Lecture 20: Summary

https://web3.princeton.edu/principles-of-blockchains/

Professor Pramod Viswanath
Princeton University

This lecture:
Design principles of blockchains
Introduction to COS/ECE 473: Elements of Tokenized Finance

Principles of Blockchains

- This course presented the **design space of blockchains**
  - **Principles** of good blockchain design choices
  - **Full-stack view**

- Pre-requisite: maturity with nearly all aspects of computer science

- Concretely: basic background in algorithms, probability, systems programming

Course begins with Bitcoin

- We started with an in-depth view of the Bitcoin design
  - The focus allows us to see the interacting components of the blockchain
  - Highlight the design constraints across the layers

- Bitcoin design is very simple and yet
  - remarkably secure, elegant in an engineering sense
  - performance guarantees backed by sophisticated mathematics
  - Outstanding case study for a deep understanding of blockchains

Module 1. Bitcoin Blockchain

- Next four lectures: Cryptographic data structures, Consensus, Peer to Peer Networking, Transaction structure, Ledger state management

- Two lectures: mathematical security guarantees of Bitcoin

- Implementation-intensive: students implement a full-stack Bitcoin client

Module 2. Scaling Blockchain

- Adapting the Bitcoin design to scale its performance

- Scaling:
  - Throughput
  - Latency
  - Computation, Storage
  - Energy
  - Layer 2 scaling

The resulting blockchain designs are at the heart of many popular cryptocurrency platforms: Avalanche, Cardano, Solana, Polygon

Module 3. Beyond Bitcoin

- Incorporating features absent in the Bitcoin design

1. Finality
2. Privacy
3. Connecting blockchains: Bridges
4. Importing data into blockchains: Oracles

The resulting blockchain designs are at the heart of many popular cryptocurrency platforms: Zcash, ChainLink

From Lecture 1: A Decentralized Platform?

- A decentralized Dropbox, eBay, Instagram?
- Incentives aligned with consumers and resource providers?
- No need for a trusted middle party?

Such is the siren song of blockchains.

The Siren Song of Blockchains

- Web2 performance
  - Storage (dropbox-style), Compute (AWS or Azure-style)
- Run 2023 applications
  - GPT4
- But decentralized trust and security
  - Natively coupled incentives for participants

Where we are

- Ethereum is a 1990 computer
  - The upgrade from PoW to PoS only got from 1987 computer to 1990
- But decentralized trust and security
  - Natively coupled incentives for participants
- Starting a new L1 involves building community
  - Hard work, not incentive-compatible with existing blockchain platforms
  - Unclear if that is

The Best Design Today

- Ethereum is a 1990 computer
  - But energetic, active community

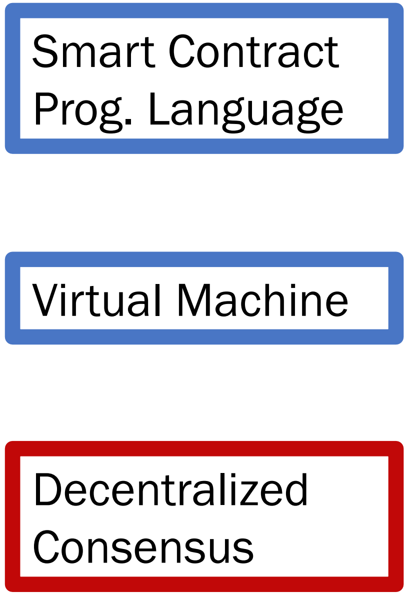
- Outsource storage
  - Data availability oracles (Lecture 14)

- Outsource computation
  - Rollups (Lecture 17)

- Restake ETH to secure applications
  - Cryptoeconomic security, programmable, on-demand
  - Eigenlayer

Technical Components

- Decentralized Computer
  - Cryptographic data structures
  - Disk I/O and Database management
  - Memory management
  - Operating systems
  - Peer to peer networking
  - Consensus and distributed algorithms
- Virtual Machine
  - Reduced instruction set, incentives
  - General purpose programming language


Smart Contract Prog. Language

Virtual Machine

Decentralized Consensus

Nearly all aspects of Computer Science

Introduction to COS/ECE 473: Elements of DeFi

https://web3.princeton.edu/elements-of-defi/

Professor Pramod Viswanath

Princeton University

Lecture 1. What is DeFi?

DeFi is tokenized finance on decentralized platforms

Tokenization

- Converting a tangible/intangible asset into a digital format
- Can be fungible (“currency”) or not (“an image or a video clip”)
- Awfully similar to **securitization**
  - Key is the **missing trusted middle party**

