ComingChat Whitepaper

introduction:

From a spark to a prairie fire, web3 only took a few years. Blockchain and encryption technology are like a giant ship, ferrying human society from the traditional Internet to the other side of web3. DeFi and NFT came into being. People broke free from the centralization of the Web2 world with amazing creativity, and took back the original ownership of their own assets, data and privacy from those unicorns.

However, despite the fact that Web3 is now flourishing with a plethora of projects and products, two very serious problems remain.

1. DeFi, GameFi, NFT, communication and social, existing Web3 products are usually positioned and classified into one of these categories. In order to complete purposes such as currency exchange and NFT purchase, it is necessary to shuttle between DEXs and NFT platforms. This makes the adoption of Web3 extremely difficult. As Elon Musk said, Web3 lacks a product like WeChat, where people can do almost everything they want with just one app.

2. Ethereum, Avalanche, Solana, BSC, It is the successive births of these mainstream public chains that have led to the change of technology, and the Web3 ecosystem that flourishes like a starry sky today. But problems followed. The ecology of various public chains is almost fragmented from each other, and people have to choose between them. So more than ever, we need a product that supports all chains and connects the public chain ecosystem from silos to continents.

In order to solve the above two dilemmas that exist at the same time, we have developed a Web3 portal application ComingChat that supports the omnichain ecology. At the use case level, ComingChat includes functions such as encrypted communication, social, swap,BTC lending, decentralized digital identity, and NFT purchases. In terms of the protocol layer, that is, the underlying blockchain architecture that interacts with the use case layer, we take supporting the omnichain ecology as the ultimate goal.

ComingChat main features:

1. Encrypted communication

In recent years, Facebook and Twitter have been fined many times for leaking user information, and privacy leaks have become the norm. Based on the concept of protecting user privacy, ComingChat adopts the Signal protocol for chat design.

The "chat" module in ComingChat is divided into three modes: private chat, encrypted group chat, and non-encrypted group chat. Among them, private chats and encrypted group chats adopt the signal protocol.

The Signal protocol is a true end-to-end communication encryption protocol and the most secure communication protocol in the world. Communication content cannot be viewed by any third party, including the server. The protocol uses KDF ratchet algorithm + public key signature for encrypted communication. Taking encrypted group chat as an example, the communication process is as follows:

(1) Each group member must first generate a random 32-byte KDF Chain Key to generate a message key to ensure the forward security of the message key, and a random Curve25519 signature key pair for message signature .
(2) Each group member encrypts the chain key and signature public key separately and sends it to other members. At this point, each member has the chain key and signing public key of all members in the group.
(3) When a member sends a message, it first encrypts the message with the message key generated by the KDF chain ratchet algorithm, then signs it with the private key, and then sends the message to the server, and the server sends it to other members.
(4) After other members receive the encrypted message, they first use the sender's signature public key for verification. After the verification is successful, use the corresponding chain key to generate the message key and decrypt it with the message key.

ComingChat provides an absolutely secure instant messaging environment for individual users or organizations, completely eliminates the risk of privacy leakage, and leaves all personal privacy under the control of users themselves.

2. Social

'DAO Moments' is a Twitter-like dynamic list that is the main form of ComingChat's social module. The multi-person interoperability group behaviors such as NFT group purchases or red envelopes distributed by DAO members will be presented in DAO Moments. Other members can interact in DAO Moments, such as comments, or click to participate.

Specifically, the social module of ComingChat mainly includes two aspects: red packets and NFT group purchases:

(1) Red Packet
Based on the instant messaging function of ComingChat, we have developed a social

application called Web3 Red Packet. Users can send red packets of specified currency, total amount and quantity to group members in the group chat of ComingChat. There are two modes of red packets: handicap red packets (each member receiving a red packet shares a random amount) and normal red packets (each person receives an equal amount). Any group member can click and receive the group red packet without paying gas fee.

ComingChat Red Packets will eventually support the issuance and collection of omnichain tokens.

The combination of Web3 red packets and instant messaging brings some new social scenarios: friends and family can send red packets to show their gifts, gratitude or blessings; community operators can create a ComingChat group chat and send red packets to members to run campaigns for marketing purposes.

