FROSTDAO: Collective management of wealth using FROST

Rahim Klabér
30/08/2023

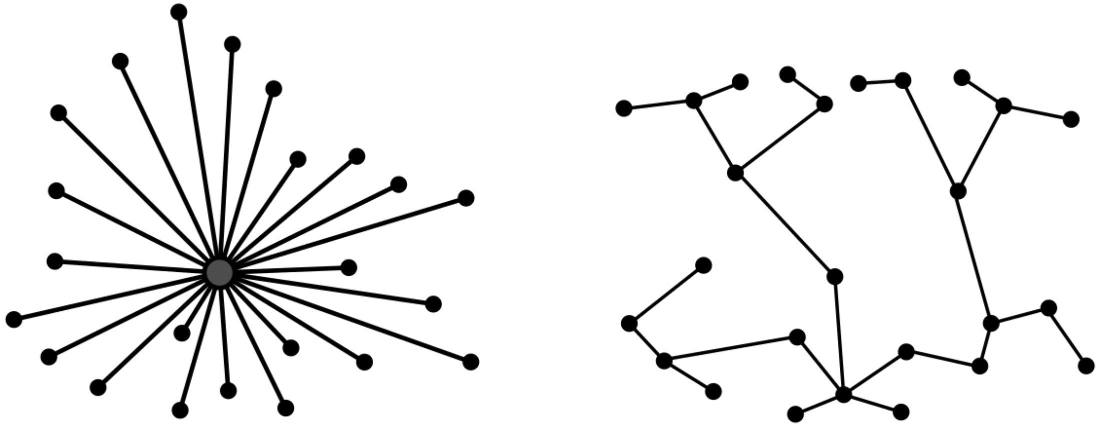
TUDelft

Structure

- Background
- Problem Statement
- FrostDAO Design & Implementation
- Experiments

Blockchain

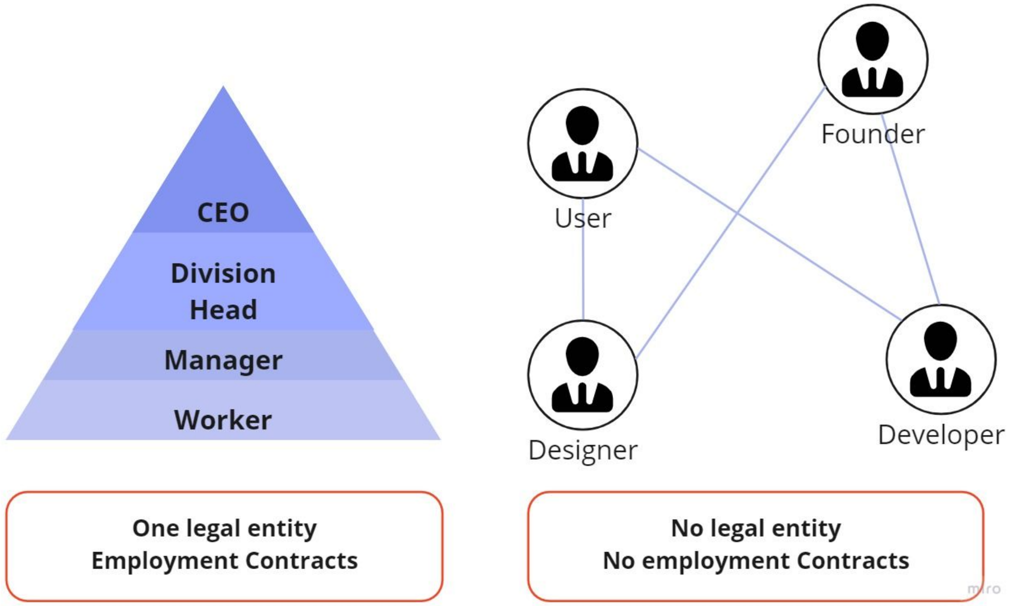
- Enables decentralized financial services.
- No central party or government.
- Anyone can participate.
- Based on public-key cryptography.



CENTRALIZED DECENTRALIZED

DAO: Decentralized Autonomous Organization

- Blockchain-based organization using smart-contracts to operate without central control.
- Actions can be proposed, which are executed using smart-contracts and Blockchain.



One legal entity
Employment Contracts

No legal entity
No employment Contracts

DAO: Decentralized Autonomous Organization

Example: The LAO

“The LAO allows Members to pool capital, invest in projects, and share in any proceeds from the investment.”

Problem Statement

Our goal is to enable a leaderless group of collaborating humans to control a Bitcoin wallet of unconstrained wealth democratically.

