Paul Doherty, 1921454
paul.doherty23@mail.dcu.ie

Blockchain Proofs:

Proof-of-Work is out,
... but is Proof-of-Stake ready to come in?

... and if not - what other Proofs are there?

Agenda

Overview

- “Blockchains use consensus algorithms to elect a leader who will decide the contents of the next block” (*Konstantopoulos, 2017*)
- A blockchain system is a distributed system which depends on a consensus algorithm to ensure agreement on the state among nodes
- The consensus algorithm is the core mechanism in determining how the system behaves
- Distributed consensus has received renewed attention since the birth of the blockchain
- Many consensus algorithms have emerged, each of which possesses varying properties and capabilities

Objectives of Consensus

Identified by *Rosic (2018)* based on data collected from Wikipedia

Seek Agreement

A consensus mechanism should aim to establish as much agreement as possible from the group involved

Cooperative

The greatest benefits will be achieved by working together towards a common goal rather than working towards individual goals

Maximum Inclusion

A large group should be established and as many as possible should be involved

Collaborative

The interests of the wider group should out weight the interests of the individual and all members should work together to achieve this

Equal Voting

All votes should be treated as equal. Each and any member of the group has equal voting rights with all others

Participatory

Active participation by as many members of the group as possible is the preferred approach

Blockchain Proofs: Consensus

Although being one component of a blockchain system, they are critical in supporting the correct functioning of a blockchain.

Consensus mechanisms establish the protocols which ensure that all nodes are synchronised and in alignment with one another.

The nodes all agree on which transactions should be appended to the blockchain based on their validation rules. Transactions are validated and checked consistently by all nodes.

Blockchains run the risk of serious attacks without a suitable consensus mechanism, e.g. double-spend attack.

Figure 1. Image of Blockchain Terms. Blockgenic (2018)

Many ways to reach consensus

Which one to choose?

Fully Decentralised Consensus
VS
Leader Based Consensus

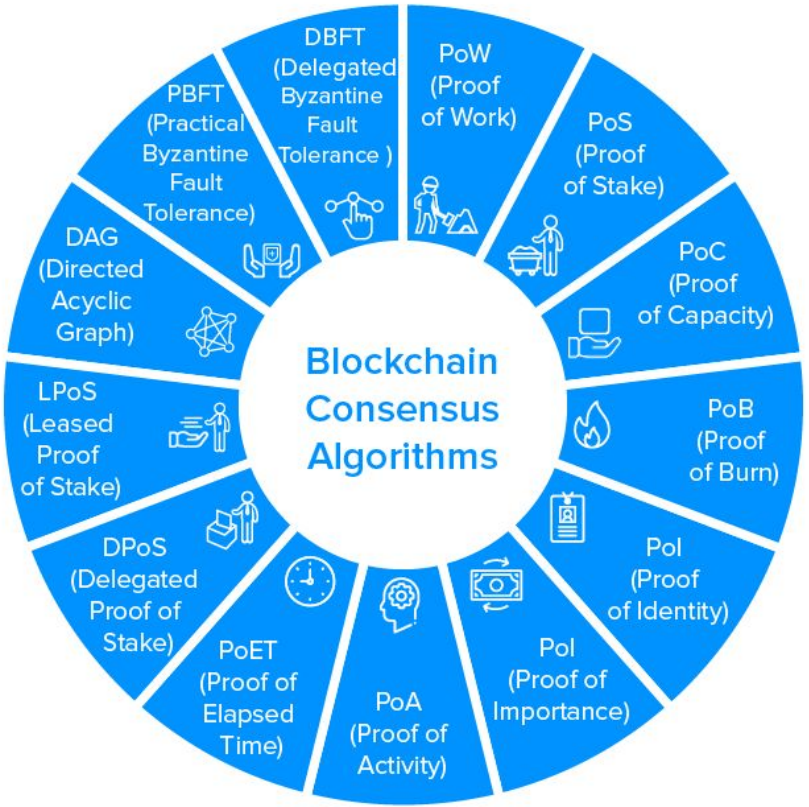


Figure 2. Blockchain Consensus Algorithms. Bhardwaj (2019)

Proof of Work

- The miners “try and solve a hard computational problem in order to validate a batch of transactions and add them as a new block to the blockchain” (*Porat et al, 2017*)
- The blocks secure the transactions by demanding a large amount of energy and computational resources be spent in order to solve the hard problem
- The computational challenge which the miner must solve has been constructed in a manner which makes it extremely difficult to solve
- When the miner eventually solves the challenge, they broadcast their “winning” block to the network and it is subsequently validated by the other nodes and they receive their award (subsidy + transaction fees)
- The actual validation to determine whether a block is valid and can be added to the chain is a far simpler process

