mosaic CHAIN

Introducing Mosaic Chain

Mosaic Chain Litepaper V1.0

Blocktopus Enterprise Ltd.

2nd Floor O'Neal Marketing
Associates Building, Wickham's Cay II
Road Town, Tortola
British Virgin Islands
VG1110

info@mosaicchain.io

www.mosaicchain.io

Telegram

Discord

Document Issued

01.10.2023

Document Version

V1.0

Table Of Contents

Abstract

The Mosaic Universe

Mosaic Universe welcomes you to build the future of the DeFi (Decentralized Finance) world together! Mosaic Universe is to provide safe and real DeFi solutions for everyone.

The Mosaic Chain is being born

The Mosaic Chain creates an ideal space for trustless financial solutions, as the technology and its implementation serve decentralized financial applications in every aspect. It also provides the highest level of interoperability with other blockchains within and outside the Polkadot ecosystem. The applications running on the Mosaic chain can be updated without compromising decentralization.

Our team had an unwavering commitment to excellence in finding the ideal blockchain for our DeFi application, that

- can serve complex financial applications
- from the Genesis block, it provides the opportunity to easily implement truly trustless applications.
- uses the safest technology available

These important aspects led us to the creation of our very own solution for ourselves, and for the blockchain community as well.

Mosaic Chain uses state-of-the-art technology and some brand-new solutions

The best available technology Substrate by Polkadot

NFT-based Validators

Plug & Play Validators

Really Decentralized 420+ validators from the genesis block

Validator Subset Selection

The Mosaic Chain is being born

Our small but strong Hungarian team is always looking for new ideas, developers, and projects to work with. We believe that collaboration and innovation are key to success, and we're confident that with your contributions, we can achieve great things together.

The Genesis Team

Our small but strong Hungarian team is always looking for new ideas, developers, and projects to work with. We believe that collaboration and innovation are key to success, and we're confident that with your contributions, we can achieve great things together.

The Early Bird is the Mosaic Alpha Platform

The Mosaic Alpha Platform provides managed Token Baskets for those who are interested in investing in crypto assets, but may not have the necessary knowledge or confidence to do it alone. We are excited to announce that the Mosaic Alpha Platform will be the first complex DeFi solution that chooses and moves to Mosaic Chain.

Working in Solidity?

We did the same for many years and then we changed for the safer, better, and more stable solution. We believe that it's important to stay up-to-date with the latest advancements in technology to ensure safety, stability, and efficiency. However, we don’t want to close out solidity developers.

We understand that there are already existing solutions out there, such as Moonbeam and Acala. We plan to provide some of these existing solutions for EVM projects in the near future, although we don't have an exact timeline yet. We may also consider creating our own solution that meets our high quality standards, or implementing a solution published by others. If you're interested in learning more or getting involved, please let us know!

The Mosaic Universe

Mosaic Universe Mission

Our mission is to offer a high-quality DeFi workplace and also to offer a DeFi station, in which other blockchain's and dapp's products can be integrated into one single interface.

