LIBRE CHAIN WHITE PAPER

Privacy Chain Project Based on Proof of Behavior Consensus Mechanism

and Dual-Channel Digital Asset Management Technology

[Technical White Paper — 2nd Edition — Revision 2]

October 29, 2021 - LibreChain Team www.libre.gold

Introduction

Blockchain technology, represented by Bitcoin and Ethereum, and the cryptocurrency ecosystem built upon it, have significantly altered and, to some extent, shaken the traditional financial landscape. However, the contradictions and conflicts between the decentralized new financial order operating on the Web3 architecture and the traditional centralized financial order have made it a formidable task to create a truly decentralized digital living space that is free, fair, and secure for the majority of people. Currently, most information, actions, and assets on blockchain public chains are publicly visible. This includes not only financial transactions but also ENS domains, POAP (Proof of Attendance Protocol), NFTs, and SBTs (Soulbound Tokens). If we want to know what tokens a particular wallet address has traded, what NFTs it has minted, or how many assets it owns in total, we can use blockchain explorers like Etherscan to grasp all the historical activities of a wallet address within minutes.

Such a mechanism has indeed greatly increased information transparency, allowing users to personally verify the asset ratios and financial flows of projects and institutions without the intervention of third parties, thus avoiding potential losses due to undisclosed information in other financial markets, and it has many practical applications in real scenarios. However, with the development of blockchain technology and applications, the connectivity between wallet addresses and user identities is gradually strengthening, and the probability of tracing back from seemingly anonymous wallet addresses to the individual is increasing. This not only raises issues of personal information abuse akin to Web2 but also poses concerns for personal safety. If the ultimate goal of Web3 is mass adoption, this mandatory public disclosure of all personal information, laying it bare for anyone to view, analyze, and use, will be a significant hindrance.

Therefore, enhancing blockchain privacy and security has become a consensus among many users and developers in recent years, recognizing the need for improvement. The emergence of the Libre privacy chain will provide extremely important exploratory experience for society's entry into a truly digital existence in the future.

The PoB consensus algorithm proposed in this paper, along with the dual-channel digital asset privacy management technology built on this consensus mechanism, represents a completely new architecture. It avoids the high energy consumption drawbacks of the PoW (Proof of Work) mechanism and also prevents the Nothing at Stake attacks and centralization risks associated with PoS (Proof of Stake). The PoB mechanism is based on blockchain-based distributed server cluster

technology (Libre chain + edge cloud), providing hardware-level protection for data assets running on the Libre public chain through a more thorough decentralized distributed node server cluster technology, with strong anti-censorship capabilities, greatly ensuring user information and asset security. At the same time, on the software application level, the dual-channel digital asset privacy management technology pioneered by the Libre chain can ensure that the main currency of the Libre chain, the Libre coin, can meet EVM standards and traditional transparency regulatory requirements, allowing it to be traded on global mainstream digital currency exchanges that comply with KYC requirements. Moreover, by upgrading traditional privacy coin and privacy chain privacy protection technologies, Libre has successfully developed the NFTpay super wallet tool, significantly enhancing the privacy and security of digital assets, providing a reliable solution for transactions that require greater security.

The Libre chain can help users quickly create, manage, and maintain enterprise-level blockchain networks and commercial blockchain applications while ensuring absolute privacy and security. It features low development costs, fast deployment, high performance, strong scalability, and reliability, ease of use, and constructs a distrustful, highly reliable, highly available, tamper-proof, and highly private information interaction system through its unique consensus algorithm, cryptographic technology, distributed data storage, and distributed node cloud computing.

I. Project Background

The development pattern of human society follows a cyclical iterative development law of "decentralization—centralization—decentralization." As the core concept of blockchain technology, "decentralization" has always developed in opposition to the centralized model of the traditional camp. Traditional interest camps are not likely to easily relinquish control over vested interests. Although blockchain technology, represented by digital currencies, has achieved decentralization in many aspects, the centralized nature of mainstream digital currency operation and management platforms such as exchanges, mining pools, and wallets still poses many risks to the entire blockchain ecosystem: trading risks due to information asymmetry between unregulated exchanges and users; regulatory risks for projects in certain countries or regions. Even the transparency of information on digital currency chains is increasing the uncertainty of personal digital asset security. To change this phenomenon and ensure "my assets are under my control" to the greatest extent, Libre team is determined to create a decentralized ecosystem that serves the digital living needs of future human

society, embodying the principles of "governed by the people, owned by the people, and enjoyed by the people." Starting from the blockchain architecture and the underlying internet technology, the team focuses on fully decentralized blockchain application scenarios and upgrades existing blockchain technology in consensus mechanisms, smart contracts, scalability, privacy and security, cross-chain interaction, and fair trading, anti-regulation, and other aspects. They have launched the Libre Chain (Libre means freedom in French), a groundbreaking and imaginative independent new public chain project that represents the core values of the future Web3 era—freedom, fairness, happiness, health, and joy (L: libre; I: impartiality; B: bliss; R: robust; E: enjoy).

II. Technical Features

Traditional blockchain technology, represented by Bitcoin, has many hard-coded limitations, some of which are natural elements of the original design (such as block frequency, maximum currency supply, confirmation number, etc.). A typical example of catastrophic consequences due to hard-coded limit changes is the block data size limit set to 250kb, which results in Bitcoin's script system being a heavy and complex function. Although it allows for the creation of complex transactions, some of its functions are disabled due to security issues, and some are not even used. The most popular Bitcoin transaction script (including two parts for the sender and the receiver) looks like this: OP DUP OP HASH160 OP EQUALVERIFY OP CHECKSIG. This script is 164 bytes long, and its only purpose is to check whether the receiver has the key required to verify their signature.

Libre Chain proposes a more secure and private fully anonymous transaction scheme that meets non-standard and irrelevant conditions. An important feature of the solution proposed by Libre Chain is its autonomy: the sender does not need to cooperate with other users or trusted third parties to conduct transactions. This solution allows users to publish a single address and receive unconditional unlinkable payments. The destination of each transaction output on the Libre Chain (by default) is a public key derived from the recipient's address and the sender's random data, leaving no trace in the process. A simple understanding of this transaction is like A taking cash to a casino and exchanging it anonymously for chips, then giving the chips to B, who then exchanges the chips anonymously for cash in the casino. In this process, there is no transaction trace recorded between A and B.

