The standards for assets and what they kick-started

Martinet Lee

/Outline

- ERC20, ERC721
- Fungible Asset Exchanges
  - ICO
  - Token Upgrade
  - DEX
- Asset Exchanges
- Oracles

/Fungible & Non-Fungible?

/Fungible asset

- Let's "code" / "create" such an asset

- Brainstorming time!
  What is essential for a fungible asset?

/Fungible Asset - ERC20

- https://eips.ethereum.org/EIPS/eip-20
- Why is ERC20 - being a standard - important?

```
function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)
```

```
function approve(address _spender, uint256 _value) public returns (bool success)
```

```
function transfer(address _to, uint256 _value) public returns (bool success)
```

/Non-Fungible asset

- Let's "code" / "create" such an asset
- Brainstorming time!
  What is essential for a non-fungible asset?
- https://eips.ethereum.org/EIPS/eip-721

/How to raise capital?

You need to create an asset (under the legal framework), distribute it to people under certain conditions, and gather their money.

E.g.

1. A legally binded signature saying that you'll provide the person some service some days later. (The legal paper itself can be seemed as a way to redeem the service)

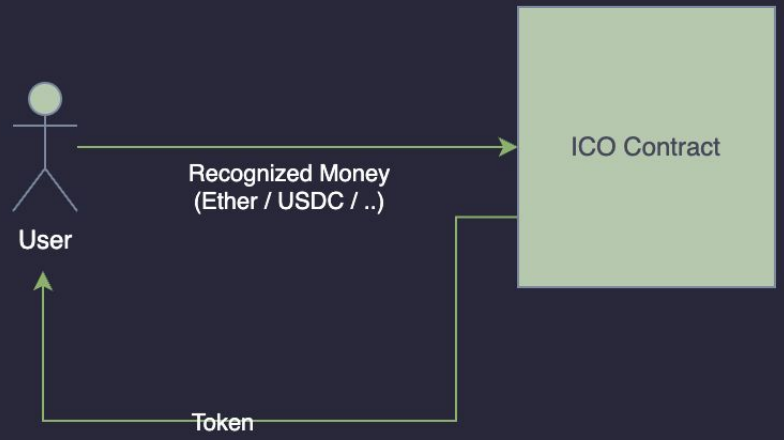
2. A legally binded signature saying that you'll provide the person an asset (company's stock, real estate, etc) later.

/ICO - Initial Coin Offering

Initial Coin Offering is a way that people raise capital.

Essentially saying:
“if you give me some real money, I’ll give you some tokens”

Typically it was Ether.



/ICO Mechanism

- Fixed price (example contract)
- Fixed price with different periods / different price
- Dutch Auction

/Dutch Auction

- Read: https://medium.com/coinmonks/dutch-auction-ipo-ico-e02d4441a286

/Dutch Auction

- Read: https://medium.com/coinmonks/dutch-auction-ipo-ico-e02d4441a286

- Example: Company XYZ wants to sell 500 shares
- Bid
  - Investor A bids for 200 shares at $7 / share
  - Investor B bids for 150 shares at $15 / share
  - Investor C bids for 250 shares at $5 / share
  - Investor D bids for 50 shares at $20 / share
  - Investor E bids for 50 shares at $25 / share
  - Investor F bids for 250 shares at $10 / share

/Dutch Auction

- Target is 500 shares
- Sort the Bids
  - Investor E bids for 50 shares at $25 / share (50)
  - Investor D bids for 50 shares at $20 / share (100)
  - Investor B bids for 150 shares at $15 / share (250)
  - Investor F bids for 250 shares at **$10** / share (500)
  - Investor A bids for 200 shares at $7 / share
  - Investor C bids for 250 shares at $5 / share

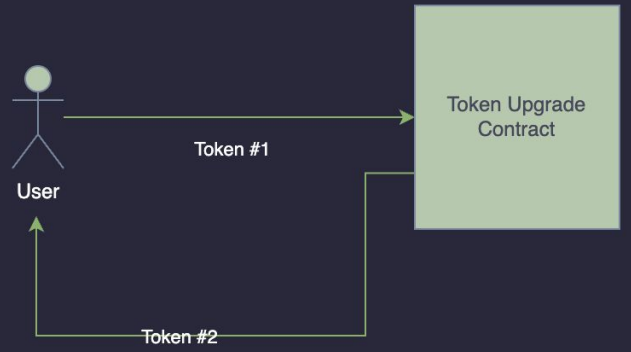
/Code Analysis of “Dutch Auction” contract

