Introduction to Blockchains and Bitcoin

CMSC 23200/33250, Winter 2023, Lecture 21

David Cash and Blase Ur

University of Chicago

This Lecture: Blockchains and Cryptocurrencies

1. How blockchains like Bitcoin work
2. Security of cryptocurrencies
3. Privacy of cryptocurrencies
4. Who benefits? Who is harmed?

The Bitcoin Story

- 2008: An anonymous paper and prototype posted
- 2008-2017: Bitcoin grows in popularity, reaching unbelievable highs
- Since: Even crazier highs and volatility

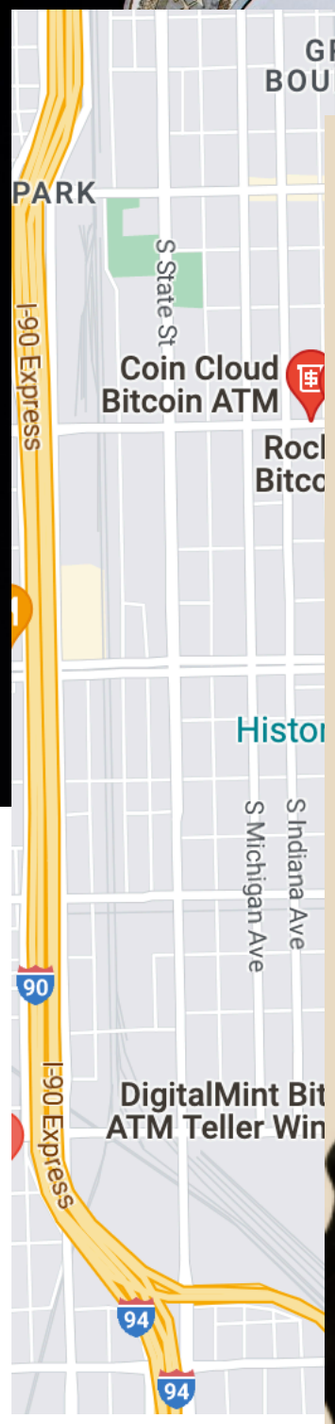
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin Price (in USD) Over Time

Cryptocurrencies Today



Early Cryptocurrency: ECash

BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use

STEVEN LEVY BUSINESS 12.01.94 12:00 PM

E-MONEY (THAT'S WHAT I WANT)

SHARE

92

The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's not only going to revolutionize the Net, it will change the global economy.

DigiCash Inc and ECash's Rise and Fall in the 1990s

(1994)

Attention Internet Shoppers: E-Cash Is Here

By PETER H. LEWIS

Special to The New York Times

CHICAGO, Oct. 18 — The first trials of an international electronic cash system will begin on Wednesday, with a bankroll of one million "cyber bucks" and several hundred volunteers eager to spend them, the system's developer said today.

Digicash Inc., which has offices in Menlo Park, Calif., and Amsterdam, hopes to establish its system as a standard for commercial transactions on the Internet, a global computer network that links millions of users. If the system proves workable in the trials, it is expected to begin commercial operations within months.

The development of an electronic cash system, which eventually would allow buyers and sellers to conduct commercial transactions entirely within the part of cyberspace known as the World Wide Web, is considered critical to the continued business growth of the Internet.

Using credit cards or other means of conventional currency transfer, a consumer would transfer a given amount of E-cash, as electronic cash is rapidly coming to be known, to his or her computer. Then, while shop-

Self-Service Air

By Bloomberg Business News

DAYTON, Ohio, Oct. 18 — AT&T Global Information Solutions and the Datamax Corporation have introduced self-service ticketing kiosks that allow travelers to get their tickets and boarding passes without

15 percent from the cost of each ticket by using the kiosks, Mr. Stellweg said.

To use the system, a customer would make travel arrangements as usual, through travel agents or di-

703 views | Nov 1, 1999, 12:00am

Requiem for a Bright Idea

Julie Pitta BRANDVOICE AdVoice

DAVID CHAUM SAVORED HIS first taste of success two years ago. A brilliant scientist whose specialty is cryptology, he started DigiCash in 1989 to create an on-line currency as secure and private as cash in the physical world. By 1997 he had lured venture backing, snagged the celebrated guru Nicholas Negroponte as chairman and signed a St. Louis bank as his first client. If the cashless society was imminent, he would be among the chief beneficiaries.

Today DigiCash is dead, and Ch

to get enough merchants to acce

to use it, or vice versa," he says.

"As the Web grew, the average level of sophistication of users dropped. It was hard to explain the importance of privacy to them."

— David Chaum, 1999

A Proto-Bitcoin: DCash, The Desert Island Currency

A Proto-Bitcoin: DCash, The Desert Island Currency

Initialization: Ben, Blase, and David all get `5 DCash coins`

TranID	From	To	Amount	
1	Ben	Blase	1	✓
2	David	Blase	2	✓
3	Ben	David	3	✓
4	Blase	David	6	✓
5	Ben	David	2	✗
…	…	…	…	

Transaction history implicitly represents how much money each person has.

Another Threat: Ledger Integrity Violations

TranID	From	To	Amount
1	Ben	Blase	1
2	David	Blase	2
~~3~~	~~Ben~~	~~David~~	~~3~~
4	Blase	David	6
5	Ben	David	1
6	**David**	**Ben**	**8**

Adding/deleting unauthorized transactions amounts to stealing money.

Minting DCash

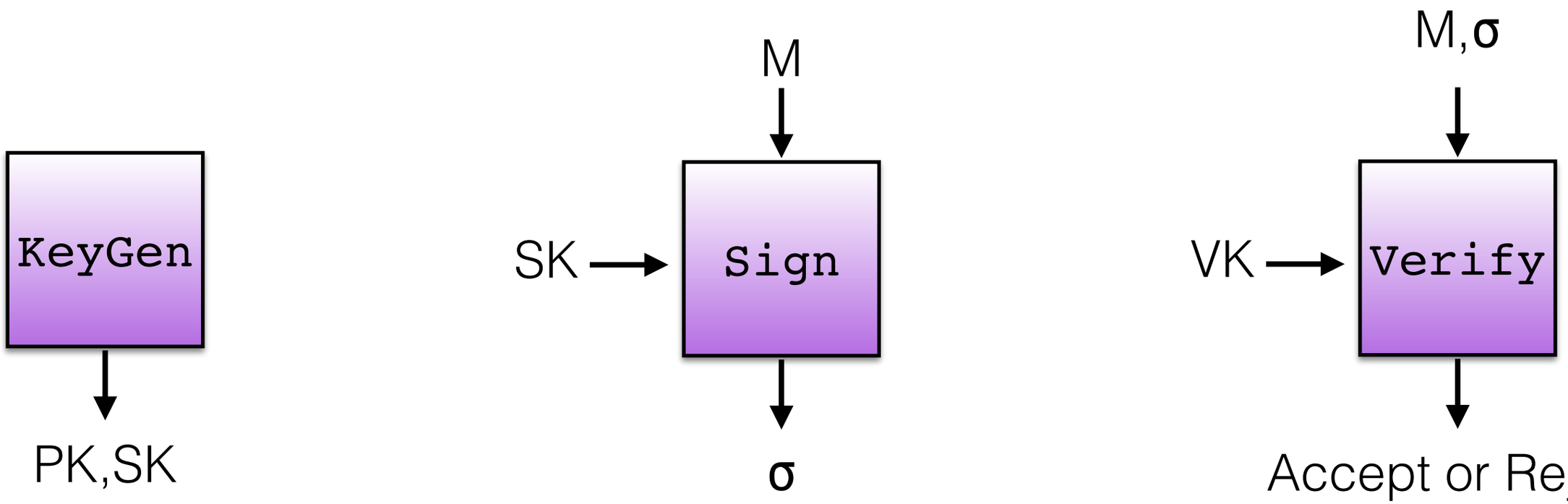
New DCash coins created via transactions with blank “From:”

TranID	From	To	Amount
1	Ben	Blase	1
2	David	Blase	2
3	Ben	David	3
4	Blase	David	6
5	Ben	David	1
6		Ben	1

Total supply of coins increases!

