KalyChain White Paper

V1. 0

October 2022

Table of contents

Abstract

In a century in which economic, scientific-technical, cultural and political circumstances advance more than ever, it is necessary to apply the use of technologies that facilitate their development, which is why Kalycoin proposes a blockchain technology infrastructure enabled for the development of Smart contracts and Dapps with a PoS consensus system that makes it highly competitive and secure without high energy cost. Blockchain-enabled smart contracts that employ proof-of-stake validation for transactions promise significant performance advantages over proof-of-work solutions. For wide adoption in the industry, other important requirements must also be met. This whitepaper fills the gap in the state of the art by introducing the

Kalycoin smart contract framework that targets sociotechnical application suitability and language expressiveness adoption of formal semantics intelligent for rapid implementation of industry best practices. We discuss the advantages of the Kalycoin utility compared to the Ethereum alternative and present future Kalycoin smart contract development plans for industry case applications.

Keywords: Smart contract, business network model, DAPP, information logistics, cross-organizational, peer-to-peer, distributed system, e-governance, Kalycoin blockchainThe amount of technology in buildings and homes is rapidly buildings.

1. Introduction

Industrial revolutions have been characterized by bringing with them disruptive products and technologies that have marked and changed the daily lives of people, becoming increasingly comfortable for their beneficiaries, just think that 2 centuries ago we still mobilized in horse-drawn carriages, it has been just over 100 years since the beginning of mass production of cars and just under 40 years ago we managed to reach the moon.

As a population we are not aware that the speed of technological growth that humanity has developed in the last 200 years has grown exponentially if we analyze it at a historical level, however, this decade is no exception since we are going through a transition from industries 3.0 (third industrial revolution) to industries 4.0 (fourth industrial revolution) which offers great technological changes that can be considered as disruptive technologies since many bring with them the programming and automation of tasks that are performed by humans routinely or daily improving the productivity of processes making them more accurate and efficient.

Blockchain technology is considered one of the technologies that brings with it the 4.0 era along with IoT, AI, and Big Data technologies since it offers transactional methods and communication between peers P2P, going through a decentralized system and with high standards in security levels (superior to centralized systems).

The latter initially find application in various environments such as, for example, financial technology, Internet of Things (IoT) applications, digital signage solutions. An essential aspect of smart contracts is a decentralized validation of transactions, initially using the so-called proof of work (PoW). The core technology that enables smart contracts is a distributed public ledger called the blockchain, which records transaction events without requiring a trusted central authority. Blockchain technology spreads in popularity with the inception of Bitcoin [23], a peer-to-peer (P2P) payment and cryptocurrency system comprising a limited set of operations at the protocol layer. Bitcoins use PoW for transaction validation, which is computationally expensive and consumes a lot of electricity.

First, validating proof-of-work transactions decreases scalability to the point where Ethereum is considered not feasible for most industry applications. Secondly, in a recent crowdfunding study, the Ethereum-affiliated Solidity smart contract was hacked due to security flaws resulting from a lack of state of the art regarding the tools for formal verifications.

The security flaw resulted in a loss of approximately $50 million. Consequently, Ethereum performed a hardfork that resulted in a schism that produced two separate versions of Ethereum.

However, another Ethereum hardfork was caused by a denial-of-service attack, and more hardforks should be expected to perform proof-of-stake transaction validation and blockchain fragmentation. More reasons limit the widespread adoption of the Ethereum industry.

For example, the inability to automate information logistics between organizations, the lack of privacy protection differentiations between related external vs. internal private contracts, secure and stable virtual machines for blockchains with better-performing proof-of-stake transaction validation, formally verifiable smart contract languages, lite wallets that do not require downloading the entire blockchain, and solutions of mobile devices for smart contracts with simple payment verification (SPV). The latter means that clients simply download block headers when connecting to an arbitrary full node [23]. While Kalycoin uses the Ethereum Virtual Machine (EVM) for a current lack of more suitable alternatives, the EVM has

shortcomings such as previously experienced attacks against poorly handled exceptions and against dependencies such as for transactions.

2. Introducing KalyChain

Let's go back to the beginning of the year of 2022 when the blockchain that would drive the technological development of the ecosystem of the KalySsi financial group and the KalyPay payment gateway was brewing in KalySsi's laboratories. Resulting in a powerful blockchain[1] with PoS consensus system and EVM integration which allows it to support the development of smart contracts and DApps with low fees, you can even download a wallet from the first KalyCoin[2] chain (not to be confused with KalyChain, which is the upgrade we will see later) that was initially developed.

However, this blockchain despite all its advantages and qualities has a competitive disadvantage compared to the other chains compatible with EVM, and is that its integration with metamask has been impossible[3] so it was decided jointly between the KalyChain development team and the community, to make an update that would allow this integration, for this we changed the concept approach and we have developed a PoSA consensus system blockchain based on the Polygon[4] network which facilitates the optimal development of the applications of the KalyChain ecosystem in terms of compatibility with metamask and other networks through bridges between chains.

