Oracles

Lecturer: Ari Juels

The Initiative for CryptoCurrencies and Contracts

CORNELL TECH

JACOBS TECHNION-CORNELL INSTITUTE AT CORNELL TECH

Decentralized Finance

Instructors: Dan Boneh, Arthur Gervais, Andrew Miller, Christine Parlour, Dawn Song

Stanford University

Imperial College London

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Berkeley UNIVERSITY OF CALIFORNIA

What we’ll cover in this lecture

- Introduction
- Basic oracle design (Part I)
- Basic oracle design (Part II)
- Advanced oracle use cases
- Oracle privacy
- DeFi applications using privacy-preserving oracles

Lecture Intro

Consider a few types of smart contracts / Dapps

- Token management
  - E.g., ERC-20
- DEXes
  - E.g., Uniswap
- NFT games
  - E.g., CryptoKitties

- Lending
  - E.g., MakerDAO
- Insurance
  - E.g., flight insurance

Consider a few types of smart contracts / Dapps

- Token management
  - E.g., ERC-20
- DEXes
  - E.g., Uniswap
- NFT games
  - E.g., CryptoKitties

No external data

- Lending
  - E.g., MakerDAO
- Insurance
  - E.g., flight insurance

Needs external data

Consider a few types of smart contracts / Dapps

- Token management
  - E.g., ERC-20
- DEXes
  - E.g., Uniswap
- NFT games
  - E.g., CryptoKitties

No external data

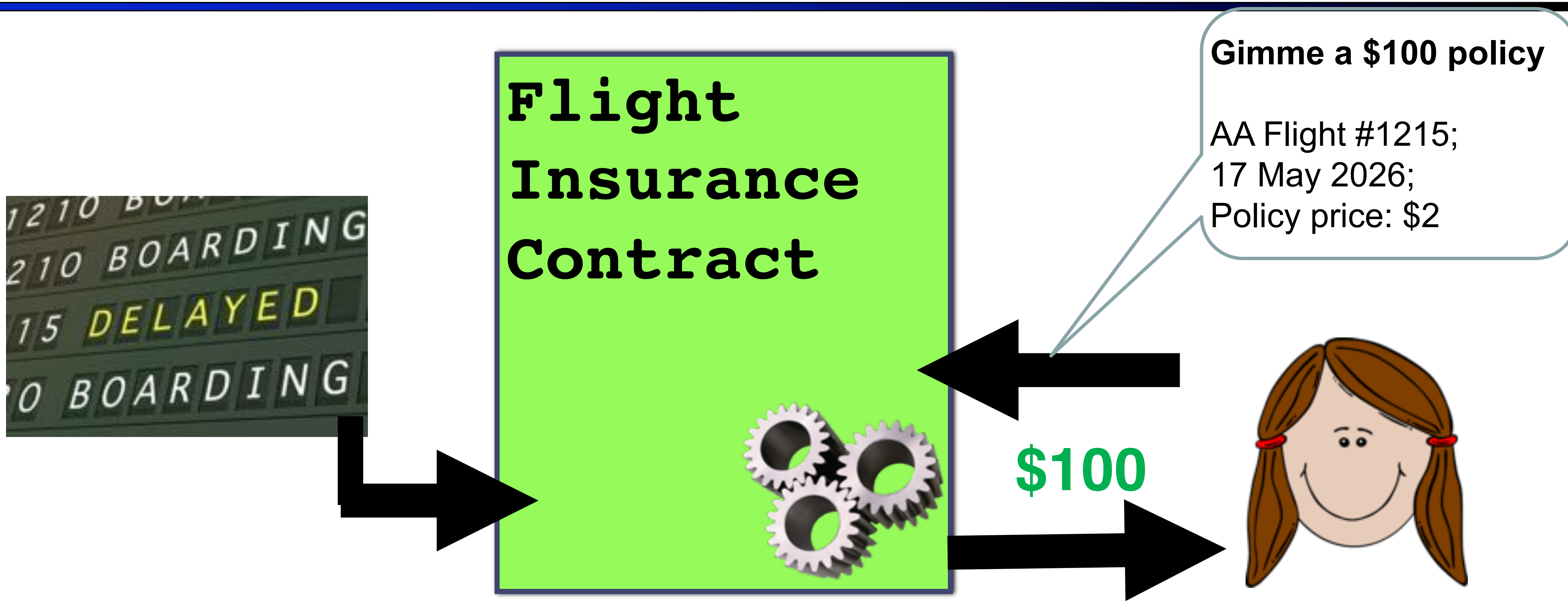
- Lending
  - E.g., MakerDAO
- Insurance
  - E.g., flight insurance
- NFT games

Needs external data

Collateralized lending contract

- How does it work?
  1. Borrower deposits collateral in a vault
     - E.g., ETH worth $300
  2. Borrower withdraws ($1) stablecoins
     - E.g., $100 in stablecoins
  3. If collateral value drops below threshold, then contract liquidates
     - E.g., if ETH worth less than $150
- How does contract know how many stablecoins to issue or when to liquidate?
  - Needs ETH-USD price feed

Parametric flight insurance



Flight Insurance Contract

Gimme a $100 policy

AA Flight #1215;
17 May 2026;
Policy price: $2

$100

- How does contract know whether to pay user?
  - Needs flight data

Other DeFi applications that need data

- Betting contracts, e.g., sports
- Wrapped cryptocurrency
- Synthetics
- Undercollateralized lending

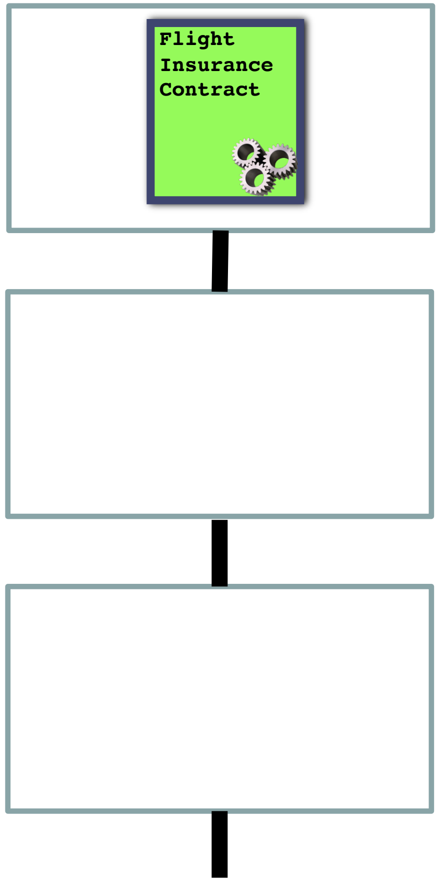
Blockchains lack internet connections!

Blockchain

DeFi smart contract

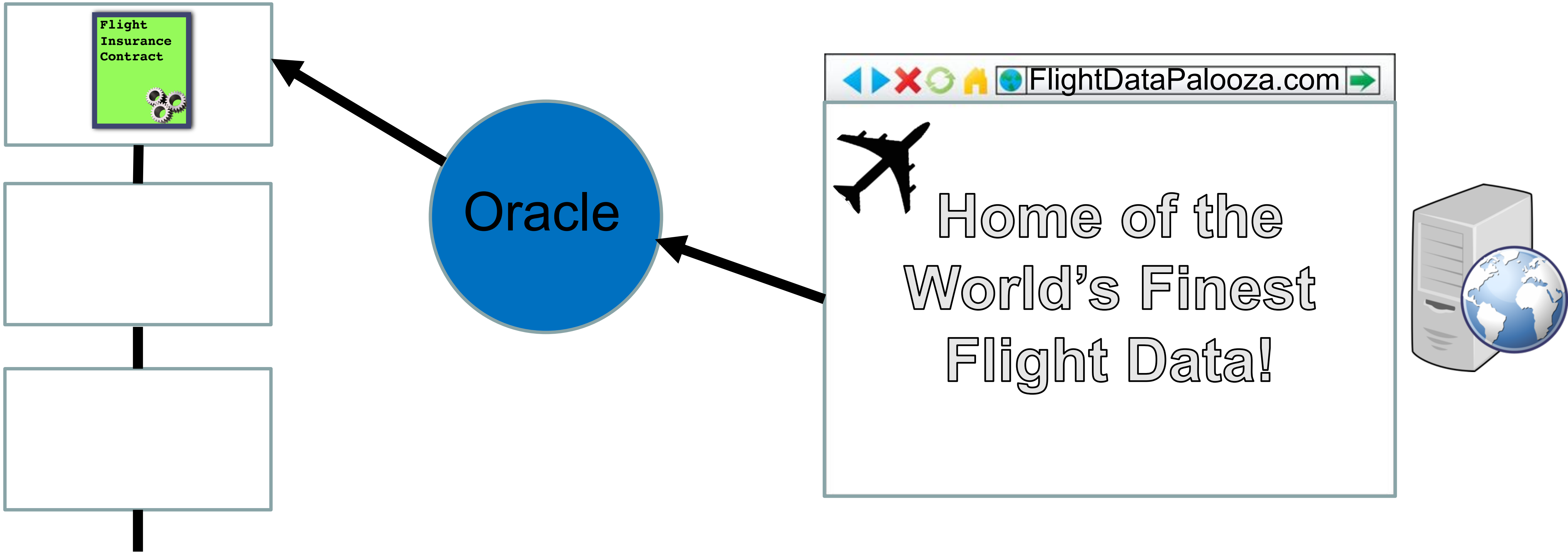
What’s the USD price of BTC?

How do we get external data to contracts?

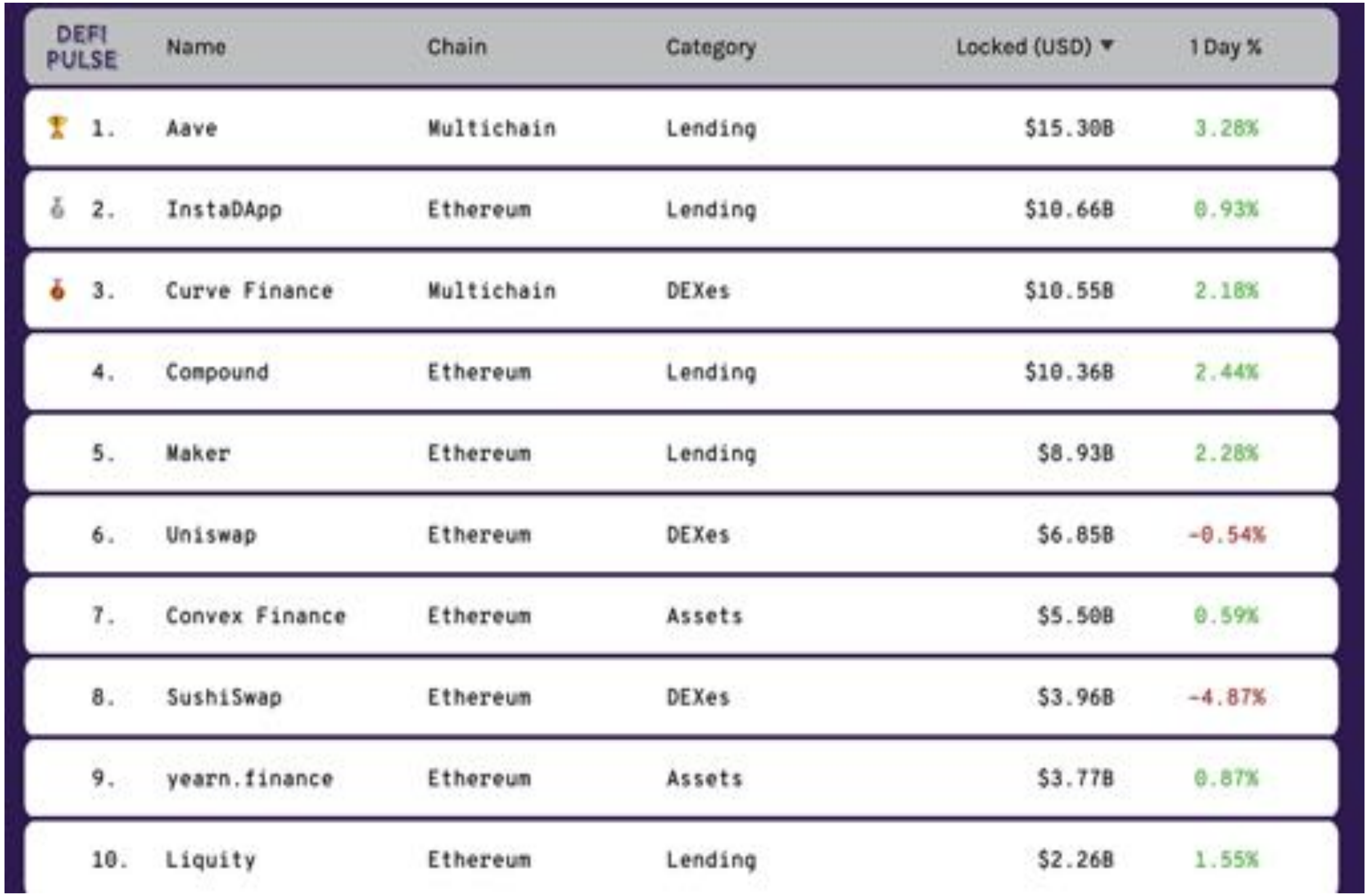


FlightDataPalooza.com
Home of the
World’s Finest
Flight Data!

Oracle


Flight
Insurance
Contract
Oracle
FlightDataPalooza.com
Home of the
World's Finest
Flight Data!

Oracle use today



DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
🏆 1.	Aave	Multichain	Lending	$15.30B	3.28%
🥈 2.	InstaDApp	Ethereum	Lending	$10.66B	0.93%
🥉 3.	Curve Finance	Multichain	DEXes	$10.55B	2.18%
4.	Compound	Ethereum	Lending	$10.36B	2.44%
5.	Maker	Ethereum	Lending	$8.93B	2.28%
6.	Uniswap	Ethereum	DEXes	$6.85B	-0.54%
7.	Convex Finance	Ethereum	Assets	$5.50B	0.59%
8.	SushiSwap	Ethereum	DEXes	$3.96B	-4.87%
9.	yearn.finance	Ethereum	Assets	$3.77B	0.87%
10.	Liquity	Ethereum	Lending	$2.26B	1.55%

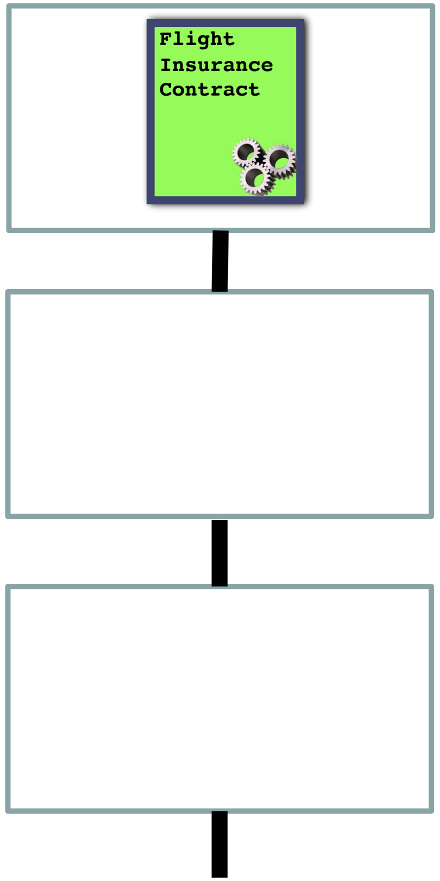
- Every single DeFi app other than DEXes uses an oracle and…
- DEXes can serve as oracles!

Defining oracles

- **Narrow definition:** Off-chain platform that relays data on chain
- **Generalized definition:** Off-chain platform that connects blockchains with other systems

Basic Oracle Design
Part I

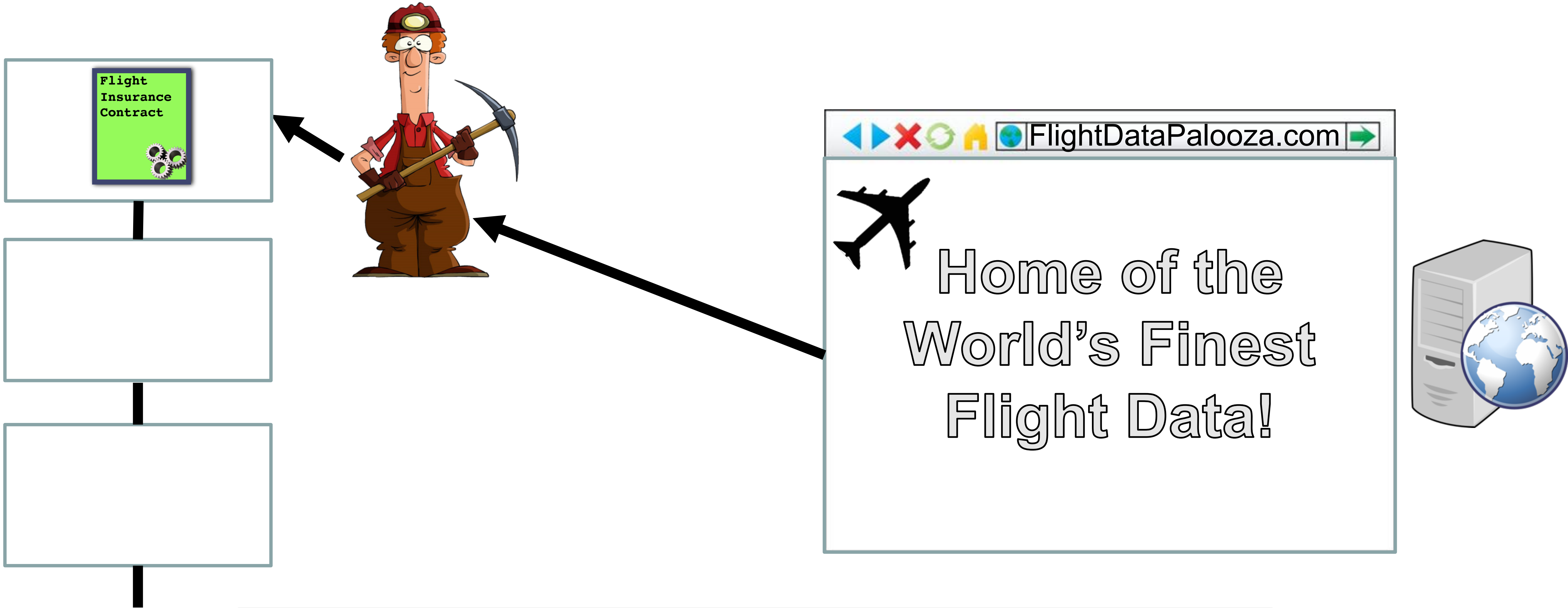
How to build an oracle?



FlightDataPalooza.com
Home of the
World's Finest
Flight Data!

- Seems straightforward!

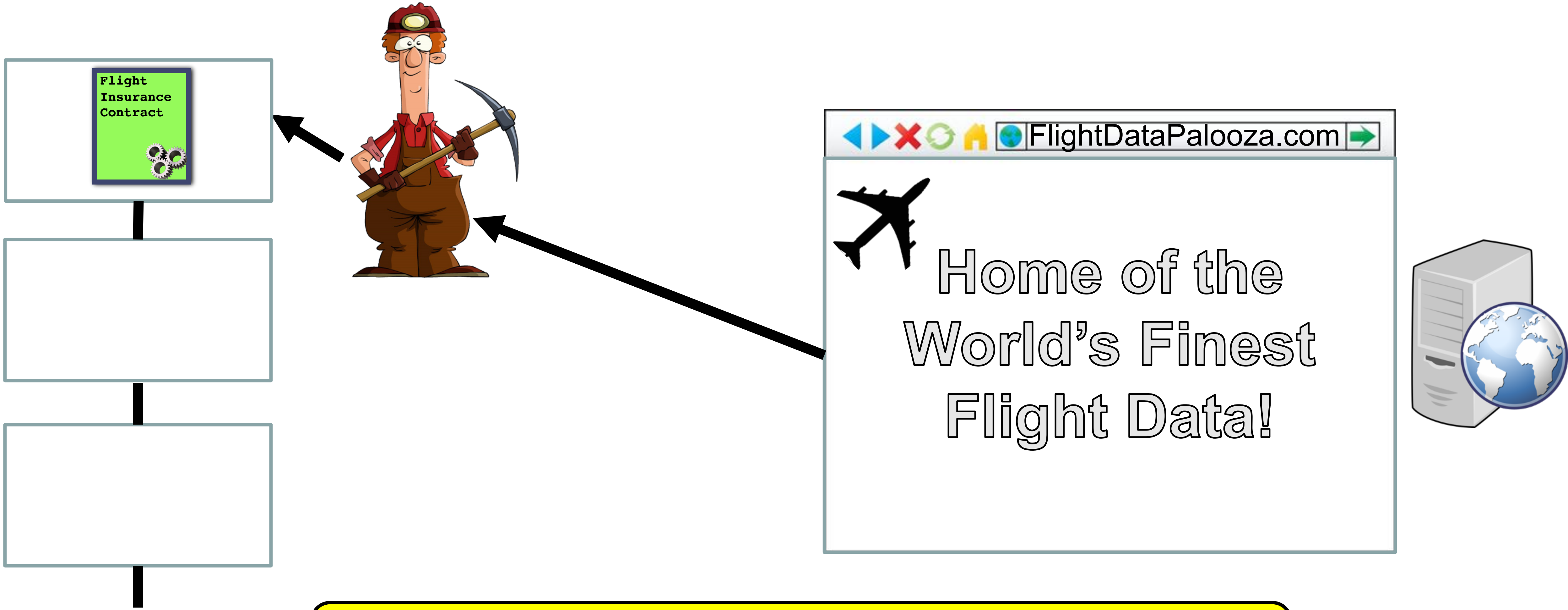
How to build an oracle?



Home of the World’s Finest Flight Data!

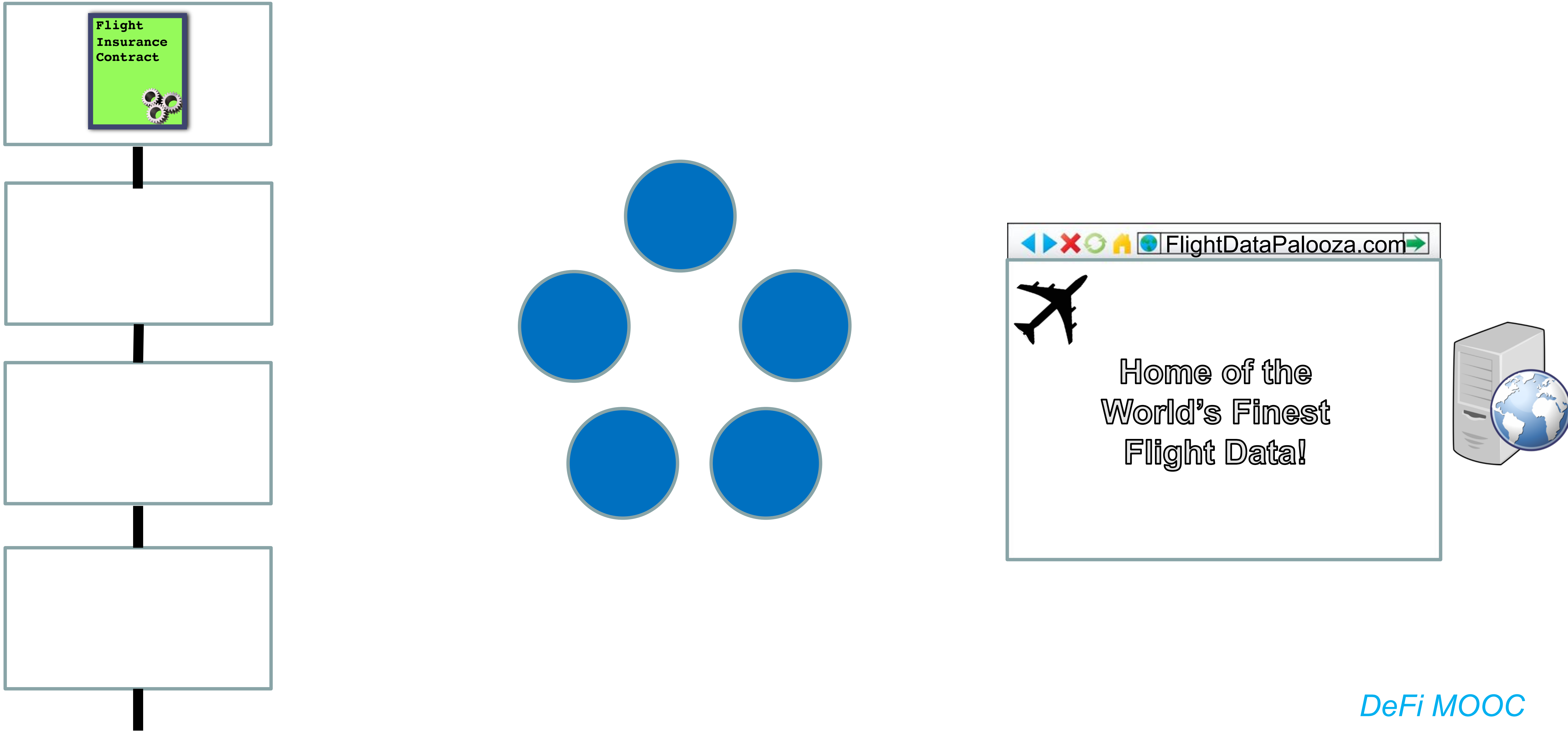
Idea: Build oracle into the consensus protocol.

How to build an oracle?


Flight Insurance Contract
FlightDataPalooza.com
Home of the World's Finest Flight Data!

Problem: What if the miner *lies / cheats?*

Oracle network

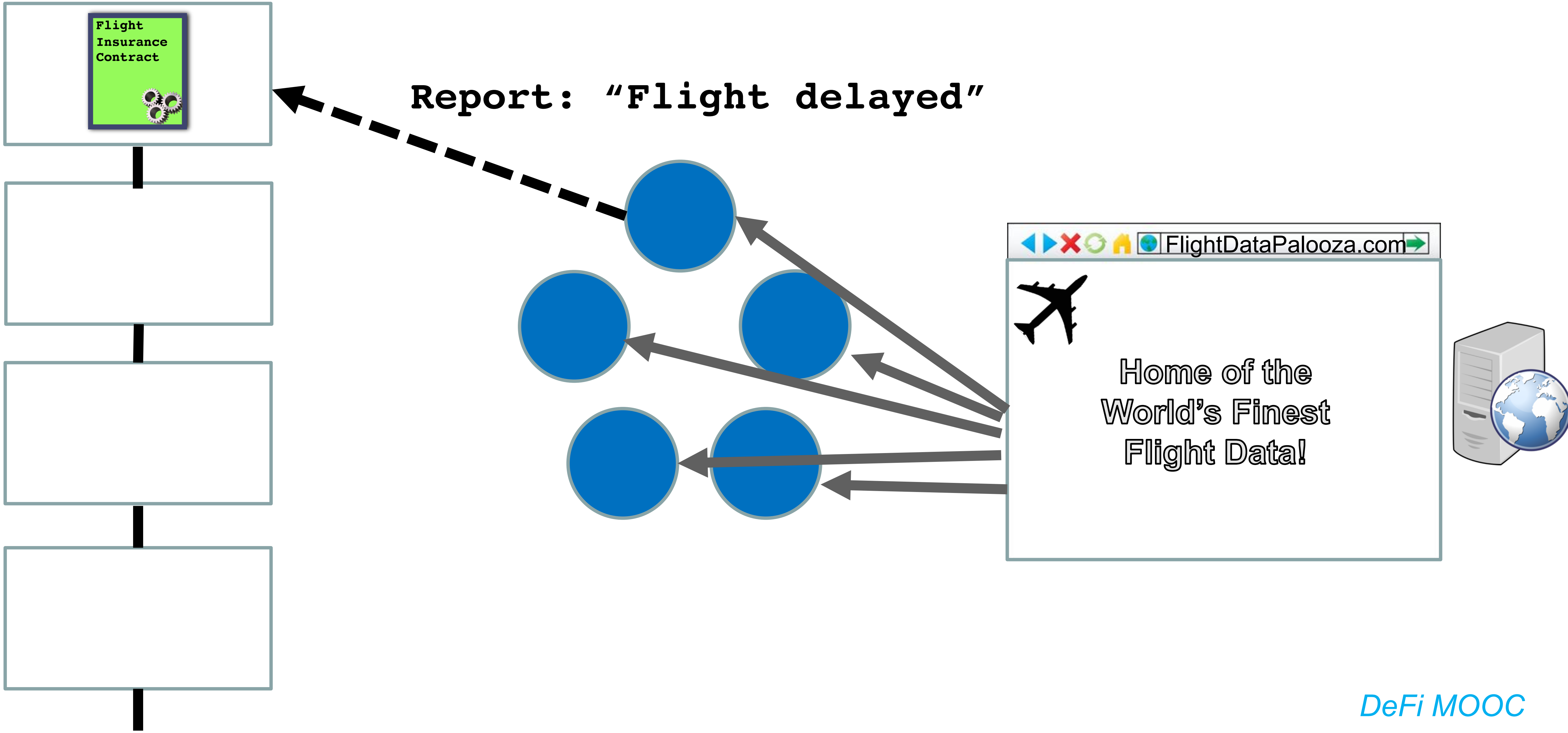


Flight Insurance Contract

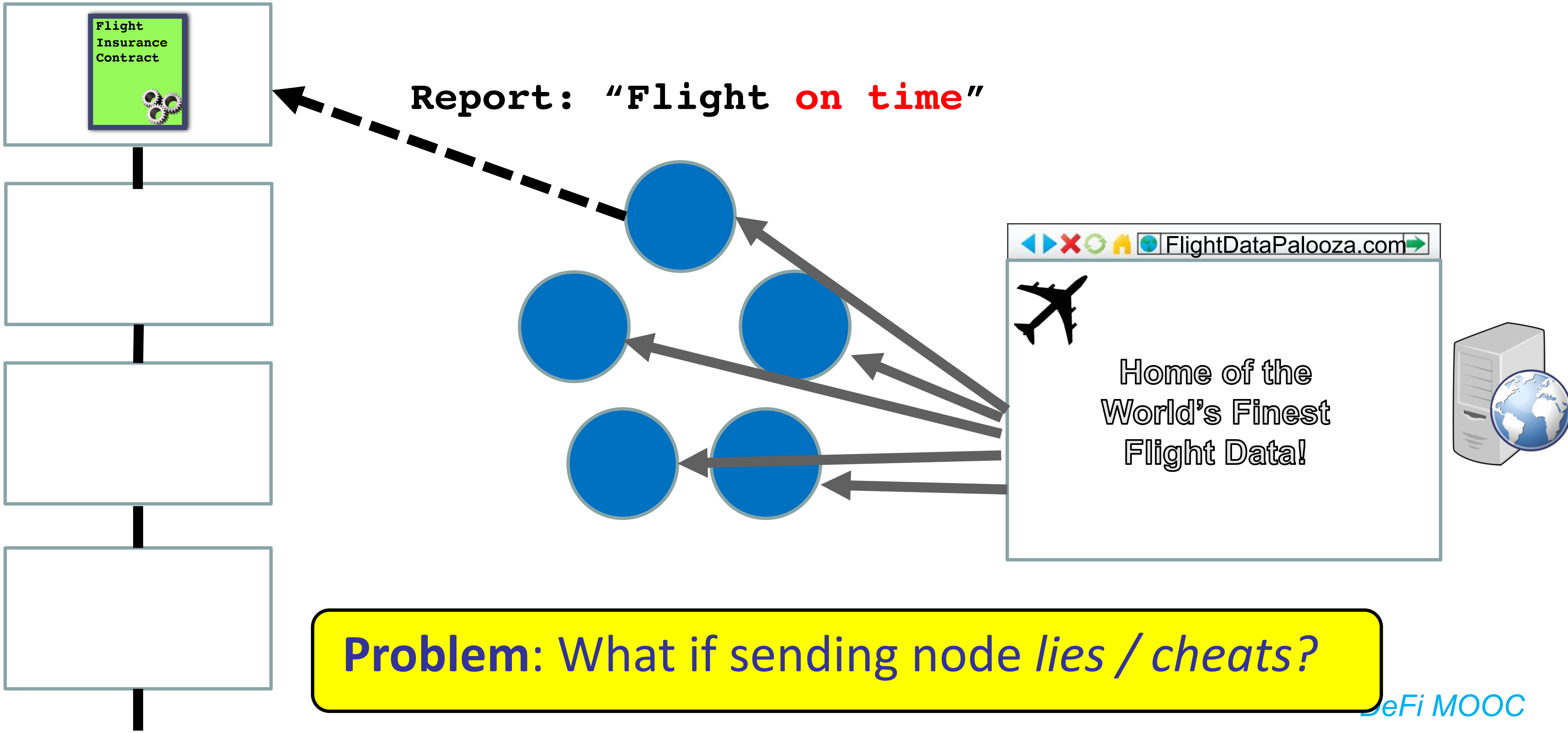
FlightDataPalooza.com

Home of the World's Finest Flight Data!

