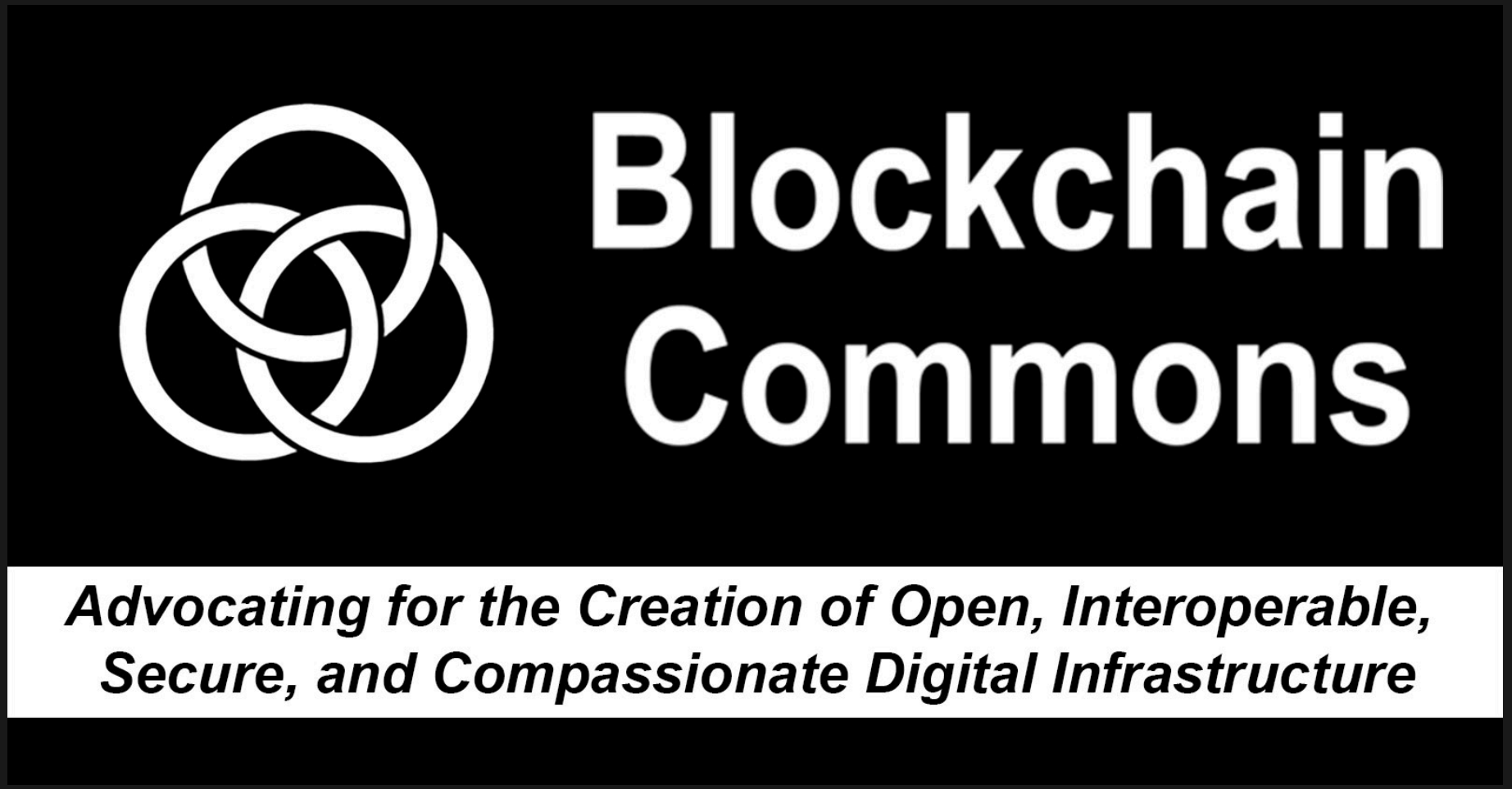


Blockchain Commons #Gordian Meeting 2025-03-05

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.

Today we're featuring a special presentation from one our partners!

Foundation Devices

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

Today's Topics

- Quantum Computing
- QuantumLink from Foundation
- PQC in the Gordian Stack
- The Zcash ZeWIF Project

Quantum Computing (I)

- Quantum Computers take advantage of superposition & entanglement
  - Can do some computing tasks faster
  - A 1994 paper described how RSA could be broken by quantum computing
  - ECDSA, ECDH, and DSA are also insecure with quantum computing
  - AES-256 and SHA-3 require larger output

Quantum Computing (II)

- Quantum computers really exist. This isn't SF!
    - Google: Willow, chip with 105 physical qubits
        - Due to error correction, this is just a handful of logical qubits!
        - Need thousands of logical qubits to break algorithms
    - Microsoft: Majorana claims a path to 1M physical qubits
    - Ultimately, these are laboratory experiments
        - Crypto attacks might be 5-10 years off, but we don't know
- We need Post-Quantum Cryptography (PQC)
    - But right now, use only if you need protection for 5-50 years

Foundation's Passport Prime

- Foundation recently announced Passport Prime
  - A Personal Security Assistant!
  - Stores Seeds, Bitcoin, 2FA codes, Security Keys
  - Encrypted Files Too
- But There's even more going on under the hood!
  - Passport Prime is moving toward a post-quantum reality

Over to Ken ...

