BLOCKCHAIN COMMONS

INTEROP: WHAT IS IT GOOD FOR?

WHAT IS BLOCKCHAIN COMMONS?

- We are a community that brings together stakeholders to collaboratively build open & interoperable, secure & compassionate infrastructure.
- We design decentralized solutions where everyone wins.
- We are a neutral "not-for-profit" that enables people to control their own digital destiny.

interoperate (v.)

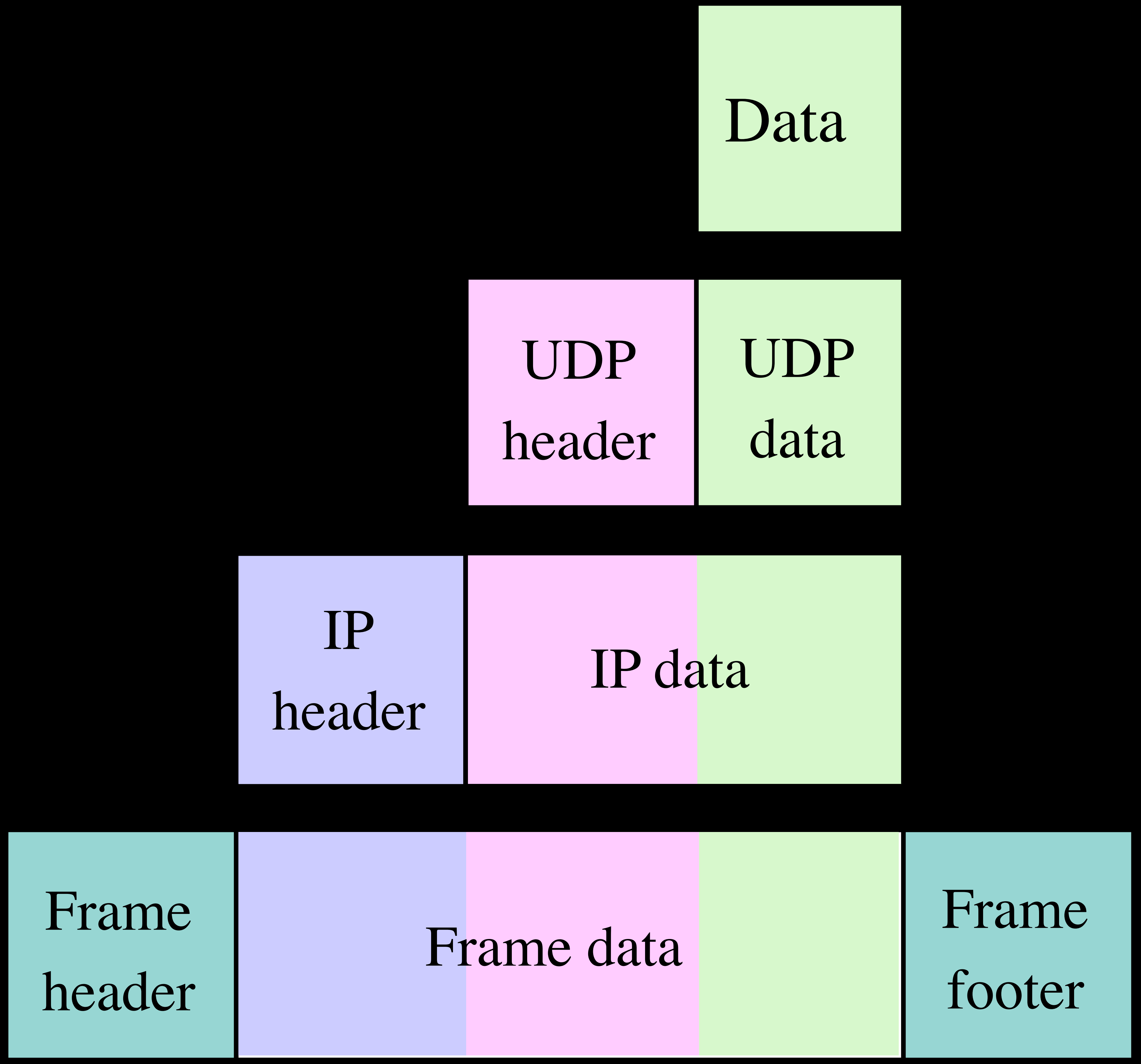
“to work in conjunction with each other”

—Oxford Languages

The Internet is Built on Interop!

But It's Limited!

