EDGERFI
An Edge to Humanity

DECENTRALIZED SECURE COMMUNICATION ECOSYSTEM ON XINFIN NETWORK

Table of Contents

Abstract

LedgerFi is an ecosystem of decentralized communication and decentralized finance solutions that allows for the frictionless exchange of digital assets via a single platform. By enabling Web 3.0 users to embrace and adapt a peer-to-peer, censorship resistant, and decentralized ecosystem, LedgerFi IT Solutions is challenging the conventional methods of trading digital assets, digital energy, and digital property.

LedgerFi's product line is censorship-resistant, decentralized, and democratic in nature, while also making sure to offer Web 3.0 consumers a seamless, straightforward, and cutting-edge platform.

One of the mainstays of the LedgerFi Ecosystem is LedgerMail.

Introduction

LedgerFi is an ecosystem of Decentralized Communication services envisioned to integrate with Decentralized Finance for enabling the seamless exchange of digital assets through a unified platform. LedgerFi consists of 5 products:

- LedgerMail – A decentralized secured end-to-end encrypted closed email solution.
- LedgerChat - A decentralized secured end-to-end encrypted Instant Messaging Solution.
- LedgerLive – A decentralized audio-video platform.
- LedgerPay – A decentralized payment solution.
- MINT – Metaverse Interconnected NFT Transfer platform.

LedgerMail is currently in production and the other products are progressing according to the roadmap.

How does the LedgerFi ecosystem works?

LedgerFi products works based on the end-to-end encryption using the user's cryptographic key pairs and the proof of the communication is recorded on the public blockchain. The users have multiple options to sign up to the ecosystem. i.e. a user can sign up using an email or can create an account using any DNS provider or a web3 social login platform. LedgerMail, the flagship product of this ecosystem is launched with the most of the features mentioned above. LedgerMail has already integrated a few platforms and many more in the roadmap for future integration.

A user can have a single sign-on to all the LedgerFi products once after creating an account under any product which is part of the ecosystem. This document concentrates on the currently

live product LedgerMail and the upcoming product LedgerChat for describing the operation of LedgerFi ecosystem.

LedgerFi uses distributed storage for storing files and attachments which are part of the email and chat communications. LedgerFi has integrated with multiple distributed storage partners providing different user experiences based on the partner features.

LedgerFi is also progressing the integration with multiple web3 and decentralized solution provider to provide better usability to the users. By default, the proofs are recorded on the XinFin blockchain. But the users have the flexibility to switch to any other decentralized storages or login with decentralized DNS services based on their preference. But each distributed storage has methods of charging the gas or transaction fees using its own tokens. If the users prefer to use a non-default distributed storage, then they are mandated to have the native tokens of their preferred distributed storage to pay the transaction fees.

Problems with Legacy Email

Insecure

Legacy email service providers rely on obsolete protocols, which are not only cumbersome to use but also highly susceptible to hacks and exploits.
In case of an IMAP/SMTP email system, a spammer can send email proxying someone else. Many cyberattacks were carried out via email, resulting in over billions in losses worldwide. In the past two years alone, 94% of cyberattacks were carried out via email, resulting in over $26 Billion in losses worldwide.

No Privacy

Legacy email service providers make their money by riffling through the user data. They read user emails and analyze their contents in order to make the user a better target for the ads. That’s their business model. Data privacy is only an illusion.

No Encryption

Legacy email service providers either don't offer any encryption at all or provide inadequate encryption in terms of network connection. However, actual email content and attachments remain unencrypted thus if a hacker manages to tap into your network, all your unencrypted messages will be exposed to the outside world.

Centralized Governance

Legacy email service providers are centralized. They control your data and, that means, they can lose control of your data too. Their servers, with your data on them, can be destroyed, on purpose or by accident, and they can be seized by malicious hackers, state, or even non-state actors. In case of a centralized system, if a malicious hacker get access to the system, he will be able to destroy the data in all the email accounts in that system.

LedgerMail as Solution

LedgerMail is an immutable, truly private, completely secure, fully customizable, and cost-effective email service that will soon render the old ways of providing email service obsolete by leveraging the power of blockchain technology.