Oracle network

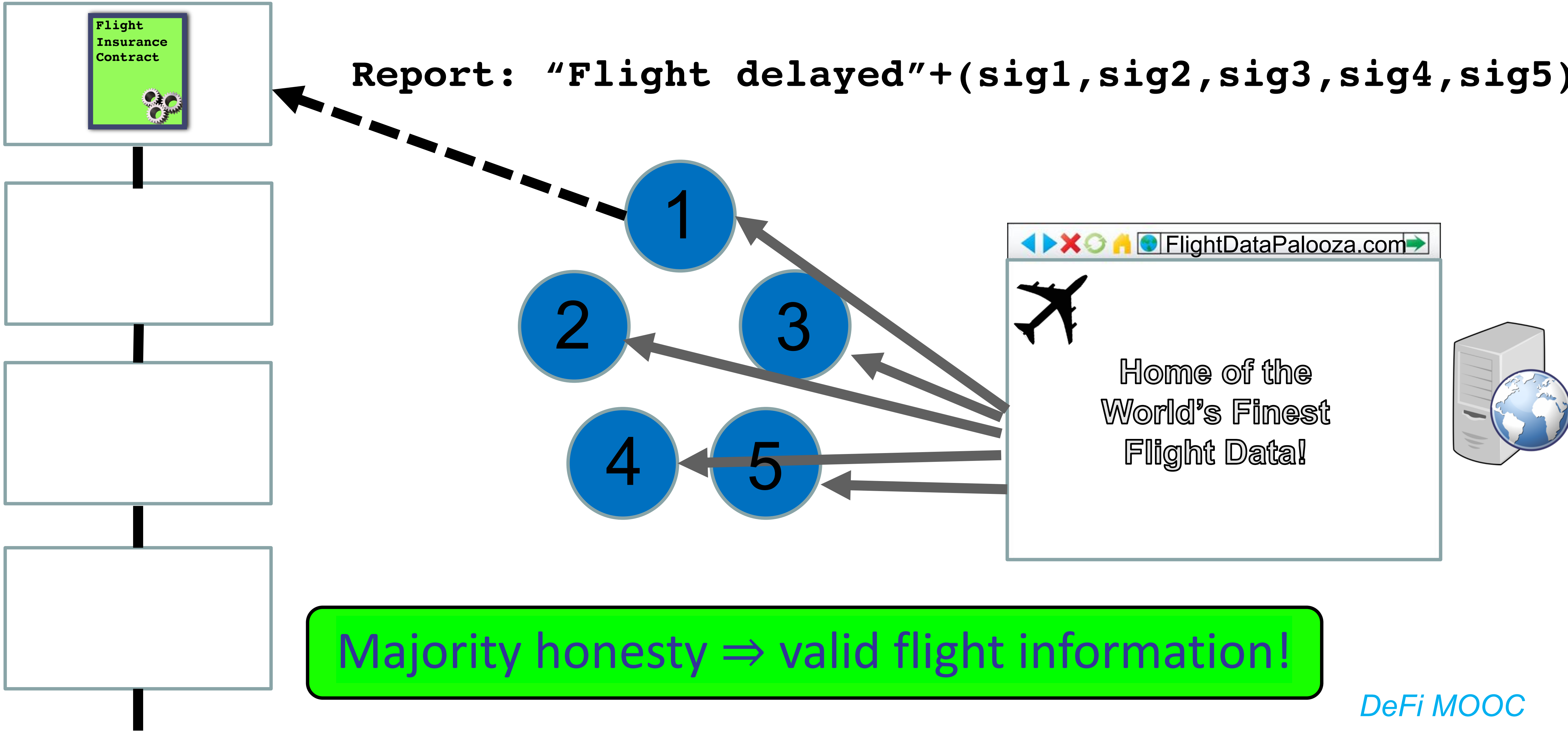

Flight Insurance Contract
Report: "Flight delayed"
FlightDataPalooza.com
Home of the World's Finest Flight Data!

Oracle network


Flight Insurance Contract
Report: “Flight on time”
FlightDataPalooza.com
Home of the World’s Finest Flight Data!

Problem: What if sending node *lies / cheats?*

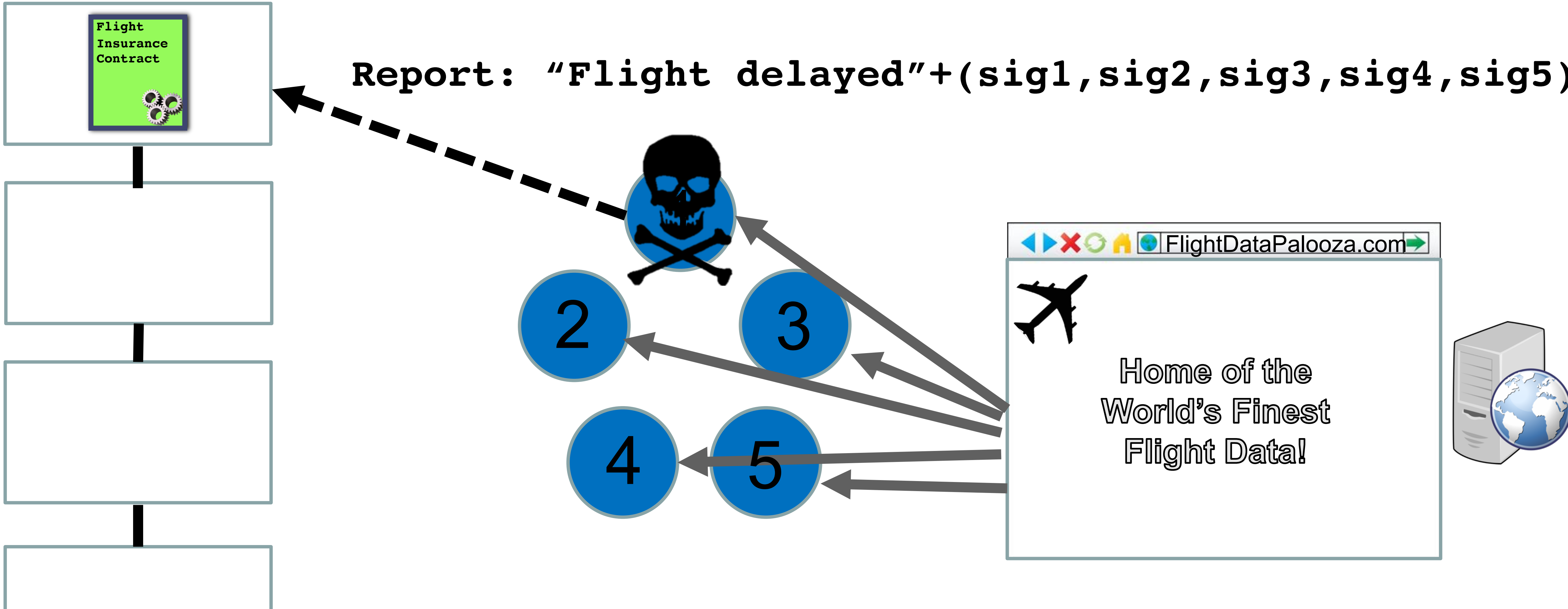
Digital signatures



Report: “Flight delayed”+(sig1,sig2,sig3,sig4,sig5)

Majority honesty ⇒ valid flight information!

Oracle-node liveness

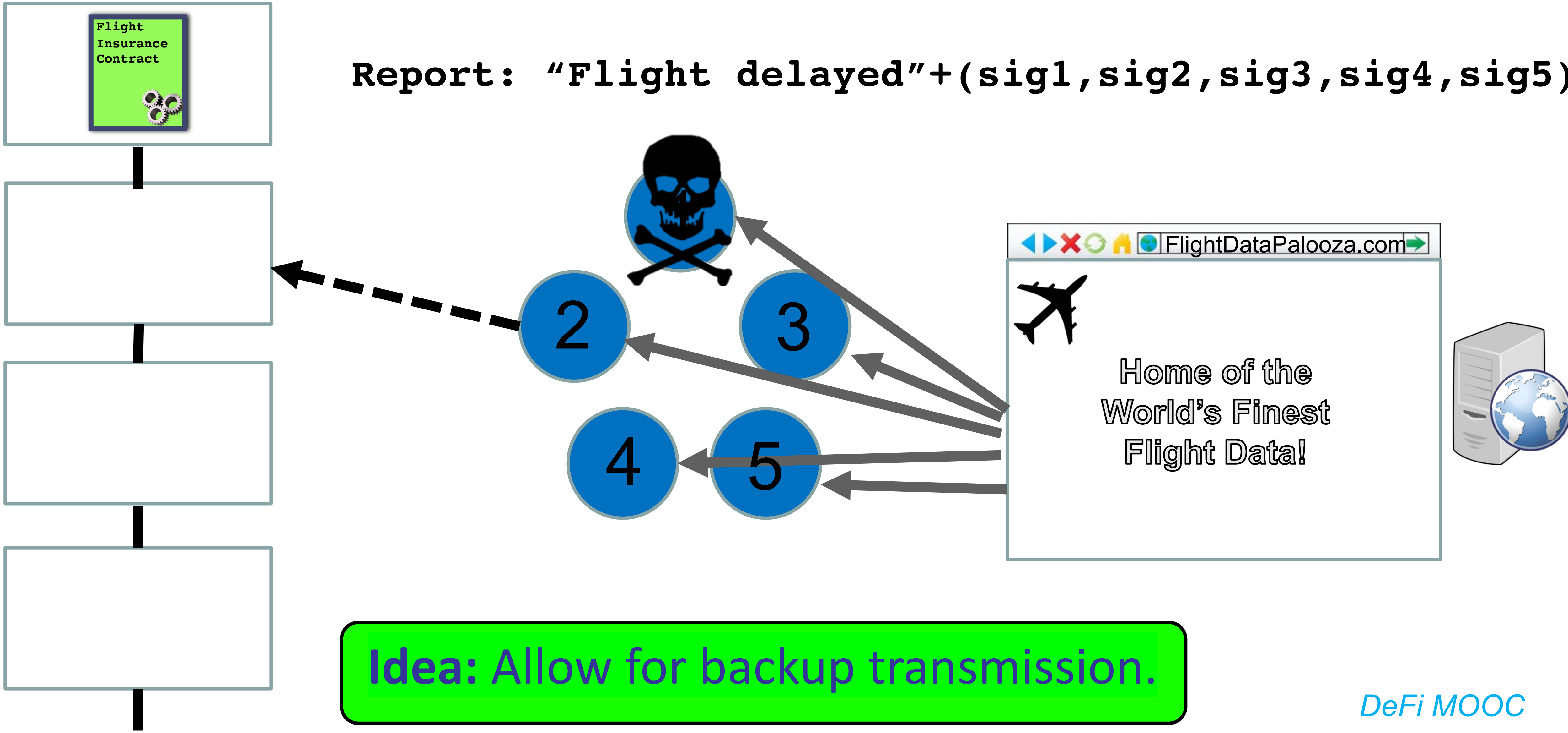


`Report: “Flight delayed”+(sig1,sig2,sig3,sig4,sig5)`

Problem: What if sending node goes down?

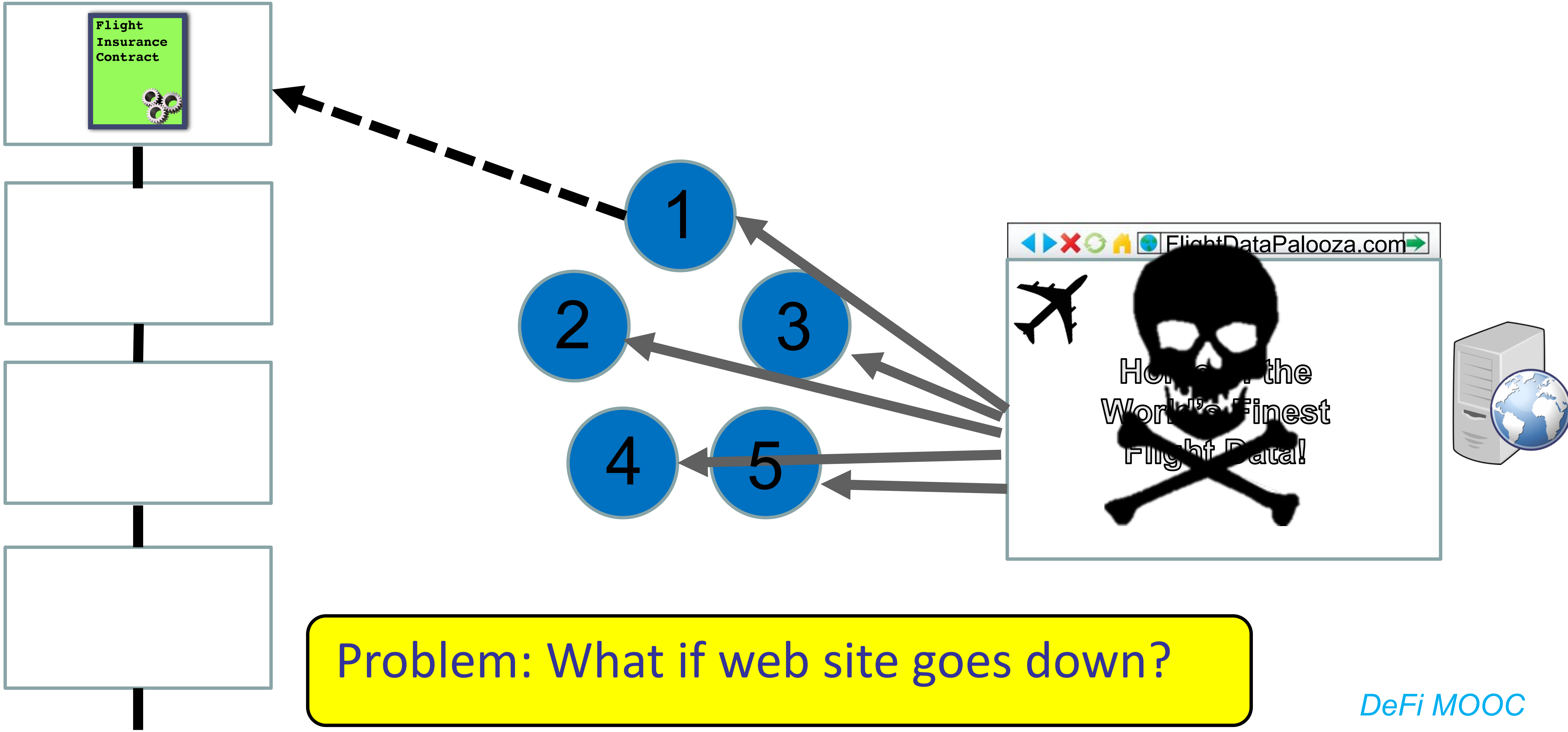
Oracle-node liveness

Report: “Flight delayed”+(sig1,sig2,sig3,sig4,sig5)


Flight Insurance Contract
2
3
4
5
FlightDataPalooza.com
Home of the World’s Finest Flight Data!

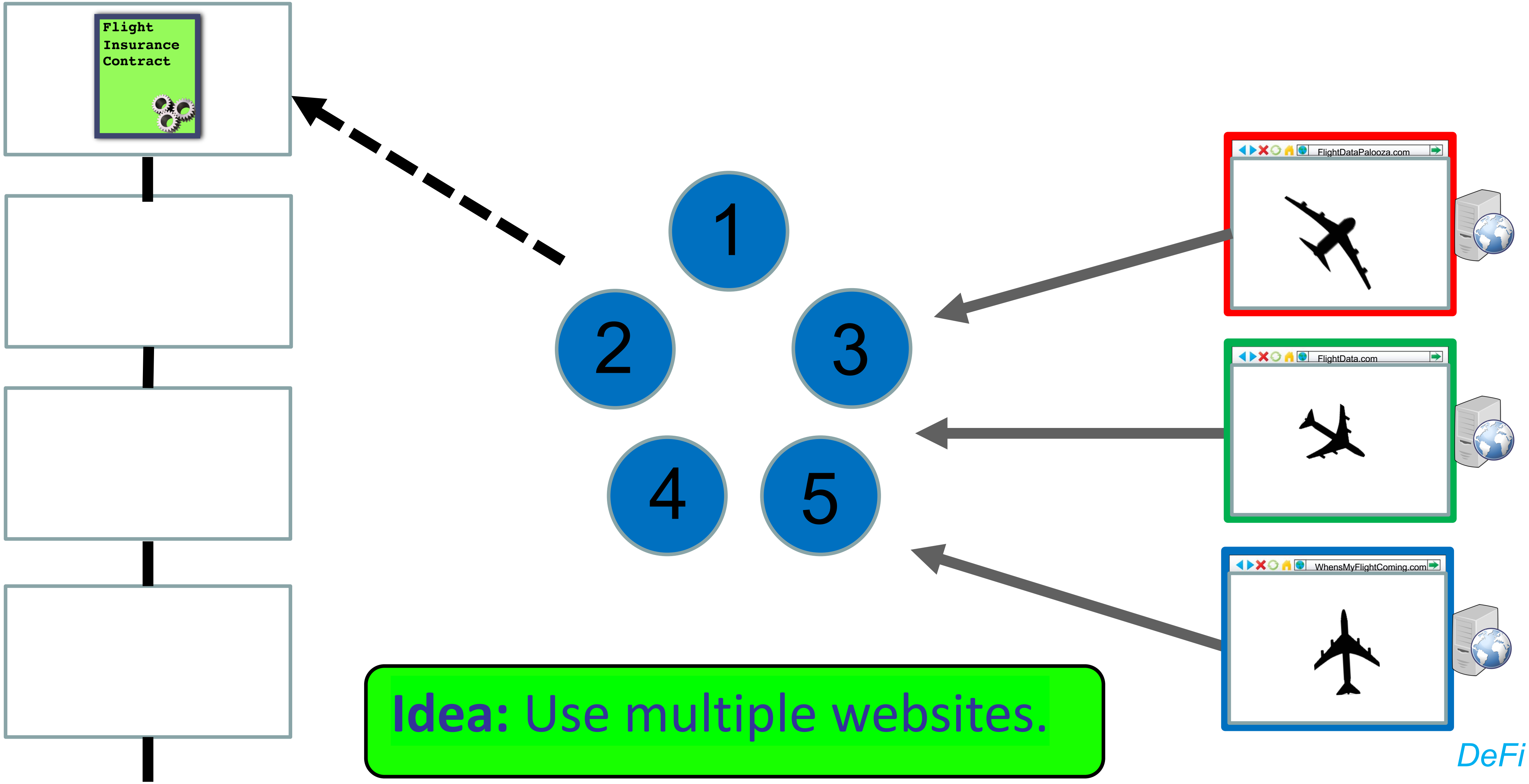
Idea: Allow for backup transmission.

Source Liveness



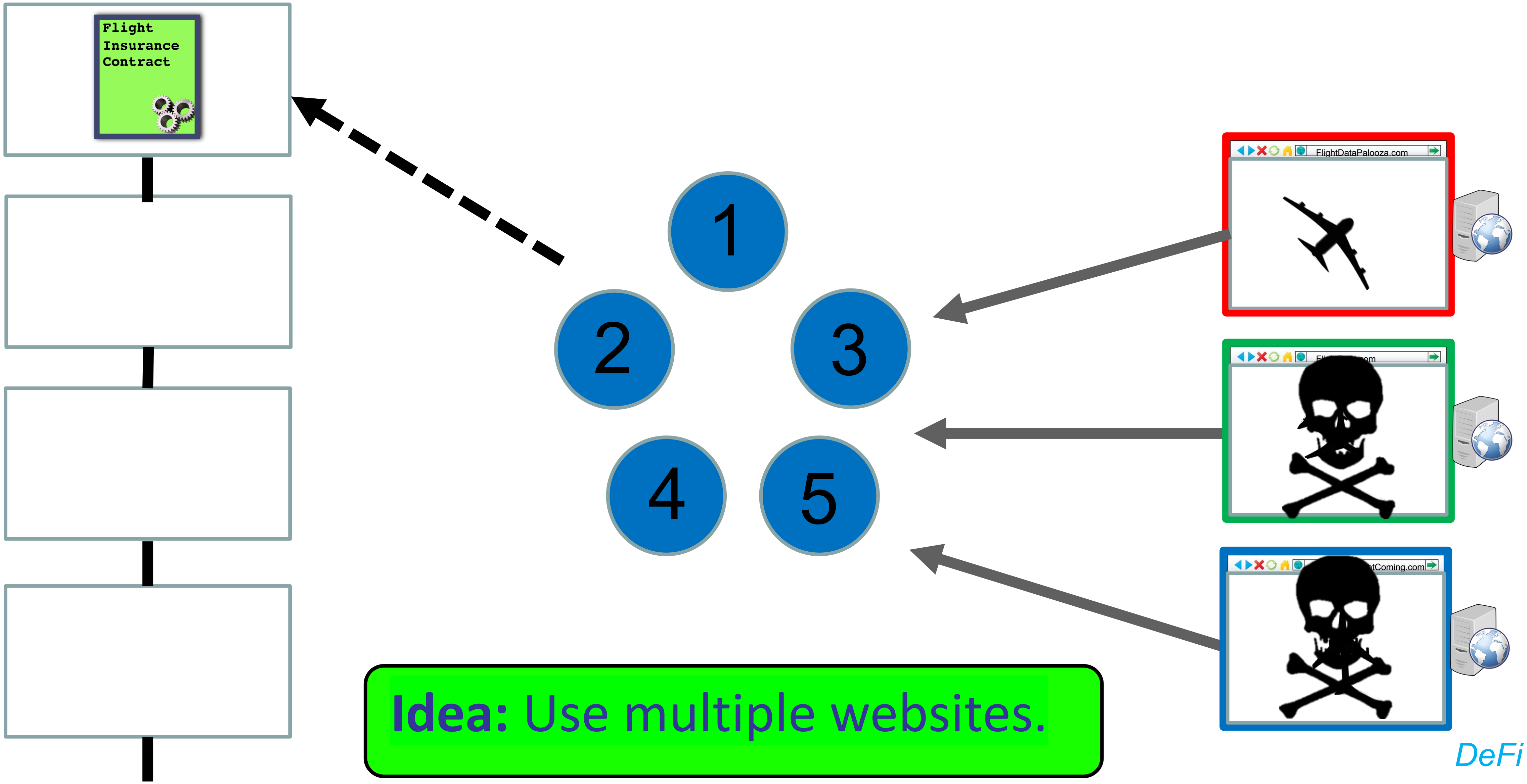
Problem: What if web site goes down?

Source Liveness



Idea: Use multiple websites.

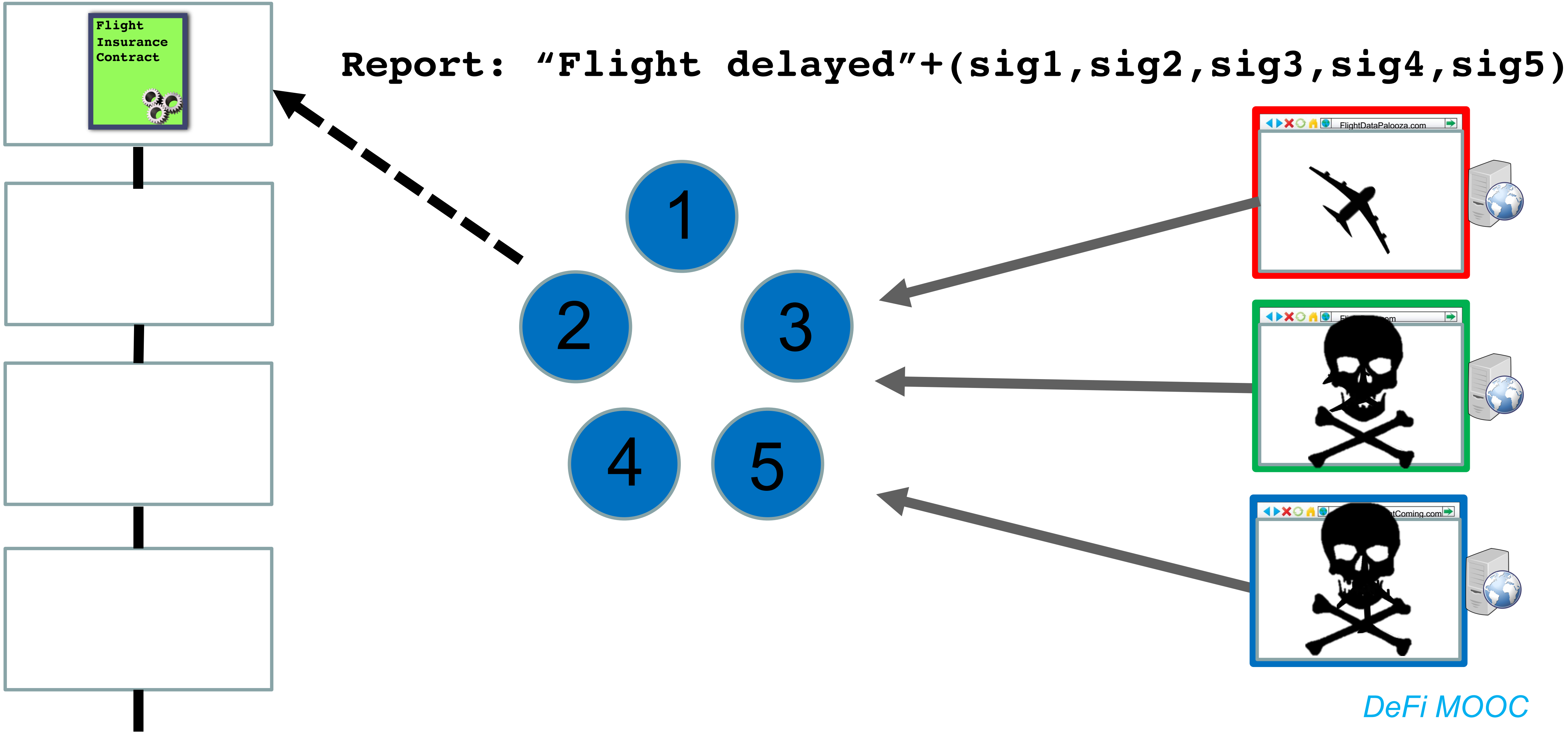
Source Liveness



Idea: Use multiple websites.

