BitTrust

The Bitcoin second layer application
technology network optimization
inscription transaction solution

Light Warp Speed For Bitcoin By Lightning
Network

white paper

Overview

Bitcoin Inscription has relatively low liquidity, which makes it more difficult and expensive to create new things in the Bitcoin ecosystem. In comparison, other blockchain platforms such as Ethereum offer more flexible and cost-effective ways to build and innovate. In the Bitcoin ecosystem, it is relatively difficult to create new applications and usage scenarios due to its different design goals. The main goal of Bitcoin is to serve as a decentralized digital currency, emphasizing security and decentralization features. Therefore, Bitcoin's functionality and scalability are subject to some limitations, making the creation of new applications and value in its ecosystem more limited.

However, as a long-termist, I am more concerned about new narratives that can create actual value, broaden Web3 usage scenarios, and take the Web out of the circle. In this regard, Ethereum and other blockchain platforms with smart contract functions provide a broader space for innovation. The openness and flexibility of the POS public chain of the Ethereum ecosystem enable developers to build various innovative projects such as decentralized applications, non-fungible tokens, and decentralized finance. Therefore, if you focus on long-term real value creation and driving the progress of Web3, the Bitcoin blockchain platform requires new technical solutions to solve existing problems; these solutions may provide a wider space for innovation and more opportunities, To realize the vision of more dimensional industries and create a new financial narrative.

Chapter 1 Introduction

Bitcoin is a decentralized digital currency and is regarded as one of the milestones of blockchain technology. This white paper aims to introduce the background, birth and development of Bitcoin, and highlight its new possible interactions as a decentralized digital inscription asset. The birth of Bitcoin can be traced back to 2008, when a person or team under the pseudonym Satoshi Nakamoto published a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." This white paper proposes the concept of a decentralized digital currency based on blockchain technology, aiming to solve the centralization problem and lack of trust in the traditional financial system. The core concept of Bitcoin is to achieve peer-to-peer value transfer in a decentralized manner and to get rid of dependence on central institutions. It is based on blockchain technology and stores transaction records on a public distributed ledger, which is jointly verified and maintained by participants throughout the network. This decentralized design gives Bitcoin many unique features and advantages.

First, the decentralized nature of Bitcoin allows no single entity to control or manipulate the entire network. This means that no central authority can freeze accounts, prevent transactions, or manipulate the currency supply. The issuance and circulation of Bitcoin are jointly determined by algorithms and network participants, ensuring fairness and transparency.

Secondly, the security of Bitcoin is guaranteed by its cryptography and consensus mechanism. The Bitcoin network uses public and private key encryption technology to ensure transaction security and user privacy protection. At the same time, Bitcoin’s consensus mechanism ensures the security of the network and its ability to resist attacks through mining.

In addition, Bitcoin, as a decentralized digital currency, is globally accessible and borderless. Anyone with an internet connection and a Bitcoin wallet is able to freely send and receive Bitcoins, no matter where they are. This opens up new possibilities for financial inclusion and financial freedom on a global scale.

The birth and development of Bitcoin provides a model of decentralized digital currency for the entire financial withdrawal industry. By promoting the application and awareness of Bitcoin, BitTrust can further promote the development of decentralized finance and achieve

a fairer and more inclusive financial system. Bitcoin has changed people's understanding of money, finance and value transmission, bringing greater financial freedom, reliability and sustainability to individuals and society. Although its early main application was in the payment field, Bitcoin's potential goes far beyond that. With the advancement of technology and the emergence of innovation, more and more people are beginning to explore the application of Bitcoin in a wide range of fields such as smart contracts, non-fungible tokens, and decentralized finance.

Two Bitcoin upgrades in early 2023, namely SegWit and Taproot, played a key role in the emergence of non-fungible tokens on the Bitcoin chain. The SegWit upgrade helps scale Bitcoin by introducing a block field to hold signatures and public keys for Bitcoin transactions. However, this design has potential vulnerabilities that force developers to limit the size of this data. When the Taproot upgrade came along, it addressed these security issues, allowing the old SegWit restrictions to be removed, paving the way for storing large chunks of non-fungible data on-chain. This means that Bitcoin’s technological evolution provides the basis for non-fungible tokens on the chain. The working principle of Bitcoin is based on the concept of fungible tokens. Each Bitcoin is of equal value and can be exchanged at equal value. The total amount of Bitcoin is 21 million, and the smallest unit is Sat, of which 1 BTC is equal to 100 million Satoshi. The Ordinals protocol is a system of numbering Satoshis, giving each Satoshi a serial number and tracking them across transactions, giving each Satoshi uniqueness. Satoshi serial numbers are assigned in the order in which they were mined. For example, the first Satoshi in the first block has a sequence number of 0, the second Satoshi has a sequence number of 1, and the last Satoshi of the first block has a sequence number of 4,999,999,999. In addition to satoshi serial numbers, the Ordinals protocol also supports inscriptions. Inscription is a file that converts any content, such as pictures, videos, etc. A protocol attached to a single satoshi, turning it into a digital artwork native to Bitcoin. By sending the Satoshi to be inscribed into the transaction, the inscription content will be displayed on the chain. This content is then linked to the corresponding satoshi, transforming it into an immutable digital artwork that can be tracked, transferred, stored, purchased, and sold. These technologies and upgrades show that Bitcoin is not static. As technology continues to develop, unexpected innovations may appear in Bitcoin, and of course loopholes may also appear. This kind of innovation and evolution provides broader possibilities for Bitcoin's application fields, including areas such as non-fungible tokens and digital artworks.

