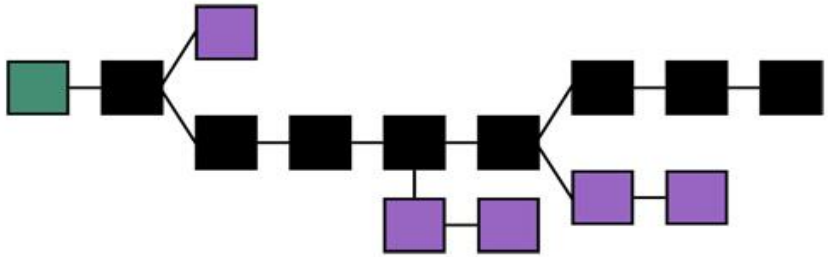
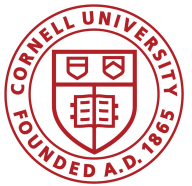
Bitcoin and Beyond:
Yesterday, Today, and the Next Ten Minutes

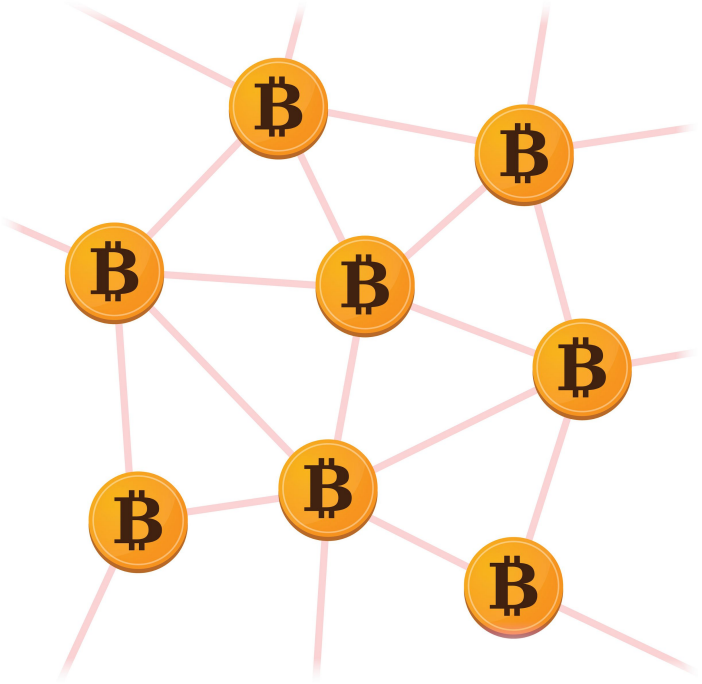


Elaine Shi
Cornell



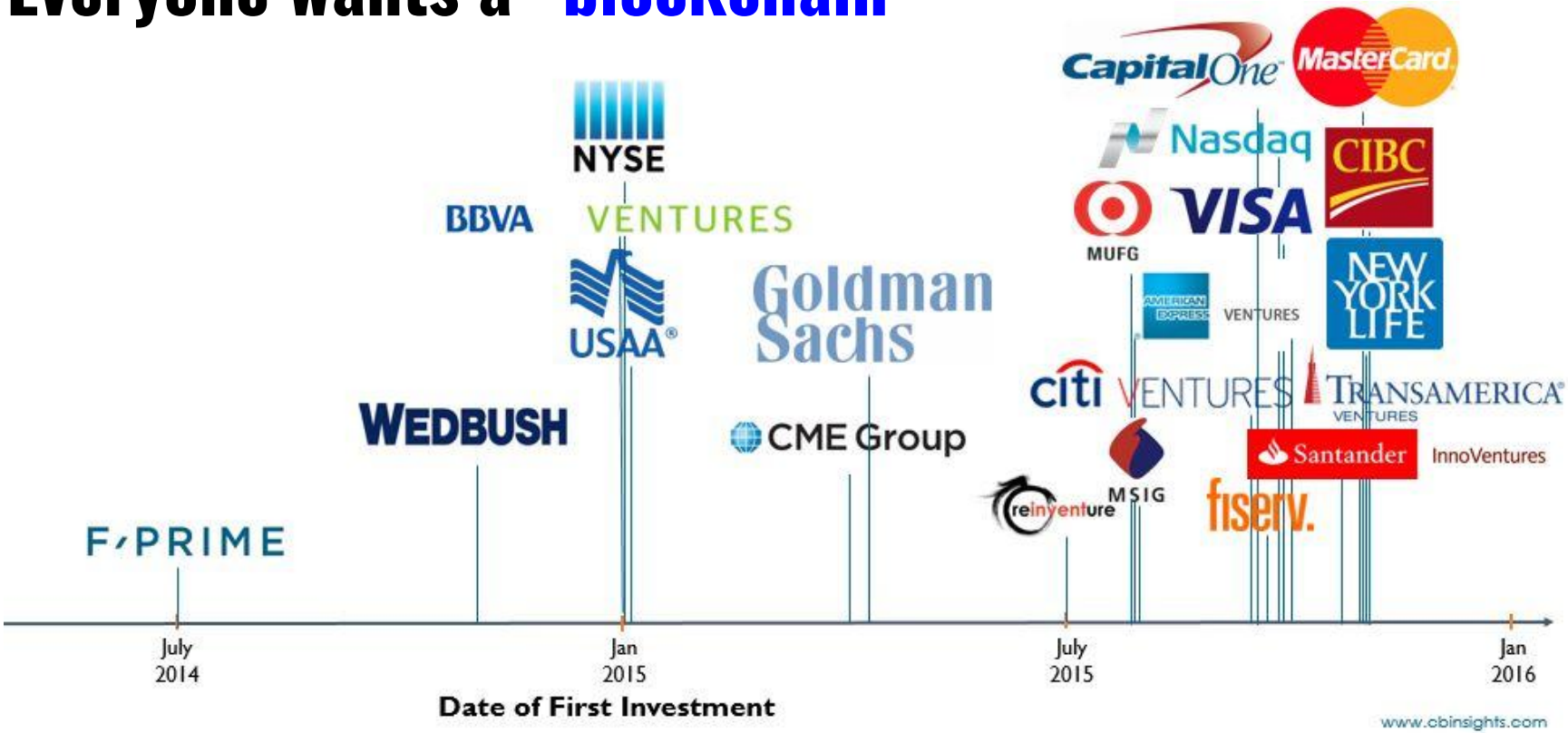
Bitcoin is the first successful decentralized digital currency

The Times 03/Jan/2009
Chancellor on brink of second bailout for banks.



