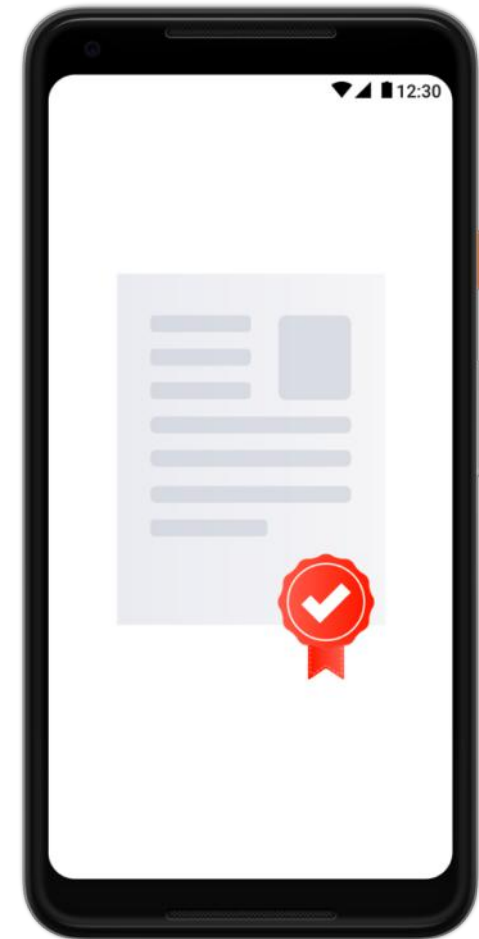


Awesome Research Areas in Blockchain and Self-Sovereign Identity

Thomas Zeinzinger



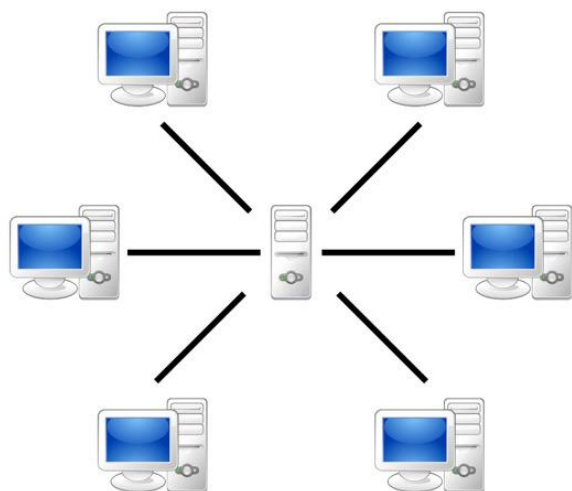
The Problem

Digital data can't be trusted!

There is systematic manipulation and access data is regularly leaked.



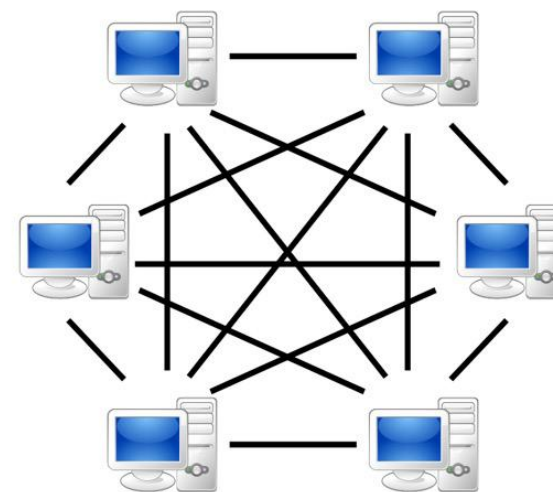
Centralized vs. Decentralized



"Central Control"

