Zero-Knowledge Financial Regulation Compliance

Eran Tromer

Boston University & Sealance Corp.

Conflicting regulatory goals for digital assets

Law enforcement

Monitor

- transactions
- identities

because

- counter terrorism financing
- anti money laundering
- securities regulations
- CYA

via

- surveillance, KYC, CDD, SAR …

Laws: BSA, PATRIOT, CDD Rule, FATCA, MLAT, ...
Regulators: FATF , FINRA, OFAC, IRS,
SEC, CFTC, FinCEN, ...

Conflicting regulatory goals for digital assets

Law enforcement

Monitor
- transactions
- identities

because
- counter terrorism financing
- anti money laundering
- securities regulations
- CYA

via
- surveillance, KYC, CDD, SAR …

Laws: BSA, PATRIOT, CDD Rule, FATCA, MLAT, ...
Regulators: FATF , FINRA, OFAC, IRS, SEC, CFTC, FinCEN, ...

Data protection

Protect privacy of
- transactions
- identities

because
- consumer protection
- personal safety
- corporate/national cybersecurity
- consent
- nondiscrimination
- censorship

Laws: RFPA, GLBA, FCRA, GDPR, ...
Regulators: FTC, CFPB, EDPB, ...

Counter Terrorism Financing case study: crypto funding of Hamas and PIJ

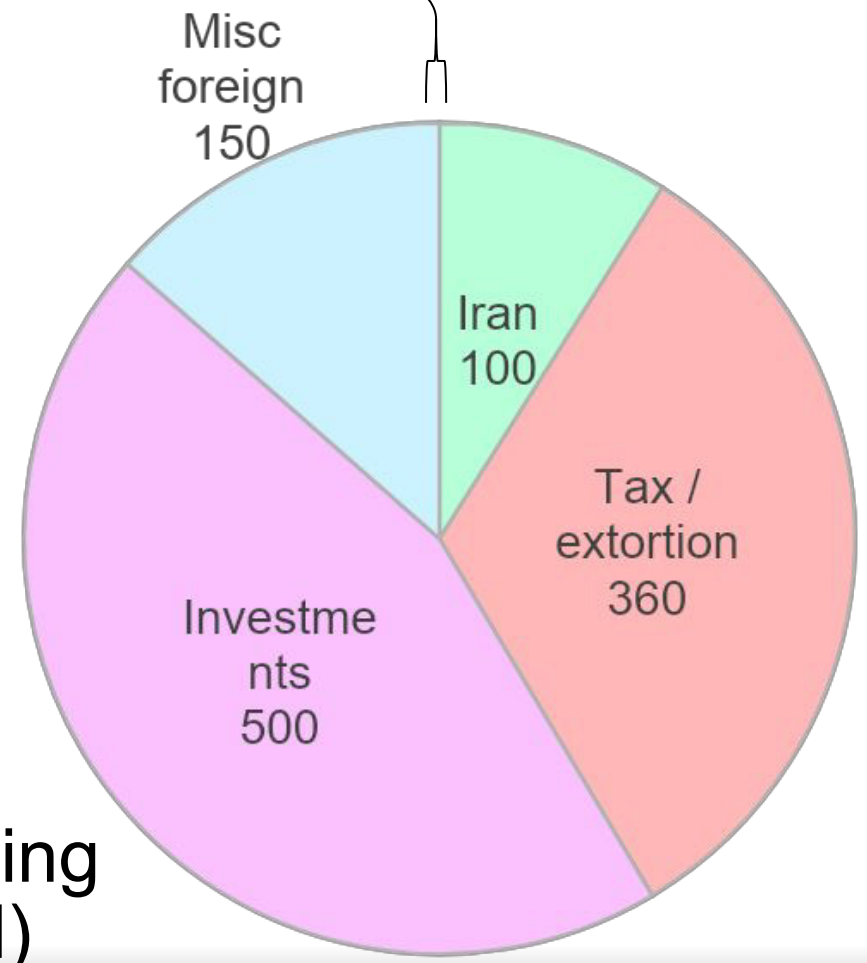
- Terror organizations accepting cryptocurrency donations since at least 2019
- CeFi account seizures by US, Israel
  $7.3M seized by 2021, and ongoing (e.g. Coinbase, Binance)
- Hamas diversified from Bitcoin to ETH, USDT, TRX and DOG
- April 2023: Qassam Brigades announced it would stop accepting Bitcoin donations
  "out of concern about the safety of donors" due to "intensification of hostile efforts against anyone who tries to support the resistance through this currency"

Scope of Hamas+PIJ crypto funding?

known crypto transfers

Sources: The Economist, NBC News, Wagman, Levitt, Congressional Research Service, Us Justice Dept., Elliptic, TRM,CoinDesk, WSJ, Reuters …

- WSJ: claims $130M raised, by Elliptic report
  … which Elliptic says the WSJ misinterpreted
- BitOK claims $41M
  … but counted total traffic of intermediaries
- Published specific examples: <$1M each
- Seizures: a few $million each
- Controversy abounds, including in Congress



Context:

Estimated Hamas+PIJ annual funding (excluding humanitarian/civilian aid)

Post-October 7th: regulators and law enforcement response

- Extensive tracing and sanctions of operatives and financial facilitators
- Account seizures
- $4B penalties on Binance by US Treasury
  for money laundering and sanctions violations,
  including transactions associated with Hamas and PIJ
- US Treasury proposed rulemaking:
  - transactions involving crypto mixing are “of primary money laundering concern”