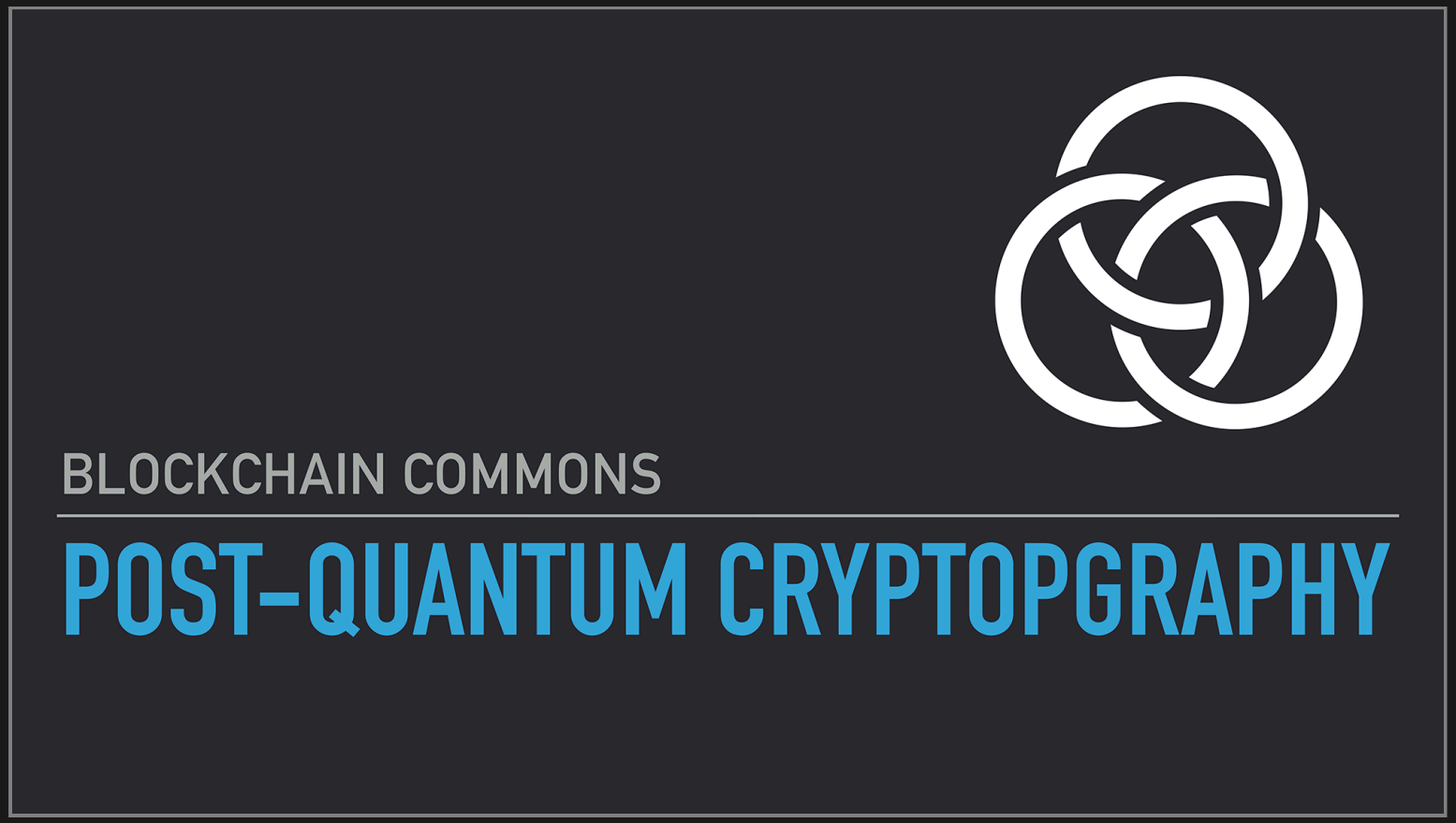
FOUNDATION

QUANTUMLINK

A Quantum-Resistant Communication Protocol for Passport Prime and Beyond

Ken Carpenter
CTO, Foundation Devices

Over to Wolf ...



The ZeWIF Project

- Working on an extensible interchange format for Zcash wallets
  - with our partner Zingo Labs
- In January, released reports
  - https://github.com/zingolabs/zcash-wallet-format
- Starting in on migration tool
  - https://github.com/BlockchainCommons/zmigrate
  - Fully reads zcashd
  - Test it on your wallet! Or give us empty wallets to test!
- Specification to follow

Why ZeWIF is Important

- Interchange allows people to freely move their funds
  - They don't get locked into a single wallet
- Standardization ensures that things don't get lost
  - ZL's ZExCavator tool will help to recover already lost funds
- These are Gordian Principles
  - Openness, Independence, Resilience!
- They support self-sovereign managment of digital assets
- We'd love to do this sort of work on other blockchains!

www.BlockchainCommons.com

Christopher Allen (@ChristopherA)