ROXE

Roxe Chain Whitepaper

Version 1.0

January 25, 2021

Content

I. Overview

Roxe Chain is a hybrid blockchain which is built for global payments. Roxe Chain is owned by Roxe Chain Foundation (RCF), a fully-decentralized independent organization, dedicated to creating a decentralized, blockchain-native, global payment currency.

Its core objective is to establish a simple, and efficient value transfer mechanism. Roxe Chain intends to bridge the divide between technology and value to achieve an open connection to existing value systems at a low cost.

Roxe Chain has been under development by the Roxe development team since early 2019, as of December 2020, we have completed more than 300 code upgrades.

We strongly believe that the outdated global payments and clearing value transfer system will achieve step-change improvements with the application of blockchain technology.

II. Roxe Chain

2.1.Network Nodes

Supernodes

21 *'Supernodes'* in the network will provide computing power and bandwidth support to ensure efficient operations for the entire Roxe Chain network. The supernode model is extremely valuable to global clearing and settlement, as it enables short block generation time, higher efficiency, and anti-fork attributes. Any organization can apply to be a supernode. Subsequently, each supernode will benefit from continued Roxe Chain ecosystem development.

Candidate nodes

In addition to supernodes, Roxe Chain anticipates having hundreds of candidate nodes. If a supernode is downgraded (unable to perform its obligations as a supernode on time), the top-ranked candidate node, determined by community voting, will step in. The upgraded candidate nodes will take over all the obligations, rights and interests of the downgraded supernodes.

2.2. High Concurrency

Graphene technology

Roxe Chain is a blockchain architecture based on open-source Graphene technology, which is written primarily in C++. Graphene technology meets the needs of vertical decentralized applications and horizontal expansion through its plug-in structure, and is based on a BFT-DPoS (Byzantine Fault Tolerance-Delegated Proof of Stake) consensus plugin and sharding.

Roxe Chain solves the problems of low performance, poor security, high development challenges, and difficult cross-chain communication in existing blockchain applications. Roxe Chain helps distributed value transfer applications maximize their performance potential.

Meanwhile, since Roxe focuses on payment and settlement services, it adopts closed smart contracts and provides corresponding clearing protocols and middleware components to enable various nodes to access Roxe easily and quickly.

2.3. Consensus Algorithm

2.3.1. aBFT-DPoS consensus

Roxe Chain is designed to achieve confirmation of irreversibility within one second using the aBFT-DPoS (asynchronous Byzantine Fault Tolerance-Delegated Proof of Stake) consensus to achieve faster irreversibility.

By adding a Byzantine Fault Tolerance algorithm to the traditional DPoS algorithm, all block producers must sign on all blocks to ensure no block producer is at the same timestamp or sign two blocks on the same block height at the same time. A block that is signed by two-thirds of the block producers is considered irreversible. Any Byzantine block producer who wants to sign two blocks at the same timestamp or on the same block height will leave cryptographic evidence. In this mode, an irreversible consensus can be reached within one second.

The asynchronous assumption-based aBFT algorithm is not dependent upon the synchronization-based assumptions practical Byzantine Fault-Tolerant algorithm PBFT, improving performance, making it more practical.

2.3.2. Transaction as Proof of Stake (TaPoS)

Unlike the underlying data structure of other blockchains, in which the latter block contains the hash of the previous block to form the blockchain, TaPos (Transaction as Proof of Stake) requires that all transactions must contain the hash of the most recent block header. This hash has two purposes:

1. Prevent replay of transactions on the blockchain fork, and these transactions do not include reference blocks;
2. Notify the blockchain network that a user and its stake are on a specific fork.

Over time, all users can directly confirm the blockchain, which makes it difficult for counterfeit chains to forge because counterfeit chains cannot transfer transactions from legitimate chains, thus preventing the verifier from maliciously operating on other chains.

2.4. High Throughput

Graphene technology

The bottom layer of Roxe Chain is based on Graphene technology. It is a blockchain tool kit. At present, the Graphene blockchain library has been adopted by many well-known blockchain projects.

Graphene has the features of fast transfer speed and high throughput. It is stable, powerful, complete, and easy to operate.

Region technology

Region technology, same as the sharding technology, is a parallel computing technology. Region technology does not run in parallel within the application. Instead, it extends the network through the cross-chain concurrency technology of the sharding chain, and through the asynchronous communication to separate the authentication and execution processes.

All transactions are separated by region numbers to form a partition chain. Each partition chain is single-threaded, and multiple partition chains can be run concurrently on a node to fully utilize the performance of each node. The performance upper limit of a single node can be expanded through clustering to achieve a high-throughput and highly scalable underlying architecture.