Bitcoin has a **$140 Billion** market cap

Competition from Bitcoin has made waves in FinTech
Everyone wants a "blockchain"



And what is this “blockchain” thing?

This Talk

- Technical underpinnings of the “blockchain”
- Smart contracts in a nutshell
- Painpoints with today’s cryptocurrencies

Cryptocurrency Design: Bit by Bit

Jacob Leshno

Hong Wan

Facebuck $: a Centralized Digital Currency

Facebuck $: a Centralized Digital Currency

Facebuck $: a Centralized Digital Currency

Facebuck $: a Centralized Digital Currency

Pros / Cons of Facebuck $

Pros:

- Dirt simple!
  - (At least simpler than Facebook privacy settings)
- Fast transactions
- Facebuck can reverse transactions

Cons:

- Everyone loves (i.e., trusts) Facebuck!
- What if Facebuck gets hacked?

Towards Decentralized Cryptocurrency

Every user keeps track of Facebuck Wall locally

Jacob: $100
Hong: $200

Jacob: $100
Hong: $200

Jacob: $100
Hong: $200

Jacob: $100
Hong: $200

$50

Jacob: $50
Hong: $250

Jacob → Hong: $50

$50

Jacob: $50
Hong: $250

Jacob → Hong: $50

Jacob: $60
Hong: $250

Jacob → Hong: $50
Elaine → Jacob: $10

$50

Jacob: $60
Hong: $250

Jacob → Hong: $50
Elaine → Jacob: $10

Jacob: $60
Hong: $250

Jacob → Hong: $50
Elaine → Jacob: $10

Jacob: $60
Hong: $250

Jacob → Hong: $50
Elaine → Jacob: $10

If we lived in Honesty Land, everyone would be 

What happens in a world
not so perfect?

If we lived in Honesty Land,
everyone would be 

Jacob →Hong: $50
Elaine → Jacob: $10

Jacob →Hong: $50
Elaine → Jacob: $10

~~Jacob → Hong: $50~~
Elaine → Jacob: $10

Jacob →Hong: $50
Elaine → Jacob: $10

~~Jacob → Hong: $50~~
Elaine → Jacob: $10

Jacob →Hong: $50
Elaine → Jacob: $10

… but, remember, we academics are experienced at resolving disputes

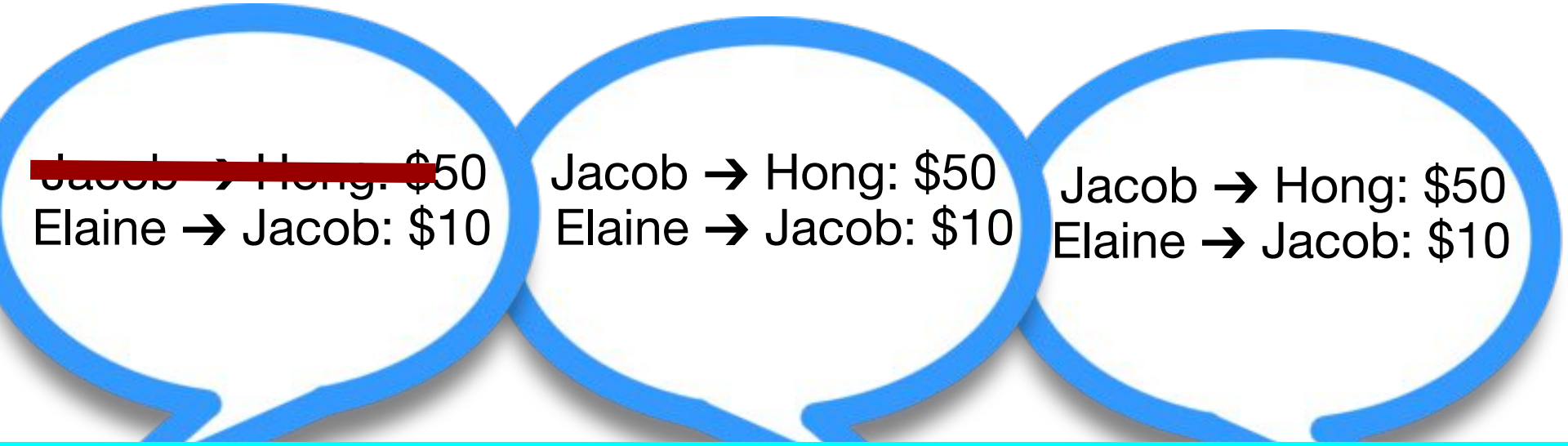
On 20 December 1973, the *Wall Street Journal* quoted Sayre as: "Academic politics is the most vicious and bitter form of politics, because the stakes are so low."

Let’s bring Elaine in, and do majority voting!

