Decentralized Finance

An Introduction

Julien Prat (CNRS, Ecole Polytechnique)

DeFi

- Build a financial industry that relies on algorithmic rules instead of social rules to create trust.

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

DeFi

- Build a financial industry that relies on algorithmic rules instead of social rules to create trust.

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

DeFi

- Build a financial industry that relies on algorithmic rules instead of social rules to create trust.

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

DeFi

- Build a financial industry that relies on algorithmic rules instead of social rules to create trust.

Encoding back office Infrastructures

PLAN

1. Cryptography
2. Distributed Ledgers (DLTs) vs Blockchains
3. The Decentralized Computer
4. Decentralization & Programmability

DeFi

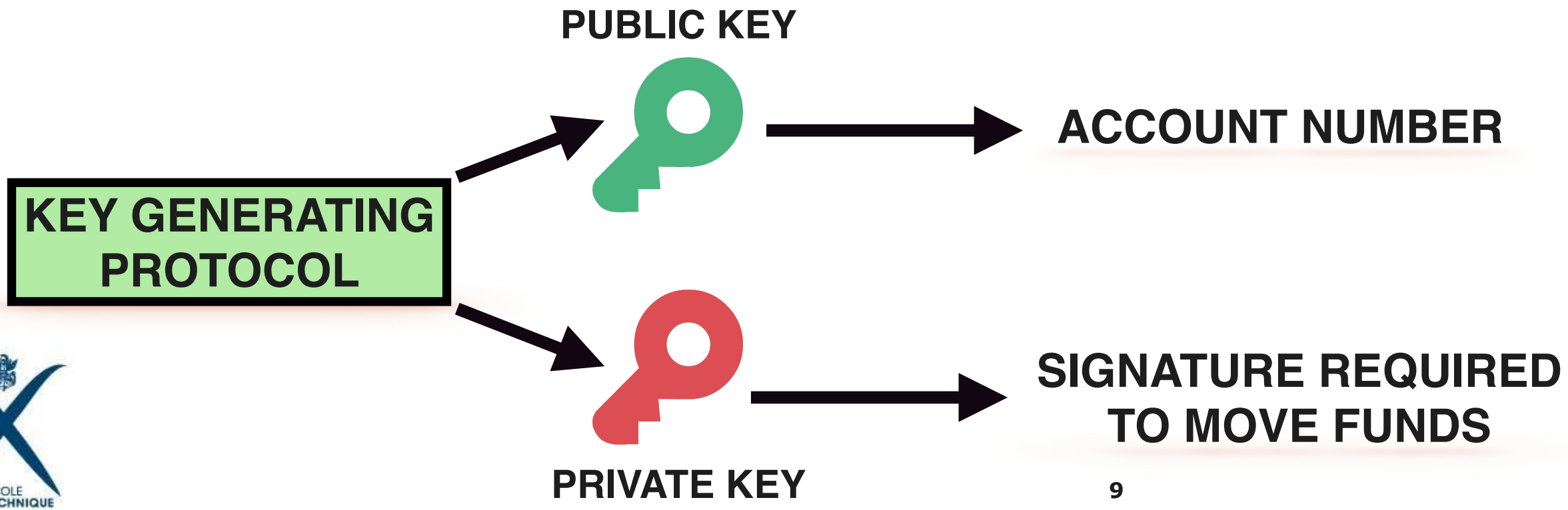
- **Build a financial industry that relies on algorithmic rules instead of social rules to create trust.**

- **First challenge:**
  - ✓ **Attract depositors**

Argentarii **counting money, Viminacium 3rd century CE**

Self-Custody

- Asymmetric cryptography allows depositors to control the custody of their funds.



Challenges of Self-Custody

- **Loss private key = Loss of funds!**
- **Transfers and thus errors are irreversible!**
- **User Experience is too complicated and risky for most users.**

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

Challenges of Self-Custody

- **User Experience is too complicated and risky for most users.**
- **Guardrails:**
  1. **Multisignature (protection against fat finger and embezzlement)**
  2. **Account Abstraction:**
     - ✓ Replace Account with *arbitrary code*
     - ✓ Permission Controls: Similar to multisignature
     - ✓ Account Recovery: Protection against loss or exposure of private key
     - ✓ Transaction limits…

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

Record Keeping

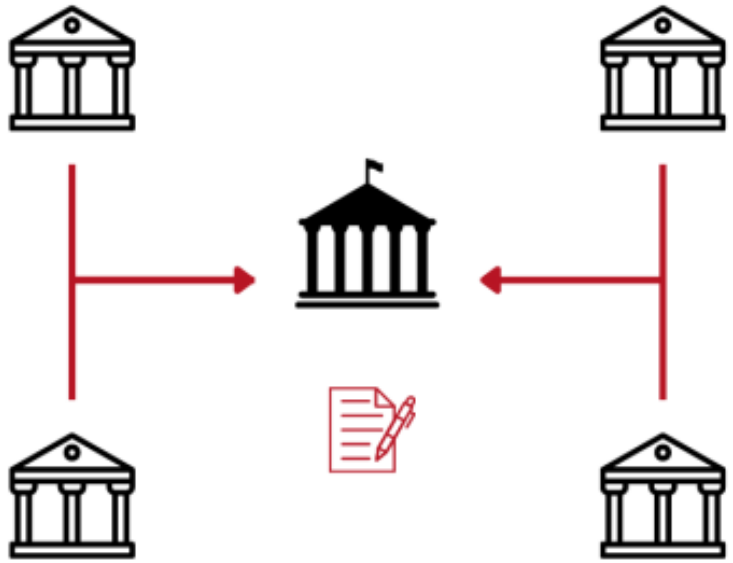
- Need a ledger that records who owns what.
- Cannot trust a central authority to keep records.
- Distribute ledgers across multiple entities.

