Whitepaper

Version 1, July 2021

JOEL KASR

FOUNDER, KAJ LABS & LITHOSPHERE

joel@kajlabs.com

lithosphere.network

kajlabs.com

MAKING SMART CONTRACTS INTELLIGENT FOR THE DIGITAL ECONOMY

Abstract

In geography, a lithosphere is the rigid, outermost shell of a terrestrial-type planet or natural satellite. On Earth, it is composed of the crust and the portion of the upper mantle that behaves elastically on time scales of thousands of years or greater. - Wikipedia

Having closely monitored the blockchain space for the last 10 years, the KaJ Labs Foundation can build a much better blockchain network learning from mistakes made by early networks.

At this time, all types of tokens have completed some basic functions of value transfer and distribution, but they are still a long way from the fully functional financial services that the real world requires, which is why, when it comes to blockchain applications in the financial sector, all we hear is thunder but no rain falls. People need a new generation of financial infrastructure based on blockchain technology that has complete financial functionality, can link different communities and tokens, and can bridge the gap between centralized and decentralized organizations as soon as possible to usher in the era of the Internet of Values.

We created a completely new "Email system" at the dawn of the Internet of Information, rather than transforming the "postal system." Similarly, when the Internet of Values arrives, we want to build a new system: a value transfer infrastructure based on a variety of tokens.
Lithosphere (Litho) is ready for the DeFi age! By establishing a layer of control management on top of various tokens through a distributed management of the tokens' private keys and by providing ports both for central organizations and for external data sources, Lithosphere will connect various past and next-gen smart contracts, solving the key problem of the current Internet of Values' insufficient interoperability.

The lithosphere is open to everybody. It connects centralized and decentralized organizations, accommodates authentication methods and anonymous trade mechanisms, and introduces on- chain data and off-chain data by integrating the cryptocurrencies and blockchains that exist today and those that may exist in the future. The lithosphere is a Turing-complete virtual computer that allows DeFi to have unlimited reverie space across multiple tokens in the future, opening up henceforth unthinkable possibilities. The Litho project's general concept, essential technology, and development strategy are presented in this whitepaper, which presents the prospect of decentralized banking based on an examination of the history of the Internet of Values.

Design Concept

Blockchain Emergence and Significance

Due to a lack of confidence, the conventional market economy has a significant cost. The major method that individuals continuously handle trust is through a centralized organization or company. The fast growth of modern human civilization was aided by people with similar ideals who were organized into institutions such as governments, political parties, and businesses. However, centralized organizations face enormous challenges: First, owing to a lack of trust between organizations and conceptual disputes, various groups become embroiled in violent rivalry, years of warfare, and even nuclear terrorism. Second, resources have been increasingly concentrated in the hands of a small number of people, widening the divide between classes. Finally, there is the concept of a "single point of failure," such as Solar Winds.

Because a few agencies have monopolized a huge quantity of resources such as power, wealth, skill, and data, the repercussions of them reneging or being hacked will be severe. Lithosphere's vision is to connect all blockchains and break the barriers between blockchains by allowing them to transact with each other. The end goal is to create a connected network of blockchains, a network of blockchains able to communicate with each other in a decentralized way.

With Lithosphere, blockchains can maintain sovereignty, process transactions quickly and communicate with other blockchains in the ecosystem, making it optimal for a variety of use cases instead of being limited to one blockchain network i.e Polkadot / Bitcoin / Ethereum / Cardano.

A very good use case of Lithosphere will be the transfer of NFT. Presently, NFT can only be transferred to parties within a given network. At the moment one can't send Ethereum NFT to a Smart Chain (BSC) user or vice versa. With Lithosphere, users in the eco-system will be able to receive and send tokens from any blockchain that supports Byzantine Fault-Tolerant (BFT) consensus.

The transition from central credit authorization by institutions to inviolable mathematical principles for documenting value exchange is a significant advancement. Currency is, in essence, a consensus. It's a standard accounting symbol for more convenient value exchange. Reviewing humanity's financial history, from bartering one thing for another, to using cattle, sheep, or shells as universal equivalents, to the use of precious metals as money, to the current use of paper currency with a strong credit base, the human currency is approaching abstract mathematics, and its nature as symbols or ledgers is more apparent. Human accounting concepts become more aligned with mathematics as a result of blockchains.

It assists the whole accounting system in moving away from a single institution's control and toward a more fair and transparent path. Financial Inclusion is a concept that aims to provide access to the financial system and low-cost financial services for disadvantaged individuals and small businesses throughout the world. Two and a half billion individuals worldwide are unable to use banks, create savings accounts, or acquire credit cards, thus cutting them off from the global economy. Banks charge exorbitant fees for cross-border transfers. Ordinary investors can only purchase very low- end financial goods from banks and other financial institutions, and they are unable to participate in early-stage investments in technology companies such as Google and Alibaba until they are listed on the stock exchange.

Many small and medium businesses are also having difficulty obtaining loan support from banks, despite having strong credit and excellent performance, because they are not traditional banks' target clients under the 80/20 rule. The development of blockchain technology is altering the conditions described above. Bitcoin is used to pay workers in other nations, such as El Salvador. Investors who took part in the initial coin offerings (ICO) of well-known blockchain projects like Bitcoin and Ethereum saw returns hundreds of times their initial investments. Inclusionary finance is reaching new heights thanks to blockchain technology. Many organizations are exploring ways to record traditional forms of assets, such as commercial bills and loyalty points, into blockchains, usually in the form of consortium chains. Cryptocurrencies are becoming more acceptable as a form of payment in financial transactions; many organizations are exploring ways to record traditional forms of assets, such as commercial bills and loyalty points, into blockchains, usually in the form of consortium chains. There has been the emergence of digital asset exchanges, which are comparable to traditional financial organizations.

The banking function of exchanging digital assets is performed by these exchanges. They are similar to stock exchanges in that they provide a platform for purchasing and exchanging tokens. The functionalities of a platform for cross-border token transfers are comparable to those of cross- border bank remittances. However, these platforms operate in a centralized way to varying degrees, which not only introduces security issues associated with centralization but also prevents the widespread use of blockchain technology. We need a distributed "bank" based on this phenomenon, where multiple digital currencies and digital assets may be moved in, out, and swapped via blockchains. We require a location where financial products and contracts based on digital currencies and digital assets may be developed and executed, as well as a secure environment to safeguard transaction privacy. Of course, such "banks" will be nothing like traditional banks, except for a few services like debit and credit, remittance, settlement, and financial product sales. Any company or individual with sufficient expertise and cash can open their business windows. They may offer a variety of services while maintaining the security of a distributed blockchain infrastructure, allowing them to deliver more financial services to more people. This is a future financial infrastructure built on digital assets and a distributed financial market, to be more precise.

Design Objectives

The major benefit of blockchain is that it aids in resolving the issue of trust that plagues humanity, making blockchain technology raising human civilization's level. Its growth is unstoppable because of the human need to reduce transactional expenses. Because each blockchain can perform peer-to-peer value transmission, unlike the original Internet of Information (IoI), blockchain technology moves us from the age of IoI to the age of the Internet of Values (IoV), which may be considered the third generation of the Internet.

Lithosphere has established the following goals based on research on cross-chain technology, AI & Machine Learning, as well as the features of decentralization and its application scenarios, to develop a more widely disseminated blockchain technology and digital asset applications:

Cross-chain Asset Transfer:

- Connecting large digital currency networks (such as Bitcoin and Ethereum) and completing asset transactions without changing the original chains' mechanisms. This allows Lithosphere to incorporate freshly created digital currency networks at a very cheap cost.
- Integrate Lithosphere with consortium chains. This handles asset transfers from original chains to Lithosphere, asset transfers from Lithosphere back to original chains, and asset trading on Lithosphere.
- Ensure that cross-chain transactions are secure and that cross-chain transaction services are stable.

Transaction Privacy Protection:

- Allow trade parties to select whether or not to execute transactions privately.
- Provide privacy protection for digital asset transfers and exchanges.
- Provide holders of digital assets with anonymous protection.

Functional Extensibility:

- Become a decentralized platform for the trading of non-fungible assets and digital currency.
- Operate a deposit and lending company for several digital currencies.
- Use digital money as a vehicle for digital asset transactions.
- Create brand new digital financial assets and exchange them.

The world has changed dramatically as a result of the Internet of Information. Human civilization is destined to undergo massive societal transformations as a result of the Internet of Values. This is due to the qualities of digitalization, intelligence, decentralization, and inclusiveness that the Internet of Values-based on blockchain technology possesses. Digitization and intelligence, which can help the Internet of Values run more efficiently, are elements that already exist on the Internet of Information, but are now being applied to the Internet of Values. Decentralization is an even more important feature since it will assist to eliminate the bottleneck caused by centralized organizations. People can better safeguard their personal property rights with private keys; they can better resolve conflicts with consensus mechanisms, and they can engage in collaboration in the division of labor with peer-to- peer networks with much lower obstacles.

People join the Internet of the Information age when they can easily transfer information over the Internet and program information using algorithms; they will enter the Internet of Values age when they can easily send value over the Internet and program value using smart contracts. The Internet of Values benefits gives it a “high-dimensional” edge over traditional collaboration models. On blockchains, all types of "values" will be expressed and easily exchanged and programmed. As a result, people's collaboration relationships and human civilization would undoubtedly be drastically altered.

