🌈WebNative🚀

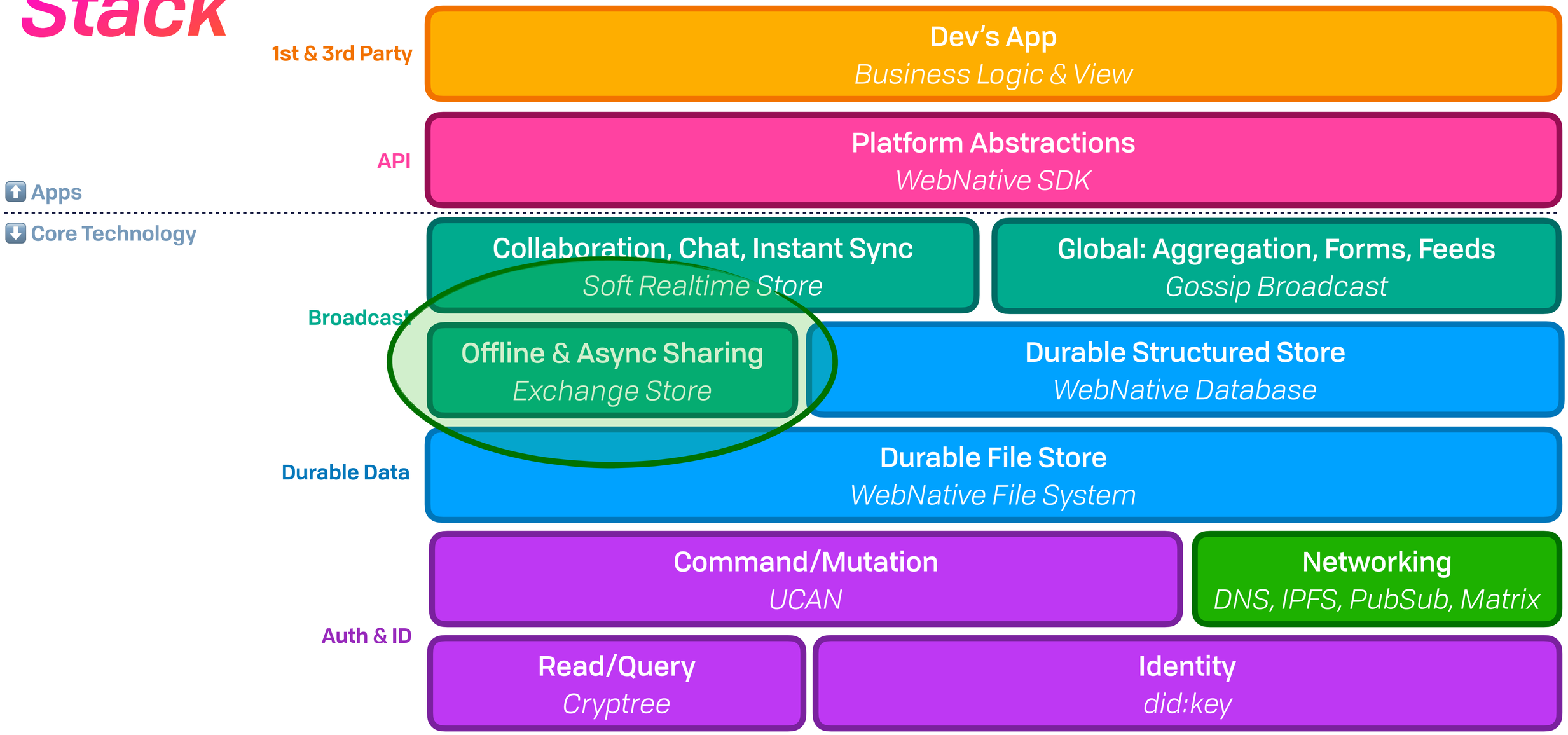
Private File Sharing R&D Preview

A (Super Quick) Primer on the

WebNative File System

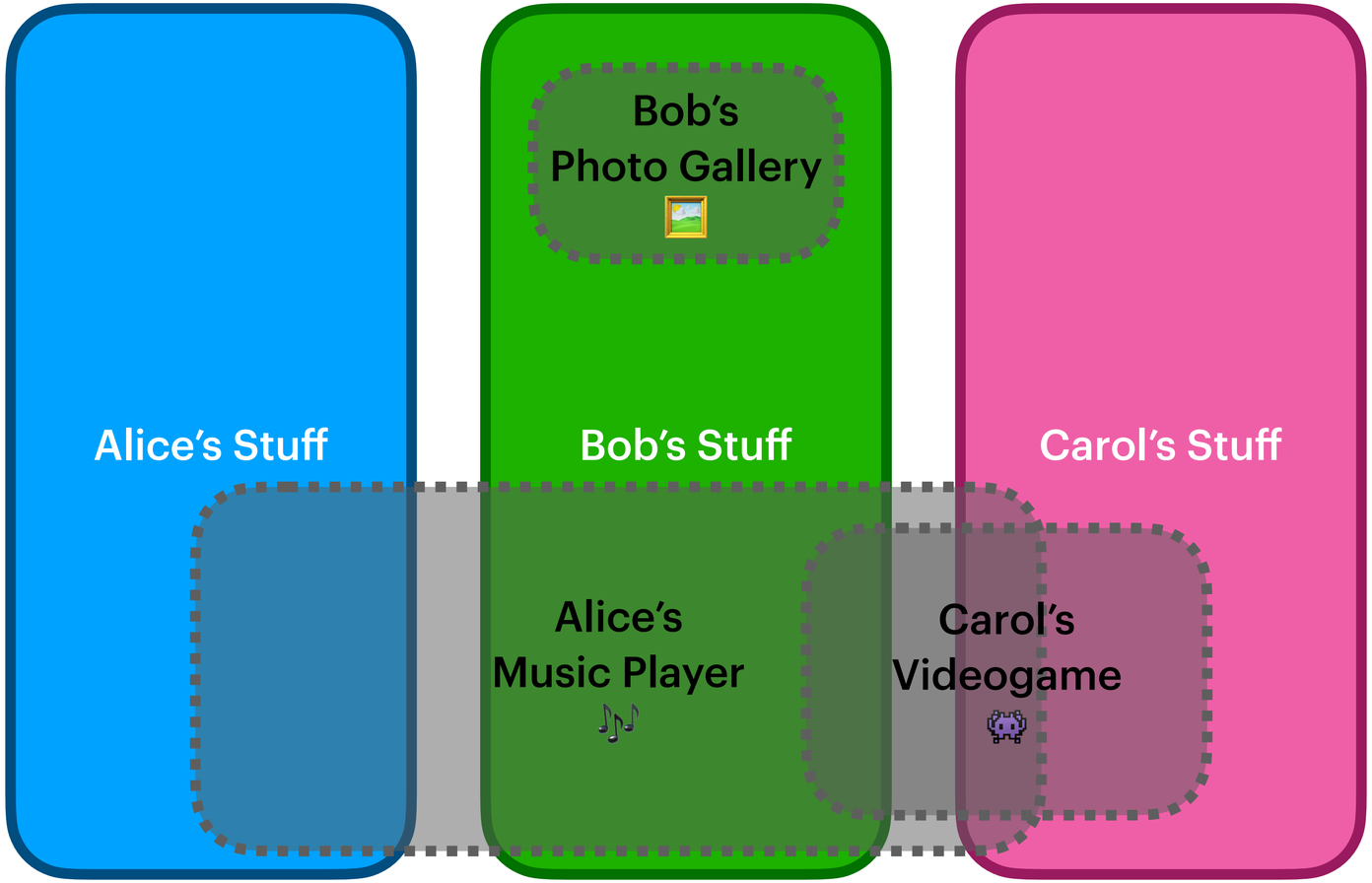
WebNative File System Review