Digital Signatures Schemes (Review)

A digital signature scheme consists of three algorithms **`KeyGen`**, **`Sign`**, and **`Verify`**



`KeyGen`: Outputs two keys. PK published openly, and SK kept secret.

`Sign`: Uses SK to produce a "signature" σ on M.

`Verify`: Uses VK to check if signature σ is valid for M.

Digital Signatures for More Secure & Private Ledgers

Initialization: Ben, Blase, and David all generate keys for digital signatures

David's verification key: VK_{david} = 5e7843…
Ben's verification key: VK_{ben} = 88f01e…
Blase's verification key: VK_{blase} = 16823a…

Ben signs transaction row

TranID	From	To	Amount	Signature
1	88f01e…	16823a…	1	91a001…
2	5e7843…	16823a…	2	2c3118…
3	88f01e…	5e7843…	3	7623a6…
4	16823a…	5e7843…	6	987234…
5	88f01e…	5e7843…	1	234b98…

Digital Signatures for More Secure & Private Ledgers

Initialization: Ben, Blase, and David all generate keys for digital signatures

David's verification key: VK_{david} = `5e7843…`
Ben's verification key: VK_{ben} = `88f01e…`
Blase's verification key: VK_{blase} = `16823a…`

David signs transaction row, *plus* entire history (prevents reordering)

TranID	From	To	Amount	
1	88f01e…	16823a…	1	91001…
2	5e7843…	16823a…	2	2c3118…
3	88f01e…	5e7843…	3	7623a6…
4	16823a…	5e7843…	6	987234…
5	88f01e…	5e7843…	1	234b98…

Digital Signatures for More Secure & Private Ledgers

Initialization: Ben, Blase, and David all generate keys for digital signatures

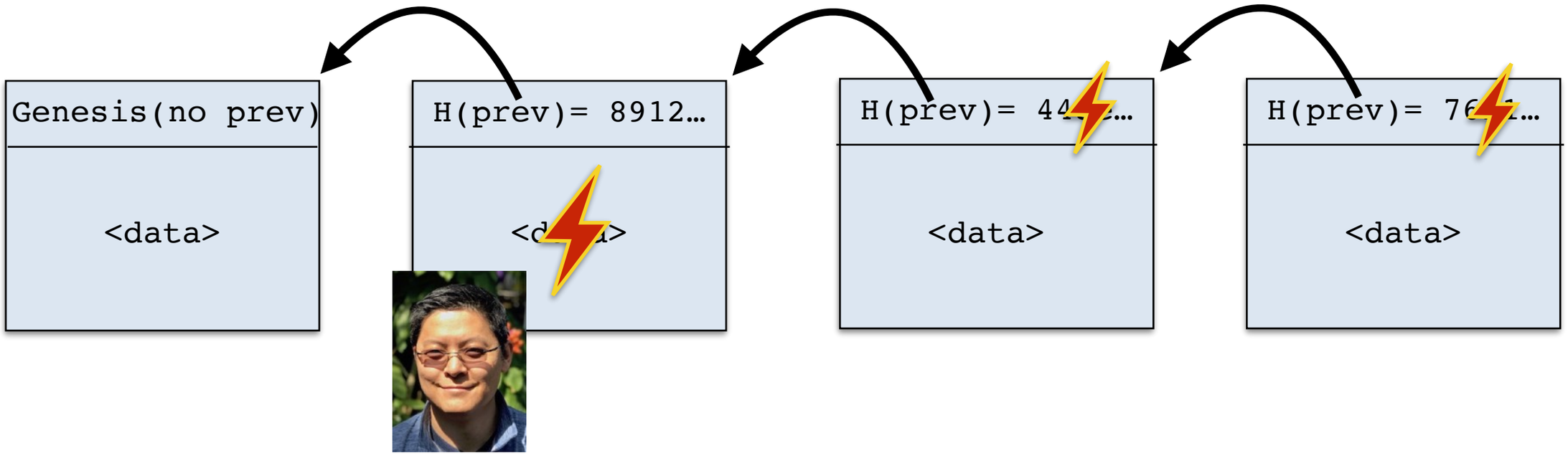
David's verification key: VK_{david} = 5e7843…
Ben's verification key: VK_{ben} = 88f01e…
Blase's verification key: VK_{blase} = 16823a…

TranID	From	To	Amount	Signature
1	88f01e…	16823a…	1	91a001…
2	5e7843…	16823a…	2	2c3118…
3	88f01e…	5e7843…	3	7623a6…
4	16823a…	5e7843…	6	987234…
5	88f01e…	5e7843…	1	234b98…

- Transactions can be added by anyone since signatures can be checked
- Anonymous… sort of

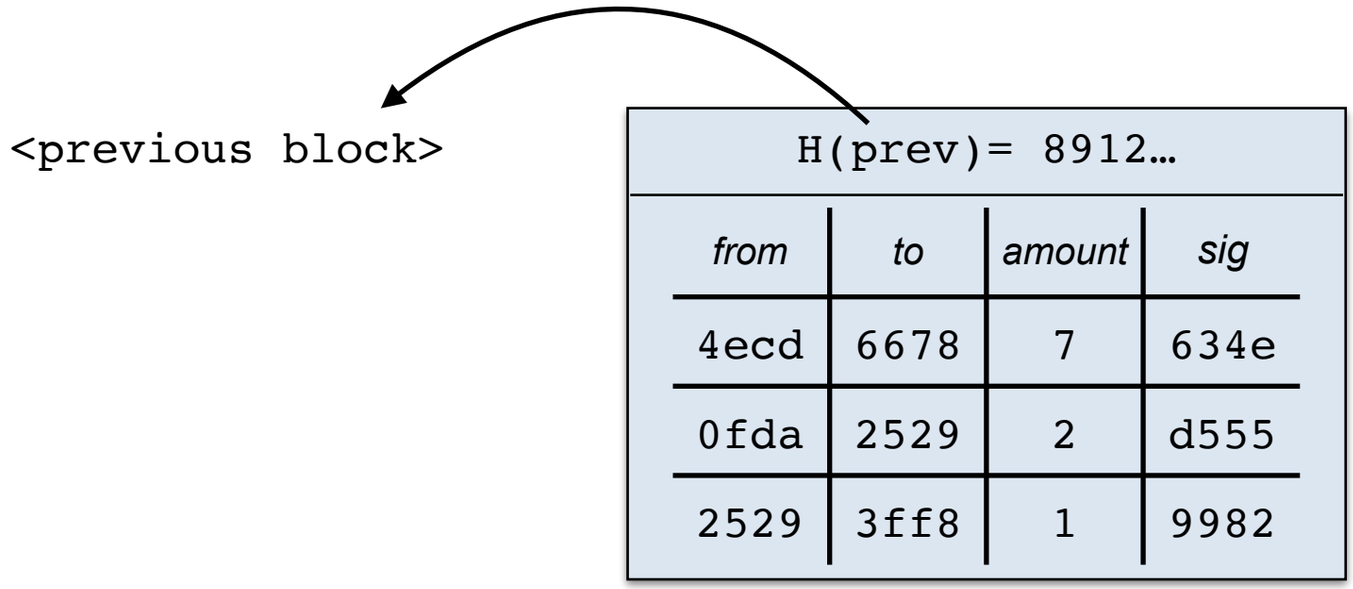
Tool for Distributed Ledgers: Blockchains