The Internet of Values will allow individuals to handle values as if they were informed, and its primary role will be to communicate values.

However, to fulfill this purpose, the Internet's worth must improve in three areas. Interoperability is the first. Values reside on many blockchains, centralization organizations, and data centers, and the Internet of Values necessitates public chains or other solutions that can interact across blockchains, centralization organizations, and data sources, as well as transfer values and perform smart contracts. The second factor is scalability. The Internet of Values must be adaptable to a variety of circumstances, including banking, industry, and government administration. The last point to consider is usefulness. The Internet of Values requires a robust ecosystem and the ability to operate a wide range of apps seamlessly so that developers can create applications quickly and consumers can easily utilize them.

However, compared to the Internet of Information, the Internet of Values is still in its early phases, with interoperability, scalability, and usability limitations.

In terms of interoperability, although the Internet of Information has been able to transmit and program words, photos, audio, and video as a unified bit of information, the Internet of Values continues to struggle with communicating values between blockchains, much alone off-chain values, and data.

Not only does the Internet of Values necessitate cross-chain connectivity, but it also necessitates connection with centralized entities and external data sources. Tokens on separate blockchains can't trade with each other since existing blockchains can't communicate with each other (synchronization of state machines). Because blockchains presently cannot communicate with centralized organizations outside of the blockchain, it is difficult to map off-chain assets onto the blockchain. Because existing blockchains can't read off-chain data, "smart" contracts on them are blind or dumb, unable to see or communicate with the outside world.

Taking cross-chain technology as an example, cross-chain communication, much alone building cross-chain smart contracts, is now exceedingly challenging. There are thousands of different types of tokens now available, but each one can only move freely on a single blockchain and has its ecosystem of wallets, smart contract creation tools, and so on. Existing blockchain networks are essentially island ecosystems, and the Internet of Values is still a long way from being genuinely interoperable.

In terms of scalability, while the Internet of Information is constantly expanding by encoding various data as bits and programming various scenarios' communication logic as applications, the Internet of Values is only just getting started by tokenizing various values as tokens and mapping various scenarios' transaction logic as smart contracts.

The Internet of Values scale is severely constrained due to its lack of compatibility. The transfer of off-chain values to the Internet of Values is hampered by the difficulty of mapping actual application scenarios involving various currencies, numerous organizations, and multiple data sources to a blockchain to build a distributed solution.

In terms of usability, whereas the Internet of Information's processing power, storage capacity, and synchronous speed were sufficient to handle most information management needs, the Internet of Values can only accommodate somewhat larger projects. In terms of standardization, platformization, functional modularity, application ecology, interoperability, and anti-quantum assaults, the Internet of Values has a lot of work ahead of it.

Interoperability is the most pressing of the three types of obstacles listed above, since it allows us to move assets between blockchains, design smart contracts with various currencies, and improve update scalability. Usability, on the other hand, is a long-term effort, but interoperability and scalability, which have slowed the growth of the Internet of Values, require a quick fix and have become the two most pressing barriers to be addressed.

Smart Contracts & Decentralized Finance (DeFi)

The goal of the Internet of Values is to link different values to blockchains so that smart contracts may control them. The Internet of Values enables decentralized, disintermediated, inclusive, and programmable collaboration among individuals. Because of these apparent benefits, diverse values will race to be mapped to blockchains. The Internet of Values will undoubtedly expand at a faster rate as blockchain constraints are addressed.

The process of mapping values to blockchains necessitates decoupling financial logic from business logic, implying that the Internet of Values was created with a significant financial component. The financial applications of the Internet of Values are those applications on the Internet of Values that have particularly significant financial features. Decentralized Finance refers to the on-chain financial operations on the Internet of Values, as well as their corresponding off- chain financial activities (DeFi).

Because the Internet of Values is built on peer-to-peer networks that use the User Datagram Protocol, there are certain obstacles. The performance of the Internet of Values will progressively approach that of the Internet of Information in the future, allowing business scenarios and financial transactions to be written in the same software. However, given the current state of affairs, we expect this will take a long time. The present Internet of Values will primarily support financial applications, i.e., DeFi apps will be the primary applications.

The Internet of Information has already had a significant influence on r lives. We may also anticipate significant changes in our lives as a result of the Internet of Values. We may be familiar with the many forms of information available on the internet, but few people talk about the “value” of the Internet of Values.

To begin with, the values on the Internet of Values are tokens represented by the blockchain, and the process of mapping values to the Internet of Values is known as asset tokenization. The connected assets will be expressed by on-chain tokens and form part of the Internet of Values if the tokens on the chains represent the title, gain, and control of the underlying off-chain assets. The Internet of Values allows more and more values to enter itself through this process, preventing "double spending" through distributed books and making transferring value without intermediaries as simple as sending information and programming values as simple as programming information, making the Internet of Values' prospects similar to what we have seen previously regarding telecommunications.

Second, tokenization is a form of asset securitization in which off-chain values are mapped onto chains as crypto assets. Because tokens may be divided indefinitely and transferred over time and space, they can be used in financial transactions like mortgages, loans, and insurance. As a result, tokenization is defined as the process of securitizing assets and converting off-chain assets into crypto assets that can be managed using private keys.

Finally, the Internet of Values will include a wider range of values. Identities, signatures, data, voting rights, and other data will be mapped to the Internet of Values as long as tokenization is profitable. As a result, the Internet of Values will have a wider range of values than traditional financial markets.

Positioning

We propose the Lithosphere project in light of DeFi's bright future and the challenges that the current Internet of Values presents. The goal of Lithosphere is to create a platform-level public chain in the digital economy era that can connect all kinds of values, provide complete financial functions, communicate diverse communities and tokens, and bridge centralized and decentralized organizations to bring the Internet of Values as soon as possible with the help of blockchain, AI, and other technologies.

Lithosphere Architecture and Technology

Distributed Private Key Management and Smart Contract Virtual Machine

Because DeFi assets are displayed as tokens, they can substantially improve the interoperability of the Internet of Values and make increasing scalability much easier if multi-token smart contracts can be implemented. The present cross-chain technology is mostly side-chain technology, which uses a two- way peg to transfer transactions to side chains and multiple signatures to exit side chains. Such a method can only produce atomic transfers, and the results are unsatisfactory in nearly every way. We need to create a public chain that allows other tokens to be mapped to it in a more inventive fashion, so that multi-token smart contracts may be created. We can substantially improve the interoperability of the Internet of Values in this manner, and this public chain will undoubtedly become one of the most important DeFi infrastructures. It not only communicates values between blockchains but also enables interfaces with centralized organizations and off-chain data sources to increase the Internet of Values' scalability. On a new public chain, how will various tokens be expressed? We envisage that the tokens’ private keys on various blockchains can be securely controlled in a distributed fashion by a public chain and in this way, the blockchain manages the control rights of tokens. It will be like a “freeway” on the Internet of Values, which can easily implement the value transfers between various tokens and multi-token smart contracts to provide various DeFi services.

Since almost all blockchain tokens are controlled by private keys, values on the Internet of Values can be distributedly managed by smart contracts as long as the private keys of their tokens can be controlled by distributed nodes of a public chain. With Turing-complete smart contracts, the public chain can also provide various functions of decentralized finance (DeFi) in a more sophisticated form.

This blockchain, which connects all tokens, does not require complex logic for various application scenarios. Its purpose is to create a layer of management across all blockchains, enabling all tokens to interact. Because it does not need to run heavy application logic, in its current usability it is capable of fulfilling various DeFi functions.

Myriad Distributed Key Management (MDKM)

The lithosphere is based on the theories and achievements of distributed key generation (DKG) in the field of cipher- sharing. The public key and the private key are both generated by nodes cooperating to communicate. The public key is broadcast in the public chain, the private key is separately stored by each node in a distributed manner through Variable Secret Sharing (VSS). The common public key is generated by the DKG algorithm, and then the account address of the Lock-in is generated by the corresponding algorithm to realize decentralized control.

Here we refer to the domain of VSS and DKG based on elliptic curve cryptography distributed key generation protocol and application research on the process described below:

Given elliptic curve E, there exists a finite field GF (q), q is a prime number with n participant sets Q = {P1, P2, ..., Pn}, pi denotes the identity of the ith participant Pi, and Pi ∈ GF * (q), where GF * (q) is a multiplicative group on GF (q). In the meantime, pi and I are interchangeable during the calculation. E/GF (q) represents the additive group on E. T is E/GF (q), the order of E/GF (q) is a prime number or prime factor, marking this prime or prime factor as p.

In this key generation protocol, it is assumed that both scalar multiplication and dot multiplications are done at ð and that the other operations are done at GF (q). To calculate Q (x) T, we first compute Q (x) and then p(x) mod p, and Q (x) mod p is the scalar multiplication on T.
Let us assume that E has another base point T ′ on the elliptic curve ð.

Threshold signature

The threshold signature technique can address the issue of signatures created by Lithosphere's departing nodes while also improving the blockchain network's stability. According to studies on node adaptation in distributed key generation networks, Lithosphere will choose appropriate nodes to join and refresh the shared key parameters in extreme circumstances to assure the chain's successful functioning.