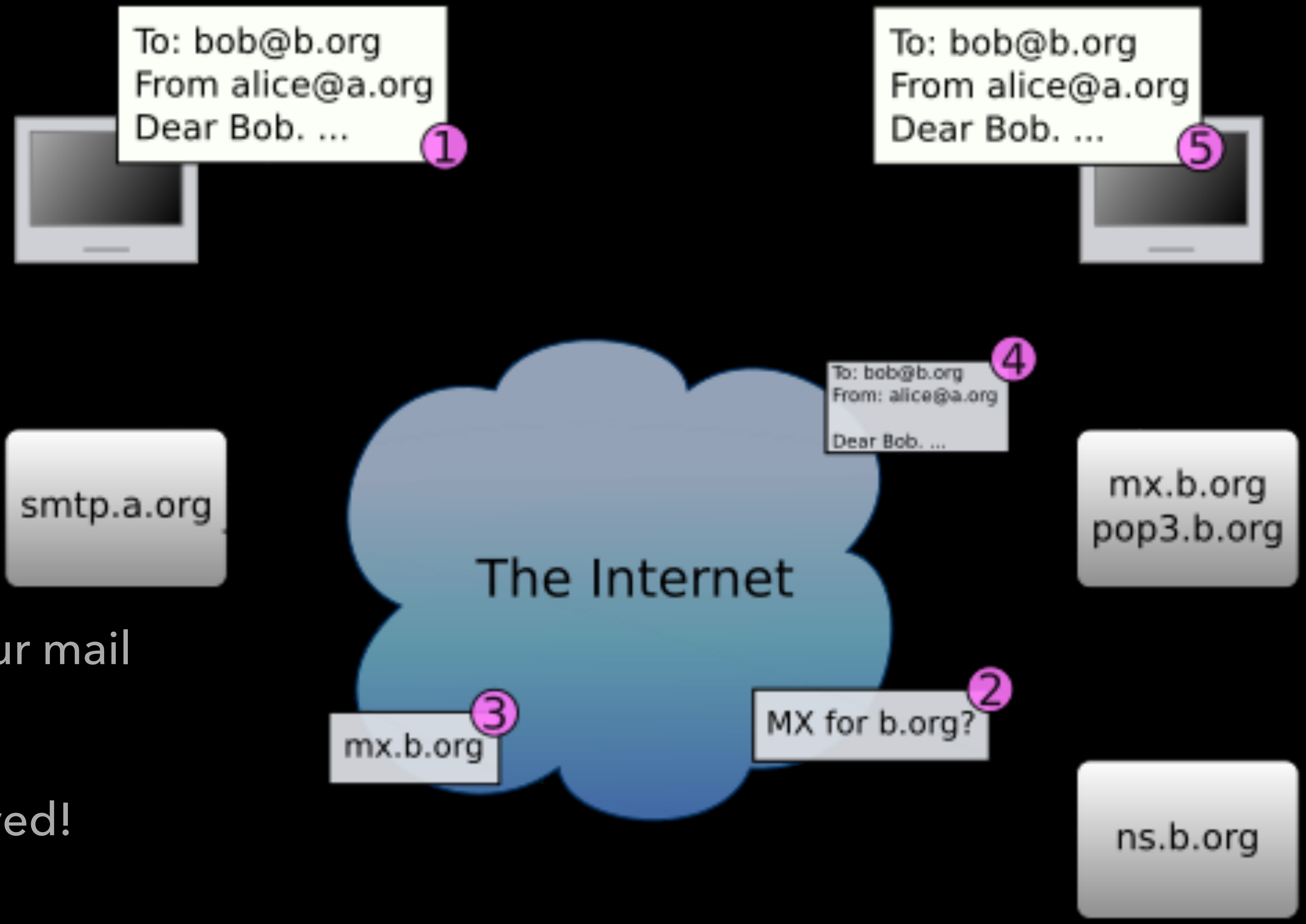
- Interop Has Mainly Focused on Communication
  - UDP
  - TCP/IP
  - FTP
  - HTTP
  - TLS
- But Interop Should Extend Much Further



Internet Interop is Limited

Take Mail as an Example

- Communication? No Problem!
  - DNS, TCP/IP, SMTP
- Storage? Mixed Protocols.
  - mbox, eml, msg
- Filtering? Ha!
  - You can use DKIM, DMARC, SPF.
  - But you can't be sure Gmail won't mark your mail as spam!
  - And then it doesn't matter if your mail arrived!
  - That's an Interop FAILURE.

