EXTROPY.IO

Blockchain Theory 2

Week 1
Lesson 2

Lesson Plan

- Review and Questions
- Blockchain data structures
- Consensus Mechanisms
- Cryptoeconomics
- Governance

Reading List

How bitcoin actually works

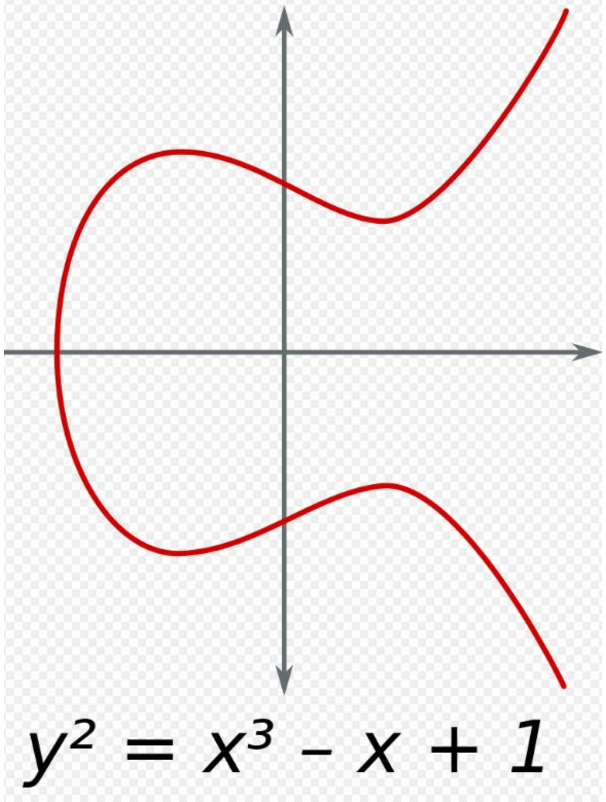
What would Satoshi think of Proof of Stake

Proof of Work is not a consensus mechanism

Review and Questions

EXTROPY.IO

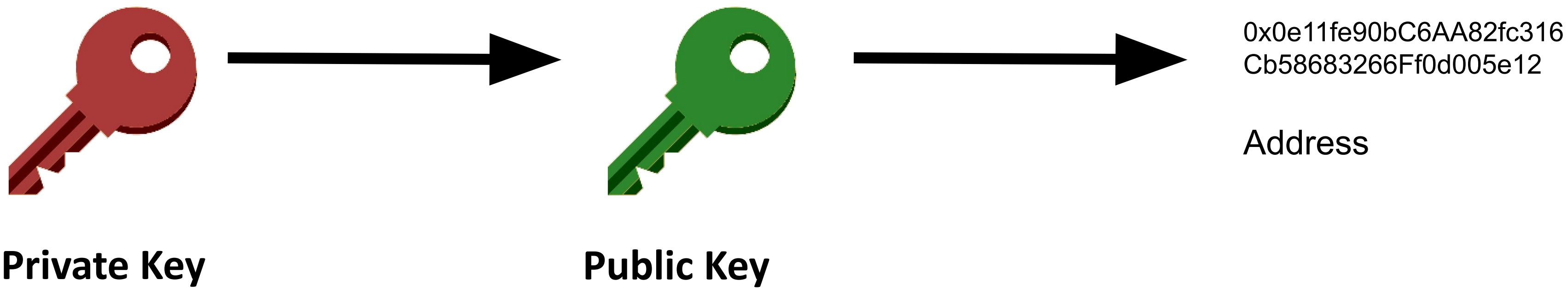
Key Cryptography used in Ethereum



Ethereum uses ECDSA (Elliptic Curve Digital Signature Algorithm)
It uses the SECP256k1 curve.

Elliptic curves have a shorter key length for the same level of security as RSA

Keys and addresses in Ethereum



0x0e11fe90bC6AA82fc316
Cb58683266Ff0d005e12

Address

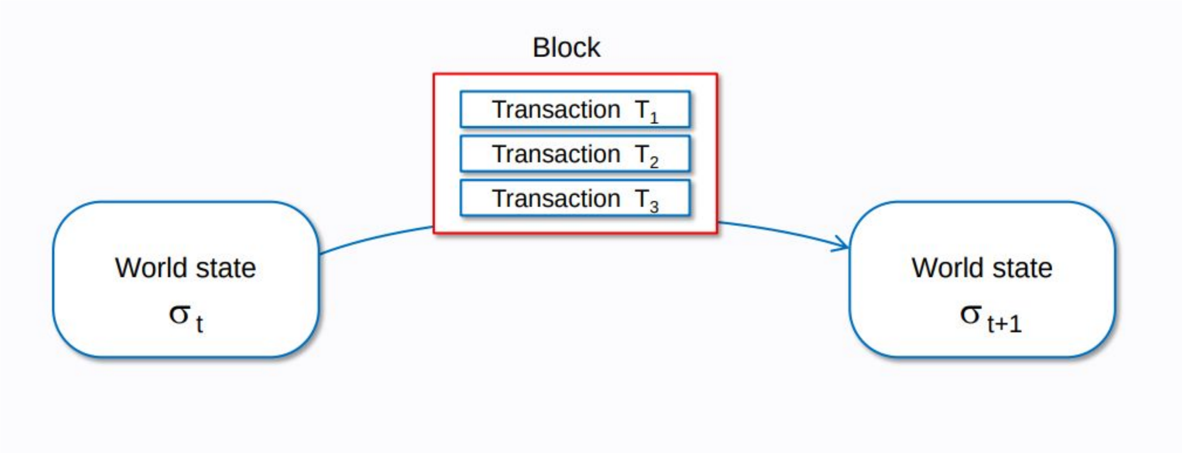
Private Key

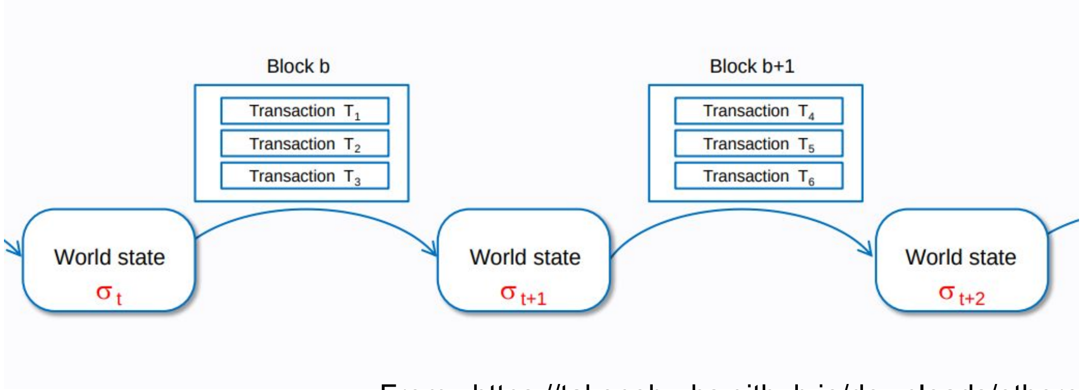
Public Key

Blockchain components in more detail

- A peer-to-peer (P2P) network connecting participants and propagating transactions and blocks of verified transactions, based on a standardized "gossip" protocol
- Messages, in the form of transactions, representing state transitions
- A set of consensus rules, governing what constitutes a transaction and what makes for a valid state transition
- A state machine that processes transactions according to the consensus rules
- A chain of cryptographically secured blocks that acts as a journal of all the verified and accepted state transitions
- A consensus algorithm that decentralizes control over the blockchain, by forcing participants to cooperate in the enforcement of the consensus rules
- A game-theoretically sound incentivization scheme (e.g., proof-of-work costs plus block rewards) to economically secure the state machine in an open environment
- One or more open source software implementations of the above ("clients")

Blockchain as a state machine





From : https://takenobu-hs.github.io/downloads/ethereum_evm_illustrated.pdf

The Blockchain Network

From : Bitcoin book

Bitcoin is structured as a peer-to-peer network architecture on top of the internet. The term peer-to-peer, or P2P, means that the computers that participate in the network are peers to each other, that they are all equal, that there are no "special" nodes, and that all nodes share the burden of providing network services. The network nodes interconnect in a mesh network with a "flat" topology.
There is no server, no centralized service, and no hierarchy within the network.

Blockchain Nodes

Nodes typically

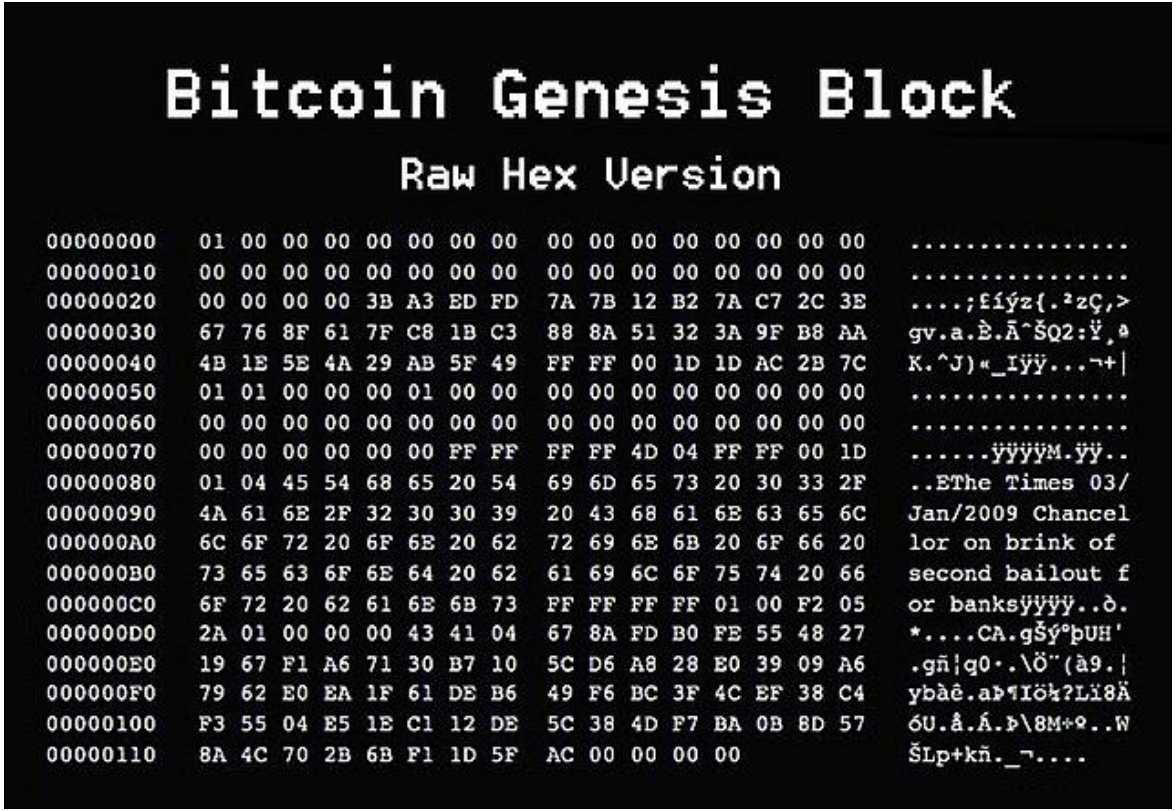
- Accept and transmit transactions (if valid)
    - they keep a mempool of pending transactions
- Provide network discovery and routing functions
    - the connections are not based on geographical proximity but proximity in a hash table
    - connections to misbehaving nodes will be dropped
- Accept blocks and update their ledger

