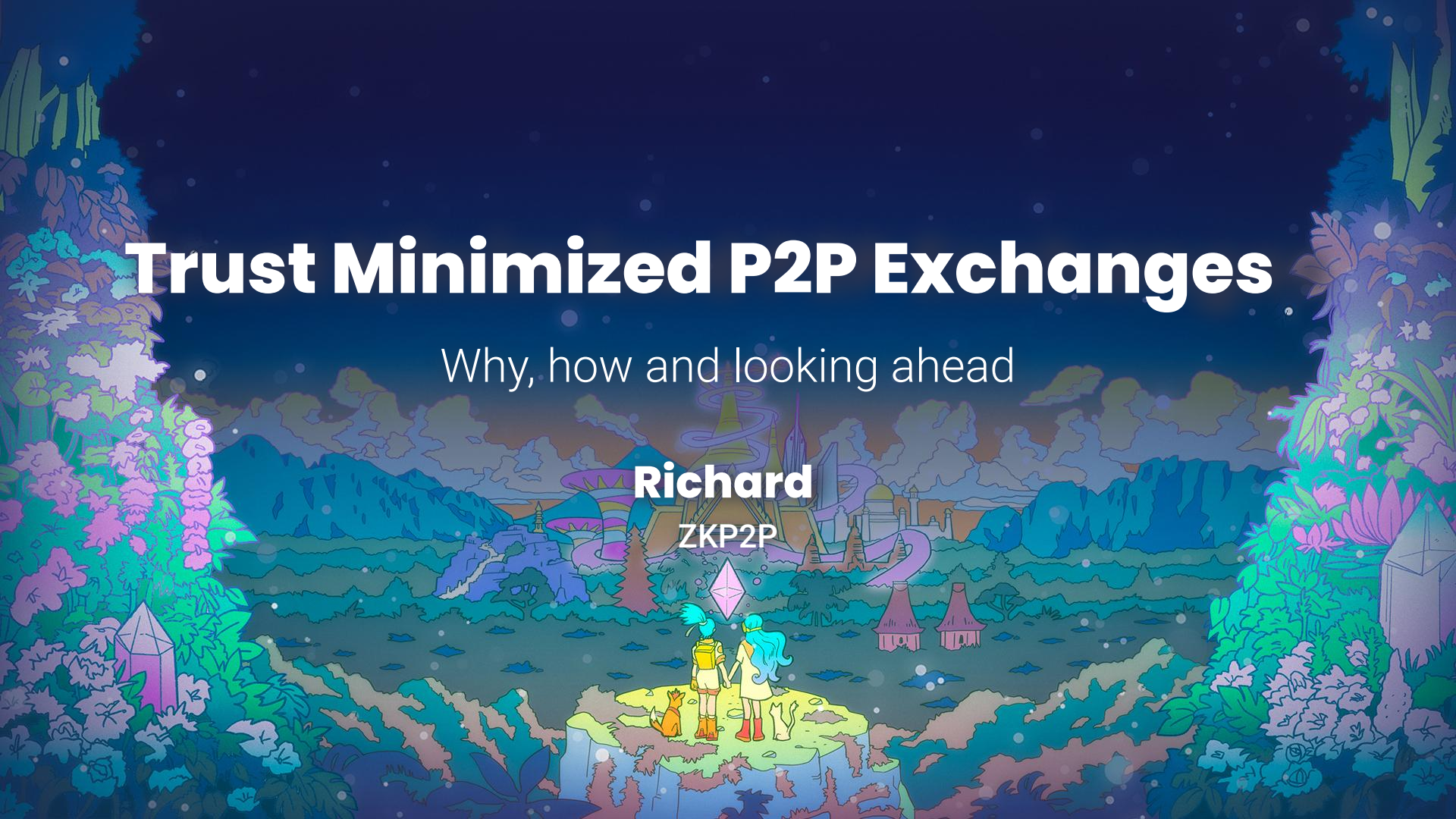# Trust Minimized P2P Exchanges

Why, how and looking ahead

Richard

ZKP2P

Why are we here?

Web 2 ‹

Fiat currencies

Social graph

Concert tickets

Domains

Centralized data silos
- High switching costs
- Extractive to users, monopolistic
- Closed APIs

Web 2 › Web 3

Web 2

Fiat currencies

Social graph

Concert tickets

Domains

Centralized data silos
- High switching costs
- Extractive to users, monopolistic
- Closed APIs

Web 3

Social graph

Stablecoins

DeFi instruments

ETH

Our permissionless database
- Parallel system from the real world
- Most of DeFi is self-referential
- "let me give you tokens to stake for more tokens"

Solution: bring the Real World to Ethereum

How?

Breaking walled gardens with cryptography (and TEEs)

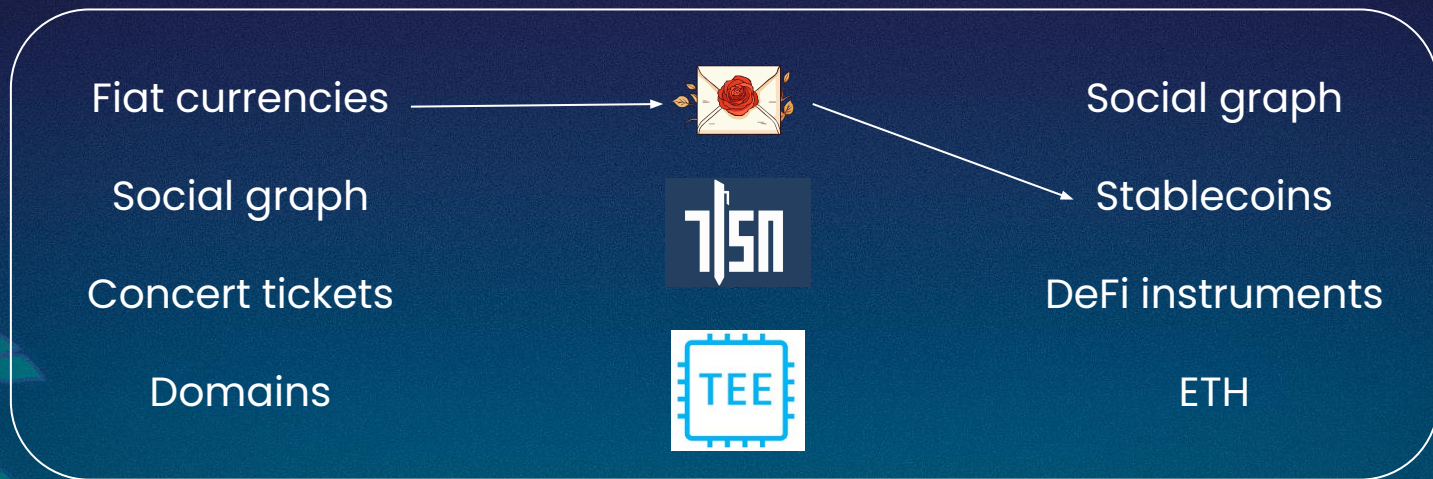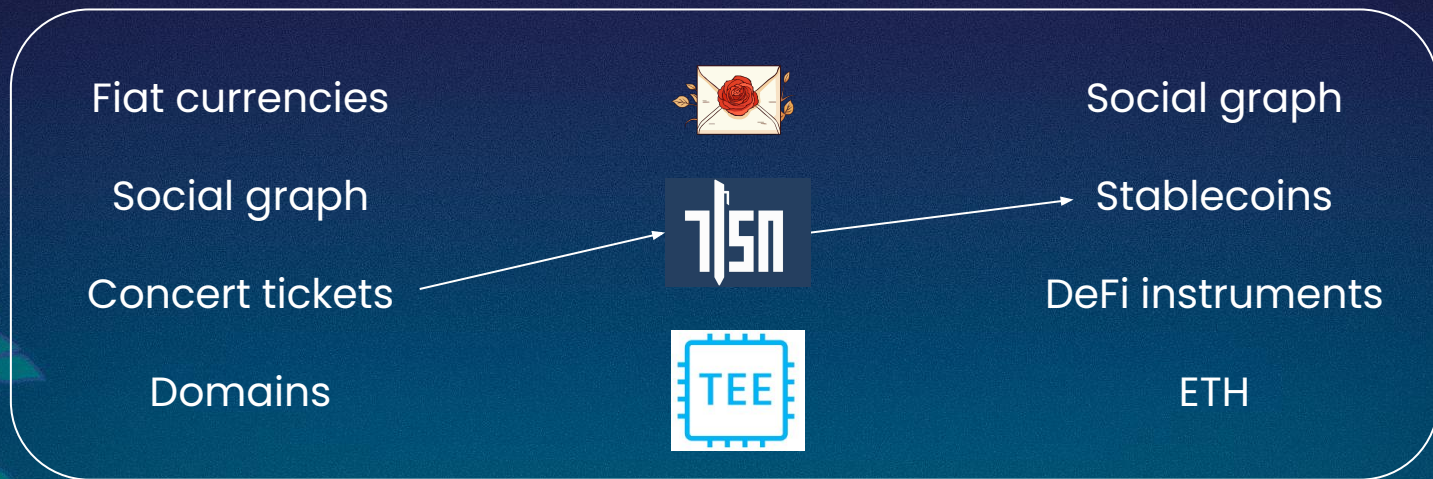|		
Fiat currencies		Social graph
Social graph		Stablecoins
Concert tickets		DeFi instruments
Domains		ETH

- Advancements to cryptography (ZK, MPC) allow us to **permissionlessly** export data from existing data silos
- Techniques such as ZKEmail and TLSNotary allow redacting sensitive data prior to export
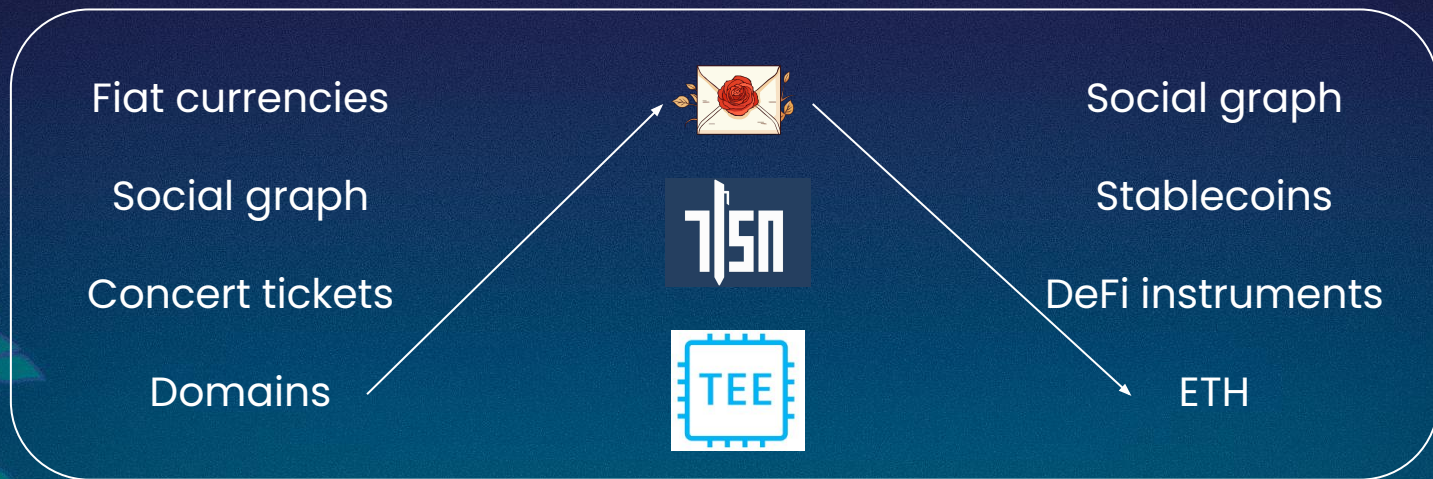
Web2 <> Web3 Integration

Fiat currencies → Social graph

Social graph → Stablecoins

Concert tickets — DeFi instruments

Domains — ETH

- With cryptography (and TEEs), now you can compose web2 actions with web3 actions

Web2 <> Web3 Integration

Fiat currencies

Social graph

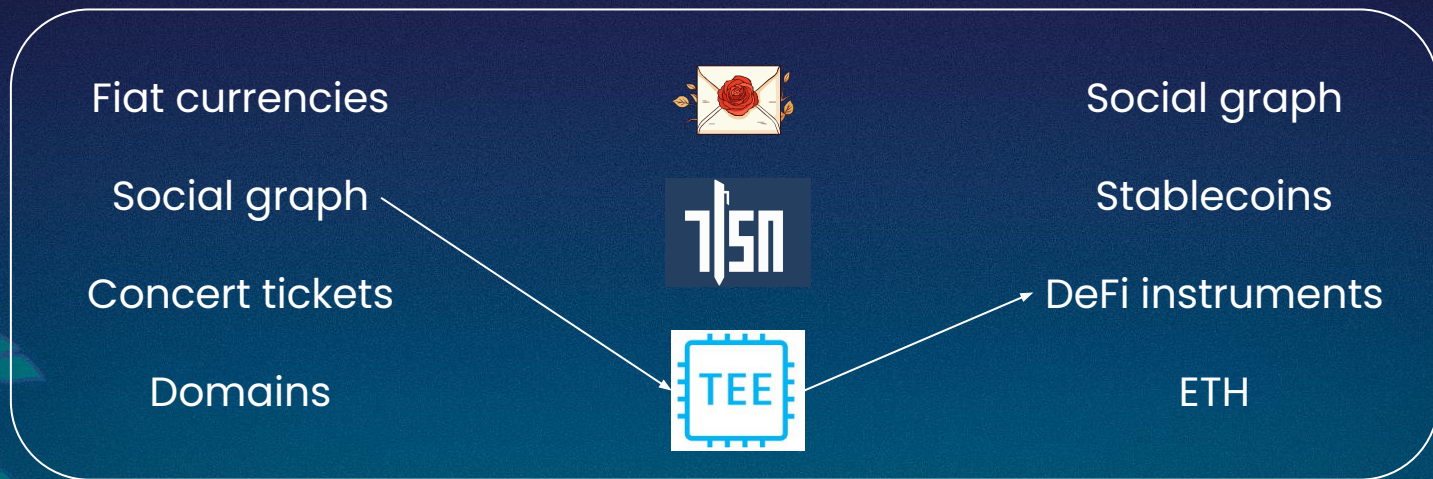Concert tickets

Domains

Social graph

Stablecoins

DeFi instruments

ETH

- With cryptography (and TEEs), now you can compose web2 actions with web3 actions

Web2 <> Web3 Integration

Fiat currencies

Social graph

Concert tickets

Domains

Social graph

Stablecoins

DeFi instruments

ETH

- With cryptography (and TEEs), now you can compose web2 actions with web3 actions

Web2 <> Web3 Integration

Fiat currencies

Social graph

Concert tickets

Domains

Social graph

Stablecoins

DeFi instruments
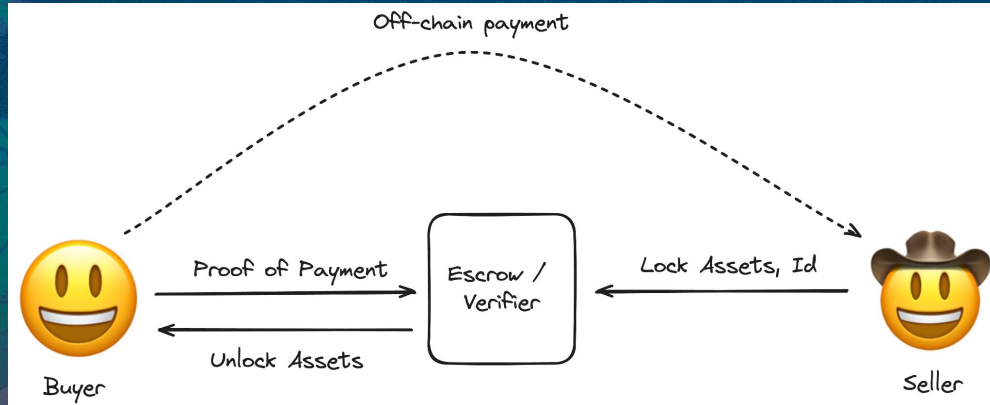
ETH

- With cryptography (and TEEs), now you can compose web2 actions with web3 actions

Example: P2P Onramp / Forex

- ZKP2P - trust minimized P2P marketplace for fiat <> stablecoins
  - Problem: ~6% fees all-in for existing solutions
- CEX (Binance) → escrow smart contract
- Manual unlock of escrow → instant unlock upon satisfying predicate using ZKEmail and TLSNotary proofs
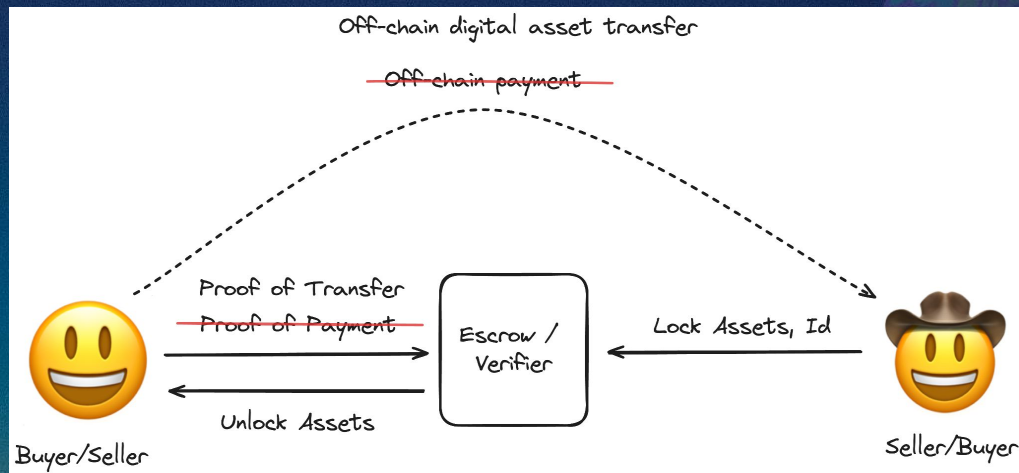

Swap

Platform: Venmo
Currency: USD

Requesting: 10 USDC   Balance: 0 **Max**

You send: 10.24 USD   Best available rate: 1.023

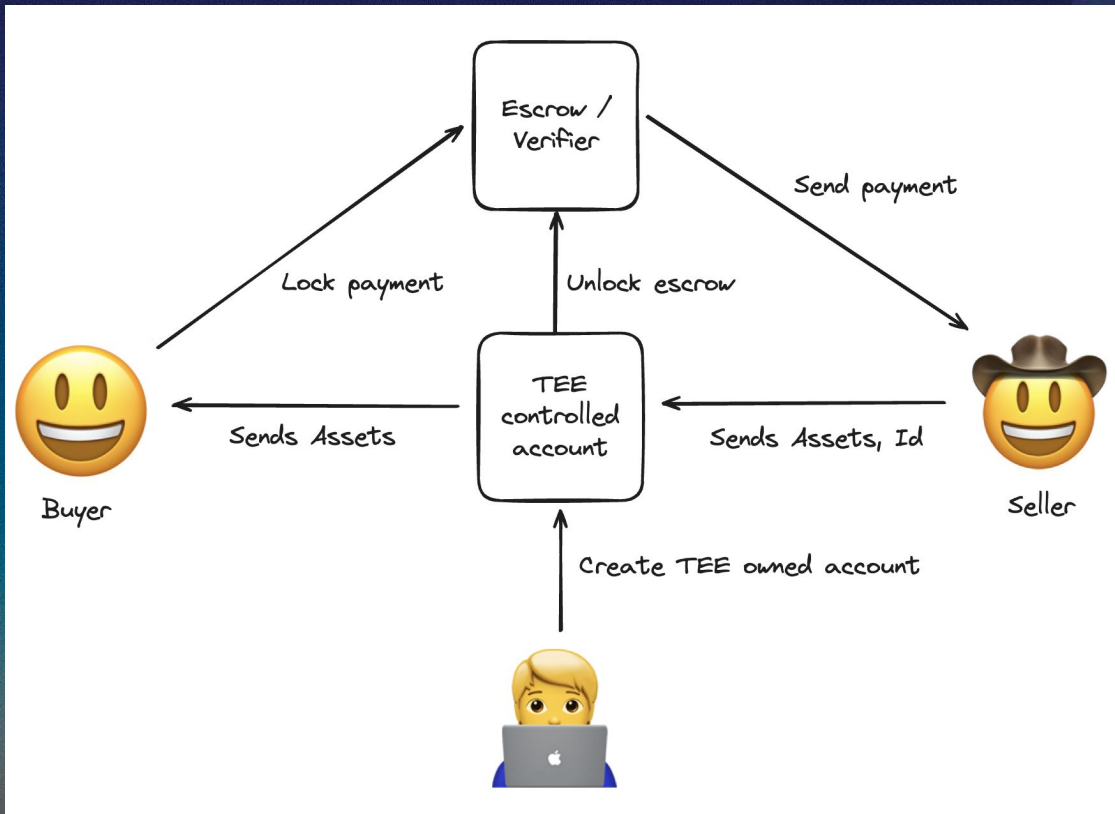**Complete Registration**

Instructions

Beyond fiat P2P marketplaces

- P2P trading tickets ✅
- P2P trading domains ✅
- P2P trading social media handles
- P2P trading CS Go skins
- P2P trading gift coupons etc
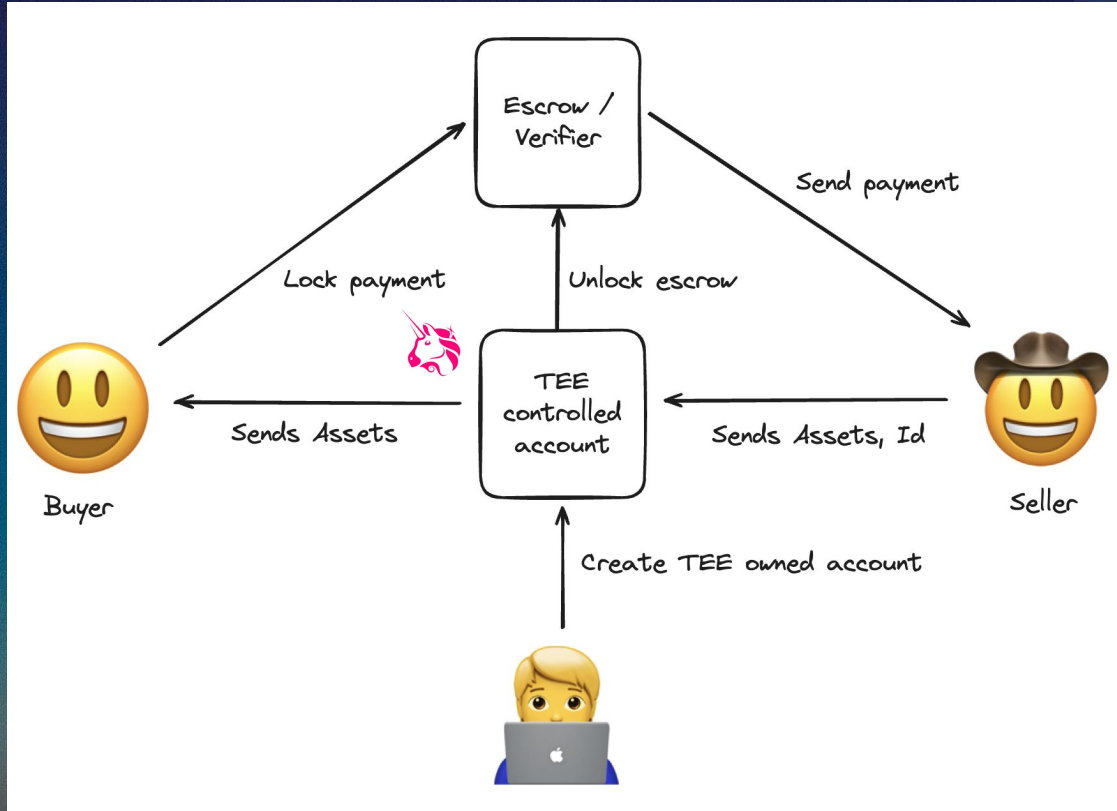- P2P trading of ZK proofs (identities)

Off-chain digital asset transfer

~~Off-chain payment~~

Proof of Transfer
~~Proof of Payment~~

Escrow / Verifier

Lock Assets, Id

Unlock Assets

Buyer/Seller

Seller/Buyer

Beyond P2P (TEEs)

- Put web2 account in a TEE
- Trusted third party

Beyond P2P (TEEs)

- Now the web2 account is programmable. I.e. TEE AMM
- Unlock escrow and send off-chain asset in 1 transaction

Time to build!

- The design space is huge for trust minimized marketplaces
- The tech is ready
  - zkEmail
  - TLSNotary
  - Proxy TLS (Reclaim)
  - TEEs
- Time to bring the real world onto Ethereum!

Thank you!

Richard
ZKP2P
Twitter: @richardzliang @zkp2p