- Suppose <data> are divided in blocks



- Can add blocks easily — Just hash prev.
- If we know the last hash (`7612…`) then we can if data was changed in any prior block.
- That's it! The big insight is in how to use blockchains.

Moving DCash “To the Blockchain”: Block Data Format



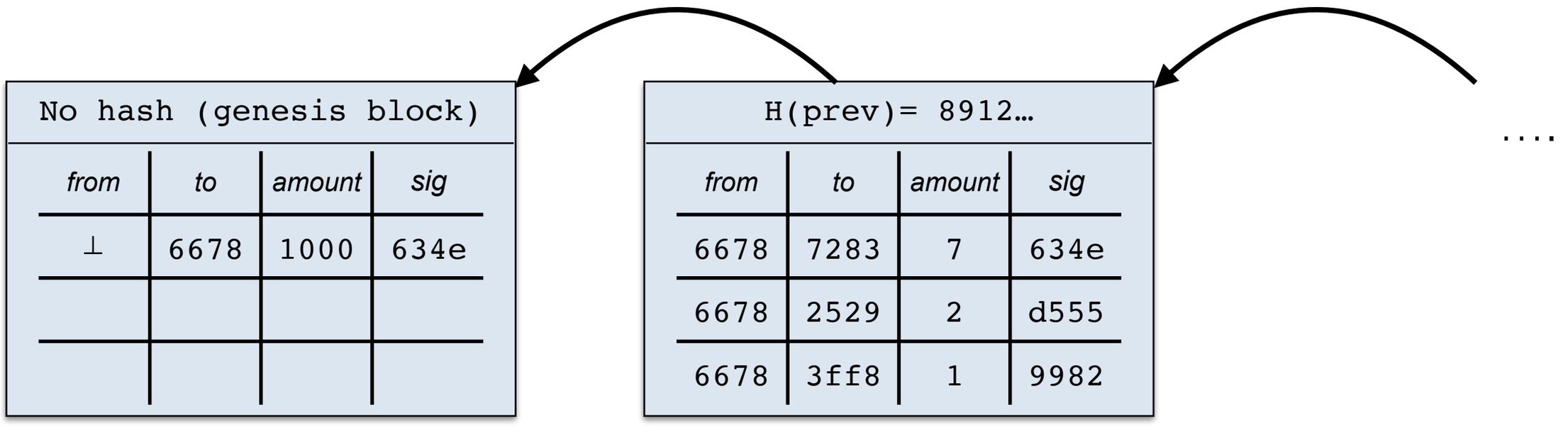
Moving DCash "To the Blockchain": The Details

Initialization:

- Step one: Choose an authority to manage chain. I choose me.
- Step two: Create genesis block that creates coins via sender-less transactions

Operation thereafter:

- Everyone sends signed transactions to authority, until block is full
- When block is full, authority publishes next block
- Everyone can check validity of transactions (signed + account balances)



DCash with an Angel instead of an Authority

Hypothetical operation:

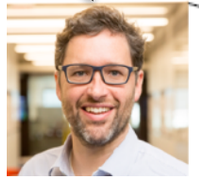
- Everyone broadcasts signed transactions to P2P network, which rebroadcasts
- Every so often, an angel randomly picks someone to be leader for the block
- That leader adds block (decides which transactions are included)
- Everyone checks validity of new block of transactions (signed + acct balances)

Broadcast:

H(prev)= 8912…

from	*to*	*amount*	*sig*
5742	ec73	1	8675
6678	7283	7	634e

Broadcast:
5742→ec73, amt:1, sig:8675



Broadcast:
6678→7283, amt:7, sig:634e

Tool to Implement the Angel: Proofs of Work

- Proof of Work: A problem that is fairly hard to solve, but not *too* hard.
- Uses a cryptographic hash function `H` (e.g. `SHA256`)

Hardness parameter: Integer `k`
Input: string `X`
Output: string `C` such that `H(X,C)` starts with `k` zeros

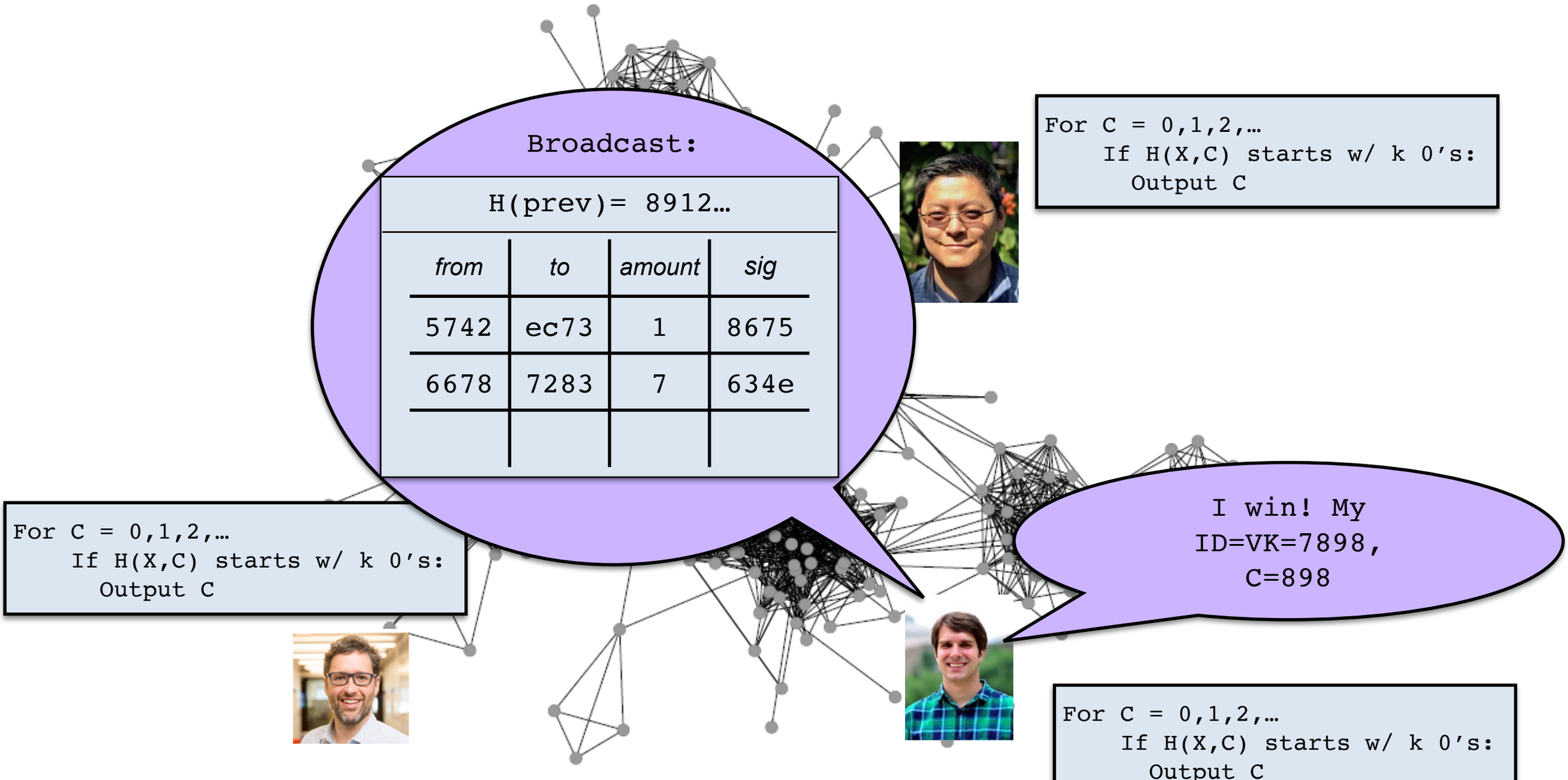
Canonical algorithm: On input `X`:

```
For C = 0,1,2,…
  If H(X,C) starts with k zeros:
    Output C
```