Stack



WebNative File System Review

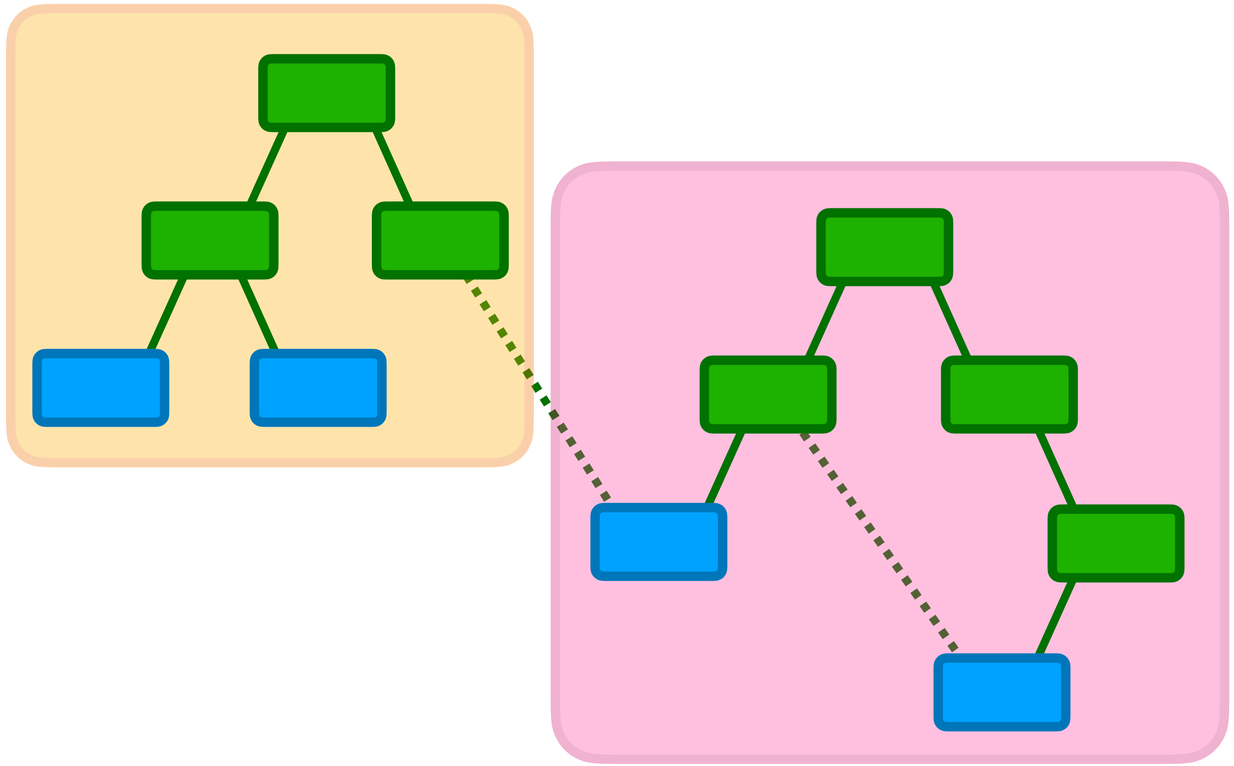
Grouped by User, Not by App



WebNative File System Review

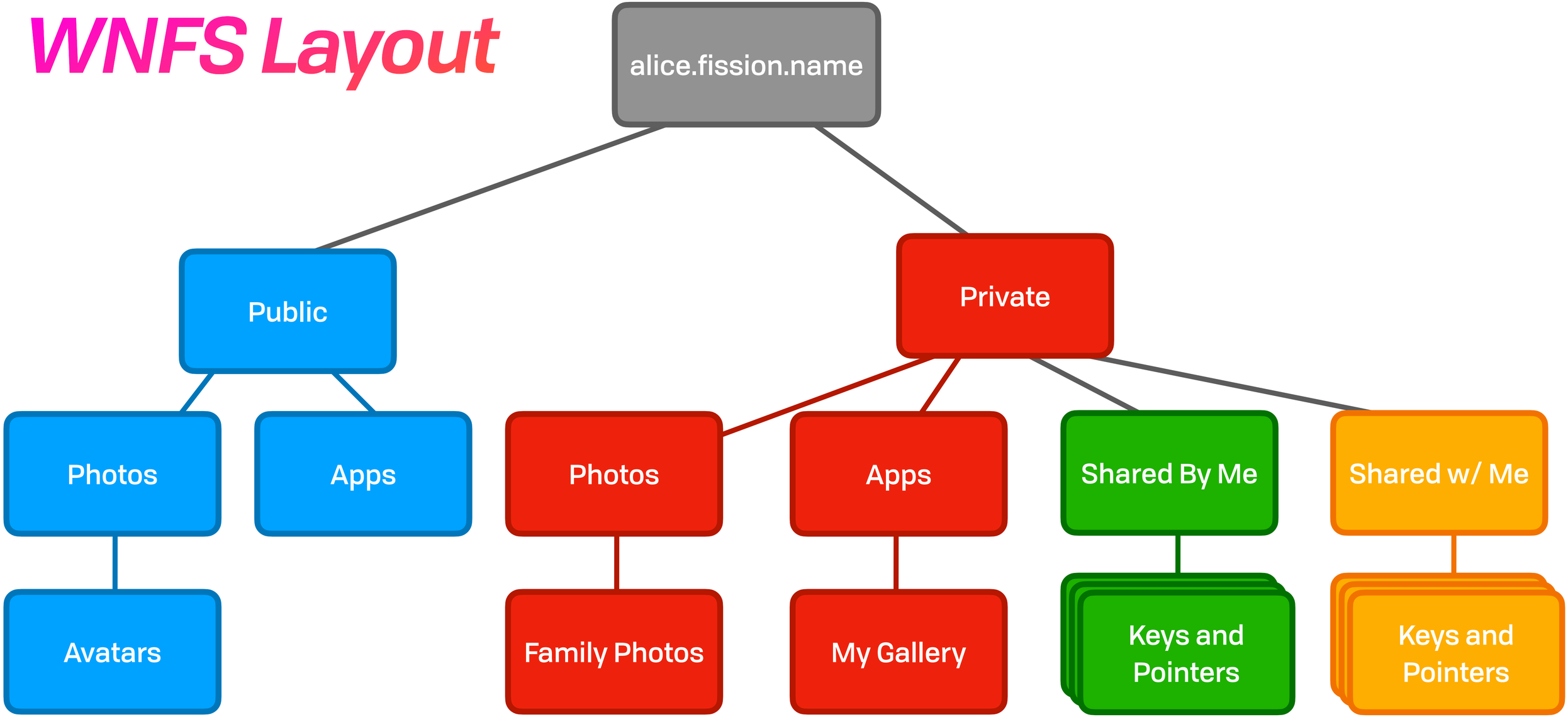
Hard & Soft Links

- Hard links
  - New for the web!
  - Direct reference
  - 2 pointers ~ duplicate
- Soft links
  - Like a symlink or web link
  - 2 pointers ~ latest
  - May break
    - Always some version available