E*xpectores* keeping record, Viminacium 3rd century CE

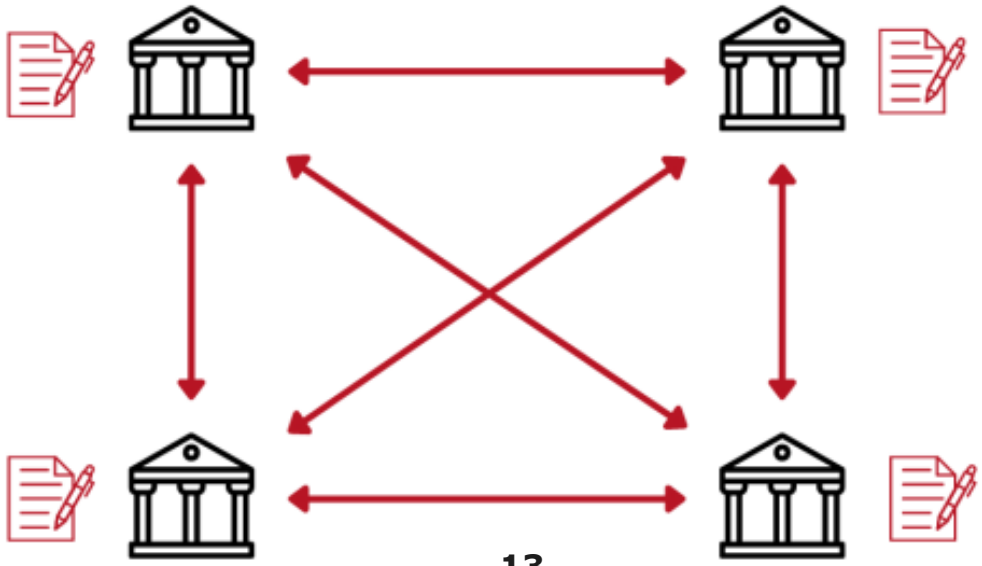
Distributed Ledger (DLT)

- **Distribution ensures that no single entity can alter the ledger.**

CENTRALIZED LEDGER



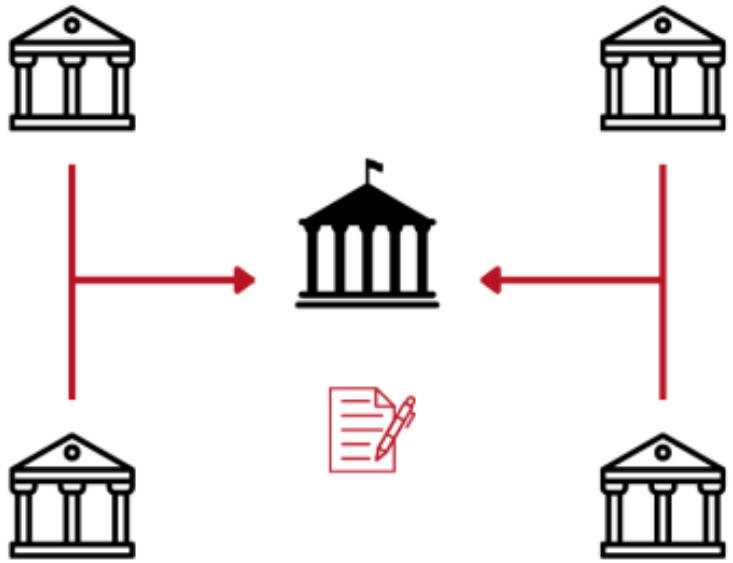
DISTRIBUTED LEDGER



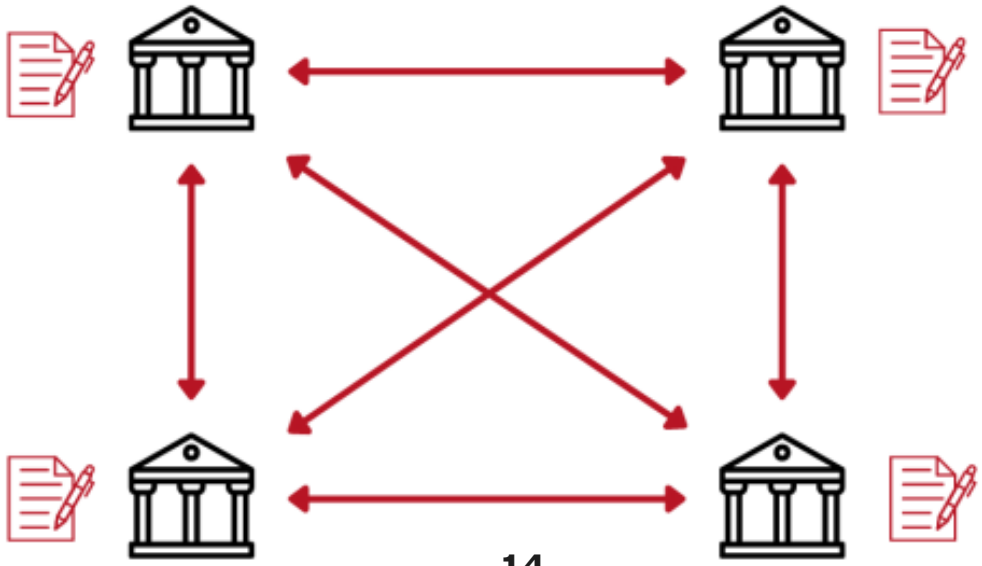
Distributed Ledger (DLT)

- Distribution ensures that no single entity can alter the ledger.
- Not censorship resistant because record keepers can collude.