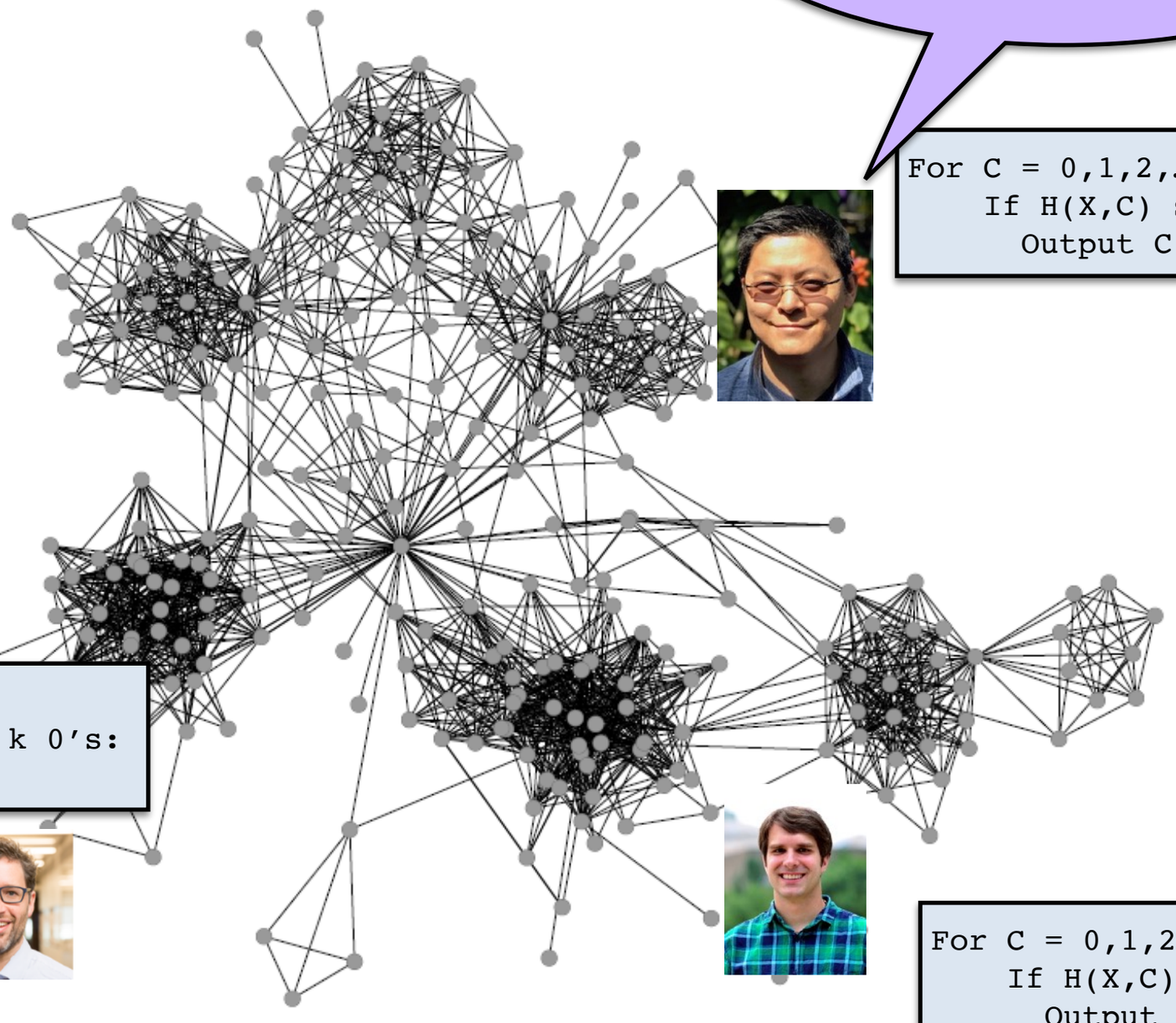
- With a secure hash function, best algorithm is the canonical algorithm
- Canonical algorithm evaluates hash 2^k times on average

Proofs of Work with Blockchains

- Everyone agrees on value of `h = H(latest-blk)`
- Each person concats `h` and their `ID` to form `X`: `X = h||ID`
- Each person tries to solve POW with their `X`
- First to solve is the leader, and adds block



But why do the POWs?

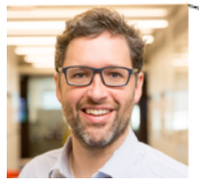


This POW is slowing down my computer… I'll let the others do the work….

```
For C = 0,1,2,…
    If H(X,C) starts w/ k 0's:
      Output C
```