- Code Analysis: https://github.com/maurelian/dutch-auction/blob/master/contracts/DutchAuction.sol

  https://github.com/miladmostavi/gnosis-contracts/blob/master/contracts/solidity/DAO/DAODutchAuction.sol

/Token Upgrade

- Token Upgrade
- Fixed price, typically 1:1, ERC20 to ERC20



/Token Upgrade - sample contract

- Why would we need this?
  - Functionality upgrade
  - Hack recovery (official blog, contract)
- Coding up one now?

/DEX - Decentralized Exchange

- What makes a decentralized exchange “decentralized”?
- DEXes
  - EtherEx
  - EtherDelta
  - IDEX
  - 0x
  - Kyber
  - Uniswap (V2, V3)
  - Curve
  - Balancer

/What is an exchange?

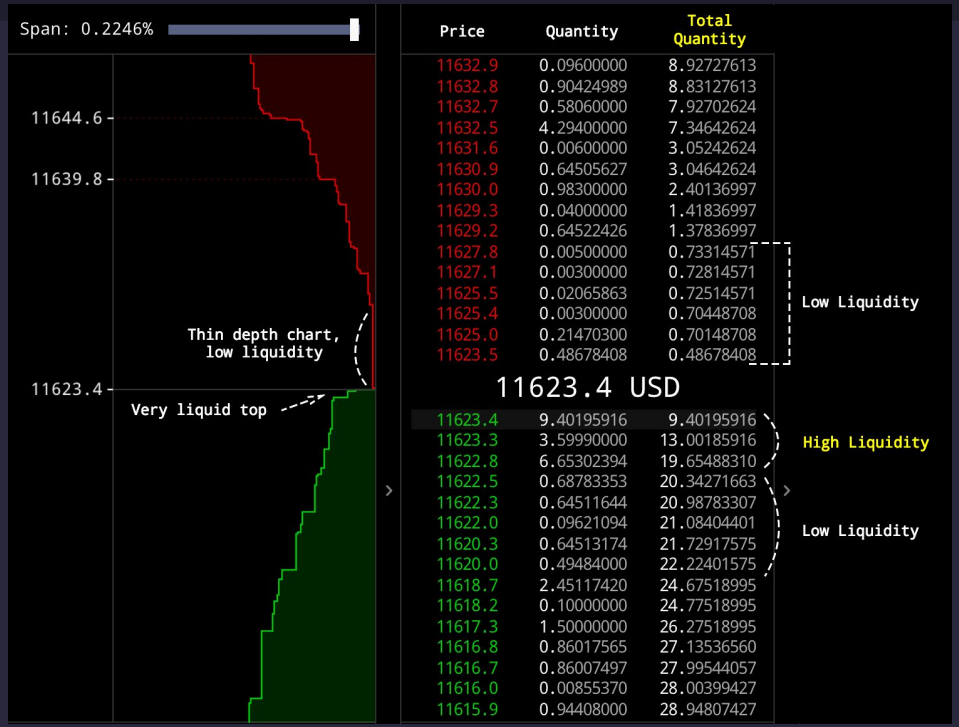
- A place to buy / sell assets.
- How to buy / sell? What are the experience in **Centralized Exchange**? (omit the part about “perpetual”)
  - Market buy / sell
  - Limit order

/What is an exchange?

1. Maker makes a trade
2. Taker finds good trade
3. Taker matches a trade, settles the fund

1. UserA makes a trade
2. UserB makes a trade
3. Matching engine matches UserA's and UserB's trades, settles the fund

/What is an exchange?



/DEX (1) OasisDex

- EtherEX / OasisDex: like a centralized exchange
  - Order book hosted on blockchain
  - Maker posts a limit order (tx)
  - Taker scans the order, identifies the preferable ones
  - Taker matches the limit order (tx)
- Problems?

/DEX (2) EtherDelta

- EtherDelta
  - Traders deposit assets into the smart contract.
  - Maker posts a limit order (signed), sends it to a centralized off-chain service
  - Taker scans the order from the off-chain service, identifies the preferable ones
  - Taker matches the limit order, sends it with the maker's signed data. (tx)
- Problems?

