Fission

Web Native File System (WNFS)

IPFS Security Working Group — Lightning Talk

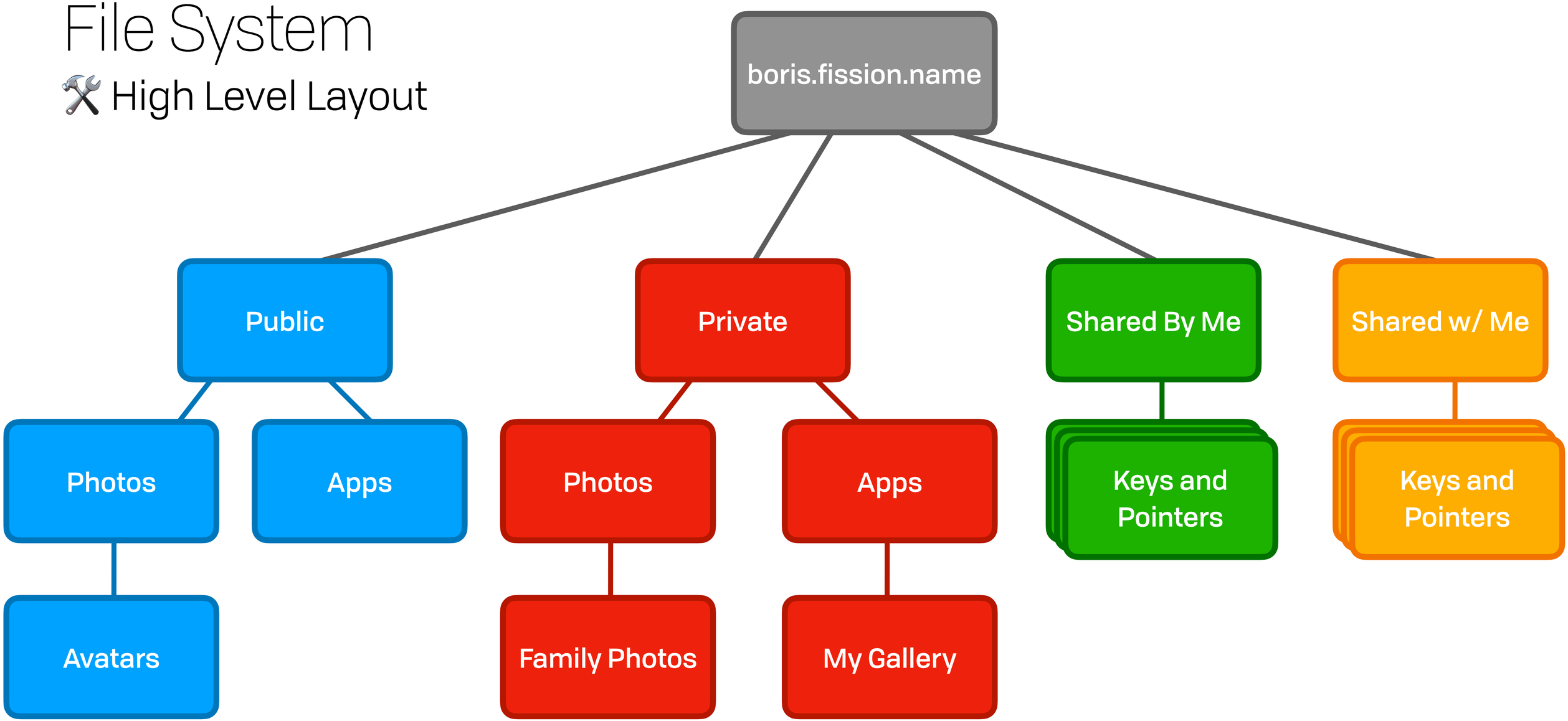
Constraints

📱 Mass Market Use Case

- User controlled — data & ID, local first, &c
- Vanilla browser, incl. mobile (browser is a hostile environment)
- No plugins, no hardware wallets
- As-good-or-better security than web 2
- User friendly, don’t assume expertise, common UX expectations
- Subgraph access control (re-share subsets of data you have access to)

