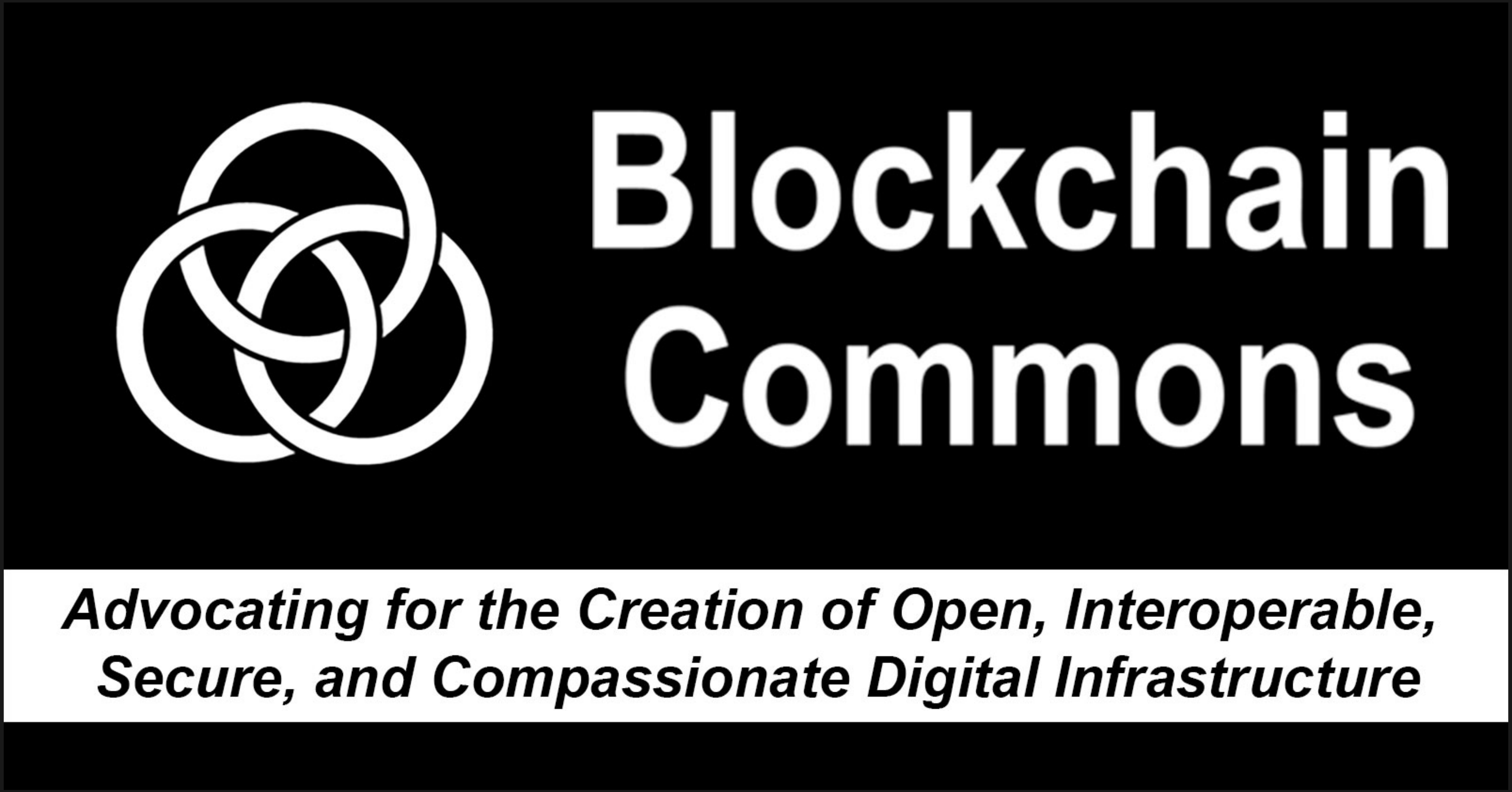


Blockchain Commons

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

Blockchain Commons #Gordian Meeting 2023-04-05

What is Blockchain Commons?

- We are a community interested in self-sovereign control of digital assets and identity.
- 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 is the Gordian Community?

- Developers jointly expand & use the Gordian specs.
- Open, interoperable, secure, compassionate infrastructure.
- Goals for 2023:
  - dCBOR & Gordian Envelope libraries
  - Reference examples of QR/UR crypto-request
    - Signing (beyond PSBT)
    - Account Policy (transaction coordinator)
  - Collaborative Seed Recovery (CSR)
  - Collaborative Key Management (CKM)

Last Meeting

dCBOR & UR Interoperability: 2023-03-01

- We introduced our dCBOR work.
- We talked about the 10 wallets now supporting URs!
- We introduced our Community Channels
    - https://www.blockchaincommons.com/subscribe.html

Today’s Topics

- Promoting Success of QR PSBT Interop
- Blockchain Commons Goes to Dispatch
- CBOR/UR Updates
- Evolving Internet-Drafts
- Legislative Work
- QuickConnect: The Next Generation
- SSKR for JavaCard

