UNSW SYDNEY | Australia's Global University

An Introduction to Blockchain and Distributed Ledger Technology

Ron van der Meyden

UNSW School of Computer Science and Engineering

The source of the buzz …

Bitcoin: A Peer-to-Peer Electronic Cash System ,
Satoshi Nakamoto, 2009

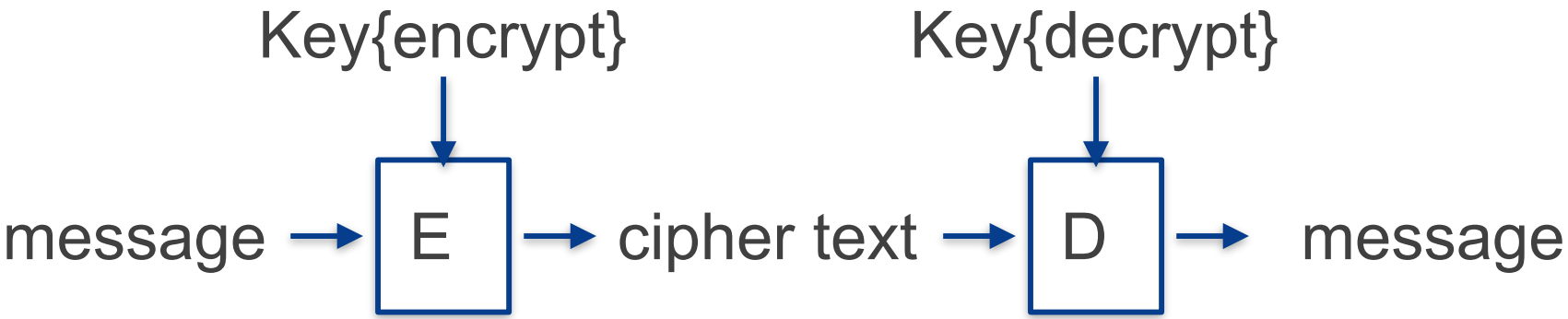
???????

Crypto-Currency: Some History

Digital Cash - Commerce on the Net, Peter Wayner (1996)

- First Virtual
- IBM: iKP
- Netcash, Netcheque
- Cybercash
- Cybercoin
- SET
- Millicent
- MicroMint
- Magic Money
- Netbill …..

A Little Cryptography



Public key cryptography:

Key{encrypt} ≠ Key{decrypt}

(public) (private)

Public Key Signatures:

Key{encrypt} = Private signature key

Key{decrypt} = Public signature verification key

A naive attempt at digital cash

01111000101011001010101011111110010101010101000001010101111010010

= “This message is worth $100”, signed Governor of the Reserve Bank

A naive attempt at digital cash

01111000101011001010101011111110010101010101000001010101111010010

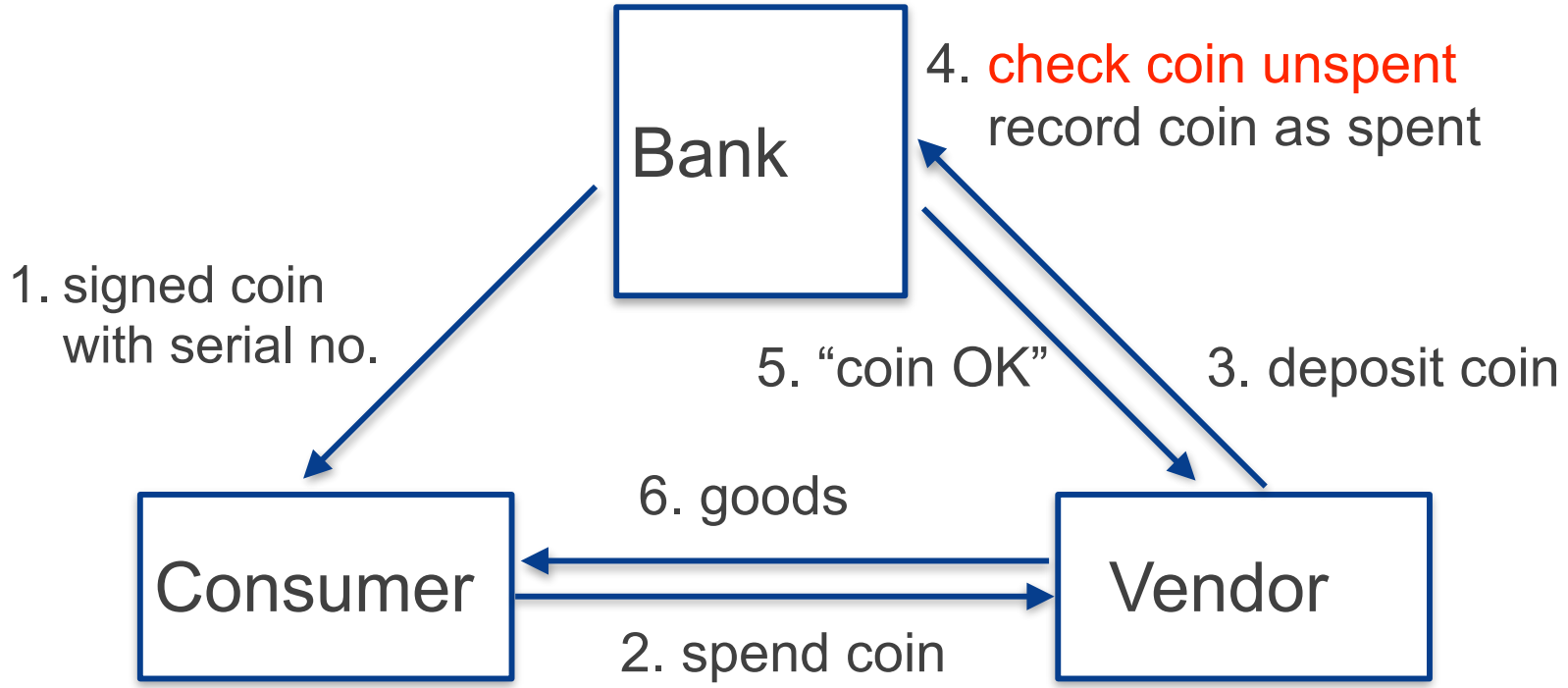
= “This message is worth $100”, signed Governor of the Reserve Bank

=copy => “This message is worth $100”, signed Governor of the Reserve Bank”

=copy => “This message is worth $100”, signed Governor of the Reserve Bank”

=copy => “This message is worth $100”, signed Governor of the Reserve Bank”

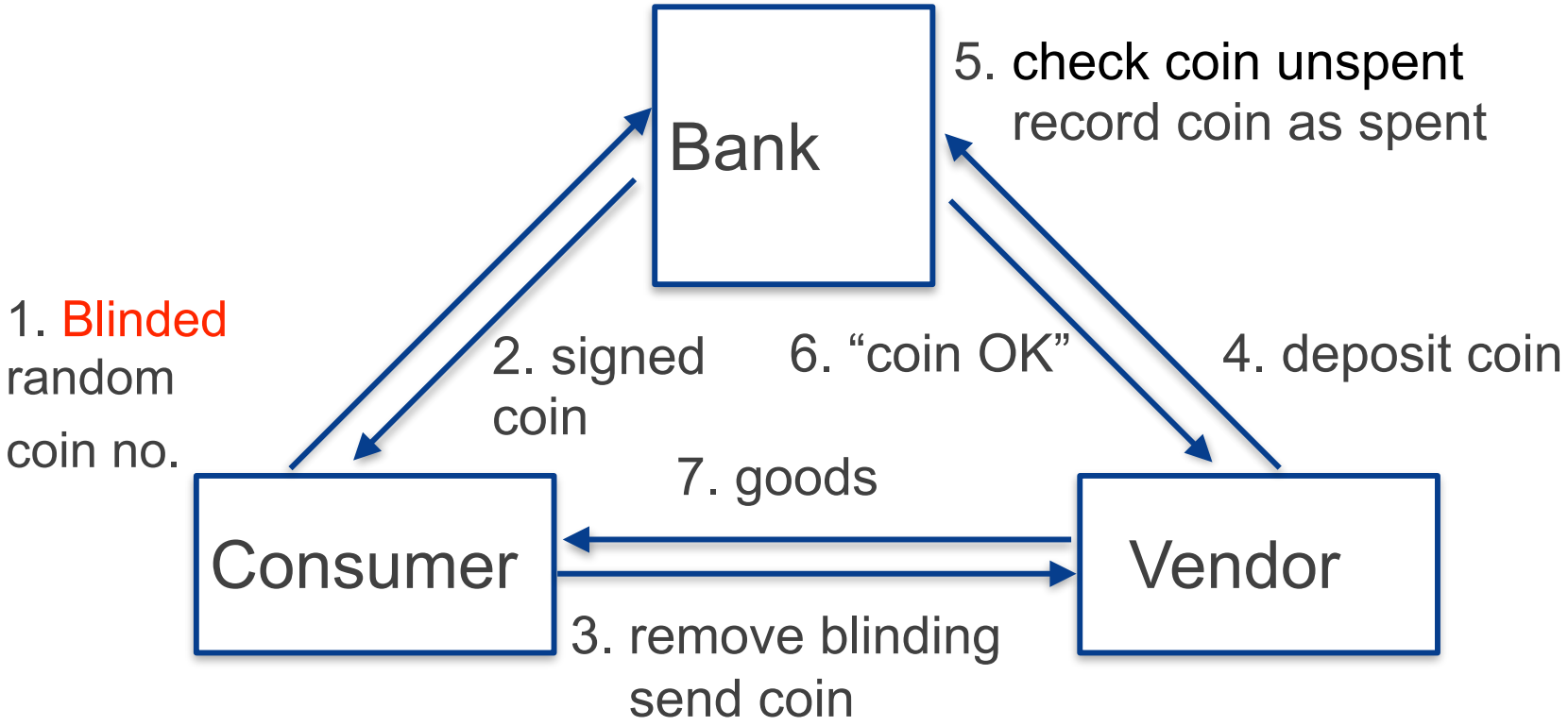
=copy => “This message is worth $100”, signed Governor of the Reserve Bank”