Node discovery

- Via DNS seed nodes

- Via locally stored list

Idealised blockchain block structure



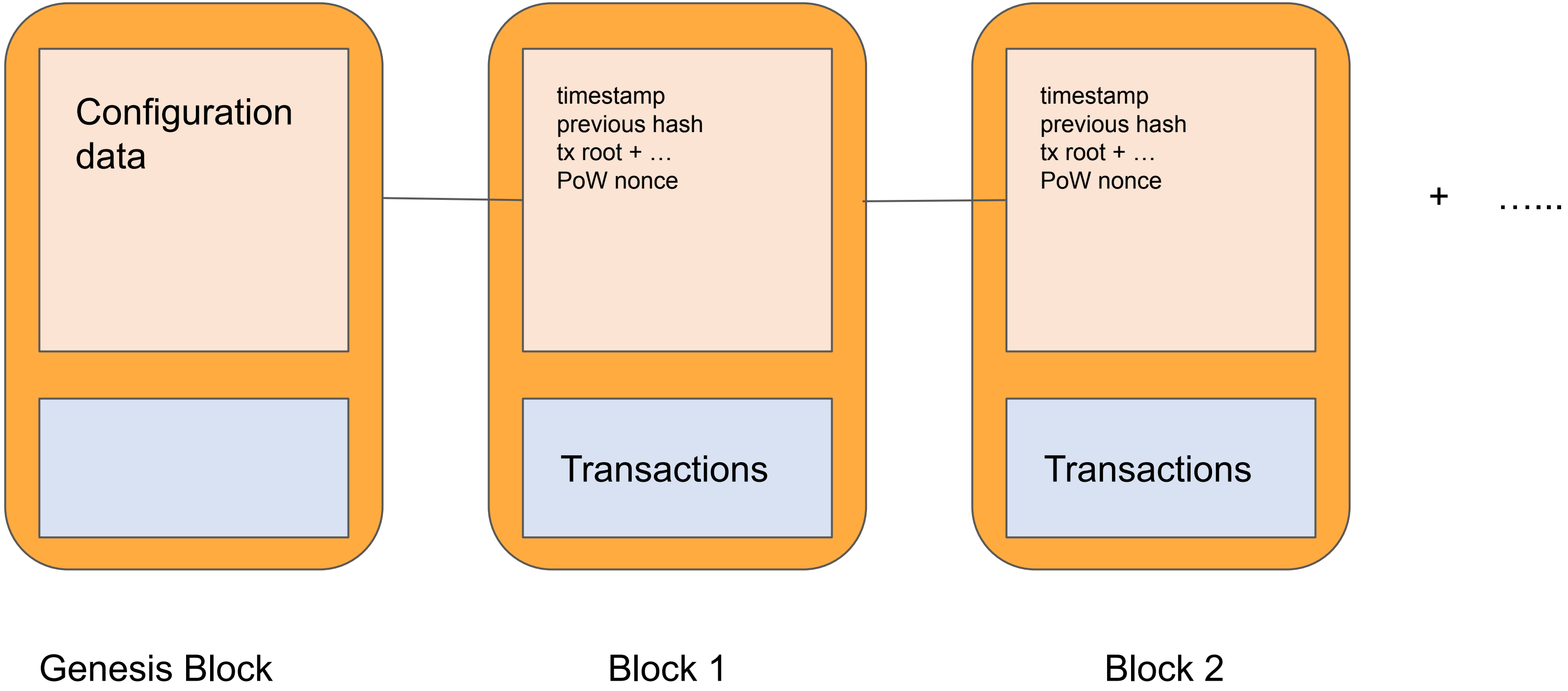
Bitcoin Genesis Block

Raw Hex Version

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

By MikeG001 - Own work, CC BY-SA 4.0,

Blockchain Data structure



Configuration data

timestamp
previous hash
tx root + …
PoW nonce

Transactions

timestamp
previous hash
tx root + …
PoW nonce

Transactions

+ ……

Genesis Block

Block 1

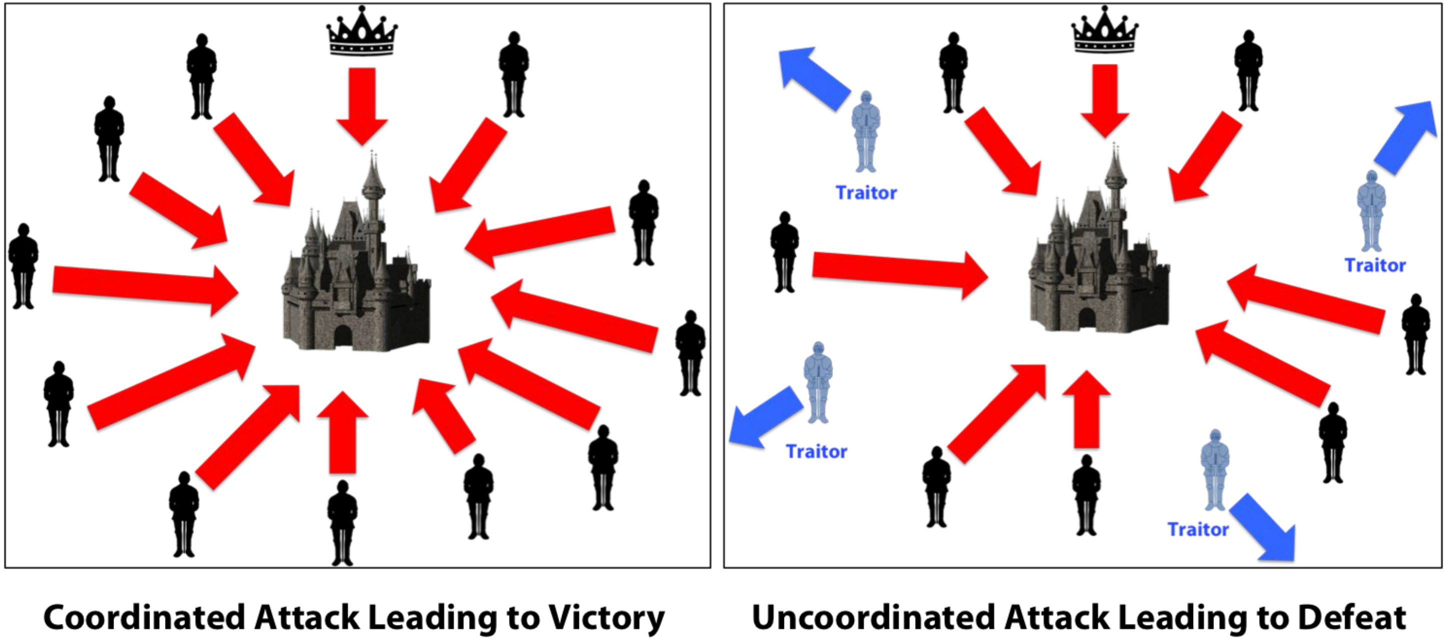
Block 2

Consensus in systems

How can we agree on the state of a system ?

Byzantine Fault Tolerance

Byzantine fault tolerance (BFT) is the dependability of a fault-tolerant computer system to such conditions where components may fail and there is imperfect information on whether a component has failed.



Coordinated Attack Leading to Victory

Uncoordinated Attack Leading to Defeat

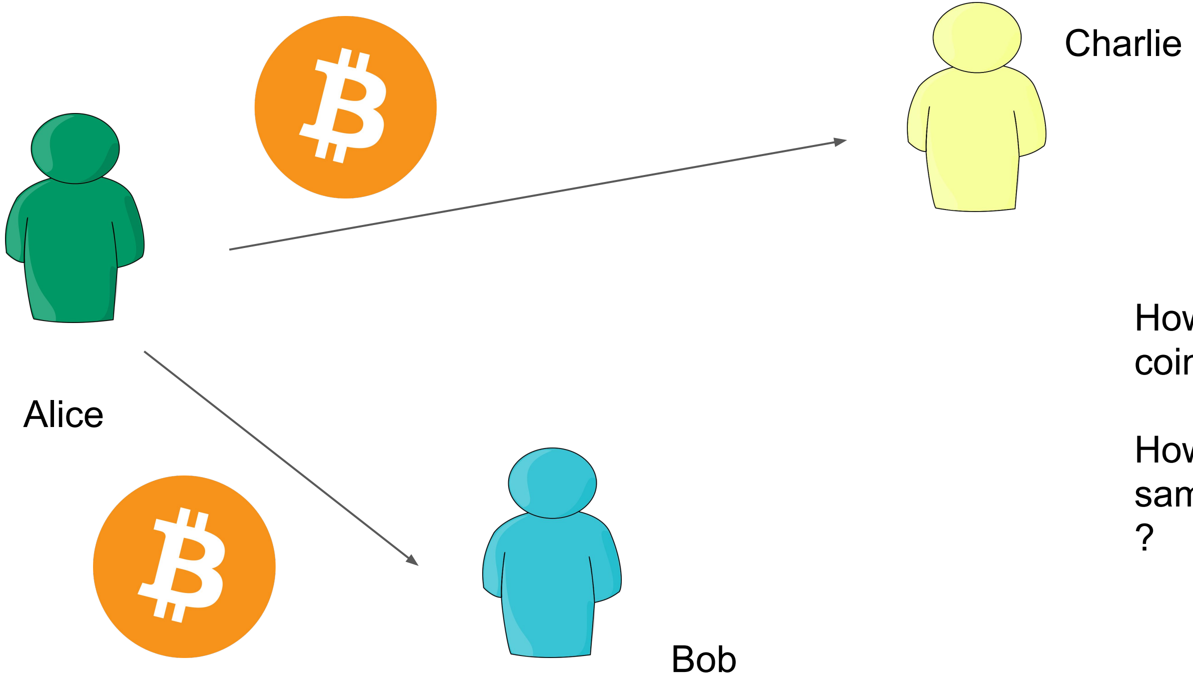
Byzantine Generals’ Problem, Image by Debraj Ghosh

The Double Spending Problem

“The double spending problem is a potential flaw in a cryptocurrency or other digital cash scheme whereby the same single digital token can be spent more than once, and this is possible because a digital token consists of a digital file that can be duplicated or falsified.”

