Blockchain Commons

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

Blockchain Commons #Gordian Meeting 2023-09-06

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.

Last Meeting

July Developer Meeting

- Return to URs & Animated QRs
- UR Experiences (thunderbiscuit)
- A LifeHash Use Case (Craig)
- Self-Sovereign Identity
- Gordian SeedTool 1.6 (Wolf)
- Standardizing for CSR

Today's Topics

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

IETF 117 Results: dCBOR

- Great meeting!
- Locked down our dCBOR as CBOR profile.
- dCBOR I-D v5 is Out
  - https://tinyurl.com/dcbor-v5
- Defined what IANA numbers we could acquire.

IETF 117 Results: Envelope

- Number clarification meant BREAKING CHANGE for Envelope
- Envelope is now Registered as CBOR tag 200!
  - https://tinyurl.com/cbor-tags
- Other Envelope tags moved to higher numbers.
- Our reference apps are up to date!
  - envelope-cli
  - Gordian Seed Tool

Attachments for Envelope (I)

- We want vendors to be able to incorporate their own data into Envelopes.
- BCR-2023-006 Defines attachments for Envelopes
- It allows for the inclusion of specific, typed data in an open way.
- We've introduced Attachments to support this.
    - Since it's vendor-specific, an attachment REQUIRES a vendor assertion.
    - a `conformsTo` assertion can help specify things.
- Allows for storage & exchange of descriptors, backups, shares, and who knows what else!

Attachments for Envelope (II)

Here’s what an attachment looks like:

```
Bytes(16) [
    isA: Seed
    attachment: {
        "Attachment Data"
    } [
        conformsTo: "https://example.com/seed-envelope-attachment/v1"
        vendor: "com.example"
    ]
    date: 2021-02-24T09:19:01Z
    hasName: "Dark Purple Aqua Love"
    note: "This is the note."
]
```

Attachments for Envelope (III)

Envelopes allow for the transmission of metadata!

Here's that same attachment output as an Envelope UR, and then read into Gordian SeedTool.

Attachments for Envelope (IV)

- We have published a detailed example of composing attachments using the `envelope` command line tool, then importing them into Seed Tool
- Gordian Seed Tool now saves and persists your attachments to seeds.

Attachments for Envelope (V)

- Now we need your feedback!
- Obviously, you can package your own data privately.
- But we want to support your creating interoperable attachments of vendor-defined data.
- Particular if you have at least one other vendor you want to exchange data with!
- What data do you want to store?
- What data do you want to exchange?

Output Descriptors for Seeds

- We have published a number of new research papers:
    - https://github.com/blockchaincommons/research
- BCR-2023-007 Defines Bitcoin output descriptors for Envelopes
    - Output descriptors can have additional metadata (name and notes)
- BCR-2023-008 Defines seeds for envelopes
    - Seeds can include attachments
    - Seeds can specify a primary output descriptor
- Envelopes are now Seed Tool's preferred exchange format for seeds, keys, and output descriptors.

New Developer Web Pages

- We've collected all of our developer docs on a new web site!
    - https://developer.blockchaincommons.com
- Info on 11 specifications & other projects
    - Plus our architectural designs
- Why are they important? How do they work?
- Test vectors, best practices FAQs, examples.
- About 60 pages right now!
- Tell us what else you need for anything!

YAML Format for Disclosing Docs (OR13)

- Disclosable Tag
- Originally JSON Payloads
- But Generalizing
- CBOR is coming

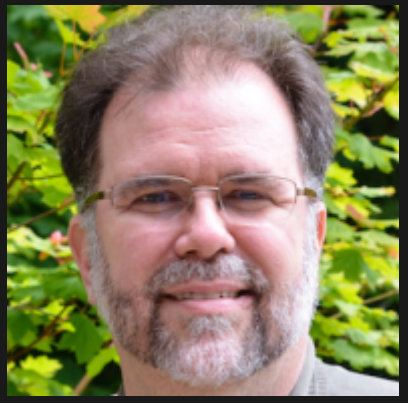
Rust Libraries in Community Review

- Take a look at the Rust Libraries for our crypto-stack, including Envelope, SSKR, and URs.
    - https://tinyurl.com/review-rust
- Are there mistakes or problems?
- Does the API meet your needs?
- Is the functionality easy to use?
- Does the usage of Rust feel proper?
- Does the library solve your problems?
- How could it be improved?

Coming in October ...

- Next Gordian Developer Meeting: October 4
- Trying to decide Europe-friendly (Pacific morning) or Asia-friendly (Pacific late afternoon)
- What Do You Think?
  - Also, let us know:
  - https://tinyurl.com/gdm-oct

www.BlockchainCommons.com



Christopher Allen (@ChristopherA)