Privacy properties:

- Vendor need not learn consumer identity
- Bank learns where consumer spent their money

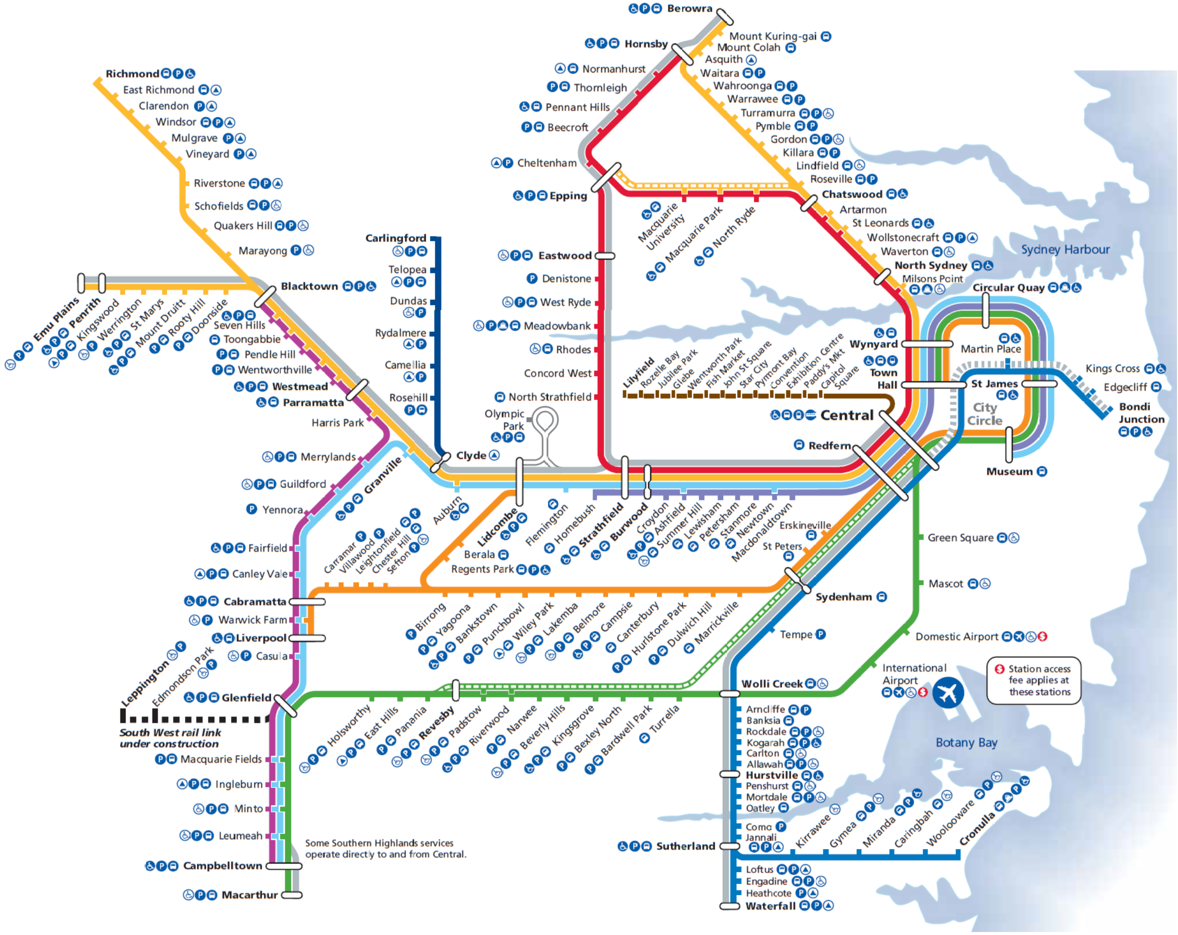
Digicash (Chaum 1983)

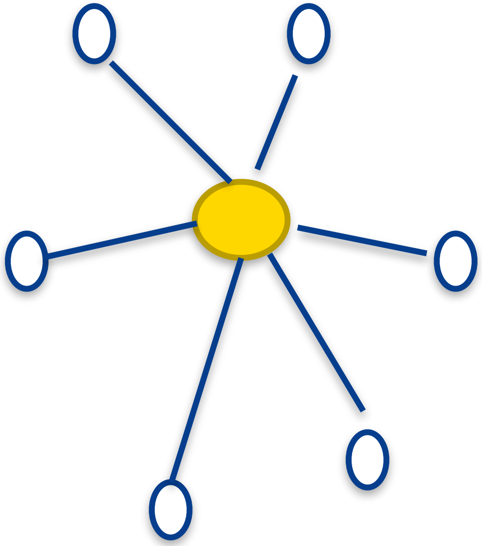


Privacy Protections:

- Vendor need not learn consumer identity
- Bank does not learn where consumer spent their money

Centralised Systems





Google

facebook

amazon.com

Problems with centralisation

Congestion

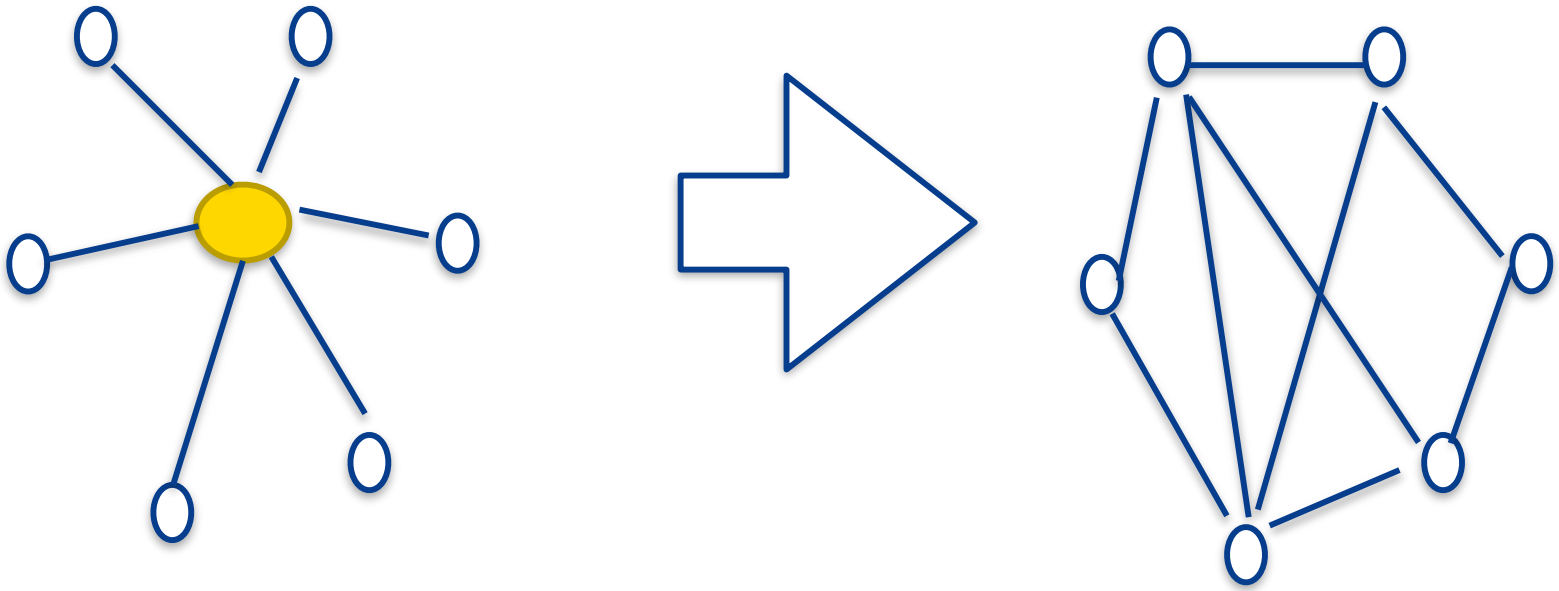
Not resilient to failure/corruption of central nodes

Privacy risks: “All your data are belong to us!”