&

Servers are 'natural' honeypots



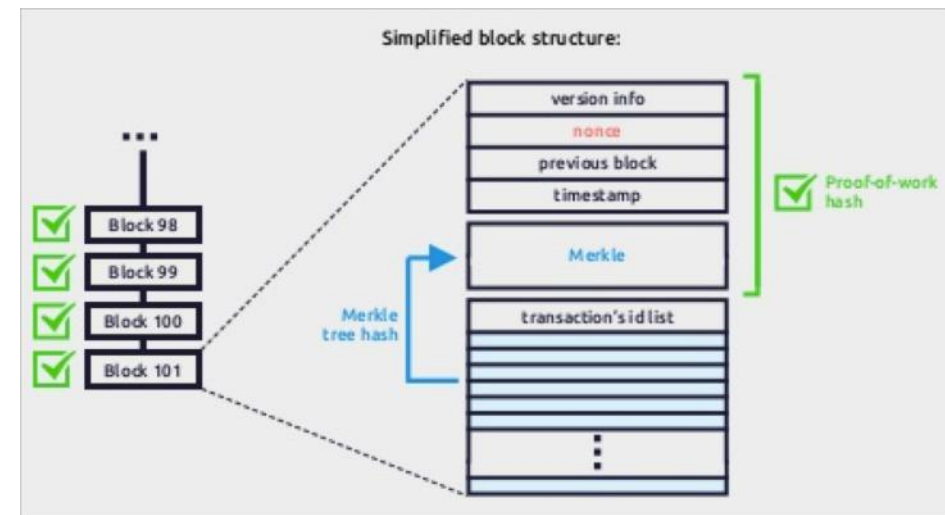
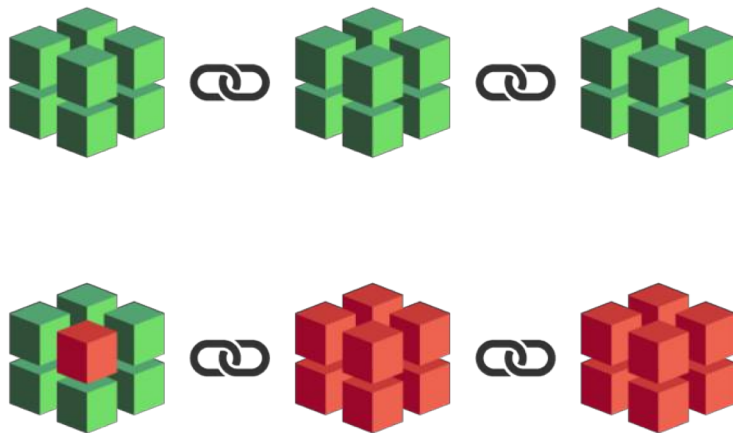
"Distributed Control"