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174

The double spend problem



How can we prevent creation of coins by digital “copy / paste” ?

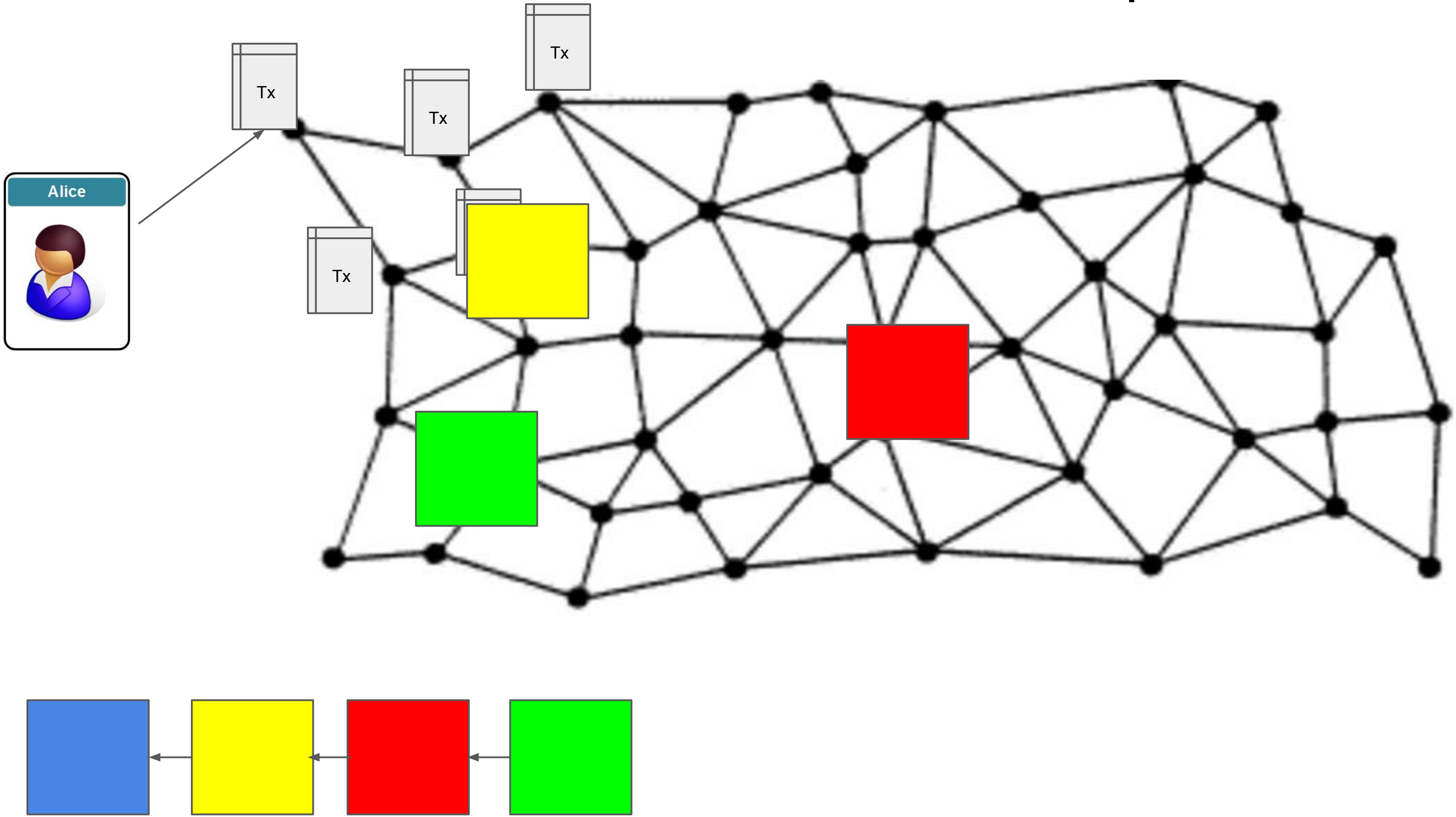
How do we prevent Alice giving the same coin to both Bob and Charlie ?

