XenBlocks: High performance Blockchain design with transactions at the speed of light

.

XenBlocks: High performance Blockchain design with transactions at the speed of light v0.1

Legal Disclaimer: Nothing in this White Paper is an offer to sell, or solicitation of an offer to buy any tokens. Fair Crypto foundation is publishing this White Paper solely to receive feedback and comments from the community. Nothing in this document should be treated or read as a guarantee or promise of how we plan to develop or give utility or value of any tokens. This paper outlines the plan, which could change in any way at our discretion during the course of development. This paper should be read as a technical overview of XenBlocks project without any statements about any future events which may or may not occur.

Abstract

This paper proposes a novel blockchain architecture based on the hybrid merge of Proof of Work (POW) with Proof of Stake (POS). The focus is to improve the current state of the art of message overhead while improving speed of the cryptographically signed transaction confirmation times with asynchronous non-blocking state replication in Byzantine Fault Tolerant state machine. The paper proposes several algorithms leveraging the strong security of POW hash discovery to improve Sybil resistance while remaining fairly decentralized with strong immutability of transaction state. The proposed blockchain leverages Bitcoin block ordering merged with Ethereum compatible programmability through the use of Smart Contracts. Standalone tests indicate transaction confirmation times as low as 200ms with throughput of 75,000 TPS using medium/large-grade node hardware.

1 Introduction

The state of the art blockchains (Bitcoin, Ethereum) often suffer from high gas feels, slow transaction confirmation times, block reorganization. While newcomers (Cosmos, Solana, Polygon) are often prioritize transaction execution time at the expense of data immutability. For example, Polygon relies on transaction settlement on the Ethereum chain, being defacto a Layer 2 solution. Solana while being extremely fast, suffers from stability issues and excessive consensus validation network chatter across their architecture. XenBlocks design introduces a concept of delegated consensus within a single blockchain layer, separating transaction confirmations (done by POS layer) from block immutability provided by the POW layer. We aim to achieve real-time (sub 200ms) transaction conformation times for the blockchain end-users, while delivering strong distributed data immutability, secured by well established mining algorithms pioneered by the POW blockchains.

2 System Design

As shown in Figure 1, the network includes generally used Proof of Work difficulty consensus, the POW group of miners is unlimited, allows anyone to join the network to participate in a race to solve a cryptographic challenge utilizing Argon2ID memory hard hashing algorithm. Participating miners help to secure the network in several ways, a). Miners jointly share the generation of the reward token - Xenium, which is used as Gas (transaction fee) which in turn reduces the likelihood of DDOS and Sybil attacks on the network. A miner, at their own discretion can stake Xenium to be elected as block proposers. The purpose of a block proposer is to package the incoming blockchain transactions into Merkle Trees, which are in turn validated (voted on) by all participating miners. Just like in Solana and EOS, the block proposer schedule is predefined with one POS node acting as a Coordinator. The Coordinator's job is to receive and sequence all incoming transactions while running as Active Coordinator. The consensus and strong data immutability is achieved by receiving a threshold amount of Votes by the miners, which examine proposed Blocks (Merkle Trees) for any errors.

In case of network partitioning the blockchain data structure is recovered by comparing the longest chains of blocks, with the longest chain winning when the network is repaired. While acting Coordinators in POS group are expected to run relatively fast hardware, the miners can be ran from home using any type of compatible hardware.