Tokenized Finance

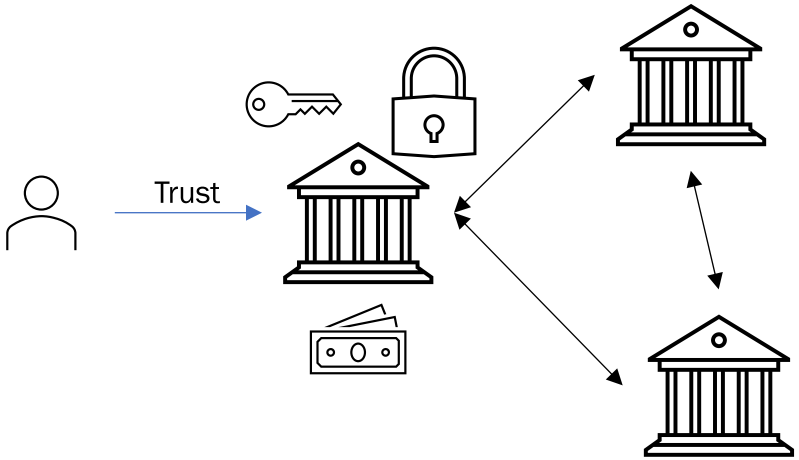
- Commerce – buying, selling
- Market places – exchanges
- Options, derivatives – financial instruments
- Borrowing, lending – banks

How is this any different from traditional finance?

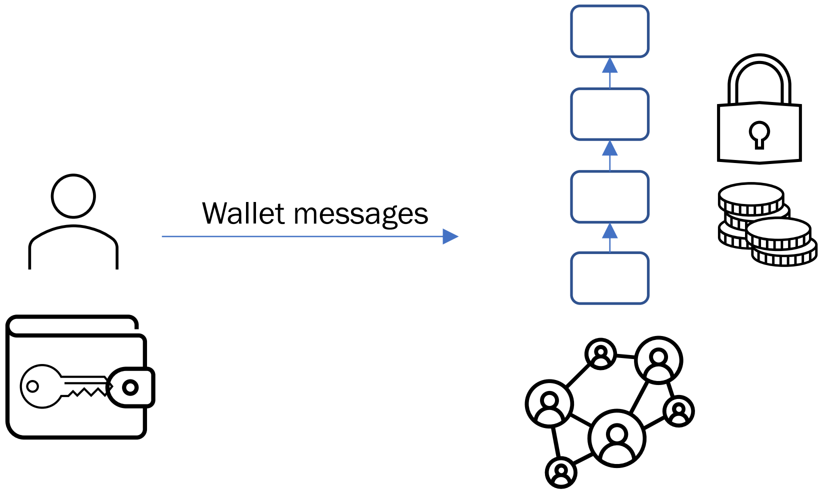
TradFi vs DeFi

DeFi is Non-custodial

- Users control ownership of their assets



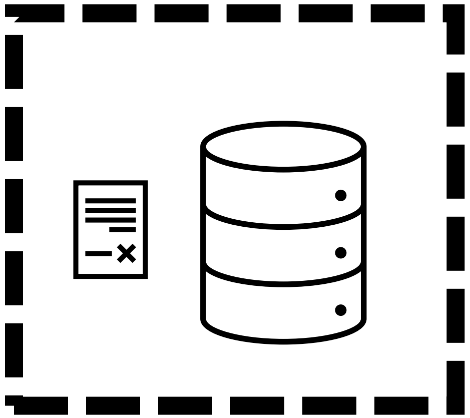
Flow of assets in control of the institution



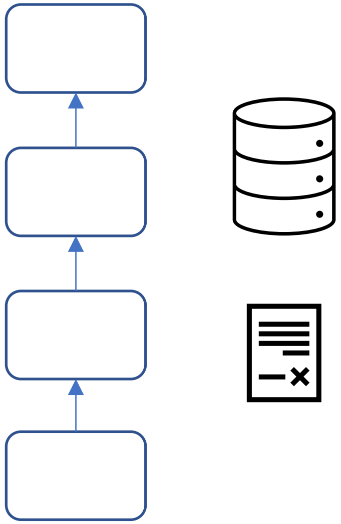
Flow of assets in control of the owner

DeFi is Openly-auditable

- Transparent execution logic of financial instruments and marketplaces



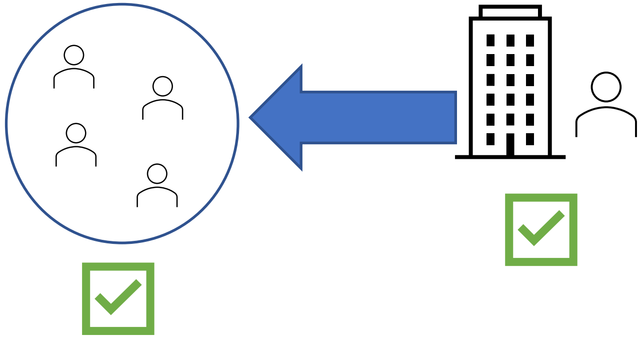
Database and its execution in a closed database, secured by regulation and audits