The Ordinals protocol, also known as the BRC20 protocol, is still in its early stages and has not yet been widely adopted in the Bitcoin ecosystem. Compared with other platforms, the functionality and ecosystem of Ordinals may still need to be further developed and improved. Additionally, since Bitcoin was not designed to be used in the first place, there may be some challenges in terms of performance and scalability. Ordinals is a protocol implemented on the Bitcoin blockchain that provides users with the ability to create, transact, and manage within the Bitcoin ecosystem. While still in its early stages, Ordinals’ decentralized nature and integration with Bitcoin make it potentially innovative. As

technology develops and user demands increase, the Ordinals protocol is expected to play an important role in the Bitcoin ecosystem. The second-generation application upgrade Lightning Network will subvert all existing Bitcoin network applications in multiple dimensions.

Chapter 2 Summary

Bitcoin is a decentralized digital currency that was proposed and implemented in 2009 by Satoshi Nakamoto. Bitcoin is based on a technology called blockchain, which is a public, distributed ledger that records all transactions on the Bitcoin network. Including unspent transaction output and Double-spending, Bitcoin achieves secure transaction verification and currency issuance control through cryptography technology. Transactions are broadcast and verified by nodes in the network, and are packaged into blocks and added to the chain. The Bitcoin network consists of thousands of nodes, each of which has a complete copy of the blockchain. This decentralized structure prevents Bitcoin from being controlled by a single entity while providing resistance to censorship and failure. The security of Bitcoin is achieved through cryptography technology and consensus mechanism. Bitcoin uses public key cryptography to ensure the security and authentication of transactions. Each participant has a public key paired with a private key, which is used to sign transactions to prove ownership. Bitcoin's consensus mechanism is Proof of Work, which uses nodes to perform complex calculations to verify transactions and add new blocks to the blockchain. This mechanism ensures the security of the network and prevents fraud such as double spending. In addition to being a decentralized digital currency, Bitcoin is characterized by global accessibility and openness. It enables fast, low-cost cross-border payments and provides financial inclusion to the unbanked. In addition, Bitcoin, as an open protocol, also provides developers with rich innovation space to build various applications and services based on Bitcoin technology.

Bitcoin Inscription serves as an important component in expanding the functionality of Bitcoin, bringing new possibilities and innovations to the Bitcoin ecosystem. Traditionally, Bitcoin has been primarily thought of as a fungible digital currency, with each Bitcoin being equivalent to every other Bitcoin. However, by introducing inscriptions, the Bitcoin network can support unique and non-fungible digital assets. Inscriptions are non-fungible tokens based on Bitcoin blockchain technology, each token has unique properties and identity. What makes Bitcoin Inscription unique compared to other blockchain platforms is that they leverage the security and decentralized nature of Bitcoin. This means that Bitcoin Inscription can benefit from the strong security of the Bitcoin network and a globally distributed (such as light node, full node) node network. The introduction of Bitcoin Inscription expands the uses of Bitcoin. They can be used for digital artwork, collectibles, gaming items, identity verification, and a variety of other applications. The introduction of Bitcoin Inscription not only expands the uses of Bitcoin, but also enhances its security. The decentralized nature of Bitcoin makes Inscription’s transactions more secure and reliable. Due to the distributed nature of the Bitcoin network, inscription ownership and transaction records are widely replicated and verified, making them more difficult to tamper with or

counterfeit. But Bitcoin Inscription also faces some challenges. Bitcoin's scripting language is relatively limited, which may limit Inscription's flexibility and functionality. However, the Bitcoin community has been working hard to improve the scripting language to provide more functionality and extensibility. The existing SegWit and Taproot are relatively fast ways to solve the Ordinals protocol in the short term.