  → enhanced recordkeeping and reporting obligations

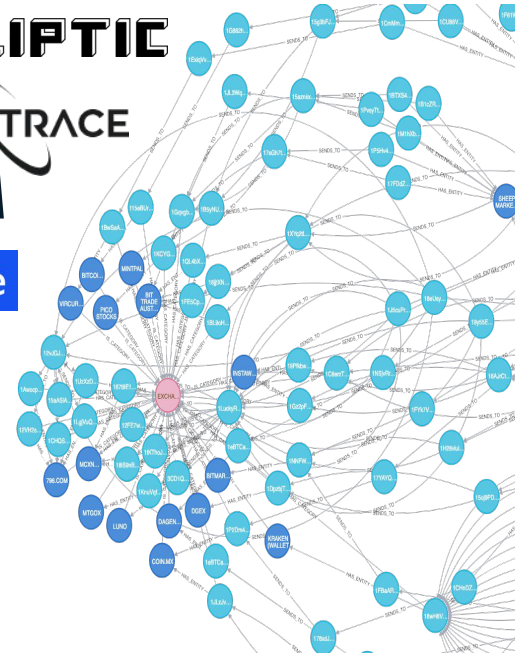
- Is this the only approach? Will work?

State of the art: centralized blockchain analytics for leaky legacy chains

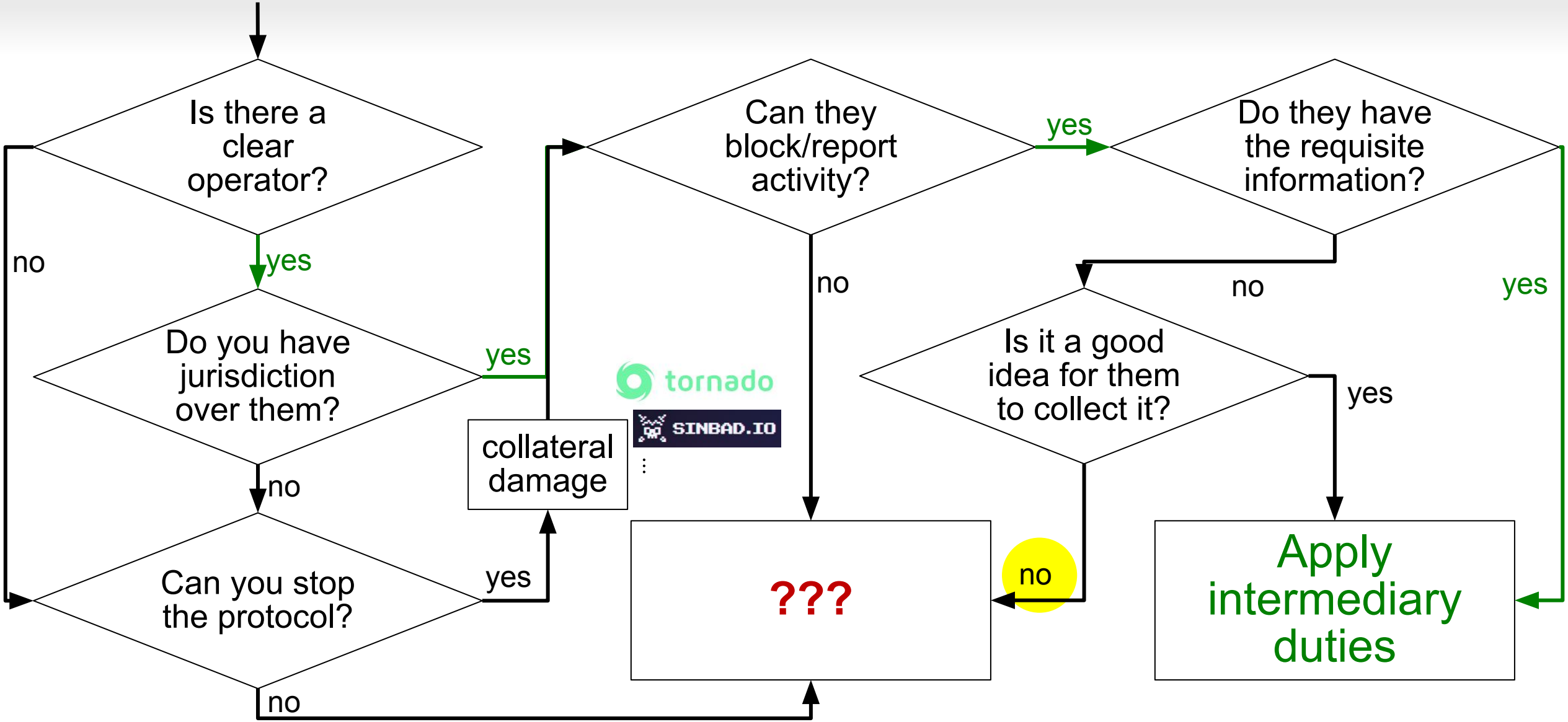
Problems:

1. Centralized collection of too much information
   - ⇨ cybersecurity, privacy and consumer-protection threat
2. Too little information
   - ⇨ heuristics go wrong
   - ⇨ noisy, partial view forces wild deductions
3. Incompatible with legitimate privacy solutions
   - ⇨ users must choose:
     be spied on by everybody,
     or increase your “risk score”
4. Incompatible with scalability, DeFi and other Layer2 tech
5. Needs redundant KYC/CDD at any VASP
   - ⇨ cost, cybersecurity risk, adoption barrier