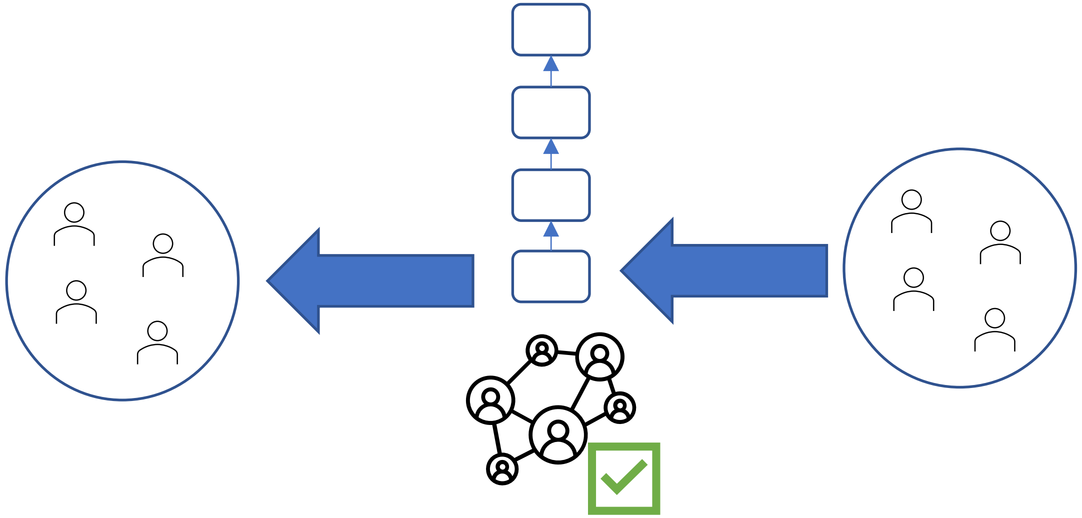
Anyone can check if the contract is programmed as expected and behaves as promised

DeFi is Permissionless

- Anyone can participate and interact with contracts
  - Wallets hold tokens and allow interaction with the blockchain
- Smart contract “regulates” that assets are managed as promised



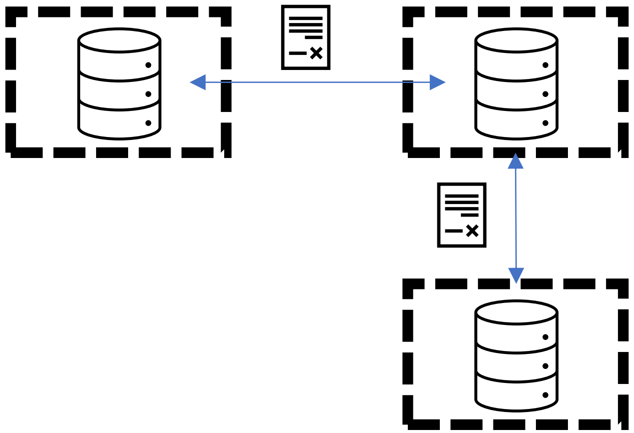
Only trusted entities can participate



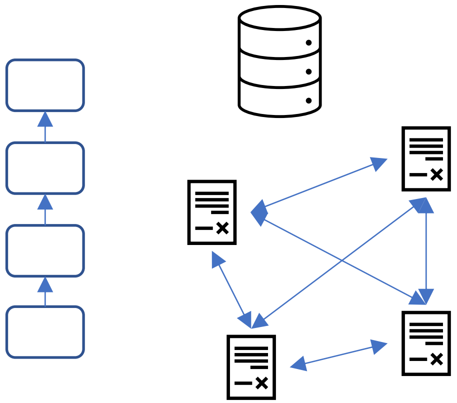
Anyone can participate, smart contracts provide trust

DeFi is Composable

- Interoperability across financial instruments



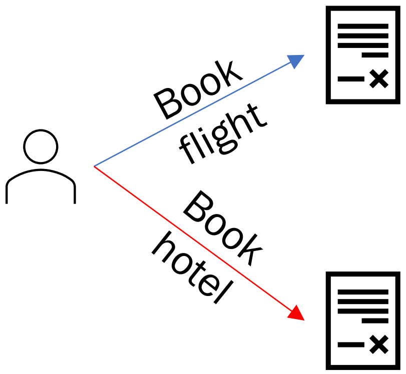
Siloed databases restricts interoperability



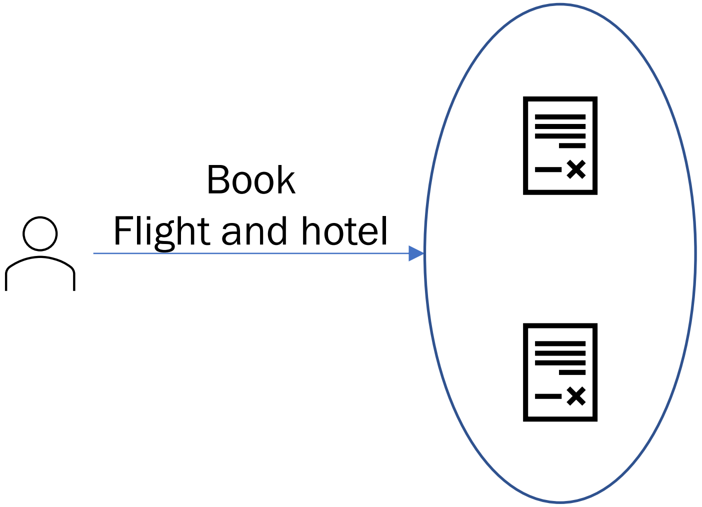
Contracts share state and can call each other while executing a transaction