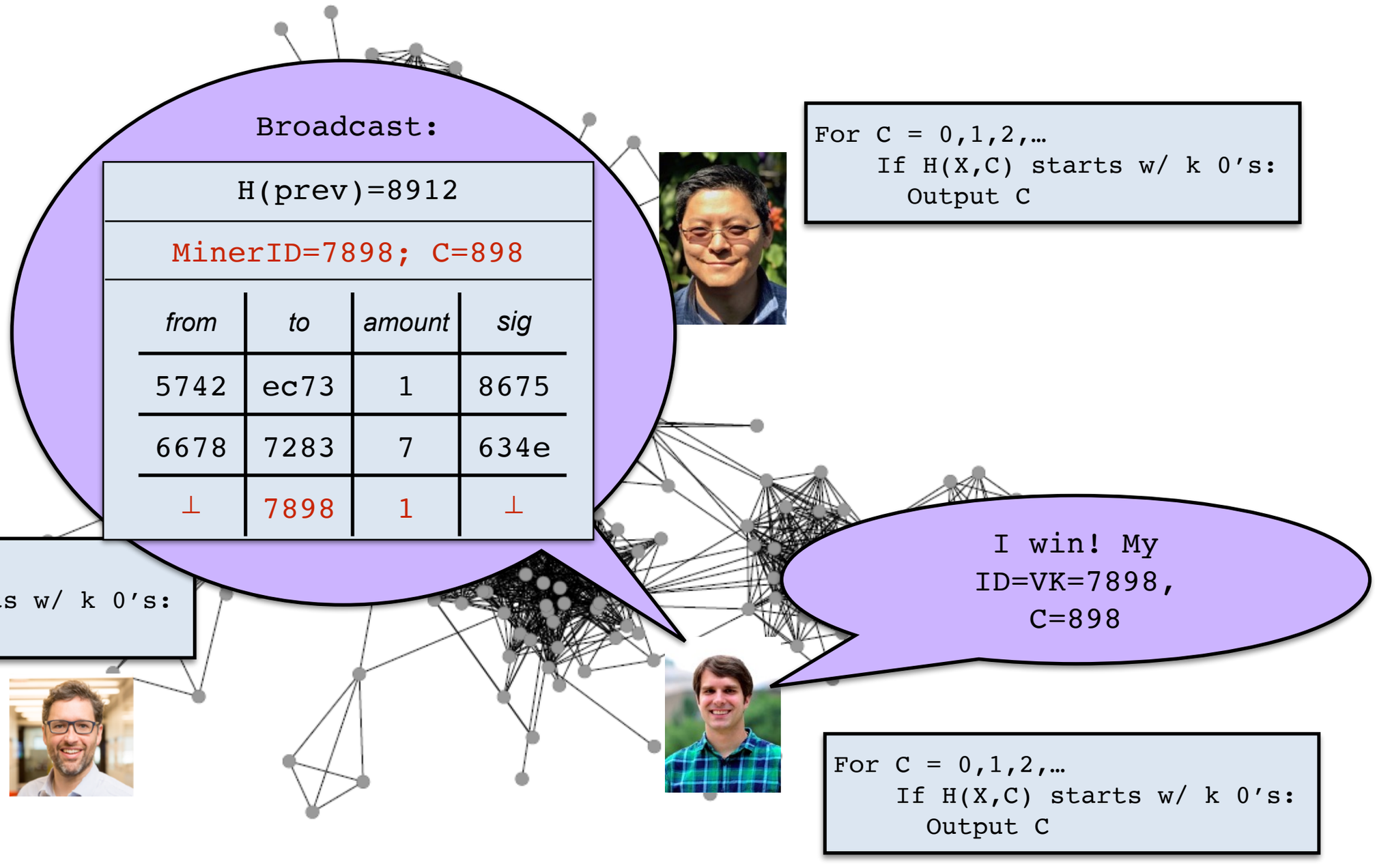
```
For C = 0,1,2,…
    If H(X,C) starts w/ k 0's:
      Output C
```




```
For C = 0,1,2,…
    If H(X,C) starts w/ k 0's:
      Output C
```

Incentivizing POWs for the Blockchain

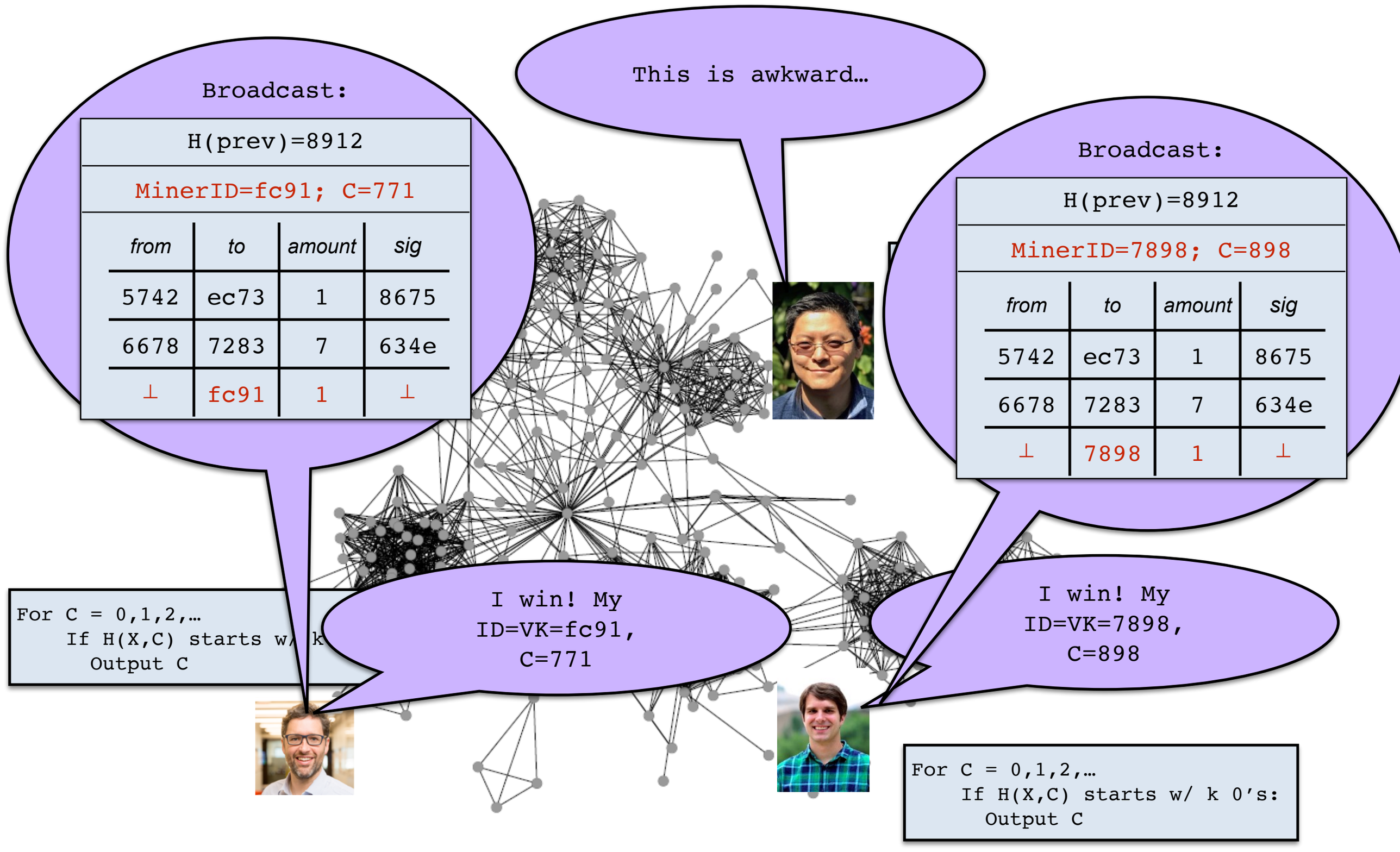
- Pay the winner, in the form of newly-minted coins
- This is called “mining”
- Also: Transactions include tips for whoever mines block