Proof of Work

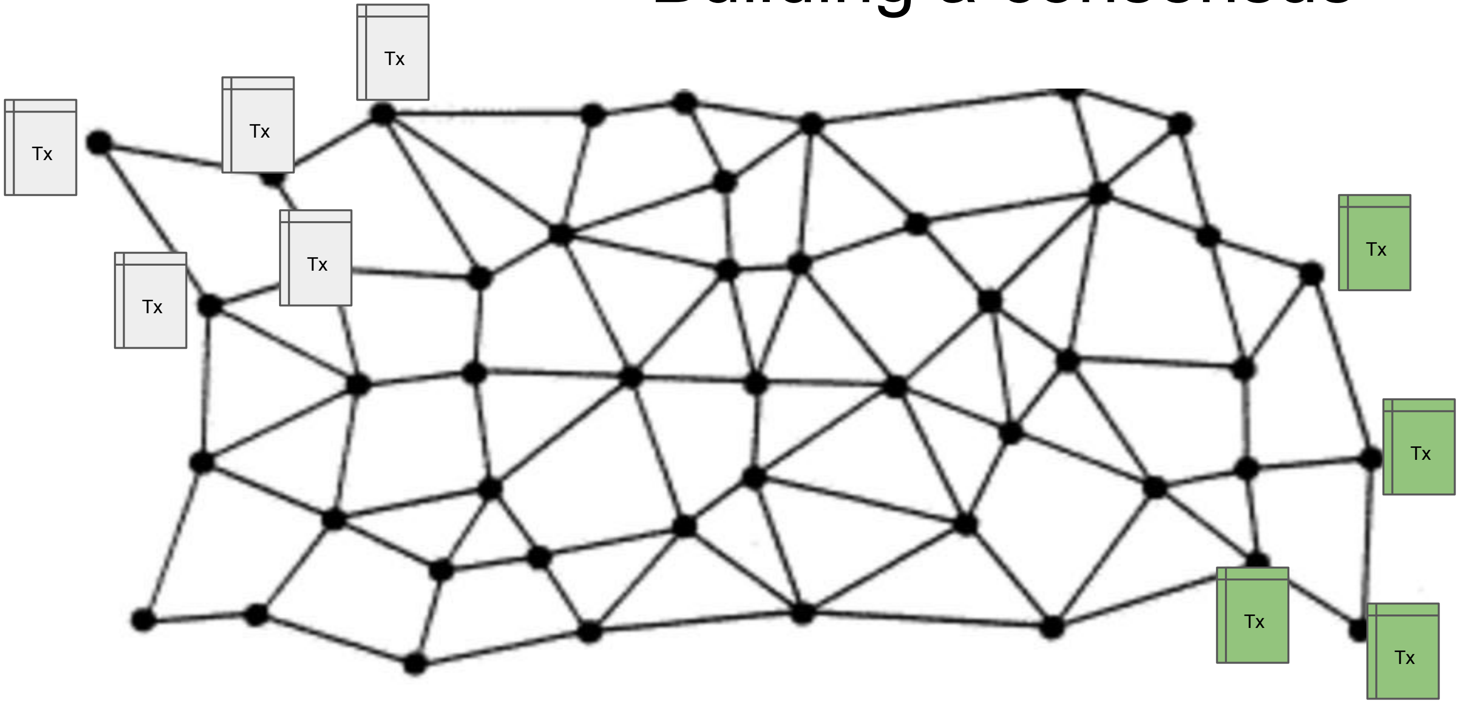
+

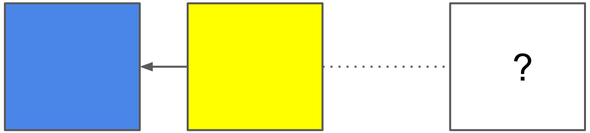
Nakamoto Consensus

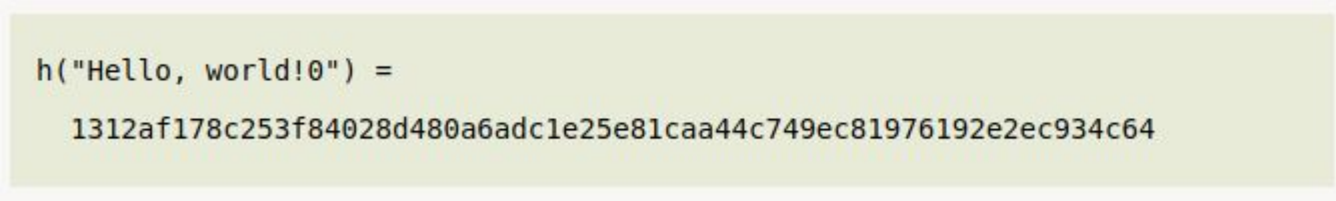
Network point of view



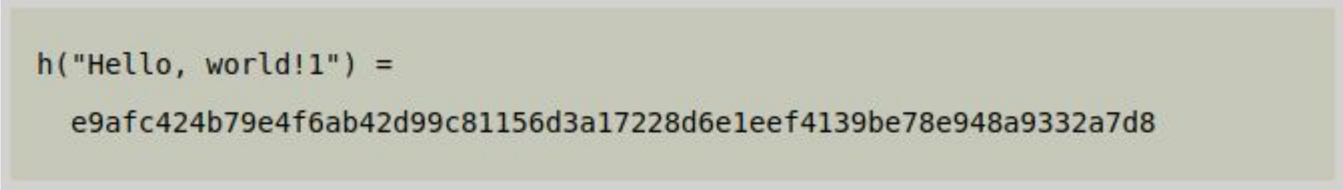
Building a consensus



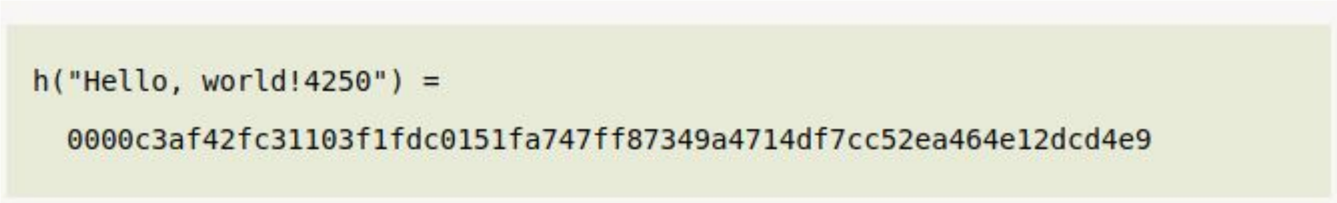




```
h("Hello, world!0") =
  1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
```



```
h("Hello, world!1") =
  e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
```