DeFi is Atomic

- Option to add - **all or none** logic of execution for transactions interacting with multiple instruments



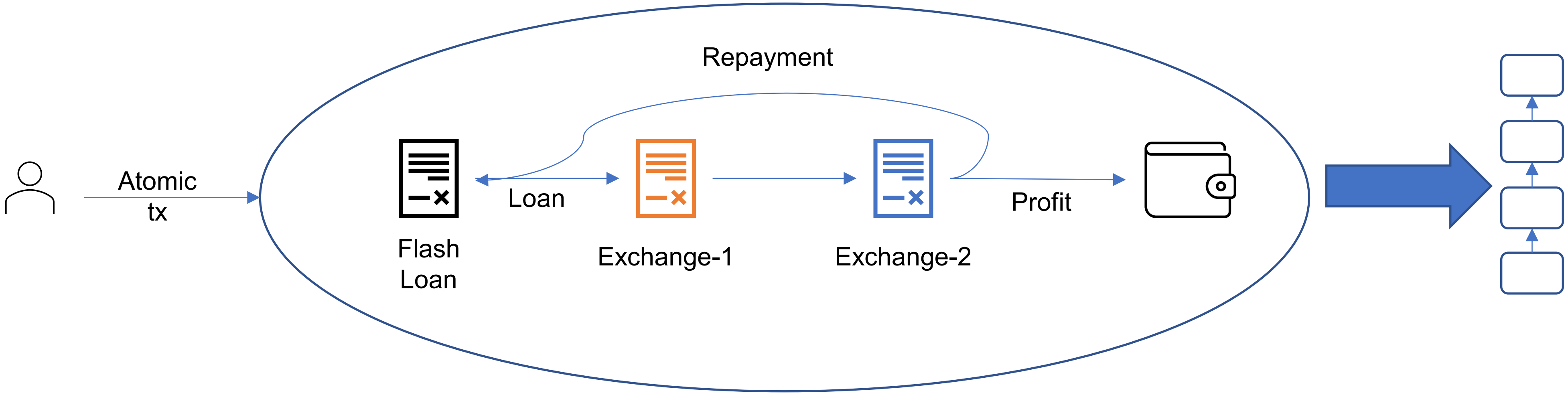
One operation might suceed and the other might fail



Perform action only if both operations succeed; else revert

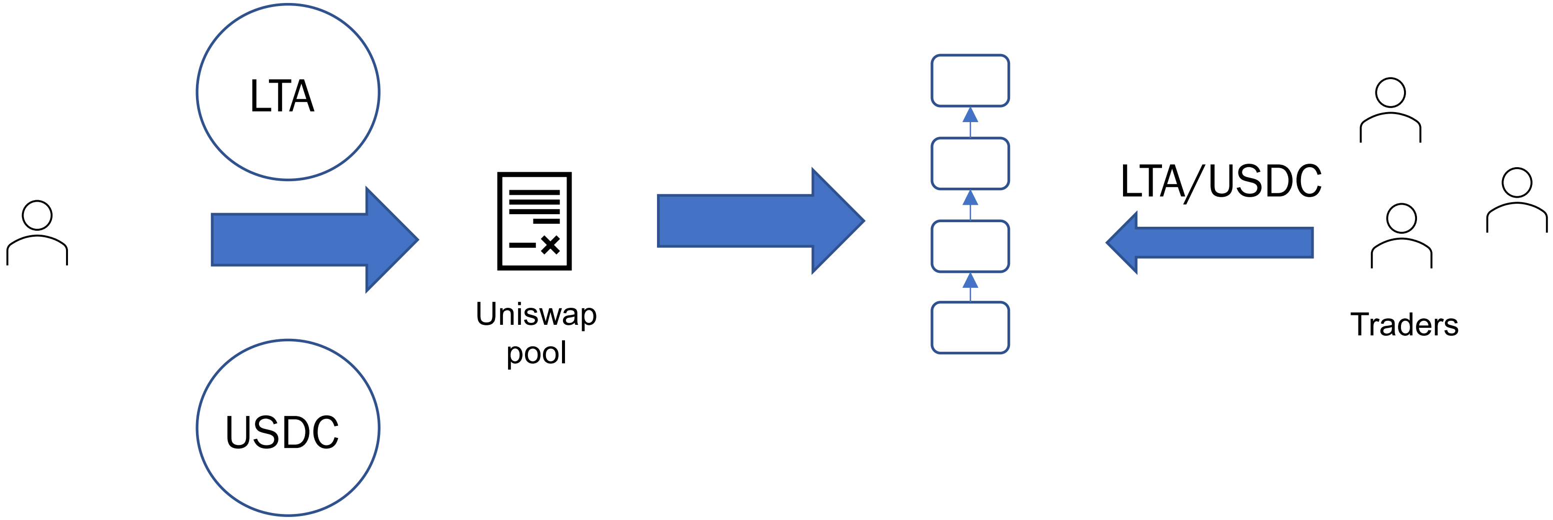
Use case: Flash loan arbitrage

- Two exchanges have a difference in price:
  - TradFi: Need to be a capital rich institution to extract arbitrage value
  - DeFi: Anyone can take a very large capital loan (with no collateral), perform arbitrage, earn money and return capital, in a **single transaction**



