Master's Thesis: Usability of payment channels wallets

March 28, 2018

Cryptocurrencies such as Bitcoin or Ethereum face scalability issues in order to achieve mainstream adoption. Proof of work Blockchain can hardly scale beyond the 100 transactions per second without scarifying security[1]. In the recent times Off-chain scaling solution were proposed. Examples are the Lightning network[2] for Bitcoin or the Raiden network[3] for Ethereum. These solutions consist in not broadcasting all transactions to the Blockchain but instead to settle the resulting balance every once in a while. It requires to open a payment channel between the 2 parties wanting to transact. This is done by depositing a collateral in a smart contract to secure their future off-chain transactions. Payment channels face usability issues. First the parties need to be online and actively exchange messages to make a transaction. Moreover they need to monitor the Blockchain and be ready to react if the other party attempt a fraud. A first goal of this thesis will be to investigate payment channel to see if there is a possibility to reduce this online presence. The next step will be to develop an experimental wallet application for smartphone supporting secure off-chain transactions. It will need a process running in the background monitoring the Blockchain and ready to accept transactions.

References

[1] Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H. and Capkun, S., 2016, October. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 3-16). ACM.

[2] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2015.

[3] Raiden network. http://raiden.network/