CENTRALIZED LEDGER



DISTRIBUTED LEDGER



ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

Decentralized Consensus

- **Decentralized ledger: Anyone can become a record keeper.**

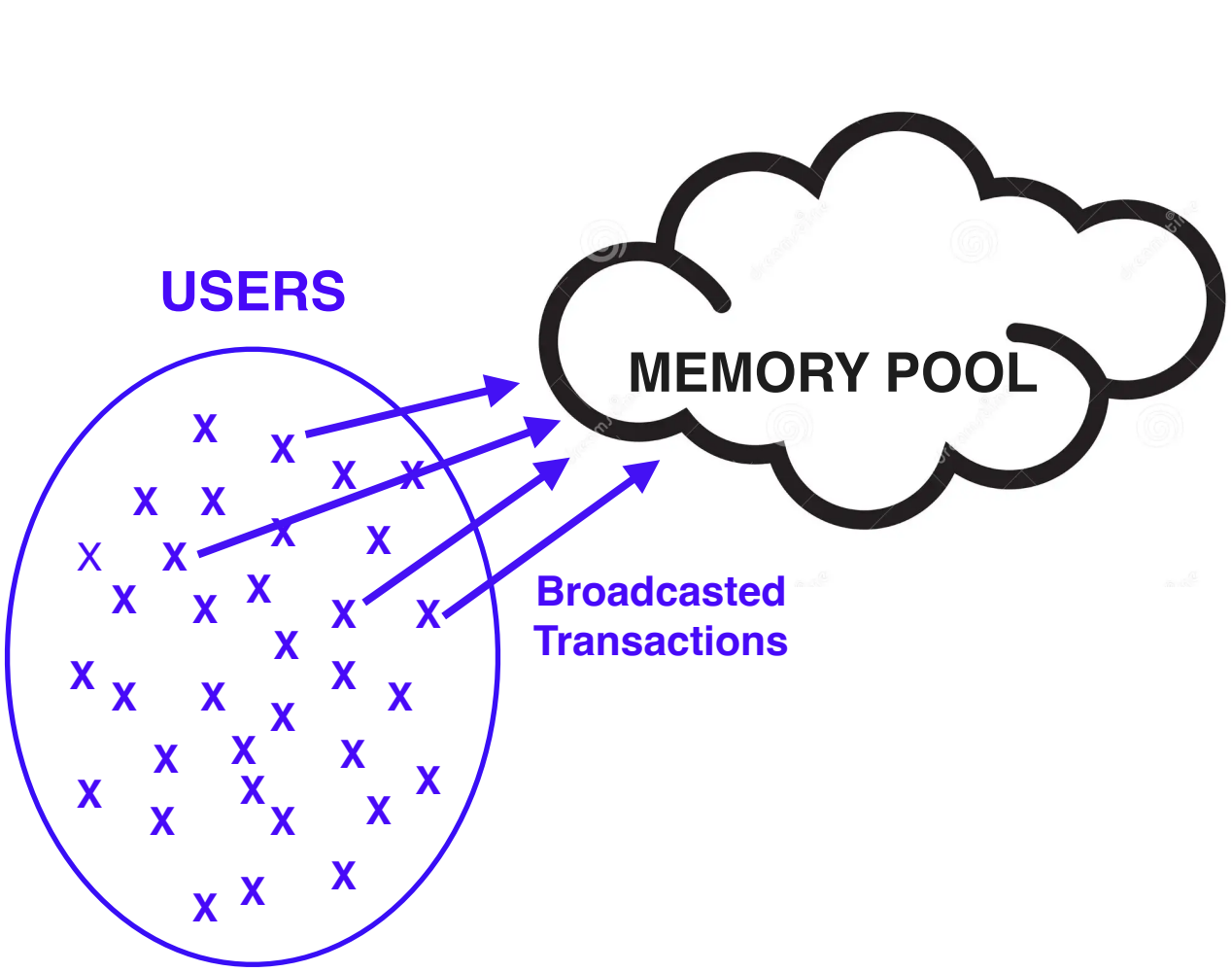
- **Different solutions:**

✓ **Proof-of-Work: Leader solves a cryptographic puzzle (e.g. Bitcoin).**

✓ **Proof-of-Stake: Probability of being selected proportional to the miner's stake in the protocol (e.g. Ethereum, Tezos).**

