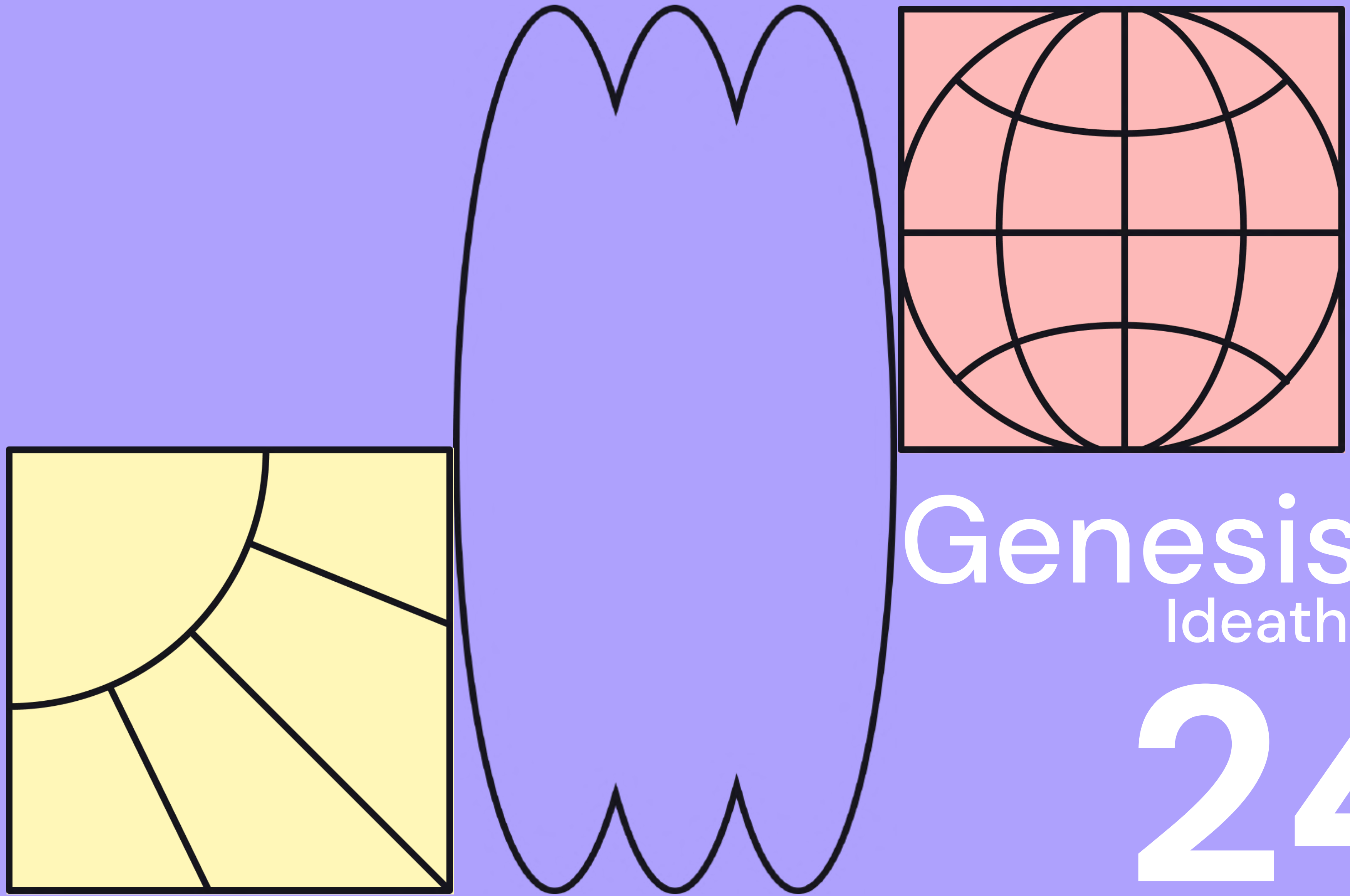
PRIVYCHAIN SOLUTIONS



Genesis
Ideathon
24

HOW DOES FINANCIAL PRIVACY IMPACT MODERN BUSINESSES?

PROBLEM STATEMENT

Users need to customize their own blockchain to make transactions more secured and private

Target Corporation

Theft of transaction information because of vulnerability of the network infrastructure → compromised the confidential information of partners and 40 million customers

1

LAYER I SOLUTION

PERMISSIONED CHAINS + ROLLUPS

CUSTOMIZED PRIVATE BLOCKCHAIN

SOLUTION

permissioned chains

+

Rollups

PRIVATE CHAINS
BASED ON THE
PUBLIC CHAIN

Pirvate Addresses Defintion

□ **Seed Generation**:

- Generates a random 256-bit seed.