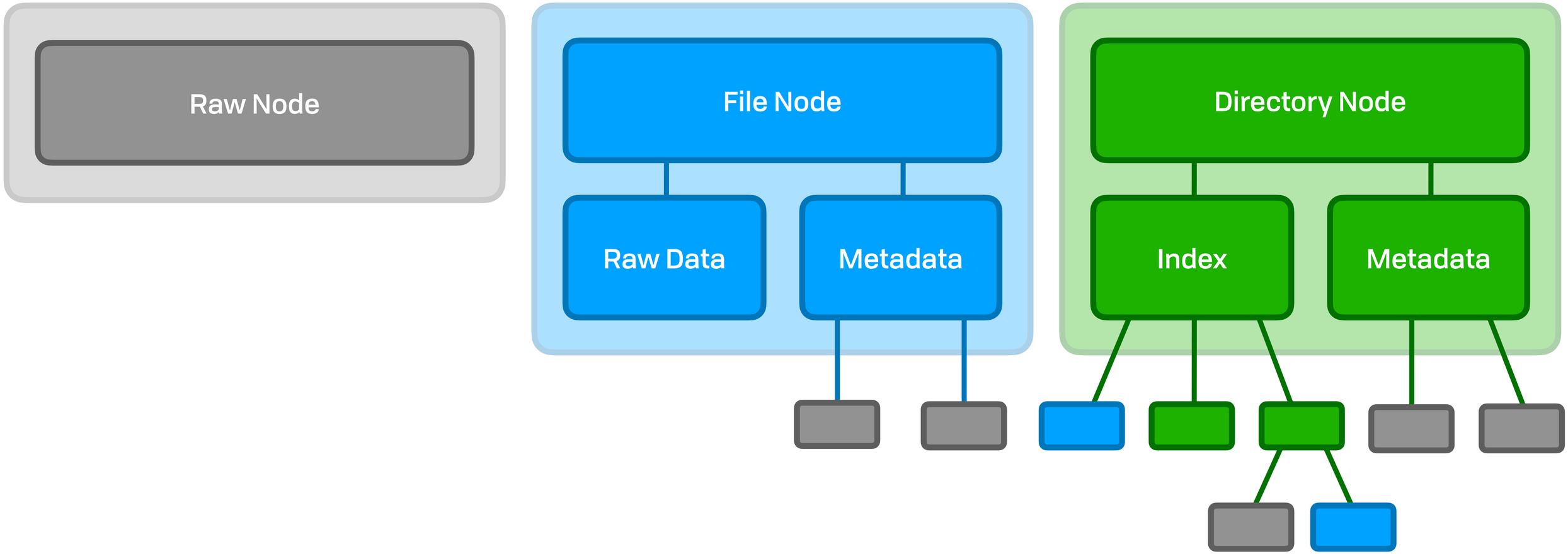
File System

🛠️ High Level Layout



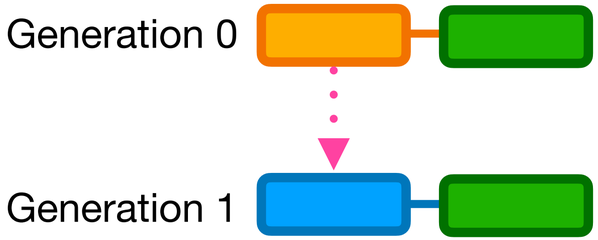
Common Concepts

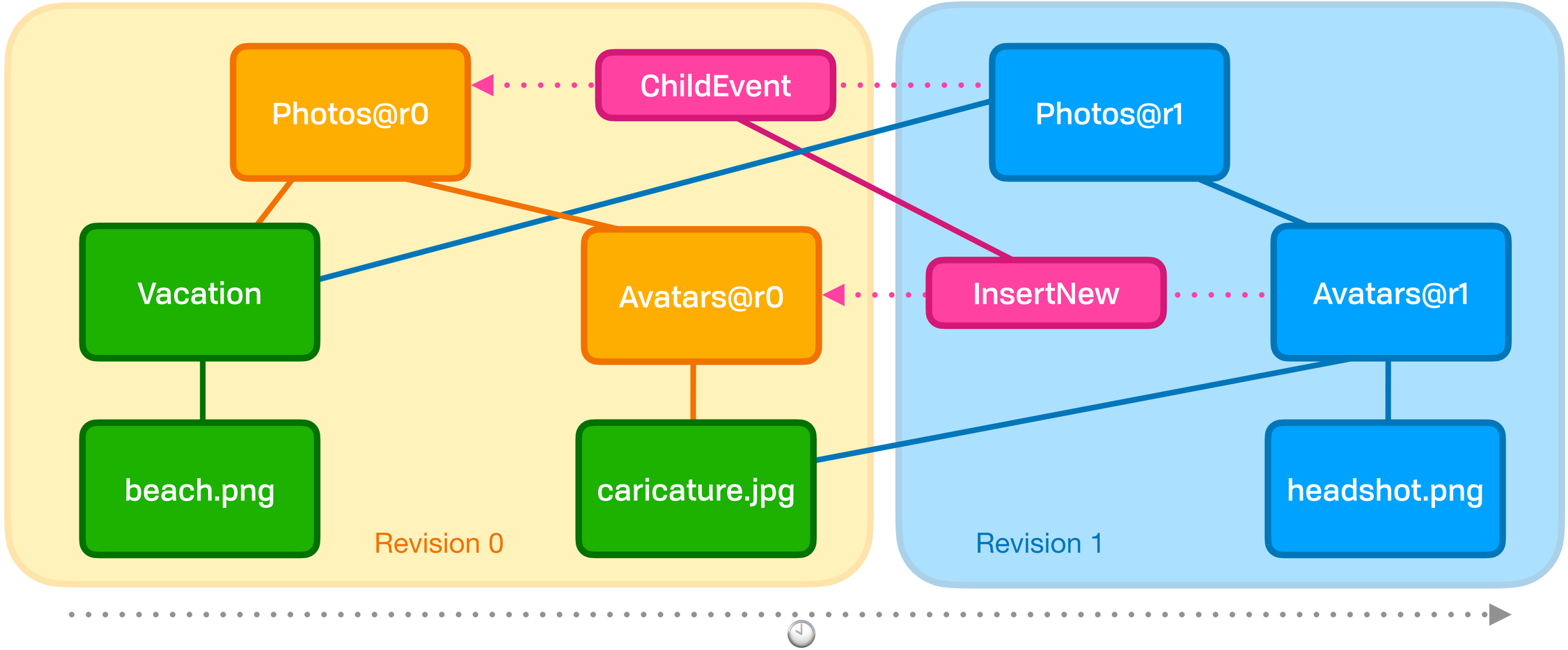
🛠️🌐 Virtual Nodes



File System

🛠️ The z-dimension: versioning & events