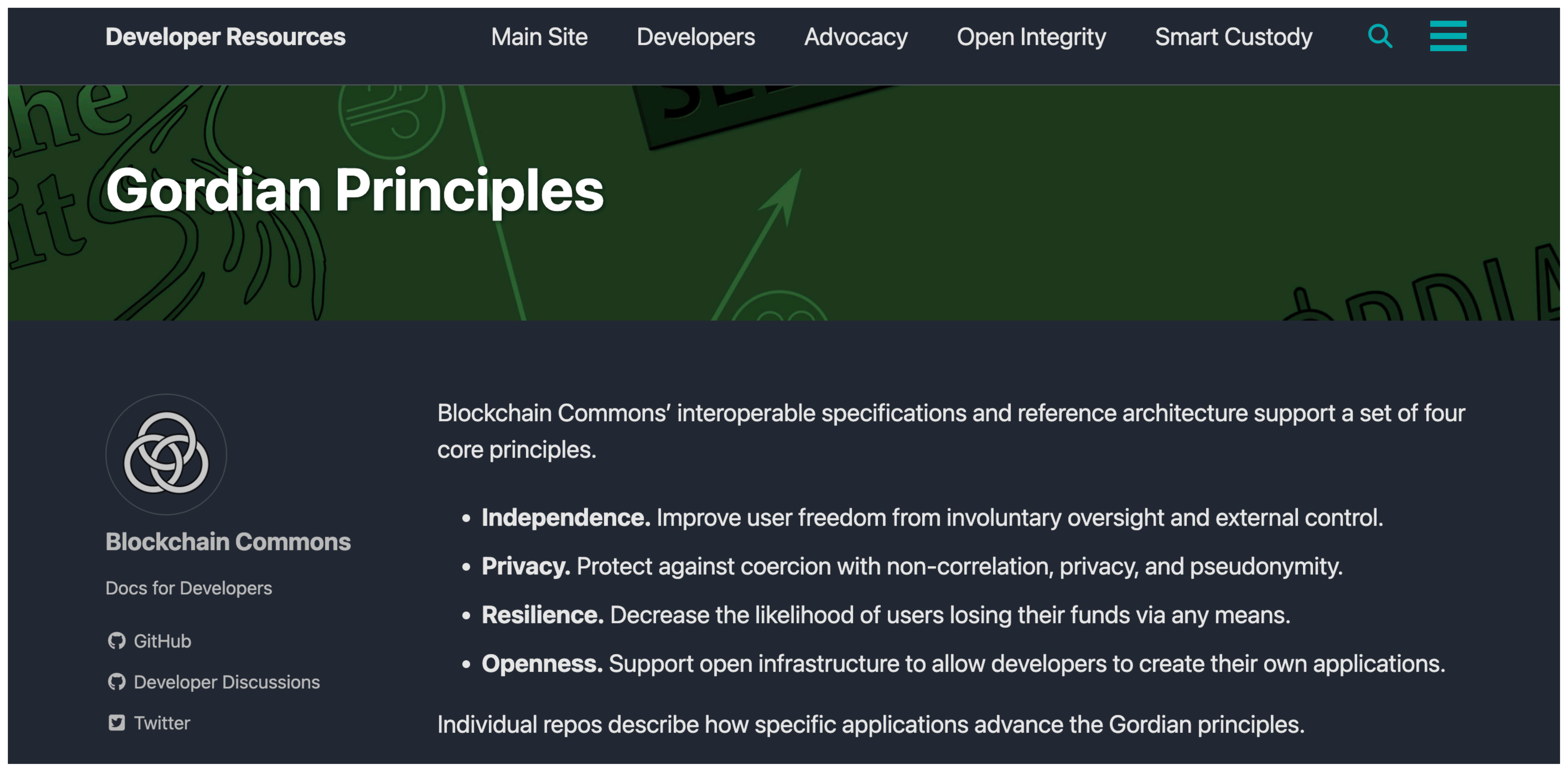


Any gap in interoperability
Endangers all interoperability

Why We Think Interop is Important

It's the Gordian Principles

- Independence
- Resilience
- Openness



Gordian Principles

Blockchain Commons' interoperable specifications and reference architecture support a set of four core principles.

- **Independence.** Improve user freedom from involuntary oversight and external control.
- **Privacy.** Protect against coercion with non-correlation, privacy, and pseudonymity.
- **Resilience.** Decrease the likelihood of users losing their funds via any means.
- **Openness.** Support open infrastructure to allow developers to create their own applications.

Individual repos describe how specific applications advance the Gordian principles.

Why We Think Interop is Important

Independence (for Users)

- Users can exchange & export data from an app or service & use it elsewhere
- They're not trapped on a single platform
- Instead, they choose an option that meets their needs

GORDIAN

Why We Think Interop is Important

Resilience (for Data)

- Data Format is Well-Known
- Data Format is Well-Understood
- Far-Future Recovery is Likely
- Try to Recover a Wordstar File
  to See the Importance!

GORDIAN

Why We Think Interop is Important

Openness (for Creators)

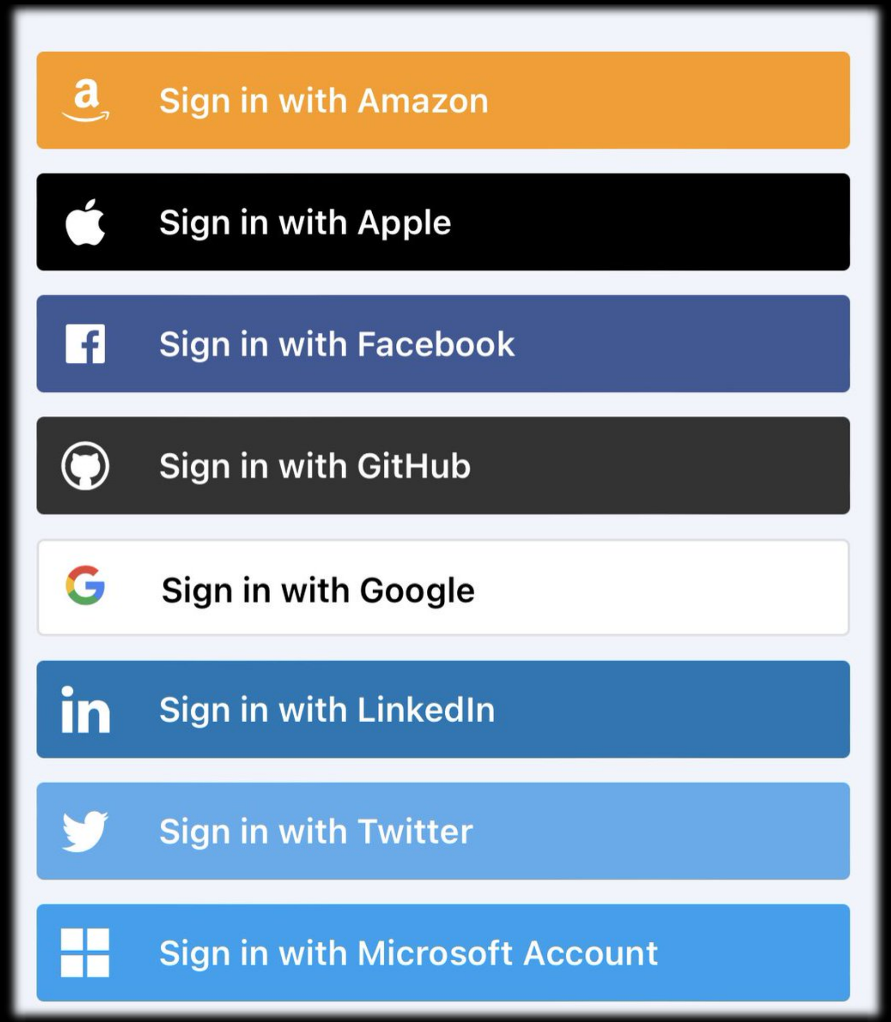
- New Creators Can Easily Join Ecosystem.
- They Bring Innovation.
- Creates a System of Coopetition.
    - Cooperative Competition

GORDIAN

Why We Think Interop is Important

Oh, and Openness Helps Users Too

- Without Openness You Have the NASCAR Problem.
- Long Lists of Choices.
  - Each is an Non-Interop Protocol.
- This is Terrible for Users.
- It Also Prevents Meaningful Automation.



