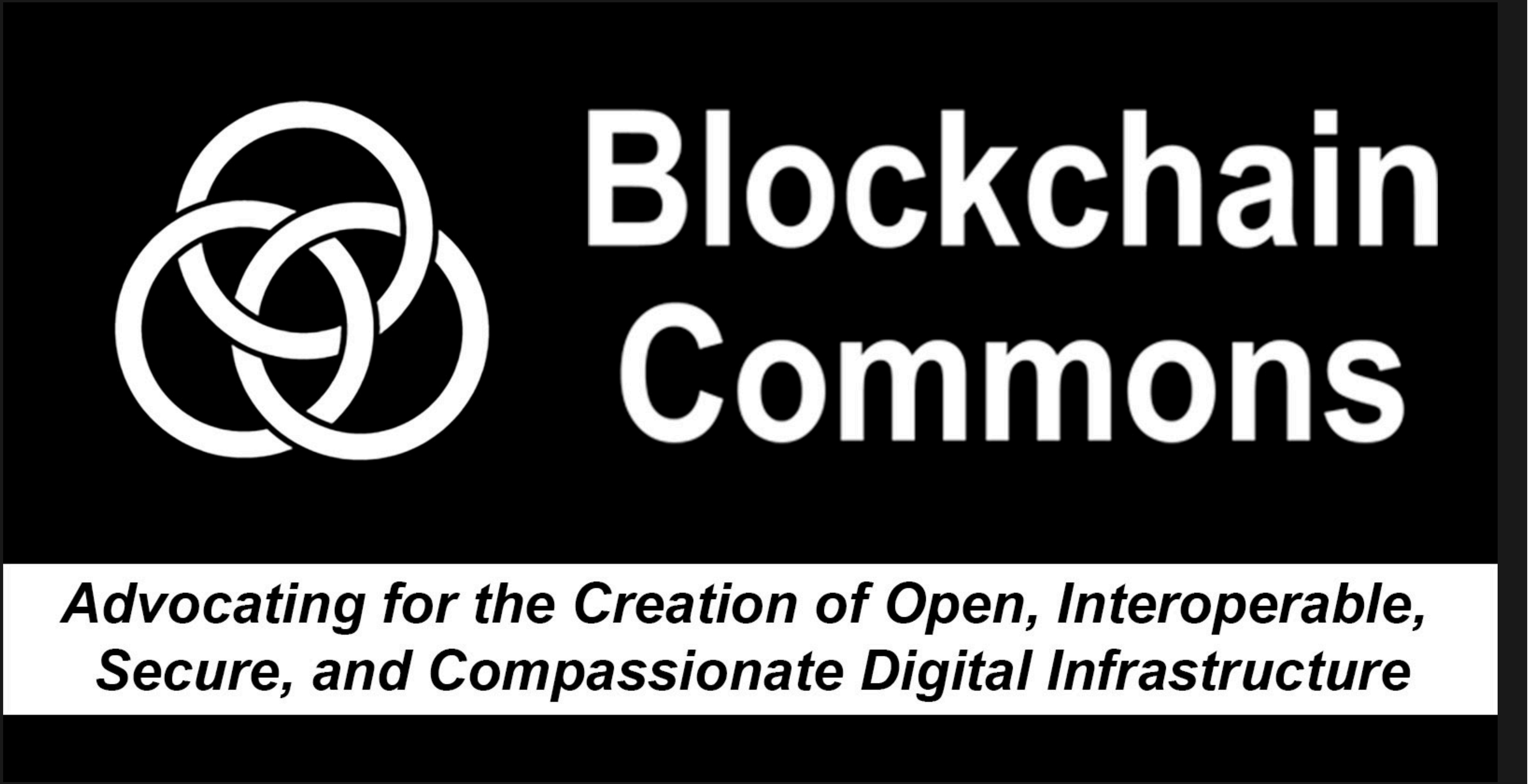

Blockchain Commons

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

Blockchain Commons #Gordian Meeting 2025-11-05

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!