/DEX (3) EtherDelta

- EtherDelta UX issues
  - When takers try to match the same order
  - How to cancel order?
  - Users need to match orders themselves, no CEX matching UX.
  - Need to wait until the blockchain mines for trade execution.
- EtherDelta security incident (DNS attack)

/DEX (4) IDEX

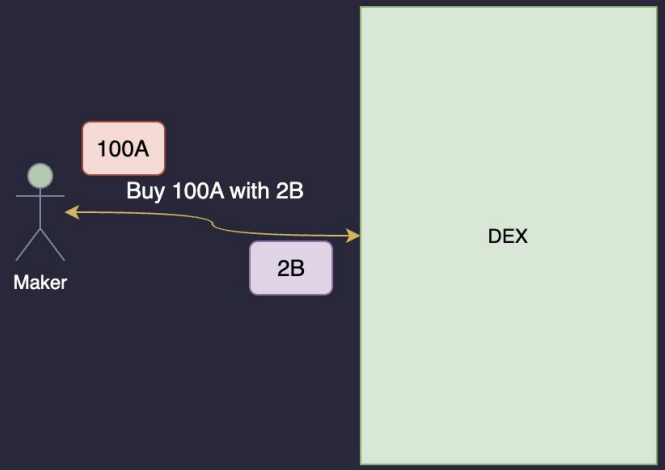
- IDEX (3B trade volume)
  - Trader deposits assets into smart contracts
  - Maker signs a limit order, sends it to centralized server (IDEX)
  - Taker scans and signs the trade on the centralized server (IDEX)
  - IDEX maintains the accounting internally (execution), and settles on-chain.

/Under the Orderbook model: CEX v.s. DEX

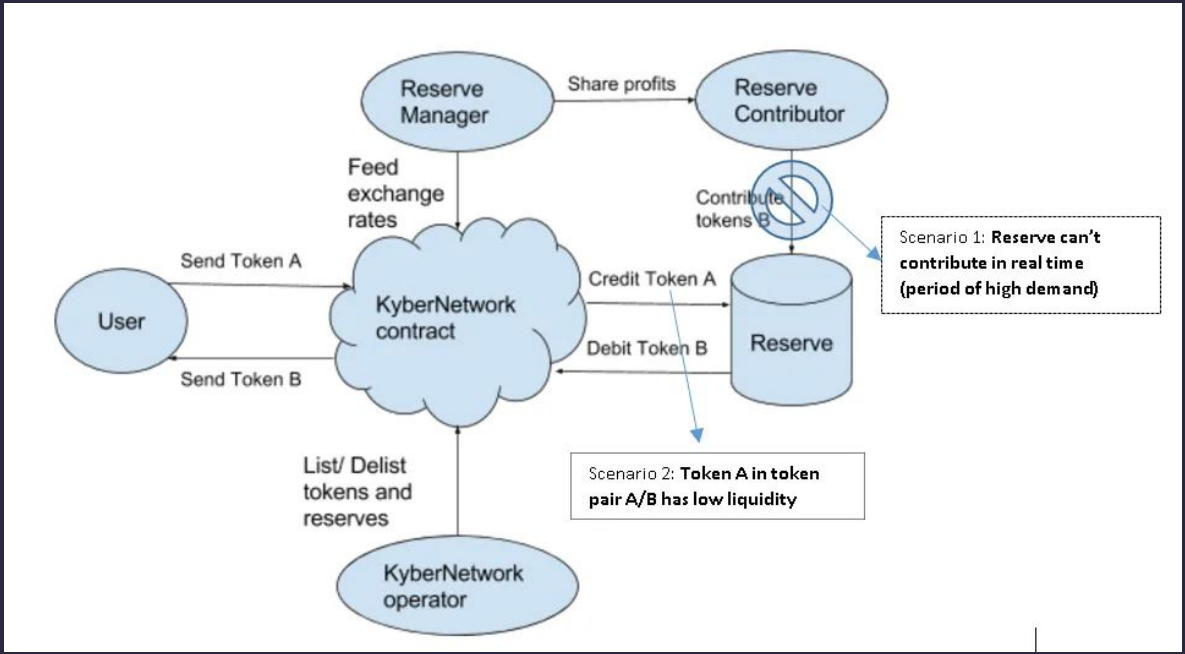
Dimensions for Comparison

- Censorship
- Availability
- Front-running
- Efficiency
- Fees

/DEX (5) Kyber



/DEX (5) Kyber


Reserve Manager
Share profits
Reserve Contributor
Feed exchange rates
Contribute tokens B
Scenario 1: Reserve can't contribute in real time (period of high demand)
Send Token A
User
KyberNetwork contract
Credit Token A
Debit Token B
Reserve
Send Token B
List/ Delist tokens and reserves
Scenario 2: Token A in token pair A/B has low liquidity
KyberNetwork operator