The Failure of OpenID Led to This Mess

Cooperate to interoperate

Compete to be elite

Major Bitcoin Interop Successes

Over a Dozen Adoptions

- URs
- Animated QRs
- SSKRs

URs & Animated QRs

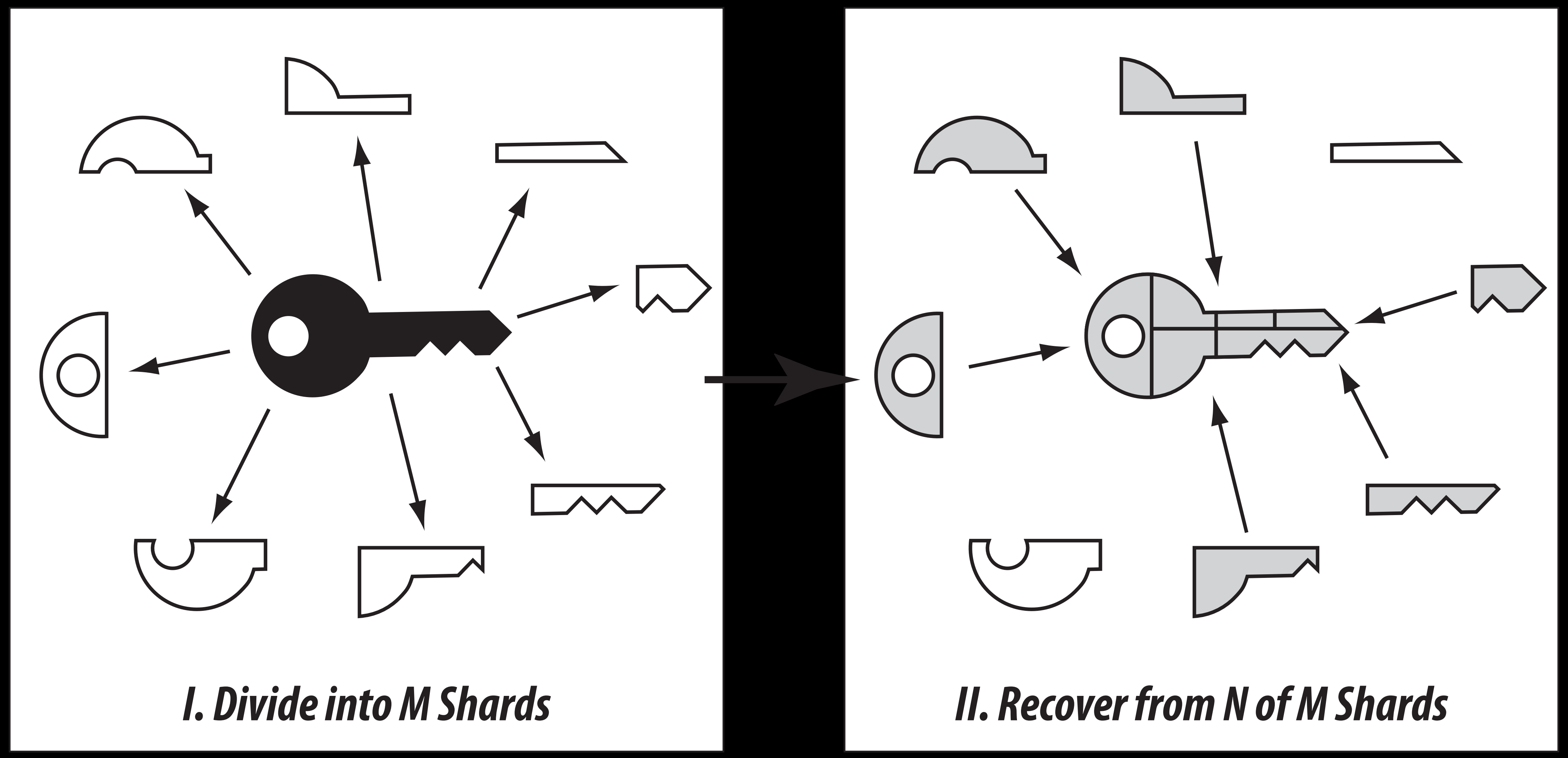
(That's Uniform Resources)

- A Pretty Typical Interop
    - About Communication
- URs Are CBOR Encoding Method
    - Allow Creation of Animated QRs
- Offered Something Not Available
    - Large Data Across an Airgap
- That's How an Interop Spec Is Adopted

SSKRs Show the Wider Power of Interop

(That's Sharded Secret Key Reconstruction)

- Standard Way to Divide (Shard) a Seed
- Currently: Shamir's Secret Sharing
- Why Is the Interop Important?
    - Allows for CSR
        - Standardized on Different Apps
        - Different Servers Store Shares
    - Allows for Recovery
        - Need Your Share in 10 Years?