Mosaic Universe Vision

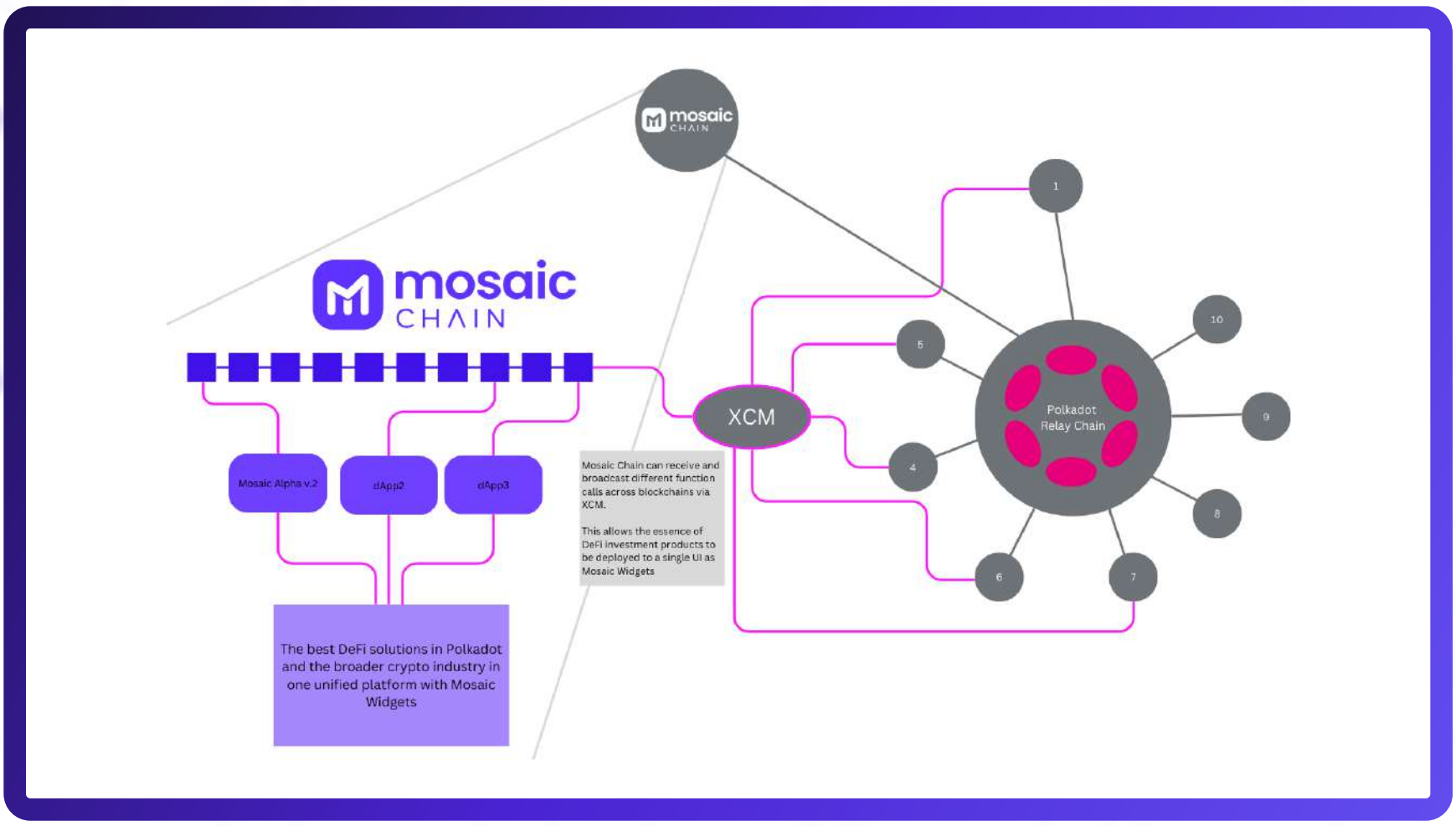
Everyday internet users are not yet Web3 users. We need to construct Web3 platforms in a way that anyone can quickly grasp and utilize decentralized services.

Nevertheless, there are currently numerous obstacles to this vision. It's not just about financial liquidity; services are also fragmented across multiple blockchains, forcing users to transact across multiple chains to access what they desire.

Our vision signifies a significant shift from a blockchain-centric to an application-centric perspective. Instead of managing multiple blockchains for various purposes, users can now use a single chain to access diverse DeFi and decentralized investment solutions. On Mosaic Chain's primary platform, users can select suitable investment products and strategies tailored to their needs. In this single UI, users can find the essence of the DeFi world presented in various widgets thoughtfully curated by diverse teams from various blockchains and dApps.

From a technological standpoint, developer teams from the Polkadot ecosystem and the broader crypto industry can seamlessly integrate their products into Mosaic Chain's execution environment (to the Runtime) using XCM and leverage Mosaic Chain's concentrated liquidity. With XCM, Mosaic Chain can receive and broadcast function calls to and from any connected blockchains, allowing all the excellent DeFi products to be displayed as widgets on a single user interface.

Mosaic Chain is poised to become a cornerstone of the crypto industry, where liquidity and various technological solutions converge. It aligns with the user experience and places innovation as a top priority because where innovation thrives, liquidity flows.



