DS 593: Privacy in Practice

Blockchains

Instructor: Alishah Chator

News?

TUNING IN TO YOUR EMOTIONS

LG TVs' integrated ads get more personal with tech that analyzes viewer emotions

LG licenses tech for interpreting TV users' feelings and convictions.

SCHARON HARDING – APR 16, 2025 4:14 PM | 135

Credit: Getty

https://arstechnica.com/gadgets/2025/04/lg-tvs-integrated-ads-get-more-personal-with-tech-that-analyzes-viewer-emotions/

Last time

- Decentralized Systems

Today

- Consensus and Blockchains

Activity

- Form into groups
- Have you group decide on a number from 1-20
- Decide on how to tell me your number

Consensus

- One of the key challenges for decentralized applications is *consensus* – coming to a collective decision

- The state of a system or program has major implications for its operation

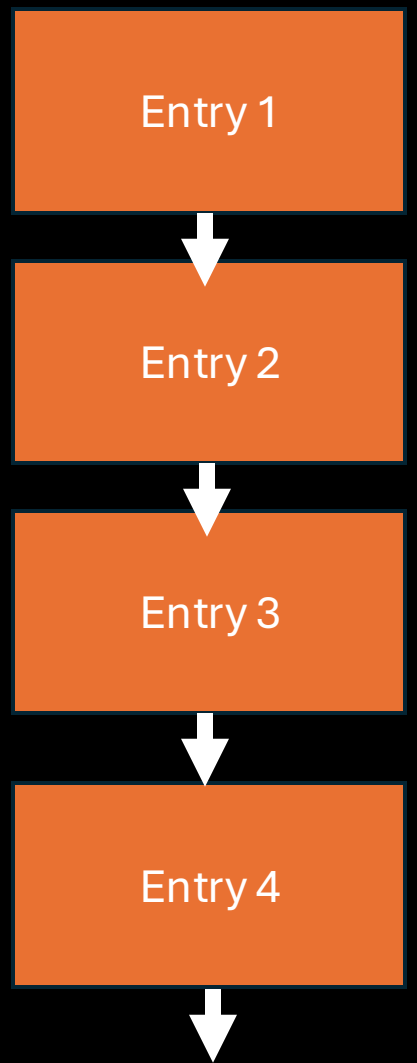
Blockchains

- A system for coming to distributed/decentralized consensus

- Formally introduced in the Bitcoin whitepaper
  - Builds on earlier ideas by Chaum, Haber, Bayer, Stornetta
  - Byzantine Fault Tolerance

Append-Only ledger

- Consider a list of entries that is *append-only*
- We can model the state of a system as a series of transitions from one entry to the next
  - Can't go backwards
- Idea: can we build a distributed ledger?



Naïve Solution to consensus

- Suppose all of the peers in the system are honest
- Each of them has a copy of the ledger
- When something changes, the change is broadcast to all peers
- Each peer updates its ledger
- Decentralized State!

What if the Peers aren’t honest?

What if the Peers aren’t honest?

- Could try a majority vote?

What if the Peers aren’t honest?

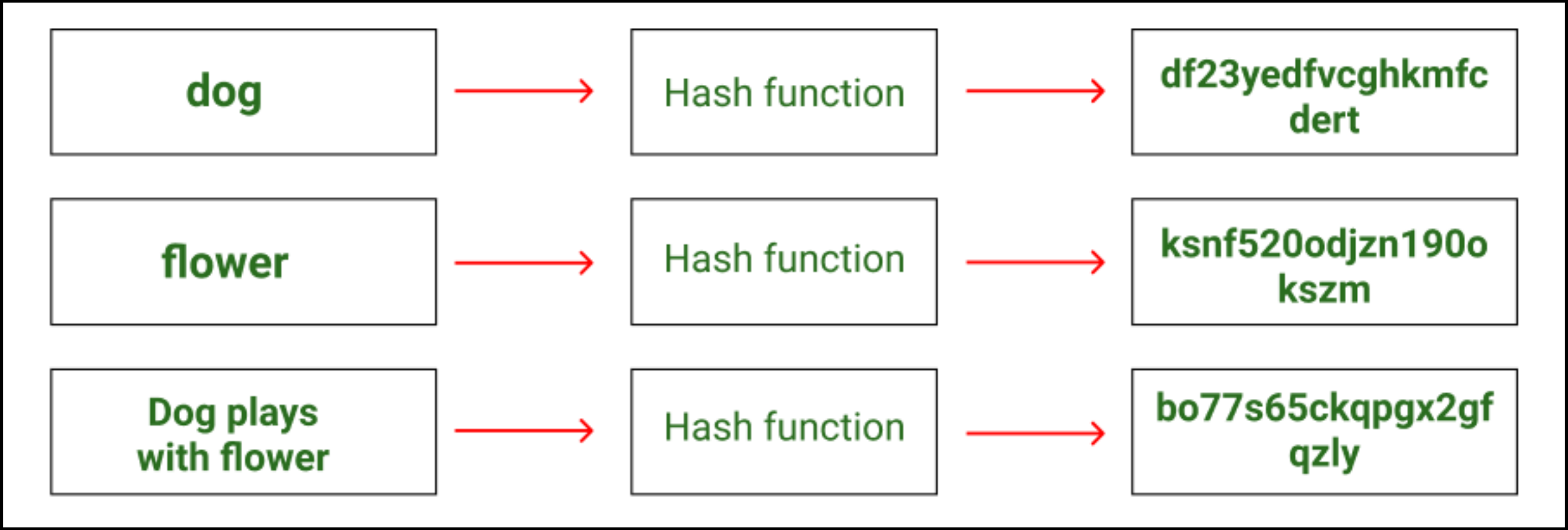
- Could try a majority vote?

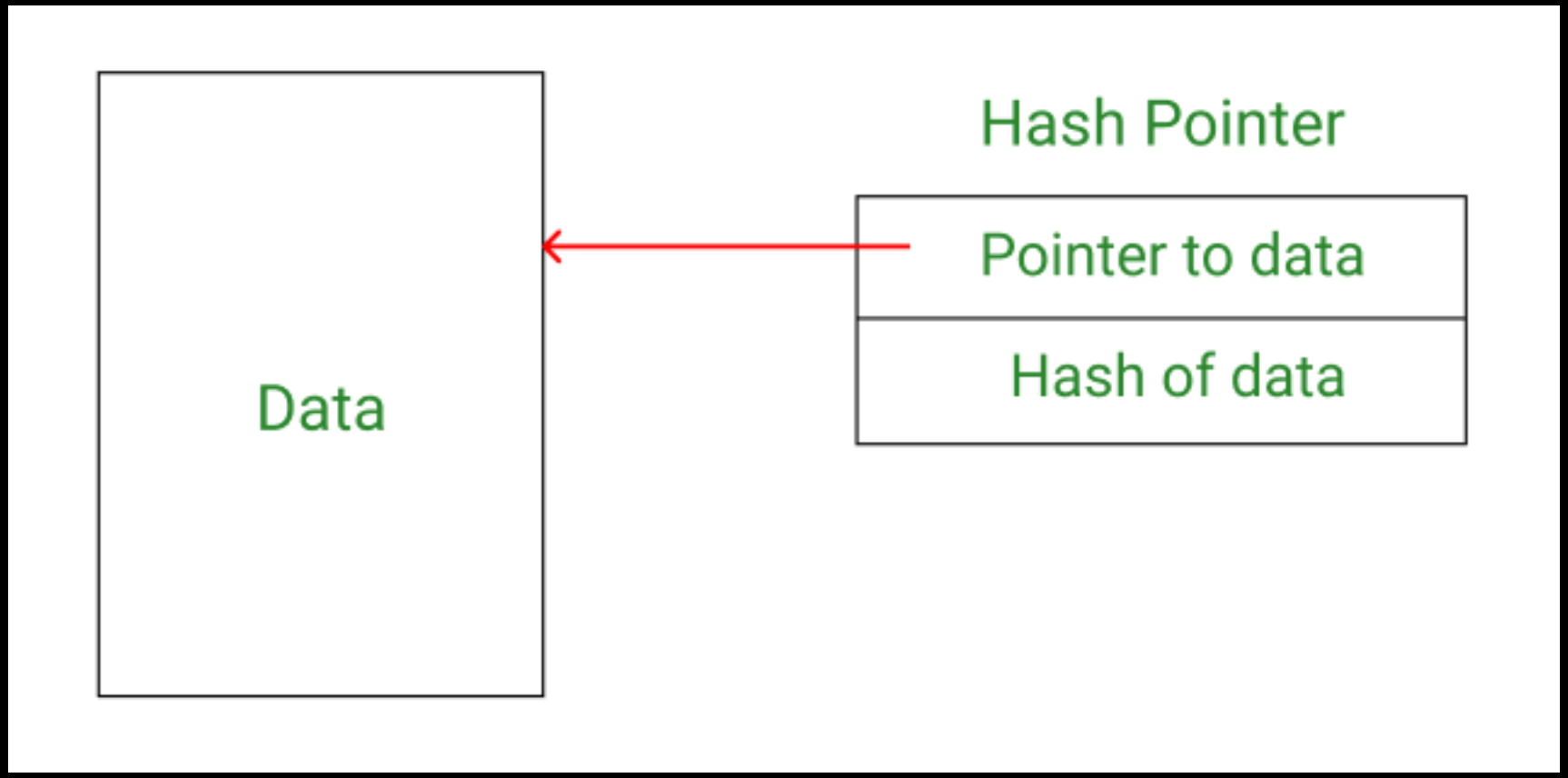
- Problems
  - Inefficient
  - 51% attacks
  - Sybil Attacks