Chainalysis
ELLIPTIC
CIPHERTRACE
TRM
coinbase



Regulating traditional finance vs. a DeFi protocol



Visibility of financial information

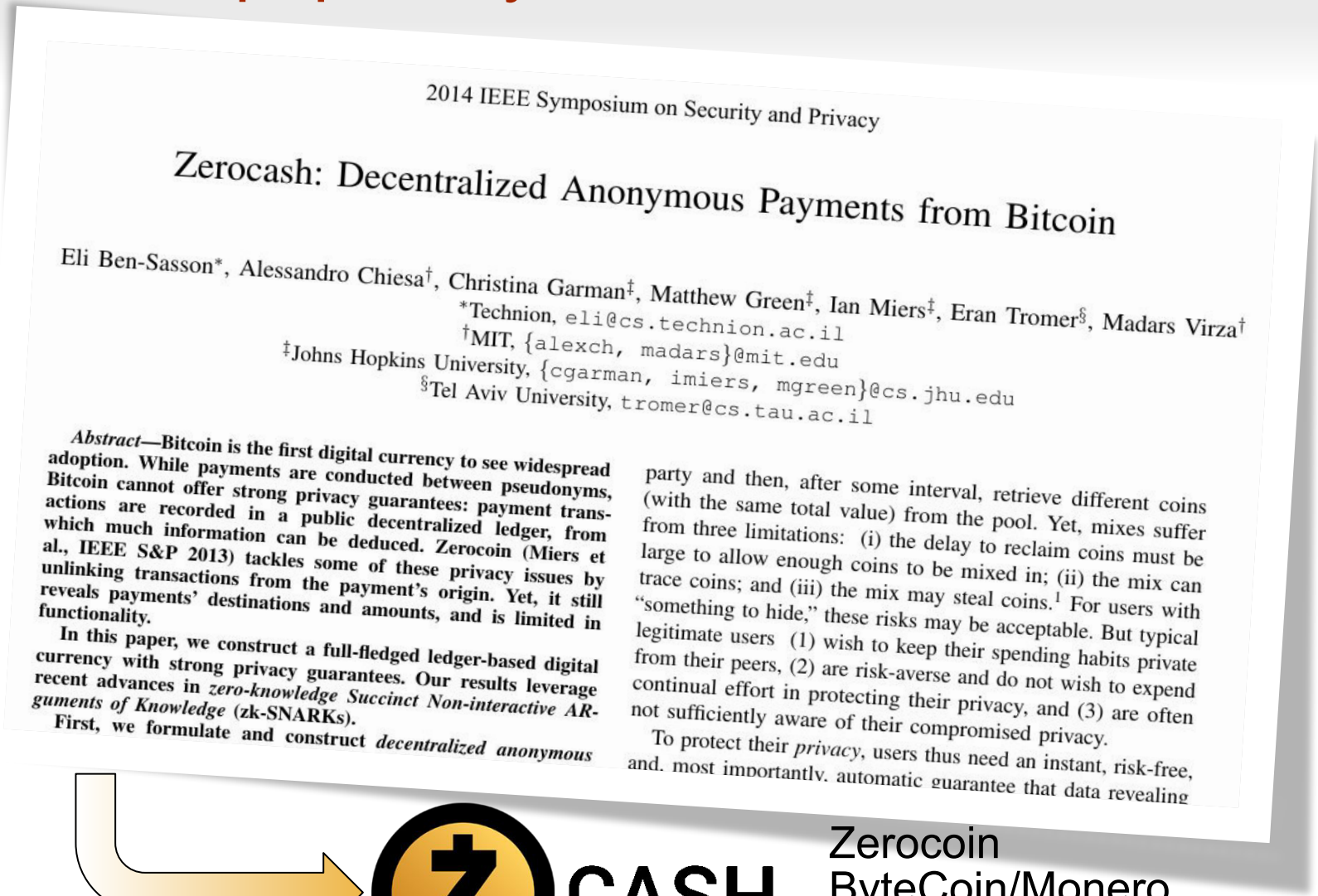
	Most blockchains (e.g., Bitcoin, Ethereum)	Private blockchains (e.g., Zcash)	Traditional finance **ZK-based compliance**
Visible to the counterparties	✅	✅	✅
Private to the general public	🚫	✅	✅
Visible to authorized parties	✅🚫 🤔	🚫	✅

ZK-based compliance: an emerging new approach

- Embed compliance rules into the protocols
  - Blockchain consensus rules
  - Smart contracts
  - Cryptographic protocols
- Enforce jurisdiction-specific compliance policies
- Reason about identity attributes certified by trusted sources
- Issue reports and enable investigations as specified by policy
- Keep information private and confidential by default
- Compatible with decentralization and blockchain innovation

First step: privacy for “I own this coin”

Privacy+compliance



2014 IEEE Symposium on Security and Privacy

Zerocash: Decentralized Anonymous Payments from Bitcoin

Eli Ben-Sasson*, Alessandro Chiesa†, Christina Garman‡, Matthew Green‡, Ian Miers‡, Eran Tromer§, Madars Virza†
*Technion, eli@cs.technion.ac.il
†MIT, {alexch, madars}@mit.edu
‡Johns Hopkins University, {cgarman, imiers, mgreen}@cs.jhu.edu
§Tel Aviv University, tromer@cs.tau.ac.il

***Abstract*—Bitcoin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bitcoin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Zerocoin (Miers et al., IEEE S&P 2013) tackles some of these privacy issues by unlinking transactions from the payment's origin. Yet, it still reveals payments' destinations and amounts, and is limited in functionality.**

In this paper, we construct a full-fledged ledger-based digital currency with strong privacy guarantees. Our results leverage recent advances in *zero-knowledge Succinct Non-interactive ARguments of Knowledge* (zk-SNARKs).

