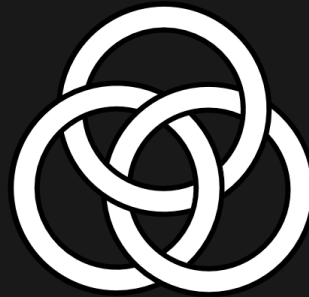


Blockchain Commons

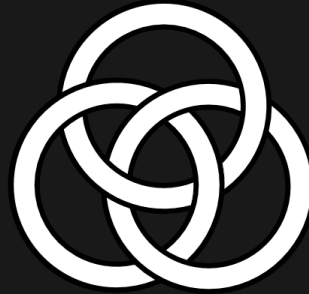
*Advocating for the Creation of Open, Interoperable,
Secure, and Compassionate Digital Infrastructure*

Blockchain Commons #ZeWIF Meeting 2025-01-24



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 have experience working with Bitcoin, Ethereum & Tezos
- Our interop standards can help all digital assets!
- We're thrilled to be working with Zcash.



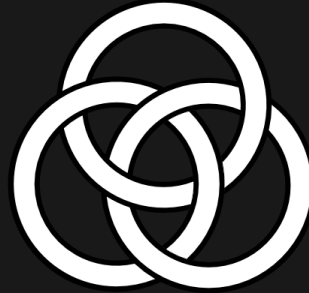
The Gordian Principles

- **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.

Thank you Zcash Community Grants for Sponsoring this Work!



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



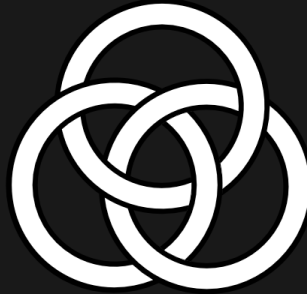
The Goals of the ZeWIF Project

ZeWIF, an extensible wallet interchange format for Zcash, is intended to:

1. Support `zcashd` deprecation
2. Empower users to move among wallets
3. Recover lost funds from older wallets

We're not trying to encode *all* data in the core format, just the *core* data, with others incorporated as *attachments*.

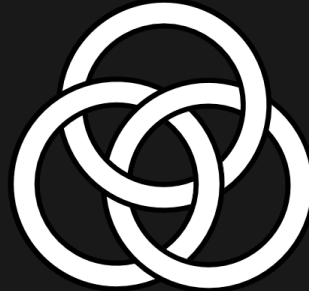
See <https://tinyurl.com/zewif-grant> for the whole proposal.



More than Just zcashd

Though zcashd was the impetus of this project ...

- Our intent is much bigger
- The format is *extensible* so that it can become a tool for the future
- We don't want to lock in *legacy* data
- We want to support an ecosystem where moving among wallets is EASY
- It's about Openness & Independence for users!
- Plus some Privacy & Resilience too!



Our Progress So Far

- We're closing out a survey of major wallets (Dorian)
 - <https://github.com/dorianvp/zcash-wallet-formats/>
- We're starting to spreadsheet data in common (Shannon)
 - <https://tinyurl.com/zewif-spreadsheet>
- Next up will be a specification (Wolf)
- We need your help to ensure the ZeWIF format works for everyone



Our Goals Today

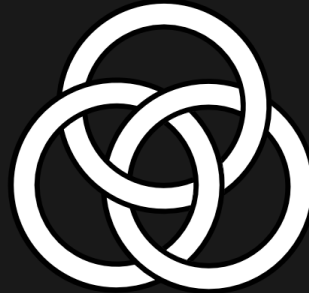
- What is the 20% of data that will get you 80% of the value?
- What data might we be missing?
- What key-value matches should be updated for the format?

But what's our data looking like so far? (With another week of work to go ...)



