Introduction to Cryptography, Blockchains, and Zero-Knowledge Proofs for Finance

Eli Jaffe
Findora Educator / Cryptography PhD @ UCLA

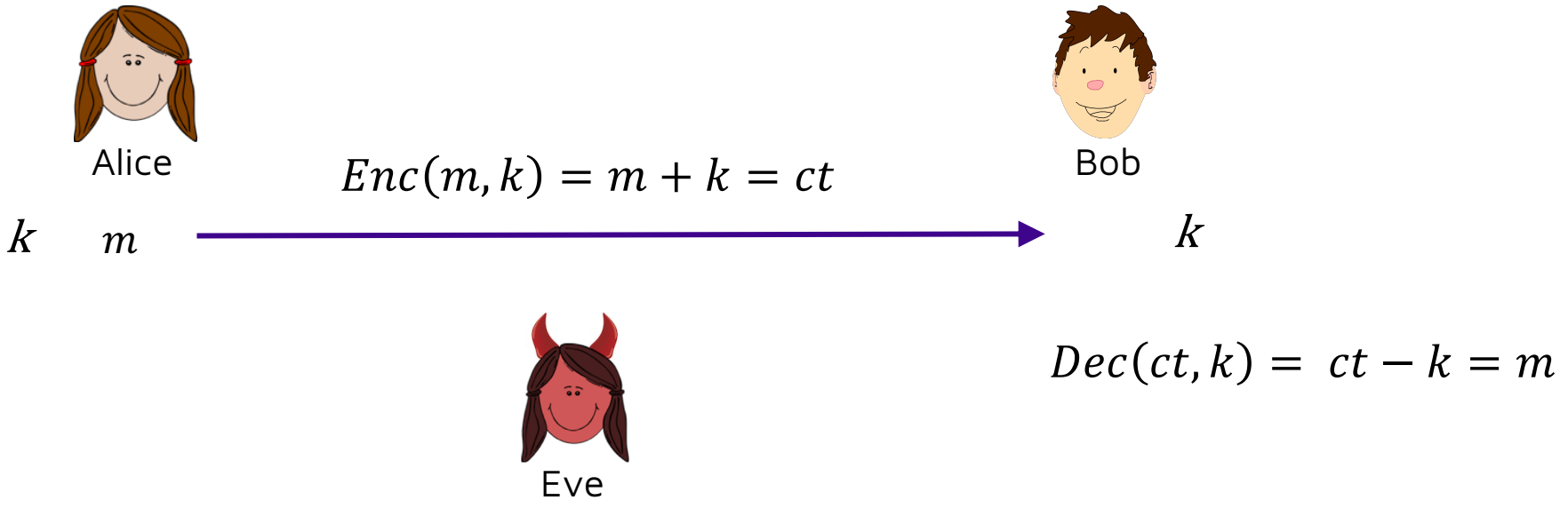
findora

building the Internet of finance

Cryptography Basics

- **How can we use data without revealing it?**

- **Example**: encrypted messaging



Cryptography Basics

- **Historical encryption schemes**
  - Roman scalp encryption
  - Enigma Machine
- **Problem:** security is claimed but eventually broken

findora

Cryptography Basics

findora

- **Modern cryptography**
  - **Provable security** from well-studied mathematical assumptions (discrete log, factoring, LWE, DDH)
  - More than just encryption
    - Pseudorandom Generators / Functions (PRGs, PRFs)
    - Homomorphic Encryption (HE)
    - Multi-Party Computation (MPC)
    - Digital Signatures
    - Blockchains / Cryptocurrencies

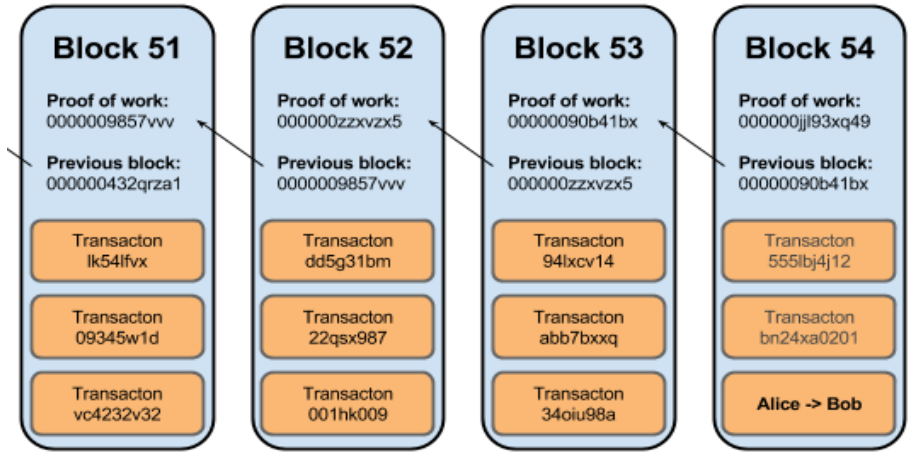
Blockchain Fundamentals

findora

Blockchain Fundamentals

findora

- **What is a blockchain?**
  - Public, decentralized, append-only ledger
    - Public: all data on the chain is available to all participants
    - Decentralized: no one person holds the data, everyone does
    - Append-only: once data is finalized, it remains forever



Blockchain Fundamentals

- **Why do we care about blockchain?**
  - Centralized ledgers are vulnerable to attack and/or abuse
    - Hacking / identity theft is a multi-million dollar industry
    - User data is bought and sold as a commodity
    - Those controlling data have incentive to modify it

findora

Blockchain Fundamentals

- **What data belongs on a blockchain?**
  - Anything that is permanent and final
    - Financial transaction records
    - Personal identification information / credentials
    - Contractual agreements (smart contracts)
    - Medical history, employment history
    - Votes for elected officials / public policy

findora

Blockchain Fundamentals

- **What about privacy?**
  - Virtually all applications (finance, medicine, voting) require some privacy
  - Some require selective revealing of private data
    - Private, auditable financial transactions
    - Medical history for authenticated personal doctor
    - Election results without exact vote counts

findora

Blockchain Fundamentals

- **What about privacy?**
  - Usually rely on centralized authority
  - "Private" blockchain:
    - Limited, registered set of users
    - No guarantee of privacy within those users
- **How can privacy and auditability exist in a public, decentralized system?**

findora

Zero-Knowledge Proofs

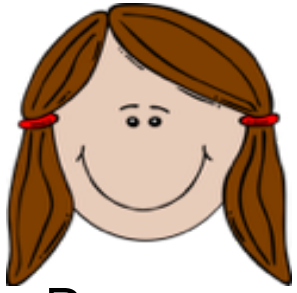
findora

Zero-Knowledge Proofs

- **What is a ZK proof?**
  - A protocol between a **prover** and **verifier**
  - **P** convinces **V** that statement *X* is true
  - **V** learns nothing except that statement *X* is true

findora

Zero-Knowledge Proofs



Peggy

"Transaction x does not exceed my current balance"

"Prove it"

Challenge

Response

Don't know the transaction amount or current balance, but it must be true!

Victor

Zero-Knowledge Proofs

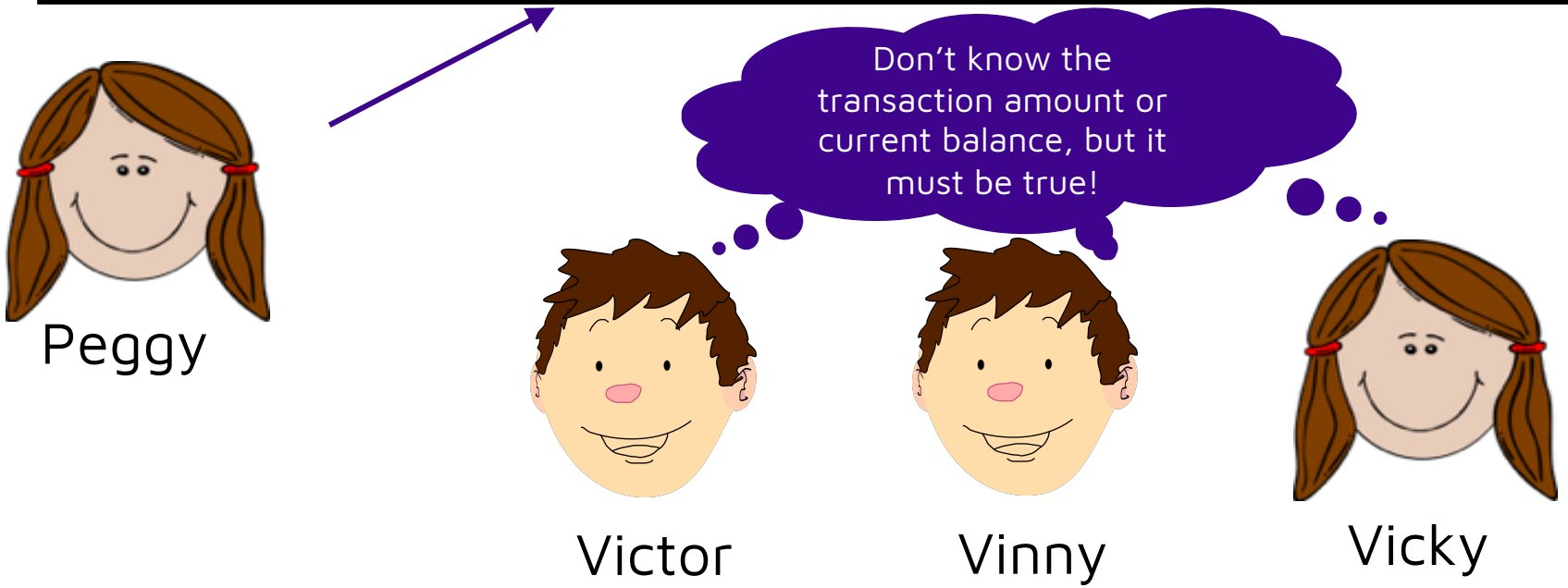
- **What is a non-interactive ZKP (NIZK)?**
  - Most ZK proofs are interactive protocols
  - Some can be made non-interactive (NIZKs)
  - **P** posts a single proof, publicly verifiable by any **V**

findora

Zero-Knowledge Proofs

"Transaction x does not exceed my current balance"

Proof: `FQIl1qEUbhqBX2faSbXThQykVxEaNfyPnanizOdaEXSjue7WqkITM6nNwmGkBra5`

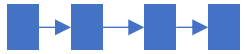


Zero-Knowledge Proofs

- **How are ZKPs and NIZKs used in blockchains?**
  - Data is not stored directly on the blockchain
  - Instead, commitment to data along with proof that committed value is valid
  - Specific verifiers can request proofs of further properties of the data

findora

Zero-Knowledge Proofs

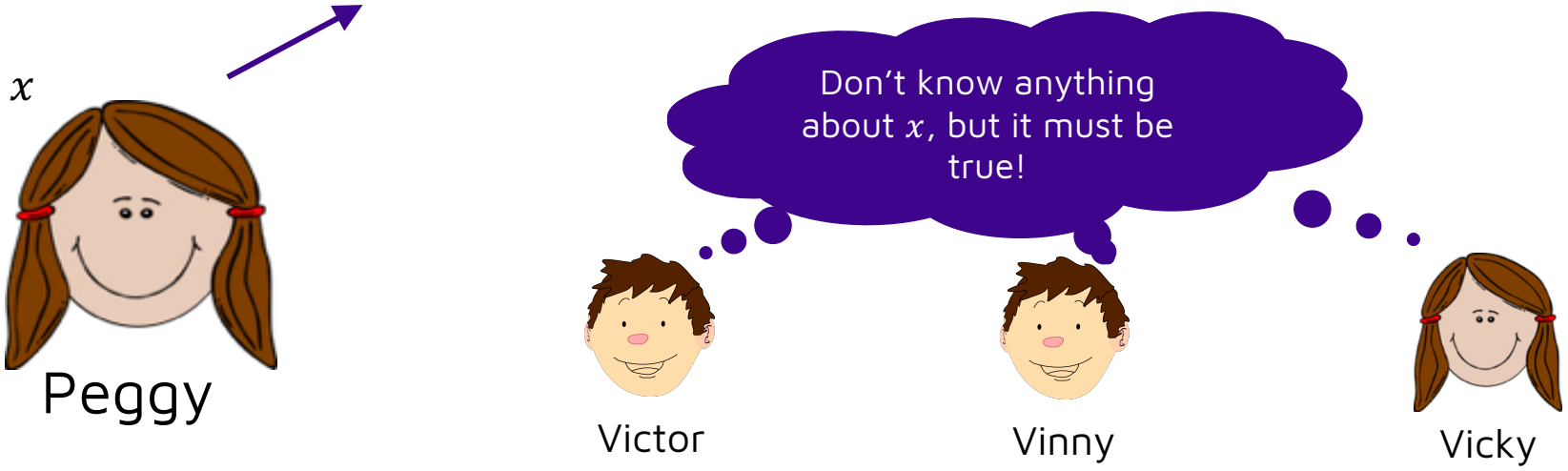


Proposed Block

"I know an x which is a valid transaction and produces commitment $h(x)$"

$h(x) =$ `HWQFcKUIBRtXSRwsQLqajtVy5xgWhclzoinxXI2m`

Proof: `FQIl1qEUbhqBX2faSbXThQykVxEaNfyPnanizOdaEXSjue7WqkITM6nNwmGkBra5`



Zero-Knowledge Proofs

- **Example usage of ZKPs in blockchain**
  - "I submitted a valid vote"
  - "I am in the correct location to collect this reward"
  - "I have a qualifying medical condition for this benefit"
  - "I correctly performed the requested computation"
  - "I performed a legal move based on the game rules"

findora

Different Flavors of Zero-Knowledge Proofs

findora

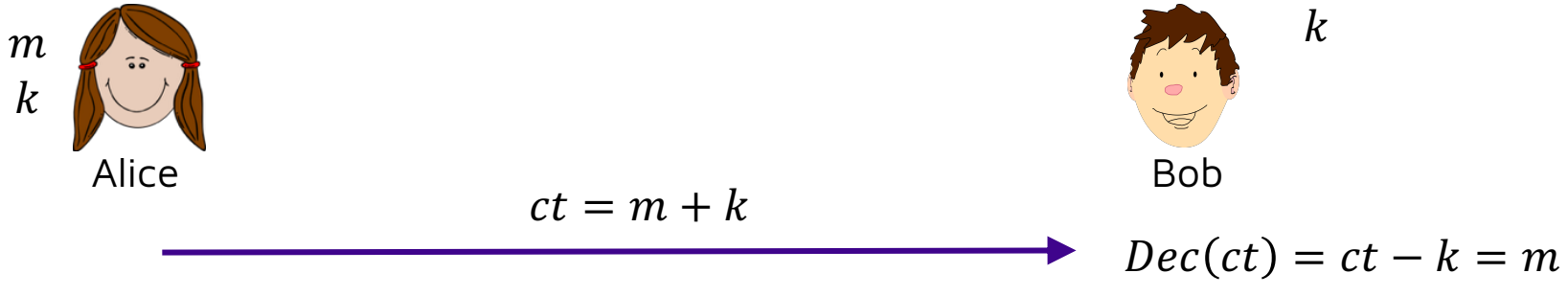
Flavors of Zero-Knowledge Proofs

- **How do we measure the quality of a ZKP system?**
  - Communication
    - Overall communication (bits)
    - Rounds of communication
  - Verifier efficiency (time, space)
  - Prover efficiency (time, space)
  - Requires trusted setup?

findora

Flavors of Zero-Knowledge Proofs

- **What is a trusted setup?**
  - Protocols can be simpler if players begin with correlated random numbers
  - Example: encrypted messaging



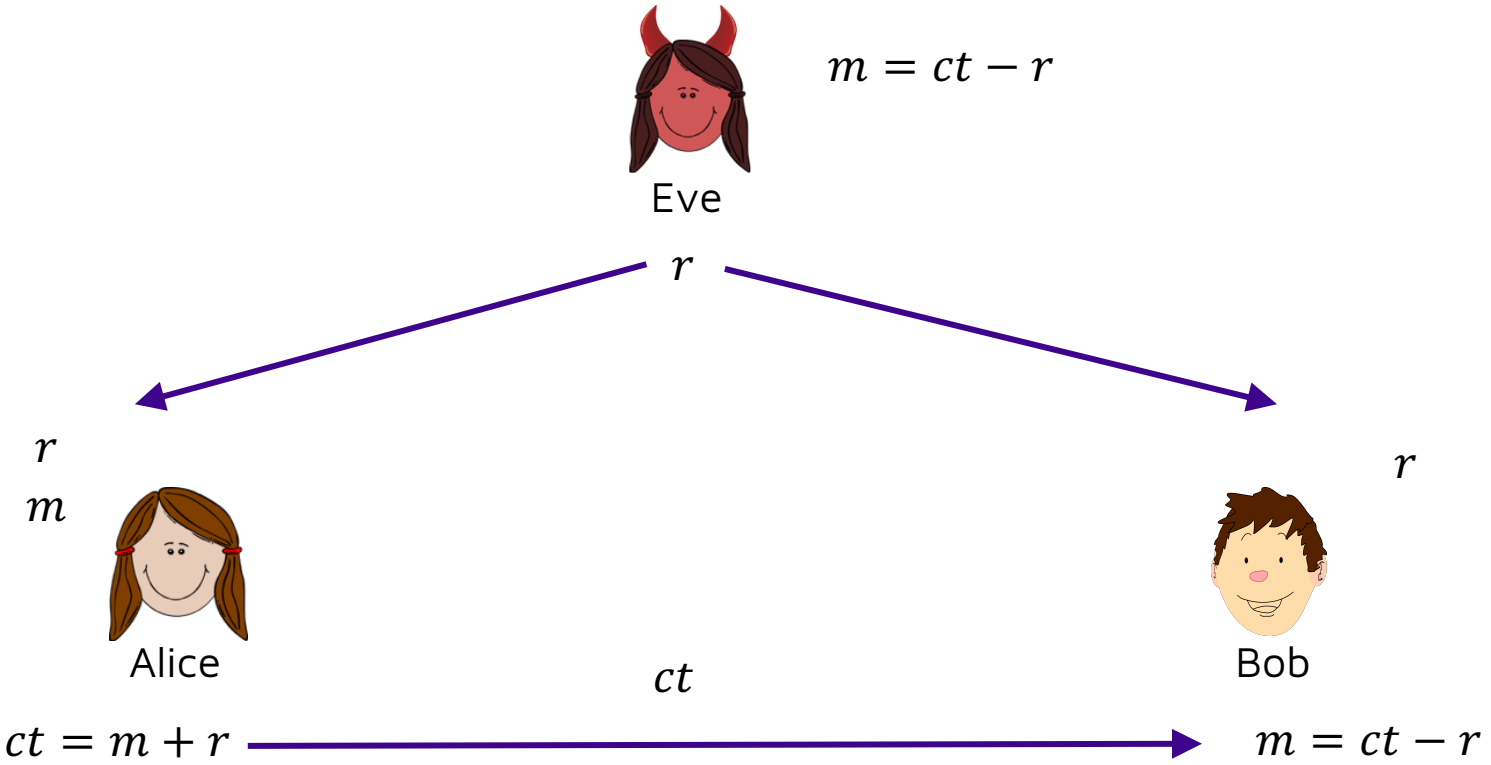
findora

Flavors of Zero-Knowledge Proofs

- **Problems with using a trusted setup**
  - Person who produces randomness must discard it
    - Otherwise, no security guarantees
    - Bad for finance: undetectable inflation
  - Multiple parties can produce the randomness together
    - Only one party must discard randomness to protect security
    - Multi-party protocol to do this is expensive and risky

findora

Flavors of Zero-Knowledge Proofs



Flavors of Zero-Knowledge Proofs

- **What would be the ideal ZKP system?**
  - Non-interactive (one round of communication)
  - Short proof length
  - Efficient prover and verifier
  - No trusted setup

findora

The State-of-the-Art: Supersonic SNARKs

findora

Supersonic SNARKs

- **What are SNARKs?**
  - **S**uccinct **N**on-interactive **Ar**guments of **K**nowledge
    - *Succinct:* proof length is less than size of validity circuit
    - *Non-interactive:* one round of communication
    - *Argument of Knowledge:* proves knowledge of some data
  - Ideal ZKP system: trustless SNARK w/ efficient **P** and **V**

findora

Supersonic SNARKs

- **What are Supersonic SNARKs?**
  - New ZKP system developed by Findora research team
  - First SNARK with
    - Logarithmic proof size
    - Logarithmic verifier computation
    - Practical prover computation
    - **No trusted setup**

findora

Supersonic SNARKs

- **What do Supersonic SNARKs mean for blockchain?**
  - We can have privacy and scalability without risky trusted setup!
  - Closest to ideal ZKP system that we currently know of

findora

Findora: Confidential Decentralized Finance

findora

Findora: Motivation

- **What problems does finance face?**
  - Financial institutions are opaque, inefficient, and high-risk
    - Auditing process is difficult, expensive, and invasive
    - Complex back-office record systems are costly and slow
    - Sensitive client data is mismanaged, abused, and hacked
  - Public trust in financial institutions is lower than any other industry

findora

Findora: Overview

- **What is Findora's vision?**
  - One global financial network, protocol, infrastructure, and standard
  - Balance **privacy** and **auditability**
  - An **"Internet of Finance"** connecting an ecosystem of transactional ledgers

findora

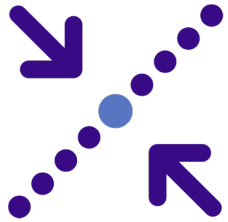
Findora: Overview

- **What is Findora?**
  - Findora is a **private and auditable ledger**
    - All transactions on Findora ledgers are encrypted, but…
    - All transactions on Findora ledgers can be audited for compliance with respect to a policy
  - Implications?
    - A Findora ledger running on a **single node** is a **private and auditable database**
    - A Findora ledger running on a **decentralized network** is akin to a **confidential Ethereum public network**

findora

Findora: Technical Tools

Efficient proofs of compliance



Compact cryptographic accumulator storage model

Confidential asset issuance, transfer, and contracts

Modular and pluggable consensus

findora

Privacy of Transactions

libra

ethereum

Payments **publicly** visible/linkable

支付宝 ALIPAY

BANK TRANSFER PAYMENT METHOD

BANK TRANSFER

微信支付 WeChat Pay

Payments only visible to **trusted** 3rd party. Optionally sender/receiver public

findora

MONERO

Zcash

Unlinkable private payments

Less private ⟷ More private

findora

Auditability of Transactions

Decentralized

Simple single-asset transfer, **publicly** auditable

Complex financial agreements, **publicly** auditable

Less auditable

More auditable

Simple single-asset transfer, central/3rd party auditor

Complex financial agreements, central/3rd party auditor

Centralized

Zero Knowledge in Findora

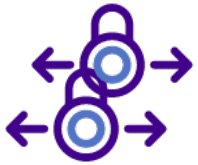
Privacy tools:

confidential transfer

hide details of a transaction while still enabling network to confirm its validity

private multi-source transfer

hide from recipient the amounts from each source, revealing only the aggregate amount



confidential assets

hide types of assets in public ledger transaction or account

privacy-preserving computation

sealed-bid auctions, fair lotteries, order-book matching (dark pools and anti-frontrunning), and more!

findora

Zero Knowledge in Findora

Compliance tools:

proof of solvency

prove assets exceed liabilities while keeping multi-asset balance sheet confidential

balance range proofs

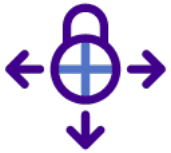
prove that a confidential account balance or transfer amount is within a specific range

proof of whitelisted assets

prove that the issuer/type of a confidential asset is whitelisted

capability-specific audit keys

authorize fine-grained viewing keys that cannot control accounts and only reveal necessary information



confidential asset tracer

allow asset issuer to trace all ownership transfers while remaining confidential to public

proofs of compliance

prove that transactions are compliant with terms of financial contract or regulation

findora

The Future of Findora

findora

- **Findora is the infrastructure for private, decentralized finance**
  - Community developers (like you!) will build Findora
  - Findora's user-friendly javascript API lets anyone write apps
  - If you're interested in joining our testnet and trying for yourself: https://forms.gle/upVNUKoxHg5JxXq19
  - Subscribe to our newsletter for updates: https://findora.org/#subscribe-form

Thanks!

https://findora.org

Eli Jaffe
Findora Educator / Cryptography PhD @ UCLA

findora

building the Internet of finance