Introduction to Cryptocurrencies

CMSC 23200/33250, Autumn 2018, Lecture 25

David Cash, Blase Ur, Ben Zhao

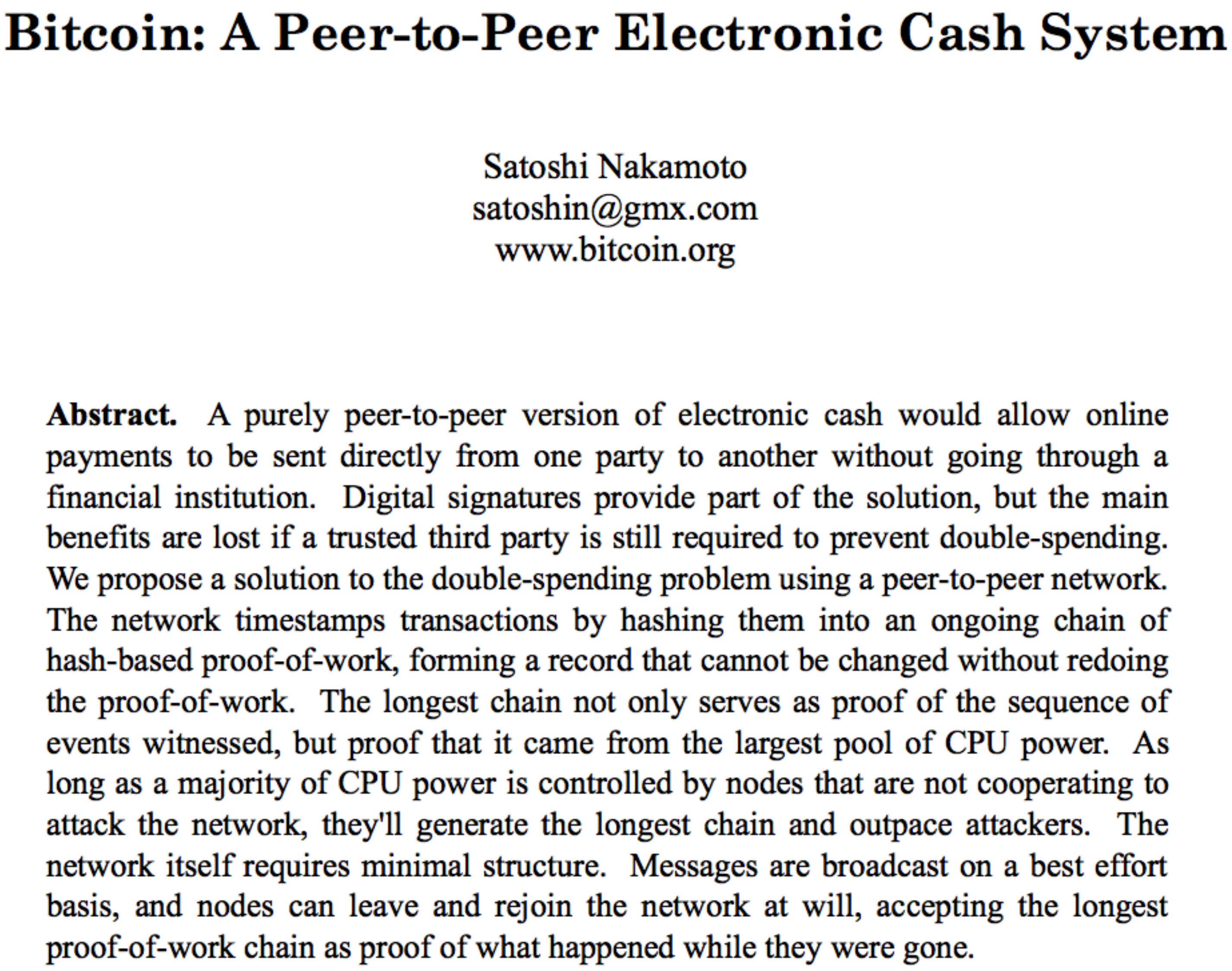
University of Chicago

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 and price
- 2017-2018: The world loses its mind

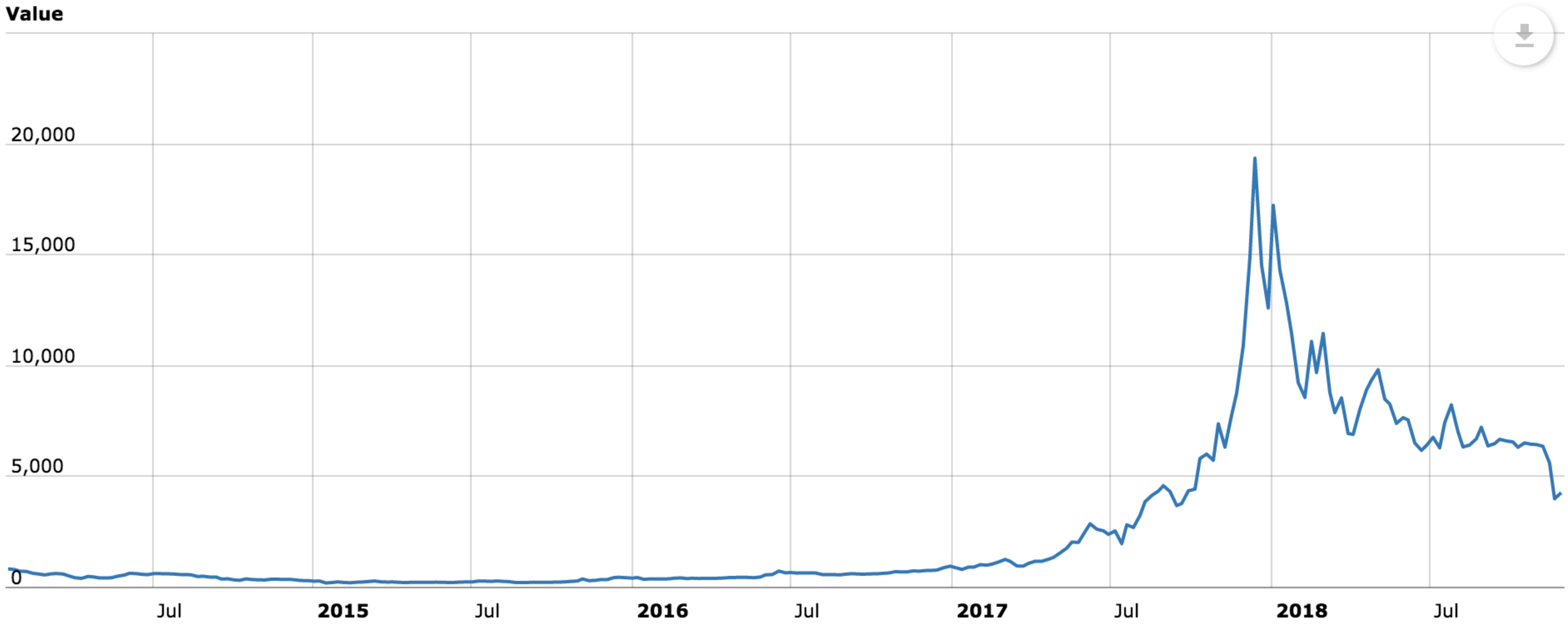


Bitcoin: A Peer-to-Peer Electronic Cash System

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

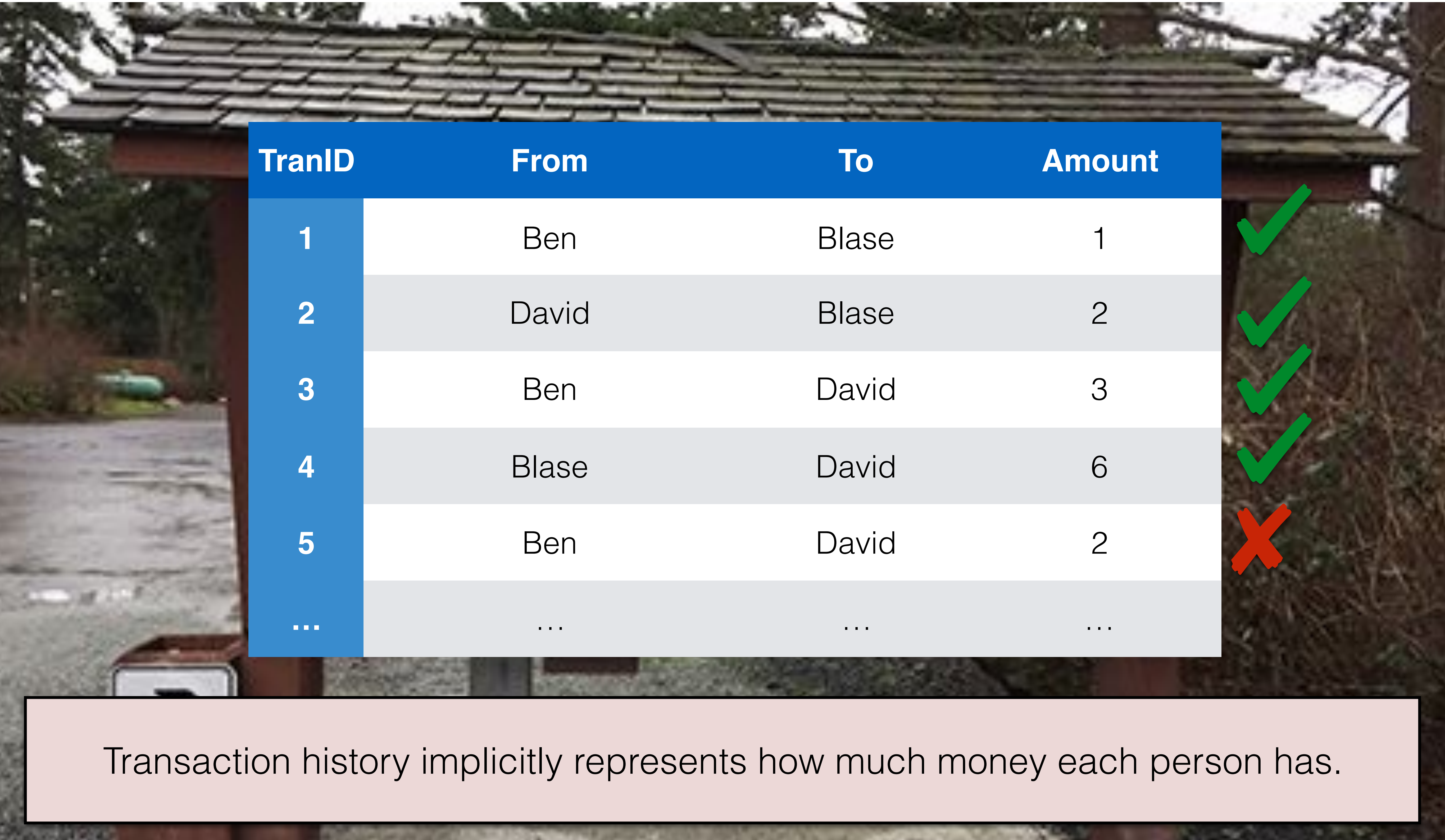


Hundreds of Altcoins Today

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.