Librechain is the first highly scalable public blockchain that integrates the advantages of existing mainstream consensus algorithms and avoids their shortcomings by introducing a unique Proof of Behavior (PoB) consensus algorithm. It combines the security of Proof of Work algorithms, the

convenience of Proof of Stake algorithms, and the efficiency of Proof of Authority algorithms to achieve VISA-level throughput and confirmation times in seconds.

Libre Chain is a fully decentralized open information interaction platform. Through open, autonomously joinable libre chain + edge cloud server cluster technology, it ensures data and asset privacy and security while achieving the robustness of the entire system, with strong risk resistance capabilities. Libre Chain can not only connect every terminal as an untraceable user to the network but also redefine numerous terminals (especially PCs and mobile terminals) as distributed cloud computing modules, and then reorganize them into a virtual cloud server, ensuring that all data on the Libre cloud server is completely decentralized. On the Libre cloud server, there will eventually be no traditional fixed, physical servers.

Libre Chain will eventually use special virtual tunnel technology to turn every terminal device loaded with Libre applications (PCs, PADs, mobile phones, routers, or even digital home appliances) into a standard computing unit in the distributed nodes. On the Libre Chain, every resource user is also a provider and maintainer of resources. By establishing an open, secure, decentralized Web3 platform with blockchain technology, and through applications such as social networking, gaming, e-commerce, and lifestyle services, a complete Libre metaverse ecosystem will gradually be established, ultimately building a decentralized "governed by the people, owned by the people, and enjoyed by the people" ecosystem for future digital living.

The construction of the Libre Chain depends on the number of terminals using Libre applications and the topological servers formed by these terminals. When the number of online terminals reaches a certain scale, numerous topological servers will naturally evolve on the Libre Chain; the number of network terminals composing each topological server is generally between 0.1K-10K. Each topological server, as a service node on the Libre Chain, provides distributed storage and computing services for applications on the Libre Chain. As contributors to the node servers, they will receive dividend rewards from various applications running on the node servers!

To support the operation of the project and to express the concept that the Libre Chain is a future digital asset that all human members deserve to have without discrimination, the founding team will issue a total of 7.6 billion Librepoints (basic points) through the Libre Chain, of which the first 100 million will be rewarded to the first phase of up to 100,000 seed miners entering the Libre Chain through a specific algorithm within half a year. The remaining 7.5 billion Librepoints will be issued

over approximately 50 years by gradually reducing the block rate (the block rate varies according to the health of different nodes' topological servers). All produced basic points (tokens) can be freely converted into basic coins (libregold) through the health of users on the chain (activity + contribution). Basic coins are digital assets that can be used across platforms supporting the libre protocol. Users can choose to use basic coins directly for consumption or map them into digital assets that comply with the EVM standard for compliant trading on mainstream digital trading platforms. The mapping method will vary depending on the mapping path; if the basic coins are obtained from the social end, they will be affected by health and mapping limits; if the basic coins are obtained from mining machines, they will not be affected by health and mapping limits. As for the mapping ratio, it will be determined based on whether the project development requires expansion or splitting.

III. Privacy and Security Solution

Compared to various complex privacy services, the concept of stealth addresses is relatively straightforward, developing with the core idea of hiding the recipient. For example: Suppose Tom wants to transfer assets to Jack, which could be a certain amount of cryptocurrency (e.g., 1ETH, 500 RAI) or an NFT. However, if Jack does not want the whole world to know that he is the recipient of this transaction, he could consider creating a stealth address with Alice to complete the transaction. The specific process is as follows:

- Jack generates his root spending secret key \(m \), and the stealth meta-address \(M \).
- Jack adds an ENS record, registering \(M \) as the stealth meta-address for Jack.eth.
- Assuming Alice knows that Jack is Jack.eth, Alice looks up Jack's stealth meta-address \(M \) on ENS.
- Alice generates a temporary key known only to her, using it once to generate this specific stealth address.
- Alice uses an algorithm to combine her temporary key with Jack's stealth meta-address to generate a stealth address. She can now send assets to this stealth address.
- Alice also generates her temporary public key and publishes it to the temporary public key registry (this can be done in conjunction with the first transaction that sends assets to the stealth address).
- To find the stealth address that belongs to him, Jack needs to scan the temporary public key registry to find the entire list of temporary public keys that anyone has published for any reason since the last scan.

- For each temporary public key, Jack attempts to combine it with his root spending secret key to generate a stealth address and checks if there are any assets in that address. If there are, Jack calculates the spending key for that address and remembers it.
- The assets within the stealth address can only be controlled by Jack.

It can be seen that stealth addresses are one-time wallet addresses that can give Jack ownership of the assets without exposing any of Jack's wallet addresses and user identities. Stealth addresses enable the recipient of the transaction to remain anonymous, thereby preventing any public connection between the sender and receiver's identities on the blockchain.

In addition, the network of the Libre chain is divided into smaller units called virtual sectors (referred to as sectors). An algorithm assigns eligible validators to sectors, ensuring that nodes are evenly distributed among sectors, depending on the tree level. Each sector contains a randomly selected consensus group. Any block proposer is responsible for aggregating transactions into a new block. Validators are responsible for rejecting or approving the proposed block, thereby validating it and submitting it to the blockchain.

1. Internal Tokens

Libre chain grants access to its network through two types of tokens. All fees for processing transactions, running smart contracts, and various contributions to the network on the Libre chain will be paid in libregold. In the EVM environment, the mapped token of libregold, libre coin, serves as the payment voucher.

2. Threat Model

Libre chain assumes a Byzantine adversary model. The protocol allows for the existence of adversaries who may hold shares or have good ratings, delay or send conflicting messages, sabotage other nodes, have faults, or collude with each other. However, as long as there is one eligible validator in a virtual sector that is honest/uncompromised, the protocol can reach consensus. The protocol assumes that adversaries are highly adaptive, but their adaptation speed cannot exceed the time range of one round. The computing power and resources of adversaries are limited. It is assumed that the honest node network forms a well-connected graph, and their message propagation has been completed within a finite time to prevent attack vectors.

