CIPHER

WHITE PAPER

Content

PART

01

SUMMAY

Summary

Cipher (CIP) aims to leverage the technology and potential of Bitcoin Inscription while providing users with a secure, private and innovative digital asset platform based on EVM. Bitcoin Inscription is a method of storing data or metadata on the Bitcoin blockchain, which can be used to create digital collectibles, tokens, certificates, contracts, and more.

Cipher (CIP) enables users to seamlessly transfer and trade Inscription assets between Bitcoin and Ethereum while enjoying the benefits of both networks by implementing a compatible Inscription protocol on EVM.

Cipher (CIP) also solves some of the problems of Bitcoin Inscription such as high fees, inefficient transactions, limited scalability, and lack of standardization by introducing some innovative features and services.

PART

02

BACKGROUND

OF THE PROJECT

Background

Bitcoin is the world's first and largest cryptocurrency, which provides a decentralized, secure and immutable peer-to-peer payments network. However, Bitcoin's functionality is not limited to currency transfers; it can also serve as a distributed state machine to support more complex applications and smart contracts. One of Bitcoin's core technologies is the Bitcoin Scripting Language, which is a stack-based programming language that allows users to perform various operations and logic on the Bitcoin blockchain. Using the Bitcoin scripting language, users can embed arbitrary data or metadata in Bitcoin transactions. This is the so-called Bitcoin inscription.

Bitcoin inscriptions have many interesting applications and stories, such as recording the birth of Bitcoin, creating digital collectibles and tokens, etc. An important feature of Bitcoin inscriptions is that they are immutable because they are permanently stored on the Bitcoin blockchain, protected by the consensus and security of the Bitcoin network. This makes Bitcoin inscriptions of unique value and significance, as they can serve as proof of digital assets, identification of identity, transmission of information, etc.

However, Bitcoin Inscription also faces some challenges and limitations, such as:

High fees: Bitcoin Inscription requires transactions to be conducted on the Bitcoin network, which means users need to pay Bitcoin transaction fees, which often depend on the network's congestion and the user's urgency. In the case of Bitcoin network congestion, the fees for Bitcoin Inscription can be very expensive, even exceeding the value of the inscription asset itself.

Inefficient transactions: Bitcoin Inscription requires transactions to be conducted on the Bitcoin network, which means users need to wait for Bitcoin's block confirmations, which often take 10 minutes or more. In the case of Bitcoin network congestion, Bitcoin Inscription transactions can take hours or even days to complete.

Limited scalability: Bitcoin Inscription requires transactions to be conducted on the Bitcoin network, which means users need to adhere to Bitcoin's technical specifications and limitations, such as block size, transaction size, scripting language, etc. These specifications and restrictions limit the scalability and flexibility of Bitcoin Inscription, such as the inability to support complex logic, interactions, and functionality.

Lack of standardization: Bitcoin Inscriptions does not have a unified standard or protocol to define and manage them, but instead different developers and projects use different methods and tools to implement and operate them. This has led to the fragmentation and non-interoperability

of Bitcoin Inscription, such as the inability to be easily transferred and traded between different platforms and wallets.

PART

03

SOLUTION

Solution

We propose the project Cipher (CIP), a protocol for creating and managing cross-chain inscribed assets on the Bitcoin blockchain. Designed for easy cross-network transfer between BRC20 and ERC20 tokens.

Cipher(CIP) enhances cross-chain interoperability by facilitating unparalleled liquidity for these tokens. We hope to resolve some of the issues with Bitcoin Inscription. Increase the liquidity and accessibility of Inscription and ERC tokens in a secure and user-friendly way.

PART

04

PROJECT OBJECTIVES

Objectives

The main goal of Cipher(CIP) is to leverage the advantages of EVM to provide users with a secure, private and innovative digital asset platform while maintaining compatibility and interoperability with Bitcoin Inscription.