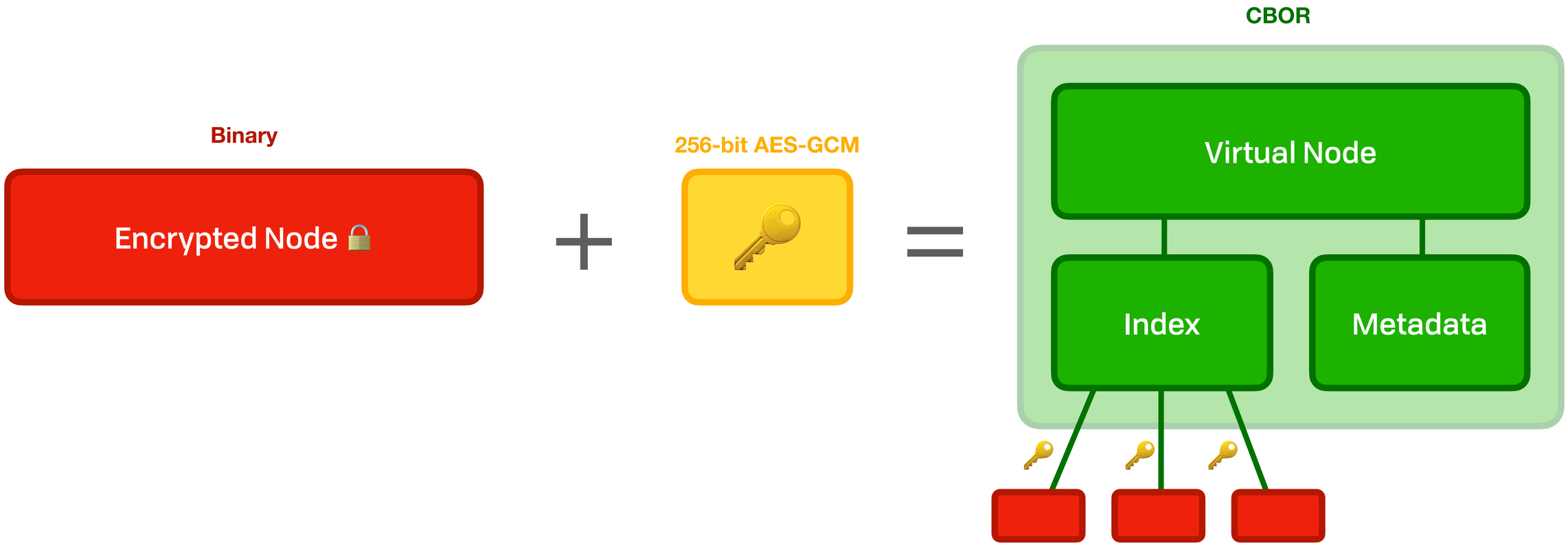




Private Nodes 🤫

Private Nodes

🛠️ Components



Private Nodes

Namefilters

- Constraints:
  - Deterministic
  - Versioned
  - Addressable
  - Prove subpath for UCAN
  - Minimal knowledge
- AES keys ~ path segments *but secret*