Interop Specs Can Build on Each Other

The More You Have, The More They Work Together

- We've long worked with Foundation
- They've adopted many of our specs
  - URs, Animated QRs, SSKR, Envelope, Request/Response, GSTP
- It's allowed their focus on higher-level needs:
  - QuantumLink: secure, quantum-resistant bluetooth communication
  - Interop specs enabled their work!

Our Newest Interop Was With Zcash

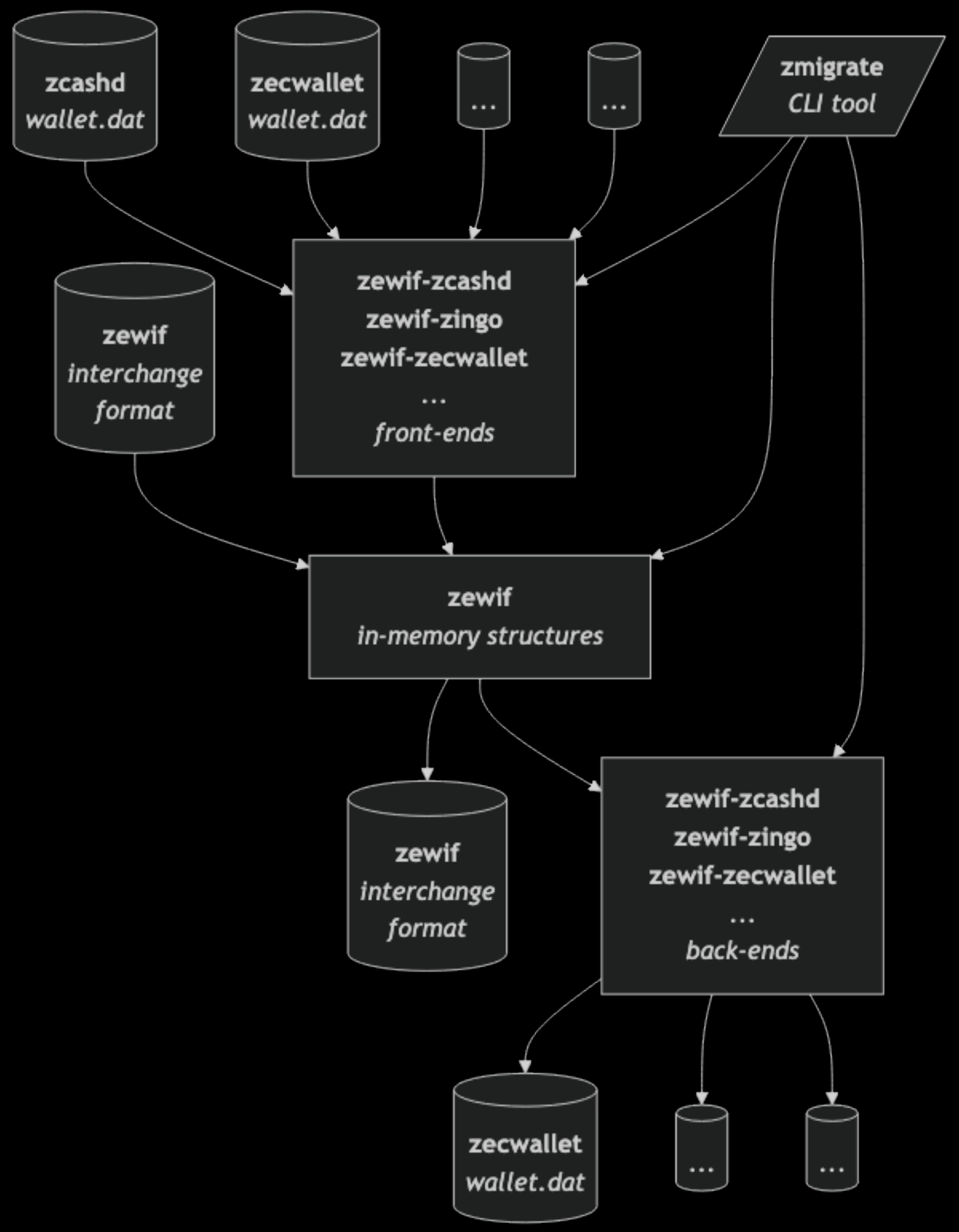
ZeWIF: Zcash extensible Wallet Interchange Format

- Zcash Needed to Deprecate Zcashd server
  - Users had to move wallet data
- Zcash Community saw the bigger picture
  - A way to exchange data among all wallets
  - A way to recover previously lost data
  - A way to keep data safe into the far future

Zcash Work Demonstrated Complexity of Interop

It Can Take a Lot of Connections!