This improvement in the chain is quite relevant and significant, given the advantages it offers us when developing useful applications for the benefit of the community and landed in reality, it brings with it a series of important changes apart from the aforementioned integration with metamask, such as:

[1] https://github.com/KalyCoinProject/KalyCoin
[2] https://github.com/KalyCoinProject/KalyCoin/releases
[3] https://olddocuments.kalycoin.io
[4] https://polygon.technology/

1. The maximum supply has gone from 125M to 7B
2. The reward has changed from 6.39189 KLC/Block to rewards for fees
3. Block time has gone from 120s/ Average to 3s/ Average
4. The consensus system has changed from a traditional PoS to a more advanced PoSA
5. It is now possible to create bridges between other chains
6. It is possible to export common tokens such as USDT and other stablecoins to the KalyChain network

As we can see, this change brings with it great advantages of competitiveness in the market and aligns with our Kai-Zen philosophy (continuous improvement), so we will continue in the search and development of the best solutions for our users and community.

As a proof-of-stake blockchain, KalyChain seeks to bring scalability, security, robustness, and utility tothe KalyPay ecosystem.

It is important to note that the KalyChain project is a blockchain that prioritizes the community and its investors, prioritizing continuous improvement and application development within the Kalychain ecosystem. Ultimately, KalyChain will provide KalyCoin users with access to an ever-growing DeFi ecosystem promoted by the KALYSSY group, which will feature blockchain-oriented software development courses on EVM-compatible chains such as KalyChain.

KalyChain is focused on the development of financial applications and solutions applying blockchain technology to both private companies and the general public.

2.1 Chain-cloud integration

The development of the blockchain to this day still does not depart from the logic of Bitcoin's block-by-time plus global synchronization verification. This is not a big problem for the use of low-interaction actions such as value transfers, but it may not be the best for application platforms. It can be seen that some simple small games can block Ethereum, EOS and other platforms, so in large-scale commercial applications, the existing public blockchain platform is inadequate. The Kalycoin team believes that the most important feature that blockchain brings to applications is not "decentralization", but rather the following three "blockchain features": ·" Four in one" authority management mechanism for accounts, addresses, funds, and identities · Comes with a natural clearing and settlement network · High-speed growth brought by incentives and liquidity. These are the features that are lacking in all existing Internet applications. Most of the existing Internet applications are deployed on the cloud, and in the foreseeable future, applications deployed on the cloud will remain mainstream. The Kalycoin team believes that the fusion of the above-mentioned blockchain characteristics with applications deployed on the cloud will generate new application forms and promote the true adoption of blockchain.

2.2 Features of KalyChain

KalyChain relies on the Polygon Edge framework to build its standalone and EVM-compatible blockchain. EVM stands for Ethereum Virtual Machine, which means that this platform with smart contract capability will be compatible with dApps implemented on Ethereum.

EVM is at the core of the Ethereum blockchain and plays a pivotal role in creating decentralized applications. In particular, it allows developers to build and implement solutions and protocols much more quickly (rather than building them from scratch). In fact, EVM-compatible protocols incorporate a robust and proven architecture and are therefore a game-changer for DeFi

product developers. And in addition to the existing protocols, KalyChain will propose its own smart contracts, thus taking advantage of the extensive DeFi ecosystem.

Bitcoin and other blockchains focused on payment/storage of value have not been able to invoke the same demandas platforms with smart contract capability. In contrast, KalyChain's ability to improve the productivity of the Web3 ecosystem promises to increase the demand for block space. This event will also play a role in the growing demand for KalyChain's native cryptocurrency, the $KLC token.

Given KalyChain's ability for high performance and decentralization, token users won't need to suffer the same user concerns associated with many PoW tokens (including low transactions per second, public chain congestion, centralized mining, and high transaction fees). In addition, KalyChain will retain a high degree of decentralization due to its PoS architecture.

KalyChain relies on a predefined number of validators to facilitate its Proof of Stake (PoS) consensus mechanism, a configuration that leads to shorter block times and lower fees. In PoS, validator candidates with the highest number of tokens wagered can become validators and produce blocks. The token also employs trim scenarios, leading to the security, decentralization, reliability, transparency, stability, and purpose of the block.

2.3 Main Features of Kalychain

Kalychain relies on the following key principles:

- **IBFT Proof-of-Stake (PoS) consensus:** Community users can participate in the network which ensures a permissionless and decentralized blockchain.
- **EVM-compatible**: Existing Ethereum smart contracts can easily be migrated to Kalychain without requiring any further modification.
- **Decentralized Governance:** Community members (token holders) can make proposals, delegate, vote on the blockchain parameters & events, and influence governance decisions.

