Ledger Seed Tool Application

by Aido

Topics

- Origin
- Assistants
- Challenges
- Current
- Demo
- Future

Origin

- BIP39 is adequate security for average person
- For the paranoid person (i.e. me) BIP39 has no redundancy
- MultiSig complexity more suited to larger organisations
- SSS a nice balance of security, complexity and redundancy
- No Ledger application for SSS
- Issue discussed on Ledger GitHub
    - https://github.com/LedgerHQ/ledger-nano-s/issues/54
    - Can conclude from issue that SSKR is the way to go
    - Issue open more than four years so no movement by Ledger

Assistants

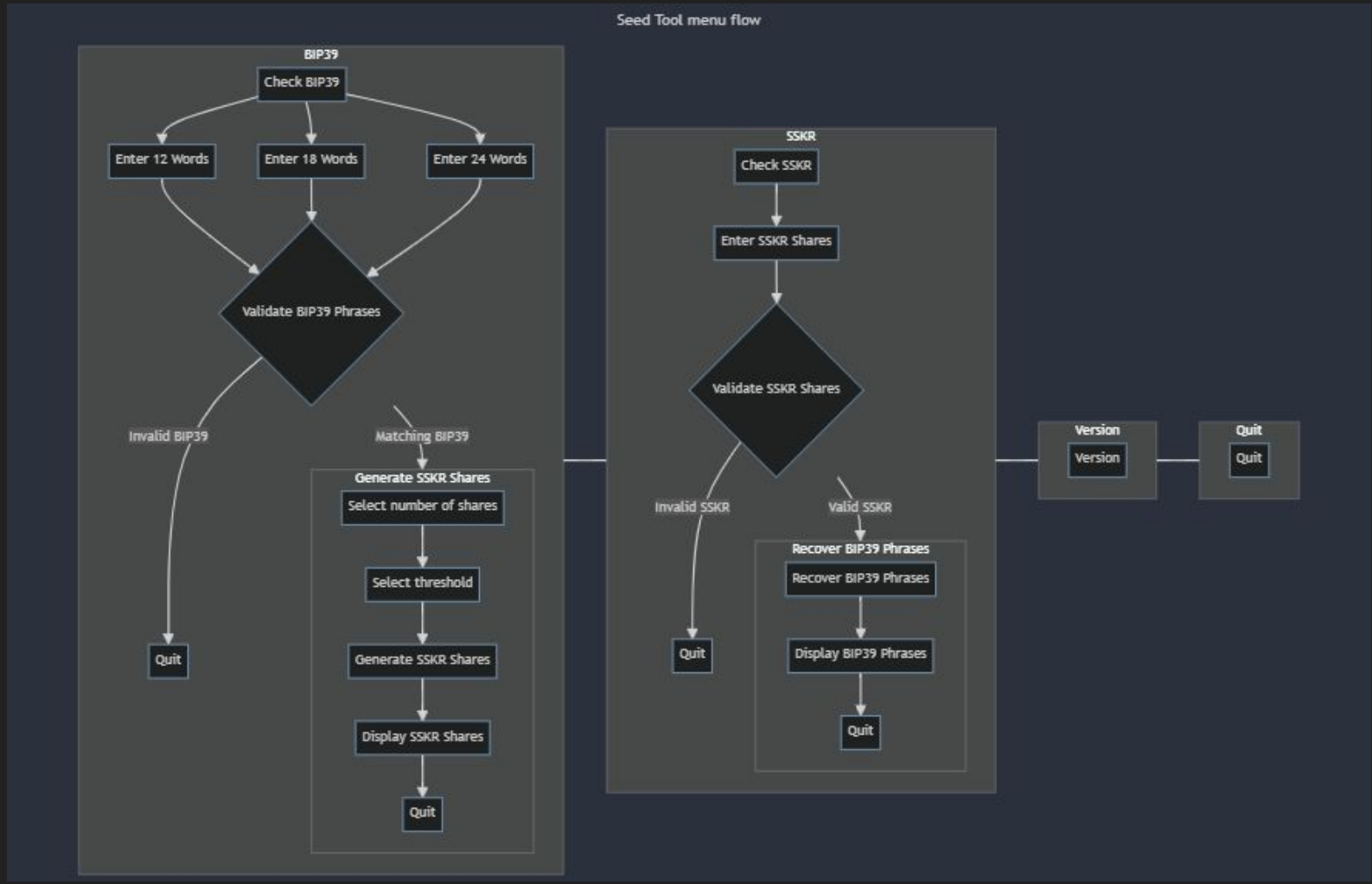
- Ledger Recovery Check application
  - https://github.com/LedgerHQ/app-recovery-check
- Blockchain Commons SSKR C library (bc-sskr)
  - https://github.com/BlockchainCommons/bc-sskr
- Blockchain Commons Shamir Secret Sharing C library (bc-shamir)
  - https://github.com/BlockchainCommons/bc-shamir
- Ledger Speculos emulator
  - https://github.com/LedgerHQ/speculos
- Blockchain Commons SeedTool command line tool
  - https://github.com/BlockchainCommons/seedtool-cli-rust

Challenges

- I am not a *real* developer
- Ledger Recover released half way through development of app and thought the service would scupper the app
- Lack of hardware/test devices
- Ledger Speculos emulator not the same as real hardware syscalls
- CRC32 broken in Speculos and device firmware
- Finite field operations not implemented in Speculos or in Nano S firmware
- Security audit

Current

- GitHub README
  - https://github.com/aido/app-seed-tool/blob/develop/README.md
- Sceenshots
  - https://github.com/aido/app-seed-tool/tree/screenshots/tests/functional/screenshots
- Ledger blog
  - https://www.ledger.com/blog/seed-tool-app
- Speculos demo on Nano S and Stax (time permitting)


Seed Tool menu flow
BIP39
Check BIP39
Enter 12 Words
Enter 18 Words
Enter 24 Words
Validate BIP39 Phrases
Invalid BIP39
Matching BIP39
Quit
Generate SSKR Shares
Select number of shares
Select threshold
Generate SSKR Shares
Display SSKR Shares
Quit
SSKR
Check SSKR
Enter SSKR Shares
Validate SSKR Shares
Invalid SSKR
Valid SSKR
Quit
Recover BIP39 Phrases
Recover BIP39 Phrases
Display BIP39 Phrases
Quit
Version
Version
Quit
Quit

Future

- Near term
  - SSKR on Stax
    - Pull request currently a work in progress
- Mid term
  - Ledger Flex
  - BIP85
    - BIP39 and password applications initially
- Long term
  - QR codes on Stax
    - Animated QR may be a possibility on Stax
  - Implement additional BIP85 sub-applications

Questions