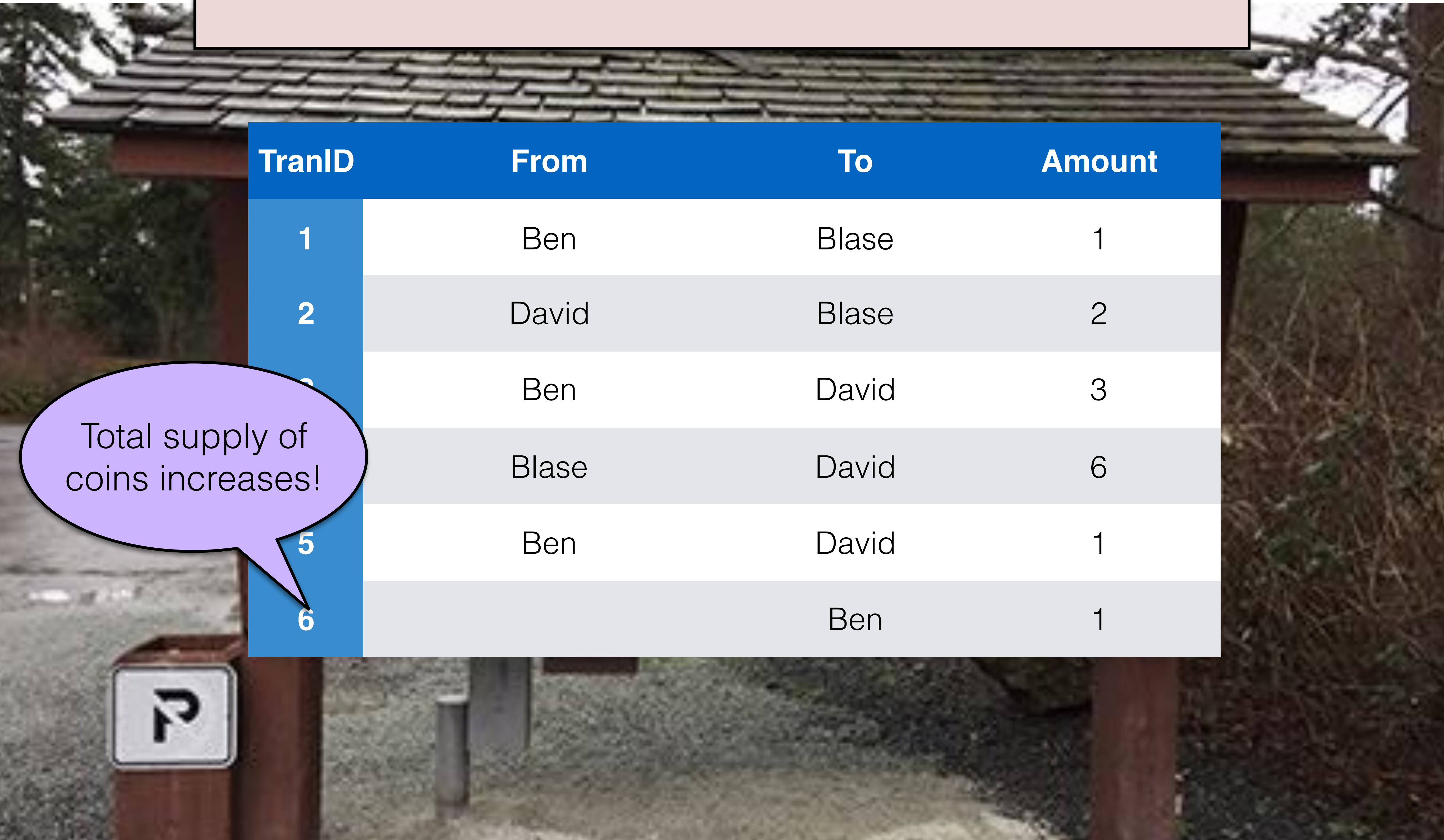
Another Threat: Ledger Integrity Violations

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
	Blase	David	6
5	Ben	David	1
6		Ben	1

Total supply of coins increases!

Refresher: Digital Signatures

Definition. A digital signature scheme consists of three algorithms **Kg**, **Sign**, and **Verify**

- Key generation algorithm **Kg**, takes no input and outputs a (random) public-verification-key/secret-signing key pair (VK,SK)

- Signing algorithm **Sign**, takes input the secret key SK and a message M, outputs "signature" σ←Sign(SK,M)

- Verification algorithm **Verify**, takes input the public key VK, a message M, a signature σ, and outputs ACCEPT/REJECT

  Verify(VK,M,σ)=ACCEPT/REJECT

Digital Signatures for More Secure & Private Ledgers

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

David's verification key: $\mathtt{VK}_{\mathtt{david}}$ = 5e7843…
Ben's verification key: $\mathtt{VK}_{\mathtt{ben}}$ = 88f01e…
Blase's verification key: $\mathtt{VK}_{\mathtt{blase}}$ = 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: $\texttt{VK}_{\texttt{david}}$ = 5e7843…
Ben's verification key: $\texttt{VK}_{\texttt{ben}}$ = 88f01e…
Blase's verification key: $\texttt{VK}_{\texttt{blase}}$ = 16823a

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

TranID	From	To	Amount	
1	88f01e…	16823a…	1	91[illegible]001…
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

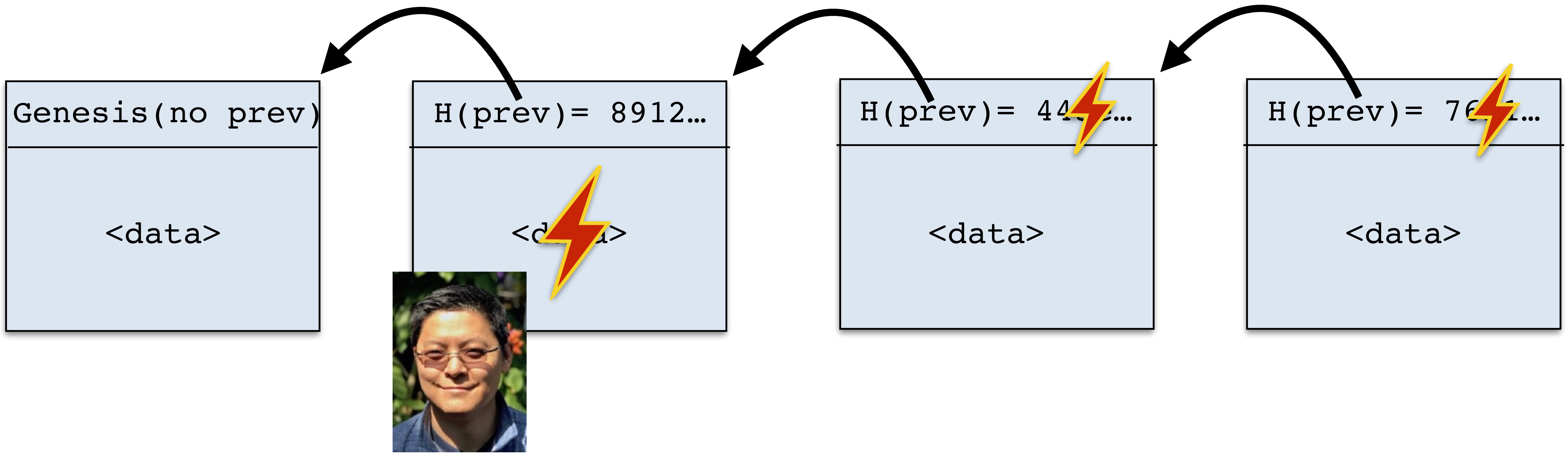
David's verification key: $\mathtt{VK}_{\mathtt{david}}$ = `5e7843…`
Ben's verification key: $\mathtt{VK}_{\mathtt{ben}}$ = `88f01e…`
Blase's verification key: $\mathtt{VK}_{\mathtt{blase}}$ = `16823a…`

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



Genesis(no prev)

