HUBERT

BLOCKCHAIN COMMONS

FROST WITH HUBERT

GORDIAN DEV MEETING

WHAT IS HUBERT?

- A “dead drop” protocol that facilites *secure multiparty transactions:*
  - 📝 **Participants write once** using random keys
  - 🆔 **Messages contain random keys** for expected responses, enabling indefinite bidirectional communication
  - 📦 **Complete opacity** to outsiders through both steganography and end-to-end encryption
  - 🛜 **No central server** required for coordination
  - 🤝 **Trustless operation** using public distributed networks

TRADITIONAL SPYCRAFT: THE DEAD DROP OPERATION

Phase 1: The Drop & The Signal

Phase 2: The Retrieval

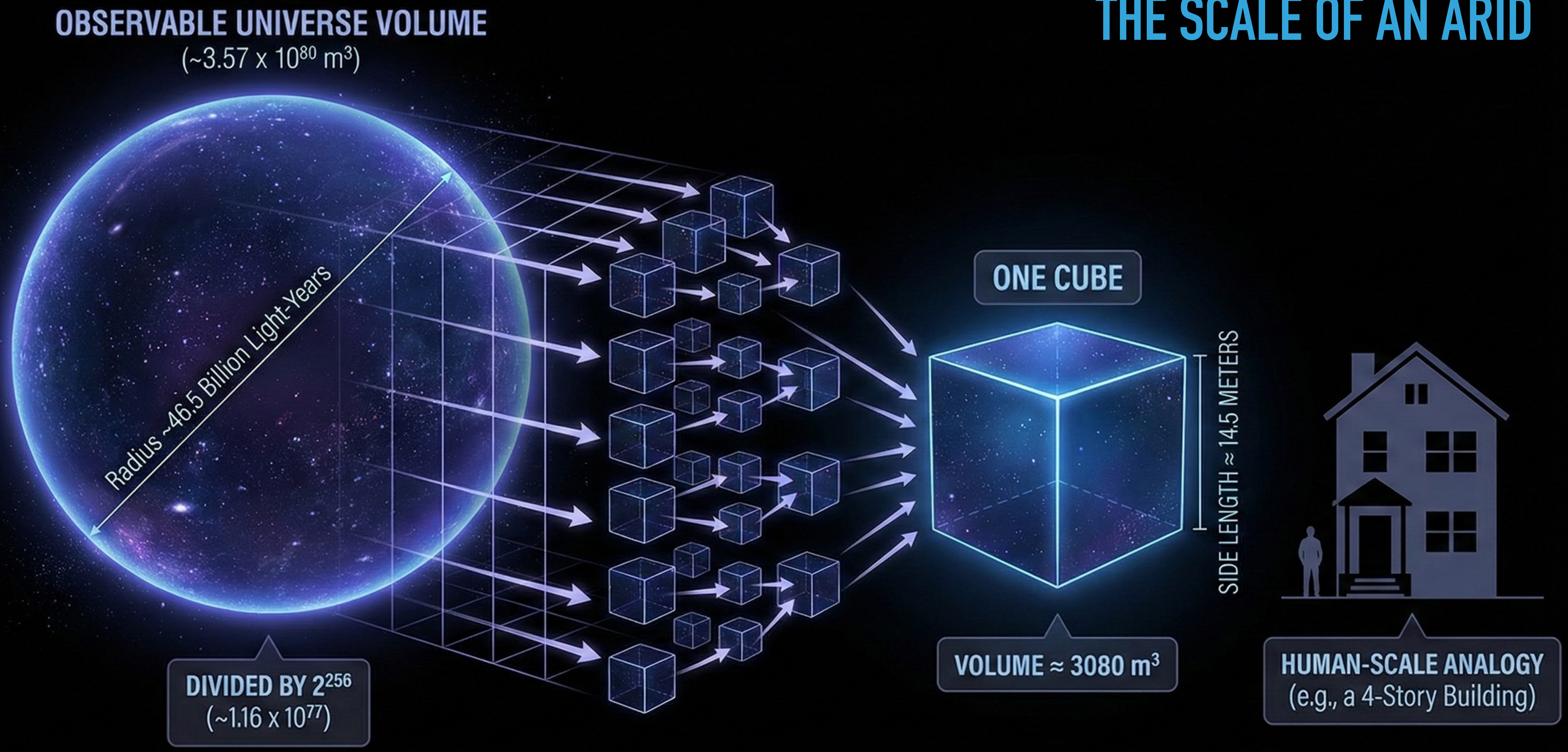
Pre-arranged Time & Location
The Signal (e.g., Chalk Mark) - Indicates 'Drop Loaded'
Signal Spotted – Drop is Ready
The Drop (Hollow Rock with Message)
Spy 1 (Sender)
Spy 2 (Receiver)
The Retrieval (Service the Drop)

Objective: Secure, One-Way Information Exchange Without Direct Meeting.