Promoting QR PSBT Interop

- This is our biggest success to date.
  - We are working on video to celebrate.
  - Please send us clip of sending and receiving a PSBT from your wallet.
- Please update your wallet details and entry on Gordan Community page:
  - https://github.com/BlockchainCommons/Gordian-Developer-Community/blob/master/README.md#urs
  - https://github.com/BlockchainCommons/Gordian-Developer-Community/blob/master/README.md#members
- If you offer a UR library, please update:
  - https://github.com/blockchaincommons/crypto-commons#bc-ur
- Don’t forget to subscribe to one our Community Channels:
  - https://www.blockchaincommons.com/subscribe.html

IETF Dispatch

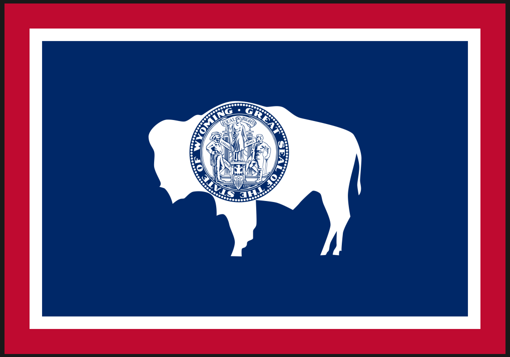
- Blockchain Commmons presented on March 27, 2023
- Feedback? We Need to Better Demonstrate:
    - Simplicity of Gordian Envelope Core: Deterministic Hash
    - More “Why” than “What” or “How”
        - Addressing RFC 6973 (Privacy) & RFC 8280 (Human Rights)
    - Transforming GUIDELINES into Requirements
- New Connections to CBOR Groups
- BOF Tentatively Planned for July IETF in SF

CBOR/UR Updates

- Planned renumbering of CBOR tags in prep. for IANA application.
    - Tags already be in use by developer community are now marked “Fixed”, not renumbered.
    - Tags 200-206 are now the “core” envelope tags: these are the ones we are going to apply to IANA for.
    - Tags 207-212 are for distributed function calls.
    - Tags 300-323 are related to Bitcoin or SecureComponents.
    - Tags 400-410 are used as output descriptor types.
    - Tag 500 is used as response type for OutputDescriptorResponse.
- Changed two UR type names:
    - crypto-digest is now just digest.
    - crypto-msg is now just encrypted.

Evolving Internet-Drafts (I-Ds)

- Envelope I-D Updates
    - Designed and added eighth case to envelope specs: compressed.
    - Behaves very much like encrypted and elided cases.
    - Together, all three are now consistently referred to in code and specs as the “obscured” cases.
    - https://blockchaincommons.github.io/WIPs-IETF-draft-envelope/draft-mcnally-envelope.html
- dCBOR I-D Updates
    - Removed requirement that map entries be non-null.
    - https://blockchaincommons.github.io/WIPs-IETF-draft-deterministic-cbor/draft-mcnally-deterministic-cbor.html



Legislative Work

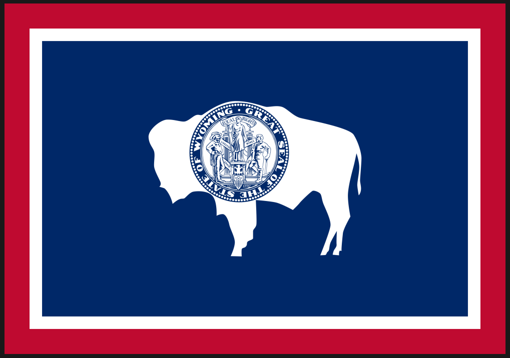
- Private Keys Will Be Protected in Wyoming!
- Digital Assets Can Be Registered in Wyoming!
- See Our New Advocacy Web Page: https://advocacy.blockchaincommons.com/

QuickConnect: The Next Generation

- QuickConnect: One of our First Projects
  - https://github.com/BlockchainCommons/Gordian/blob/master/QuickConnect/
  - btcstandup://rpcuser:rpcpassword@kshcahsaihslalsichs78yb2ud8d.onion:833
- Next generation: nostrnode
  - https://github.com/Fonta1n3/nostrnode-macOS

Proxy Updates

- Demo: SSKR in JavaCard
    - https://github.com/proxyco/jc-sskr
- Discussion: NFC for Secure Transfer



Next Monthly Call

- Will be held in conjuction with Silicon Salon IV
  - First Wednesday, May 3, 2023 9am-Noon PDT (**not 4pm!**)
  - We will send you code for free registration
- **Topics**
  - Anti-Exfil: Preventing Key Exfiltration Through Signature Nonce Data. (Andrew Poelstra)
  - Scalar and Vector Draft Biginteger instructions for the Power ISA (Luke Leighton & David Calderwood)
  - Open Hardware Discussion. An open discussion on applying open-source principles to hardware.

As always, we hope that you will
financially support us on GitHub:
https://github.com/sponsors/BlockchainCommons

Christopher Allen (@ChristopherA)
www.BlockchainCommons.com