Cyberscope

Audit Report

Kalichain

June 2024

Blockchain https://explorer.kalichain.com/

Audited by © cyberscope

Table of Contents

Introduction

The purpose of this audit report is to provide a comprehensive analysis and evaluation of the Kalichain blockchain, which is a fork of the Ethereum blockchain. This audit will assess the technical and functional aspects of Kalichain, its security protocols, governance structure, tokenomics, and overall performance. By understanding the intricacies of Kalichain, stakeholders can gain insights into its strengths and areas that may require improvement.

Kalichain Overview

Kalichain is a decentralized layer-1 blockchain and ecosystem focused on certification. It is designed to provide secure and transparent solutions for product authentication and various decentralized applications. Utilizing Near Field Communication (NFC) and Non-Fungible Tokens (NFTs), Kalichain ensures the authenticity of products and offers a robust platform for numerous blockchain-based activities.

The proprietary blockchain holds full control over its protected applications. This allows Kalichain to manage users' access and protect sensitive information. It also ensures the blockchain meets the specific needs of authenticity verification across industries, offering a secure certification solution for brands and consumers.

The Kalichain ecosystem is extensive. It encompasses a (web3) clothing brand, an investment platform focused on tokenization, a payments platform, a global marketplace, a blockchain explorer, and a flagship product certification method, Kalicertif.

Kalicertif uses advanced algorithms and AI to verify products. Every distinct product can be recorded and verified on its blockchain as an NFT. This authenticates a product's authenticity, regardless of how often ownership is transferred.

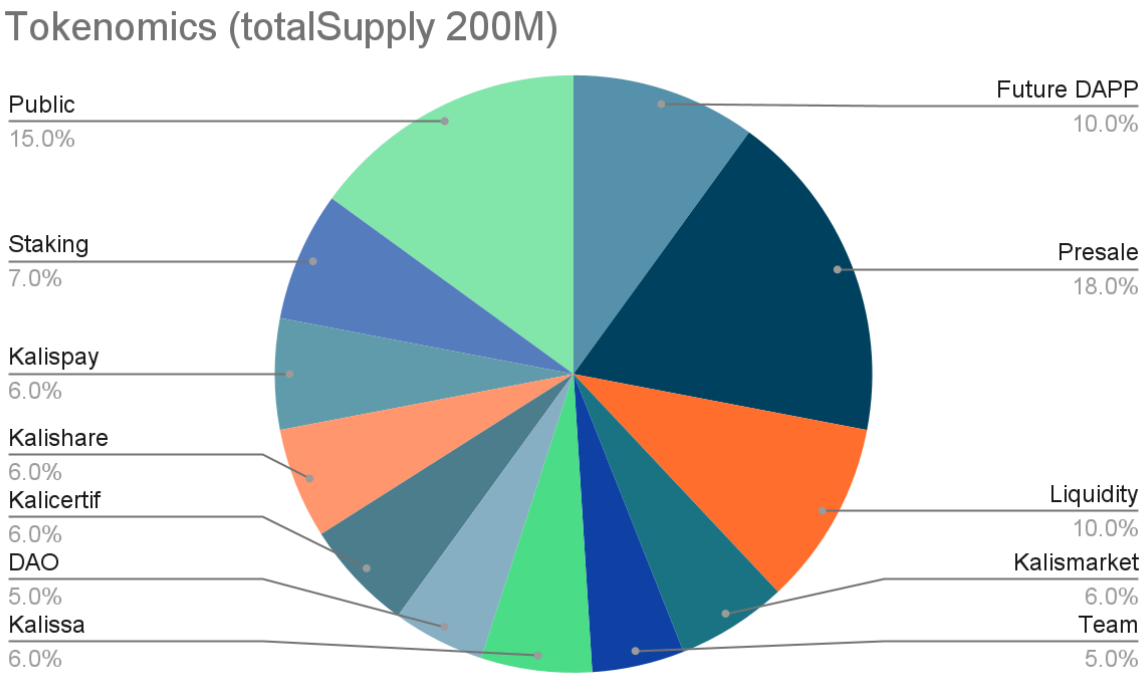
Via the NFC function or a QR code on the dedicated mobile app, users can easily scan a product and access metadata about its background, origin, and chain of custody. Here's why this use case matters.

Tokenomics

The Kalichain ecosystem operates with its native cryptocurrency, KALIS, which facilitates transactions and incentivizes participation within the network. Launched on March 19, 2024, KALIS has a total supply of 200 million tokens, with 75% allocated for distribution. The token distribution includes presale, public sale, staking rewards, and funds for future DApp development.