Use case: Market for low volume assets

- Need to set up a market for a low volume fungible asset:
  - TradFi: Centralized order-book exchanges don’t work due to lack of market making
  - DeFi: Anyone can create liquidity pool for the low volume asset and ensure availability of market



Nine elements of DeFi

1. Token transfers: native blockchain transactions
2. Market making via smart contracts
3. Oracles: importing external data
4. Borrow/Lending: banking functionality
5. Cross border finance: bridges, wrapped tokens
6. Stable coins: tying tokens to fiat
7. Synthetics and Perpetuals: self-adapting financial instruments
8. NFT: digital collectibles
9. DAO: tokenized governance

DeFi elements are smart contracts

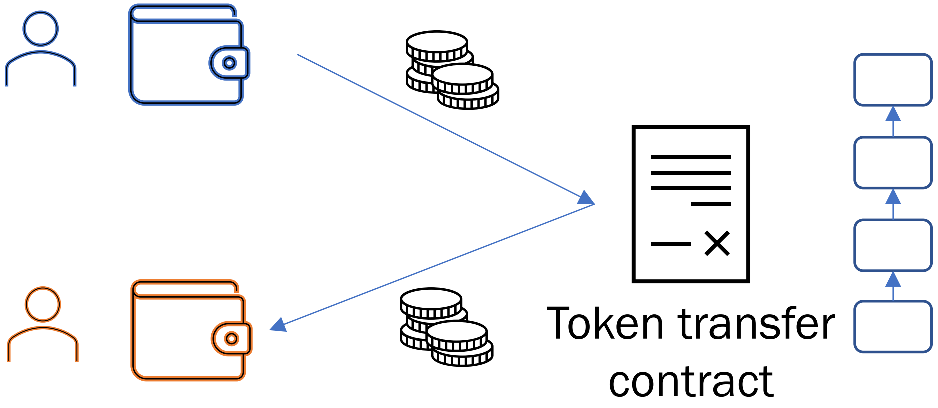
- Each element implemented via smart contracts
- Smart contracts “manage” the input/output of the tokens
- Smart contracts “regulate” the logic of the DeFi element

The underlying blockchain ledger maintains the time sequence ordered contract operations

