Alternative Consensus

HOW MIGHT A DISTRIBUTED LEDGER WORK?

Users initiate transactions using their *Digital Signatures*

→ Users *Broadcast* their transactions to *Nodes*

→ One or more *Nodes* begin validating each transaction

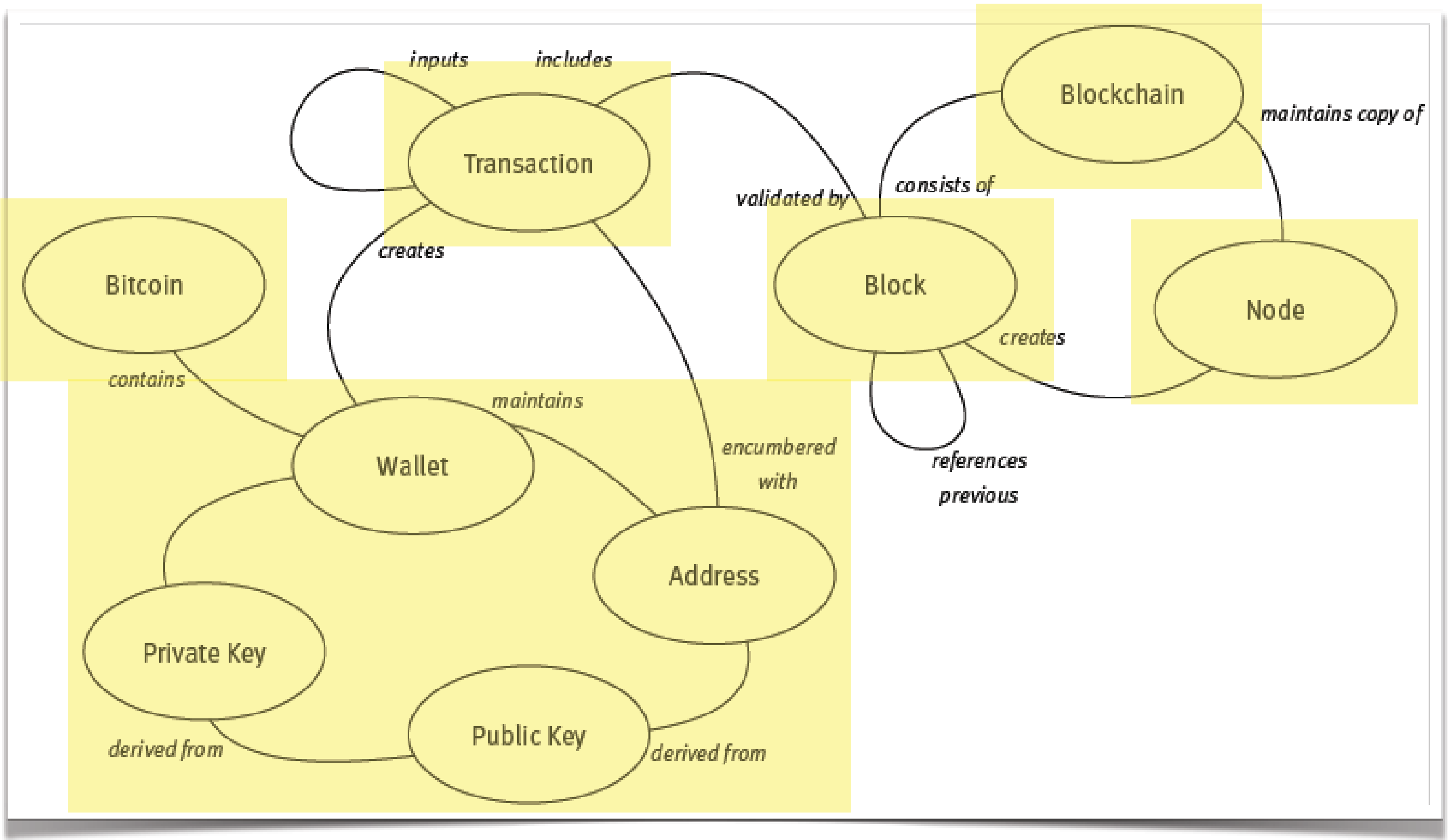
→ *Nodes* aggregate validated transactions into *Blocks*

→ *Nodes Broadcast Blocks* to each other

→ *Consensus* protocol used

→ *Block* reflecting "true state" is chained to prior *Block*

Blockchain and Bitcoin



Key characteristics of blockchain

- *Decentralisation.*
  - *Peer to peer to network*
- *Persistency.*
  - *Transactions stored persistently*
- *Anonymity.*
  - *Avoid Identity exposure*
- *Auditability.*
  - *Easily verifiable and traceable*