□ **Master Keys Generation**:

- Uses HMAC-SHA512 with the seed to generate a master private key and chain code.

□ **Derivation Path**:

- Defines the BIP-44 path for Ethereum: m / 44' / 60' / account' / change / address_index.

□ **Child Key Derivation**:

- Derives child keys from the master keys using the specified path.

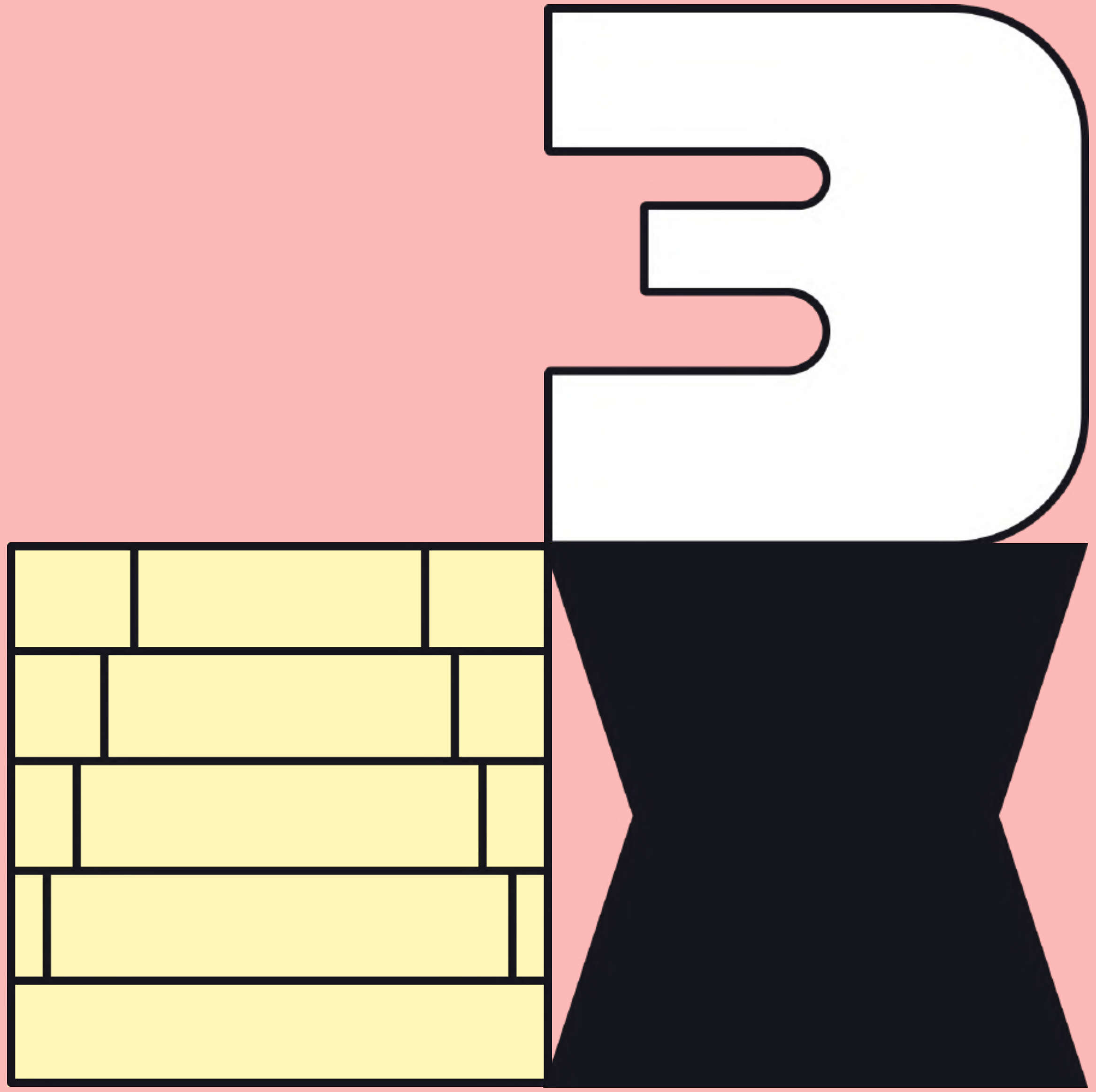
□ **Ethereum Address Generation**:

- Converts the derived private key to an Ethereum address by computing the public key and then hashing it with Keccak-256

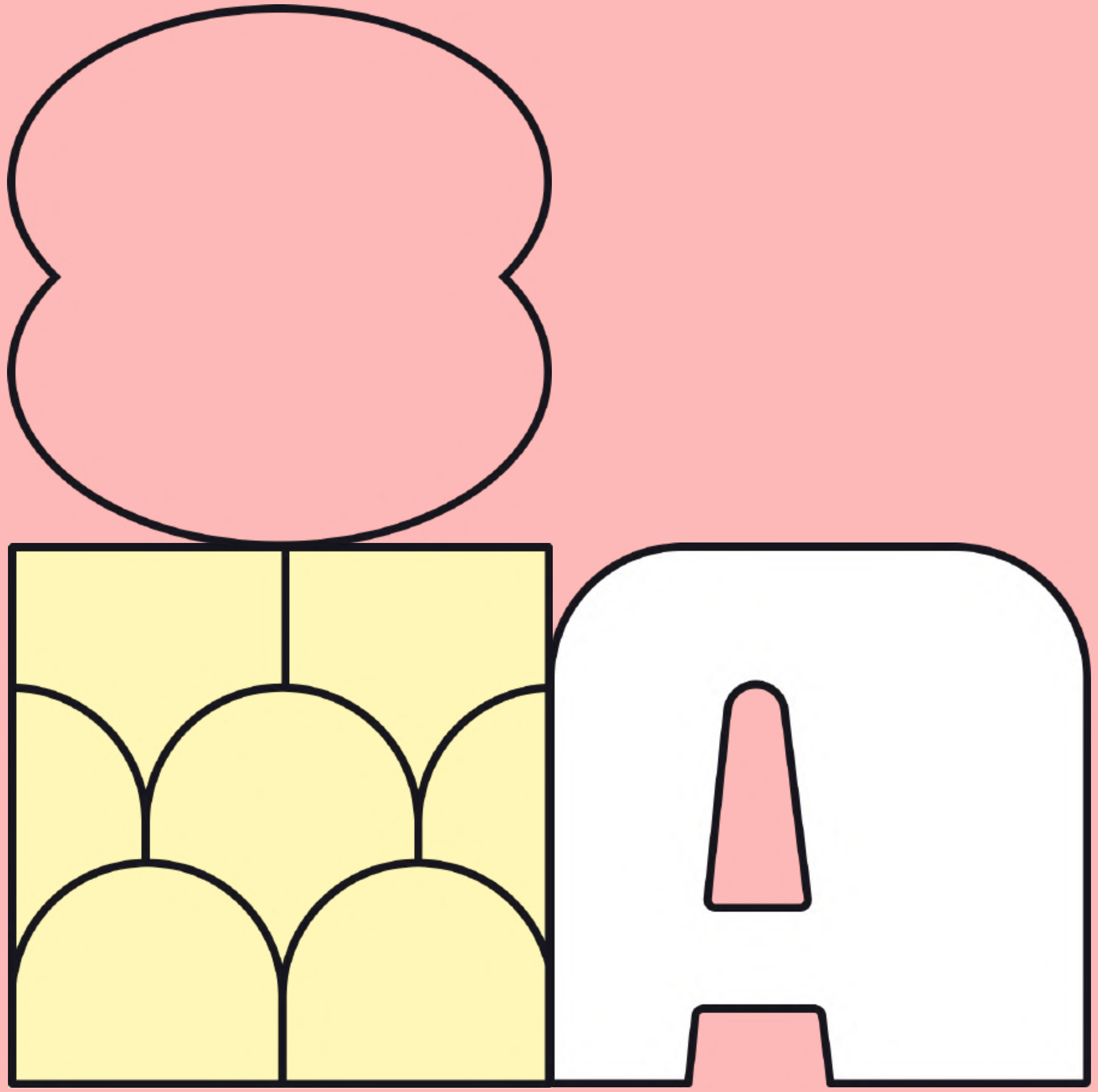
SOLUTION

Hierarchical Deterministic (HD) Wallets based on Ethereum-specific BIP-44 standard.

1. **Seed Generation**:
    - Start with a high-entropy seed, usually 128 to 256 bits. This seed is the master private key.
2. **Master Keys Generation**:
    - Generate a master private key and a master chain code from the seed using HMAC-SHA512.