2.5. High Security

Supernode and transparent forging

The tradeoff between transaction speed and data security on the blockchain has been a problem since the early stages of digital assets. If block confirmation speed is too fast, this can cause double payment (double-spending problem), resulting in insecure blockchain transaction data. Through the transparent forging mechanism, the nodes of the entire network confirm the bookkeeper (supernode) in advance, saving the time of searching for miners, thereby increasing the speed of block transactions and ensuring the security of transactions.

Roxe Chain plans to utilize 21 supernodes. The block generation orders for supernodes and the auditing orders for all network transactions are all automatically calculated by the system and irregularly changed so that they can be efficiently upgraded while preventing corruption and avoiding hard forks.

Ownership model to defeat DoS attacks

DoS attacks (Denial-of-service attack) occurs when malicious attackers send a large volume of spam traffic to the network, which causes the network to be paralyzed and unable to process legitimate requests. At present, some networks have been vulnerable to DoS attacks. In comparison, Roxe Chain is less vulnerable to DoS attacks due to the ownership model.

Network bandwidth, storage space, and computing power will be allocated in proportion to the number of platform tokens held by users. Therefore, malicious attackers have to consume the corresponding proportion of network resources held by platform tokens without disrupting the entire network. Even if many malicious agents try to create junk congestion for several large-scale network applications, this approach will ensure the bandwidth reliability and computing power of small-scale startup investment projects on the network.

Node acceptance mechanism

Roxe Chain will use a permissioned-public hybrid network, but there are currently no plans to adopt a *fully* open network approach. Acceptance mechanisms will be implemented for supernodes, candidate nodes, and cross-chain gateways. Nodes must comply with the mandatory security control standards of the Roxe Protocol. Only those who pass the screening can access and enable the node. At the same time, the node also needs to set an IP whitelist and visit policy to limit the direction and path of communication within the network to ensure maximum security within the chain.

2.6. High Scalability

Plug-in

Roxe Chain uses the Graphene code base as its foundational architecture and implements a flexible modular plug-in mechanism. A layer of template classes is inserted between the abstract plug-in class and the specific function class to decouple

the inter-plugin dependent calls from the specific function class. This is conducive to the cohesion of plug-in functions and the expansion of new plug-ins.

The plug-in-designed Roxe Chain is highly decoupled, and the function modules can be independently developed and combined freely as needed. At the same time, a variety of functional middleware plug-ins and components based on Roxe Chain will be launched in succession.

Smart Contract

Roxe Chain smart contract uses Web Assembly (WASM). Web Assembly is an emerging and high-performance virtual machine. It has an LLVM compilation backend and is compatible with all programs written in high-level languages such as C, C ++, and Java. The learning cost for developers is low.

At the same time, WASM byte code is flexible, which can be compiled into machine code for execution or can be directly executed using an interpreter, with both compatibility and performance. The advantage of compilation execution is that its execution speed is fast. However, the disadvantage is that every time the smart contract is updated, the witness' server must recompile to generate binary machine code, which is generally used for deterministic smart contracts that are executed multiple times. The interpretation and execution are just the opposite in that no pre-compilation is required, but the execution speed is much lower than that of compilation and execution. It is generally used for debugging or temporary smart contracts.

Independent architecture of virtual machine

Roxe Chain is built with a virtual machine independent architecture and supports multiple virtual machine sandbox operations. Any virtual machine that meets the conditions of performance, certainty, correctness, and sandboxing can be connected. In addition to Web Assembly, it also supports the Ethereum Virtual Machine (EVM) that runs on existing Ethereum contracts.

Based on the EVM, any smart contracts on Ethereum can run on the Roxe Chain, with minor modifications. Also, projects on Ethereum can be smoothly migrated to the Roxe Chain.

2.7. Account System

Easy-to-use account system

With *Accounts*, a readable account system, 1 to 12 human-readable characters can be used to create an account. The name is chosen by the account creator. The account creator must purchase RAM space for storing new account data and collateralize tokens to get CPU and Net bandwidth. More data to store, more RAM needed. After use, RAM could be released and sold.

Permission management based on roles

Roxe Chain provides an Assertion permission management system that allows accounts to exercise both highly granular and high-level control. Identity authentication and permission management are standardized and isolated from the application business logic so that permissions can be managed without impacting adjacent systems while providing performance optimization capabilities.