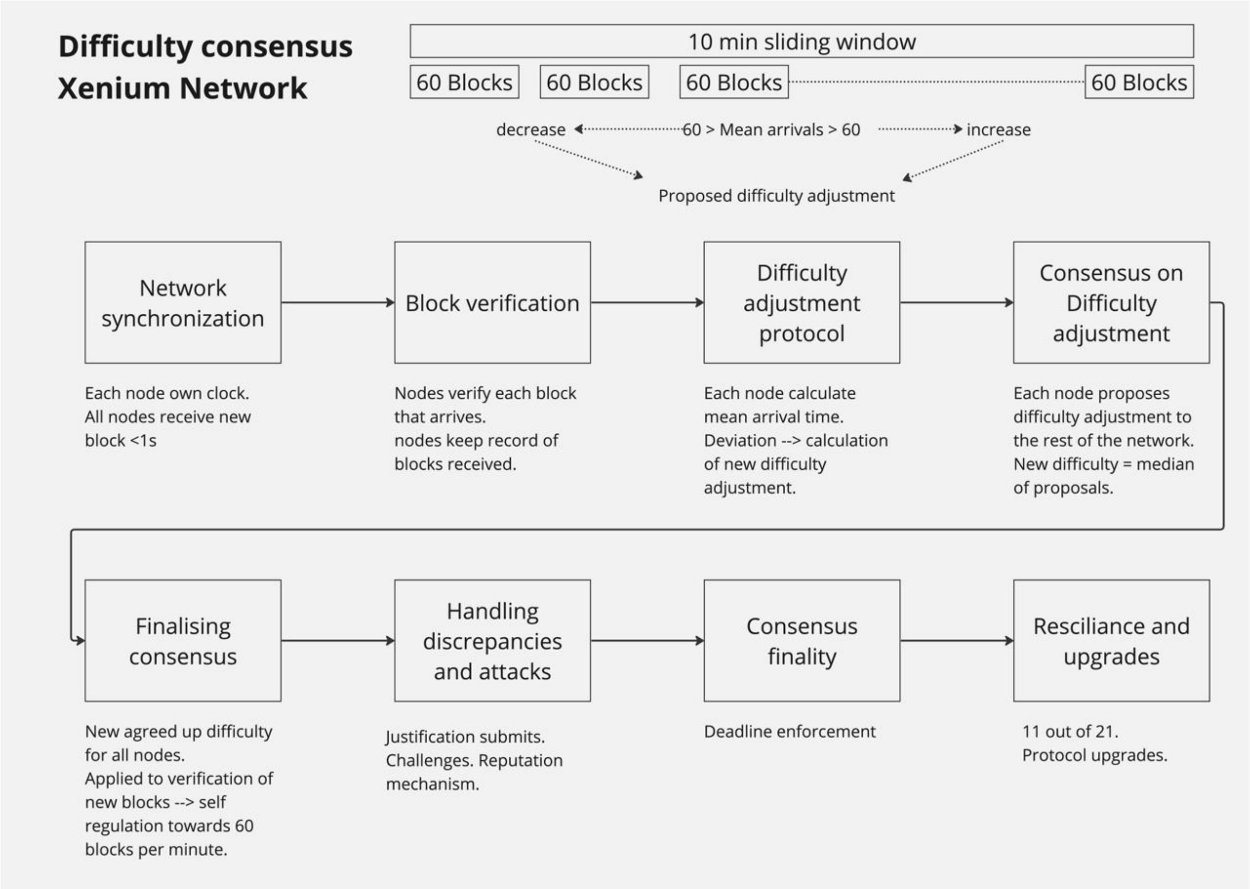
Difficulty consensus
Xenium Network
10 min sliding window
60 Blocks
60 Blocks
60 Blocks
60 Blocks
decrease
60 > Mean arrivals > 60
increase
Proposed difficulty adjustment
Network synchronization
Block verification
Difficulty adjustment protocol
Consensus on Difficulty adjustment
Each node own clock. All nodes receive new block <1s
Nodes verify each block that arrives. nodes keep record of blocks received.
Each node calculate mean arrival time. Deviation --> calculation of new difficulty adjustment.
Each node proposes difficulty adjustment to the rest of the network. New difficulty = median of proposals.
Finalising consensus
Handling discrepancies and attacks
Consensus finality
Resciliance and upgrades
New agreed up difficulty for all nodes. Applied to verification of new blocks --> self regulation towards 60 blocks per minute.
Justification submits. Challenges. Reputation mechanism.
Deadline enforcement
11 out of 21. Protocol upgrades.

Figure 1.

3.1 Proof Of Work

Participating Miners utilize Argon2ID, a memory hard one-way hash algorithm. Argon2ID difficulty adjusts the memory requirement shared by all miners which is GPU and ASIC resistant in nature. Large memory requirements make ASIC development rather costly, while GPUs being 20-30x faster to provide a solution require relatively large VRAM allocation reducing the hash speeds as difficulty moves up. Miners are rewarded with three types of tokens, which are merged mined, XENIUM, XUNI and Superblocks (X.BLK). Tokens can appear in any produced Hash and do not require a separate mining process. XENIUM is rewarded at the rate of 10 XENIUM per discovered block, while XUNI can only be mined at the top of the hour. SuperBlocks (X.BLK) are about 1000x harder to find within the generated Hash. Miners coordinate block inclusion into the blockchain using traditional sha256 hash of a hash process, where the block's merkeroot is hashed with a previous block. All blocks are distributed across participating full nodes using P2P.