Central node can censor, deny access

The Key Theme of Distributed Computing

Decentralisation!



Business impact: Disintermediation!

Bitcoin Composition

Bitcoin Security Properties

•(Eventually, probably) Immutable history of transactions

- Pseudonymous identity (multiple keys/person)
- Censorship resistance
- Byzantine fault-tolerant consensus formation
- Lack of central authority / single point of failure

Cryptographic Hash Functions

H: Long strings -> short numbers

Given x, **easy** to compute H(x)

Given y, **very hard** to find x such that H(x) = y

Given x, H(x), **very hard** to find *another* x' such that H(x') = H(x)

=> Once H(x) has been recorded, it is **very hard** to tamper with x.

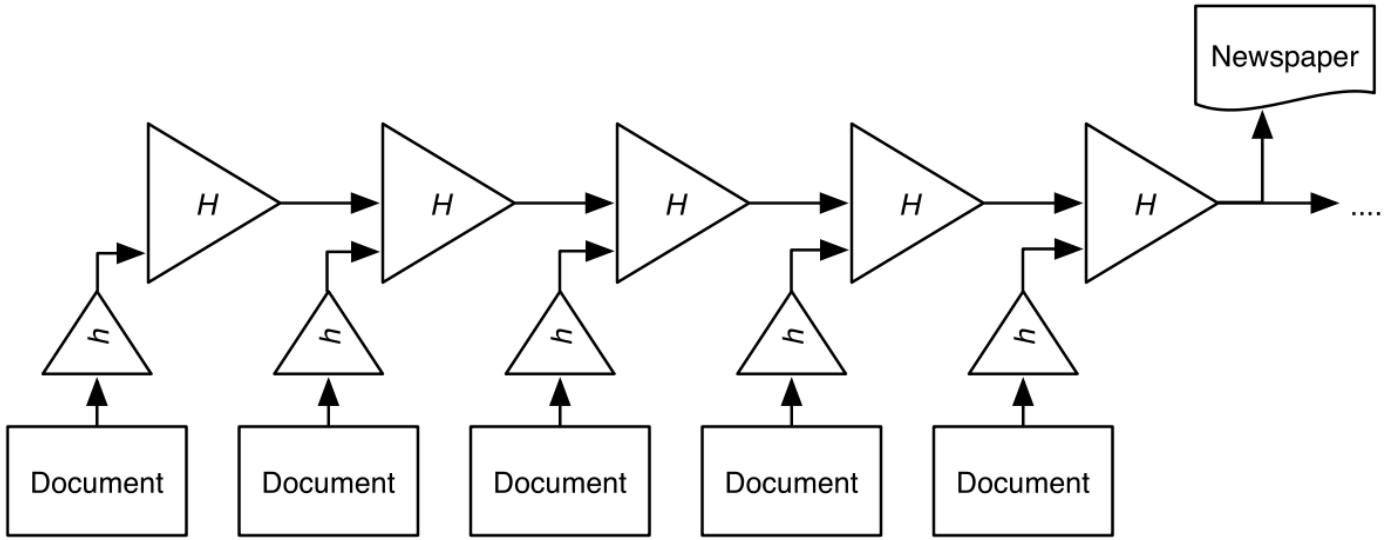
Best know way to find x given y:

enumerate possible values of x,
compute h(x),
until h(x) = y

(This costs time/energy)

Secure Timestamping using Hash Chains

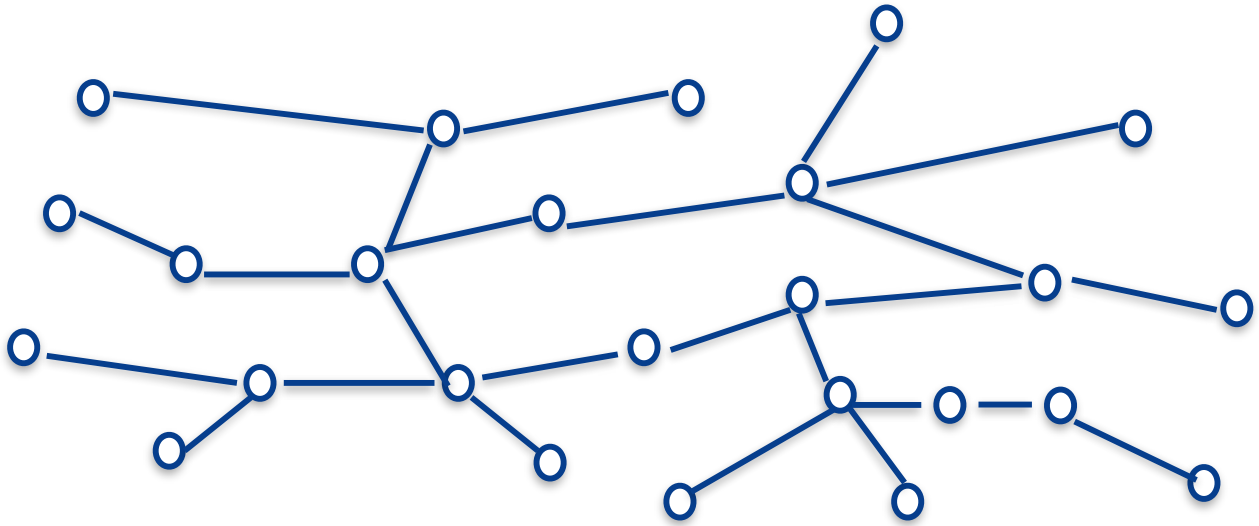
How to Time-Stamp a Digital Document,
Haber & Stornetta AT&T 1990



- Startup: Surety Technologies 1994—

Bitcoin Consensus Process

- **Open Network**: Anyone can join the network and contribute to maintaining the distributed ledger (be a “miner”)
- Transaction requests are broadcast to all nodes



- **Censorship resistance**: the miner proposing the next block of transactions is selected by a random process (hash puzzle)
- **Ledger Validity:** All miners check blocks proposed by others for correctness, ignore if not valid, else extend by adding a new block to the hash chain.

Spam: The Daily Mail you'd rather not get

You win $1M from Google! (*Give us all your private data first*)

Look at this funny cat video! (*that has a virus*)

You are invited to be Keynote Speaker! (*if you pay*)

Grow your hair back in ten days!!

Russian girl wants to meet you!

You have been hacked, verify your password here!

Cheap drugs!