Blockchain challenges and opportunities: a survey - by Zibin Zheng et al., 2018

Categories

- Public blockchain
  - Anybody can join anytime
- Private blockchain
  - Fully controlled by one organization who could determine the final consensus
- Consortium blockchain
  - Only a selected set of nodes are responsible for validating the block

Comparison

Table 1 Comparisons among *public blockchain*, *consortium blockchain* and *private blockchain*

Property	*Public blockchain*	*Consortium blockchain*	*Private blockchain*
Consensus determination	All miners	Selected set of nodes	One organisation
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralised	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

Basics: The consensus problem

There are n nodes, that each have an input value. Some of these nodes are faulty or malicious. A distributed consensus protocol has the following two properties:

- It must terminate with all honest nodes in agreement on the value.

- The value must have been generated by an honest node.

Consensus in Bitcoin

What will the consensus be about?

What are the practical challenges?

- latency, lack of global clock, arbitrary failures
- no control on identities
- arbitrary failures, including deliberate attempts to subvert

What about those consensus impossibility results?

Consensus in Bitcoin

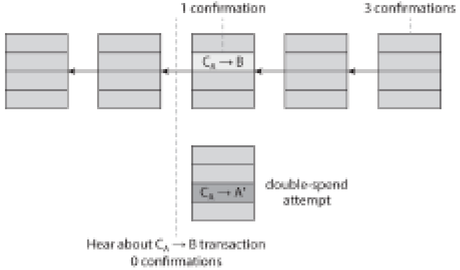
Nakamoto consensus

- Proof of Work: Random node in the network gets to choose the next block to be added.
- Other nodes choose to accept/reject block: ideally based on validity of transactions (unspent, signed).
- Incentives for proof of work: Block reward, transaction fees.
- Forking possible: Only the blocks in the longest chain will typically be accepted by the majority.

Consensus in Bitcoin

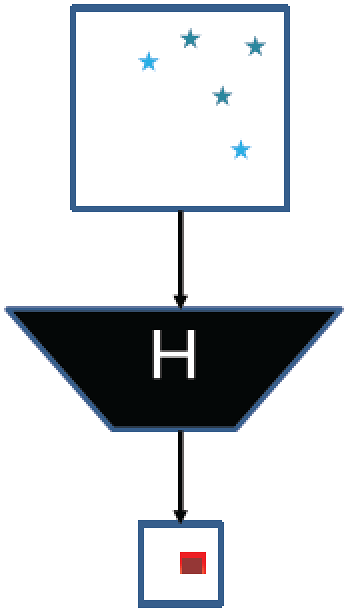
Nakamoto consensus: potential problems?

- Stealing coins: Not without breaking digital signature
- Denial of service: “Victim” needs to wait for a next honest random node.
- Double spending: May succeed (the double-spend probability decreases exponentially with the number of confirmations)



Mining and proof of work

- Hash puzzle: Difficult to compute
  $H(nonce||prev\_hash||tx||tx||\ldots||tx) < target$
- Parametrizable cost: Rate limit the block creation ~10 minutes per block
- Trivial to verify: For other nodes to validate

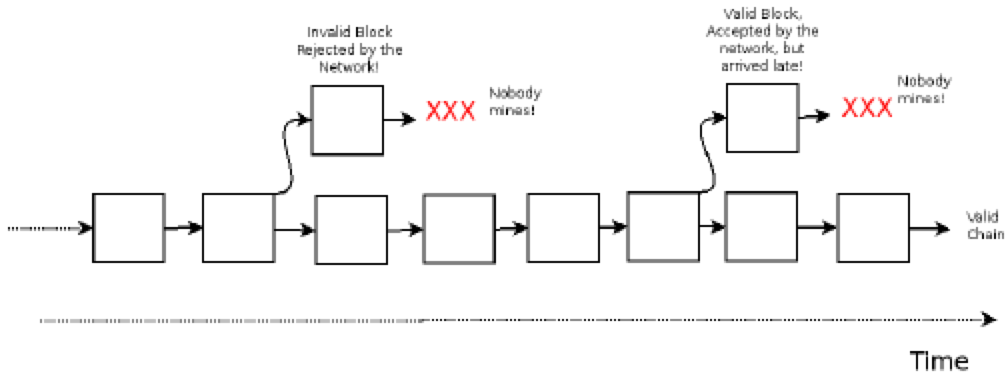


Hardware investment and operational (electricity) costs are barriers to entry and abuse (but also cause of concentration).