Mosaic Alpha Platform

For individuals who lack professional experience in finance and blockchain technology, investing in cryptocurrencies can seem like a daunting task. However, many people still desire to set aside money for their future and protect themselves against inflation.

The Mosaic Alpha Platform is the first DeFi product from the Mosaic Team, and it has been battle-tested and proven successful both technologically and from a business perspective. If you're interested in giving it a try, you can access it at www.mosaicalpha.com.

From the very beginning, we had set our standards high for the Mosaic Alpha platform. We knew that creating our own blockchain was the way to go, but waiting for it to be completed was not an option. We decided to launch it on the Binance Smart Chain network, a temporary solution that would allow us to provide a cost-effective environment with low gas fees and ample liquidity. We are working tirelessly on our own blockchain and look forward to implementing it in the future.
Our platform's use case centers around Token Baskets, which enable investors to diversify their portfolio by investing in various crypto assets from the Binance ecosystems. Token baskets contain several cryptos bundled together into a new crypto asset. With Mosaic Alpha, you can enjoy a genuinely decentralized environment that is safe and secure, giving you peace of mind as you explore the world of crypto investments.
In more technical details , in the token baskets, the users' stakes are represented as a collective proportion of other crypto assets, which are managed by Basket Managers and held by the investors in their crypto wallet. In the crypto wallet, the representation of the Token Basket is shown as a basket token. Moreover, these Token Baskets offer some advantageous features. They are considered decentralized actively managed investment products, as the token basket managers of each basket can manage the composition of the baskets on an ongoing basis.

For more detailed information, such as token baskets, investors, capitals, compositions, or basket managers, visit app.mosaicalpha.com.

The Mosaic Chain

From the beginning, the Mosaic Team tried to find a blockchain that is suitable for their high-quality standards to build upon. However, this research was inconclusive and the team did not find a suitable blockchain specifically for decentralized business services, but the technology research revealed that the most obvious solution would be to develop their own blockchain specifically for such needs using the novel Substrate blockchain builder framework on Polkadot foundations.

NFT-based Validators

The Mosaic Chain DPoS consensus mechanism is designed to be NFT-based, in which the validators who have these NFTs are able to participate in the networking. In the blockchain industry, there isn't any NFT-based consensus mechanism, except Mosaic Chain.

Plug & Play Validators

Everybody can be a validator without technical expertise thanks to a specialized Linux distribution which is booting the Mosaic Chain nodes automatically on the validator's own hardver. It is easy to keep this special-purpose system up-to-date while power users retain control over how they maintain them.

Validator Subset Selection

The Mosaic dev team wrapped the Aura consensus mechanism to increase the possible number of validators above five hundred. The Mosaic Chain is designed to run with possibly thousands of validators, but only a subset of 250 validators will be actively participating in the consensus at any time. A randomized selection algorithm dynamically sets the length of sessions based on the number of validators. The objective of the Mosaic DPoS validator subset selection is to statistically even out participation in the consensus and therefore block rewards week-by-week.

Introducing Mosaic Chain

For more up-to-date information, please visit www.mosaicchain.io.

Mosaic Chain is built on Substrate

Polkadot as a Layer 0 chain, guaranteeing Shared Security for all the connected Layer 1 blockchains, the Parachains

Today, the Polkadot Network is the only blockchain that can increase the security of other Layer 1 blockchains and provides instant and secure token transfers between them. Polkadot can provide these essential functions through its shared security model, where all data flows between individual blockchains are monitored and validated by Polkadot. This ensures continuous monitoring and protection of the connected blockchains. This is why Polkadot is actually called Layer 0, because it can coordinate and secure other Layer 1 blockchains, which we call Parachains (Parallelized blockchains).

After the Mosaic Chain will successfully be connected to the Polkadot Relay Chain, Mosaic's and Polkadot's consensus mechanisms will be melded, which technically means that Mosaic will be secured by Polkadot. Then Mosaic will be one of the Parachains of the Polkadot Network.

