BLOCKCHAIN KALYCOIN

2022 Whitepaper 1.0

Motivation is the catalyzing ingredient for every successful innovation.

COMPANY

Kalycoin Project

Kalycoin was launched in 2020 on the Smart Chain Binance, the Kalycoin Project helps to manage the general development, progress, and privileges of open source community projects through the development of good governance mechanisms. It is committed to the development and construction of the Kalycoin Project and the advocacy and promotion of governance transparency to promote the safe and harmonious development of the project.

The design goals of the Kalycoin Project governance structure mainly consider the sustainability of open source community projects, the effectiveness of management, and the safety of raised funds.

KalyCoin

Kalycoin is a cryptocurrency created by the Kalypay payment platform for usability in the real market to deal with a highly competitive digital financial ecosystem.

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.

KalyCoin

The development of a productive and sustainable blockchain is one of the pillars of the Kalycoin project.

Introduction

Industrial revolutions have been characterized by bringing with them disruptive products and technologies that have marked and changed people's daily lives, becoming more and more comfortable for their beneficiaries, just think that 2 centuries ago we were still mobilizing in horse-drawn carriages, It has been a little over 100 years since the beginning of the mass production of automobiles and a little less than 40 years ago we managed to reach the moon. We as a population are not aware that the speed of technological growth that humanity has developed in the last 200 years has grown relatively exponentially if we analyze it at a historical level, however, this decade is not the 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 because many bring with them the programming and automation of processes that are performed by humans routinely or daily improving these wells making them more precise and efficient.

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

“Creativity is the power to connect the seemingly disconnected”
William Plumber

Search & Development Performance

Unlike Bitcoins, many smart contract systems are equipped with the Turing-complete Solidity language that resembles JavaScript syntax and targets for enactment, for example, the Virtual Ethereum machine [44]. Ethereum is the de facto leading smart contract system despite being riddled with several shortcomings.

The latter initially find application in various domains such as, for example, financial technology [6], Internet of Things (IoT) applications [33], digital signage solutions [11].

An essential aspect of smart contracts is a decentralized validation of transactions, initially using the so-called proof of work (PoW) [42]. 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 electricity-intensive.

> *“Everyone wants to live on top of the mountain, but all the happiness and growth occurs while you’re climbing it.”*

The amount of technology in buildings and homes is rapidly growing and changing. The most significant

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 tools for formal verifications [3].

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 [2] and blockchain fragmentation [20].

More reasons limit the widespread adoption of the Ethereum industry [8]. For example, an inability to automate information logistics between organizations, the lack of privacy protection differentiations between external vs. related internal private contracts, secure and stable virtual machines for blockchains with better-performing proof-of-stake transaction validation [2], formally verifiable smart contract languages, lite wallets that do not require downloading the entire blockchain and mobile device solutions for smart contracts with simple payment verification (SPV) [14]. 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, according to [19], the EVM has shortcomings such as previously experienced attacks against poorly handled exceptions and against dependencies such as for transaction.

2. Kalycoin Performance Advantages

The Kalycoin BlockChain platform executes the SHA-256 cryptographic algorithm maintaining the UTXO model used by Satoshi Nakamoto in 2009 with the creation of bitcoin, however it offers great changes and added values compared to blockchains such as bitcoin since It integrates a virtual machine (Ethereum EVM) with the difference that it runs a PoS consensus system, which makes it more efficient and scalable in the long term. Owning a virtual machine makes possible the development of smart contracts (smart contracts) and Dapps, it consists of a programmed agreement between P2P peers or business-to-business B2B in which all the requirements and conditions are stipulated for the smart contract to be executed correctly, is to clarify and emphasize that a smart contract is only as smart as the person who programmed it.

For the operation of some Smart contracts in blockchains, the use of Oracles is necessary, which play the role of judges (only when future information must be verified), offering the smart contract the pertinent information for the smart contract to be executed. For example, suppose that you want to develop a smart contract in your university or company which will reward the performance above the average of the employees of said entities, in the case of the university you will reward the professors whose students obtained a average higher than 4.0 (on a scale of 1 to 5) or in the company to the one who stands out among the staff or improves the performance of the company directly / indirectly, rewarding them with a reward of $ 100 USD (equivalent in Kalycoin cryptocurrencies) to each person who meets these requirements, for the smart contract to fulfill its function, it must have access to a database or oracle that provides pertinent information on the status of the beneficiaries of the rewards, so these smart contracts are so secure as the blockchain it is associated with and as weak as its oracles or developers can bee.