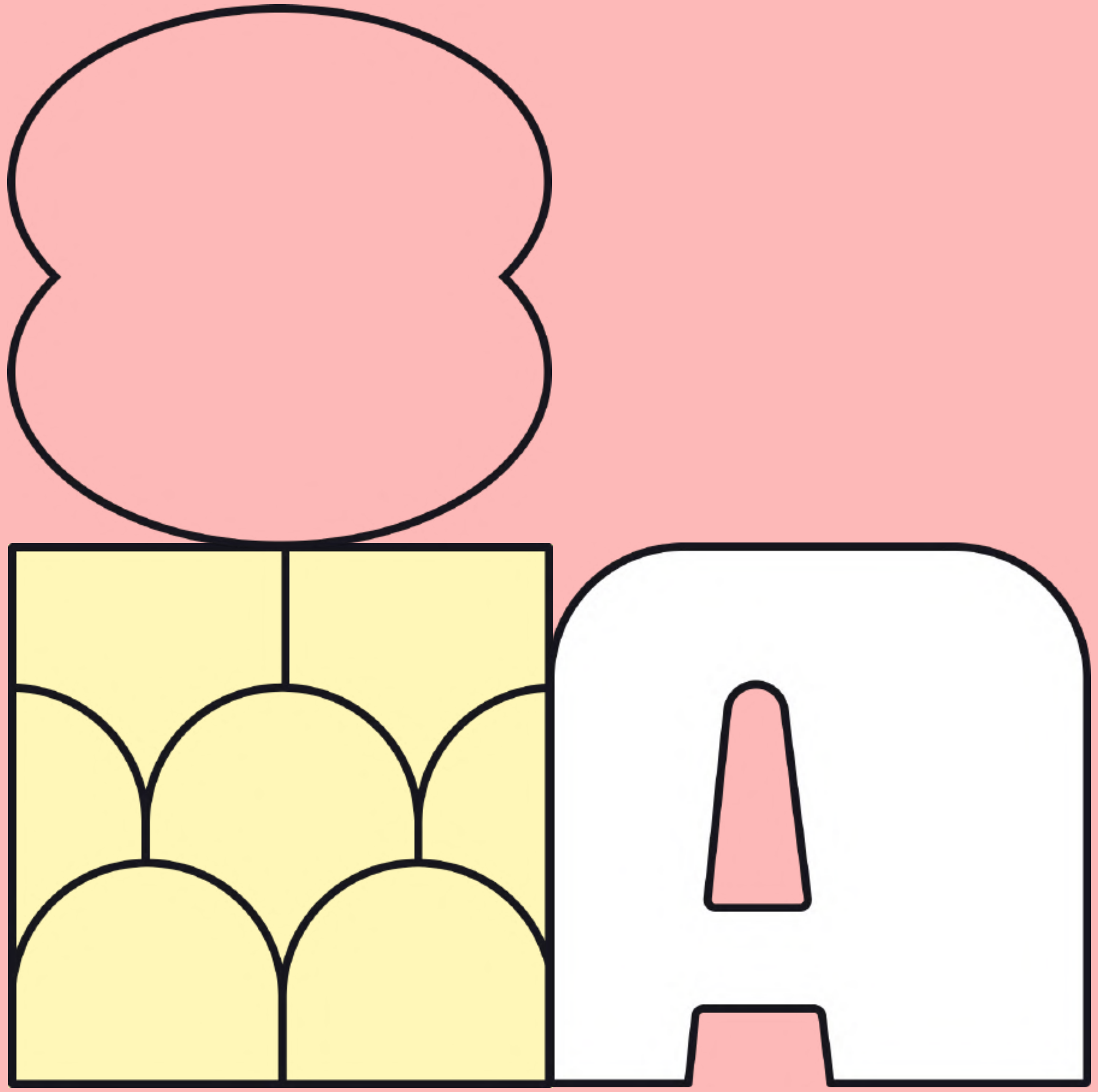


HIERARCHICAL DETERMINISTIC (HD) WALLETS



3. **Derivation Path for Ethereum:**
   - Use the BIP-44 derivation path for Ethereum: m / 44' / 60' / account' / change / address_index.
     - m refers to the master node.
     - 44' is a constant indicating BIP-44.
     - 60' is the coin type for Ethereum.
     - account allows for multiple user accounts.
     - change is 0 for external addresses and 1 for internal/change addresses.
     - address_index is an incrementing index to generate multiple addresses.

HIERARCHICAL DETERMINISTIC (HD) WALLETS



4. **Child Key Derivation:**
   - Derive child private keys and chain codes from the master private key and chain code.
5. **Generate Ethereum Addresses:**
   - Convert the derived private keys to Ethereum addresses.