Polkadot can scale by design, via Parachains

Polkadot has the most advanced scaling solution in the blockchain industry. All the Parachains connected to Polkadot effectively become shards of it. So, in this case, Mosaic Chain does not have to worry about scalability issues because Mosaic Chain becomes one of the shards of Polkadot once it becomes a Parachain.

Since Polkadot has several Parachains connected to it, they are not left to validate alone. Polkadot helps them: every block of the Parachains (Parablocks) is finalized by Polkadot in the end. Therefore, every small state change on the sides of the Parachains is checked by Polkadot. This approach technically spreads the execution of transactions across multiple blockchains, making the entire Polkadot ecosystem unable to be overloaded, including Mosaic Chain. In conclusion, the scaling of a blockchain is based on Polkadot's unique architecture, which is why we are committed to Polkadot.

Mosaic Chain is built on Substrate

Trustless token transfers across blockchains, thanks to XCM

We all know how difficult and dangerous it is to bridge assets from chain A to chain B. These bridge technologies often rely on unreliable people who control the private keys of the crypto addresses behind the bridge and have inadequate technological backgrounds with low economic security. More than 2 billion USD worth of cryptocurrency was stolen by hackers in 2022, and these vulnerabilities in bridges have not been fully addressed to date.

Only Polkadot's other advanced technology, the so-called Cross-Consensus Messaging (XCM), can solve the interoperability issues in a completely trustless and secure way in the blockchain industry. The most compelling reason we chose Polkadot as our core infrastructure is XCM. With XCM, our blockchain can send and receive crypto assets from other blockchains securely and quickly. That's not all: XCM provides us with a high level of flexibility and efficient programmability, allowing us to fully configure the applications running on the Mosaic Chain without having to conform to other blockchain standards.

Agile and easy blockchain upgrades without hard forks

Considering blockchains as unique distributed software, we might rightly think that these blockchains should be updated at certain intervals, just like traditional software, to keep them up-to-date. These occasions to update blockchains are called hard forks and have disadvantages in many ways.

When a blockchain network is upgraded via a hard fork, what effectively happens is that all validator operators maintaining the blockchain have to download new software to the validator's hardware. After the successful upgrade, the blockchain will operate with the new software's logic, not based on the old software's logic. Now, the operation can only be done with great difficulty and effort. Hence, updates via hard forks are not very agile, require a lot of off-chain coordination, and are also slow and dangerous, as transactions can be compromised during a hard fork. Not to mention that hard forks can split the community, not just the blockchain.

Polkadot's approach is quite the opposite: it is seamless, fast, and does not require off-chain coordination between the operators of the validators. Polkadot and all the other Substrate-based chains are using a novel, industry-leading blockchain upgrading technology: Forkless Runtime Upgrades. Instead of placing the software that contains the blockchain's operational logic in the validators, they integrated it into the blockchain itself. So validators approve blocks according to the logic (runtime) of the blockchain, not according to the logic of the software downloaded to their hardware. This solution allows Mosaic Chain to keep up to date with runtime upgrades similar to Polkadot.

The Genesis Team

Our small but strong Hungarian team is always looking for new ideas, developers, and projects to work with. We believe that collaboration and innovation are key to success, and we're confident that with your contributions, we can achieve great things together.

Attila Vidákovics
CEO

economist, crypto whiz kid, university lecturer (DeFi), radio presenter

Péter Molnár
CTO

economist, software engineer, smart contract wizard, blockchain architect, blockchain strategist