Naive solution: use Bitcoin Script multisig

- Scripts that decide how Bitcoins can be spent.
- A **locking** script specifies the spending condition.
- An **unlocking** script contains the inputs for the unlocking script.
- Multisig allows **n** individuals to jointly control a Bitcoin account.
- Only **m** participants, with **m ≤ n**, are required to spend funds.

locking: <m> <pubkey...> <n> OP_CHECKMULTISIG

unlocking: <signature...>

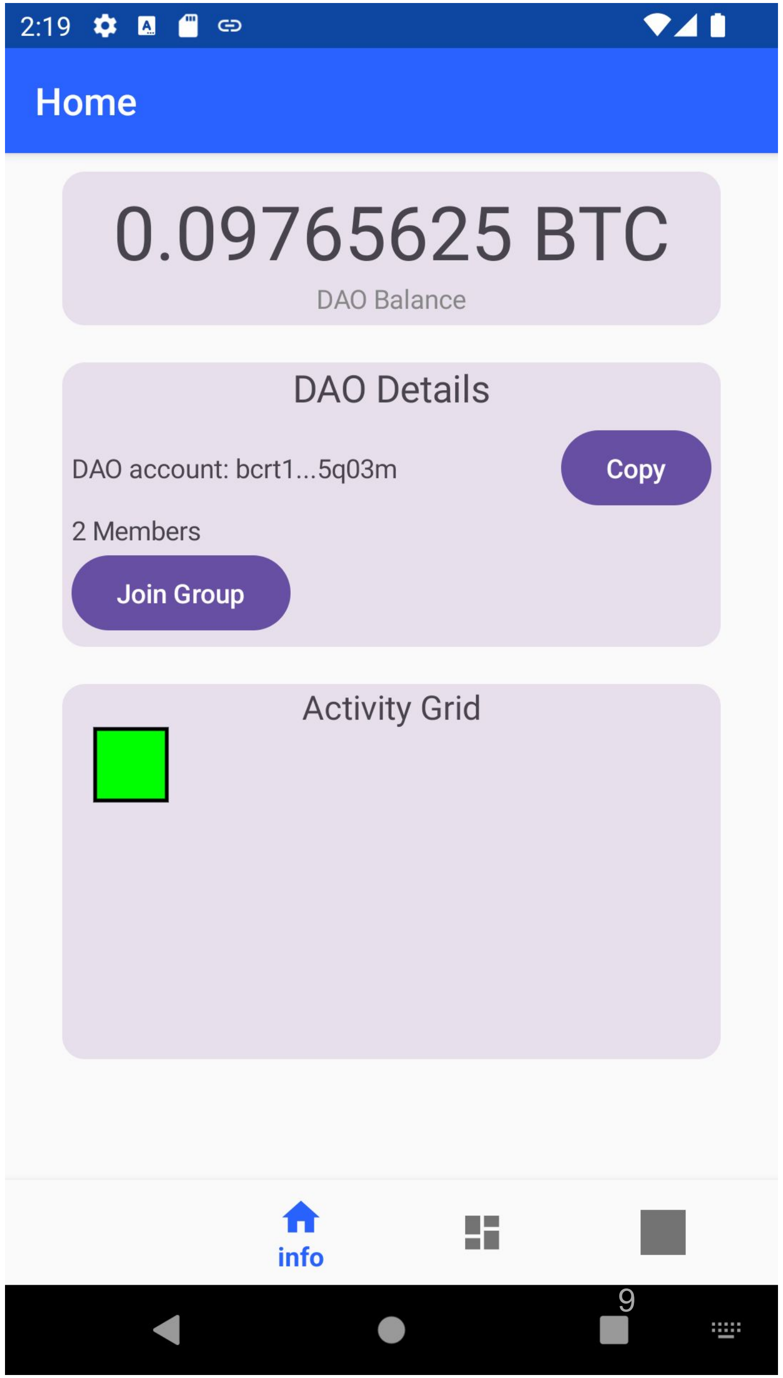
Naive solution: use Bitcoin Script multisig

Disadvantages

- Low scalability
- High transaction costs

FROSTDAO

- Shared Bitcoin wallet using cryptography (FROST)
- Peer-2-peer network using IPv8
- Create and join group
- Vote on which actions to take
  - Requires a majority
- Open-source code