&

One server is neglectable

Blockchain for the Rescue

Public Blockchains are resistant to changes
Attacks are immediately discovered



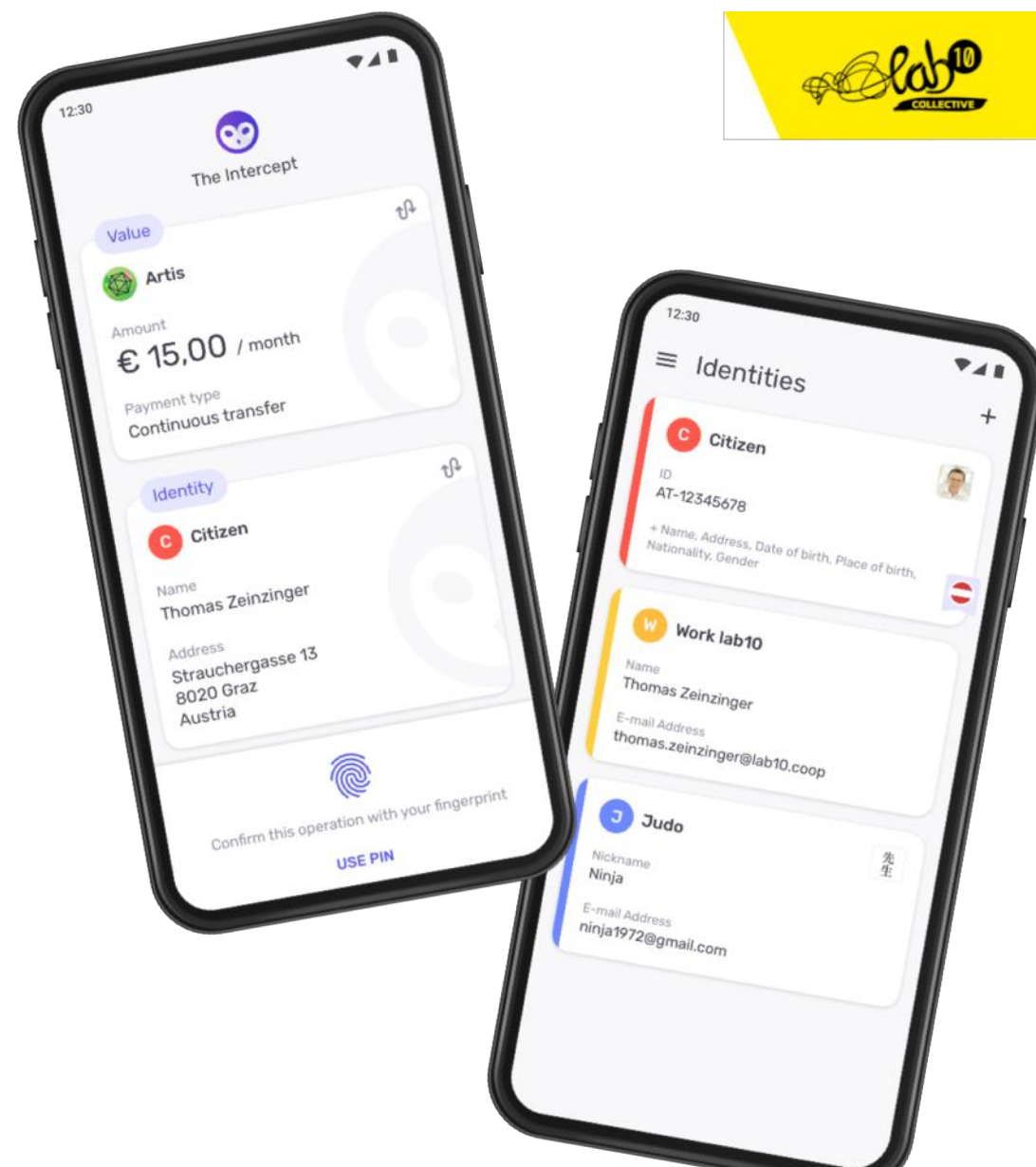


Self-Sovereign Identity for the Rescue

Users are in full control over their identities

Identities can be used for single-sign-on (SSO)