- ZeWIF Creates an In-Memory Structure
  - Represents Wallet Data
- But We Need to Import From Many Places
  - And to Export to Many Places
- We also Had to Design a Data File Format
  - (Fortunately We Had Envelope)
- Ultimately ZeWIF is a TOOL for Interop

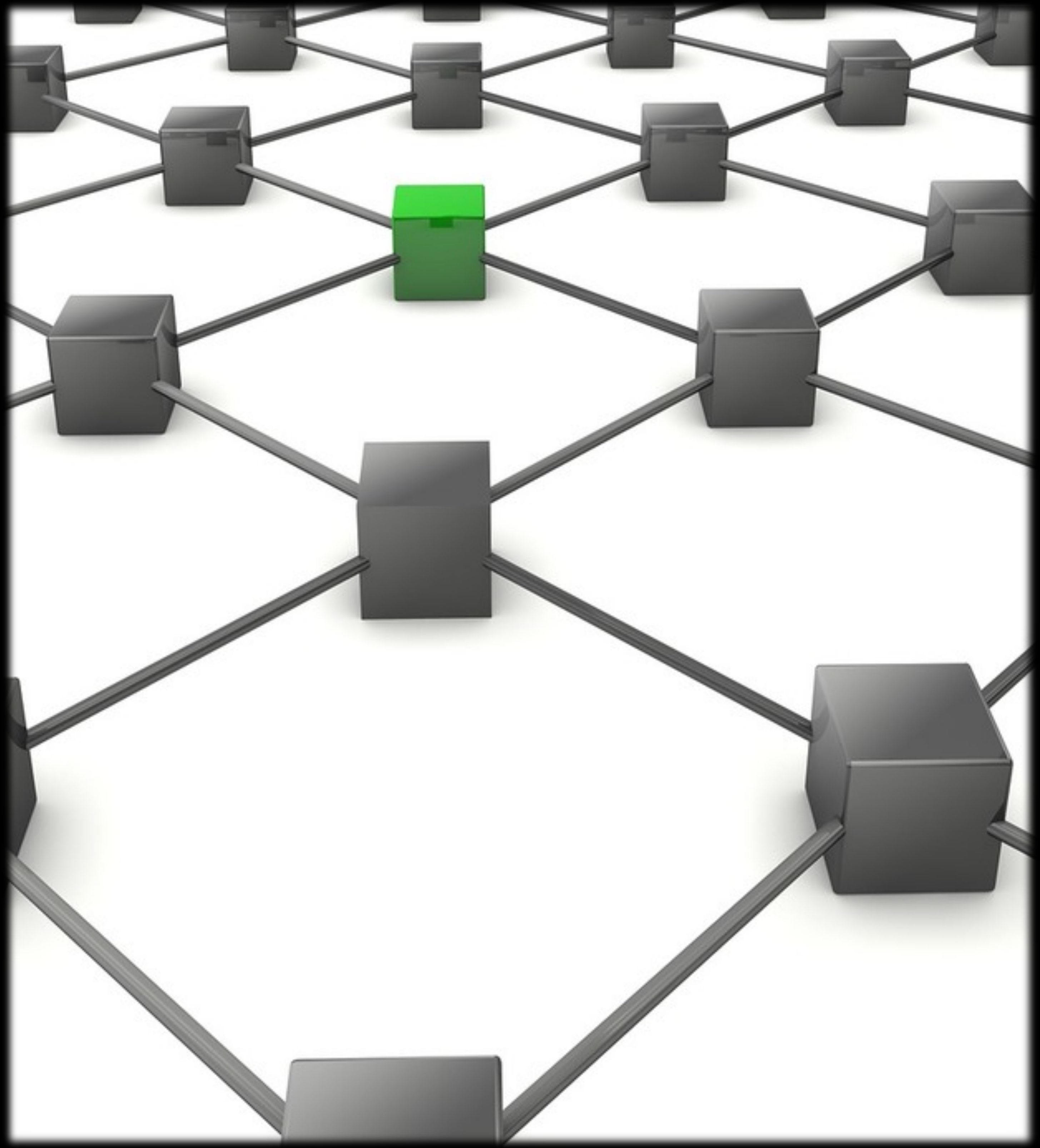


Users May Not Notice Interop But They Will Notice Its Absence

Why Interoperate?

Or: What's It Good For?