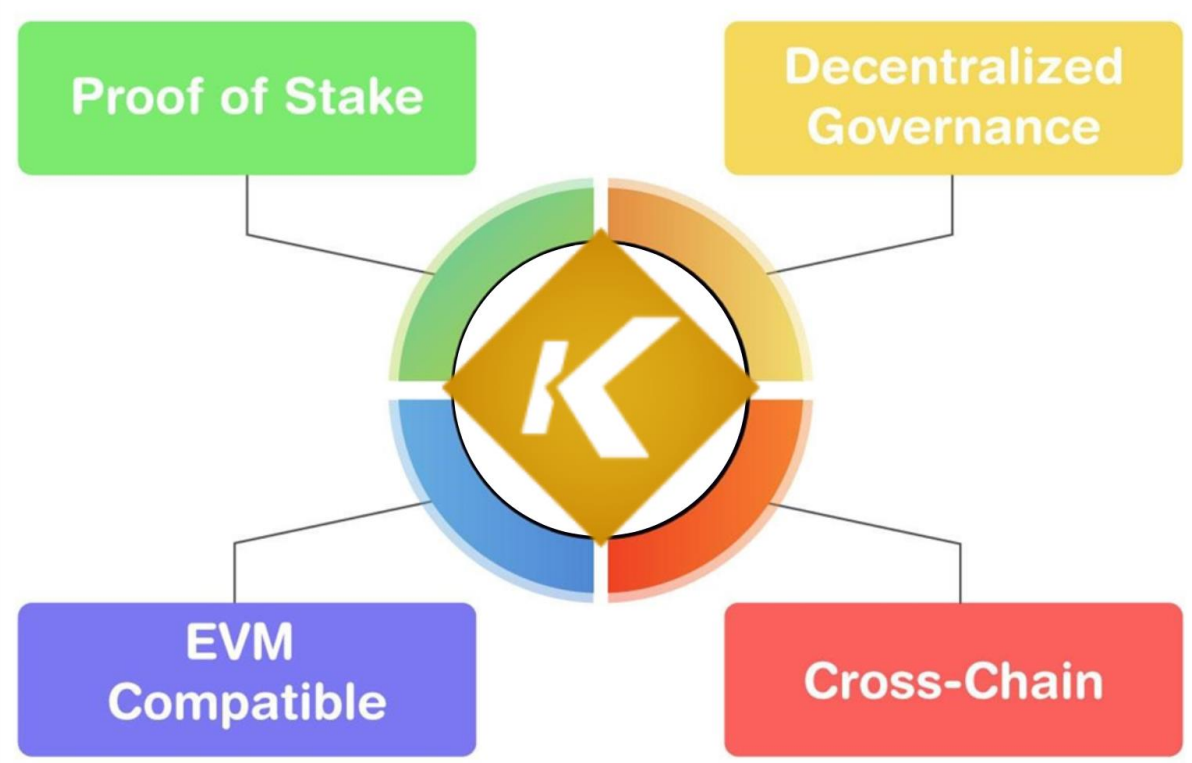


Fig1. High-Level Features of Kalychain

3. Background

3.1 Cryptographic Hash Functions

An essential tool in blockchain technology is the cryptographic function that ensures transaction integrity and immutability. The hash function is the mathematical algorithm that produces a fixed size numerical output (called fingerprint or digest) consisting of input data. More specifically, a hash function can be denoted as:

$$H:\{0,1\}^* \rightarrow \{0,1\}k$$

A hash function takes on the input of any size and produces a fixed k length output. In addition, it must satisfy the following properties:

- It is easy to compute H regardless of input data size.
- Given any h, it is computationally infeasible to find an input x such that H(x) = h.

- Given any x, it is also computationally infeasible to find y such that H(y) = H(x) and x≠ y.
  ●It is computationally infeasible to find any (x, y) such that H(x) = H(y) and x≠ y.

SHA-256 and Keccak-256 are widely used in several blockchains, and they produce a hash (output) of 256 bits in size.

3.2 Digital Signatures

3.3.1 Secp256k1 Curve

Note that all elliptic curves are equations defined as $y^2 = x^3 + ax + b$. The code Secp256k1 is an elliptic curve used by several blockchains to implement public and private key pairs. For instance, we can define Secp256k1 as a = 0 and b = 7 (i.e., secp256k1 lives on the equation $y^2 = x^3 + 7$).

Before a user generates a public and private key pair (pk, sk), he/she must first generate a sufficiently large random number (which is going to be sk) and use it to multiply with the private key by the generator point G as sk. G (which is going to be the pk).

We use this number to define a point on the secp256k1 curve. Due to the underlying discrete log problem (DLP), no one can derive the private key from the given public key and the generator point (as long as the key size is sufficiently large).

Note that for each value of x, the y component is squared in this equation leading to having two symmetric points across the x-axis. Hence, there are two values of y called odd and even numbers. Therefore, public keys can be identified by the x-coordinate and the parity of the y-coordinate. In the blockchain space, this feature is crucial, as it saves significant data storage.

3.3.2 ECDSA Signature Algorithm

Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic algorithm for creating digital signatures. More concretely,

Setup

● Public Parameters: Let Fq be a finite field, two parameters a and b define an elliptic curve C over Fq , a seed which validates C, a prime integer , $n > 2^{255}$ and a point $G \in C$ of order n where q is either prime or a power of 2.
● Private Key: An integer d in [1, n − 1].
● Public Key: Q = dG.

Signature generation for a given message

● Generate $k \in [1, n - 1]$
● Compute

$$(x_1, y_1) = kG$$

$$r = x_1 \bmod n$$

$$s = \frac{H(M) + dr}{k} \bmod n$$

- If r = 0 or s = 0, try again. The signature is (r, s).
- Signature: (M, r, s).

Verification:

- Given (M, r ', s')● Verify if

r' and s' are in [1, n − 1] and that r' = x_1 mod n for $(x_1, y_1) = u_1 G + u_2 Q, u_1 = \frac{H(M)}{s'} \bmod n$, and u_2 = $\frac{r'}{s'} \bmod n$.s').