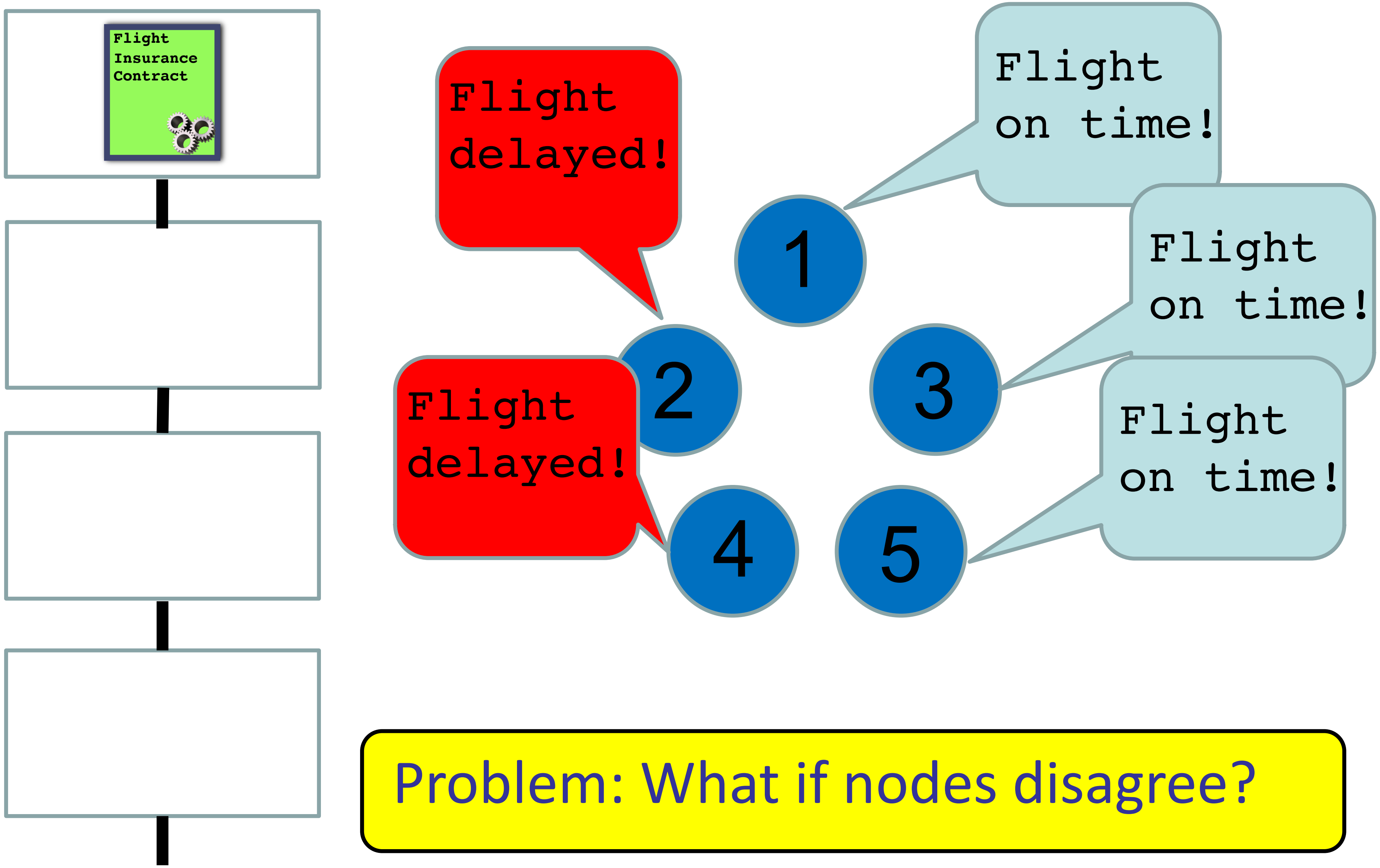
Basic Oracle Design Part II

We’ve achieved decentralization + good liveness



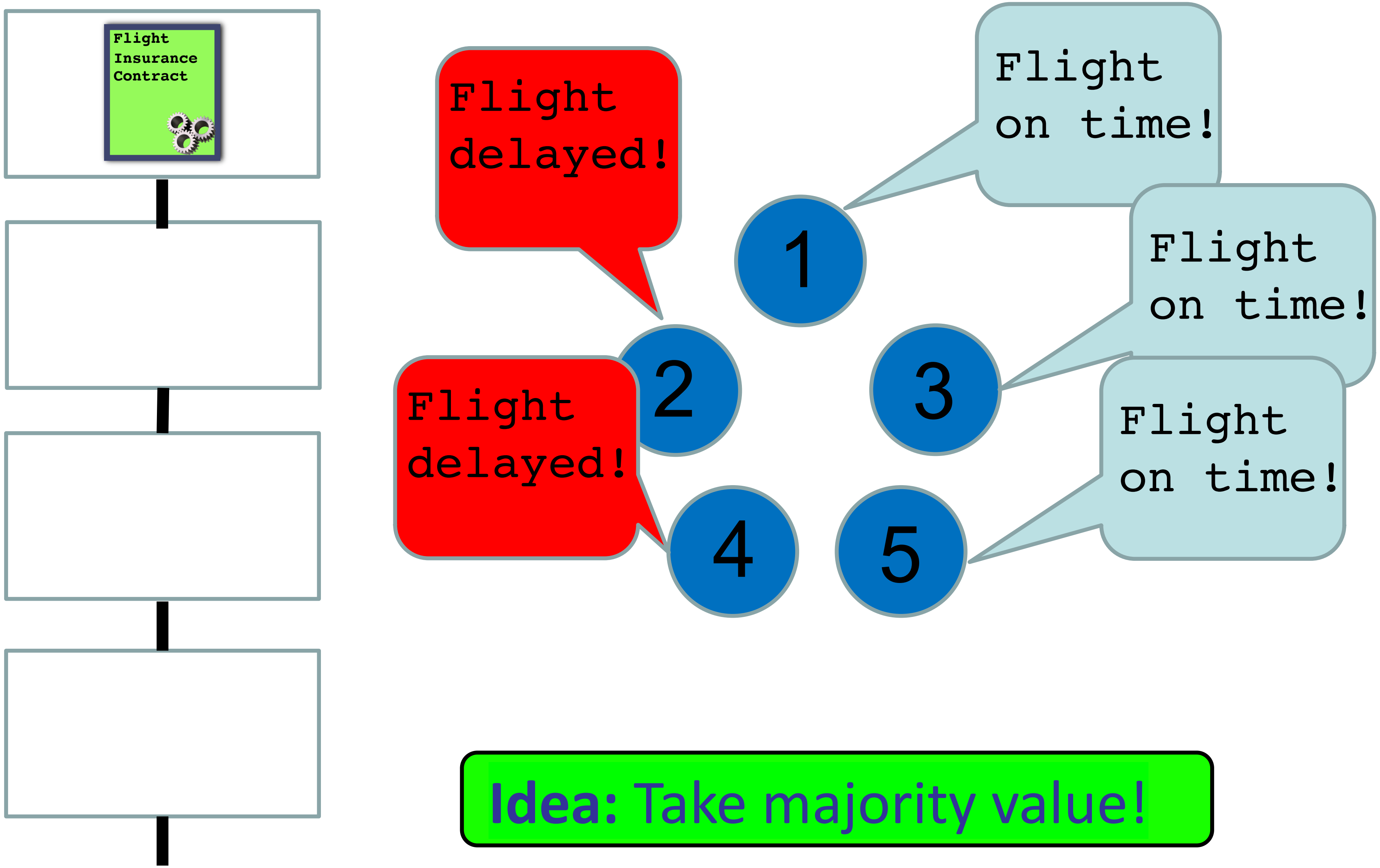
Report: “Flight delayed”+(sig1,sig2,sig3,sig4,sig5)

Heterogeneous data



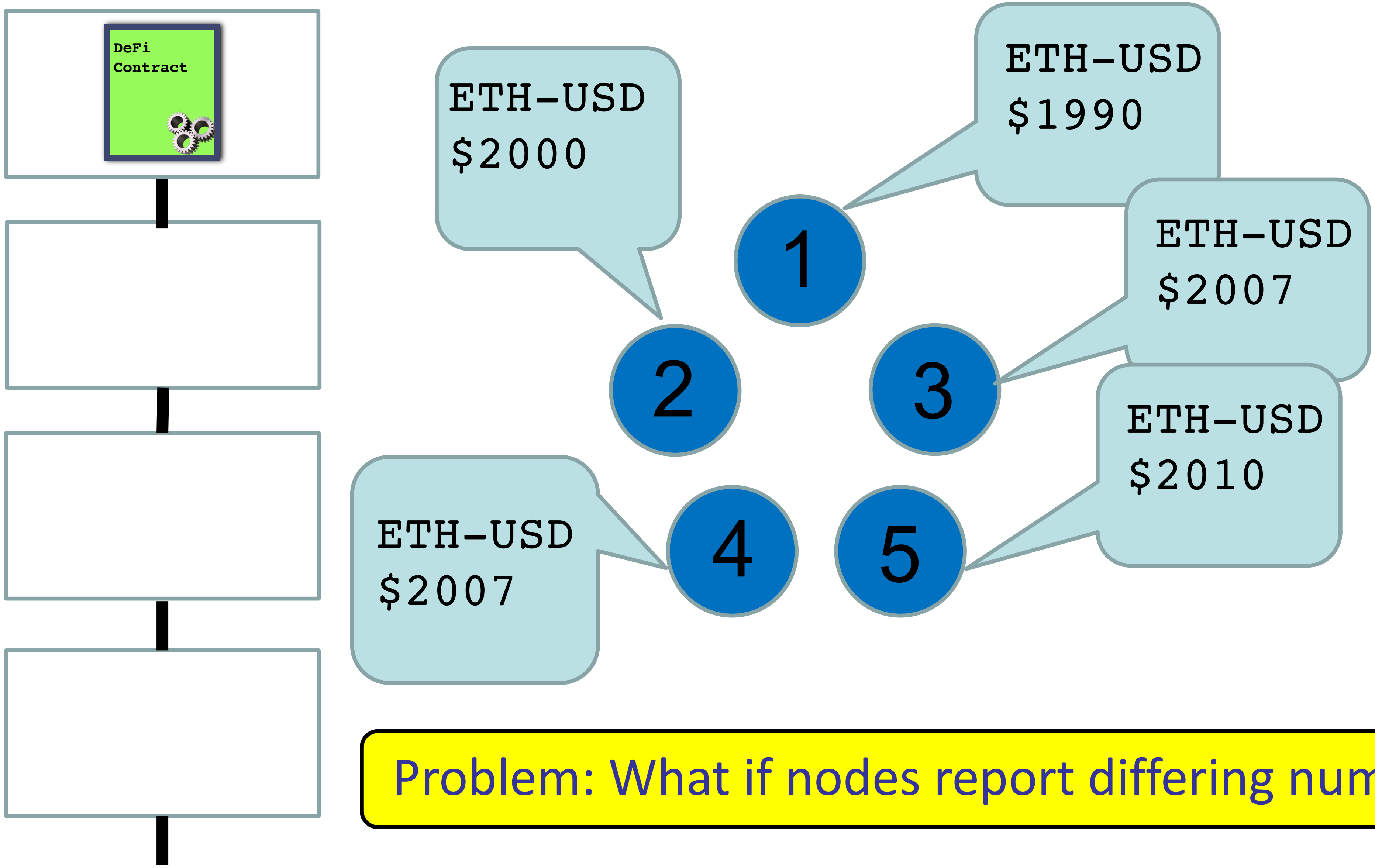
Problem: What if nodes disagree?

Heterogeneous data



Idea: Take majority value!

Heterogeneous data



Problem: What if nodes report differing numerical values?

Combining reports

DeFi Contract

$1985

$1991

$1999

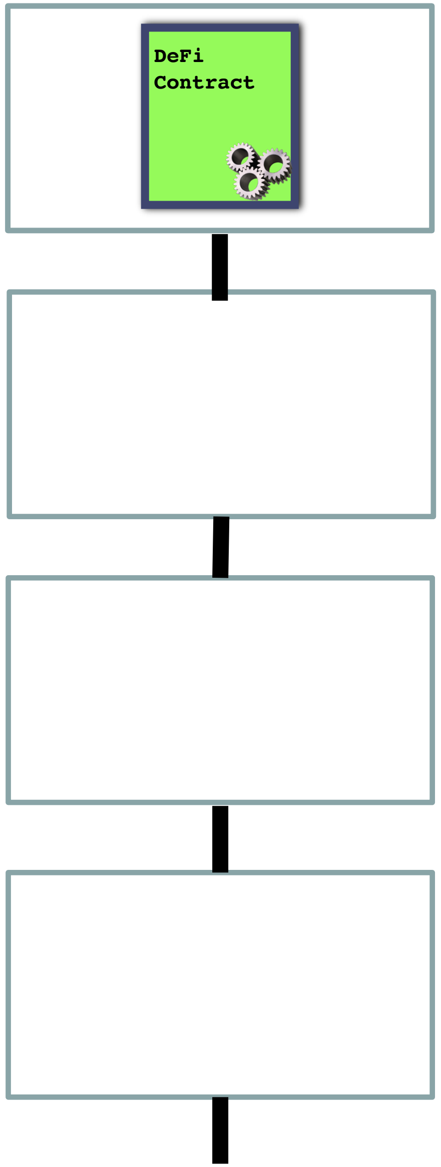
$2000

$2007

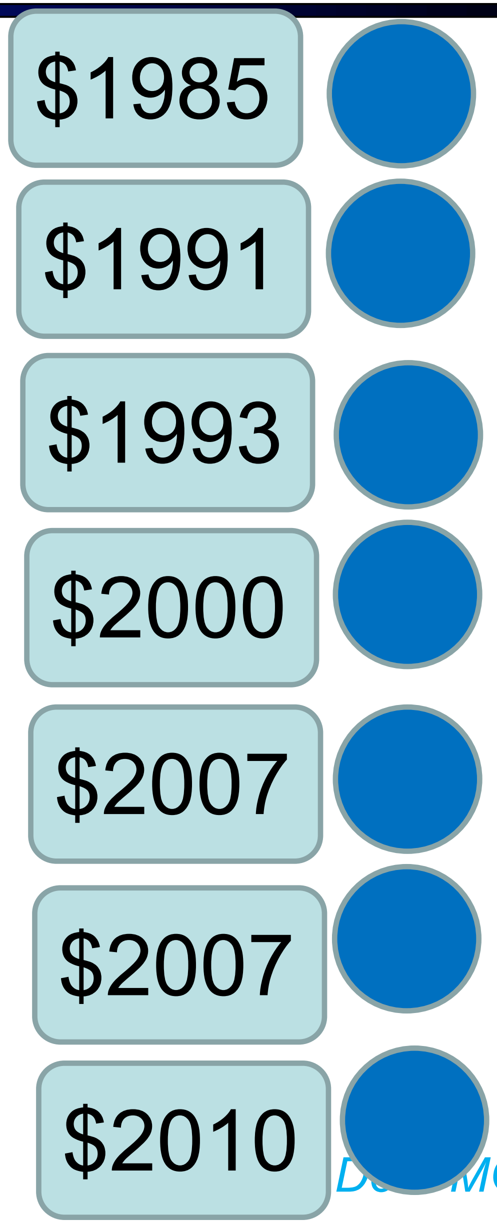
$2007

$2010

Combining reports



Mean = $1999



$1985

$1991

$1993

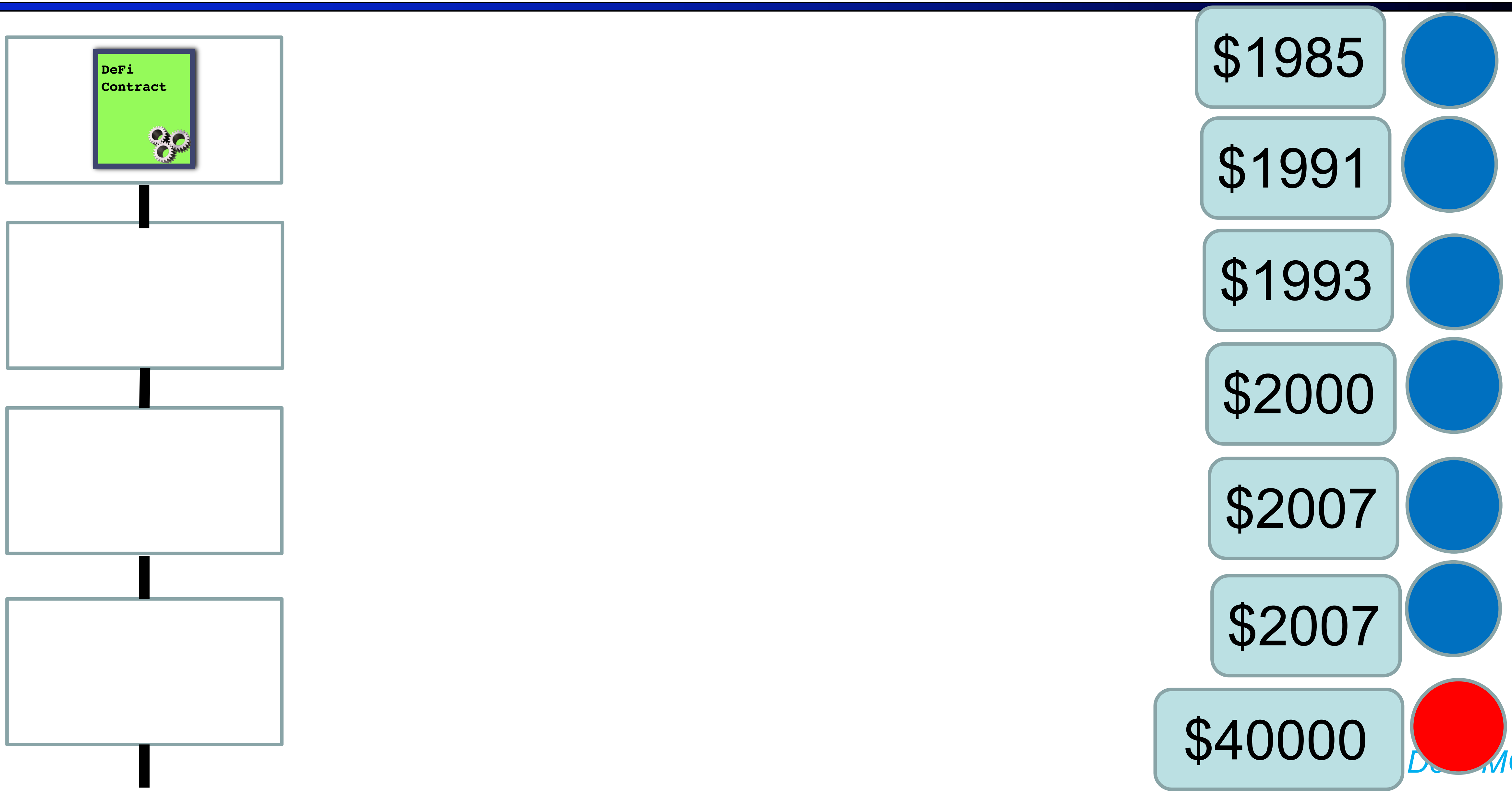
$2000

$2007

$2007

$2010

Combining reports



$1985

$1991

$1993

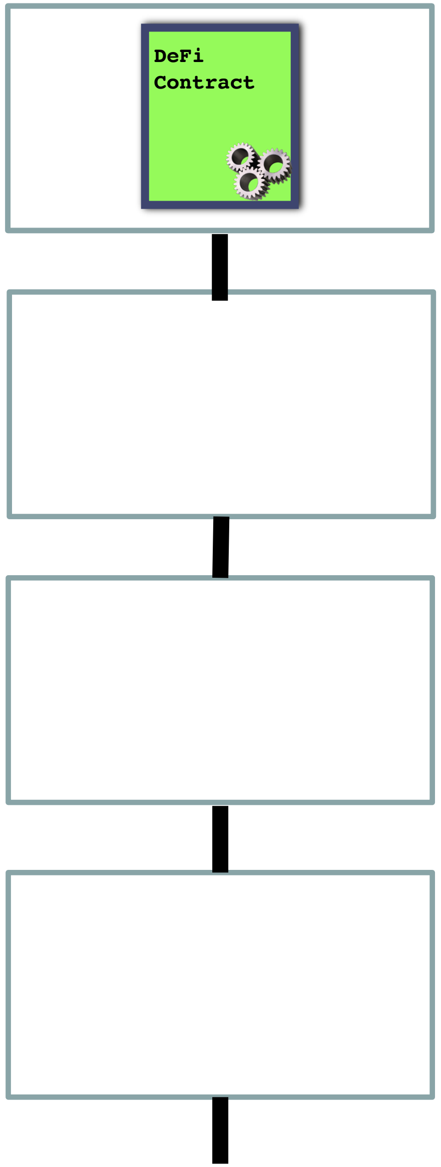
$2000

$2007

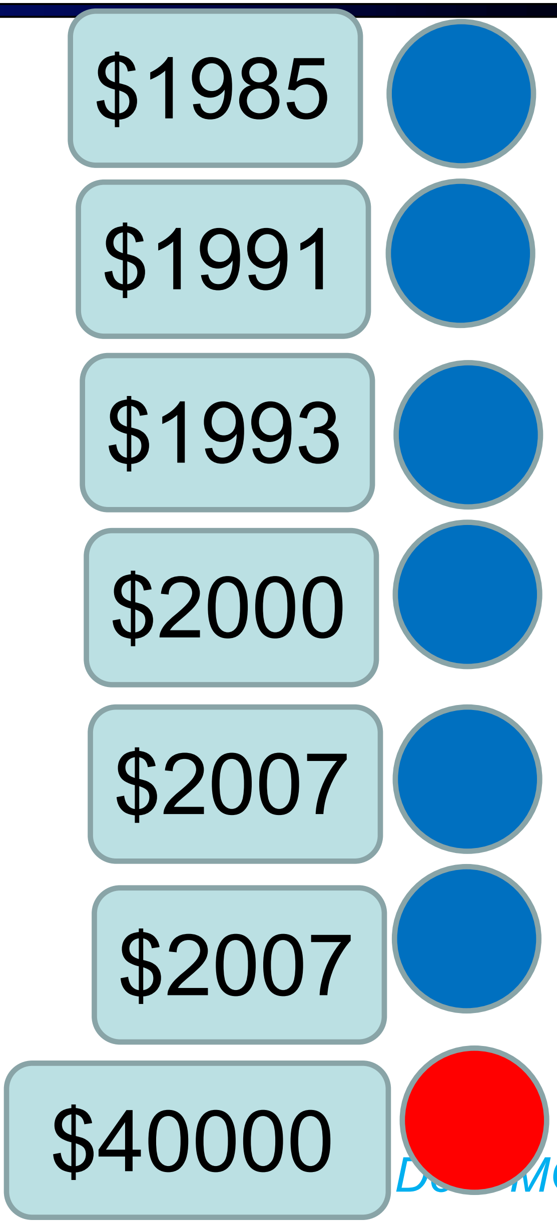
$2007

$40000

Combining reports



Mean = $7427



$1985

$1991

$1993

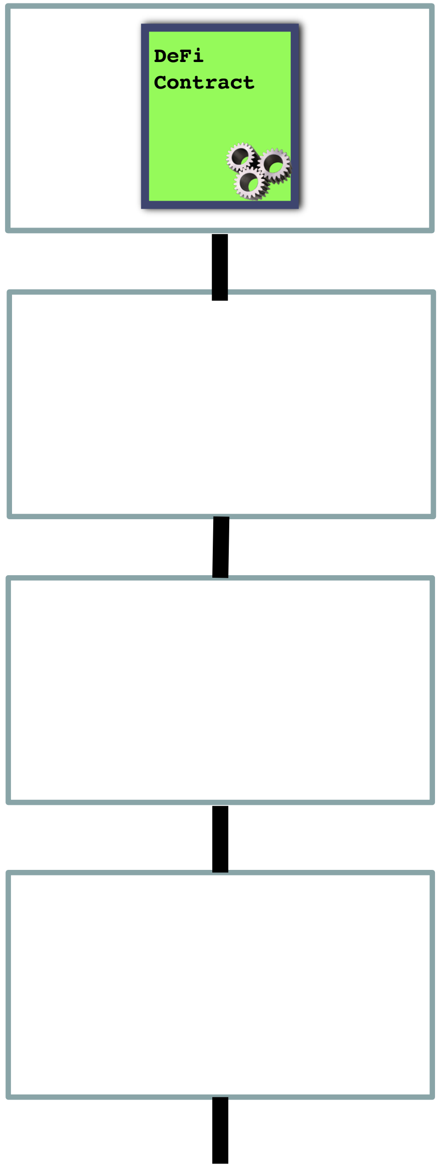
$2000

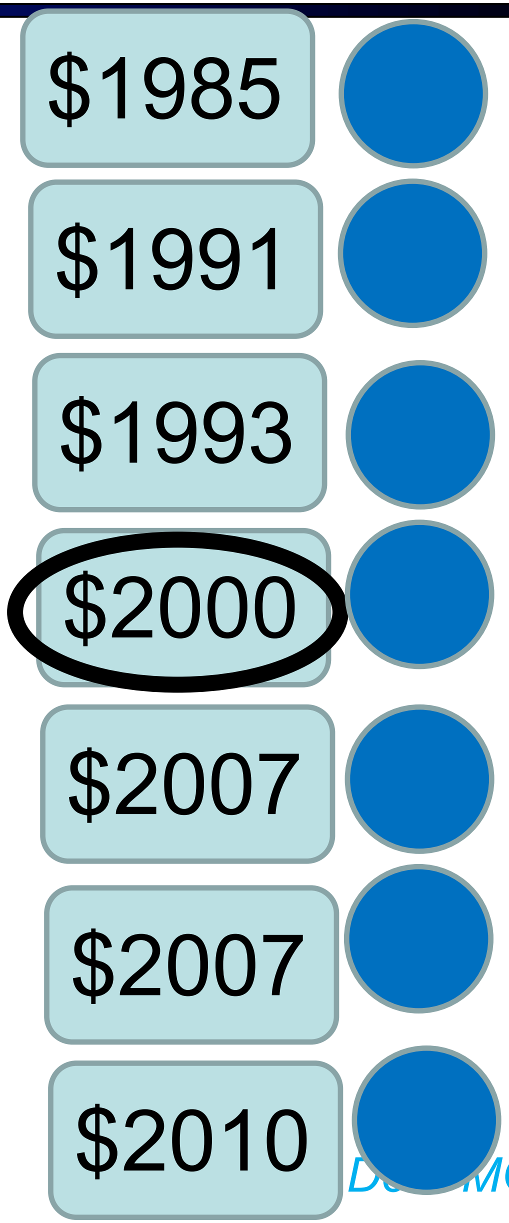
$2007

$2007

$40000

Combining reports

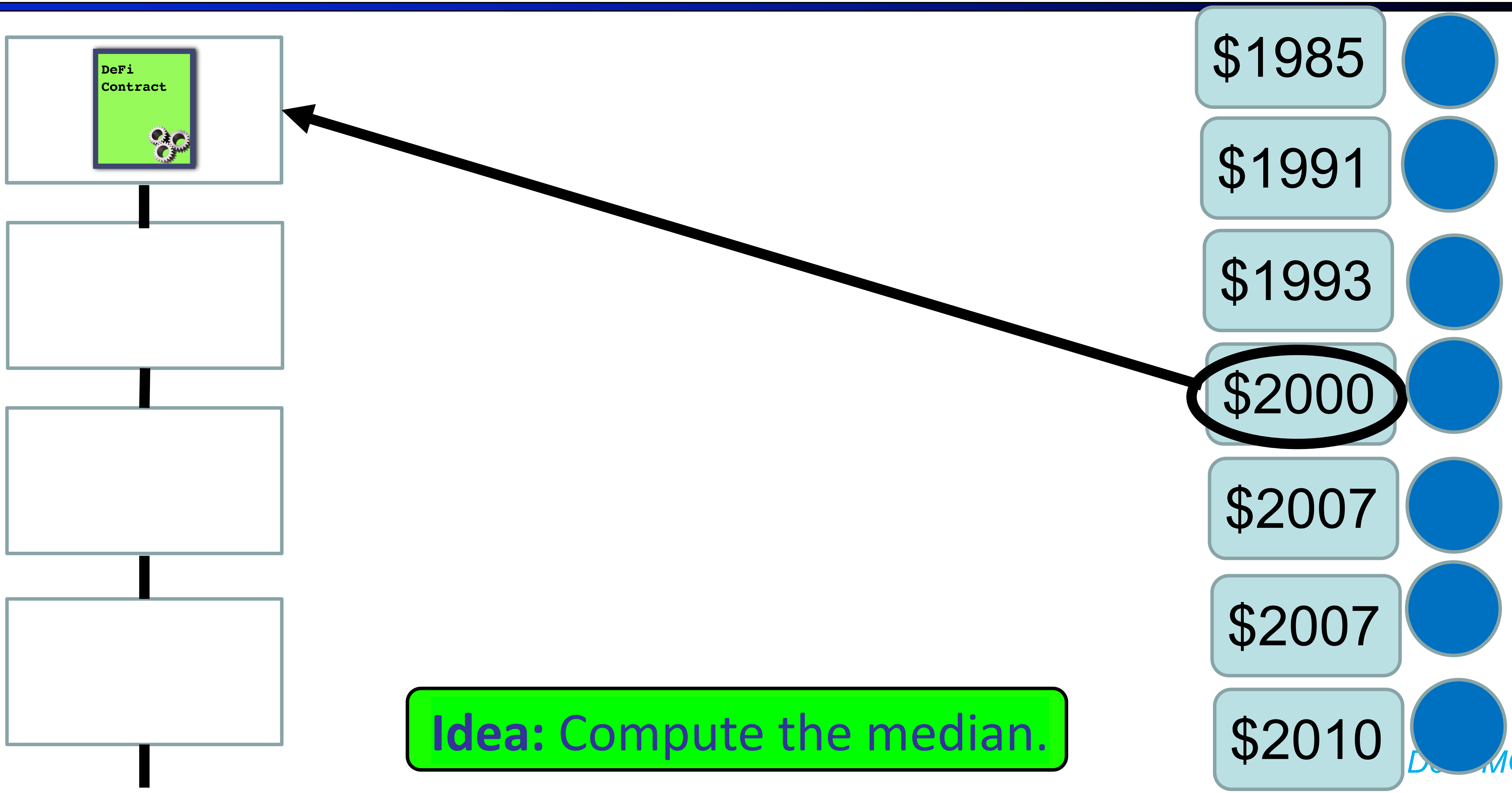




- $1985
- $1991
- $1993
- $2000
- $2007
- $2007
- $2010

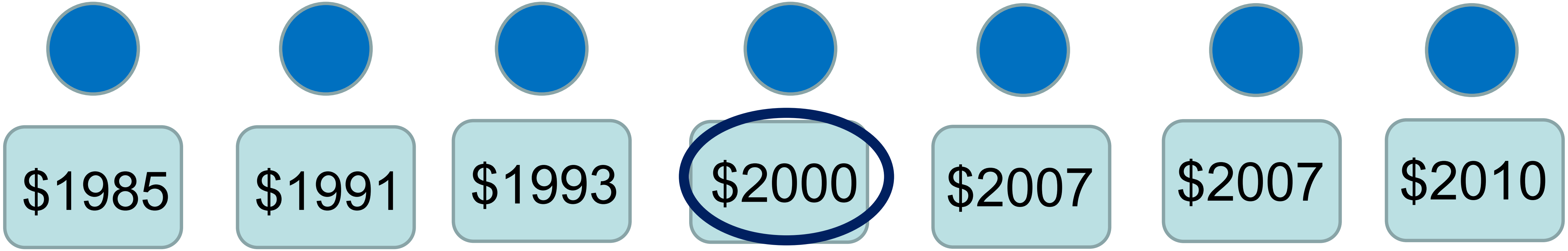
Idea: Compute the median.