In contrast to Bitcoins, many smart-contract systems are equipped with the Turing-complete language Solidity that resembles JavaScript syntax and targets for enactment, e.g., the Ethereum Virtual [44] machine. Ethereum is the de facto leading smart-contract system despite being plagued by several deficiencies. First, proof-of-work transaction validation diminishes scalability to the point where Ethereum is considered to not be feasible for most industry applications.

2.1 Limitations of Ethereum Industry Adoption

Second, in a recent crowdfunding case study, the Ethereum affiliated Solidity smart contract was hacked because of security flaws resulting from a lack in the state of the art with respect to tools for formal verifications [3]. The security flaw resulted in a loss of ca. $50 million. Consequently, Ethereum performed a hard fork resulting in a schism yielding two separate Ethereum versions. Yet another Ethereum hard fork was caused by a denial of service attack, and more hard forks must be expected for realizing proof-of-stake [2] transaction validation and blockchain sharing [20].

More reasons limit widespread Ethereum industry adoption [8]. For example, an inability to automate cross-organizational information-logistics, lacking privacy protecting differentiations between external- versus related internal private contracts, secure and stable virtual machines for blockchains with better performing proof-of-stake [2] transaction validation, formally verifiable smart contract languages, lite wallets that do not require downloading the entire blockchain, and mobile-device solutions for smart contracts with simple payment verification (SPV) [14]. The latter means that clients merely download block headers when they connect to an arbitrary full node [23].

While Kalycoin uses the Ethereum Virtual Machine (EVM) for a current lack of more suitable alternatives, according to [19], the EVM has deficiencies such as earlier experienced attacks against mishandled exceptions and against dependencies such as for transaction-ordering, timestamps, and so on. It is also desirable for a smart-contract system to achieve industry-scalability with employing sidechains [10] and unspent transaction outputs (UTXO) [10], achieving compatibility to other blockchain systems such as Bitcoins [23], or Colored coins [36]. Furthermore, an adoption of features from the Bitcoin Lightning Network [35] yields scalability via bidirectional micropayment channels.

While smart-contract systems such as Ethereum attract attention, a widespread industry adoption does not exist for the above discussed reasons.

2.1.2 Kalycoin's Uniqueness and Comparison with Ethereum

This whitepaper addresses the gap by specifying the Kalycoin framework for smart-contract systems that answers the question of how to develop a smart-contract solution to satisfy critical customer requirements for enabling cross-organizational information logistics to reduce costs and time? To establish a separation of concerns, we pose the following sub-questions. What differentiating technological performance advantages do Kalycoin smart-contract solutions provide? What are critical smart-contract requirements the Kalycoin framework satisfies? What are the unique features of cross-organizational information logistics automation the Kalycoin framework aims to support? We will answer this and more questions throughout the document.

One of Kalycoin's main goals is to build a decentralized smart contract system based on UTXO with a proof-of-stake (PoS) consensus model [37] this means that the creator of the next block is chosen at random based on the wealth held in cryptocurrencies within their wallet and the maturity of the same, constantly rotating addresses to ensure decentralization and the participation of the entire network.

Therefore, blocks are usually built or minted rather than mined, there are block rewards in addition to transaction fees, and builders receive a percentage of "interest" on the amount of funds they bet.

This allows the chain to achieve high levels of security without excessive energy consumption, since to participate as an applicable active node for staking it is enough to have a Raspberry-Pi, laptop or 64-bit desktop PC which do not have such a high consumption compared to Proof of Work string mining rigs.

Kalycoin supports the Bitcoin and Ethereum ecosystems and aims to produce a variation of Bitcoin with Ethereum Virtual Machine (EVM) support. Following a pragmatic design approach, Kalycoin employs industry use cases with a strategy that integrates a metaverse within the blockchain, which will open up a world of possibilities for the continuous development of real-use applications. The latter allows Kalycoin to promote blockchain technology to a wide range of Internet users and thus decentralize the validation of PoS transactions globally while proceeding to create a secure and stable network in the long term.

The rest is structured as follows. Section 3.1 compares the advantages of Bitcoin UTXO versus the ethereum account model. Next, Section 3.2 discusses the consensus platform for the Kalycoin blockchain. Section 3.3 shows the integration of Kalycoin contracts into the EVM. Finally, Section 3.4 describes the payment model for Kalycoin's operations.

