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 20, 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 [2]) 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. With offline transaction, we intend a transaction created from a device which has no local access to the public blockchain.

5 PROBLEM

Access to the network in extreme situations or within 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 one of the party the value exchange is not able to host an entire blockchain node.

In some other cases, it might be required to make a blockchain transaction in order to transfer some monetary value (i.e. payments) or the property of an asset (as it is happening in countries like Sweden and India [1]).

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 assured, preserving it from malicious attacks or loss of information.

7 PURPOSE

The purpose of the proposed project is to present a new approach that aims at creating a transaction whenever the conditions are adverse or simply the creator of the signature does not want to host the entire ethereum blockchain node.

8 GOAL(S)

The aim is to create a transaction where the creator is partially, if not completely, offline, guaranteeing the same level of security provided by cold wallets (no third party participating in the transaction). We achieve this without the constraint of holding a blockchain node or any piece of software/plugin that requires an high amount of bandwidth.

9 TASKS

Write a simple client server system able to join an Ethereum contract and make transactions. The server holds a blockchain node and it must be able to receive a singed transaction via HTTP (or any another protocol of choice) and send it to the blockchain network. The client is held accountable for creating a transaction and signing it.
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 and consistent signed transaction. The transaction should be created and sent without loss of data..

11 MILESTONE CHART

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

30 September: have a general understanding regarding how the ehtereum transaction is built and start its implementation. 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 description provided in the Task section.

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

30 December: submit the report.

REFERENCES

[1] Joon Ian Wong. *Sweden's blockchain-powered land registry is inching towards realityprovi*. 2017. URL: https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/ (visited on 09/20/2017).

[2] Gavin Wood. *A Next-Generation Smart Contract and Decentralized Application Platform*. 2014. URL: https://github.com/ethereum/wiki/wiki/White-Paper (visited on 09/20/2017).