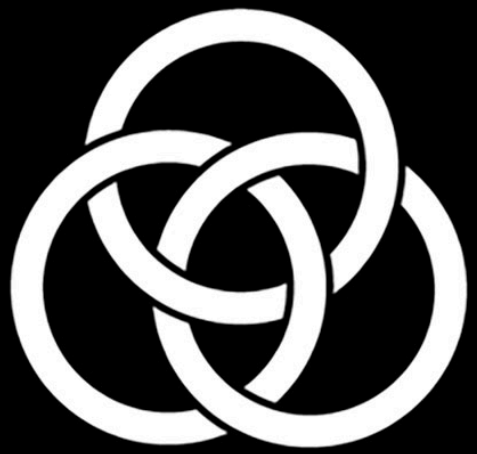


Blockchain Commons

Advocating for the Creation of Open, Interoperable,

What is Blockchain Commons?

- We are a community supporting the self-sovereign control of digital assets.
- We bring together stakeholders to collaboratively develop interoperable infrastructure.
- We design decentralized solutions where everyone wins.
- We are a neutral "not-for-profit" that enables people to control their own digital destiny.

Thank you to our Sponsors!

Sponsorships

- It's been a tough year! We've lost a number of sponsors!
    - They remain interested in supporting our technology.
    - But they're having problems with funding.
- Become a sponsor, mail us at team@blockchaincommons.com
- We can also support your company on specific projects
    - Open source & related to our specifications
    - Talk to us!
- Thanks to:
    - HRF for a Recent FROST Grant!
    - Foundation Devices for recent GSTP Research Funding!

Thanks also to individual sponsors!

Subscribe to Our Announcements

- https://www.blockchaincommons.com/subscribe/
    - Announcements for Gordian Developers, FROST
        - Announcements-only Mailing List
        - Signal Discussion Channel
- For Google Calendar invite to regular Gordian meetings:
    - Request from Christopher
        - ChristopherA@LifeWithAlacrity.com

Last Meeting

- Seedtool in Rust
- Why SSH?
    - SSH Envelope-CLI Updates
- Gordian Sealed Transaction Protocol (GSTP)

Today's Topics

- Seed Resilience
- Seeds in Blockchain Commons Tools
- BIP-85
- Ledger Seed Tool
- What's Next?

Seed Resilience

- Seeds are the heart of Digital Asset Security
- The “Layer 0” of Cryptographic Security
- Just 12 or 24 Bytes, But Crucial
- How do We Keep them Safe? (Security)
- How do We Avoid Losing them? (Resilience)
- We'll Explore that Today!

Blockchain Commons Specs & Tools

- What's working so far?
  - UR/Envelope for Seed Storage
  - SSKR Sharding for Seed Resilience
  - Request/Response for Seed Transfer & Key Derivation
- Reference Apps
  - Seedtool-CLI-Rust
    - Create & manage seeds on the command line
    - Integrate with Envelope-CLI & Other Apps
  - iOS Seedtool
    - Best Practices app on your iPhone
  - For helping developers implement & test standards!

ffa11a8

[604b93f2]

Yinmn Blue Acid Exam

Seed as Gordian Envelope

```
ur:envelope/lftpsogdhkwzdtfthptokigtvwnnjsqzcxknsktdoyadcsspgmgreefy
```

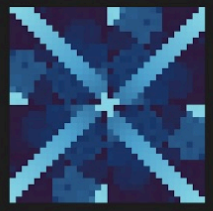
Minimal Bytewords convert to dCBOR:

```
82d8c95059f2293a5bce7d4de59e71b4207ac5d2a10118c8

82                                      # array(2)
   D8 C9                                # tag(201)
      50                                # bytes(16)
         59F2293A5BCE7D4DE59E71B4207AC5D2 # "Y\xF2):[\xCE}M\xE5\x9Eq\xB4 z\xC5\
   A1                                   # map(1)
      01                                # unsigned(1)
      18 C8                             # unsigned(200)
```