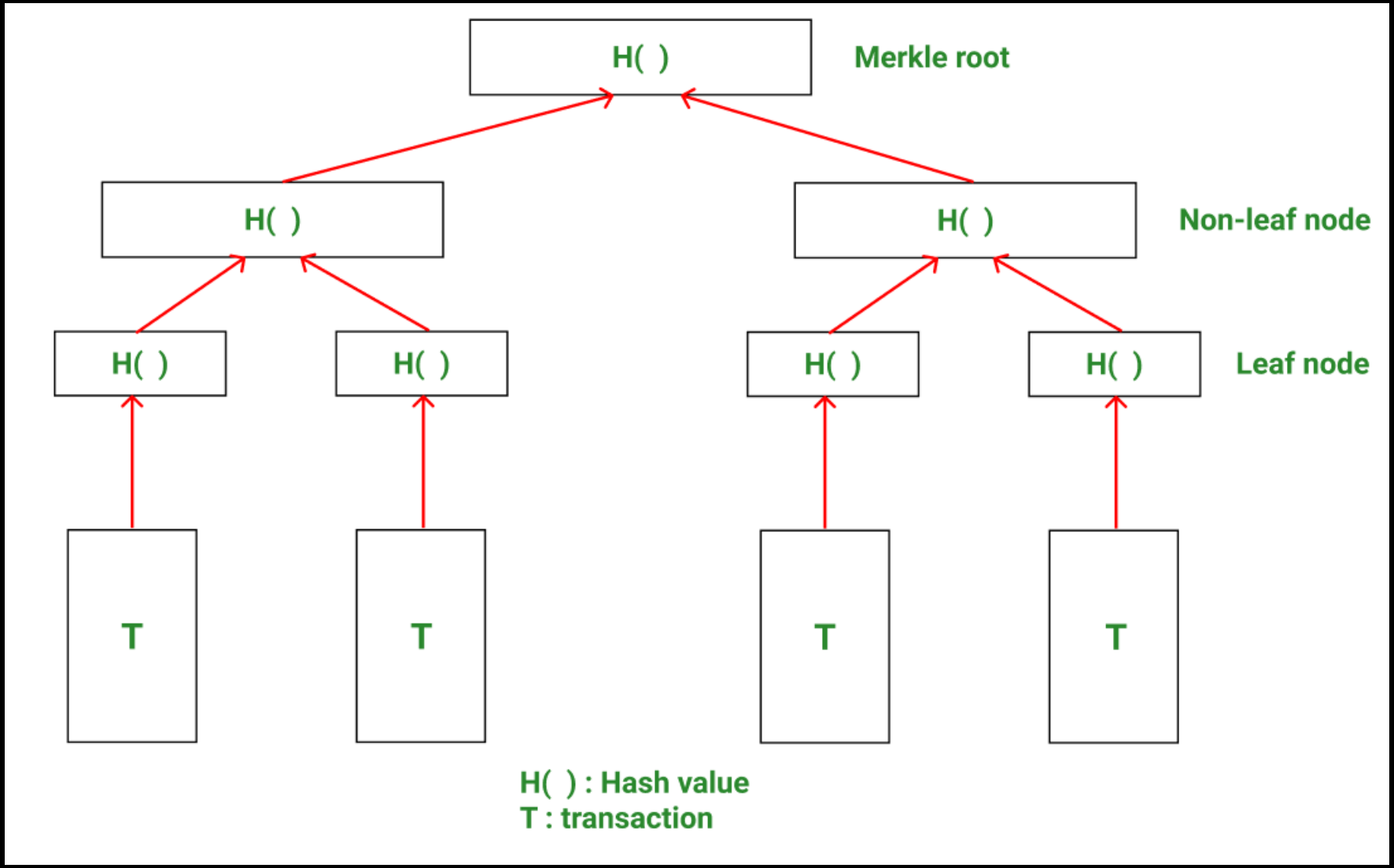
What do we need?

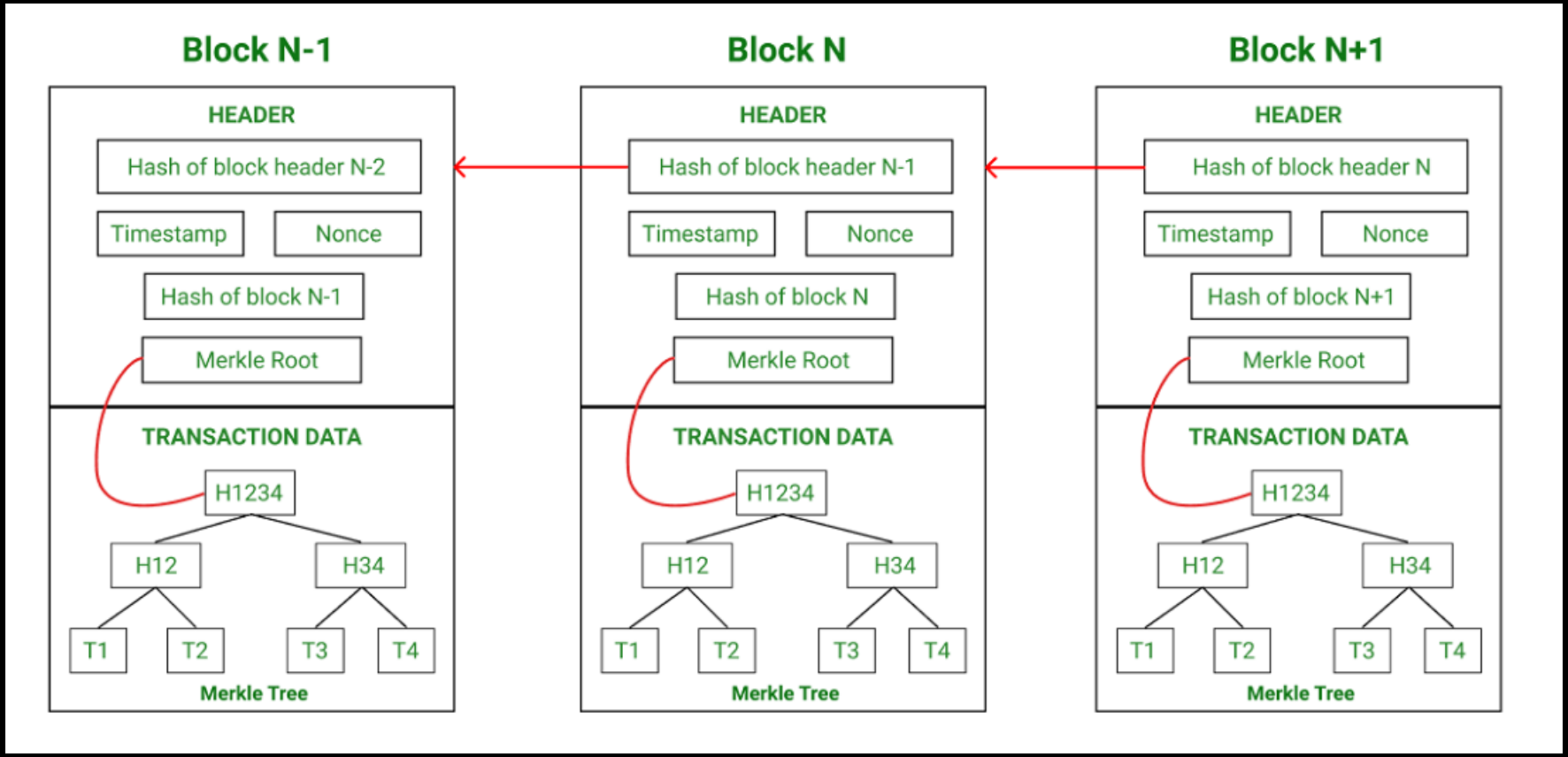
- Efficient way to reach consensus
- Enforces append-only nature
- Resilient to sybil attacks
  - Hard to get an outsized influence on the network

