Blockchains & Cryptocurrencies

Applications II

Instructors: Matthew Green & Abhishek Jain
Johns Hopkins University - Spring 2019

Housekeeping

- Two readings added for next time:
    - Augur (white paper)
    - Arwen (white paper)
- Presentations coming up 4/22

News?

Welcome to the hub of all hubs: Cosmos has launched

Jon Evans @rezendi / 3 weeks ago

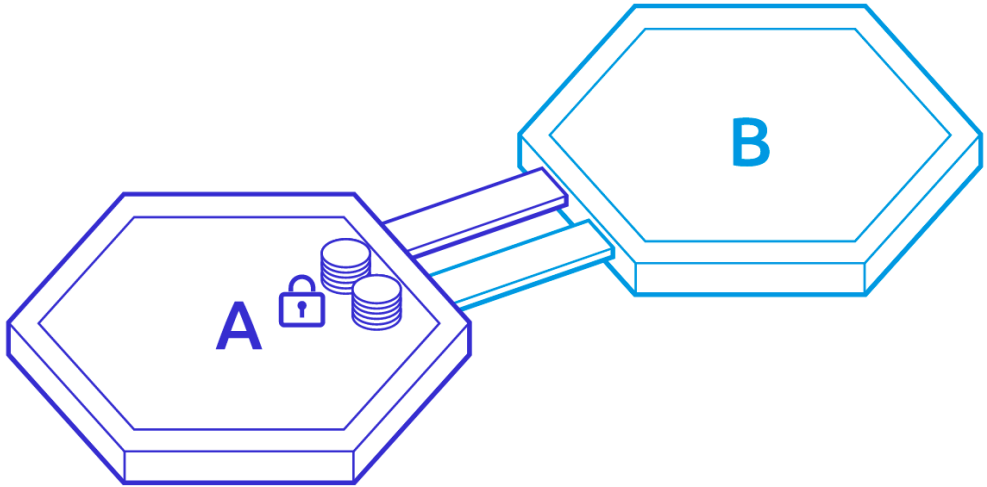
Comment

Tracking

Continuously, chain B receives the headers of chain A, and vice versa. This allows each chain to track the validator set of the other. In essence, each chain runs a `light-client` of the other.

Bonding

When the IBC transfer is initiated, the ATOM are locked up (`bonded`) on chain A.



Prediction markets & real-world data feeds

Assertions about the outside world

- **Idea**: add a mechanism to assert facts
  - election outcomes
  - sports results
  - commodity prices
- Bet or hedge results using smart contracts
- Forwards, futures, options...

General formulation: **prediction market**

Prediction markets

- **Idea**: trade *shares* in a potential future event
- Shares worth X if the event happens, 0 if not
- Current price / x = estimated probability