~~Jacob → Hong: $50~~
Elaine → Jacob: $10

Jacob → Hong: $50
Elaine → Jacob: $10

Jacob → Hong: $50
Elaine → Jacob: $10

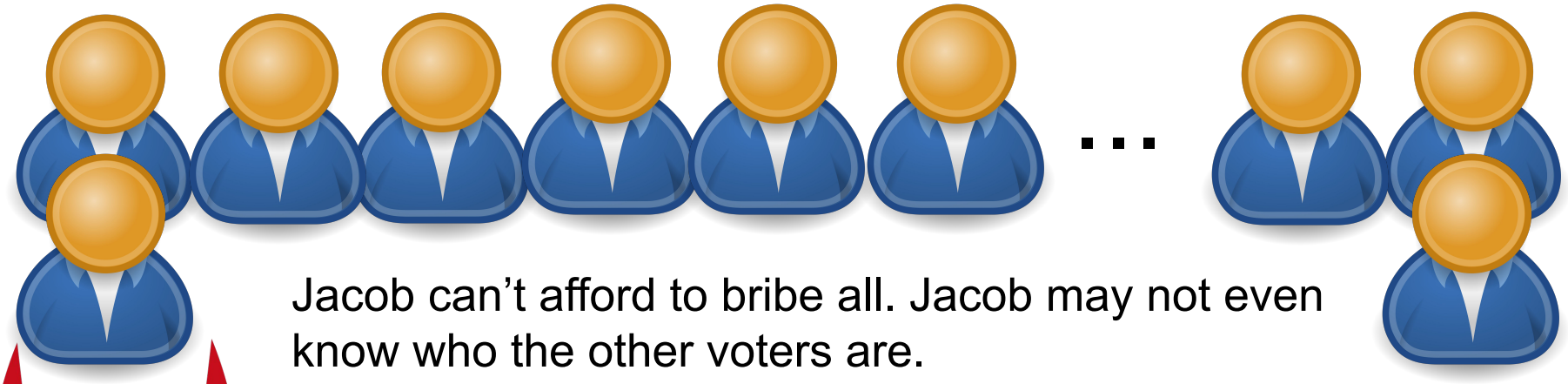


Brilliant idea! But need to jump through technical hoops to make it work!

Challenge 1: Bribery

Let me buy you a fancy dinner in Chicago

Idea: Have thousands of users on the Internet vote



Jacob can't afford to bribe all. Jacob may not even know who the other voters are.

Challenge 2

"On the Internet, nobody knows you're a dog."

Challenge 2: Attack of the Clones





...

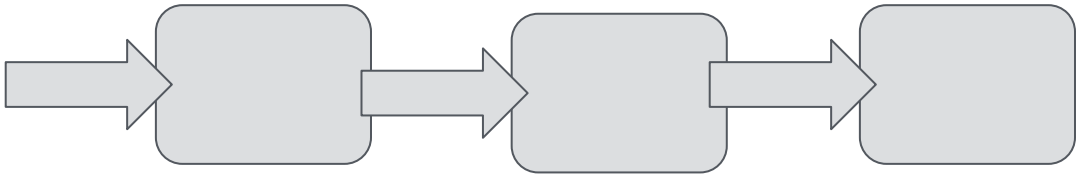

“All of your Internet is mine, hahaha.” -- [Jacob, and his wicked laugh]



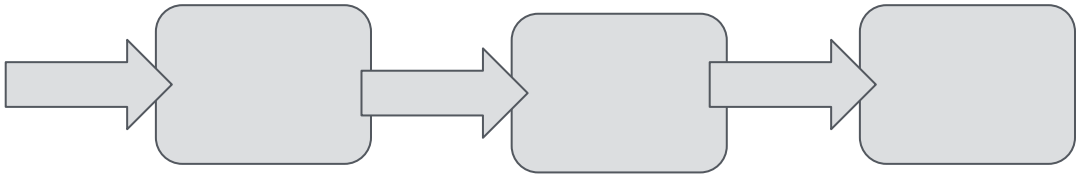
Idea: Proof-of-Work Puzzles

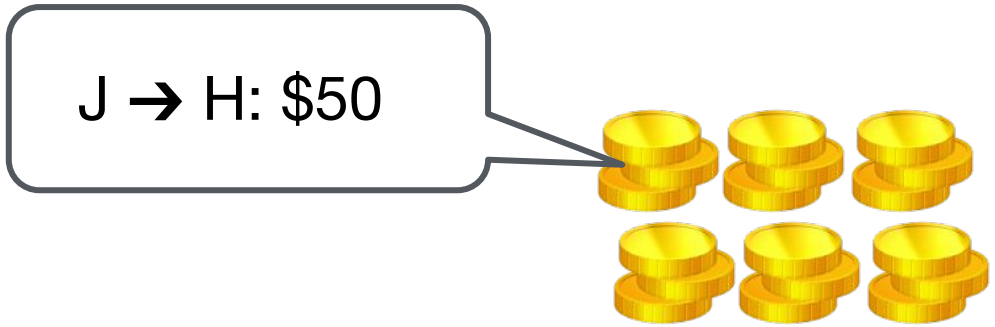
Users have to do work to cast votes.