Bitcoin: bits & pieces

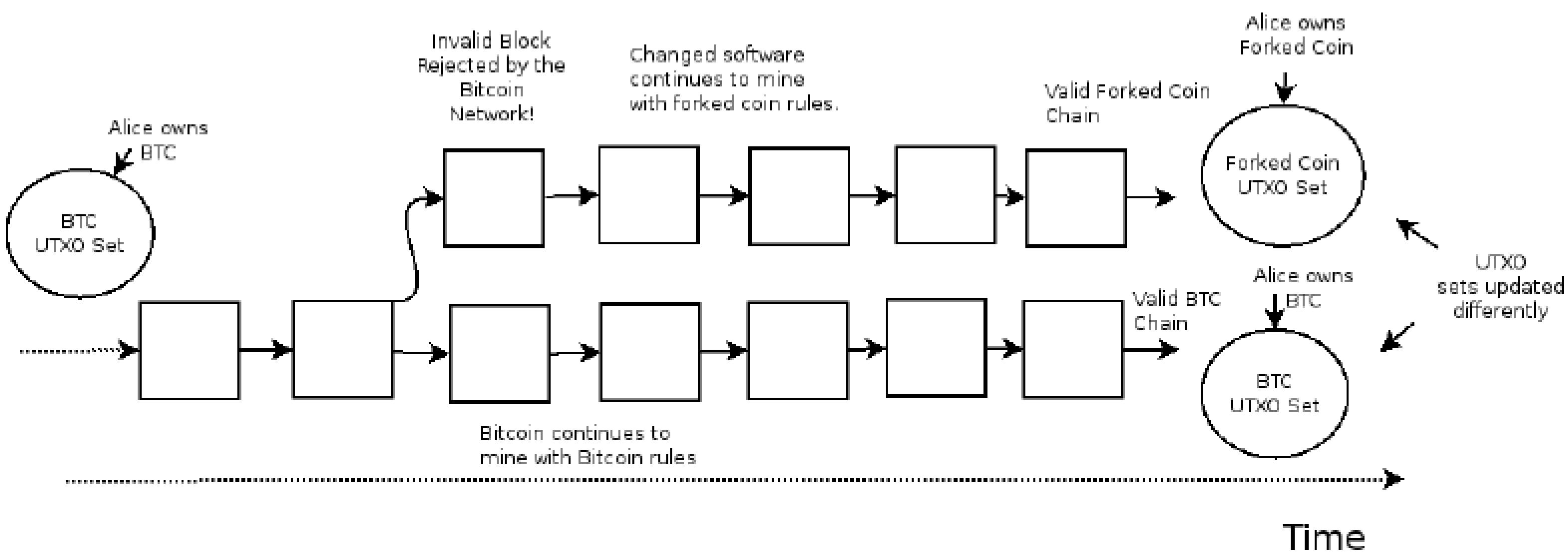
Bitcoin Network

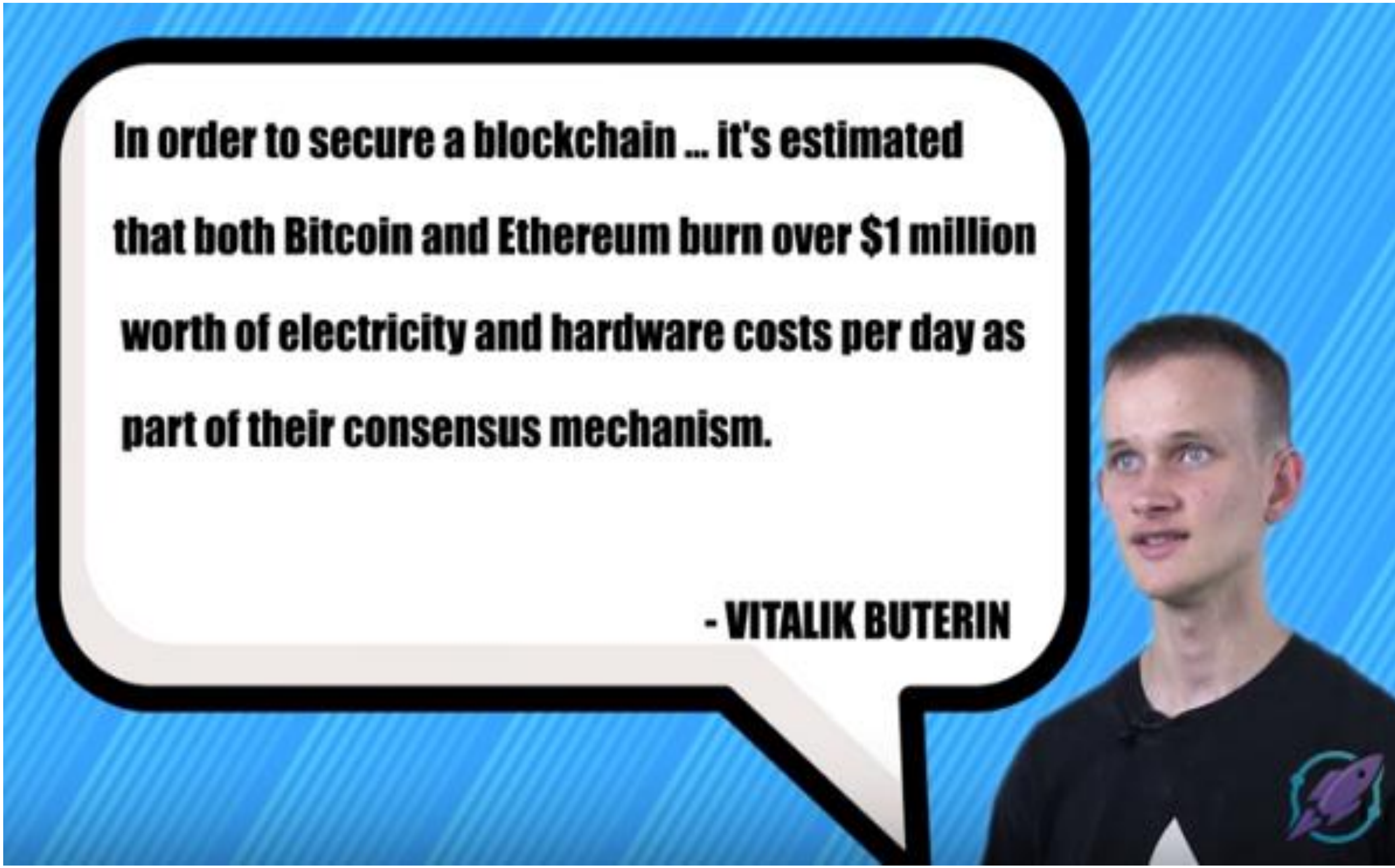
- Randomized peering
- Flooding based transaction propagation
  With local checks: race condition
- Block propagation: forks & longest chain



Bitcoin: bits & pieces

Bitcoin Fork Projects




In order to secure a blockchain ... it's estimated that both Bitcoin and Ethereum burn over $1 million worth of