2.2 UTXO versus account model

In the UTXO model, transactions use as input unspent Bitcoins that are destroyed and as transaction outputs, new UTXOs are created. The results of unspent transactions are created as exchange and returned to the spender [1]. In this way, a certain volume of Bitcoins is transferred between different private key owners, and new UTXOs are spent and created in the transaction chain. The UTXO of a Bitcoin transaction is unlocked by the private key that is used to sign a modified version of a transaction. In the Bitcoin network, miners generate Bitcoins with a process called coinbase transaction, which does not contain any input. Bitcoin uses a scripting language for transactions with a limited set of operations. In the Bitcoin network, the scripting system processes data by stacks (Main Stack and Alt Stack), which is an abstract data type that follows the LIFO principle of Last-In, First-Out.

In the Bitcoin client, developers use the isStandard() [1] function to summarize scripting types. Bitcoin client support: P2PKH (Pay to Public Key Hash), P2PK (Pay to Public Key), MultiSignature (less than 15 private key signatures), P2SH (Pay to Script Hash) and OP_RETURN. With these five types of standard scripting, Bitcoin clients can process complex payment logics. On top of that, a non-standard script can be created and executed if the miners agree to encapsulate such a non-standard transaction.

For example: using P2PKH for the process of creating and executing scripts, we assume that we pay 0.01BTC for bread in a bakery with the imaginary Bitcoin address "Bread Address". The result of this transaction is:

OP_DUP OP_HASH160 <Bread Public Key Hash> OP_EQUAL OP_CHECKSIG Operation OP_DUP duplicates the top element of the stack. OP_HASH160 returns a Bitcoin address as the main item. To establish ownership of a bitcoin, a Bitcoin address is required in addition to a digital key and a digital signature. OP_EQUAL produces TRUE (1) if the two main elements are exactly the same and otherwise FALSE (0). Finally, OP_CHECKSIG produces a public key and a signature along with a validation for the signature corresponding to the hash data of a transaction, returning TRUE if a match occurs.

The unlock script according to the lock script is: <Brown signature> < Pan public key> The combined script with the previous two:

<Pan Sign> <Pan Public Key> OP_DUP OP_HASH160

<Bugging public key hashes> OP_EQUAL OP_CHECKSIG

Only when the unlock script and the lock script have a matching predefined condition is the execution of the script combination true. It means that the bread signature must be signed by matching the private key of a valid bread address signature and then the result is true.

Unfortunately, Bitcoin's scripting language is not Turing-complete, for example, there is no loop function. The Bitcoin scripting language is not a commonly used programming language. Limitations mitigate security risks by avoiding the emergence of complex payment terms, for example, the generation of infinite loops or other complicated logical loops.

In the UTXO model, it is possible to transparently track the history of each transaction through the public ledger. The UTXO model has parallel processing capability to initialize transactions between multiple addresses that indicate extensibility. In addition, the UTXO model supports privacy in the sense that users can use Change Address as the output of a UTXO. Kalycoin's goal is to implement smart contracts based on the innovative design of the UTXO model.

Compared to the UTXO model, Ethereum is an account-based system. More precisely, each account experiences direct transfers of value and information with state transitions. A 20-byte ethereum account address comprises a noun as a counter to ensure the unique processing of a transaction, the balance of the main internal cryptographic fuel to pay transaction fees called Ether, an optional contract code, and empty account storage by default.

The two types of Ether accounts are, on the one hand, external controlled by private key and, on the other hand, controlled by contract code. The old null code account type creates and signs transactions for message transfer. The latter activates the code after receiving a message to read and write the internal storage, create contracts or send other messages.

On Ethereum, balance management resembles a bank account in the real world. Each newly generated block potentially influences the overall status of other accounts. Each account has its own balance, storage, and code space base for calling other accounts or addresses, and stores the respective execution results. In the existing Ethereum account system, users perform P2P transactions through remote client procedure calls. Although it is possible to send messages to more accounts via smart contracts, these internal transactions are only visible in each account's balance and tracking them on Ethereum's public ledger is a challenge.

Based on the discussion above, we consider the Ethereum account model to be a scalability bottleneck and see clear advantages of the UTXO model of the Bitcoin network. Since the latter enhances the network effect we wish to offer, an essential design decision for the pending launch of Kalycoin is the adoption of the UTXO model.

2.3 Account Abstraction Layer

To achieve the interoperability and combine the UTXO model and the smart contract Account model, and decouple the value transfer layer from the contract execution layer, Kalycoin created the Account Abstraction Layer (AAL).
Kalycoin developed optimizations for the interface and conversion between smart contract operations and UTXO operations, and developed four new opcodes:
OP_CREATE: create a smart contract
OP_CALL: call smart contract (send KLC to the contract)
OP_SPEND: spend KLC in smart contract
OP_SENDER: allow address other than contract call sender to pay for Gas.

