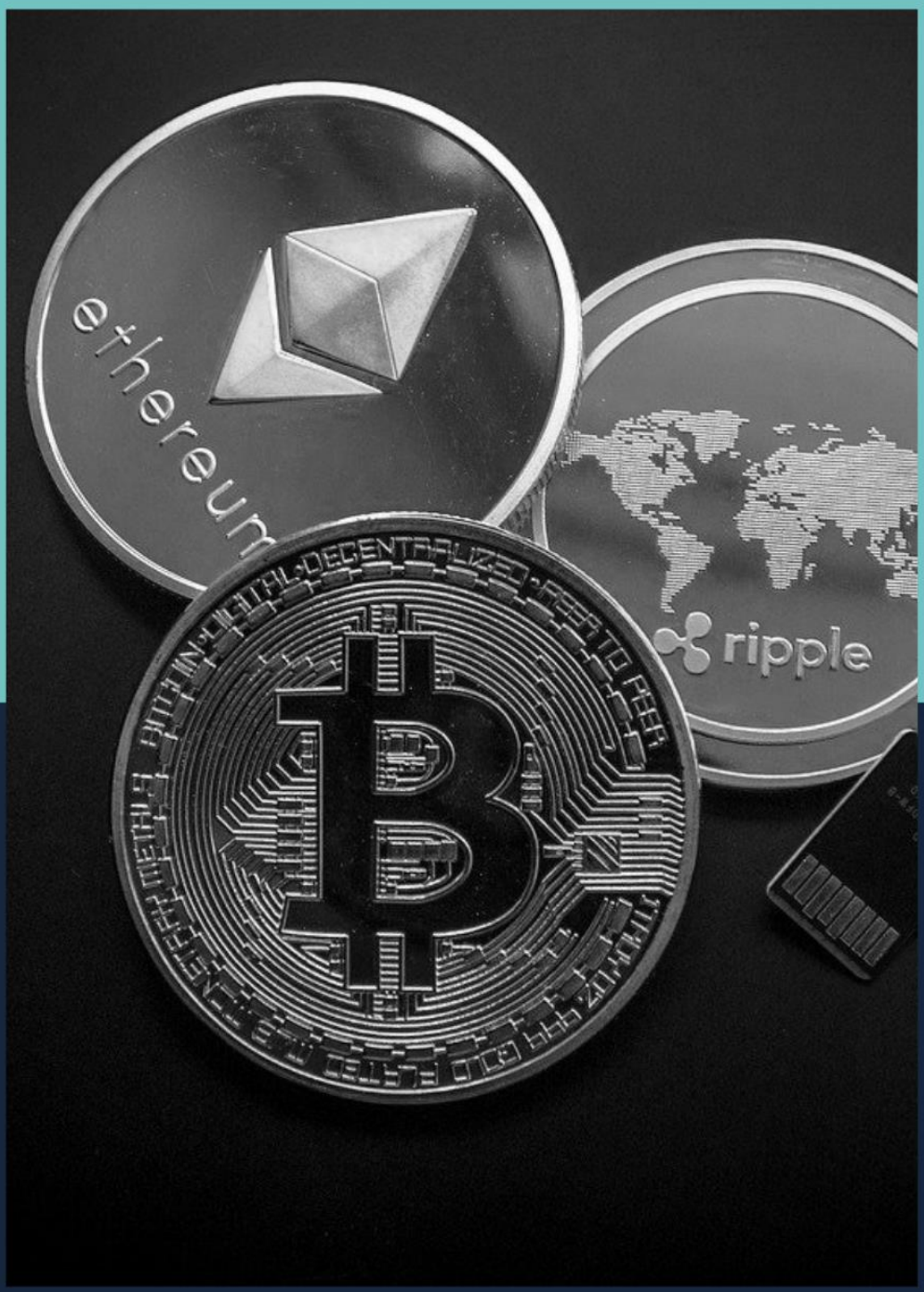

CONSENSUS ALGORITHM

-Project Proposal-

Consensus Algorithm

Synopsis:

Development of a universal yet Flexible **consensus algorithm** supporting the participation of IoT and Mobile devices with the most efficient utilization of resources.