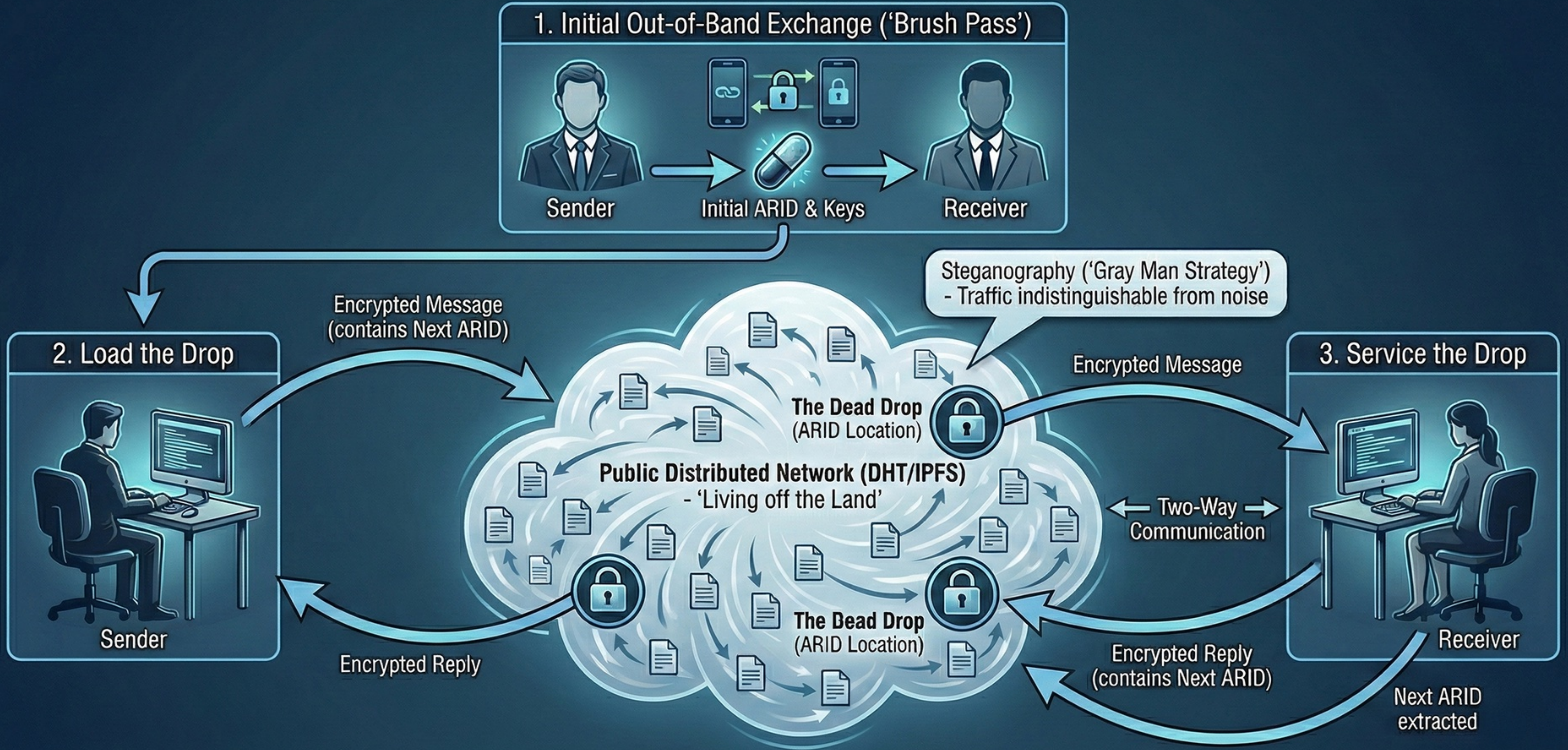
WHAT IS AN ARID?

- 🆔 ARID: Apparently Random Identifier
  - Defined in **BCR-2022-002**
    - https://github.com/blockchaincommons/research
  - 256 statistically random bits (32 bytes)
  - Can refer to anything
  - But cannot be correlated to anything
  - In Hubert, ARIDs are addresses of cryptographic *dead drops.*

THE SCALE OF AN ARID


OBSERVABLE UNIVERSE VOLUME
(~3.57 x 10^{80} m^3)
Radius ~46.5 Billion Light-Years
DIVIDED BY 2^{256}
(~1.16 x 10^{77})
ONE CUBE
SIDE LENGTH ≈ 14.5 METERS
VOLUME ≈ 3080 m^3
HUMAN-SCALE ANALOGY
(e.g., a 4-Story Building)

Hubert: A Digital Linked Dead Drop System



1. Initial Out-of-Band Exchange ('Brush Pass')

Sender

Initial ARID & Keys

Receiver

2. Load the Drop

Sender

Encrypted Message (contains Next ARID)

Encrypted Reply

Steganography ('Gray Man Strategy') - Traffic indistinguishable from noise

The Dead Drop (ARID Location)

Public Distributed Network (DHT/IPFS) - 'Living off the Land'

The Dead Drop (ARID Location)

3. Service the Drop

Encrypted Message

Two-Way Communication

Receiver

Encrypted Reply (contains Next ARID)