The DCash Blockchain, So Far

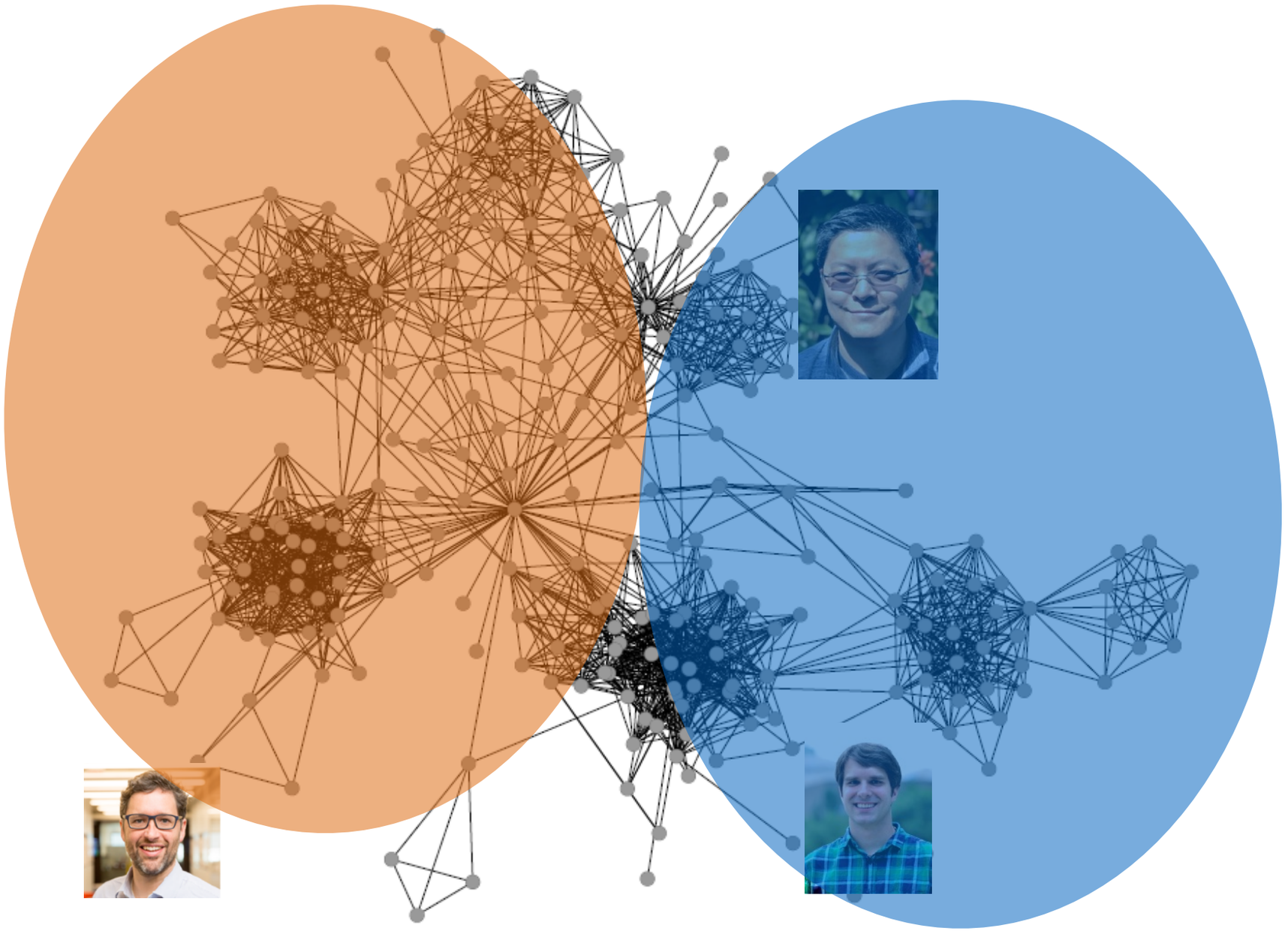
1. Digital version of ledger; Accounts defined by history
2. Genesis block gave chosen group a pile of coins
3. Transactions signed by senders, aggregated into blocks
4. Blocks added by whoever wins POW game
5. Participants incentivized via mining

Forking in the Blockchain



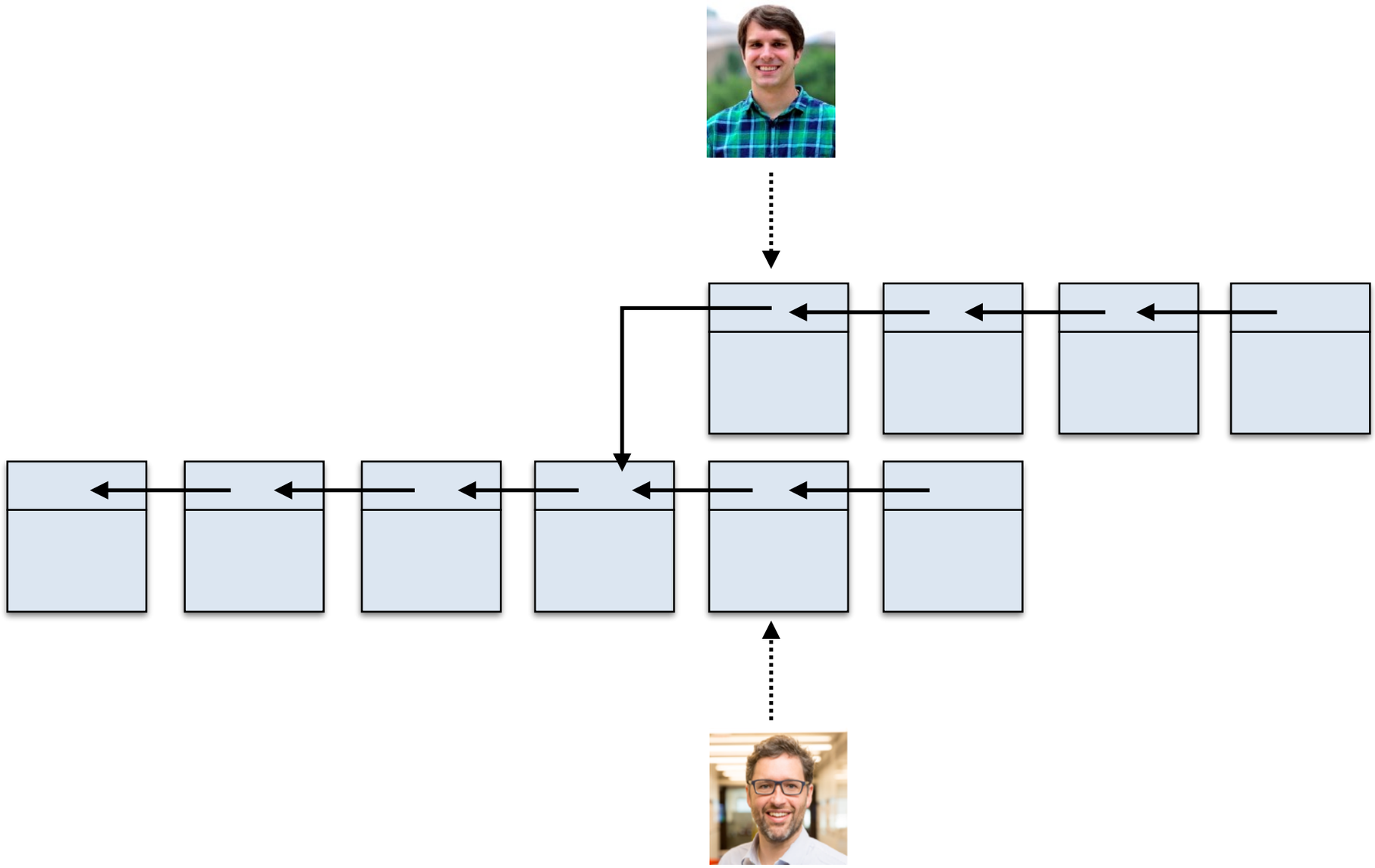
Forking in the Blockchain

- Other parties accept whichever block they hear about first
- … But parts of the network will accept different blocks