SOLUTION

ROLLUPS TO PUBLICH CHIAN

Collaboration and kindness took center stage.

1. **Transaction Aggregation**:

- Multiple transactions that occur within the private addresses are collected over a period of time. These transactions are typically stored and managed off-chain.

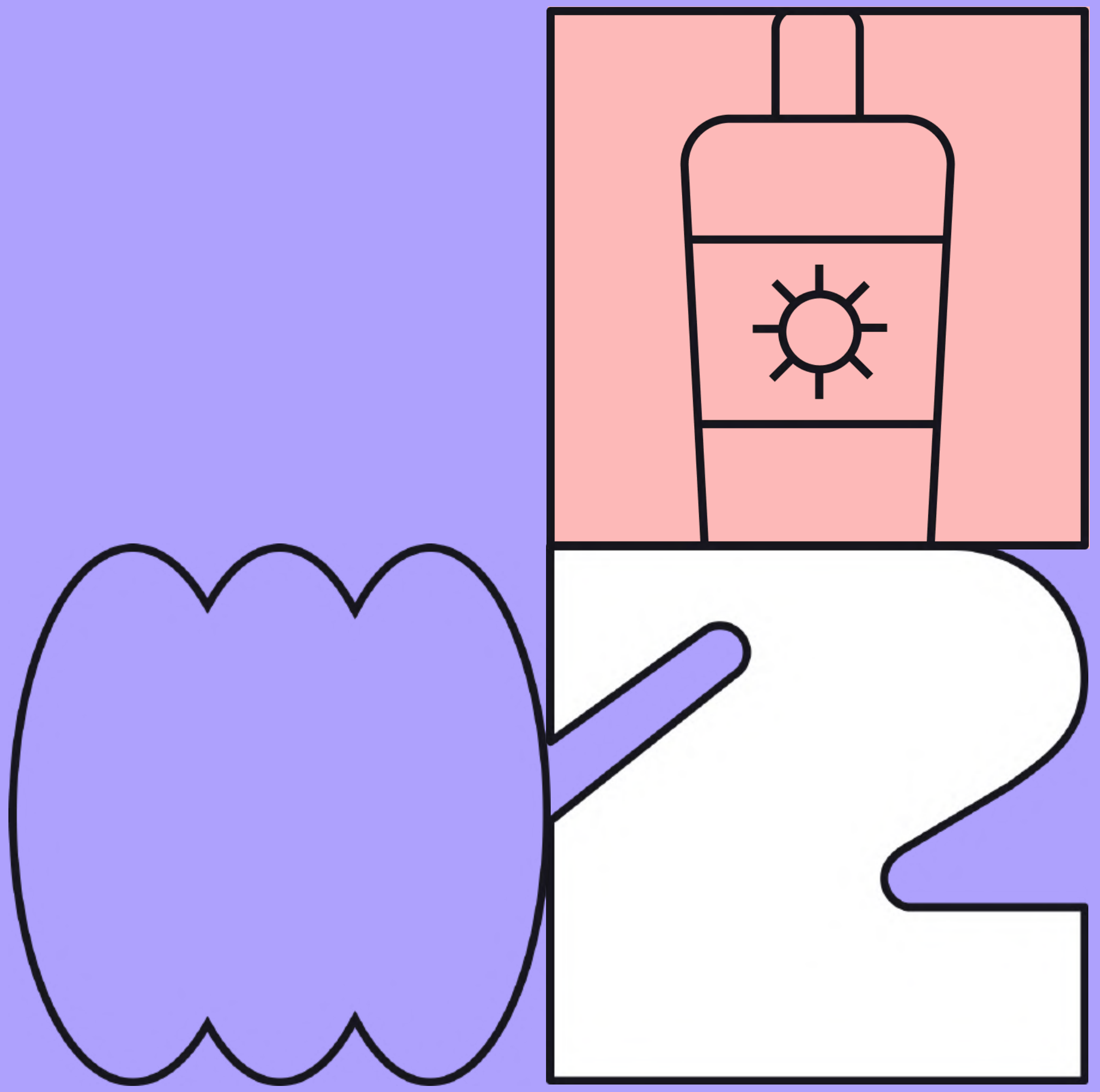
2. **State Transition and Proof Generation**:

- Compute the new state resulting from all the aggregated transactions. This includes updating balances, smart contract states, etc.

