LITHOSPHERE

Litepaper

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

KaJ Labs Foundation is building a new generation of financial infrastructure based on blockchain technology. The project, Lithosphere, aims to build a value transfer infrastructure for the Internet of Values. It will connect past and next-gen smart contracts, solving the problem of insufficient interoperability.

Design Concept

The lithosphere is a network of blockchains able to communicate with each other in a decentralized way. Lithosphere's vision is to connect all blockchains and break the barriers between blockchains by allowing them to transact with one another. The end goal is to create a connected network of blocks that can process transactions quickly and communicate with other blockchains. Two and a half billion individuals worldwide are unable to use banks, create savings accounts, or acquire credit cards. Many organizations are exploring ways to record traditional forms of assets, such as bills and loyalty points, into blockchains. Inclusionary finance is reaching new heights thanks to the development of blockchain technology.

Design Background

Lithosphere aims to develop a more widely disseminated blockchain technology and digital asset applications. The world has changed dramatically as a result of the Internet of Values. Lithosphere's goal is to create a decentralized platform for the trading of non-fungible assets and digital currency. Internet of Values will allow individuals to handle values as if they were informed. The Internet of Values is still in its early phase, with interoperability, scalability, and usability limitations.

It must be adaptable to a variety of circumstances, including banking, industry, and government administration. The Internet of Values has a lot of work ahead of it in terms of standardization, platformization, functional modularity, application ecology, interoperability, and anti-quantum assaults. Interoperability is the most pressing of the three types of obstacles listed above. It allows us to move assets between blockchains, design smart contracts, and improve update scalability. The Internet of Information has already had a significant influence on our lives.

We may also anticipate significant changes in our lives as a result of the Internet of Values. The Internet of values will have a wider range of values than traditional financial markets. It will allow more and more values to enter themselves through the process of tokenization.

Positioning

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 with the help of blockchain, AI, and other technologies.

Lithosphere Architecture and Technology

Architecture

The Internet of Values (DeFi) can substantially improve its interoperability if multi-token smart contracts can be implemented. The present cross-chain technology uses a two-way peg to transfer transactions to side chains and multiple signatures to exit side chains. We need to create a public chain that allows other tokens to be mapped to it in a more inventive fashion. In this key generation protocol, we use elliptic curve cryptography to generate keys for VSS and DKG. The process is based on a finite field GF (q) with n participant sets Q = P1, P2, Pn, pi, Pi, where p(x) mod p is a prime number or factor.

Threshold signature

The threshold signature technique can address the issue of signatures created by departing nodes while also improving the network's stability. Lithosphere will choose appropriate nodes to join and refresh the shared key parameters in extreme circumstances.

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. The currency of choice in the Lithosphere network is $LITHO although another crypto can be used as well.

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

The lithosphere is a new platform that aims to build an infrastructure platform to run decentralized applications. The goal of Lithosphere is to use blockchain technology to create value interoperability between different types of tokens. When a registered asset is moved from the original chain to Lithosphere, Lithosphere will issue equal tokens in existing contracts.

Cross-Chain Integration

The lithosphere is a decentralized trading platform that allows you to trade and exchange tokens with other users.

Cross-Chain Transactions

Token Lock-in is a process that enables distributed key management and asset mapping for all key-managed tokens. After Lock-out is completed, control of the digital asset is returned to the owner, restoring complete key storage and centralized key management. The goal is to improve the security, liquidity, and DeFi applications of current digital assets.

Deep Neural Networks (DNN)

Deep neural networks (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 platforms. Lithosphere implements DNN to make smart contracts smarter by incorporating large-scale deep neural networks.

LEP100 Multi-chain Token Standard

The LEP100 token development standard for the Lithosphere network is similar to ERC20, but it's more user-friendly. It allows a single contract to represent numerous fungible and non-fungible tokens. The tokens can also be easily integrated into any other networks or chains.

Validators

The lithosphere is a decentralized, proof-of-stake cryptocurrency. In the system, nodes have a non-negative amount of voting power and nodes that have positive voting power are called validators. They participate in the consensus protocol by broadcasting cryptographic signatures to agree upon the next block.

Linear-communication BFT Consensus

The Lithosphere protocol uses a Byzantine Fault-Tolerant consensus algorithm. This algorithm guarantees safety for up to a third of Byzantine, or malicious, actors. It allows public and private blockchains to transfer tokens to each other. In the future, it could be possible that every participant could be honest for one block, and malicious for another.