Distribution Breakdown:

- Presale: 18%
- Liquidity: 10%
- Future DApp Development: 10%
- Public Sale: 15%
- Staking: 7%
- Kalismarket: 6%
- Team: 5%
- Kalissa Project: 6%
- DAO: 5%
- Kalicertif: 6%
- Kalipay: 6%
- Kalishare: 6%



KALIS tokens are used to pay for services within the Kalichain ecosystem, and their value is closely linked to the network's growth and transaction volume. The token is currently available for purchase on the MEXC exchange.

Governance

Governance within Kalichain is community-driven, with nodes playing a crucial role in maintaining network security and functionality. The network encourages node ownership, which supports its operation and provides rewards to node operators. Plans include establishing a Decentralized Autonomous Organization (DAO) to decentralize governance further, allowing users to propose and vote on network developments, and giving users more control over the network's growth.

Currently, Kalichain employs a decentralized governance model involving 39 nodes that maintain and secure the network. Node owners are rewarded for their contributions and have a stake in the network's future. Governance is community-centric, allowing members to propose and vote on changes, ensuring that the network evolves in line with the collective vision.

Kalichain Structure

Kalichain, a fork of the Ethereum blockchain, retains much of Ethereum's foundational architecture while integrating its unique features and enhancements. This section delves into the technical architecture of Kalichain, examining its core components, execution environment, and the mechanisms that ensure its robust and scalable operation.

Kalichain's blockchain structure comprises a decentralized ledger that records all transactions and smart contract interactions. Each block in the Kalichain network contains a list of transactions, a reference to the previous block. The design is intended to ensure security, immutability, and transparency.

Ethereum Virtual Machine (EVM)

At the heart of Kalichain's functionality is the Virtual Machine (VM), a decentralized computational engine that executes smart contracts. The VM is responsible for managing the state of the blockchain, executing transactions, and ensuring that the contract code behaves as expected. Smart contracts on Kalichain are written in high-level languages such as Solidity and Vyper, which are then compiled into bytecode for execution by the EVM.

Nodes and Clients

Kalichain's network comprises various types of nodes, each fulfilling specific roles:

- Full Nodes: These nodes store the entire blockchain, validate transactions and blocks, and propagate transactions to other nodes.
- Light Nodes: Light nodes store only a subset of the blockchain and rely on full nodes for validation. They are suitable for devices with limited storage capacity.
- Archive Nodes: These nodes store the historical states of the blockchain, making them ideal for data analysis and forensic purposes.

Each node runs an execution client and a consensus client. The execution client handles transaction processing, state management, and the VM, while the consensus client manages block propagation and the consensus protocol.

Execution Client

The execution client in Kalichain is responsible for processing transactions, maintaining the state of the blockchain, and executing smart contracts. It creates execution payloads, which include transaction data and state updates and interacts with the VM to ensure the correct execution of smart contract code. Additionally, the execution client provides an interface for users and developers to interact with the blockchain through JSON-RPC API methods.

Consensus Client

The consensus client maintains the integrity and consistency of the blockchain by running the consensus algorithm. It receives blocks from peers, validates them, and ensures that the node follows the chain with the greatest accumulated stake or work. Kalichain is adopting Geth's Proof of Authority (POA) consensus mechanism. This strategy allows Kalichain to leverage the foundation of Ethereum while introducing efficiencies and innovations tailored to its unique application in product certification.

Storage and Data Management

Kalichain utilizes a combination of volatile and persistent storage to manage blockchain data. The VM uses linear, volatile memory for transaction runtime operations, while persistent storage (state) maintains long-term data such as account balances and smart contract codes. The state is stored in a modified Merkle Patricia Trie, which enables efficient and secure data retrieval and updates.

Gas and Transactions

Gas is a fundamental aspect of Kalichain's architecture, serving as the unit of computational effort required to execute transactions and smart contracts. Each operation in the VM consumes a specified amount of gas, and users must pay for gas in KALIS, the native cryptocurrency. This mechanism ensures that resources are used efficiently and prevents spam on the network.

Conclusion

Kalichain's technical architecture is a robust and scalable system built upon the proven foundations of the Ethereum blockchain. By leveraging the Virtual Machine (VM), and a well-defined gas model, Kalichain ensures secure and efficient execution of transactions and smart contracts. This architecture supports the diverse applications within the Kalichain ecosystem, from decentralized finance (DeFi) to non-fungible tokens (NFTs) and beyond.