Litho Coin

Litho is the native coin of Lithosphere. Both cross-and intra-chain transactions consume a certain amount of Litho. Litho is also used in security deposits for the cross-chain verification nodes. Litho / $LITHO is the currency of choice in the Lithosphere network although another crypto can be used as well since the Lithosphere blockchain supports interoperability.

LAX - Algorithmic Stablecoin

Litho Algorithmic stablecoin coin (LAX) is similar to algorithmic stable coin protocols operating on the Ethereum blockchain, but unlike coins like U.S. Dollar Coin (USDC) and Tether (USDT) which are backed by audited holdings of U.S. dollars or crypto assets like PAX Gold (PAXG), Litho USD coin is not pegged to the U.S. dollar or any crypto collateral. Rather than using crypto, fiat, or commodities as collateral, the Lithosphere protocol adjusts its LAX crypto supply every 24 hours in a process called “rebasing” to maintain a stable price.

Consensus Mechanism

Lithosphere adapts a proof of stake consensus mechanism.

The goal of Lithosphere is to use blockchain technology to build an infrastructure platform to run decentralized applications and on the platform, multiple types of tokens will be able to freely interact through smart contracts to achieve value interoperability. Lithosphere aims to implement Myriad Distributed Key Management to build smart contracts for DeFi.

When an unregistered asset is moved from the originating chain to Lithosphere, Lithosphere will construct a new asset based on the cross-chain transaction information, utilizing a built-in asset template to deploy a new smart contract. When a registered asset is moved from the original chain to Lithosphere, Lithosphere will issue equal tokens in existing contracts, ensuring that the original chain assets may still be traded on Lithosphere.

Cross-Chain Integration

Asset mapping refers to the process of producing matching tokens for bookkeeping on Lithosphere for a controlled item. One token can freely interact with other mapped assets thanks to mapping. Lock-in and Lock-out operations are used to establish and de-manage distributed control.

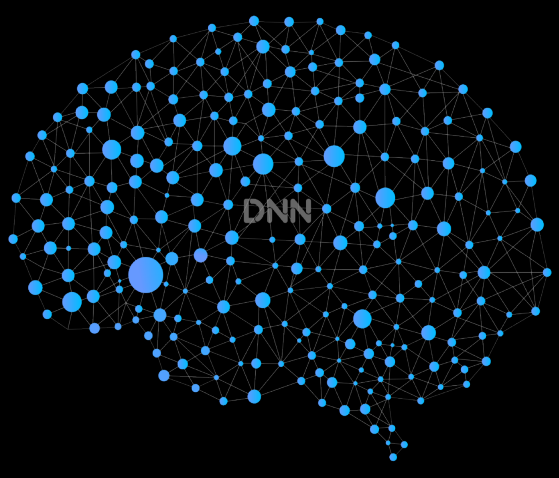
Cross-Chain Transactions

Asset Lock-in is a process that enables myriad distributed key management and asset mapping for all key-managed tokens.

Asset Lock-out) is the reversal of Lock-in, and it consists of two parts: control rights management and asset mapping disassembly. After Lock-out is completed, control of the digital asset is returned to the owner, restoring complete key storage and centralized key management. By improving the security, liquidity, and DeFi applications of current digital assets, adopting multifarious key distribution management will improve the value of digital assets.

Deep Neural Networks (DNN)

David Yang PhD, proposes Deep neural networks (DNNs) for Lithosphere smart contracts. DNNs are very useful in blockchain applications such as DeFi and NFT trading. However, training / running large-scale DNNs as part of a smart contract is infeasible on today's blockchain platforms, due to two fundamental design issues of these platforms. First, blockchains nowadays typically require that each node maintain the complete world state at any time, meaning that the node must execute all transactions in every block. This is prohibitively expensive for computationally intensive smart contracts involving DNNs. Second, existing blockchain platforms expect smart contract transactions to have deterministic, reproducible results and effects. In contrast, DNN is usually trained / run lock-free on massively parallel computing devices such as GPUs, TPUs, and/or computing clusters, which often do not yield deterministic results.



For the first time in smart contracts, Lithosphere implements DNN to make smart contracts intelligent by incorporating large-scale deep neural networks (DNNs) into the code, which has numerous potential applications. For instance, in decentralized finance (DeFi), a DNN might help detect abnormal token price movements, which could be part of a flash-loan attack. A decentralized autonomous organization (DAO) might trade tokens automatically with a DNN trained continually through reinforcement learning. A content creator might apply a generative adversarial network (GAN) to generate visual art images, and subsequently tokenize them as non-fungible tokens (NFTs) tradable in a decentralized exchange.

LEP100 Multi-chain Token Standard

The LEP100 is a novel standard for multi-tokens, allowing for a single contract to represent multiple fungible(currency) and non-fungible tokens (NFT) and batched operations for increased gas efficiency proposed by Joel Kasr, creator of Lithosphere. Most importantly, LEP100 tokens can exchange for any other token equivalents. LEP100 tokens are fueled using the native Litho coin (LITHO).

. When pegged with the LEP100 tokens, you may also peg onto any networks utilizing any major digital assets. The token is multi-contract compliant and has basic features like transferring, returning a balance, and examining a token's possession. A LEP100 token, unlike ERC20 or BEP20, allows a single contract to represent numerous fungible and non-fungible tokens, allowing for a wide range of applications in everyday use. It is the most efficient token for DeFI platforms, gaming platforms, NFT, and another high-demand contract–compatible platforms. LEP100 may also be easily integrated into any Ethereum dApps or other chains because it can be traded for ERC20, ERC-721, ERC-1155, BEP2, and BEP20 tokens. The LEP100 establishes best practices for managing cross-chain tokens. Due to their similarities, the tokens are compatible with ERC20, ERC-721, ERC-1155, BEP2, and BEP20.

The LEP100 token standard also allows for token time-slicing in smart contracts. When a token is sliced, it is split into two parts: one is a time-limited slice (here TL is for Time-Lent), and the other is an infinite end (here TL stands for Time Restricted, since its utility is limited for a time but not locked). Both slices can be split into two more time slices if needed, allowing for sophisticated DeFi such as options and futures trading.

Validators

In classical Byzantine fault-tolerant (BFT) algorithms, each node has the same weight. In Lithosphere, nodes have a non-negative amount of voting power, and nodes that have positive voting power are called validators. Validators participate in the consensus protocol by broadcasting cryptographic signatures, or votes, to agree upon the next block.

Validators' voting powers are determined at genesis or are changed deterministically by the blockchain, depending on the application. For example, in a proof-of-stake application such as the LithoSwap, the voting power may be determined by the amount of staking tokens bonded as collateral.

Linear-communication BFT Consensus

The Litho protocol utilizes a BFT (BFT stands for Byzantine Fault-Tolerance) algorithm to achieve this. A Byzantine Fault-Tolerant consensus algorithm guarantees safety for up to a third of Byzantine, or malicious, actors. Byzantine faults within distributed systems are some of the most difficult to deal with.

A blockchain framework like Lithosphere powered by BFT allows public and private blockchains to transfer tokens to each other.

A BFT powered blockchain network (Lithosphere) allows interoperability with other PoS / fast finality blockchains like Cosmos, Binance or Proof of Authority & PoW blockchains.

Lithosphere adapts a new consensus algorithm, LinBFT proposed by Dr. David Yang. The Linear-communication BFT Protocol (LinBFT) applies to a permissionless, public blockchain system, in which there is no public-key infrastructure, based on the classic PBFT with 4 major improvements:

- Per-block consensus. There is consensus for each block, rather than for a group of blocks. This limits the power of the block proposer, and, thus, mitigates selfish mining.
- Rotating leader. The LinBFT protocol changes the leader (i.e., block proposer) for every block, which reduces the risk of denial-of-service attacks on the leader.
- Changing honesty. In Pyramid LinBFT, a participant can be honest for one block, and malicious for another (e.g., one containing a transaction of interest to the participant), as long as over 2/3 of all participants are honest for each block. In other words, it is possible that every participant is malicious at some point, and yet the blockchain remains secure at all times.
- Dynamic participant set. LinBFT allows nodes to join and leave the protocol at the beginning of epochs. As a result, different blocks may be verified by completely different sets of nodes.

Further, in the ordinary case, LinBFT involves only a single round of voting instead of two in PBFT, which reduces both communication overhead and the confirmation time and employs the proof-of- stake scheme to reward all participants. Extensive experiments using data obtained from the Ethereum test net demonstrate that LinBFT consistently and significantly outperforms existing in- production BFT protocols for blockchains.

Myriad Distributed Key Management

Myriad Distributed Key Management realizes the generation of public-private key pairs and addresses and the transaction signatures on the target blockchain in a distributed manner through several nodes and according to digital signature algorithms adopted by the target blockchain, thus realizing the control and management of accounts and assets on the target blockchain in a distributed manner.

Such a technical route enables MDKM to be compatible with as many digital assets controlled by encryption algorithms as possible, whether these digital assets are generated on a centralized or decentralized basis. By supporting a signature algorithm with MDKM, a series of encrypted digital assets with the same signature algorithm can be controlled and managed.