Roxe Chain also supports multi-account control, which provides account security and reduces hacker attack risk. Through named message processing groups, it is even allowed to define what types of secret keys or accounts can send a specific message type to another account. Named message processing groups can be referenced when other accounts configure permission levels. Mapping can be completed between permission levels and message processing groups: Assign a message processing group to a certain permission level, or conversely, define various message processing groups at certain permission levels.

The default permission groups are Owner and Active. Owner can do anything and is generally used for cold backup. If Active permission is lost, Owner permission can be used to restore that permission. Active permissions can do everything except modify the Owner. Routine business can be handled with Active permission. All other permission groups are also derived from Active permissions.

Secret Key Recovery

Roxe Chain provides a secret key recovery mechanism if an account balance becomes zero after the private key is stolen or the password is forgotten.

On other chains, when the secret key is lost, the entire account is also lost. However, the secret key recovery mechanism based on Roxe Chain can recover the key using any Owner permission key and a designated partner within 30 days. In this case, the partner cannot recover the key without the assistance of the owner, and the partner will not participate in any daily transaction.

Roxe Chain protects account assets through a safe combination of accounts, key-pairs, wallets, and authorities & permissions.

2.8. Cross-chain

Cross-chain communication

Roxe Chain simplifies the generation of Proof of Action existence and Proof of Action sequence to promote cross-chain interaction on blockchains. These proofs are combined with the application architecture designed around message passing, which hides the details of cross-chain communication and verification proofs from the application developers. Developers are only presented with high-level abstractions.

Merkle proof

Roxe Chain uses the "Merkle proof" as Proof of Action verification to achieve blockchain interaction. The Merkle tree is also called a hash tree, for which any changes in the underlying data will be passed to its parent node to the root of the tree. The use of Merkle Proof for Light Client Verification (LCV) is to produce a relatively lightweight proof of transaction existence; this can verify the proof by tracking a lightweight data set, that is to prove a specific transaction is included in a specific block, and this block is included in the history of the specific blockchain that has been verified.

SegWit

SegWit (Segregated Witness) means that, after the irreversible inclusion of a transaction in the blockchain, the signature of the transaction is no longer relevant.

Once the transaction is tamper-proof, the signature data can be cut off, and everyone else can reach the current state. Since signature data occupies a large part of most transactions, SegWit can significantly reduce disk usage and synchronization time.

The same concept can be used in Merkle Proof in cross-chain communication. Once a proof is accepted and irreversibly recorded on the blockchain, the 2kb file of the sha256 hash, used as a proof is no longer needed to reach the correct blockchain status.

2.9. Special Network

Closed smart contract

To maintain business efficiency and speed while ensuring the purity and security of Chain, Roxe Chain does not support open smart contracts, and all basic services are supported by the accepted nodes and chain modules.

Based on the ecosystem development plan and the Roxe Chain business requirements, corresponding smart contracts will be released to the Roxe Chain only after they have been approved by the Foundation’s management committee, and all contracts on the chain should undergo security audits.

2.10. Trust mechanism

Within Roxe, settlement nodes follow the Roxe Protocol to audit the asset mapping request. Meanwhile, Roxe not only provides technical capabilities, but it also contains a series of authorization mechanisms to ensure all business of authorized nodes will be periodically reviewed. If nodes fail the review, Roxe Chain will initiate a credit adjustment as an incentive mechanism for nodes.

Distributed Depository Mechanism

The distributed depository mechanism is the basic service of Rox. All mapped currencies will be escrowed into the distributed escrowed-asset pool and managed by

the corresponding settlement node. It accepts triple layers of supervision from other nodes, Roxe Chain, and audit institutions.

Unified KYC and Fast Verification

Each node will have KYC (Know Your Customer) requirements, with requirements varying based on the region. At the same time, Roxe Chain will also recognize the behavior of the same user in different nodes, share security information among nodes while adhering to relevant privacy considerations, and maintain blacklists. Roxe Chain will also build a self-learning trading mode detection based on user behaviors, which can identify and prevent suspicious fraudulent activities.

Roxe Protocol

The Foundation uses the Roxe Protocol to manage complex asset networks and value transfer relationships. Roxe Protocol formats the processes and data for each type of asset conversion business and unifies the exchange of data messages on each business functional interface, facilitating the connection of each functional module.

Roxe Middleware

In addition to the Roxe protocol, Roxe also provides nodes with secure Roxe middleware components to quickly access settlement nodes. Roxe middleware is a set of infrastructure components based on the Roxe Protocol, including: asset registration, rapid mapping, hot and cold wallets, smart contracts, security authorization, node verification, credit fast settlement, asset access, and auditing. The nodes can be used in combination according to the access method, and services type.