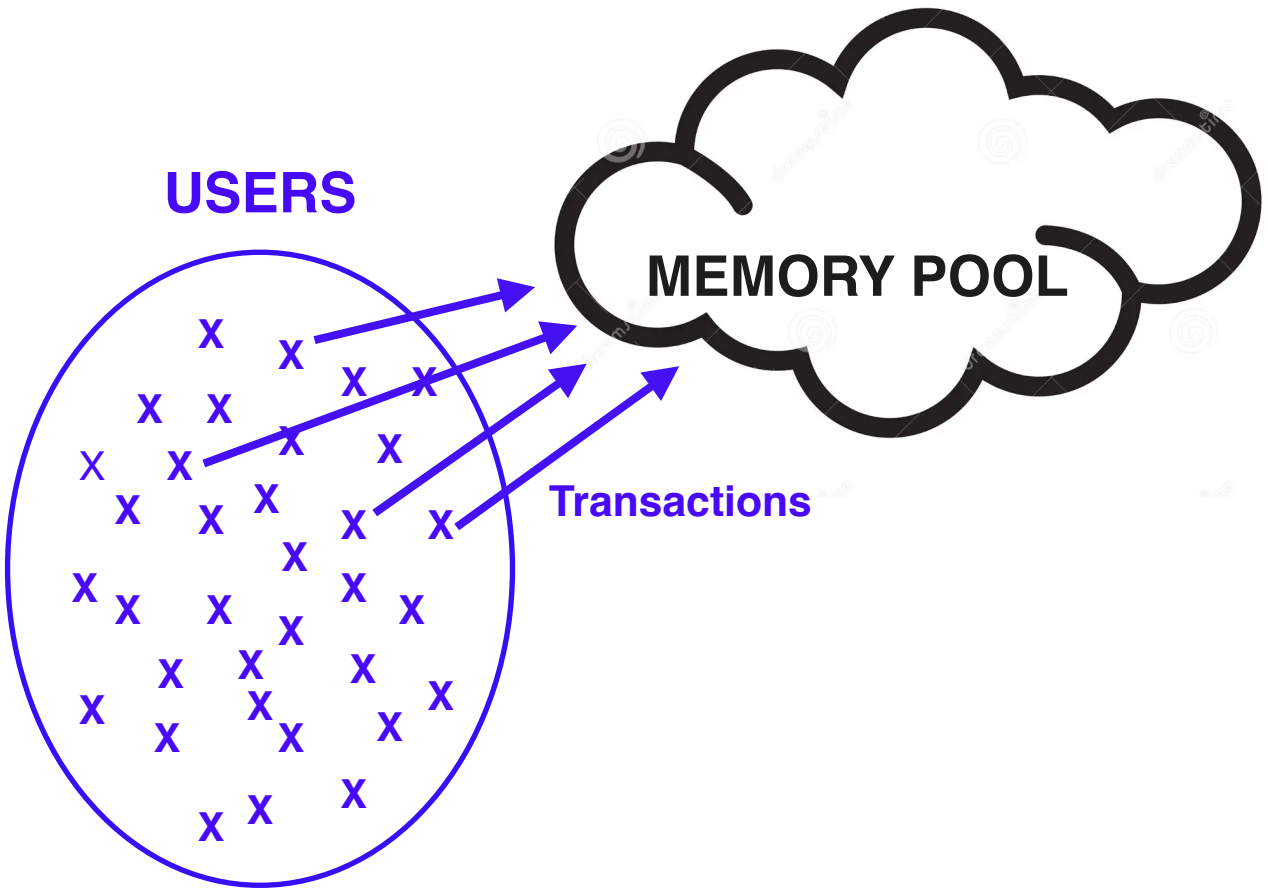
Decentralized Ledger

- **Anyone can become a record keeper!**



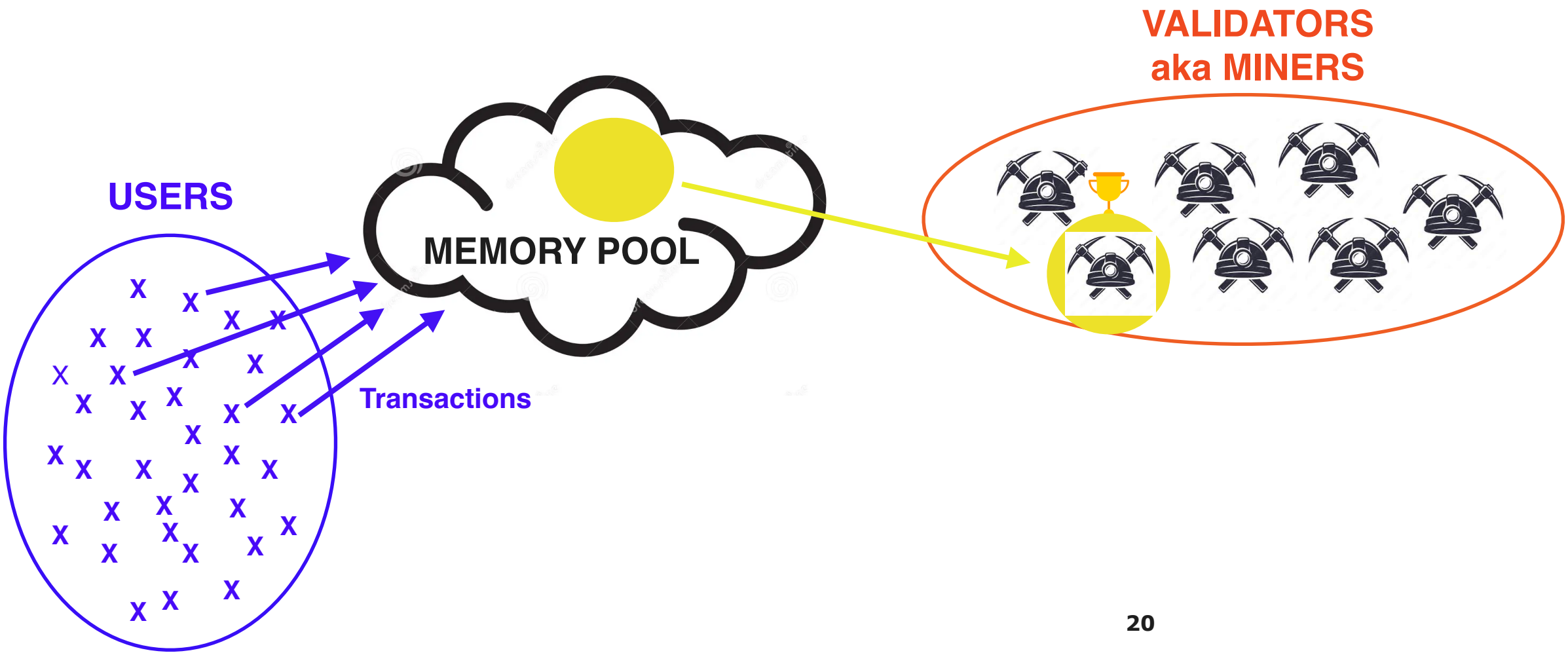
Decentralized Ledger

- Randomly select a record keeper.