Seedtool iOS & macOS Features

- Create Seeds
- Identify Seeds
    - Name, LifeHash, Object Identity Block
- Backup Seeds
    - BIP-39, ByteWords, Hex
    - Envelope
        - Metadata, Name, Date, Note, Output Descriptors
    - QRs
- Shard Seeds
    - SSKR, SSKR-Envelope (CSR/Gordian Depository)
- Derive Keys
    - Bitcoin, Ethereum, Tezos
- Sign Bitcoin PSBT requests



ffa11a8

[604b93f2]

128-bit Seed Public Test Vector (Yinmn Blue)

Yinmn Blue in SeedTool for iOS/macOS

Yinmn Blue for offline PDF

Seedtool-CLI Features

- Create Seeds
- Backup Seeds
    - BIP-39, ByteWords, Hex
    - Envelope
        - Metadata, Name, Date, Note
    - Multipart URs
- Shard Seeds
    - SSKR, SSKR-Envelope (CSR/Gordian Depository)
- Translate Seeds
- Integrate with Envelope-CLI
    - Signing
    - Eliding
    - Encryption

Using Seedtool-CLI

```
$ seedtool
89290acafd0aafb21bd53904de47ed80
$ seedtool -i hex 89290acafd0aafb21bd53904de47ed80 -o bip39
matrix embark razor wheel priority suit hungry poet age vendor window abandon
$ seedtool -i hex 89290acafd0aafb21bd53904de47ed80 -o sskr -g 2-of-3
ur:envelope/lftansfwlrhdcetbsorflpmelgyaguurjzbdiyguetbzcyyacmldcwjennhnaysklgm
ur:envelope/lftansfwlrhdcetbsorflpmelgyaguurjzbdiyguetbzcyyacmldcwjennhnaysklgm
ur:envelope/lftansfwlrhdcetbsorflpmelgyaguurjzbdiyguetbzcyyacmldcwjennhnaysklgm
$ seedtool -i hex 89290acafd0aafb21bd53904de47ed80 -o envelope | envelope forma
Bytes(16) [
    'isA': 'Seed'
]
```

What's Next?

- Our main topic for the day!
- What's upcoming & just becoming available?
- How do we support it?
- How do we improve SECURITY & RESILIENCE for seeds?

BIP-85

- BIP-85 Uses a Single Seed for Multiple Wallets
- Children Seed Derived from Parent Seed
    - with a Simple Index
- *One Seed to rule them all, One Key to find them, One Path to bring them all, And in cryptography bind them.*

Ledger Seed Tool Application

- A New Tool for Seed Resilience!
- Shamir's Secret Sharing on Ledger
    - with Blockchain Commons' SSKR
    - And Lots More Assistants!
- https://www.ledger.com/blog/seed-tool-app
- 7 million hardware wallets can now use SSKR!

Key Exfiltration

- We need to stay up to date with modern threats
  - We've known about key exfiltration since 2018!
- It's about how keys could be compromized
  - Through untrustworthy signatures
    - Specifically, non-random nonces
  - But randomness is important to seeds too!
  - GSTP and FROST can help with both.

What's Next?

- There are lots of other ways to protect seeds
  - BIP-85 for hot wallets is an example
- There are lots of adversaries to be concerned about
  - Key Exfiltration is getting attention today
- What else?
- What features do we want for
  - iOS Seedtool & Seedtool-CLI?
  - Ledger Seed Tool?

Possible Additions

- Child Seed Derivation
  - BIP-85
- More Key Derivations
  - ZCash, Monero?
- Backup Mechanisms
  - GSTP and Gordian Depository Deployment
  - NFCs on NREF or smart JavaCards
- Key Generation and Multi-Party Computation
  - Trusted Dealer & Distributed; MUSIG2 & FROST
- What Else?

Get Involved!

- Use Our Existing Specs
  - UR for interoperable connections & animated QRs
  - SSKR bytewords for simple sharding
  - Envelope for Smart Storage
- Get In On the Next Thing: Collaborative Seed Recovery
  - Shard your seeds & metadata with SSKR-Envelope
  - Support GSTP, Host a Gordian Depository

www.BlockchainCommons.com

Christopher Allen (@ChristopherA)