LEMOON

MAKE WEB3 LINKS EASIER

A web3 synthetic wallet consisting of HD wallet, MPC wallet, and multi-signature wallet

INTRODUCTION

Lemoon redefines the custody of encrypted assets. The world's first synthetic web3 wallet consists of three product units: HD wallet, MPC wallet and multi-signature wallet. It provides you with complete control over your assets. Multi-party governance aims to protect your assets and manage your assets. Explore the latest trends and opportunities in GameFi, SocialFi, Defi, and NFTs with lemoon Web 3.0 portfolio.

WEB 3.0 GAME STORE

Lemoon is committed to creating the 'Steam' of Web 3.0, building a web 3.0 game ecosystem based on web 2.0, assisting traditional game manufacturers to upgrade web 3.0 games, providing the necessary infrastructure, and open source web 3.0 game development tools and other applications

NATIVE/MPC DUAL-CORE SWITCHING MODE WALLET

Web3.0 ecological seamless connection

- Users can easily enter the Web3.0 Crypto ecosystem and connect seamlessly
- Use more DApps and manage your asset tokens
- DApp realizes automatic chain switching

Simple and convenient to use

- Users can freely switch between native wallets or MPC wallets as needed
- No mnemonic mode can beselected to create a wallet
- EVM, MOVE and other multi- chain asset wallets

More Advanced Security Solutions

- Secured by Multi-Party Computation (MPC) Technology
- Account reset and recovery through Thresh-old Signature Scheme (TSS)
- Server-side identity validation

Better Wallet Experience

- Team management with Co- Admin Mode
- Import, export, and sync MPC Unit
- DApp integration within the dashboard

SECURE MULTI-PARTY COMPUTATION (MPC) SCHEME-1

The initialization of the Lemoon wallet will independently generate an MPC unit on the user's local device, the Lemoon server, and the third-party cold storage. The signature is completed when any two of the three MPC units run the Multi-Party Secure Computing (MPC) protocol. This 2-3 threshold signature management scheme will not generate any complete private key, which minimizes the risk of wallet single-point failure.

SECURE MULTI-PARTY COMPUTATION (MPC) SCHEME-2

Security Through Lemoon Server.

Lemoon's MPC server dynamic node strategy ensures efficient and stable operation of wallet services, Lemoon server can provide additional and optional user-identity validation when logging in, authorizing DApps, initialing transactions, or changing account settings. The validation process consists of Login Password, Payment PIN, Email Verification Code, and other 2FAs that can be toggled on/off by the user. Control your digital assets towards efficient accessibility, multi-layer security, or both at your fingertips.

SECURE MULTI-PARTY COMPUTATION (MPC) SCHEME-3

Account Recovery Made Possible

Lemoon delivers a fail-safe mechanism powered by the MPC algorithm that eliminates the horrible situation where your device is lost or stolen and the awful experience of contacting customer support to try to recover account access. We have contemplated every scenario and have designed the best solution to reset and recover your account to save the day.

SECURE MULTI-PARTY COMPUTATION (MPC) SCHEME-4

DApp Approval Management

Lemoon displays the pre-authorized token amount for each approved project/contract when viewing that asset. Users can quickly identify which approval was unauthorized or mistaken and can de-authorize them with a single click from Lemoon.

The Co-Admin Mode

Add co-admins to the wallet, entitling them to the responsibility to approve or decline transactions, authorizations, and other actions initiated by this wallet. Activating the Co-Admin Mode will maximize the wallet's security, qualifying for an institutional-level wallet solution.

CREATE THE ECOLOGY OF WEB 3.0-1

Native dApp Network

Access Web3 dApps from your wallet, including Dexs, GameFi, Exchanges, Social media, NFT marketplaces, and more.

Web3.0 Games Store

GameFi's publishing and trading ecology serving the Web3.0 ecology

CREATE THE ECOLOGY OF WEB 3.0-2

NFT Gallery

Store, buy, and swap NFTs across multiple chains platforms. Easily display, safely store, and conveniently access your NFTs all in one place.