IV. Technical Traceability

The design of Libre chain is inspired by mature technologies such as ETH, Omniledger, Zilliqa,

Algorand, IPFS, and Monero. Our architectural design has undergone significant technical upgrades, which can be seen as an enhancement of existing models, focusing on achieving a better balance between security, scalability, and decentralization while improving performance.

ETH (Ethereum)

The success of Ethereum can be largely attributed to the introduction of its decentralized application layer through the EVM, Solidity, and Web3. Although Dapps have always been one of the core functions of Ethereum, scalability has proven to be an urgent limitation. A significant amount of research has been invested to address this issue, but so far, the results have been negligible. Compared to Ethereum, Libre chain addresses the high energy consumption drawback of the PoW proof-of-work consensus algorithm and the low barrier to entry 导致的 project deforestation defect of the PoS proof-of-stake consensus algorithm by implementing PoB consensus and using transaction processing parallelism through virtual sectors.

Omniledger

Omniledger proposes a novel horizontally scalable distributed ledger that maintains long-term security under permissionless operation. It ensures security and correctness by using a bias-resistant public randomness protocol to select large, statistically representative virtual sectors to process transactions. To perform transactions atomically across virtual sectors, Omniledger introduced Atomix, an efficient cross-virtual sector commit protocol. This concept is a two-stage client-driven "lock/unlock" protocol that ensures nodes can fully commit transactions across virtual sectors or obtain a "rejection proof" to abort and unlock the state affected by partially completed transactions. Omniledger also optimizes performance by parallel transaction processing within virtual sectors, ledger pruning through collective signature state blocks, and low-latency "trust but verify" verification for low-value transactions. The consensus used in Omniledger is a BFT variant called ByzCoinX, which improves performance and robustness against DoS attacks.

Compared to Omniledger, Libre chain's consensus group is randomly selected more quickly and enhances security by replacing the set of validators after each round (10-30 seconds) instead of every epoch (1 day).

Zilliqa

Zilliqa allows the mining network to process transactions in parallel and achieves high throughput by dividing the mining network into shards. Specifically, its design allows for a higher

transaction rate as more nodes join the network. The key is to ensure that each shard processes different transactions without overlap, thus preventing double spending. Zilliqa uses pBFT for consensus and PoW to establish identity and prevent Sybil attacks.

Compared to Zilliqa, Libre chain's goal is not only EVM compliance but also to maximize the privacy and security of user assets held on the libre chain, especially as a third-party asset security management tool, providing highly private and secure traceless transaction services.

Algorand

Algorand proposes a public ledger that maintains the convenience and efficiency of centralized systems without the inefficiencies and weaknesses of current decentralized implementations. Leaders and validator sets are randomly selected based on the number of signatures applied to the last block. These selections are unmanipulable and unpredictable until the last moment. Consensus relies on a novel message-passing Byzantine agreement that allows the community and protocol to evolve without hard forks. Compared to Algorand, Libre chain is not a single blockchain but provides a dual-channel model of libregold + libre to achieve asset privacy and compliant transactions through its own independent public chain + EVM open protocol technology.

IPFS (InterPlanetary File System)

IPFS (InterPlanetary File System) is a file storage and content distribution network protocol that combines existing successful systems such as distributed hash tables, BitTorrent, version control systems like Git, self-certified file systems, and blockchain.

IPFS has the following advantages:

1. Decentralization and distributed storage: IPFS uses distributed hash tables (DHT) and content addressing, with each file uniquely identified by the hash value of its content. This design ensures the uniqueness and verifiability of files and improves the network's resistance to attacks and scalability.

2. Efficient content distribution: IPFS communicates peer-to-peer through nodes in the network, which can cache accessed file content, reducing redundant transmissions and improving network performance. Additionally, IPFS can be used as a CDN, with hot data having copies around the world, allowing users to pull content based on content addressing and proximity, increasing the efficiency of content distribution.

3. Economic incentive system: Filecoin is an incentive layer running on IPFS, where miners earn rewards by providing storage and retrieval services. This economic model encourages nodes to

provide stable storage and bandwidth services, forming a large-scale decentralized network.

However, IPFS currently has the following disadvantages:

1. Node stability and security issues: Since IPFS nodes are primarily contributed by home users with storage and bandwidth, these nodes are less stable, and home bandwidth has slower upstream speeds. Additionally, the lack of economic incentives may lead to malicious nodes being easily attacked. Although IPFS uses complex identity and reputation mechanisms, there are still security risks.

2. Technical implementation complexity: IPFS splits files into data blocks and organizes these blocks using Merkle DAG, which improves file reliability and verifiability but also increases technical implementation complexity, potentially leading to slower file download speeds.

3. User experience issues: Due to the low efficiency of DHT retrieval and node instability, users may not expect efficient and stable file services. Moreover, large files split into multiple data blocks may affect download speed and integrity if some nodes are offline.

Libre chain has undergone significant upgrades based on IPFS, deploying a large number of distributed micro-node servers (mining machines) to build a blockchain-based edge cloud platform. By developing its own PoB social behavior consensus algorithm, it addresses the economic incentive issues and potential security issues of IPFS. At the same time, through ecological competition, naturally evolved nodes at different levels (super nodes, standard nodes, micro nodes) can better achieve data redundancy and load balancing for chain users during access, ensuring efficiency and stability when accessing data.

Monero

Monero's core advantage lies in its high level of privacy protection and security. Monero achieves highly anonymous transactions through unique designs, including ring signatures, stealth addresses, and other privacy-enhancing technologies, protecting users' financial privacy.

Monero's specific technical features include:

- Ring signature technology: Monero uses ring signatures to obfuscate the sender of a transaction, making it impossible for external observers to determine who the real sender is.
- Stealth addresses: Monero generates unique one-time addresses for each transaction, protecting the privacy of the recipient.
- Ring Confidential Transactions (RingCT): This technology makes transaction amounts invisible on the blockchain, further enhancing privacy protection.