(2) NFT Group Buying
In order to solve the problem of low circulation rate due to high pricing of head NFTs in the current market, we designed a new way to buy NFTs with strong social attributes; NFT group purchase allows users to buy NFTs in a fragmented form, giving more people the opportunity to enter the NFT field. Create an NFT DAO in ComingChat and team up with your friends to buy NFTs and gain exclusive benefits such as voting rights.

Specifically, a user first selects an NFT on an NFT platform (e.g. Opensea) as a target, then initiates a group purchase in ComingChat, and any other ComingChat users who also want to purchase that NFT can choose to join the group, and the members of the group will collectively raise the price to purchase the NFT. Upon successful purchase, members of the group will receive shard tokens in proportion to their contribution, which represent the user's new pricing rights to the NFT.

Users who purchase the same NFT will create a group in ComingChat to discuss the new pricing strategy for the NFT among members of the organization. In addition, users who initiate or participate in a group purchase of an NFT can post an invitation link to the group purchase of that NFT, which will be displayed on the individual ComingChat pages and will be shown to users who have purchased the same NFT together. Users can join the organization that purchased that NFT by clicking on that link.

3. Wallet

ComingChat mainly includes the following two categories of wallets:

(1) Omnichain wallet
Simple and easy-to-use omnichain self-hosted wallet, private keys and mnemonics are

stored in the user's own device, and the user has complete control over their digital currency and NFT assets.

Up to now, ComingChat Wallet mainly supports the following networks:

EVM. Including Ethereum
/BSC/Arbitrum/Optimism/KCC/ChainX-EVM/SherpaX-EVM/Avalanche/Polygon

BTC. Including Bitcoin/Dogecoin

Substrate. Including Polkadot/Kusama/ChainX-WASM/SherpaX-WASM/MiniX

Cosmos ecology. Including Terra/Cosmos

Solana Ecology.

In order to further achieve the goal of the omnichain, the ComingChat Wallet will continue to be updated to support more ecosystems.

(2) Bitcoin, Dogecoin threshold signature wallet
On the basis of traditional multi-signature wallets, ComingChat applied Taproot technology to develop BTC/Dogecoin threshold signature wallets. Due to the off-chain aggregation of Taproot private key fragments, it is impossible to determine whether a transaction is a threshold multi-signature or a single-signature transaction from the data on the chain. Therefore, the threshold wallet is more private and safer than ordinary multi-signature wallets.

ComingChat threshold wallet provides the most secure and reliable fund management tool for asset custodians such as Bitcoin Trust. Users can safely transfer funds to the aggregate address composed of the respective addresses of the trust members. Any actions that want to transfer assets on the aggregate address must go through a threshold signature, and the transfer can be successful only when a certain percentage of trust members sign.

4. Decentralized digital identity ComigChat ID (hereinafter referred to as CID)

CID is a new type of verifiable identity for the web3.0 network world. It allows individuals or organizations to fully own, manage and control their digital identities and their data.

CID is composed of 1 to 12 digits, and can also be used with ".btc" at the end. Each cid account contains the following abstract structure:

Owner- The ultimate owner of the cid, the administrator who can transfer the account and set up the account
Controller - the administrator of the cid, who can manage the records of the account
Registry - The resolution record table for this cid account. A parsing record is a series of key-value pairs, defined by the user or application.

CIDs have the following characteristics:
(1) Easy to read and easy to remember. Such as: 12345 or 12345.btc

(2) Decentralization and censorship resistance. The CID creation process requires no permission and does not reveal any personal information.

(3) Compatibility. CID is based on ChainX's EVM and can be compatible with other public chains at a very low cost.

(4) Lightweight. CID is a smart contract running on ChainX EVM with extremely high programmability and scalability.

Application scenarios of CID in ComingChat:
(1) As a collection account of cryptocurrency
Users can add friends through CID, and initiate cryptocurrency transfers to the friends in the chat box of the "Chat" interface. This process does not require the input of complex and lengthy addresses, which greatly simplifies the cryptocurrency transfer process.