Decentralized Identifiers (DID)

Generate and control your own digital identity with Lemoon in surfing the Web 3.0. Your new Web 3.0 DID will be as secure as your Lemoon-stored digital asset. Enjoy the Lemoon ecosystem.

LEMOON SYNTHETIC WALLET

Lemoon is the world's first web3 synthetic wallet. It consists of three product units: HD wallet, MPC wallet and multi-signature wallet. It not only takes into account the use of professional users and organizations with multi-signature joint management of funds, but also takes into account the novice users without private key mode. use.

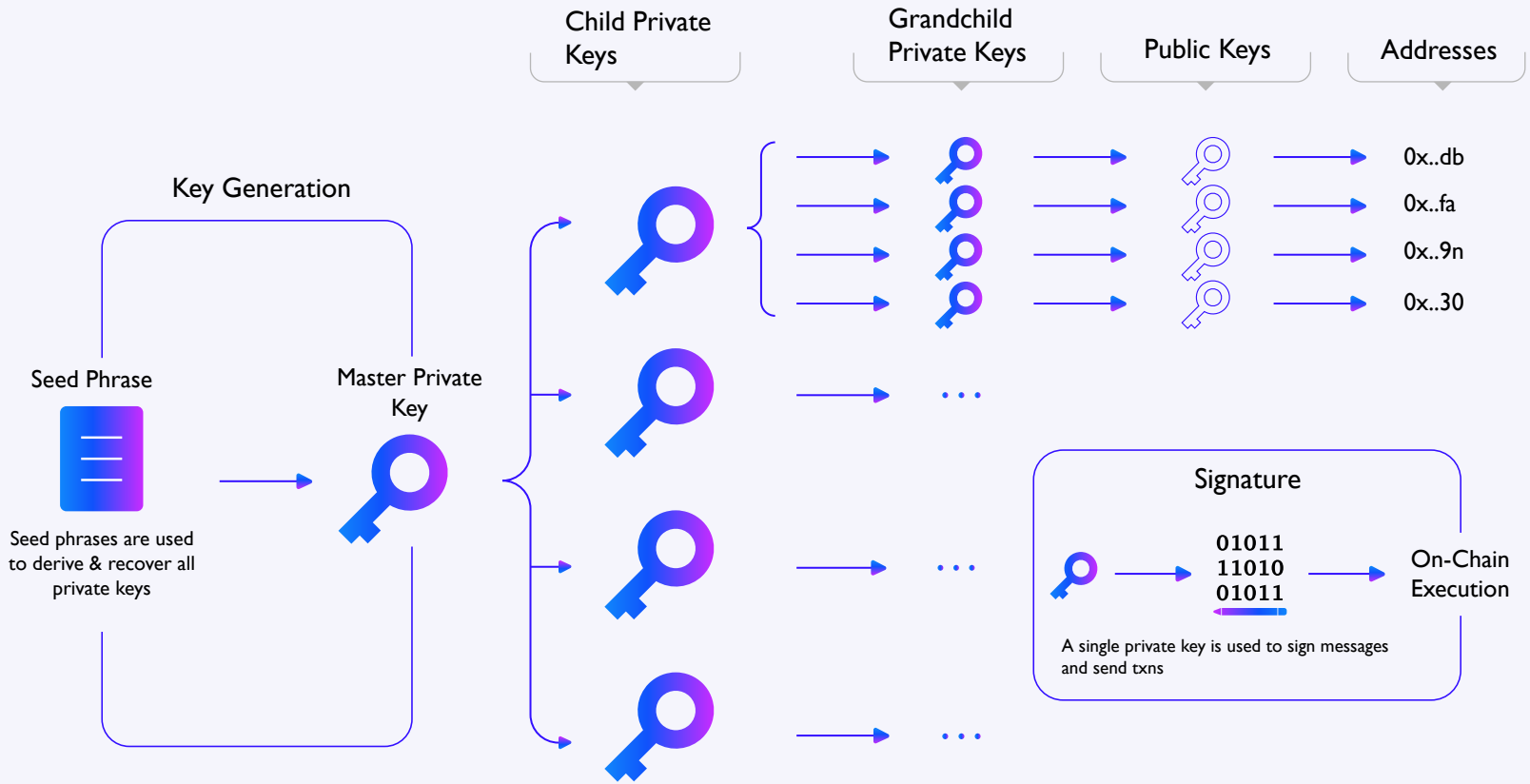
Lemoon's multi-party secure computing (MPC) wallet and multi-signature wallet (smart contract wallet), both types of wallets eliminate single points of failure.