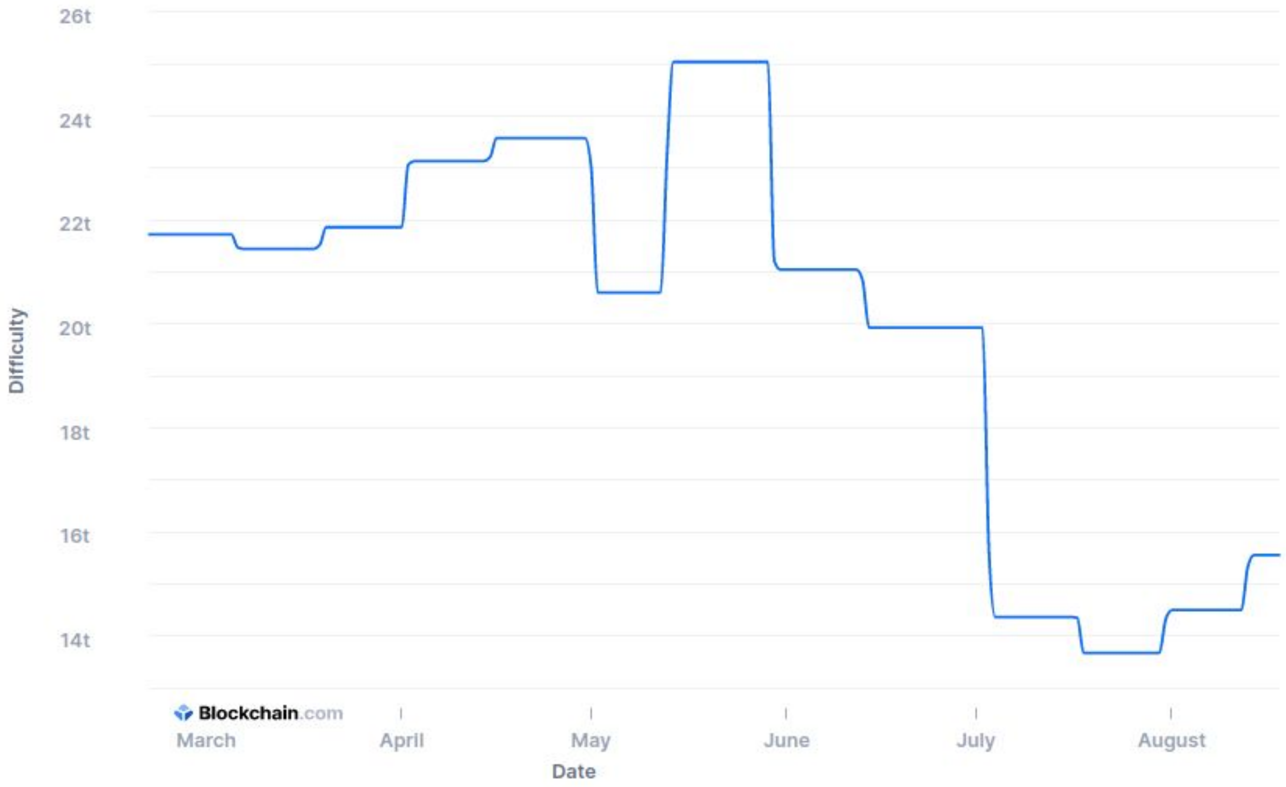
```
h("Hello, world!4250") =
  0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Useful tool for trying out hashes and blocks

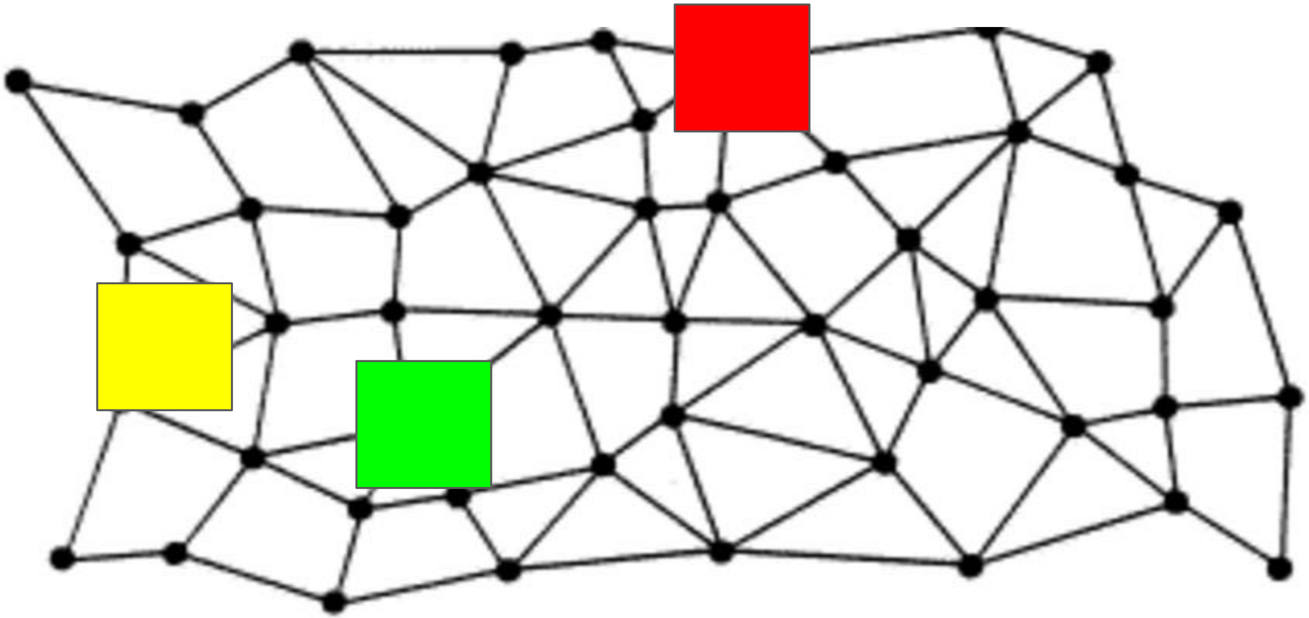
[Blockchain Demo]

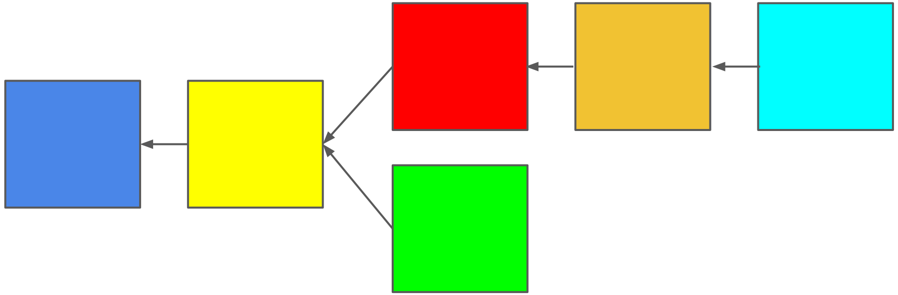
Network Difficulty

A relative measure of how difficult it is to mine a new block for the blockchain.



Nakamoto Consensus





Security

In proof of work we rely on economic incentives to prevent malicious behaviour .

- The block reward
- The cost of producing (useless) work

Contrast this open approach to the way that centralised systems use layers of access control to prevent bad actors entering the system.

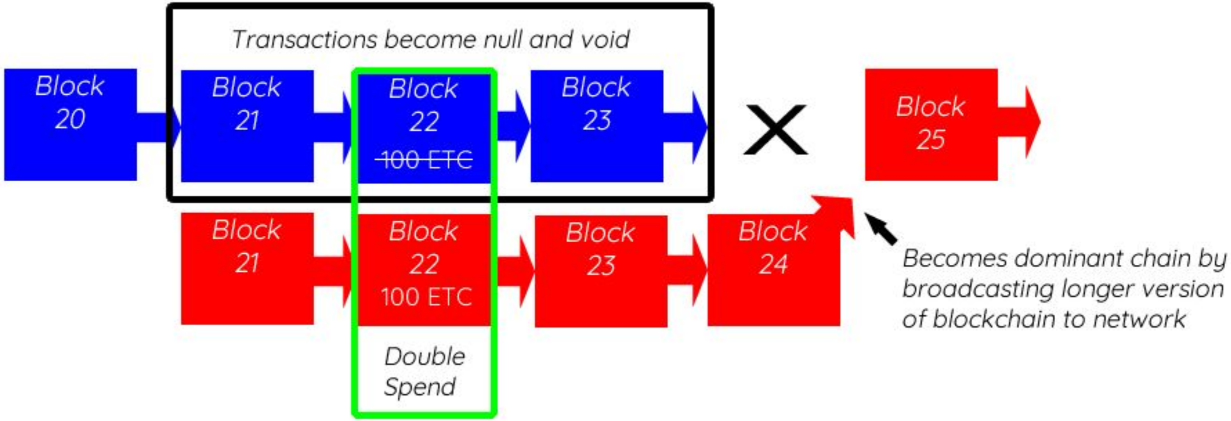
51 % Attacks

A user (or group) gains sufficient hashing power to control 51% of the hashing power of the whole network

Class question :

If someone had 51% of the hashing power what could they do ?
Could they create a double spend ?

51% Attack (double-spend)



Transactions become null and void

Block 20

Block 21

Block 22 ~~100 ETC~~

Block 23

Block 21

Block 22 100 ETC

Double Spend

Block 23

Block 24

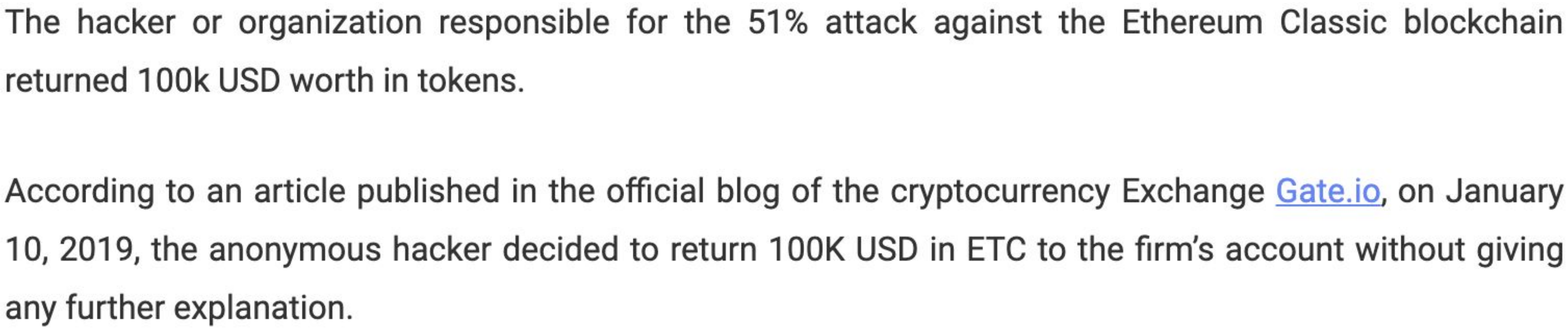
Block 25

Becomes dominant chain by broadcasting longer version of blockchain to network

🟦 Original (honest) blockchain <50% hash power

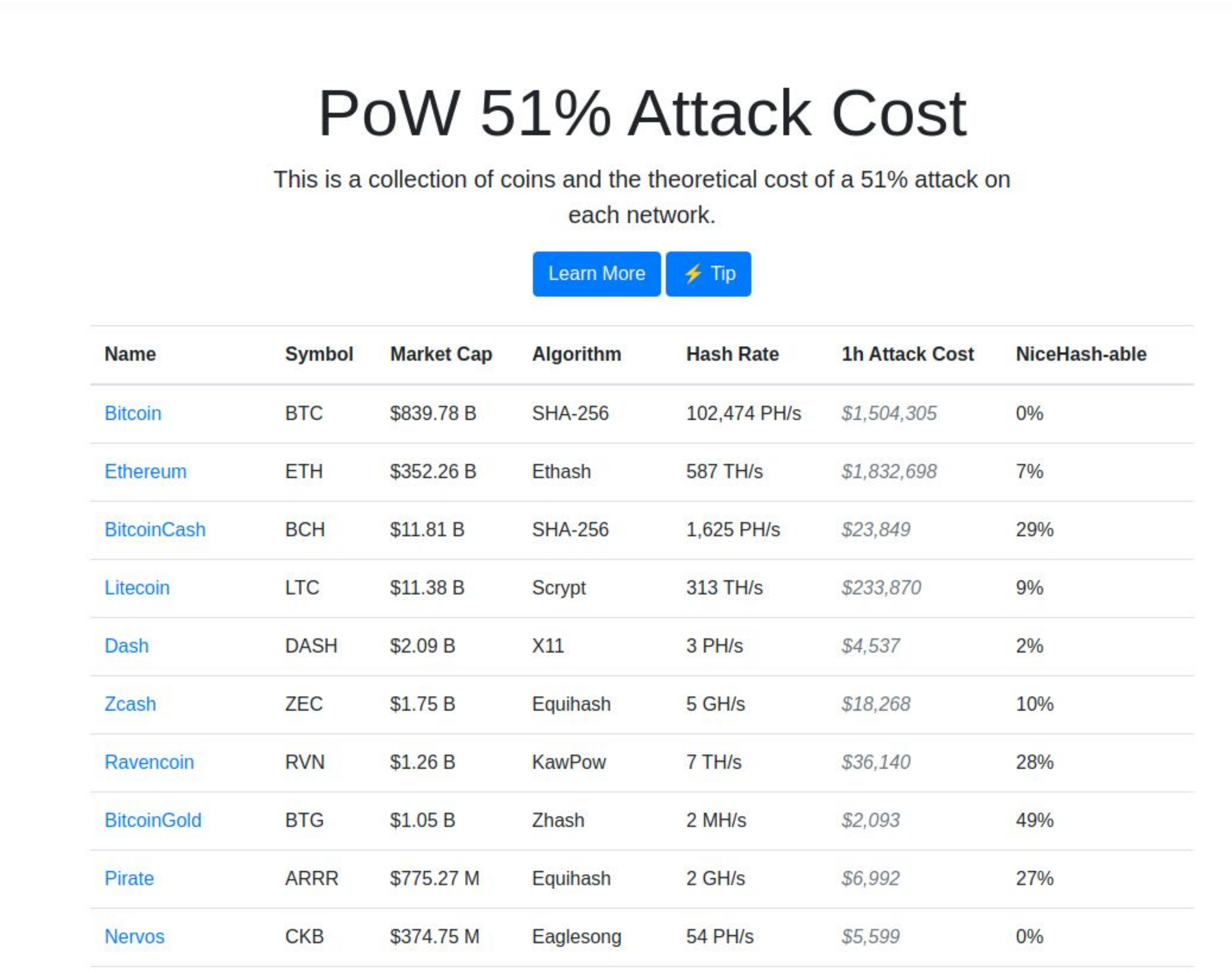
🟥 Malicious blockchain >50% hash power

© Andrew Butler



The hacker or organization responsible for the 51% attack against the Ethereum Classic blockchain returned 100k USD worth in tokens.

According to an article published in the official blog of the cryptocurrency Exchange Gate.io, on January 10, 2019, the anonymous hacker decided to return 100K USD in ETC to the firm’s account without giving any further explanation.



PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$839.78 B	SHA-256	102,474 PH/s	*$1,504,305*	0%
Ethereum	ETH	$352.26 B	Ethash	587 TH/s	*$1,832,698*	7%
BitcoinCash	BCH	$11.81 B	SHA-256	1,625 PH/s	*$23,849*	29%
Litecoin	LTC	$11.38 B	Scrypt	313 TH/s	*$233,870*	9%
Dash	DASH	$2.09 B	X11	3 PH/s	*$4,537*	2%
Zcash	ZEC	$1.75 B	Equihash	5 GH/s	*$18,268*	10%
Ravencoin	RVN	$1.26 B	KawPow	7 TH/s	*$36,140*	28%
BitcoinGold	BTG	$1.05 B	Zhash	2 MH/s	*$2,093*	49%
Pirate	ARRR	$775.27 M	Equihash	2 GH/s	*$6,992*	27%
Nervos	CKB	$374.75 M	Eaglesong	54 PH/s	*$5,599*	0%

Proof of Work

Advantages

- Well understood and easy to implement
- Has seen to be robust in adversarial conditions over 10 years

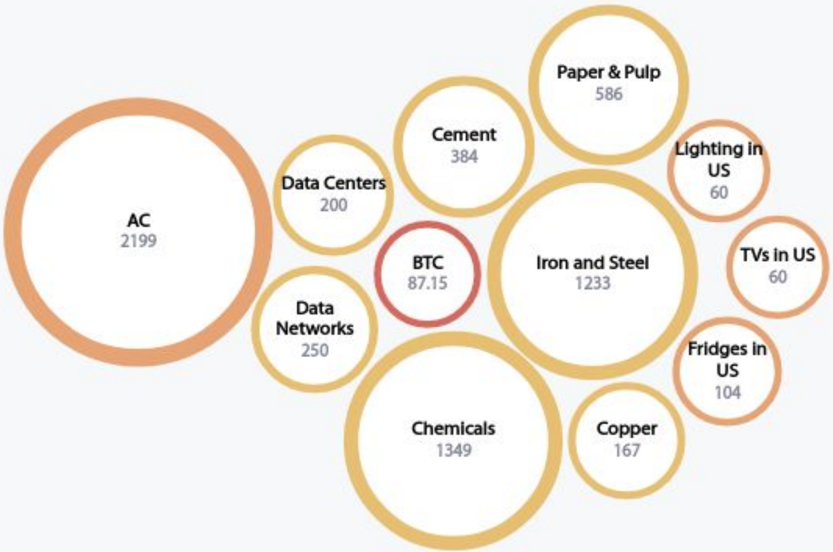
PoW Disadvantages

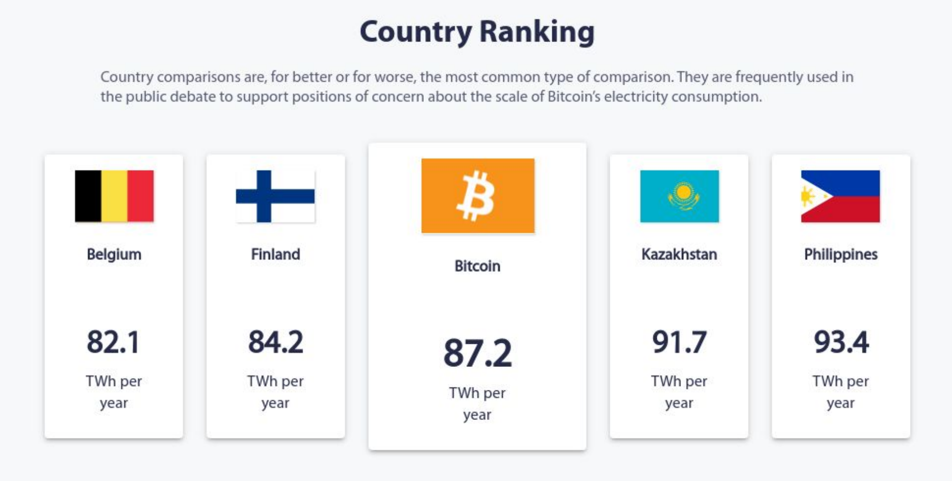
Centralisation of

- Mining Hardware
- Hash power

Cambridge Bitcoin Electricity Consumption Index

UNIVERSITY OF CAMBRIDGE Judge Business School | Cambridge Centre for Alternative Finance





Country Ranking

Country comparisons are, for better or for worse, the most common type of comparison. They are frequently used in the public debate to support positions of concern about the scale of Bitcoin's electricity consumption.

Belgium	Finland	Bitcoin	Kazakhstan	Philippines
82.1	84.2	87.2	91.7	93.4
TWh per year	TWh per year	TWh per year	TWh per year	TWh per year

Other Consensus Mechanisms

History

Practical Byzantine Fault Tolerance (pBFT) Castro and Liskov 1999

Nakamoto Consensus (PoW) 2008

Now many “Proof of ….

Stake / Authority / History / Burn / Elapsed Time / Spacetime ….”

Proof of Kernel Work (mine)

Proof of Stake

Many implementations of PoS

Common features

- Potential block producers have to submit a stake of the native crypto currency to be eligible
- The current block producer is chosen at random, the probability of being chosen will depend on the amount of stake offered.
- If the block producer behaves maliciously they lose their stake