Wigy
LeadDev

software engineer, runtime and pallet writer, Rust developer

Tom the Great
Project Lead

engineer, economist, controller, project management expert, former IT COO

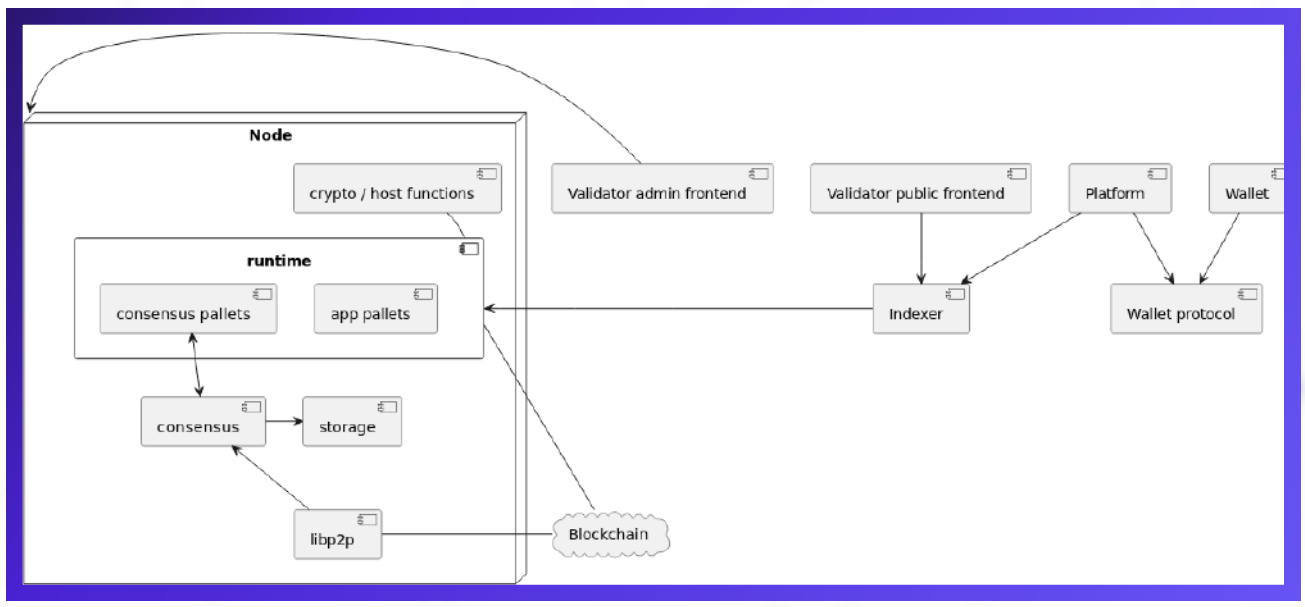
Six
Lead Advisor

Polkadot head ambassador, security analyst, auditor

For more details, visit mosaicchain.io

Technical Details

Architectural design of the Mosaic Chain



Our high-level architecture is similar to other substrate-based projects

1. **Node:** The Node is the backbone of our network, responsible for peer discovery, managing transaction requests, reaching consensus with peers, and responding to RPC calls.
2. **Runtime:** The Runtime defines the network's business logic for executing the state transition function of the blockchain. The architecture allows for on-chain runtime upgrades to remain agile and adapt to evolving requirements.
3. **Indexer:** Our Indexer provides efficient data querying, enabling developers and users to access blockchain data swiftly and reliably.
4. **Public Frontend:** Our Public Frontend, backed by the Indexer, offers anyone an intuitive interface to explore blockchain data and access essential information.
5. **Validator Frontend:** A user-friendly control panel for node operators, simplifying node management and facilitating real-time monitoring of node health, performance, and relevant on-chain data such as staking status and block rewards.
6. **Wallet and wallet protocol:** User-friendly asset management interface for storing, sending, and receiving digital assets.
7. **Platform:** The platform provides a familiar web interface to interact with the blockchain's services. It can be thought of as a dApp. The first platform supported by the chain will be Mosaic Alpha V2.

Our design focuses on user-friendliness, with special consideration for first-time validators. We aim to simplify the validator setup process, making it approachable for newcomers to participate confidently in the network.

Technical highlights and challanges

NFT-based validators

Mosaic Chain has three separate NFTs:

- **PoS NFTs** can be owned by validators. With these NFTs, the validator can participate in the consensus with its own self-stake.
- **DPoS NFTs** can be owned by validators. With these NFTs the validator can participate in the consensus with its own self-stake and with other delegators delegated stakes, plus with a Delegation NFT.
- **Delegation NFTs** represent more stakes in MOS coins. This is an NFT which has a nominal value in MOS coins and can be delegated to DPoS validators by delegators.