Roxe Chain can also be used as a storage infrastructure. The fast open ledger can perform functions such as high concurrent throughput, and fast transaction confirmation at low costs.

Clearing Protocol

XMoney Fast Clearing Protocol

The XMoney Protocol is a fast-clearing protocol on Roxe Chain.

Since nodes often provide clearing for the same user (i.e., user transfers between exchanges), to improve the efficiency of clearing between nodes and the speed of funds transfer between different nodes of the same customer, nodes with XMoney Protocol can accelerate the instant clearing of assets.

The XMoney Protocol has formulated various execution scenarios and specifications under fast clearing. At the same time, authorized nodes have priority clearing rights and fast pre-settlement privileges.

Executing the same settlement protocol helps regulate the settlement agreement between nodes, reducing the difficulty of communication between new nodes and existing nodes, thus making the settlement between nodes faster, clearer, and more standardized.

III. Cross-Chain Gateway RSS

RSS (Roxe Settlement Service) is an important part of the Roxe Chain.

3.1. Cross-Chain Asset Mapping

Roxe will use both sub-chain and side-chain technology to achieve cross-chain transactions, and cross-chain asset mapping, solving the technical limitations of isolated and fragmented main chains and gradually realizing a truly, decentralized mapping technology.

The main chain creates sub-chains by logic, and these sub-chains share supernode computing resources and interact through a cross-chain mechanism. Each adaptive sub-chain is connected by the cross-chain main chain. There is no trust relationship between sub-chains, but the trust is passed through the main chain. The adaptive

sub-chains and the main chain interact according to a protocol, for the purpose of trust transfer and transaction transfer.

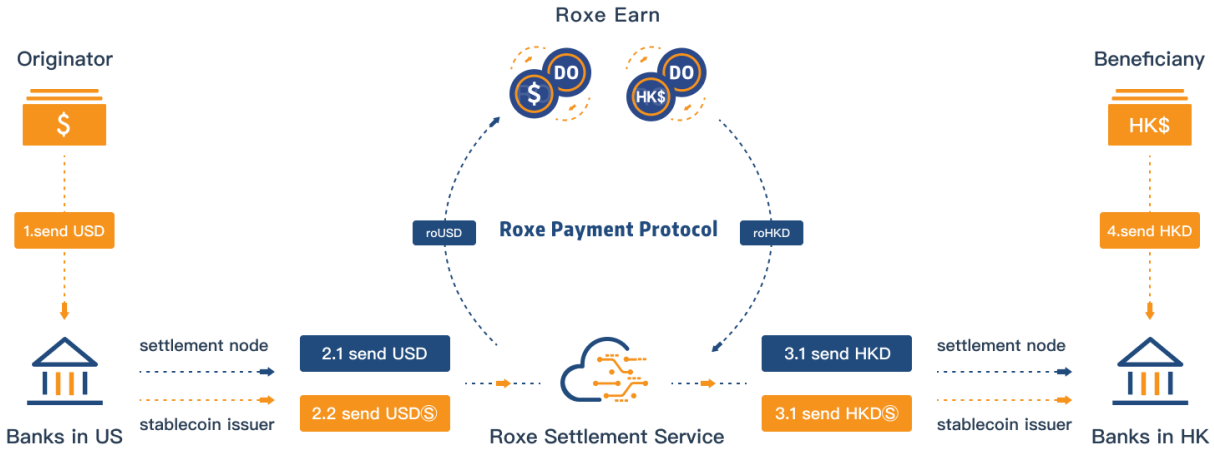
The side chain is an independent chain directly initiated by the Roxe Chain source code. Similar to a hard fork, the side chain can have its own committee, computing resources, and tokens. The side chain is based on anchoring some tokens on the original chain, verifying data from other block chains, enabling assets to be transferred between different blockchains to form a new open platform. An example is a sidechain that can create micropayment channels under the main chain.
Roxe will continue to improve the application of cross-chain technology on different platforms to decentralize the custody mapping of more assets and provide a more secure, reliable and trustworthy infrastructure for asset custody.

3.2. Digitize Fiat Currency On-chain

RSS provides a platform to digitize domestic fiat currency. By opening a collateral account with a bank, fiat in the bank account is mapped 1:1 to the Roxe Chain to form a Roxe Smart Ownership called roFIAT (e.g., roUSD, roEUR, etc). That can be freely transferred on the chain.