2:19

Home

0.09765625 BTC

DAO Balance

DAO Details

DAO account: bcrt1...5q03m

2 Members

Activity Grid

Shared Bitcoin Wallet using FROST

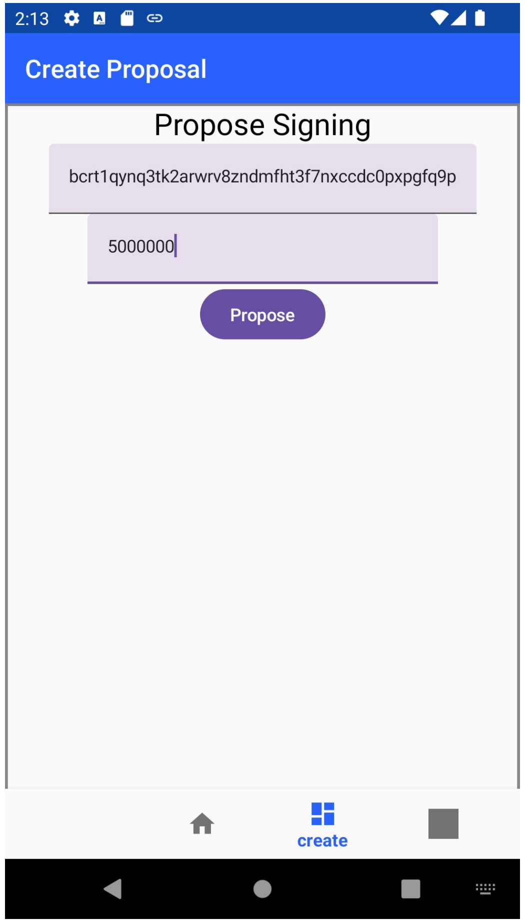
- FROST → flexible round-optimized Schnorr threshold signatures
- Same idea as multisig, but using cryptography and not limited by transaction size
    - **n** participants jointly control a key pair. **t** participants, where **t ≤ n**, can work together to create a valid signature.
- Indistinguishable from normal Bitcoin transactions
- Consists of two interactive protocols: signing and key generation

Shared Bitcoin Wallet using FROST

Limitations

- Key generation is required every time someone leaves or joins.
- “Off-chain” computation
-