Idea 1: Use Hash Functions




Hash Pointer
Pointer to data
Hash of data
Data


H( )
Merkle root
H( )
H( )
Non-leaf node
H( )
H( )
H( )
H( )
Leaf node
T
T
T
T
H( ) : Hash value
T : transaction


Block N-1
HEADER
Hash of block header N-2
Timestamp
Nonce
Hash of block N-1
Merkle Root
TRANSACTION DATA
H1234
H12
H34
T1
T2
T3
T4
Merkle Tree
Block N
HEADER
Hash of block header N-1
Timestamp
Nonce
Hash of block N
Merkle Root
TRANSACTION DATA
H1234
H12
H34
T1
T2
T3
T4
Merkle Tree
Block N+1
HEADER
Hash of block header N
Timestamp
Nonce
Hash of block N+1
Merkle Root
TRANSACTION DATA
H1234
H12
H34
T1
T2
T3
T4
Merkle Tree

- This lets us check for consistency in an efficient manner
- However, we still have our sybil problem

Idea 2: Hard Consensus Problem

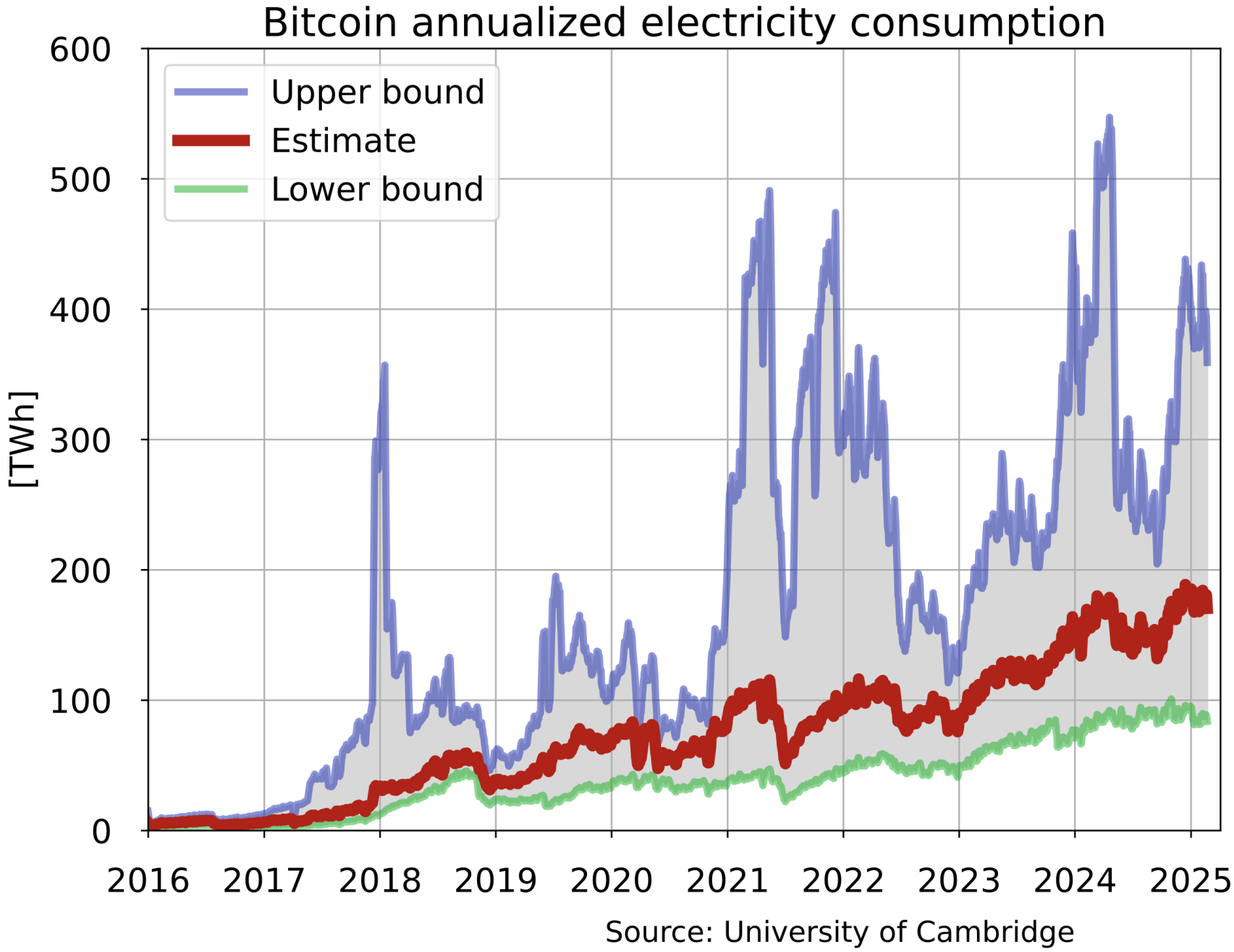
- Need some way to enforce how to add a change to the ledger
- Idea is for whoever is proposing the chain to have to meet some requirement
  - All the other peers should easily be able to verify this
- Only add a block to your view of the ledger if it verifies
- Ideally, this limits who can propose new blocks

Proof of Work

- Introduced in 1993 by Dwork and Naor
- Originally intended to prevent denial of service and spam
- Make everyone have to do something computationally hard
- Core idea is setting a hash rate
  - Need to brute force a hash with a certain number of leading 0s

Proof of Work Consensus

- For a new block to be accepted, the proposer must demonstrate that they completed the proof of work
- For bitcoin hashrate is roughly 10 minutes
- Wait for a few blocks to be confirmed to be certain
- Doesn’t quite solve the 51% attack
- Enviromental Impact ☹


Bitcoin annualized electricity consumption
Upper bound
Estimate
Lower bound
[TWh]
600
500
400
300
200
100
0
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
Source: University of Cambridge

Proof of Work is expensive!