electricity and hardware costs per day as part of their consensus mechanism.
- VITALIK BUTERIN

EDITOR'S PICK | 23,388 views | Apr 19, 2018, 11:09pm

Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That

Sherman Lee Contributor
I write about deep tech, crypto, and artificial intelligence.

Back to Articles

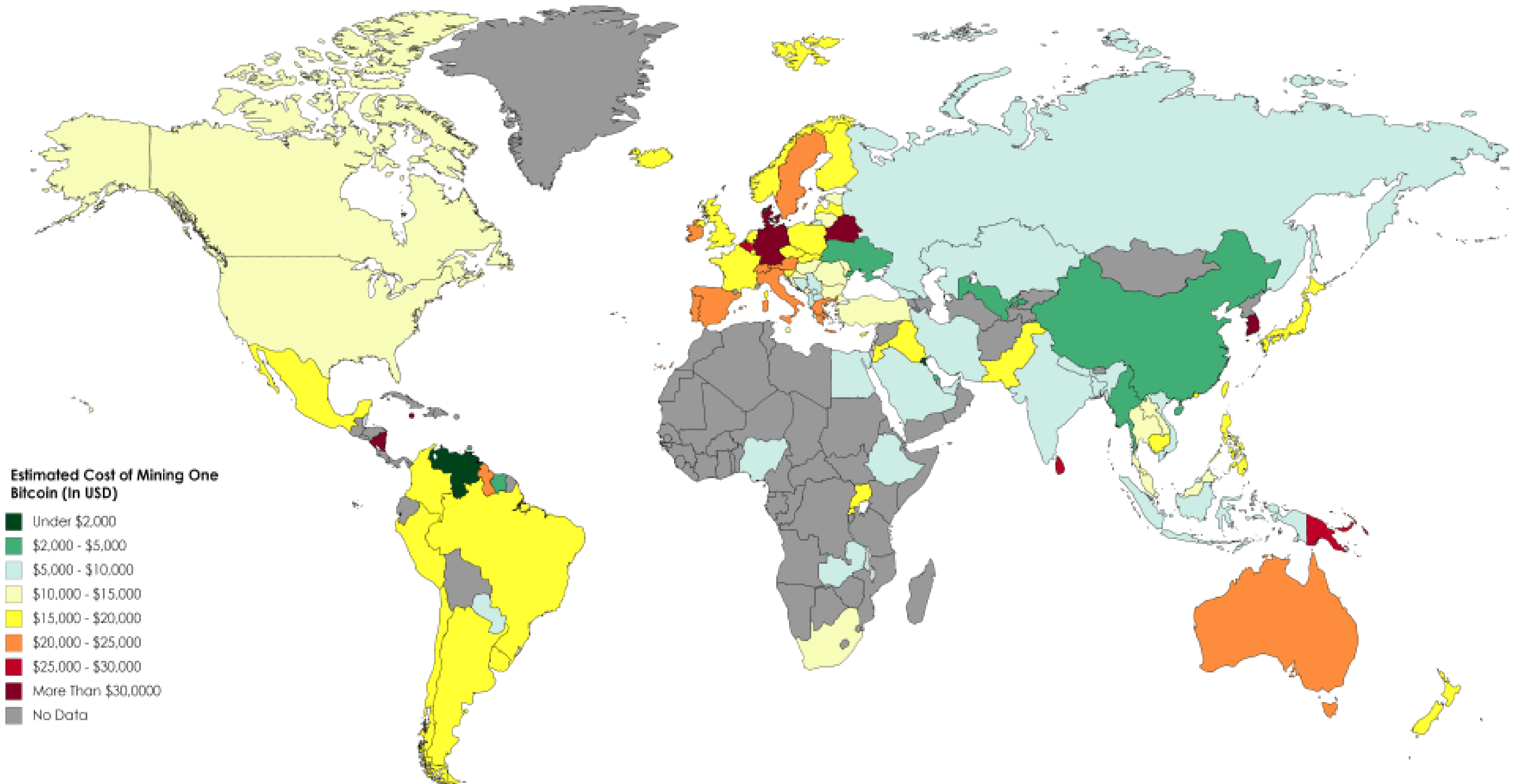
Bitcoins Energy Consumption An Unsustainable Protocol That Must Evolve?