3.3 Ethereum Virtual Machine (EVM)

A virtual machine is a layer of abstraction between the executable code and the executing machine. This layer is necessary to improve the portability of software and to ensure that applications are separated from each other and from their hosts.

The Ethereum Virtual Machine (EVM) is a software platform that developers can use to build decentralized applications (dApps) on Ethereum. All Ethereum accounts and smart contracts live in this virtual machine.

The Ethereum virtual machine and EVM codes are designed using memory, bytes, along with blockchain concepts such as Proof-of-Work (PoW) or Proof-of-Stake (PoS), Merkle tree, and hash functions. The purpose of the EVM is to determine what the total Ethereum state will be for each block in the blockchain.

3.4 Consensus Protocols

3.4.1 Proof-of-Work (PoW) - Nakamoto Consensus

Proof-of-Work (PoW) is a decentralized consensus protocol that can be handled securely in a peer-to-peer network without requiring any trusted third party. It solves the difficulty of Byzantine general problem in an open network where miners can generate arbitrary identities (also called a Sybil attack) to compete for the next generated blocks by solving a random hash puzzle.

In order to avoid a Sybil attack, PoW is used to force the miners to have and run predefined computational resources. Additionally, PoW protects the security of the blockchain from the longest chain attacks. Unfortunately, PoW requires a large amount of energy which keeps increasing as more miners join the network.

3.4.2 Istanbul Byzantine Fault Tolerant (IBFT)

IBFT is another Byzantine fault-tolerant protocol based on Practical Byzantine Fault Tolerance (PBFT). On a high level, Byzantine consensus is achieved deterministically as follows:

4. A leader or bidder/proposer is selected.
5. Each proposed block goes through several stages of communication between the nodes before being added and confirmed on the blockchain.

There are four types of messages which are exchanged between the nodes:

- **Pre-Prepare, Ready, Commit:** Used through ordinary consensus algorithms operations.

- **Round robin:** Used to select a new block producer when the current producer is suspected of failing or when the block has not been created within a specific time frame.

Additionally, there are two approaches in the Polygon Edge framework for choosing block producers:

- **Round-robin:** This is a block producer selection strategy where a different bidder is chosen for every block producing phase.
- **Attached bidder**: A new bidder is only selected whenever a malicious behavior has been detected by the current bidder.

In these two approaches, every validator knows in advance which one of them is going to be the next block producer. This is because the decision is made through deterministic calculations based on node IDs. Similar to PBFT, IBFT also guarantees that there will be only one single bidder in each round.

Moreover, the bidder is required to get responses from the other nodes in order to continue executing its further tasks. This means that in the case of a network partition with more than n nodes (at least more than 3n+1 nodes), the protocol does not make any decisions not to break the consensus until the partition is fixed and their communication is timely synced. This also allows immediate finality where no forks are ever allowed to occur.

3.4.3 IBFT Proof of Authority (PoA)

In PoA, validators are responsible for creating blocks and adding them sequentially to the blockchain. All validators create a dynamic set of validators where validators can be added or removed from the cluster using a decentralized voting mechanism.

This means that validators can be included or excluded from a validator group if the majority (51%) of validator nodes voted to add/remove a particular validator from the set. Thus, malicious validators can be detected and removed from the network at any point in time, and new trusted validators can be added to the network.

All validators propose the next block in turn (by means of the round-robin leader selection). For a block to be validated/added to the blockchain, the overwhelming majority of the validators (i.e., more than 2/3) must approve that block. In addition to the validators, there are also non-validators who do not participate in block generation directly but take part in the block validation process. IBFT PoA is the default consensus mechanism of the Polygon Edge framework

3.4.4 IBFT Proof-of-Stake (PoS)

The Polygon Edge Proof-of-Stake (PoS) implementation is intended to be an alternative to the existing IBFT PoA implementation by giving node operators the ability to easily select between the two when starting the chain. Epochs are considered to be specific timeframes (in blocks) during which a given set of validators can generate blocks.
The epoch length can be changed, meaning that the node operators can set the length of the epoch during instance creation. At the end of each epoch, an epoch block is created, and after this event, a new epoch begins. Validator sets are updated at the end of every epoch period. Nodes request a set of validators from the staking smart contract during the creation of an epoch block and store the resulting data in local storage.

This query and saving the cycle are recurring at the end of every epoch period. Fundamentally, this allows the staking smart contract to have full control over the addresses in the validator group, leaving only one task to the nodes. Each contract query is executed only once per period to obtain the latest information about the validator set. This removes the responsibility of dealing with validator sets from individual nodes.

3.4.5 RAFT

Raft is a distributed consensus mechanism that relies on Paxos. The Raft protocol works with a node failure model where each error (e.g., missing messages, network partitions, or hardware-only failure) is considered a node failure.

Hence, it should run $n \geq 2f+1$ where f is the maximum number of nodes that can fail and n is the total number of nodes. The Raft protocol first selects a leader among a set of nodes and then makes the leader fully responsible for receiving transaction requests and handling the copying of logs (i.e., blocks) on other nodes.

Each node can be either a candidate, a follower, or a leader. The leader selection procedure is deterministic, so the protocol cannot run until the leader is selected by more than half of the nodes.

3.5. Comparison and Selection

IBFT protects the blockchain against various malicious attacks, while Raft only protects against node failures. If we assume that all nodes will never be corrupted, then Raft can be used without having any concern.