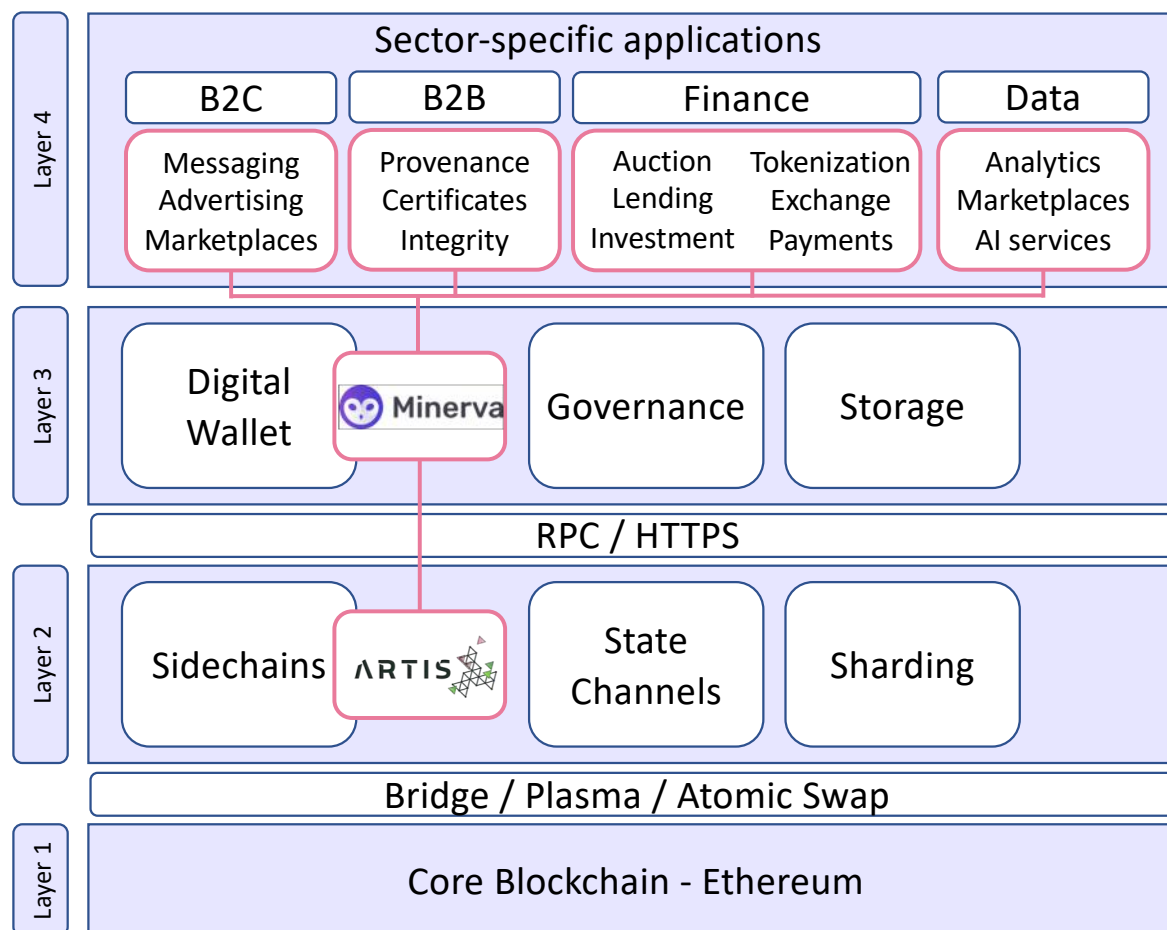
- Decentralized Identifiers (DID)
- Decentralized Authentication (DAuth)
- Verifiable Credentials



Building a Decentralized Infrastructure

4 Layers

- reduced complexity
- allow scalability
- increase security



Layer 4 Research

SonnWende+

Automated Charging and
payment via blockchain

Presented at:



© lab10 collective eG

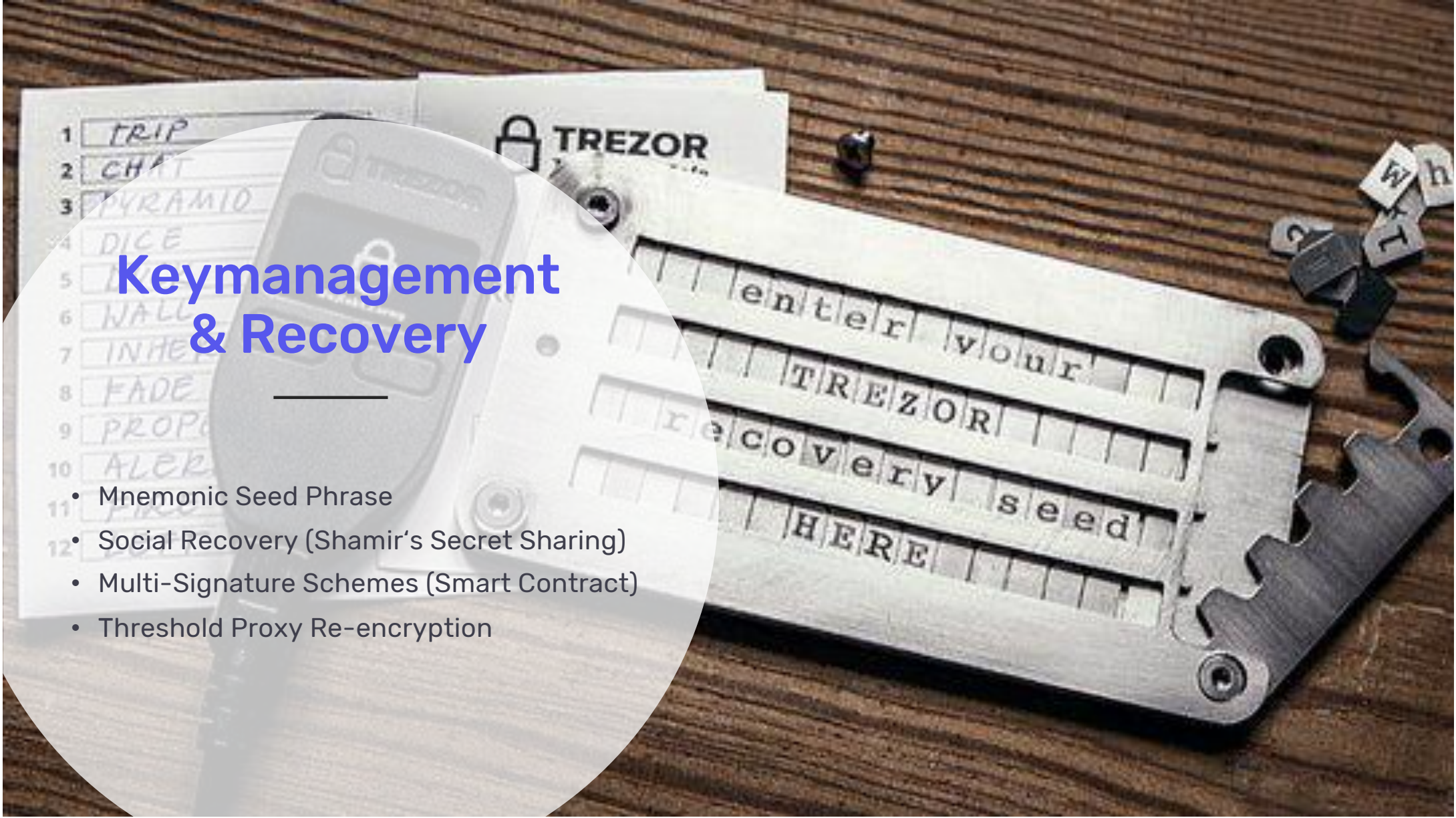


Layer 3 Research

- Keymanagement & Recovery
- Usability – UX/UI
- DID / DAuth / Verifiable Credentials
- IPFS / SWARM
- Fully Homomorphic Encryption