3

3

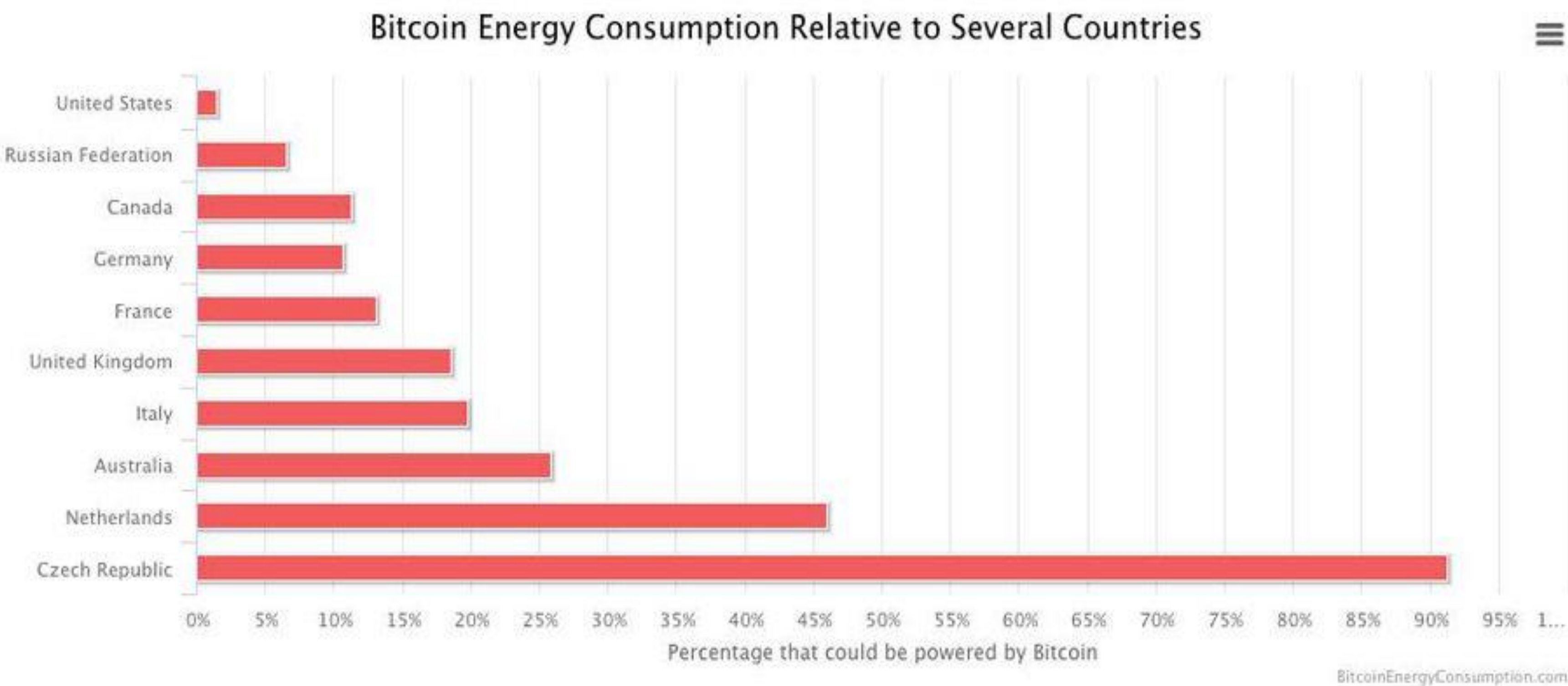
By john lilic #Blockchain 101 #Blockchain for Business #Blockchain for Investors