First, we formulate and construct *decentralized anonymous*

party and then, after some interval, retrieve different coins (with the same total value) from the pool. Yet, mixes suffer from three limitations: (i) the delay to reclaim coins must be large to allow enough coins to be mixed in; (ii) the mix can trace coins; and (iii) the mix may steal coins.[1] For users with “something to hide,” these risks may be acceptable. But typical legitimate users (1) wish to keep their spending habits private from their peers, (2) are risk-averse and do not wish to expend continual effort in protecting their privacy, and (3) are often not sufficiently aware of their compromised privacy.

To protect their *privacy*, users thus need an instant, risk-free, and, most importantly, automatic guarantee that data revealing

Zerocoin
ByteCoin/Monero
Horizen
Tornado.cash
Railgun …

Ongoing

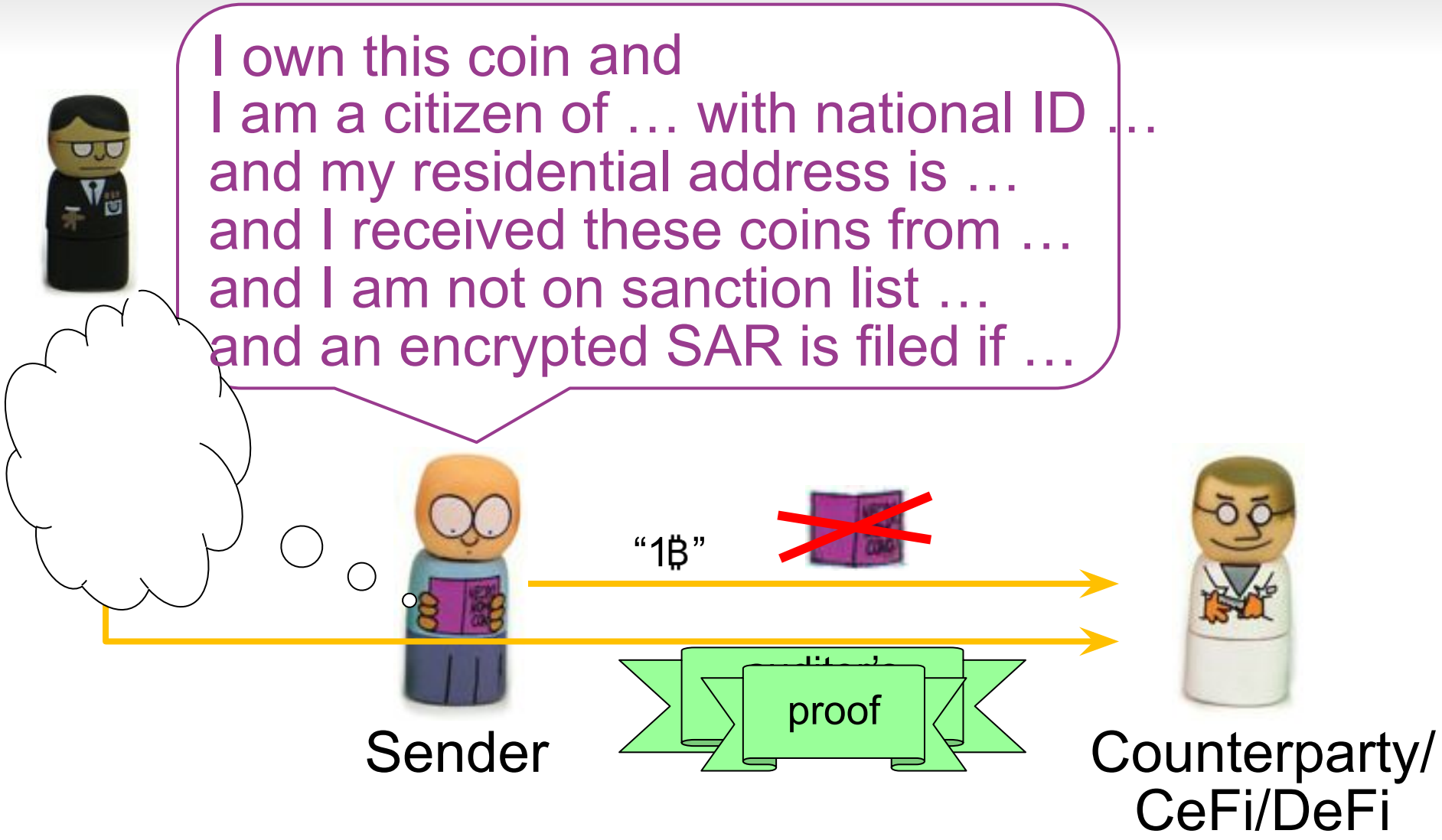
- Academic research
- Implementations
- FinTech startups

Foreshadowing regulation in the *Zerocash* paper (2014)

X. Conclusion

Decentralized currencies should ensure a user's privacy from his peers when conducting legitimate financial transactions. Zerocash provides such privacy protection, by hiding user identities, transaction amounts, and account balances from public view. This, however, may be criticized for hampering accountability, regulation, and oversight. Yet, Zerocash need not be limited to enforcing the basic monetary invariants of a currency system. The underlying zk-SNARK cryptographic proof machinery is flexible enough to support a wide range of policies. It can, for example, let a user prove that he paid his due taxes on all transactions *without* revealing those transactions, their amounts, or even the amount of taxes paid. As long as the policy can be specified by efficient nondeterministic computation using NP statements, it can (in principle) be enforced using zk-SNARKs, and added to Zerocash. This can enable privacy-preserving verification and enforcement of a wide range of compliance and regulatory policies that would otherwise be invasive to check directly or might be bypassed by corrupt authorities. This raises research, policy, and engineering questions over what policies are desirable and practically realizable.

