GOAL(S)

The aim is to create a transaction where the creator is offline, guaranteeing the same level of security as if with cold wallet (no third party to participate in the transaction) but without the constraint of hosting the blockchain node or any plugin requiring an high amount of bandwidth.

9 TASKS

Write a simple client server code able to join an Ethereum contract and make transactions. The server must be able to receive the transaction via http or another protocol of choice and upload it in its local node.
Then an evaluation part is needed; where a certain amount of transactions will be run altogether both in the standard approach following the hot wallet procedure (which allows the user not to host the blockchain node) and the new suggested approach.

10 METHOD

The project will use the analytic method since it must respect the Ethereum specifications in order to create a reliable signed transaction without loss of data and that will be consistant once is sent to the uploader server through any kind of protocol.

11 MILESTONE CHART

The project has been started on Saturday the 16th of September with the code implementation.

30 September: have a general understanding regarding how the transaction is built nad start the implementation of it. At the same time keep track of what has been learned while writing the paper.

30 October: Evaluate the solution in a system according to the modalities described in Task section.

30 November: the paper has been written and ready for proof of read.

30 December: submit the report.

12 REFERENCES