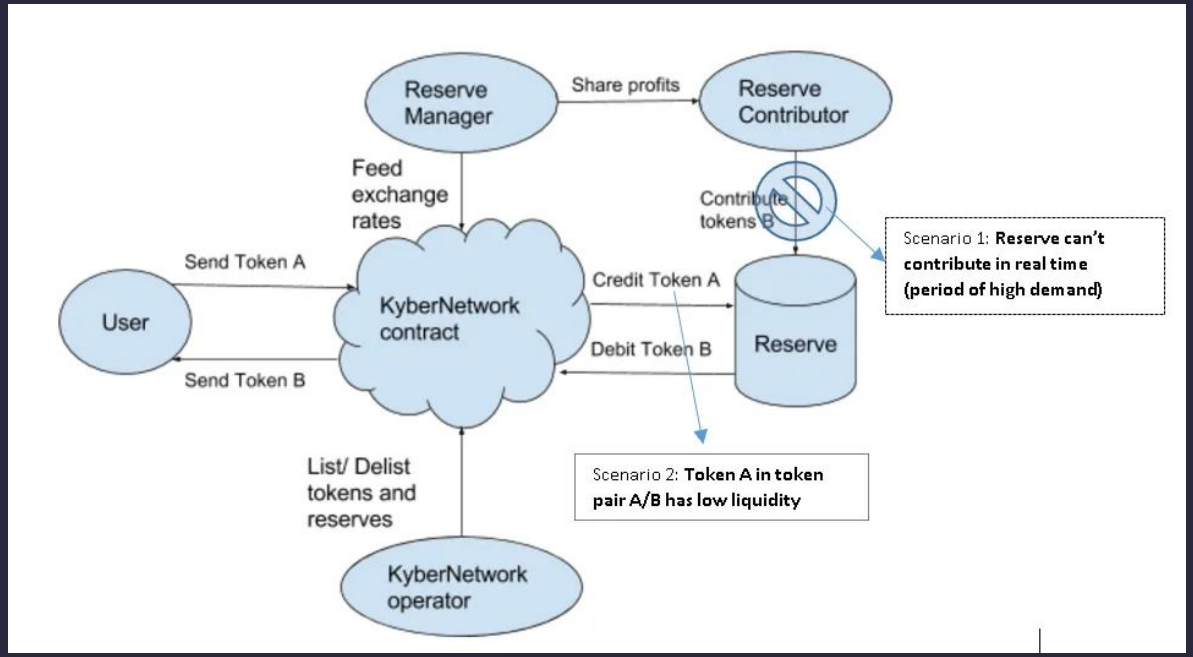
/DEX (6) Kyber

3.5. Comparison to existing systems

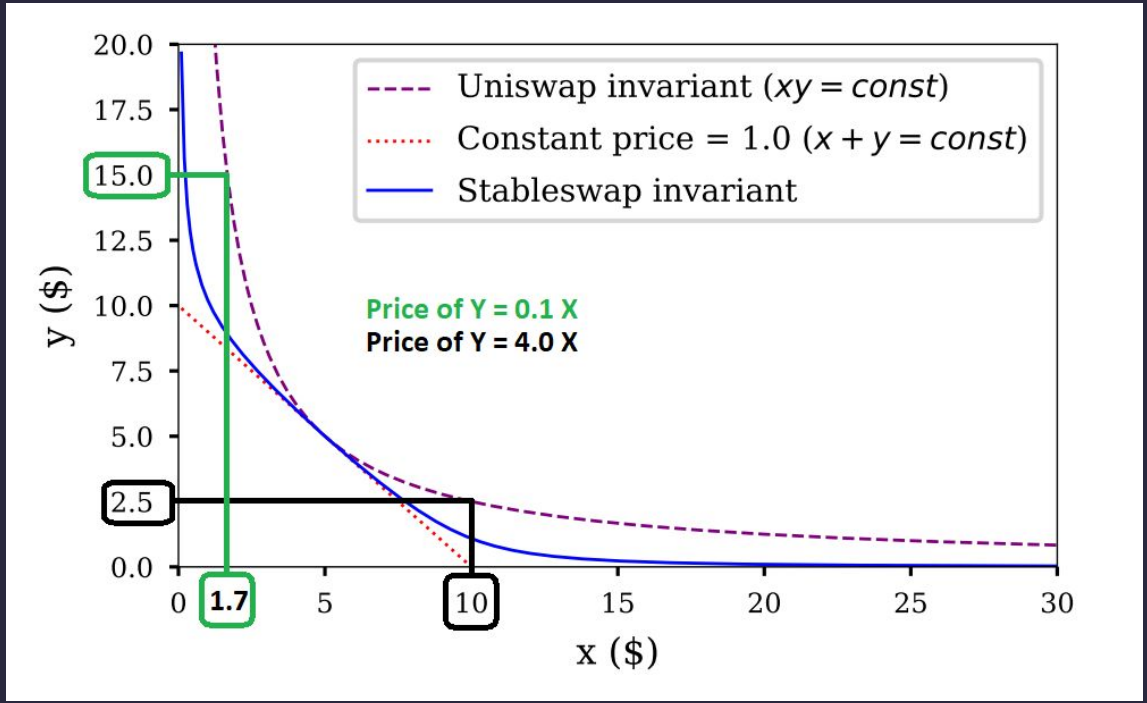
We compare KyberNetwork to existing systems in the table below. We left out Bancor intentionally as they claim (from our private conversation) to be a platform that focus on community tokens, rather than general purpose exchange.

Exchange	Trading Cost [7]	Trustless	Instant Trades	On-chain	Guaranteed Liquidity	SecureAgainst Attacks
Kraken/Poloniex	Low	No	No	No	Yes	No
Shapeshift	Low	No	Yes	No	Yes	No
Coinbase	Low	No	Yes	No	Yes	No
EtherDelta Oasis Index	High	Yes	No	Yes	No	Yes
Swap.tech 0xProject	Low Low	Somewh-at[8]	No	Hybrid	No	Not sure[9]
KyberNetwork	Low	Yes	Yes	Yes	Yes	Yes