Next ARID extracted

Defense in Depth: Message is Encrypted & Authenticated

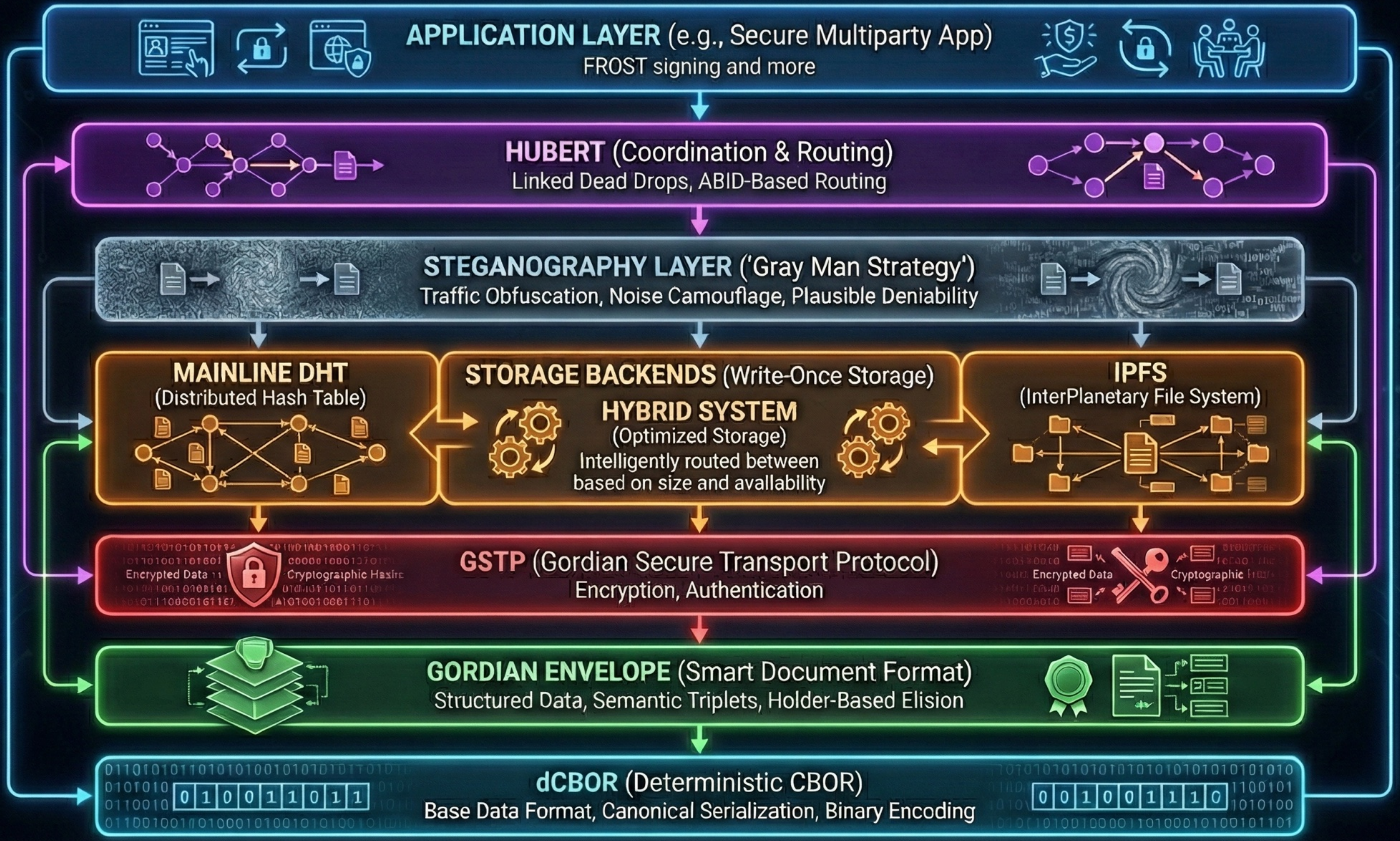
STORAGE LAYERS

BitTorrent™

IPFS

SQLite

HUBERT: SECURE MULTIPARTY COORDINATION STACK



APPLICATION LAYER (e.g., Secure Multiparty App)
FROST signing and more

HUBERT (Coordination & Routing)
Linked Dead Drops, ABID-Based Routing

STEGANOGRAPHY LAYER ('Gray Man Strategy')
Traffic Obfuscation, Noise Camouflage, Plausible Deniability

MAINLINE DHT
(Distributed Hash Table)

STORAGE BACKENDS (Write-Once Storage)
HYBRID SYSTEM
(Optimized Storage)
Intelligently routed between based on size and availability

IPFS
(InterPlanetary File System)

GSTP (Gordian Secure Transport Protocol)
Encryption, Authentication

GORDIAN ENVELOPE (Smart Document Format)
Structured Data, Semantic Triplets, Holder-Based Elision

dCBOR (Deterministic CBOR)
Base Data Format, Canonical Serialization, Binary Encoding

WHAT ARE URS?

- UR: Uniform Resource
  - Defined in **BCR-2020-005**
    - https://github.com/blockchaincommons/research
  - Encodes binary data as typed, easy to handle text URI
  - ur:type/bytewords

DEMO

HUBERT

FROST