Consensus Mechanism

Kalichain represents a significant evolution in blockchain technology, branching out as a fork from Ethereum and adopting Geth's Proof of Authority (PoA) consensus mechanism. This strategic pivot allows Kalichain to leverage the robust foundation of Ethereum while introducing efficiencies and innovations tailored to its unique application in product certification.

Genesis Configuration

To initialize the Kalichain network, the following genesis configuration is essential. This setup marks the commencement of the Kalichain blockchain, utilizing chain ID 654 and implementing the PoA consensus through the Geth framework.

The following genesis file is a critical first step, ensuring all network nodes begin from a common initial state, enabling seamless interaction and transaction verification under the PoA consensus model.

```
{
    "config": {
      "chainId": 654,
      "homesteadBlock": 0,
      "eip150Block": 0,
      "eip155Block": 0,
      "eip158Block": 0,
      "byzantiumBlock": 0,
      "constantinopleBlock": 0,
      "petersburgBlock": 0,
      "istanbulBlock": 0,
      "berlinBlock": 0,
      "clique": {
        "period": 5,
        "epoch": 30000
      }
    },
    "difficulty": "1",
    "gasLimit": "8000000",
    "extradata":
"0x0000000000000000000000000000000000000000000000000000000000000000047e8
4757cf1a1ac54d55d395c6234f1e35ee372c0000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000",
    "alloc": {
        "59d1D6e83e7d4552B7C56d12218FA38971022caa": { "balance":
"19999999800000000000000000"},
        "8551e2DB9d59907B390FEb7faBfCFF78c1ff720D": { "balance":
"2000000000000000000"}

      }
  }
```


Genesis File Breakdown

The genesis file for the Kalichain network contains several key variables that define the initial state and configuration of the blockchain.

- config: This section outlines the various blockchain configurations and the activation blocks for different Ethereum Improvement Proposals (EIPs). Each EIP listed (e.g., Homestead, Byzantium, Constantinople) has a block number set to 0, indicating that the features and changes introduced by these proposals are active from the genesis block.

- chainId: The unique identifier for the Kalichain network is set to 654. This ID distinguishes Kalichain from other blockchains and ensures that transactions meant for Kalichain are not mistakenly accepted by other chains.
- clique: This subsection specifies parameters for the Clique proof-of-authority (PoA) consensus algorithm. The period is set to 5 seconds, dictating the time between each block. The epoch is set to 30000, which defines the interval after which a new set of signers is allowed to be selected.
- difficulty: This parameter is set to "1", indicating minimal difficulty for block creation. This is typical in PoA networks where block creation is controlled by pre-approved validators rather than computational power.
- gasLimit: Set at "8000000", this variable determines the maximum amount of gas that can be used per block. Gas is a unit of computational work required for transactions and smart contracts.
- extradata: This field includes arbitrary data relevant to the PoA setup. It often contains the list of initial signers or validators authorized to validate transactions and create new blocks.
- alloc: This section pre-allocates balances to specific addresses. For instance, the address "59d1D6e83e7d4552B7C56d12218FA38971022caa" is allocated a balance of 199,999,998 KALIS, and "8551e2DB9d59907B390FEb7faBfCFF78c1ff720D" is allocated 2 KALIS. This allocation ensures that certain accounts have predefined balances at the network's start.

This genesis configuration is essential for initializing the Kalichain network, ensuring all nodes begin from a consistent state, and enabling seamless operation under the PoA consensus model.

Proof of Authority (PoA)

Proof of Authority (PoA) is a consensus algorithm that delivers an efficient solution for blockchains, particularly private ones. Coined by Gavin Wood in 2017, PoA relies on a limited number of approved validators to secure the network. Validators earn the right to generate new blocks by passing a strict vetting process, ensuring trustworthy validation.

How PoA Works

- Validator Selection: Validators are preapproved and must verify their identities publicly, ensuring accountability and trust.
- Block Creation: Validators use software to automate the organization of transactions into blocks. They do not need constant monitoring but must maintain their systems reliably.
- Validation Process: When a new transaction is proposed, validators independently verify its validity. Once a majority concurs, the transaction is included in a new block and broadcast to the network.

Advantages

- Efficiency: PoA is highly efficient, requiring less computational power than PoW and less staking capital than PoS.
- Speed: Transactions are processed quickly due to the small number of validators.
- Security: Validators' public identities and reputations make the network resilient to malicious activities.
- Governance: PoA networks are often used in private or consortium blockchains where governance is essential. Validators can make decisions collectively based on the network’s requirements.
- Scalability: PoA networks can scale efficiently, as they are not limited by resource constraints as in PoW or PoS.