Combining reports



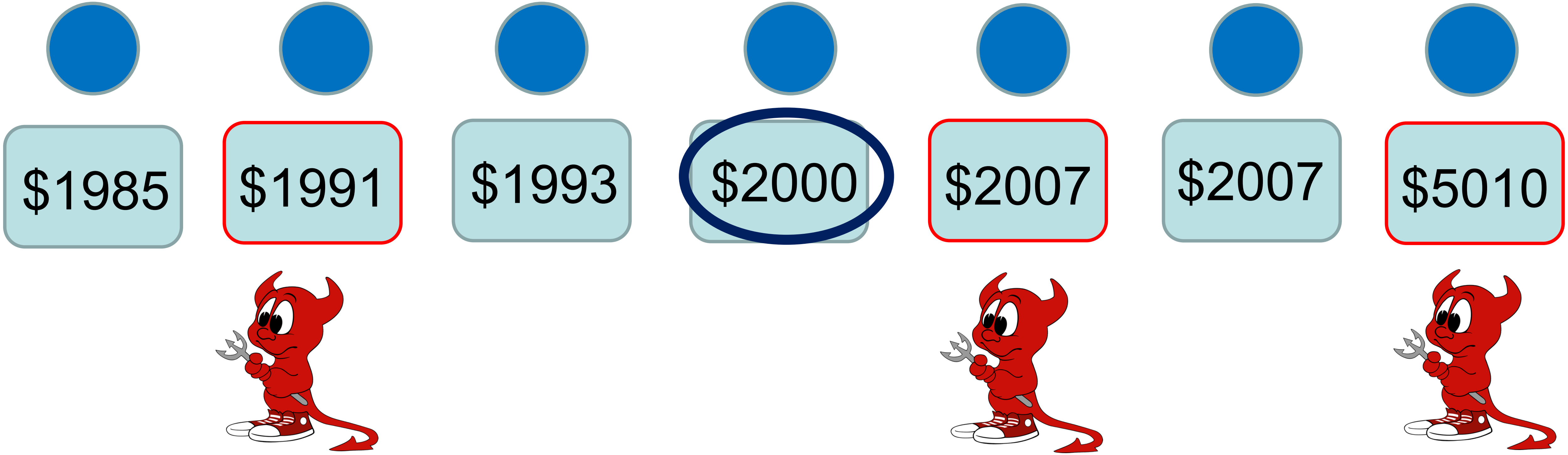
Idea: Compute the median.

The beauty of medianization



$1985 $1991 $1993 $2000 $2007 $2007 $2010

The beauty of medianization



$1985

$1991

$1993

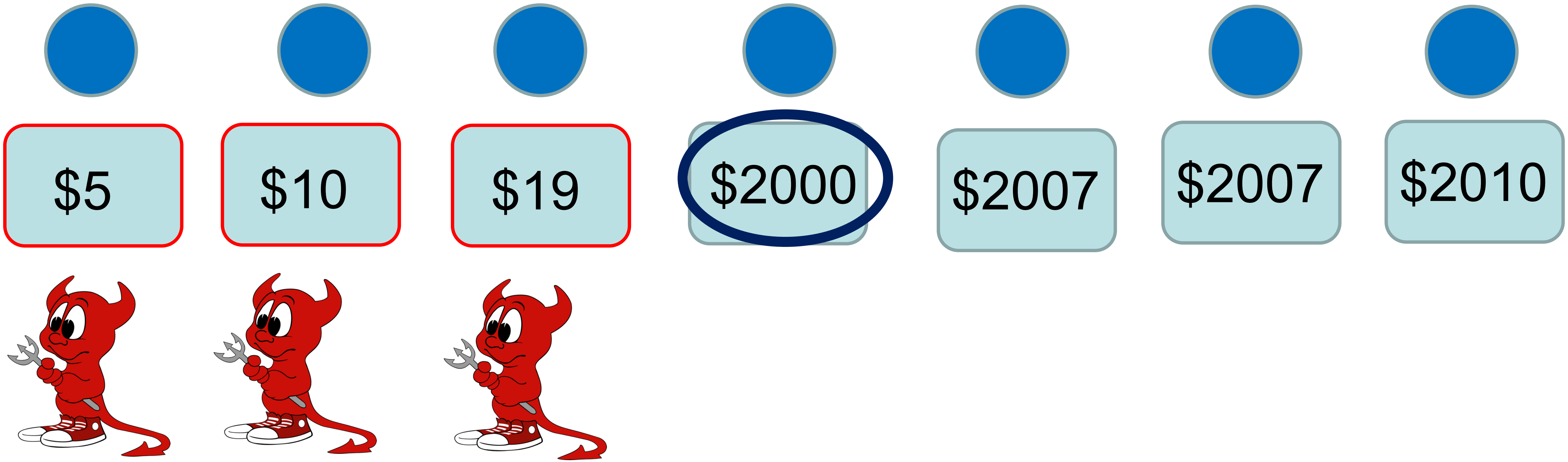
$2000

$2007

$2007

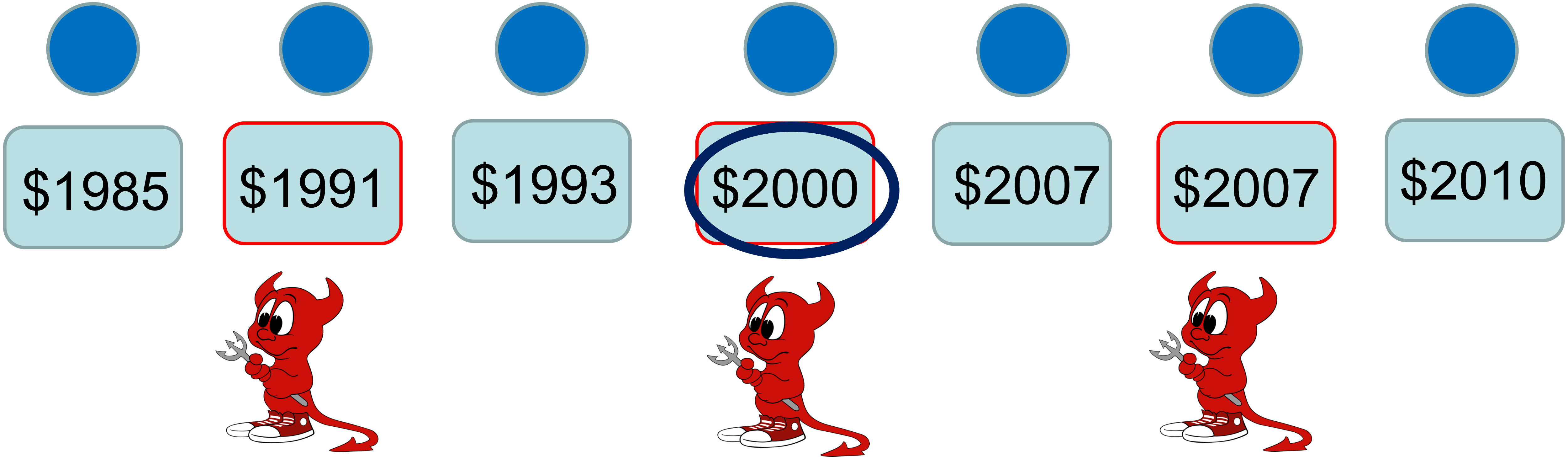
$5010

The beauty of medianization



$5 $10 $19 $2000 $2007 $2007 $2010

The beauty of medianization



$1985

$1991

$1993

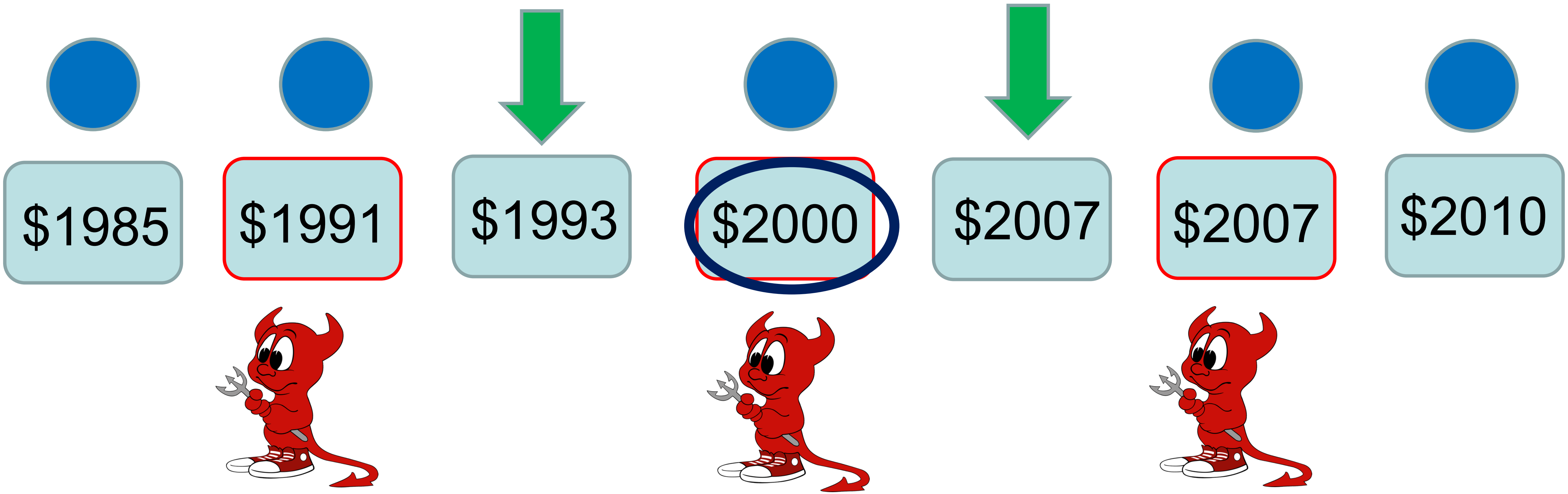
$2000

$2007

$2007

$2010

The beauty of medianization



$1985

$1991

$1993

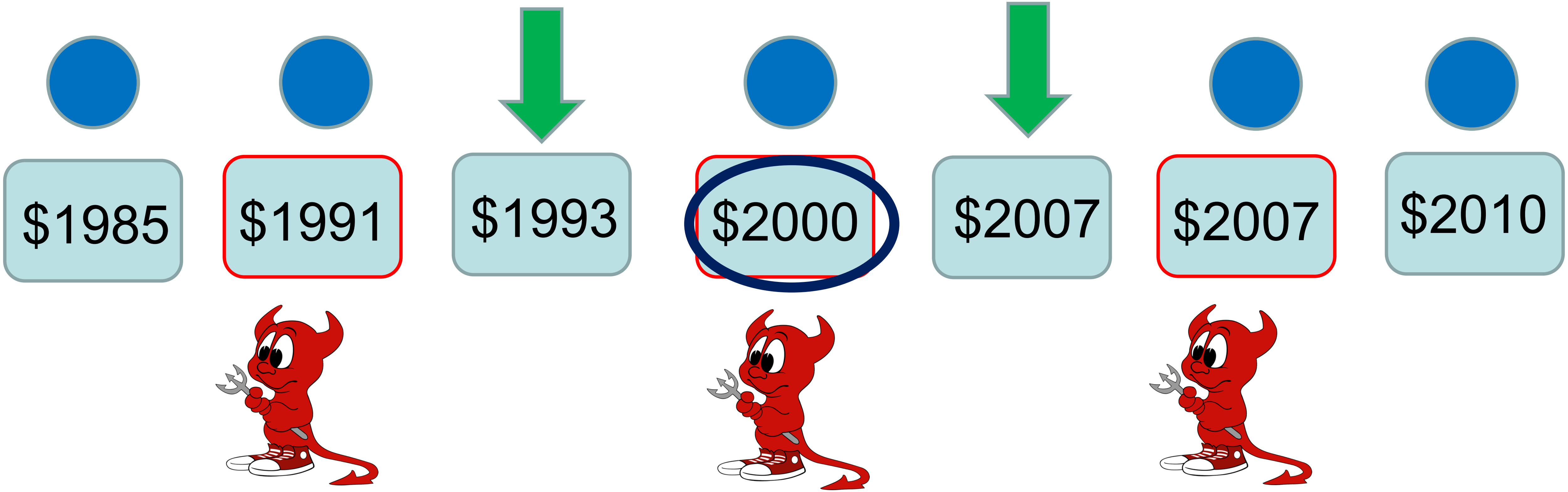
$2000

$2007

$2007

$2010

The beauty of medianization



Fact: Given a minority of bad values, median is an honest value or bounded by honest values.

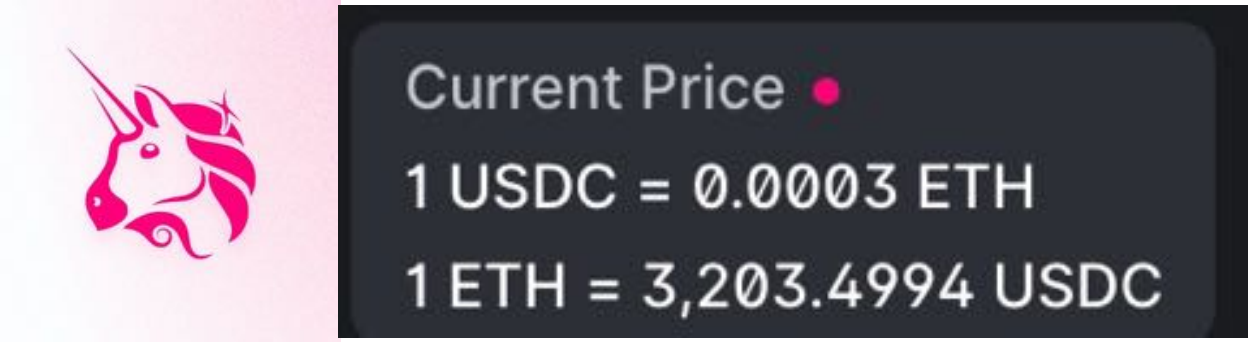
Other problems

- How do we ensure nodes get paid for service?
- How to ensure that oracle reports are mined in a timely way?
- How do we ensure that a majority of nodes are honest?

Advanced Oracle Use Cases

DEXes

- DEXes enable on-chain trading of various asset pairs.
- Side effect: *current valuation of asset price.*
- Mispricing reveals *arbitrage opportunity*.
  - E.g., ETH on Uniswap: $3000 (e.g., USDT), but $2900 on another exchange
- So we can use a DEX as a price oracle!



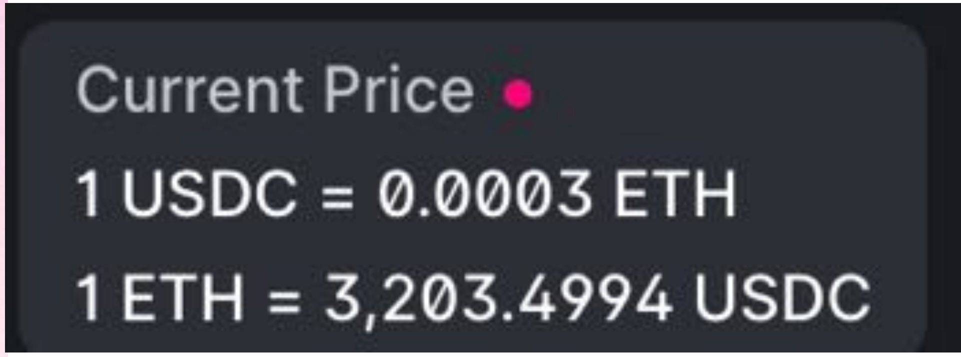
Current Price ●

1 USDC = 0.0003 ETH

1 ETH = 3,203.4994 USDC

Cryptoeconomic Oracles

- Pros:
  - Instant response
    - Composable with other contracts!
  - Economic assurance of correctness



Current Price ●

1 USDC = 0.0003 ETH

1 ETH = 3,203.4994 USDC

Cryptoeconomic Oracles

- Cons:
  - Only good for price information
  - Can be manipulated!

bZx price-oracle attack

- bZx used Kyber exchange as price oracle
  - ETH loans with sUSD collateral based on Kyber price
- Attacker:
  - Sold ETH for sUSD on Kyber to drive down ETH / sUSD price
  - Borrowed ETH cheaply on bZx
    - I.e., used little sUSD
  - Ran away with the loan…
  - Made almost $700k with one (multi-step) transaction!

bZx price-oracle attack

Attack steps:

- Borrow ETH from bZx via flash loan
- Buy some sUSD with ETH
- Drive down ETH-USD price on bZx
  - Manipulate bZx Kyber price oracles
- Borrow more dollars using ETH
- Borrow ETH (**cheaply**) on bZx using sUSD
- Pay back ETH flash loan on bZx

- Profit = 2381.41 ETH ($673+k!)

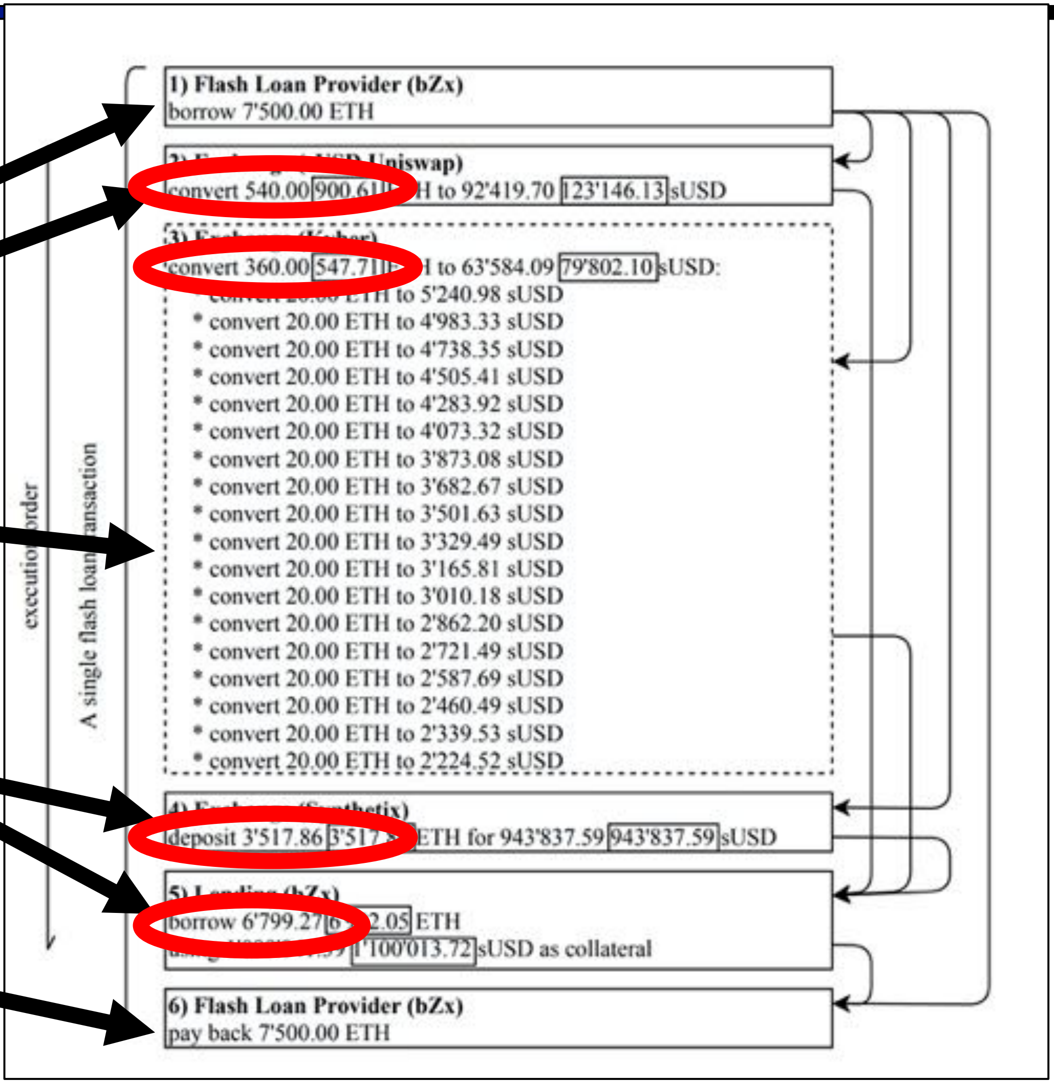
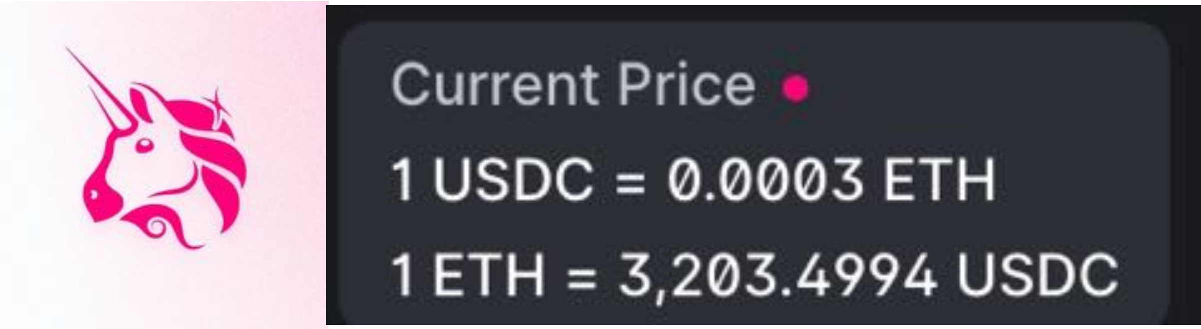

1) Flash Loan Provider (bZx)
borrow 7'500.00 ETH
niswap)
convert 540.00 900.61
H to 92'419.70 123'146.13 sUSD
3)
convert 360.00 547.71
I to 63'584.09 79'802.10 sUSD:
ETH to 5'240.98 sUSD
* convert 20.00 ETH to 4'983.33 sUSD
* convert 20.00 ETH to 4'738.35 sUSD
* convert 20.00 ETH to 4'505.41 sUSD
* convert 20.00 ETH to 4'283.92 sUSD
* convert 20.00 ETH to 4'073.32 sUSD
* convert 20.00 ETH to 3'873.08 sUSD
* convert 20.00 ETH to 3'682.67 sUSD
* convert 20.00 ETH to 3'501.63 sUSD
* convert 20.00 ETH to 3'329.49 sUSD
* convert 20.00 ETH to 3'165.81 sUSD
* convert 20.00 ETH to 3'010.18 sUSD
* convert 20.00 ETH to 2'862.20 sUSD
* convert 20.00 ETH to 2'721.49 sUSD
* convert 20.00 ETH to 2'587.69 sUSD
* convert 20.00 ETH to 2'460.49 sUSD
* convert 20.00 ETH to 2'339.53 sUSD
* convert 20.00 ETH to 2'224.52 sUSD
4)
deposit 3'517.86 3'517
ETH for 943'837.59 943'837.59 sUSD
5)
borrow 6'799.27 6
2.05 ETH
1'100'013.72 sUSD as collateral
6) Flash Loan Provider (bZx)
pay back 7'500.00 ETH
execution order
A single flash loan transaction

Figure from Qin et al. 2020

DeFi MOOC

Cryptoeconomic Oracles

- Countermeasure: Time-Weighted Average Price (TWAP)



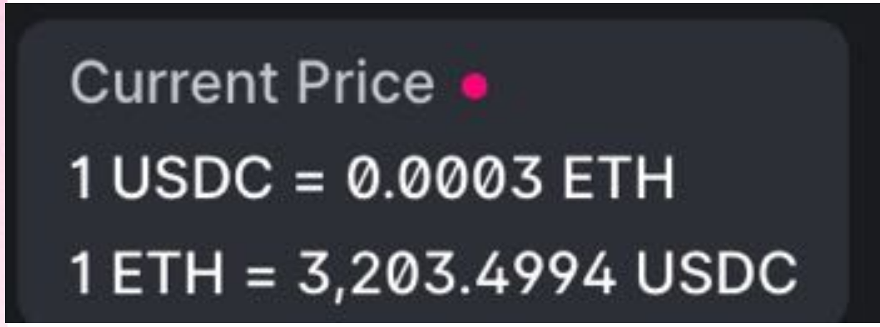
Current Price ●

1 USDC = 0.0003 ETH

1 ETH = 3,203.4994 USDC

Cryptoeconomic Oracles

- Cons:
  - Only good for price information
  - Can be manipulated
  - Countermeasure: Time-Weighted Average Price (TWAP)
    - Less accurate than current price!



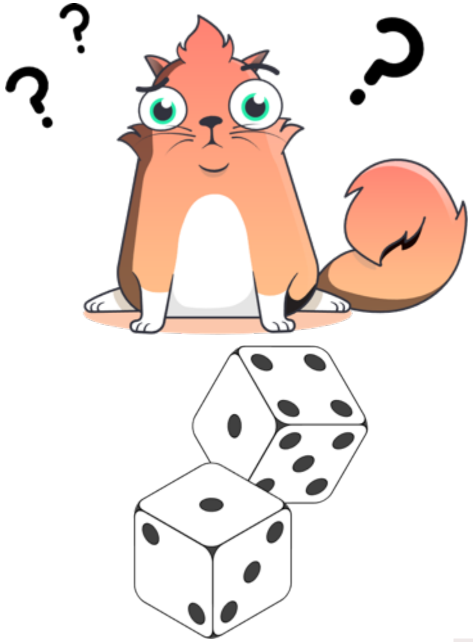
Current Price ●

1 USDC = 0.0003 ETH

1 ETH = 3,203.4994 USDC

NFT-based games

- How do NFT games work?
  - NFT = “Non-Fungible Token”
    - Token that is *unique* (ERC-721)
  - In NFT games, pieces / characters are NFTs
    - E.g., Axie Infinity, CryptoKitties
  - NFTs generated *randomly*
    - E.g., CryptoKitty breeding
- Where does the randomness come from?
  - Trustworthy randomness essential for *fairness*.



Fairness in ERC token markets: A Case Study of CryptoKitties

Kentaro Sako, Shin'ichiro Matsuo, and Sachin Meier

No Institute Given

Abstract. Fairness is an important trait of open, free markets. Ethereum is a platform meant to enable digital, decentralized markets. Though many researchers debate the market's fairness, there are few discussions around the fairness of automated markets, such as those hosted on Ethereum. In this paper, using pilot studies, we consider unfair factors caused by adding the program. Because CryptoKitties is one of the major blockchain-based games and has been in operation for an extended period of time, we focus on its market to examine fairness. As a result, we concluded that a gene determination algorithm in this game has little randomness, and a significant advantage to gain profit is given to players who know its bias over those who do not. We state incompleteness and impact of the algorithm and other factors. Besides, we suppose countermeasures to reduce CryptoKitties' unfairness as a market.