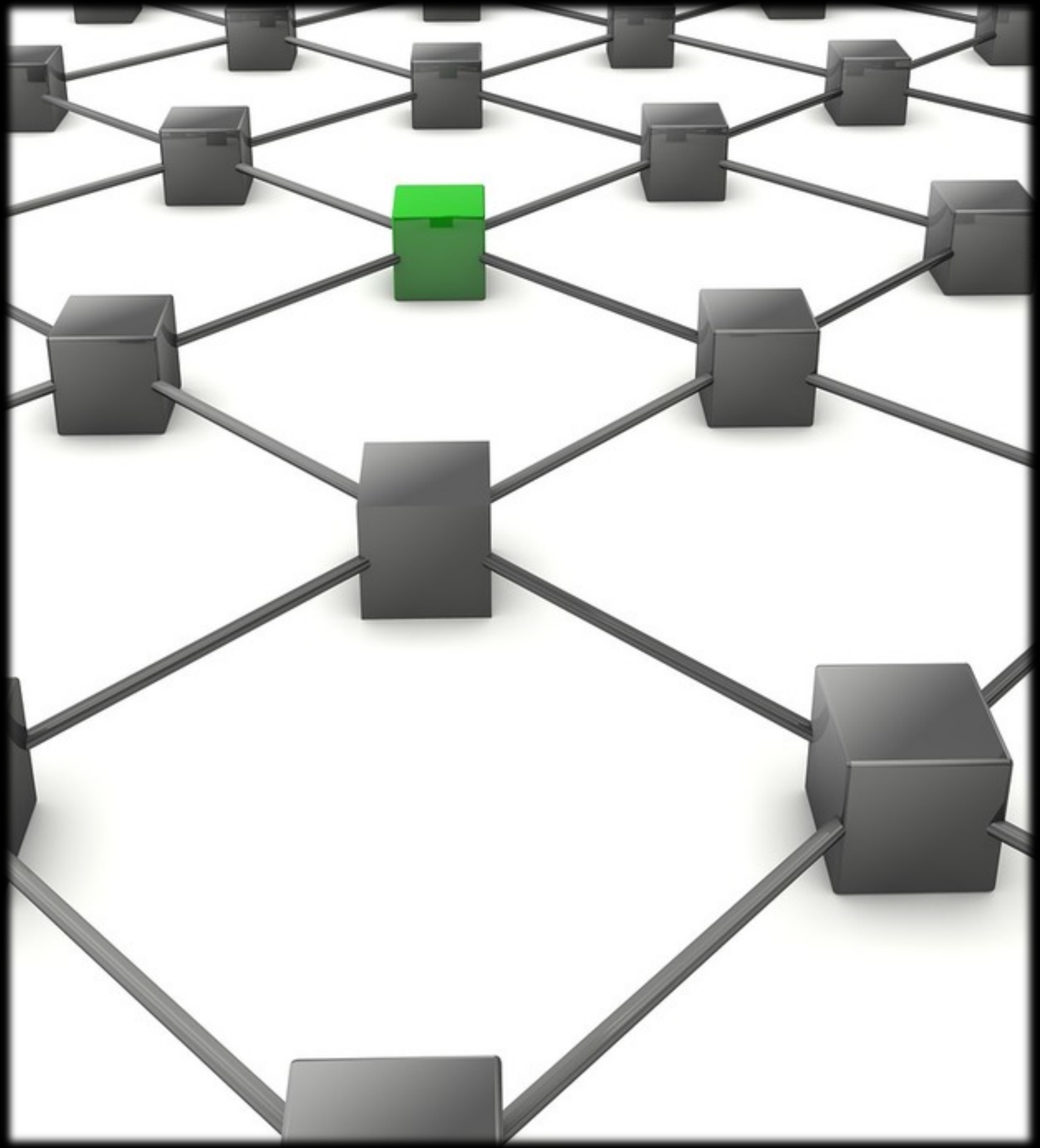
- If You're NOT the Market Leader
  - It Gives You an In
- If you ARE the Market Leader
  - It Supports Your Users
- If You Have Sensitive Data
  - It Makes It Easier to Recover



What’s the Most Important Element for Interop?

Community Support!

- Community Has Expertise.
- Community Understands Deployment.
- Community Can Do Testing.
- Community Ultimately Makes a Spec a Success.
- (It’s All About the Community!)
  - Which is to say You. Thank you!

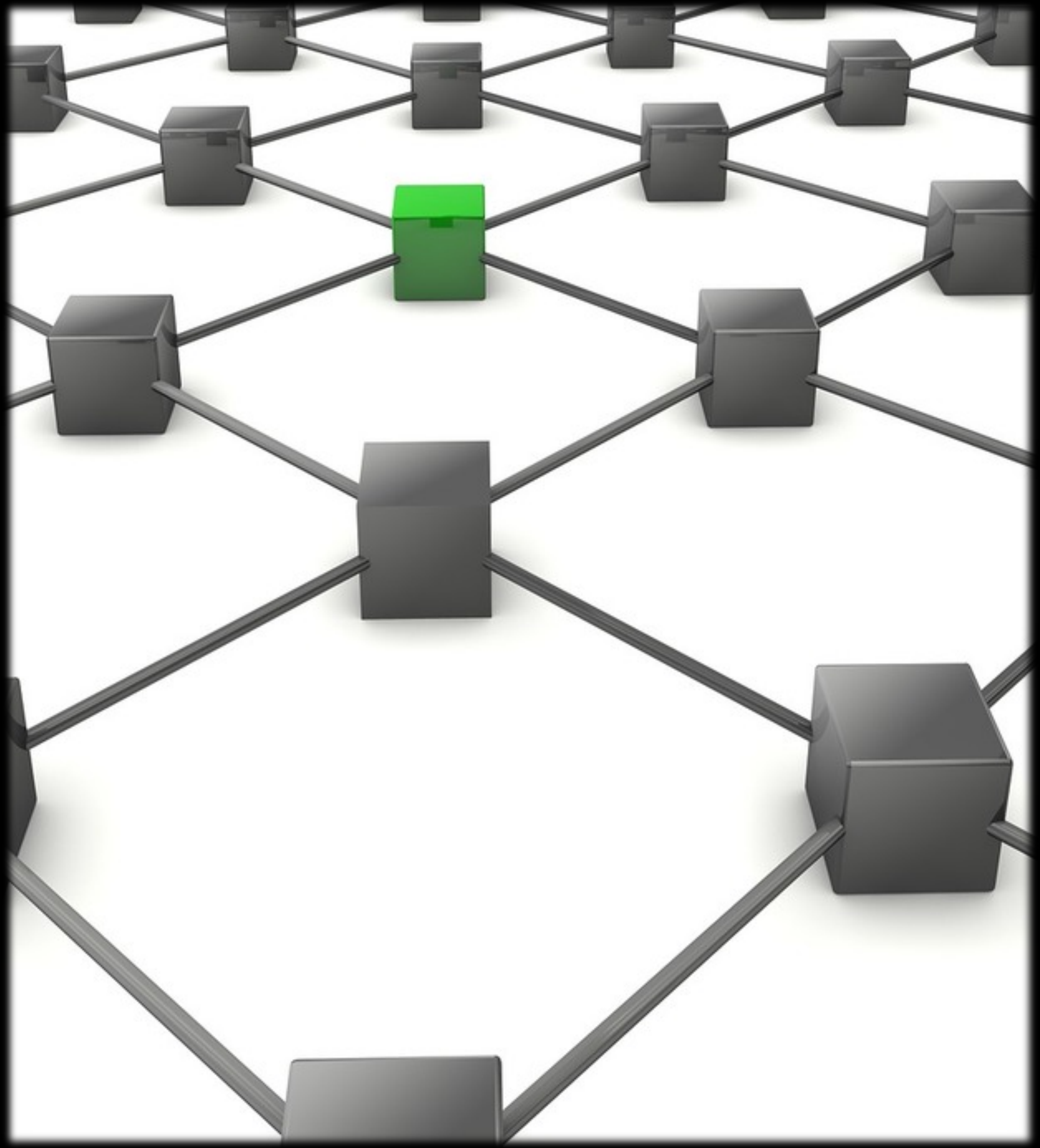


Without Community Buy-In, Interop Will Fail.

