

Blockchain Commons

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

Blockchain Commons #Gordian Meeting 2023-06-07



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?

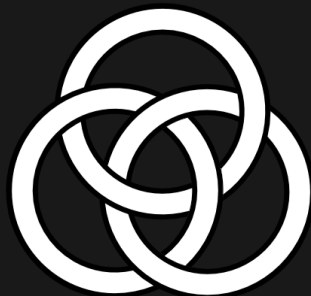


Christopher Allen (@ChristopherA)
Principal Architect & Executive Director



What are the #Gordian Meetings?

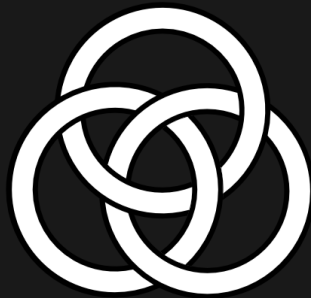
- Developers jointly expand & use the Gordian specs.
- Open, interoperable, secure, compassionate infrastructure.
- Goals for 2023:
 - dCBOR libraries
 - Gordian Envelope usage
 - Collaborative Seed Recovery (CSR)
 - Collaborative Key Management (CKM)



Last Meeting

Silicon Salon 4 - May 3, 2023

- Anti-Exfiltration
- Big Integer Arithmetic Instruction Design
- Hardware Open Source
 - How Do We Do It?
 - Does It Even Make Sense?
- <https://www.siliconsalon.info/salon4/>
- Next Silicon Salon is July 26. Propose a Presentation!



Today's Topics

- Shamir Updates
- Engraving & Fountain Codes (SeedHammer)
- Signing Updates
- New Use Cases for Gordian Envelope
 - Educational
 - Wellness
- QuickConnect: The Next Generation (Peter)
- Gordian for Rust (Wolf)



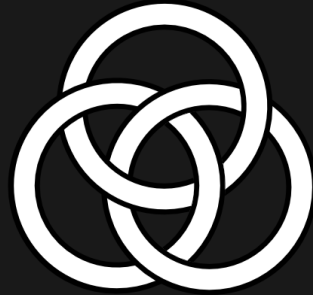
Shamir Updates

- Sharding is coming into wider usage
- Trezor has long used SLIP-39
- New CODEX-32 from Poelstra Y O'Connor
- Ledger Recovery uses shards
 - But huge controversy
- Proxy has implemented SSKR for JavaCard
 - <https://github.com/proxyco/jc-sskr>
- Non-production SSKR in WASM
 - <https://github.com/AndreasGassmann/bc-sskr-wasm>
- New SSKR in RUST
 - <https://github.com/BlockchainCommons/bc-sskr-rust>



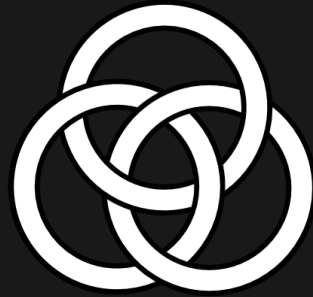
From SSKR to CSR

- SSKR has plenty of advantages
 - bc-sskr & bc-shamir are security reviewed!
 - Conversions at "Crypto Commons" repo
 - Small & simple
 - Great for seeds & other high-entropy data
 - But not for other data, no metadata
- CSR is the next step
 - more versatile
 - more resilient
 - supports metadata



SeedHammer: Engraving & Fountain Codes

- Steel Backup Specialized for Bitcoin Multisig Wallets
 - Self-contained
 - Engraved!
 - <https://seedhammer.com/>
- Fountain code discussion
 - Reproducibility & simplification
 - <https://github.com/BlockchainCommons/Research/issues/1>



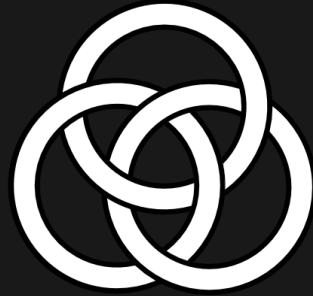
Signing Updates

- Signing meeting on February 24
 - Current implementations
 - Crypto-request, crypto-response, Envelope
 - Cold Card signing, Casa Health Check
 - Future goal: single round-trip signing
- Any progress?



New Use Cases for Gordian Envelope: Educational

- We presented to W3C's VC-ED group
- "The Dangers of Digital Credentials in Education"
 - "And How to Resolve them Using Holder-Based Hashed Elision"
- Threats: identity theft, discrimination, institutional liability
- Our Answers
 - Holder-Based Elision — let the student decide
 - Hashed Elision — maintain proofs & signatures
- Meetings listed at <https://tinyurl.com/gordian-meetings>



New Use Cases for Gordian Envelope: Wellness

- We wrote new use cases for activity trackers & health info
 - How do you keep that data safe?
 - How do you safely share with medical professionals?
 - How do you safely & provably share with clinical trials?
 - How do you safely do contract tracing?
- Overview article: <https://tinyurl.com/gordian-well>
- All of our use cases: <https://tinyurl.com/gordian-use>
 - New use cases: <https://tinyurl.com/gordian-use-well>
- <https://github.com/BlockchainCommons/Gordian/tree/master/Envelope/Use-Cases>



QuickConnect: The Next Generation

- QuickConnect: One of our First Projects
 - <https://tinyurl.com/quickco-v1>
 - `btcstandup://rpcuser:rpcpassword@kshcahsaihsalsichs78yb2ud8d.onion:8333`
- Need to understand requirements for other services
 - Spotbit, Esplora, raw transaction distribution
 - Maybe even bootstrap of P2P services or Tor Client auth
- Next generation: nostrnode
 - <https://tinyurl.com/quickco-v2>



Gordian for Rust

- New work on Rust libraries
 - `bc-dcbor-rust`
 - `bc-ur-rust`
 - `bc-shamir-rust`
 - `bc-sskr-rust`
 - `bc-envelope-rust`

Rust Dependencies



Next Monthly Call

- July 6, 2023
 - 10am PDT
 - Europe-friendly time!
 - Let us know your topics!
- We are also planning a side meeting at IETF 117
 - Late July, SF
 - More info to come!



www.BlockchainCommons.com



Christopher Allen (@ChristopherA)