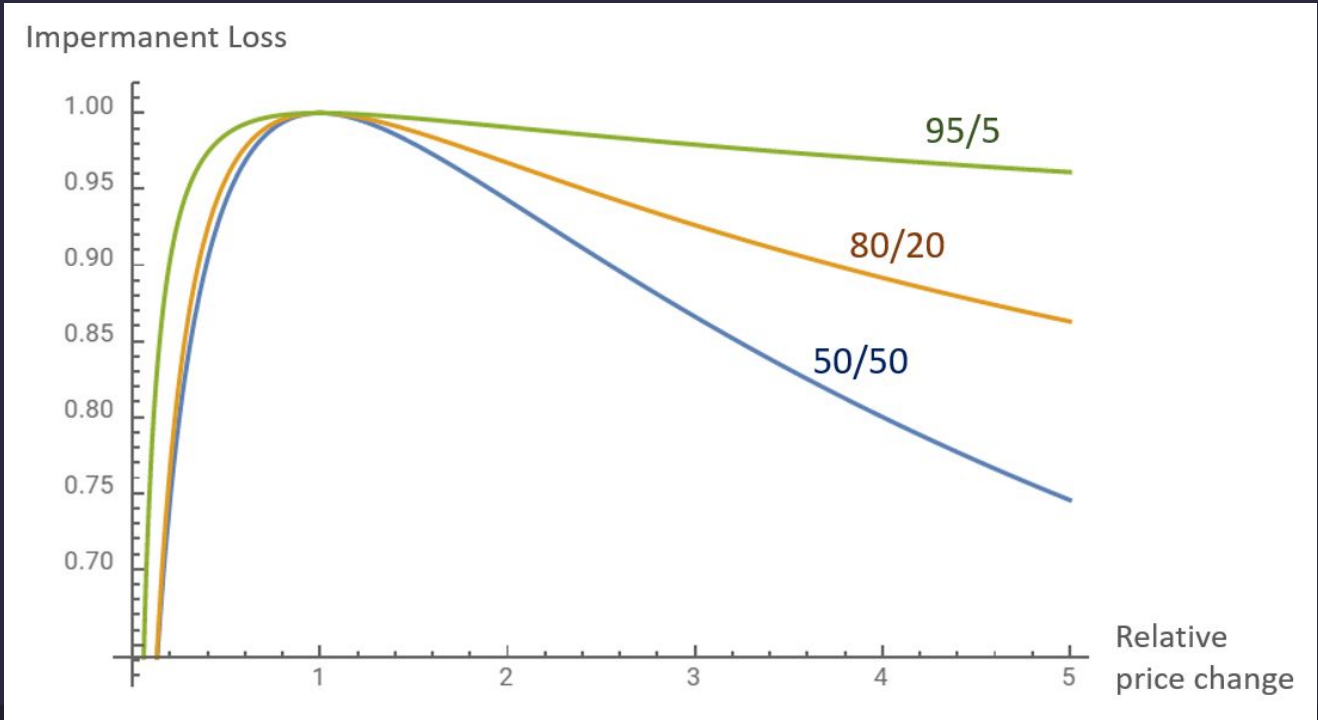
/DEX (7) Kyber


Reserve Manager
Share profits
Reserve Contributor
Feed exchange rates
Contribute tokens B
Scenario 1: Reserve can't contribute in real time (period of high demand)
Send Token A
User
KyberNetwork contract
Credit Token A
Reserve
Debit Token B
Send Token B
List/ Delist tokens and reserves
Scenario 2: Token A in token pair A/B has low liquidity