When the Kalycoin blockchain generates new blocks, in addition to making regular checks on transaction scripts, it also needs to check whether transactions contain the above-mentioned opcodes.

OP_CREATE is used to pass the contract bytecode to the virtual machine. OP_CALL sends data, gasPrice, gasLimit, VMversion and other key parameters required to run smart contracts through transaction scripts, and finally passes them to the virtual machine. Relying on this design, the Kalycoin x86 virtual machine can run on the blockchain in parallel with the EVM (Ethereum Virtual Machine), without the need to significantly modify the underlying protocol and retaining good functional scalability. In the future, any virtual machine based on the account model can be adapted to run on the Kalycoin blockchain.

In addition to a large number of adaptations and improvements in functionality, the Kalycoin also borrowed the concept of Gas from Ethereum, used the Gas model in the contract operation, and optimized the Gas model of the EVM.

Use of the Gas model can prevent endless loops caused by errors and malicious attacks, can allow miners to get rewards for performing calculations based on actual workload, and encourage contract designers and users to make reasonable use of on-chain resources. Normally the address of the contract call sender pays the Gas, but the OP_SENDER opcode allows a third-party address, such as a distributed application service provider, to pay the Gas.

Similar to EVM, there is also a state rollback for “out of Gas” and a refund of remaining Gas after successful execution. In response to these situations and some rare boundary use cases, Kalycoin has appropriate processing to ensure the normal and efficient operation of smart contracts.

2.4 x86 Virtual Machine

Based on the strong scalability of the AAL, the Kalycoin Chain can implement multiple virtual machines running in parallel without changing the underlying architecture. Kalycoin is developing a new design Kalycoin x86 virtual machine. The x86 virtual machine uses Von Neumann computer architecture, which means that the code is data, which conforms to the mainstream contemporary programming model.

The basic principles of the x86 virtual machine ensure that it is possible to write smart contracts that run on the Kalycoin blockchain by making simple modifications and using many existing compilers and programming languages. Almost all compilers currently support the x86 architecture instruction set, so the actual bytecode and architecture support is very complete. Kalycoin's x86 virtual machine will support the i686 instruction set and will initially support the Rust language.

Therefore the x86 virtual machine will automatically inherit the support of this upper-level language and development tools so that Kalycoin can get rid of the limitations of EVM computing limitations and Solidity language issues, and can implement features more efficiently, such as variable-length key values, linear memory, and bring real-time on-chain data analysis. The use of x86 virtual machine can also provide developers with more standard libraries. These standard libraries will exist like pre-compiled contracts, and their fees and prices can be managed through

DGP, which will greatly reduce the difficulty of developing smart contracts and development operating costs. In addition to the kernel of the virtual machine, the Kalycoin x86 virtual machine includes the design of a storage lease model and a new state storage model to solve the problem of excessive growth for the blockchain

2.5 Decentralized Governance Protocol

Blockchain communities often split and generate new blockchains through contentious hard forks because of different opinions about the development direction of a project. These different opinions can be roughly divided into three categories: ·Disagreements in the development direction of project algorithms and functions; ·Fix key loopholes and rollback successful attacks; ·Disagreements on certain parameters of the blockchain. The first two must be solved using a hard fork in most cases, but the third type of problem can be solved more gently. DGP's framework is implemented through several smart contracts deployed in the genesis blocks. The basic governance structure is that miners (stakers), developers, and KLC holders within the entire ecosystem are involved in blockchain governance. The process of governance is completed by voting, and the blockchain can realize self-management, upgrades, and iteration. The implementation of DGP core logic is composed of a series of smart contracts (including framework contracts and feature contracts). The Kalycoin nodes contain code that incorporate these smart contract parameters to control Gas pricing and block size. These critical consensus parameters can be modified by the DGP process for an on-chain software update which does not require a hard fork.

2.6 Offline Staking

In the standard Kalycoin PoS system, the nodes participating in staking must stay online, and online stakers improve the security and operations of the network, but this design has limitations for ordinary holders. The offline staking mechanism that Kalycoin is developing can solve the above problems well. Ordinary users can delegate the rights of staking to special online staking nodes, so there is no need to keep their nodes online, and they always have control of their tokens which can be safely held offline and spent at any time.

2.7 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.

3.Governance Mechanism

As a decentralized public chain, for Kalycoin
It is essential to ensure a decentralized blockchain that makes decisions for the benefit of the stakeholders of the project, in order to meet proposed objectives that take into account the participation of both the community and the main development team and investors in order to achieve long-term sustainable development, fulfilling the main purpose of blockchain technology: DECENTRALIZATION.