3. Background

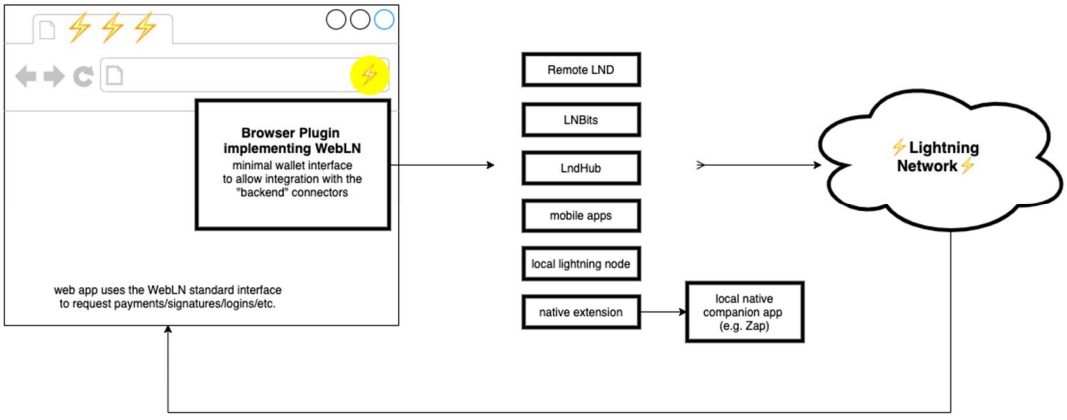
During the BTC network transfer process, the UTXO-based calculation model means that each transaction generates a large number of input balances and output balances. When associated with the user's account balance description, this detail forms a sum in the blockchain record, That is the combination of input and output. Additionally, each Bitcoin unit is made up of smaller denominations called Satoshis, with one Bitcoin containing one hundred million Satoshis (10^8 sats). Therefore, 50 BTC in the network can be transferred as 4,999,999,999 sats. When users conduct BTC transactions through the network, the records are as follows:

During the BTC network transfer process, the UTXO-based calculation model means that each transaction will generate a large number of input balances and output balances. When associated with a user's account balance description, this detail forms a sum in the blockchain record, a merging of inputs and outputs. The use of sats follows a first-in-first-out principle, following a specific order, with the earliest generated sat being used first in a transaction. This includes the first SAT minted in a block, the initial SAT mined during the difficulty adjustment, the first SAT generated during the halving event, and more. Serial numbers assign unique identifiers to moons that were minted at these different moments or have unique characteristics, classifying them into varying degrees of rarity to enhance their collectible appeal. Thanks to two major upgrades previously implemented on the BTC network, Ordinals has made it possible to embed token-related information into the BTC network.

In August 2017, the BTC network underwent a Segregated Witness upgrade, which is a strategic improvement that mainly separates the transaction signature data, witness data, and its information content, transaction data. Signature data finds a new home in so-called "Segwit" blocks, while transaction information remains in the original block. This structural modification enables a single BTC network block to accommodate a greater number of transactions, thereby enhancing the Bitcoin network's transaction processing capabilities and facilitating network expansion. In 2018, the BTC network underwent another transformation with the Taproot upgrade, which brought greater flexibility and privacy to the ecosystem. An important component of this upgrade is the implementation of Tapscript, an enhanced version of the Bitcoin programming language Script. This addition helps

incorporate supplemental content into transaction inputs. The combination of SegWit and Taproot upgrades effectively overcomes the data storage limitations of the BTC network. As a result, Ordinals are able to preserve various data formats such as text, images, JSON data in the witness data. Additionally, the stored data is exempt from execution, allowing it to remain permanently within the BTC network.

Therefore, the essence of BRC-20 at this stage is as follows: ordinal numbers are integrated into the BTC network in the form of JSON, similar to a text ledger containing deployment, minting and transfer logic that ultimately forms an inscription. Any data injected is called an inscription. On this basis, identifiers are assigned to sats, coupled with inscription injection, enabling users to issue or mint BRC-20 tokens through the Ordinal protocol. For example, the first BRC-20 token is ORDI, named after the first four letters of Ordinal, with a total supply of 21 million. Users only need to pay on-chain GAS fees to mint. Most BRC-20 tokens are deployed primarily through third-party tools. The BRC20 Wallet simplifies this process, providing a lightweight wallet plug-in that speeds up the deployment and trading process of BRC-20 tokens, but the platform leverages Lightning technology to expand even more possibilities. Most BRC-20 tokens are deployed primarily through third-party tools. Mainstream wallets simplify this process, providing a lightweight wallet plugin that speeds up the deployment and trading process of BRC-20 tokens. At the same time, the wallet is not a native Bitcoin starting with 1. After setting up the wallet, users can explore the corresponding official website market and view various BRC-20 token information and listing prices. Users can also choose to search for tokens that have not completed the minting process on the BRC-20 token search page provided by the old market, and then continue minting. Likewise, once the tokens are minted, they can be sold on the market. Users can deploy domain names or mints with custom parameters on the old platform official website. Users can upload files, mint domains, or BRC-20 tokens. If the receiving address is verified to be accurate, the user needs to pay the corresponding GAS fee. Generally speaking, within 10-30 minutes, or even an hour, users will find newly minted BTC Inscription assets in their wallets.