"Proof of Work", an anti-spam mechanism

Idea: impose a (computation) cost on the sender

(Dwork & Naor, 1992, Back 1997)

Recipient produces random challenge C

Sender of message M must find X such that the first k bits of H(M,C,X) are 0…0

Proof of Work in Bitcoin

Miner of a set of transactions T extending previous block P must find X with

$$H(P,T,X) < N$$

N is tuned so expected time for network to find X ≈ 10min

- randomly distributes mining success by share of computational power, defeats sybil attacks (multiple sock puppet identities)
- defeats censorship
- *Blocks* of transactions, else 1 transaction/10mins

Incentivising Miners

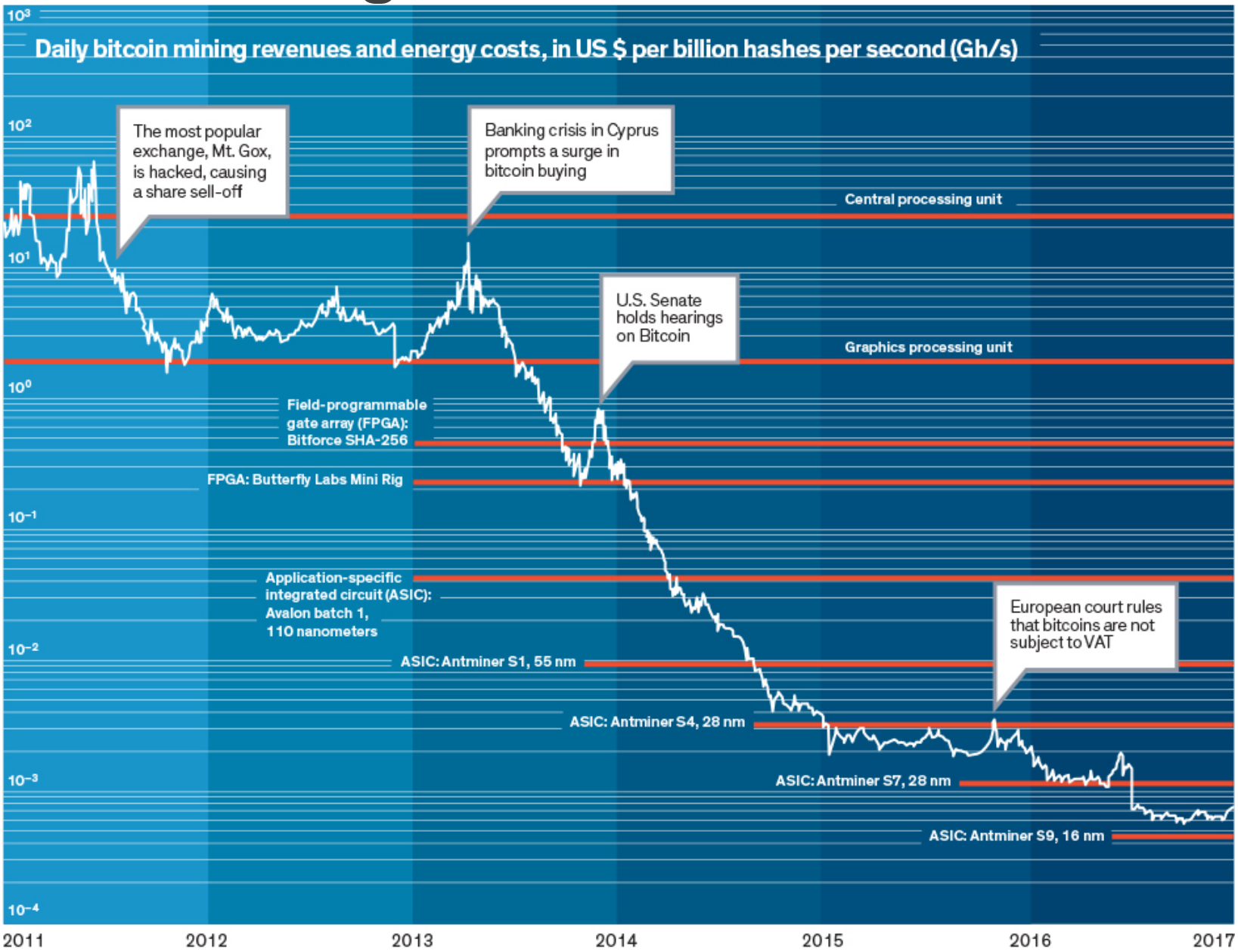
Why burn energy to mine blocks?

Miner Rewards:

- Miner gets to *create some new coins*, pay to self
- Miner collects *transaction fees* for transactions they included in a block

Profitable provided rewards exceed machinery/ energy costs

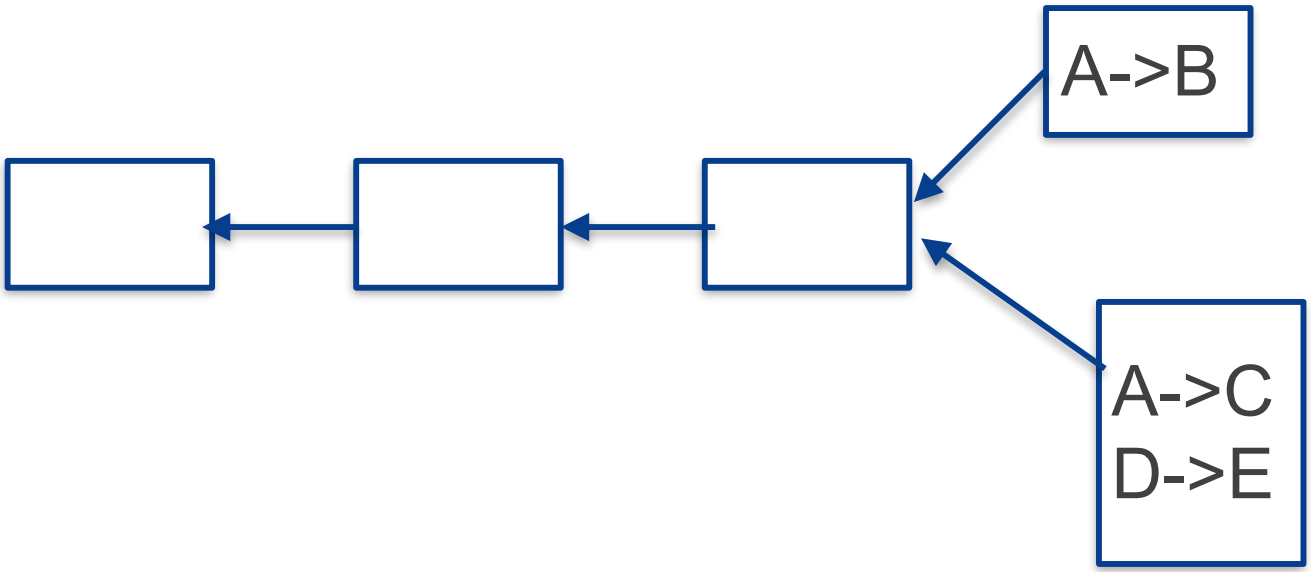
Mining costs vs revenues



Source: Harald Vranken, in *Current Opinion in Environmental Sustainability*, 2017, 28: 1–9

Chain Forks

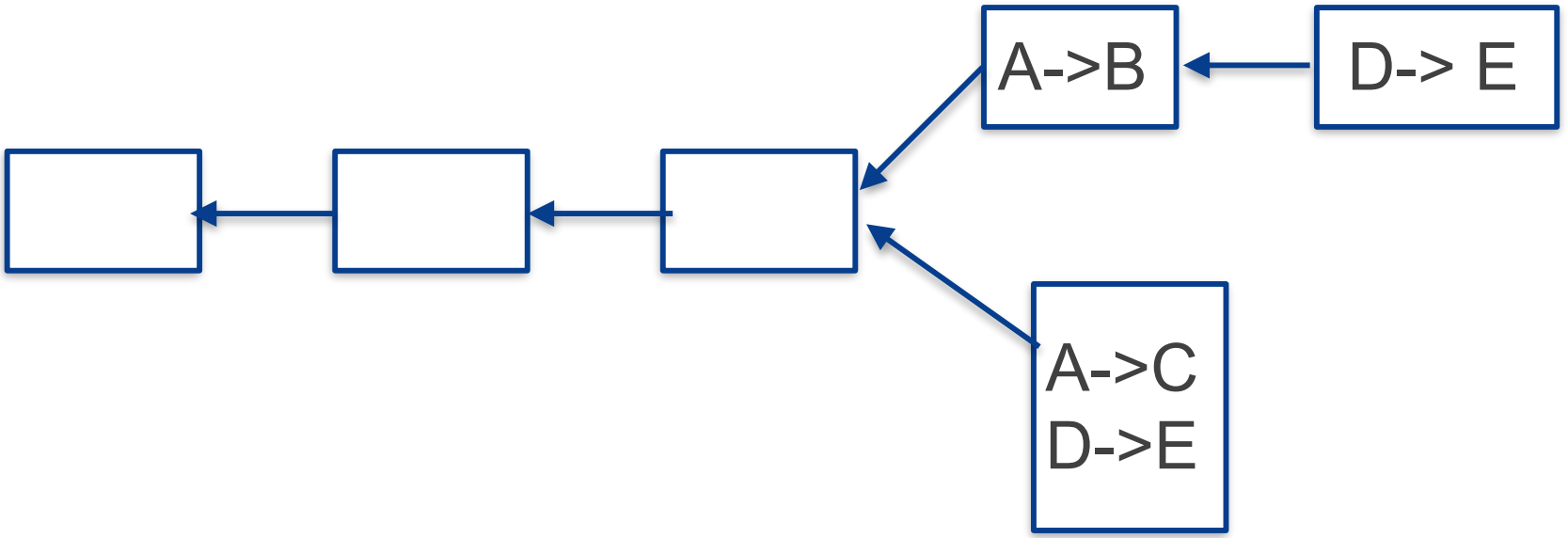
Two competing miners could still solve the hash puzzle at roughly the same time



Transactions on the branches may conflict (double spend!)