- Dynamic block size: Monero adopts a dynamic block size limit, adjusting the block size according to network demand, improving network flexibility and scalability.
- ASIC-resistant mining: Monero's mining algorithm is designed to be ASIC-resistant, aiming to prevent mining monopolies and maintain the security of a decentralized network.

These technical features of Monero have made it perform well in the market, with a steady increase in market value and trading volume, especially as privacy demands continue to grow, the overall trend shows a stable growth potential.

Libre chain has made bolder upgrades based on Monero's privacy technology, combined with the latest steganography technology. The so-called steganography technology usually refers to a method of writing and saving data such as images, text, and audio on the data packets of digital assets like BTC using the Ordinals protocol. Libre chain combines multimedia digital steganography technology with Monero's privacy protection technology to successfully develop a super NFT application: NFTpay, which for the first time gives NFT practical value. By injecting Bitcoin, Ethereum, and other third-party digital currencies into libreNFT, highly private and secure transactions are achieved through libreNFT. Transactions of digital currencies through libreNFT are similar to those of privacy coins like Monero, with transaction traces and wallet address assets being opaque, thus ensuring the goal of "my assets are under my control."

A brief description of the implementation logic of steganography technology is as follows:

In image data, each pixel consists of three bytes of data, corresponding to red, green, and blue colors. Some image formats add a fourth byte corresponding to transparency, the "alpha" byte. In this implementation, the encrypted digital information to be entered is scattered into the last bit of each pixel in the digital asset information, that is, by changing the last bit of each byte in the image data with the encrypted digital information, modifying the last bit of the pixel value is not visible to the naked eye, which means no one can distinguish the difference between the original image and the image modified by steganography, thereby hiding one bit of data. This 可以实现 the steganography of the encrypted digital information in the digital asset information, thus obtaining the steganographed asset information. For example, if 1K bytes of encrypted digital information need to be steganographed into the digital asset information, a theoretically required 8K byte image file is needed, that is, the corresponding digital asset information is at least 8K bytes.

It should be noted that during the storage of image data, each color representation requires 8 bits,

that is, 256 colors, totaling 256 cubed colors, that is, 16,777,216 colors. The human eye can distinguish about 10 million different colors, and the remaining indistinguishable colors are 6,777,216.

Specifically, the color of each pixel point in the image data can be represented by decimal values from 0 to 255, which can represent RGB (218, 150, 149) in binary as: R=11011010, G=10010110, B=10010101. By modifying the least significant bit (LSB) of the RGB color components, the human eye will not notice the changes before and after, so this implementation only modifies the binary LSB of the above pixel point's RGB to: R=11011011, G=10010111, B=10010100, that is, modifying the above pixel point's RGB to (219, 151, 148). At this time, the changes in the image data of this pixel point are hardly noticeable to the naked eye, and each pixel point carries one bit of information. Therefore, this implementation can use the LSB of eight bytes to store one bit of information, and this bit of information can be converted into an ASCII character, thus achieving the purpose of steganography.

V. Consensus Mechanism

Proof of Work (PoW) is the first blockchain consensus algorithm based on work, used by Bitcoin, Ethereum, and other blockchain platforms. In PoW, each node must solve a mathematical puzzle (difficult to compute but easy to verify). The first node to complete the puzzle is rewarded. While the PoW mechanism successfully prevents double-spending, DDoS, and Sybil attacks at the cost of high energy consumption, this advantage is also its greatest drawback, namely, high energy consumption.

Proof of Stake (PoS) is a novel and more efficient consensus mechanism, serving as an alternative to the intensive energy and computational use in the PoW consensus mechanism. PoS can be found in many new architectures, such as Cardano and Algorand, and is also used for the next version of Ethereum. In PoS, the node that proposes the next block is selected through a combination of stake (wealth), randomness, and/or age. It alleviates the energy issue of PoW but also raises two significant issues: the Nothing at Stake attack and a higher risk of centralization.

Proof of Meme, as envisioned in Constellation, is an algorithm based on a node's historical participation on the network. Its behavior is stored in a weight matrix on the blockchain and supports changes over time. Additionally, it allows new nodes to gain trust by establishing a reputation. The main drawback of Sybil attacks is mitigated through the NetFlow algorithm.

Delegated Proof of Stake (DPoS), found in Bitshares and Steemit, is a hybrid of Proof of

Authority and Proof of Stake, where a few nodes responsible for deploying new blocks are elected by stakeholders. Although it has a high throughput, this model is susceptible to social issues related to humans, such as bribery and corruption. Moreover, the small number of representatives makes the system vulnerable to DDoS attacks and centralization.

Proof of Behavior (PoB)

Libre chain's consensus method involves classifying and identifying various behaviors of miners on the libre chain, statistically modeling them, and ultimately obtaining the best combination of different behaviors. These behavioral data are fragmented and stored on different nodes in the form of specifically encrypted data blocks with a certain level of redundancy.

The algorithm is described in the following steps:

Each node (ni) is defined as a tuple of a public key (Pk), a rating (default is 0), and a locked stake. If (ni) wishes to participate in the consensus, it must first register through a smart contract by sending a transaction that includes an amount equal to the minimum required stake and other information (Pks, a public key derived from (Pk) and nodeid, which will be used for the signing process to avoid using real wallet addresses).

Node (ni) joins the node pool and waits for the sector allocation at the end of the current epoch (e). The sector allocation mechanism creates a new set of nodes that includes all nodes that joined during epoch (e) and all nodes that need reshuffling (fewer than 1 per sector). All nodes in this set will be reassigned to the sector's waiting list. (Wj) represents the waiting list for sector (j), and (Nsh) represents the number of sectors. Nodes also have a key (sk), which is essentially not public.

$ni = （Pki, rating（i）, stake（i）） \quad ni \in Wj ， \quad 0 \leq j < Nsh$

At the end of the epoch it joined, the node will move to the list of qualified nodes (Ej) for sector (j), where (e) is the current epoch.