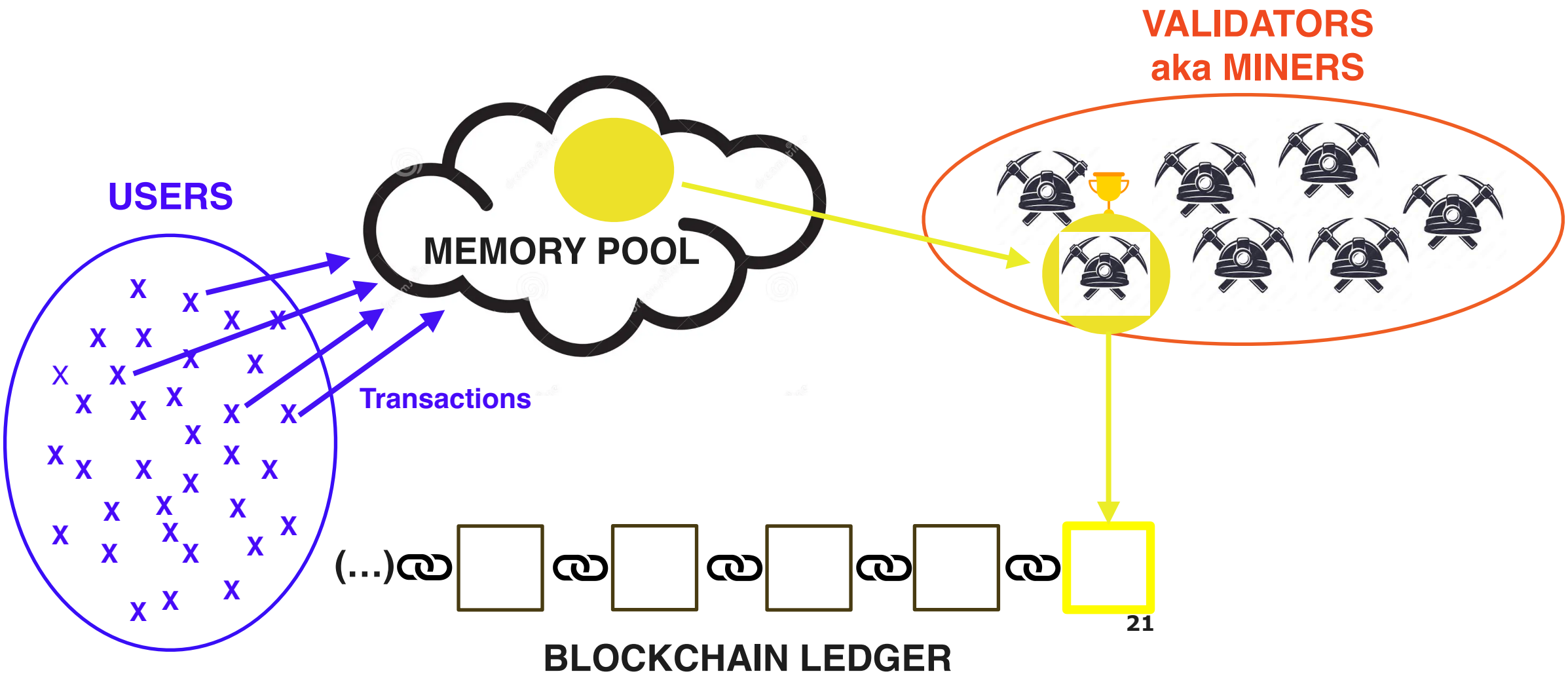
Decentralized Ledger

- **Winner picks a set of outstanding transactions.**



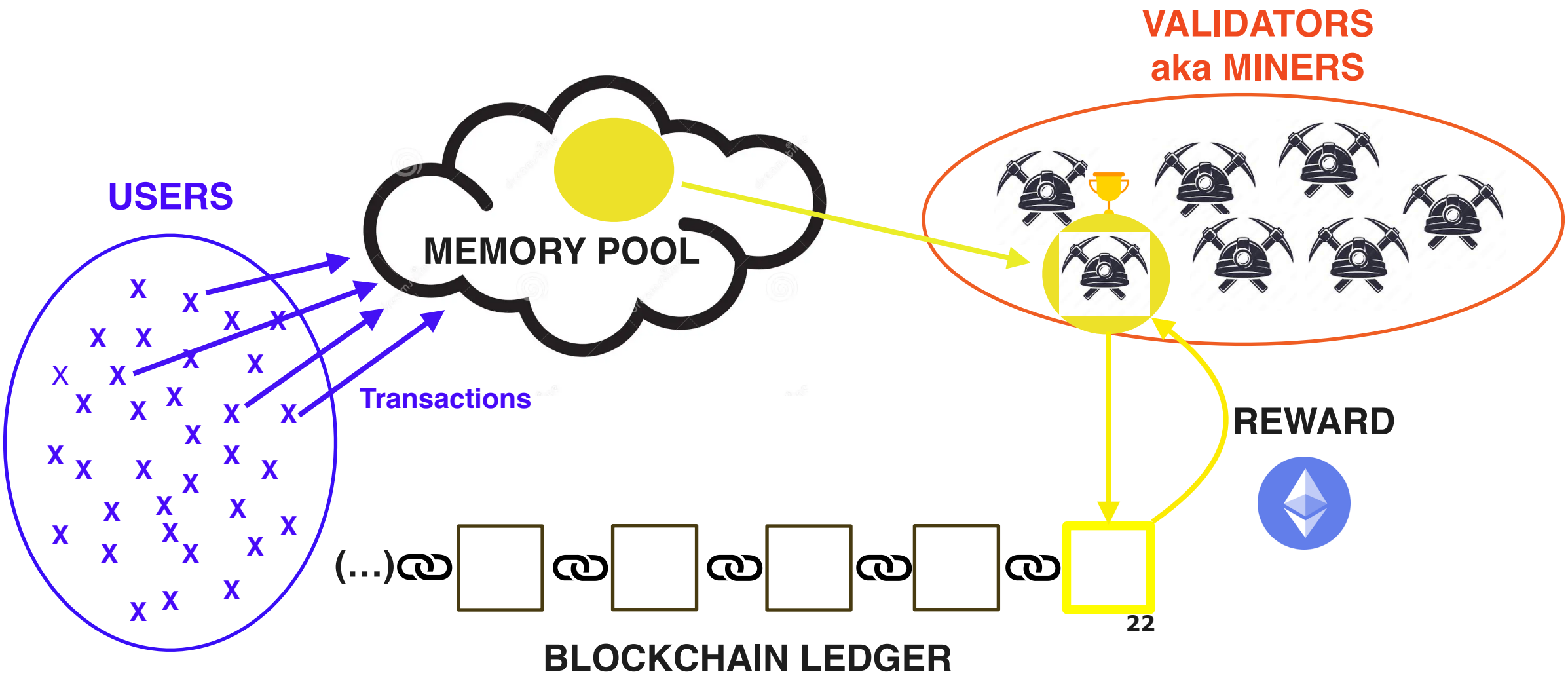
Decentralized Ledger

- Winner adds the last block of transactions to the ledger.



Decentralized Ledger

- **Validator rewarded with freshly minted coins.**



Computer in the sky

Blockchain is a digital ledger

- **Without a central authority**

- **Open**
  - Anyone can own an account
  - Anyone can write new entries

- **Resilient**
  - Cannot be censored
  - Cannot be altered

Computer in the sky

Blockchain is a digital ledger

- **Without a central authority**

- **Open**
  - Anyone can own an account
  - Anyone can write new entries

- **Resilient**
  - Cannot be censored
  - Cannot be altered

Blockchain is a general-purpose computer

- **Without an owner or operator**
  - Runs “in the sky”, public good

- **Open**
  - Anyone can use existing programs
  - Anyone can deploy new programs

- **Resilient**
  - Cannot be shut down
  - Cannot be tampered with

Source: Tim Roughgarden, 2024

Computer in the sky

NETWORK OF PHYSICAL COMPUTERS

Source: Tim Roughgarden, 2024

Computer in the sky

NETWORK OF PHYSICAL COMPUTERS
+
BLOCKCHAIN PROTOCOL

SIMULATED (VIRTUAL) COMPUTER

Source: Tim Roughgarden, 2024

Trust Machine

- **Algorithmic trust has two building blocks:**
    1. **Self-Custody;**
    2. **Decentralized Consensus.**

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

Trust Machine

- **Algorithmic trust has two building blocks:**
  1. **Self-Custody;**
  2. **Decentralized Consensus.**

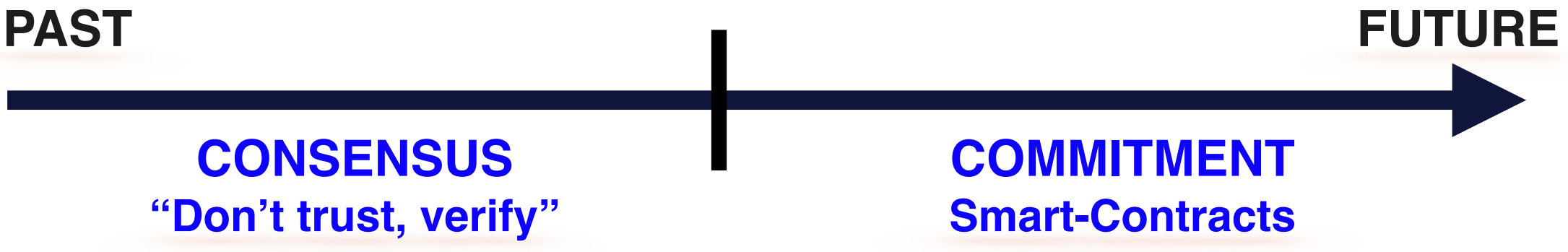
- **A Blockchain is a decentralized computer that is:**
  - ✓ **Immutable: Keeps record of all past transactions;**
  - ✓ **Open: Anyone can write and validate new transactions;**
  - ✓ **Unstoppable: Process incoming transactions.**