Spending funds



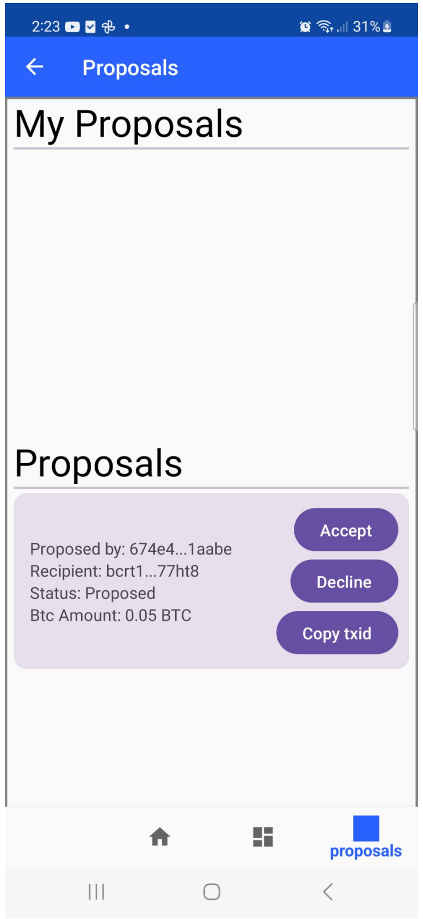
2:13

Create Proposal

Propose Signing

bcrt1qynq3tk2arwrv8zndmfht3f7nxccdc0pxpgfq9p

5000000



2:23

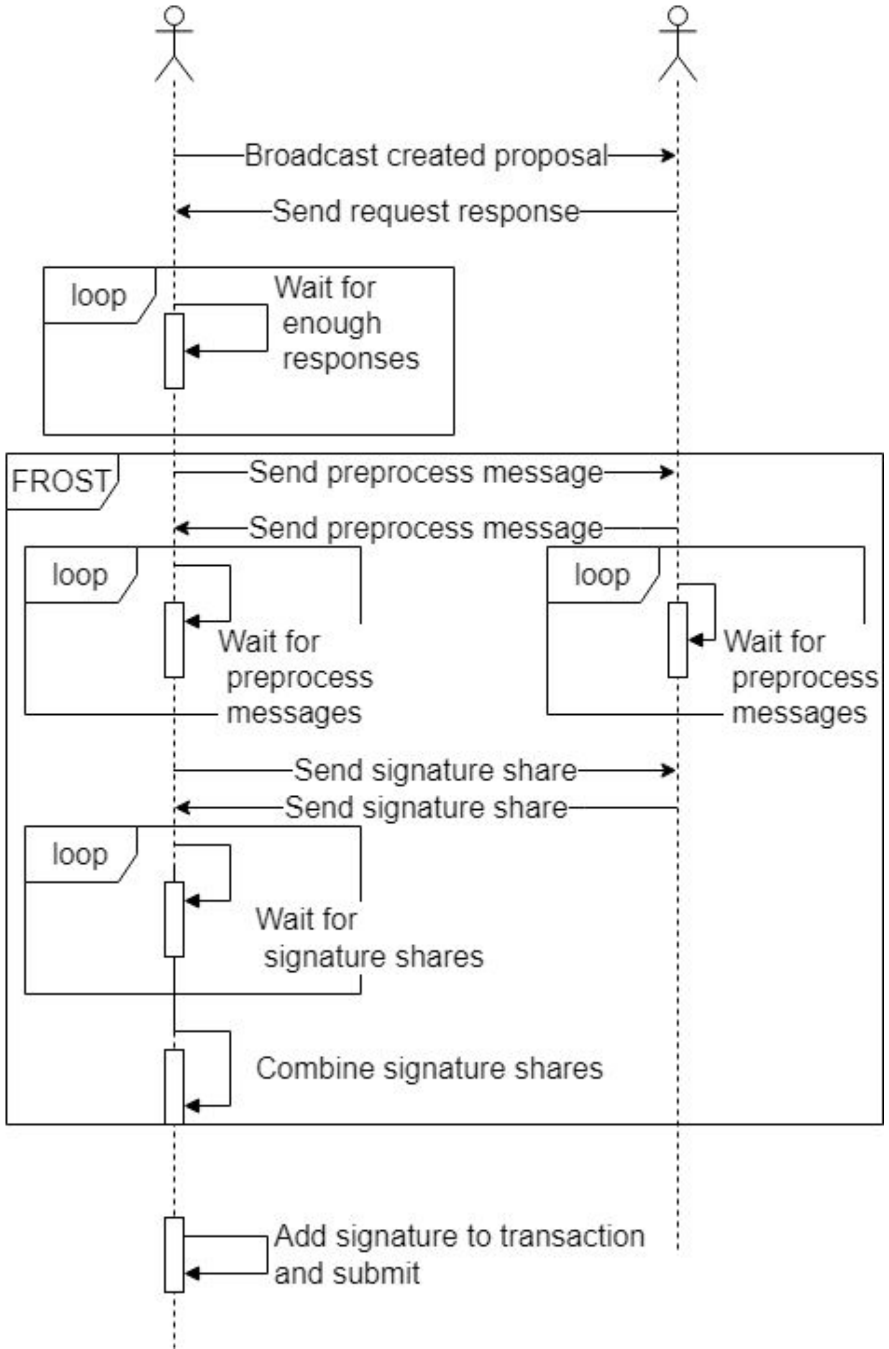
Proposals

My Proposals

Proposals

Proposed by: 674e4...1aabe
Recipient: bcrt1...77ht8
Status: Proposed
Btc Amount: 0.05 BTC