$ni \in Wj， e-1 \rightarrow ni/\in Wj， e， \quad ni \in Ej， e$

Each node in the list Ej can be selected as part of the optimal dimension consensus group through a deterministic function based on the randomness source added to the previous block, round (r), and a set of variable parameters (in terms of security and communication). All sector nodes know a random number through gossip, which is unpredictable before the block is actually signed by the previous consensus group. This attribute makes it a good source of randomness and prevents highly adaptive malicious attacks. We define a selection function to return the set of selected nodes

(consensus group) Nchosen , the first of which is the block proposer, using the following parameters: E, (r), and (sigr-1) - the signature of the previous block.

Nchosen= f (E, r, sigr-1), where Nchosen ⊂ E

The block will be created by the block proposer, and validators will co-sign it based on the modified Practical Byzantine Fault Tolerance (pBFT).

If, for any reason, the block proposer does not create a block within its assigned slot (malicious, offline, etc.), round (r) will be used with the randomness source of the last block to select a new consensus group.

If the current block proposer acts maliciously, the rest of the block proposers will apply negative feedback to change its rating, thereby reducing or even eliminating the chance of that particular node being selected again. The feedback function for the block proposer ((ni)) in integer (r), with parameter (ratingModifier ∈Z), is calculated as:

feedbackfunction = ff (ni, ratingModifier, r)

When (ratingModifier < 0), a slashing occurs, and node (ni) loses its stake.

Facing DDoS attacks, the consensus protocol has a large number of potential validators from list E (hundreds of nodes), and the order of validators cannot be predicted before selecting the validators, thus maintaining security.

To reduce the communication overhead brought by the increase in the number of sectors, consensus will be run on a composite block. This composite block consists of:

- Ledger block: The ledger to be added to the sector, containing all transactions within the sector and cross-sector transactions with received confirmation proofs;
- Multiple mini-blocks: Each block holds cross-sector transactions for different sectors; consensus will only be run once on the composite block containing both intra-sector and cross-sector transactions. After reaching consensus, the block headers of each sector will be sent to the metachain for notarization.

VI. Encryption Layer

1. Feature Analysis

Digital signatures are cryptographic primitives used to achieve information security by providing multiple attributes such as message authentication, data integrity, and non-repudiation. Most schemes used for existing blockchain platforms rely on the discrete logarithm (DL) problem: the one-way

display function (y→a y mod p). It has been scientifically proven that computing discrete logarithms with respect to a base is difficult. Elliptic Curve Cryptography (ECC) uses points instead of a set of cyclic integers. This scheme reduces computational workload, thus providing the same level of security as RSA, Elgamal, DSA, and other companies for key lengths of 1024-3072 bits with only 160-256 bits of key length. ECC provides a similar level of security for smaller parameter lengths because existing attacks on elliptic curve groups are weaker than existing integer DL attacks, and the complexity of this algorithm on average requires (√p) solution steps. This means that using a 256-bit length Prime P on average provides security that would require 2128 steps to break.

Both Ethereum and Bitcoin use curve encryption techniques, as well as the ECDSA signature algorithm. The security of the algorithm heavily relies on the random number generator, as private keys may be leaked if the generator does not produce different numbers upon each query.

Another digital signature scheme is EdDSA, which is a Schnorr variant based on twisted Edwards curves, supporting fast arithmetic. Compared to ECDSA, it is provably non-malleable, meaning that it is impossible to find another set of parameters defining the same point on the elliptic curve starting from a simple signature. Additionally, EdDSA does not require a random number generator because it uses a random number computed as the hash of the private key and the message, thus avoiding the attack vector of a compromised random number generator that can leak private keys.

Algorithm Model	Encryption System	Security Level (bit)			
		80	128	192	256
Integer Factorization	RSA	1024	3072	7680	15360
Discrete Logarithm	DH、DSA	1024	3072	7680	15360
Elliptic Curve	ECDH /ECDSA	160	256	384	512
Symmetric Key	AES、3DES	80	128	192	256

Table 1: Bit Lengths of Public Key Algorithms for Different Security Levels

Schnorr signature variants are gaining increasing attention due to their native multi-signature capabilities and proven security in the random oracle model. Multi-signature schemes are combinations of signing and verification algorithms where multiple signers (each with their own

private and public keys) can sign the same message to produce a single signature, which can then be checked by a verifier who has access to the message and the signers' public keys. A suboptimal approach would be for each node to compute its own signature and then concatenate all results into a single string. However, this method is impractical because the size of the resulting string grows with the number of signers. A practical solution is to aggregate the output into a fixed-size signature, independent of the number of participants. There have been multiple proposals for such schemes, most of which are vulnerable to rogue-key (cancel) attacks. One solution to this problem is to introduce a step where each signer must prove ownership of the private key associated with their public key.

Bellare and Neven (BN) proposed a secure multi-signature scheme without ownership proofs under the discrete logarithm assumption in the plain public key model. Participants first commit their shares (Ri) by distributing its hash to all other signers, so they cannot compute its function. Each signer then calculates different challenges for their partial signatures. However, this scheme sacrifices public key aggregation. In this case, the verification of the aggregate signature requires the public keys of each signer. A recent paper by Gregory Maxwell et al. proposed another multi-signature scheme under the "One More Discrete Logarithm" (OMDL) assumption in the plain public key model. This approach reintroduces the high complexity cost of key aggregation from previous schemes by reducing the number of communication rounds from 3 to 2.

BLS is another interesting signature scheme derived from the Weil pairing, whose security is based on the computational Diffie-Hellman assumption on certain elliptic curves and generates short signatures. It has several useful properties such as batch verification, signature aggregation, and public key aggregation, making BLS a good candidate for threshold and multi-signature schemes.

Dan Boneh, Manu Drijvers, and Gregory Neven recently proposed a BLS multi-signature scheme [5], leveraging ideas from previous work [35], [30] which provides defense against rogue-key attacks for the scheme. The scheme supports efficient verification, requiring only two pairings to verify a multi-signature, and no knowledge proofs. Librechain is a BLS multi-signature [5], faster overall than other options due to only two rounds of communication.