A well-functioning consensus mechanism is indispensable for any blockchain. Our primary objective was to make this consensus algorithm as robust and decentralized as possible. This is precisely why we incorporated delegation NFTs into the system. These NFTs signify increased stakes, and when delegators entrust these NFTs to validators, it enhances the economic security of the blockchain. Furthermore, these NFTs will be subject to slashing in the event of misbehavior by the delegated validator.

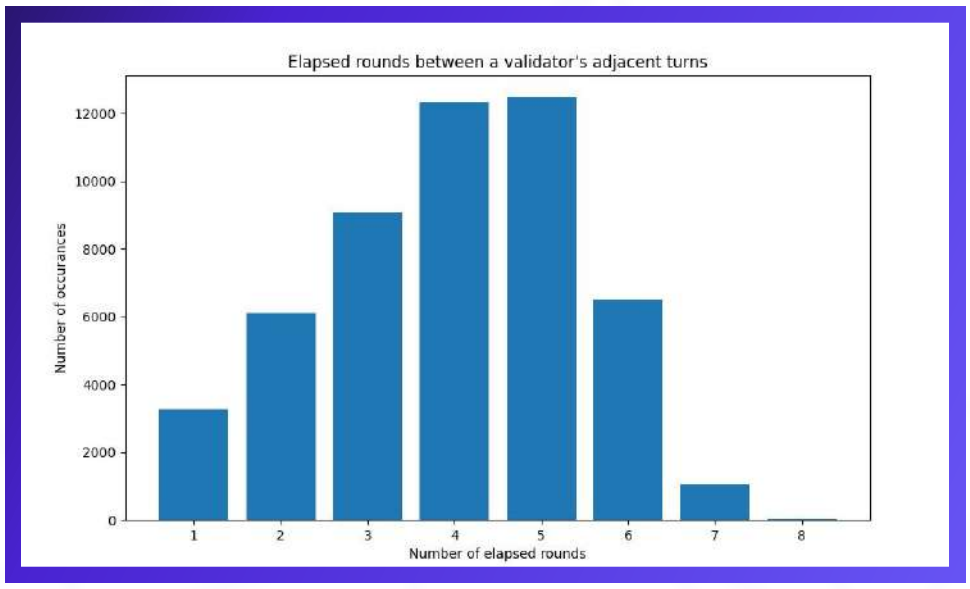
Validator subset selection

The Mosaic Chain will start with more than 420 validators and the Aura consensus algorithm has quadratic time complexity. That's why in every session only a subset of the validators participate in the consensus mechanism. We would like to choose approximately 250 validators for every round to propose new blocks. The purpose is to maximize uniformity of weekly selection counts in the population, while maximizing unpredictability(variance) in selection.
After examining the possibilities and running several simulations on different algorithms, we decided to use the following solution.

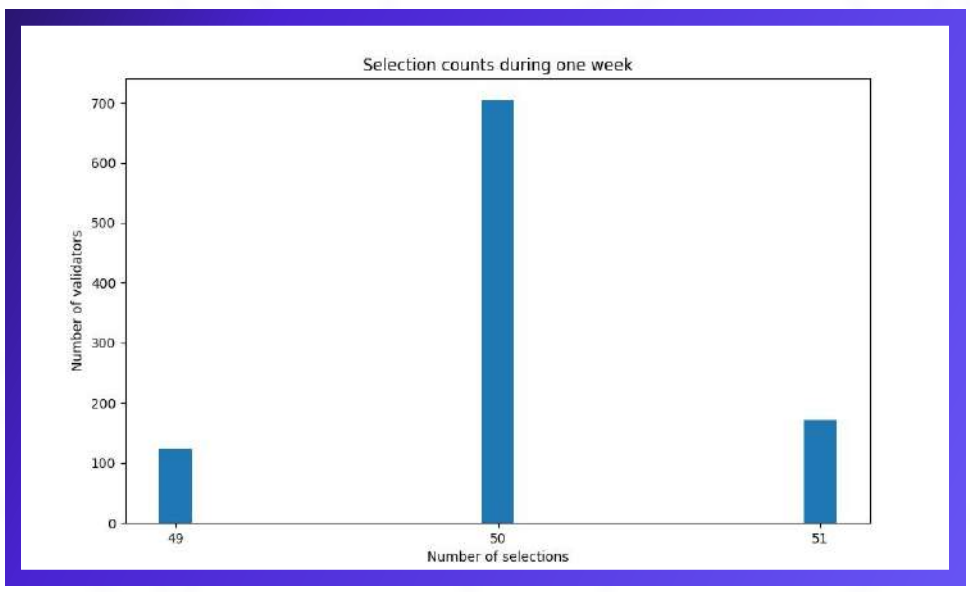
Improved bucket selection algorithm:

1. Every validator has two buckets initialized with independent uniform random numbers between 0 and 1.
2. In a round every bucket's value is increased by subset_size/(2 * number_of_validators).
3. The validators with at least one full bucket (value greater or equal to 1) are the chosen subset for this round. One of their full buckets is decreased by the 0.5. The other 0.5 decrease is uniformly distributed between the validator's two buckets. After that we go to the 2. step.

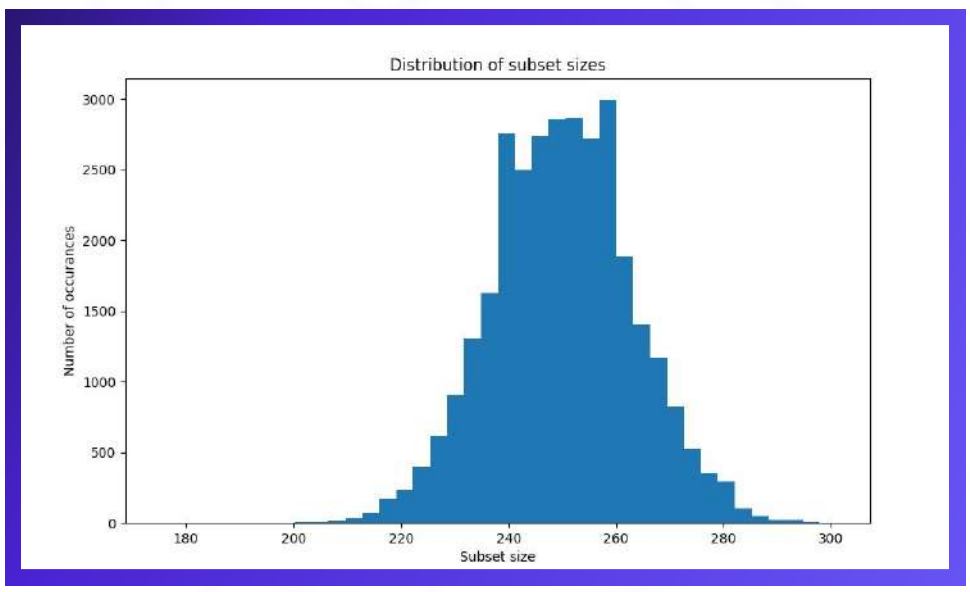
With this algorithm and parameter setting the distribution of the selection counts is nearly uniform and the unpredictability (variance) is high.
To support these claims, we present some diagrams, which are the results of a simulation run with 1000 validators, and 250 target subset size for a one-week timeframe with 12 seconds block time. This means that the simulation lasts 201 sessions. (The last diagram is from a 31449 rounds long simulation to get a closer picture about the distribution.)
In the first bar chart, we can see the distribution of the elapsed rounds between validators' adjacent turns. We can observe that it is possible to select a validator in two adjacent sessions, the maximum waiting time is 8 sessions and the average is 4. Without more information, it's hard to predict the next turn of a validator.



In the next bar chart, we can examine that in a one-week timeframe, every validator was selected 49, 50, or 51 times in the simulation and the distribution is nearly uniform. If we look at longer time frames these little differences totally balance out.



It's a consequence of the bucket selection algorithm that the subset sizes are not always 250. The last histogram shows the distribution of the subset sizes. It's a binomial distribution with 250 mean and 13.8 empirical standard deviation and can be effectively approximated with a Gaussian distribution.