However, if there is an assumption of only having partial trust in the validators, then it would be better to utilize IBFT. **Since Kalychain is decentralized and permissionless, it is going to run IBFT as its underlying consensus protocol.**

4. Kalychain (KLC) Architecture

Kalychain uses the Polygon Edge framework to build a standalone blockchain. Consequently, it doesn't use Polygon's "security as a service" features but rather relies on its own set of validators. It's worth noting that Kalychain disables two Polygon Edge features - its checkpointing mechanism and its mainchain contracts.
With this framework, our community of developers can build a blockchain network that better suits their needs and demands. They can achieve this because Polygon Edge employs a modular and extensible framework for creating EVM-compatible blockchain networks, sidechains, and global scaling solutions. After all, Polygon Edge is primarily used to launch new blockchain networks that are fully compatible with Ethereum smart contracts and transactions.

Finally, Polygon Edge uses the IBFT consensus mechanism since it provides for PoA and PoS. Likewise, the Kalychain EVM blockchain invokes IBFT PoS with built-in system contracts. With the help of Polygon Edge, Kalychain can employ the following features:

- Reuse existing Ethereum smart contract technology and its API.
    - Users can interact with standard wallets via JSON-RPC.

○Developers enjoy Solidity/Vyper programming and full EVM support.
○Access to popular Ethereum tools, development tools, and libraries.
○Optimized UX when performing cross-network transactions.

- Communication between networks.
    - Completely trustless and decentralized embedded Ethereum Bridge solution.
    - ○Asset transfers from any EVM compatible network, particularly Polygon and Ethereum mainnets.

○Transferring of ERC20 tokens, NFTs, or local tokens in the shell.
○The ability to customize bridge functionality with existing plugins.

- Special Functions.
    - Building network usability via the development of plugins

○The capacity to replace core functionalities with consensus plugins.
○Going beyond Ethereum smart contracts by incorporating Runtime

Thanks to the underlying Polygon Edge architecture, Kalychain can achieve full compatibility with Ethereum smart contract technology. It can also use IBFT PoS to ensure high network decentralization, security, and scalability.

4.1 Kalychain Layering Architecture

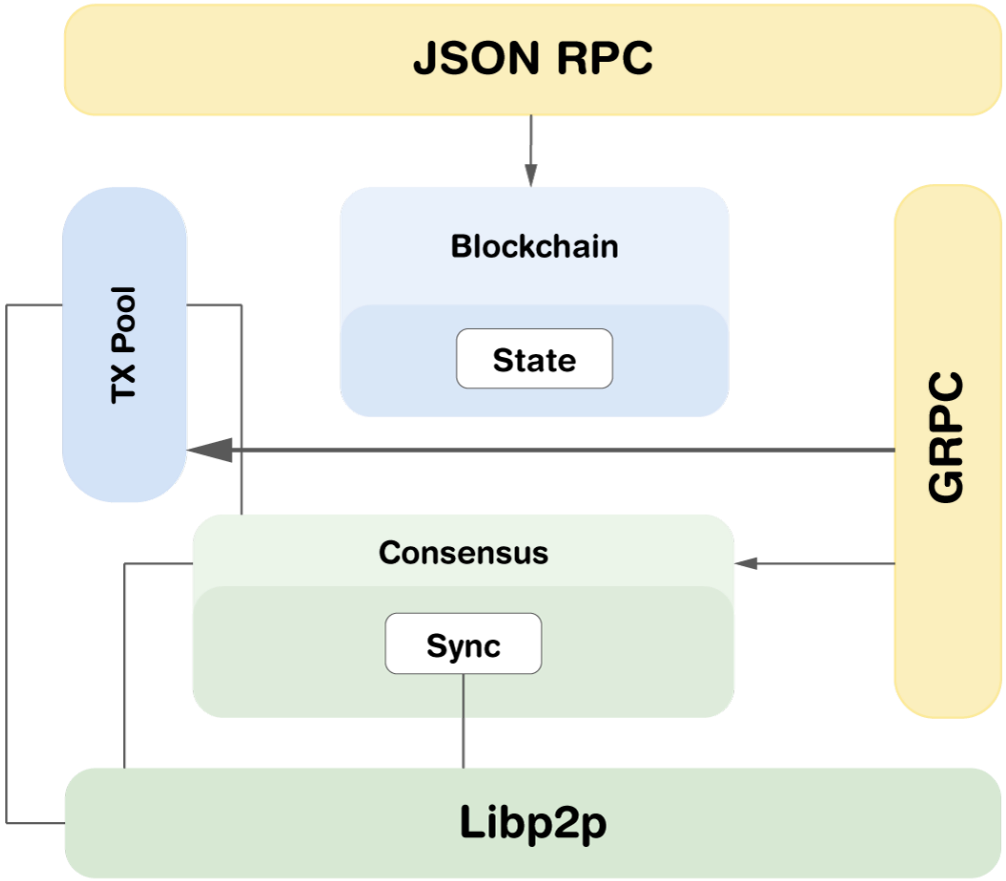


Fig 2. Kalychain Layered Architecture

- **Libp2p:** This module always begins at the underlying network layer. Libp2p is modular, extensible, and fast. In particular, it provides an excellent foundation for more advanced features.