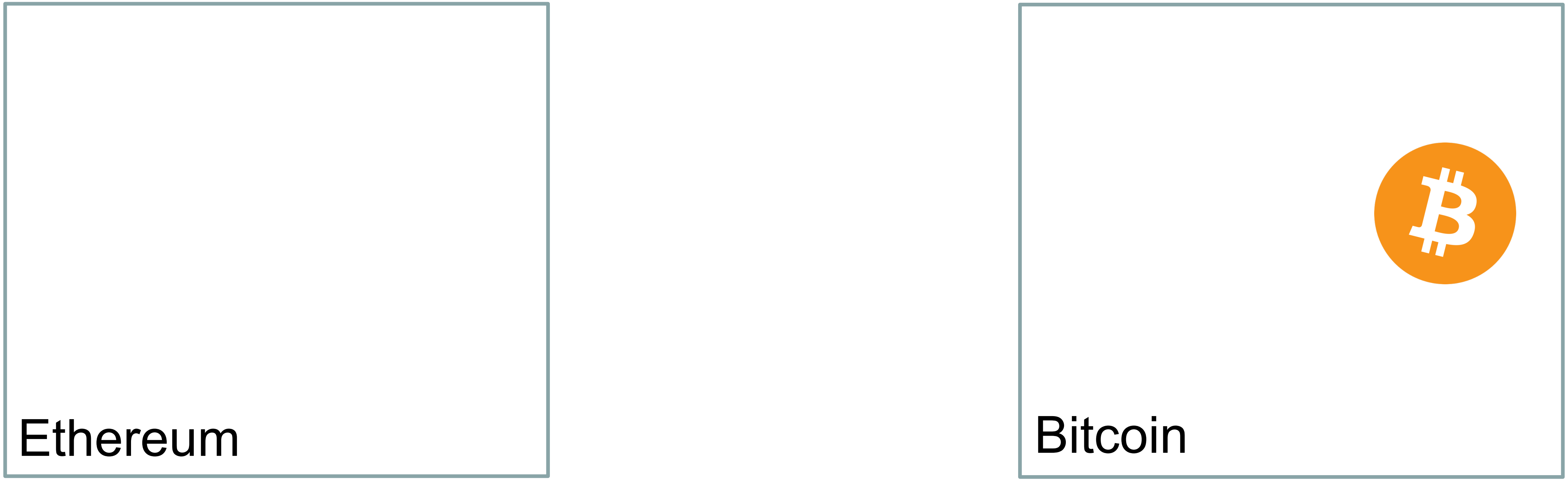
Keywords: CryptoKitties · Smart contracts · Financial market fairness.

Verifiable Random Functions (VRFs)

- Idea: Oracle uses secret key to generate randomness
  - Actually *pseudorandom,* not *random*
- Correctness of randomness is *verifiable*
  - Again, like digital signature
- Best of both worlds
  - Unpredictability -> fairness
  - Verifiability -> no cheating by oracle

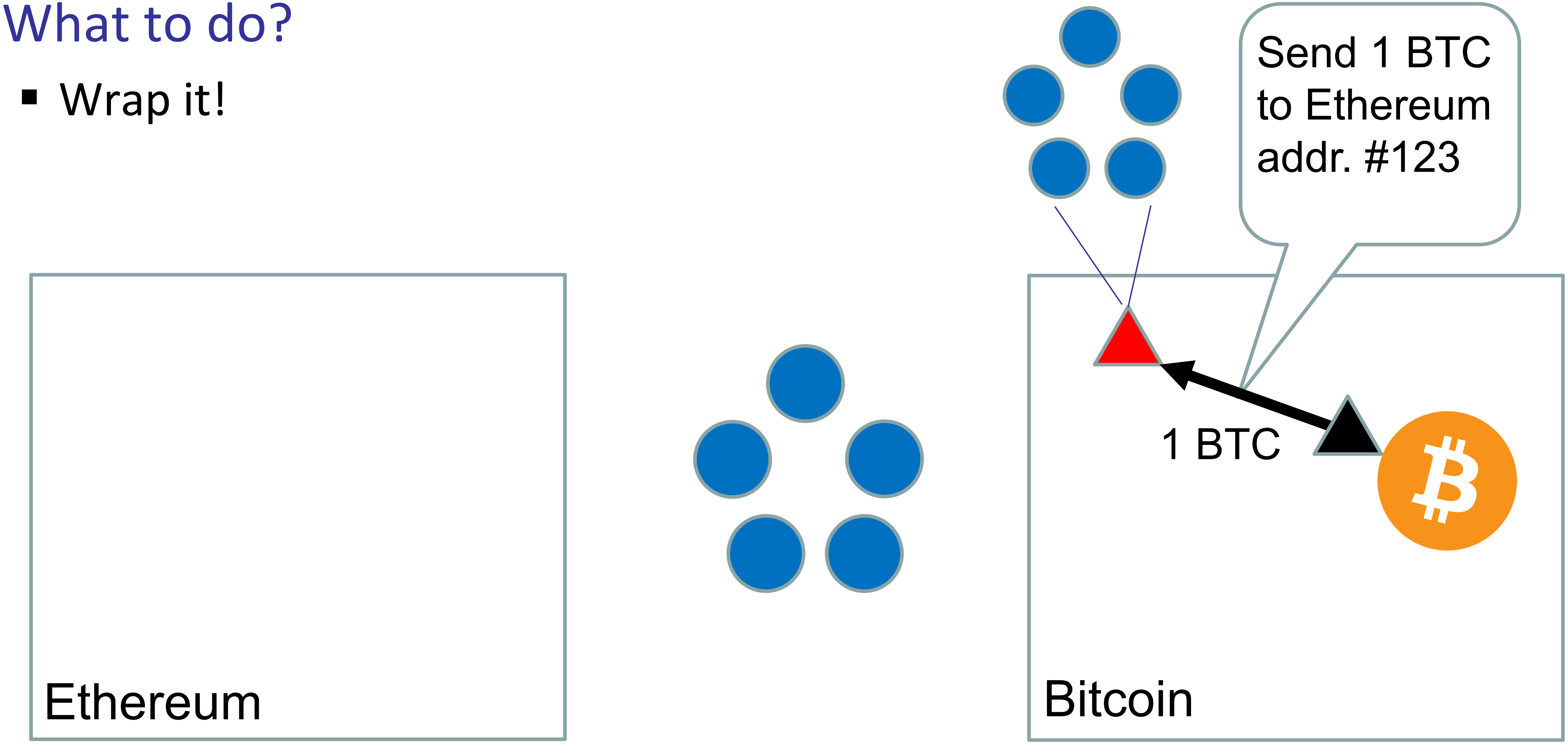
Wrapped currency

- Suppose you have a Bitcoin you want to use in Ethereum.



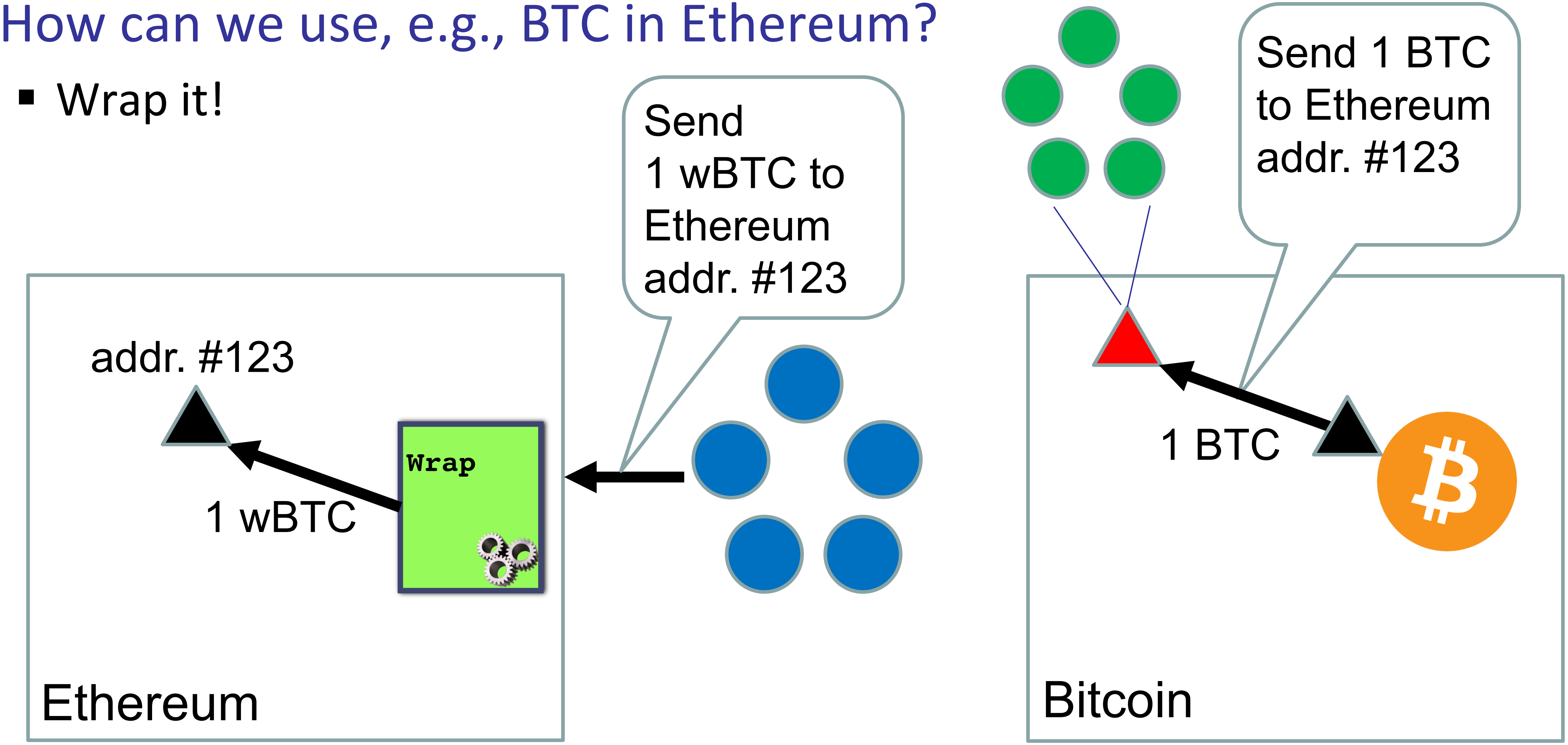
Wrapped currency

- What to do?
  - Wrap it!



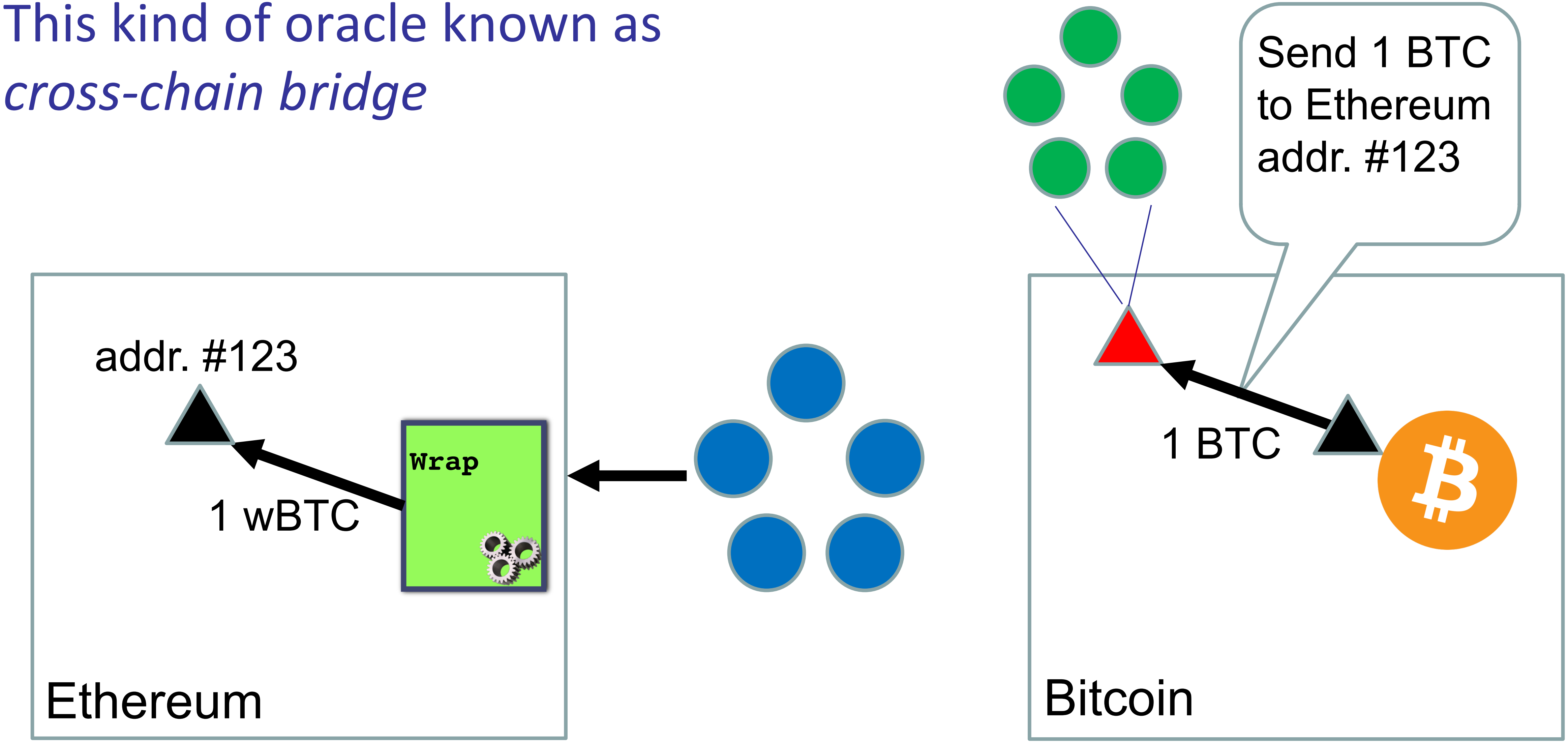
Wrapped currency

- How can we use, e.g., BTC in Ethereum?
  - Wrap it!


Send 1 BTC to Ethereum addr. #123
Send 1 wBTC to Ethereum addr. #123
addr. #123
1 wBTC
Wrap
1 BTC
Ethereum
Bitcoin

Wrapped currency

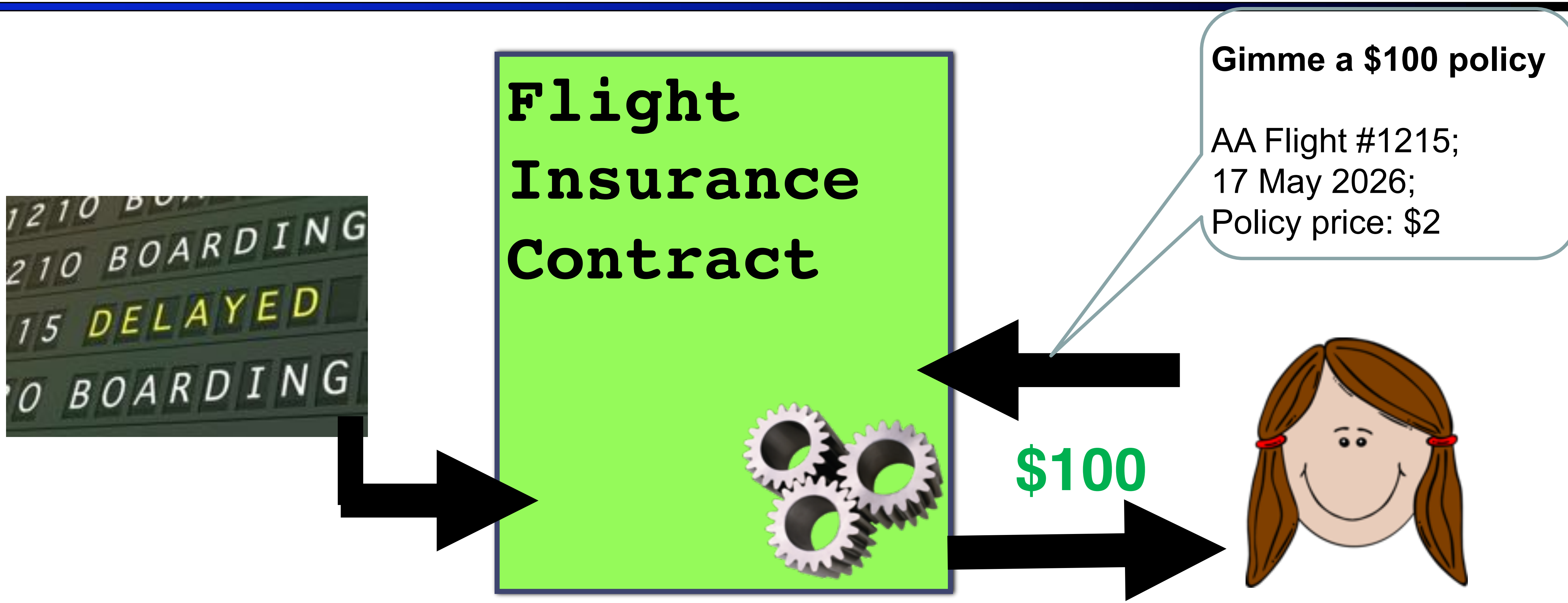
- This kind of oracle known as *cross-chain bridge*



Oracle Privacy

https://defi-learning.org

Parametric flight insurance



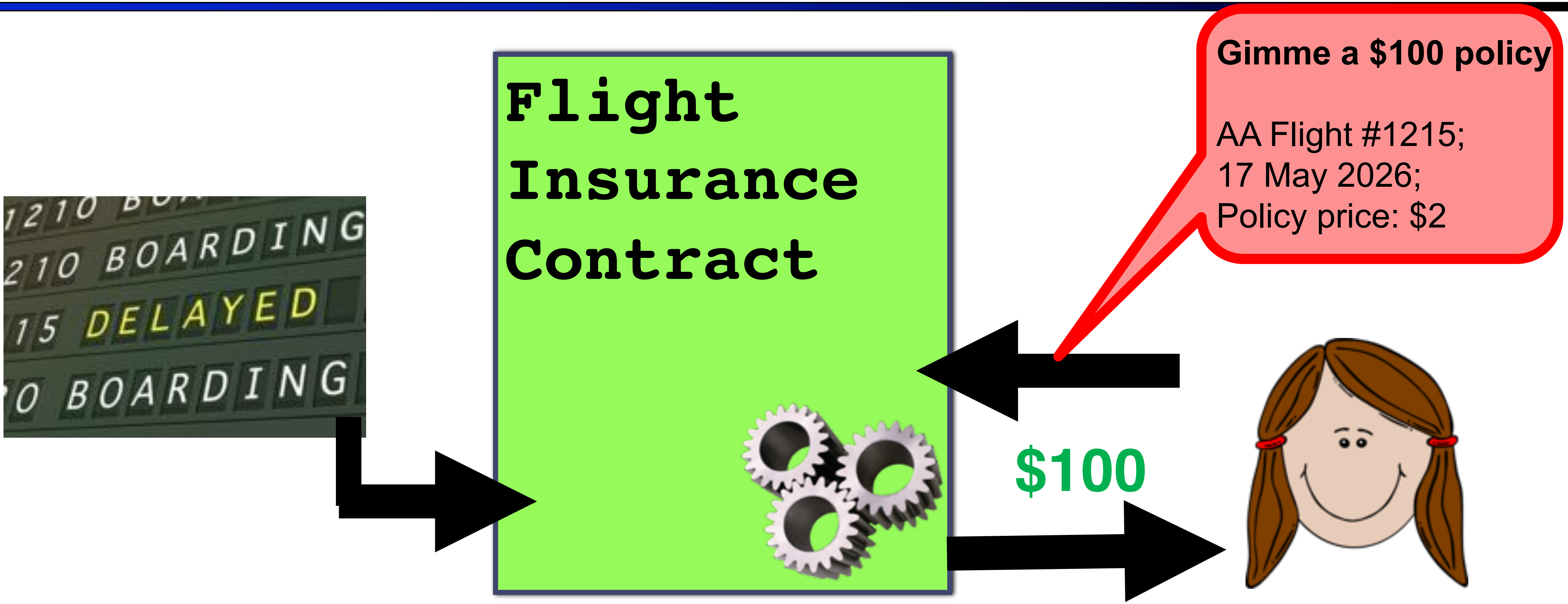
Flight Insurance Contract

Gimme a $100 policy

AA Flight #1215;
17 May 2026;
Policy price: $2

$100

Parametric flight insurance



Flight Insurance Contract

Gimme a $100 policy

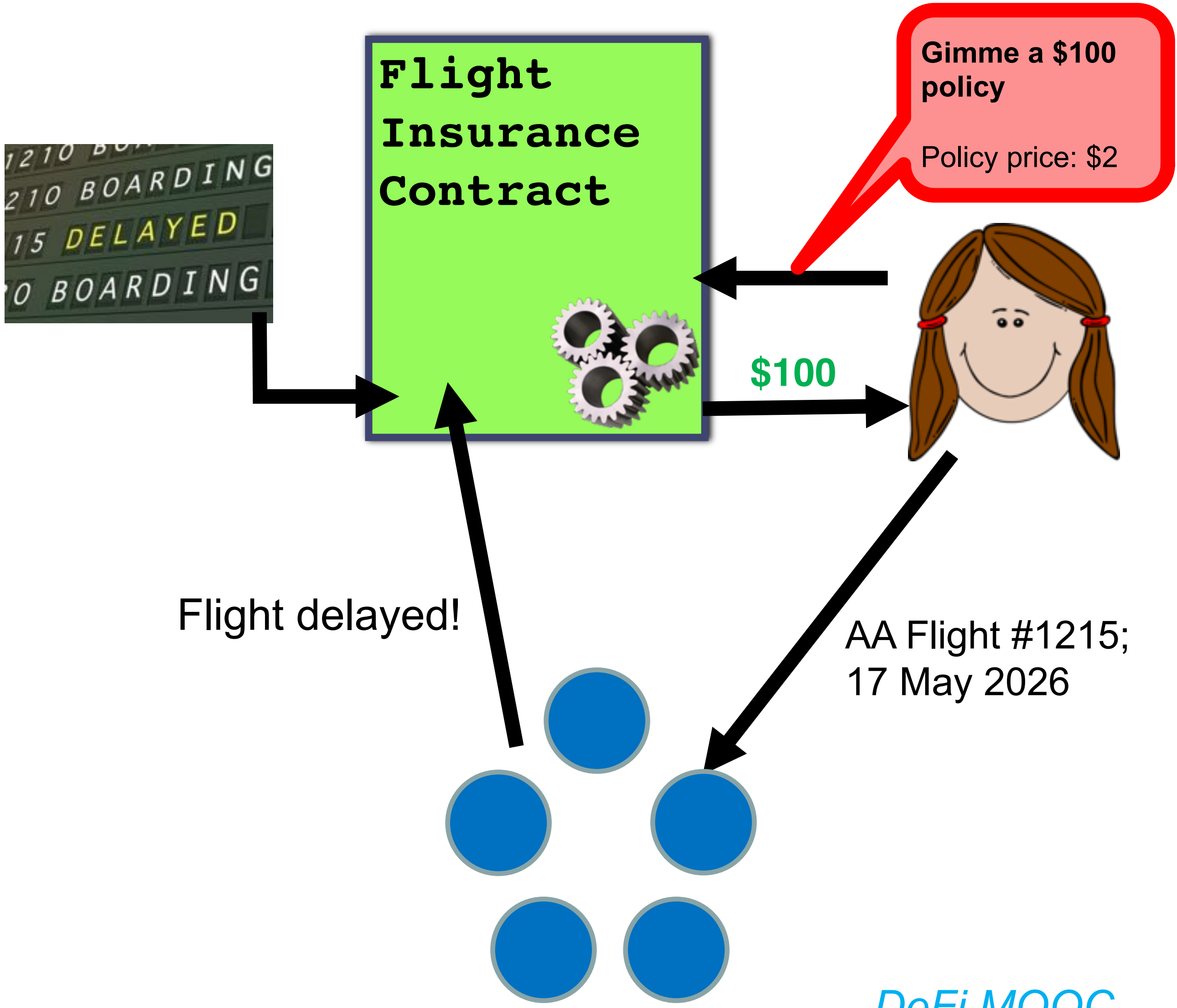
AA Flight #1215;
17 May 2026;
Policy price: $2

$100

Problem: Alice has published her itinerary on the blockchain!

A partial solution

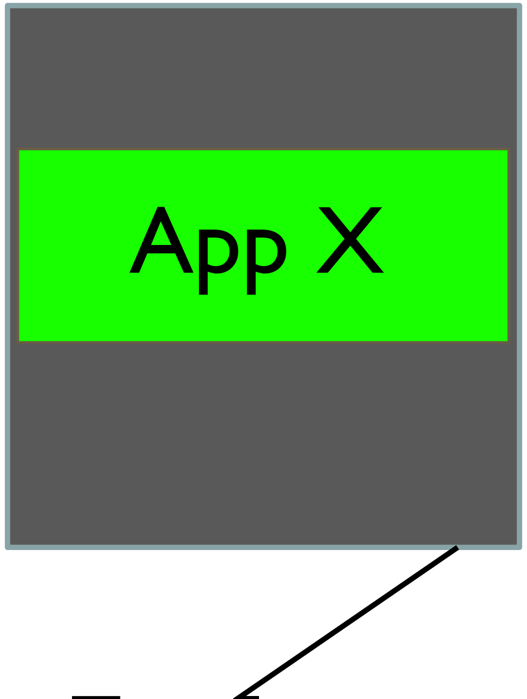
- Flight data not revealed on chain!
- But data revealed to oracle…



Trusted execution environments (TEEs)

Integrity

Even owner of computer with TEE can’t tamper with execution of X. *



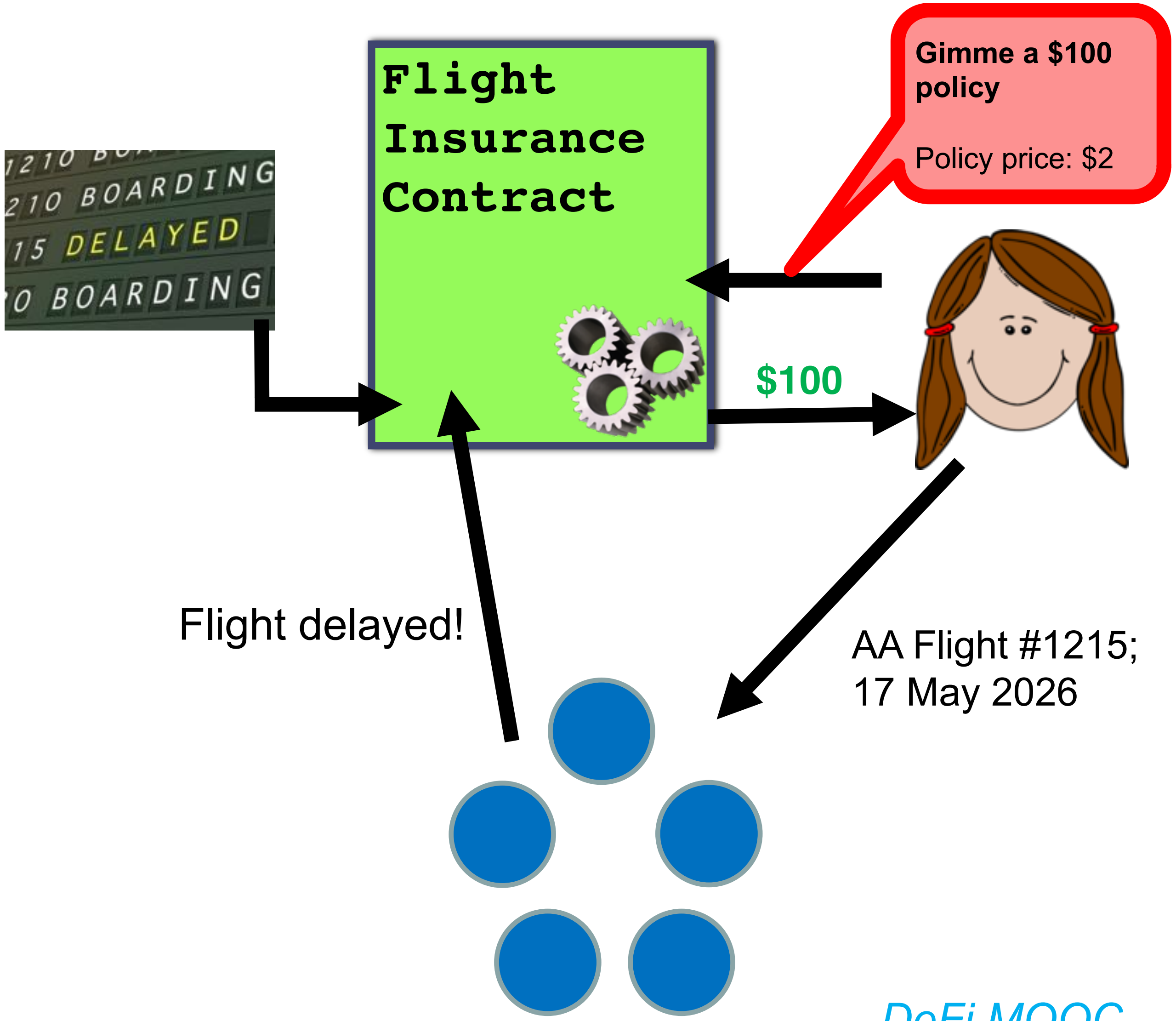
Enclave

Confidentiality

Even owner of computer with TEE can’t learn data used by X. *

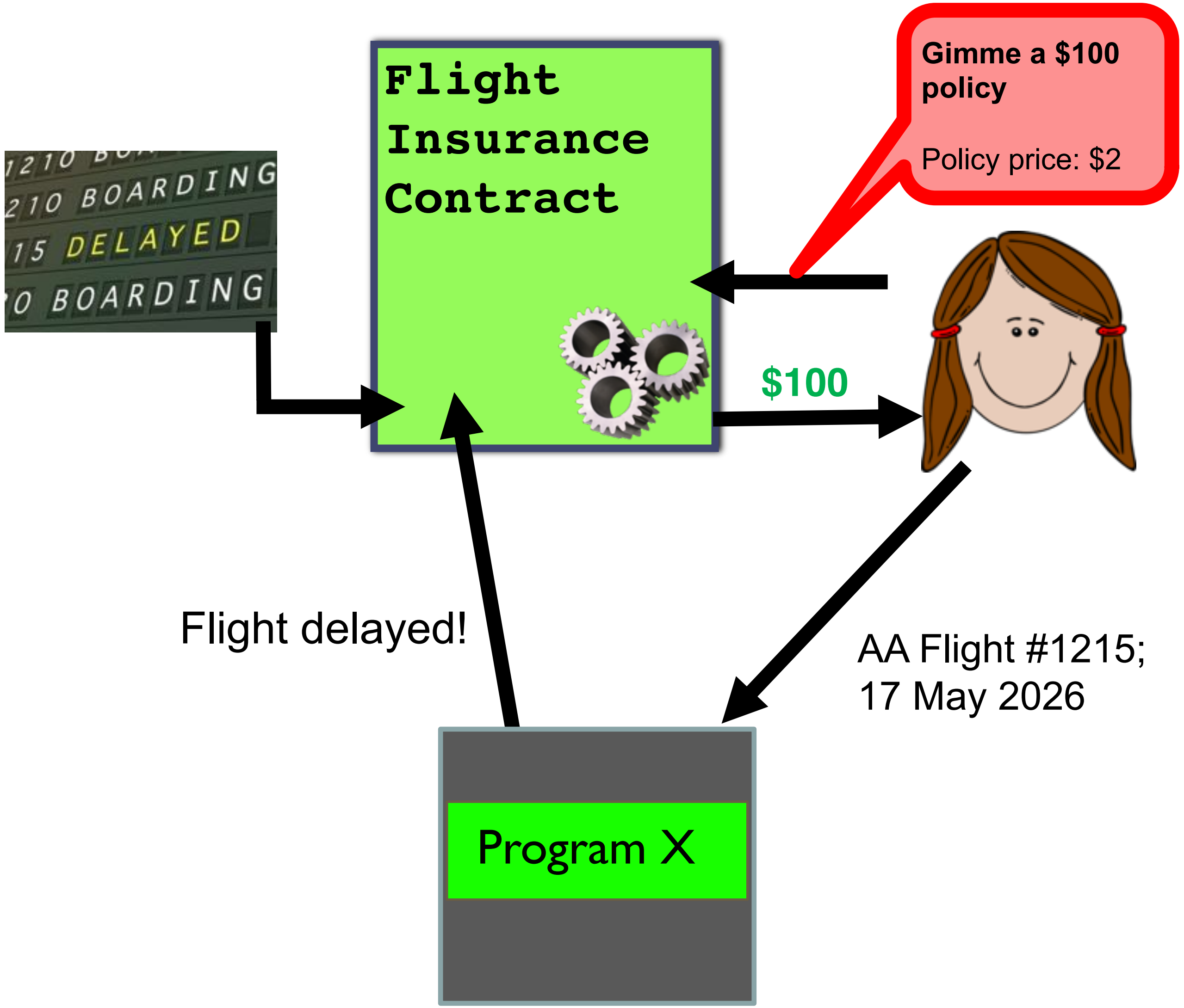
* *There are important provisos here*

Strong privacy



Strong privacy

- Now, we can use a TEE instead of ordinary nodes.
- Town Crier
  - Zhang et al. 2016