Implementing a compatible Inscription protocol

Cipher (CIP) implements a compatible Inscription protocol on EVM, allowing users to seamlessly transfer and trade Inscription assets between Bitcoin and Ethereum while enjoying the advantages of both networks . Cipher(CIP)'s inscription protocol supports multiple types of inscriptions, such as pictures, text, audio, video, etc., as well as inscriptions in multiple formats, such as NFT, Token, certificates, contracts, etc. Cipher(CIP)'s inscription protocol also supports multiple ways of inscription, such as storing data directly on the chain, storing data off the chain and storing indexes on the chain, storing hashes on the chain, etc.

Reduced fees and improved efficiency

Cipher(CIP) reduces user fees and improves user efficiency by conducting inscription transactions on EVM. Cipher(CIP) transaction speed is determined by the EVM network, which typically has block times of 15 seconds or less. Cipher(CIP) transactions can also leverage the EVM

network’s second-layer solutions, such as Arbitrum, Optimism, Starknet, etc., to further reduce fees and improve efficiency.

Increased scalability and flexibility

Cipher(CIP) increases scalability and flexibility for users by running Inscription applications on the EVM. Cipher(CIP)'s inscription applications can use EVM's smart contract functions to implement complex logic, interactions and functions, such as auctions, lending, games, social networking, etc. Cipher(CIP)'s Inscription application can also interact with other applications on the EVM network.

PART

05

TECHNICAL REALIZATION

Technologies

Inscription Agreement

Cipher (CIP) implements a compatible Inscription protocol on EVM, allowing users to seamlessly transfer and trade Inscription assets between Bitcoin and Ethereum while enjoying the advantages of both networks.

Cipher(CIP)'s inscription protocol supports multiple types of inscriptions, such as pictures, text, audio, video, etc., as well as inscriptions in multiple formats, such as NFT, Token, certificates, contracts, etc.

Cipher(CIP)'s inscription protocol also supports multiple ways of inscription, such as storing data directly on the chain, storing data off the chain and storing indexes on the chain, storing hashes on the chain, etc.

Cipher(CIP)'s inscription protocol is based on a standard called ORC-69, which is a universal protocol for creating and managing inscription assets on the Bitcoin blockchain. Cipher(CIP)'s inscription protocol has made some improvements and extensions based on ORC-69, making it able to run on EVM and be compatible and interoperable with other applications and protocols on EVM.

The specific functions of the inscription protocol are as follows:

Creation of inscription assets

Users can convert any type of data or metadata, such as pictures, text, audio, video, etc., into a unique inscription identifier (CID) through the Cipher (CIP) inscription protocol, and Store it on the Bitcoin or Ethereum blockchain. Users can also set some properties and parameters for inscription assets, such as name, description, owner, expiration time, etc.

Transfer of inscription assets

Users can transfer inscription assets from the Bitcoin or Ethereum blockchain to another blockchain through the Cipher (CIP) inscription protocol. Users only need to send a transaction containing the CID and target address of the inscription asset to complete the transfer of the inscription asset. The Cipher (CIP) inscription protocol will verify and synchronize between the two blockchains to ensure the consistency and uniqueness of the inscribed assets.

Transaction of inscription assets

Users can exchange or transfer inscription assets with other assets on the Bitcoin or Ethereum blockchain through the Cipher (CIP) inscription protocol. Users only need to send a transaction containing the CID of the inscription asset and the transaction conditions to complete the transaction of the inscription asset. The Cipher (CIP) inscription protocol

will match and execute between the two blockchains to ensure the security and validity of the inscribed assets.