3. **Submission to the Public Blockchain**:

- Submit the aggregated transactions and the proof (for zk-rollups) or state root (for optimistic rollups) to the public blockchain. This usually involves a smart contract on the public chain that verifies the proof or handles disputes.

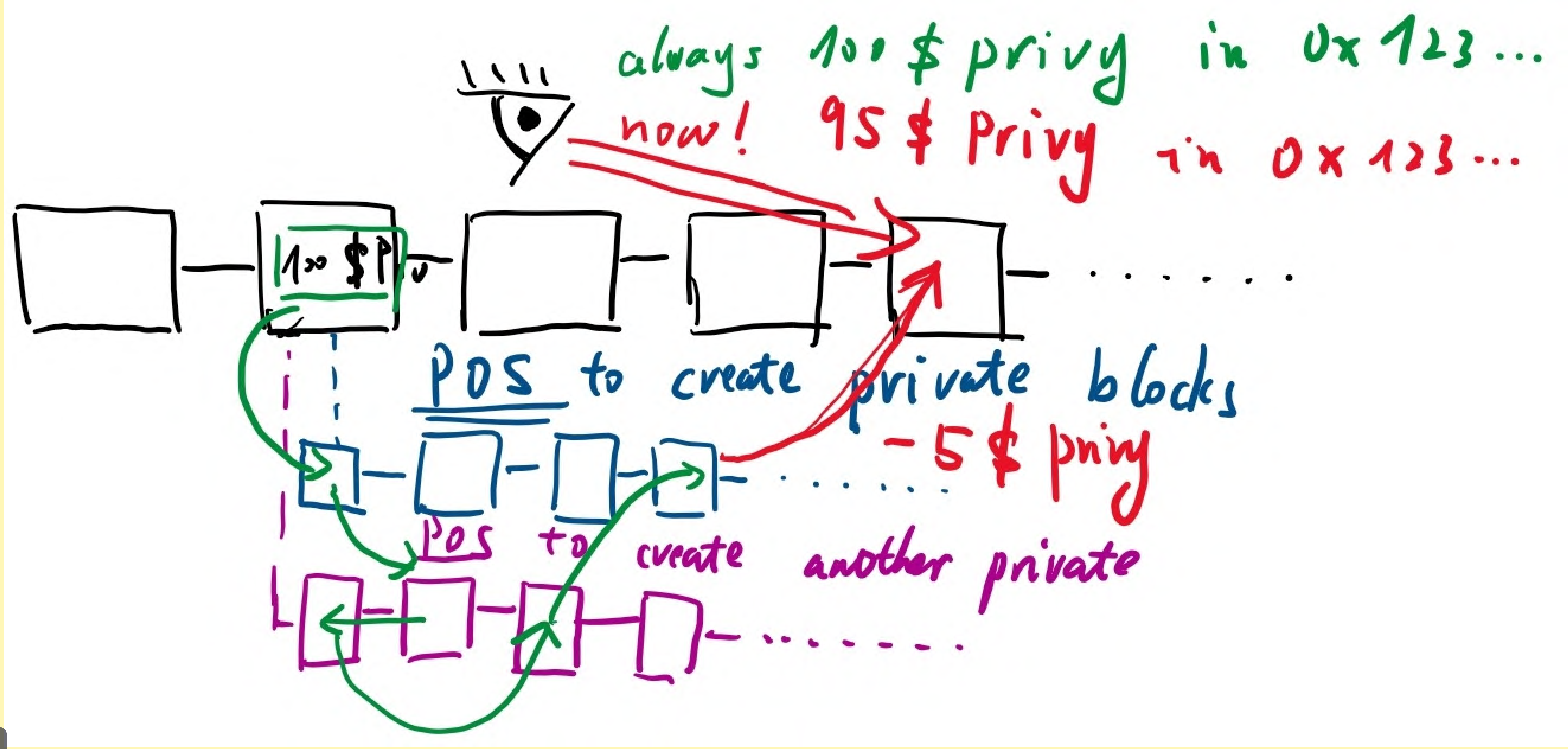
4. **Verification and State Update**



IMPACT

1. **Enhanced Privacy**
2. **Security**
3. **Competitive Advantage**
4. **Flexibility**

FEASIBILITY


always 100 $ privy in 0x123...
now! 95 $ Privy in 0x123...
100 $ Priv
POS to create private blocks
-5 $ priv
POS to create another private

THANK YOU

TEAM PRIVYCHAIN

AYŞENUR ÖZBEK

DANIIL KORENKOV

PHILLIP LI

XIYUE ZHANG