At present, most (over 80%) of encrypted digital currencies adopt the same ECDSA signature algorithm as Bitcoin and Ethereum, so MDKM first chooses to implement support for the ECDSA signature algorithm. In addition, MDKM will support encryption currencies that use different signature algorithms, such as Stellar's Ed25519 signature algorithm [JL17], and Schnorr's signature algorithm.

LEP100 Token Standard

LEP100 specifications are followed by all Lithosphere tokens. The Lithosphere network is a multi-chain architecture that allows anybody to develop dApps and other blockchain-based digital assets. It also ensures cross-chain trade, minimal gas consumption, and quick transactions with safe transactions.

LEP100 makes it possible for tokens on the Lithosphere blockchain to function properly. As a consequence, everyone benefits from low transaction fees.

Furthermore, regardless of the blockchain network's structure, the cross-chain DeFI mechanism improves the interoperability of all tiny contracts. The Lithosphere environment is highly supportive, and the Litho Launchpad finances all bootstraps with various DeFI programs.

Why should your DeFi project use the LEP100 Token Standard?

LEP100 tokens may be used to represent a variety of assets, including stocks, fiat currency, and crypto-assets. Other tokens from various blockchains may easily be pegged to the LEP100 token. As a result, it enables developers to construct different versions of crypto assets using the same tokens.

All validators that transfer the LEP100 token will receive LITHO as a reward. The incentive is paid out in the form of a transaction charge. When compared to other token standards such as ERC20, it has minimal gas prices for all transactions. It's built on the Lithosphere network, which offers fast transaction speeds of more than 10,000 TPS compared to Ethereum's ERC20's 15 TPS and Bitcoin's 4 TPS.

Integrating DeFI projects with LEP100 tokens is simple. You may also list items for free on DEX such as LithoSwap, PancakeSwap, and Uniswap

LEP100 Token Features

The LEP100 token offers many outstanding features, including

- High-speed transaction speeds: the LEP100 token standard enables high-speed transaction rates, making it extremely scalable.
- Low transaction fees: unlike Ethereum Networks, users will not be charged hefty gas prices.
- Cross-chain compatibility: The LEP100 tokens are supported by ERC20, ERC-721, ERC-1155, BEP2, and BEP20 networks and blockchains.
- Compatible with nearly every major cryptocurrency wallet on the market today.
- Easy to sell on exchanges: The LEP100 tokens are simple to list on exchanges and have a better probability of being sold.

Verification Nodes

To earn a portion of the transaction fees, a Validator completes the recording of transactions on Lithosphere. According to the stake it owns, a Validator receives a corresponding key share and calculates the associated signature share to be appended to the transaction. According to the key share percentage, the Validator gets the transaction fee associated with the verification transaction. The transaction fee cannot be collected if the key sharing information is unavailable or lost. If the nodes sign the incorrect transaction, the Validator's credentials will be removed as well.

In summary, the verification node incentive system will encourage Authenticators to give proper transaction proof, Validators to faithfully finish Lithosphere recording, and Record-keepers to stay online and keep their key shares secure.

Verification nodes are only available to individuals with a large enough stake in the Lithosphere network. General nodes are nodes that do not qualify as verification nodes. The general nodes are unable to participate in the cross-chain transaction verification process, but they can commit their stakes to the trusted verification nodes. The transaction fees received by the entrusted verification nodes are distributed to the general nodes in proportion to the entrusted stakes. General nodes will suffer a comparable loss if the delegated verification node is penalized.

Stakeholders in Lithosphere can gain stake-related advantages while also being motivated to commit their stakes to trusted verification nodes thanks to this incentive mechanism. This enhances Lithosphere's security and stability.

Locked Account Generation Scheme

The Locked Account Generation Scheme is based on threshold key sharing and safe multi-party computing.

Introduction

Distributed cryptography's theoretical foundation and a basic challenge of distributed computing are both secure multi-party computation.

The hypothesis is based on the 1982 book "Yao's Millionaires' Problem." Simply defined, secure multi-party computing refers to a set of players known as P1 Pn who collaborate to safely calculate the function f(x1, xn)=(y1, yn). Then each of the n participants has one of the function f inputs. Pi has the secret input xi and receives the output yi after calculation. In this case, security necessitates ensuring the validity of the computing result, even if some individuals cheat throughout the computation process. This implies that after the computations are finished, each participant must receive the right result yi, and all participant input is protected. Through the calculation, Pi can obtain no further information other than (xi,yi).

General Nodes

The threshold key sharing method is intended to address the issue of secure key management. The security of cryptography is dependent on the security of the keys, according to contemporary cryptography design principles. Cryptography's security will be jeopardized if secure keys are compromised. As a result, key management is critical in cryptography security research and design. It might be challenging to handle the distribution of keys safely when an account is maintained by numerous persons with diverse interests. Cryptographer Adi Shamir devised the Shamir's Secret Sharing threshold key sharing technique to tackle this problem.

A key is split into n pieces and handed to n participants in this system. Each participant has a piece of the key share, and the key must be reconstructed using a minimum of k key shares. As a result, each activity on an account will need the cooperation of at least k individuals to maintain the account's security and reliability.

Based on safe multi-party computation and threshold key sharing, we created the Locked Account creation technique. Lithosphere Validators (Record-keepers) are in charge of maintaining and managing the keys to the Locked Accounts to guarantee that they are secure and reliable. Furthermore, in an ad-hoc network with no set topology, this technique reduces the danger of keys being lost and offers high flexibility and stability.

The following is the Locked Account Generation Scheme:

Design Description

Step 1: Choose a safe random number.
On Lithosphere, there are n validators known as P1.....Pn. Each validator chooses a safe random integer di as well as a k-degree polynomial fi (x)=di+ai,1 x++ai,k-1xk-1. The technique delivers fi (j) to other validators through a secure channel and broadcasts di G to every network node, with G being the elliptic curve's base point.

Step 2: Verify that the messages are proper.
Pj will examine the messages' correctness after receiving messages from other validators: lag=Check(f1 (j),.....,fn (j)) lag=Check(f1 (j),. ,fn (j)) lag=Check(f1 Pj accepts and stores it locally if flag=true. If flag=false, Pj rejects the message and needs other validators to resubmit it.

Step 3: You will be given a key to distribute.
When all messages have been delivered and checked out, each validator receives their key share as follows: fj(k),k=1,.....,n key sharek=(j=1) fj(k),k=1,.....,n

Step 4: Determine the Locked Account's address.
Locked Account Address=GenerateAddress(d1 G,.....,dn G) n Any activity on the Locked Account will necessitate the involvement of at least k of n validators.

Scheme Generation

The private key is never produced or reconstructed throughout the whole network during the Locked Account creation procedure. The involvement of at least k validators is required to generate the signature of the Locked Account. They compute signature shares independently using the key shares they own and then use signature shares to reconstruct the complete signature. The Signature Scheme for Locked Accounts is as follows:

Calculate the Signature Shares in Step 1 Using key shares, several n Lithosphere Validators compute signature shares of the message.

Step 2: Distribute the signatures.
Each Validator transmits his or her signature share to the others.

Step 3: Reassemble and broadcast the whole signature.
When a Validator gets more than k signature shares, it reconstructs the signature in its entirety and broadcasts it to other Validators:
signature=Construct Sig(signature share1,. ,signature sharek)

Step 4: They produce the Locked Account's complete signature, which includes the following information:
signature sharej=Generate Sig(m,key sharej)

Advantages

Even if a portion of the network is paralyzed or some important shares are lost, the entire system maintains stability and security. To reduce the threat posed by key share exposure, every validator's key share is updated regularly or when a triggering circumstance is satisfied.

Easy Integration and Efficient Data Storage

The initial transaction of the original chain is used to perform any operation on the Locked Account. There are no new transaction types or verification mechanisms. As a result, any chain may theoretically be merged with Lithosphere at a low cost. At the same time, unlike the multi-signature account scheme, which uses smart contract logic to accomplish multiparty management, the Locked Account creation strategy uses cryptographic principles to achieve multiparty management. There is just one signature on the final transaction, not multiple. As a result, this technique is more data storage efficient.

Smart Contract Token Transaction Anonymity

To achieve anonymity in smart contract token transactions on Lithosphere, ring-signature and one- time accounts are used. To make the sender anonymous, ring-signature combines the transaction sender with a group of false members. Each transaction generates a one-time account that cannot be connected to the actual owner.

A technique to lock the assets of the originating chain is required in almost all cross-chain transaction schemes. The locked assets will only be unlocked and returned to the original account or another account after the triggering condition is satisfied.

The Hashed TimeLock Contract system, the Trusted Third-Party Escrow Account strategy, and the Multi-Signature Account method are examples of existing techniques.

Fully Decentralized without Third-Party Participation

Secure multi-party computation is used to produce the Locked Account. A trustworthy third- participation party or endorsement is not required in this procedure. All we need is secure routes for information exchange and computation by Validators. The Locked Account generation technique is less expensive and more flexible than the trusted third-party escrow account scheme.

Secure and stable

Shamir's Secret Sharing Scheme (a.k.a. Shamir's (k, n)-threshold secret sharing scheme) is used to distribute the key for the Locked Account to Lithosphere validators. One component of the key share is held by each Validator. Even if several Validators go offline or lose their key shares, the Locked Account's signature can still be produced, and the trans-action can still be completed with at least k validators. As a result, the creation strategy for Locked Accounts can assure that.