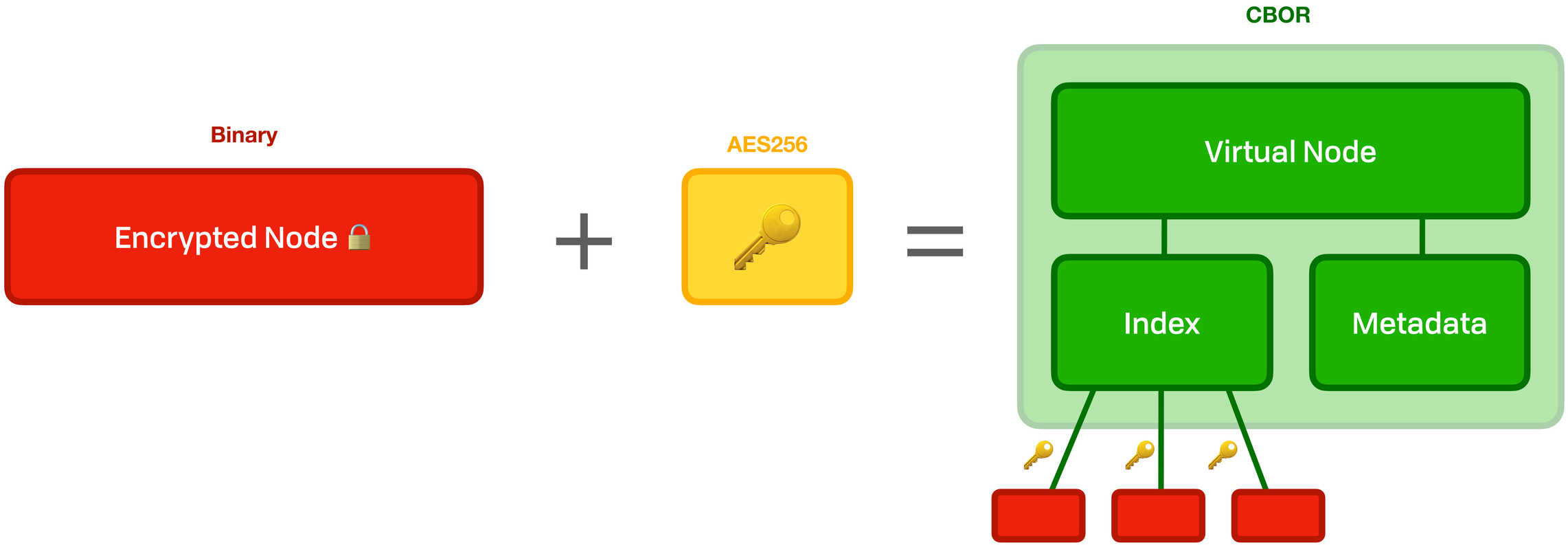
WebNative File System Review

WNFS Layout



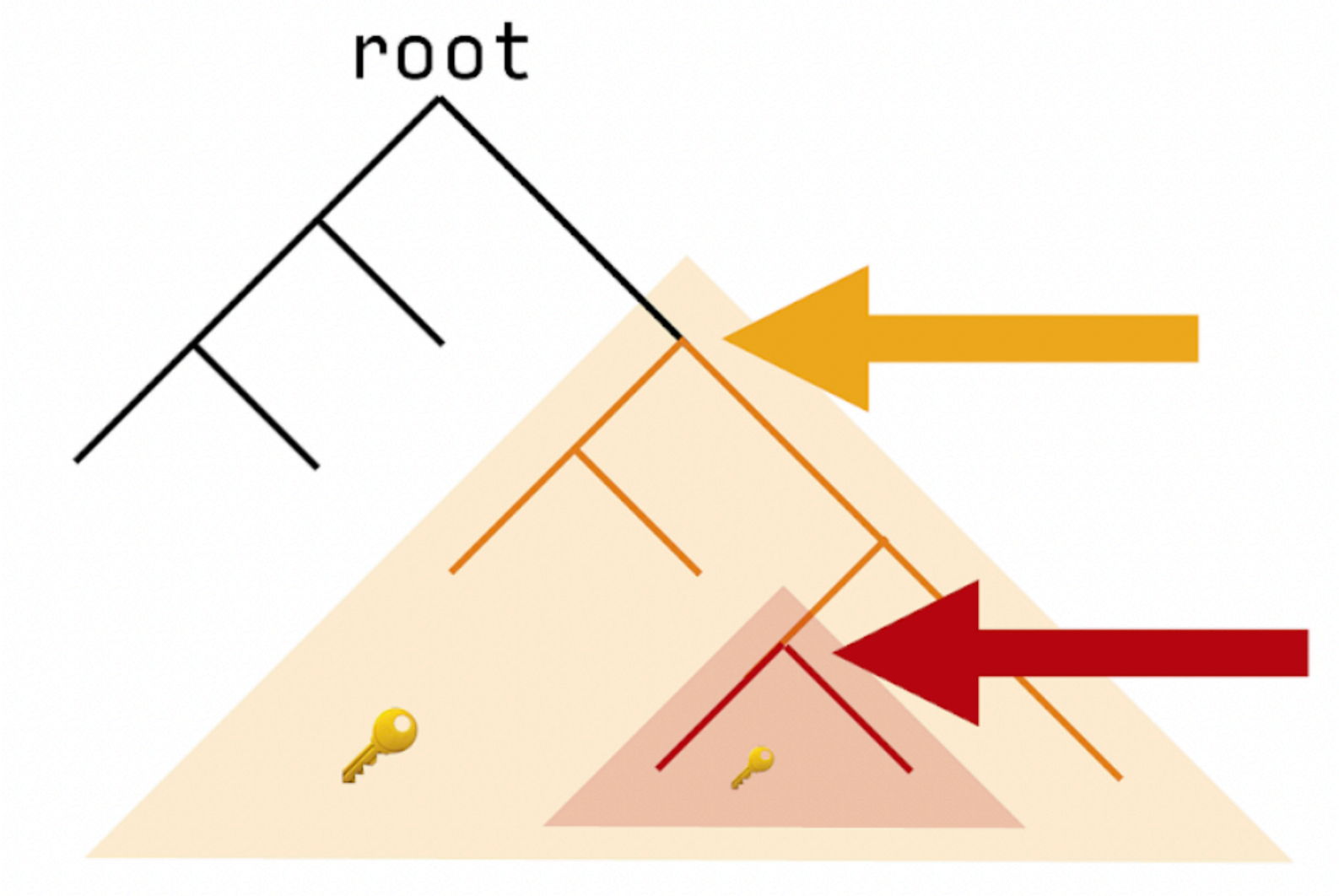
WebNative File System Review

Private Nodes 🙈



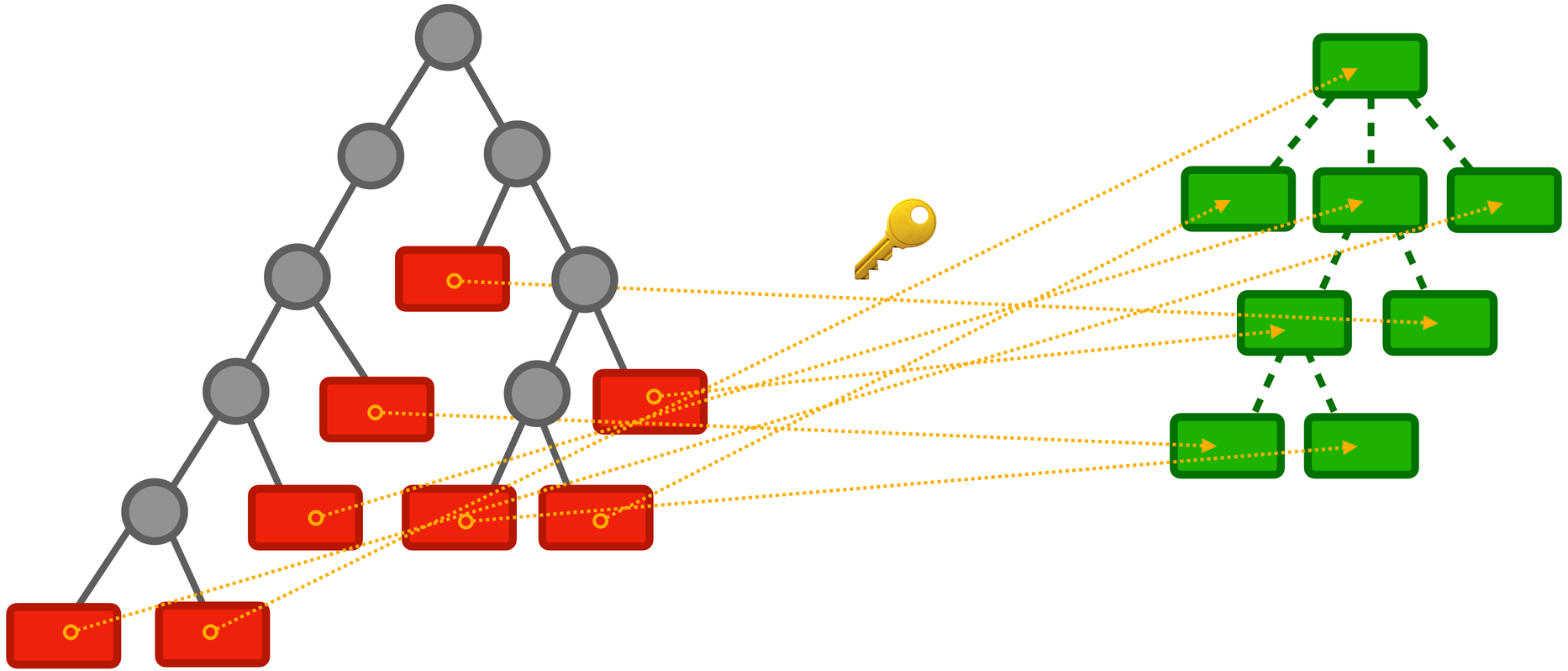
WebNative File System Review

Subtree Read Access