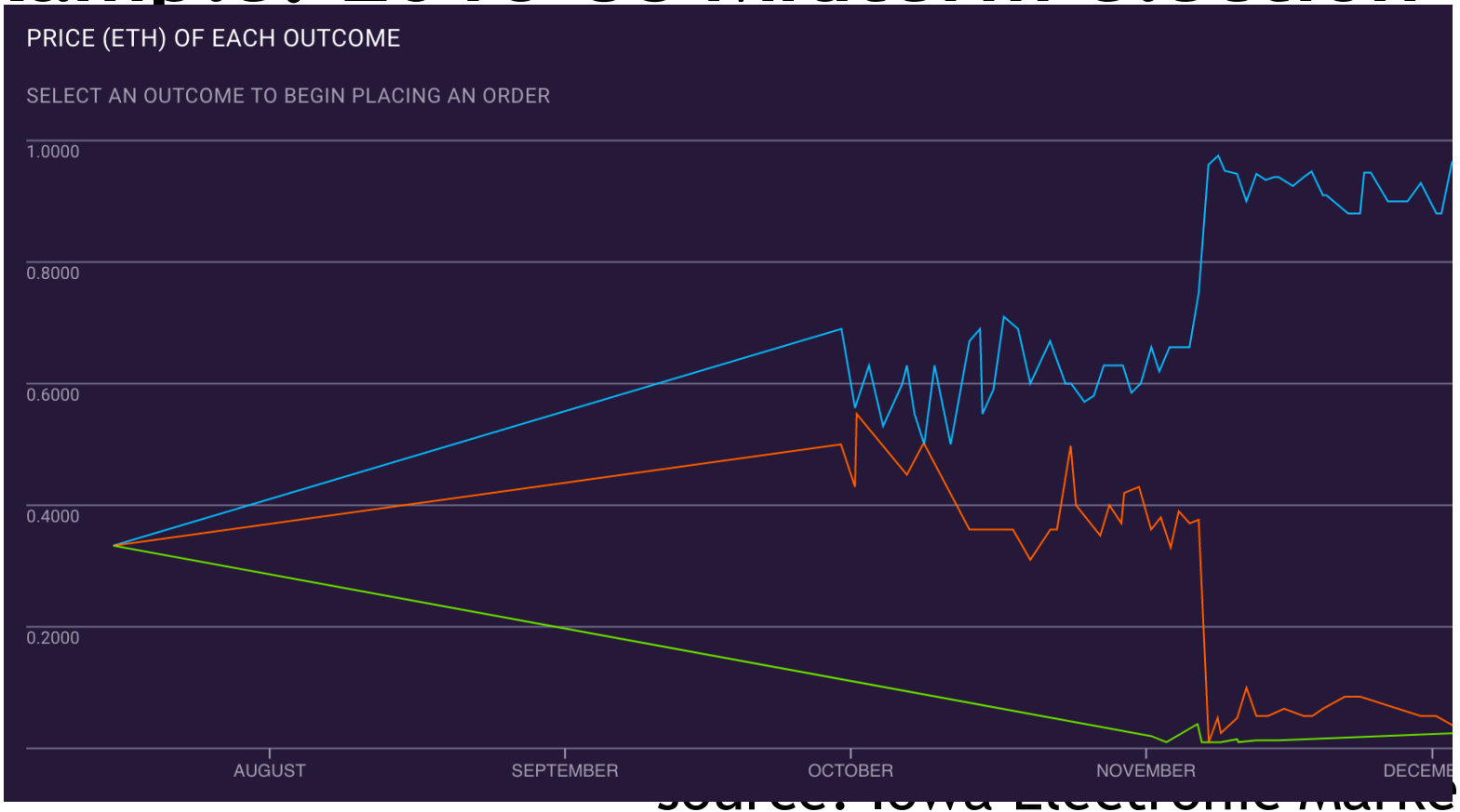
Example: World Cup 2014

					
pre-tournament	0.12	0.09	0.22	0.01	0.05
after group stage	0.18	0.15	0.31	0.06	0.00
before semis	0.26	0.21	0.45	0.00	0.00
before finals	0.64	0.36	0.00	0.00	0.00
final	1	0	0	0	0

Can immediately profit!

Should have shorted

Example: 2018 US Midterm election



Source: Iowa Electronic Markets

Prediction markets

- Economists love them
  - reveal all knowledge about the future
    - (under a number of assumptions)
  - allows profit from accurate predictions
  - “a tax on BS”
- Often beat polls and expert opinions
- Significant regulatory hurdles
  - InTrade shut down in 2013

Decentralized prediction markets?

- Decentralized payment & enforcement
- Decentralized arbitration
- Decentralized order book

Decentralized payment & settlement

- Simple solution: Bitcoin + trusted arbiters
- Better solution: altcoin with built-in support

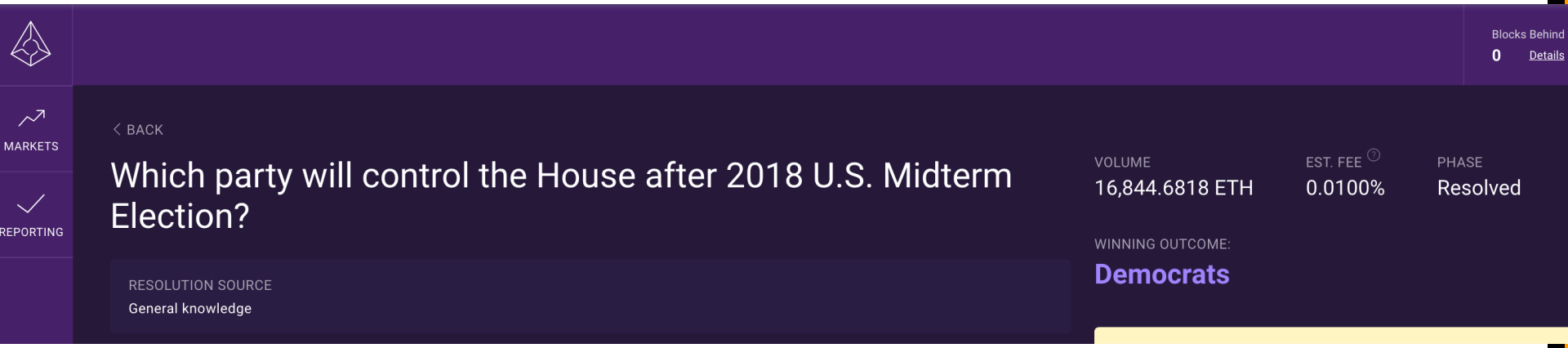
Four stages

- Creation - Make a new market
- Trading - Users place bets
- Reporting - Report the outcome
- Settlement - Pay users holding winning shares