Forking in the Blockchain

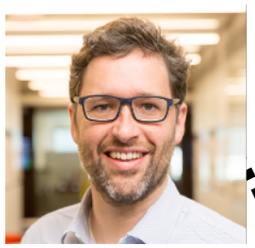
- Blockchain network is in a “forked” state



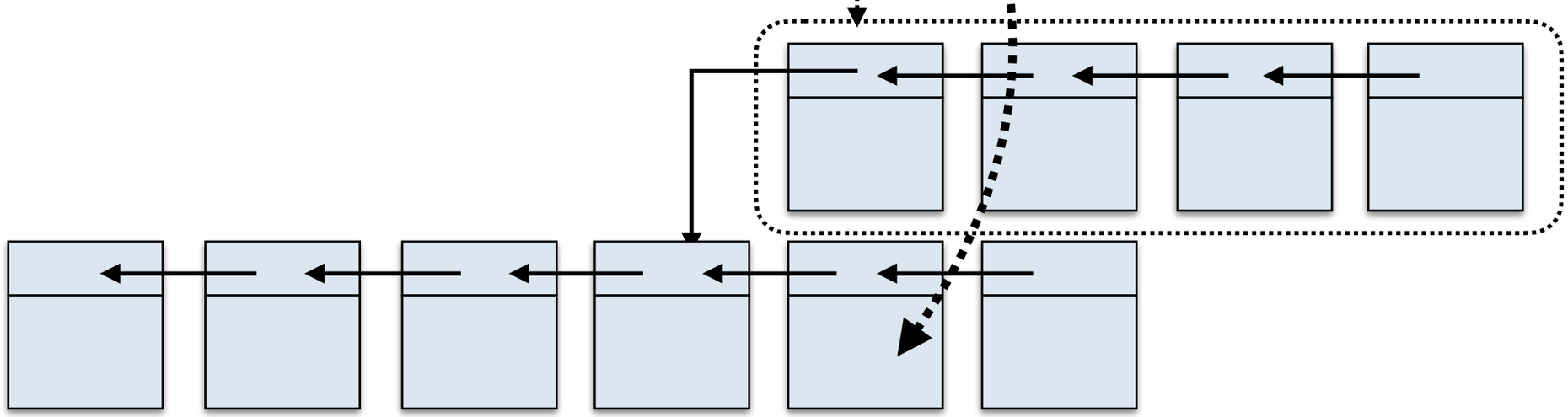
- Resolution: Any node will switch to the longest chain it has seen

Implication: The Power to Re-write History

- Suppose one party (David) can mine faster than the rest of the network



Step 1: Buy bananas from Blase on main fork.
Step 2: Eat bananas.
Step 3: Mine a fork longer than main fork. Omit banana transaction.
Step 4: Announce longer fork, switching network.



- When network switches to my fork, the banana transaction disappears.
- Free bananas! (Sorry Blase, see Step 2)

By some theories, such an attack requires 51% of total compute power.
This has been disputed (both higher and lower).

Bitcoin Gold Suffers a 51% Attack, Leads to Double Spend Problem

by Aradhana S. | 2 minutes read | Jan 30

Story from **Markets** →

Why Exchanges List Small-Cap Coins Despite 51% Attacks

Feb 11, 2020 at 20:30 UTC ▪ Updated Feb 11, 2020 at 21:07 UTC

Blockchain Mining

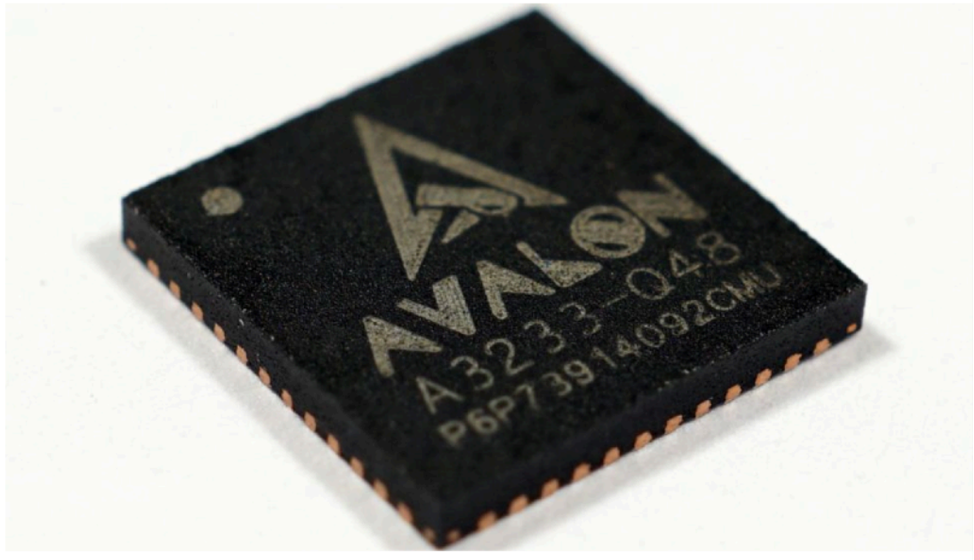
- Current reward for mining a block is: About $150,000 (6.25 BTC)
- POW hardness adjusted to control transaction rate
- Most compute power is in “Mining Pools”
- Currently, Bitcoin mining uses amount of electricity similar to the entire country of Bangladesh (by one estimate)

News > Best ASIC devices for Bitcoin mining in 2018

Best ASIC devices for Bitcoin mining in 2018

By Nate Drake July 11, 2018 Internet

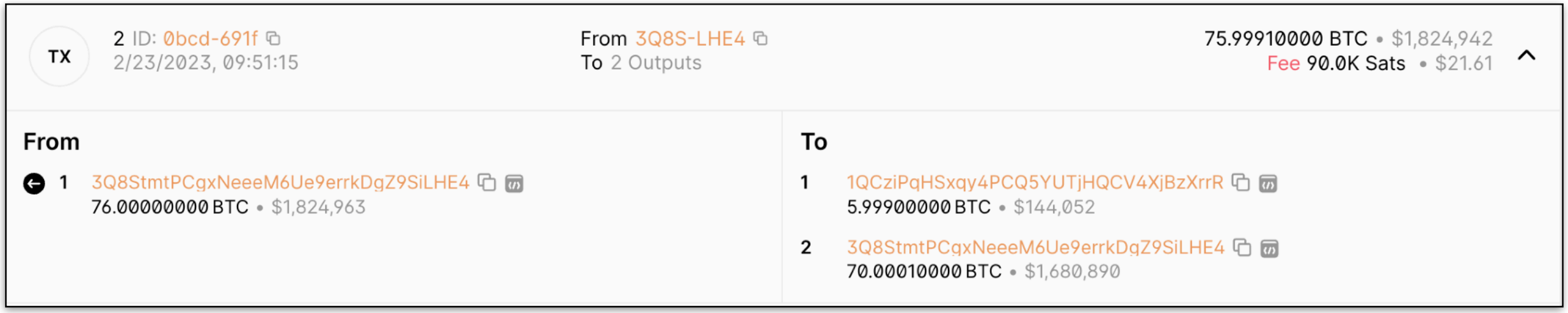
Mine like a pro with the latest ASIC hardware



If you want to get started with mining your own Bitcoin (BTC), these days you need ASIC (application-specific integrated circuit) devices, which are specifically built for the purpose.

