NUMMULARIUS:

Cryptocurrency Exchange with Trusted Computing

Recently, a new wave of insider exploits and a lack of transparency captured the world of centralized exchanges.

Is it possible to achieve transparency at centralized exchange, where the funds are in the hands of code and not the operator?

01 PURPOSE

This work aims to propose and implement a proof-of-concept of exchange using trusted computing, especially the Intel SGX enclaves.

The focus is on exchange security, non-equivocation, and secure management of the private keys.

AUTHORS

Bc. Tomáš Sasák (xsasak01@vutbr.cz)

Ing. Ivan Homoliak Ph.D (Supervisor)

02 METHODOLOGY

Exchange maintains its ledger stored in a history tree, where every single node is an exchange microblock.

A microblock contains the exchange microtransactions, such as bidding, depositing, or withdrawing of coins.

Using the history tree as a ledger, the exchange can provide signed incremental proof, that the selected microblock precedes the exchange's latest microblock.

All of this is happening inside the Intel SGX enclave out of the exchange operator's reach.

Smart contract on public blockchain stores the ledger root hash and serves as undisputable proof of the ledger state and history.

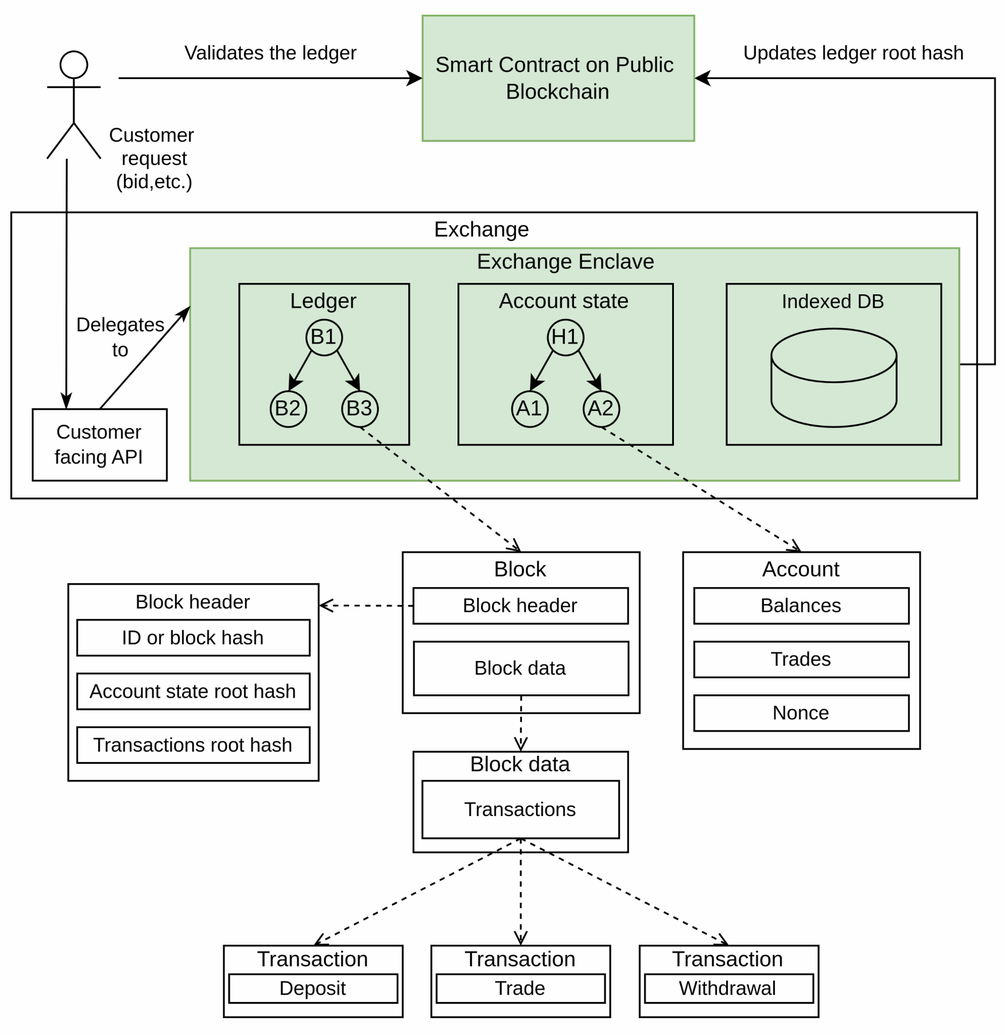

Figure 1: The exchange desing, green are trusted secure components.

03 RESULTS

With the use of PostgreSQL as our indexing database, exchange scales well with an increasing number of accounts.

Problems appear with multiple concurrent requests, as the account state (Merkle-Patricia tree) cannot be updated in parallel.

Implementation achieved **35 deposits per second** and **23 bids per second for a single coin-pair**.

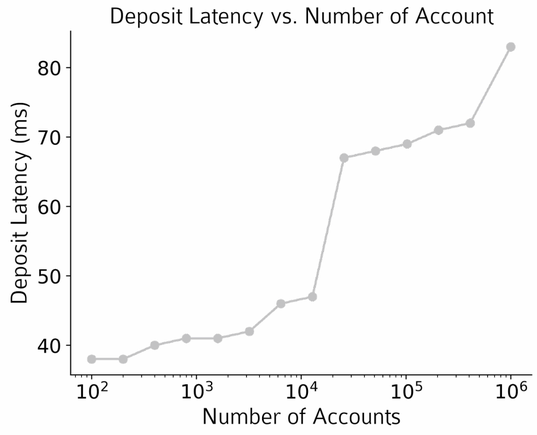

Figure 2: Latency of single deposit requests compared to the number of existing accounts.

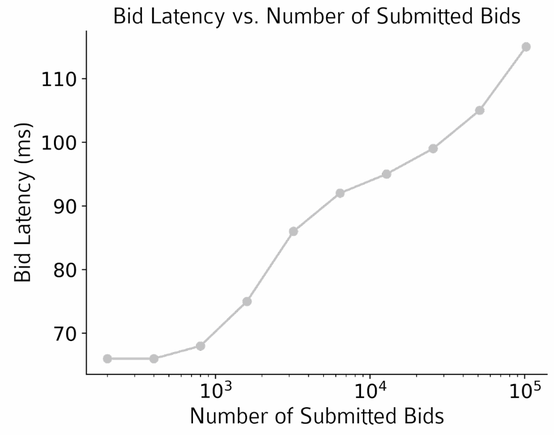

Figure 3: Latency of a single bid resolution compared to the number of available bids.

Excel@FIT 2023

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY