Programmable Privacy

Are we stuck?

27.05.2025

Marti - NP Labs

Blockchains to date

	Transfers	Programmable
Public	Bitcoin	Ethereum
Private	Zcash	Covered today!

Why do we need onchain privacy?

(not so) 🔥Hot take🔥:

Success of web3 depends on institutional adoption.

No privacy = no adoption

Talk outline

1) Privacy: anonymity vs. confidentiality

2) Case study: token exchange

3) Overview of approaches

    a) Shielded pools & **AMM**

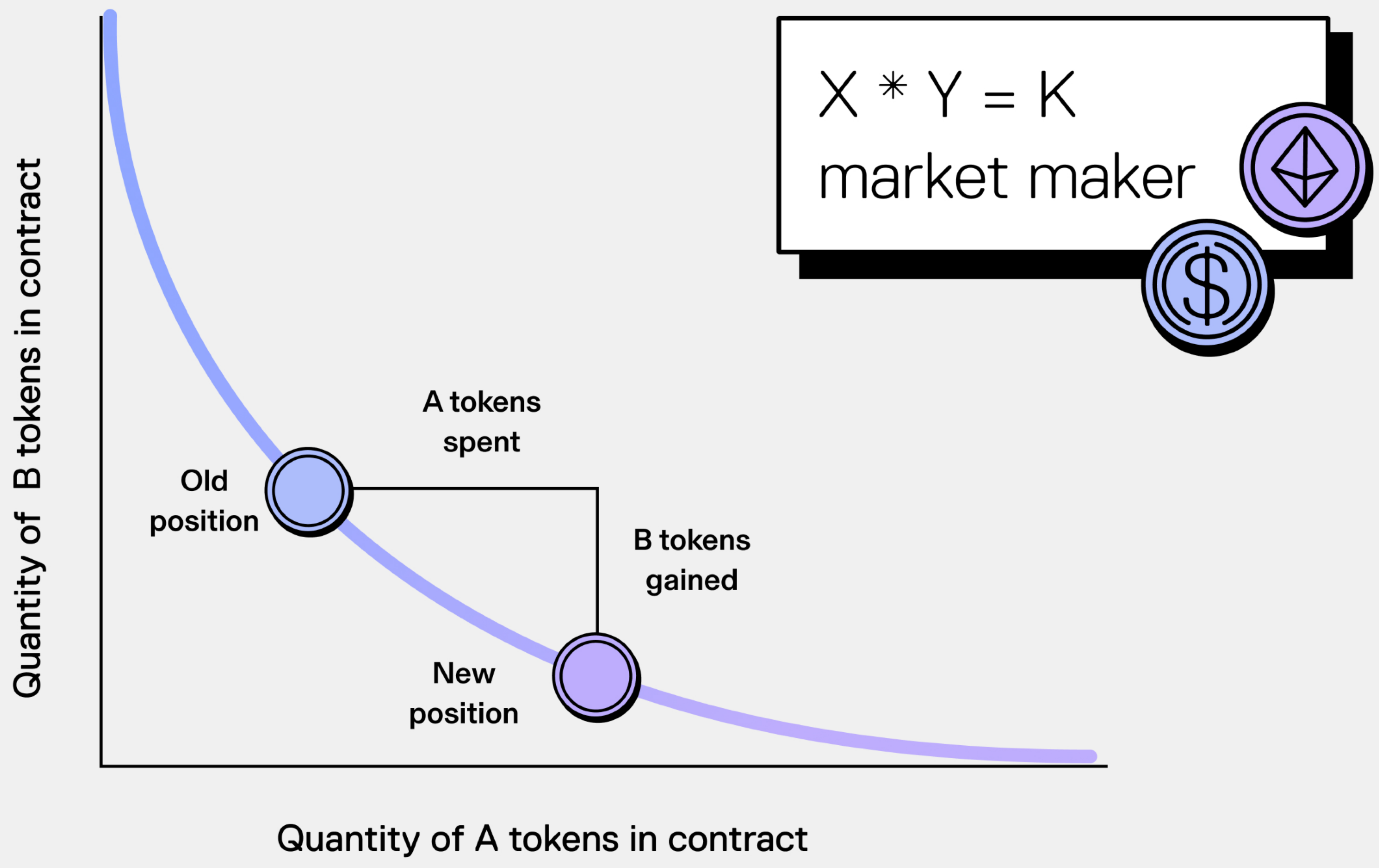
    b) Edge execution & **orderbook**

    c) Private shared state & **dark pool**

What is privacy?

Anonymity (who?)	Confidentiality (what/how much?)
Someone holds 10 ETH	Alice holds *some token*

Token swap today (simplified)


Quantity of B tokens in contract
A tokens
spent
Old
position
B tokens
gained
New
position
Quantity of A tokens in contract

X * Y = K
market maker

Token swap today (simplified)

UX

- Peer-to-protocol (no counterparty online) ✓

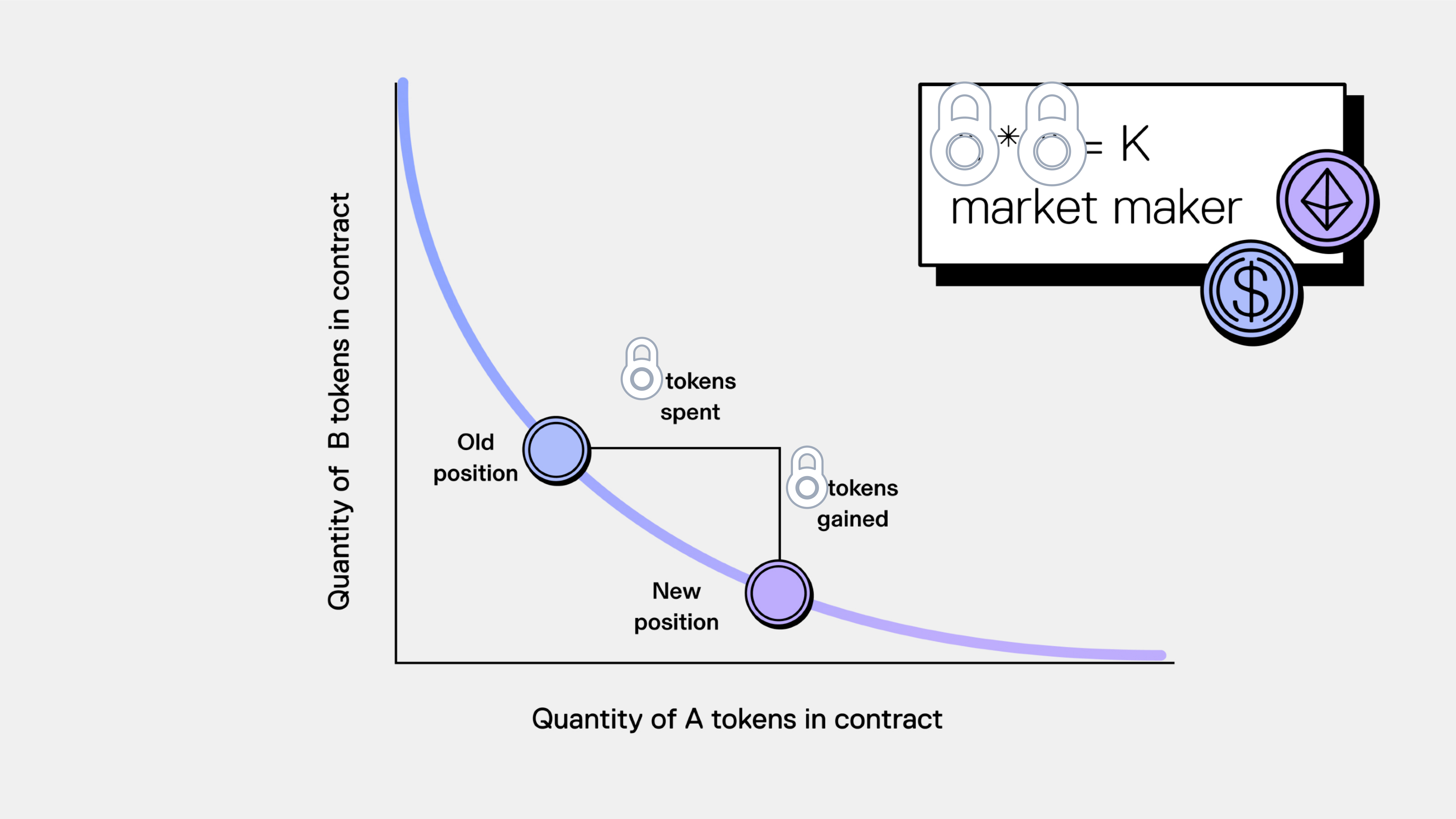
cost

- Transparent pricing ✓
- Susceptibility to arbitrage ✗

Privacy

- No privacy ✗

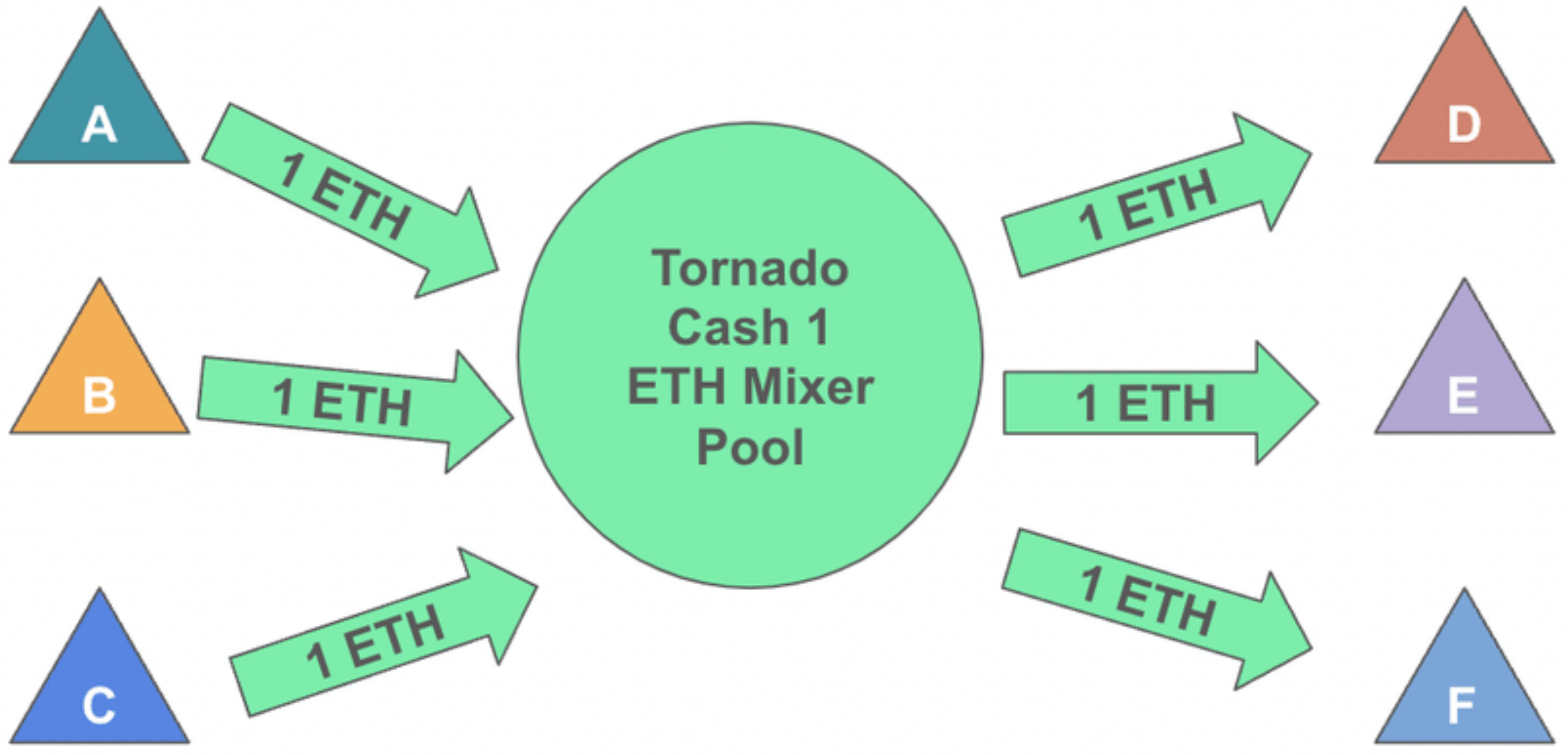
Private token swap (broken)



What to do, how to swap?

Shielding pools (a.k.a. mixers)	Edge execution (accounts & notes à la ZEXE)	Private shared state (a.k.a. delegated state)
Users mix their funds, withdraw to a fresh address.	Users execute and prove their own state transition (edge); validators verify proofs.	A network of nodes compute on private state from multiple parties.

Shielding pools



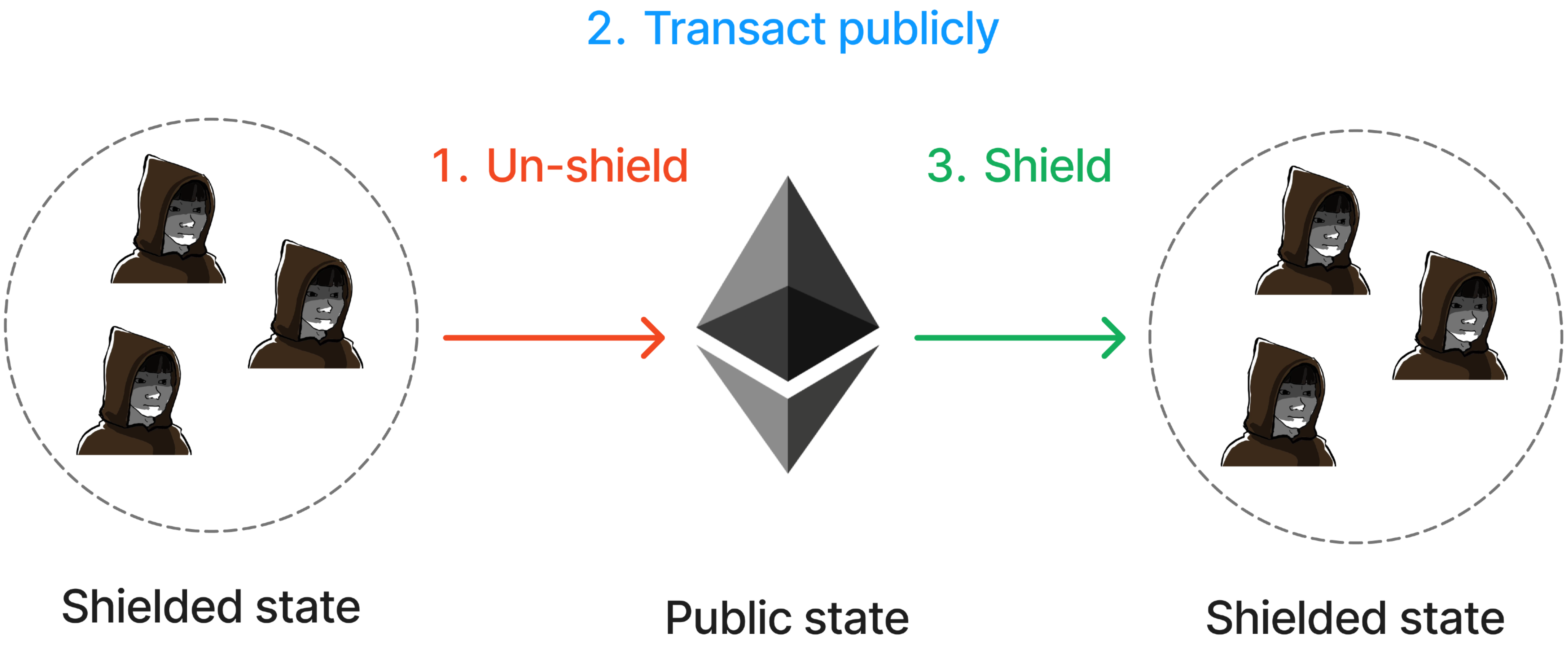
To **deposit** into the pool:

- Lock 1 ETH in the smart contract
- Sample a random value, commit to it (hiding), append to MT

Upon **withdrawal** from the pool, provide:

- Proof of knowledge of random value
- Proof of commitment present in MT
- Unspent nullifier

Shielding pools



2. Transact publicly

1. Un-shield

3. Shield

Shielded state

Public state

Shielded state

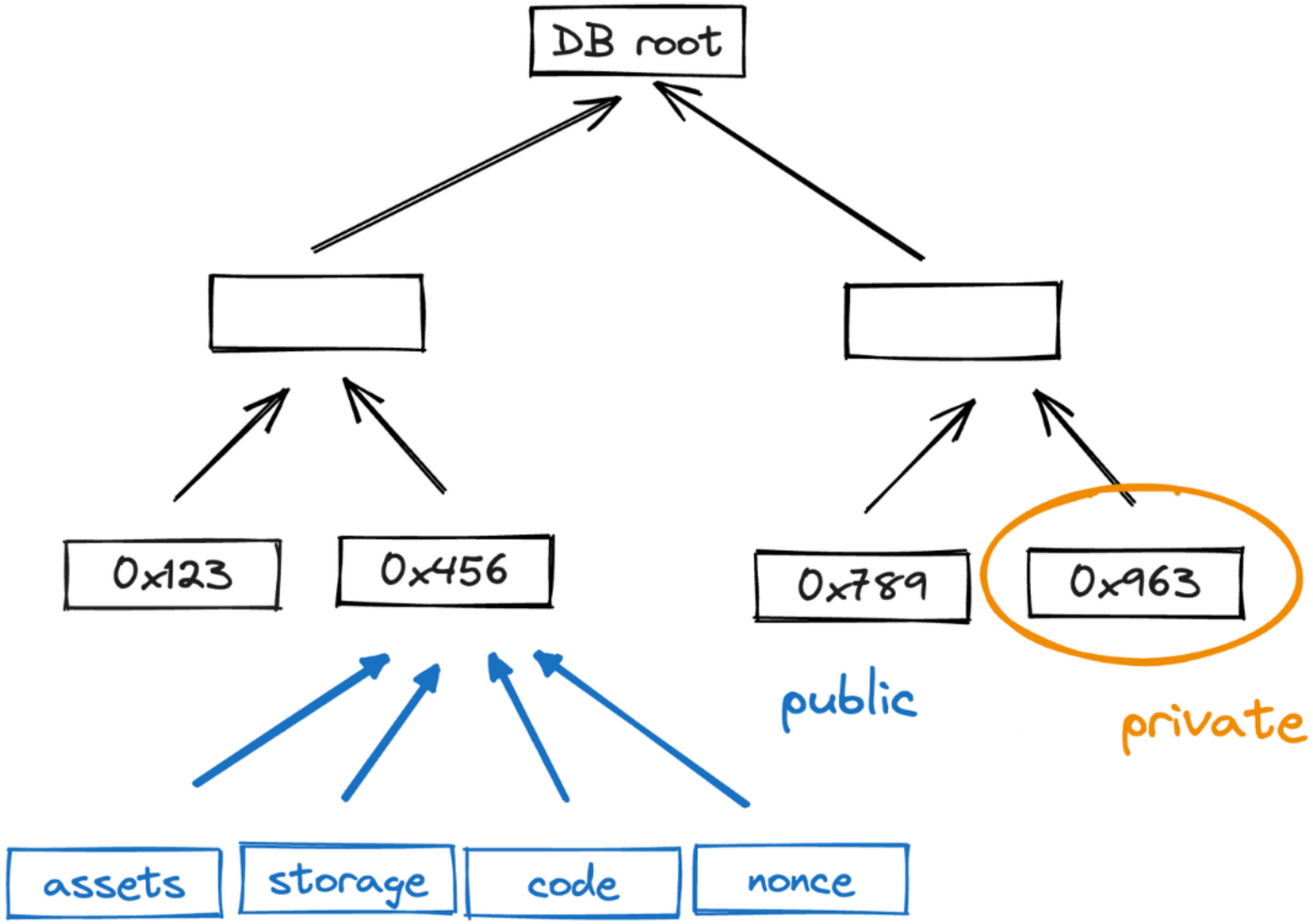
Shielding pools: AMM

Anonymity	Confidentiality	Performance	DevEx
🟢*	🟡	🔴	🟢

* depends on anonymity set

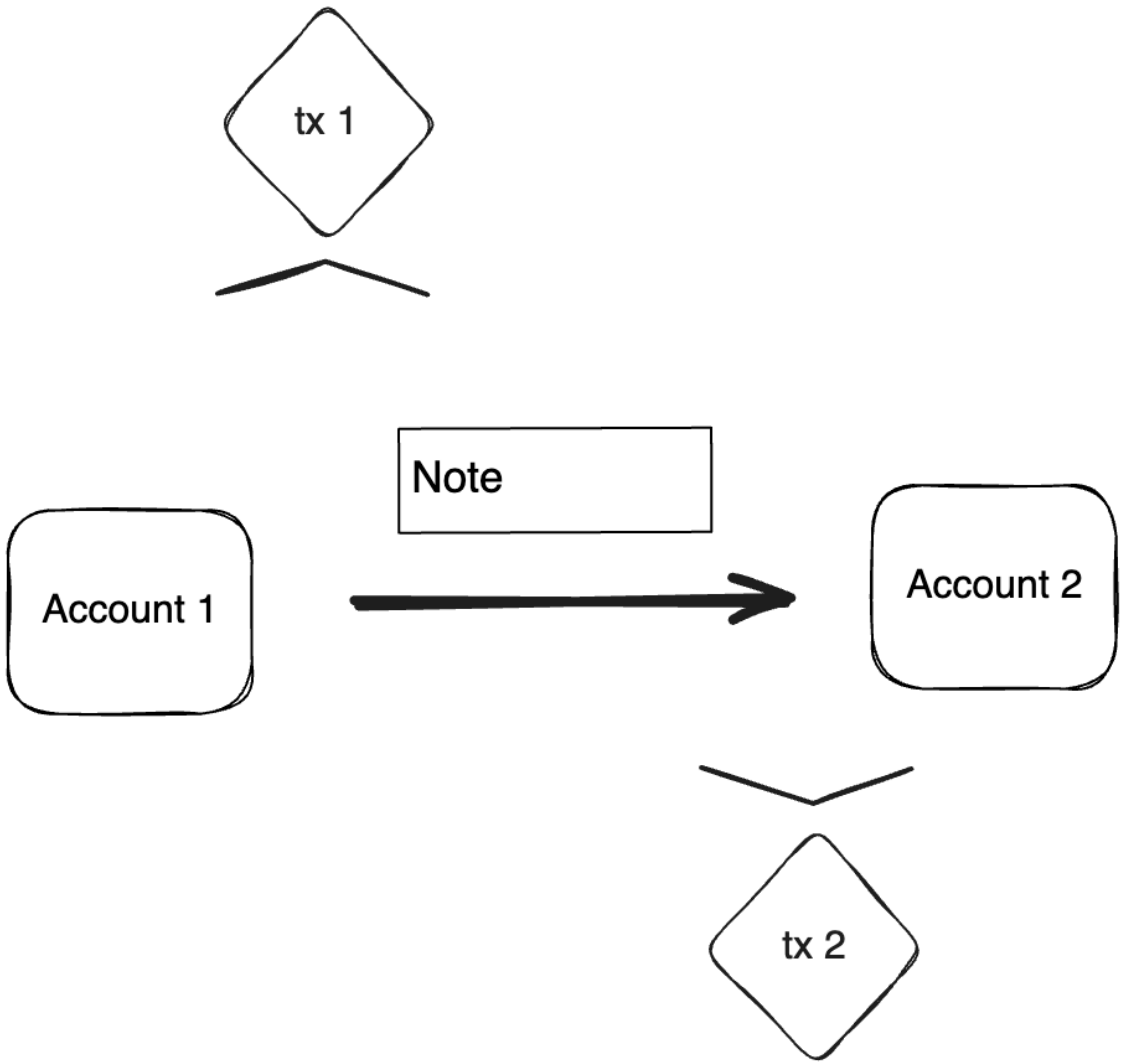
Edge execution

- Only account *commitment* onchain
- Account *data* owned by user



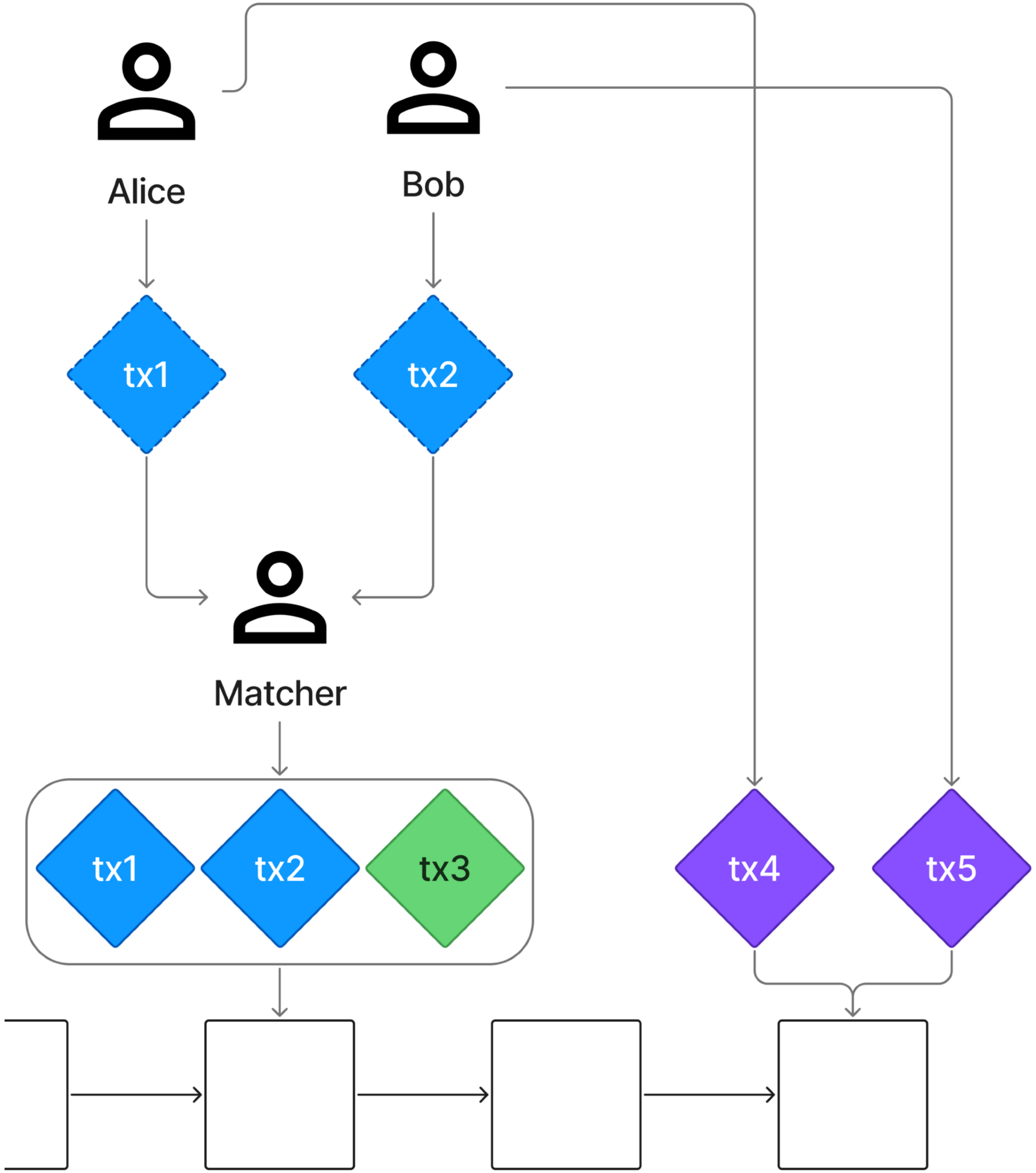
Edge execution

- Value transferred via *notes*
- *Create* a note in one tx
- *Consume* a note via another tx
- Proof associated with each state transition



Edge execution: orderbook

- Self-custody: *notes* have programmable spend conditions
- Trustless intermediary matches orders and submits onchain
- Users claim *payback notes*
- Fully parallelizable: no global state



Edge execution: orderbook

Anonymity	Confidentiality	Performance	DevEx
🔴	🟢	🟢	🟡

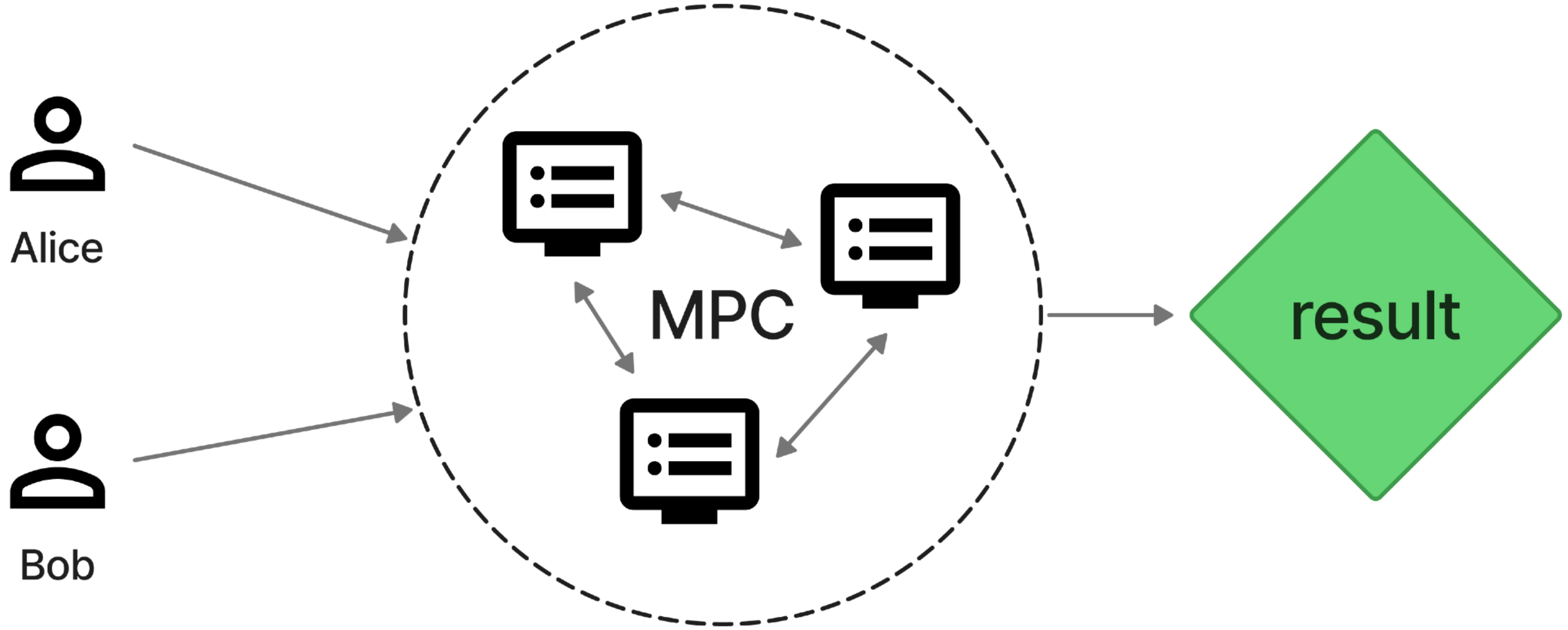
Private shared state

- Multiple parties contribute *private state*

encrypted vote,

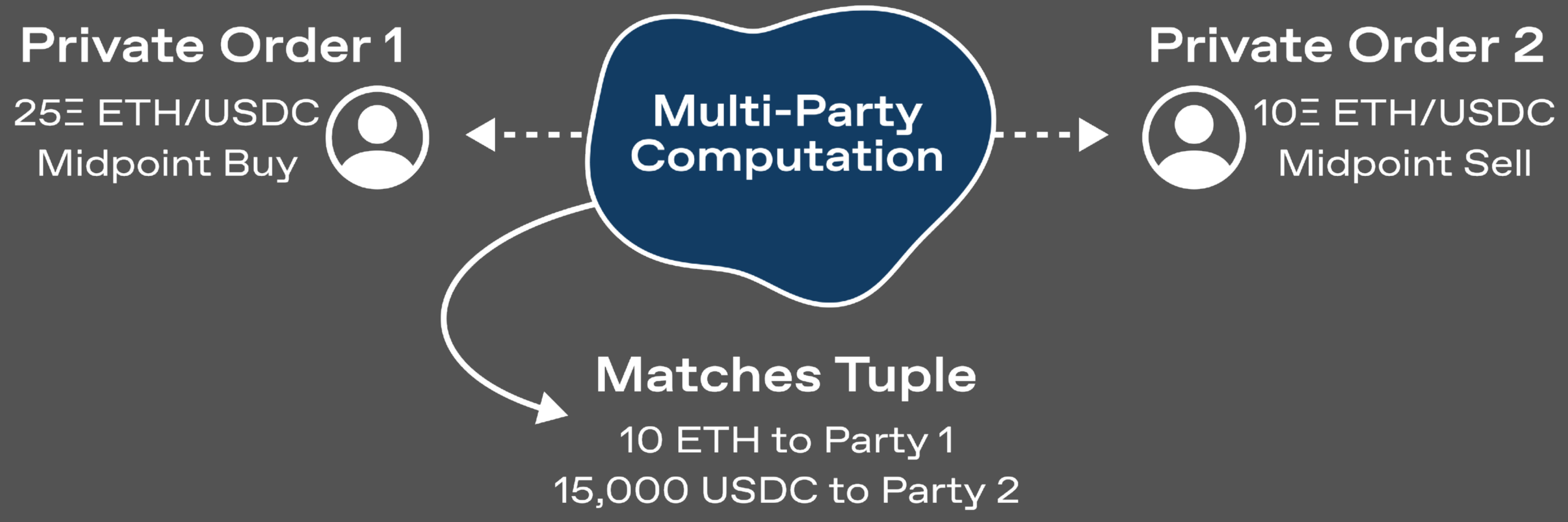
marketplace order, …

- Network of nodes participate in MPC to compute a function on *private states*
- Eventually, reveal the result



Private shared state: Dark pool

- Two users commit to their order requests (*private state*)
- Run a matching engine in MPC (compute on private states)
- Result:
  - Match found (submitted onchain by either party), or
  - No match (no information leaked, proceed to another peer)
- Pairwise p2p (but intermediated by relayers in practice)



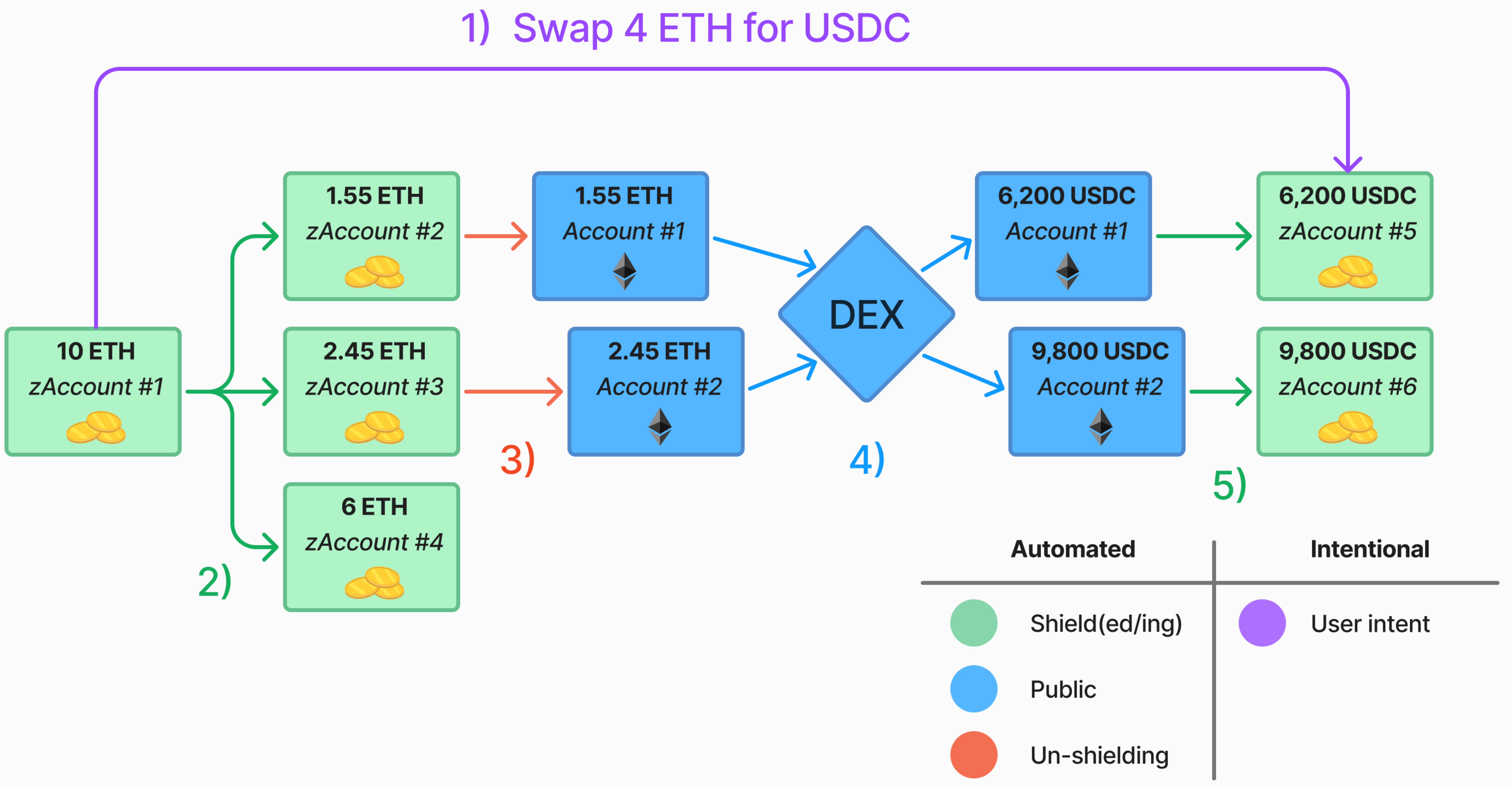
Private shared state: dark pool

Anonymity	Confidentiality	Performance	DevEx
🟢	🟢	🔴	🔴

Comparison

	Shielding pools: AMM	Edge execution: orderbook	Private shared state: dark pool
Anonymity	🟢*	🔴	🟢
Confidentiality	🟡	🟢	🟢
Performance	🔴	🟢	🔴
DevEx	🟢	🟡	🔴

Improvement: private hops (a.k.a. z2z in Zcash)



Comparison: the bright future

	Shielding pools: AMM	Edge execution: orderbook	Private shared state: dark pool
Anonymity	🟢	🟢	🟢
Confidentiality	🟢	🟢	🟢
Performance	🔴	🟢	🔴
DevEx	🟢	🟡	🔴

Closing thoughts

- **Shielding pools**: hard to scale at application level
  - Can build shielding primitives into the protocol instead: EVM+
- **Edge execution** would benefit from public accounts
  - Unlocks “standard” web3 use-cases (but not parallelizable)
- **Private shared state** opens up new use cases, but use with care
  - Voting ✓
  - Decentralized exchange ✗

Sources

- **Tutela:** An Open-Source Tool for Assessing User-Privacy on Ethereum and Tornado Cash
    - **https://www.researchgate.net/publication/357925591_Tutela_An_Open-Source_Tool_for_Assessing_User-Privacy_on_Ethereum_and_Tornado_Cash**
- **Miden** Docs:
    - **https://0xmiden.github.io/miden-docs/**
- **Renegade** Docs:
    - **https://docs.renegade.fi/core-concepts/mpc-explainer**
- **Differential Privacy in Constant Function Market Makers:**
    - **https://eprint.iacr.org/2021/1101.pdf**

Thank you

X & Telegram
@m2magician

marti@np.engineering

Marti