Looking at the Major Categories

- Jump in if you have thoughts!
- Seeds, Keys, Addresses, Transactions, State, Config, Auth



Seeds

- HD Seeds
- Fingerprints
- Mnemonic Phrases
- Chain Codes



Keys

- Orchard, Sapling, Sprout, Transparent, Unified
- Spending Keys, Viewing Keys, Public Keys, Private Keys
- But also metadata!
 - Key Types
 - Key Paths
 - Seed Fingerprints
 - Creation Times



Addresses

- Again, metadata is going to be the challenge
 - Names
 - Descriptions



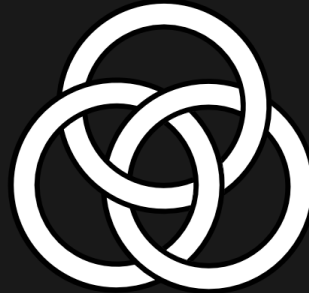
Transactions

- The challenge is here what's not recreatable?
 - Prices
 - Addresses
 - Recipients
 - Scripts
 - Full Viewing Keys
 - Notes
- And is there recreatable data that we want anyway?



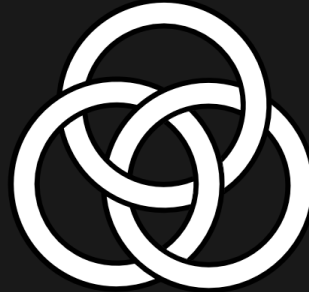
State, Config & Auth

- State: commitment trees, block info, prices, precalculations
- Config: wallet, version, wallet variables
- Auth: wallet keys, encryption keys



Summing Up

- Again:
 - What's the 20% that gets you 80% of what you need?
 - What are we likely missing?
 - Other thoughts on ZeWIF

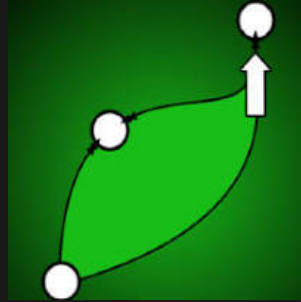


Closing Out Initial Stage Next Week

- Give Us Your Thoughts!
- Here's the data:



- Use Issues or comment the spreadsheet
- Or email shannon.appelcline@gmail.com



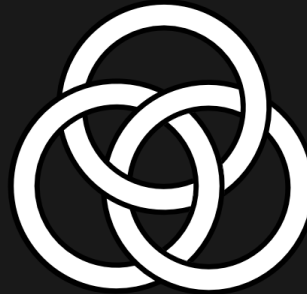
ZExCavator

- ZeWIF is just one element of the project
- Zingo Labs is Building ZExCavator on top of ZeWIF
- Recovers buried ZEC from old zecwallets
- Dorian has more!

ZExCavator

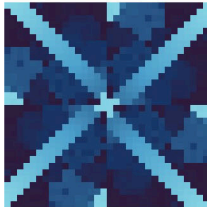

The screenshot shows the GitHub repository page for `zingolabs/uzw-parser`. The repository is public and forked from `james-katz/uzw-parser`. The main branch is `main`, and there is 1 branch and 0 tags. The repository has 18 commits, with the most recent commit by `dorianvp` titled "feat: Integrate with abscissa" 3 hours ago. The file list includes `cli`, `lib`, `.gitignore`, `Cargo.toml`, `README.md`, `generated_from_zwl.db`, `zec.db`, and `zecwallet-light-wallet.dat`. The README section is titled "zw-parser (Zcash Wallet Parser)" and describes the project as a universal Zcash wallet parser designed to read wallet files and extract addresses, keys, and seeds. It also mentions that the project is currently in its prototype stage and supports partial parsing of ZecWallet Lite and YWallet files.

- <https://github.com/zingolabs/uzw-parser>
- [@james-katz](#) has been helping us a lot!



The Next Step: Seed Standardization

- We Hope to Do More in the Future
- Starting With Helping to Standardize Seeds



ffa11a8
[604b93f2]

Yinmn Blue Acid Exam

Size: 128 bits
Strength: **Very Strong**

- This is our "Object Identity Block"
- <https://developer.blockchaincommons.com/seed-128/>
- <https://developer.blockchaincommons.com/oib/>



More Interoperable Specs

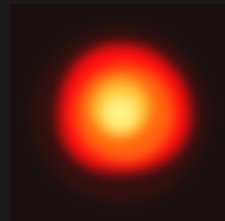
- Animated QRs
 - for airgapping large amounts of data
- SSKR
 - sharding of seeds
- CSR
 - collaborative seed recovery with SSKR
- We hope to discuss these more at a future meeting!



www.BlockchainCommons.com



Shannon Appelcline (@ShannonA)



Darío Paz (@dorianvp)