Drawbacks

- Centralization: PoA can be criticized for centralization since validators are chosen entities, which might lead to collusion or power concentration.
- Limited Decentralization: PoA does not offer the same level of decentralization as PoW or PoS, which can be a concern for some applications.

- Sybil Attacks: If a malicious entity gains control of the majority of validators, it could compromise the network's integrity.

PoA Common Attacks

Distributed Denial-of-service attacks (DDos)

A Distributed Denial-of-Service (DDoS) attack is an attempt to render an online service unavailable by flooding it with traffic from multiple sources. An attacker transmits a large number of transactions and blocks to a network node in an effort to disrupt its operation and render it inaccessible. Due to the pre-authentication of network nodes by the PoA mechanism, only nodes that can withstand DoS attacks can be granted block generation rights.

51% Attack

In PoA consensus, a 51% attack necessitates an attacker obtaining control over 51% of network nodes. This differs from the 51% attack for Proof-of-Work consensus types, in which an attacker must possess 51% of the network's computational capacity. Controlling the nodes in a permissioned blockchain network is much more difficult than acquiring computational capacity.

With Proof-of-Authority, individuals acquire the right to become validators, so there is an incentive to maintain the position. Validators are rewarded with repute, allowing them to maintain their authority as nodes. PoA only permits non-consecutive block approval from any validator, thereby centralizing the risk of severe harm to the authority node.

Conclusion

Kalichain's fork from Ethereum, combined with the strategic use of Geth's PoA consensus, represents a forward-thinking approach to blockchain development. By focusing on product certification, Kalichain seeks to address specific industry challenges while benefiting from Ethereum's proven infrastructure. The project's presence on GitHub serves as an open invitation for developers to contribute to this innovative blockchain venture.

Smart Contracts and DApps

Kalichain, leveraging the same foundational technology as Ethereum, incorporates smart contracts and decentralized applications (DApps) to provide a secure, efficient, and transparent blockchain ecosystem. These elements are crucial for automating agreements and creating decentralized solutions across various industries.

Smart Contracts on Kalichain

Smart contracts in Kalichain are self-executing contracts where the terms of the agreement between the buyer and the seller are encoded directly into the blockchain. These contracts automatically enforce the agreed-upon conditions without the need for intermediaries, ensuring trust and reducing the risk of human error.

How Smart Contracts Work

1. Agreement Terms: The terms of the contract, such as the sale of a digital asset, are agreed upon by the parties and encoded into a smart contract.
2. Execution: When the specified conditions are met, such as the receipt of payment, the smart contract automatically executes the agreed-upon actions, like transferring ownership.
3. Finalization: The transaction is completed, and the details are recorded on the Kalichain blockchain, providing a permanent and tamper-proof record.

For example, in a supply chain scenario, a smart contract could automatically release payment to a supplier once the goods are delivered and verified, streamlining the process and reducing the need for manual checks.

Advantages

- Automation: Automates contract execution, minimizing the need for intermediaries and manual intervention.
- Security: Ensures tamper-proof execution and storage of contract terms on the blockchain.
- Efficiency: Reduces transaction times and costs by eliminating the middlemen.
- Transparency: Provides a transparent record of all transactions, which is accessible and auditable by all parties involved.

Technology

Kalichain smart contracts are typically written in Solidity, a high-level programming language similar to JavaScript. The Virtual Machine (VM) on Kalichain executes these contracts, ensuring that the terms encoded in the contract are carried out accurately and securely.

Decentralized Applications (DApps) on Kalichain

DApps on Kalichain leverage blockchain technology to provide decentralized solutions that operate without a centralized authority. These applications typically use one or more smart contracts to function, offering various services from finance to digital art marketplaces.

Key Characteristics

- Decentralization: Operate on the Kalichain network without reliance on a central server.
- Transparency: Transactions and operations are transparent and recorded on the blockchain.
- Security: Benefit from the cryptographic security of the blockchain, making it resistant to tampering and fraud.

Operation

DApps interact with smart contracts to perform their functions. For instance, a decentralized finance (DeFi) application on Kalichain might use smart contracts to facilitate lending and borrowing without traditional financial intermediaries. Users interact with these DApps through web interfaces, while the underlying smart contracts handle the transaction logic on the blockchain.

Benefits

- Trustless Interactions: Users can interact with the DApp without needing to trust a central authority.
- Reduced Costs: Lower fees due to the elimination of intermediaries.
- Innovative Solutions: Enable new business models and solutions that leverage the decentralized nature of the blockchain.