work = **expend compute power**

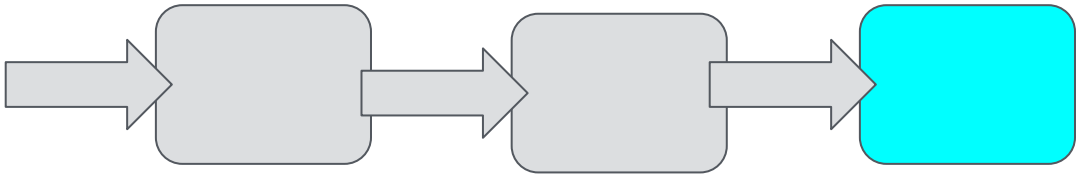


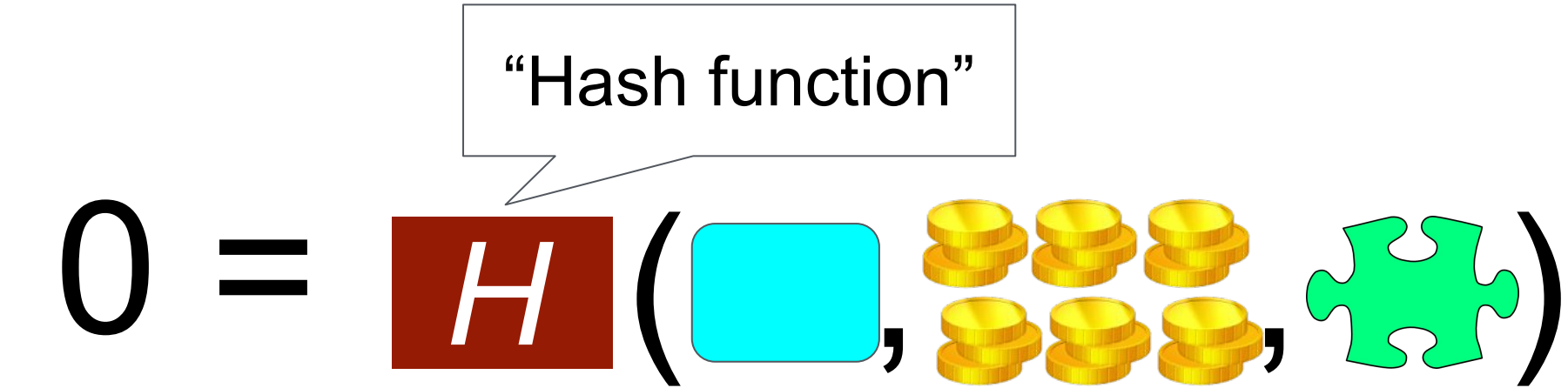
How to build a “blockchain”



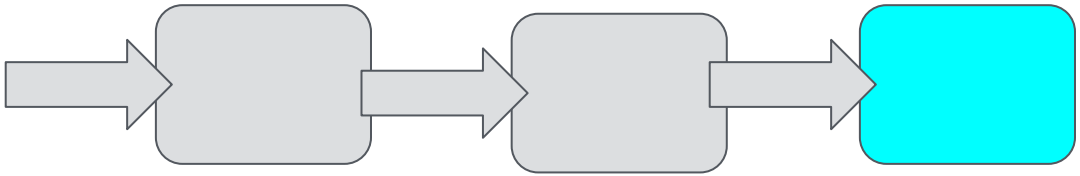


How to build a “blockchain”

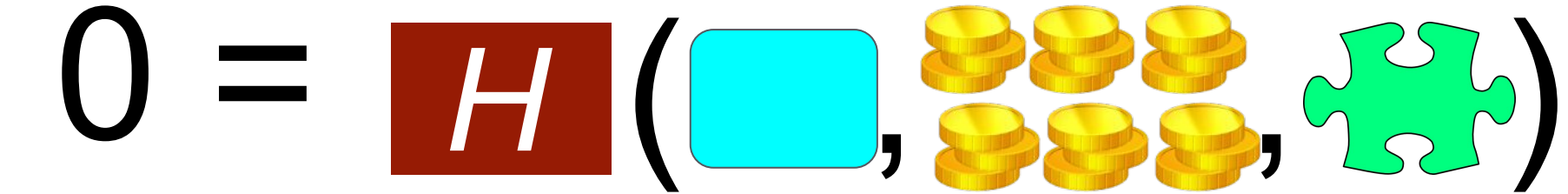




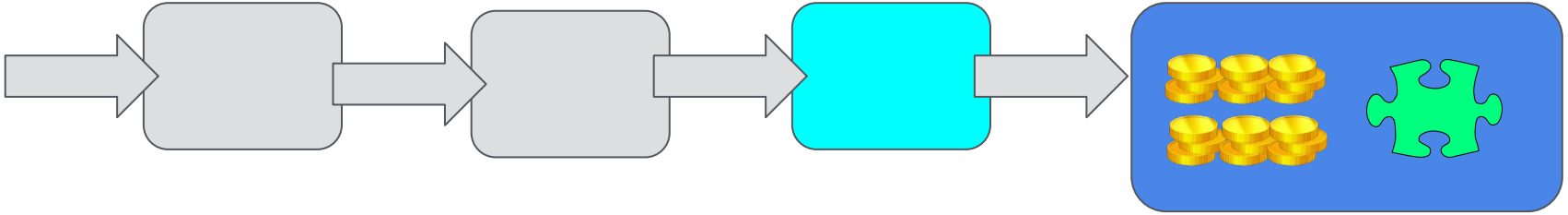
How to build a “blockchain”



puzzle solution



Search for a puzzle solution

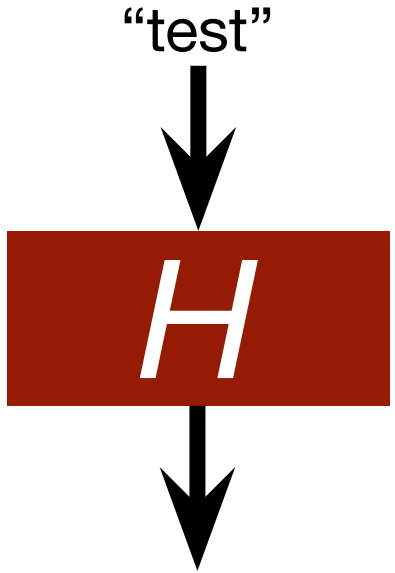


$$0 = H(\square, \text{coins}, \text{puzzle})$$

We found a new block

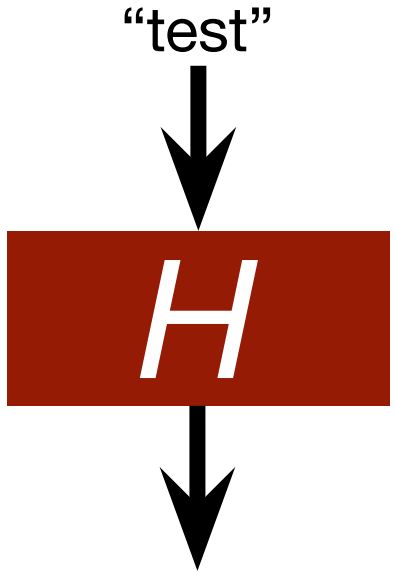
Hash function

- A *hash function H* is a deterministic cryptographic function
- *H* takes as input any desired bitstring / text *B*
- Outputs a *random*(-looking) fixed-size (256-bit) value *H*(*B*)