- Proof of Work only works if you assume a large amount of the network is trying to propose the next block
  - Otherwise the active members can control what happens
- Requires contributing a lot of computational resources
  - How to incentivize participation?
- Enter Cryptocurrencies

Bitcoin

- A cryptocurrency proposed by Satoshi Nakamoto in 2009
  - Who?
- A cryptocurrency is a decentralized payment system, generally built on top of a blockchain
  - Bitcoin was first prominent example, but ecash dates back to 1983
- Blockchains and cryptocurrencies have a bit of a symbiotic relationship

The Bitcoin Protocol

- Uses a proof-of-work based blockchain
- Peers run the bitcoin client which manages interaction with the rest of the network
  - Official vs Unofficial Clients
- A P2P payment system

Bitcoin Mining

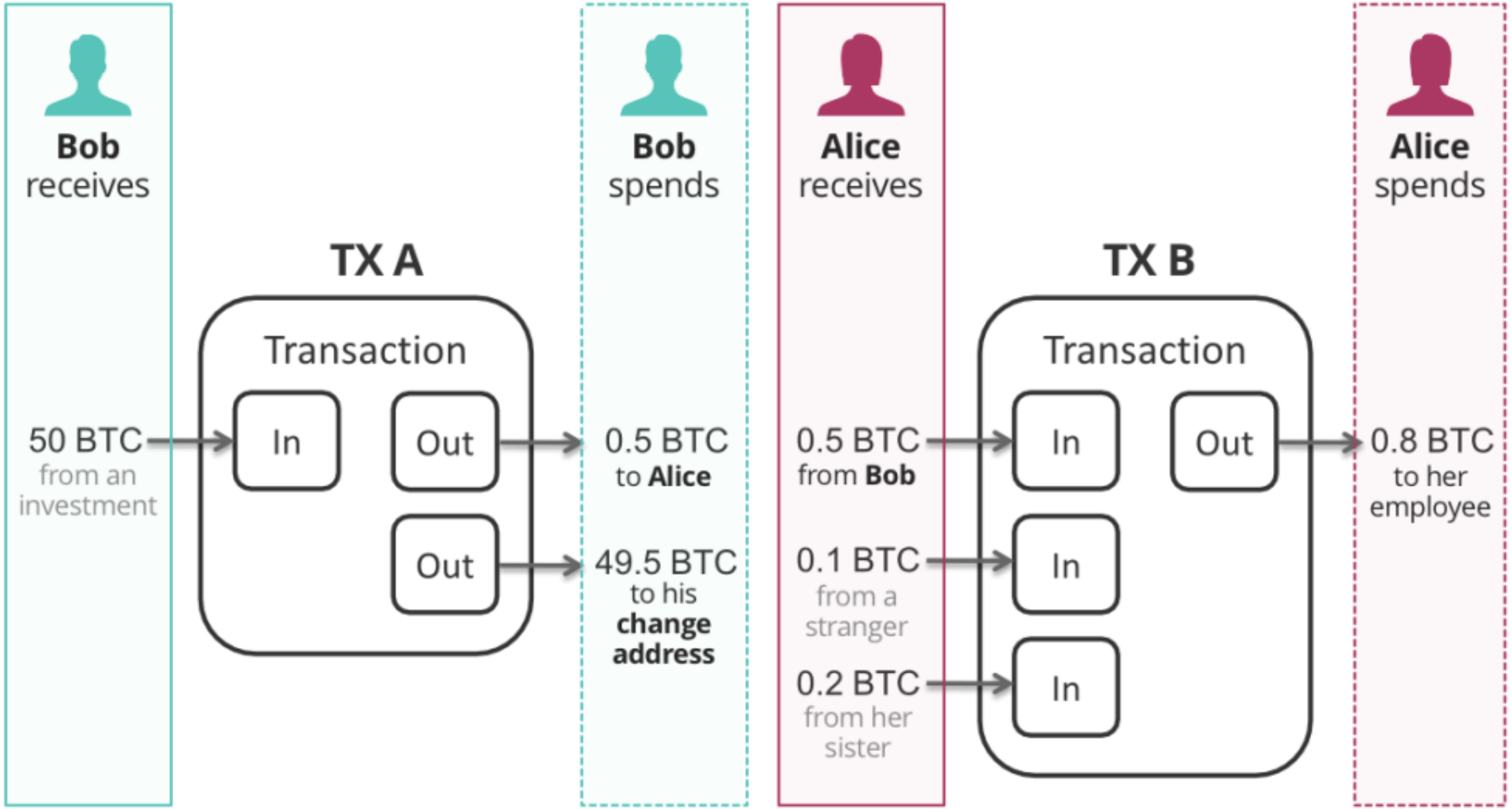
- Miners are the peers competing to generate the next block
- The goal was 1 person 1 vote
- Miners are incentivized as having your block accepted comes with come Bitcoin as a reward

Bitcoin Accounts and Transactions

- Your bitcoin account is represented by a public key pair
  - Each of your bitcoins is “signed”
  - Linked to the public key and possession of private key shows ownership
  - What happens if you lose your key?

- ”Spending” a coin involves using your private key and the recipients public key

- You produce a transaction that is sent to the network


Bob
receives
50 BTC
from an
investment
TX A
Transaction
In
Out
Out
Bob
spends
0.5 BTC
to Alice
49.5 BTC
to his
change
address
Alice
receives
0.5 BTC
from Bob
0.1 BTC
from a
stranger
0.2 BTC
from her
sister
TX B
Transaction
In
In
In
Out
Alice
spends
0.8 BTC
to her
employee

Bitcoin transactions

- Peers, and in particular, miners see new transactions as they are broadcast to the network
- Miners include the transactions they see into the blocks they propose
  - They get a “fee” for including a transaction
- Once a block containing a transaction is confirmed by the network, it is officially considered spent
  - Why is this binding?

