ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

Make Bitcoin Exchanges Truly Transparent

A major contribution of the success that Bitcoin is having today has to be attributed to the emergence of Bitcoin exchanges. A Bitcoin exchange is a platform that facilitates buying and selling bitcoins for fiat money like US dollars. This enables a larger public to come in contact with bitcoins, increasing their value as a means to pay for goods and services. Exchanges also provide the ground truth for the value of bitcoins by publishing their trade book and allowing market dynamics to find a price for the traded bitcoins. Finally, much of the media attention focuses on the rapid gain in value that these services have enabled.

In contrast to Bitcoin's decentralized and transparent nature, exchanges are centralized and opaque. Over time several exchanges have been accused of reinvesting the holdings of their users, maximizing their income while exposing their users to risks they did not sign off. The recent failure of MtGox, and consequent loss of 500 million USD, would likely have been detectable and preventable if MtGox had performed regular audits on their assets.

At all times an exchange should be able to pay out all of its user's holdings. In order to guarantee that they have the required liquidity, some exchanges started having regular audits by trusted auditors, which compare the exchange's assets with the sum of its user's holdings. These audits are extremely expensive, can be performed only rarely and require auditors trusted by the community. We believe we can do better by creating an audit system that performs the auditor's tasks at a fraction of its time and its costs.

The goal of this thesis is to build an audit system that takes the exchange's assets and user accounts, producing a proof that the user holdings are covered by the assets, without revealing the assets and the user account details to the general public.

Requirements: Good programming skills. Some basic knowledge about Trusted Platform Modules (TPM) is advantageous.

Interested? Please contact us for more details!

Contacts

- Christian Decker: cdecker@tik.ee.ethz.ch, ETZ G64.2
- Jochen Seidel: seidelj@tik.ee.ethz.ch, ETZ G61.1