KyberNetwork operator

/DEX (8) Uniswap, Curve, Balancer, Bancor



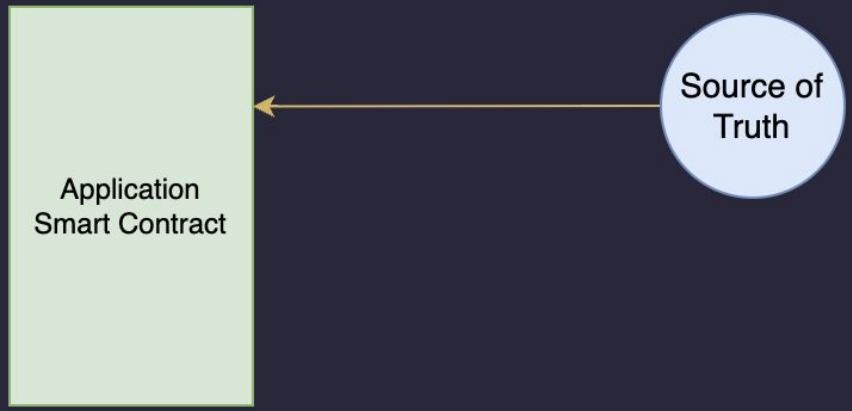
/DEX (9) Impermanent loss



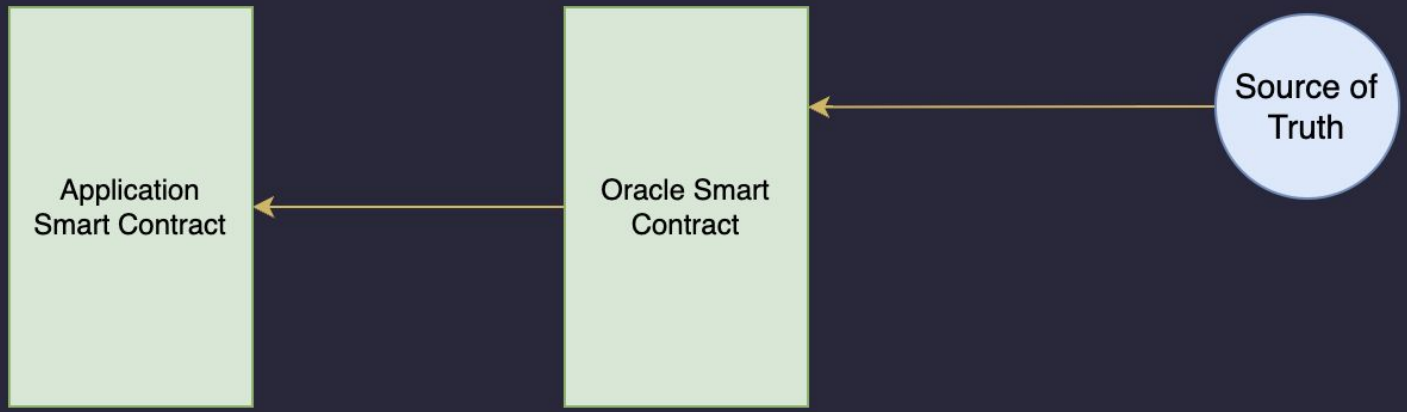
/Oracle

- Blockchain does not have external data
- There are applications that would need external data - because we need to trust these data, the data source is called Oracle.