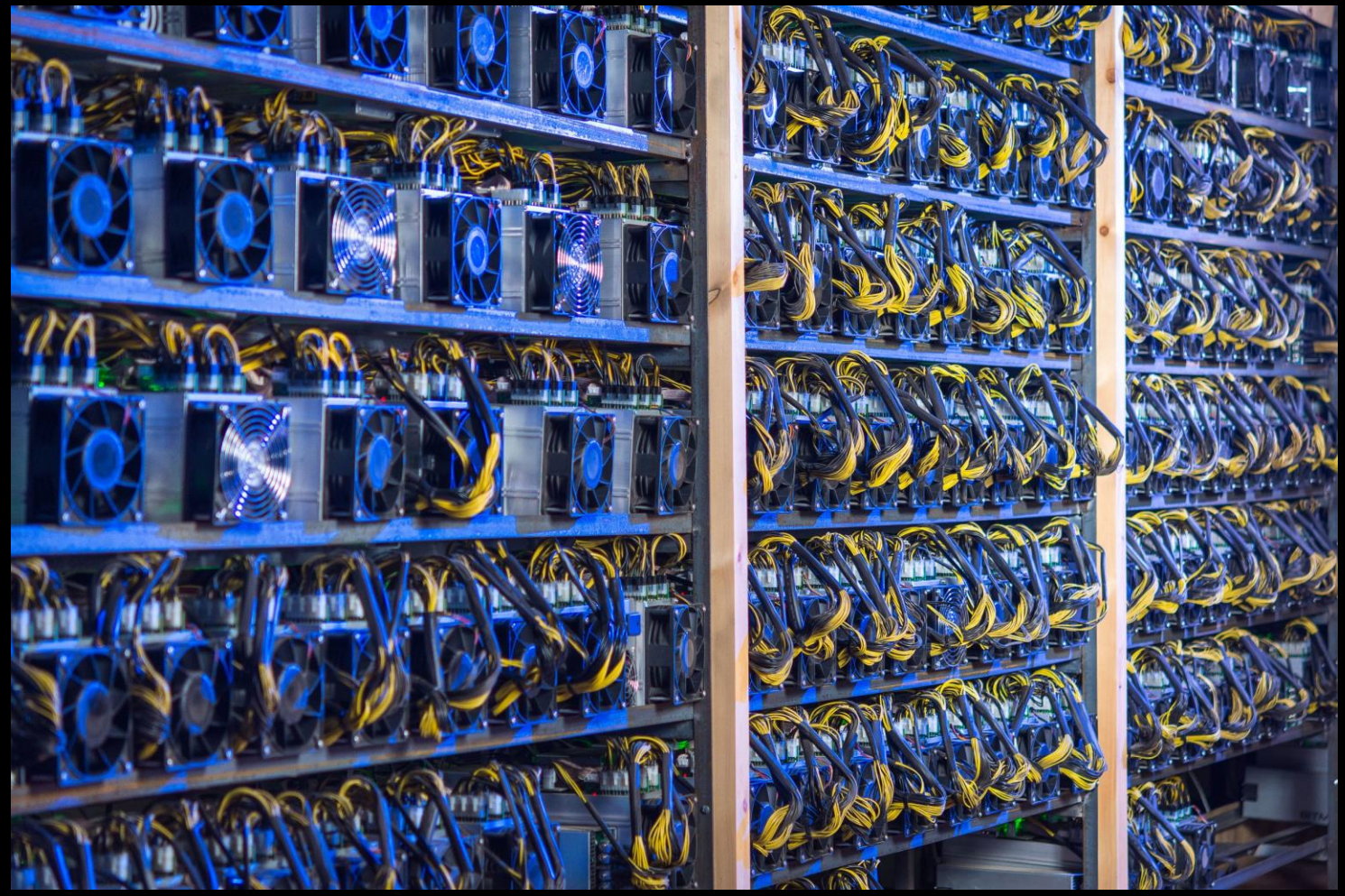
How to get Bitcoin

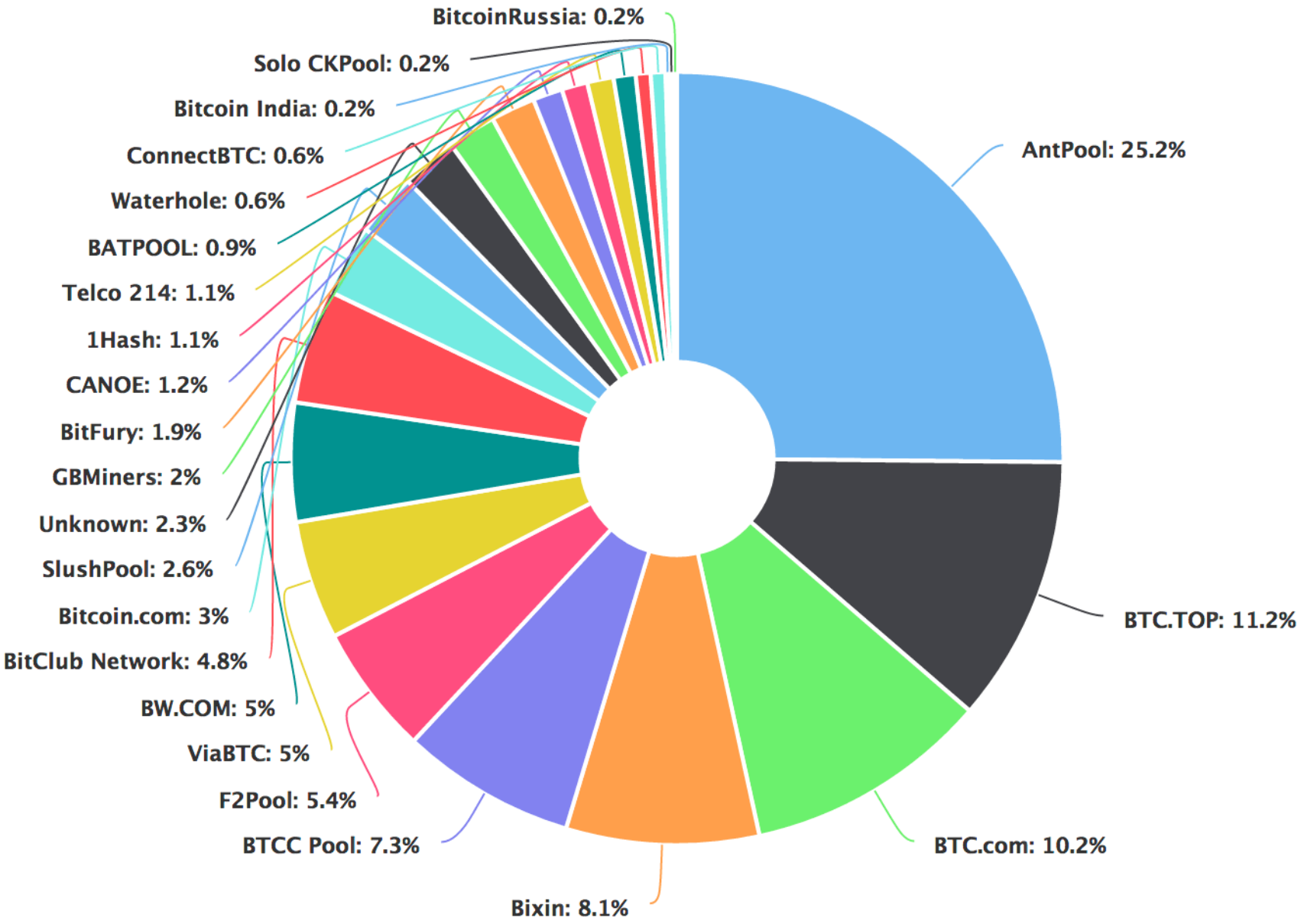
- Exchanges
- Mine a new block and get a reward
- Mine a new block and get fees

Challenges and considerations

- Not exactly ”1 person 1 vote”
- Exchanges can lead to some centralization
- Fees can get quite high
- Hard to change
- Is it actually private?