Chain Forks

One of the competing blocks is extended first (with high probability)



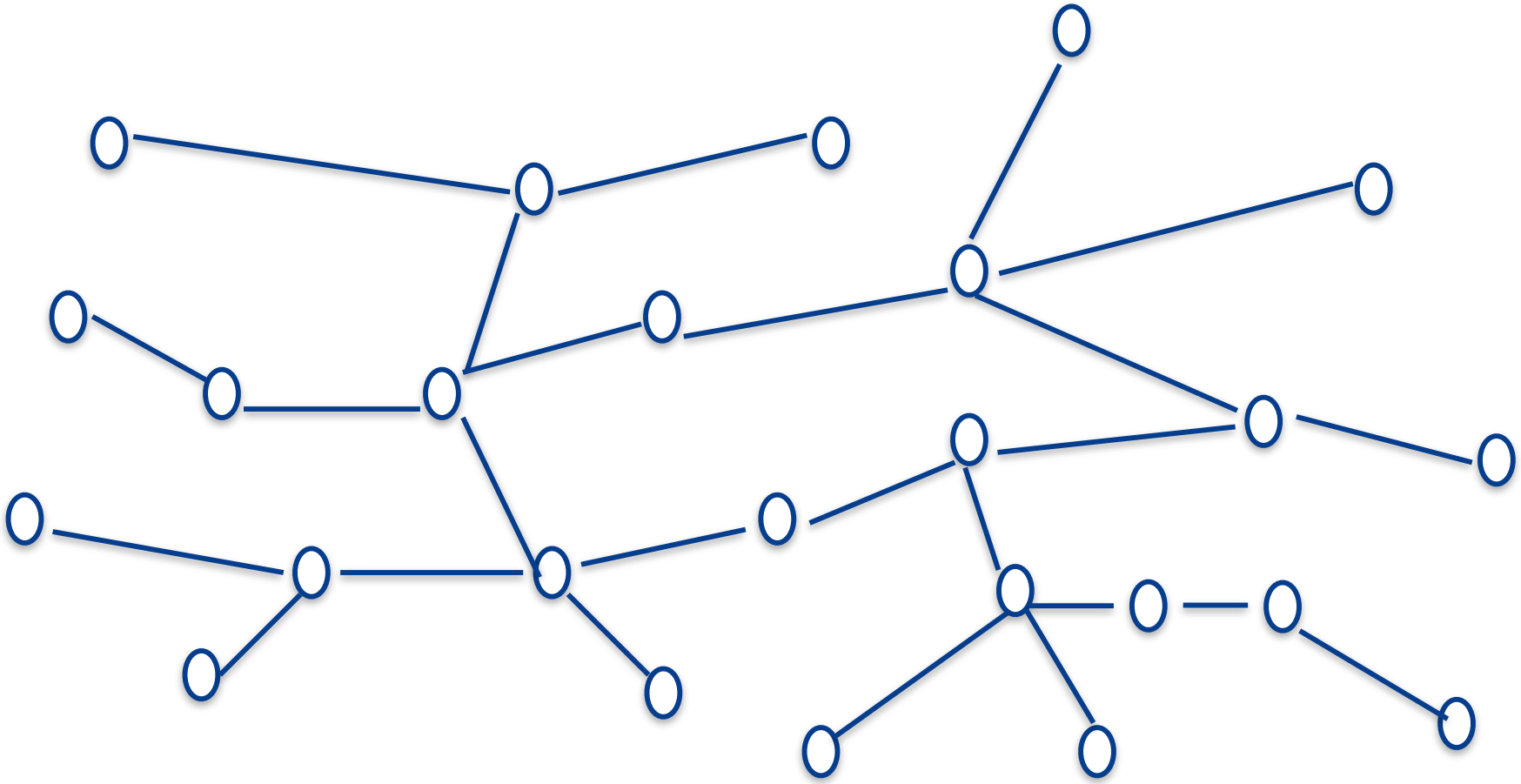
Bitcoin: the **longest** chain is the official history

The longest chain is that produced by the **majority of mining power**

Assumption: the majority of mining power is honest

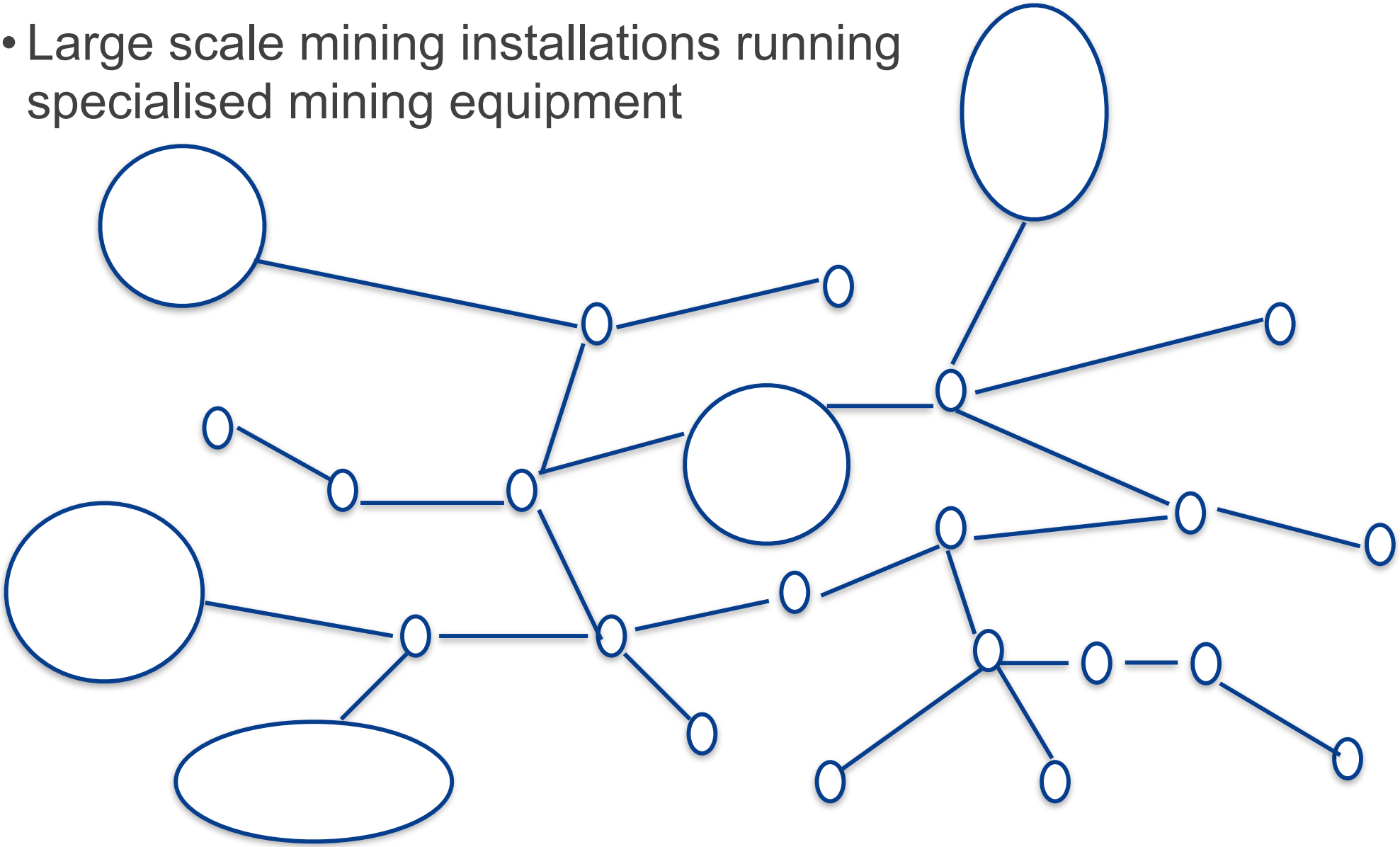
Nakamoto's vision for Bitcoin Consensus

- Anyone can be a miner



How it has played out (1)

