Blockchain Commons

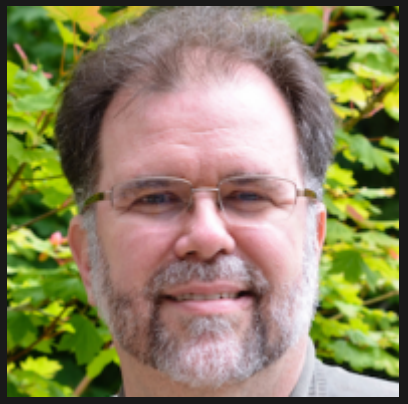
Advocating for the Creation of Open, Interoperable, Secure, and Compassionate Digital Infrastructure

Blockchain Commons #GordianDevelopers Meeting 2023-03-01

What is Blockchain Commons?

- We are a community interested in 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.

Who am I?



Christopher Allen (@ChristopherA)

Principal Architect & Executive Director

What are the #Gordian Meetings?

- Developers jointly expand & use the Gordian specs.
- Open, interoperable, secure, compassionate infrastructure.
- Goals for 2023:
    - dCBOR libraries
    - Gordian Envelope deployment
        - Swift & Rust Libraries
        - IETF/W3C Backing
        - Crypto-request Signing
    - Collaborative Seed Recovery (CSR)
    - Collaborative Key Management (CKM)

Last Regular Meeting

It’s Been a While!

Getting Back into Gear Today!

Monthly 1st Wednesdays Calls
+ special topic calls

Today’s Topics

- Community Channels
- UR Interoperability Success
- dCBOR & Community Review
- Crypto-Request for Signing
    - ExampleSigner
    - Future Proofing
- Next Month’s Priorities

Community Channels

- Virtual Meetings: 1st Wednesdays
  - *(possibly swap back and forth between 9am and 4pm to allow EU & Asia folk)*
  - Some Special Topic Calls
  - Send me mail if you want gCal invites
- Ephemeral & Synchronous
  - Signal: Gordian Developer
  - *(Also: Speciality Signal groups like UR Signing, Silicon Salon)*
- Peristent & Asynchronous
  - Github Discussion: Gordian Developer Community
- Announcement Lists
  - Join Here
  - Gordian Developer
  - Silicon Salon

UR Interoperability Success

The following wallets use Gordian UR-based Animated QRs for PSBTs or other URs:

Wallet	Animated PSBT	ur:crypto-psbt	ur:crypto-*	Future
Sparrow	YES	YES	-account, -address, -bip39, -hdkey, -output, -seed	
Passport	YES	YES	(-request/response with Casa for health check)	-account
CASA	YES	YES	-hdkey (-request/response for health check)	
SeedTool	YES	YES	-account, -address, -bip39, -hdkey -output, -seed, -sskr	
Keeper	YES	YES	-account	
Fully Noded	YES	YES	?	
DIYBitcoin	YES	?	?	
Jade	YES	?	?	
Keystone	YES	?	?	
SeedSigner	YES	?	?	

Submit corrections in the Gordian Developer repo:

https://github.com/BlockchainCommons/Gordian-Developer-Community/blob/master/README.md#urs

dCBOR & Community Review

- dCBOR Libraries for Rust and Swift Released
  - https://github.com/BlockchainCommons/bc-dcbor-rust
  - https://github.com/BlockchainCommons/BCSwiftDCBOR
- dCBOR-CLI
  - Currently Swift on macOS & soon Linux
    https://github.com/BlockchainCommons/dcbor-cli
- Presentation: What is dCBOR?
- Community Review
  - Can you test them?
  - Are the APIs expressive for your needs?
  - Are the APIs idiomatic?
- Submit for use by CBOR standards groups at IETF & W3C

ExampleSigner

- Educational mockup of a Bitcoin-based (ECDSA) message signing service in Swift.
- Uses Gordian Envelope as the transport encoding for requests and responses.
- Demonstrates the Uniform Resource (UR) format.
- Built on deterministic CBOR (dCBOR).

Future Proofing Signing

Many scenarios for Envelope `crypto-request`:

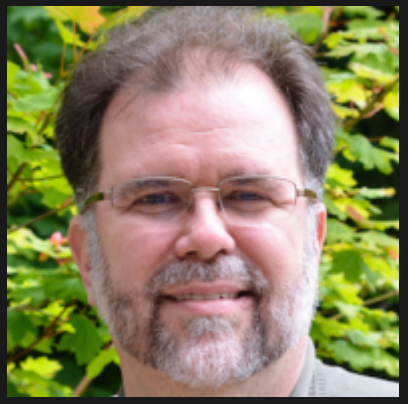
- Both Signing & Auth, safely
    - Not make SIWE (Sign-In With Ethereum) mistakes
- Simple single-round-trip and multi-round-trip scenarios
    - Legacy message, multi-device & multiparty processes
- Establish pairing for multig coodinators & MuSig/FROST
- *Signatures*: ECDSA; Schnoor; *Formats*: hash-only; PSBT; legacy messages; other payloads; P2SH; Taproot; BIP-344; SIWB
- Summary of special call available
- Add more requirement & prioritize in Requirements for Gordian UR Signing & Auth Discussions #102

Next Month Priorities

- Blockchain Commons
  - Envelope-Rust library
  - Update Envelope BLAKE3 ⇒ SHA256
  - Present Envelope at IETF
  - Demo of crypto-envelope CSR-SSKR
- Gordian Developer Community
  - SSKR code for constrained JavaCard
  - QR Demo of Legacy Bitcoin Messages

Join us on April 7th!

www.BlockchainCommons.com



Christopher Allen (@ChristopherA)