Block Signatures in Librechain

For block signatures, Librechain uses curve cryptography based on the BLS multi-signature scheme on the bn256 bilinear group, which implements optimal Ate pairings on 256-bit

Barreto-Naehrig curves. The bilinear pairing is defined as:

e : g0 ×G1 to Gas Turbine (1)

where (g0), (g1) , and (gt) are elliptic curves of prime order (p) defined by BN256, and (e) is the bilinear map (i.e., the pairing function). Let (G0) and (G1) be the generators of (g0) and (g1). Additionally, let (H0) be the hash function generating points on the curve (g0):

H0 : M to g0 (2)

where (M) is the set of all possible binary messages of arbitrary length. The signature scheme used by Librechain also employs a second hashing function with well-known parameters:

Signature: H1 : M to Zp (3)

Each signer (i) has their own private key/public key pair (ski, PKi), where (ski) is randomly selected from Zp). For each key pair, the property (PKi = ski • G1) holds.

Let (L = PK1, PK2, ..., PKn) be the set of public keys for all potential signers during a specific round, which in the case of Librechain, is the set of public keys of all nodes in the consensus group. The following describes the two stages of the block signature process: signing and verification.

Practical Signing - Round 1

The leader of the consensus group creates a block containing transactions, then signs this block and broadcasts it to the members of the consensus group.

Practical Signing - Round 2

Each member of the consensus group who receives the block (including the leader) must validate it; if found valid, they sign it using BLS and send the signature to the leader:

Signature i = ski ∗ H0(m) (4)

where Signature i is g0.

Practical Signing - Round 3

The leader waits to receive signatures within a specific time frame. If it does not receive at least (2 • n + 1) signatures, the consensus round is aborted. However, if the leader does receive (2 • n + 1) or more valid signatures, they use them to generate an aggregate signature: Secret Key (valid in the plain public key model).

For traceability and security reasons, reaching consensus based on a set of reduced verifiers requires the public key of each signer. In this case, our analysis concludes that the most suitable multi-signature scheme for block logging is one where SigAgg is a point on g0.

The leader then adds the aggregate signature to the block along with the chosen signers bitmap (B), where 1 indicates that the corresponding signer in list (L) has added their signature to the aggregate signature SigAgg.

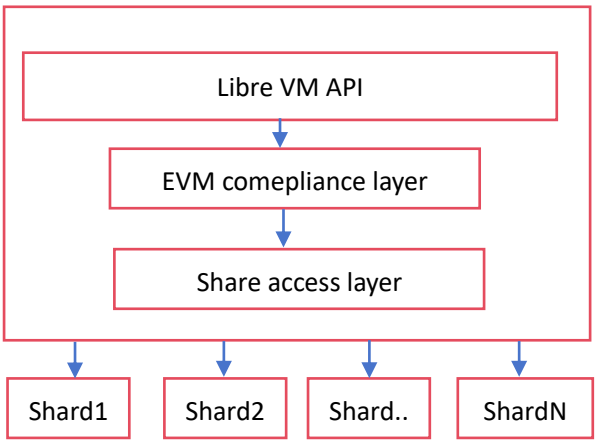
Consensus will only be run once on the composite block containing both intra-sector and cross-sector transactions. After reaching consensus, the block headers of each sector are sent to the metachain for notarization.

VII. Smart Contracts

The execution of smart contracts is a key element of all future blockchain architectures. Most existing solutions avoid proper interpretation of transactions and data dependencies. This context leads to the following two scenarios:

When there is no direct correlation between smart contract transactions, any architecture can employ out-of-order scheduling. This means there are no additional restrictions on the timing and location of executing smart contracts.

The second scenario refers to the parallelism caused by transactions involving related smart contracts. This situation adds additional pressure on performance and significantly increases complexity. Essentially, there must be a mechanism to ensure that contracts are executed in the correct order and in the right location. To cover this aspect, the Librechain protocol proposes a solution that assigns and moves smart contracts to the same sector where their static dependencies reside. In this way, most SC calls will have dependencies within the same sector and will not require cross-sector locking/unlocking.



Librechain focuses on the implementation of the virtual machine on the libre chain, which is an engine compliant with the EVM standard. Given the vast number of smart contracts built on the Ethereum platform, compliance is extremely important for adoption purposes. The implementation of the Librechain virtual machine will mask the underlying architecture, isolating smart contract developers from the system internals, ensuring the proper level of abstraction as shown in the diagram above. In Librechain, cross-chain interoperability can be achieved by using the virtual machine-level adapter mechanism proposed by Cosmos. This approach requires dedicated adapters and external media for communication between adapter SCs for each chain that will interoperate with Librechain. Value exchange will operate using some specialized smart contracts as asset custodians, capable of holding adapted chain-native tokens and issuing Librechain-native tokens.

1. Infrastructure

Librechain builds its infrastructure on the libreVM framework, which is an executable semantic framework where programming languages, calculi, type systems, or formal analysis tools can be defined. The greatest advantage of using the libreVM framework is that with it, the smart contract language can be clearly defined, eliminating the possibility of undefined behavior and hard-to-detect errors. The libreVM framework is executable because the semantic specifications of the language can be used directly as a working interpreter for the relevant language. More specifically, programs can be run directly using the core implementation of the libreVM framework, and interpreters for various programming languages can also be generated. These are also known as "backends." For the convenience of execution speed and interoperability, Librechain uses its own customized libreVM Framework backend.

2. Smart Contract Languages

One of the significant advantages of the libreVM framework is the ability to generate interpreters for any language defined within libreVM without additional programming. This also means that interpreters generated in this manner are "Correct-by-construction." Several smart contract languages have already been specified within the libreVM framework, or their specifications are under development. The Librechain Network will support three low-level languages: IELE VM, KEVM, and WASM.

IELE VM is an intermediate-level language with an LLVM-style approach but tailored for blockchain. It is built directly with libreVM, and there are no other specifications or implementations

outside of the libreVM framework. Its purpose is to achieve human readability, speed, and to overcome some of the limitations of the EVM. Librechain uses a slightly modified version of IELE - most changes relate to account address management. Smart contract developers can program directly in IELE, but most will choose to code in Solidity and then use the Solidity to IELE compiler.