Arbitration models

- Trusted arbiters
  - allow anybody to define & open a market
  - risk of incorrect arbitration, absconding
- Users vote
  - requires incentives, bonds, reputation
- Miners vote
  - may be disinterested or not know

Augur


Blocks Behind
0
Details
MARKETS
REPORTING
BACK
Which party will control the House after 2018 U.S. Midterm Election?
VOLUME
16,844.6818 ETH
EST. FEE
0.0100%
PHASE
Resolved
WINNING OUTCOME:
Democrats
RESOLUTION SOURCE
General knowledge

Augur (market creation)

- Any user can create a new market
  - Specify the nature of the bet, e.g.,
    "No Deal Brexit will occur on April 12, Yes/No"
  - Designates a reporter
  - Must specify two bonds in a public ETH transaction:
    - "Validity" bond: paid back if market resolves correctly
    - "Reporter no-show" bond

Augur (matching)

- This is conducted by a matching engine
- Consider a market with two outcomes (A, B)
    - Alice bets .3 ETH on outcome A
    - Bob bets .7 ETH on outcome B
    - Total eventual payout is 1 ETH (after event reported)
- Shares in either event can be traded continuously

Augur (reporting)

- Eventually the designated reporter submits an outcome
- This must be transmitted to the blockchain by a user

Augur (reporting)

- Eventually the designated reporter submits an outcome
- If designated reporter doesn't, then anyone can report
- Reports must be transmitted to the blockchain by users
    - To prevent dishonesty, such a user must post a "bond" (in REP tokens, which are a native format)
    - If nobody disputes this outcome, market eventually settles

Augur (reporting)

- Eventually the designated reporter submits an outcome
- This must be transmitted to the blockchain by a user
    - To prevent dishonesty, the user must post a "bond" (in REP tokens, which are a native format)
    - If nobody disputes this outcome, market eventually settles
    - If people dispute, this becomes a voting process

Augur (reporting)

- Eventually the designated reporter submits an outcome
- This must be transmitted to the blockchain by a user
    - To prevent dishonesty, the user must post a "bond" (in REP tokens, which are a native format)
    - If nobody disputes this outcome, market eventually settles
    - If people dispute, this becomes a voting process
    - **What if nobody can reach agreement?**