Spending funds

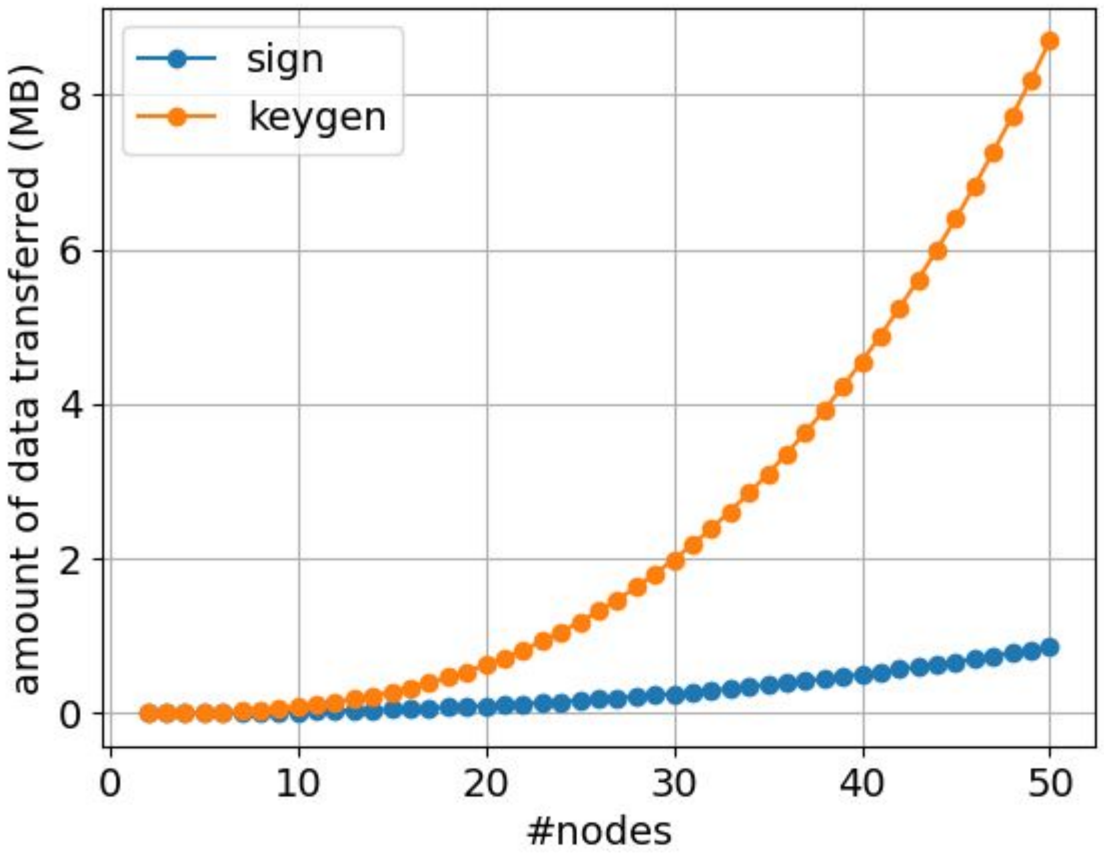

Broadcast created proposal
Send request response
loop
Wait for enough responses
FROST
Send preprocess message
Send preprocess message
loop
Wait for preprocess messages
loop
Wait for preprocess messages
Send signature share
Send signature share
loop
Wait for signature shares
Combine signature shares
Add signature to transaction and submit

Evaluation

- Performance evaluation of key generation and signing.
- PC experiments for large amount of participants
    - Limited to 50 participants due to IPv8 issues
- Android experiments to determine effects of Android.