WebNative File System Review

Encrypted Tree Scrambles Structure

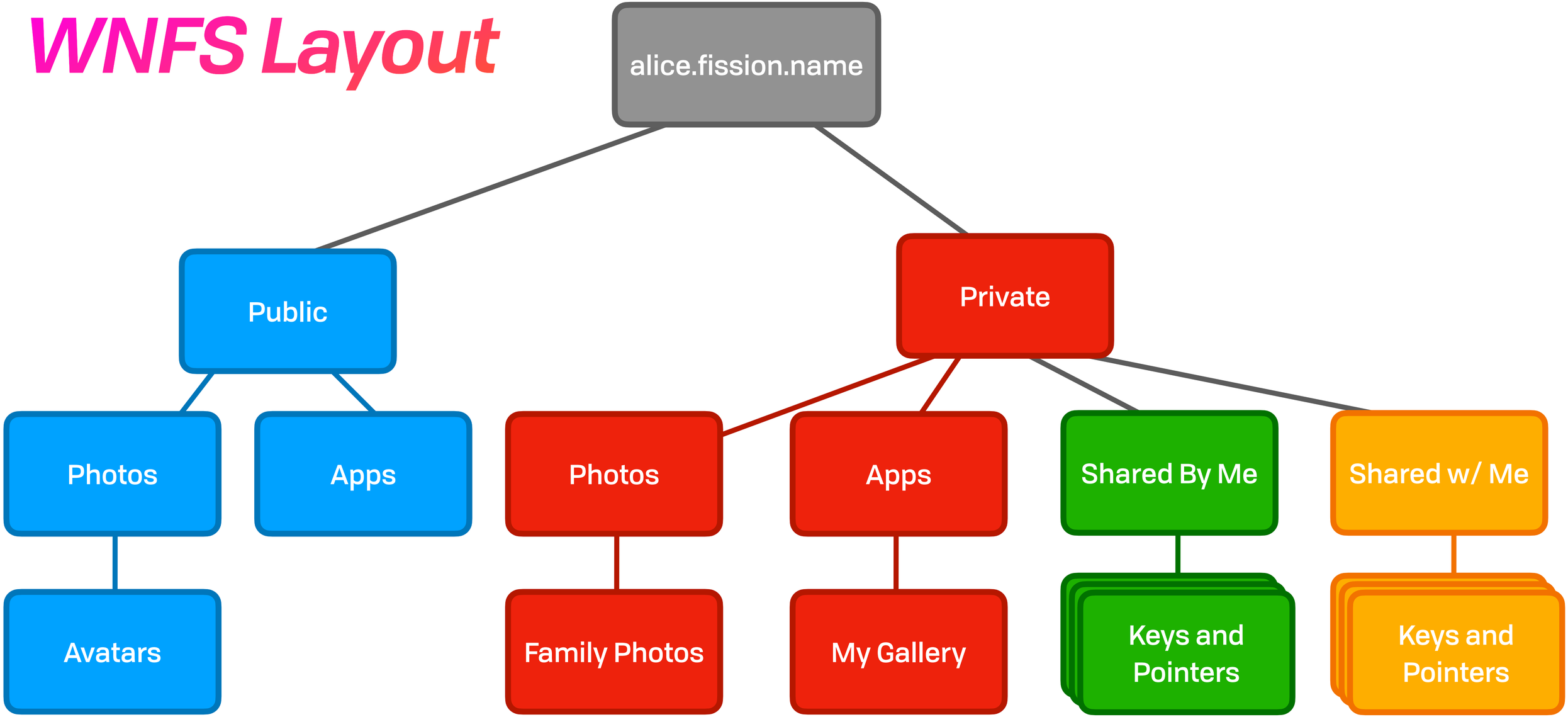


Private File Sharing Mechanics

Fast Async File Exchange

Private File Sharing Mechanics

WNFS Layout



Private File Sharing Mechanics