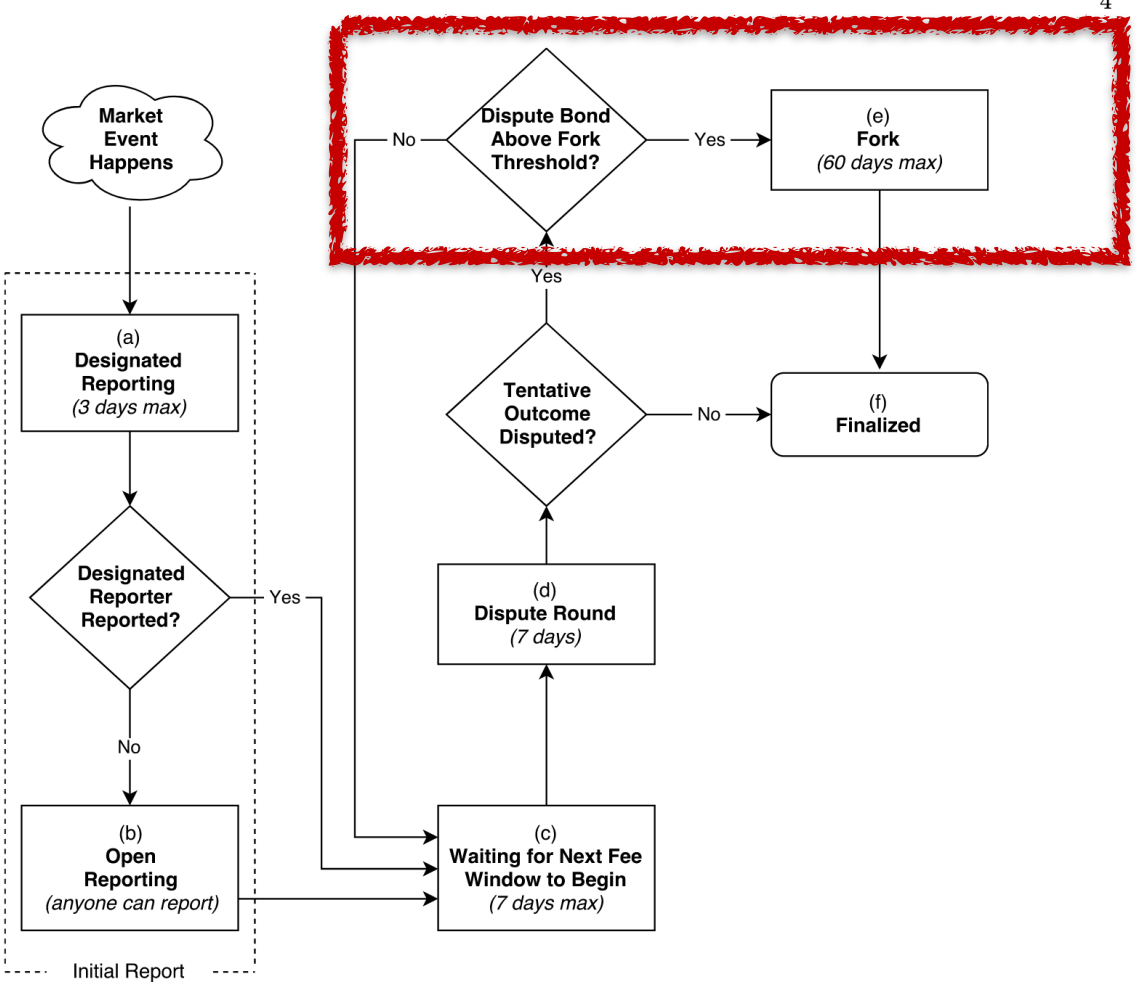


Figure 2. Reporting flowchart.

Augur (reporting)

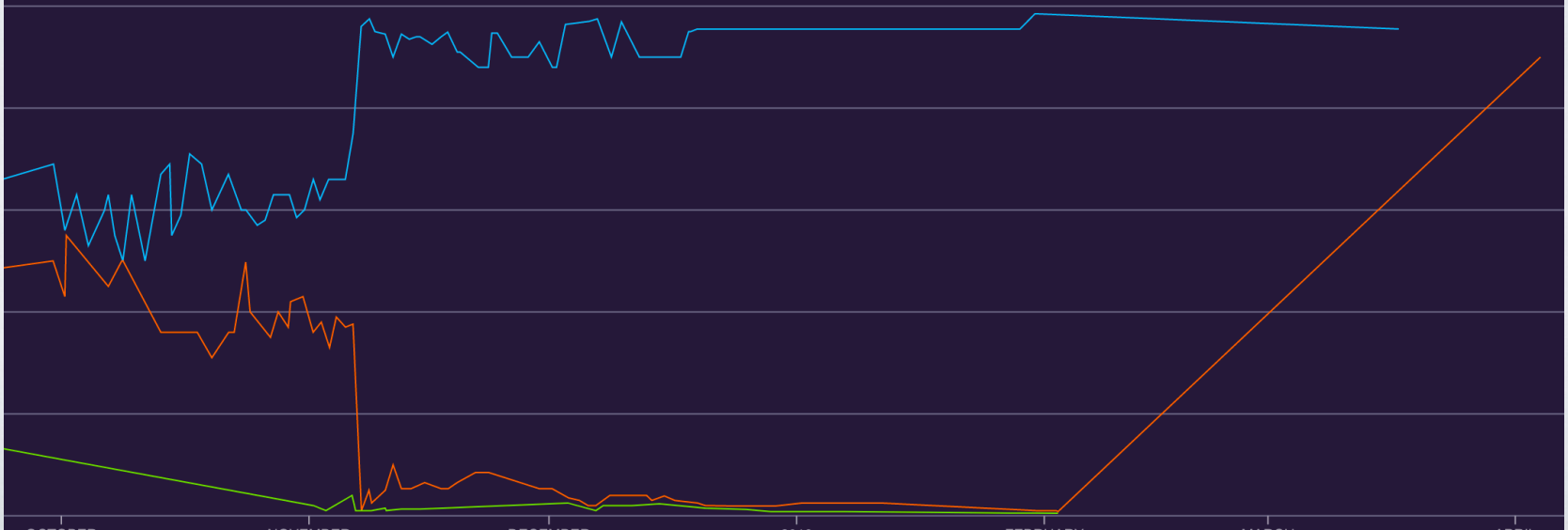
EVENT ENDED & REPORTING STARTED

December 11, 2018 4:00 AM (UTC 0)

December 10, 2018 11:00 PM (EST) (Your Timezone)

MARKET AUTHOR

0xc64e96319366da7d00ef4bc14b42e8b1f3a31f52



Augur (disputing)

- If users don't like the outcome, they can dispute
- At this point, the opposing sides must stake increasing amounts of REP on the result, until one side fails to produce enough money

Augur (disputing)