- Large scale mining installations running specialised mining equipment

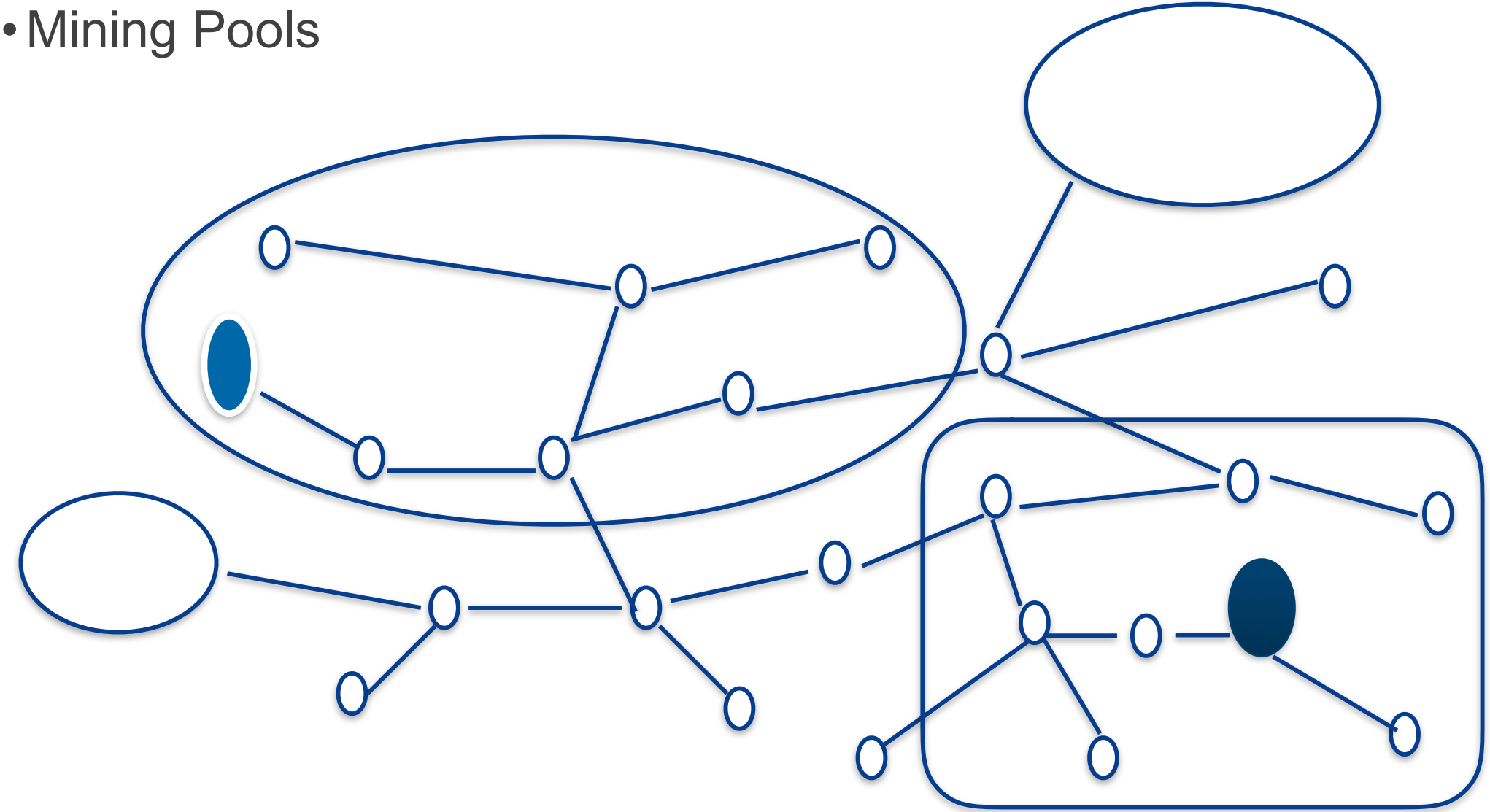


Bitcoin mining in Inner Mongolia

Photos: IEEE Spectrum Oct 2017

How it has played out (2)

- Mining Pools



``Is Bitcoin money?”

“The existence of a common and widely accepted medium of exchange rests on a convention: our whole monetary system owes its existence to the mutual acceptance of what, from one point of view, is no more than a fiction” —- Milton Friedman “Money Mischief - Episodes in Monetary History” 1992