Bitmark
chia
CROSSBAR
DCD
FOUNDATION
Human Rights Foundation
unchained capital
Zcash
Community Grants

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

TODAY'S TOPICS

- Exodus Protocols
- Hubert Dead-Drop Hub

CLUBS: A PRELUDE

- We introed this last month!
- ***Clubs*** are Autonomous Cryptographic Objects.
- They allow transmission of information without infrastructure.
- They support coordination, collaboration.
- Clubs was our first example of an Exodus Protocol

For more: https://developer.blockchaincommons.com/clubs/

Exodus Protocol. *Noun Phrase*. Infrastructure that can’t be revoked and that survives when platforms disappear, built on mathematics instead of permission.

WE'RE FIGHTING AGAINST INFRASTRUCTURE THAT DISAPPEARS!

- Email, Photos, MP3s
- Link Services (del.icio.us, mag.nol.ia, Pocket)
- Google+ Circles
- Internet Radio

Sometimes the "disappearance" is purposeful:

- Financial Censorship (WikiLeaks, Canadian Truckers)

Everyone has their own story of loss by this point!

ANOTHER EXAMPLE OF AN EXODUS PROTOCOL: BITCOIN!

- Miners Come and Go
- Spin Up Your Own Node!
- Create Transactions Offline
- Transmit via QR Codes!
- Send When and Where You Want!

BITCOIN PROVED SOMETHING PROFOUND

Fundamental capabilities can exist as mathematical rights rather than centralized privileges.

When your ability to transact depends on a bank's approval, it's not a right—it's permission.

Bitcoin made value transfer a right

For fifteen years it has demonstrated autonomous infrastructure that works. No servers to shut down, no administrators to pressure, no companies whose failure matters.

BUT … BITCOIN IS A SINGLE USE CASE

- Bitcoin supports Value Transfer on the internet
- We need to support Coordination, Collaboration, Identity
- Clubs is just a first step
- We will need many Exodus Protocols
- Not for all use cases
    - Sometimes centralization is required!
- But as a strong foundation!

FIVE PATTERNS FOR EXODUS PROTOCOLS

1. Operate without external dependencies
2. Encode rules in mathematics, not policy
3. Make constraints load-bearing
4. Preserve exit through portability
5. Work offline and across time

Pattern 1: Operate Without External Dependencies

- **The principle:** If it requires permission to operate, it's not autonomous.
- **The pattern:** Self-contained cryptographic objects that work without asking permission.
- **Bitcoin's approach:** Distributed verification across thousands of independent nodes. No central server, no phone home behaviors.

We need coercion-resistant architecture.

Pattern 2: Encode Rules in Mathematics, Not Policy

- **The principle:** Math doesn't discriminate, doesn't take sides, doesn't change its mind under pressure.
- **The pattern:** Cryptographic proof replaces administrative decision-making. Verification is deterministic.
- **Bitcoin's approach:** Consensus rules in protocol code, not administrator decisions.

Code can be coerced; mathematics cannot.

Pattern 3: Make Constraints Load-Bearing

- **The principle:** What can't be changed can't be weaponized.
- **The pattern:** What appears as limitation is actually freedom.
  - *Can't expire = works forever*
  - *Can't phone home = perfect privacy*
- **Bitcoin's approach:** Each "limitation" protects against capture.
  - *Can't reverse transactions = can't seize funds by fiat.*

This is coercion-resistant design.

Pattern 4: Preserve Exit Through Portability

- **The principle:** Lock-in is the opposite of sovereignty. **Exit is not escape, it's leverage.**
- **The pattern:** Interoperability and open standards. No proprietary formats that trap users.
- **Bitcoin's approach:** Your keys work in any wallet. Open protocol means freedom to switch implementations.

Without the ability to walk away, consent collapses into coercion.

Pattern 5: Work Offline and Across Time

- **The principle:** Infrastructure that requires connectivity can be denied connectivity.
- **The pattern:** Asynchronous operation. Works during outages. Survives across decades.
- **Bitcoin's approach:** Sign transactions offline, broadcast later. The protocol doesn't care about connectivity.

