The University of Sydney

School of Information Technology

INFO5993 Research Methods - Assignment II

Outline of Research Deploy Unforkable Blochain with Zero Knowledge Contingent Proof on Mobile Devices

---

Author:
Lin Han

Supervisor:
Dr. Vincent Gramoli

October 15, 2017

1 Introduction & Motivation

With the dramatical popularity of cryptocurrencies all over the world, people give more concerns on the security and performance issues on blockchain technology. While several forms of blockchain are proven to be secured under most circumstances, possible attacks still arises. Gaps exists where newly developed unforkable blockchain and real-life application overlap. Deployment of unforkable blockchain enables the possibility to integrate the secured distributed system into trustless transactions. The *Zero Knowledge Contingent Payments*, known as ZKCP, which enables a trustless transaction where neither payer or payee can cheat, is also another supplements to enhance the security of blockchain. Hence, its is of vital importance to explore to deploy unforkable blockchain onto mobile so that an evidence could be made to show a more reliable and efficient way to replace current cryptocurrencies' blockchain technology.

2 Contributions

In this project, the aim is to explore how the unforkable blockchain, especially the Red Belly Blockchain in this case, can be deployed on mobile devices and whether Zero Knowledge Contingent Payments can be integrated into it without the support of scripting language.

First of all, I will implement a Java version of client for the Red Belly Blockchain and to test the performance of it. After that, an Android version of client will be implemented which plays the role of a client with full functionalities including showing balance and history, proposing transaction, and multiple-servers connection. Further, a discussion and exploration on ZKCP on the Red Belly Blockchain will be given, the performance, namely the speed of transaction, will be measured.

3 Methodology

I intend to further implement the existing code base of Red Belly Blockchain to fully interact with remote procedural call. In particular, it should be able to establish secured chanel between the Golang server and Java/Android client.

Then a full implementation of client in Java and Android will be written. The client should have functions including showing balance, showing history, and proposing transactions. I will also make the client to allow dynamic settings including servers/DNS servers addresses, account import, encryption.

At the end, after the client is implemented and tested to be compatible with Red Belly Blockchain, I intend to explore the possibility of Zero Knowledge Contingent Payments without scripting language. The speed of transaction will be given if the attempt succeeds.

4 Conclusion

Unforkable blockchain has given enough theoretical proof on the advances in security and performance compared to the traditional blockchain technology. With the possibility of deploying it on mobile with ZKCP enabled, people could easily make trustless transactions even without third-party involved in.