Estimated Electricity Cost Of Mining One Bitcoin By Country



Source: https://powercompare.co.uk/bitcoin-electricity-cost/

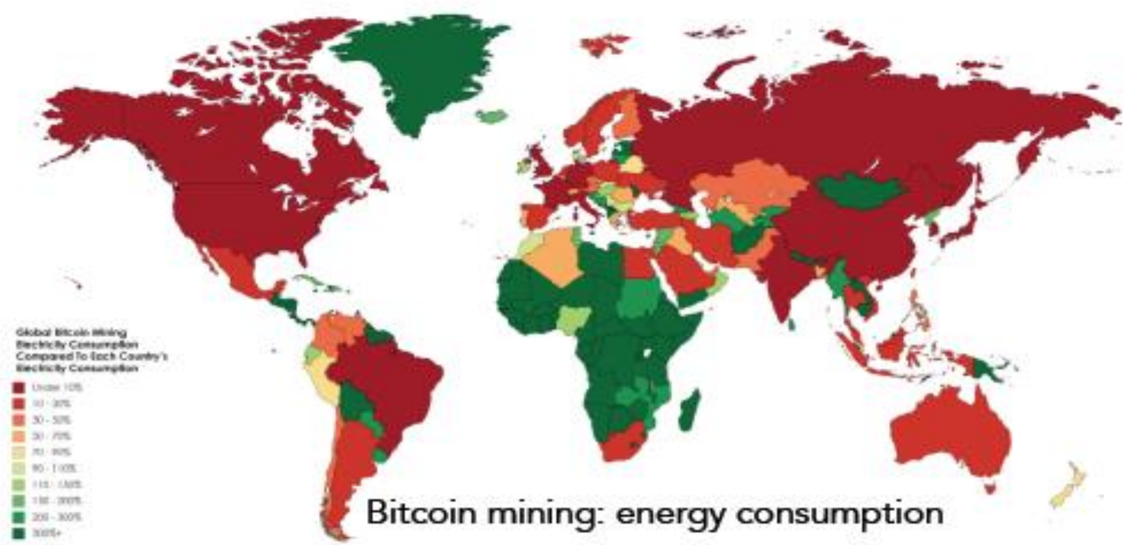
The Bitcoin POW mechanism is so costly that it consumes the same amount of electricity it takes to power a country like Switzerland in one year. Bitcoin's current estimated annual electricity consumption is 61.4 TWh, which is also equivalent to 1.5% of the electricity consumed in the United States.



Proof of X

Proof of Stake

- And others: Burn, Elapsed time, Capacity



Bitcoin mining: energy consumption

Proof-of-X

- Proof-of-X (PoX) schemes is an umbrella term for systems that replace PoW with more useful and energy-efficient alternatives to Proof-of-Work (PoW).

Proof-of-Stake

Miner/Mining Vs. Validator/Minting or forged

- POS requires people to prove the ownership of a certain amount of currency
  - It is believed that people with more currencies would be less likely to attack the network.
  - If richest person attacks, currency value falls and it may be a loss for the attackers!
- Many blockchains adopt PoW at the beginning and transform to PoS gradually.
  - For instance, Ethereum is planning to move from Ethash (a kind of PoW) (Wood, 2014) to Casper (a kind of PoS) (Zamfir, 2015).

Proof-of-Stake

- PoS alternatives consume less energy and reach higher transactions per second.
- But they have also still to prove their attack-resistance in real open public settings like PoW so far.
- Challenge for proof-of-stake systems is to keep track of the changing stakes of the stakeholders.

Proof-of-Stake

- Selection by account balance would result in undesirable centralization because the single richest member would have a permanent advantage as it gets richer.

