ComingChat Whitepaper

09/14/2022

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.

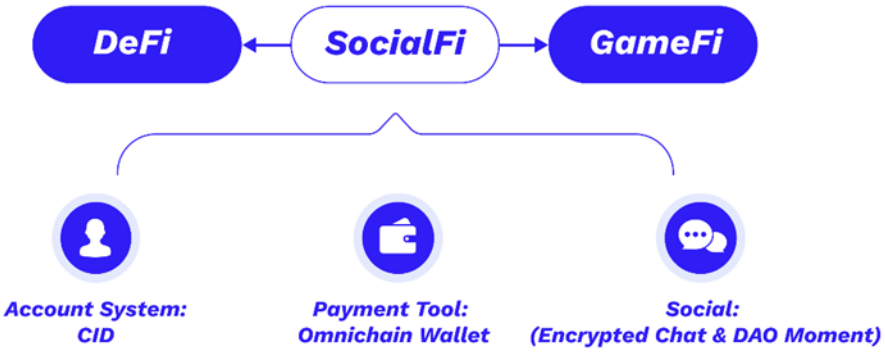
However, despite the fact that Web3 has flourished, projects and products emerge in an endless stream, there are still two very serious problems:

1. DeFi, GameFi, NFT, communication and social networking, 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, Aptos, Sui, Solana, BSC, it is the successive birth of these mainstream public chains that has prompted the change of technology, resulting in today's prosperous Web3 ecosystem. But problems followed. The ecology of each public chain is almost split, and people must choose between public chains. Therefore, more than ever, we need a product that supports all chains and connects the public chain ecosystem from isolated islands to continents.

In order to solve the above two dilemmas at the same time, we have developed a SocialFi-based web3 portal app ComingChat with DeFi and GameFi functions.

At the use case level, ComingChat includes decentralized digital identity, wallet, encrypted communication, social networking, DeFi, GameFi and other functions. 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 is a SocialFi-based web3 portal app with DeFi and GameFi functions.

SocialFi in ComingChat:

In ComingChat, SocialFi means the collection of the following three:
1. Decentralized Account System (CID)
2. Payment tool (omnichain wallet)
3. Social system (Chat+DAO Moments)

The above solves the three problems of "people", "money", and "connection" respectively, and provides the basis for DeFi and GameFi

1. Decentralized digital identity ComigChat ID (CID for short)

CID is a new type of identity that can be verified and applied to 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 this cid, who can manage the records of this 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 supports the omnichain ecosystems. CID will not only be deployed on the current mainstream EVM public chains, but also on the new-generation Move public chains Aptos/Sui to support the Aptos/Sui ecosystems.

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) Full-chain 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.

2. Wallet

ComingChat mainly includes the following two wallet categories:

(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 class:
Ethereum/BSC/Arbitrum/Optimism/KCC/Avalanche/Polygon

BTC class:
Bitcoin/Dogecoin

Substrate class:
Polkadot/Kusama/ChainX

Cosmos ecology:
Terra/Cosmos

Solana.

Move public chains:
Aptos/Sui

(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.

3. Social

3.1 Encrypted chat
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 use 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 receiving the encrypted message, other members 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.

3.2 DAO Moments

'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, ComingChat social networking mainly includes two aspects: red packets and NFT group purchases:

(1) Red packets

Based on the instant messaging function of ComingChat, we have developed a social application called Web3 Red Packet. Users can issue red packets of specified currency, specified total amount and quantity to group members in the ComingChat group chat. The red packets are divided into two modes: lucky red packets (the amount received by each member who receives the red packet is random) and ordinary red packets (the amount received by each person is equal). Any group member can click and receive group red packets without paying gas fees.

Likewise, ComingChat red packets will eventually support the issuance and collection of omnichain tokens.

The combination of Web3 red packets and instant messaging has brought some new social scenarios: family and friends can send red packets to express gifts, gratitude or blessings; Community operators can build Group chat and distribute red packets to members to carry out activities and achieve marketing purposes.

(2) NFT group purchase
In order to solve the problem that the price of top NFTs is too high and the circulation rate is low in the current market, we have designed a brand-new NFT purchase method with strong social attributes. NFT group buying allows users to buy NFT in a fragmented form, giving more people the opportunity to enter the NFT field. Build NFT DAO in ComingChat, team up with your friends to buy NFT, and get exclusive rights such as voting rights.

Specifically, a user first selects an NFT on an NFT platform (such as Opensea) as a target, and then initiates a group purchase in ComingChat. Any other ComingChat user who also wants to purchase the NFT can choose to join the group purchase organization, and the organization members will Co-raise the money to buy the NFT. After the purchase is successful, the members of the group purchase organization will receive the corresponding fragmented tokens in proportion to their contributions, and the tokens represent the user's new pricing power for the NFT.