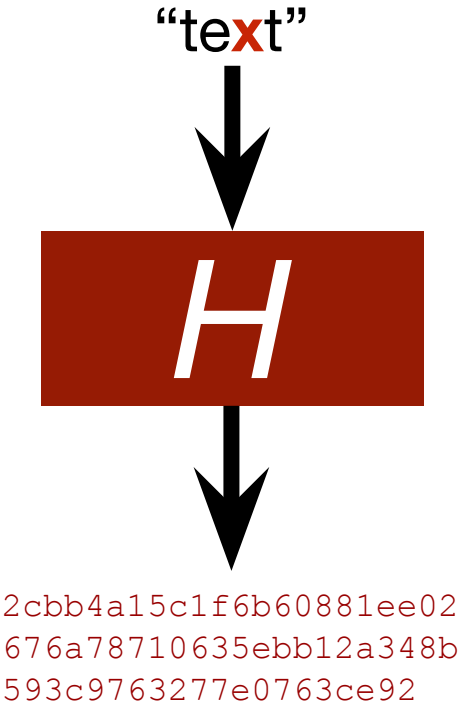
Hash function

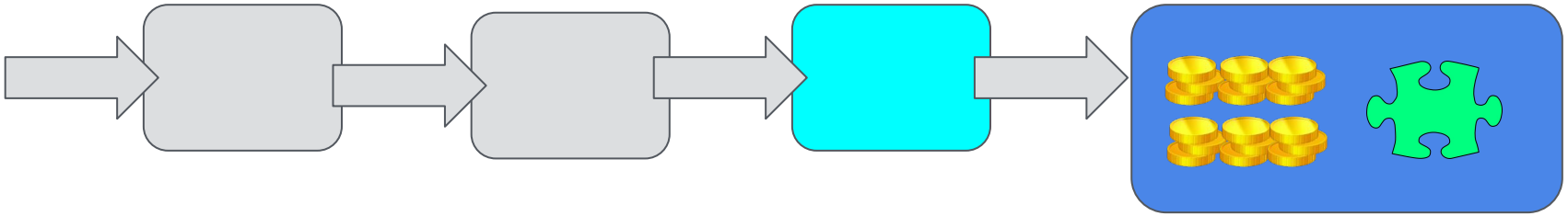
- Same input ***B*** **always produces same output**
- **Any *B'* ≠ *B* produces *completely different*, random-looking output *H*(*B'*)**

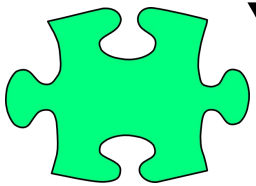


Hash function

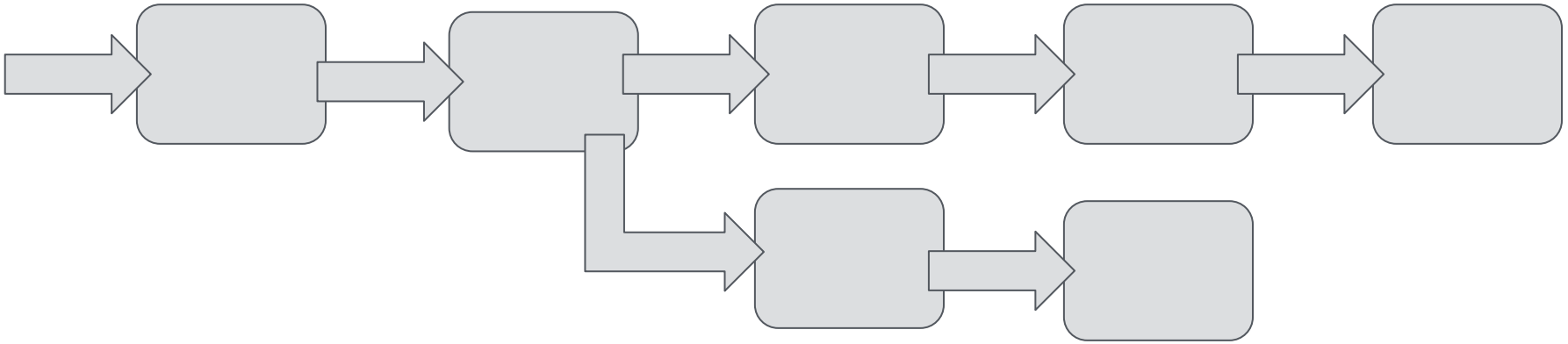
- Same input ***B*** **always produces same output**
- **Any *B'* ≠ *B* produces *completely different*, random-looking output *H*(*B'*)**