Key tool: cryptographic zero-knowledge SNARK proofs



Intuition: "virtual auditor" using cryptographic proofs.

Publications on ZK-based blockchain regulatory compliance

- Garman Green Miers 2016
  Accountable Privacy for Decentralized Anonymous Payments
  https://eprint.iacr.org/2016/061
- Bowe Chiesa Green Miers Mishra Wu 2018
  Zexe: Enabling Decentralized Private Computation
  https://eprint.iacr.org/2018/962
- Azgad-Tromer Ramaswamy Tromer 2022
  We can finally reconcile privacy and compliance in crypto
  https://fortune.com/2022/10/28/finally-reconcile-privacy-compliance-crypto-new-technology-celsius-user-data-leak-illicit-transactions-crypto-tromer-ramaswamy/
- Burleson Korver Boneh 2022
  Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs
  https://a16zcrypto.com/posts/article/privacy-protecting-regulatory-solutions-using-zero-knowledge-proofs-full-paper/
- Beal Fisch 2023
  Derecho: Privacy Pools with Proof-Carrying Disclosures
  https://eprint.iacr.org/2023/273
- Azgad-Tromer Garcia Tromer 2023
  The Case for On-Chain Privacy and Compliance
  https://stanford-jblp.pubpub.org/pub/onchain-privacy-compliance/release/1
- Buterin Illum Nadler Schär Soleimani 2023
  Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium
  https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364
- Sahu Gajera Chaudhary 2023
  zkFi: Privacy-Preserving and Regulation Compliant Transactions using Zero Knowledge Proofs
  https://arxiv.org/pdf/2307.00521.pdf

+ various components and variants

sealance

You must collect and verify identity+financial information according to complex policies!

BSA/PATRIOT/
FinCEN/IRS/
OFAC/FINRA/
SEC/CFTC/
FATF

OK, I'll collect my customers' data, check it, and keep it very secure.

Traditional finance

You must protect secrecy of personal+financial information!

GDPR/RFPA/
GLBA/FCRA/
FTC/CFPB/EDPB

Decentralized finance

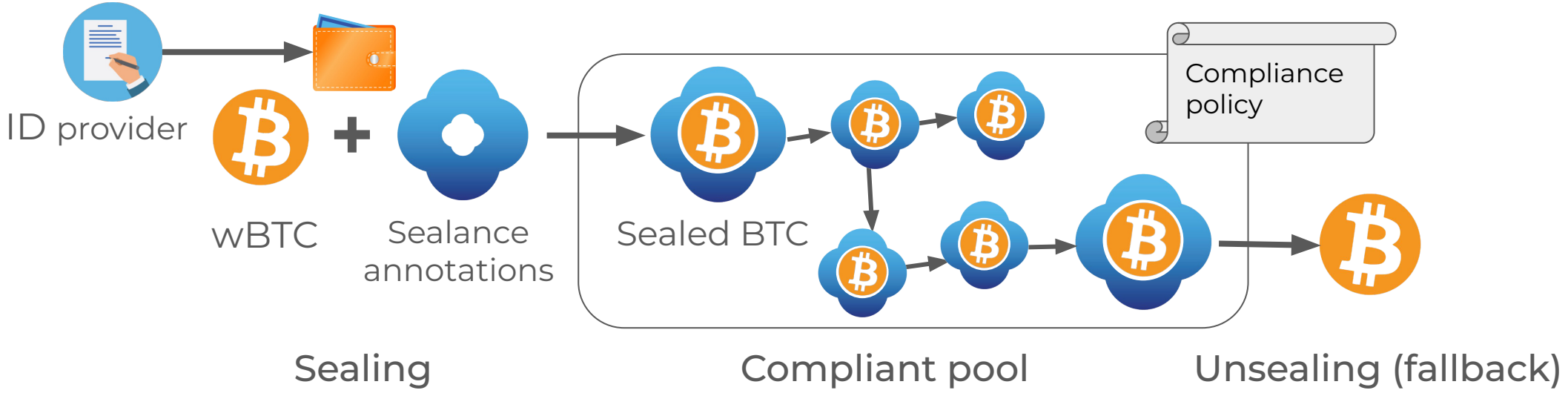
I'm a technological innovator,I can't keep people's secrets!

But I can use cryptography to enforce policies on private data I can't see, using Zero Knowledge proofs.

Compliance overlay for all ledger-based assets

Any coin/token can be “sealed” using a Sealance-compliant wallet / server, to voluntarily subject it to a regulatory policy.

Sealed asset represented on the same chain, using attached annotations.



+ **data access:**
aggregate transaction data, investigative capabilities, insights for customers and regulators

What policies can Sealance enforce?