3.2 Transaction Ordering

Every transaction received by the Coordinator is signed by utilizing Keccak256 ethereum compatible algorithm, allowing for the use of popular wallets like Metamask, Rabby and others. Transaction ordering does not require Proof of History (in case of Solana) as a generally accepted nonce counter is used as a necessary part of the transaction. Nonce itself is hashed and is part of the transaction signature. The active Coordinator is able to order transactions by verifying nonce, ensuring there is no front-running of double spending is possible by the user account. The Coordinator runs transaction verification by using the standard Ethereum libraries, if accepted adding transactions to the merkle tree along all other transactions. While there is no minimum block size, the Coordinator packs all transactions into the Merkle Tree data structure producing the MerkleRoot hash, which can be later verified by the other participating nodes.

3.3 Voting

While a set of coordinators propose blocks containing transactions, the voting for the block is done by all available miners at the time of hash discovery. The valid POW Hash acts like a ticket that allows the miner to vote on (and validate) the proposed block. A threshold amount of votes (10, 20, 40) based on the current network mining difficulty is required for all blocks to be deemed valid and be accepted into the blockchain. Miners produce at least one hash solution per second and are chosen randomly by the network given the order of discovered blocks is driven by the elliptic curve hashing algorithm (Argon2ID) is impossible to predict. The randomness of the solution discovery provides natural resistance to Miner/Coordinator collision. Miners are disincentivized at providing incorrect votes and are punished with Xenium reward slashing. Coordinators are disincentivized to propose incorrect blocks due to slashing of their staked Xenium. Coordinators receive rewards from transaction fees of every correctly assembled block.

3.4 Scaling

The network archives horizontal scaling due to the asynchronous nature of Miners and Coordinators. Shared network difficulty allows for an unlimited number of miners to participate (just as in Bitcoin blockchain), where Coordinators are picked by the network from a group of willing miners. Coordinators do not ever have to wait for miners to include blocks into the blockchain when confirming transactions. In the traditional blockchain designs (Bitcoin, Ethereum), transaction confirmations are produced by miners, which makes confirmations slow and transactions expensive. In the new blockchain designs (Solana) transactions, while being inexpensive, cause excessive network chatter creating network instability and expensive hardware requirements for all participants. XenBlocks leverage algorithmic block voting without suffering from any of those problems.

3.5 Overhead and benchmarking

Ryzen (consumer grade) CPUs are able to process up to 75,000 transactions per second without any need for specialized hardware like GPUs. Miners are often able to use cloud based GPUs with inexpensive consumer grade gear (Nvidia 3060, 3070, 3090, 4090). CPU mining is possible but slow. Block broadcasting is naturally asynchronous with P2P engines like LIBP2P gossip protocol. Coordinators are able to utilize websockets without much of the network overhead achieving near real-time network speeds using the PUBSUB (Listener/Broadcaster) model.

3.6 Elections of Coordinators

Any participating miner can become a validator by staking Xenium. The POS Coordinator group consists of 21 (or larger) of nodes minimum. The coordinator schedule is published ahead of time with active Coordinator staying in their specific epoch for at least 1,000 Blocks (16.6 minutes). Should proposed coordinators crash or otherwise disappear from the set, a new Coordinator is elected and placed in the waiting set. The schedule of Coordinators are broadcasted across the network with P2P. Any Coordinator that produces an incorrect block, either due to a bug or intentional modification of transactions is removed from the set, potentially slashed and a new Coordinator is elected.

3.7 Slashing

Any Miner or Coordinator that produced an incorrect vote or block is punished by reward reduction or stake slashing.

3.8 Finality

Transaction finality is achieved by the inclusion of the block into the blockchain becoming irreversible as more new blocks continuously added using gossip P2P protocol. The finality time is expected to be achieved within 30 to 45 seconds from the time the block is produced due to the asynchronous nature of the Gossip Protocol.

3.9 Censorship

Censorship of transactions could occur if a Block Proposer (Coordinator) is active maliciously. Given that the set of Coordinators is random, requires staking, this should rarely occur. To make the network of Coordinators harder to compromise, a random RPC node (or a set of nodes) is chosen to broadcast headers of all transactions to the network. Should the headers be inconsistent, a censoring Coordinator is removed from the set immediately and potentially slashed.

3.10 Smart Contracts

Modified version of the Ethereum client (Geth) is to be used to handle all EVM calls on the network. Transactions and smart contract state is assembled and replicated across the network with methods described in previous sections