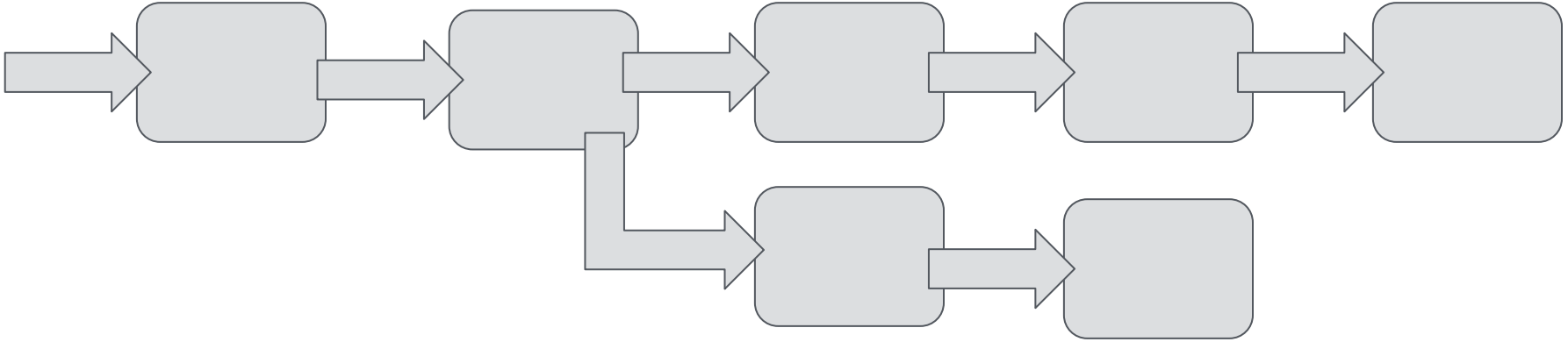


$$0 = H(\square, \text{  }, \text{  })$$

Best way to find a solution is brute-force search

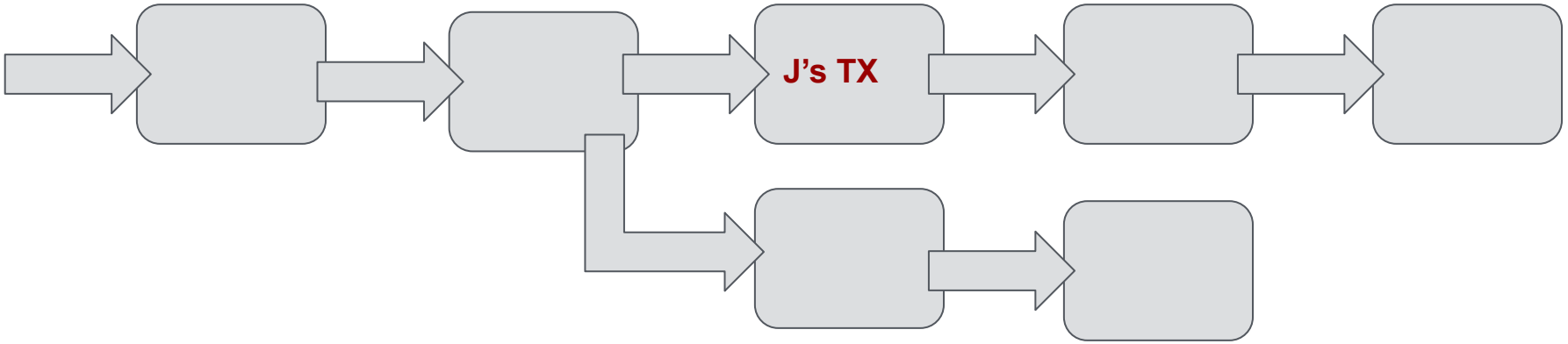


What if you join this “voting network” and you see this.

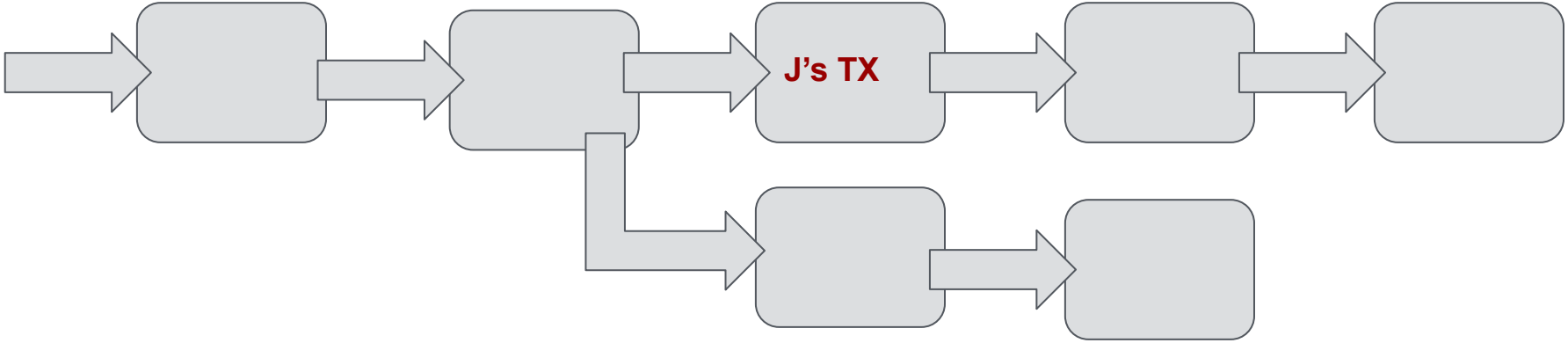


Honest nodes vote for the

“longest chain”



For Jacob to erase his transaction, he has to find a longer chain!



He cannot do this unless he has majority hashpower.

I’ve just told you how Bitcoin works!

Why should miners mine?

Whichever miner finds the new block first gets a reward

- Today, 12.5 Bitcoins (about $100,000)
- Miner also gets transaction fees, but these tend to be small

Recap: Bitcoin Core ideas

Decentralized Consensus

i.e., users agree on an ordered list of TXs

Recap: Bitcoin Core ideas

Decentralized Consensus

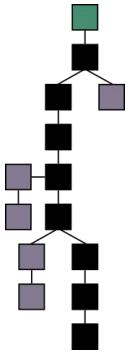
i.e., users agree on an ordered list of TXs

- Majority voting
- Proof-of-work
- 1 vote per hashpower

Recap: Bitcoin Core ideas

“The Blockchain”

i.e., users agree on an ordered list of TXs



- Majority voting
- Proof-of-work
- 1 vote per hashpower

Rest of the Talk

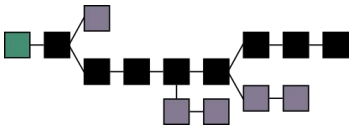
- Quick Introduction to Smart Contracts
- Painpoints Today

Bitcoin: “payment” system atop distributed consensus

payment

Decentralized Consensus

“Blockchain”

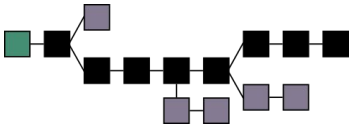


Beyond payments

General programs

Decentralized Consensus

"Blockchain"