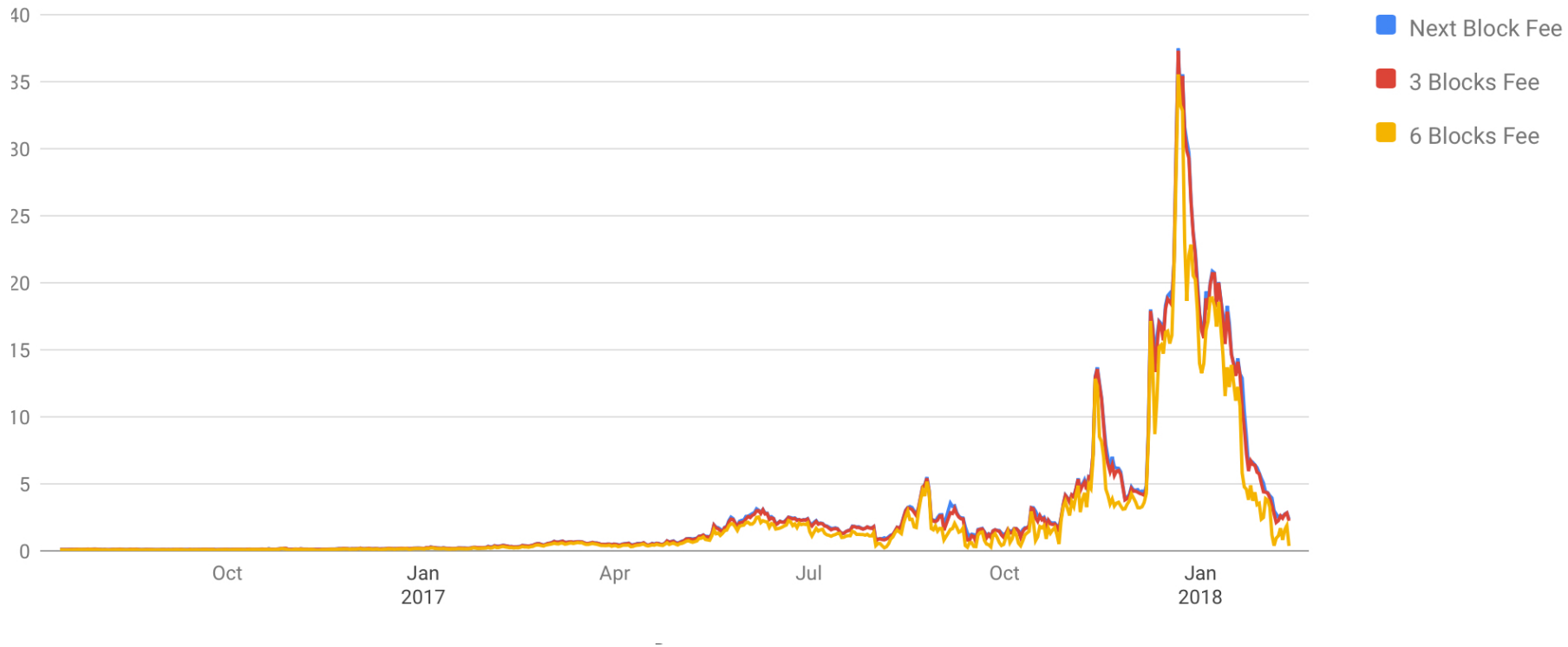
Bitcoin Transaction Rates

Time to have a transaction included in a block on the chain : 10 min

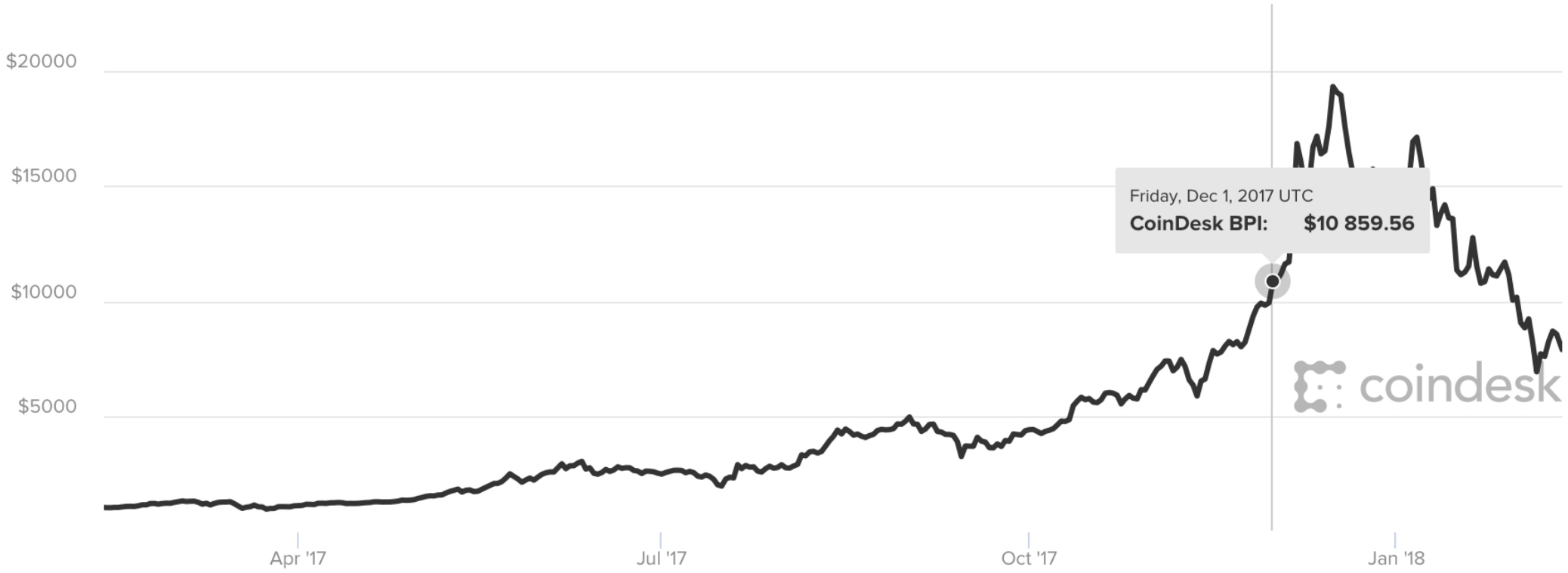
Recommended time to be confident that the trans. will stay on the *longest* chain: 6 blocks (60 mins)

Network throughput: 7 transactions/sec (cf. Visa 56,000 trans/sec)

Average transaction fees in $US from bitcoinfees.info:



Medium of exchange? / Unit of Account? / Store of Value?



Altcoins

Minor Variants of Bitcoin:

Litecoin, Bitcoin Cash, Dogecoin , ……

More expressive smart contract facility:

Ethereum, …

Variants with stronger privacy using advanced cryptographic techniques:

ZCash, Monero, ….

More rigorously engineered (?):

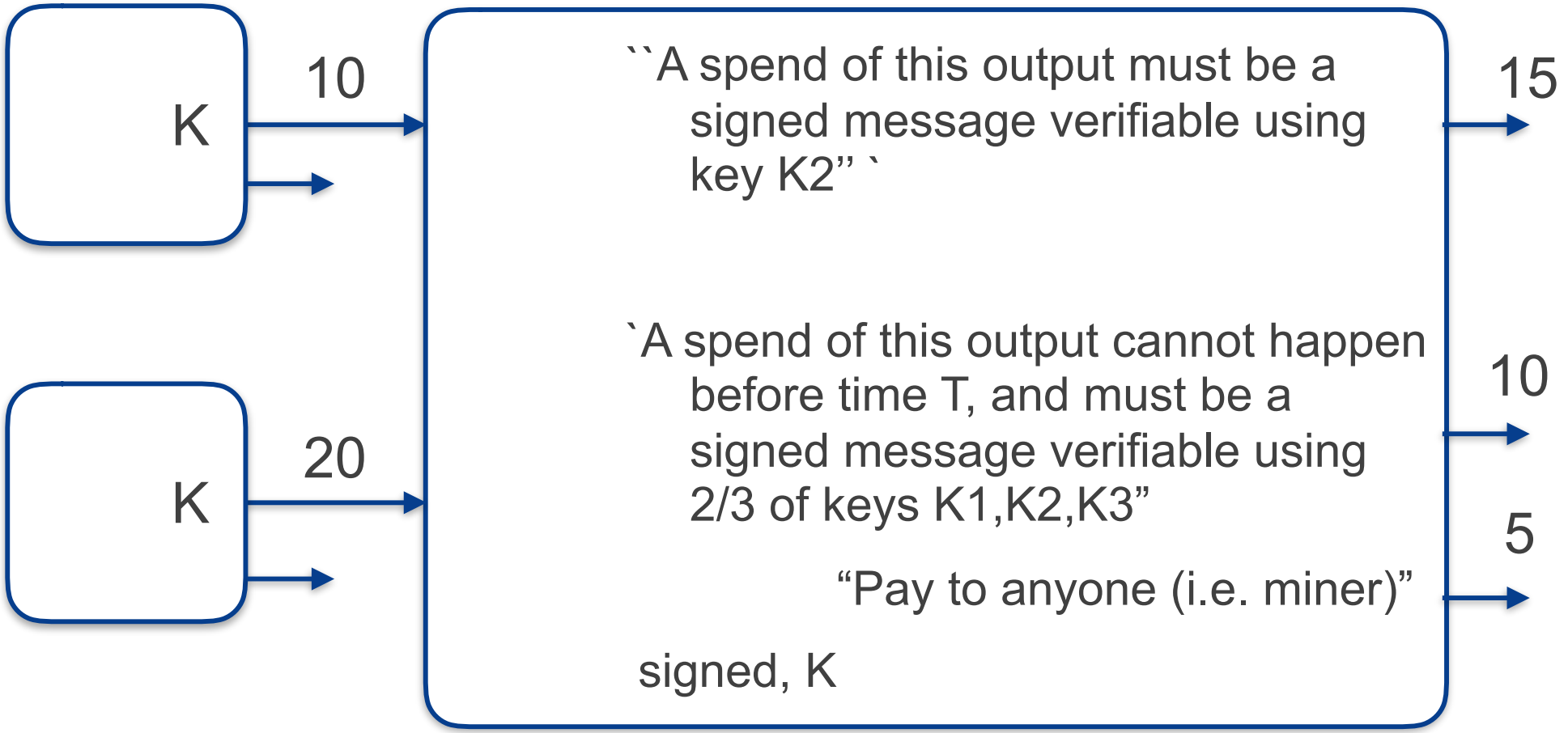
Tezos, Cardano

“No value, utility or purpose” :

EOS

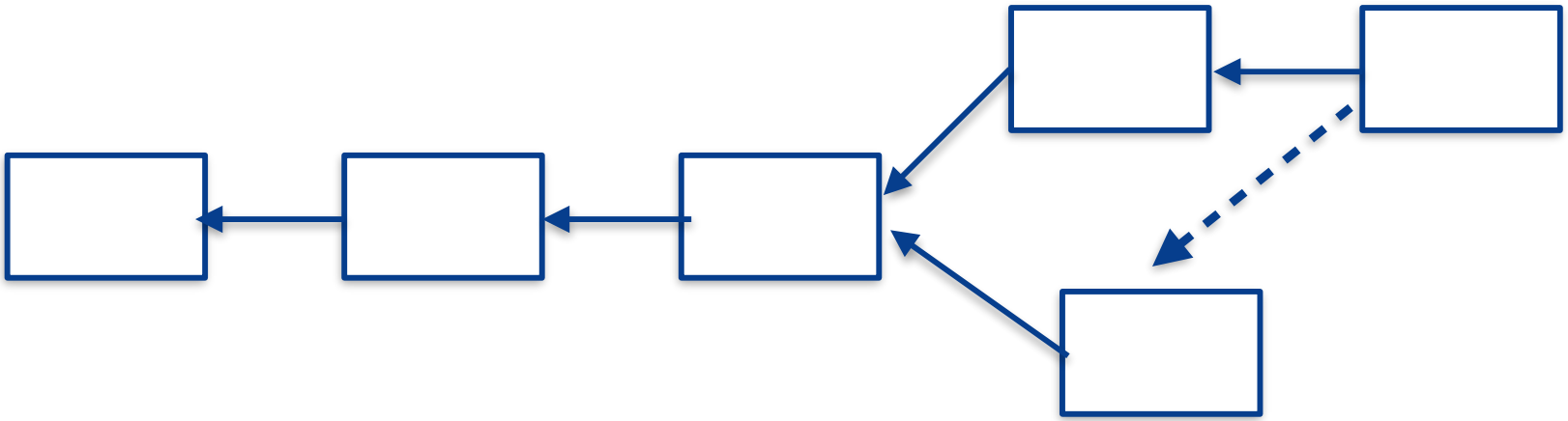
Towards Smart Contracts

Bitcoin transaction outputs have associated programs, that express conditions under which the output can be spent:



Chain Forks

One of the competing blocks is extended first (with high probability)



Ethereum: grant a consolation reward to the losing miner

the chain with the greatest **weight** is the official history

Game theory of such protocols an active research area!