One-Time Account System

The one-time account method is particularly essential as a basis for anonymity. Each user has a single primary account as well as several sub-accounts. So, if someone wishes to remain anonymous in a smart contract token transaction, they must create a related account and a one-time primary account in addition to their original one.

Ring Signature Scheme

In 2001, the Ring Signature method was introduced. It's a type of Group Signature scheme that's a little different. A trusted centre and secure setup are required for a Group Signature scheme, which means that the signer may be tracked by the trust centre. By eliminating the trusted hub and securing the system, the Ring Signature method overcomes this major problem.

Since the introduction of the Ring Signature method, numerous practical systems based on Elliptic Curve Cryptography (ECC), such as the trapdoor approach, have been developed. Trapdoor Ring Signature, Linkable Ring Signature, Anonymity Revocable Ring Signature, and Deniable Ring Signature are the four types of Ring Signature systems.

The Ring Signature method based on ECC is developed in Lithosphere to offer anonymity in Smart Contract Token transfers.

The Ring Signature scheme is divided into three sections. The following are the details, using the signer (P,x) as an example:

Get the public parameters using GEN. The signer uses the method GeneratePublicKeySet( ) with the public key as a parameter to build a public key set with n members from the global state:
publickeyset=GeneratePublicKeySet(P)
I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I
RING SIGNATURE: Create the ring signature. The signer uses GenerateRingSignature( ) to produce the ring signature for message m, using public keyset, I, and x: ringsig=GenerateRingSignature(m,public keyset,I,x)
VERIFY THE RING SIGNIFICANCE VerifyRingSignature( ), which returns true or false with public keyset, I, and rings: lag=VerifyRingSignature validates the ring signature of message m. (m,publickeyset,I,ringsig)
The ring signature is valid if the flag is true. Otherwise, it is void.

The key picture and ring signature in the Ring Signature scheme cannot be matched with a signer from the public key set. Anyone can check whether or not a signature is genuine, but no one can identify the signer.

Cryptography Based Security Guarantee

Many existing cross-chain trades employ logical security mechanisms, which rely on participants to watch out for their self-interest. To put it another way, players will not disrupt cross-chain transactions if it means harming their interests. This is known as "The Rational Participants Hypothesis." Lithosphere employs threshold secret-sharing technology, as well as original elliptic curve cryptography, to assure the security of the original signature solution.

The multi-party computing-based locked account management solution;

The ring signatures and one-time accounts-based privacy protection method for smart contract token transactions.

After beginning a cross-chain transaction, all following actions are performed automatically between Lithosphere validator nodes and do not require coordination from transaction participants. This leaves the security of cryptographic methods to ensure the system's seamless operation.

Smart Contracts

Identifying and defining various parties' financial links Smart contract improvements.

A Smart Contract is a contract that defines the relationship and value interaction conditions of one or more digital assets among multiple participants in terms of temporal succession and spatial location and is used to complete financial transactions of one or multiple digital assets among multiple participants.

The assets mapped on the Lithosphere chain by digital assets Lock-in, which allows Lithosphere's smart contracts to specify connections among many different digital assets at the same time, are referred to as digital assets.

The owners or consumers of various digital assets are referred to as multiple participants. They are represented as accounts in the Lithosphere chain, including user and contract accounts. Contract participants in crypto smart contracts might comprise numerous user accounts as well as many contract accounts.

The definition of financial transactions through smart contracts becomes a description of the connections among various digital assets and diverse ownership in time and space because the core of finance is the exchange of values across time and place.

The following are the limitations of current smart contracts:

- Can only operate on the same digital asset between two parties on the same chain;
- Can only transfer ownership of digital assets, making usage and ownership indivisible;
- Can only be triggered by a transaction, with no off-chain trigger conditions or legitimate off-chain information input.
- Realize applications of ownership and usufruct among multiple parties and multiple digital assets;
- Effectively get off-chain data input;
- Call other smart contracts in a smart contract in an enclosed or parallel manner as if the smart contract were a smart contract.

Key Distribution in Myriad Token management has permitted interaction between various digital assets and has become the object to define and program for Lithosphere's smart contracts. As a result, it has the capacity and the need to implement DeFi features like multi-role, multi-token, and usufruct separation (rights).

The capacity of a smart contract to handle many distinct account types while also defining the connections between numerous users and various smart contracts is referred to as multi-role.

After mapping distinct digital assets to Lithosphere using Lock-in, a smart contract on Lithosphere may describe the relationship between many different digital assets at the same time.

Separation of usufructs refers to the ability to separate the usufructs (rights) and ownerships of digital assets. The present smart contract may only transfer tokens as a whole from one party to another, and it is not feasible for one party to gain ownership of a digital asset while the other party obtains the usufruct, implying that ownership and usufruct are separate in traditional smart contracts. It is simple to establish more than two user accounts or contractual accounts in a single smart contract, allowing for the separation of ownership and usage accounts as well as financial activities such as mortgage loans across various digital assets.

The transfer of digital assets will be possible if the link between them is solely specified in terms of space. It is a borrowing connection between them if the relationship is characterized in terms of time. When the connection is described in terms of object attribution, it represents the ownership and usufructs of the objects. As a result, the logical abstraction of one or more relationships in terms of time, space, and object attributions can lead to the construction of various transactions ranging from simple to complex between various digital assets, even eliciting yet-to-be-realized financial innovations, allowing for limitless imagination.

Contract multi-triggering mechanism Diversity of triggering conditions

Because the present smart contract is triggered by a transfer to the contract, the current implementation of smart contracts is based on the transfer of ownership of digital assets.

When a user starts a transfer to a smart contract, for example, a node must first validate the legality of the transfer, which includes determining if the user's current financial balance on the blockchain supports the transaction. The smart contract then runs the relevant function for accepting the gift and judges it based on the function's predetermined response condition. For example, the smart contract will examine the entire amount of the donation and only accept it if it does not over the quota. Finally, a modified contract value or smart contract state will be placed into the block to indicate that the transaction has taken place.

We can see from the preceding analysis that the smart contract's functions will involve judgments on some criteria, but these conditions will not be checked if the smart contract is not triggered in the first place. The execution of the following rules in the smart contract will not be triggered even if the required circumstances are satisfied. Many financial transactions scenarios, such as a passive quantitative trading strategy, are impossible to execute if a smart contract cannot be triggered by factors other than a transaction. As a result, improving the triggering mechanism is the first step towards improving smart contracts for DeFi applications. Aside from supporting the existing active triggering method, two new triggering mechanisms are introduced: time triggering and event triggering. The extended triggering mechanism is also known as the multi-triggering mechanism.

The three trigger modes of the multiple triggering mechanisms are as follows:

- The active triggering mode is similar to the current smart contract triggering mode and is compatible with all smart contracts.
- Timing triggering mode refers to the ability of a smart contract to be activated by time circumstances such as a time point or duration.
- Event triggering mode indicates that a smart contract will be activated when a certain event happens, such as usual swaps over time, and such applications will be fully supported by time triggering mode. Capturing events is critical in automated trading and quantitative trading, for example. The events triggering mode must be used to initiate such occurrences.

At the moment, smart contracts can only handle information from within their blockchain, however, in the event of multiple triggering mechanisms, some of the triggering information will come from outside. As a result, smart contracts will provide an external information input interface and use different techniques to verify the validity and authenticity of off-chain data.

To do so, Lithosphere will first transmit outside data through HTTP or socks to the nodes, depending on common APIs offered by third-party data sources. Lithosphere will encapsulate data calls from certain widely used off-chain data sources, which will function similarly to a system call to supply data for node acquisition. Nodes can, however, create their datasources using the aforementioned data collection routes to get important data information.

The consensus process verifies the validity of the off-chain data acquired. When a node discovers that off-chain data is linked to specific smart contract triggering circumstances, the node will run and broadcast the smart contract. If a malicious node purposefully broadcasts a smart contract over the whole network, the network may simply terminate the smart contract during the execution phase if it is judged malicious, because the smart contract will be re-verified by other honest nodes before execution. Such malevolent conduct will have no impact on the smart contract's real operation, and there will be no opportunity to profit from unearned or arbitrage profits.

Incentive methods can also help with the issue of off-chain data entry effectiveness. Because data confirmation requires network consensus, nodes can only increase their revenue by pursuing quicker and more trustworthy data sources and accurately validating triggering circumstances. The high- efficiency network nodes would be rewarded due to the nature of the efficient market and resource allocation. The validity of the final data is unaffected by data generated by a few rogue nodes.

Enhancements and compatibility

Based on Ethereum and other blockchain smart contracts, Lithosphere's smart contract will be upgraded and developed. Functionality additions, such as triggering mechanisms, will be added depending on compatibility with existing smart contracts. Smart contracts already operating on Ethereum and other blockchains will be able to simply move to Lithosphere, and smart contract developers will be able to swiftly create on Lithosphere.

The next step will be to optimize programming languages and virtual machines for a more robust application development environment, as well as to provide more intuitive application development tools and debug environments for developers with less coding knowledge.