1.Hierarchical Deterministic (HD) Wallets

The wallet uses mnemonics and a Hierarchical Deterministic (HD) structure to derive private keys, corresponding public keys, and on-chain addresses. The wallet allows users to generate private keys for signing transactions and restore all keys using the mnemonic.

Advantages of Lemoon HD Wallet

Directly interact with blockchain applications, provide DAPP browser extensions, support hardware wallets such as Ledger and Trezor, thereby reducing risks, and can protect private keys offline, thereby providing better security.

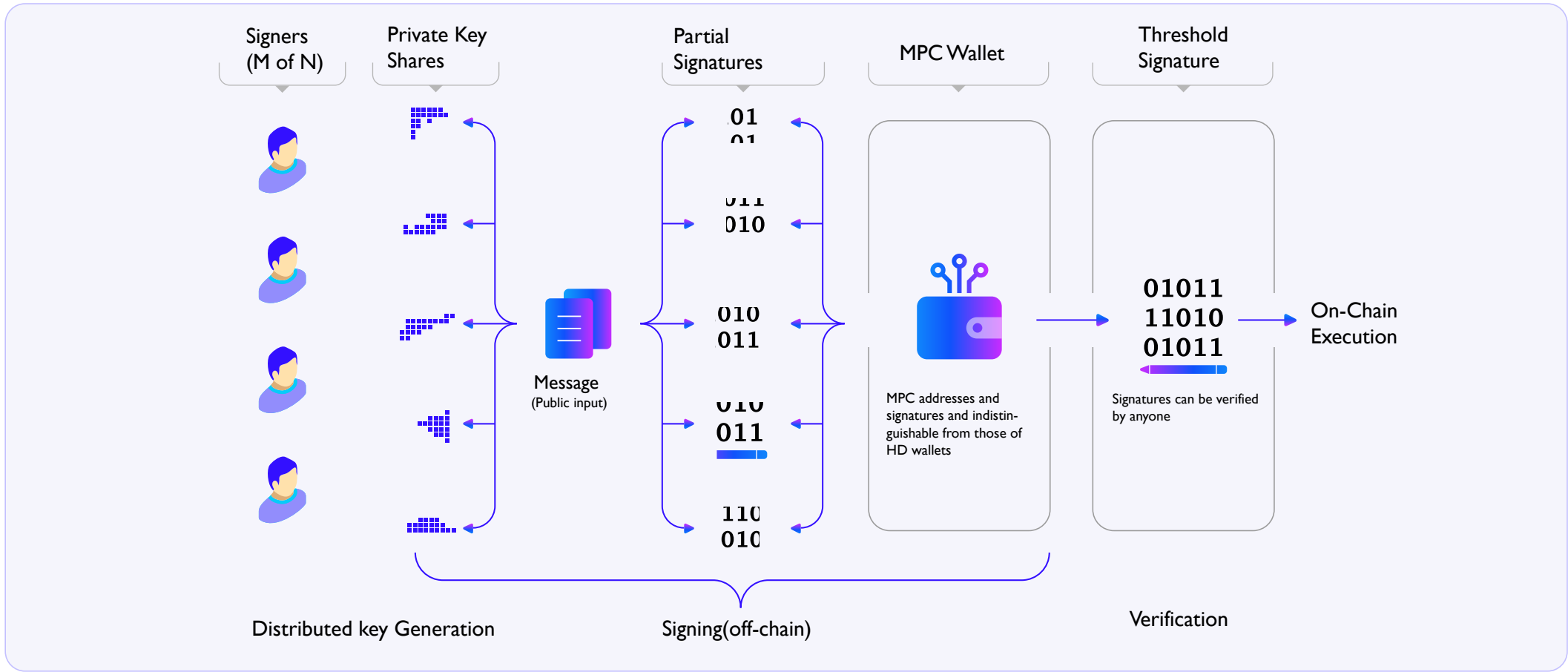


2.Multi-Party Computation(MPC) Wallets

Enables a group of mutually distrusting parties to jointly compute a function based on their inputs while keeping those inputs private. MPC wallets eliminate single points of failure by using a Threshold Signature Scheme (TSS). In this paradigm, we create and distribute parts of the private key so that no one person or machine has full control over the private key—a process known as distributed key generation (DKG). We can then sign messages and transactions by merging the parts and co-generating the public key without exposing the parts between the parties. To sign messages and transactions, each party enters the secret shared part with the public input (the message to sign) to generate a digital signature. Since the key part is combined and the signature is generated off-chain, there is no difference between the transaction generated by the MPC wallet and the transaction of the traditional private key wallet during normal use.

Advantages of Lemoon MPC Wallet

- No single point of failure. A complete private key is never centralized on one device at any time, and there is no seed phrase.
- Adjustable signature scheme. Approved fixed headcounts can be modified as individual and organizational needs change while maintaining the same address. Organizations can dynamically adjust signature schemes without having to notify counterparties of a new address every time (compared to multi-sig wallets).
- Lower transaction and recovery costs (compared to multi-signature wallets), MPC wallets are represented on the blockchain as a single address, and their gas fees are the same as regular private key addresses.



3.Multi-Signature wallets

Multi-signature wallet (smart contract wallet) - strong dependence on HD traditional native wallet

Ethereum currently has two account types:

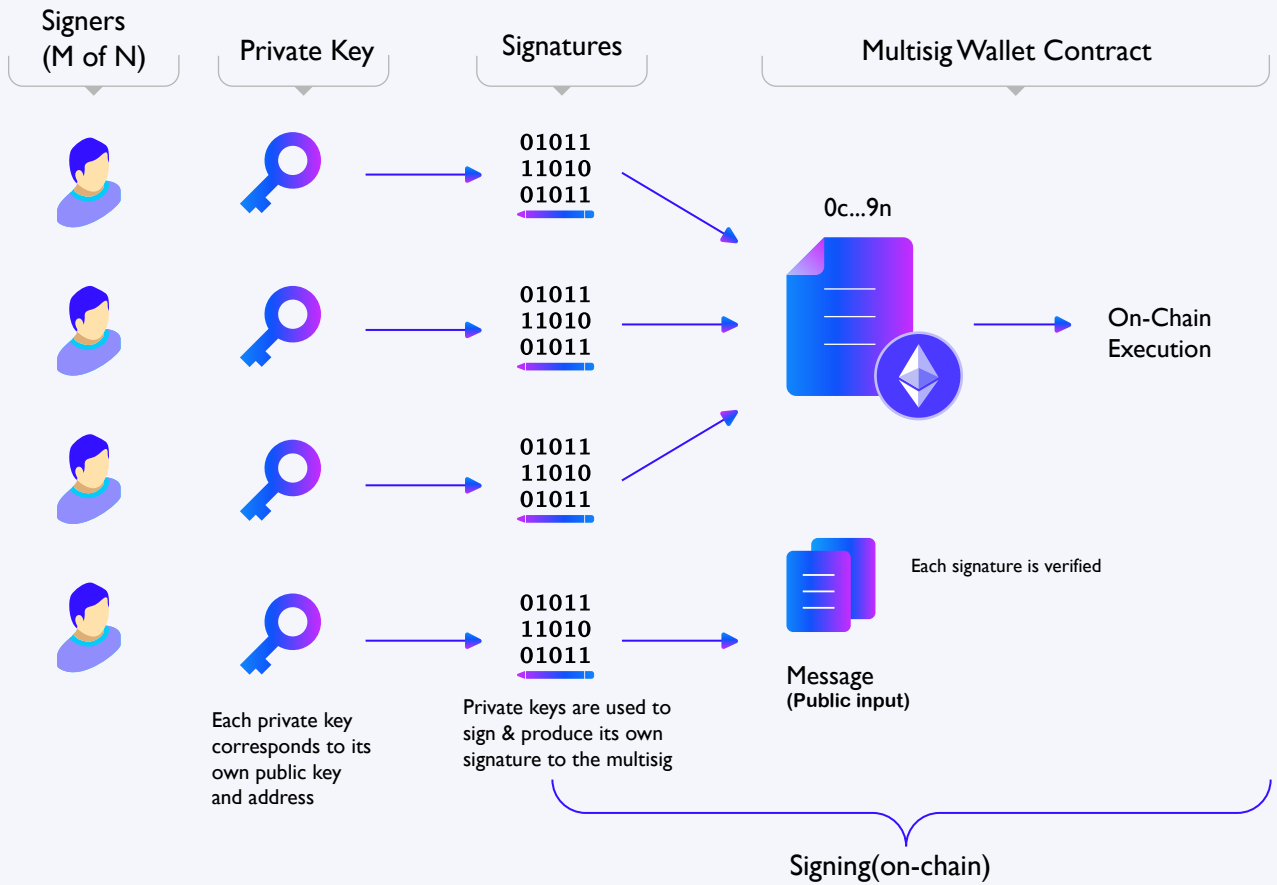
- Externally Owned Account (EOA) - controlled by private key
- Smart contract account - controlled by code

A multi-signature wallet (smart contract wallet) is a smart contract that behaves like a wallet, that is, an interface that allows users to manage funds, log in to web3, and interact with dApps. Unlike private key wallets, the creation of smart wallets requires an initial Cost, because smart contracts need to be deployed on-chain.

Multi-signature wallets are smart contract wallets that require signatures of M-of-N keys to execute transactions. Multi-signature uses different signatures generated by different private keys to sign transactions, which makes it compatible with existing private key wallets and is one layer above traditional wallets.

Advantages of Lemoon multi-signature wallet (smart contract wallet)

- No single point of failure. Multiple signatures are required to execute a transaction.
- Programmable access control. Users can define different security policies, set time locks, spending limits, etc.
- Transaction batch processing can be realized to save costs.
- Scalable. The free composability of smart contracts.
- Contract open source. Code Auditing Available to Everyone



ROUTE MAP

2022
October–December

- Lemoon App version 1.0 is online
- Lemoon 1.0 Web-side plug-in
- Lemoon 1.0 WebChrome version is online
- Lemoon 1.0 web plug-in Opera version is online
- Lemoon 1.0 Web-side plug-in Firefox version is online
- Lemoon 1.0 Web-side plug-in Brave version is online
- Lemoon-DAO Community Founded Issue Lemoon-DAO Genesis NFT

2023
January–March

- Lemoon App 1.1 MPC enhanced version is online
- Lemoon 1.1 social plug-in version is online
- Lemoon-DAO community operation reaches 10K+ users
- Support Ledger and Trezor hardware wallet function is online

2023
April–July

- Lemoon APP version 2.0 is online
- Lemoon Web3.0 GameStore version is online
- Lemoon NFT aggregation transaction version is online
- The download volume of Lemoon App reaches 100K+ users

2023
August–December

- Lemoon APP version 3.0 is online
- The download volume of Lemoon App has reached more than 500K+ users

LEMOON

www.lemoon.cash