Consensus Protocols

n nodes, at most *f* < *n* may be faulty/malicious

Faulty nodes may

- crash
- send incorrect messages
- delay an honest node's message (but not forever)

Goal: Honest/correct nodes should correctly maintain the ledger even with the faulty nodes present

Subject to assumptions about determinism, asynchrony, this is achievable provided

- *f* < *n/2* (crash failures)
- *f* < *n/3* (malicious byzantine failures)

A wave of innovation in consensus protocols

OPEN NETWORKS

Variants of Nakamoto consensus / Proof of Work:

- Proof of elapsed time (Trust Intel SGX)
- Proof of storage
- Proof of useful work (e.g. gene folding computation)
- (Collateralised) Proof of Stake

CLOSED NETWORKS

Variants of Practical Byzantine Fault-tolerant consensus PBFT (Castro Liskov 2002)

- Tendermint, Hyperledger, Red-Belly (Sydney U.)

HYBRID / OTHER

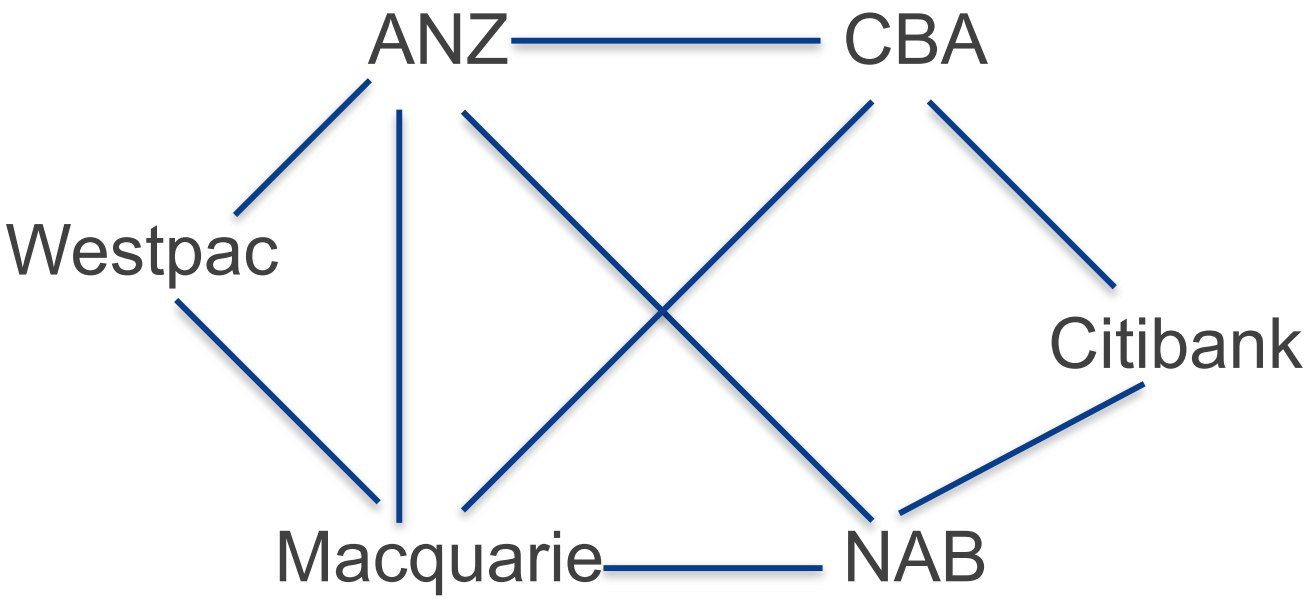
Trust Networks/Quorum (Ripple/Stellar)

Probabilistic/dag rather than chain based protocols (IOTA, Hashgraph, R3 Corda)

Ethereum: Proof of work -> Hybrid POW/POS -> POS

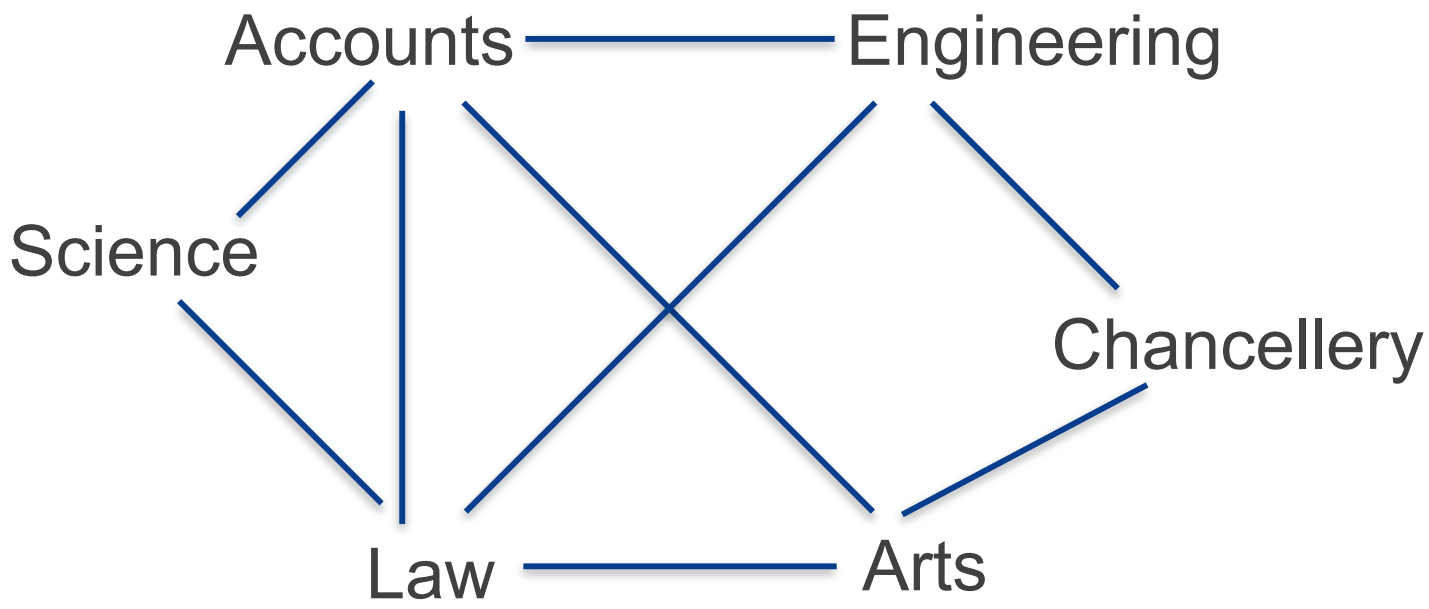
Consortium/Permissioned Blockchains

- Restricted set of consensus agents
- Variants of classical byzantine agreement protocols
- Limitations on transaction flow through the network
- Examples: Digital Asset (for ASX), R3 Corda



Enterprise Blockchains

- Permissioned blockchains internal to an organisation
- Motivation: audit records / security against insider attacks / consistent global view of data



Blockchain Use Cases beyond Currency

- International Exchange (Ripple)
- Clearance and Settlement (Digital Asset for ASX)
- Financial Instruments (R3)
- Energy trading / Green Electrons (UNSW, PowerLedger, Solara, Enosi)
- Loyalty Programs (LoyaltyX, Gazecoin)
- Supply Chain (Agri Digital)

- Alternative Democracy / Voting (Flux, Securevote)
- Genomic Data Access Control (E-nome/Garvan)
- Copyright protection (Veredictum)

Only the beginning!