<data>

H(prev)= 8912…

<d a>

H(prev)= 44 …

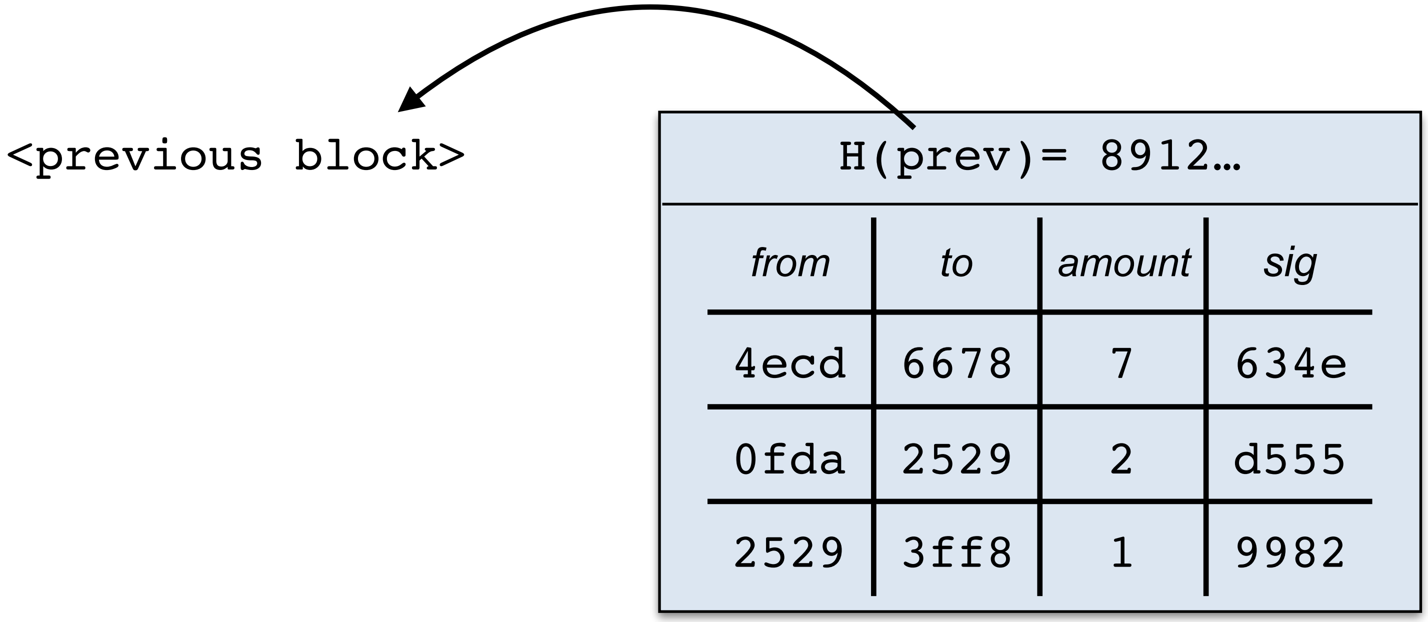
<data>

H(prev)= 76 …

<data>

- 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.
- Additionally, blockchains cure cancer, end all wars, feed the hungry, etc

Moving DCash “To the Blockchain”: Block Data Format



`<previous block>`

`H(prev)= 8912…`

from	*to*	*amount*	*sig*
4ecd	6678	7	634e
0fda	2529	2	d555
2529	3ff8	1	9982

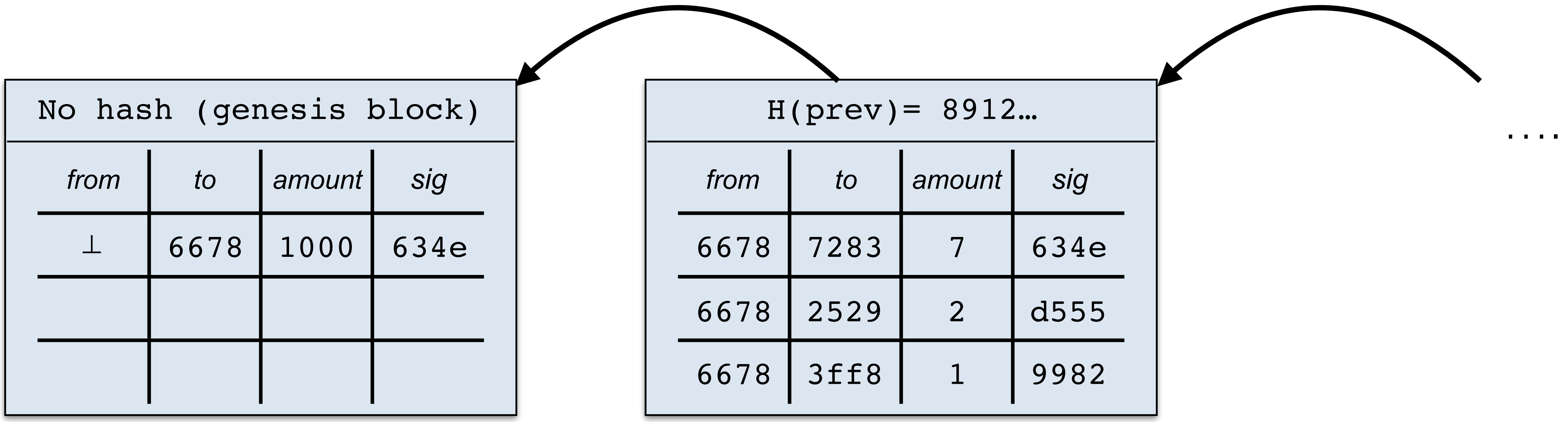
Moving DCash “To the Blockchain”: The Details

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)



No hash (genesis block)