- If 2.5% of all REP staked dispute the report, then the Augur network (REP) forks into two different tokens
    - One token represents Outcome A, one represents Outcome B
    - Holders of the original REP, can then decide to convert their tokens into REP-A or REP-B
    - All ongoing markets move to the branch that gets the most tokens

Posted by u/EventLogs 2 months ago

19

Status of Midterm Election Disputes

Here is the status of "**Which party will control the House after 2018 U.S. Midterm Election?**" https://predictions.global/augur-markets/0xbbbc0a8baa03535e0a680ee2f057162aaaafd570:

On 1/11/19, this person paid $3,600 for Republicans to continue the dispute: https://etherscan.io/address/0xF2153d402f5A5D4FF5eF6Bdb815c3C962c9d3E53#tokentxns

The Democrats now have to come up with $7,200 before 1/23/19 to defend their position.

Here are the 5 brave people who last funded the Democrats in this dispute:

https://LogFile.info/Tit

And here are their current balances (Ether and Tokens):

Centralized order books

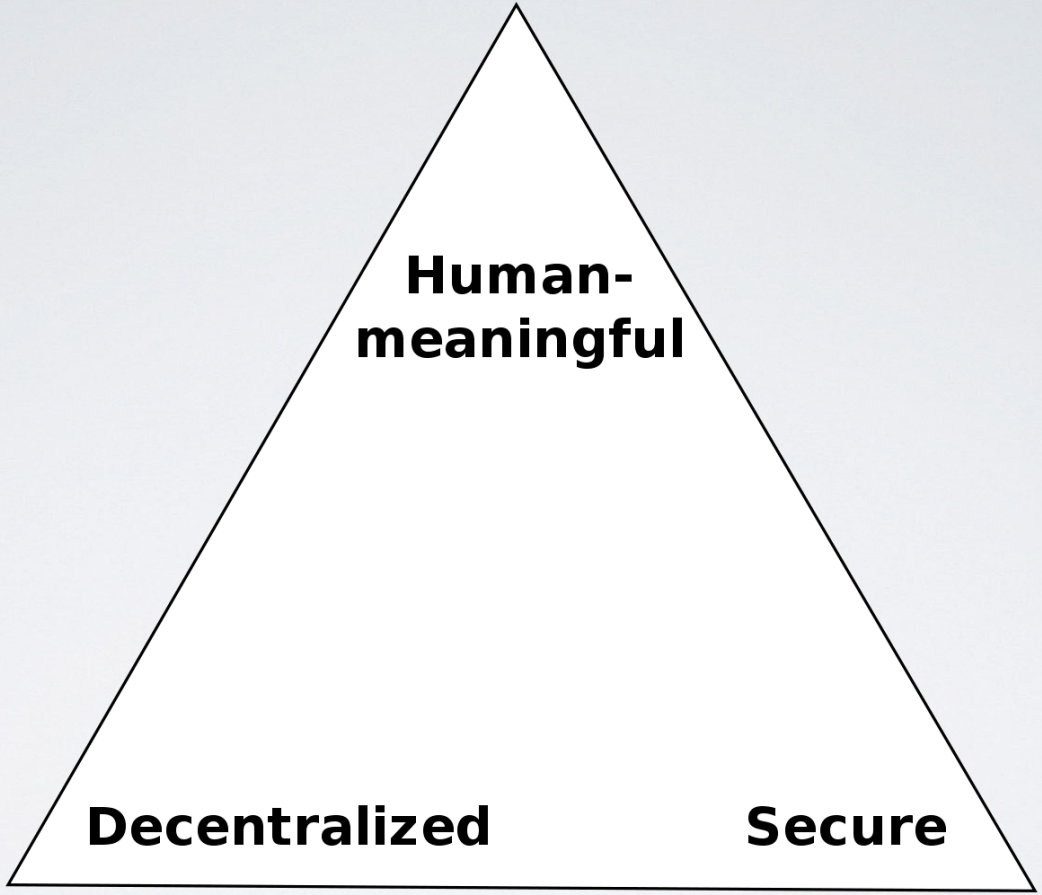
- Traditional model
- Promise to split surplus between buyer, seller
- Front-running is considered a serious crime!
  - require regulation, auditing, monitoring

Decentralized order books

- **Idea:** Submit orders to miners, let them match *any* possible trade
- Spread is retained as a transaction fee
- May be less efficient
  - Higher fees
  - Slower trades to avoid higher fees

PKI

- Blockchains can be used as a key/value store
- Associate a public key with a domain name
- Examples: Namecoin, Handshake
    - Does this solve Zooko's triangle?


Human-
meaningful
Decentralized
Secure

Ledger-conditioned computation

- Most of the solutions discussed so far use **cryptography** to secure **ledgers** (blockchains)
- Why not use ledgers to secure cryptography?