While the recent enthusiasm surrounding the BTC ecosystem lags far behind traditional NFTs, the evolution of ideas related to BRC-20 tokens continues unabated. For example, Binance highlighted another token format, ORC-20, on May 13. The format is a technological step forward from BRC-20, with greater adaptability and customizable features, enhancing its security and reliability. Features such as the ability to adjust the initial supply and maximum mintable volume, as well as the ability to use any size designation, make the ORC-20 a potential catalyst for wider adoption in the future. In another development, the Litecoin community launched a forked version of the BRC-20 token, called the LTC-20 token, on May 2. Due to the efficiency of the Litecoin network, the time to generate a block is 2.5 minutes and the cost per transaction is approximately 0.1u. Litecoin’s solution is to enable a concept similar to Bitcoin’s lightning technology. And more people are paying attention to the fact that it is the third new upgrade of Bitcoin, the Lightning Network payment solution.

BitTrust by Technical interface, the entire system has achieved comprehensive improvements in the three channels of the Lightning Network. Through channel management, BOLT12 agreement, and the LNURL protocols, not only improve the performance and reliability of the Lightning Network, BitTrust also brings broader improvements to the expansion of inscription and Bitcoin itself. BitTrust's BRC20 Bitcoin Lightning Network wallet offers a unique experience in terms of technology. By using the BRC20 standard smart contract, the Lightning Network extends the functionality of Bitcoin, allowing users to experience richer functions and applications in their wallets. In addition, channel management has been optimized to enable an unlimited number of off-chain transactions, thereby increasing transaction speed and reducing transaction fees. By introducing the BOLT12 agreement and the LNURL protocol, it improves routing and payment paths, increasing network stability and efficiency. At the same time, BitTrust utilizes advanced encryption technology and security measures to protect users' assets and privacy from threats. These technical advantages allow BitTrust's Lightning Network wallet to provide users with an efficient, secure, and low-cost transaction experience and expand the functions and application scenarios of Bitcoin, especially the second-tier track.

Chapter 3 Technical Overview

Bitcoin’s Lightning Network is a technological innovation designed to solve the pain points in the existing second-layer network field. By introducing private payment channels and fast routing mechanisms, the Lightning Network provides an efficient, low-cost solution that improves the speed, scalability and cost-effectiveness of inscription transactions. In Bitcoin's Lightning Network, the solution to the double-spend problem involves multi-signature determination, Revocable Sequence Maturity Contract, RSMC, Hashed Time-Locked Contract, HTLC and Commitment Transaction professional solutions. First, BitTrust will briefly introduce the Lightning Network.

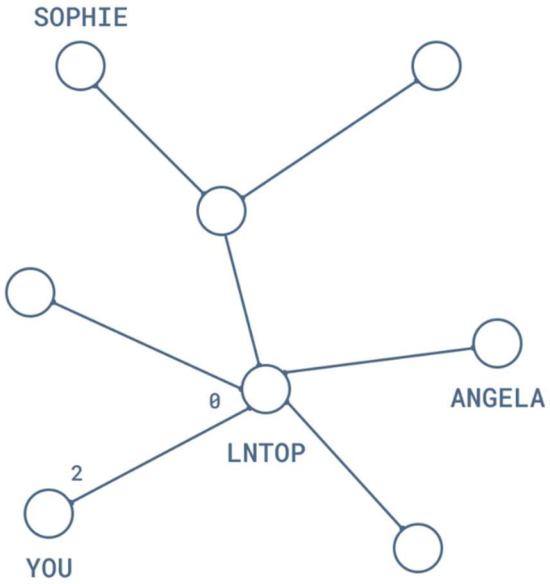
1 Lightning Channel:

Multi-Signature Confirmation: The Lightning Network channel uses multi-signature confirmation technology, which means that during the opening and closing process of the channel, the signatures of multiple participants are required to execute transactions. Multi-signature provides an additional layer of security, ensuring that funds within a channel can only be controlled and transferred between participants.

Multi-Signature: Lightning Network’s channels use multi-signature technology, a cryptographic technology that requires the signatures of multiple participants to execute a transaction. Multi-signature usually adopts the M-of-N mode, where M represents the minimum number of signatures required and N represents the total number of participants. When the channel is opened, participants will jointly create a multi-signature address, which requires at least M signatures to unlock funds. Bitcoin's scripting language provides a multi-signature function. Participants can use their own private keys to sign and add multiple public keys to the transaction to achieve multi-signature verification.