Amount of data transferred

- Cubic vs quadratic scaling

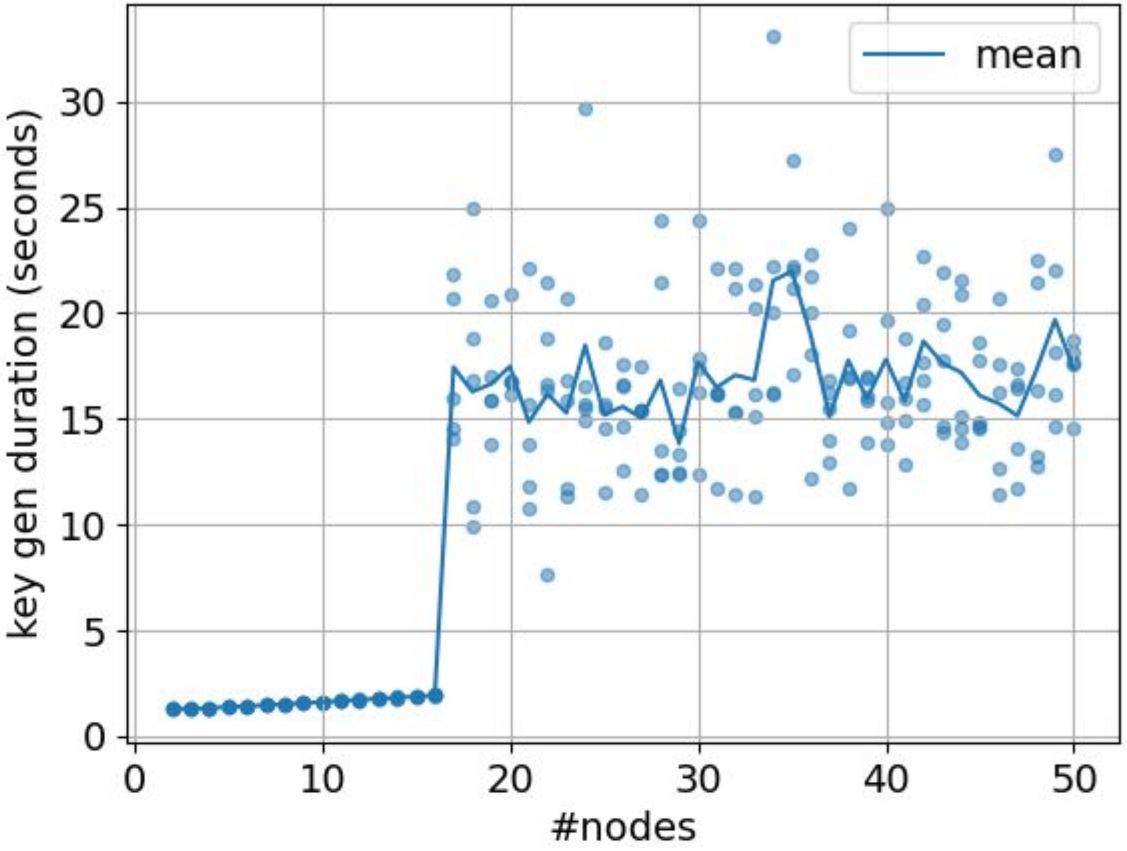


TU Delft

Key generation duration

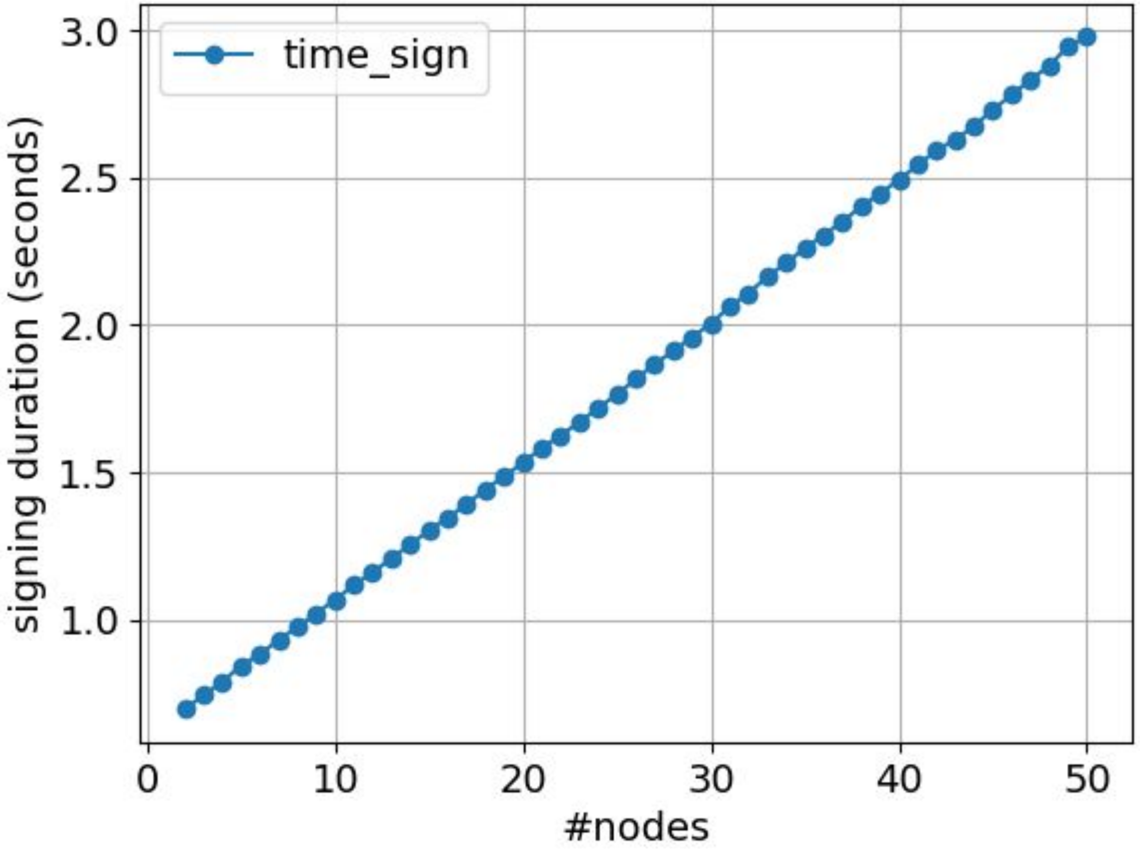
Low performance due to

- IPv8’s data transfer protocol EVA