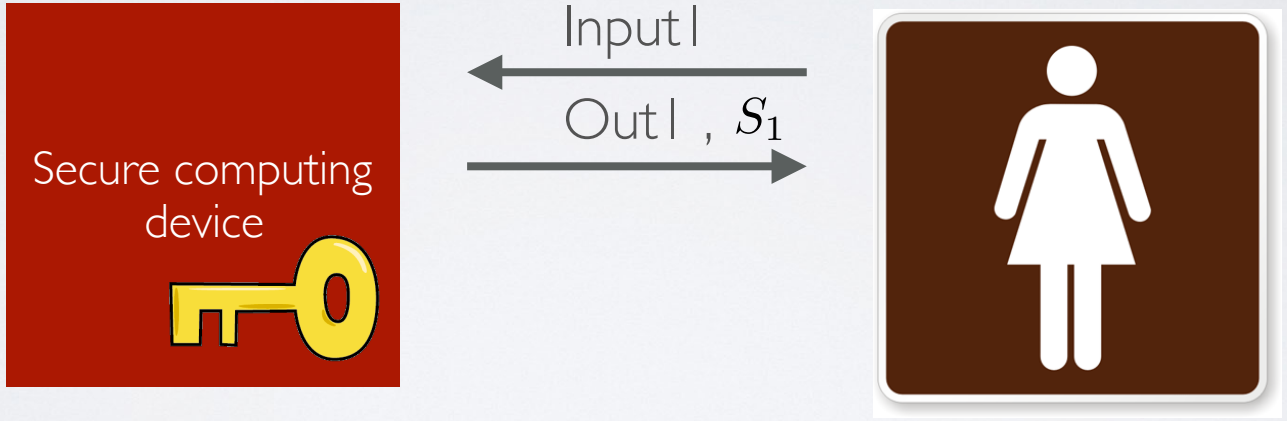
Ledger-conditioned computation (Setting 1)

- Assume a trustworthy computing device with internal secrets — but no ability to keep state
- These devices can be constructed inexpensively from hardware, or "virtually" from cryptographic obfuscation and/or MPC
- Assume we want multi-step interactive computation

Ledger-conditioned computation (Setting 2)

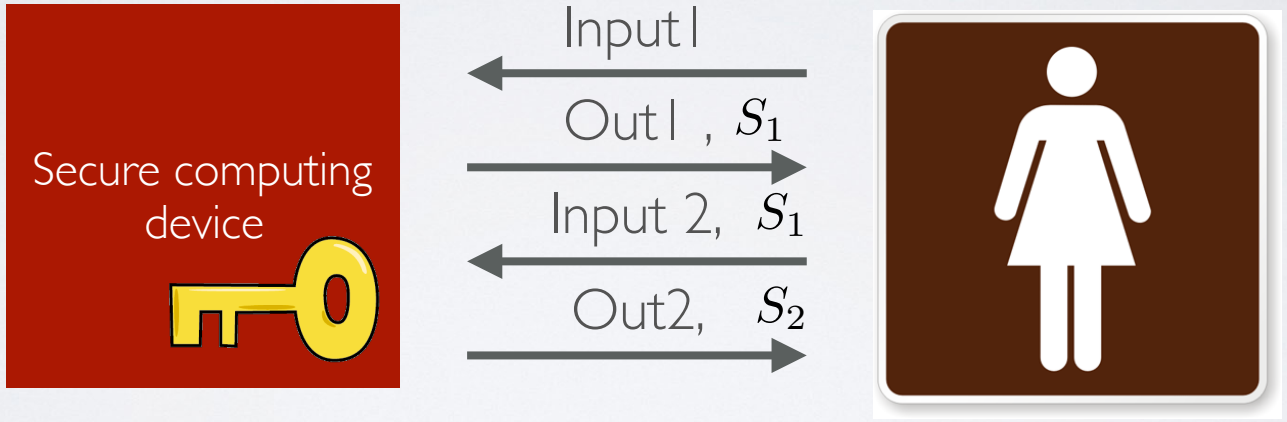
- Alternatively, imagine a network of identical trustworthy computing devices, each provisioned with secrets
- We want to run a single multi-step interactive computation where the node performing the computation can be replaced between steps
- "Private smart contracts"
  "AWS Lambda"