Element 1: Native Blockchain Transactions

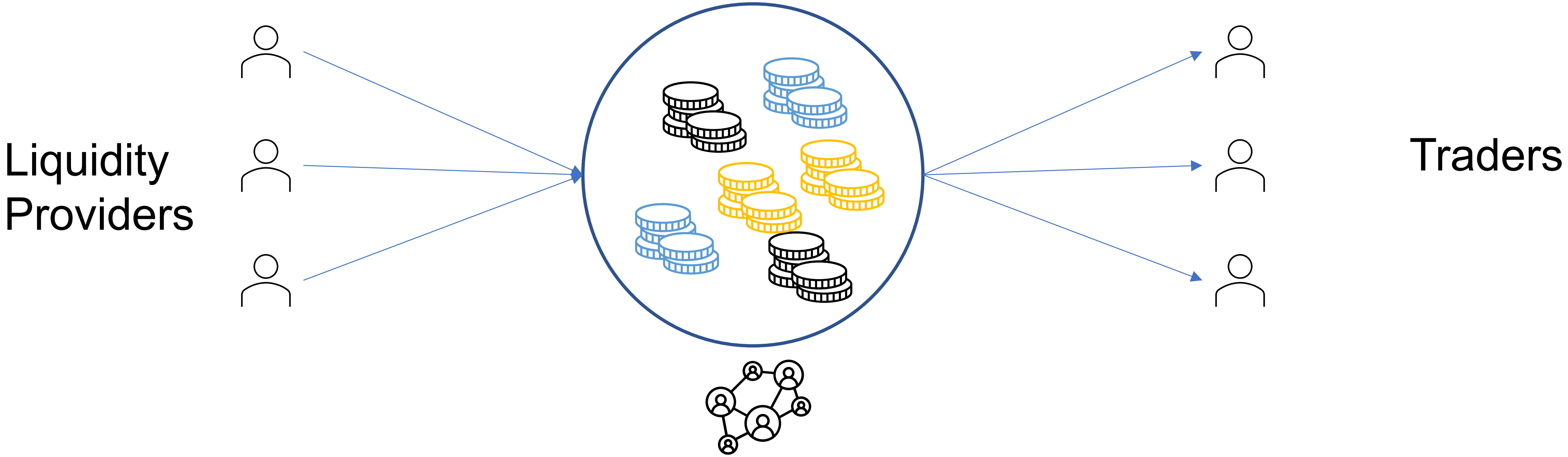
Token transfer

- No intermediaries, direct access via the blockchain
- Sending and receiving



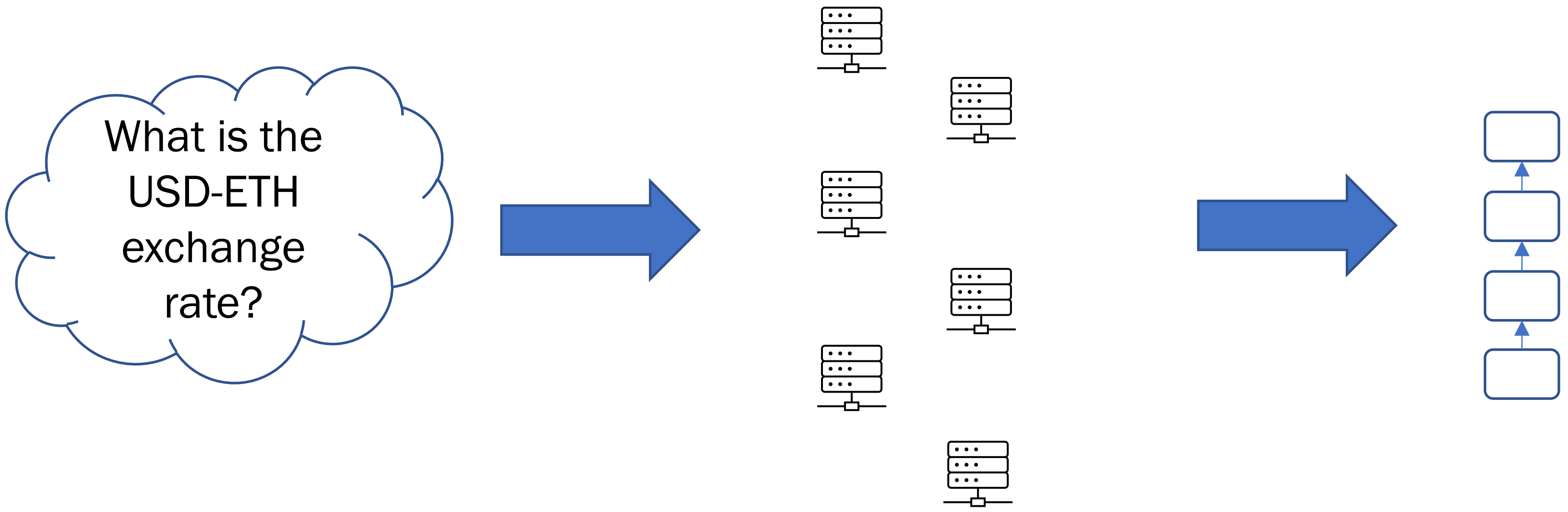
Element 2: Market Making

- Swapping Tokens
  - Market making via smart contracts
  - Liquidity providers and traders interact via the contract
- Peer-to-pool-to-peer Mechanism



Element 3: Oracles

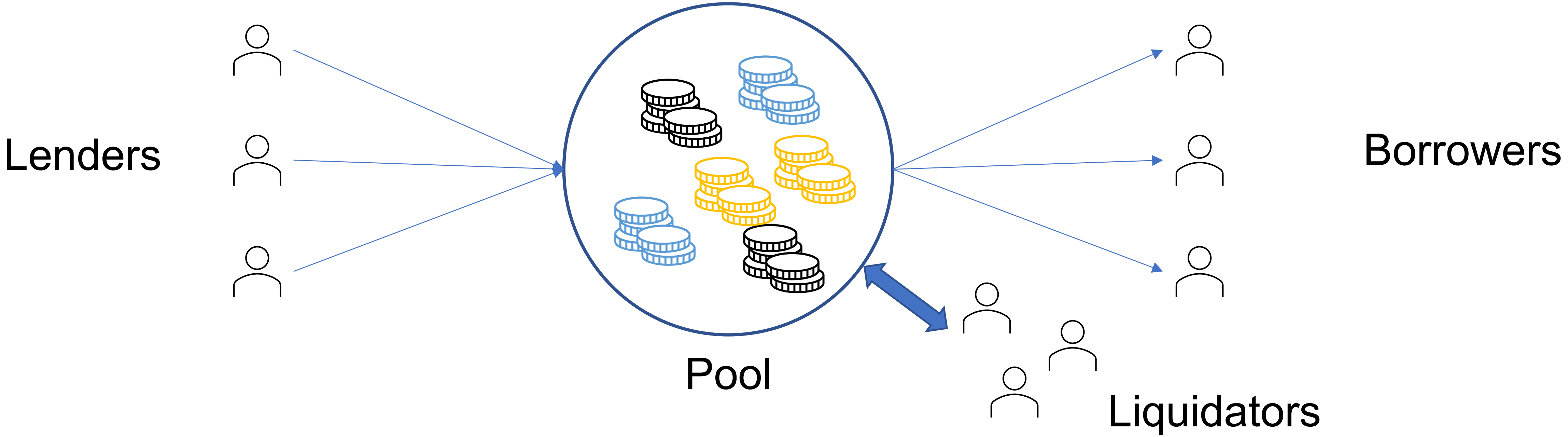
- A set of nodes import off-chain data into the blockchain
- Robust statistics ensure accuracy of data