Another application: Sale of online goods

- Suppose Alice wants to sell Bob a Steam game for ETH…

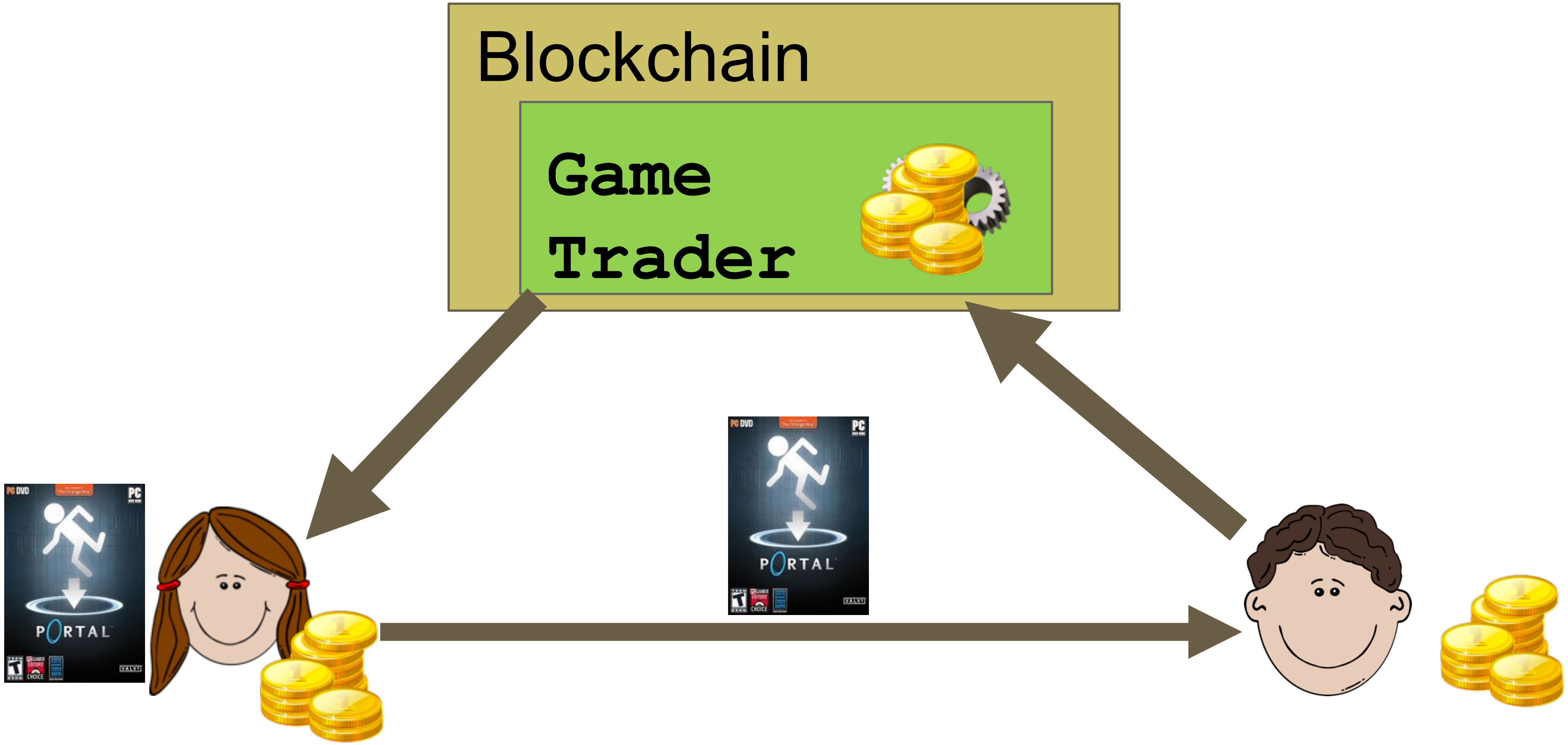
PORTAL
ETHE
ACCEPTED HE
STEAM

Online game license

Ether

Steam Community Marketplace

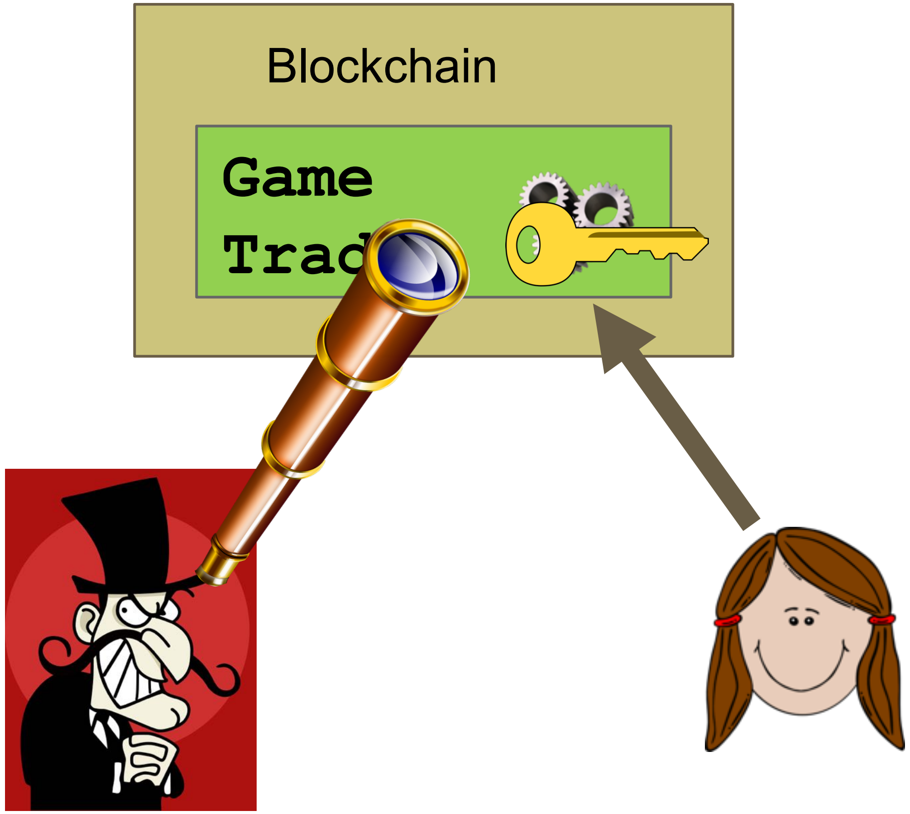
Smart contract for fair exchange



Blockchain

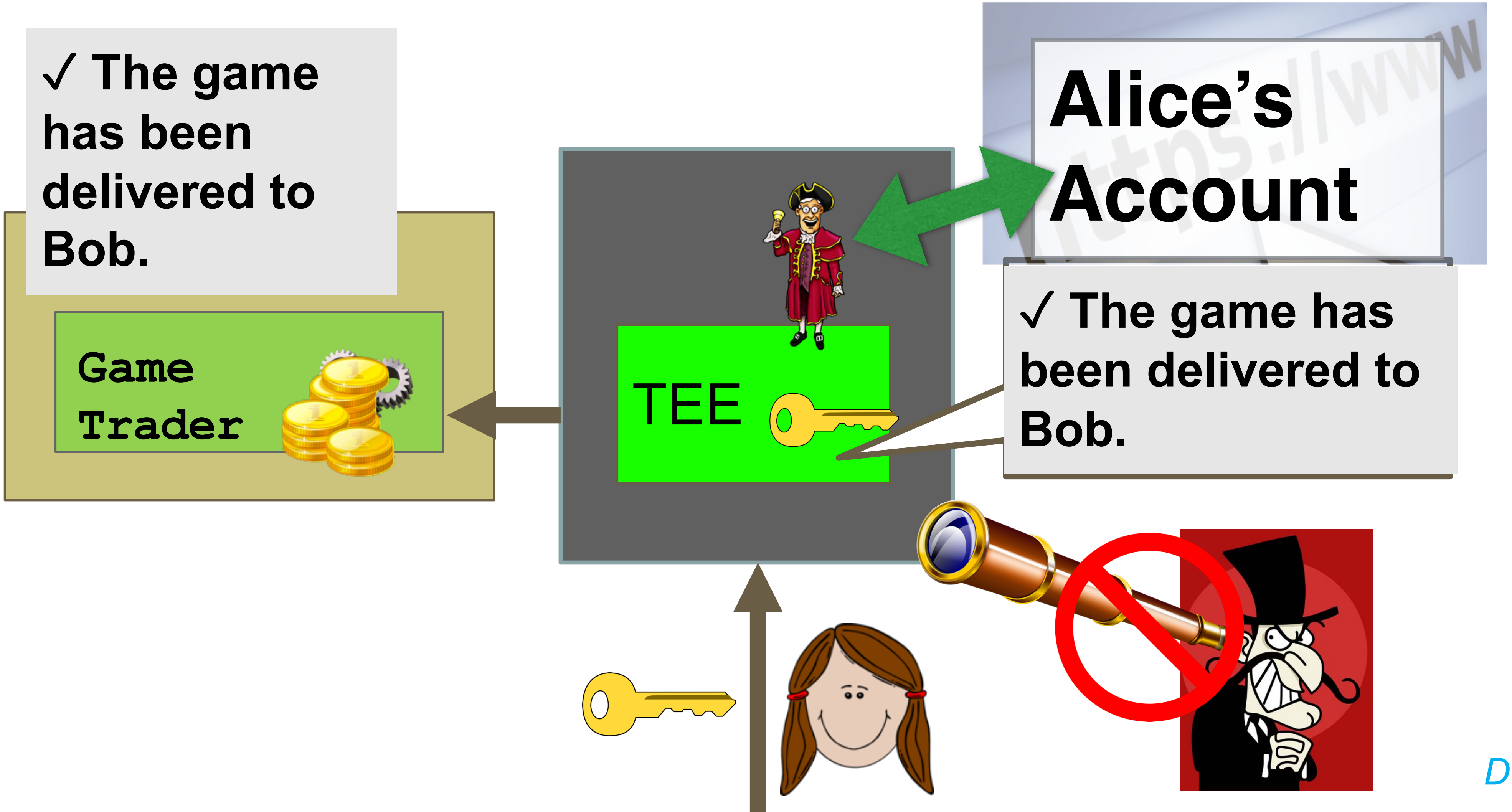
Game Trader

There’s just one problem…



- `GameTrader` needs to verify delivery
- Requires Alice's (or Bob's) Steam marketplace credentials
- But there are no secrets on blockchains!

Again, we can leverage enclave confidentiality…



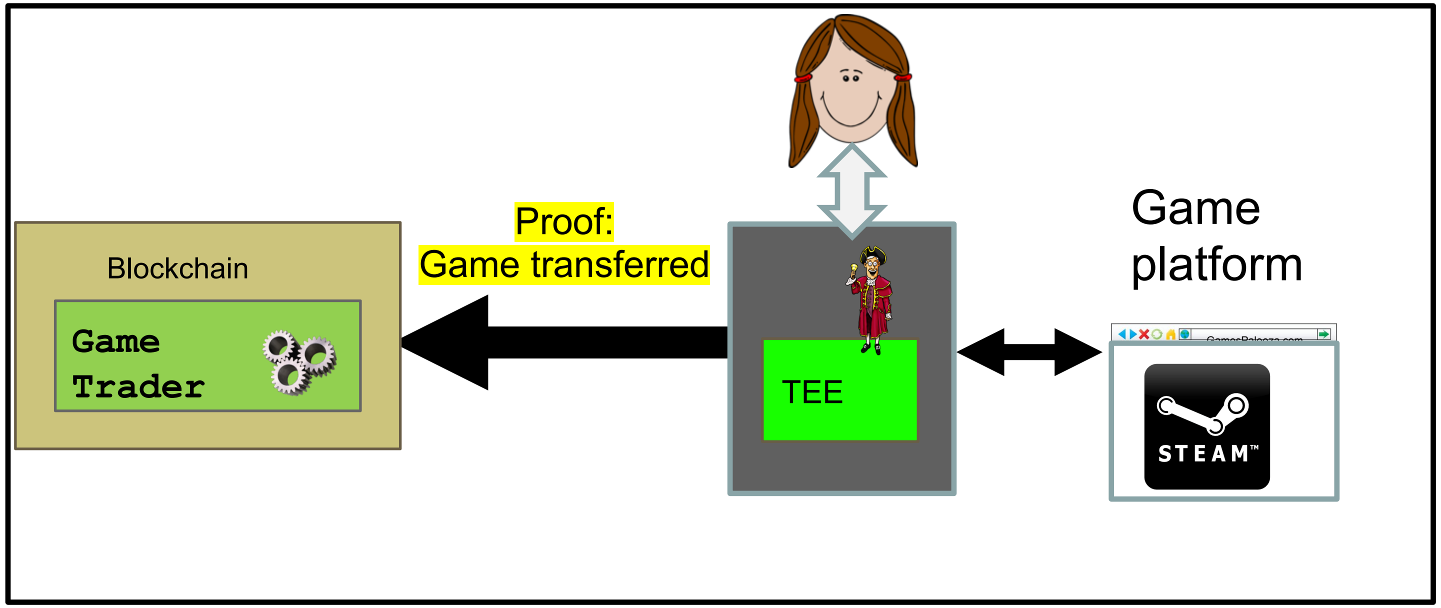
✓ The game has been delivered to Bob.

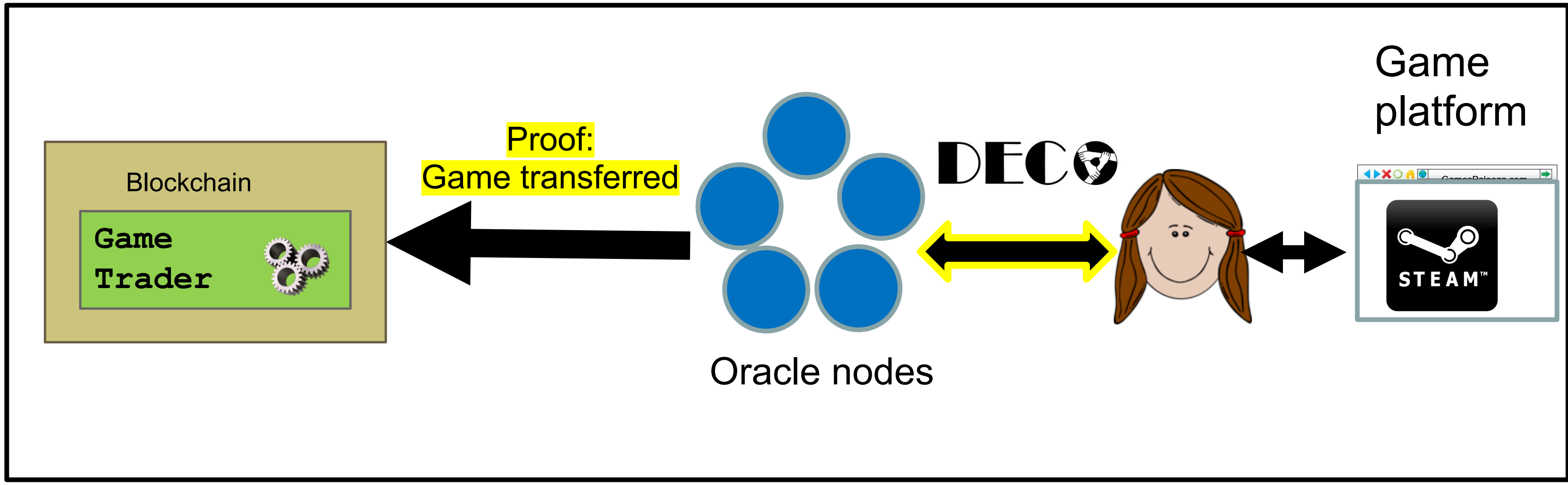
✓ The game has been delivered to Bob.

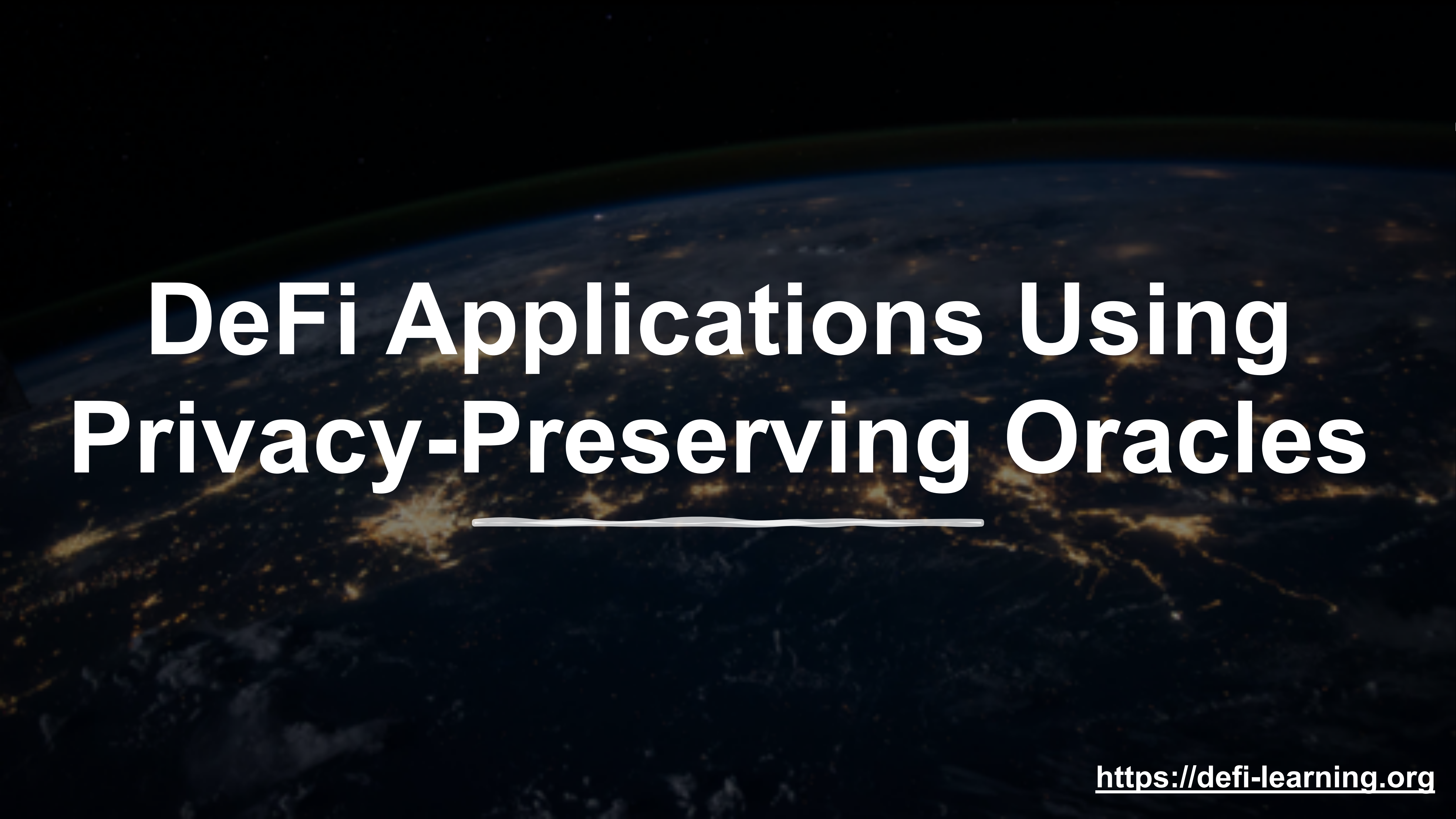
DECO

- Main hardware-based TEE has had serious vulnerabilities
  - Intel SGX
- DECO: alternative to Town Crier using *cryptographic techniques*
- DECO enables a user to prove facts about a web session (TLS sessions) *to oracle nodes*

TEE vs. DECO


Blockchain
Game Trader
Proof:
Game transferred
TEE
Game platform
STEAM™


Blockchain
Game Trader
Proof:
Game transferred
DECO
Game platform
STEAM™
Oracle nodes



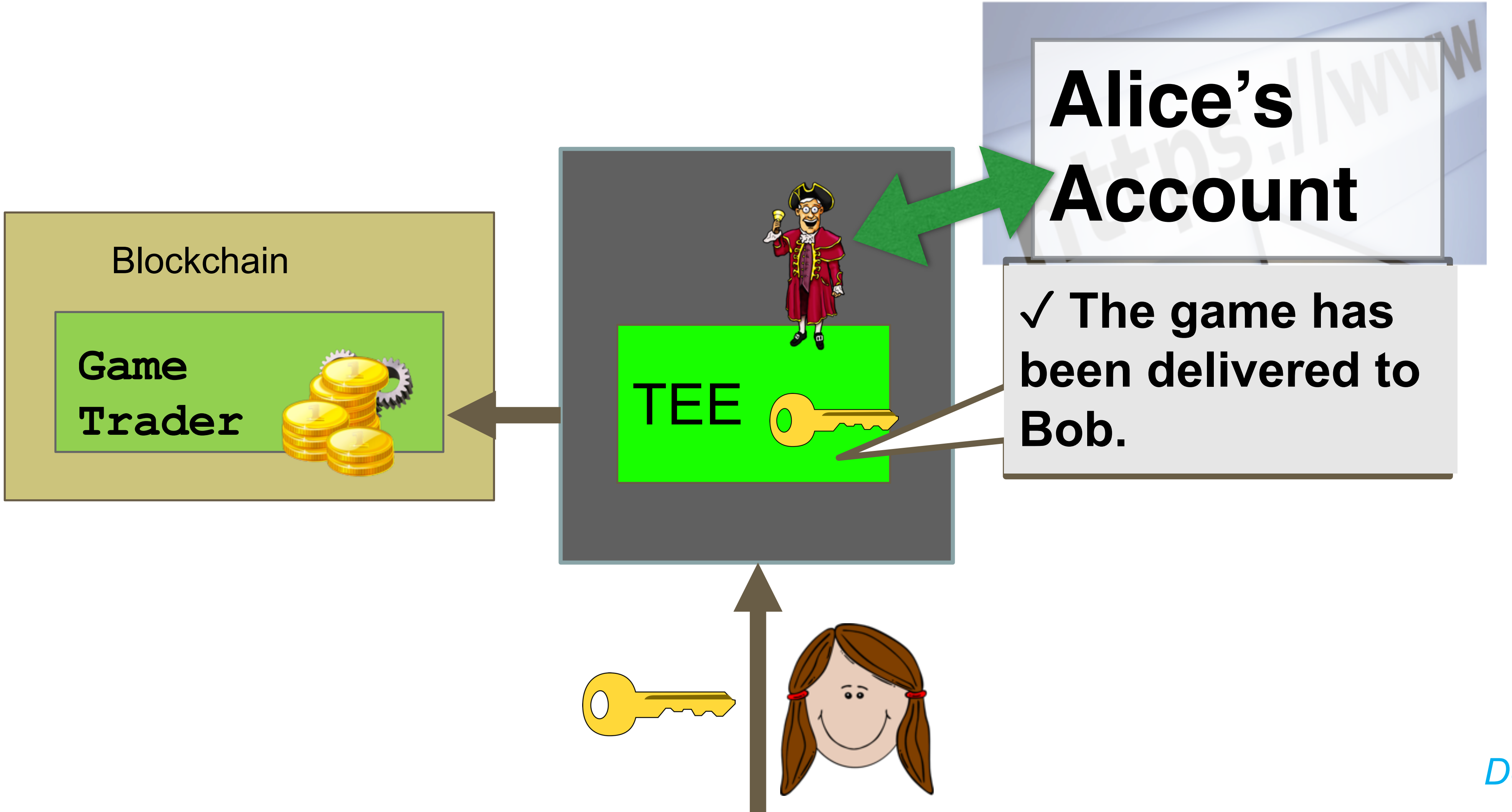
DeFi Applications Using Privacy-Preserving Oracles

https://defi-learning.org

Example DeFi applications

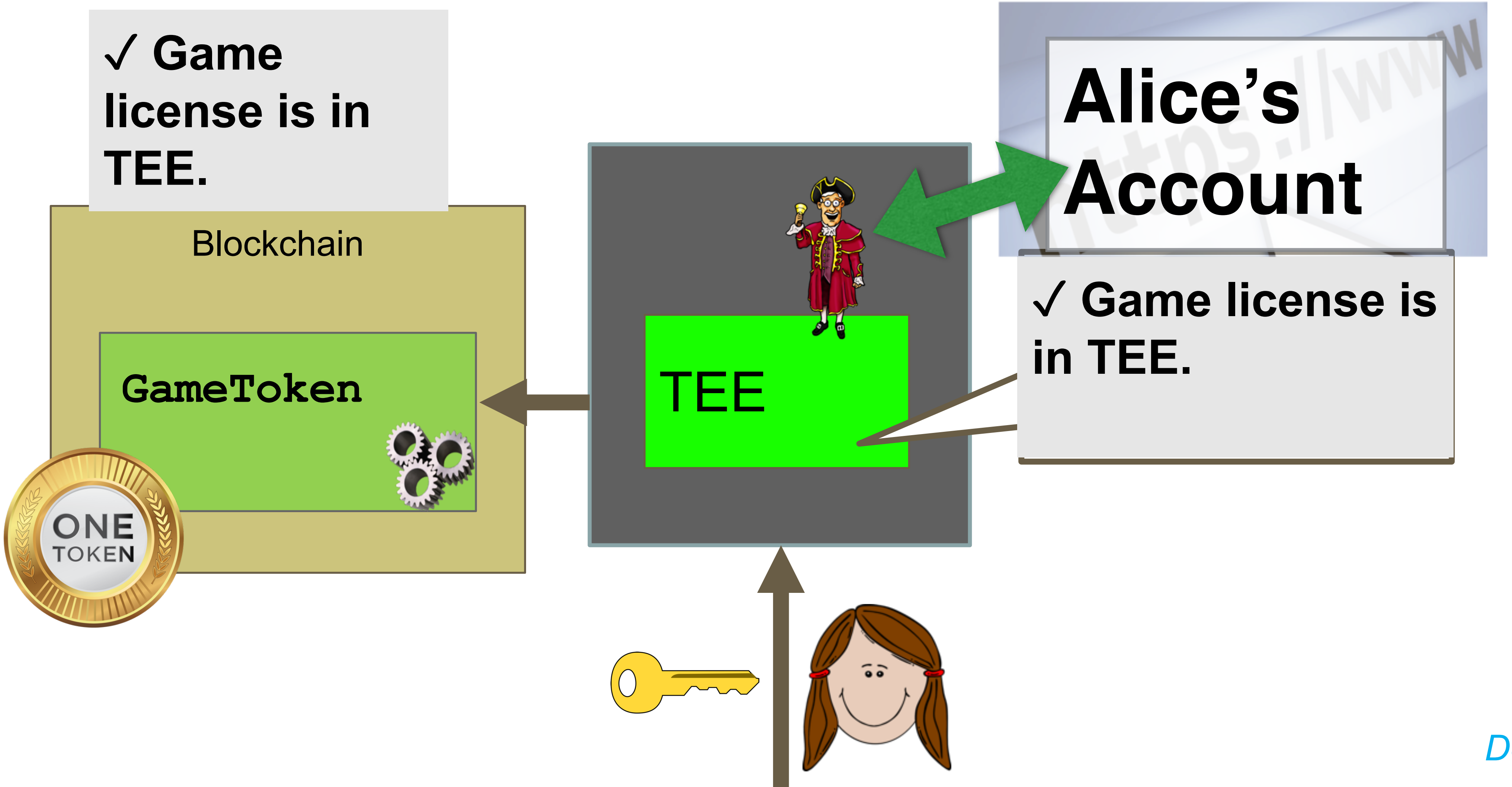
- Application 1: Tokenizing digital assets
- Application 2: Private DeFi
- Application 3: Decentralized identity

Recall



✓ The game has been delivered to Bob.