Replacement of Traditional Protocols

LedgerMail replaces traditional, obsolete and cumbersome Email transfer protocols such as IMAP/SMTP with immutable, tamper-proof and revolutionary Blockchain Technology. Transfer of each email is considered as a Blockchain Transaction and each transaction is validated with XDPoS 2.0 consensus mechanism.

Security

In collaboration with XDC Network, LedgerMail operates on 4th generation Hybrid Blockchain Platform which is a lightning fast, enterprise-ready, super secure, accountable and forensic control enabled military grade fabric based on Delegated Proof of Stake (XDPoS 2.0) algorithm with 108 transaction-validating master nodes (and 192 additional standby nodes) scattered around the globe.

Cryptographic Encryption

LedgerMail uses Cryptographic Algorithms with asymmetric encryption on the client side with recipients public key. The emails sent on the network are verified & authenticated for the correct recipient. This avoids any hacks of modified headers and spam emails possible in existing email protocols.

Decentralization

LedgerMail operates on fully decentralized network where nodes are distributed across the network to form immutable network which makes it impossible to be controlled and hacked by external parties. There is no single authority to manipulate and control user data and LedgerMail ensures to bring zero trust mechanism.

Key Features

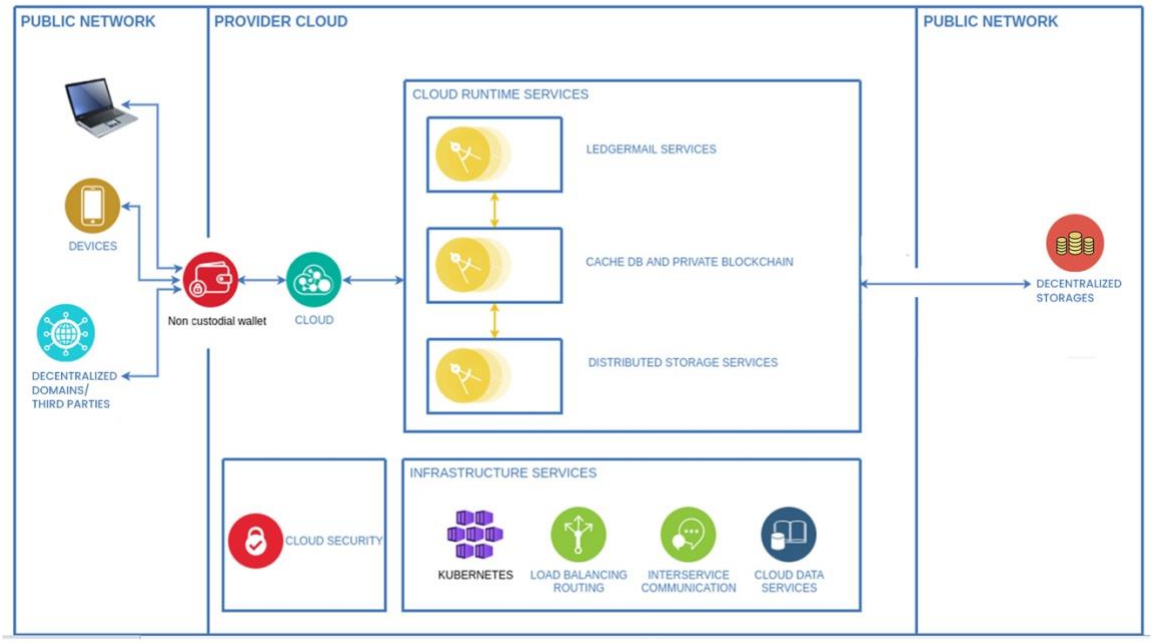
- Decentralized Secure Trustless key sharing Mechanism
- No protocol level dependency on current email systems
- End to End offline asymmetric encryption with open-source cryptographic algorithms
- Decentralized, Tamer-proof and Encrypted sharing of Emails, Files and Attachments.

Technical Details

Architecture

LedgerMail is a secured email communication platform operating on the Hybrid Blockchain model with XinFin (XDC) and decentralized storage.

To mitigate the challenges of on-chain data computation which results in higher transaction fees, lower transaction through-put and suppressed scalability, LedgerMail follows the Layer 2 scaling model. It also uses decentralized storages in order to achieve more distributed decentralization. The below diagram shows the high level LedgerMail architecture



Wallet and Key Management

LedgerMail creates a non-custodial wallet at the time of signup and provides the mnemonics to the user for creating the public and private keys for that wallet. As LedgerMail is not storing the mnemonics or the private keys, the wallet is in full control of the user.