Examples

- DeFi Platforms: Allow users to lend, borrow, and earn interest on cryptocurrencies without traditional banks.
- NFT Marketplaces: Facilitate the creation, buying, and selling of non-fungible tokens (NFTs), offering a decentralized marketplace for digital assets.

- Supply Chain Management: Track and verify the provenance of goods, ensuring transparency and reducing fraud in supply chains.

In summary, Kalichain's use of smart contracts and DApps mirrors the robust capabilities of Ethereum, offering a secure, efficient, and transparent ecosystem for various applications. By leveraging these technologies, Kalichain provides innovative solutions that enhance trust and streamline operations across multiple industries.

Kalichain Security Review

As a blockchain ecosystem forked from Ethereum, Kalichain inherits many of the inherent strengths and challenges associated with Ethereum. This section reviews the current and potential future security challenges that Kalichain may face, drawing parallels to the well-documented issues of Ethereum. These include scalability, transaction costs, centralization fears, privacy concerns, and Maximal Extractable Value (MEV).

Scalability

One of the primary challenges for Kalichain, as with Ethereum, is scalability. Blockchain technology inherently struggles with scalability, and Kalichain is no exception. The ability to process transactions efficiently and quickly is crucial for widespread adoption. For instance, Ethereum currently can handle about 15-30 transactions per second. As Kalichain grows, it will need to address similar scalability issues to avoid network congestion and high transaction fees, especially during peak usage periods.

Traditional methods of increasing node sizes or block sizes are no longer viable solutions due to the centralization risks they pose. Modern approaches focus on Layer-2 solutions and rollups to enhance scalability without compromising decentralization.

Increasing Transaction Costs

High transaction costs have been a significant issue for Ethereum, particularly during periods of high demand. During the DeFi boom, gas fees on Ethereum surged to prohibitively high levels, making it difficult for average users to interact with the network. Kalichain, leveraging similar mechanisms, might face similar challenges as it grows. Keeping transaction costs low is essential to ensure accessibility for all users. Solutions such as optimizing gas fees and implementing efficient Layer-2 solutions will be critical in managing transaction costs.

Centralization Fears

Kalichain, like Ethereum, transitioned to a proof-of-stake (PoS) consensus mechanism to enhance security and efficiency. However, this transition introduces new centralization concerns. In a PoS system, validators with significant stakes have more influence,

potentially leading to a concentration of power among a few large stakeholders. This could undermine the decentralized ethos of the blockchain. Ensuring a wide distribution of staked KALIS tokens and promoting participation from a diverse validator base will be crucial to mitigating these centralization risks.

Privacy

Privacy remains a significant challenge for Kalichain. The transparency of blockchain technology means that all transactions are publicly accessible, which can be a drawback for users seeking privacy. While solutions like zero-knowledge rollups provide some privacy enhancements, they are still under development and have limitations, particularly regarding smart contract deployment. Kalichain will need to adopt and innovate privacy solutions to cater to users who require confidential transactions.

Maximal Extractable Value (MEV)

MEV refers to the maximum value that validators can extract from transaction ordering within blocks. On Kalichain, similar to Ethereum, MEV poses a risk of economic manipulation. Validators might engage in practices like front-running or sandwich attacks to maximize their profits, potentially at the expense of regular users. This could undermine trust in the network. Implementing measures to detect and mitigate malicious MEV extraction will be essential to maintaining the integrity of the Kalichain network.

Smart Contract Vulnerabilities

Smart contracts on Kalichain, like those on Ethereum, are susceptible to various security vulnerabilities. These include coding errors, logic flaws, and exploits that can lead to significant financial losses. Ensuring rigorous security audits, employing formal verification methods, and following best practices in smart contract development are critical steps to prevent exploits and enhance the security of smart contracts on Kalichain.

Summary

Kalichain is pioneering the integration of blockchain technology with real-world applications, particularly in product certification and authenticity. Its comprehensive ecosystem, supported by robust tokenomics and community-driven governance, positions it as a leader in bridging traditional finance (TradFi) and Web3. As Kalichain continues to grow and innovate, it aims to provide secure, transparent, and efficient solutions for various industries.

While Kalichain benefits from the robust and tested framework of Ethereum, it also inherits several of its challenges. Addressing scalability, managing transaction costs, preventing centralization, enhancing privacy, mitigating MEV risks, and securing smart contracts are essential for the sustainable growth and security of the Kalichain network. Proactive measures and continuous innovation will be key to overcoming these challenges and ensuring a secure and efficient blockchain ecosystem.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope’s prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope’s position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io