The Kalycoin governance model includes two main aspects. One is on-chain governance using DGP, the other is off-chain governance, which
established Kalycoin initially, it applies both human governance and public blockchain governance code, thus realizing decentralization of blockchain governance and effective governance decision-making.of blockchain.

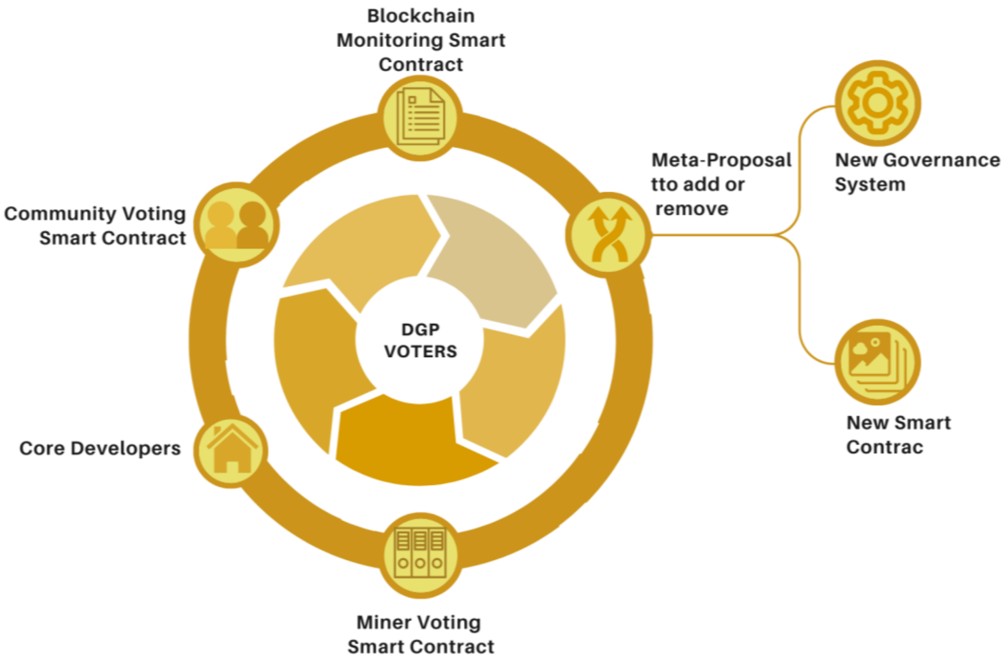
3.1 On-chain Governance Mechanism Based on Decentralized Governance Protocol

On-chain governance is the negotiation and execution process of the blockchain network update protocol embedded in the Kalycoin blockchain system. Kalycoin Chain provides a new on-chain governance model for blockchain networks by the design of DGP.

The core character of DGP is that in addition to allowing KALYCOIN token holders to participate in the voting and negotiation of the upgrade and iteration of the blockchain network, it also introduces a way for other participants in the ecosystem, including developers, community member representatives, miners, and other multi-party participants to propose and vote for on-chain governance proposals.

3.1.2 Smart Contract as the Carrier of On-chain Governance

DGP manages the parameters of the blockchain network through smart contracts embedded in the genesis blocks and clarifies the governance seats and proportion of governance participants for each party. Any participant can initiate a proposal, and the type of proposal includes the increase of management or governance seats, deletion, modification of common network parameters, etc. Participants with governance seats vote on the proposal, decide whether the proposal is approved, and execute the approved proposals through smart contracts.


Blockchain Monitoring Smart Contract
Meta-Proposal tto add or remove
New Governance System
Community Voting Smart Contract
DGP VOTERS
New Smart Contrac
Core Developers
Miner Voting Smart Contract

The on-chain governance mechanism on the DGP is compulsory and automatic. It can realize the automatic upgrade and continuous update iteration of the Kalycoin blockchain system through real-time effective decision-making and execution mechanisms. At the same time, the on-chain governance process is public and transparent, and the process is easy to audit and traceback, which helps to ensure the fairness of the entire governance process and improves decision-making efficiency without worrying about the impact of the soft and hard forks on the network and the community.

3.2 KALYCOIN PROJECT
GOVERNANCE STRUCTURE

The Kalycoin Project governance structure includes operational procedures and rules for daily work and special situations. The organization structure of the Kalycoin Project is as follow

MEET OUR CREATIVE TEAM

The Kalycoin Project governance structure includes operational procedures and rules for daily work and special situations. The organization structure of the Kalycoin Project is as follows:

Abdoulaye

CEO Kalyssi

Responsible for the overall operation of the company and reports to the Board of Directors. Sets the company's strategic vision and is responsible for its execution.

