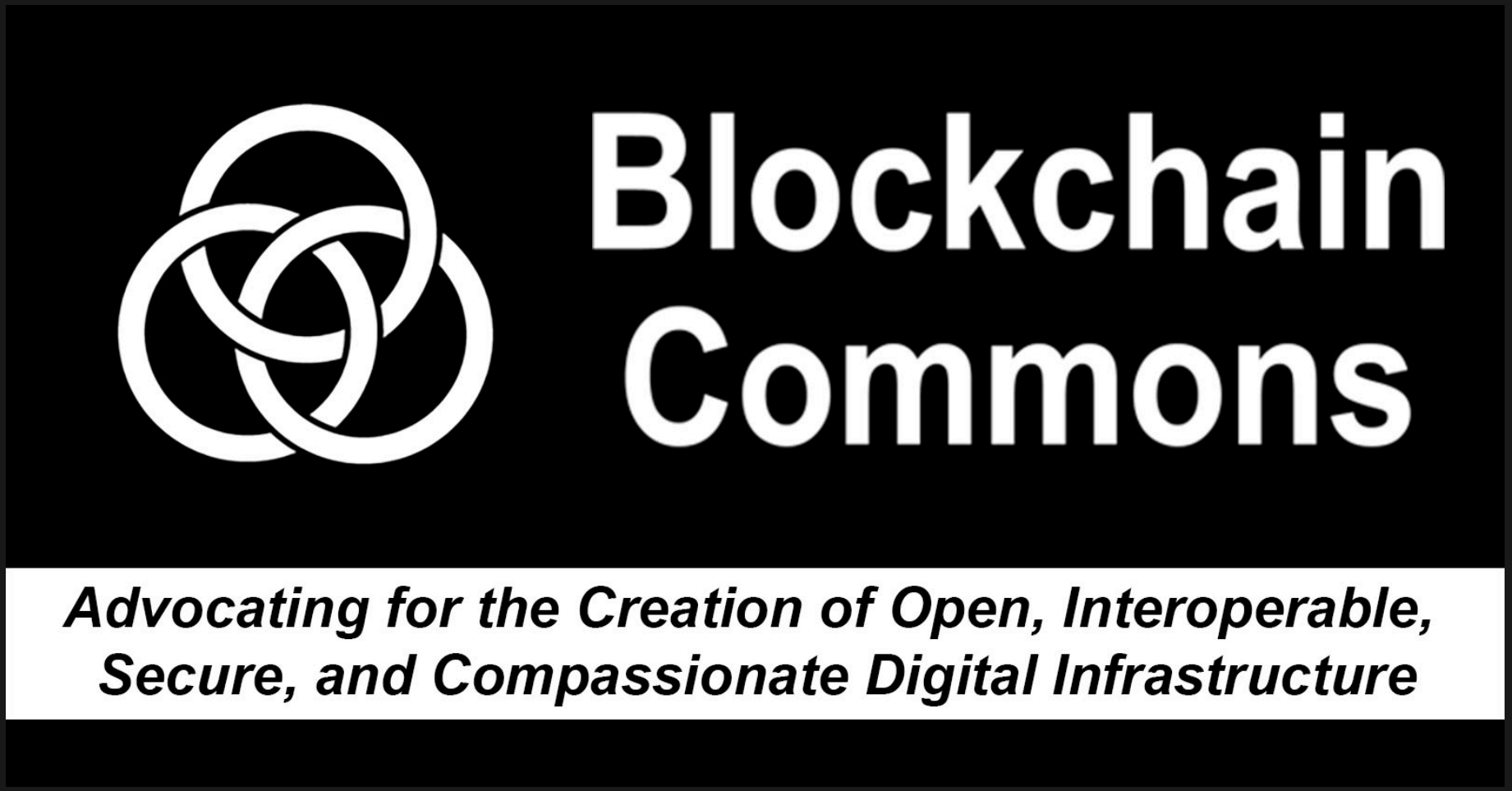

Blockchain Commons #Gordian Meeting 2024-07-10

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!

Sponsorships

- It's been a tough year! We've lost a number of sponsors!
    - They remain interested in our tech.
    - But they're having problems with funding.
- Become a sponsor, mail us at team@blockchaincommons.com
- We can also support your company on specific projects
    - Open source & related to our specifications
    - Talk to us!
- Thanks to:
    - HRF for a Recent FROST Grant!
    - Foundation Devices for recent GSTP Research Funding!

Thanks also to individual sponsors!

Subscribe to Our Announcements

- https://www.blockchaincommons.com/subscribe/
    - Announcements for Gordian Developers, FROST
        - Announcements-only Mailing List
        - Signal Discussion Channel
- For regular google calendar invite to Gordian meetings:
    - Request from Christopher
        - ChristopherA@LifeWithAlacrity.com

Last Meeting

- PayJoin Presentation!
- SSH-Envelope
- The Request/Response Use Case

Today's Topics

- Seedtool in Rust
- Why SSH?
    - SSH Envelope-CLI Updates
- Gordian Sealed Transaction Protocol (GSTP)

Seedtool-CLI-Rust Release

- Seedtool-CLI Is Now Available in Rust
  - `seedtool-cli-rust`
- Updated to Our Newest Specifications
- See The New User Manual
- What's Next?
  - Descriptors? Attachments? BIP-85?
  - We'll have a full presentation on BIP-85 next month!

Why SSH?

- We're updating Envelope-CLI for SSH
- Traditionally, SSH keys have been used for authentication
- But now they can be used for code signing
    - Git & GitHub are the leaders here
    - We'd like to see more tools for software supply chain
- Offer SSH keys also shows flexibility of Envelope.
    - Not agility, but flexible.
- So here's what we've done ...

Envelope-CLI Updates

- `bc-envelope-rust` is now at 0.9.0
  - The older `envelope-cli-swift` has been deprecated
    - diffs & mermaid output not yet ported
- New Envelope-Rust Features
  - `generate signer` has options for deriving SSH keys
  - `import` & `export` SSH keys
  - `sign` with SSH keys!
  - `info` on URs with SSH keys & signatures
  - Verify SSH signatures!

Envelope-CLI Breaking Changes

- `--prvkeys` is now `--signer`
- `--pubkeys` is now `--verifier`

Gordian Sealed Transaction Protocol (GSTP)

- GSTP is our Envelope Protocol for Secure Transmissions
  - See BCR-2023-014
  - Uses Envelope Request/Response with Encryption
- New! Support for Bidirectional Cryptographic Continuation
  - Preserve the state to pick up operation at a later time
  - Methodology for doing this now standardized
- Our Research Sponsor for this work is FOUNDATION DEVICES
  - https://foundation.xyz/
  - Want to sponsor specific work? Let us know!

Next Month's Meeting!

- Back to our Regular First Wednesday Date
  - Wednesday, August 7
- Planned Topics
  - A Special Presentation on BIP-85
  - More on Using SSH with Envelope

www.BlockchainCommons.com

Christopher Allen (@ChristopherA)