Monero multi-signatures
ExaWallet
Fastsync protocol

Multi-signatures

Monero multi-signatures: origins

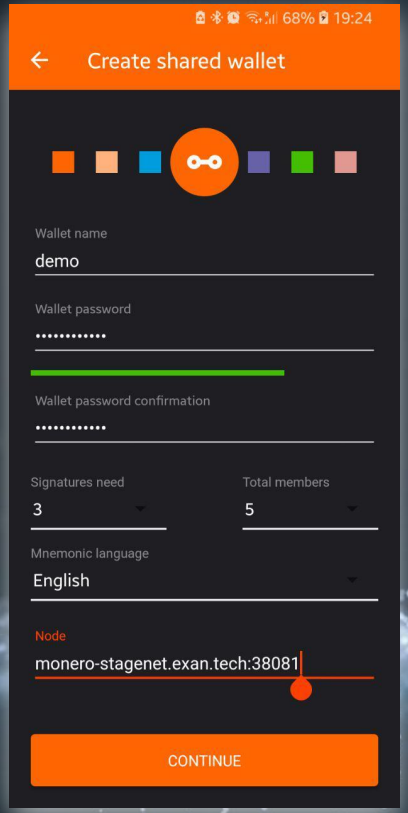
1. N/N and N-1/N are not enough
2. Works only with complex exchange of key images and partial keys in CLI
3. Requires secure channel for data exchange

Multi-signatures: extended

- Research current state and prepared a report
- Implemented M/N generalized multi-signature scheme
- Fixed some bugs along the way

Exa Wallet

- Supports classic and multisignature wallets up to M/N
- Uses open-source backend component to work with multisignatures
- Allows fully encrypted data exchange with own key pair
- Mobile optimizations



Current state

- Beta releases in AppStore & Play [stagenet]
- WIP version for desktop (Electron JS)
- Backend protocol v1 is completed
- Backend protocol v2 (total encryption) is testing

We’re looking for beta-testers

Apply via form

Light wallets

Monero light wallet

1. Popular use case
2. OpenMonero is hard to setup & maintain
3. Requires special wallet type and full resync

Monero Fastsync protocol

https://github.com/exantech/monero-fastsync

- Seamless switch between classic / fastsync nodes
- Ready-to-use backend solution (w/ libwallet patch)
- Uses secret view & public spend keys
- Optimized for wallet restore procedure

Performance

Server
H/w: PX61-SSD
S/w: PostgreSQL 9.6, nginx, FastSync daemon 0.1.3

Desktop wallet (~234k blocks)

Full resync, origin daemon: 280 sec.
Full resync, fastsync, “cold” address: 270 sec.
Full resync, fastsync,“warm” address: 64 sec.

Performance

Server

H/w: PX61-SSD

S/w: PostgreSQL 9.6, nginx, FastSync daemon 0.1.3

Mobile wallet

Android Galaxy S9, Exa Wallet

Full resync, origin daemon: 950 sec.

Full resync, fastsync, “cold” address: 540 sec.

Full resync, fastsync,“warm” address: 175 sec.

Monero & Exantech

- https://monero.exan.tech/, https://monero-stagenet.exan.tech/
- Nodes: monero-stagenet.exan.tech, monero.exan.tech, monero5sjoz5xmjn.onion
- https://exan.tech/en/projects/monero/
- https://wallet.exan.tech/

Thank you!

Denis Voskvitsov
dv@exan.tech