KEVM is a version of the Ethereum Virtual Machine (EVM) where certain vulnerabilities of the EVM are fixed in the libreVM version, or entirely omitted vulnerable functions.

Web Assembly (WASM) is a binary instruction format for stack-based virtual machines that can be used to run smart contracts. The WASM infrastructure allows developers to write smart contracts in C/C++, Rust, C#, and more.

Having language specifications and generating interpreters is only half the challenge. The other half is integrating the generated interpreters with the Librechain network. We have built a universal VM interface that allows us to plug any VM into the Librechain node. Each libreVM has an adapter that implements this interface. Each contract is saved as bytecode for the VM it was compiled for and runs on its corresponding VM.

Smart Contracts on Sector Architecture

Smart contracts on the sector architecture are still in the early stages of research and development and face significant challenges. Protocols like Atomix or S-BAC are a starting point. Dynamic smart contract dependencies cannot be resolved by moving SCs to the same sector because all dependencies cannot be calculated at the time of deployment.

Research in the field currently focuses on solutions such as:

- Locking mechanisms that allow the atomic execution of smart contracts from different sectors, ensuring that the involved SCs are either executed together or not at all. This requires synchronization between multiple interaction messages and consensus across different sectors.
- Ethereum 2.0's cross-shard contract tug proposal moves the smart contract code and data to the caller's shard at execution time. Atomic execution is not required, but locking mechanisms are mandatory on the moved SC, preventing SC execution from other transactions. The locking mechanism is simpler, but it requires the transmission of the entire internal state of the SC.

Following Ethereum's model, Librechain has the following transaction types:

- SC construction and deployment: Transactions receive an empty address, and the data field contains the smart contract code in the form of a byte array.

- SC method invocation: Transactions have a non-empty receiver address that has an associated code.
- Payment transactions: Transactions have a non-empty receiver, and the address has no code.

Librechain addresses this issue by using an asynchronous cross-shard execution model for smart contracts. Users create a smart contract execution transaction. If the smart contract is not in the current shard, the transaction is treated as a payment transaction, deducting the transaction value from the sender's account and adding it to the block of the shard where the sender's account resides, and to the mini-block of the target shard where the recipient's account resides. The transaction is notarized by the metachain and then processed by the target shard. In the target shard, the transaction is treated as an SC method call because the recipient address is a smart contract existing within this shard. For smart contracts, a temporary account is called that will hide the balance of the transaction value from the sender.

After execution, the smart contract may return results that affect multiple accounts from different shards. All results affecting accounts within the shard are executed in the same round. For those accounts not in the shard where the smart contract is executed, transactions called Smart Contract Results (SCR) are created, saving the output of each account's smart contract execution. SCR mini-blocks are created for each target shard. These mini-blocks are notarized in the same way as cross-shard transactions on the metachain and are then processed by the corresponding shard where the account resides. If a smart contract dynamically calls another smart contract from another shard, this call is saved as an intermediate result and treated as the same as the account.

This solution involves multiple steps, and the completion of a cross-shard smart contract call requires at least 5 rounds, but it does not require cross-shard locking and state movement.

VIII. Security Assessment

When a malicious majority proposes an invalid block, the sector state root is tampered with, resulting in invalidity (after including invalid changes to the state tree). Honest nodes can challenge by providing combined Merkle proofs for multiple accounts. Honest nodes will provide the transaction block, the previously reduced Merkle tree of all affected accounts before applying the challenged block, and the smart contract state, thereby proving the invalid transaction/state. If a query with proof is not provided within a bounded time frame, the block is considered valid. The cost of an invalid query is the full stake of the node that initiated the query.

The Libre chain detects inconsistencies through proposed queries and proofs, either invalid

transactions or invalid state roots. This can be traced, and the consensus group can be slashed. At the same time, the challenger can receive a reward that is a portion of the slashed amount. Another issue arises when a malicious group hides invalid blocks from other nodes - non-malicious nodes. However, by forcing the current consensus to disseminate the generated blocks to peer sectors and observer nodes, data can no longer be concealed. Further reduction of communication overhead can be achieved by only sending intra-shard miniblocks to peer sectors. Cross-shard miniblocks are always sent on different topics accessible to interested nodes. Finally, multiple honest nodes may propose challenges. Another security protection is provided through the setting of P2P topics. Communication from a sector to the metachain is accomplished through a set of defined topics/channels, and any honest validator can listen to these topics/channels - the metachain will not accept any other messages from other channels. This solution introduces some delay in the metachain only in the event of challenges, which are very few and highly unlikely, as nodes will face the risk of full staking if detected (the likelihood of detection is high).

IX. Performance Benchmarks

Designing distributed architectures on blockchains faces several challenges, among which the most challenging is the difficulty in maintaining operability under contextual stress conditions. The main components that determine performance stress are complexity, system size, and transaction volume.

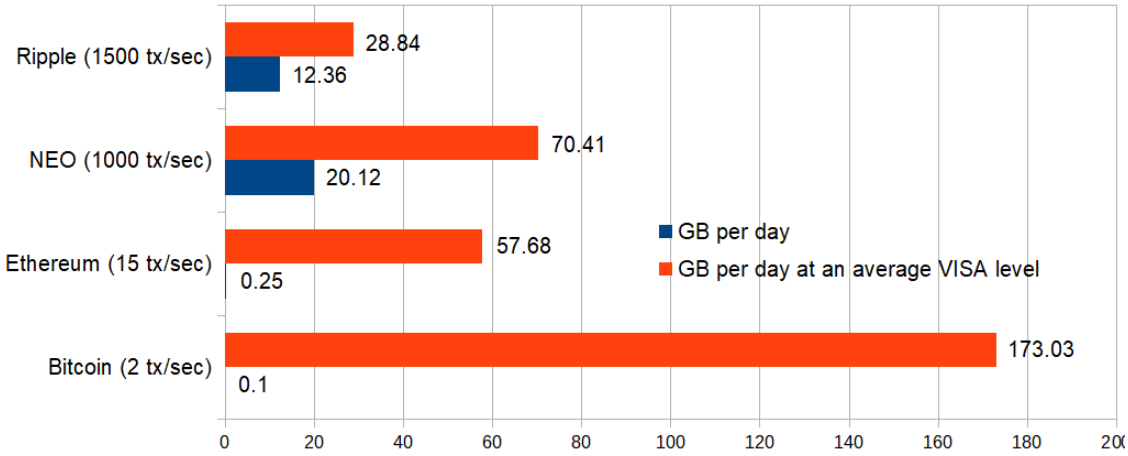
Increasing the number of nodes in existing proven architectures forces a severe decline in performance and leads to higher computational costs, which is the price that must be paid. Sectors seem like a good approach, but sector size plays a significant role. Smaller sectors are agile but more susceptible to the influence of malicious groups; larger sectors are more secure, but their reconfiguration affects system activity.