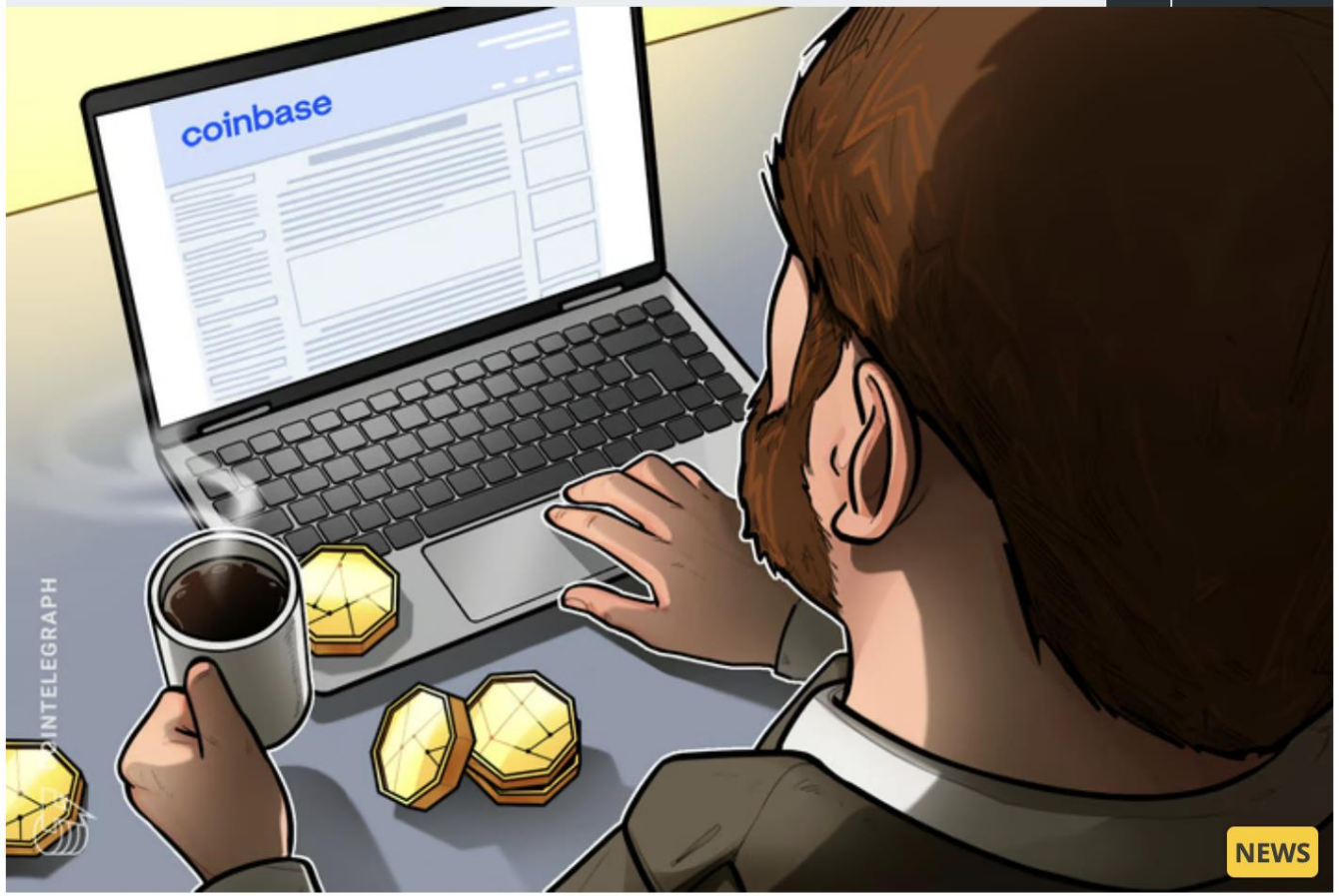
Modern Mining

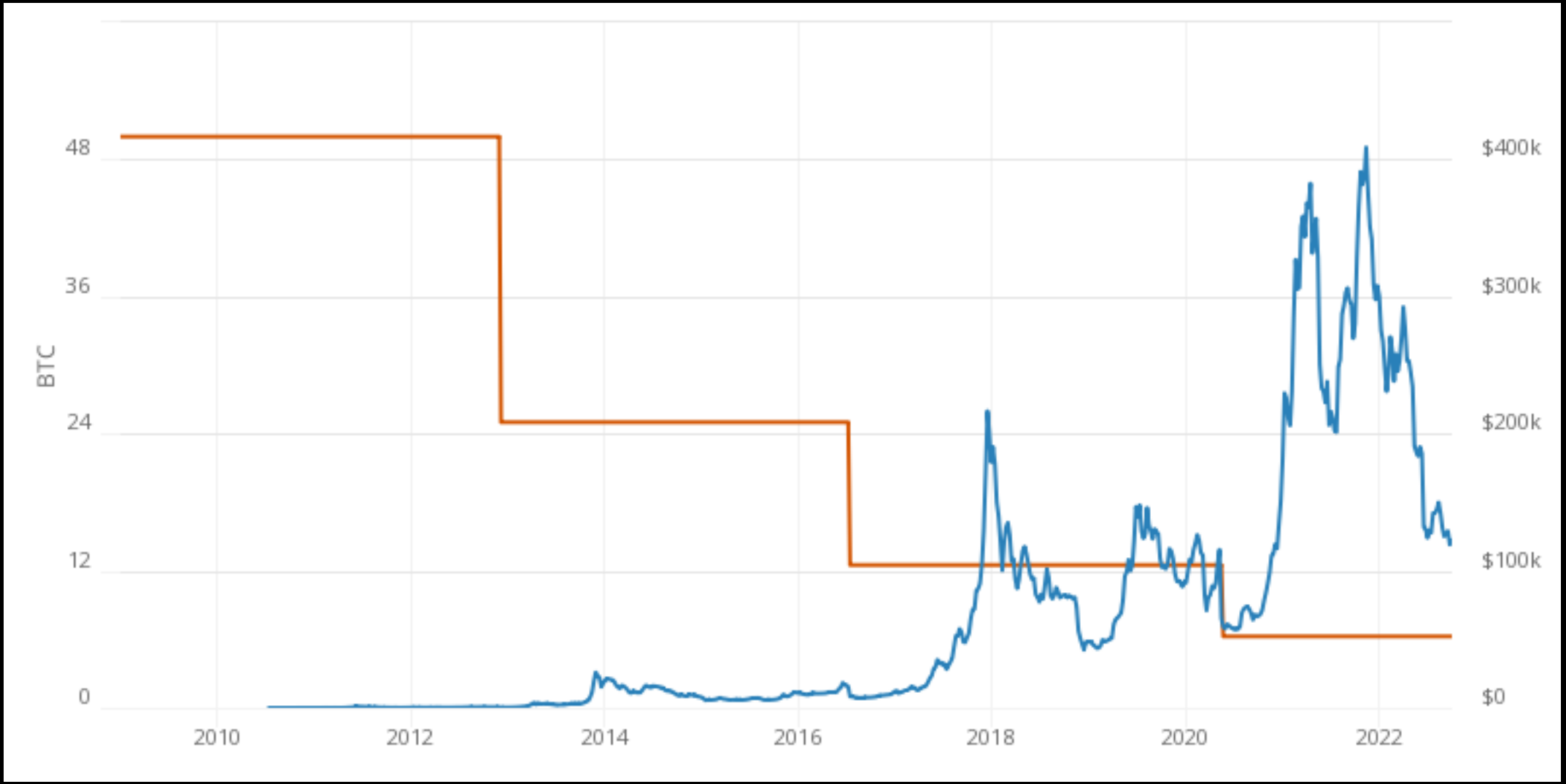



BitcoinRussia: 0.2%
Solo CKPool: 0.2%
Bitcoin India: 0.2%
ConnectBTC: 0.6%
Waterhole: 0.6%
BATPOOL: 0.9%
Telco 214: 1.1%
1Hash: 1.1%
CANOE: 1.2%
BitFury: 1.9%
GBMiners: 2%
Unknown: 2.3%
SlushPool: 2.6%
Bitcoin.com: 3%
BitClub Network: 4.8%
BW.COM: 5%
ViaBTC: 5%
F2Pool: 5.4%
BTCC Pool: 7.3%
Bixin: 8.1%
BTC.com: 10.2%
BTC.TOP: 11.2%
AntPool: 25.2%