- **Synchronization & Consensus**: The separation of synchronization and consensus protocols enable modularity and the implementation of customizable synchronization and consensus mechanisms (depending on how the client operates). Polygon Edge also offers pluggable consensus algorithms out-of-the-box.
- **Blockchain:** The Blockchain layer serves as the core layer for managing tasks within the Polygon Edge system.
- **State:** The State layer provides the logic for transitioning between states. It deals with how the state changes when a new block is added.
- **JSON RPC**: dApp developers use this layer as an API layer in order to interact with the blockchain.
- **TxPool:** The TxPool layer is a transaction pool and is tightly coupled to other modules in the system (as transactions can be added from multiple entry points).
- **GRPC:** The GRPC layer is crucial for enabling interaction with the operator. This layer ensures that node operators can interact with the clients easily, providing a usable and efficient UX.

4.4 KalyChain Native Currency: The $KLC Token

KalyChain introduces a native cryptocurrency: **the KalyChain** token **($KLC).** This community-centric token serves as a primary governance token for the KalyChain blockchain and comes with several use cases. It is worth noting that the entire $KLC token supply will be mined prior to the launch of the mainnet.

4.5 KalyChain Configurations

- An IBFT PoS with built-in system contracts will be used as a core consensus algorithm by KalyChain.
- The average block time is expected to be 2 seconds.
- Initially, 21 nodes will be run to comply with BFT (Byzantine Fault Tolerance).
- The block size will be dynamic and decided by the Validator set. The initial limit for block gas is 30,000,000.
- The expected number of validator nodes in the chain shall be at least 21.
- Any account that has more than 10,000,000 $KLC tokens and passes community authority and authentication will be able to join the Validator Set.
- KalyChain has pre-deployed contracts for staking. This allows the betting of $KLC tokens, providing rewards to holders.
- If the block is not produced or accepted within the expected time, the next validator would take over the duty of the proposer.
- There is no newly minted block reward for block production.
- All transaction fees will be valued at $KLC.

5. VE Model for KalyChain

$veKLC is an acquisition and performance system based on curve's veCRV mechanism. By using this model, users can lock their $KLC for up to 4 years to get up to four times the amount of KLC $ve as a reward. (for example, $100 KLC blocked for 4 years returns 400 $veKLC). $veKLC is not a transferable token nor is it traded on liquid markets. It is more like an account-based points system that means the duration of the acquisition of the wallet's locked KLC $ve tokens within the protocol.

5.1 Voting power

EachKLC $ve will have 1 vote on governance proposals. Betting 1 $KLC tokens for the maximum time, 4 years, would generate 4 KLC $ve. Users can exchange their KLC $ve tokens for $KLC tokens, once the acquisition period ends. Meanwhile, the user can also increase their KLC $ve balance by locking $KLC tokens, extending the end date of the lock, or both.

It is worth noting that $veKLC is non-transferable and each account can only have a unique blocking duration. This means that a single address cannot block $KLC tokens for different periods of time. For example, a user will not be able to block one set of $KLC for 2 years and then another set of $KLC tokens for 3 years. All $KLC per account must have a uniform lock time.

5.2 How to useKLC $ve

$veKLC tokens cannot be sold or transferred. Instead, they have other use cases, including:

- Earn extra airdrop from $KLC tokens;
- Receive random prizes/lottery rewards;
- Governance: voting on how the protocol awards grants to developers, etc.;
- Serve as a network validator: A certain number of tokens will be required fromall validators.

6. KalyChain Smart Contracts

The management of the validator along with its selection, distribution of rewards and bets are carried out using the protocol's smart contracts. These contracts are deployed in the genesis block. At KalyChain, there are six different types of smart contracts.

- **Governance contract:** manages the proposals and votes of the validator.
- **Validator set contract :** classifies validators and decides which ones should be chosen or eliminated.
- **Vault Contract:** Receives all chain bridge withdrawal fees.
- **Betting Contract:** Manages betting operations and the distribution of block rewards.

- **Trim Contract** – Handles disciplinary actions against validators who do not follow the chain's default rules.

6.1 Governance contract

Blockchain networks are autonomous platforms that evolve on their own and provide transparency through the democratic interaction of the community between peers. On-chain management is an approach to recommending and making changes to blockchains. In this type of governance, change initiation rules are usually encoded in the blockchain protocol.

Validators selected by the community suggest possible ideas through code updates and written suggestions. All chosen validators and regular users vote to accept/reject the proposed change. Under the governance contract, community members vote democratically on proposals that will advance the development of the blockchain network. In order to recommend a proposal, the user must have a sufficient number of $KLC tokens shared.

On the other hand, people with a certain amount of $KLC tokens can vote on the proposals. There will also be an option to report on management commitments to report misuse of contracts.
The following sample options are subject to change following community feedback:

- Minimum bet amount to be a validator
- Minimum bet amount for the general user
- Minimum bet amount to give a proposal
- Etc...

6.2 Validator Set Contract

This contract validates and stores nodes that meet the requirements to become a validator. In addition, the contract lists the main validators and their addresses, the last block created and approved, and classifies the blocks produced by specific validators.

6.3 Vault Contract

All chain bridge removal fees are sent to the Vault Contract.