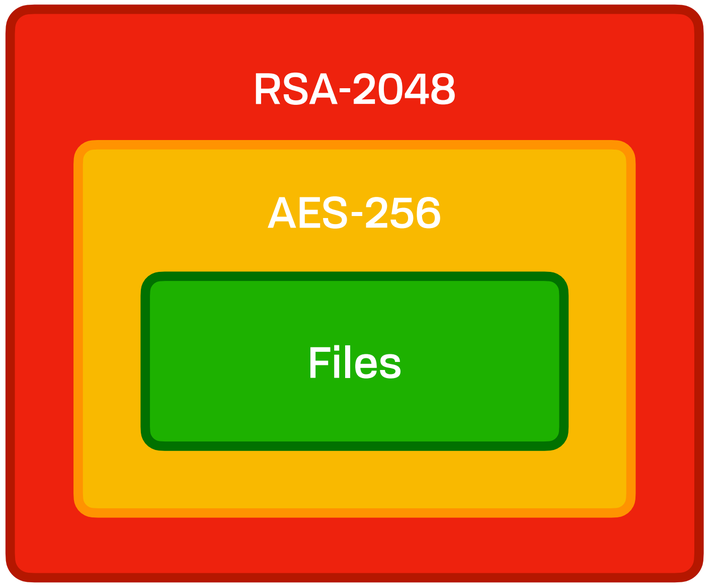
The Problem

- Sharing credentials is trivial when you are both online
- What when a user is offline?
  - Trust keys to a server?
  - Password?
    - That’s less secure & clunky!
    - Requires out of band communications: email / SMS / in person