© lab10 collective eG



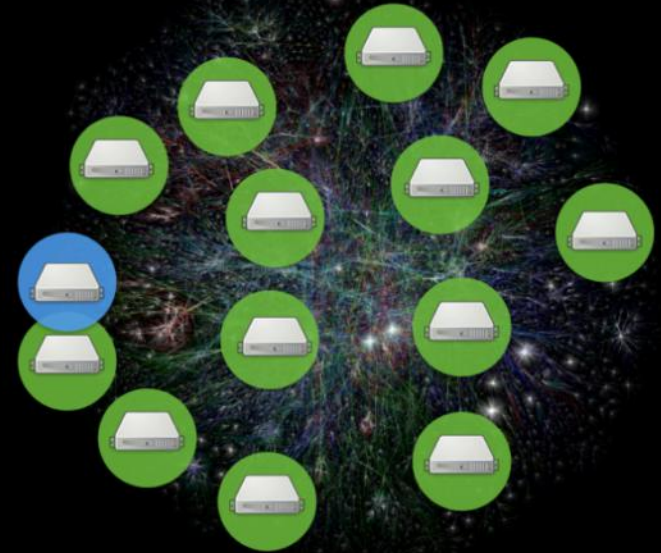
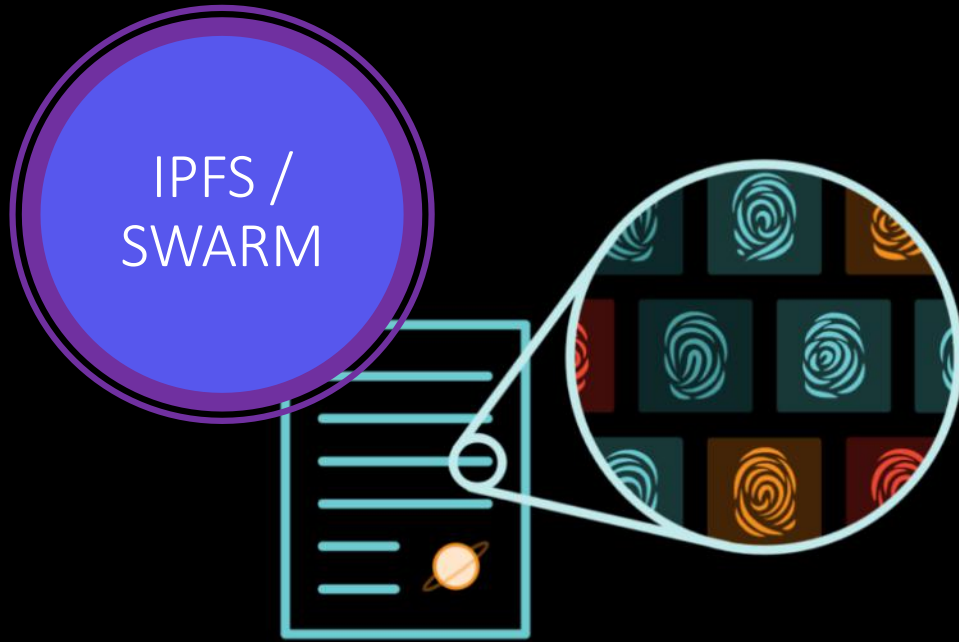
The background image shows a wooden surface with a Trezor hardware wallet, a seed phrase recovery sheet, and a metal recovery tool. The recovery sheet has a list of words and a grid for entering a recovery phrase. The metal tool has a grid for entering a recovery phrase and a small display. The Trezor wallet is a small, silver, rectangular device with a screen and buttons.

Keymanagement & Recovery

- Mnemonic Seed Phrase
- Social Recovery (Shamir's Secret Sharing)
- Multi-Signature Schemes (Smart Contract)
- Threshold Proxy Re-encryption

