Blockchain Commons

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

Blockchain Commons #Gordian Meeting 2023-11-01

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 are a neutral “not-for-profit” that enables people to control their own digital destiny.
- We are working together on Gordian Envelope, Collaborative Seed Recovery.

Thank you to our Sponsors!

Become a sponsor!

Mail us at team@blockchaincommons.com

September Developer Meeting

- IETF 117 Results
- Attachments for Envelope
- Developer Web Pages
- YAML Format for Disclosing Docs (OR13)
- Rust Libraries in Community Review

Today’s Topics

- Output Descriptors (Discussion)
- Envelope CLI (Wolf)
- CSR Depository (Wolf)
- Recent Musings

Output Descriptors

- We Need an Interoperable Way to Store Descriptors!
    - They’re the future of wallet interoperability!
    - Keys, scripts, derivation paths!
- Our Original Proposal
    - ur:crypto-output and ur:crypto-account
    - BCR-2020-10 and BCR-2020-15
- Our Current Proposal
    - Gordian Envelope with Metadata
- SeedHammer Proposal
    - Research/issues/135 (SeedHammer)
- We’ll get to each in turn!

Our Original Proposal

- BCR-2020-10 and BCR-2020-15
- We were unable to allocate IANA numbers we thought we could!
- One reason that we've largely moved to our updated Envelope
- We weren't communicative about deprecating the original!
    - Deprecated just means superseded: we have a preferred new proposal.
    - Is there something else we should do here?
- Our work with community is a Learning Process!
- We remain small and need resources.

Revamping Our Specification Process

- Blockchain Commons Research papers (BCRs) are fluid
    - We're happy to see external BCRs!
    - https://github.com/BlockchainCommons/Research
- Blockchain Commons Proposals (BCPs) promise more community involvement
    - https://github.com/BlockchainCommons/bcps
- BCRs become BCPs when we have two external parties implementing them!
- Does this work? What else should we do to make our specifications work for everyone?

The New Envelope Format

- Our Current Proposal
  - Gordian Envelope with Metadata
  - https://tinyurl.com/gordian-descriptors

```
"Example" [
    outputDescriptor: "wpkh([37b5eed4/84'/0'/0']xpub6
        isA: OutputDescriptor
        hasName: "Example"
        note: "This is the note."
    ]
]
```

Descriptors Concerns & Discussions

- Are there alternatives the community prefers?
    - SeedHammer Proposed BIP?
        - Research/issues/135 (SeedHammer)
- Are there concerns over complexity?
    - Use bare dCBOR instead of Envelope?
    - Separate & reference keys?
- Do formats include the required info? Are they extensible?
- Three options: which way do we go?
- How can we discuss & finalize?

Envelope CLI

- Our Rust envelope-cli is Available for Preview!
- `bc-envelope-cli-rust` in the Blockchain Commons repo.
- Working example of our new Rust stack.
- Doesn't require XCode tools like our Swift CLI.
- Slightly different syntax (no defaults!).
- Demo from Wolf.

CSR Depository

- CSR is Almost Here!
- Wolf has a framework for a Web Server Running
    - Front-end: Warp
    - Back-end: MariaDB
    - API based on ExampleStore
        - https://tinyurl.com/ExampleStore
    - Authentication via TOFU
    - Another Example of our Rust Stack
- TODO
    - First review release
    - SSH Key Backup?
    - Gordian Companion Integration.
    - TorGap
    - Release!

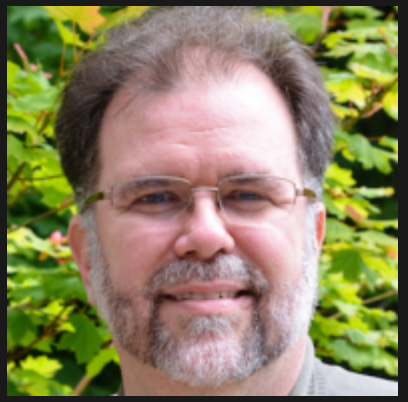
What's the Goal of CSR?

- To create an interoperable ecosystem of share servers.
- To give users the choice.
    - They decide where their shares reside.
    - They decide what authentication they're comfortable with.
    - Unlike Ledger Recover, which makes the choices for you, and requires KYC!
- Our CSR Depository is an example!
    - More are needed to create that ecosystem!

Recent Musings

- Self-sovereign Computing
- Least & Miminal Design Patterns
- An Intro to Schnorr
- Available from https://blockchaincommons.com
- Also: https://lifewithalacrity.com

www.BlockchainCommons.com



Christopher Allen (@ChristopherA)