Let’s tokenize it!



√ Game license is in TEE.

√ Game license is in TEE.

What’s an NFT?

- **NFT** = **N**on-**F**ungible **T**oken
- Fungible tokens
  - Every token is *identical*
  - Like currency, e.g., stablecoins
  - Examples: MKR, Uniswap tokens, etc., etc.

What’s an NFT?

- **NFT** = **N**on-**F**ungible **T**oken
- NFTs
  - Every token is *unique*
  - Fractionalization not straightforward
  - Popular for artworks, games
  - E.g., real estate

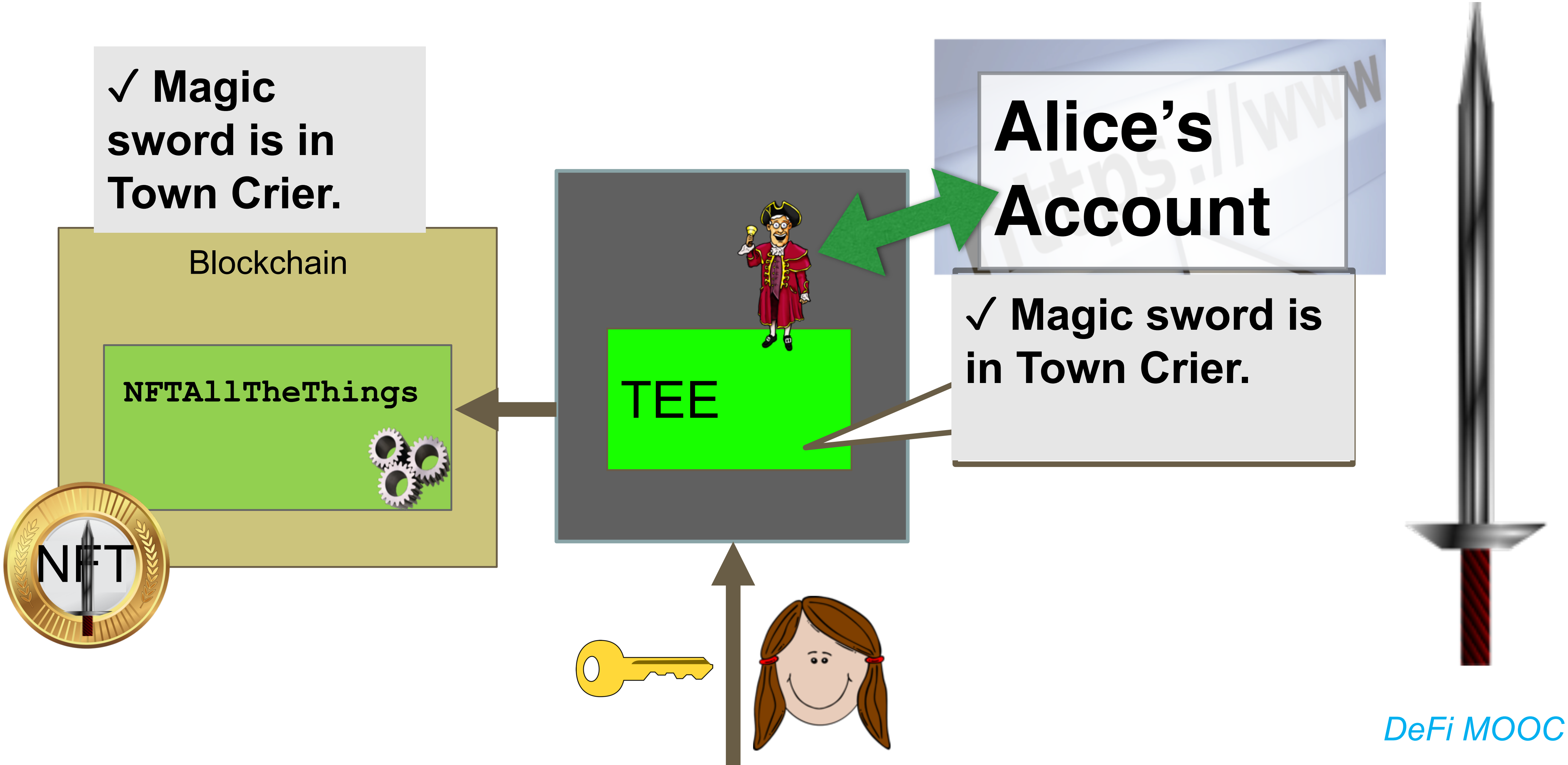
Beeple’s EVERYDAYS sold for $69+ million

Let’s NFT all the things!

Let’s NFT all the things!

In-game magic sword

Let’s NFT all the things!



√ Magic sword is in Town Crier.

Blockchain

NFTAllTheThings

TEE

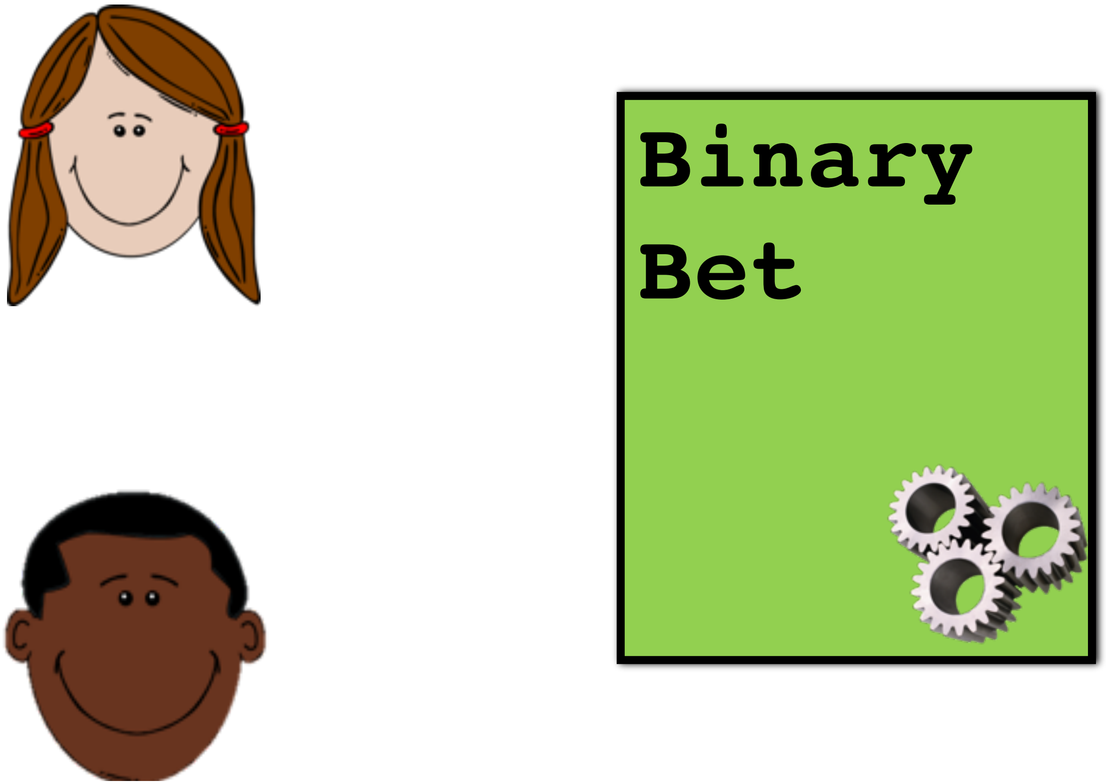
Alice’s Account

√ Magic sword is in Town Crier.

Example DeFi applications

- Application 1: Tokenizing digital assets
- **Application 2: Private DeFi**
- Application 3: Undercollateralized lending

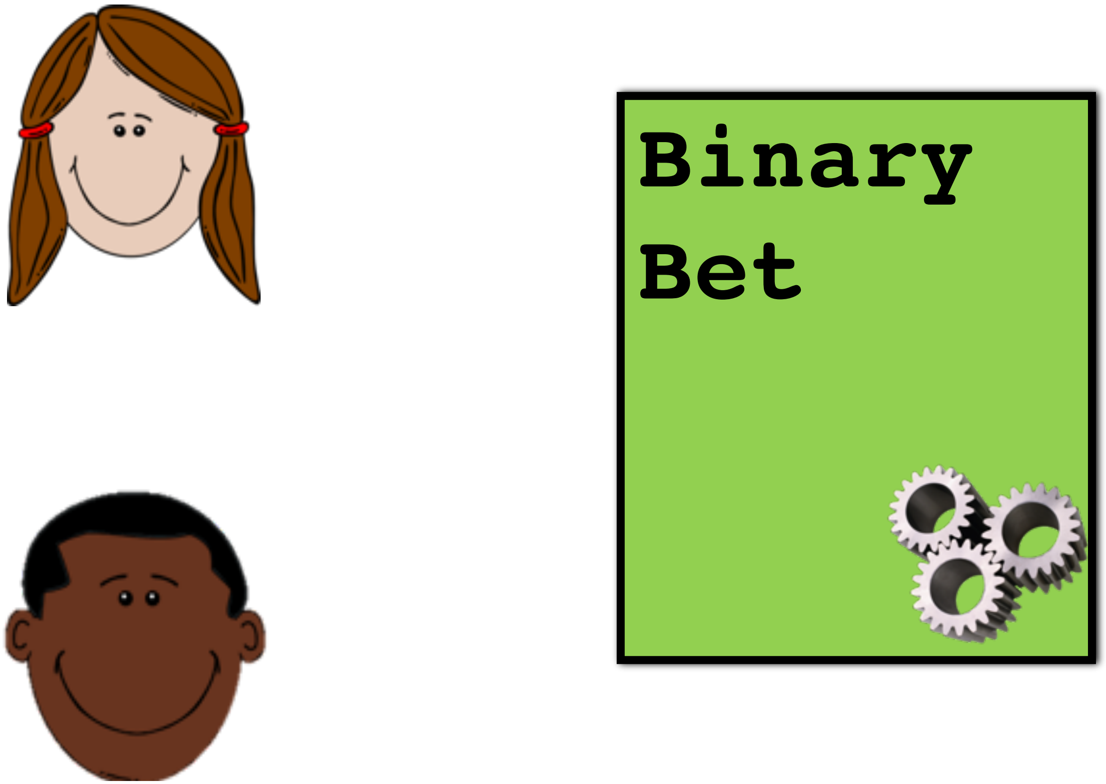
A simple DeFi contract



Binary Bet

A simple DeFi contract

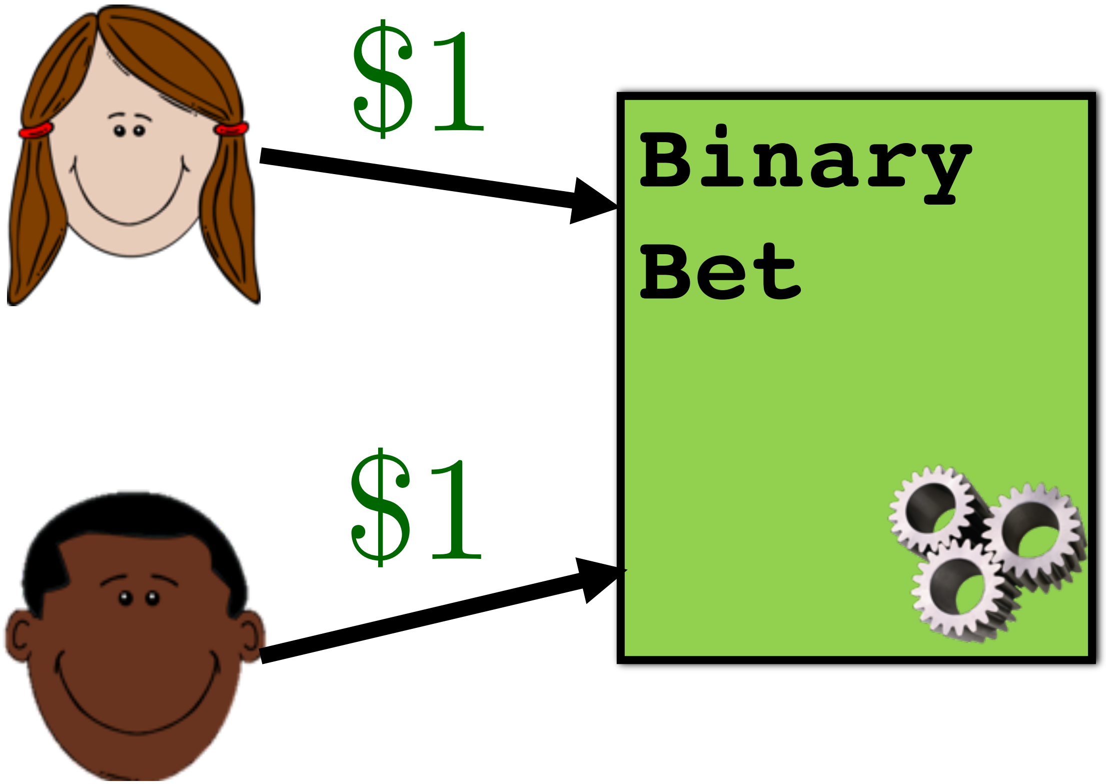
Will BTC price reach $1 million by 1 Jan 2024?



Binary Bet

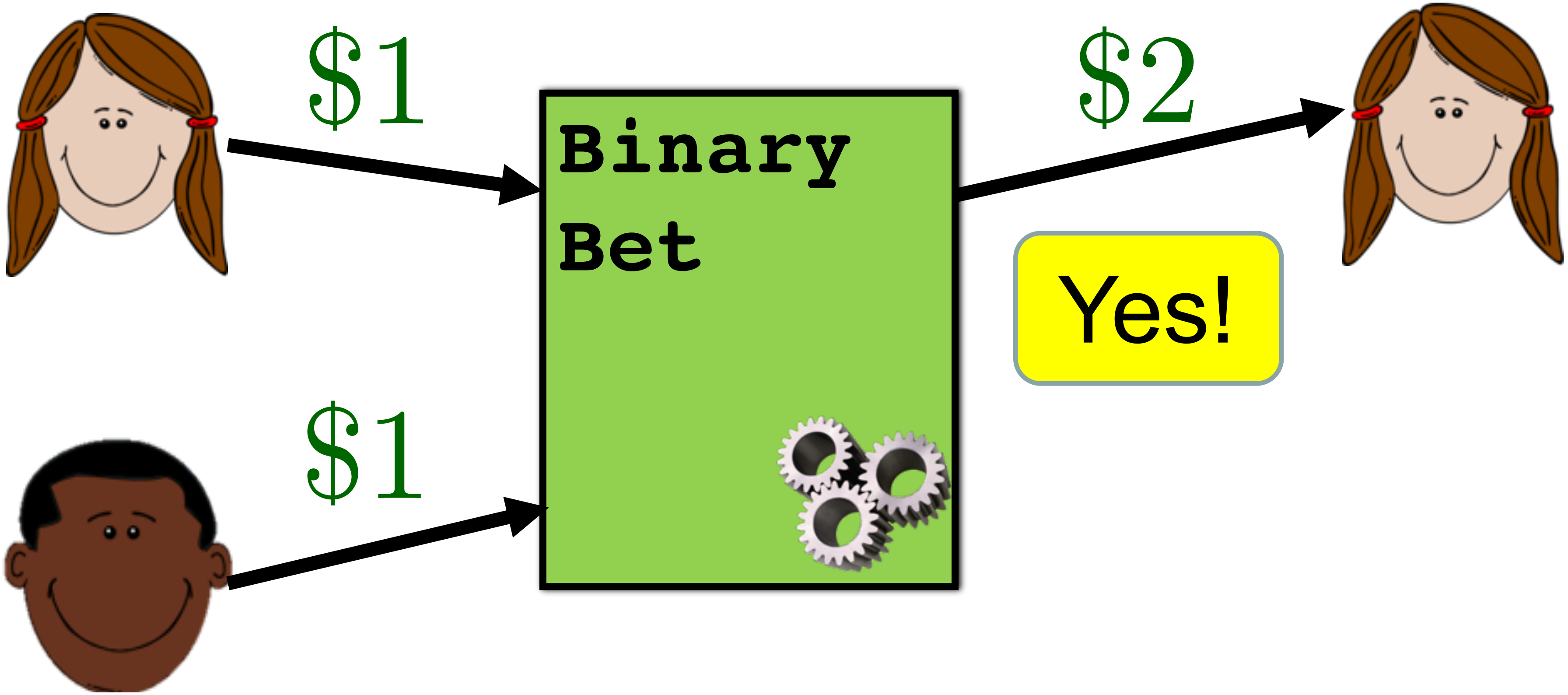
A simple DeFi contract

Will BTC price reach $1 million by 1 Jan 2024?



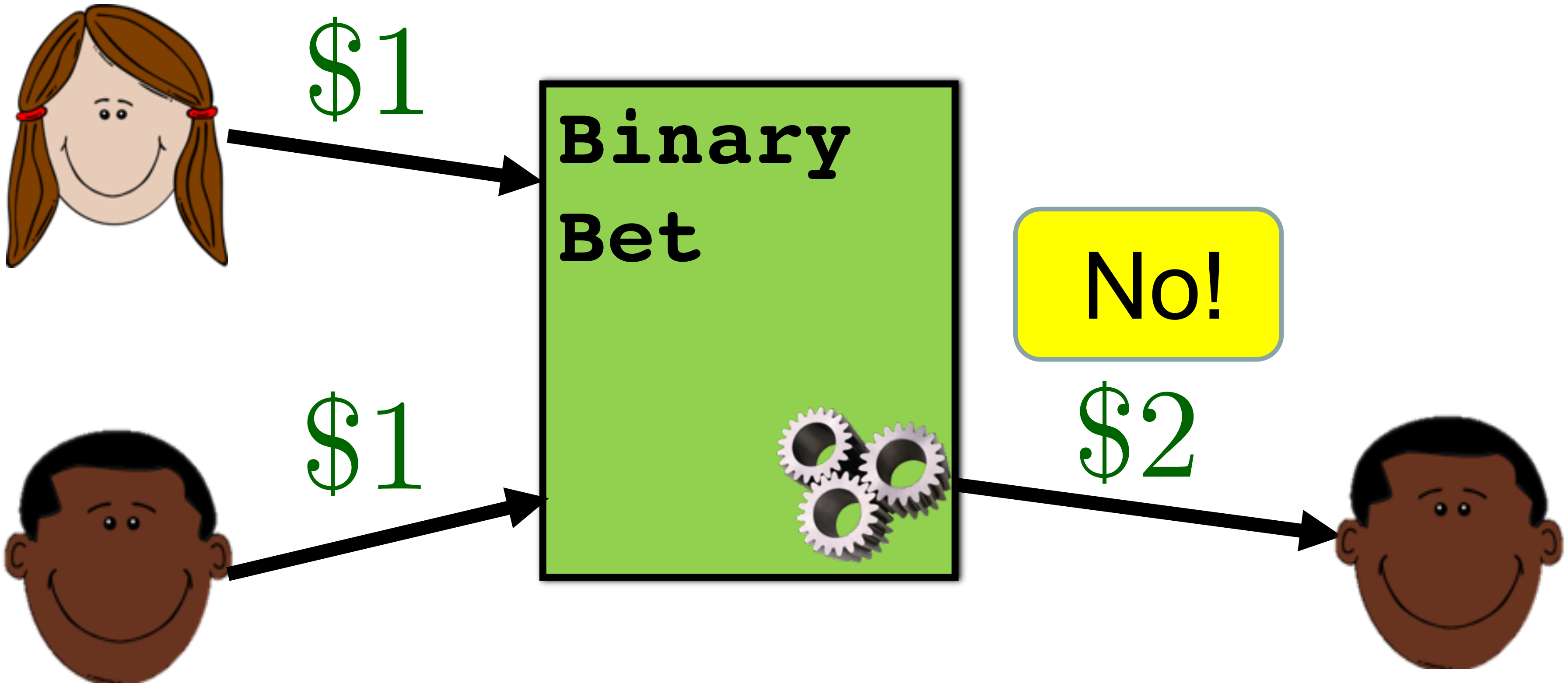
A simple DeFi contract

Will BTC price reach $1 million by 1 Jan 2024?



A simple DeFi contract

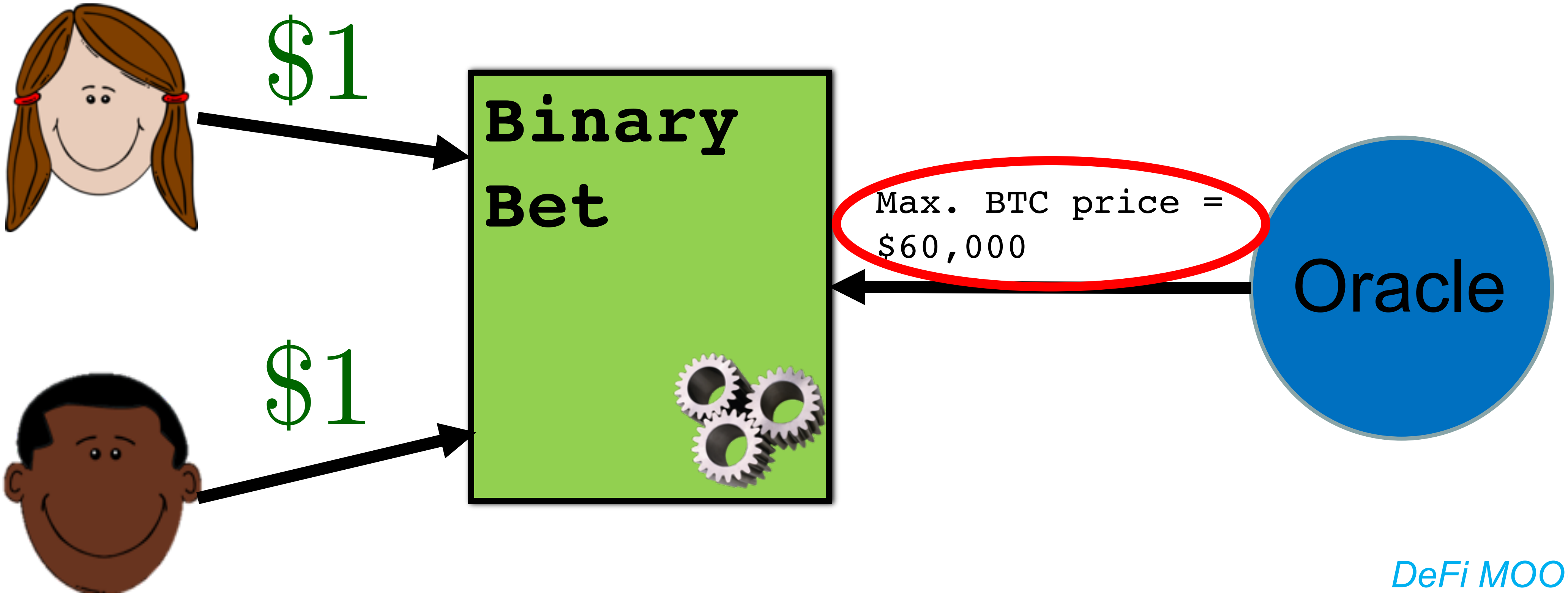
Will BTC price reach $1 million by 1 Jan 2024?

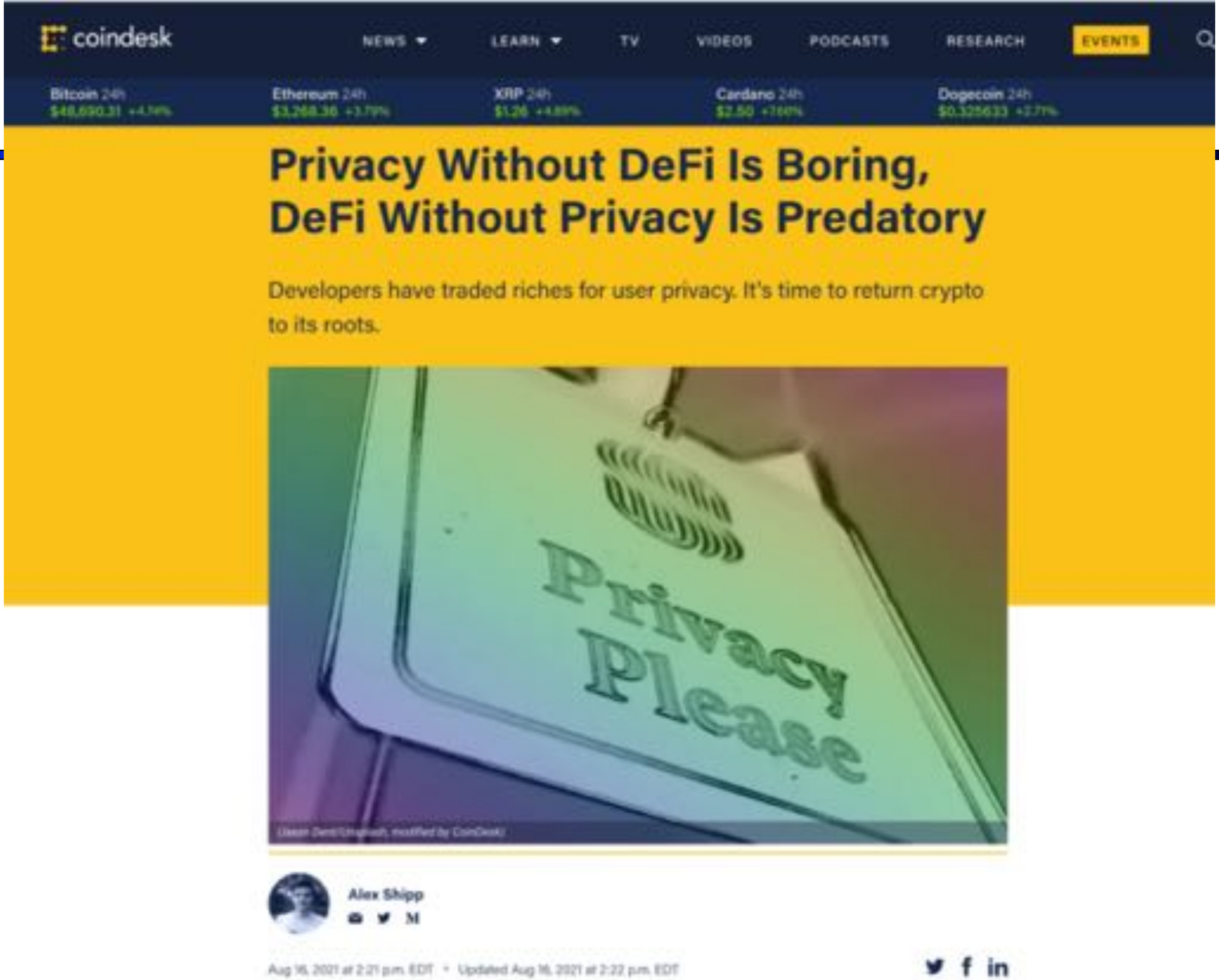


DeFi MOOC

Privacy problem

Will BTC price reach $1 million by 1 Jan 2024?





coindesk

NEWS ▾ LEARN ▾ TV VIDEOS PODCASTS RESEARCH EVENTS

Bitcoin 24h
$48,690.31 +4.74%

Ethereum 24h
$3,268.36 +3.79%

XRP 24h
$1.26 +4.89%

Cardano 24h
$2.50 +7.66%

Dogecoin 24h
$0.325633 +2.71%

Privacy Without DeFi Is Boring, DeFi Without Privacy Is Predatory

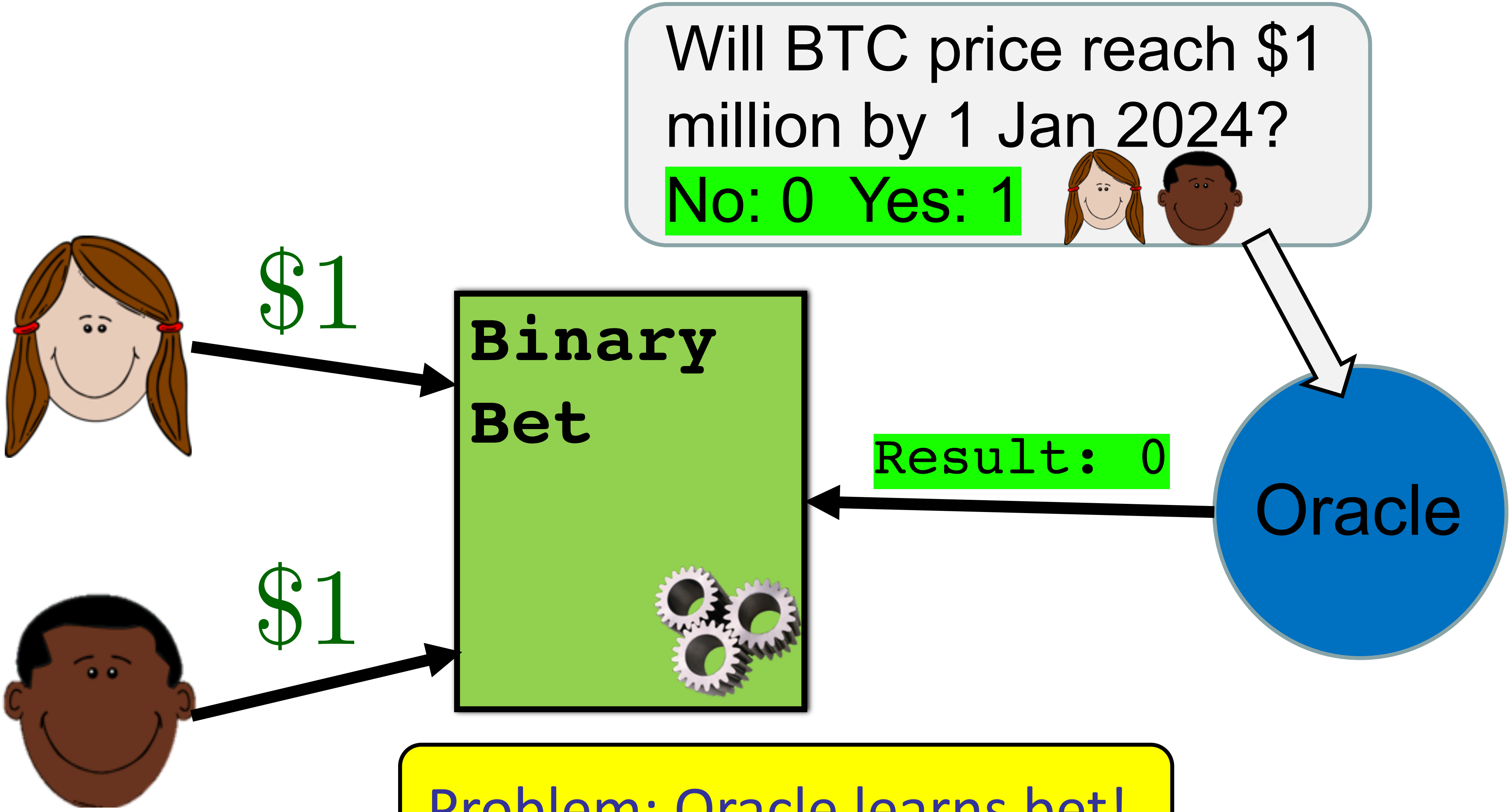
Developers have traded riches for user privacy. It's time to return crypto to its roots.