Contract enclosed call

The above improvements to current smart contracts will eventually allow smart contracts on Lithosphere to define relationships and interaction rules based on various conditions, among various values and participants, in time and space, allowing smart contracts on Lithosphere to build DeFi applications.

On Lithosphere, a smart contract may not only change account status and data, but it can also call another smart contract during execution if certain criteria are satisfied.

The following activities must be completed to implement Smart Contract A's call to Smart Contract B:

(1)Create an enclosed call smart contract.

A preset condition judgment and a preset condition rule for invoking the smart contract B are added to the code of smart contract A, and the parameter of the target smart contract address index is generated. The data input when smart contract A is triggered, as well as the outcome of the data computation, provides the foundation for the condition judgment. If the predefined criteria are met, the node will download and execute smart contract B.

The call condition is divided into two parts: rules and time. Rules are pre-programmed computation routines in a smart contract. Time conditions can be a pre-defined condition in a smart contract that is triggered when the smart contract is executed or a condition that checks the state of a smart contract regularly.

(2)The procedure for making an enclosed call.

i.When the smart contract A is activated, it will determine whether or not it is required to execute the smart contract B based on the preset calling circumstances.

ii. When the calling circumstances are satisfied, the preset calculation function is called, and the result is used as the smart contract B's input.

iii. The node that performed the smart contract A downloads the smart contract B to the local computing environment, inputs the data determined in the preceding step as the smart contract B's input data and starts executing the smart contract B.

The procedures outlined above can be used to execute smart contract A's call to contract B. We call the logic link between them an enclosed call of a smart contract because smart contract B is based on the state of smart contract A as the trigger and input data.

Smart contracts not only make decisions based on their business logic, but they may also invoke other smart contracts based on predefined criteria. It is therefore simple to create network-like call interactions between distinct smart contracts, establishing the value interaction across connected financial apps and thus allowing the creation of complicated applications. As a consequence, sophisticated financial services, such as a loan application based on future cash flow, maybe developed using enclosed smart contract calls. The Lithosphere platform can achieve complicated financial activities thanks to these features and the multi-trigger mechanism, which will be explained in the section on multi-trigger mechanisms.

Contract development

To fulfill a smart contract, the following steps need to be completed:

(1)Build a smart contract

The Lithosphere smart contracts are an evolution of current smart contracts. There should be two components to the contract: definition and description.

The defining section is consistent and Ethereum smart contract compliant. As a result, current Ethereum smart contracts are compatible with Lithosphere. It contains contract status, contract values, and methods for defining response conditions and rules.

(2)Release a smart contract

Following the publication of the smart contract, the definition section is recorded on the blockchain following current smart contracts. The description section will be merged with the trigger conditions of all smart contracts in the current blockchain to create a calling list that will be recorded in the block and accessible to the whole network.

Each row of entries in the calling list corresponds to a smart contract. In addition to the material in the description, each record has an index address that corresponds to the stored smart contract.

The next step will be to optimize programming languages and virtual machines for a more robust application development environment, as well as to provide more intuitive application development tools and debug environments for developers with less coding knowledge.

Timing and trigger conditions

Proactive triggers are similar to how smart contracts in Ethereum are activated, which is by a transfer to a contract address. The following procedures will be used to create the new time triggering mode and event triggering mode:

(1)Judge the trigger conditions by nodes

For execution, the Calling list is downloaded to the local node. To determine if each item in the list matches the trigger condition, the node will poll the list and download matching or local data.

(2)Trigger a smart contract

When the accounting node discovers that the condition of a certain smart contract is met while polling at a specific time, the node acquires the smart contract address from the Calling list and sends a particular transaction to activate the smart contract. At the same moment, the smart contract for the selected transaction will be downloaded by the whole network of accounting nodes.

(3)Execute the smart contract

A smart contract is performed in the same way as the current smart contract, that is, it is executed in the node's operational environment (virtual machine). The contract differs in that it has additional triggers and may be integrated into other contracts through triggering conditions, resulting in a chain of occurrences.

Rapid development and interface

Lithosphere will provide development environments for smart contracts as well as function libraries. These functions may be used by developers to speed up the creation of smart contracts. To make it simpler to access and interact with data, the development environment will encapsulate different blockchain, smart contracts, data sources, and so on as interfaces.

Here are some typical interfaces:

(1)Key management

- Initializing the key pair, creating and returning the public key address are all functions that must be implemented.
- Returning the signature hash value after entering the public key address and the associated signature.

(2)Blockchain data acquisition

If blockchains are thought of as systems that allow distributed applications (DApps), smart contracts collecting blockchain data will be the same as getting the blockchain system's global variables. Smart contracts can access the following information on the blockchain using this interface:
Aim for a specific block height. The sender's information. The recipient's information.

(3)Call of smart contracts

Smart contracts are used to implement all of the Lithosphere's functionalities.
The use of a transfer smart contract may be used to make a transfer in a smart contract. To encompass typical financial applications, Lithosphere will employ more basic smart contracts. As a result, developing a smart contract on Lithosphere entails embedding simple smart contracts into conventional financial apps and then enhancing their functionality by adding more complicated functionalities.

Lithosphere will identify fundamental financial contracts, resulting in a smart contract library for developers to employ.

(4)Off-chain Datasource interface

On trigger circumstances, smart contracts employ off-chain data. Such data is frequently obtained using a standard HTTP or socks-based API supplied by a third party. A third-party interface call function, for example, will obtain the destination URL's address through HTTP and return a JSON packet.

This interface method can also be used to get information from other blockchains, such as querying and confirming whether a transaction in another chain is confirmed by the block where it is located.

The Foundation will be used by Lithosphere to discover third-party interfaces and create third-party interfaces for smart contracts to call.

(5)Rapid development

Lithosphere will provide several smart contract templates for common applications for reference and usage by application developers in the early phases of the project. However, application developers must still fulfill certain code standards.

Application developers can use smart contracts by creating preconditions to actualize the desired financial apps as the platform's underlying functionalities and common financial basic applications grow more resourceful and complex. . To further improve such a development environment and drastically reduce the development threshold for developers, Lithosphere's plan includes visual and modular application development tools, a compilation environment, an application test environment, which will allow smart contract developers to focus on innovations in financial applications and a Launchpad to launch dApps.

(6)Programming language and virtual machine

For interoperability with smart contracts and quick porting of existing smart contracts, Lithosphere will initially employ Ethereum's Solidity programming language. We will provide compilers for several languages in the future to accommodate more smart contract development languages.

We'll create a smart contract sandboxing system that performs particular fail-safe checks and fuel cost minimization using a browser or programming editor.

To use multiple triggers to realize complex financial functions

Existing smart contracts can only passively wait for a transaction's trigger to be performed by a transaction, which presents the issue of needing the introduction of a trusted broker to establish who has the right to trigger a smart contract and under what conditions. On the Lithosphere platform, smart contracts will describe the relationships between parties through code (whether by common smart contract or by enclosed contracts). Multiple triggers will automate the execution of these smart contracts, allowing them to be engaged one after the other without the need for human interaction. As a result, many parties may trust each other using smart contract codes to perform a range of complicated financial activities. Lithosphere smart contracts provide the capacity to program ownership and usufruct independently, allowing triggers to lend usufruct to another depending on time or other conditions and execute them as promised until the final right of usufruct and ownership is restored to the participants.

Smart contracts may now perform a wide range of financial activities thanks to this functionality. For example, if you want to borrow money, you may design the Lithosphere smart contract to borrow tokens, return fresh currency, and pay interest. Using the Lithosphere platform as an example, a smart contract may autonomously administer a fund, including taking the usufruct of various tokens into a smart contract, keeping various digital assets, producing management fees, paying the dividend, and so on. Using the example of various derivatives, the smart contract may take margins and perform operations such as modifying margins, liquidating, and settling using external data source triggers.

Community operation plan

The KaJ Labs Foundation, as the project's main sponsor, is aiming towards a promising blockchain ecosystem rather than corporate profitability as typical enterprise and startup initiatives do. The Lithosphere platform, which benefits all token holders, is not owned by any single entity or person. The whole blockchain token community owns the Lithosphere platform. Lithosphere makes token usage more flexible and accessible, as well as giving tokens the potential to offer sophisticated DeFi services. The value of all tokens will increase.

In reality, the Internet of Values' cross-chain ecosystem is a massive project. The Kaj Labs Foundation must progress the ecosystem, which must be joined and participated in by the whole community, and whose blockchain must be enhanced via continual iteration. This is exactly what the features of a blockchain project are. Blockchain initiatives begin with a critical need or problem to be addressed, which must be continually investigated by participants and those in need to encourage continuous progress. At the same time, it will draw more individuals into the community, causing demand to shift the projects in a better direction and encourage the advancement of its technology. The purpose of the echoes is to generate a positive feedback loop of incentives, applications, and usage. As a result, project operations concepts must be community-oriented from the start, and community operations are linked to the success or failure of the blockchain project.

The following people make up the community:

- The Core development team and the Kaj Labs Foundation. They are the project's platform's sponsors and facilitators.

  Programmers who want to be a part of the project. They can join the Foundation development team or independently create and optimize Lithosphere as a third party if they are interested in projects or project technologies.