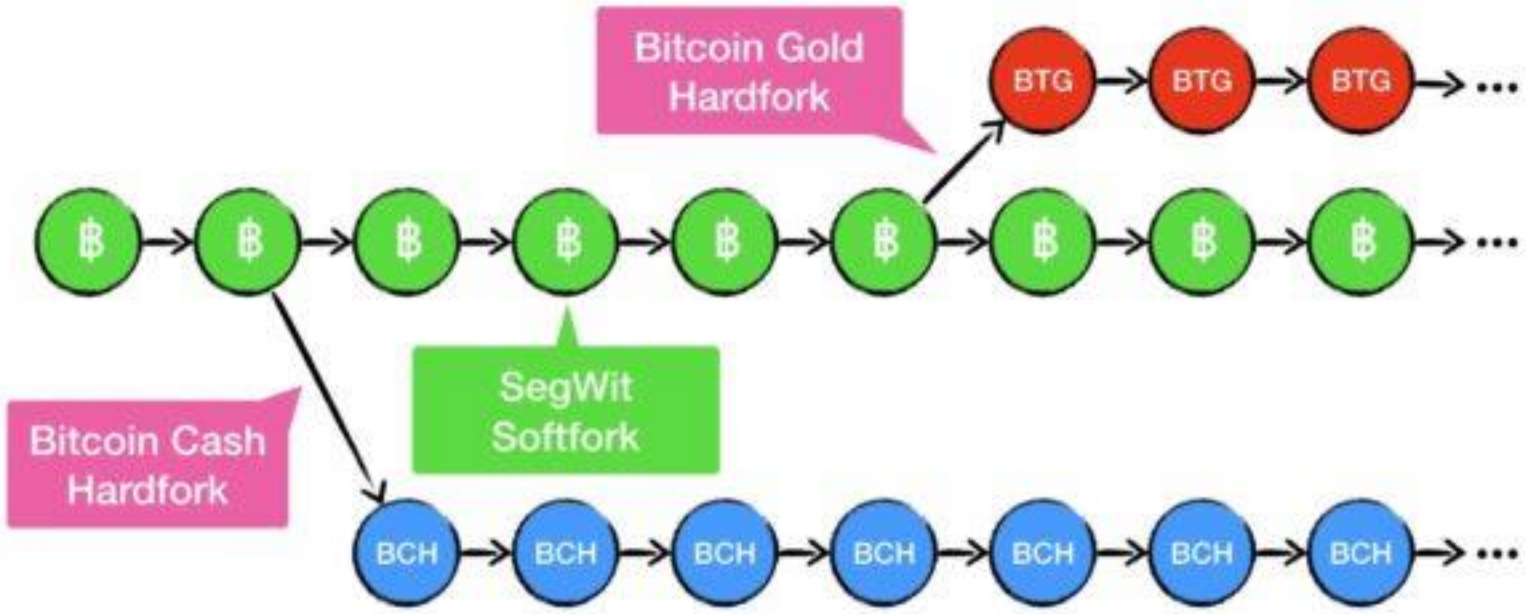
Coinbase website down as crypto exchange cites ‘system-wide outage’

Crypto exchange Coinbase suffered a “system-wide” outage, rendering the platform unusable.




BTC
48
36
24
12
0
$400k
$300k
$200k
$100k
$0
2010
2012
2014
2016
2018
2020
2022

Bitcoin Forks 2017



Is Bitcoin private/anonymous

- Account is only linked to your key pair
  - More like a pseudonym
  - Often gets reused

- Transactions are only linked to this account as well

PRESS RELEASE

Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside

Monday, June 7, 2021

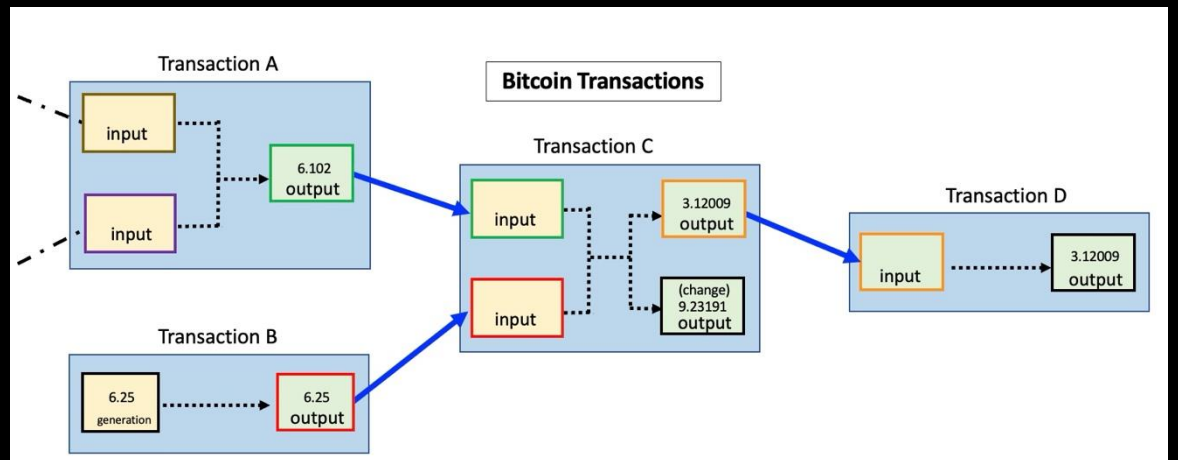
For Immediate Release

Office of Public Affairs

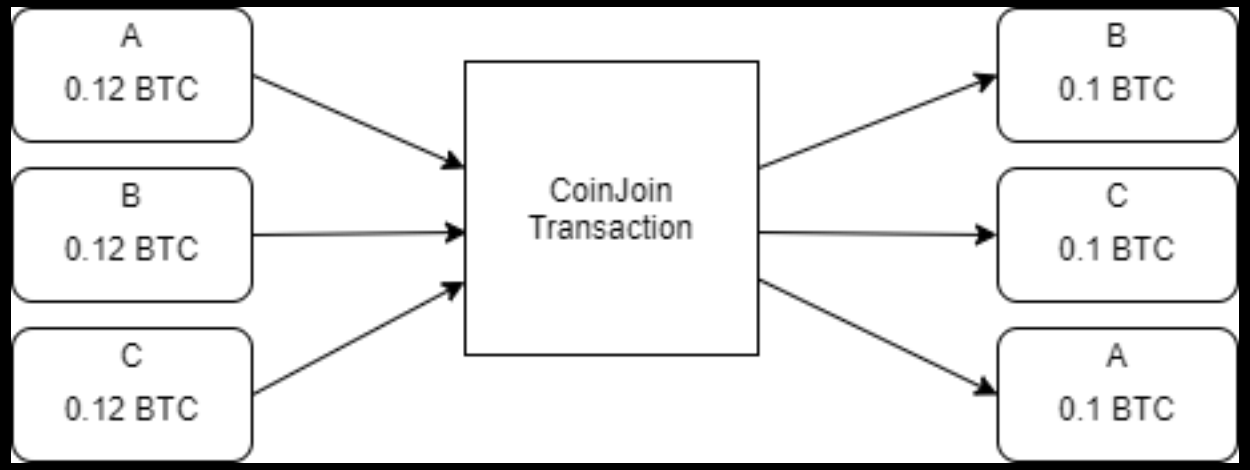
https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

Bitcoin transaction graph

- Recall, blockchains are public by design
- Each bitcoin has a publicly viewable history
  - Albeit pseudonymous
- Arguably less private in some senses