Identity Identity verification (KYC/KYB/Beneficiaries)

Enforce rules over parties' identity, credit risk/score or user history without publishing or exposing their PII

Sanction enforcement, blocking and freezing

Reg D/ECP

Reg D/ECP attestation for accredited investors, and Reg S attestation for foreign investors

Transaction limits

Funds provenance / source of funds

Attach Suspicious Activity Report annotations to transactions that can be seen only by designated entities/law enforcement

Travel rule (hosted and unhosted)

Robustly protect confidential information
Except when dictated by policy

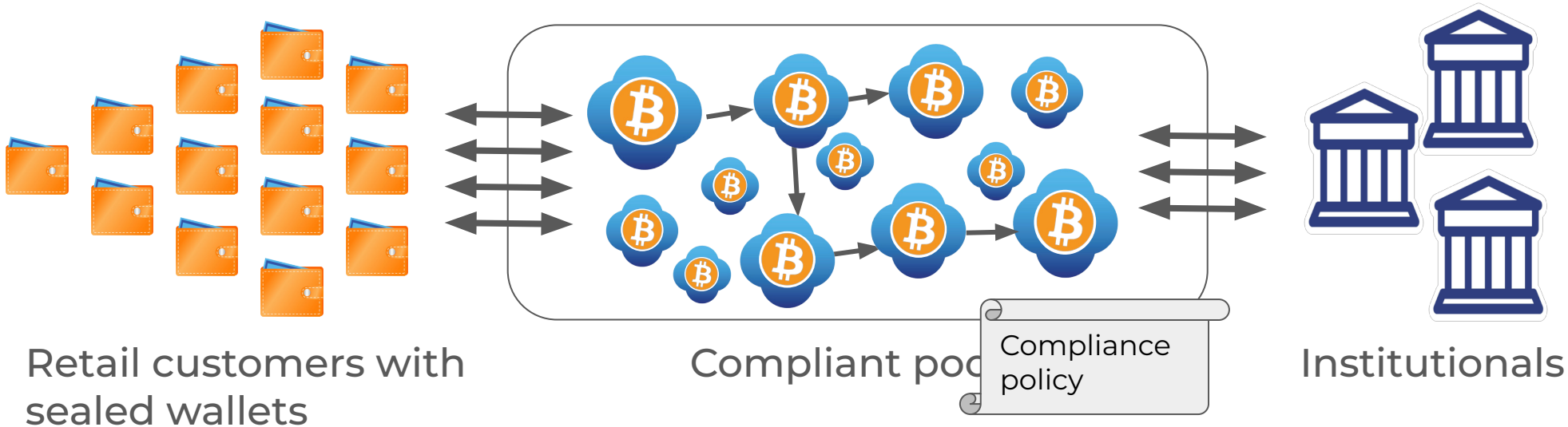
Compliance through cryptography

- Enforcement is inherent and automatic on-chain
  Transactions that violate the jurisdictional policy are automatically rejected
- Uses powerful cryptographic tools to preserve privacy and integrity: zero-knowledge proofs, secure multiparty computation, fully-homomorphic encryption

- Runs on existing chains
  - Bitcoin, Ethereum, Polygon, Cosmos, Tezos, Celo, etc.
- Supports existing and future assets as an overlay
  - ERC-20 tokens, stablecoins, wrapped assets, NFT
- Compatible with DeFi, Dapps, L2 tech and ledger-based CBDCs

Compliant pools

Shared liquidity between compliance-sensitive institutionals and legitimate retail