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

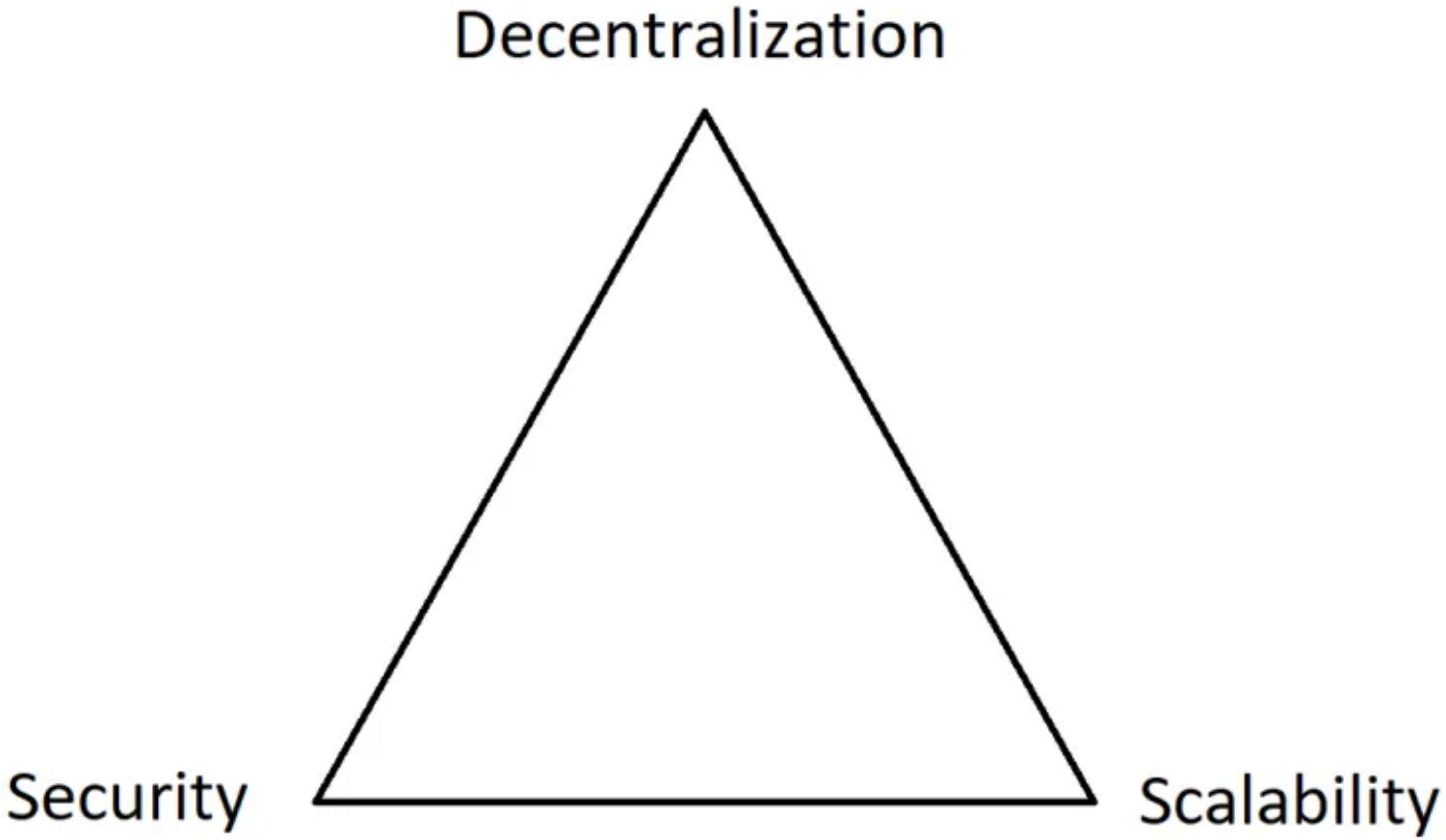
Trust Machine

- **Algorithmic trust has two building blocks:**
  1. **Self-Custody;**
  2. **Decentralized Consensus.**

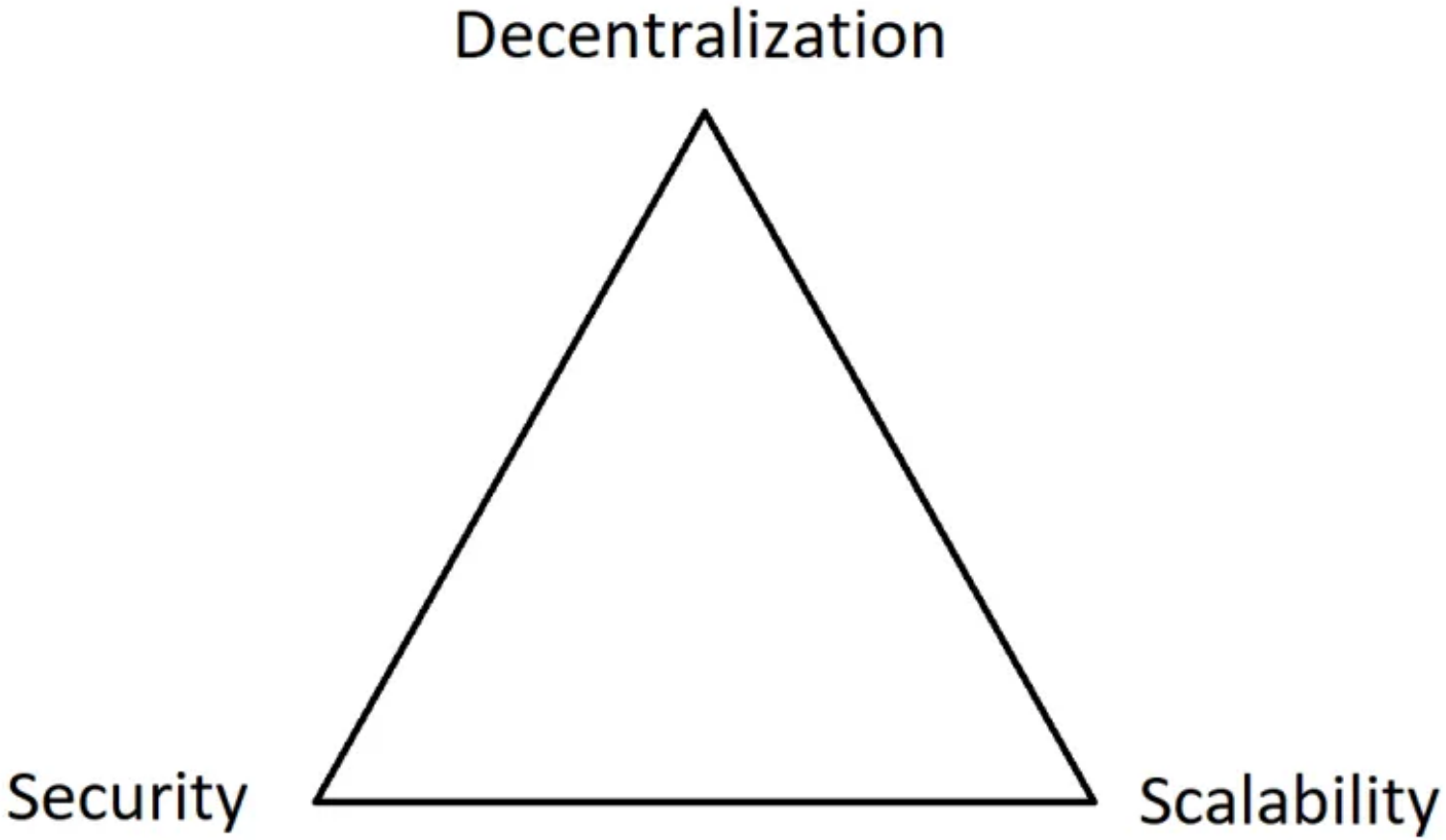
- **A Blockchain is a decentralized computer that is:**
  - ✓ **Immutable: Keeps record of all past transactions;**
  - ✓ **Open: Anyone can write and validate new transactions;**
  - ✓ **Unstoppable: Process incoming transactions.**