Private File Sharing Mechanics

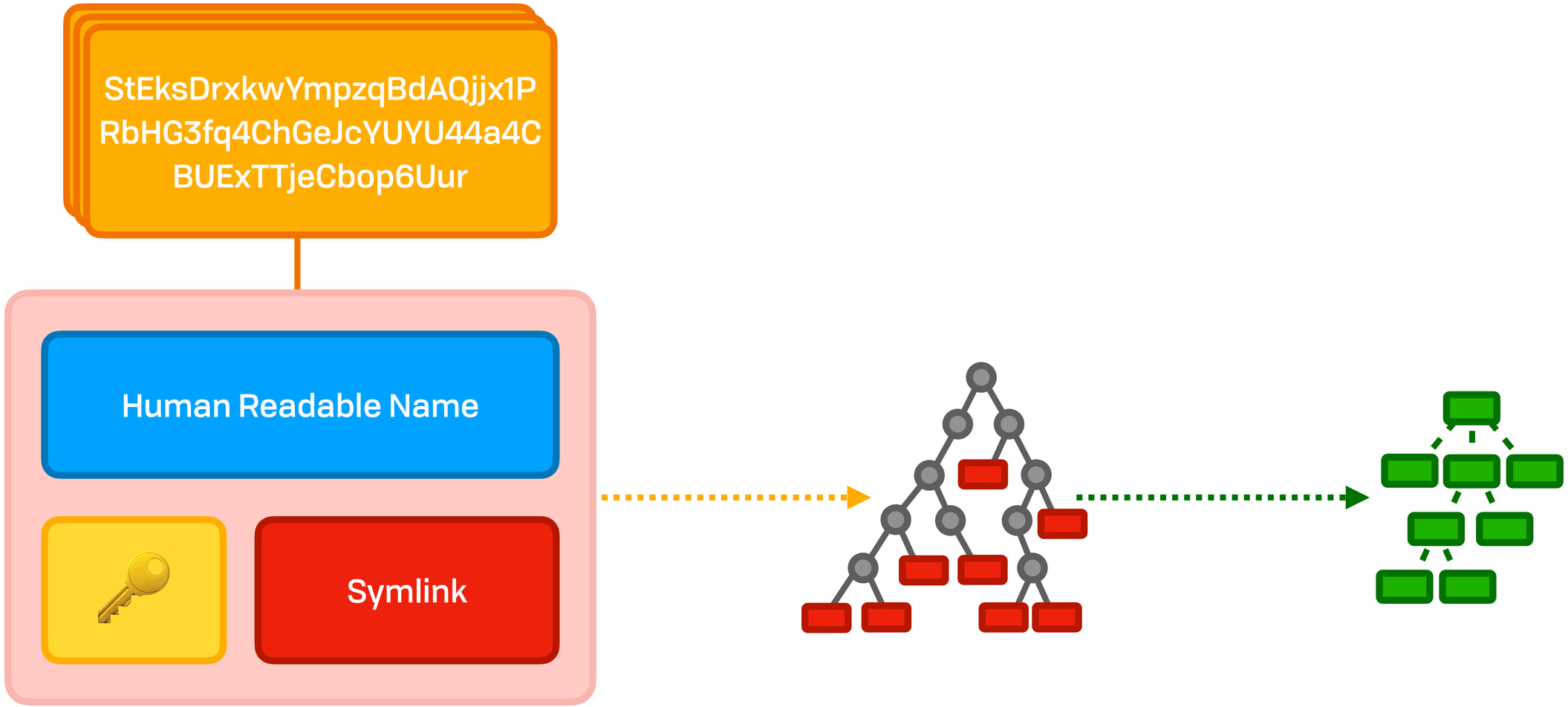
The Solution: Key Exchange 🪆

- DH is very battle tested ⚔️
- Standardize on RSA-2048 (at least for now)
- Contains a 256-bit AES key
- Each device needs its own exchange keys (non-exportable)
- Used ***exclusively*** for exchange (not your main DID key)
  - Exchange key (transfer data)
  - Signing key (sign data)



Private File Sharing Mechanics

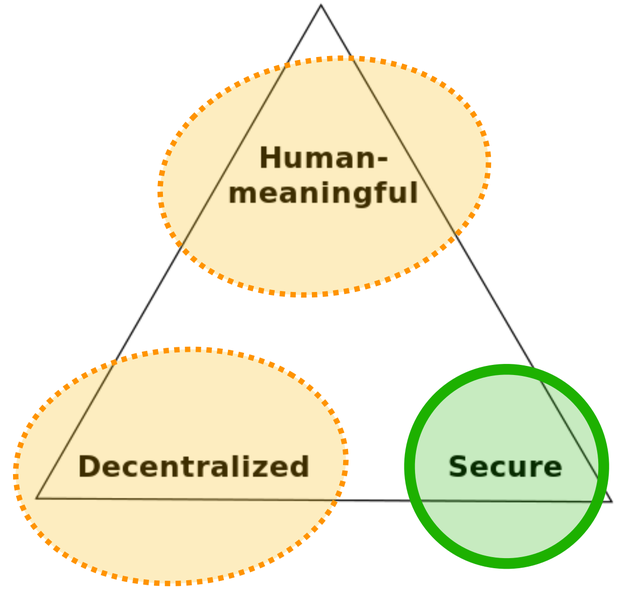
File Sharing



Private File Sharing Mechanics

How to Broadcast Public Keys?

- Use the file system itself!
- Roughly like a `.well-known`
- Public keys are… public (safe to broadcast)
- Deterministic discovery by name
  - DNS (username) ➡️ WNFS(user) ➡️ Exchange Keys