State without ledgers



$S_1 \leftarrow \mathsf{Encrypt}(K, \mathsf{state}_1)$

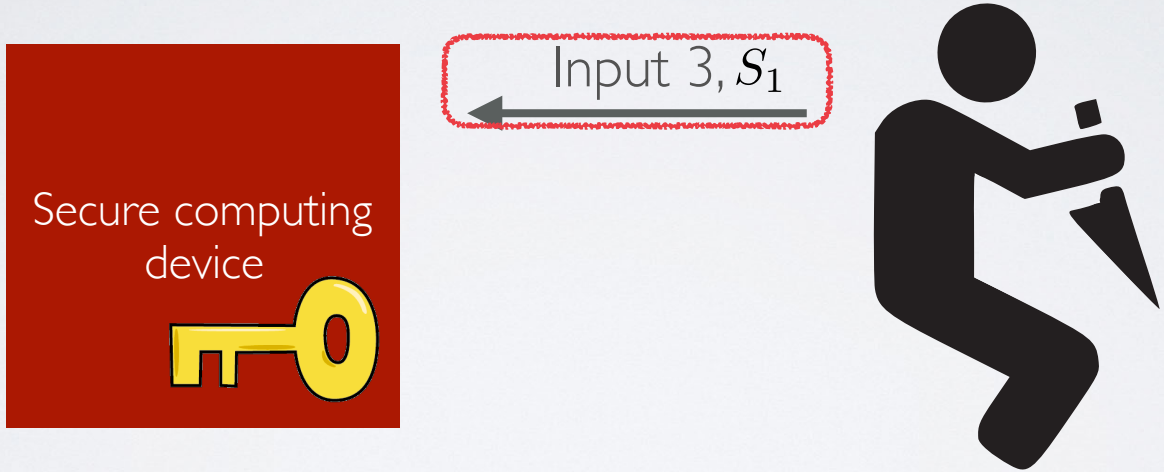
State without ledgers



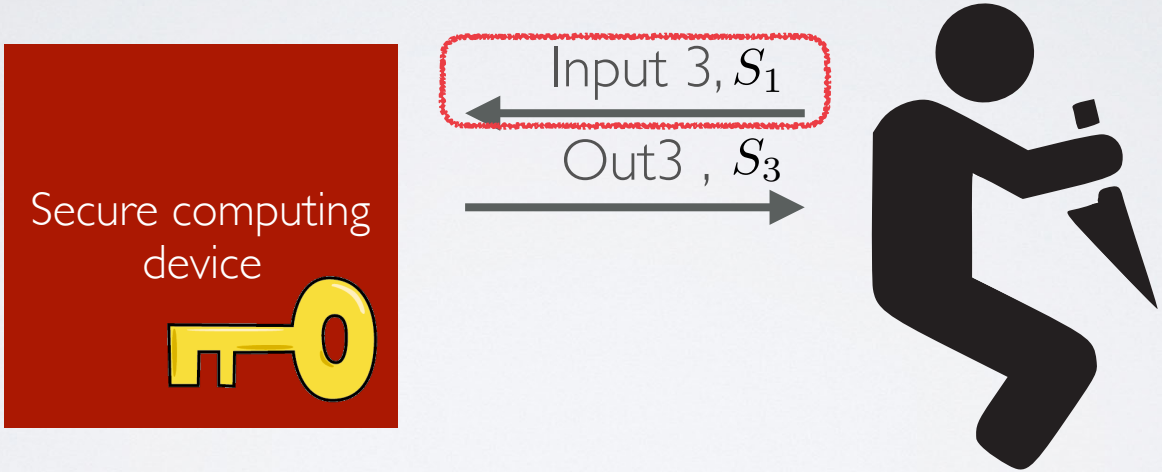
$\text{state}_2 \leftarrow \text{Decrypt}(K, S_1)$

$S_2 \leftarrow \text{Encrypt}(K, \text{state}_2)$

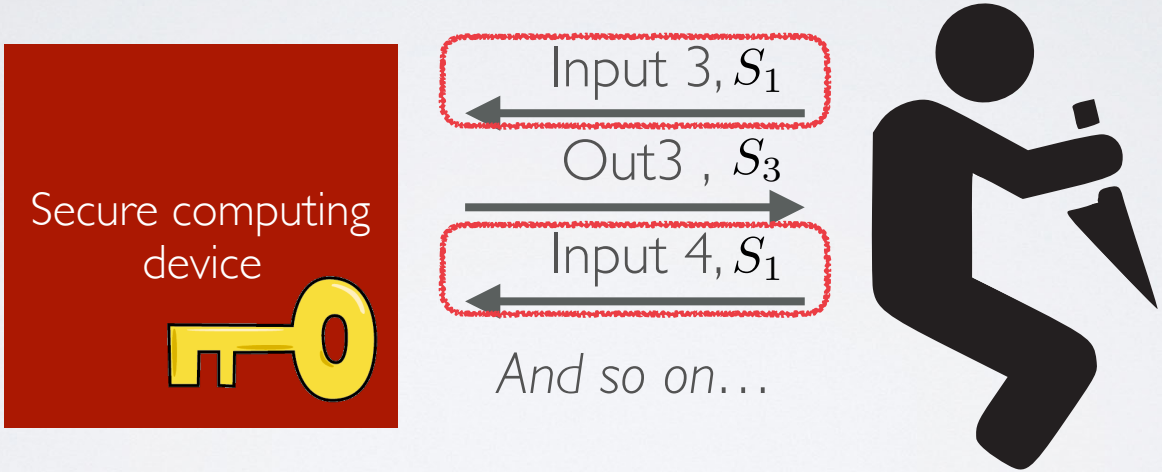
Reset attacks



Reset attacks



Reset attacks

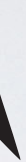


Imagine we have a "publicly verifiable" blockchain:

1. We can post a string S
2. Obtain a copy of the full Ledger, plus a proof that the ledger is valid

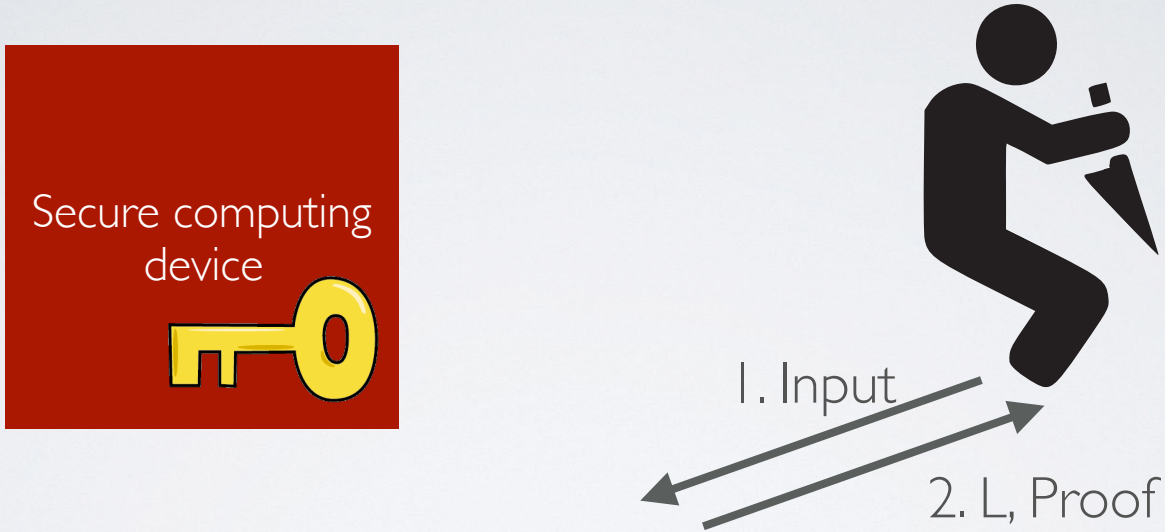
(This covers most private blockchains, many public blockchains if we make an economic assumption)

Secu

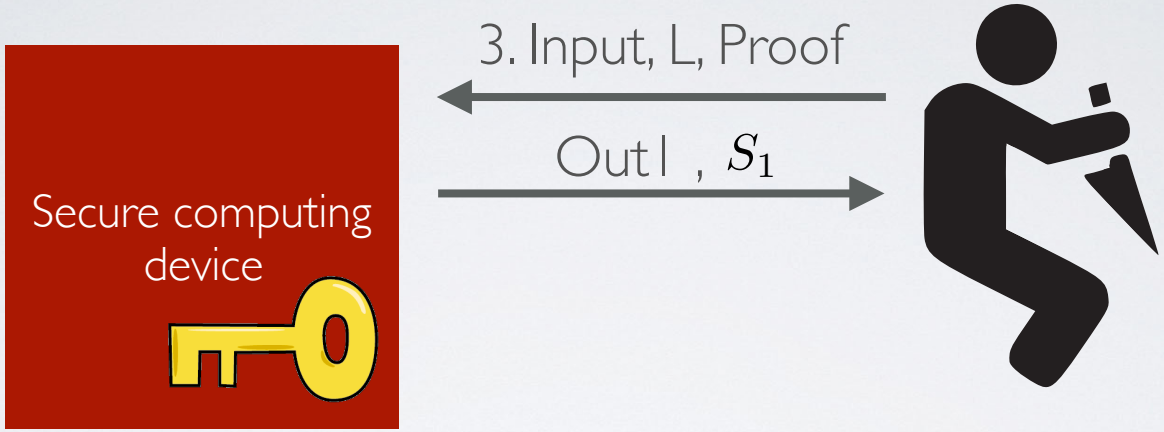


Publicly-verifiable ledger

Securing state with ledgers



Securing state with ledgers



Publicly-verifiable ledger