True autonomy works when
coercion's attempts to deny — fail

BUT ...

Autonomous systems like Clubs implement these patterns.

But they still need to coordinate.

- Threshold signature ceremonies (FROST)
- Governance decisions
- Access updates
- Capability delegation

Traditional coordination requires servers.
Servers create centralization.

How do we enable communication without breaking the patterns?
The Answer: Hubert, a Dead-Drop Protocol
~ Coordination via dead-drops ~

MEET HUBERT:
THE DEAD-DROP HUB

Hubert = Hub of Berts

- Distributed infrastructure for secure multiparty transactions
- Enables coordination without servers or intermediaries
- Complete opacity to network observers
- Built on write-once distributed storage + cryptographic addressing

HUBERT'S TECHNICAL FOUNDATION

Two Gordian Stack Technologies:

- **Gordian Envelope** - Smart documents with encryption & progressive disclosure
    - Structured data format supporting elision (reveal in layers)
    - Self-contained cryptographic proofs
- **ARIDs** - Apparently Random Identifiers become capabilities
    - Cryptographic addresses for write-once storage
    - Derived to storage keys via HKDF
    - Never exposed publicly (shared via secure channels)
    - Possession = read access, creation = write access

Result: Messages opaque to networks, transparent to recipients

HUBERT'S COORDINATION PROTOCOL

That's all that's *required* for Hubert, but another Gordian Stack Technology supports coordination, with authentication & encryption of messages:

- **GSTP** - Gordian Sealed Transaction Protocol built on Envelopes
  - Sender authentication + receiver encryption
  - Multi-recipient capable with encrypted state continuations
  - Network sees only encrypted envelopes
  - Complete metadata protection

HUBERT IMPLEMENTS EXODUS PATTERNS

1. **No external dependencies:** Distributed storage (DHT, IPFS)
2. **Mathematics, not policy:** Cryptographic addressing (ARIDs)
3. **Constraints are load-bearing:** Write-once = immutability
4. **Portability preserves exit:** Open protocols, no lock-in
5. **Works offline/across time:** Asynchronous coordination

EXAMPLE: FROST CEREMONY

Scenario: 3-of-5 threshold signature

1. Coordinator publishes encrypted signing request with response ARIDs
2. Participants retrieve request from distributed storage
3. Each generates signature share
4. Participants publish encrypted shares at coordinator's ARIDs
5. Coordinator retrieves shares and completes signature

Network observers see: Only encrypted envelopes

No server coordinated this ceremony!

REAL-WORLD COORDINATION NEEDS

What Hubert enables beyond FROST:

- **Journalists** protecting sources with distributed storage
- **Activists** coordinating during network disruption
- **Immigrants** with credentials that don't "phone home"
- **Disaster response** teams working without infrastructure
- **Privacy-focused communities** organizing without metadata exposure

All without servers. All without surveillance.

STORAGE BACKENDS

Four options:

- **BitTorrent Mainline DHT** - Fast, lightweight (≤1 KB)
- **IPFS** - Large capacity (≤10 MB)
- **Hybrid** - Automatic size optimization
- **Server** - Testing/controlled deployments

All use write-once semantics

- Eliminates race conditions
- Ensures message immutability
- No one can modify or delete published messages

THE XANADU LINEAGE

- **Ted Nelson's Xanadu:**
  - Basic object = **bert** (Bertrand Russell)
  - Club System (early capability-security)
  - Vision of decentralized coordination
- **Mark S. Miller's Evolution:**
  - Refined capability security model
  - Object capabilities in E language
- **Hubert = Hub of Berts**
  - Where autonomous objects coordinate
  - Cryptography finishes what Xanadu started

NOW THE TECHNICAL DEEP-DIVE

Wolf will demonstrate:

- ARID generation and derivation
- Storage backend operations
- Bidirectional coordination flows
- CLI and API usage

Let's see the code!

Status: Hubert v0.1.0 - Community Review Phase

https://github.com/BlockchainCommons/hubert-rust www.BlockchainCommons.com

Christopher Allen (@ChristopherA)