6.4 Betting contract

This contract performs the staking, calculation of rewards and distribution of rewards to both users and validators. This contract also periodically updates the rewards received by validators and shareholders.

6.5 Trimming contract

KalyChain adopts a cutting methodology similar to that used by Binance Smart Chain. In addition to improving the security of the KalyChain chain, the cut is used to safeguard its

governance mechanisms in the chain of malicious or dishonest behavior through disciplinary actions.

Evidence of the KalyChain chain forward slash can be presented by anyone. It's worth noting that every transaction shipment demands proof of trimming and is subject to fees. That said, it also produces a higher reward if it succeeds.

Two types of cutting behaviors are considered below:

- **Double signature:** Suppose two different block headers have the same height and the same parent block hash. If these two block headers are sealed by the same validator and different signatures are created, then this validator will be punished and permanently imprisoned.
- **Not available:** If a validator loses 48 blocks every 24 hours, they will not be able to receive rewards from block fees. If a validator loses more than 96 blocks during 24 hours, the validator will be punished for 10,000 $KLC tokens and will be jailed for 3 days. During jail time, you will still be able to produce or validate blocks.

7. KalyChain Staking

The KalyChain project will allow users to access three different token staking models for returns:

- Wagering $KLC tokens on the chain will provide additional rewards of $KLC.
- Betting $KLC tokens on the KalyChain Ve model will allow users to receive tokens $veKLC. They can select a rights acquisition time between half a year and 4 years, with longer rights acquisition periods that grant higher KLC rewards and more KLC $ve in return.

The staking process is as follows:

1. Users can wager the $KLC they received as rewards on the Ve model and receive additional rewards from $veKLC.
2. Users can wager $KLC on KalyChain and lock themselves for a period of time to receive $KLC rewards.

8 . Potential applications on top of KalyChain

8.1 NFT

KalyChain will provide its users with the ability to publish their own NFTs following the ERC721 protocol. Since this proven NFT standard is widely accepted by markets and metaverses, KalyChain NFT owners will be able to integrate their NFT into the existing NFT landscape.

8.2 DeFi

As an EVM-compatible blockchain, DeFi protocols such as Uniswap and SushiSwap can be seamlessly integrated with KalyChain. $KLC is a DeFi-capable cryptocurrency that can be locked into various liquidity pools and provide rewards to their holders

In addition, several Layer 2 solutions found within the Polygon Edge architecture (including ZK Rollups and Optimistic Rollups) will allow KalyChain to make improvements to its existing transaction speeds in DeFi and address some privacy concerns.

8.3 GameFi

KalyChain will provide developers with the ability to build entire virtual worlds and blockchain games within KalyChain's smart contract framework. As a result, the $KLC cryptocurrency will allow users to participate in virtual gaming economies and share digital resources on their favorite metaverses.

8.4 KalyChain RoadMap

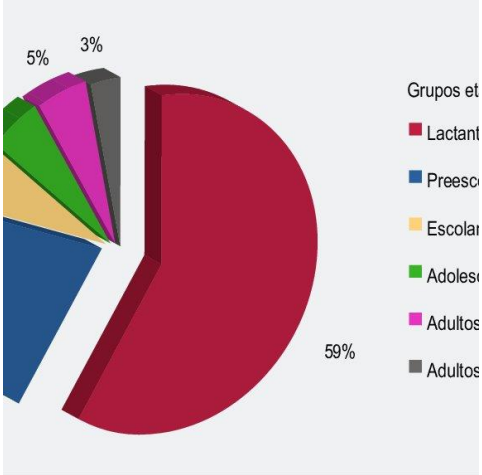
8.4 KLC Distribution

As previously mentioned there will be a maximum supply of 7 Billion coins that were mined from the beginning, to encourage the decentralization of the network, 51% of KLC coins will initially be allocated to the community through public and private sales that will be carried out gradually to avoid inflation and devaluation of the currency.

In turn, in order to ensure the long-term development of KalyChain, 49% of the remaining coins will be blocked in different periods that will be destined for the growth of the KalyChain ecosystem and the total will be distributed as follows:

Premine Distribution

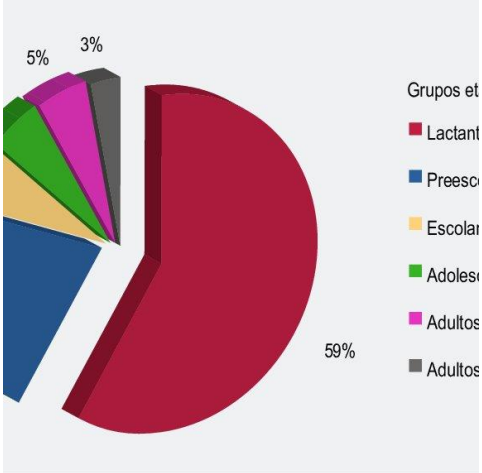
Allocation	Amount	Vesting
Public & Private Sale	51%	No blocking
Founding Team	9%	locked for 3 Years
Business Development	10%	4 years locked in with a distribution of 5 million/year
Education and courses for the community	5%	No blocking
Continuous improvement	10%	2 Years locked
Network Operations	3%	4 Years locked
Treasury	7%	5 Years locked
Advisors & Marketing	5%	2 Years locked
Total:	100%	-



Regarding the sale of 51% of the supply, the profits obtained will be destined for the development of the Road Map 1.0 and 2.0 which is composed of a series of centralized applications of the KalySsi group and decentralized applications for the community such as a swap and a DAO, in addition to the creation of a Learning Management System to encourage blockchain development within the Kalychain community. All of the above in order to propose a continuous development within the ecosystem that provides solutions to real problems and needs of the crypto ecosystem.