domain name

/dns/example.com/foo/bar/baz.png



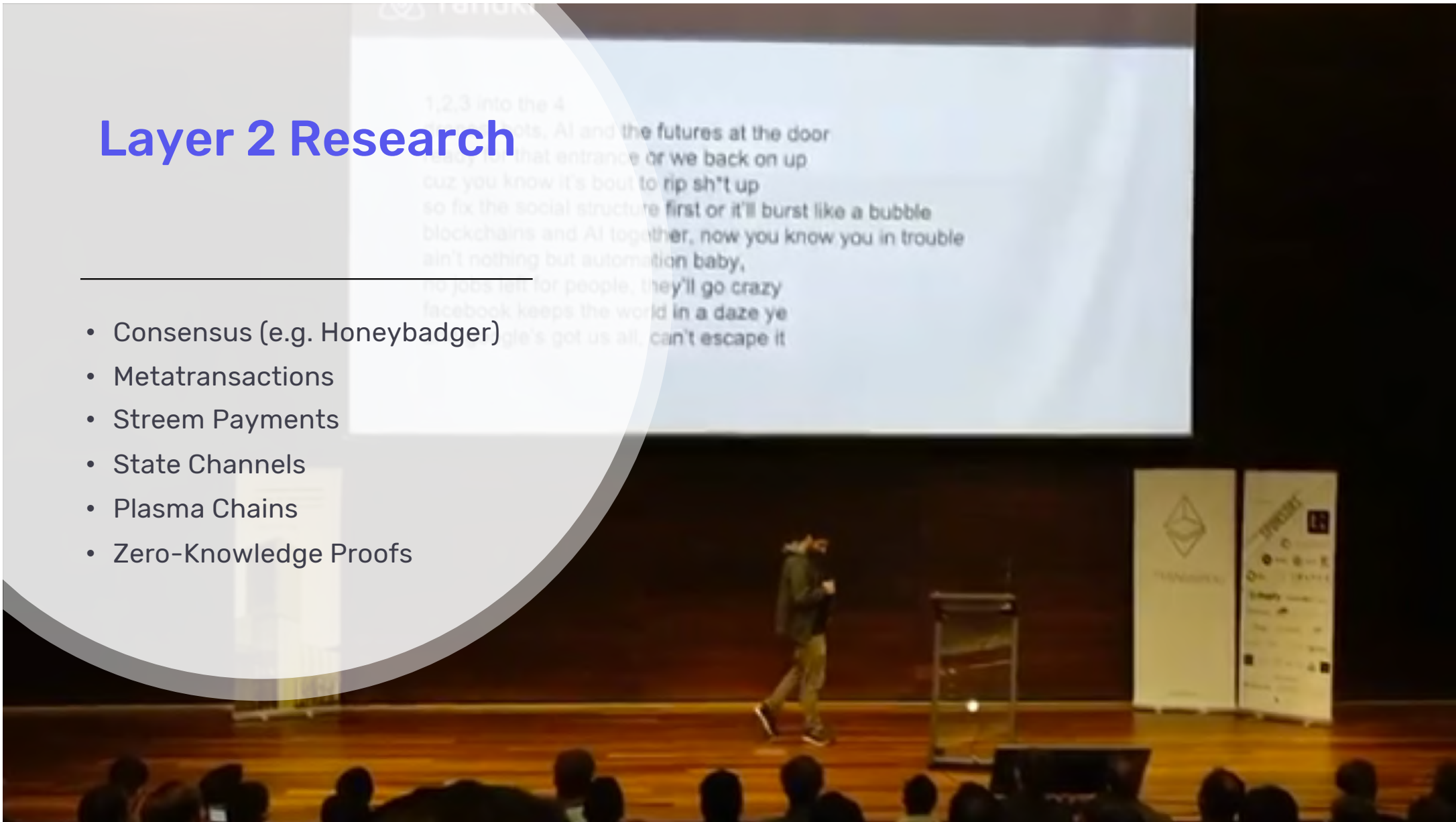
content address

/ipfs/QmW98pJrc6FZ6/foo/bar/baz.png

Layer 2 Research

- Consensus (e.g. Honeybadger)
- Metatransactions
- Stroom Payments
- State Channels
- Plasma Chains
- Zero-Knowledge Proofs

1,2,3 into the 4
...bots, AI and the futures at the door
ready for that entrance or we back on up
cuz you know it's bout to rip sh't up
so fix the social structure first or it'll burst like a bubble
blockchains and AI together, now you know you in trouble
ain't nothing but automation baby,
no jobs left for people, they'll go crazy
facebook keeps the world in a daze ye
...gle's got us all, can't escape it



Zero-Knowledge Proof

- zkSNARK
- zkSTARK
- Bulletproof
- Aurora





Zero-Knowledge Proof

	Toxic-waste free	Proof time	Verify time	Proof size
SNARKs	No	2.3 s	10 ms	~200 B
STARKs	Yes	~1.6 s	~16 ms	~45,000 B
Bulletproofs	Yes	~30 s 1 order of magnitude too big	~1100 ms 2 orders of magnitude too big	~1300 B
Aurora	Yes	~10 seconds 1 order of magnitude too big	~100 milliseconds 1 order of magnitude too big	~100,000 B 2 orders of magnitude too big

Source: Zcash, @Zooko @ Devcon 4, 2018

© lab10 collective eG



Who we are

www.lab10.coop



Thomas Zeinzinger (BizDev, Board)

E-Mail: thomas@lab10.coop

Tel: +43 660 9348567



Dietmar Hofer (ARTIS Dev)

E-Mail: d10r@lab10.coop

Tel: +43 650 5156156