Channel Opening: Channel opening is achieved by creating a normal transaction on the Bitcoin blockchain. This transaction is called a Funding Transaction and contains the necessary information needed to open the channel. To open a transaction, participants need to provide their respective public keys, fund distribution, and multi-signature output scripts. Participants can use Bitcoin wallet software or a specific Lightning Network wallet

to create this opening transaction and broadcast it to the Bitcoin network. Once this transaction is confirmed and recorded on the blockchain, the channel is successfully opened and participants can begin conducting fast and cheap transactions within the channel.



Channel Payment: Once a channel is opened, participants can make multiple peer-to-peer payments and transactions within the channel without recording each transaction on the Bitcoin blockchain. These transactions only require status updates within the channel and final settlement when required. Participants can make payments by updating the channel's balance status, and these updates require signatures between participants to take effect. Bitcoin’s normal signature mechanism is used to verify the legitimacy of transactions and ensure the authorization of participants. In the Lightning Network, payments and transactions within a channel are implemented through multiple signatures and status updates between participants.

Channel Closure and Settlement: When participants decide to close a channel, they can complete settlement by submitting a normal transaction on the Bitcoin blockchain. This transaction is called the Closing Transaction, and it updates the channel’s balance status and distributes funds to the parties. When the channel is closed, participants need to sign the transaction to confirm the closing operation. Once this transaction is confirmed and recorded on the blockchain, the channel is successfully closed and participants can withdraw their funds in the channel. The Lightning Network also provides a mechanism

called Settlement Transaction to handle balance imbalances when the channel is closed and ensure the correct distribution of funds.

In the Lightning Network, a channel is opened by creating an ordinary transaction on the Bitcoin blockchain. This transaction is called the Funding Transaction, and it contains the necessary information needed to open the channel, such as the participants' public keys, fund distribution, and multi-signature output scripts. To open a transaction, participants need to jointly create a multi-signature address, which requires the signatures of at least multiple participants to unlock the funds in the channel.

Multi-signature script: A multi-signature script is a special script in the Bitcoin script language that is used to implement multi-signature functions. Participants can sign transactions using their respective private keys and add multiple public keys to the transaction. The multi-signature script defines the minimum number of signatures required and the list of participants' public keys.

M-of-N mode: Multi-signature usually adopts M-of-N mode, where M represents the minimum number of signatures required and N represents the total number of participants. Only when at least M valid signatures are collected, the transaction can be recognized and executed. This mode allows flexible configuration of multi-signature schemes to suit different security requirements.

Multi-signature address: When a channel is opened, participants jointly create a multi-signature address. This address is associated with a multi-signature script that requires at least M signatures to unlock the funds within it. Multi-signature addresses provide a flexible way to manage funds and ensure that transactions can only occur when the required number of signatures is met.

Hashed Time-Locked Contract, HTLC, is a protocol contract in the Lightning Network that is used to ensure the security and reliability of transactions within the channel. It combines a hash function and a time locking mechanism so that transactions can be executed under specific conditions. For example, the payer can only unlock the funds and complete the transaction when the payee provides a predetermined hash value.

For example, suppose Alice and Bob jointly create an opening transaction in which 1 Bitcoin Inscription is locked as funds within the channel.

This opening transaction contains Alice and Bob's public keys and a multi-signature script. The multi-signature script uses two public keys and requires the signatures of at least two participants to unlock the funds. The purpose of this design is to ensure that the funds in the channel can only be used under the joint control of both parties, increasing security and trust.

Once the channel is open, Alice and Bob can conduct fast, cheap, and private payments and Lightning Network transactions. For example, Alice can send Bob 0.1 Bitcoin inscription, and they can record this transaction by accounting inside the channel. Such an accounting process does not need to be recorded on the Bitcoin blockchain, so it can be completed quickly and without incurring high transaction fees.

When Alice and Bob decide to close the channel, they can complete settlement by submitting the final channel balance to the Bitcoin blockchain. Assuming the final channel balance is 0.8 Bitcoin Inscriptions, they can create a settlement transaction that allocates this balance to their respective Bitcoin addresses. In this way, all transactions within the channel are aggregated and recorded on the Bitcoin blockchain, ensuring the security and credibility of the final transaction results.

Channel opening and fund locking: In the Lightning Network, channel opening involves participants jointly creating a multi-signature opening transaction (Funding Transaction) and locking a certain amount of funds in the channel. These funds are used for payments and transactions within the channel. The opening of the channel only requires recording an opening transaction on the Bitcoin blockchain, rather than recording each transaction in the channel, which is consistent with the role of a catalyst in biochemistry.

In the Lightning Network, a multi-signature transaction jointly created by participants is called a Funding Transaction, which includes the public keys of multiple participants and corresponding multi-signature scripts. These multi-signature scripts use multiple public keys to verify the validity of transactions, ensuring the security and controllability of funds within the channel, much like substrates and catalysts in biochemistry.