Through RSS, the minting and redemption of roFIAT can be done in real time.
The following criteria are followed when digitizing fiat on-chain:

- 1:1 Full Asset Anchoring
- Real-time Minting and Redemption
- Real-time disclosure of on-chain mapped fiat data and bank account balance
- Read the audit through a trusted auditor
- The collateral bank or trust company is compliant with applicable regulations



IV. ROC

The ROC is a utility token issued by Roxe Chain Foundation, the fuel for the operation of the Roxe Chain and is the only token used to generate the DO series stablecoin and the ecosystem token for the Roxe Payment Network.

Roxe's digital utility token, Roxe Cash (ROC), is a transferable representation of the attribute functions specified in the Roxe code/protocol and is intended to play a primary role in the operation of the Roxe Chain ecosystem and to be used only as the primary utility token on the network.

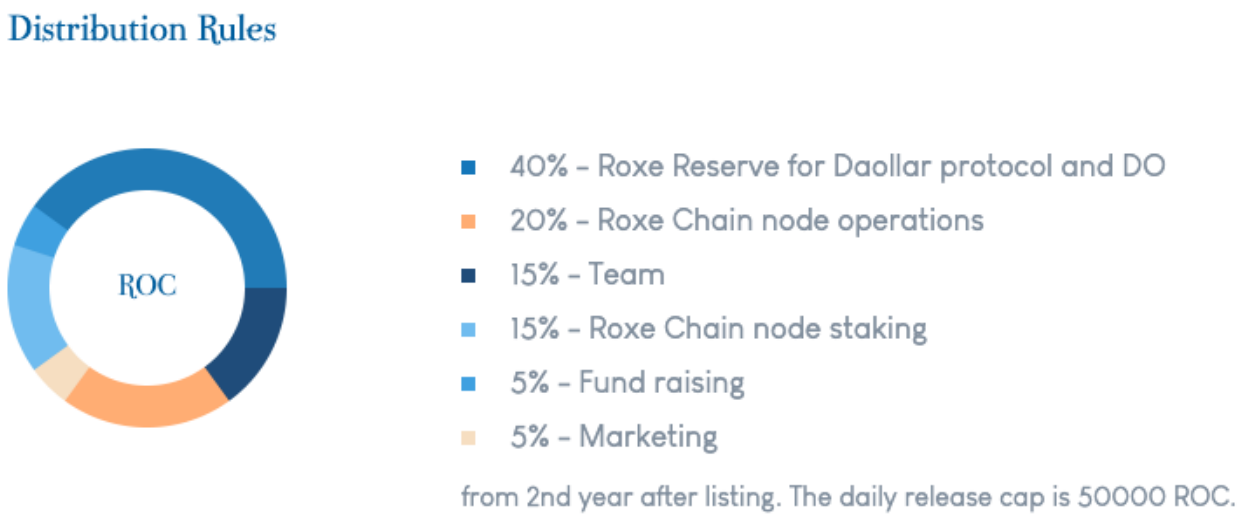
4.1 ROC Issuance

ROC is a token embedded into smart contracts. 90% of ROC are sold decentralized through smart contracts.

There is no cap on the total issuance amount. A total of 100 million will be issued in the first four years. Starting from the fifth year, the community which based on the market supply and demand, will vote to decide whether to issue additional ROC and how much

additional to be issued.

ROC is distributed as following:



V. Roadmap

Q4 2019

- Roxe Chain V1 goes live on Test Net.
- Supernode collaboration on Test Net started.

Q2 2020

- Roxe Chain V2 goes live on Test Net.
- RSS (Roxe Settlement Service) V1 goes live.

Q3 2020

- Roxe Chain V3 goes live on Test Net.
- Four Super nodes access the Roxe Chain.

Q4 2020

- Roxe Chain V1 goes live on Main Net.
- RSS(Roxe Settlement Service) and RCP(Roxe currency platform) V2 iterations go live.
- The blockchain explorer V1 goes live on Roxe.tech
- Roxe decentralized wallet web version V1 goes live.

Q2 2021

- Daollar protocol implemented

- Ruby product implemented
- The blockchain explorer V2 goes live on Roxe.tech
- Completion of 21 supernode implementation

Q4 2021

- Roxe Chain V2 goes live on Main Net.
- Finish 100 candidate nodes implementation
- The blockchain explorer V3 goes live on Roxe.tech
- More strategic partner implemented

Q4 2022

- Roxe Chain V3 goes live on Main Net.
- Number of supernodes and candidate nodes reach 50 countries and regions worldwide.

Q4 2023

- Subsequent iterations of Roxe Instant Settlement Network and related blockchain products to improve the performance and security of the new products.

For more information, please visit: www.roxe.tech