from	*to*	*amount*	*sig*
⊥	6678	1000	634e

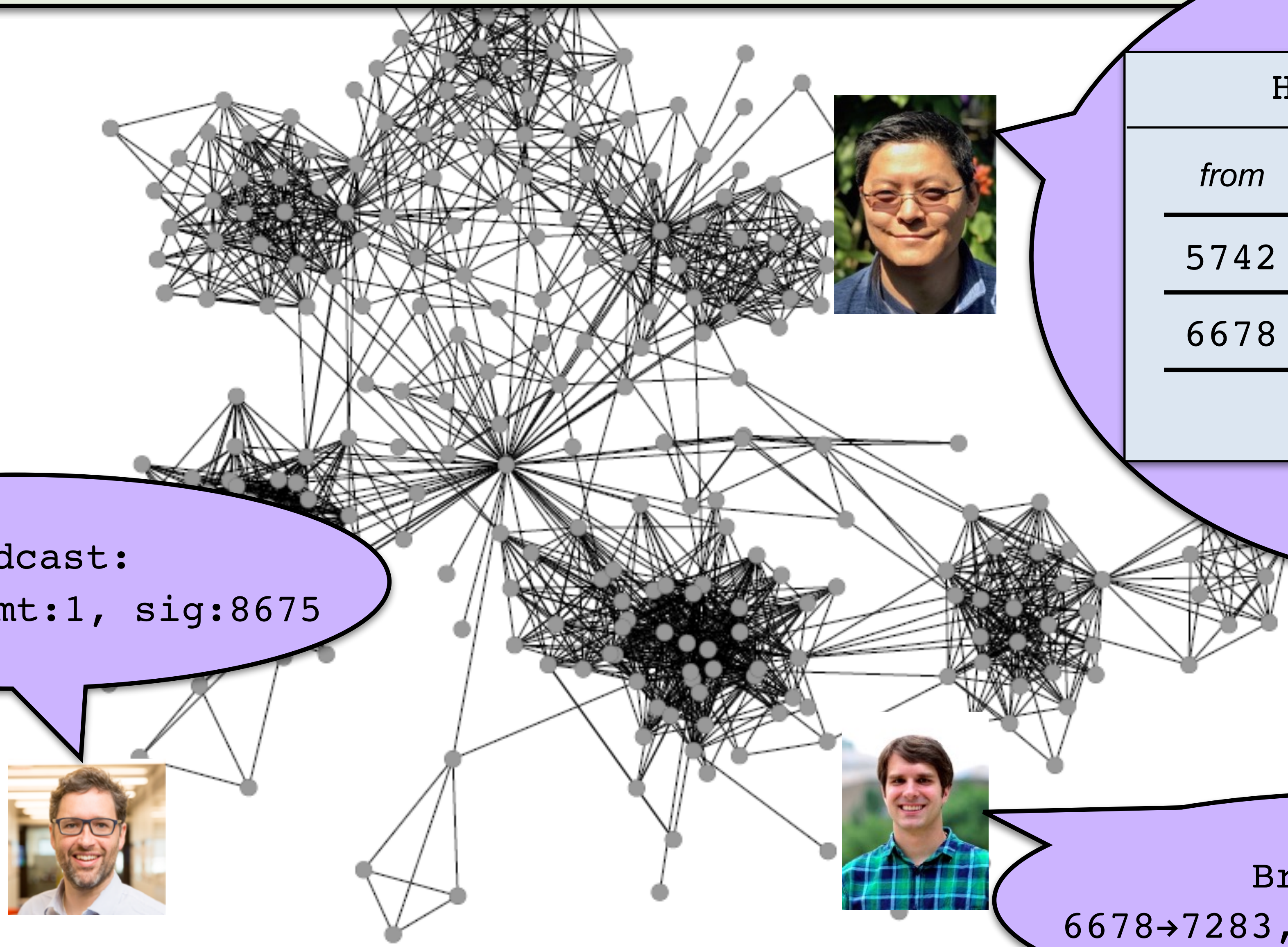
H(prev)= 8912…

from	*to*	*amount*	*sig*
6678	7283	7	634e
6678	2529	2	d555
6678	3ff8	1	9982

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

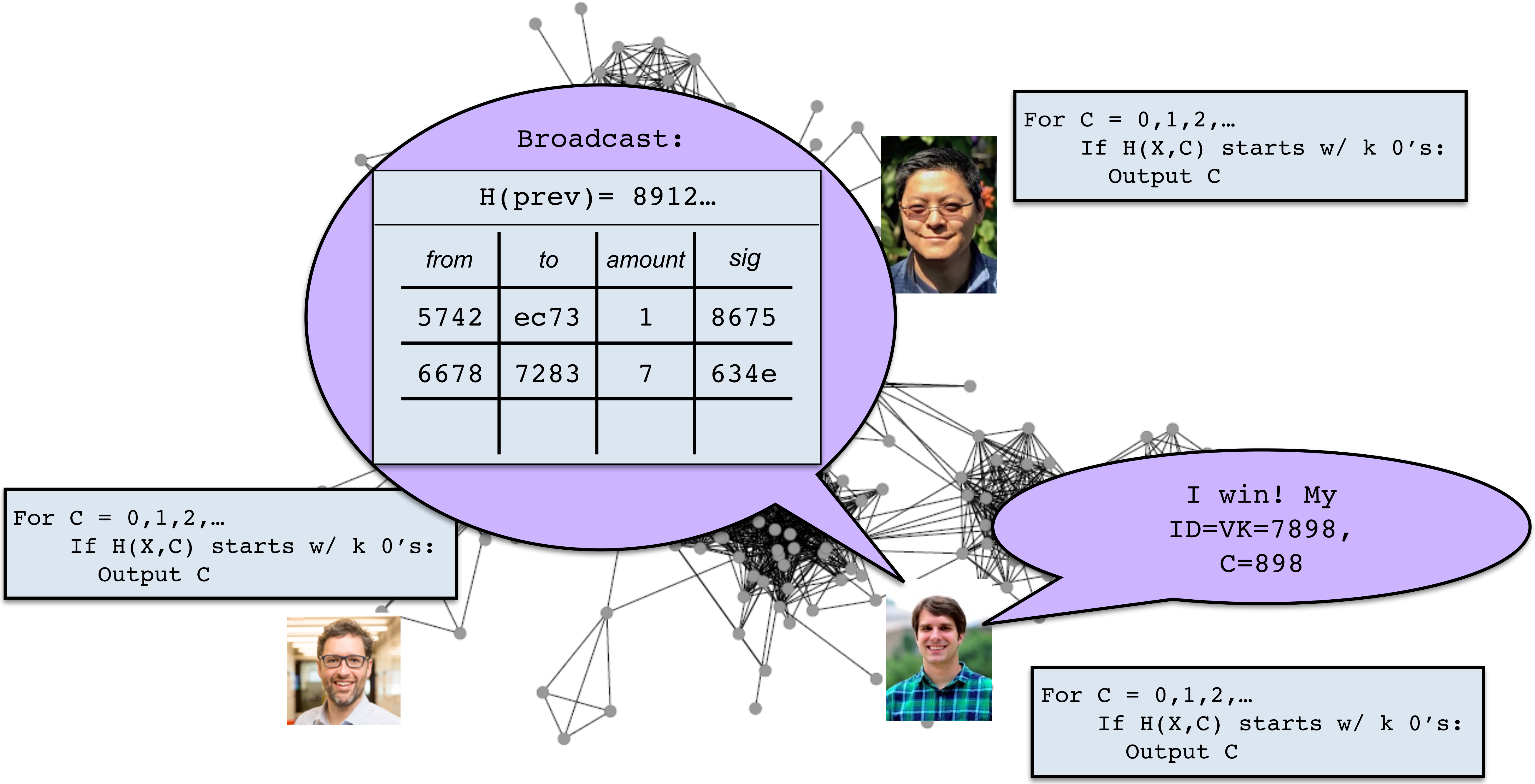
Canonical algorithm: On input `X`:

```
 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



Broadcast:

H(prev)= 8912…			
from	*to*	*amount*	*sig*
5742	ec73	1	8675
6678	7283	7	634e

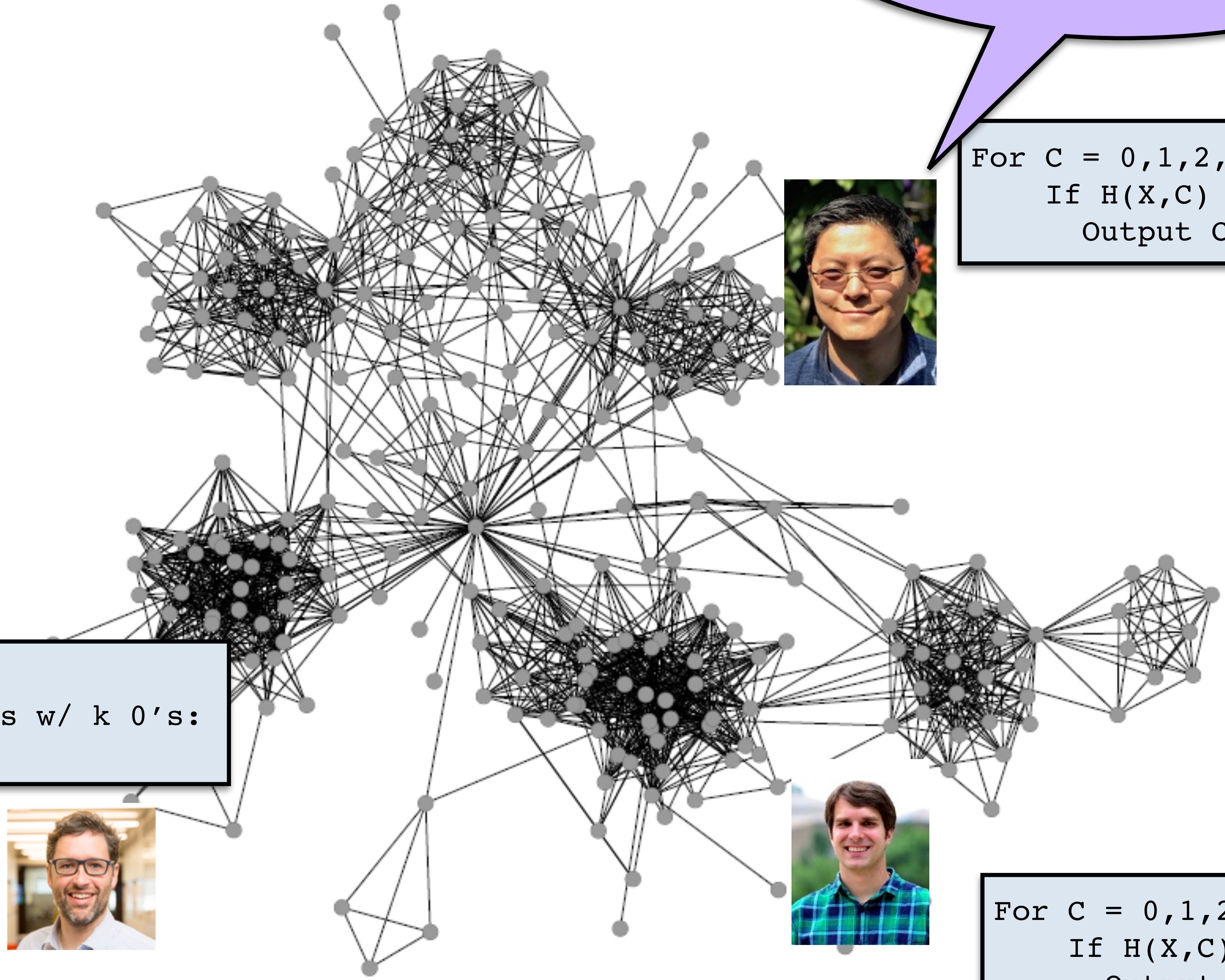
```
For C = 0,1,2,…
    If H(X,C) starts w/ k 0’s:
      Output C
```

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

I win! My ID=VK=7898, C=898

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

But why do the POWs?



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

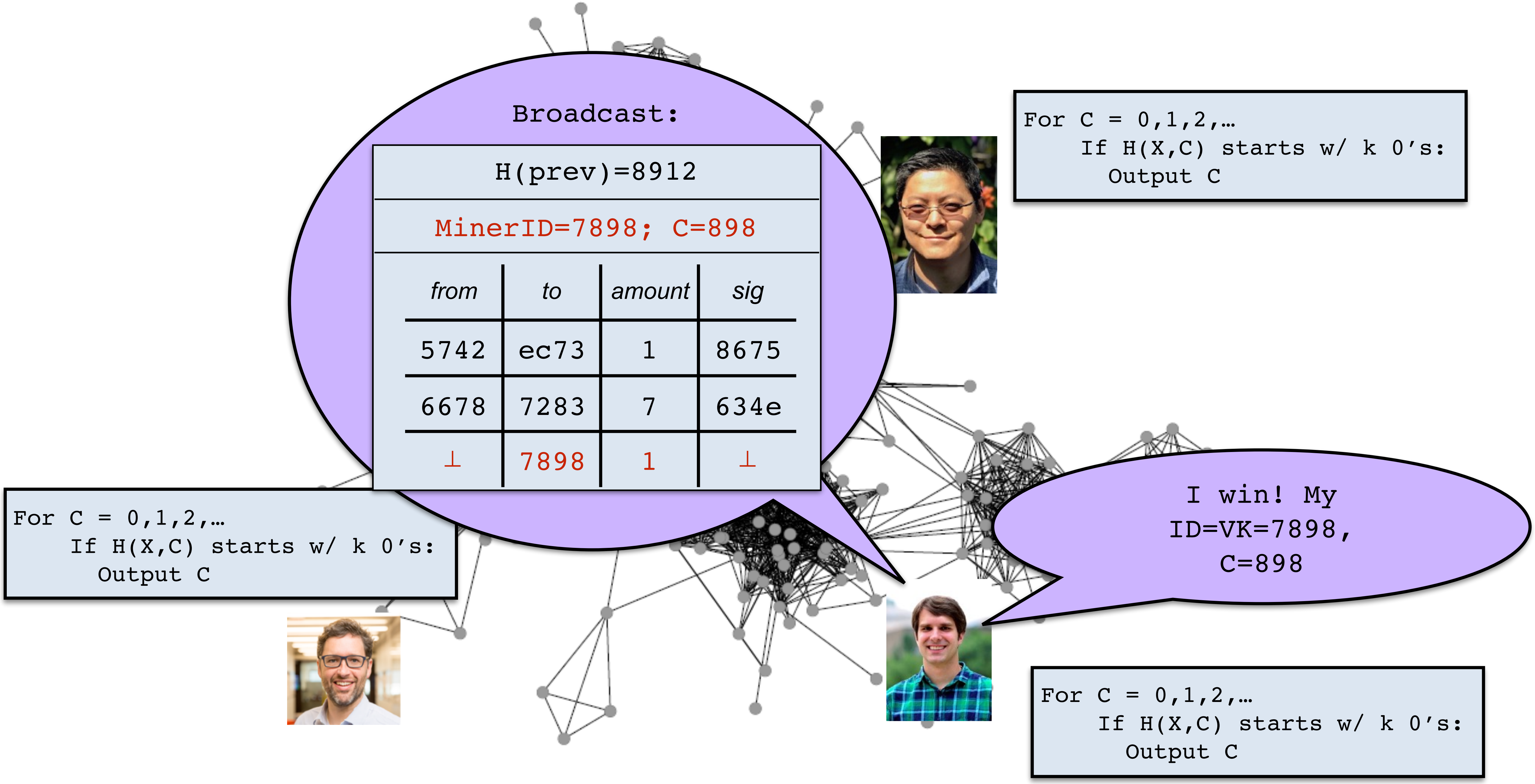
```
For C = 0,1,2,…
    If H(X,C) starts w/ k 0’s:
      Output C
```