- Participating nodes in the Lithosphere They make money by keeping track of ledgers and operating smart contracts while also maintaining Lithosphere.

- Users of the Lithosphere platform. For DeFi and other services, they employ the Lithosphere platform. • On the Lithosphere platform, DeFi service providers such as payment institutes, centralized or decentralized exchanges, lending institutes, and other financial service providers.

- Lithosphere token holders, such as private equity companies, early-stage investors, late-stage investors, and potential investors.

- Other parties involved in the development of Lithosphere, such as the media, government, and so on.
  The goal of community operations is to gather as much force as possible and arrange it in the most efficient way possible so that Lithosphere can iterate, improve, influence, and serve a wider community.

  The growth of the community is inextricably linked to both the core and outlying communities. The two are mutually beneficial, with the core community serving as the focal point. The peripheral community, on the other hand, must continue to participate in the creation of the key community since the core community will originate from and borrow from the peripheral community, and the peripheral community will require the core community's resources to support them. We discovered that Bitcoin, Ethereum, and other projects have all grown in the same way. The core community consists of early adopters, blockchain technology communities, and blockchain value communities, while peripheral resources include additional investors, users, developers, journalists, and other interested parties.

Project promotion method

- The concept separates community operations into two categories: core and periphery. The former prefers the offline mode, whilst the latter prefers the internet mode. The following is the strategy for key community operations:

- Lithosphere Foundation team: the team will be rewarded with tokens. One reason is to compensate for the resources used in the previous time, and the other is to allow anybody to become a shareholder and expect them to contribute to Lithosphere in the future.

- Community for blockchain technology.

- Technology is both the most important and the most difficult aspect of blockchain development. We will utilize online and offline methods to discover and nurture a group of top-tier talents to promote the technological community, using the founding team's technical expertise and social resources.

- Blockchain value community: Using the blockchain technology community, we can organize gatherings with holders to disseminate blockchain knowledge while also promoting opportunities for collaboration with the private value community.

A movement to Promote Blockchain Technology

The Internet of Values presently has a usability bottleneck, which will require continuing work in the future to improve. The usefulness of the Internet of Values is strongly connected to the Lithosphere project. To contribute to the usefulness of blockchain technology, we will start the "blockchain technology promotion movement." For the Kaj Labs Foundation, this will be a long-term project.

In the form of technical salons, training camps, and seminars, this movement will continue to amass skills and technical information. We will encourage participants to provide content, which will be published on numerous websites and in the media. To grow the technical community of blockchain, we will provide monthly training sessions to recruit conventional Internet employees and other technical staff.

The blockchain technology promotion movement will bring together all forces, including universities, research institutes, businesses, institutions, governments, and alliances, to create a cooperative partnership and pool resources to support blockchain technology's advancement.

The Standardization of Blockchain Interfaces Movement

The Internet of Values has interoperability and scalability problems that require many parties to address. The Lithosphere project is inextricably linked to these two obstacles' breakthrough development and advancement. By establishing the "Blockchain Interface Standardization Movement," we will help to enhance them. For the Lithosphere Foundation, this will be a long-term project.

The movement will encourage standardization of interfaces not just between blockchains, but also between decentralized and centralized organizations, as well as between blockchains and external data sources.

Lithosphere Applications

Borrowing and Lending

Using digital money to produce new value and earn revenue is an unavoidable trend as it grows in importance as a medium of value exchange and a value storage carrier. Bitcoin, for example, is used to fund blockchain mining companies and other crypto initiatives. Direct investment options for digital currency have expanded as the variety of applications for digital money has grown.

Those who generate value with digital currencies need more of them, and people who own digital currencies want to raise their value, thus demand for borrowing and lending digital currencies will rise.

Consider the cryptocurrency Ethereum (ETH). On Lithosphere, a service provider creates a deposit application and sets the interest rate using a smart contract.

Through a cross-chain transaction, a user sends ETH from the Ethereum blockchain to the Lithosphere smart contract address. The deposit on Lithosphere generates a voucher (Lithosphere tokens that look like deposit bank receipts) that is credited to the user's Lithosphere account. The smart contract then calculates the interest for you. When the user wants to withdraw the money, the voucher is sent to an intermediate address, and a cross-chain transaction is carried out. On the original chain, the ETH corresponding to the voucher is unlocked and sent back to the original user's account. Deposit reserves (the assets locked on the originating chain that correspond to the intermediate address) are always visible.

Payment and Settlement

Businesses are increasingly accepting digital assets such as Bitcoin as a form of payment. There will be more applications in the future that employ a range of digital currencies for payment. There are several payment options available today, including VISA, Paypal, and Alipay, each with its own set of payment and settlement procedures. The lithosphere is a multi-currency distributed platform that combines many banking ledgers into a single unified ledger. Without needing to install several digital currency wallets, any business or user may utilize the Lithosphere wallet to make multi- currency payments and settlements.

Transaction and Exchange

At the moment, centralized exchanges and over-the-counter marketplaces are required to complete digital currency trades. Every transaction is dependent on the exchanges' and intermediaries' confidence. After several currencies have been linked with Lithosphere, exchanges and intermediaries may use smart contracts to enable multi-currency auction trading and one-to-one curb transactions. On Lithosphere, the privacy protection transaction mechanism supports transactions that require privacy protection. Importing digital money into Lithosphere, starting private transactions on Lithosphere, and moving digital currency back to the original chain are all possible with Lithosphere. The original chain's privacy is protected to some extent by concealing the fund tracking paths. Lithosphere can handle 10,000 transactions per second (TPS) compared to Bitcoin which processes 4.6 transactions per second, Ethereum does 15 TPS, and Ripple handles 1,700 TPS. Visa does around 1,700 transactions per second on average (based on a calculation derived from the official claim of over 150 million transactions per day).

Investment and Financing

Traditional institutions are increasingly turning to consortium chains to store assets such as commercial invoices, loyalty points, future earning rights, and accounts receivable. More financial assets will be recorded on consortium chains-based distributed ledgers in the future. When these consortium chains connect to Lithosphere, they become financial asset providers, and investors may acquire these assets with their digital currencies. It's similar to buying financial goods at a bank, as in the traditional banking company. The main distinction is that more intermediaries can participate, and asset owners can finance themselves directly.

In the blockchain world, Initial Coin Offerings (ICOs) / initial exchange offerings (IEOs) have become a popular way to raise funds, and the practice is expanding to non-blockchain domains. Smart contracts are being used directly for ICOs by an increasing number of projects, particularly those built on Ethereum or BSC, making the process more open and equitable. However, ICOs that exclusively accept Ether annoy investors who possess other digital currencies. The ICO issuer can use Lithosphere to create a smart contract that enables multi-currency investments. Investors may invest more easily using Ethereum, Bitcoin, or any other blockchain token linked with Lithosphere, and issuers can manage their funds more simply. Furthermore, when a new blockchain is released, the Lithosphere cross-chain transactions may be used to convert the crowdfunded shares to the local currency. With Lithosphere, we're entering a new age of blockchain-based digital right issuing

More Applications

The financial applications mentioned above are meant to help readers better grasp Lithosphere's rationale and value. More examples include multi-currency credit cards based on digital money, asset- backed securities that bundle a range of assets, peer-to-peer lending firms based on digital currencies, and crowdfunding, among others.

Major banks see blockchain technology as an essential strategy, but they're also looking at how it might be used to alter traditional business.

Banking, such as currency exchange, has been flourishing in the realm of digital money. In these sectors, blockchains are progressing on two parallel tracks, but with the emergence of digital assets and their increasing integration into the actual economy, these two tracks will eventually cross. Bank balance sheets will be largely moved to blockchains, and digital assets will be incorporated in bank balance sheets (banks that enable the loan and deposit of digital assets) (fiat money is represented and accounted for by blockchain tokens). This future integration will be supported by Lithosphere's inter-ledger technology.

Current Lithosphere Features

Interoperability

Cross-chain interoperability through a decentralized custodian model (MDKM)

Next-generation Blockchain for NFTs

A scalable, decentralized, cross-chain network designed to bring non-fungible tokens to everyone.

Time-Lock Feature

Lithosphere's unique Time-Lock feature enables you to extract time-value out of your digital assets

Security

Manage and control private keys in a distributed manner with MDKM technology

Scalability

Solving the scaling problem is an open issue for PoW blockchains like Bitcoin and Ethereum v1. Currently, Bitcoin & Ethereum nodes process every single transaction and also store all the states. Since Lithosphere's proof-of-stake can commit blocks much faster than Proof-of-work, EVM zones powered by Lithopshere's consensus and operating on bridged-crypto can provide higher performance to PoW blockchains Ethereum, Litecoin & Bitcoin.

Digital Assets

Create, manage or even lend your own digital assets & NFT's using the Lithosphere's LEP100 protocol.

Cross-chain gaming assets.

Game economies, owned by players.
Create in-game assets that are available forever. Bring lasting value to gamers by letting them take their loot to another game or into the real world on the JOT ART blockchain-powered by Litho.