Shuffles and Mixes



Other types of cryptocurrencies

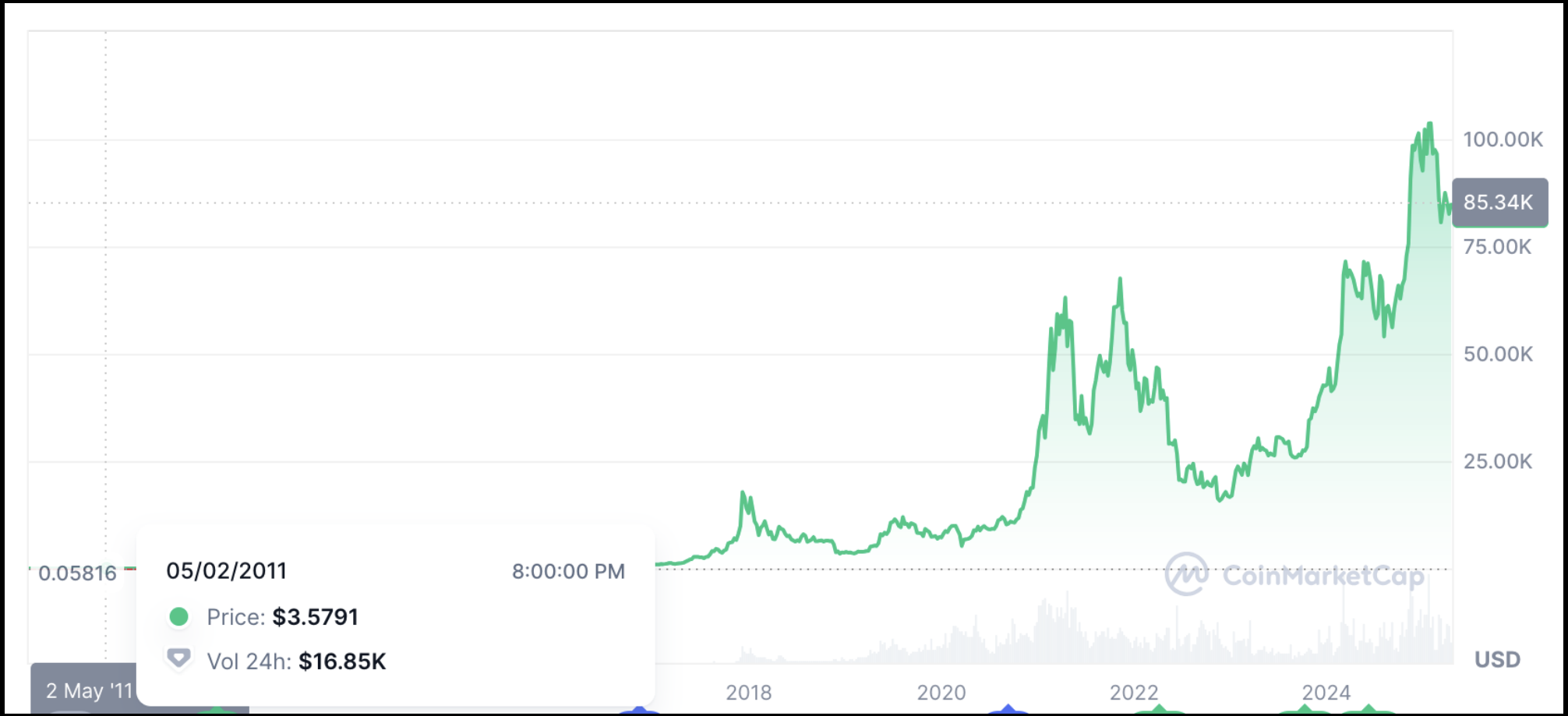
- Can vary in consensus algorithm, level of decentralization, hashrate, blocksize, and more

- Bitcoin-likes
  - Litecoin
  - Dogecoin

- Private
  - Monero
  - Zcash
  - Dash

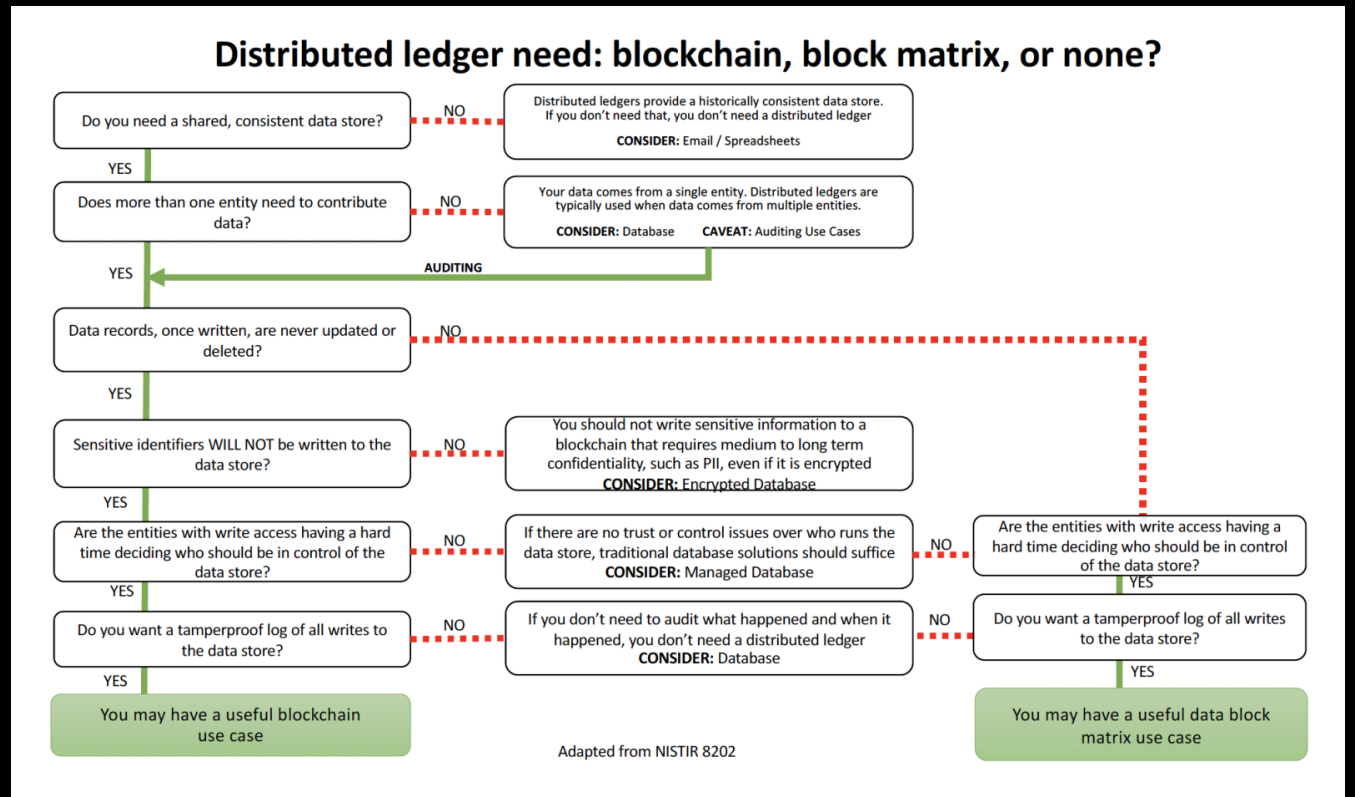
- More featured
  - Ethereum
    - Proof-of-Stake
    - Smart Contracts
    - Bitcoin also has scripts but they are much more limited

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
1	Bitcoin BTC	$84,749.77	0.31%	0.92%	3.39%	$1,682,503,962,449	$26,089,305,002 309.35K BTC	19.85M BTC
2	Ethereum ETH	$1,598.38	0.32%	1.06%	0.35%	$192,922,139,733	$14,159,313,358 8.89M ETH	120.69M ETH
3	Tether USDT	$0.9994	0.00%	0.07%	0.00%	$144,731,860,004	$54,855,015,423 54.86B USDT	144.8B USDT
4	XRP XRP	$2.10	0.50%	1.13%	4.33%	$123,016,655,899	$2,989,425,304 1.42B XRP	58.33B XRP
5	BNB BNB	$586.88	0.09%	0.79%	1.55%	$82,686,271,375	$1,407,570,581 2.40M BNB	140.89M BNB
6	Solana SOL	$133.85	0.64%	6.26%	16.35%	$69,124,668,854	$4,611,940,014 34.72M SOL	516.4M SOL
7	USDC USDC	$0.9997	0.00%	0.04%	0.03%	$60,388,497,925	$10,098,301,637 10.09B USDC	60.4B USDC
8	TRON TRX	$0.2471	0.41%	2.89%	2.70%	$23,471,239,666	$728,744,274 2.94B TRX	94.95B TRX
9	Dogecoin DOGE	$0.1567	0.05%	2.05%	0.15%	$23,332,299,794	$736,963,088 4.71B DOGE	148.88B DOGE
10	Cardano ADA	$0.6212	0.67%	2.29%	0.69%	$21,921,031,485	$583,286,563 947.23M ADA	35.28B ADA


100.00K
85.34K
75.00K
50.00K
25.00K
0.05816
05/02/2011
8:00:00 PM
Price: $3.5791
Vol 24h: $16.85K
CoinMarketCap
USD
2 May '11
2018
2020
2022
2024

Blockchain proposed applications

- Cryptocurrencies
- Distributed Apps (dApps)
  - Web 3.0



Next Time

Federation, DRM, and Open Source