- Different versions: random selection, age-based stake selection (number of coins stake multiply by the time they have been staked, when selected, time reset to 0)…

Proof-of-Stake: Randomization

- Blackcoin (Vasin, 2014) uses randomization to predict the next generator.
- It uses a formula that looks for the lowest hash value in combination with the size of the stake.

Proof-of-Stake: Coin age

- Peercoin (King and Nadal, 2012) favours coin age-based selection.
- In Peercoin, older and larger sets of coins have a greater probability of mining the next block.
- Once a user has forged a block, their coin age is reset to zero and then they must wait at least 30 days again before they can sign another block.

Proof-of-Capacity

- Sometimes stake could be other things.
- For example, proof of capacity (burstcoin, 2014).
- In proof-of-capacity, participants vote on new blocks weighted by their capacity to allocate a non-trivial amount of disk space.
- Other Examples: PermaCoin, SpaceMint

Proof-of-Capacity

- PermaCoin repurposes Bitcoin’s PoW with a more broadly useful task: providing a robust, distributed storage.
- SpaceMint employs a consensus protocol based on a non-interactive variant of proof-of-capacity (called proof-of-space).

Proof-of-Deposit

- Miners ‘lock’ a certain amount of coins, which they cannot spend for the duration of their mining.
- One such system is Tendermint, where a miner’s voting power is proportional to the amount of coins they have locked.
- Deposit could be revoked if they misbehaved.

Proof-of-Activity

- To combine the benefits of POW and POS, proof of activity (Bentov et al., 2014) is proposed.
- In proof of activity, a mined block (based on PoW) needs to be signed by N validators (PoS) to be valid.
- In that way, if some owner of 50% of all coins exists, he/she cannot control the creation of new blocks on his/her own.
- Since POA marries POW and POS, it draws criticism for its partial use of both.

Delegated Proof-of-Stake

- In Delegated PoS (DPOS), stake-holders don’t vote on the validity of the blocks themselves, but vote (proportionately weighted based on the stake) to elect delegates to do the validation on their behalf.

- The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic.

- Users can also delegate their voting power to another user who will vote on their behalf.

Delegated Proof-of-Stake

- Higher Throughput: With significantly fewer nodes to validate the block, the block could be confirmed quickly, making the transactions confirmed quickly.

- Dishonest delegates could be voted out easily.

- Examples: Steem and BitShares

Proof-of-Burn

- Method for distributed consensus and an alternative to Proof of Work and Proof of Stake

- Miners prove that they have destroyed a quantity of coins, for example by sending them to a verifiably unspendable address.

- Slimcode implemente this approach in 2014 but has recently been discontinued.

Proof-of-Elapsed-Time

- Often used on the permissioned blockchain networks.
- Each node in the blockchain network generates a random wait time and goes to sleep for that specified duration.
- The one to wake up first – that is, the one with the shortest wait time – wakes up and commits a new block to the blockchain, broadcasting the necessary information to the whole peer network
- The same process then repeats for the discovery of the next block.

Proof-of-Elapsed-Time

- The POET network consensus mechanism needs to ensure two important factors:
  - First, that the participating nodes genuinely select a time that is indeed random and not a shorter duration chosen purposely by the participants in order to win, and
  - Second, the winner has indeed completed the waiting time.

Proof-of-Elapsed-Time

- The POET concept was invented during early 2016 by Intel.

- It offers a readymade high tech tool to solve the computing problem of "random leader election."

Hyperledger Fabric : PBFT

- Practical byzantine fault tolerance (PBFT) is a replication algorithm to tolerate byzantine faults (Miguel and Barbara, 1999).

- Hyperledger Fabric (hyperledger, 2015) utilises the PBFT as its consensus algorithm since PBFT could handle up to 1/3 malicious byzantine replicas.

Ripple

- Ripple (Schwartz et al., 2014) is a consensus algorithm that utilises collectively-trusted subnetworks within the larger network.

- In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds.

- In contrast to that PBFT nodes have to ask every node in the network, each Ripple server has a Unique Node List (UNL) to query.

Ripple

- UNL is important to the server. When determining whether to put a transaction into the ledger, the server would query the nodes in UNL.
- If the received agreements have reached 80%, the transaction would be packed into the ledger.
- For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20%.