PART

06

INSCRIPTION BRIDGE

Bridge

ORC-Cash protocol

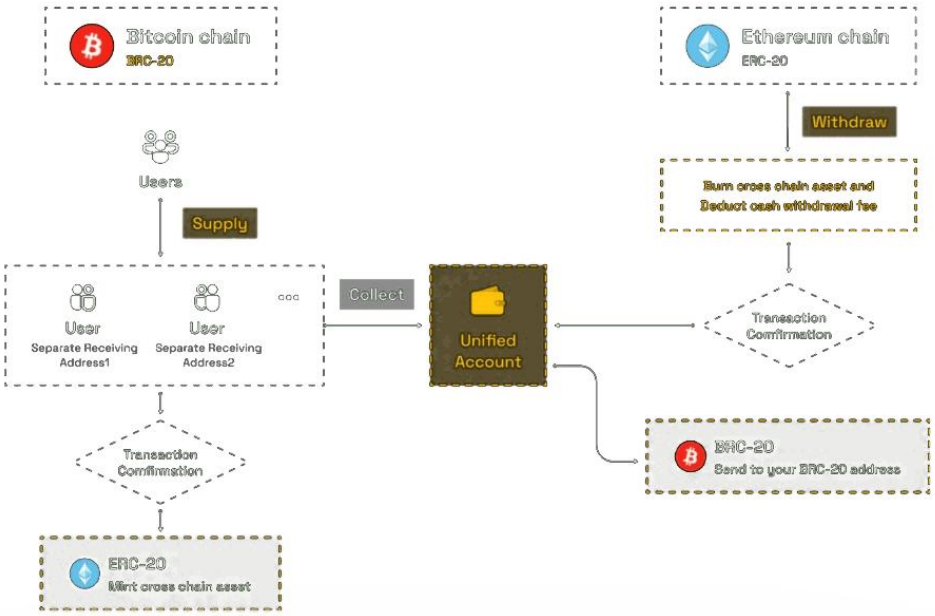
Cipher (CIP) will provide an inscription bridge service, which is a relay node responsible for transferring and verifying inscription assets between Bitcoin and Ethereum.

Inscription Bridge uses a protocol called ORC-Cash, which is a protocol for creating and managing cross-chain Inscription assets on the Bitcoin blockchain. Designed for easy cross-network transfer between BRC20 and ERC20 tokens. Cipher(CIP) enhances cross-chain interoperability by facilitating unparalleled liquidity for these tokens.

Our mission is simple: increase the liquidity and accessibility of BRC and ERC tokens in a secure and user-friendly way. Through the ORC-Cash protocol, Inscription Bridge can lock the inscription assets on the Bitcoin blockchain to a special address, and then generate a corresponding inscription asset on the Ethereum blockchain, or vice versa. Inscription Bridge can also verify the consistency and validity of inscription assets on two blockchains through the ORC-Cash protocol to prevent double spending and fraud.

The operation of Inscription Bridge is maintained and supervised by a group of nodes called Inscription Guardians. They are users who hold CIP

tokens. They can participate in the consensus and governance of Inscription Bridge by staking CIP tokens, and at the same time obtain certain benefits. Rewards and punishments.



Inscription applications

Cipher(CIP) supports a series of inscription applications, which are smart contracts or decentralized applications that use inscription assets to provide various services and functions. Inscription applications can use EVM's smart contract capabilities to implement complex logic, interactions and functions, such as auctions, lending, games, social networking, etc.

Inscription applications can also integrate and collaborate with other applications and protocols on the EVM network, such as Uniswap, Compound, and others. The development and operation of the Inscription

application is driven and supported by Cipher(CIP)'s community, which provides tools and resources to the community, such as developer documentation, testnets, reward programs, etc.

PART

07

MARKET ANALYSIS

Market analysis

Market demand

Market demand for Cipher(CIP) comes from interest and demand for Bitcoin Inscription, as well as interest and demand for digital assets.

Bitcoin Inscription is a method of storing data or metadata on the Bitcoin blockchain.

Digital assets are virtual assets created and managed using cryptography principles and blockchain technology. They can have multiple attributes and functions such as currency, rights, certificates, and information.

Both Bitcoin inscriptions and digital assets have unique value and meaning because they serve as identity, expression, creation, communication, etc. in the digital world.

With the development and popularization of blockchain technology, the market demand for Bitcoin inscriptions and digital assets will continue to grow and expand, especially in the following areas:

(1) Digital collectibles

Digital collectibles are unique digital items created and managed using blockchain technology.

They can be works of art, game props, sports memorabilia, etc. The market size of digital collectibles has exploded in the past few years, especially in 2021, when digital collectibles transactions reached billions of dollars.

The market demand for digital collectibles comes from the love and pursuit of digital items, as well as the recognition and guarantee of the scarcity and authenticity of digital items. Bitcoin inscription can be used as a method to create and manage digital collectibles. It can take advantage of the immutability and security of the Bitcoin blockchain to ensure the uniqueness and authenticity of digital collectibles.