- Large amount of data



Signing duration

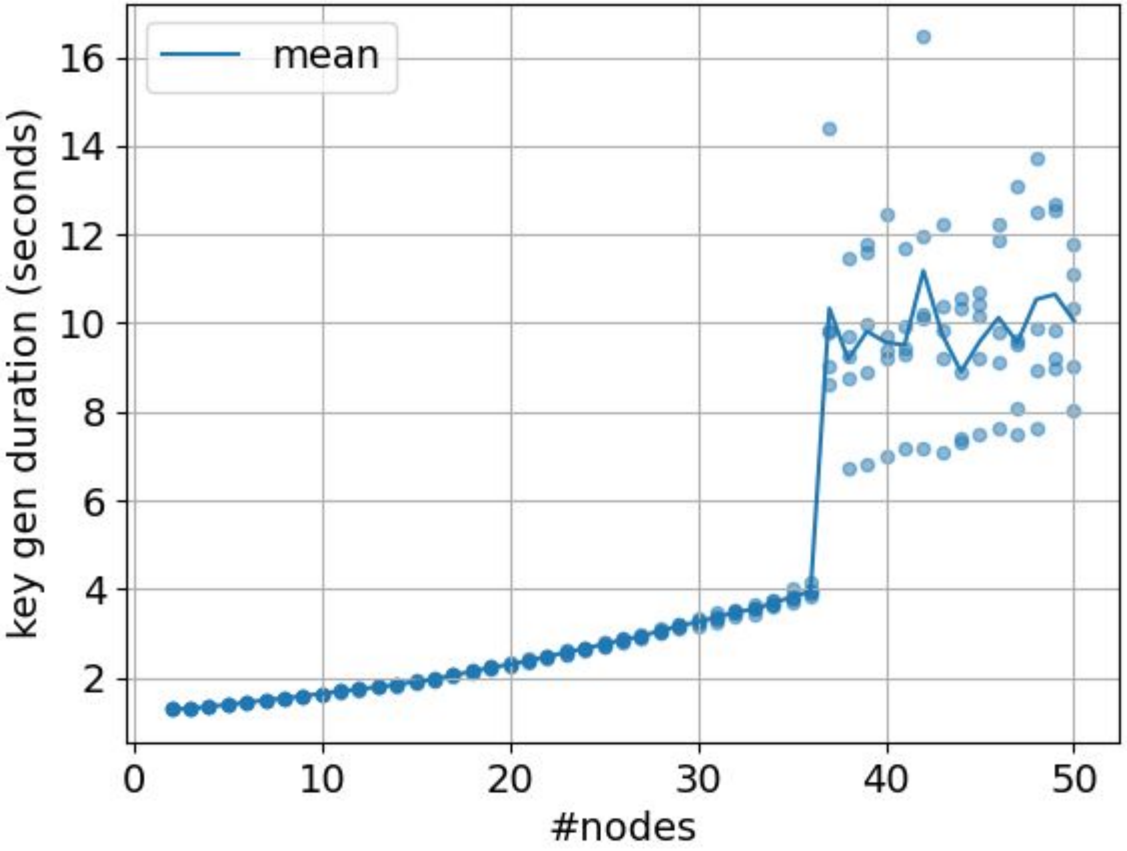
- Extremely fast
- Duration is mostly due to network
- Can be improved with precompuation



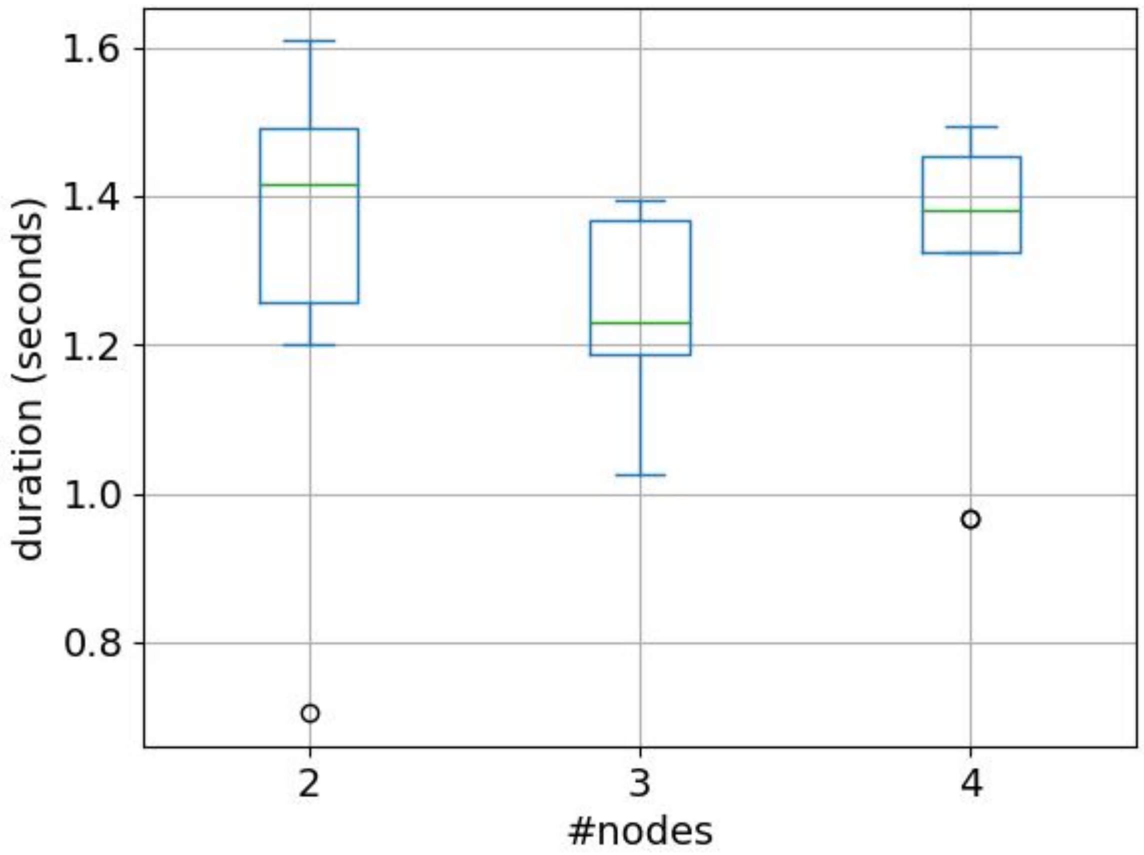
Improved key generation duration

How?