Figure 3. Proof of Work. Chainbits Staff (2018)

Proof of Work - Positives

1. **Simplicity**
   No additional mechanisms are needed to manage bad behaviour
   All actors need to expend money on equipment and energy
   Stood the test of time

2. **Difficult to find solution but easy to verify**
   A high degree of trust can be placed on the longest chain of blocks due to the aggregated amount of work involved

3. **Defence from Denial of Service**
   The costs to do a DoS are very high due to the computational power needed
   Messages only enter the network after adequate work has been performed

4. **Open**
   The network is open to all with any computing power and no stake is needed

Proof of Work - Limitations

1. **Security attacks**
   Majority attack (51% attack)
   Attacker has power to control most events in the network
   Monopolise generating new blocks and reverse transactions

2. **Energy consumption**
   Large amounts of electricity are required
   Energy used is bad for environment

3. **Huge expenses**
   Highly specialized computer hardware
   Move from CPU, GPU, FPGA to ASIC
   Barrier to entry and participation
   Can lead to “centralisation”

4. **“Uselessness” of computations**
   The calculations are not applicable anywhere else

5. **Scalability**
   Low transaction throughput
   Reduced performance

Proof of Stake - A Quotation

...“is a vastly more efficient alternative to PoW ‘mining’ and enables blockchains to operate without mining’s high hardware and electricity costs..”

(*Buterin & Griffith, 2017*)

Proof of Stake

- "...is a category of consensus algorithms for public blockchains that depend on a validators economic stake in the network (*Buterin, 2019*)
- A process is initiated which randomly selects one of the nodes to be the validator / minter of the next block
- The chance of the validator being selected is proportional to the "stake" that each of them own
- The validator is discouraged from double-spending or publishing a corrupt block as they risk losing their stake
- The stake is time locked to ensure that the validator must wait a certain period of time before collecting their rewards
- Does not require miners to invest large amounts of resources and effort computing hard problems

Figure 4. Proof of Stake. Chainbits Staff (2018)

Proof of Stake - Positives

1. **More energy efficient**
   Extreme computation not required
   Less impact to environment
   "more energy efficient, mechanism that can provide similar guarantees" (*Kiayias et al, 2017*)

2. **Better Scalability**
   Higher number of transactions per second
   Sharding - splitting the network into shards

3. **Potentially Enhanced Security**
   Less danger of majority (51% attack) as attacker needs to gain control of >50% of stake

4. **Lower Transaction Costs**
   Transaction costs are lower as their is not as much effort required to validate them and to keep the blockchain secure

Proof of Stake - Limitations

1. **Initial Distribution**
   The mechanisms for distributing the initial coins are questionable

2. **Nothing at Stake**
   Validators can stake their coins on forked chains
   No opportunity cost to doing so
   “Voting” on all forked versions

3. **Centralisation**
   Although the barriers to entry in terms of computing power are significantly reduced, larger token holders have increased potential stakes which they can lay

4. **Long-Range attacks**
   Branch going back to genesis block and attempting to overtake the main chain by producing a valid alternate history

Other Approaches

There are other modified variations of the 2 proofs that could be applied.

These include both specific customisations of the proofs and combinations of the pair of them.

01 | Hybrid PoW / PoS

02 | Delegated Proof of Stake

03 | ProgPOW

PoW Outlook

- Proven technology and large market share
- Shortcomings related to energy consumption could be addressed through using renewable energy
- Issues relating to centralisation and expensive hardware costs could be addressed by moving to more dynamic algorithms (e.g. Monero, ProgPOW) that are specifically built for CPU & GPU
- Analysis of industry doesn't seem to suggest that it is on its way "out". It seems like it is very much here to stay perhaps in an enhanced version of its current form

PoS Outlook

- Newer technology with significantly less market share
- It is being backed by some large players (e.g. Ethereum). There has been continued progress in PoS refinement since it was first suggested as an alternate proof
- Increasing number of blockchain implementations are looking to use PoS and this can be seen in recent research, development and deployments