Once the channel is opened, participants can make fast, cheap and private payments and transactions, and these transactions do not need to be recorded on the Bitcoin blockchain, but are achieved through in-channel accounting. In-channel accounting refers to the

process of making transactions between channel participants that are not immediately broadcast to the Bitcoin blockchain, but are instead settled once and for all when the channel is closed. This is similar to the intermediate products in a biochemical reaction, which do not need to be recorded, only the starting materials and final products are focused on.

Fast and Cheap Transactions: Because Lightning Network's intra-channel transactions do not need to be recorded to the blockchain every time, fast and cheap transactions can be achieved. Participants can conduct multiple peer-to-peer transactions within the channel and only need to update the balance status of the channel and perform final settlement when needed. This approach greatly reduces transaction costs and time.

Channel Closure and Settlement: When participants decide to close a channel, they can complete settlement by submitting the final transaction status on the Bitcoin blockchain. The final transaction status will reflect the latest balance within the channel and allocate funds to the parties. This process ensures the security and reliability of transactions within the channel.

In the Lightning Network, when a participant opens a channel, a multi-signature Bitcoin transaction is created, which requires the signatures of multiple participants to be valid. Multi-Signature is a Bitcoin script that requires at least a specified number of private key signatures to unlock Bitcoins when executing a transaction.

Commitment Transaction is a transaction type in the Bitcoin Lightning Network, used to record the distribution of funds within the channel. Whenever a participant within the channel makes a transaction, a Commitment Transaction is created to update the channel's status. This transaction requires the signatures of multiple participants to be effective, and only the latest Commitment Transaction will be recognized.

The following are the technical details of Commitment Transaction:

1. Inputs: The input of the Commitment Transaction is the output of the previous Commitment Transaction, that is,

The output of the previous transaction. Typically, each participant will have an input representing the proportion of their funds in the channel.

2. Outputs: The output of the Commitment Transaction defines the new fund allocation situation. Each output contains a Bitcoin amount and a Bitcoin address of the recipient. These outputs define new ways of allocating funds within the channel.

3. Signature: Commitment Transaction uses a signature script, which requires the signatures of multiple participants to unlock Bitcoin when executing transactions, including miner mining signatures, mine farm signatures, and mining pool signatures. This ensures that only all participants agree that the transaction can take effect, preventing a single participant from maliciously double-spending. Commitment Transaction requires each participant to sign the transaction to take effect. These signatures are typically generated using the elliptic curve digital signature algorithm and broadcast to the Bitcoin network along with the transaction.

4. Update and close the channel: Whenever a participant makes a transaction in the channel, they create a new Commitment Transaction to update the channel's status. When the channel needs to be closed, the final Commitment Transaction will be submitted to the Bitcoin blockchain to record the final status of the channel and the distribution of funds.

Through the creation and update of Commitment Transactions, the Bitcoin Lightning Network enables fast, private and secure transactions. At the same time, the double-spend problem is prevented from occurring.

HTLC is another Lightning Network contract type that is used to implement cross-channel atomic swaps. The HTLC contract sets a time lock condition and a hash condition to ensure that only transactions that meet specific conditions can take effect and prevent double-spend problems from occurring.

Revocable Sequence Maturity Contract is a protocol contract type in the Bitcoin Lightning Network, used to implement the withdrawal and update of funds in the channel. The RSMC contract ensures that participants can reverse the previous transaction status before the channel is closed by defining a series of conditions and rules.

Here are the technical details of RSMC:

1. RSMC output: In each Commitment Transaction, the RSMC contract will create a special output, called RSMC output. The RSMC output contains a portion of the funds within the channel and can only be unlocked and used under certain conditions.

2. Transaction cancellation conditions: The RSMC contract defines some conditions that allow participants to cancel the previous transaction status. These conditions usually include Time Lock and Sequence Number.

3. Time Lock: The time lock condition in the RSMC contract specifies the time that must be waited before the channel is closed. This time lock can be a fixed time period or a time interval relative to the previous transaction.

4. Sequence Number: The sequence number in the RSMC contract specifies the order and priority of transactions. Transactions with higher sequence numbers have higher priority and can override transactions with lower sequence numbers.

5. Revocable Transaction: When participants want to revoke the previous transaction status, they can create a revocable transaction. The revocation transaction contains the unlocking conditions for RSMC output and can unlock the funds in the channel when the conditions are met.

6. Revocation Key: The revocation key in the RSMC contract is the private key used to unlock the revocation transaction. Each participant has a revocation key that is used to reverse the previous transaction state and reallocate funds.