Sending Email

LedgerMail is a secure, closed platform where users can only send emails to other users who have registered. Every email sent from a user to a recipient is protected by LedgerMail by being encrypted at various stages during transmission and only being decrypted at the client system after reception.

Basic email validations are performed on the client side while server-side requests are made to validate recipient email addresses and user names. A temporary cryptographic key pair is formed and provided to the client system as part of the response to that request, with the server storing the private key.

Encryption

Encryption at Client

1st Level of encryption

Encryption of the email data is taken care at the 1st level of encryption. A random string is generated and the email body is encrypted using that string.

2nd level of encryption

The random string and the user mnemonics are attached to the file. Then the whole file is encrypted using the temporary public key received through the previous server response. This 2 level encrypted data is send back to the server through a secured HTTPS request.

Encryption at Server

When the encrypted file is received, the server retrieves the private key associated to the encryption dynamic public key and decrypts the file. From the decrypted file, the server retrieves the random string used for encrypting the email body and again encrypts it with public key of each recipient and attaches back to the file as secret. Each recipient will have a secret attached in the file which would be encrypted with his/her public key.

Sign ups

Sign up with current Email id

LedgerMail is ID agnostic which means, users can Sign Up to LedgerMail with their existing and valid email ID irrespective of domain.
Users can have an email ID with any custom domain such as gmail.com, yahoo.com, aol.com, outlook.com or even customized premium company domains.

LedgerMail treats each email transfer as a blockchain transaction and users will be assigned a unique Wallet ID which will get mapped internally with a given Email ID.
However, users don't need to worry about these complex backend operations and focus on having a seamless experience of using LedgerMail.

Sign up through third party

LedgerMail features various third-party integrations, allowing users to log in using their favourite third-party program.

Decentralized Storages

All email data is secured and kept in a decentralized storage system by LedgerMail. Different procedures are used to manage the files kept in the decentralized storages.

LedgerMail currently integrates with a number of decentralized storage systems and plans to do so in the future. Emails and attachments are encrypted and stored on decentralized storage. The user has the choice to save his email files to additional distributed storage.

Private Offchain

LedgerMail uses private blockchain for offchain processing. This module is continuously evolving and a propitiatory method is under development for offchain rollups. These offchain rollups will help for higher scalability and reduced transaction fees.

LedgerFi nodes

LedgerFi nodes will start getting hosted with the launch of LedgerChat. They will cater the distributed LedgerChat network to manage the messages when the receiver is offline. Also, these servers will make sure of the delivery of each message to the recipient. The community members will have to stake LFT tokens to host the LedgerFi Nodes. Each node will get a share from the 10% of LFTs minted in every minting. Node management will be explained in detail during the launch of the LedgerChat application.

Blockchain / Multichain

Currently, LedgerMail is storing its proof on the open Xinfin blockchain. The user's non-custodian XDC wallet, which was generated at the time of registration, is used to pay the gas fees for the blockchain transaction. Other blockchains are currently being integrated with LedgerMail. The users can select the blockchain of their choice to record the proof of their email transaction after these integrations are complete.

LedgerFi Token (LFT)

LFT is the native token of the LedgerFi ecosystem. It will give a seamless payment experience to the users inside the LedgerFi ecosystem.

As mentioned above, the fees charged for each distributed storage are paid using their own token, So the users will have to maintain multiple tokens in their wallet to pay the fees based on their distributed storage preference in the LedgerFi ecosystem. LFT smoothens these transactions by charging the transaction fees to the users only through the LFT tokens. The transaction fees for different integrated systems are converted into LFT and the users are required to hold only the LFT tokens to operate the LedgerFi ecosystem.

How does it work?

LFT tokens are XRC20 tokens minted on the XinFin Network. The minting, distribution, and burning of the tokens are done based on the functionality of the LedgerFi ecosystem. As discussed earlier, LedgerFi is a communication ecosystem and LFTs are minted when a minting trigger happens in the ecosystem. To start in a simple way, Let us consider only LedgerMail.