Features of My Proposed Algorithm:

- Even using smaller devices like a mobile phone, people can participate.
- No need for large funds to join the network.
- Super speed transactions.
- Can be adapted to public and private use.
- Resistant to network splits and network anonymous attacks.
- A small amount of bandwidth required for the effective working of the network.
- Everyone in the network gets a fair amount of chance despite of computational power or the size of the stake.
- Can be used for various real-life application.
- Customizable according to the need.
- Comparatively less usage of resources.
- Energy efficient.
- Secure.

Impact:

This idea will enhance the adaptability of the system. The easy customization will allow businesses to set up their unique blockchain system according to their needs. Super speed transaction will help to use this blockchain for real-life problems. The low cost of participation will help to develop a blockchain "FOR MASSES". Reduced use of bandwidth will help to use this technology in a remote area and thus increases accessibility. The energy efficiency of the system will support greener development. Controllable transparency of the system will help to use it in the public sector, where transparency is important as well as in the private sector, where transparency varies with companies.

Execution plan:

Step 1: Research

I will research various consensus algorithms and their features.

Step 2: Define

I will propose an Algorithm

Step 3: Validate

Then I will discuss my idea with my peers in Zeeve Inc. Make corrections by hearing their suggestions about my idea.

Step 4: Build/Code

I and my Peers will start working to convert our idea into a working project.

Deliverable:

By **June 20:** Completion of first two steps (Research & Define).

June 21-June 27: Discussing existing solutions, Targeted Audience and their data. Confirming the tech stacks going to be used. Making final project Proposal including all this data.

June 28: Validating project idea

June 29-July 18: Making of Prototype 1.0

July 19 - July 25: Testing and Debugging of Prototype (phase 1).

July 26 - August 16: Making of Prototype 1.1 Based on the data got from Testing and Debugging phase 1.

August 17 - August 23: Testing and Debugging Prototype 1.1 (phase 2)

August 24 - September 13: Making of Final Prototype. Based on the data got from Testing and Debugging phase 2.

September 14 - September 20: Doing final correction and preparations for prototype presentation.

September 23: Project Presentation.

Related Work:

Transecure:

Developed Transecure, a decentralized intracompany transaction management system to ensure that all transactions are transparent and all finances are accounted for which is realized by using Blockchain Technology.

Tech stacks used: Python, Flutter, Javascript, Html, CSS.

Project repo: https://github.com/lijozech-12/transecure

Escrow Smart Contract:

I had worked on an escrow smart contract project with my friend. I was involved in the ideation phase and mainly contributed to brainstorming new ideas for the project. It is a financial instrument held by a third party on behalf of two other parties who are completing a transaction. It helps make transactions more secure by keeping the payment in a secure escrow account which is only released when all of the terms of an agreement are met Escrow service using blockchain can successfully solve the buyer-seller dilemma by being the trusted third party that holds the funds securely while the other party delivers its end of the deal. With the intervention of Escrow systems, the seller is sure that he/she gets paid once the goods or services are delivered while the buyer is sure of getting the goods before the funds are released to the seller.

Project repo: https://github.com/annu12340/Escrow-Smart-contract

Project PPT: https://www.canva.com/design/DAENGP6GxxY/6NrmU-13vStgoMxMgu8JrA/view?utm_content=DAENGP6GxxY&utm_campaign=designshare&utm_medium=link&utm_source=publishpresent

Different Consensus Algorithms.

Name	Pros	Cons	Resources	Marks (out of 10)
Proof of work (POW)	Solved byzantine general issue on a larger scale. In this algorithm, it is very hard to find the solution to the mathematical problem. But it is easy to verify the answer.	51% attack: It is possible to combine the top 3 or 4 mining pools in the world and achieve the majority of blocks. It will destroy the decentralized nature of blockchain technology. Time-consuming: Since Mining of new block takes time from 10 to 60 minutes. It's very time consuming and it's not instantaneous. Resource consuming: Mining of each block Consumes a lot of electricity, money, space and hardware. So, it is consuming valuable resources. The reward for mining a block diminishes with time and eventually, it will become less profitable to mine a blockchain. Crypto currency based on POW don't have a stable price ex: bitcoin. Mining pools cause centralization and opposes decentralization idea of blockchain.	https://www.geeksforgeeks.org/proof-of-work-pow-consensus/ https://bitcoin.org/bitcoin.pdf https://youtu.be/3EUAcxhuoU4	3