PoS as implemented by Nxt

Network security is governed by peers having a *stake* in the network.

- A *cumulative difficulty* value is stored as a parameter in each block, and each subsequent block derives its new difficulty from the previous blocks value. In case of ambiguity, the network achieves consensus by selecting the block or chain fragment with the highest cumulative difficulty.
- To prevent account holders from moving their stake from one account to another as a means of manipulating their probability of block generation, tokens must be stationary within an account for 1,440 blocks before they can contribute to the block generation process. Tokens that meet this criterion contribute to an account's *effective balance*, and this balance is used to determine forging probability.
- To keep an attacker from generating a new chain all the way from the genesis block, peers allow chain re-organization of no more than 720 blocks behind the current block height. Any block submitted at a height lower than this threshold is rejected.
- Due to the extremely low probability of any account taking control of the blockchain by generating its own chain of blocks, transactions are deemed safe once they are encoded into a block that is 10 blocks behind the current block height.

PoS as implemented by Mina

Mina Protocol uses a PoS consensus mechanism called Ouroboros Samasika, based on Cardano’s PoS Ouroboros.

Features

- Uncapped participation
- Fork resolution does not rely on long term history
- Stakes do not need to be locked

See

Mina Staking

ETH 2 staking solutions

PBFT

Castro and Liskov 1999 - Practical Byzantine Fault Tolerance" (PBFT) algorithm

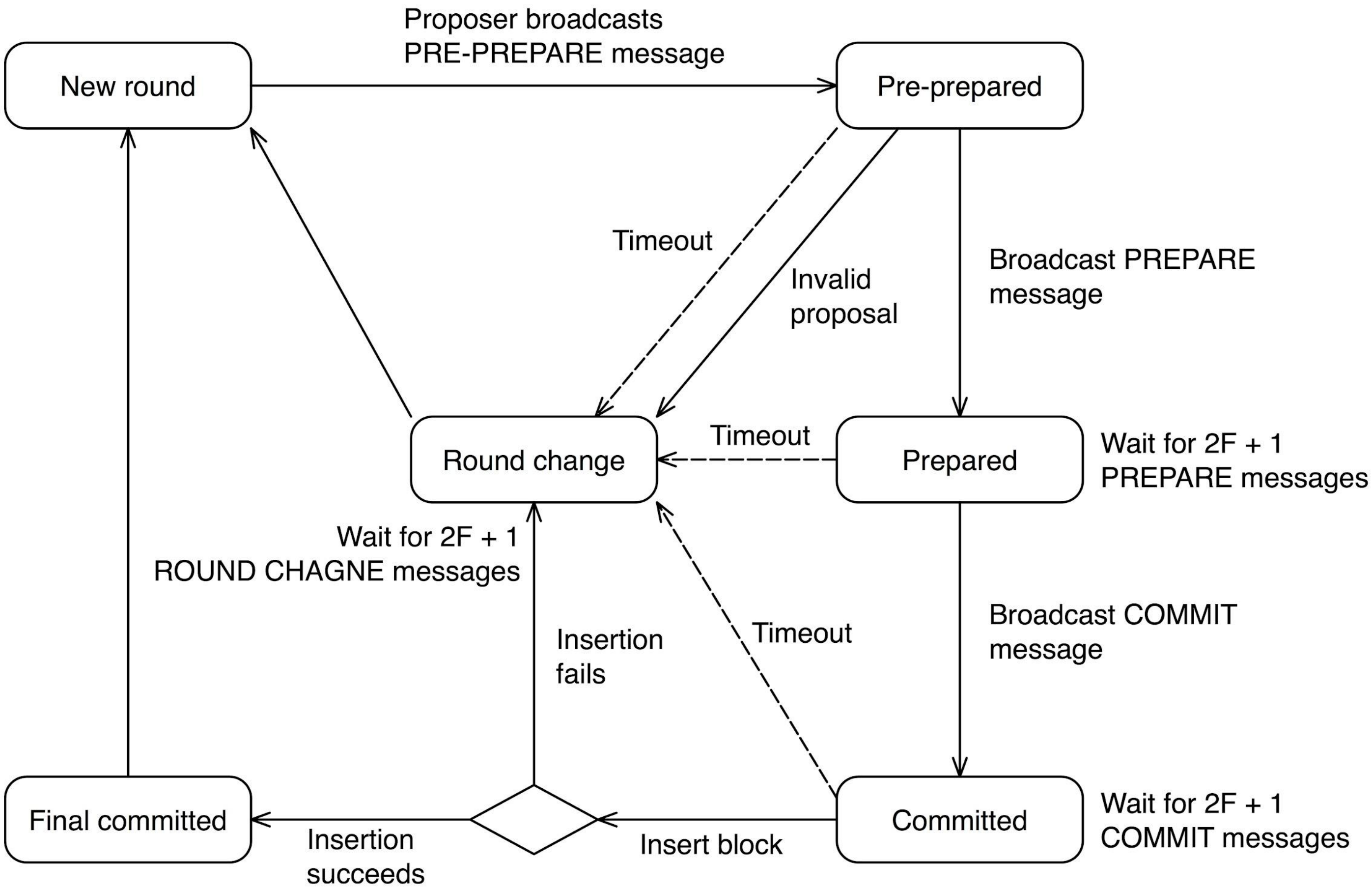
Consensus : Istanbul

- In a network of N nodes can withstand F of Byzantine nodes where N = 3F + 1
- The algorithm has 4 phases – Propose, Pre-Prepare, Prepare, Commit
- The proposer multicasts the block proposal to the validators
- Validators agree on the block and broadcast their decision to others
- Each validator waits for 2F + 1 commits from different validators with the same result before inserting the block into blockchain

Pros
Byzantine fault tolerant
Settlement finality
High throughput

Cons
Complex

Also see https://es.slideshare.net/YuTeLin1/istanbul-bft



New round
Proposer broadcasts
PRE-PREPARE message
Pre-prepared
Timeout
Invalid
proposal
Broadcast PREPARE
message
Round change
Timeout
Prepared
Wait for 2F + 1
PREPARE messages
Wait for 2F + 1
ROUND CHAGNE messages
Insertion
fails
Timeout
Broadcast COMMIT
message
Final committed
Insertion
succeeds
Insert block
Committed
Wait for 2F + 1
COMMIT messages

Consensus : RAFT

- Well known consensus algorithm for distributed databases
- Useful for closed membership/ consortium settings
- At the start of the network, a leader is elected
- The leader proposes the blocks and other node validate the same
- A new leader is elected when the current leader goes down or term ends
- Leader election is completely random

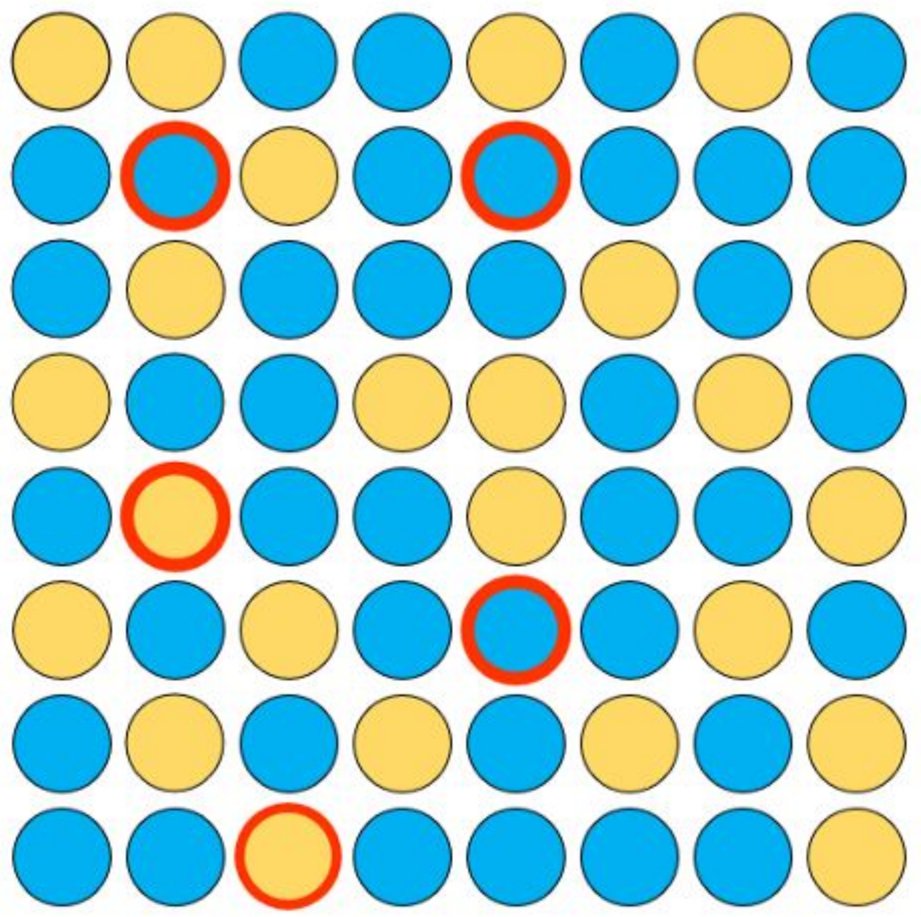
Pros
Faster block time (25 – 50 millisecs)
Settlement finality

Cons
Is not byzantine fault tolerance
Requires interconnected network

See : http://thesecretlivesofdata.com/raft/ and https://raft.github.io/

Repeated random subsampling

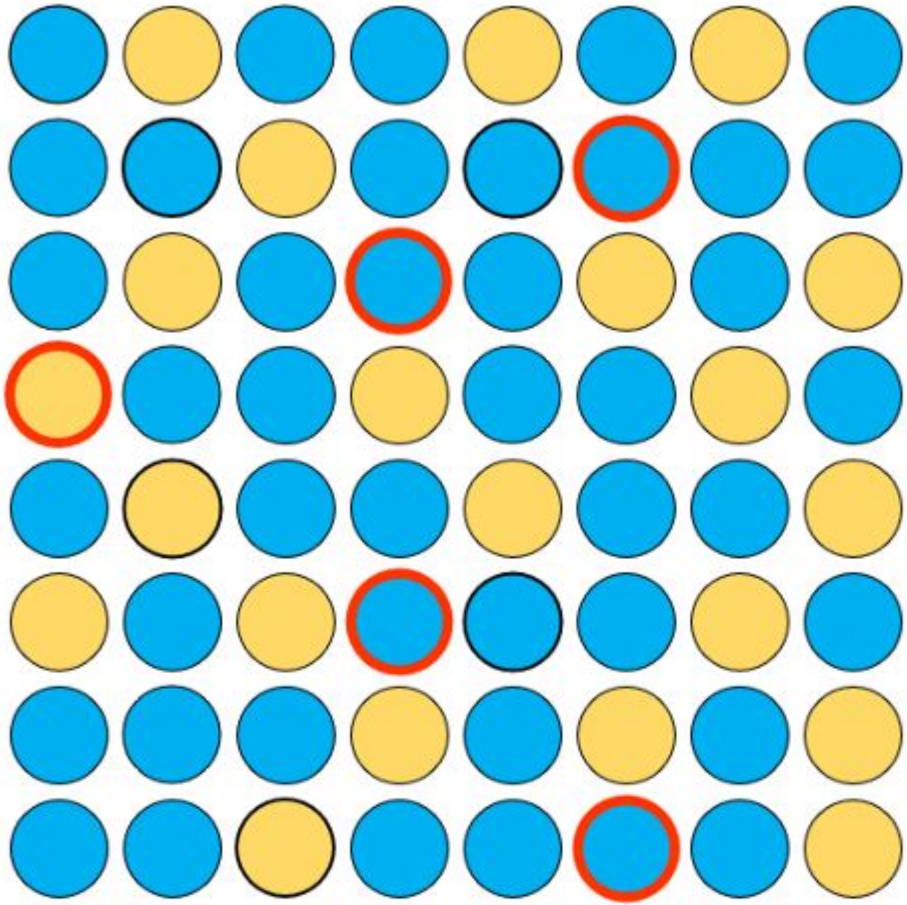
Round 1



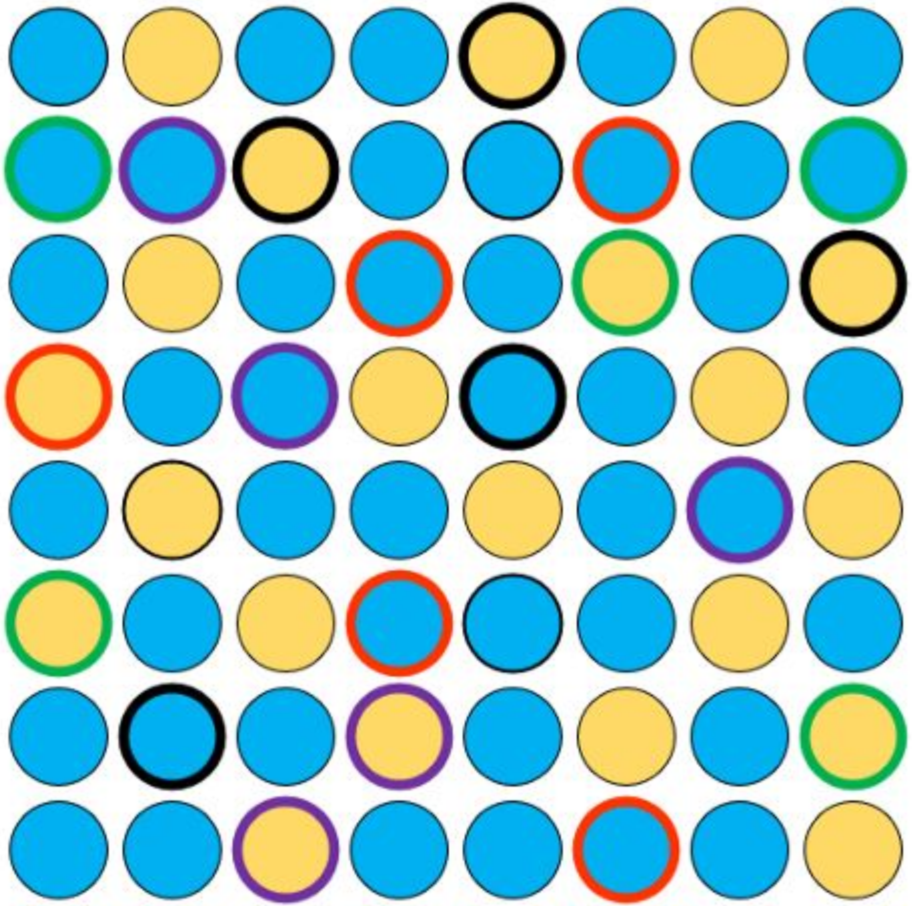
From Avalanche Consensus

EXTROPY.IO

Round 2

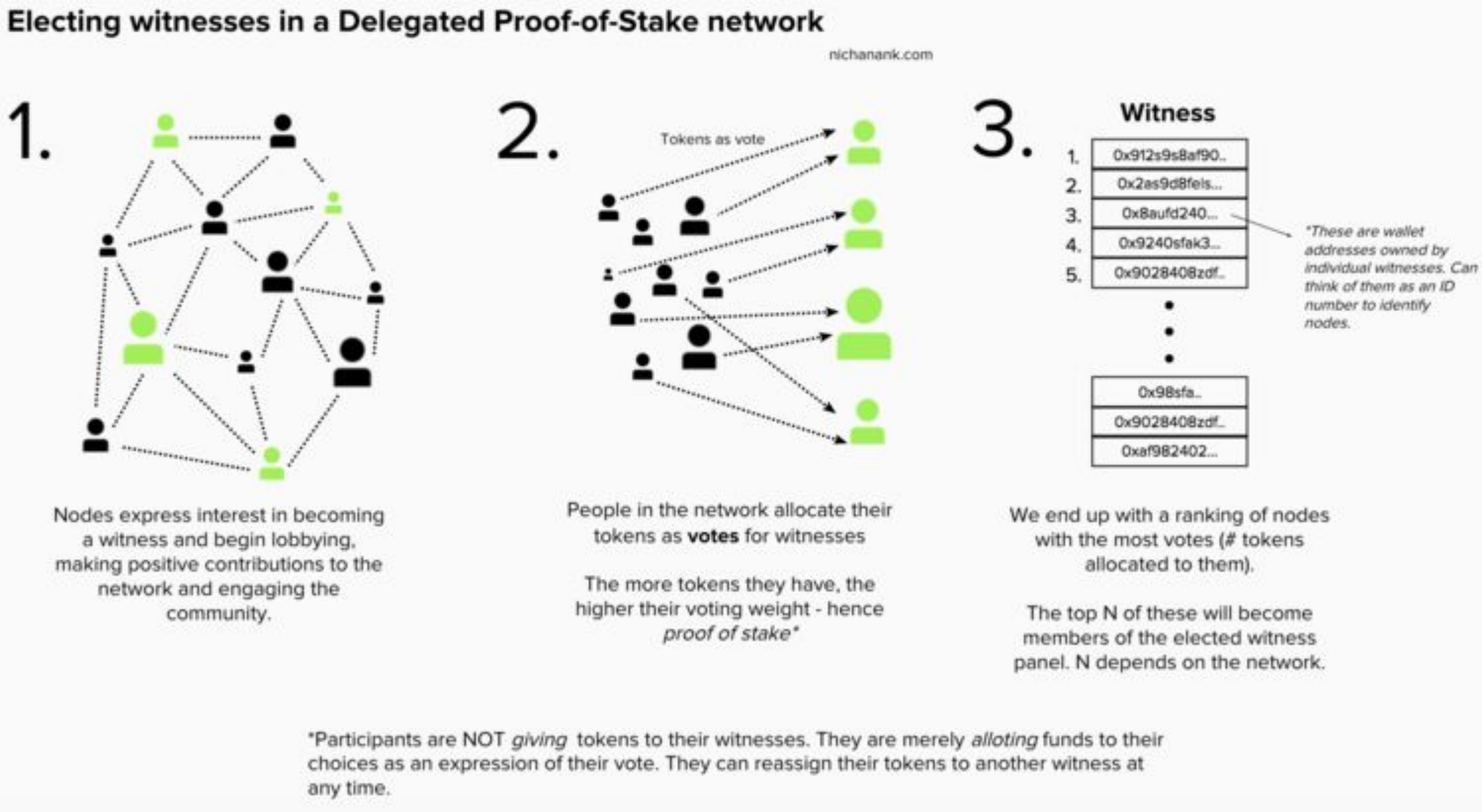


Other nodes simultaneously update



Delegated Proof of Stake

(EOS / Lisk / Steem)



Electing witnesses in a Delegated Proof-of-Stake network

nichanank.com

These are wallet addresses owned by individual witnesses. Can think of them as an ID number to identify nodes.