Earnings Distribution

	Allocation	Amount	Vesting
	Exchanges Listing	15%	50% locked for 6 months
	Kalypay	25%	No Blocking
RoadMap 1.0	**Kalyssi Exchange**	20%	No Blocking
	Kaly Swap (DEX)	5%	No Blocking
	Kankou Moussa DAO (DeFi 2.0)	5%	No Blocking
	Deployment of KalySynthex	5%	2 Months Locked
	LMS for the community	5%	No Blocking
	Road Map 2.0	20%	Locked for 6 monts
	Total:	100%	-



9. Implementation details

Source codes and more information are available in
https://github.com/KalyCoinProject/kalychain

10. References

- A.M Antonopoulos. Dominating bitcoins, 2014.
- A. Biryukov and D. Khovratovich. Equihash: Asymmetric proof of work based on the generalized birthday problem. Minutes of NDSSˆaA¯Z16, February 21–24, 2016, San Diego, CA, USA ISBN 1- 891562-41-X, 2016
- O. Bussmann. The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation, pp. 473–486. Springer International Publishing, Cham, 2017.
- Marco Mazzoni, Antonio Corradi, Vincenzo Di Nicola. Evaluating the Performance of Authorized Blockchains for Financial Applications: The ConsenSys Quorum Case

Study, Blockchain: Research and Applications, Volume 3, Issue 1, 2022, 100026, ISSN 2096-7209, https://doi. orrg/10.1016/j. BCRA. File 2021.100026.

- Cryptographic power consumption. https://www. moneysupermarket. com/gas-and-elec tricity/features/crypt o-energy-c onsump tion/, 2021.
- Optimistic Rollups vs ZK Rollups: Examining six of the most exciting Layer 2 scaling projects for Ethereum, https://limechain.tech/blog/optimistic-rollups-vs-zk-rollups/, Aug 2021.
- Ethereum virtual machine. https://ethereum.org/en/developers/docs/evm/.
- The edge of the polygon. https://github.com/0xPolygon/polygon-edge https://polygon.technology/solutions/polygon-edge/
- Paxos, Raft, EPaxos: How has distributed consensus technology evolved? https://www.alibabacloud.com/blog/paxos-raft-epaxos-how-has-distributed-consensus-te chronology-evolved_597127, Jan 2021.
- An introduction to Binance Smart Chain (BSC), https://academy.binance.com/en/articles/an-introduction-to-binance-smart-chain-bsc September 2021.
- Shiba Token, https://shibatoken.com/ , 2021.
- Raft's consensus algorithm, https://raft.github.io/ 2021.
- Paxos Consensus for Beginners, https://medium.com/distributed-knowledge/paxos-consensus-for-beginners-1b8519d336 0f, May 2020.
- Ongaro, J. Ousterhout, In Search of an Understandable Consensus Algorithm Proceedings of the USENIX Conference 2014; 19–20; Philadelphia, PA, USA, USENIX ASSOCIATION, pp. 305-320, June 2014.
- Optimistic vs. ZK Rollup: Deep Dive, https://blog.matter-labs.io/optimistic-vs-zk-rollup-deep-dive-ea141e71e075, November 2019.
- Bitcoin White Paper. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf, Oct 2008.
- M. Castro and B. Liskov, "Practical byzantine fault tolerance", in Proceedings of the 13th Symposium on Operating Systems Design and Implementation, vol. 99, 1999, pp. 173-186.
- The edge of the polygon. D. Ongaro, J. Ousterhout, In Search of an Understandable Consensus Algorithm, in: Proceedings of the 2014 USENIX Conference; 19–20 June 2014; Philadelphia, PA, USA, USENIX ASSOCIATION, 2014, pp. 305-320. L. Lamport, The part-time parliament, ACM Trans. Syst. 16 (2) 133–169, 1998.
- Leslie Lamport. 1998. The part-time parliament. ACM Trans. Computation. Syst. 16, 2, 133–169. DOI: May https://doi.org/10.1145/279227.279229 , 1998.
- I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev and J. Mendling. Monitoring and execution of untrusted business processes using Blockchain, pages 329–347. Springer International Publishing, Cham, 2016.
- T. Tenso, A. Norta and I. Vorontsova. Evaluating a new agile method of requirements engineering: a case study. In Proceedings of the 11th International Conference on Evaluation of Novel Software Approaches to Software Engineering - Volume 1: ENASE, pp. 156–163, 2016.
- Q Vasin. BlackcoinaˆA ˙Zs proof-of-stake protocol v2, 2014.'

- M. Vukoli'c. The search for a scalable blockchain fabric: proof of work vs. bft replication. In International Workshop on Open Problems in Network Security, pages 112–125. Springer, 2015.
- G. Wood.Ethereum: A decentralized and secure generalized transaction ledger. Ethereum Yellow Paper Project, 2014