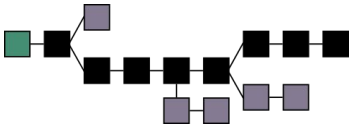


Smart contracts

General programs

Decentralized Consensus

“Blockchain”



Smart Contract Example: Flight Insurance

If you pay me $5 I will pay you $200 if your **“flight gets delayed or cancelled”**

“blockchain”
contract program

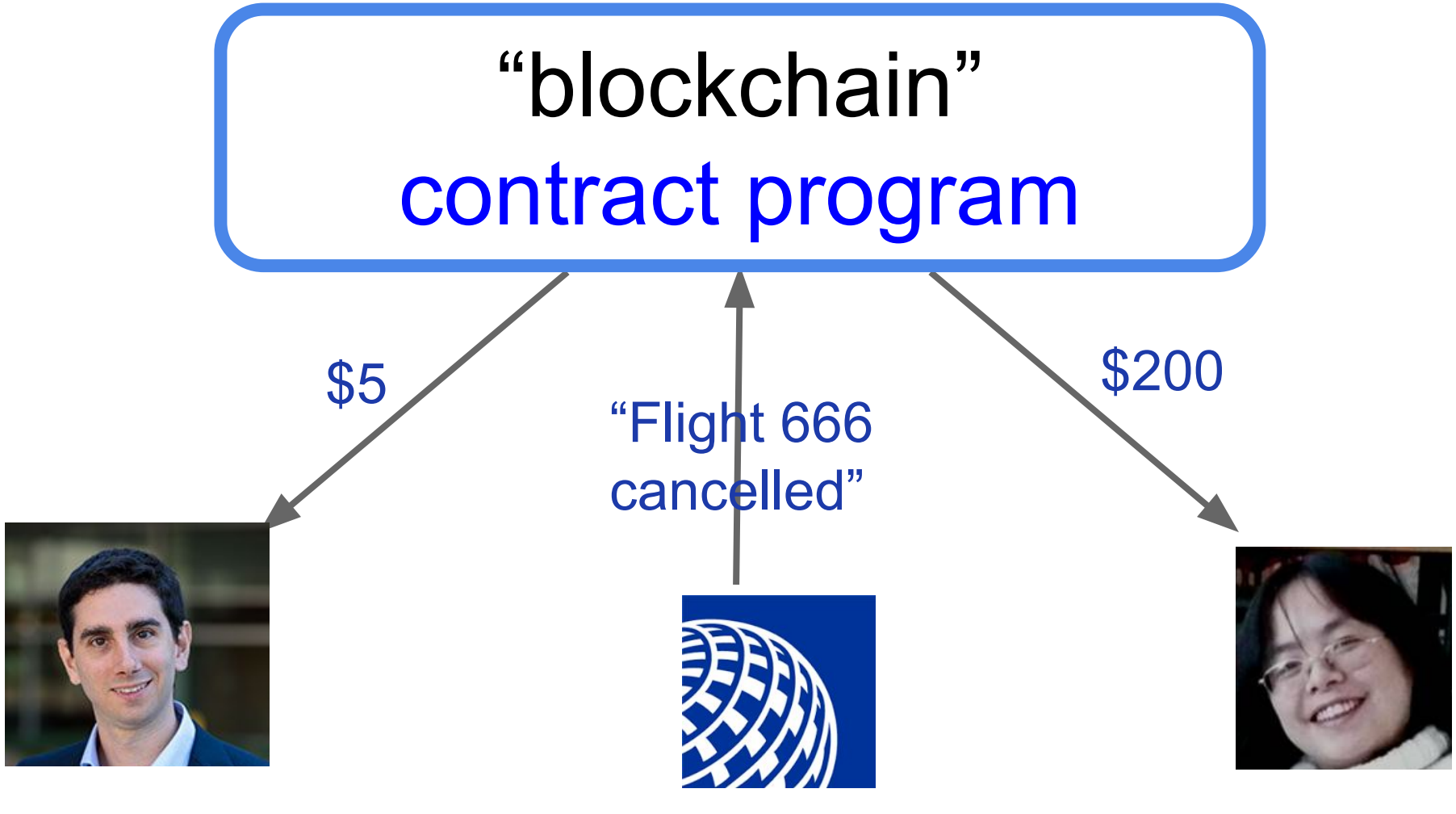
$200 collateral

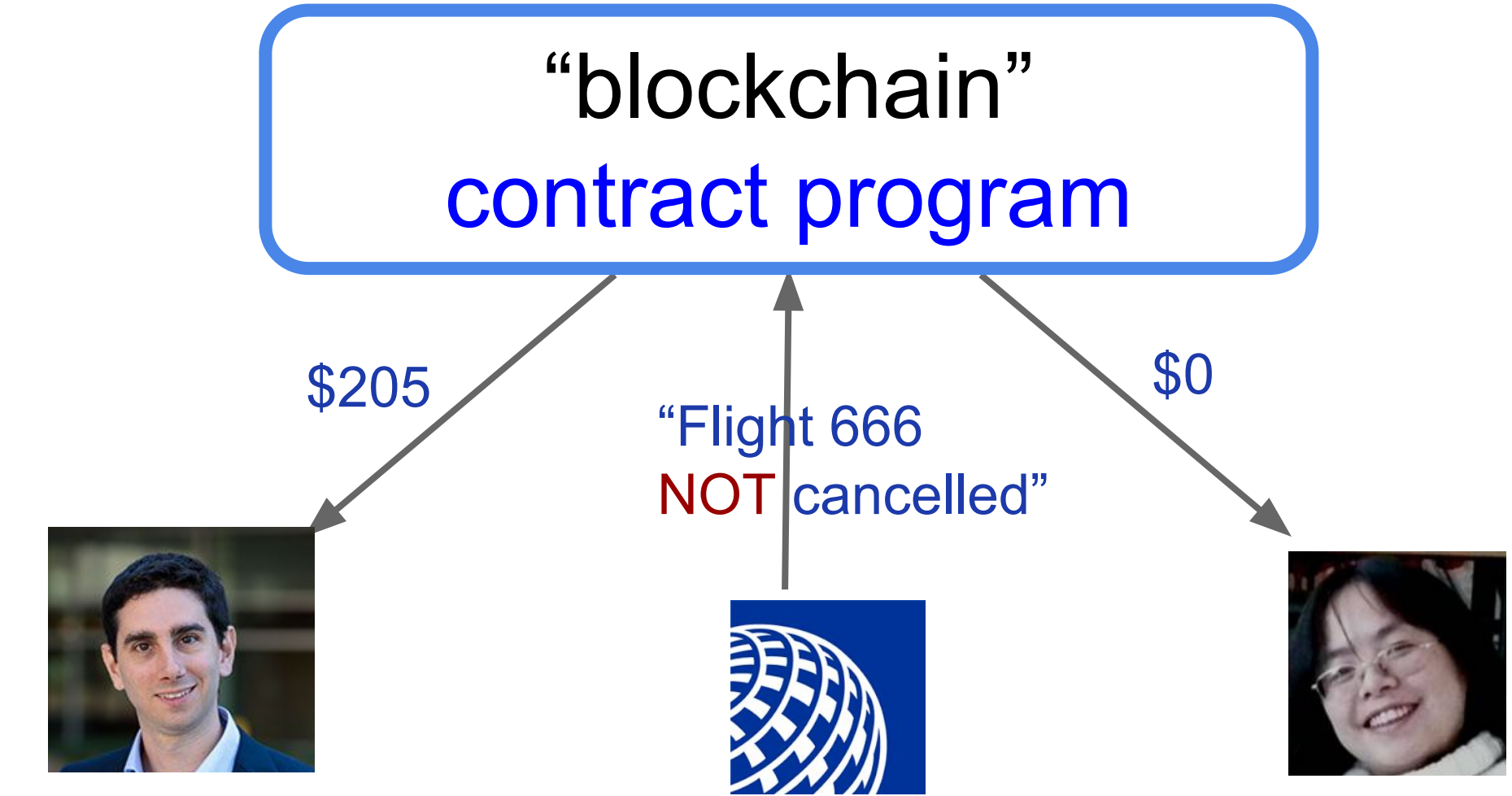
$5

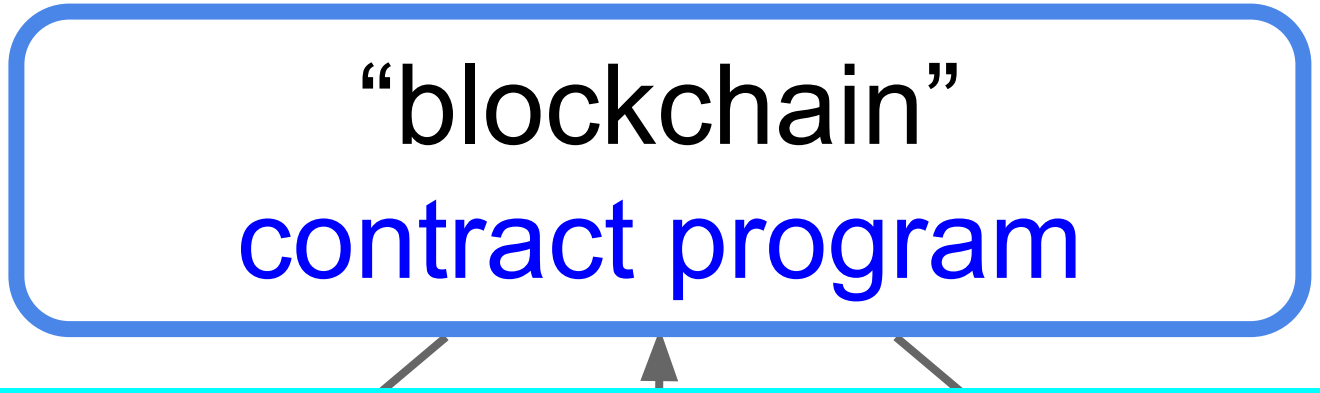
“blockchain”

contract program

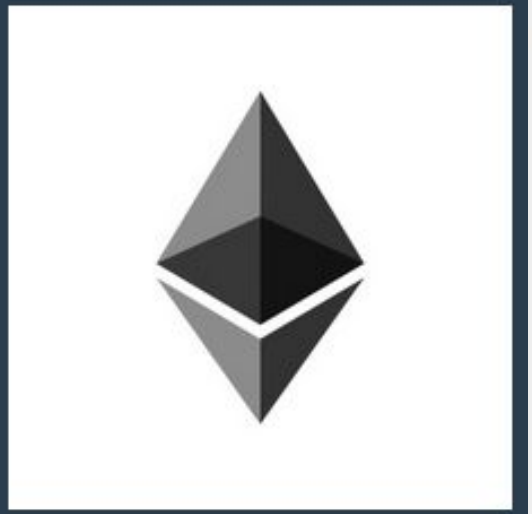
“Flight 666 cancelled”


"blockchain"
contract program
$5
"Flight 666 cancelled"
$200


"blockchain"
contract program
$205
"Flight 666
NOT cancelled"
$0



- Smart contracts run “on blockchains”
- Conceptually thought of a trusted party that enforces the contract



Ethereum

```
contract decentralisedAuction{
        struct auction {
                uint deadline;
                uint highestBid;
                address highestBidder;
                address recipient;
        }
        mapping(uint => auction) Auctions;
        uint numAuctions;

        function startAuction(uint timeLimit) returns
                auctionID = numAuctions++;
                Auctions[auctionID].deadline = block
                Auctions[auctionID].recipient = msg.
        }
        function bid(uint id) returns (address highe
                auction a = Auctions[id];
                if (a.highestBid + 1*10^18 > msg.val
```

Bitcoin: Today's Painpoints

and other problems...

Thank you!

elaine@cs.cornell.edu