(2) **Token**

Token is a digital representation created and managed using blockchain technology.

It can represent a currency, a right, a certificate, a piece of information, etc. The market size of Token has also shown rapid growth in the past few years, especially in 2020, when the total market value of Token exceeded the level of US$500 billion. The market demand for Token comes from the demand and use of digital representatives, as well as the exploration and innovation of the flexibility and diversity of digital representatives. Bitcoin Inscription can be used as a method to create and manage Tokens. It can

take advantage of the decentralization and openness of the Bitcoin blockchain to ensure the autonomy and interoperability of Tokens.

(3) Certificate

A certificate is a digital certificate created and managed using blockchain technology.

It can prove an identity, a qualification, an achievement, a transaction, etc. The market size of certificates has also shown steady growth in the past few years, especially in 2020. The application scenarios of certificates cover education, medical care, finance, etc.

Market size

Market size of Bitcoin inscriptions: According to data from , as of November 2023, the total data volume of Bitcoin inscriptions has reached 1.2 GB, which contains more than 1 million inscription assets, such as ordinals, sats, rats, cats, etc. The total market value of these inscription assets has exceeded US$1 billion. These data show that Bitcoin inscription has formed a large and active market, and there is still a lot of room and potential for growth.

Market trend

Market trends are mainly affected by the following factors:

(1) Development of blockchain technology

Blockchain technology is the foundation and driving force of Cipher(CIP). With the continuous development and innovation of blockchain technology, Cipher(CIP) will also improve and optimize its own Functions and services, such as supporting more inscription types and formats, achieving higher performance and security, providing more functions and services, etc. The development of blockchain technology will also bring more users and funds, expanding the market size and influence of Cipher (CIP).

(2) Demand for digital assets

Digital assets are the core and goal of Cipher (CIP). As the trend of digitization and decentralization continues to strengthen, the demand for digital assets will continue to increase and diversify, such as more people Will want to own and trade their own digital identity, digital assets, digital content, etc. The demand for digital assets will also bring more creativity and value, promoting the innovation and development of Cipher (CIP).

(3) Awareness of privacy protection

Privacy protection is the feature and advantage of Cipher (CIP). As users'awareness of the privacy and security of their data and assets continues to increase, the demand for privacy protection will continue to increase and strengthen. For example, more people will want to conduct

safe and efficient transactions and verifications without revealing their information. The need for privacy protection will also bring more trust and cooperation, enhancing the Cipher(CIP) community and ecosystem.

PART

08

COMPETITIVE ADVANTAGE

Competitive Advantages

Unique positioning

Cipher (CIP) is a digital asset platform based on Bitcoin Inscription. It takes advantage of EVM to provide users with a secure, private and innovative digital asset platform while maintaining compatibility and interoperability with Bitcoin Inscription. Operability.

Cipher(CIP) is uniquely positioned to attract not only users who are interested in Bitcoin Inscription but are not satisfied with the limitations and inconveniences of Bitcoin Inscription, but also those who are interested in Ethereum but are not satisfied with the limitations and inconveniences of Bitcoin Inscription.

Users who want to take advantage of the technology and potential of Bitcoin Inscription. Cipher(CIP) is also valuable in its positioning to provide users with a more advanced and flexible platform to create and trade various types and formats of inscribed assets while enjoying the advantages of Bitcoin and Ethereum.

Powerful technology

Cipher(CIP)’s technology is powerful. It implements a compatible inscription protocol based on Ethereum’s ERC-20 standard, allowing users to

seamlessly transfer and trade inscriptions between Bitcoin and Ethereum. assets.

Cipher(CIP) technology also uses ZKP technology to achieve high-speed and low-cost transactions and verification, protecting user privacy and security. Cipher(CIP) technology also provides some innovative functions and services, such as Cipher cross-chain bridge, providing users with some creative and valuable functions and services.

Large market

The market advantage of Cipher(CIP) is that it can satisfy those who are interested in the digital assets of Bitcoin Inscription and Ethereum, but want to be able to create and trade various types and formats on a more advanced and flexible platform The needs and expectations of users of inscribed assets.