```
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”



Broadcast:

H(prev)=8912

MinerID=7898; C=898

from	to	amount	sig
5742	ec73	1	8675
6678	7283	7	634e
⊥	7898	1	⊥

```
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
```

I win! My
ID=VK=7898,
C=898

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

The DCash Blockchain, So Far

1. Digital version of ledger; Accounts defined by history

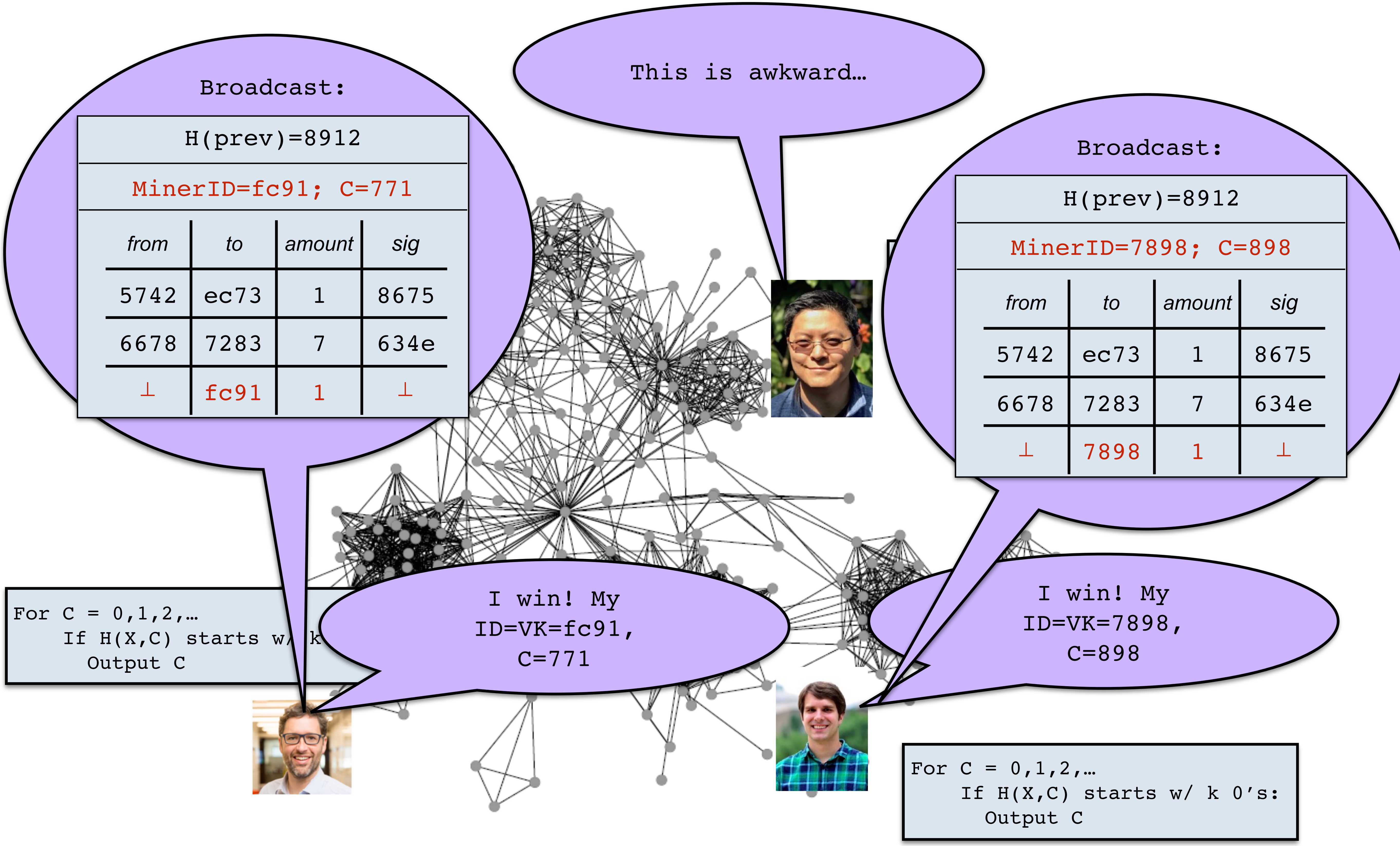
2. Genesis block gave chosen group a pile of coins

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



Broadcast:

H(prev)=8912

MinerID=fc91; C=771

from	to	amount	sig
5742	ec73	1	8675
6678	7283	7	634e
⊥	fc91	1	⊥

This is awkward…

Broadcast:

H(prev)=8912

MinerID=7898; C=898

from	to	amount	sig
5742	ec73	1	8675
6678	7283	7	634e
⊥	7898	1	⊥

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

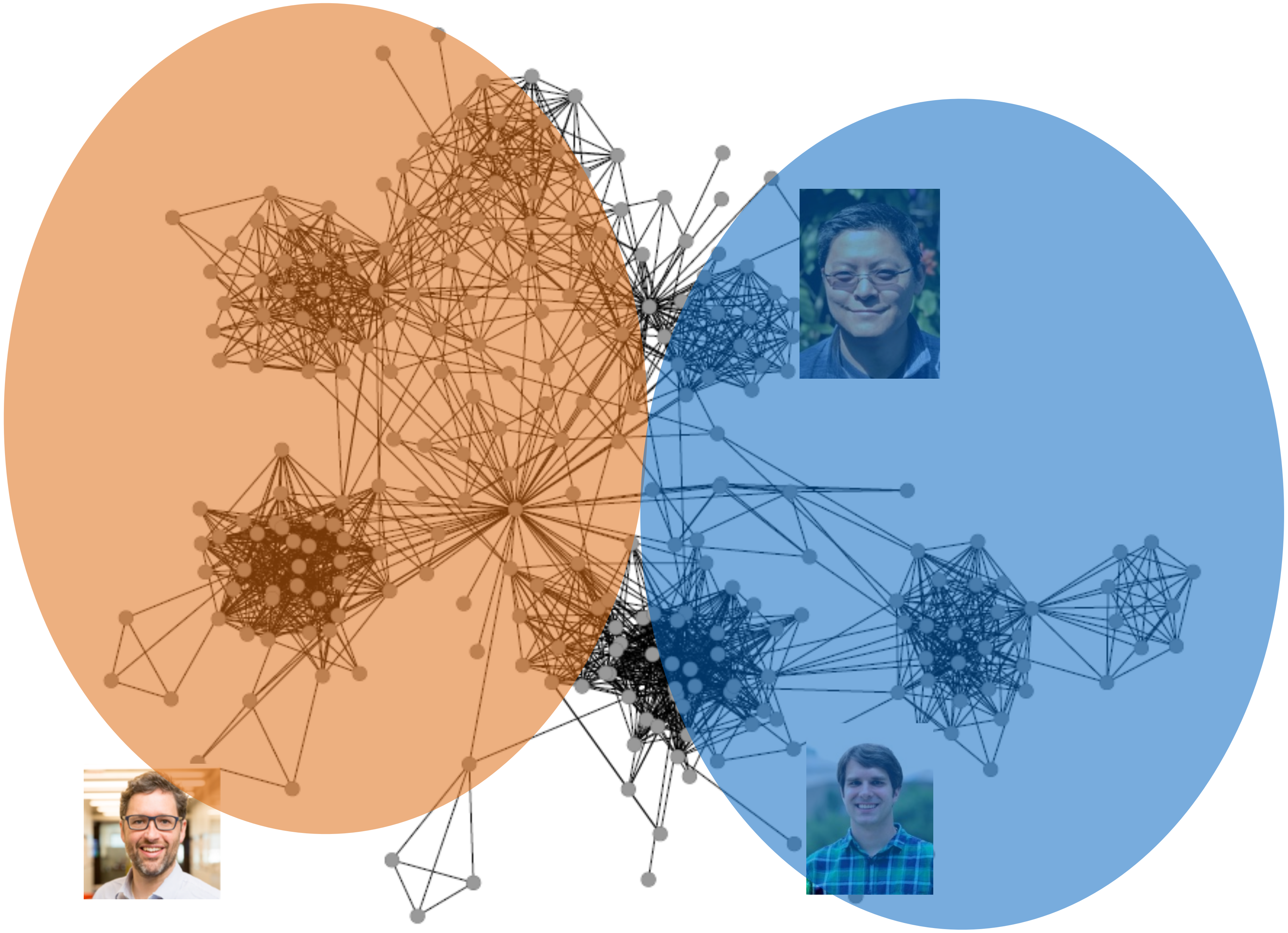
I win! My ID=VK=fc91, C=771

I win! My ID=VK=7898, C=898

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

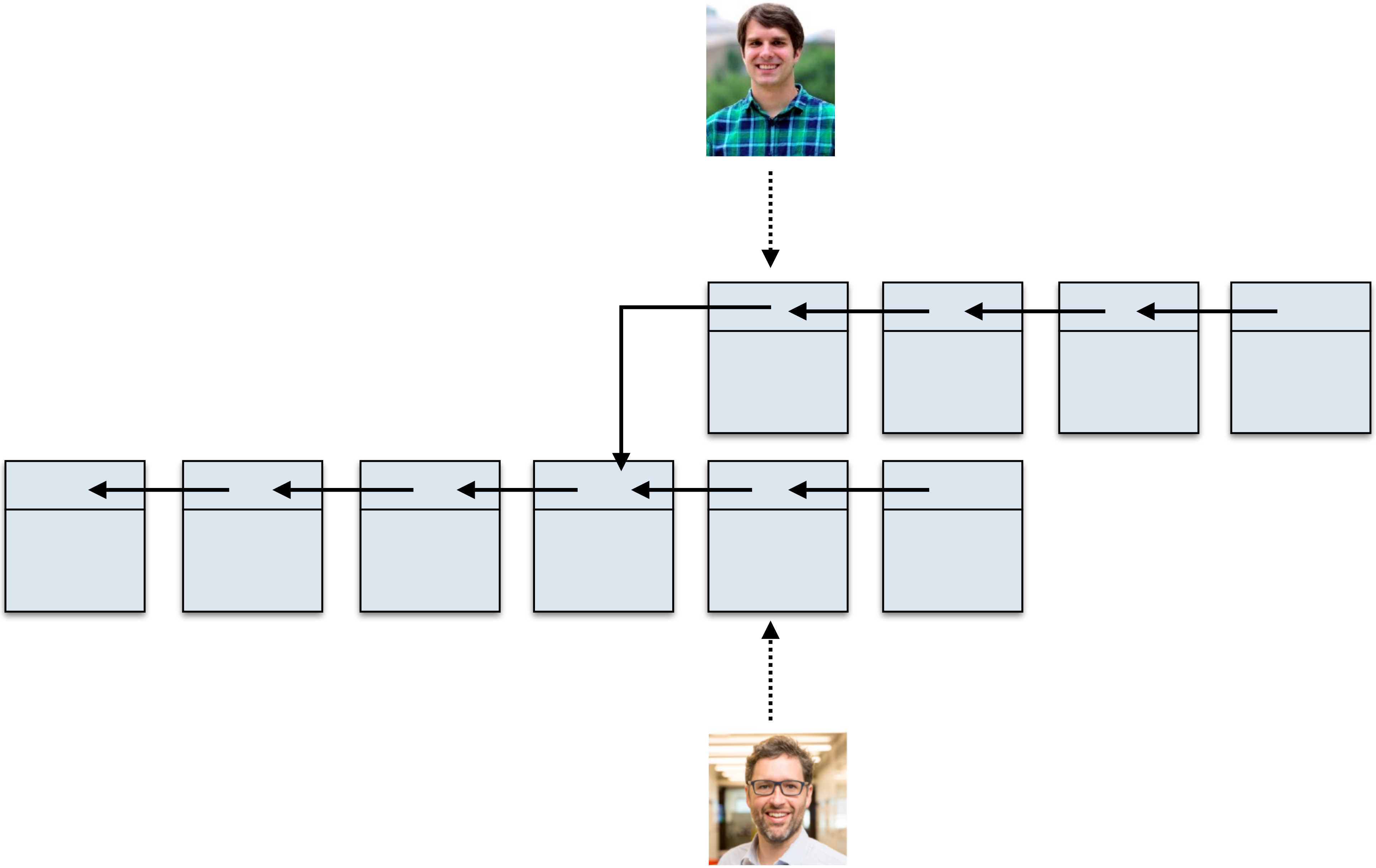
Forking in the Blockchain

- 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

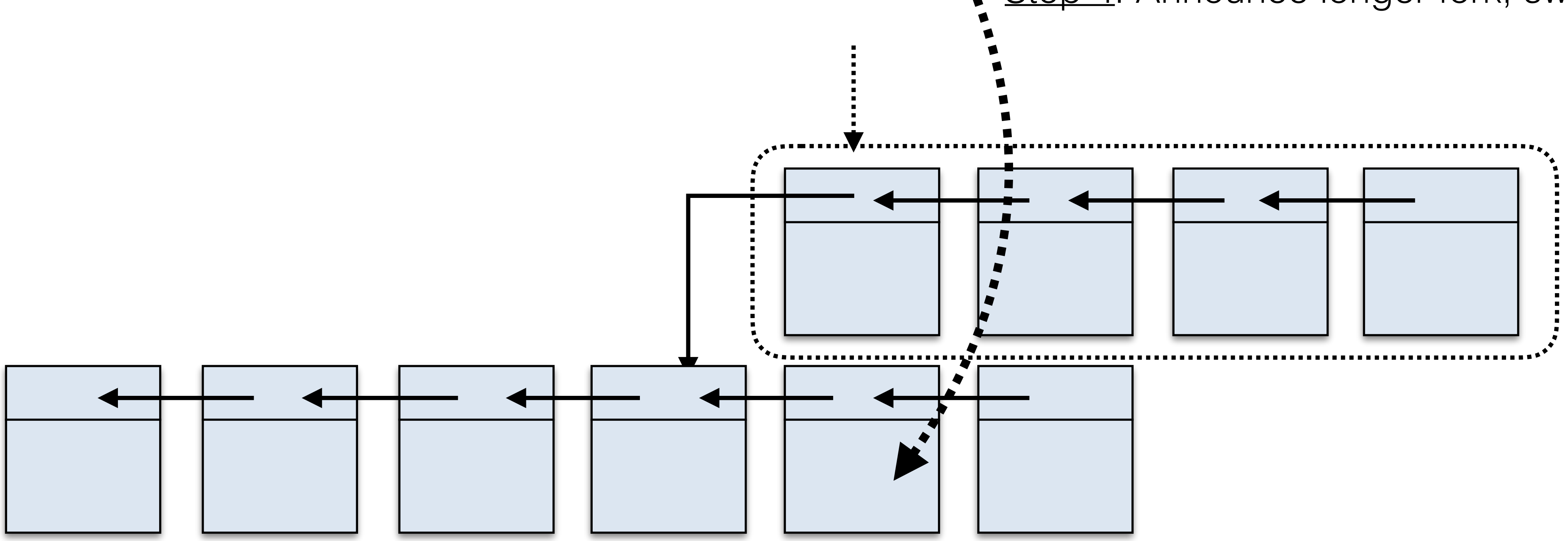


- Resolution: Any node will switch to the longest chain it has seen

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.

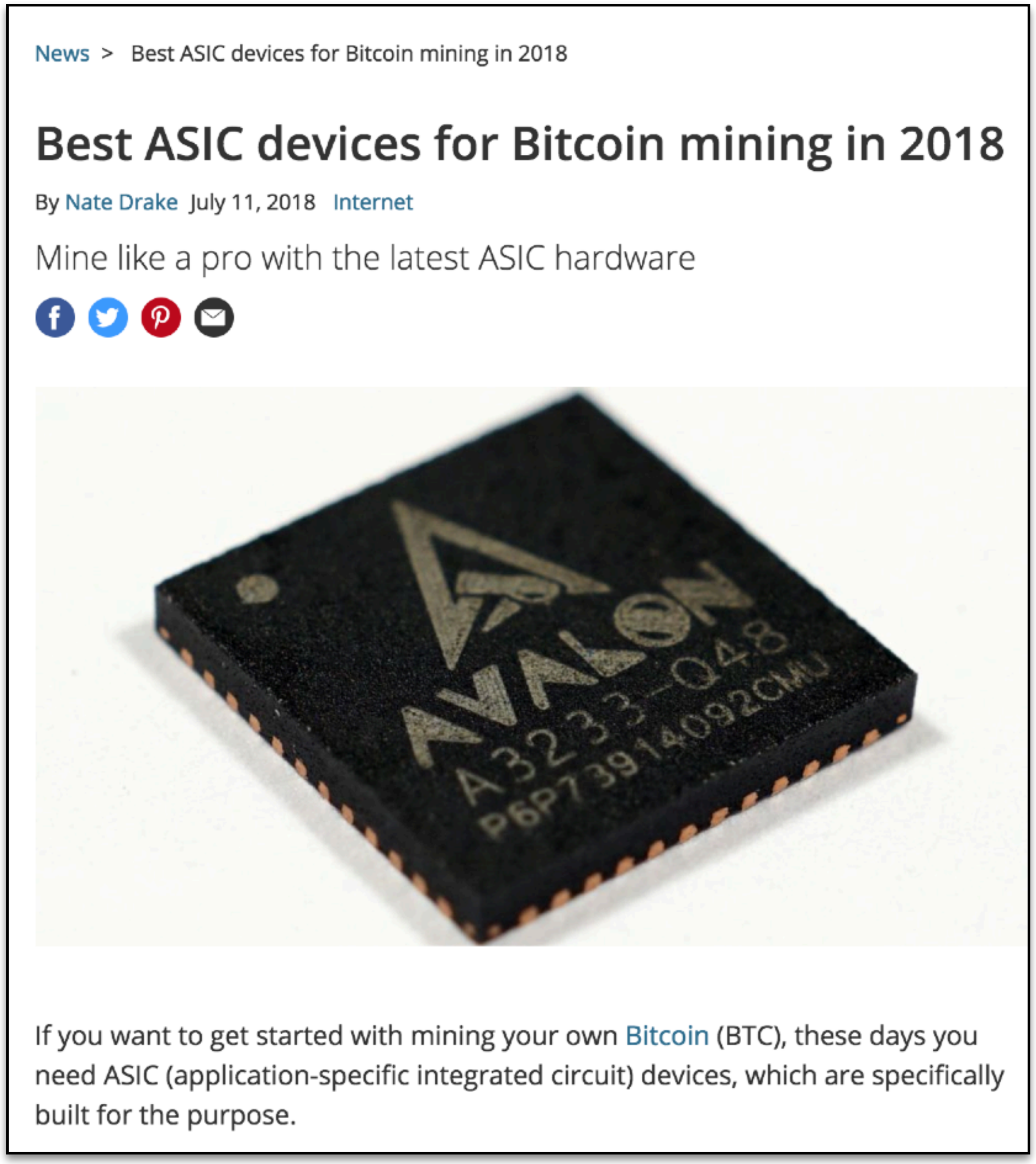


- When network switches to my fork, the banana transaction disappears.
- Free bananas! (Sorry Blase, see Step 2)