Plug & Play Validators

We make sure not only our users, but also our validators get a comfortable and safe user experience. Our specialized Debian-based Linux disk image will be configured with the crucial security required by a p2p network node by default.

Upgrades to the system and the blockchain node binaries will come from our repositories by default, but we leave the distribution open for tinkering by power users knowing their sysadmin fu. Also, all our validator software will be open-sourced so anyone with an understanding of how to maintain other Substrate-based blockchain nodes get a familiar experience.

Unfortunately, as the block production/import process is almost entirely single-threaded, you will need top-of-line hardware to get reliable block rewards.

- Recommended CPUs - Intel Xeon E-2386/2388 or Ryzen 9 5950x/5900x
- Recommended storage - 1 TB NVMe
- Recommended RAM - 32 GB RAM

We are planning to incentivize optional services that will require high-end GPUs in the future, but not for now. Some data centers like Hetzner provide dedicated machines like these, but be aware that Hetzner has shut down some blockchain nodes in the past without a warning. Even if you run your system outside a data center, redundancy of power and network connection and a public IP address will be needed for the nodes.

Main metrics available

Our tokenomics is under a thorough review so we can satisfy the expectations of our existing investor base and also let the Polkadot ecosystem enter our DAO.
Initial token supply, maximum supply, and yearly expansion will be published in a future version of the litepaper.
Block-time is 12s, because we are going to be a synchronously backed parachain and we will start the chain with 420+ initial nodes.

Runtime components

Pallets are modules or components that carry specific functionalities and business logic that the blockchain's runtime can execute.
We can group the required pallets into two main groups:

1. Consensus-related pallets: These pallets are essential for the consensus mechanism, ensuring the network's security and integrity.
2. Application-related pallets: These pallets contain the logic necessary for decentralized applications (dApps) such as "Mosaic Alpha”.

Main consensus related pallets

NFT-permission:

- The pallet is built on top of the 'pallet-nfts' pallet to manage the creation, ownership, and attributes of the permission NFTs.
- The pallet allows users to mint new permission NFTs, bind/unbind NFTs to/from their accounts, and chill/unchill NFTs to prevent/re-enable their use.

Validator-subset-selection:

- The pallet makes it possible to select a subset of the validators to create blocks in the next session.
- Manages sessions so that a session's length is equal to the number of selected validators.

Staking:

- The pallet provides functionality to stake/unstake currency/NFTs and to kick NFTs.

NFT-Delegation:

- The pallet manages NFTs representing delegation rights in a staking system.
- Allows for minting, binding, unbinding, and slashing these NFTs.
- It handles expiration checks for bound tokens and provides a trait for custom logic when an NFT expires.

Application-related pallets

After the development of the consensus-related pallets we will implement the features of the early bird Mosaic Alpha platform into application-related pallets.

The MOS Coin

MOS coin is the native cryptocurrency of Mosaic Chain.
It serves as a native token usually serves

- fueling the entire operation of the blockchain PoS, DPoS mechanism
- used by holders in the governance system
- paying and receiving block rewards, slashing, and other transactions nominated in MOS

1 MOS = 10^18 TILE

Roadmap

1.

Implement a robust DPOS with NFTs on Aura

1. Validator subset selection
2. Slashing optimization with NFTs
3. Validator candidates

2.

Adding Mosaic Chain Pallets

1. Optimize core Runtime Pallets
2. Build Mosaic Alpha V2 Pallets

3.

Testing Mosaic Chain Testnet with Rococo

1. Testing Runtime functions and Cumulus
2. Testing Runtime upgrades
3. Testing XCM calls
4. Optimizations and improvements

4.

Mosaic Chain mainnet launch

1. Add Mosaic Alpha V2 pallets into the runtime logic
2. Future optimizations

5.

Parathread registration on Polkadot Relay Chain and Participate on Polkadot Slot Auction

6.

Win on Polkadot Slot Auction

1. Opening a VRMP channel with Polkadot
2. Opening HRMP channels with other Parachains
3. Parachain token integrations on Mosaic Alpha V2.

7.

18%

Developing Phase of the unified Mosaic DeFi platform with external ecosystem integrations