7. Commitment transaction update: When participants make a new transaction in the channel, they will create a new Commitment Transaction to update the status of the channel. The new Commitment Transaction will contain the updated fund allocation and new locking conditions for RSMC output.

Through the RSMC contract, participants in the Bitcoin Lightning Network can safely revoke previous transaction status and reallocate funds in the channel based on the latest Commitment Transaction. The design and implementation of the RSMC contract ensures the correct allocation of funds within the channel and the revocability of transaction status, thereby enhancing the security and credibility of the Lightning Network.

The Inscription Protocol solves the long-term problem of how to represent any fungible token asset on the Bitcoin blockchain. The Inscribed Token standard finally brings colored coins to Bitcoin and uses each Satoshi to represent a unit of ownership of a deployed token. This means that each unit of the token is forever backed by 1 Satoshi, which acts as a kind of “digital gold content” that supports the token’s value. This also means that by definition, each token can never be worth less than 1 satoshi.

Bitcoin Inscription It is a programming language for building and verifying smart contracts and non-fungible tokens (NFTs). Inscription uses native Satoshi units to represent each coin, meaning they can be split and combined just like regular Bitcoins.

Using Bitcoin Inscription, anyone can mint Inscription tokens and transfer them to any Bitcoin address type. This makes the issuance and transfer of Inscription tokens very flexible and can be used with wallets that support UTXO (Unspent Transaction Output) options. When it comes to the deployment of Inscription tokens, there are two common modes: direct deployment and decentralized deployment. Direct deployment means minting Inscription tokens directly into a designated Bitcoin address, which is simple and straightforward. Decentralized deployment disperses Inscription tokens into multiple Bitcoin addresses to improve security and flexibility. Additionally, Bitcoin Inscription comes with a built-in ticker service, providing a globally unique name system for tickers. The stock name registered for the first time is permanent and cannot be used again. This built-in name system provides a unique identity for Inscription Tokens, making it easier for users to identify and trade. To summarize, Bitcoin Inscription is Bitcoin’s scripting language for building and validating smart contracts and non-fungible tokens. It uses native Satoshi units to represent each token and can be used with wallets that support UTXO selection. Inscription tokens can be issued and transferred via direct deployment or decentralized deployment. Additionally, Inscription provides a built-in ticker service, providing a globally unique name system for tokens.

Chapter 4 Preprocessor Working Principle

Bitcoin Inscription works based on Bitcoin's blockchain technology and the Inscription scripting language. Here are the general steps for creating and tracking unique digital assets and ensuring their ownership and transferability:

1 Create a token: Using the Bitcoin Inscription scripting language, you can create a token that represents a specific asset. This token can contain metadata related to the asset, such as name, description, image, etc.

2 Minting Tokens: New inscription tokens can be minted by performing a special transaction on the Bitcoin blockchain. This transaction will contain an output containing the inscription script representing the new inscription.

3 Proof of Ownership: Bitcoin's blockchain records the history of every transaction, including the minting and transfer of inscriptions. By looking at transaction records, you can prove that an address owns a specific inscribed token.

4. Transfer tokens: To transfer ownership of Inscription tokens, you can create a new Bitcoin transaction and include a new Inscription script in the output of the transaction to transfer the tokens to a new Bitcoin address. In this way, the new address becomes the new owner of the token.

5. Verify Ownership: Anyone can verify the ownership of an Inscribed Token by checking transaction records on the Bitcoin blockchain. As long as a transaction containing a specific inscription script can be found, the current owner of the token can be confirmed.

The decentralized pre-casting process is as follows:

1 Create token

Decentralization is initialized with ticker, reward per mint, total mint allowed, starting block height, and metadata. Deployers can initialize a code such as $myticker123 to be awarded a minting pool award of 1,000 units, for a total of 10,000 allowed minting pools and start at block height 810,000 containing image.jpg , metadata, description, links and terms.

Initialization (init-dft)

The basic format for decentralized initialization using the Atomics CLI is as follows:

npm run cli init-dft <tick> <per_mint_amt> <mint_count> <start_height> <image>

Optional flags:

--mintbitworkc=<prefix>

--meta=@metadata.json

--satsbyte=<number>

Scatter initialization function initializes dft allows minting stocks tick to proceed as-dft command (described below) only starts from the starting block height and allows up to minting pool count total number of minting requests, each awarding a per minting pool amount to the request the token unit of the user. The effective total maximum supply is per_mint_amt * mint_count.

Notes: 3 block confirmations are required for the tick to take effect and the ticker will be claimed. You can query the status via npm run cli get <atomicalID> or npm run cli find-tickers

Required parameters:

Check: Globally unique stock code name

per_mint_amt: Number of token units rewarded for each successful minting. Satoshi amount.

Minting Pool Count: The total number of coins allowed before the quota is exhausted and "fully minted"

Starting Height: The starting block height at which casting can begin. Block height can be set to 0 or any future block height.