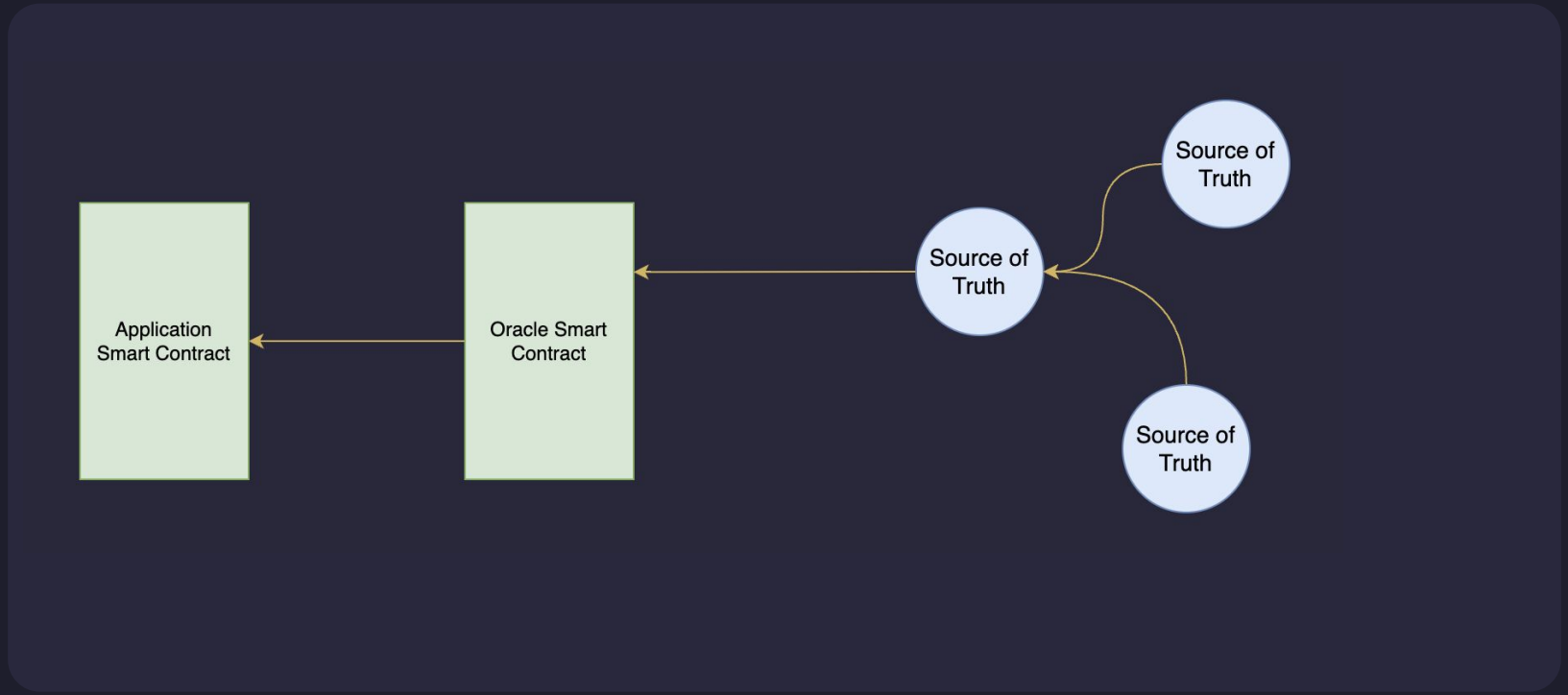
/Oracle



/Oracle


Application
Smart Contract
Oracle Smart
Contract
Source of
Truth

/Oracle


Application Smart Contract
Oracle Smart Contract
Source of Truth
Source of Truth
Source of Truth

/Oracle

- Not just true or false? How about numeric like prices.
- NFT prices?
- Security issues
  - Oracle Manipulation?
  - Wrong source

/THAT'S A WRAP!  (mic drop)