Oracle node operators

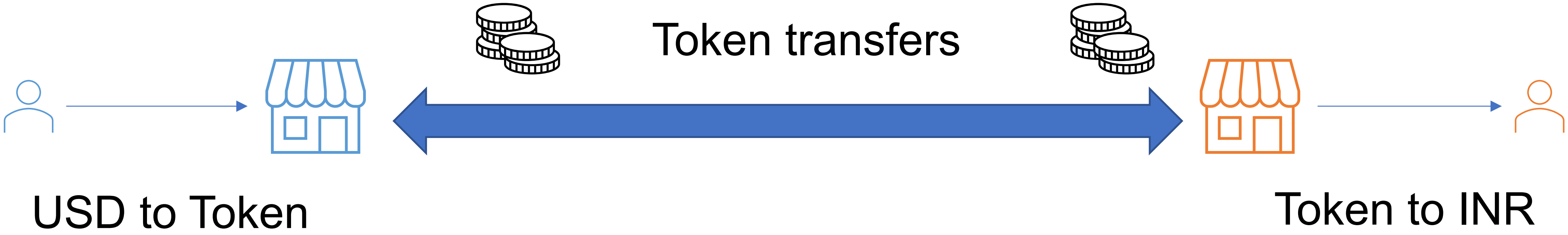
Element 4: Borrowing and Lending

- Deposit asset into the pool to earn interest
- Borrow assets collateralized by the deposited asset and pay interest



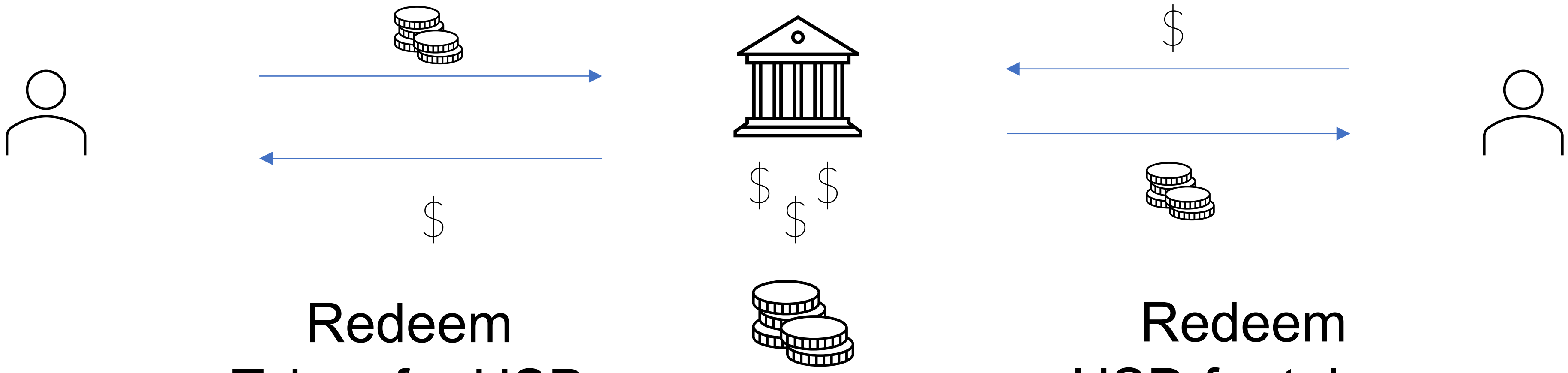
Element 5: Cross Border Transactions

- Token transfers on blockchains have the same security properties across different countries



Element 6: Stable Coins

- Token's value can be pegged to the value of a fiat currency through a variety of reserve mechanisms

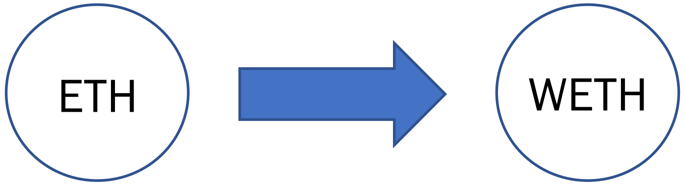


Redeem
Token for USD

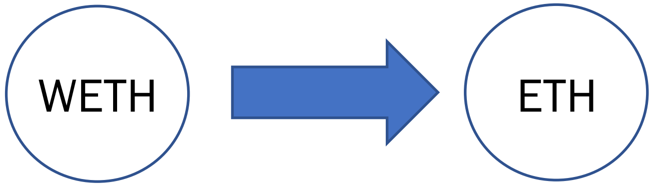
Redeem
USD for token

Element 7: Synthetics and Perpetuals

- Generate tokens whose value
  - Tracks value of another token
  - Tracks a value “derived” from another token