Lithosphere Products

- Lithosphere blockchain (PoS) Litho cross-chain native token
- LithoSwap - cross-chain DEX with NFT exchange support.
- LEP100 Token Launchpad - Litho Launchpad
- Thanos Multi-currency, cross-chain wallet
- JOT NFT Platform (NFT marketplace, NFT DEX, SDK to distribute NFT anywhere cost- effectively, cross-chain)
- FLEEK - Decentralized community-powered gig platform on the blockchain.
- LAX - Algorithmic Stablecoin

Lithosphere Project Governance

Council Members

Elected to represent passive stakeholders in two primary governance roles: proposing referenda and vetoing dangerous or malicious referenda. Lithosphere creator Joel Kasr chairs the council committee.

Technical Committee

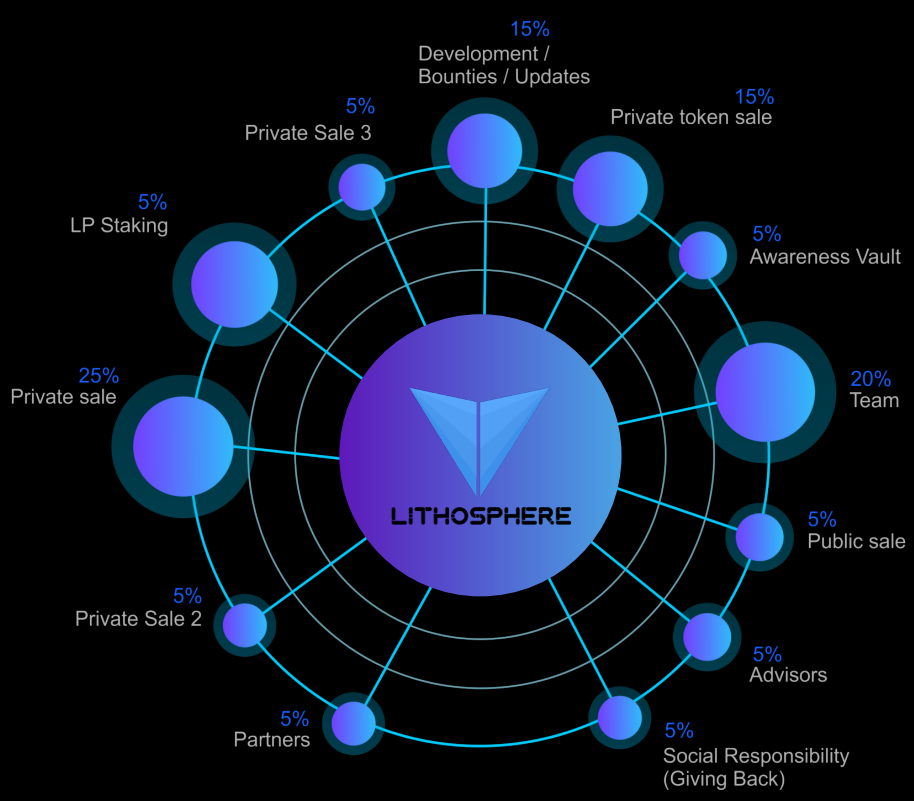
Composed of core teams actively building Litho. Can propose emergency referenda, together with the council, for fast-tracked voting and implementation.

Community Members

Can make and vote on proposals to improve Lithosphere.

Tokenomics

Total Supply : 1 billion



Funding for the project:

The initial distribution of litho coin and validators on Kamet (the first version of Lithosphere network) will go to the donors of the Lithosphere Fundraiser (70%), lead donors (5%), KaJ Labs Foundation (10%), network awareness (10%) and the core team members (10%). From Kamet onward, 1/3 of the total amount of $Litho will be rewarded to bonded validators and delegators every year.

One of the vaults / Capsules in the Lithosphere will be set up to hold marketing/awareness funds.

Roadmap

Q3 2021

- Finalize network concept
- Core development team formation
- Lithopshere White paper published
- Establish key partnerships
- Major announcements

Q4 2021

- NFT DEX Testnet
- Media presence
- Introduce new token standard - LEP100
- Introduction of governance in the Lithosphere network using native Litho token.
- Litho token presale

Q1 2022

- Launch of Jot NFT Platform testnet
- Launch cross-chain wallet - Thanos Wallet
- Team expansion

Q2 2022

- Jot Art NFT marketplace mainnet live.
- Implement DNNs in LithoSwap
- Lithosphere core team augmentation.
- Establish Litho network testnet
- Public Token sale / IEO.

Q3 2022

- Implement DNNs in Thanos Wallet.
- JOT Token Private Sale
- Start development of Decentralized community powered gig platform on Blockchain - Fleek
- Release Jot Art SDK
- Launch Litho Launchpad
- Release blockchain mobile game on JOT NFT Platform
- LAX - Algorithmic Stablecoin

Conclusion

The Lithosphere project has created a BFT algorithm, a new token standard, Litho currency (LITHO), and a key distribution mechanism to achieve the goal of the inclusive decentralized platform. The design of the native token is mostly comprised of the following five elements:

1.Number. A total of one billion tokens are available. This amount will allow the token to launch at an acceptable price and continue to grow steadily from there.

2.A system for distributing tokens. To achieve the idea of non-inflation, the supply of tokens should be limited. This benefits the early members and makes the system more stable in the long run.

3.The allocation of tokens. To realize the decentralized notion, the token distribution must be properly balanced. We award a 10% ratio to the Lithosphere team because of their continuous devotion and efforts to promote Lithosphere's inclusivity in cross-chain, cross-organization, and cross-data source initiatives. Furthermore, because Lithosphere's accounting nodes perform more complex functions than ordinary public chains, they will get around one-third of the entire sum. The remainder will be utilized for environmentally friendly buildings.

4.Environmentally-friendly construction. More than half of the funds will go to the Foundation to help the project flourish, particularly in terms of cross-chain, cross-organization, and cross-data features. To allow additional value to be conveyed on the chain and to aid the development of new smart contract applications, the project will also require a token exchange mechanism.

5.Fuels and miners In a distributed node control system, a range of values will enter the Lithosphere. To control tokens, the chain requires a large number of dispersed nodes. The more nodes there are, the more secure the chain will be, and the more nodes are required as the chain's value grows. The chain must compensate miners by releasing tokens and charging service fees to sustain the number of nodes and calculation power.

Lithosphere was born out of necessity. Our development teams have always been spread throughout the world from the beginning of KaJ Labs, yet we've always had problems working effectively. We have to enhance our entire performance and processes for our teams to stay distributed.

We recognized there were several inefficiencies with the existing commonly utilized blockchains like Ethereum, Cardano, and others after working on numerous blockchain projects. The most serious issue was that these blockchain networks were unable to connect. You couldn't buy ERC721 NFT using a BEP20 token, BTC, DOT, or BNB until Lithosphere. Blockchain networks must be in sync with one another for blockchain and DeFi to grow into the future we all want. Transaction expenses/gas fees are another challenges that networks like Ethereum confront. On the Ethereum network, almost every activity costs money. The KaJ Labs team set out to create a worldwide blockchain network that is quicker, cheaper, and more environmentally friendly than existing blockchains such as Cardano, Polkadot, and Ethereum 2.0. Lithosphere may be thought of as the foundation for both old and new blockchains. The Lithosphere ecosystem is powered by the native currency $LITHO /Litho.

Disclaimer

This Lithosphere Whitepaper is for information purposes only. The KaJ Labs Foundation does not guarantee the accuracy of or the conclusions reached in this whitepaper, and this whitepaper is provided “as is”. KaJ Labs Foundation does not make and expressly disclaims all representations and warranties, express, whether explicit, implied, statutory, or otherwise, whatsoever, including, but not limited to: (i) that the contents of this whitepaper are free from error; (ii) that such contents will not infringe third-party rights; and (iii) warranties of fitness for a particular purpose, suitability or function. KaJ Labs Foundation and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this whitepaper or any of the content contained herein, even if advised of the possibility of such damages. In no event will KaJ Labs Foundation or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs, or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this whitepaper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses.

Glossary

LEP100: Lithosphere Evolution Proposal

WHITE PAPER: A guide about a specific topic and the problem that surround it. It is meant to educate readers and help them to understand and solve an issue.

BLOCKCHAIN: A growing list of records, called blocks, that are linked together using cryptography.

TOKEN: A token represent a set of rules encoded in a set of smart contracts. Each token belongs to a blockchain address. It is essentially a digital asset that is stored securely on the blockchain.

DECENTRALIZED: Type of cryptocurrency exchange which allows for direct peer-to- peer cryptocurrency exchange to take place online securely and without the need for an intermediary.

EVM: Ethereum virtual machine is a computation engine which acts like a decentralized computer that has millions of executable projects.

BSC: Binance smart chain

PEGGED COINS: LEP100 tokens pegged to external assets.

DAPPS: Decentralized Applications are digital applications that run on a blockchain or peer-to- peer network of computers instead of a single computer.

NFT: A non-fungible token is a unit of data stored on a digital ledger, called blockchain, that certifies a digital asset and therefore not interchangeable.

INTEROPERABILITY: The ability of computer systems or software to exchange and make use of information.

ERC: Ethereum request for comments

BURN: A process by which digital currency miners and developers can remove tokens or coins from circulation.

TRACTION: Drawing or pulling rate in a business.

DEFI: Decentralized finance

CROSS CHAIN: It is the interoperability between two relatively independent blockchains.

DEX: Decentralized exchange