Users who purchase the same NFT will create a group in ComingChat to facilitate discussions among organization members about the new pricing strategy for the NFT. In addition, users who initiate or participate in a certain NFT group purchase can publish the NFT group purchase invitation link, which will be displayed on the ComingChat personal page and will be displayed to users who have jointly purchased the same NFT. Users can join the organization that purchased the NFT by clicking on this link.

DeFi in ComingChat

ComingChat is the mobile portal of OmniBTC, an omnichain financial platform. That is to say, ComingChat includes the three core functions of OmniBTC: OmniSwap, OmniLending and OmniBridge.

OmniBTC

OmniSwap

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

Up to now, the OmniSwap function has supported one-click swaps between dozens of tokens in BSC, Arbitrum, Ethereum, Avalanche, and other networks. With the version update, the OmniSwap function will support more networks and eventually support the omnichain ecology.

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.

OmniLending
On the ComingChat "OmniLending" interface, users can mortgage various assets such as XBTC and borrow various stablecoins on any chain with one click.

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.

OmniBridge
Decentralized ultra-light node cross-chain bridge, the main business is to open up the EVM ecology and the Aptos/Sui ecology, so that assets can be freely circulated between the two. Currently under development.

GameFi in ComingChat

GameFi development trend
In 2022, the crypto market cools down. As of April, the total TVL of DeFi in 2022 dropped from $237.1 billion to $202.9 billion, a decrease of 14.38%. The GameFi market is attracting the attention of users and the capital market. Judging from the total number of users, GameFi was not affected by it, and did not show obvious user loss. The overall number of users in the first quarter basically remained around 1.2M. In the future, as the market recovers, the GameFi field will usher in a new round of outbreaks.

Move public chain Sui
Currently, there are about 200 game projects deployed on BSC. Compared with Ethereum, BSC has higher transaction efficiency, lower gas fees, and is more friendly to the development of game projects from ecological resources to infrastructure. However, with the development of the GameFi field, the BNB chain is still unable to meet the high requirements of chain games for public chain performance. The new public chain Sui built in the Move language greatly improves the transaction processing speed through parallel processing and non-universal consensus mechanism. After testing, the unoptimized 8-core Macbook Pro can reach 120k TPS. It can be said that the emergence of the Move public chain Sui will bring GameFi to an

unprecedented prosperity.

ComingChat GameFi
Like Tencent QQ in the Web2 era, ComingChat SocialFi includes account system (CID), payment tool (OmnichainWallet) and Chat+DAO Moment (social system). This allows ComingChat users to experience GameFi services without additionally binding a third-party wallet as a login account or for payment, and can interact with other players within the app.

Based on the above GameFi development background and combined with ComingChat's unique SocialFi advantages, we plan to do two things:

1. Blockchain Mini-Game Studio
Mini-games are new game product forms with mini-programs as the carrier, and have the characteristics of no download, click-to-play, and light experience.
Users can play various types of blockchain mini games in ComingChat Mini Game Studio, and "Play to earn" on the mobile phone anytime, anywhere.

2. GameFi NFT Marketplace on Sui
ComingChat will build an NFT trading platform for game vertical classification on Sui. Provide game players on Sui with a fast and convenient place to trade NFT assets such as game props.

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/Arbitrum/Optimism/Cosmos/Polkadot, etc., and will soon support the Aptos/Sui Move ecosystem.

On the ComingChat Discover page, users can quickly enter and use almost all Dapps in the entire chain ecosystem. The app binds the corresponding address 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 will inevitably require digital currencies led by Bitcoin to have the same level of transaction processing capabilities as the existing legal currency payment systems. The Lightning Network establishes a state channel between the two parties of the transaction, and places the intermediate transaction process off-chain. Only the initial and final balance information is recorded on the chain, so the Bitcoin network can be infinitely expanded, making its transaction processing speed reach millions of times per second. .

In the next phase, ComingChat will integrate Lightning Network in wallets to enable instant micropayments of Bitcoin and USDT (coined on the Bitcoin network through the omnilayer protocol). It is foreseeable that with the development of Lightning Network technology, Bitcoin will be widely adopted in real life, and then ComingChat will replace Alipay and Visa as the daily payment choice for billions of people around the world.

Summarize

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 chains inadvertently raises the entry barrier, and people must spend enough time 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 idea, this article introduces ComingChat, a SocialFi-based Web3 portal application with DeFi and GameFi functions. Specifically, ComingChat supports the omnichain ecology, integrating multiple functions such as decentralized digital identity, omnichain wallet, encrypted communication, social networking, DeFi, GameFi, and Discover.