The minting of LFT tokens are done using any one of the two triggers. A time based trigger which would be triggered on every hour, or a message count based trigger which would get triggered when 'X' number of emails (which is always calculated using a mathematical formula based on the total number of emails in the system) are sent inside LedgerMail. For each minting 'N' tokens get minted in the system.

When the LedgerChat becomes live, the count 'X' will be calculated using both emails and the chats. A chat count will be considered only for a pair of messages which consists of a sent message and a reply.

When 'N' tokens are minted in the ecosystem, it will be allocated to different stakeholders based on the predefined distribution percentage. 30% of the minted LFTs are distributed to the users who sent the email and the chats. Another 30% percentage is distributed to the Investors, another 30% to the Company and the remaining 10% to the community members who hosts the nodes.

When the LFTs are minted, they are allocated to the respective contracts based the predefined distribution. There are different contracts for users , investors, company, and the community. The stakeholder token allocations will be calculated off-chain and each stakeholder will have to accumulate a minimum amount of LFTs (e.g 500 LFTs) to withdraw from the contract. This policy will help to always lock a certain number of LFTs in the system. Also, the stakeholders will have to withdraw all his accumulated LFTs in a single withdrawal from the contract.

The minimum number of LFTs to be accumulated for a withdrawal may vary based on the supply and demand of the LFTs. This will influence the circulating supply of the LFTs and help to keep the token value higher.

Once LedgerChat is live, the user token allocation will be divided to both email and the chat users. Similar way, while progressing through the LedgerFi roadmap, the minting will be integrated with the triggers from LedgerLive and MINT.

Let us get into the details of the LFT tokenomics.

The total LFTs: 500 million
Pre-minted: 80% : 400 million
Remaining tokens to mint: 100 million

The remaining 100 million tokens need to be minted in 7 years. With an hourly minting, total 61368 minting will be triggered in 7 years. So in each minting 1629.5 LFTs will be created and distributed to participated users, investors, company and the community. The allocation percentages are as given below.

Users: 30%
Investors: 30%
Company:30%
Community:10%

A LFT can be divided into 1E+018 units. Here we will see how the user allocation is done when new LFTs are minted. Let us assume 1629.5 LFTs are minted in a minting round and X=1000 (i.e. 1000 emails need to be sent to trigger a count based minting). Then 30% (488.85 LFTs) of the minted LFTs are allocated to the participating users, then each email sender will be getting 0.488854125928824 tokens per email.

As the number of participating users may vary for each minting, the token distribution to each user can also drastically change. If the number of participating users decreases, then each user will get a larger number of tokens and it would be not fair and would look like a lottery. To mitigate the uneven token distribution, a max limit of .5% token allocation (2.44 LFTs) is applied for each user from the 30% user allocation. This can increase based on the offers set by the LedgerFi ecosystem.

The above token distribution is explained using 1629.5 LFTs/minting just for the simplicity of explaining the token allocation. In the actual scenario, 'N' number of tokens will be minted, where N would be calculated based on formulae depending on the remaining LFTs to be minted and the number of mintings left out.

In a minting round, if there are not enough user participation to allocate 30% of the newly minted tokens (i.e. 488.85 LFTs) , then the remaining tokens will be moved to a burning contract. The system keeps on transferring the unallocated tokens to this burning contract and after reaching 100000 LFTs, the system will burn them together. When 100000 LFTs are burnt, it will increase the remaining count of LFTs to be minted and will change the amount of LFTs minted in a round.

The tokens locked in the burning contract will be part of the total supply, but will never be a part of the circulating supply. This will always add more demand to the circulating LFTs.

Reference

1. Y. A. Baker El-Ebiary et al., "Blockchain as a decentralized communication tool for sustainable development," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, 2021, pp. 127-133, doi: 10.1109/ICSCEE50312.2021.9497910.
2. On Distributed Communications, http://www.rand.org/pubs/researchmemoranda/RM3420.html, 1962, last accessed February 20th, 2017.
3. Decentralized Web Summit, https://www.decentralizedweb.net/, last ac-cessed February 20th, 2017.
4. K. Khullar, Y. Malhotra, and A. Kumar, “Decentralized and secure communication architecture for fanets using blockchain,” Procedia Computer Science, vol. 173, pp. 158–170, 2020. doi: 10.1155/2021/6679882.