Rafael

CTO Kalyssi

Responsible for the technical direction of a company. Oversee the technology team and make sure that the products and services the company offers are using the latest and most efficient technology.

Hien

COO Kalyssi

Ensure that the daily operation of the company is being carried out in the most efficient and effective way possible. Coordinate and supervise all departments of the company.

Agre

CFO Kalyssi

Responsible for planning, coordinating and controlling all activities related to the economic-financial management of the company.

Boubacar

Legal Manager Kalyssi

Responsible for the management and administration of legal department. They also provide advice and guidance on legal matters to senior managers and directors.

Gbamou

Advisor Kalyssi

Provide support in planning, finance, marketing, and advising organization officials on the appropriateness and overall merits of policies and activities

Andrzej

Blockchain Developer

Development of smart contracts and DApps within the Kalycoin network, in addition to offering long-term sustainable solutions without neglecting network security, prepared for a highly competitive ecosystem.

.

Manda S.

Web & Mobile Development

In charge of web development and mobile applications of Kalycoin blockchain.

.

4. Economic Model

The maximum supply is 125 million coins, and 75 million coins were initially pre-mined.

To protect the interests of investors and ensure the long-term healthy operation of the project, in addition to the regulations on the use of KalyCoins, the Kalycoin Project will allocate its coins to the following areas:

FIVE FACTS

01 Private y Public Sale

02 Founding Team and Development Team

03 Private Investors

04 Business Development

05 Academic Research, Education

KalyCoin will carry out public and private sales to collect part of the initial capital for the medium-term development of the project, a part of the income will be destined to the founding team and development team while during the process a part of the circulating coins will be granted to investors. private.

Throughout the existence of KalyCoin, a part of the funds will be allocated to research and promote the development of applications in the block chain by the community with academic aid and courses taught by Kalycoin developers, which will allow growth appropriate within the industry

4.2 Staking Reward

As mentioned above, the block rewards incentive for stakeholders (miners) is given in three parts: a newly minted KLC subsidy, transaction fees from KLC token transfers, and gas fees for using contracts. smart. In addition to the initially issued tokens, newly minted KLCs with block rewards will be issued.
Initially, the initial block reward subsidy was 14,000 KLC per block, this only during the first 5,000 blocks that formed the premine, from block 5,001 the reward was set at 6.39 Kalycoin coins, therefore, in the first four years (after block 5000), the annual issuance rate (inflation rate) is 0.7% of the total coin supply. With the issuance increasing and block rewards halving, the issuance rate will gradually decrease until there is no further issuance. According to the Kalycoin node code, every 985,500 blocks (for the code, see kalycoin/src/chainparams.cpp), the block reward subsidy will be halved, Calculated at the design block interval of 128 seconds, the Kalycoin block reward will be halved approximately every 4 years with a total of 7 Halvings in which the last coin will be mined for a total of 125,000,000 KLC as max supply.

5. Implementation and Iteration

2021-I

- ✓ KLC deployment on the Binance smart chain
- ✓ Private Sale

2021-II

- ✓ ICO
- ✓ Latoken Listing
- ✓ B2BP2 Listing

2022-I

- ✓ Listing on Coinsbit
- ✓ Listing on Azbit
- ✓ Listing on Whitebit
- ✓ KalyCoin PoS EVM blockchain Design
- ✓ QT wallet

2022-II

✓ Audit

✓ Correction

✓ Audit

2023-I

◉ Migration of KLC BEP20 to KRC20 network

◉ Bounty bug

◉ Mobile wallet

◉ Listing on LBank

◉ Listing on Bitmart

◉ Deployment of DEX KalySwap

◉ Blockchain Update to PoSA consensus

2023-II

◉ Deployment of rebase and collateralized stablecoin on Kalycoin

◉ Deployment of the DAO KANKOU MOUSSA

◉ Listing on the CEX exchange of the KALYSSI group

◉ Deployment of KalySynthex

2024

Coming soon!