One major omitted detail: Bitcoin Transactions

- My description of transactions is correct in spirit, but highly inefficient
  - How to check if transaction is valid? (Re-run entire history!)
- Blockchains actually tie transactions to specific previous transactions
- Each transaction takes an input one or more “unspent transaction outputs” (UTXOs), and produces one more UTXOs




bitcoin
Free Home & Business Heating
Mobile App Development
Cyber Security
1923
271

Zcash: Privacy via Zero-Knowledge Proofs

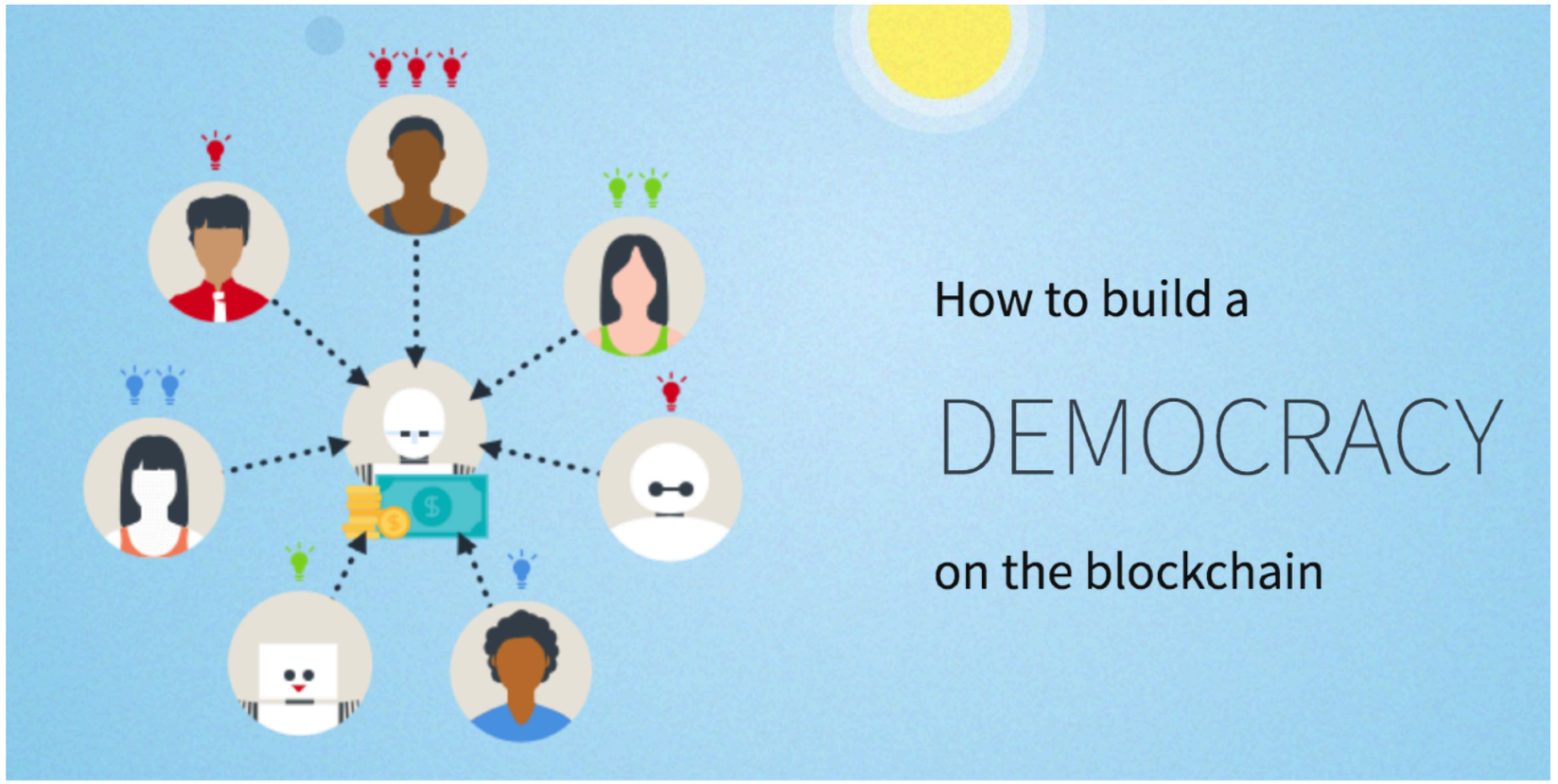
- If you can connect a Bitcoin public key to a person, then you can see their entire transaction history
- Zcash is an altcoin that addresses this:
  - When adding a block, network doesn't depend on blockchain history to check validity
  - Instead, you give a zero-knowledge proof that your transaction is valid, without revealing why

Ethereum and “Smart Contracts”

- In a simple blockchain, “Transactions” are just transfer amounts
- But instead one include scripts in “Transactions”, for example:
  - “Transfer 2 to Ben on Jan 1, 2019”
  - “Transfer 3 to Blase if the temperature is above freezing tomorrow”
  - “Transfer 1 to David if he sends software with hash=h to Ben by tonight”
- Blockchain history is still verifiable, so script rules are enforced by network.

The Ethereum DAO

- Smartcontracts are code. They take inputs and produce outputs.
- Smartcontracts are “authoritative”: Their output is correct by definition.
- What could go wrong?



- “The DAO” is a smart contract that allows transfers into a fund, and then voting for how to invest the fund

The DAO Hack

Haseeb Qureshi Follow

GP at MetaStable Capital. @Airbnb, @earndotcom alum. Instructor @BradfieldCS. Writer. Effective Altruist. Former poker pro. One always finds one's burden again.

Jul 20, 2017 · 16 min read

A hacker stole $31M of Ether—how it happened, and what it means for Ethereum

- Bug in the smartcontract code allowed hacker to transfer money out
- Hacker would have stolen more, but whitehats noticed and also exploited flaw, saving around $150M more from being stolen

The Fork (July 2016)

- Solution: Introduce a new smartcontract that undoes the theft, and get everyone to choose the fork including this smartcontract.
- Not allowed under the original rules; Some (10%) voted against the fork.
- Arguably undermines the point of smartcontracts (i.e. “Code is law.”)

ethereum

ethereum

$1640 USD

ethereum classic

$22 USD

Other Application of Bitcoin: Ransomware

BITCOIN CRIME AUGUST 02, 2018 07:45 CET

SamSam Ransomware Makers Rake in $6 Million in Bitcoin: Research

Other Application of Bitcoin: Buying Drugs

- Silk Road was online market for drugs and other illegal products
- Shut down in 2013, owner convicted and given life sentence
- Bitcoins confiscated by FBI and auctioned off for $48M (worth $614M today)

The End