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

Blockchain Mining

- Current reward for mining a block is: About $53,400 (12 BTC)
- Current setting for k in POW is: About 72
- Most compute power is in "Mining Pools"
- Currently, Bitcoin mining uses amount of electricity similar to the entire country of Bangladesh (by one estimate)



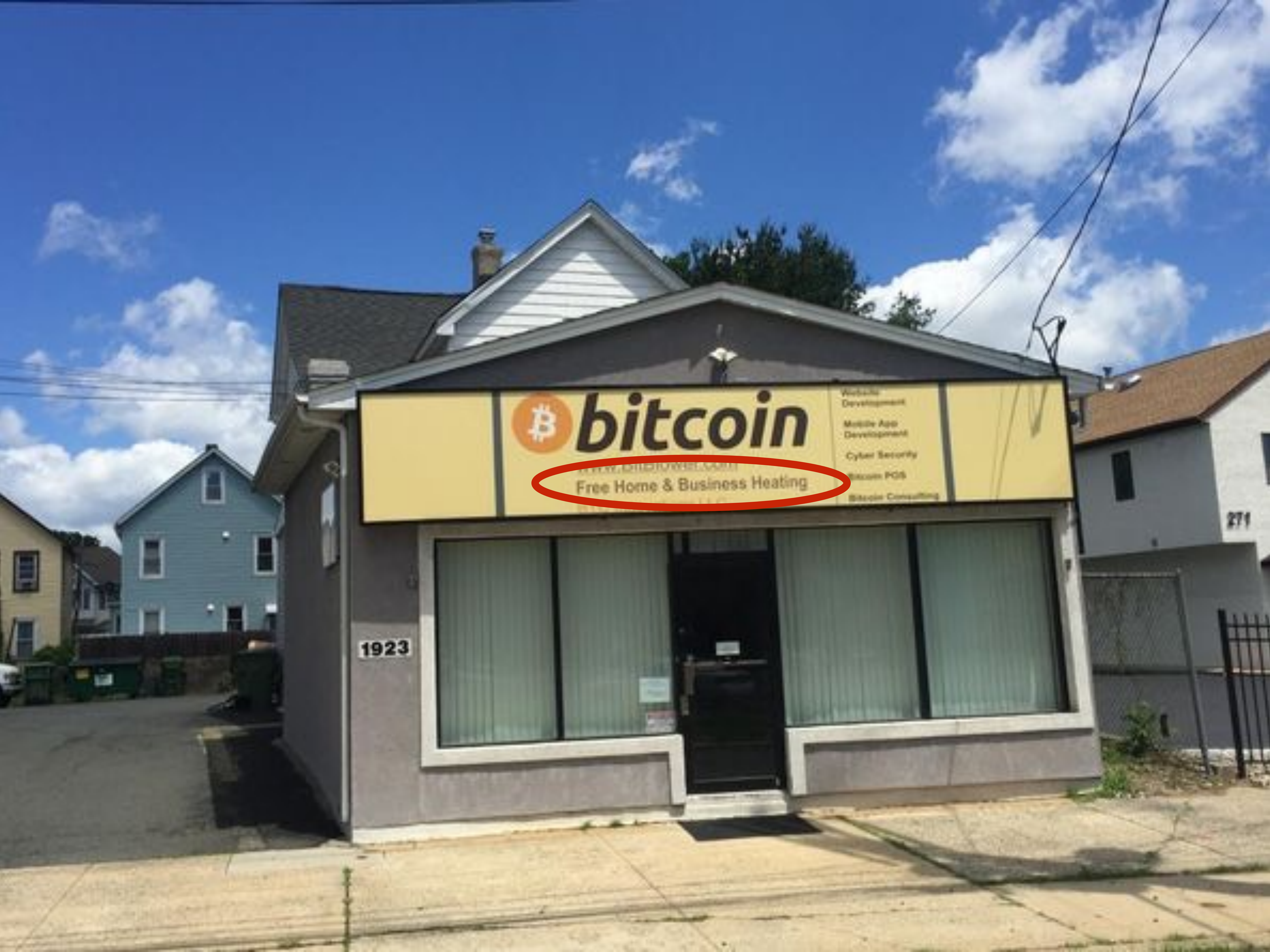
News > Best ASIC devices for Bitcoin mining in 2018

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.


bitcoin
www.BitBlower.com
Free Home & Business Heating
Website Development
Mobile App Development
Cyber Security
Bitcoin POS
Bitcoin Consulting
1923
271

Zcash: Privacy via Zero-Knowledge Proofs

Zcash

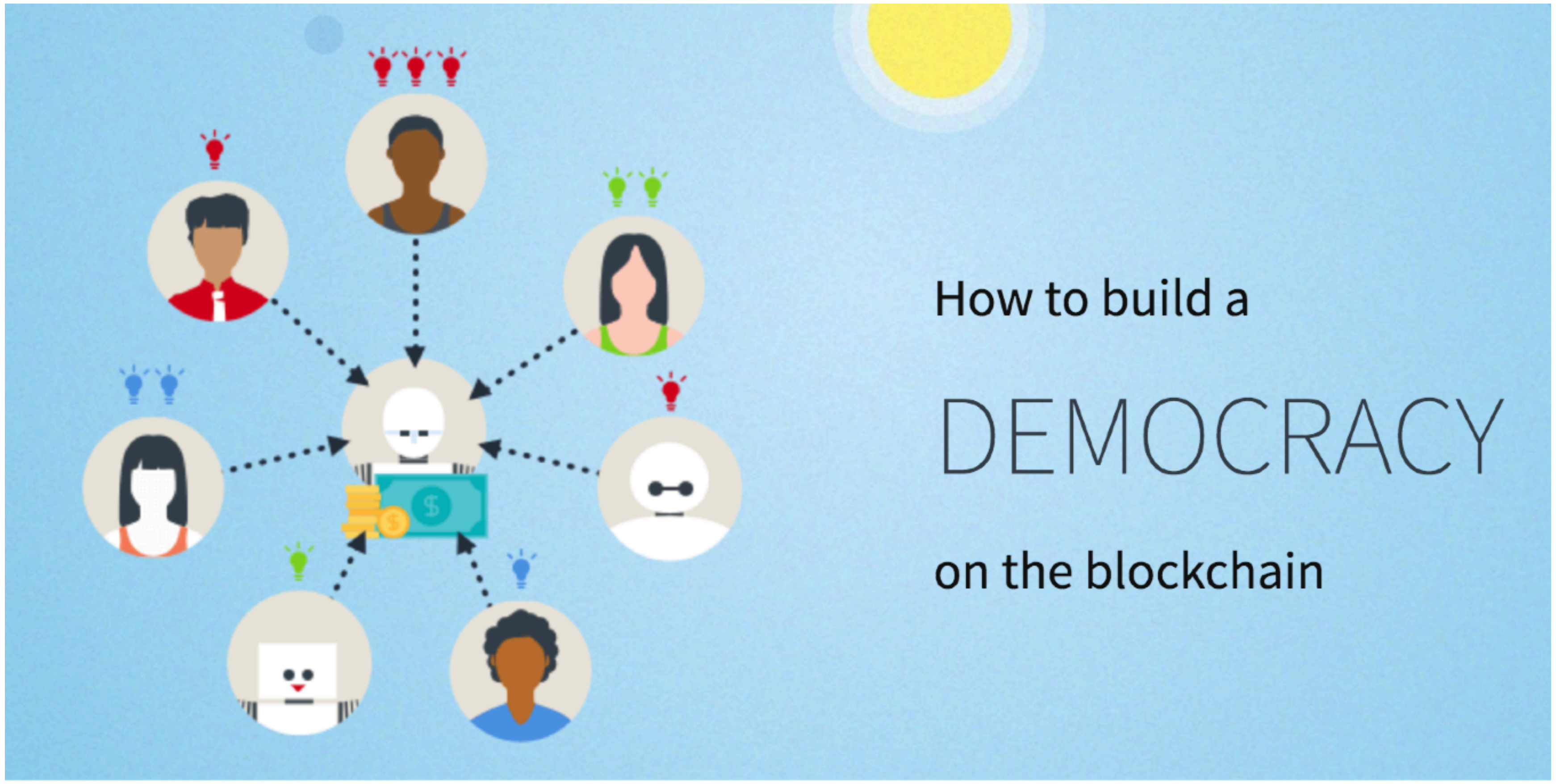
- If you can connect a Bitcoin public key to a person, then you can see their entire transaction history
- Zcash is an altcoin that addresses this:
  - When adding a block, network doesn’t depend on blockchain history to check validity
  - Instead, you give a zero-knowledge proof that your transaction 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.