Blockchain Trilemma

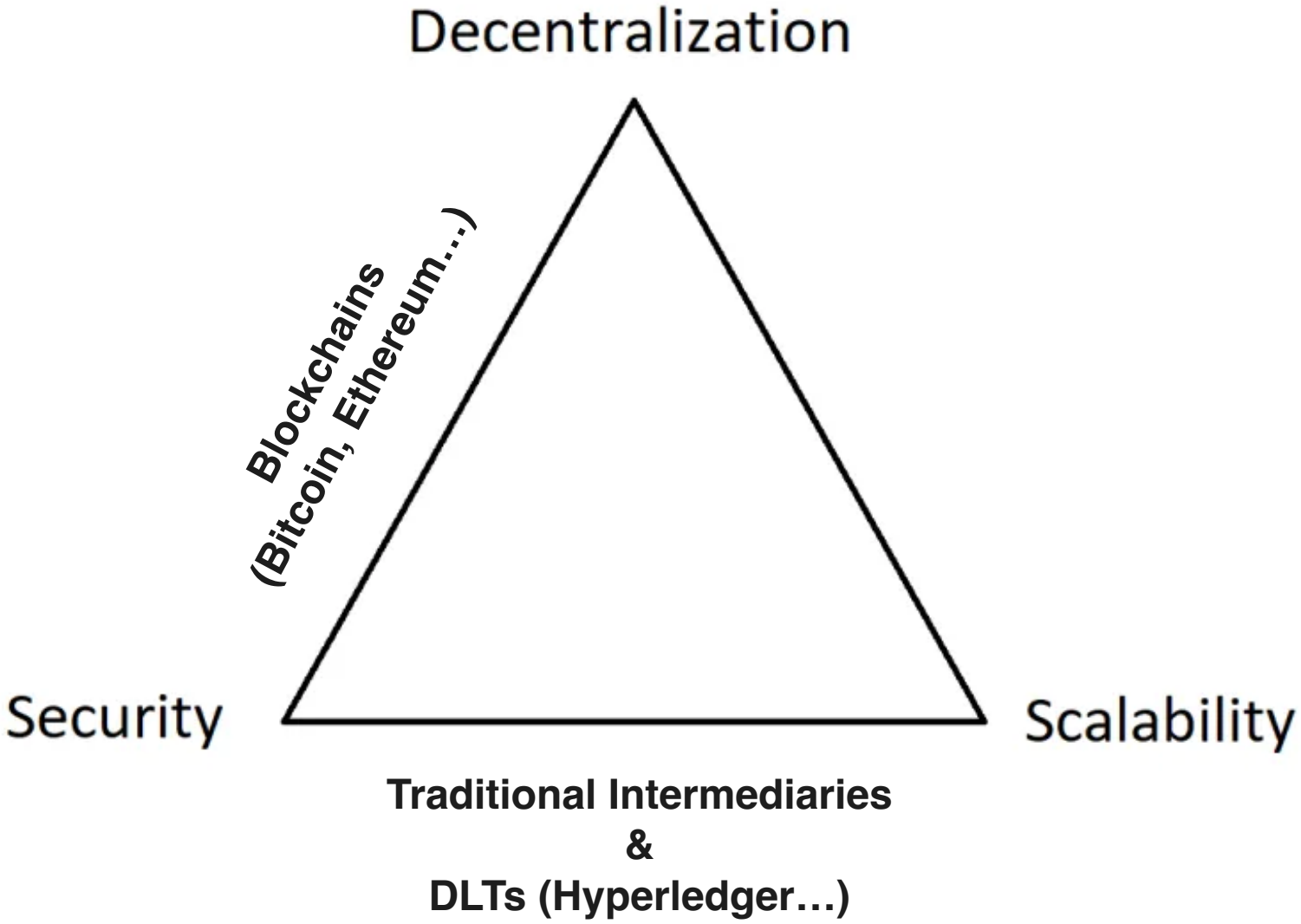


Blockchain Trilemma

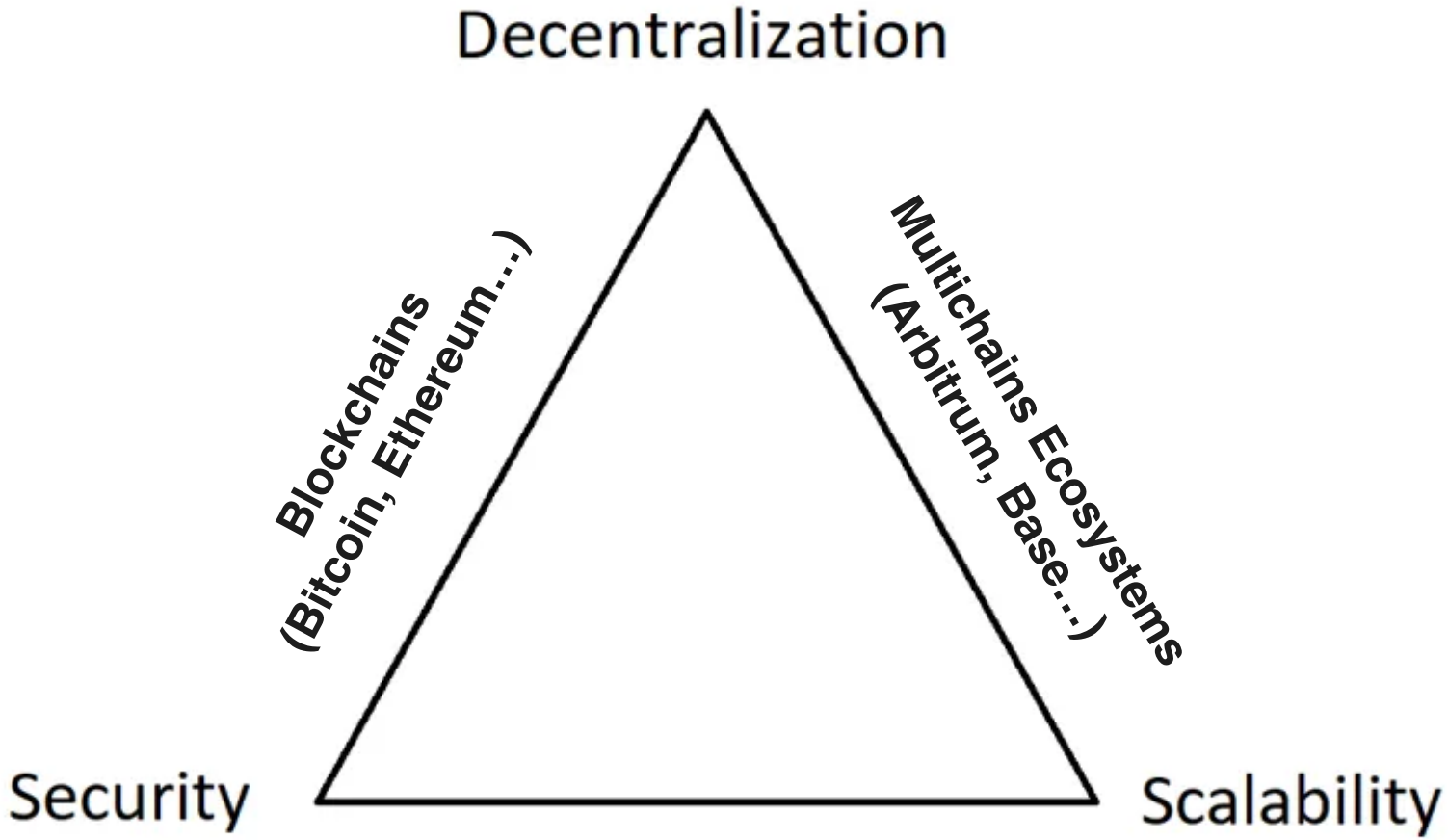


Traditional Intermediaries
&
DLTs (Hyperledger…)

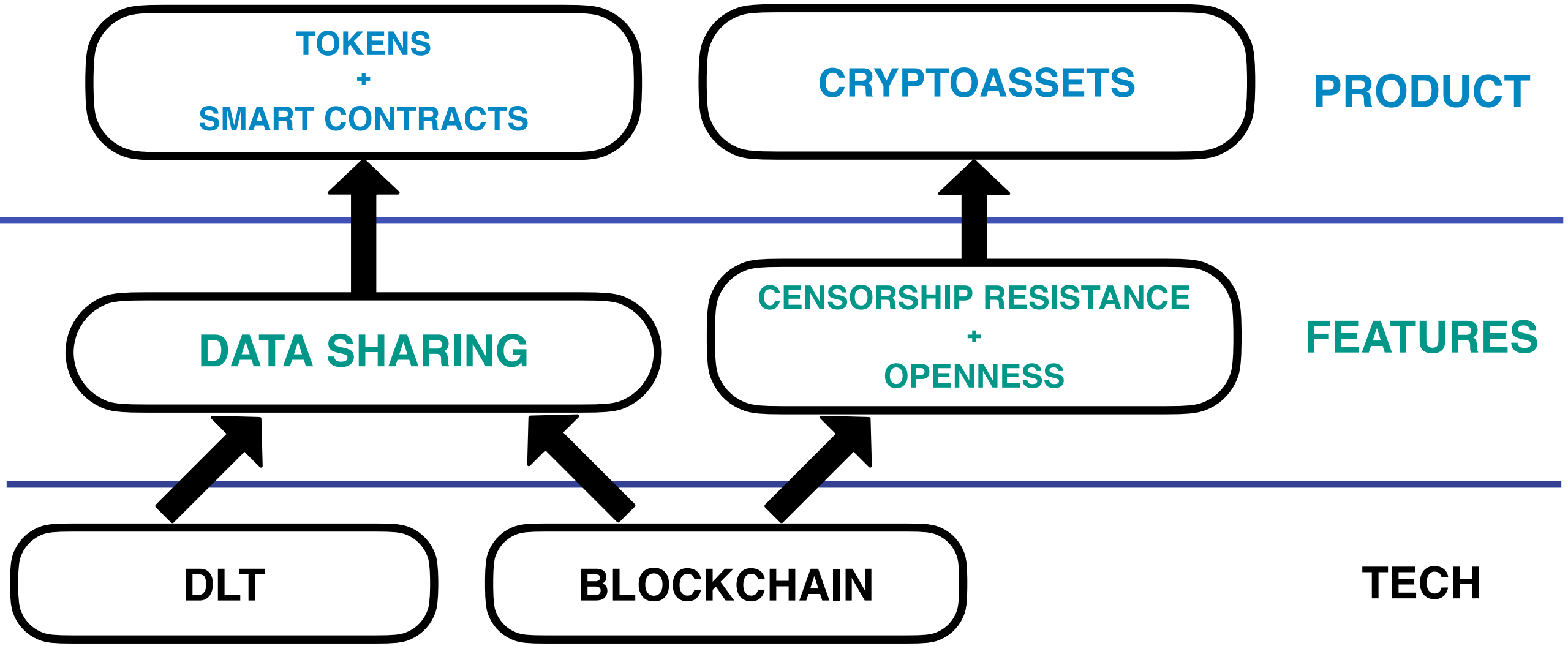
Blockchain Trilemma



Blockchain Trilemma



Decentralization vs. Programmability



Roads Ahead

DLT

✓ Pros:

- Control over infrastructure
- Regulation by design
- High throughput

✓ Cons:

- High-level of coordination
- Infrastructure building
- Risk of rent extraction

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION

Roads Ahead

DLT

✓ **Pros:**

- Control over infrastructure
- Regulation by design
- High throughput

✓ **Cons:**

- High-level of coordination
- Infrastructure building
- Risk of **rent extraction**

BLOCKCHAIN

✓ **Pros:**

- Neutral Infrastructure
- Innovative ecosystem
- World outreach

✓ **Cons:**

- Privacy & Scalability
- Regulation compliance
- Coexistence with malevolent actors

ÉCOLE POLYTECHNIQUE EXECUTIVE EDUCATION