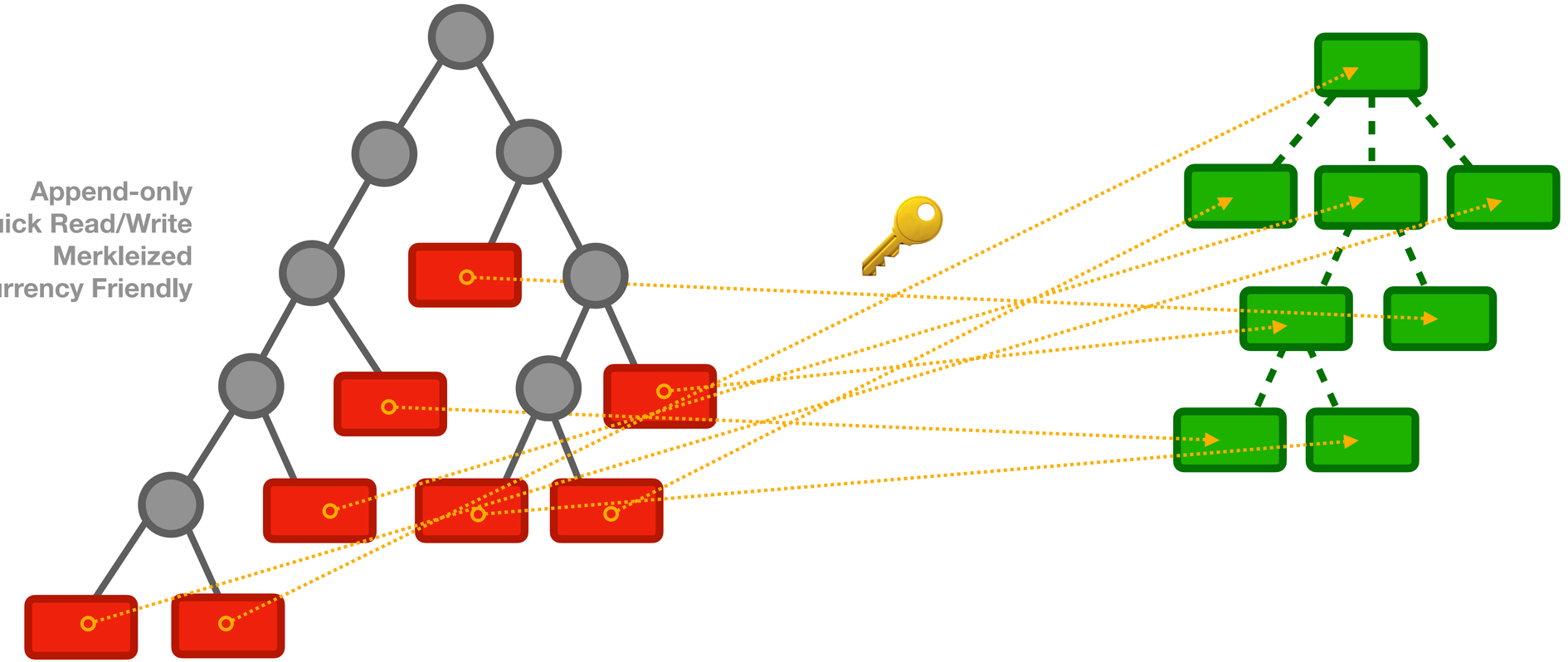
- bareFilter
  - `parentFilter`
    - `AND bloom(SHA(aesKey))`
    - `AND bloom(SHA(aesKey ++ revision))`
- Saturation
  - `nameFilter AND bloom(SHA(nameFilter))`
  - Repeat until threshold bits flipped

Private Nodes

🌐 Private Data Store

Prefix Tree 16^3 = 4,096 items
(weight 16) 16^4 = 65,536 items

Append-only
Quick Read/Write
Merkleized
Concurrency Friendly



Private Nodes

🔐 Serverless Auth in the Browser (UCAN)

- OCAP, provable chains, revocable
- Non-exportable RSA2048/Ed25519