Proof of Stake (POS)	More energy efficient than proof of work. No need of buying expensive hardware. This will encourage more people to be the part of proof of stake. Safer than pow since nobody is able to attain 51% of the stakes. If a person has more stakes he will try to establish the security of the system. He knows if the system fails he will lose his earnings. Cost of Attack is larger than potential reward. More stable price for the crypto currency.	It's more complicated system and difficult to secure. Adding punishment and collateral creates new variables in the algorithm all of which need to be tested, and each of which could present a security weakness if the algorithm is not written correctly. Harder for an average investor to participate. Tend towards centralization. People with more stake have more chance to get more through forging the block.	https://www.investopedia.com/terms/p/proof-stake-pos.asp#:~:text=The%20Proof%20of%20Stake%20(PoS,more%20mining%20power%20they%20have. https://www.skalex.io/proof-of-work-vs-proof-of-stake/#:~:text=4.-,Benefits%20%26%20Drawbacks,system%20and%20difficult%20to%20secure https://youtu.be/psKDXvXdr7k	6
Delegated Proof of work (DPos)	Protection from centralization and malicious usage. Small stake holder get opportunity. Scalable than POW. Faster than POW and POS. Energy efficient and environmental friendly Considered as the most decentralized approach on consensus mechanism Strong protection against double spend attack.	For the successful existence of network requires genuinely Interested group of people It is vulnerable to centralization. Same flaws as a classic real life voting.	https://en.bitcoinwiki.org/wiki/DPoS	6.5

Proof of Burn (POB)	Reduces Inflation Combination of POW,POS and POB Don't take to much resources other than burned coins. Due to the decay of burned coins over the time it avoids the unfare advandage of early miners and promotes regular activity by the miners.	Leads to coin scarcity Still not tested on large networks yet.	https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp https://coinmarketcap.com/alexandria/glossary/proof-of-burn-pob#:~:text=Proof%2Dof%2Dburn%20(PoB)%20is%20a%20blockchain%20consensus,permanently%20eliminating%20cryptos%20from%20circulation.	6.5
Ripple Protocol Consensus algorithum	Strong correctness for byzantine failures Ideal for financial transaction due it's speed, low latency and provable security We can transfer any commodity. Trancation are much quicker and cheaper. Many Banks started using it.	Highly centralized. Ripple lab owns 61% of coins making it a monopoly. Not ready for Real world use. Highly vulnerable for attack.	https://ripple.com/files/ripple_consensus_whitepaper.pdf https://www.geeksforgeeks.org/how-does-ripple-control-protocol-algorithm-work/ https://reasonabledeviations.com/notes/papers/ripple_consensus_protocol/ https://www.upgrad.com/blog/what-is-ripple-blockchain/	5.5
Proof of Elapsed Time (PoET) (created by Intel)	Workflow is similar to POW. But energy and resource efficient Every node get fair chance Readymade high tech tool Highly Scalable	Targets private blockchains Highly dependent on intel's technology Highly vulnerable to attacks and software,hardware bugs.	https://sawtooth.hyperledger.org/docs/core/nightly/0-8/introduction.html#proof-of-elapsed-time-poet https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp	4