- Efficient serialization.
- Improved EVA.



Android key generation duration

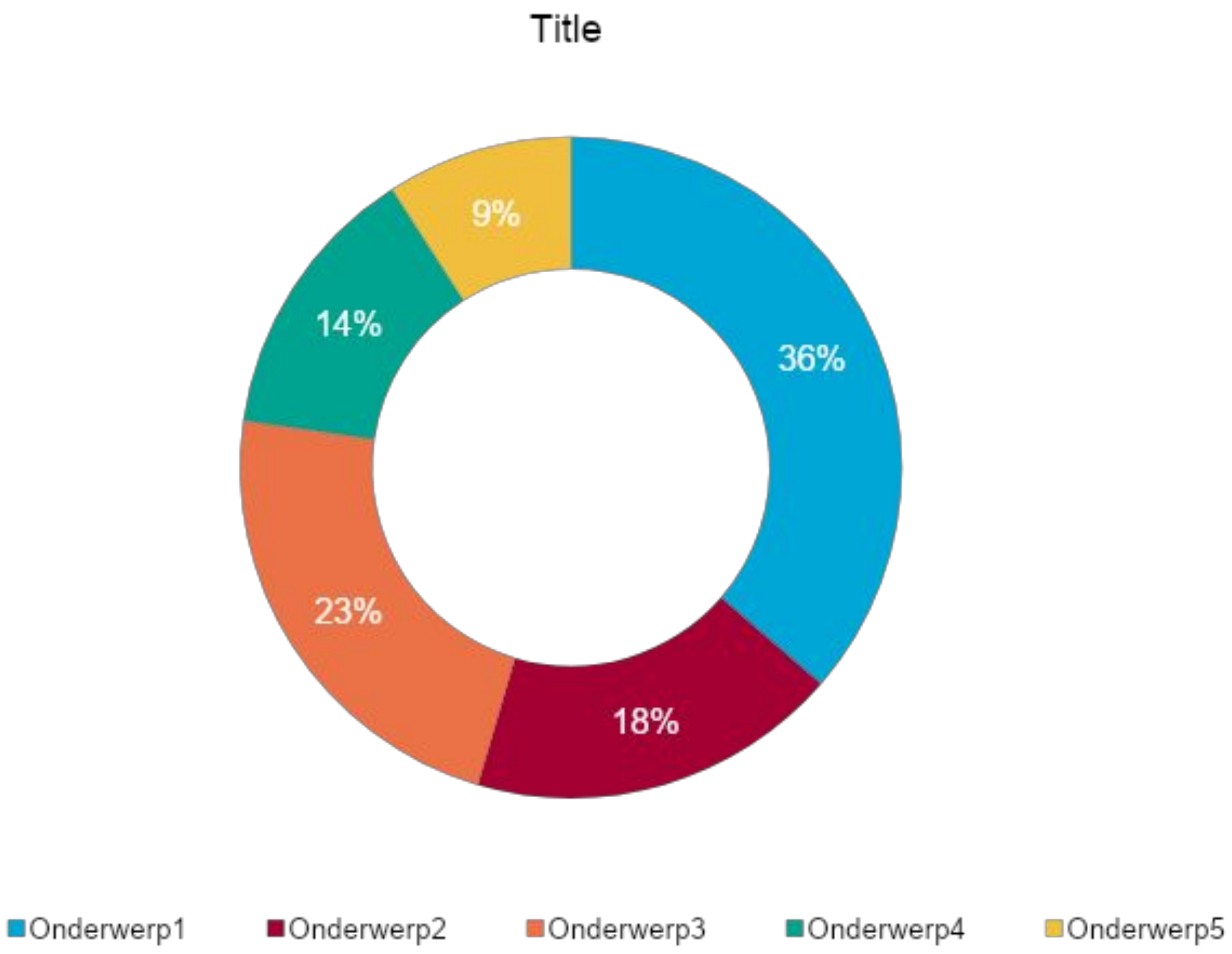


Future work

- Large scale experiments with Android devices
- Improving key generation performance
- Explore applications of the system
    - Lighting?

Title

- Lorem ipsum dolor sit amet, consectetur adipiscing elit
- Sagittis eu volutpat odio facilisis mauris sit amet.
- Massa placerat duis ultricies lacus.



Thank you for your attention

Name