1. Nodes express interest in becoming a witness and begin lobbying, making positive contributions to the network and engaging the community.

2. People in the network allocate their tokens as **votes** for witnesses

The more tokens they have, the higher their voting weight - hence *proof of stake**

3. We end up with a ranking of nodes with the most votes (# tokens allocated to them).

The top N of these will become members of the elected witness panel. N depends on the network.

*Participants are NOT *giving* tokens to their witnesses. They are merely *alloting* funds to their choices as an expression of their vote. They can reassign their tokens to another witness at any time.

Cryptoeconomics

We have had decentralised and fault tolerant systems before, but what sets blockchains apart is cryptoeconomics

"Cryptoeconomic approaches combine cryptography and economics to create robust decentralized P2P networks that thrive over time despite adversaries attempting to disrupt the network."

From Cryptoeconomics 101

From Internet Policy Review : Cryptoeconomics

The term *cryptoeconomics* entered casual usage in the formative years of the Ethereum developer community in 2014-5. The phrase is typically attributed to Vitalik Buterin with the earliest public usage being in a 2015 talk by Vlad Zamfir entitled “What is Cryptoeconomics”

Properties required for a cryptocurrency

- Eventual consensus. At any time, all compliant nodes agree upon a prefix of what will become the eventual “true” blockchain.

- Exponential convergence. The probability of a fork of depth n is O(2−n). This gives users high confidence that a simple “k confirmations” rule will ensure their transactions are settled permanently.

- Liveness. New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time.

- Correctness. All blocks in the chain with the most cumulative proof of work will only include valid transactions.

- Fairness. A miner with X% of the network’s total computational power will mine approximately X% of blocks.

From - Vitalik Buterin on Cryptoeconomics and Markets in Everything

“Whatever your rules are for rewarding, penalizing inside of the mechanism, they have to be specified as a piece of Solidity code, Viper code, whatever programming language you’re using in that set. That’s a much tighter constraint than policymakers writing laws have.”

“Another one is, of course, that all of the actors are anonymous, and what that means in practice is that you cannot drag people’s utility down below zero. If I have 70 ether, and I put that 70 ether into a mechanism, the worst thing you can do to me is you can take away that 70 ether.

You cannot throw me in jail. You cannot socially ostracize me so I can’t earn any money again because I can always just switch identities. But to the extent that I’m willing to lock that ether up and make it vulnerable to a mechanism, then you have the ability to motivate me to that extent.”

Incentives

"An incentive is any design element of a system that influences the behavior of system participants by changing the relative costs and benefits of choices those participants may make."

From Why incentives matter

We can incentivise through

- Rewards
  - For example the block reward, or transaction fee
  - Privileges within the system

- Punishments
  - Direct : Loss of deposit (see proof of stake consensus mechanism)
  - Indirect : Loss of potential reward / privileges

Cryptoeconomic terminology

- Cryptoeconomic security margin: an amount of money X such that you can prove “either a given guarantee G is satisfied, or those at fault for violating G are poorer than they otherwise would have been by at least X”

- Cryptoeconomic proof: a message signed by an actor that can be interpreted as “I certify that either P is true, or I suffer an economic loss of size X”

