

Blockchain Commons

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

Blockchain Commons #Gordian Meeting 2024-01-10



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.

Thank you to our Sponsors!



Become a sponsor! Mail us at team@blockchaincommons.com



Happy New Year!

- In December We Talked about ...
 - Output Descriptor v3
 - URs & The Need for Improved Docs/BIPs
 - Gordian Depo!
 - Open Development



Today's Topics

- dCBOR: The Latest Update
- Gordian Seed Tool: Now with Tezos
- Multi-Part Implementation Guide for URs
- Recent Research Papers
- New Research Statuses



dCBOR

- dCBOR Now Released as I-D 07
 - <http://tinyurl.com/dcbor-v7>
- Builds on new CDE I-D
 - Common Deterministic Encoding
- Carsten Bormann is Now Co-Author
- CBOR WG met this morning ...



GST: 25519 Interop & Tezos

- Gordian Seed Tool (iOS/Mac) now supports three cryptocurrencies
 - Bitcoin & Ethereum use secp256k1, Tezos uses ed25519, an IETF standard
- You can use your seed to generate addresses for any chain
 - but these are optional default presets
- Meanwhile, GST can provide resilience for those keys
 - Gordian Envelope, SSKR, print-outs, NFC
- Museums are increasingly collecting NFTs
 - Some interest major museum in Share Depo for their NFT artists
 - We hope this will support them
 - And provide a model for others to do the same
- Original Tezos Release (TZ2) is On Testflight, TZ1 soon
- New 1.6 Release Will Be Out to Store this Month



Multi-Part Implementation Guide for URs

- Animated QRs Are Our Biggest Success
- But We've Used Source as Our Documentation
 - Thank you for feedback that wasn't enough!
- We Have New Docs Explaining How Things Work
 - <https://github.com/BlockchainCommons/Research/blob/master/papers/bcr-2024-001-multipart-ur.md>
- Are They Sufficient?
- Sparrow's Hummingbird library now supports latest UR Tags. Sparrow reads but does not output them yet.
 - <https://github.com/sparrowwallet/hummingbird>
- Next Step: BIPs








Recent Research Papers

- BCR 2023-11: URs for Public Keys
- BCR 2023-12: Envelope Expressions
- BCR 2023-13: Envelope Encryption
- BCR 2023-14: Gordian Sealed Transaction Protocol (GSTP)
- BCR 2023-19: UR Account Descriptor (v2)
- See: <http://tinyurl.com/bc-research>



Research Status

- **XXX** — withdrawn
- **X** — superceded
-  — research
-  — reference implementation
-  — multiple implementations
-  — standards track
-  — standardized

First pass: <https://github.com/BlockchainCommons/Research/>



Thoughts on Research Status

- We want to be clear the current status of our specifications!
- Withdrawn vs supercede is one important distinction
 - Do we suggest backward compatibility or not?
- Research, Ref Imp, Multiple Imp, Standards Track also important
 - It reveals how stable a specification is!
- Can list multiple statuses with system
 - ★★✗ — two implementations, but superceded, for example
- Two independent implementations remains our gold standard.



Secure NFCs

- We will be doing some additional work with NFCs in 2024:
 - ***open development*** javacard-based libraries and apps
 - <https://github.com/proxyco/jc-sskr>
 - leveraging some commodity NFC smartcards
 - <https://www.cardlogix.com/product/nxp-jcop-4-java-card-3-0-5-classic/>
 - Bitcoin PSBTs, envelope-based SSKR, and digital message signing.
- See Gordian SeedTool for some initial work.
- If you have interest or expertise, please let us know!

The Limitations of Open Source

- Acknowledge Achievements of Open Source:
 - Open Source revolutionized software development.
 - Set a foundation for collaborative and accessible coding.
- Address Limitations:
 - Open source focuses mainly on licensing, less on processes.
 - Can lead to gaps in design, docs, security, and long-term support.
 - Heartbleed!
- Open Development - Beyond Licenses:
 - Encompasses collaborative creation of code, standards, and practices.
 - Fills in these gaps with a more integrated "holistic" approach to development.

Principles of Open Development

- **Accessibility:** Open to all, with clear participation and membership rules.
- **Collaboration:** Inclusive decision-making involving developers, users, and distributors.
- **Diversity:** Embracing varied backgrounds and perspectives to enhance creativity.
- **Strategy:** Community-focused planning rather than individual whims.
- **Transparency:** Openness in processes, decisions, and support mechanisms.
- **Sustainability:** Long-term commitment to upgrades and fixes.
- **Openness:** Commitment to interoperability and freedom from platform lock-in.

Levels of Open Development

- **Level 0: Open Source** - Basic code availability under open license.
- **Level 1: Inspectable** - Current, versioned code in public repositories.
- **Level 2: Observable** - Transparent development processes, including bug tracking and releases.
- **Level 3: Reproducible** - Compilable code with stubs for private components.
- **Level 4: Testable** - Comprehensive testing suites for public code.
- **Level 5: Cooperative** - Community involvement in roadmaps, specs, and contributions.
- **Level 6: Distributed** - Multi-organizational commitment and shipped products.
- **Level 7: Standardized** - International standards for interoperability and no vendor lock-in.

Our Call to Action: Embrace Open Development!

- **Integrate Principles & Practices:**
 - Integrate Open Development principles into your organizational strategy for collaborative, transparent progress.
 - Improve your Open Development best practices to maximize the benefits of openness and collaboration.
- **Actively Engagement and Improvement:**
 - Collaborate with to shape and refine Open Development practices in your industry.
 - Invest resources to expand and evolve these practices for collective advancement.
- **Financial Support:**
 - Allocate financial resources to support organizations advocating and implementing Open Development in our communities.
 - Invest in developing technology openly and responsibly for future generations.



www.BlockchainCommons.com



Christopher Allen (@ChristopherA)