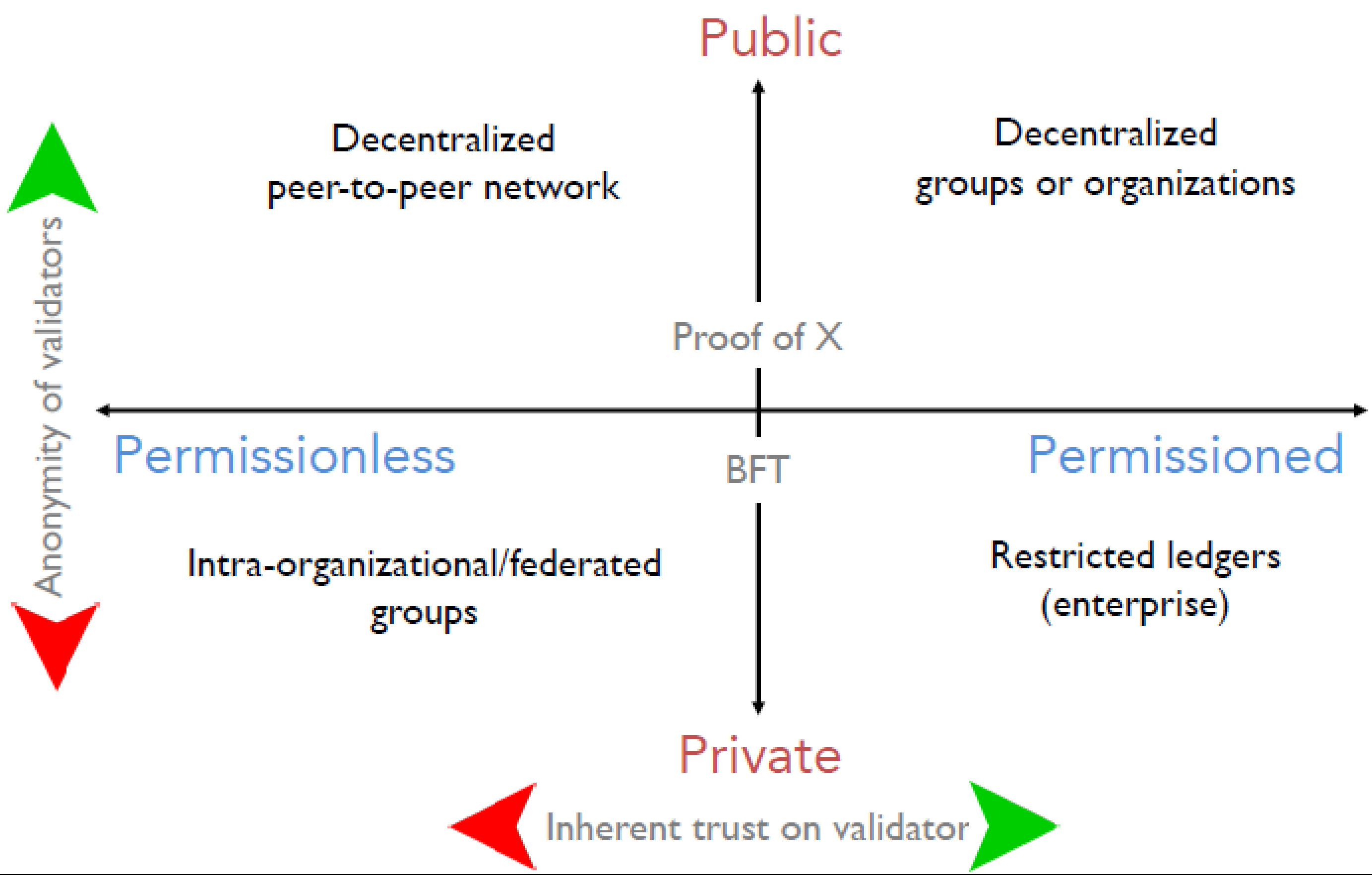
Consensus: A Comparison

Table 2 Typical consensus algorithms comparison

Property	*PoW*	*PoS*	*PBFT*	*DPOS*	*Ripple*	*Tendermint*
Node identity management	Open	Open	Permissioned	Open	Open	Permissioned
Energy saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	$< 25\%$ computing power	$< 51\%$ stake	$< 33.3\%$ faulty replicas	$< 51\%$ validators	$< 20\%$ faulty nodes in UNL	$< 33.3\%$ byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

Blockchain challenges and opportunities: a survey - by Zibin Zheng et al., 2018

Distributed ledger technologies



Proof of X: Attacks

- nothing-at-stake attack: A miners are incentivized to extend every potential fork. Since it is computationally cheap to extend a chain, in the case of forks, rational miners mine on top of every chain to increase the likelihood of getting their block in the right chain.
- grinding attack: A miner re-creates a block multiple times until it is likely that the miner can create a second block shortly afterwards.
- long-range attack: An attacker can bribe miners to sell their private keys. If these keys had considerable value in the past, then the adversary can mine previous blocks and re-write the entire history of the blockchain.