Cipher(CIP)’s market advantage also lies in its ability to leverage the large and active markets of Bitcoin Inscription and Ethereum to attract and retain more users and funds, forming a strong and stable community and ecosystem.

About the Team

Cipher(CIP)’s team advantage is that it is composed of a group of professionals from different fields and backgrounds, who have rich experience and knowledge, as well as passion and vision for Bitcoin inscriptions and digital assets.

The advantage of Cipher(CIP)'s team is that it has good cooperative relationships with some well-known institutions and organizations. These data show that Ethereum has formed a large and active market, and there is still a lot of room and potential for growth.

Ecosystem

The ecological advantage of Cipher(CIP) is that it can interact and collaborate with the ecosystems of Bitcoin and Ethereum, using the resources and partners of the two networks to expand the application scenarios and influence of Cipher(CIP).

The ecological advantages of Cipher (CIP) enable it to seamlessly integrate and interoperate with other platforms and protocols in the field of digital assets, such as unisat, ZKSwap, etc. The ecological advantages of Cipher(CIP) also enable it to establish and maintain a strong and active community and ecosystem in the field of digital assets, allowing users to participate in the development and decision-making of Cipher(CIP) projects through voting and governance.

PART

09

ECONOMIC MODEL

Economic Model

Total number of tokens

The total number of Cipher(CIP) tokens is 21 million. This number refers to the total number of Bitcoin tokens to reflect the association and compatibility of Cipher(CIP) with Bitcoin Inscription. The total amount of Cipher (CIP) tokens is fixed and will not be issued or reduced to ensure the scarcity and value of the tokens.

Token distribution

40% is used for public sale to raise funds from the community and users to support the development and operation of the Cipher (CIP) project. Tokens for public sale will be released according to certain rules and schedules to prevent excessive circulation and volatility of tokens.

20% is used for teams and consultants to motivate the founders and partners of the Cipher(CIP) project and promote the innovation and quality of the Cipher(CIP) project. Tokens of teams and advisors will be locked and unlocked according to certain rules and schedules to prevent excessive concentration and abuse of tokens.

20% is used for ecological construction, rewarding developers and contributors of the Cipher(CIP) project, and expanding the functions and

services of the Cipher(CIP) project. Tokens for ecological construction will be distributed and issued according to certain rules and standards to prevent excessive consumption and waste of tokens.

10% is used for reserve funds to deal with the future needs and risks of the Cipher (CIP) project and ensure the stability and security of the Cipher (CIP) project. The tokens of the reserve fund will be used and managed according to certain rules and conditions to prevent excessive occupation and loss of tokens.

10% is used for community governance, allowing Cipher(CIP) project currency holders and users to participate in the decision-making and management of the Cipher(CIP) project, and realizing the decentralization and autonomy of the Cipher(CIP) project. Community-governed tokens will be voted and governed according to certain rules and mechanisms to prevent excessive control and influence of tokens.

Usecases of CIP token

Payment fees

Users can use Cipher(CIP) tokens to pay various fees on the Cipher(CIP) platform, such as fees for creating, transferring and trading inscribed assets, and using Cipher NFT, Cipher DAO, Cipher DEX, etc. Fees for features and

services. Tokens paid for handling fees will be destroyed to reduce the circulation of tokens and increase the value of the tokens.

Rewards

Users can obtain rewards of Cipher(CIP) tokens by using various functions and services on the Cipher(CIP) platform, or participating in various activities and tasks of the Cipher(CIP) project, such as creating and trading inscriptions. Asset rewards, as well as rewards for participating in Cipher DAO and Cipher DEX. The tokens for obtaining rewards will be issued from the tokens of ecological construction to encourage users' participation and contribution.

Participate in governance

Users can participate in the governance of the Cipher(CIP) project by holding Cipher(CIP) tokens, such as voting and decision-making on the direction and strategy of the Cipher(CIP) project, as well as supervising and auditing the operation of the Cipher(CIP) project. and finance. Tokens participating in governance will be deducted from community governance tokens to reflect the rights and responsibilities of users.