Game Theory

Game theory investigates how individuals react to each other and make decisions in specific (simplified) settings. It looks at the incentives for possible options and usually assumes that the individuals will make decisions in order to maximise what they perceive as their outcomes. It uses payoff matrices to show the benefits to the players and looks for equilibrium, that is states of the system where the players will want to stay with the choice they have made.
In simplified settings, researchers have looked at the payoff between cooperative or selfish behaviour.

"that while the “best” option in many real world situations may be to cooperate, rational players, thinking as individuals, will choose not to cooperate with each other since they cannot trust the other player to cooperate."
From Intro to game theory

Equilibrium in the system

It is important to understand the points of equilibrium within the system, there may be multiple points which you will want to match with the desired outcomes of the system.

From Simple Economics of the blockchain

“... two key costs affected by blockchain technology – the cost of verification of state, and the cost of networking – change the types of transactions that can be supported in the economy.”

“Whereas the reduction in the cost of verification is what allows Bitcoin to settle transactions without an intermediary, the reduction in the cost of networking is what allowed its ecosystem to scale in the first place”

Blockchain Governance

“The greatest challenge that new blockchains must solve isn’t speed or scaling, it’s governance”

- Kai Sedgwick - Why Governance is the Greatest Problem for Blockchains To Solve

It is useful to think of governance in the following areas

Consensus

- Who is involved and how do they come to consensus ?

Information

- How does relevant information reach the participants ?

Incentives

- How are the incentives aligned to ensure
  - Correct Behaviour
  - There is a sufficient level of participation

Procedures

- In a decentralised system how are
  - Proposals made
  - Votes submitted
  - Consensus reached

On Chain

The mechanism to change the protocol is part of the protocol

Typically participants can vote to accept or reject proposals to upgrade the protocol or some aspects of the system

Coordination and communication is usually more efficient than in off chain solutions

Off Chain

The mechanism to change the protocol are external to the system

The process is often

- ad hoc
- may be poorly specified
- communication and coordination can be problematic

Developers may have a key role in deciding and implementing changes to the protocol

Tezos

‘Self Amending Ledger’

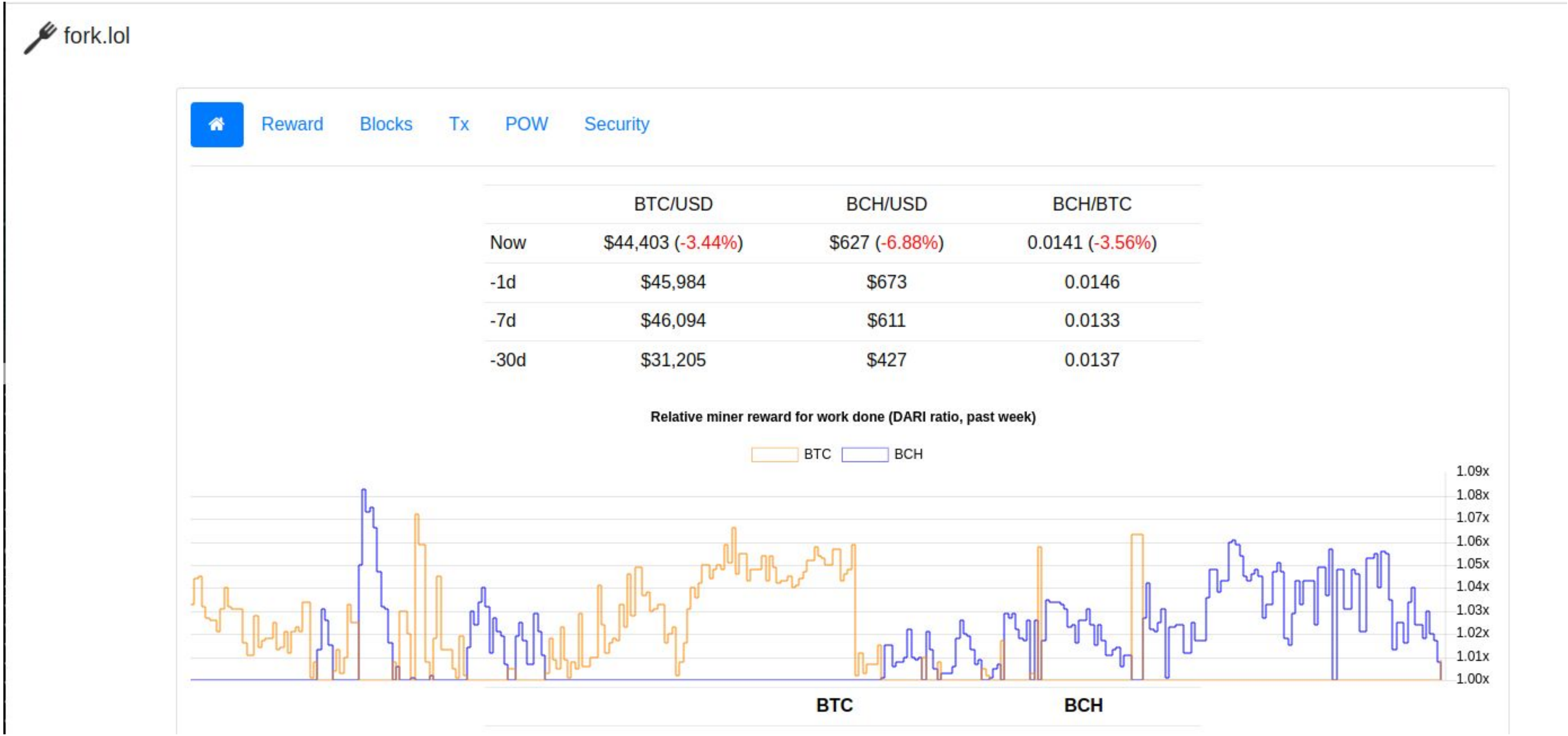
- Proof of Stake Consensus
- Governance Process
  - Code updates are open to anyone
  - On chain vote pushes change to test network
  - Confirming vote pushes change to the live network

- Contributions are rewarded with tokens
- Power moves away from miners and developers
- Allows delegated democracy

https://everipedia-storage.s3.amazonaws.com/NewlinkFiles/16739988/8d4d1f1b-8/white_paper.pdf

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247150

When Governance fails



	BTC/USD	BCH/USD	BCH/BTC
Now	$44,403 (-3.44%)	$627 (-6.88%)	0.0141 (-3.56%)
-1d	$45,984	$673	0.0146
-7d	$46,094	$611	0.0133
-30d	$31,205	$427	0.0137

Relative miner reward for work done (DARI ratio, past week)

BTC	BCH

Homework

Imagine you are designing a new blockchain system

What behaviour / aspects of the system do you want to encourage ?
What behaviour / aspects of the system do you want to discourage ?

What means do you have for this incentivisation ?

Next lesson
Introduction to Solidity