Proof of Authority (POA)	Easily scalable system. Energy efficient. Can be utilized in real life application like supply chains or trade network. Fees are extremely low and Fast transaction. Blocks are created under 5 seconds. Reduces network maintenance cost.	Decentralization is not possible Preferable in private blockchains. Reputation can't keep participants from malicious activityies. Not widely used in Practice	https://changelly.com/blog/what-is-proof-of-authority-poa/ https://www.geeksforgeeks.org/proof-of-authority-consensus/	4
Proof of Space	Phones can be used for mining process. No need expensive hardware.	Requires lot of P2P interaction. So, Leads to network congestion Need of storage space lead to another arm race for components.	https://en.wikipedia.org/wiki/Proof_of_space	5.5
Leased Proof of Stake.	Covers diverse needs. Easy creation of custom crypto currency tokens. Harder to 51% attack. Ensures no third party involvement.	New technology it's vulnerabilities not yet fully exposed. Where members lease most coins can get a unfair adavandage. Only Full node owners can validate. Tokens are fixed	https://academy.binance.com/en/articles/leased-proof-of-stake-consensus-explained	5
Practical Byazantine Fault Tolerance (PBFT)	Fast, Scalable	Used in private, permissioned networks	http://pmg.csail.mit.edu/papers/osdi99.pdf	6
Delegated Byazantine Fault Tolerance(dBFT)	Good for any network Fast, Scalable Support large scale commercial application.	Everyone is fighting for becoming root chain. There can be several root chain.	https://finance.yahoo.com/news/delegated-byzantine-fault-tolerance-dbft.	7

	Upto 10000 TPS			
Proof of Retrievability. (Used by Microsoft).	Data integrity Minimizes storage and computational overhead Used mainly in cloud computing.	Don't know.	https://eprint.iacr.org/2008/175.pdf http://oaji.net/articles/2017/1992-1514448044.pdf	5
Proof of weight	Based on algorand consensus model. Energy efficient Highly customizable and scalable	Incentivization can be hard.	https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-capacity-space/proof-of-weight-poweight https://arxiv.org/pdf/1607.01341.pdf	5
Proof of reputation	Energy efficient Secure. Faster. Decentralized.	Only used in private, permissioned blockchain.	https://medium.com/gochain/proof-of-reputation-e37432420712	6
RAFT	Simpler model Implementation available in many languages.	Used in private, permissioned networks.	https://en.wikipedia.org/wiki/Raft_(algorithm) https://raft.github.io/raft.pdf	5
MOKKA	Resistant to network spilits and anonymous attack. compacts		https://arxiv.org/ftp/arxiv/papers/1901/1901.08435.pdf https://ega-forever.github.io/mokka/	6

	Blockchain Type	Transaction Finality	Transaction Rate	Token needed	Cost of participation	Scalability of peer network	Trust model	Adversary Tolerance
POW	permissionless	Probabilistic	Low	Yes	Yes	High	Untrusted	<=25
PoS	Both	Probabilistic	Low	Yes	Yes	High	Untrusted	Depends on specific algorihm used
PoET	Both	Probabilistic	Medium	No	No	High	Untrusted	Unknown
BFT and variants	Permissioned	Immediate	High	No	No	Low	Semi-trusted	<=33%
Federated BFT	Permissionless	Immediate	High	No	No	High	Semi-trusted	<=33%
Delegated Proof of work (DPos)	Permissionless	Algorthamic	High	Yes	Yes	High	Untrusted	Unknown
Proof of Burn (POB)	Permissioned	Probabilistic	Low	Yes	Yes	High	Trustless	<=30%
Ripple Protocol Consensus algorithm	Permissioned	Probabilistic	High	Yes	Yes	High	Trusted	<=20%

Proof of Authority (POA)	Permissioned	Immediate	High	No	Yes	High	Trusted	<=49%
Proof of Space	Permissionless	Don’t know	Low	No	Yes	Medium	Trustless	Don’t know
Leased Proof of Stake	Permissionless	Immediate	High	Yes	Yes	High	Trustless	<=33%
Proof of Retrievability.	Permissioned	Immediate	High	No	No	High	Trusted	Don’t know
Proof of weight	Permissioned	Probabilistic	High	Don’t know	Don’t know	High	Don’t Know	Don’t Know
Proof of Reputation	Permissioned	Immediate	High	No	Yes	High	Trusted	<51%
MOKKA	Permissionless	Immediate	High	No	Don’t Know	High	Trustless	<51%
RAFT	Permissionless	Probablistic	Medium	Yes	Don’t Know	Low	Trustless	Don’t know

Submitted by

Lijo Zechariah James

3rd year B-Tech Computer Science

Government Model Engineering College

Thrikkakara, Ernakulam, Kerala, India