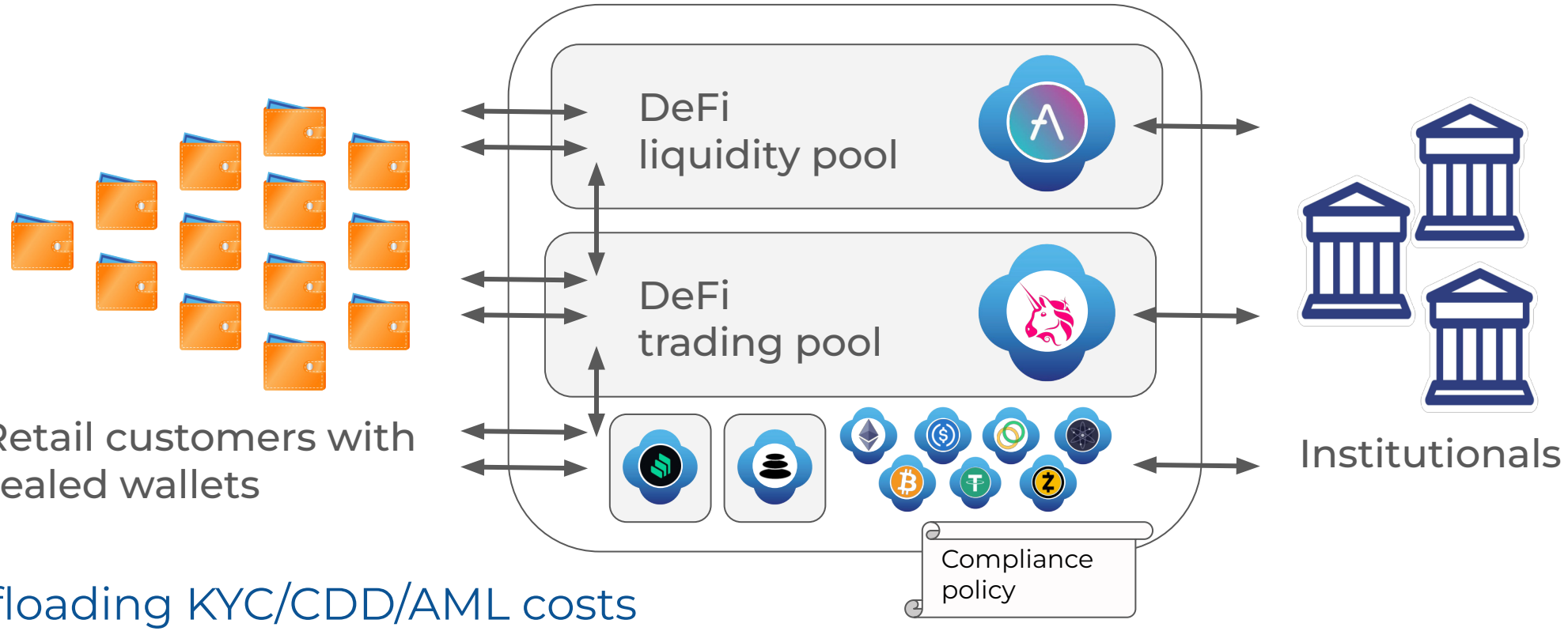


Offloading KYC/CDD/AML costs

- credential reuse/reliance
- automated policy enforcement
- cross-pool compliance tracking

Compliant pools with DeFi

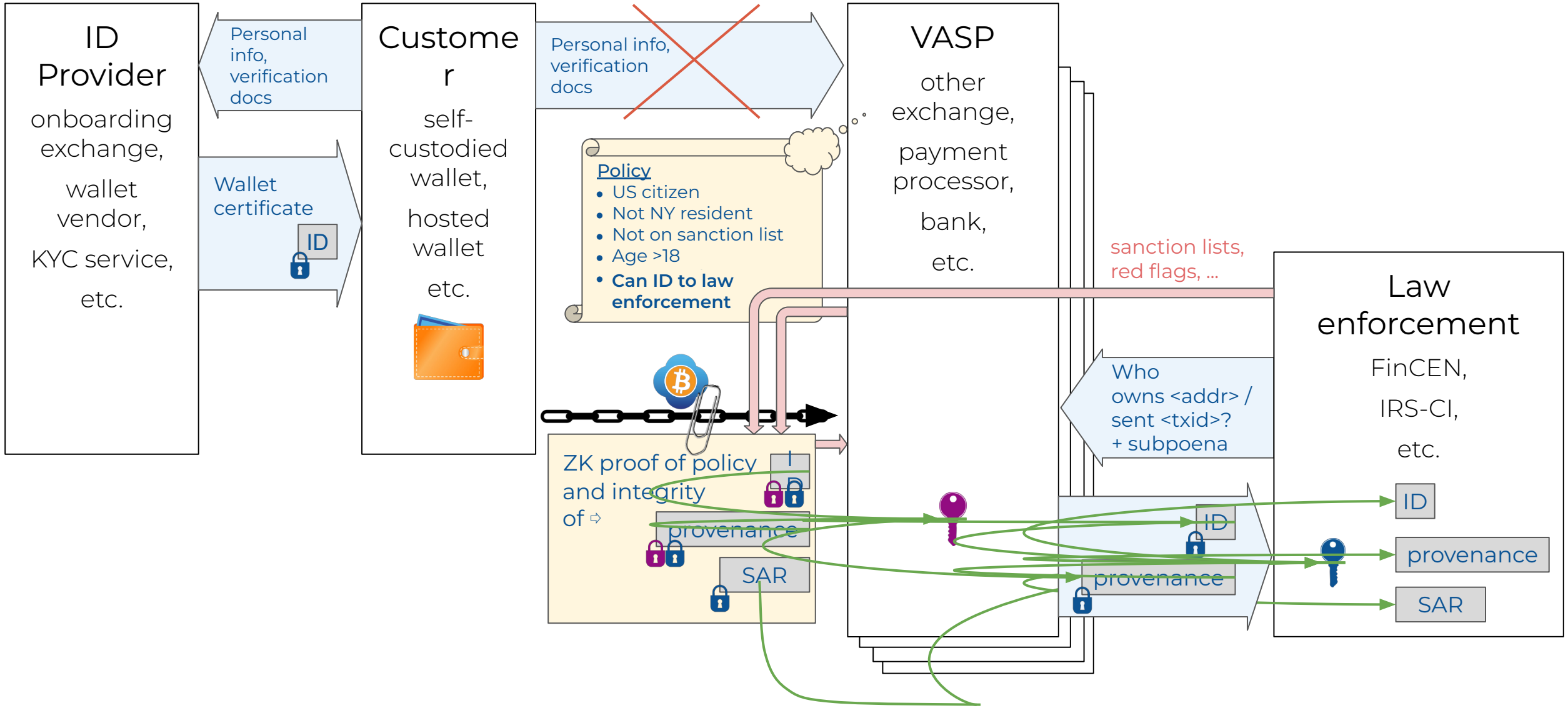
Shared liquidity between compliance-sensitive institutionals and legitimate retail