Myriad Distributed Key Management (MDKM)

Myriad Distributed Key Management realizes the control and management of accounts and assets on the target blockchain in a distributed manner. By supporting a signature algorithm with MDKM, a series of encrypted digital assets with the same signature algorithm can be controlled and managed. Most (over 80%) of encrypted currency adopt the same ECDSA signature algorithm as Bitcoin and Ether.

LEP100 Token Standard

The Lithosphere network is a multi-chain architecture that allows anybody to develop dApps and other blockchain-based digital assets. It ensures cross-chain trade, minimal gas consumption, and quick transactions with safe transactions. LEP100 makes it possible for tokens on the Lithosphere chain to function properly.

Verification Nodes

The lithosphere is a network that allows people to verify transactions and earn transaction fees. 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.

Locked Account Generation Scheme

Cryptographer Adi Shamir devised the Shamir's Secret Sharing threshold key sharing technique. The method is intended to address the issue of secure key management in distributed computing. Each activity on an account will need the cooperation of at least k individuals to maintain the account's security.

Smart Contract Token Transaction Anonymity

The lithosphere is a smart contract token system that allows users to send and receive tokens in the same chain. To achieve anonymity, ring-signature and one-time accounts are used. The Hashed TimeLock Contract system, the Trusted Third-Party Escrow Account strategy, and the Multi-Signature Account method are examples of existing techniques.

Advantages

- Fully Decentralized without Third-Party Participation
- Secure and stable
- One-Time Account System
- Ring Signature Scheme
- Ring Signature Scheme

Cryptography Based Security Guarantee

The lithosphere is a new cross-chain trading system for smart contract tokens. Lithosphere uses cryptosystems to ensure the security of cryptographic methods to ensure its seamless operation. The technology is based on "The Rational Participants Hypothesis," which states that players will not disrupt cross-Chain transactions if it means harming their interests.

Smart Contracts

Lithosphere's smart contracts can only operate on the same digital asset between two parties. This means they can only transfer ownership of digital assets, making usage and ownership indivisible. The lithosphere is working on improvements to its smart contracts that will allow it to identify and define various parties' financial links.

Smart Contracts

The lithosphere is a smart contract platform that allows for multi-role, multi-token, and usufruct separation (rights) It has the capacity and the need to implement DeFi features like multi-user, multi-token, and multi-contracts.

Contract multi-triggering mechanism

The current implementation of smart contracts is based on the transfer of digital assets. Many financial transactions are impossible to execute if a smart contract cannot be triggered by factors other than a transaction. Time triggering and event triggering mechanisms have been added to improve smart contracts for DeFi applications. The lithosphere is a new smart contract system that will allow nodes to receive data from outside the chain. It will use different techniques to verify the validity and authenticity of off-chain data. Lithosphere will encapsulate data calls from certain widely used third-party data sources, which will function similarly to a system call for node acquisition.

Enhancements and compatibility

The lithosphere is a smart contract platform that will allow developers to create and develop smart contracts on the same platform as existing smart contracts. Lithosphere's next step is to optimize programming languages and virtual machines for a more robust application development environment, as well as to provide more intuitive development tools and debug environments for developers with less coding knowledge.

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

(1) Create an enclosed call smart contract.

(2) The procedure for making an enclosed call.

Contract development

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

(1) Build a smart contract

(2) Release a smart contract

To use multiple triggers to realize complex financial functions.

The lithosphere is a platform that allows smart contracts to perform complex financial activities without the need for human interaction. 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.

Community operation plan

The Internet of Values' cross-chain ecosystem is a massive project. The KaJ Labs Foundation, as the project's major sponsor, is aiming towards a promising blockchain ecosystem rather than corporate profitability. Lithosphere makes token usage more flexible and accessible, as well as giving tokens the potential to offer sophisticated services.

Project promotion method

The Lithosphere project is a community-run organization that aims to make the internet accessible to all users. The concept separates community operations into two categories: core and periphery. The former prefers the offline mode, whilst the latter prefers the internet mode. In the future, the team will be rewarded with tokens for their efforts, and they will be able to contribute to the project.

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. To contribute to the usefulness of blockchain technology, we will start the "Decentralize Everything" movement. The movement will be a long-term project, with monthly training sessions for conventional Internet employees and other technical staff.

Lithosphere Applications

- Borrowing and Lending
- Payment and Settlement
- Transaction and Exchange
- Investment and Financing

More Applications

Current Lithosphere Features:

- Interoperability
- Next-generation Blockchain for NFTs
- Time-Lock Feature
- Security
- Scalability
- Digital Assets
- Staking
- Cross-chain gaming assets.

Conclusion

The Lithosphere project has created 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: A total of one billion tokens are available. 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.