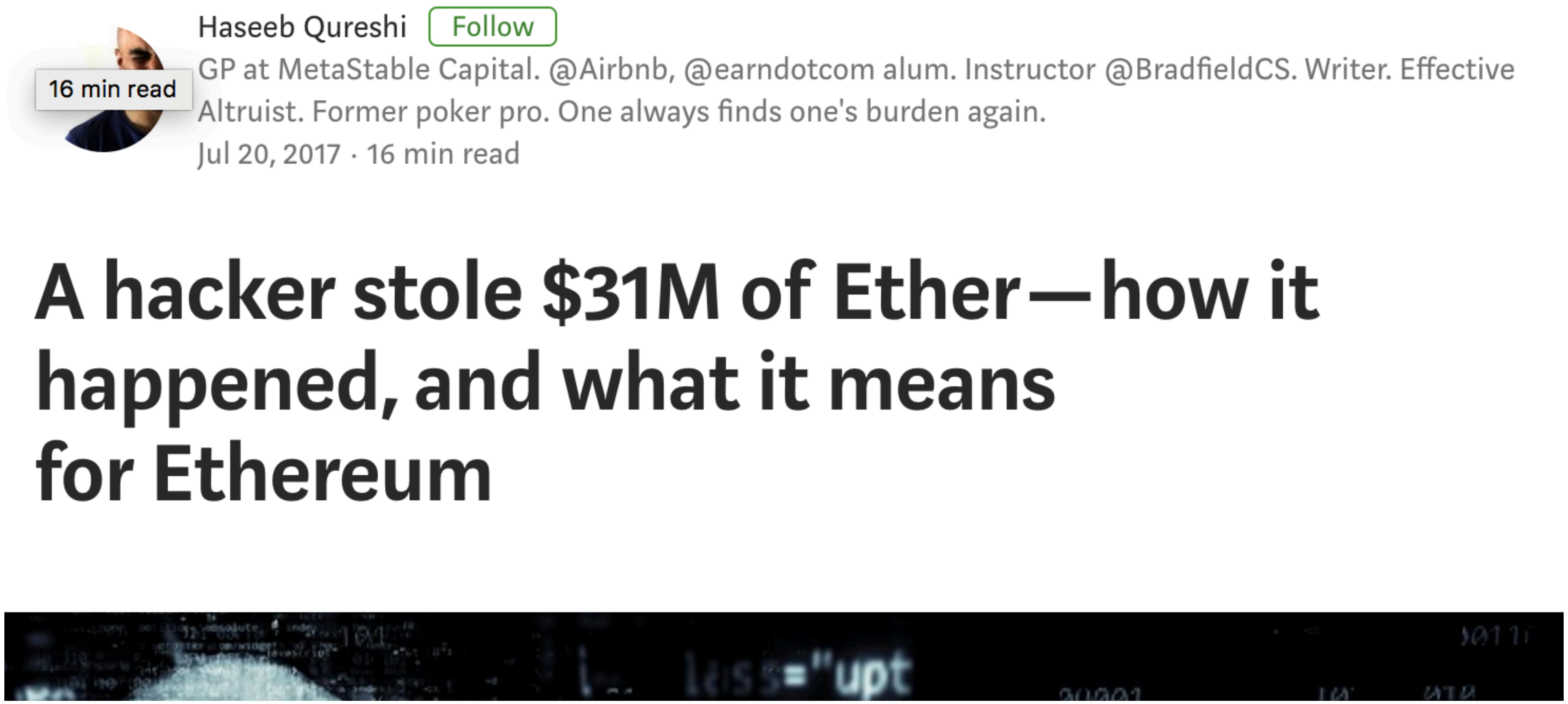
The Ethereum DAO

- 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



16 min read

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.

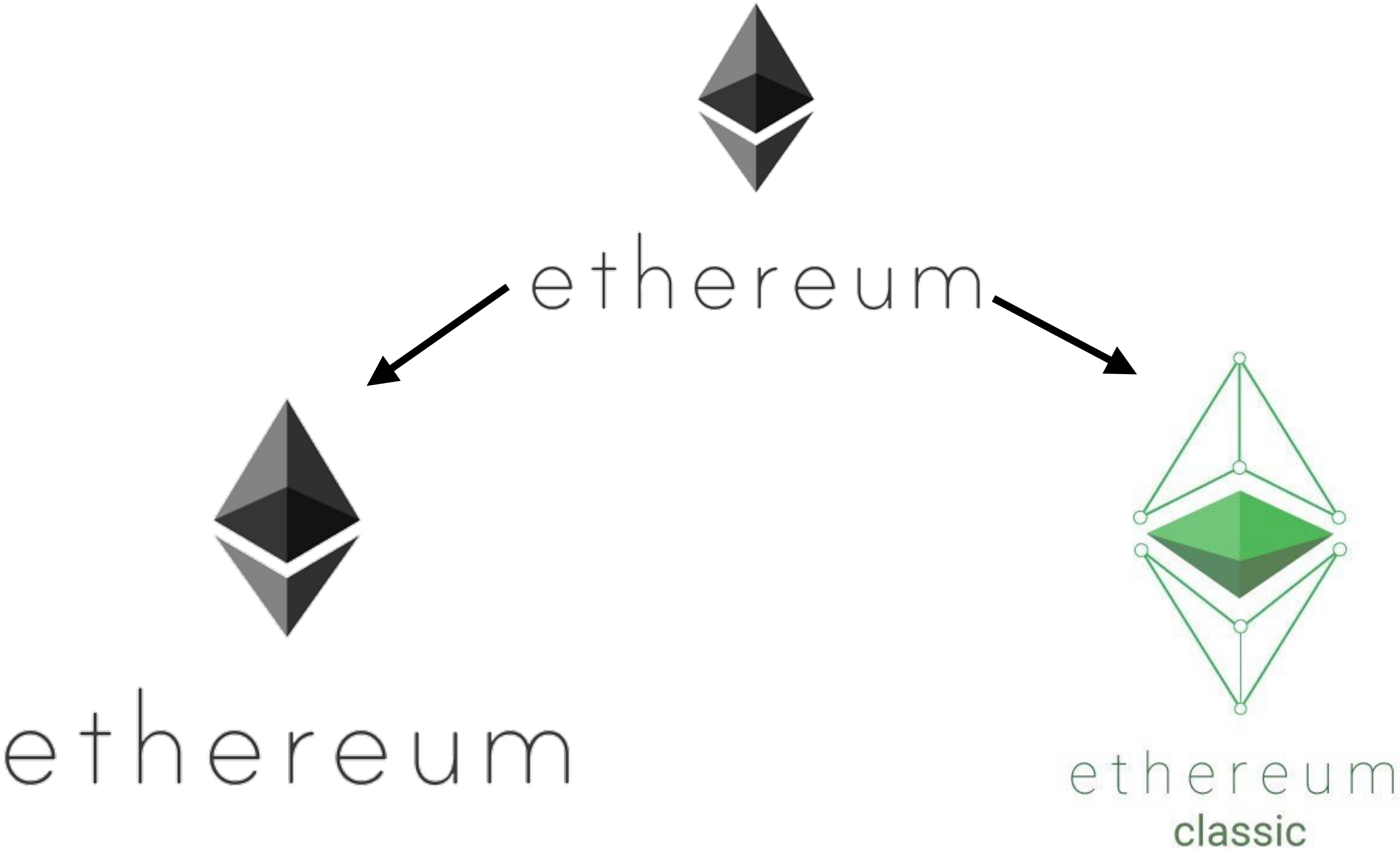
Jul 20, 2017 · 16 min read

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.”)



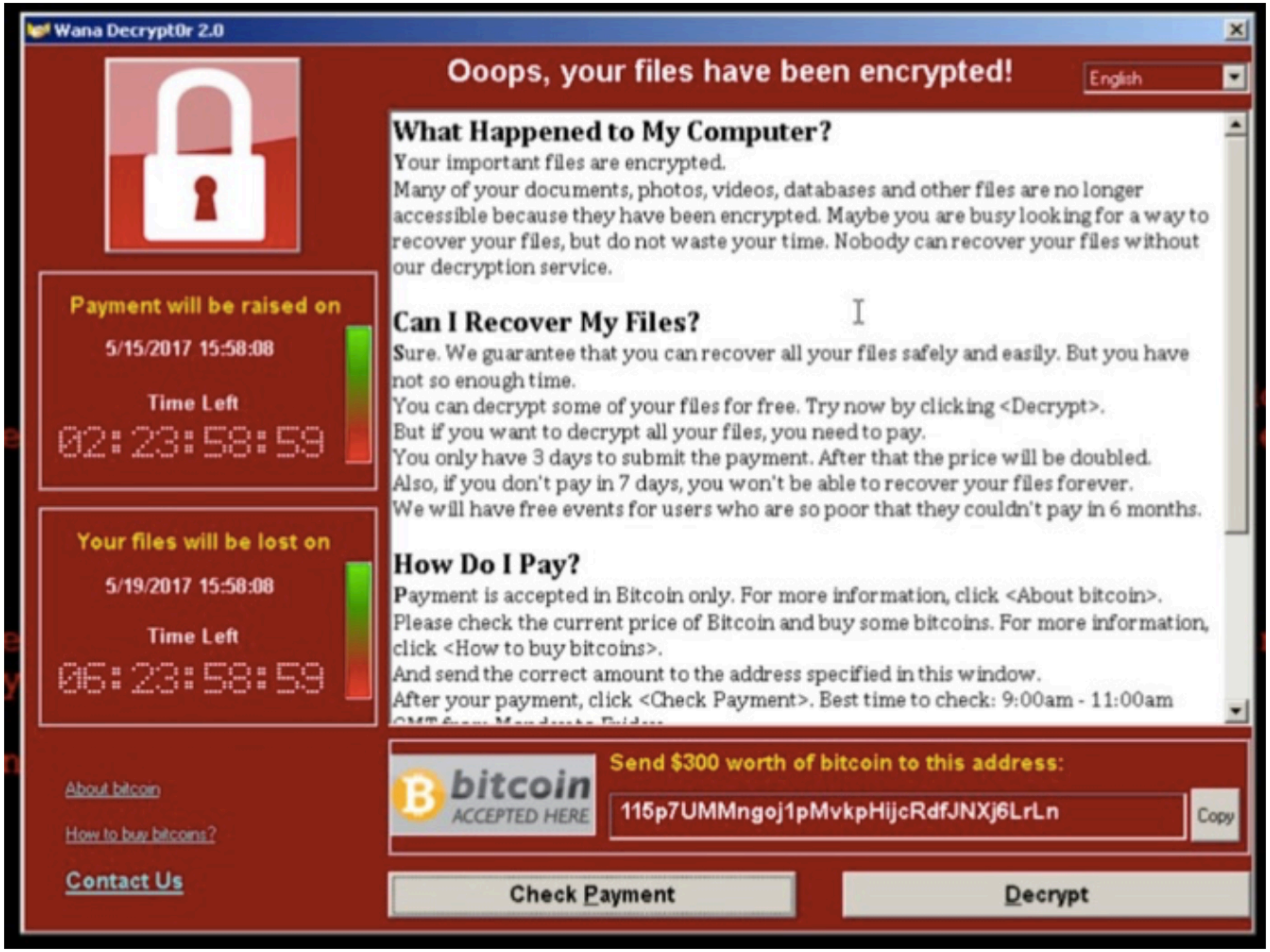
$112 USD

$4 USD

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)

Other Application of Bitcoin: Ransomware



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

BITCOIN CRIME AUGUST 02, 2018 07:45 CET

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

The End