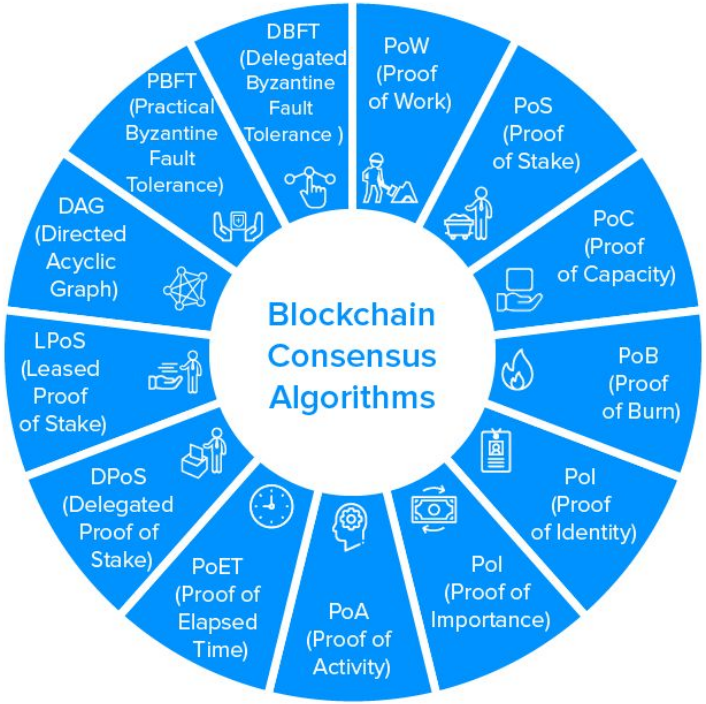
Industry Outlook

- The public blockchain industry continues to grow and “and is projected to reach $23.5 billion by 2030, advancing at a 48.7% CAGR” (Research and Markets, 2020)
- The market is of significant size and variety to embrace a variety of consensus mechanisms that cater for different kinds of business problems
- Bitcoin currently are using PoW and operating a large share of the market with no plans to change so PoW will maintain a large share of the total market capitalization of cryptocurrencies

Is PoS Ready?

- Yes! And No!
- Certain consensus mechanisms are likely to fit better depending on the specific challenge that the implementation is trying to address. i.e . security, throughput, scalability, cost. When it comes to consensus there isn't a one-size-fits-all
- Not as proven as Proof-of-Work in terms of widespread implementations
- There are some security issues that need to be addressed

Overall many alternative consensus mechanisms are welcome as this industry matures



Diversity in consensus is encouraged

Thank you

References

- Konstantopoulos, Georgios (2017). Understanding Blockchain Fundamentals, Part 2: Proof of Work & Proof of Stake. Available online: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb [Accessed 19/04/2020]
- Rosic, Ameer (2018). Blockchain Consensus: A Simple Explanation Anyone Can Understand. https://blockgeeks.com/guides/blockchain-consensus/ [Accessed 20/04/2020]
- Figure 1. Image of Blockchain Terms. Blockgenic (2018). Different Blockchain Consensus Mechanisms. Available online: https://hackernoon.com/different-blockchain-consensus-mechanisms-d19ea6c3bcd6 [Accessed 19/04/2020]
- Figure 2. Blockchain Consensus Algorithms. Bhardwaj, Chirag (2019). A 14 Minute Guide to Understanding Blockchain Consensus Algorithms. Available online: https://appinventiv.com/blog/blockchain-consensus-algorithms-guide/ [Accessed 22/04/2020]
- Porat et al. (2017). Blockchain Consensus: An analysis of Proof-of-Work and its applications.. Available online: https://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf [Accessed 20/04/2020]
- Figure 3. Proof of Work. Chainbits Staff (2018). Proof of Work Definition. Available online: https://www.chainbits.com/cryptocurrency-terms/proof-work-definition/ [Accessed 19/04/2020]

References

- Buterin, Vitalik & Griffith, Virgil (2017). Casper the Friendly Finality Gadget. Available online: https://arxiv.org/pdf/1710.09437.pdf [Accessed 21/04/2020]
- Buterin Vitalik (2019). Proof of Stake FAQ. Available online: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ [Accessed 24/04/2020]
- Figure 4. Proof of Stake. Chainbits Staff (2018). Proof of Stake Definition. Available online: https://www.chainbits.com/cryptocurrency-terms/proof-stake-definition/ [Accessed 19/04/2020]
- Research and Markets (2020). Global Blockchain Devices Industry, Forecast to 2030. Available online: https://www.prnewswire.com/news-releases/global-blockchain-devices-industry-forecast-to-2030---market-to-grow-from-300-million-in-2019-to-23-5-billion-by-2030--exhibiting-a-cagr-of-48-7-301037661.html [Accessed 25/04/2020]