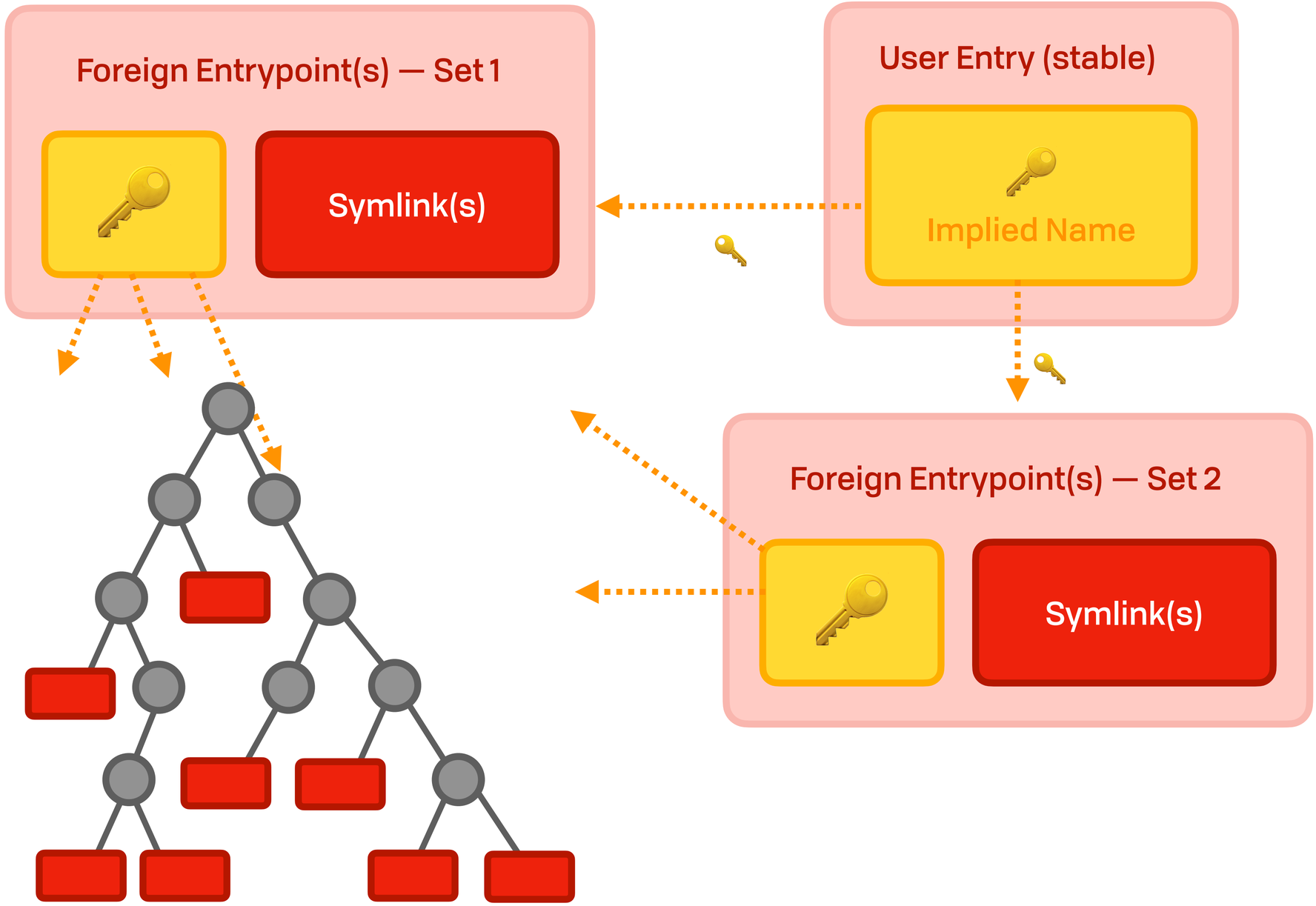
Private File Sharing Mechanics

Plug the Leaks! 🚿

- Store in private the same tree as the private file system
- Index name is different / the space is huge
  - More than the number of atoms in the known universe 🌌
- `hash(${senderExchangeKey}${recipientExchangeKey})`
- You know all of your keys, and all of their keys
  - `O(|recipientKeys|)` creation, `O(|senderKeys|)` lookup
  - Typically in low single digits, fast on human time scales, infrequent

Private File Sharing

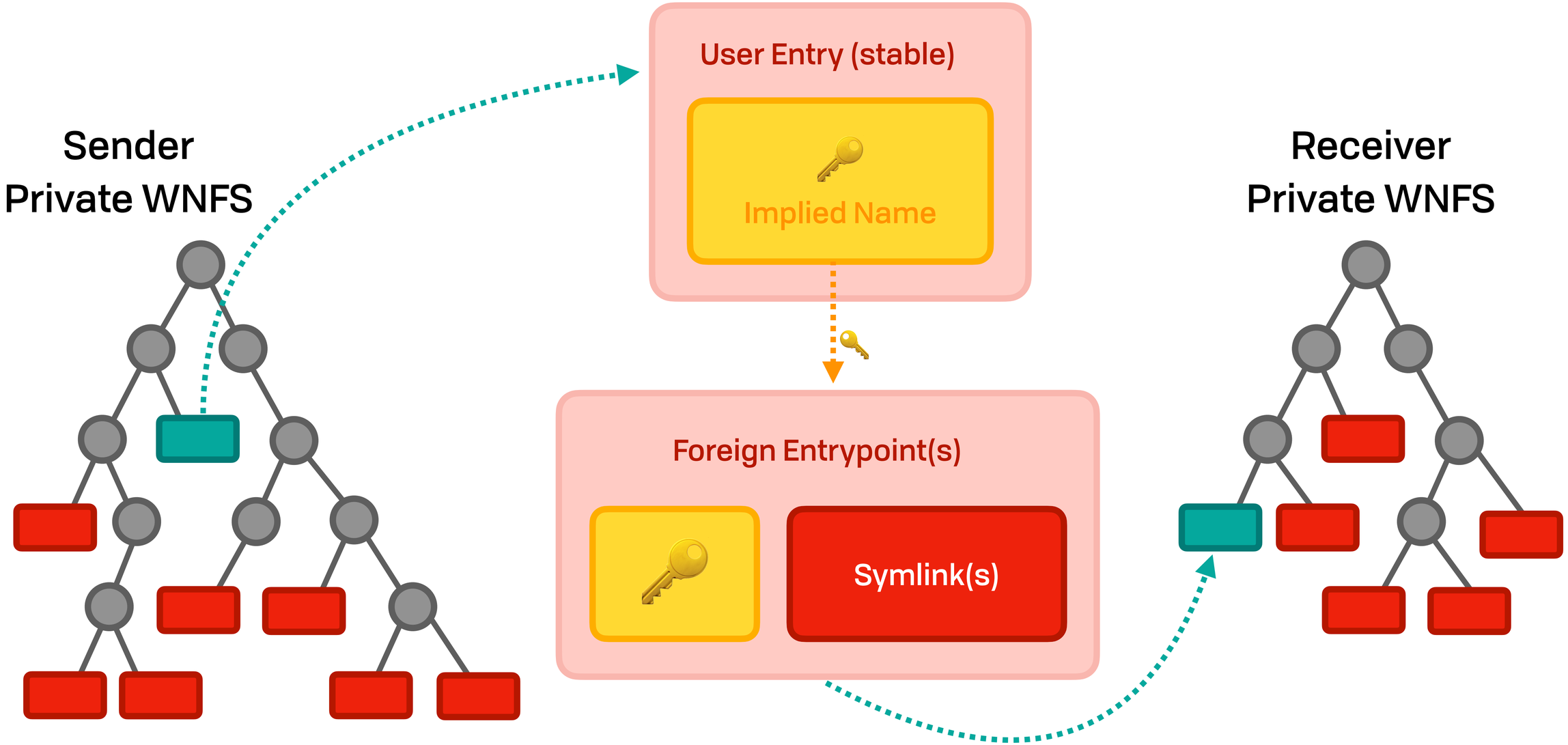
Lookup



- Entrypoint names:
  `hash(encryptAES(${impliedName}${setVersion}))`

Private File Sharing Mechanics

Don't You Forget About Me 🎶



Private File Sharing Mechanics

What Does This Get Us?

- Async sharing
- Secure
- Performant
- Automated discovery of new files
- Key based
- Possible to do anonymous link-based sharing
- Builds on existing WNFS implementation

😄 Thank You 🎉