Compared to other projects, the last item on the list has a higher correlation, indicating transaction processing performance. To properly measure the impact of this criterion, it must be analyzed from the following two perspectives:

C1 Transaction Throughput - How many transactions the system can handle per unit of time, known as TPS, the output of the system;

C2 Transaction Finality - The speed at which a specific transaction is processed, referring to the interval between its initiation and completion - the input-to-output path.

C1. The Transaction Throughput in a single-chain architecture is very low and can be improved by using solutions such as sidechains. In a sector-based architecture like ours, transaction throughput is affected by the number of sectors, the computational capacity of validators/block proposers, and the messaging infrastructure. Generally, as shown in the figure below. This is good for the public, but although this metric is important, it only provides a fragmented view.



Storage Estimation - Verified Distributed Architecture, Average VISA TPS Operation

X. Mode of Operation

The establishment of the Libre chain depends on the number of terminals using Libre applications and the topology servers constituted by these terminals. When the number of online terminals reaches a certain scale, numerous topology servers will naturally evolve on the Libre chain. The number of network terminals that make up each topology server generally ranges from 0.1K to 10K. Each topology server, as a service node on the Libre chain, provides distributed storage and computing services for applications on the Libre chain. When a certain number of node servers appear on the Libre chain, it will naturally attract different application developers to develop and share Libre-based applications within the Libre ecosystem, covering various scenarios such as gaming, social networking, e-commerce, and lifestyle services. As contributors to node servers, they will receive dividend rewards from various applications running on the node servers!

There are three different levels of roles in the Libre chain—miners, node maintainers, and application publishers.

As miners, after downloading and installing the mobile app and registering to activate, the system will start the mining function. By optimizing local PoW computing power and obtaining cloud

PoB computing power through sharing with friends. The first phase mainly involves earning daily 收益 through LIBRE's distributed computing, with cloud capacity depending on the number of successfully shared terminals and the duration of online mining by the terminals. It is important to note that librepoints generated daily should be collected in a timely manner; otherwise, they may be collected by other miners or destroyed due to natural decay. Additionally, miners have the opportunity to discover unexpected mysterious "gold mines" when collecting their own or others' librepoints daily!

As node maintainers, when a miner shares with a certain number of friends (0.1K-10K) and meets the health degree set by the system's algorithm, their topology network will automatically activate to become a node server. A node server is a topology server constituted by all miner terminals as the smallest service unit. The activation method of the node server adopts an ecological competition strategy, ensuring that all units participate in operations in accordance with the rules of biological evolution. As contributors to the node server and maintainers of the health degree of node terminals, they will enjoy rewards from third-party applications running on that node server (topology server), such as receiving transaction dividend rewards from a cloud exchange running on that node server!

As application publishers, when a certain number of node servers appear on the Libre chain, it will naturally attract different application developers to develop and share Libre-based applications within the Libre ecosystem, covering various scenarios such as gaming, social networking, e-commerce, and lifestyle services.

XI. Ecological Construction Plan

As a green, efficient, secure, and convenient digital asset management platform and digital living space based on a new social behavior consensus mechanism algorithm (PoB), Libre aims to build an "oasis" that provides comprehensive digital living services for future humanity. Residents in this digital world of Libre will be able to possess new digital avatars and identities, experience highly immersive VR/AR interactions (socializing, entertainment, office work, meetings, business, etc.), create and experience new life experiences in this world, and even generate wealth that belongs to the real world. If the experience in the real physical world is everyone's first life, then the experience in the Libre digital world is the second life that allows everyone to unleash the soul.

.

Libre chain was launched on October 29, 2021, and successfully went live on its mainnet on January 10, 2024. The Libre technology has been continuously iterated and developed, gradually implementing a variety of ecological applications, and has also planned more ambitious ecological application scenarios, as follows:

1. Instant messaging (librechat, Secret Chat, already launched and in trial operation)
2. Community management (libreDAO, already launched and in trial operation)
3. Web3 wallet (librepay, already launched and in trial operation)
4. Exchange (LEX, already launched and in trial operation)
5. Super wallet (NFTpay, already launched and in trial operation)
6. Token e-commerce (Comebei Points, already launched and in trial operation)
7. Gaming (LibreGameFi, planning for the Libre Metaverse social life platform)
8. Edge cloud (Libre Cloud, planning for a decentralized node server cluster platform)

In 2025, after completing the main coin offering, Libre will focus on operating the NFTpay super wallet and building the Libre edge cloud platform serving AI and the Metaverse. The NFT super wallet will be a phenomenon-level product that can change the current digital currency trading landscape. Through NFTpay super wallet, the principle of "my assets are under my control" will be maximized, avoiding the privacy risks and asset security risks brought about by excessive transparency of personal digital assets in traditional models. The Libre edge cloud will be a super platform participated in and operated by many independent individuals, managed in a non-corporate way, serving AI and Metaverse ecological applications, and adhering to the principles of "governed by the people, owned by the people, and enjoyed by the people."

LibreChain Founding Team

Official Twitter: @LIBRECHAINTEAM

Official Email: librechain@gmail.com

Official Website: https://www.libre.gold