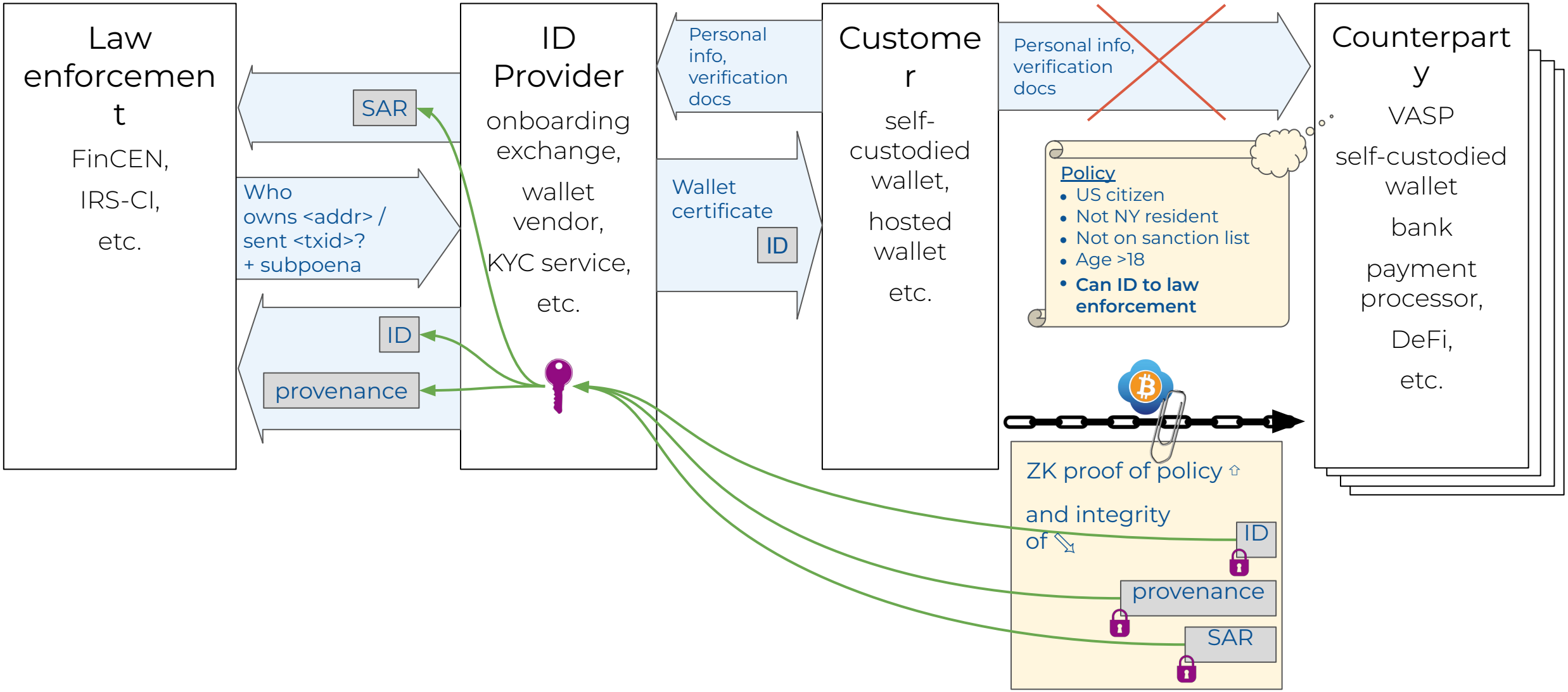
Offloading KYC/CDD/AML costs

- credential reuse/reliance
- automated policy enforcement
- cross-pool compliance tracking

Example flow: KYC + SAR + investigation: VASP model



Example flow: KYC + SAR + investigation: P2P model



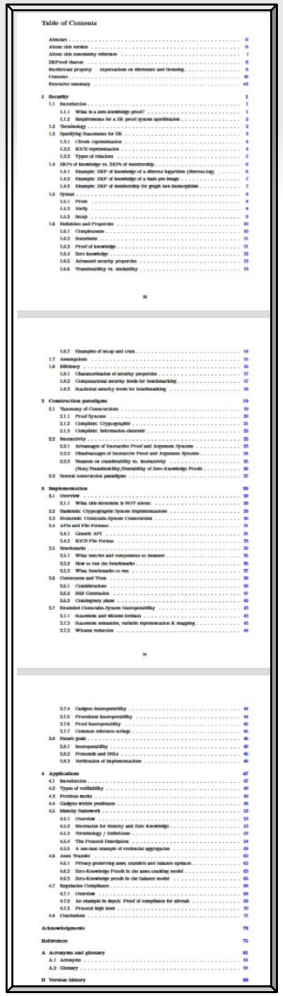
Technical challenges

- Scalability
  - ZK proof complexity
    - Research progress
      linear-time proving, recursion, batching, accumulators, folding
    - Huge statements handled (e.g., DARPA SIEVE)
  - EVM gas costs
    - Rollups, sharding
- Integrations with assets, protocols, wallets CeFi's
  - Smart contract wallets and account abstraction
- Policy configuration ↓

Regulation and compliance challenges

- Presumption of legitimate use
- Ambiguity in law/policies
  - Computers need rules specified upfront
  - So do the startups that write the software
- Innovation sandboxes needed to prove viability
- Recognizing reliance via technical means such as cryptographic protocols

ZKPROOF standardization effort zkproof.org



Aleo · Algorand Foundation · AZTEC · Beam · CPIIS Institute for Information Security · clearmatics · Least Authority Privacy Matters · Matter Labs · Microsoft · Nervos · nevi · Protocol Labs

Cobra Concordium Blockchain Research Center Aarhus · Deloitte. · DHVC · Dystopia Labs · ethereum foundation · firo · qedit · r3. · STRĀTUMN · Tezos · Trail of Bits

Google · Hacera · Horizen Labs · Hyperledger · ING · Input | Output · URVentures · vmware · Zcash Foundation

Discussion