How Blockchain Commons Builds Specifications

(Our Standard Methodology for Supporting Interop)

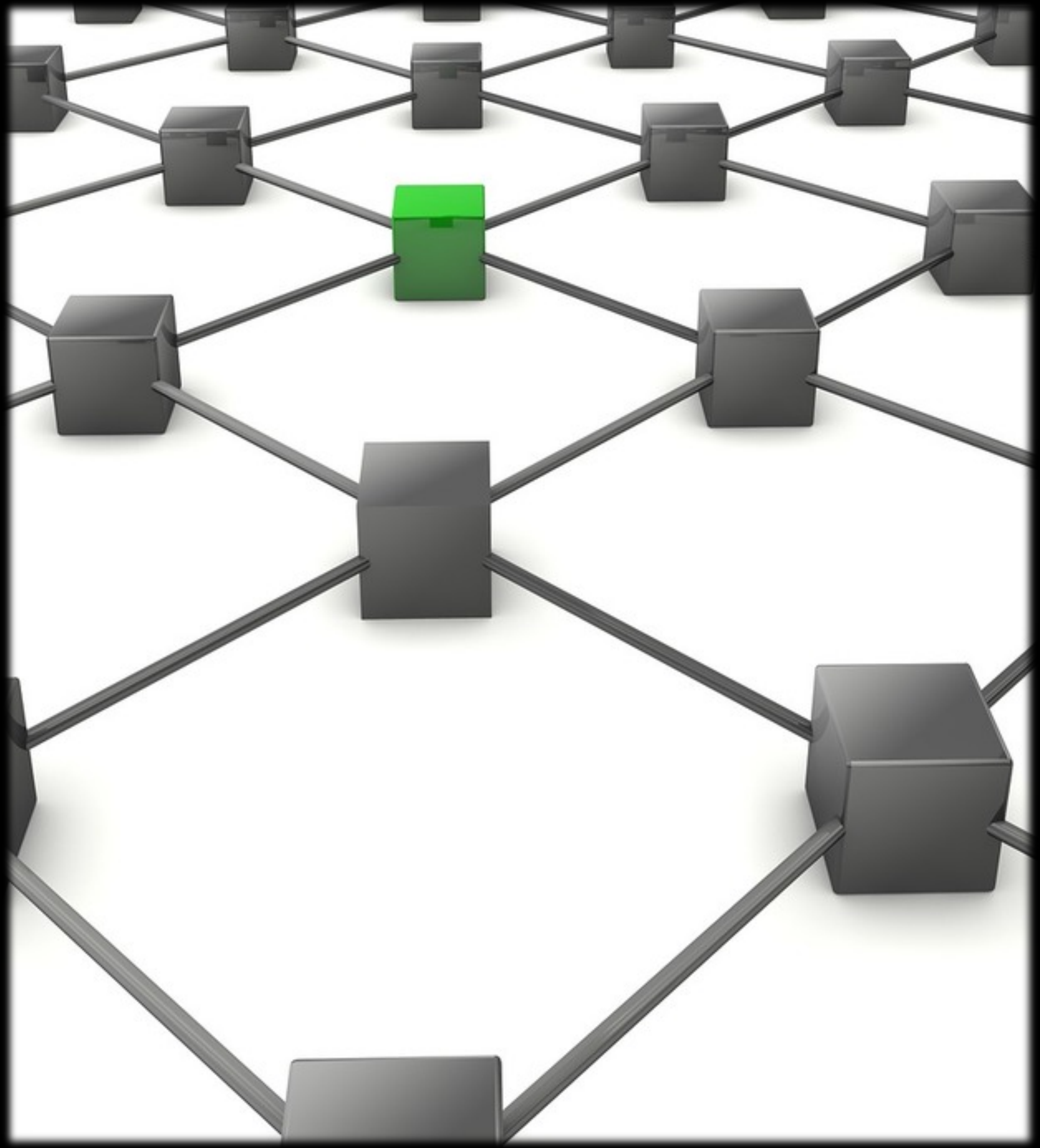
- We Identify a Need
  - No Need? No One Will Adopt!
- We Architect Desirable Features
- We Talk with the Community
- We Produce a Specification
- We Revise with the Community



What's Next?

We'd Love to Work with Other Ecosystems

- Have an Upcoming Conversion or Transition?
- Want a Standard Wallet Interchange Format?
- Want to Exchange Seeds or Shares?
- Want to Integrate Existing Specs?
- Talk to us at:
  - team@blockchaincommons.com



“Interop: What’s It Good For?”

https://www.blockchaincommons.com/musings/musings-interop/

@BlockchainComns in company/blockchain-commons

“Advocating for the creation of open, interoperable, secure & compassionate digital infrastructure to enable people to control their own digital destiny and to maintain their human dignity online”