(2) as a login credential
All services in the Web2.0 era require an account and password to log in. Multiple websites use the same password, which is a security issue. Multiple websites use different passwords, and there are extremely high password management costs. Each CID account is associated with at least one pair of public and private keys. Other dapps can sign login operations by using the private key associated with the CID.

(3) Omnichain reputation aggregation
ComingChat conducts a quantitative evaluation of the user's reputation based on the past behavior of the user's address to determine what level of service to provide. In addition, under the background that ComingChat supports the whole chain ecology, CID can no longer obtain the reputation of a user's address, but the reputation of all addresses of the user in all public chains.

5. OmniBTC

ComingChat is the mobile portal of OmniBTC, an omnichain financial platform. That is to say, ComingChat includes two core functions of OmniBTC: Omnichain Swap and BTC Omnichain Lending.

Omni Swap
On the ComingChat "Omni Swap" interface, users can swap native assets on two different chains with one click without using a cross-chain bridge.

Up to now, the Omni Swap function has supported one-click swaps between dozens of tokens in Ethereum, BSC, Avalanche, Polygon, Arbitrum, Optimism ChainX, , and other networks. With the version update, the ComingChat Omni Swap function will support more networks and eventually support the omnichain ecosystem.

This function is implemented mainly by deploying Client contracts and Server contracts that call the corresponding DEX on the source chain and target chain. Interchain messaging is achieved by integrating the LayerZero protocol.

Omni BTC Lending
On the ComingChat "Omni BTC Lending" interface, users can mortgage XBTC and borrow a variety of stablecoins on any chain with one click.

Existing bitcoin lending services, such as AAVE, Compound, etc., require users to first cross-chain WBTC to BSC/Avalanche/Polygon and other networks on a third-party cross-chain bridge, and then they can borrow the stable assets on these chains. currency. The Omni BTC Lending function saves users this step. The implementation of this process is mainly realized by deploying the XBTC mortgage contract on ChainX and the Client contract that calls the target chain, and deploying the single-coin pool contract on the target chain and the Server contract responding to the call from the source chain. It is achieved by integrating the LayerZero cross-chain interoperability protocol.

6. Discover

The "Discover" page of ComingChat supports many existing mainstream Dapps in Web3, such as Uniswap, Opensea, etc., and classifies them according to DeFi, DEX, and NFT. Below the primary classification, the secondary classification is performed according to the chain to which Dapps belong. Currently, the ecosystems supported by the Discover page include Ethereum/BSC/Polygon/Avalanche/Arbitrum/Optimism/Cosmos/Polkadot, etc.

On the ComingChat Discover page, users can quickly enter and use almost all Dapps in the omnichain ecosystem.These dapps are bound to the corresponding addresses in ComingChat Wallet by default, and users can also change the address by selecting Connect Wallet.

The Future: Digital Currency Payments

The popularity of Web3 inevitably requires digital currencies, led by Bitcoin, to have the same level of transaction processing capabilities as existing fiat payment systems. The Lightning Network creates a stateful channel between the two sides of a transaction, placing the intermediate transaction process off-chain, with only the initial and final balance information recorded on the chain, thus allowing the Bitcoin network to scale indefinitely, allowing it to process transactions at millions of times per second.

In the next phase, ComingChat will integrate the Lightning Network in its wallet to enable instant micropayments of Bitcoin, USDT (minted in the Bitcoin network via the omnilayer protocol). It is foreseeable that with the development of lightning network technology, bitcoin will be widely adopted in real life, and at that time, ComingChat will replace Alipay and Visa as the daily payment choice for billions of people worldwide.

Conclusion

At present, the proportion of the global population exposed to crypto and web 3.0 is still at a low level. Part of the reason is that the separation between web 3.0 products and the public chain has inadvertently raised the entry barrier, and people must spend enough energy to learn the principles and operating steps of multiple products at the same time. We believe that the Web3 world should not shut anyone out. Based on this concept, this paper introduces ComingChat, a Web3.0 super app that supports the omnichain ecosystem and combines encrypted communication, social, wallet, NFT, decentralized digital identity, omnichain swap, bitcoin lending, and Discover, etc.