CONCLUSIONS

This whitepaper introduces the Kalycoin framework for a smart contract blockchain technology solution, We show Kalycoin's specific implementation of transaction processing that uses proof-of-stake validation. In addition, Kalycoin integrates the Ethereum virtual machine (EVM) along with Bitcoin's unspent transaction outgoing protocol. Please note that Kalycoin EVM is still consistently backward compatible

- In addition, Kalycoin's framework recognises that smart contract lifecycle management is important to support proper security research by collaborating parties. To support Kalycoin's lifecycle management, the current lingua franca Solidity lacks suitability. Consequently, Kalycoin's emerging framework requires a new smart contract language with an improved utility.
- While the non-scalable Ethereum solution does not allow for mobile solutions, Kalycoin aims to achieve democratized and highly distributed proof-of-stake transaction validation with its mobile strategy.

The Kalycoin framework has a clear understanding of the quality criteria that future developments must satisfy. Regarding functional requirements, Kalycoin plans to develop an application layer for smart contract lifecycle management. Most importantly, such lifecycle management is important for investigating collaborating parties to reduce security breaches such as those Ethereum recently experienced, resulting in multiple hardforks of the latter.

The adoption of proof-of-stake in Kalycoin constitutes a considerable saving of computational effort over the Ethereum alternative that still uses proof of work. While Ethereum also plans to adopt proof-of-stake, it's unclear when such a new version will be released.

Also the use of unspent transaction outputs is more scalable compared to Ethereum account management. In combination with simple payment verification, Kalycoin is already developing a

The value transfer protocol for information logistics at Kalycoin comprises a business network model for choreographing several collaborating organizations. The latter can provide services with on-premises contracts that must match the specified runtime behavior of the service type process views in the enterprise network model. With a multi-layered smart contract management layer, collaborating parties protect the privacy of their trade secrets that represent a competitive advantage by hiding extension steps in local contracts.payment verification, Kalycoin is already developing a smart contract mobile device solution.

In summary, the Kalycoin framework recognizes that smart contracts are sociotechnical artifacts that must also take into account the quality requirements essential to achieve widespread adoption by users. Continuous real-life industry projects with Kalycoin applications result in a continuous collection of empirical requirements. The mobile strategy in support of highly distributed proof-of-stake transaction processing points to a significant breakthrough in the state of the art. Still, Kalycoin also recognizes that smart contract lifecycle management requires the development of application layers with a sophisticated front-end user experience that current solutions don't pay enough attention to.

REFERENCES

1. A.M Antonopoulos. Dominating bitcoins, 2014.
2. I. Bentov, A. Gabizon and A. Mizrahi. *Cryptocurrencies without proof of work*, pages 142-157. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
3. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy and S. ZanellaB'eguelin. Formal verification of smart contracts: Short paper. In *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*, PLAS '16, pp. 91-96, New York, NY, USA, 2016. ACM.
4. A. Biryukov and D. Khovratovich. Equihash: Asymmetric proof of work based on the generalized birthday problem. *Minutes of NDSS ˆaA˘Z16, February 21–24, 2016, San Diego, CA, USA ISBN 1-891562-41-X*, 2016.
5. B. Bisping, P.D. Brodmann, T. Jungnickel, C. Rickmann, H. Seidler, A. Stuber,̈ A. Wilhelm-Weidner, K. Peters and U. Nestmann. Mechanical verification of a constructive test for flp. In *International Conference on Interactive Theorem Proving*, pages 107–122. Springer, 2016.
6. O. Bussmann. *The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation*, pp. 473–486. Springer International Publishing, Cham, 2017.
7. C. Cachin. Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016.
8. K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the Internet of Things. *ACCESS IEEE*, 4:2292–2303, 2016.
9. L. Chung, B.A. Nixon, E. Yu and J. Mylopoulos. *Non-functional requirements in software engineering*, volume 5. Springer Science & Business Media, 2012.
10. K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gun Sirer, D. Song and R. Wattenhofer.̈ *On Scaling Decentralized Blockchains*, pages 106–125. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
11. N. Emmadi and H. Narumanchi. Reinforce the immutability of authorized blockchains with keyless signature infrastructure. In *Proceedings of the 18th International Conference on Distributed Computing and Networking*, ICDCN '17, pages 46:1–46:6, New York, NY, USA, 2017. ACM.
12. R. Eshuis, A. Norta, O. Kopp and E. Pitkanen. Outsourcing of services with process views. *IEEE Transactions on Services Computing*, 99(PrePrints):1, 2013.
13. R. Eshuis, A. Norta and R. Roulaux. Evolution of process views. *Information technology and software*, 80:20 – 35, 2016.
14. D. Frey, M.X. Makkes, P.L. Roman, F. Taïani and S. Voulgaris. Bringing secure bitcoin transactions to your smartphone. In *Proceedings of the 15th International Workshop on Adaptive and Reflective Middleware*, ARM 2016, pages 3:1–3:6, New York, NY, USA, 2016. ACM.
15. J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami. Internet of Things (iot): A vision, architectural elements and future directions. *Future Generation Computer Systems*, 29(7):1645 – 1660, 2013.
16. A. Kiayias, I. Konstantinou, A. Russell, B. David and R. Oliynykov. A demonstrably secure proof-of-stake blockchain protocol , 2016.
17. G. Kotonya and I. Sommerville. *Requirements engineering: processes and techniques*. Wiley Publishing, 1998.
18. L. Kutvonen, A. Norta and S. Ruohomaa. Management of commercial transactions between companies in open service ecosystems. In *Enterprise Distributed Object Computing Conference (EDOC), 2012 IEEE 16th International*, pp. 31–40. IEEE, 2012.
19. L. Luu, D.H. Chu, H. Olickel, P. Saxena and A. Hobor. Make smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pp. 254–269, 2016.