(Jason Dent/Unsplash, modified by CoinDesk)

Alex Shipp

Aug 16, 2021 at 2:21 p.m. EDT • Updated Aug 16, 2021 at 2:22 p.m. EDT

A partial solution



Will BTC price reach $1 million by 1 Jan 2024?

No: 0 Yes: 1

$1

$1

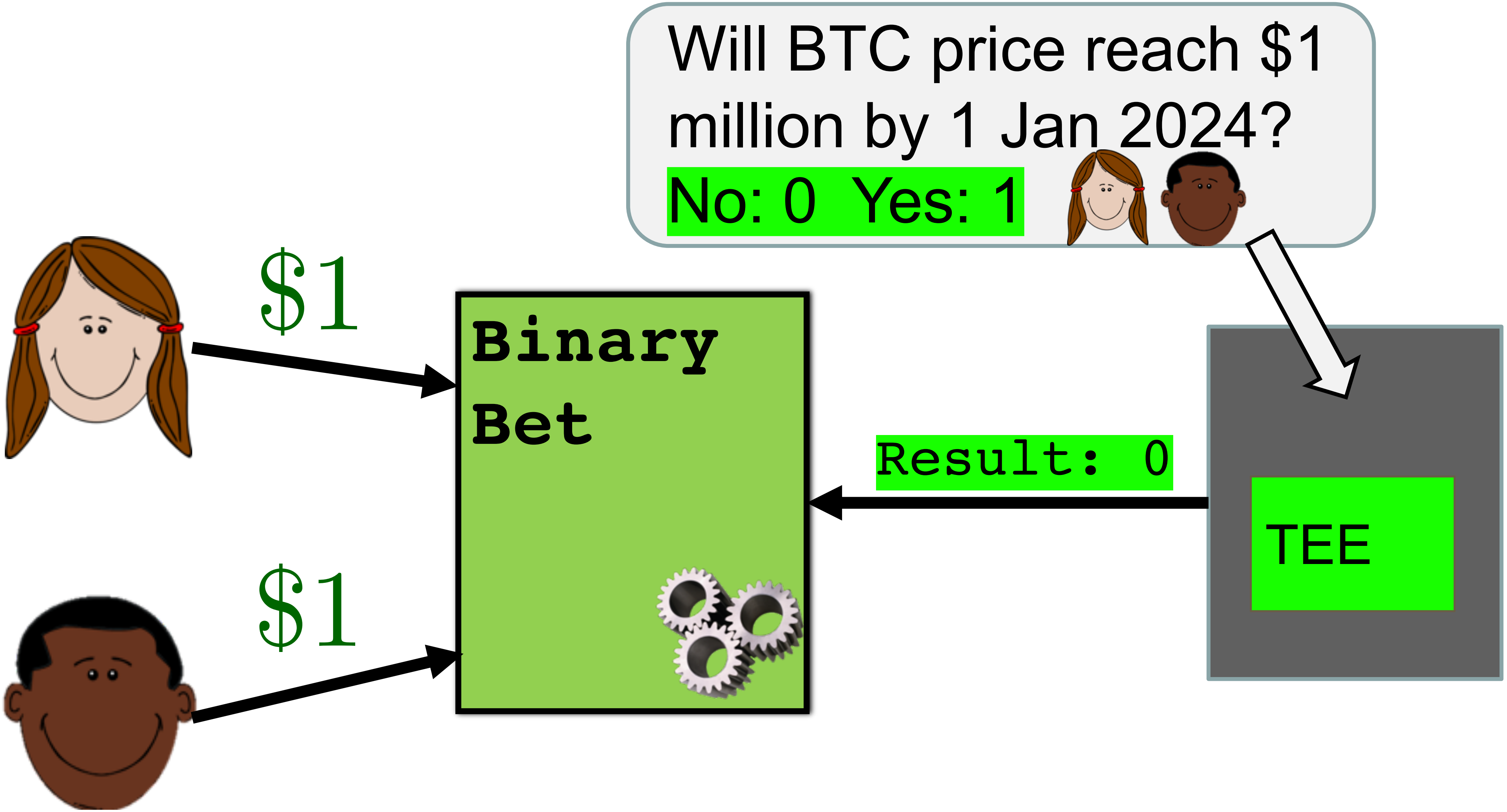
Binary Bet

Result: 0

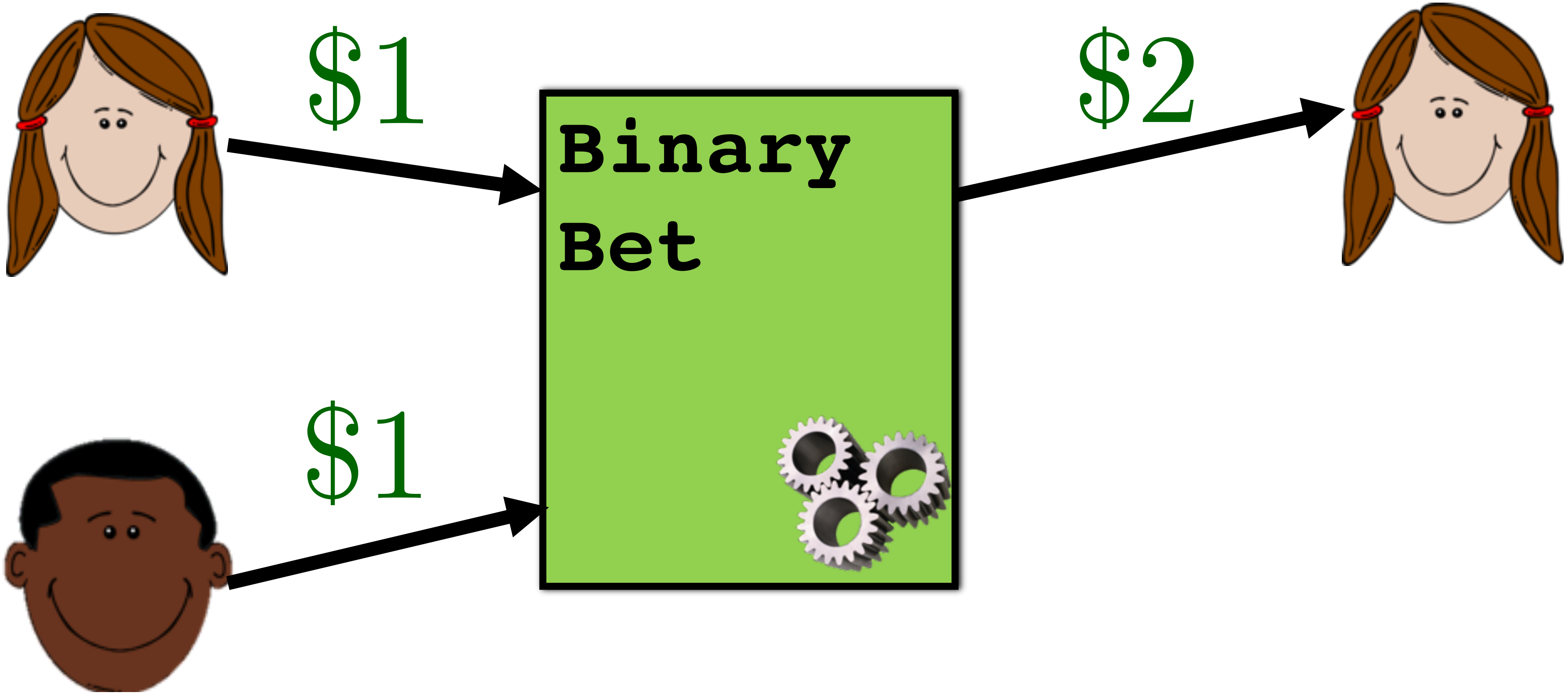
Oracle

Problem: Oracle learns bet!

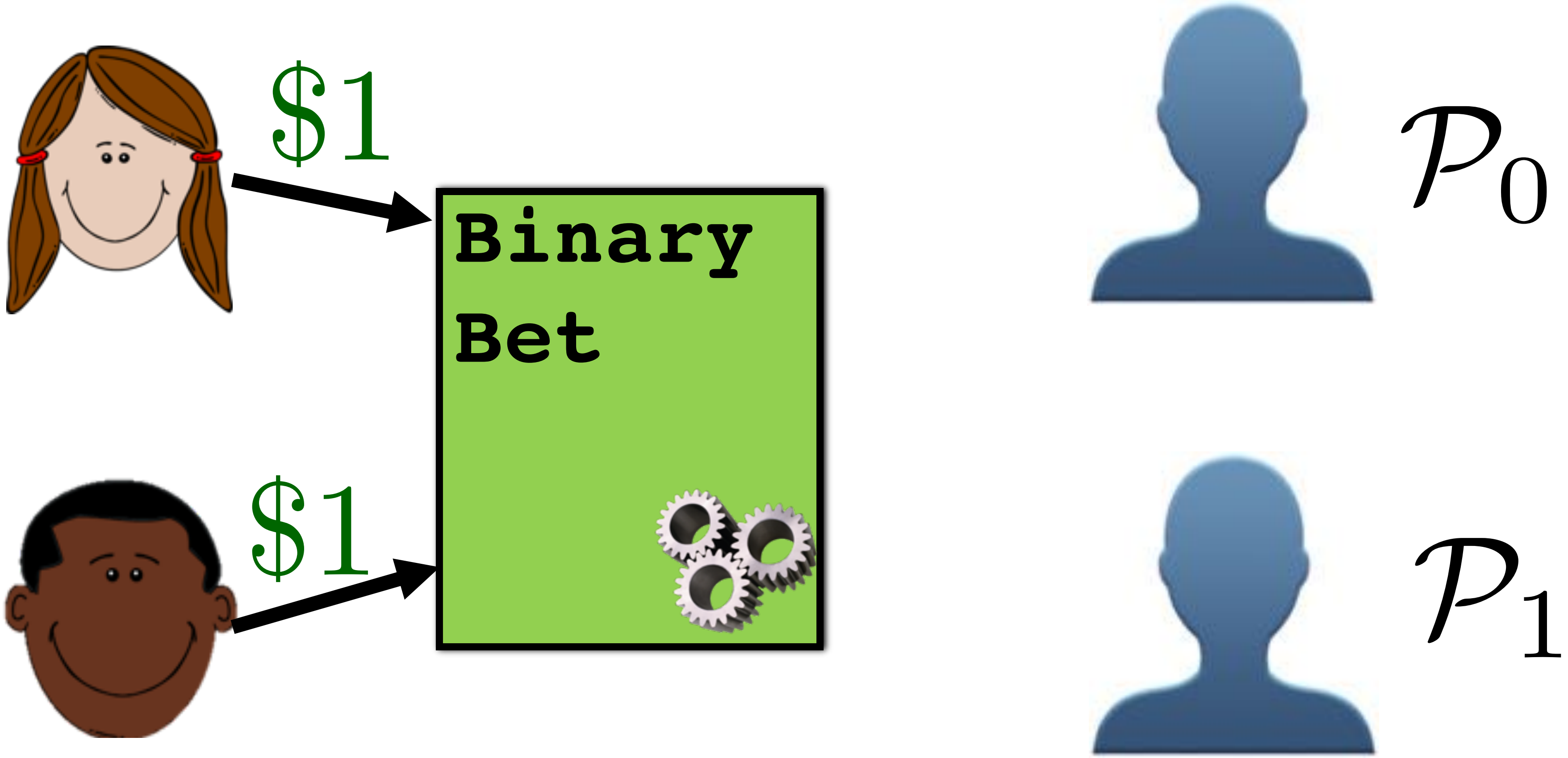
A partial solution



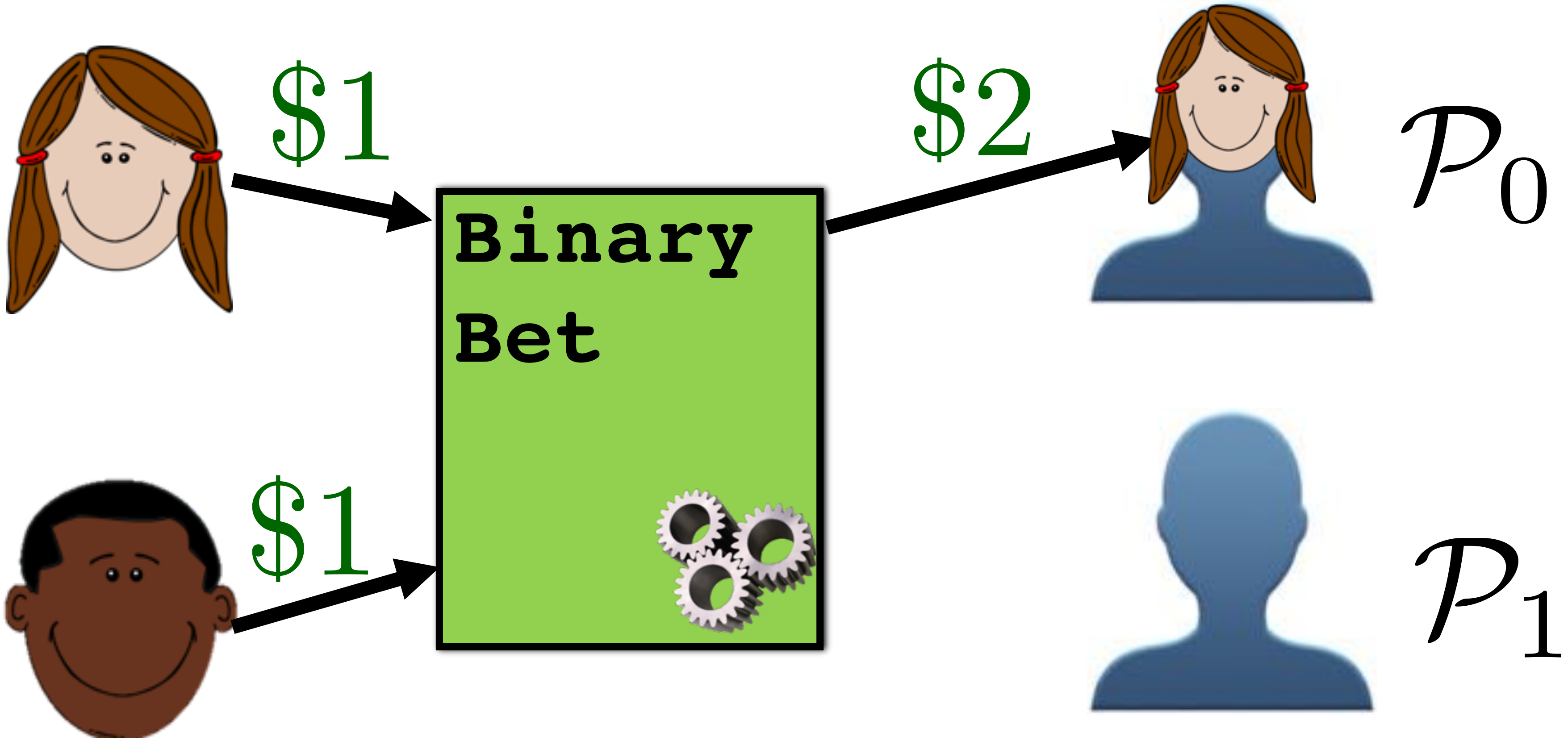
A simple DeFi contract



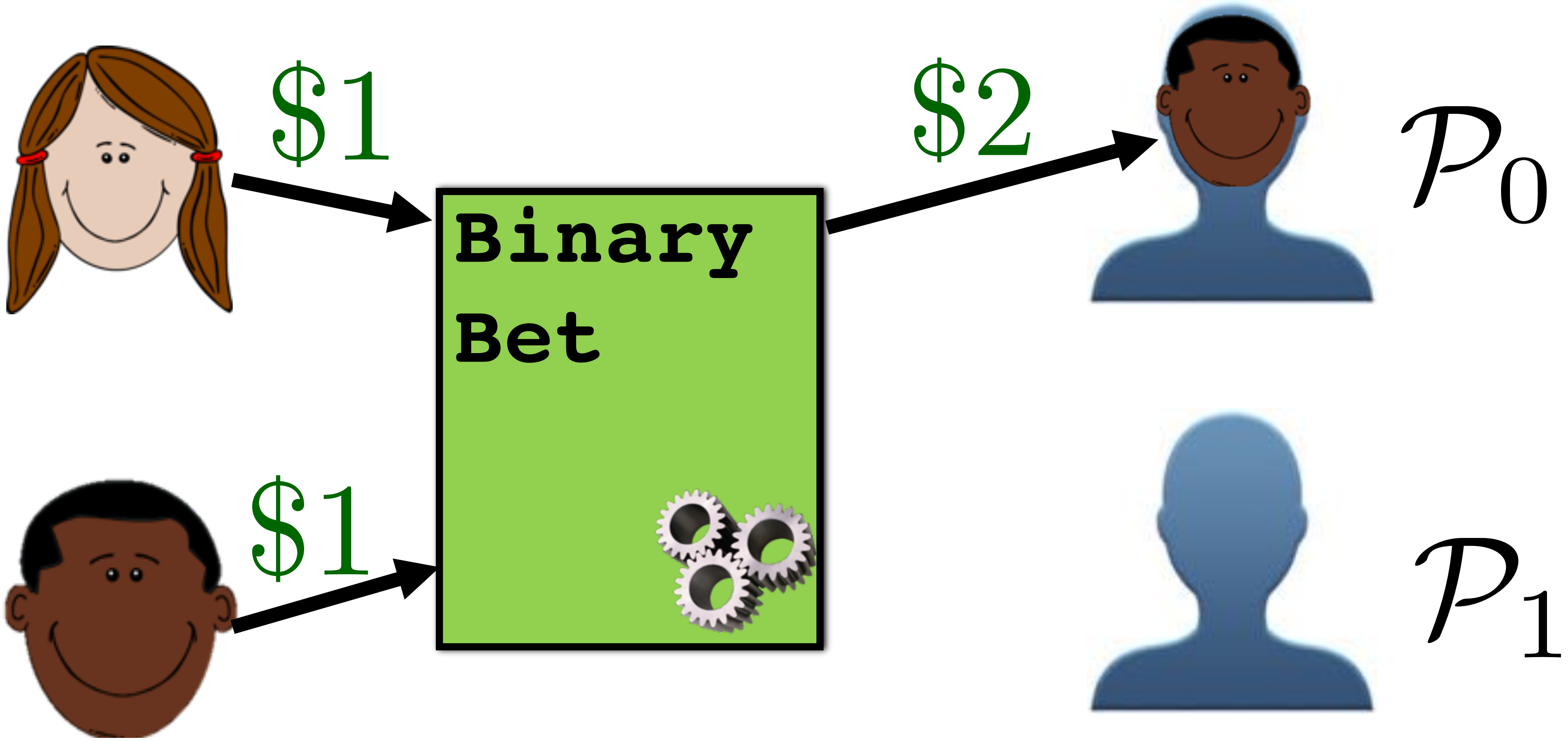
Mixicle



Mixicle



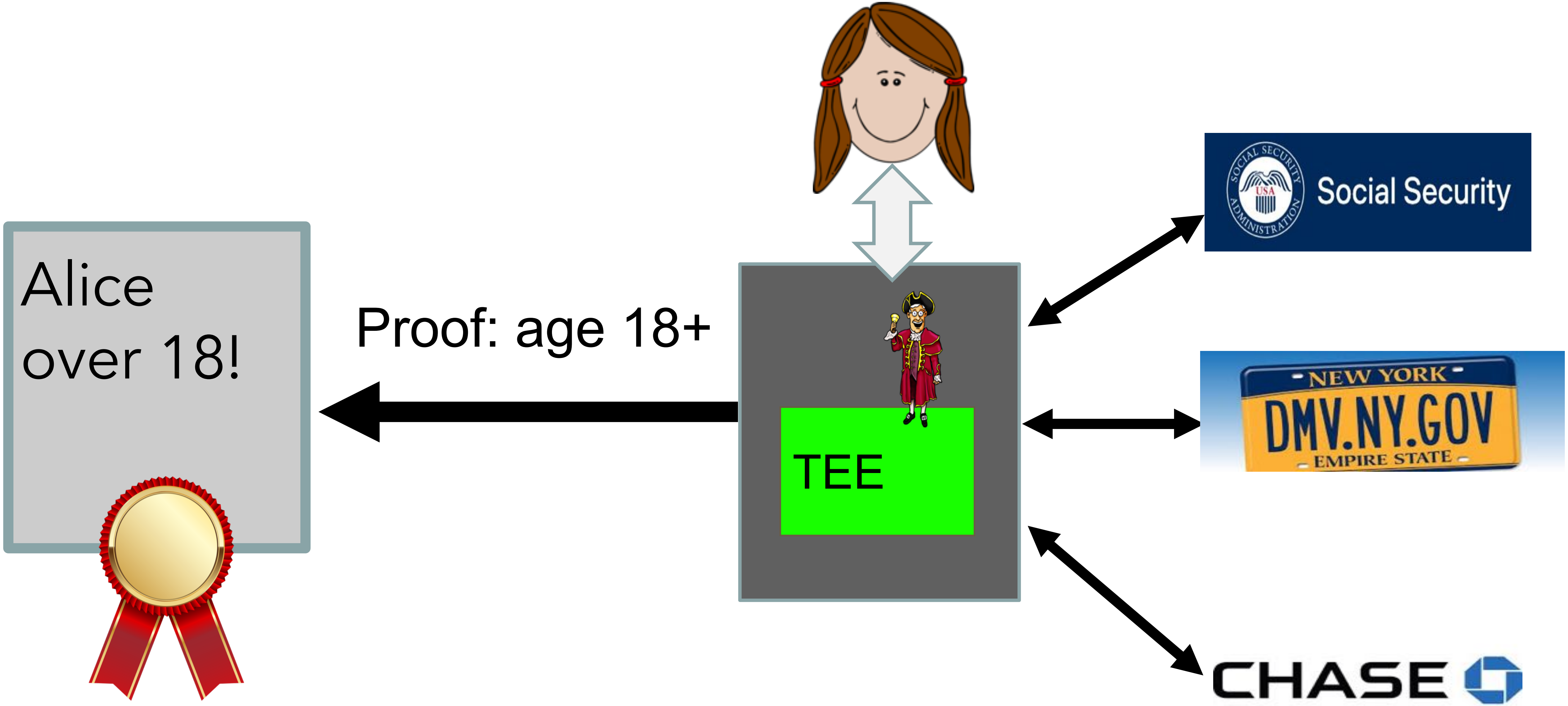
Mixicle



Some DeFi applications

- Application 1: Tokenizing digital assets
- Application 2: DeFi for real-world (hard) assets
- **Application 3: Decentralized identity**

Decentralized Identity



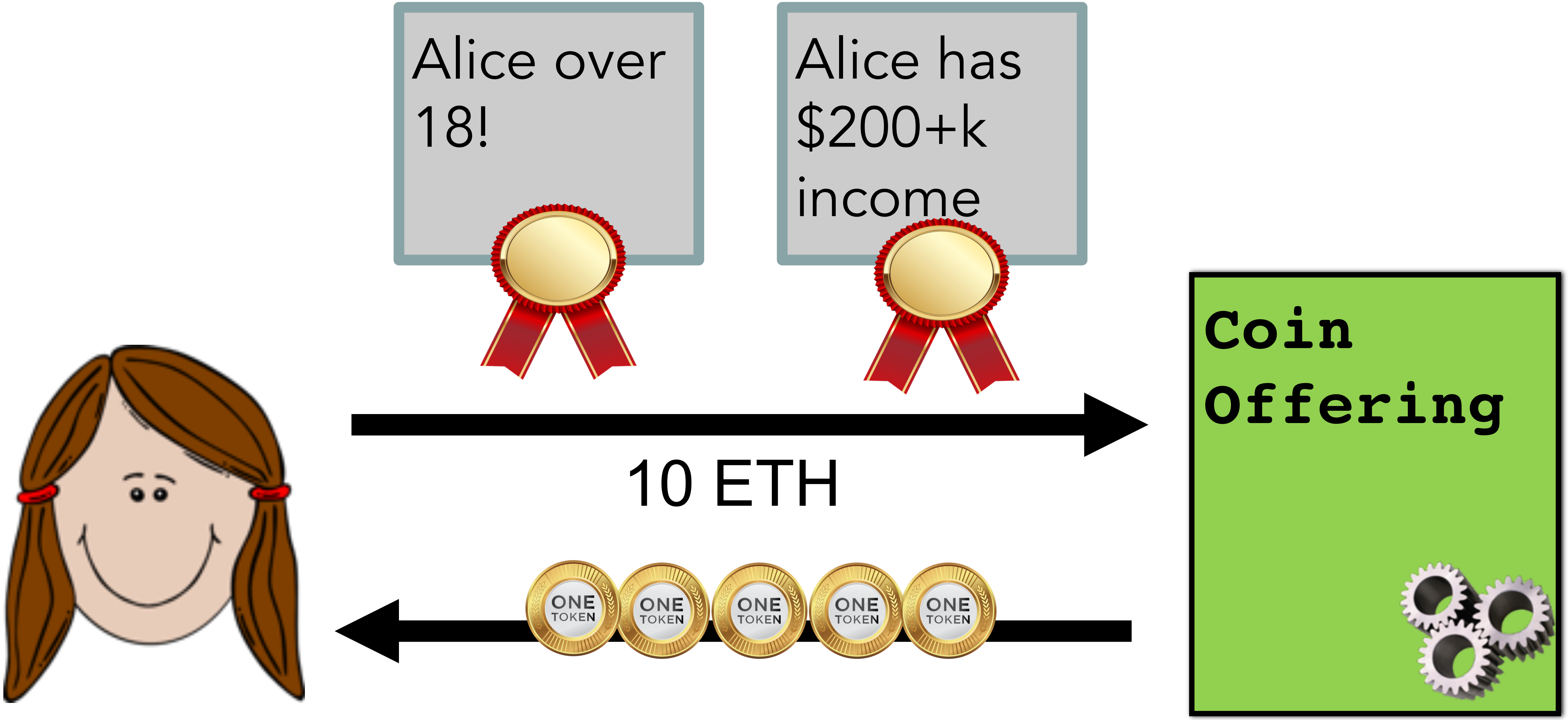
Alice
over 18!

Proof: age 18+

TEE

OC

Accredited Investment



Alice over 18!

Alice has $200+k income

10 ETH

Coin Offering

Summary

https://defi-learning.org

Summary

- Oracles deliver off-chain data to smart contracts.
- But they can do much more!
  - Oracles are a general-purpose fabric connecting blockchains with other systems (including other blockchains).
- Oracle systems entail technical challenges, e.g.,
  - Robustness (against node and data failures)
  - Privacy
- Oracles are necessary for most interesting DeFi applications.