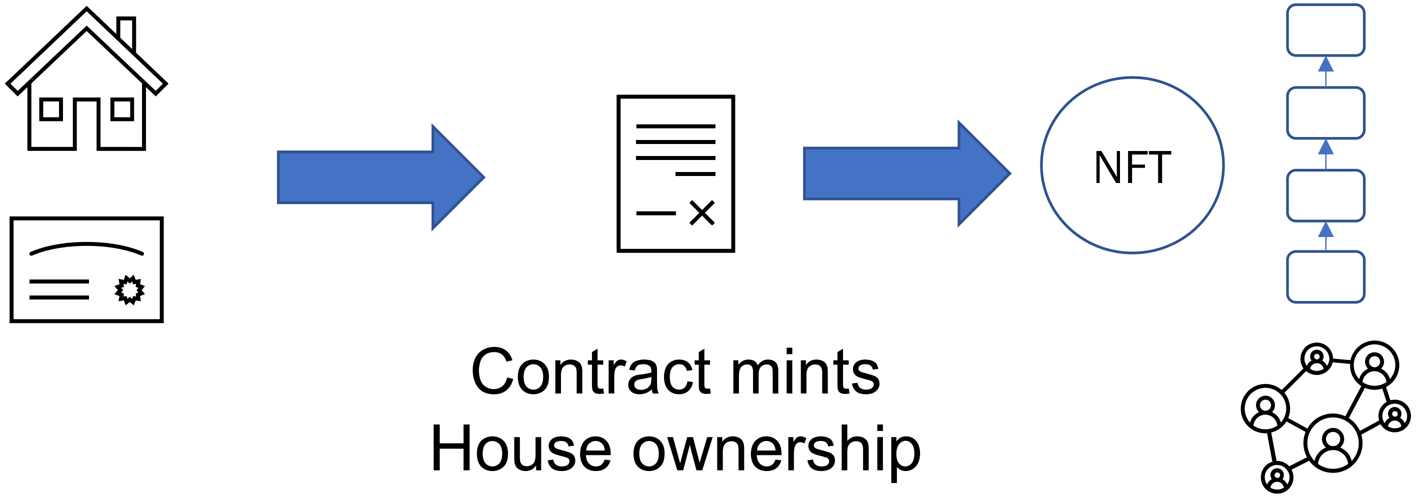
Deposit ETH mint
WETH



Burn WETH get
ETH

Element 8: Non-Fungible Tokens (NFT)

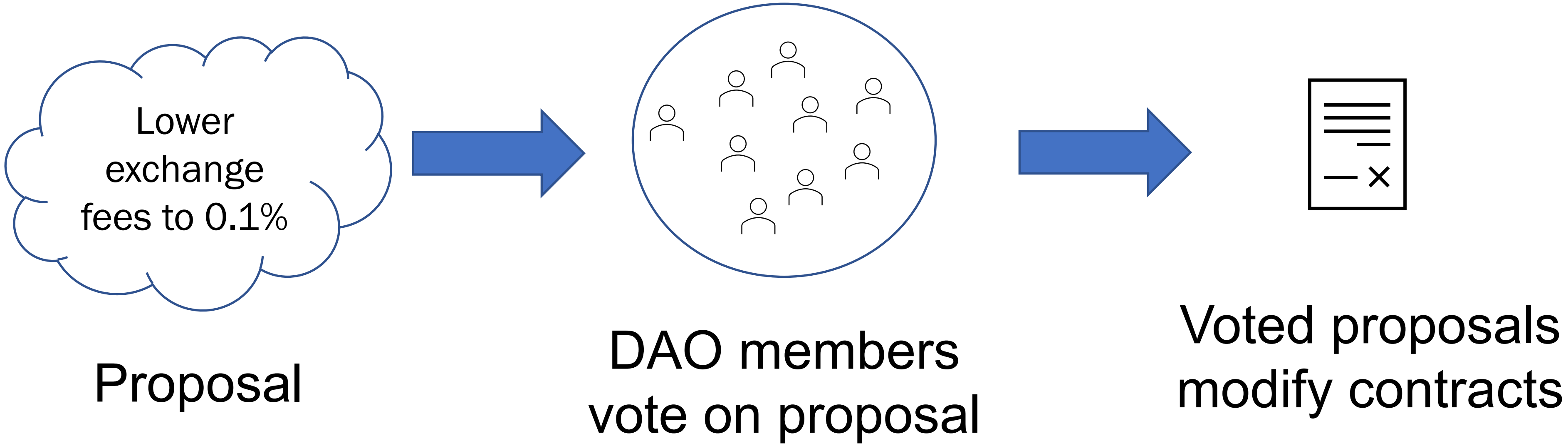
- Representation of unique asset on-chain
- Supports variety of functions on that asset
  - Asset transfers
  - Asset splits, sale commissions, sale tracking



Contract mints
House ownership
NFT

Element 9: Decentralized Governance (DAO)

- Contracts and protocols can be managed by a decentralized organization
- Protocol updates can be voted on by organization members
- Anyone can join the organization in a sybil resistant way



Lower exchange fees to 0.1%

Proposal

DAO members vote on proposal

Voted proposals modify contracts

Structure of the Course

Each class meeting is divided into two components:

- Lecture
  - Slides, oral presentation of the material
  - Outcome: a conceptual and theoretical understanding of the material

- Lab
  - In-class, hands-on activity
  - Largely on public blockchains
  - Outcome: hands-on, practical experience on major blockchain platforms

Attendance : NFT Drop

https://poap.website/be-resource-commercial

- Mint token to Metamask.
- Submit tx hash for attendance claim