20. L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert and P. Saxena. A secure fragmentation protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 17-30, New York, NY, USA, 2016. ACM.
21. J. Marshall. Modeling based on agents of emotional objectives in digital media design projects. *International Journal of People-Oriented Programming (IJPOP),* 3(1):44–59, 2014.
22. Business Process Model. Notation (bpmn) version 2.0. *Object Management Group Specification*, 2011. http://www.bpmn.org.
23. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1(2012):28, 2008.
24. N.C. Narendra, A. Norta, M. Mahunnah, L. Ma and F.M. Maggi. Solid conflict management and resolution for collaborations between virtual companies. *Computing and Service-Oriented Applications*, 10(3):233–251, 2016.
25. A. Norta. *Exploration of dynamic collaboration between inter-organizational business processes*. Doctoral thesis, Eindhoven University of Technology, Department of Information Systems , 2007.
26. A. Norta. *Creation of Smart Contracting Collaborations for Decentralized Autonomous Organizations*, pages 3-17. Springer International Publishing, Cham, 2015.
27. A. Norta. *Establishing Distributed Governance Infrastructures for the Enactment of Collaborations Among Organizations*, pages 24–35. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
28. A. Norta, P. Grefen and N.C Narendra. A reference architecture for the management of dynamic inter-organizational business processes. *Data and Knowledge Engineering*, 91(0):52 – 89, 2014.
29. A. Norta and L. Kutvonen. A cloud hub for business process intermediation as a service: a "meetup" platform that supports the discovery of semi-automated partners with background checks for cross-enterprise collaboration. In *SRII Global Conference (SRII), 2012 Annual*, pp. 293–302, July 2012.
30. A. Norta and L. Kutvonen. A cloud hub for business process intermediation as a service: a "meetup" platform that supports the discovery of semi-automated partners with background checks for cross-enterprise collaboration. *Srii Annual* Global *Conference*, 0:293–302, 2012.
31. A. Norta, L. Ma, Y. Duan, A. Rull, M. Ko˜lvart and K. Taveter. Properties of the choreography and choreography language of eContractual towards business collaboration between organizations. *Journal of Internet Services and Applications*, 6(1):1–23, 2015.
32. A. Norta, A.B. Othman and K. Taveter. Conflict resolution lifecycles for the collaboration of autonomous decentralized governed organizations. In *Proceedings of the 2015 2Nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, EGOSE '15, pp. 244–257, New York, NY, USA, 2015. ACM.
33. Aafaf Ouaddah, Anas Abou Elkalam and Abdellah Ait Ouahman. *Towards a new privacy-preserving access control model based on Blockchain technology in IoT*, pages 523-533. Springer International Publishing, Cham, 2017.
34. E. Paja, A.K. Chopra and P. Giorgini. Specification based on the trust of sociotechnical systems. *Data and Knowledge Engineering*, 87:339 – 353, 2013.
35. J. Poon and T. Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2015.
36. M. Rosenfeld. Overview of colored coins. *White paper, bitcoil. co. il*, 2012.
37. Fr. Sergei. A probabilistic analysis of the nxt forging algorithm. *Ledger*, 1:69–83, 2016.
38. L. Sterling and K. Taveter. *The art of agent-oriented modeling*. MIT Press, 2009.
39. 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.
40. P Vasin. Blackcoinaˆ A˘ Zs proof-of-stake protocol v2, 2014.'
41. 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.

42. M. Vukoli'c. *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*, pages 112-125. Springer International Publishing, Cham, 2016.

43. 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.

44. G. Wood.Ethereum: A decentralized and secure generalized transaction ledger. *Ethereum Yellow Paper* Project, 2014.