Image: An image icon representing the token. The file name will appear in the token. Use caution, first rename the file completely and include it as "image.jpg" or "image.png"

Optional flags:

--mintbitworkc=<prefix>

Defines an optional Bitwork mining prefix target for the mint. If set, the minter must expend CPU power to find a match for the prefix target in order to successfully mint. This forces minters to perform proof-of-work mining in a similar manner to Bitcoin mining itself.

It is recommended to choose a prefix between 4 and 6 hexadecimal digits. You can use any valid hexadecimal number between a-f0-9. It is purely a vanity trade ID, any value is enough to require the minter to expend effort to mint the coin.

Example time estimate for minter time required:

Notes: It can be any number in the range a-f0-9, BitTrust uses all 7 for illustration purposes only.

3 hex digits prefix "777" takes approximately 4 seconds to mine

The 4 hex digit prefix "7777" will take approximately 1 minute to mine

The 5 hex digit prefix "77777" will take approximately 16 minutes to mine

The 6 hexadecimal digit prefix "777777" will take approximately 256 minutes to mine

--meta=@metadata.json

Define optional metadata details in the token. The recommended format follows the convention sample-ft-meta.json

```json

{

"Name": "",

"describe": "",

"decimal": 0,

"Link":{

},

"legal": {
```

"Terms": ""

},

"Issuer": {

}

}

````

None of the fields in the metadata are required and can take any shape and form as long as it is a valid JSON object. But it is recommended that at least the name, description and legal information be provided to inform users of the token of its nature.

--satsbyte=<number>

Sets the satoshi per byte for transactions and overrides the default value.

2 Mint Token Valve (mint-dft)

The basic format of a decentralized mint using the Lightning Network CLI is as follows:

npm run cli mint-dft <tick>

Optional flags:

--satsbyte=<number>

The decentralized minting function mint-dft allows minting of stock quotes starting from the block height start_height.

Follow the on-screen instructions to cast.

Required parameters:

Tick: Globally unique stock code name

Optional flags:

--satsbyte=<number>

Sets the satoshi per byte for transactions and overrides the default value.

3 Header title
````

npm run cli mint-ft <tick> <total_supply> <image.jpg>

Optional flags:

--satsbyte=<number>

--meta=@metadata.json

The second way to mint or create a BRC-20 token type is to directly create a single output containing the total supply, with each Satoshi representing one unit of the token.

For example, to mint a token with a supply of 100,000,000, simply create an output containing exactly 1 full Bitcoin (since 1 BTC = 100,000,000 Satoshis). One advantage of using the direct minting model is that the team creating it must provide the required number of Bitcoins to substantiate the total minted supply; this greatly reduces the possibility of dishonest actors printing coins out of thin air.

Direct minting is ideal when a team or company wants to maintain control over the initial distribution and decide how the tokens are used at a later point in time.

Note: 3 block confirmations are required before claiming an offer. You can query the status using npm run cli get <atomicalID> or npm run cli find-tickers

Required parameters:

Tick: Globally unique stock code name

Total_supply: total supply units for direct casting

image: Image icon representing the token. The filename will appear in the token. Use caution, first rename the file completely and include it as "image.jpg" or "image.png"

Optional flags:

--satsbyte=<number>

Sets the satoshi per byte for transactions and overrides the default value.

--meta=@metadata.json

Define optional metadata details in the token. The recommended format follows the convention sample-ft-meta.json

```json

{

"Name": "",
```

"describe": "",

"decimal": 0,

"Link":{

},

"legal": {

"Terms": ""

},

"Issuer": {

}

}

````

None of the fields in the metadata are required and can take any shape and form as long as it is a valid JSON object. However, it is recommended to at least provide a name, description, and legal to inform users of the token of its nature.
````

Chapter 5 Functions of Bitcoin Inscription Trading Platform

There are some key differences between Bitcoin Inscription and traditional NFTs. Here are a few key differences between them:

1Function and purpose

Bitcoin inscriptions are mainly used to represent the ownership and transaction history of assets within Bitcoin. They record Bitcoin transfer and transaction information, ensuring the security and transparency of the Bitcoin asset network. The first was Bitcoin itself, then the USDT OMIN protocol assets, and now the Inscription protocol assets. Traditional NFTs are used to represent unique digital assets, such as artwork, music, game props, etc. NFTs can represent any digital content, and each NFT is unique, with unique properties and ownership.

Bitcoin Inscription is a scripting language primarily used to represent Bitcoin ownership and transaction history. They record Bitcoin transfer and transaction information and ensure the security and transparency of the Bitcoin network. Bitcoin Inscription is used in Bitcoin's transaction output model by using a scripting language to define the conditions and rules of a transaction.

Traditional NFTs are a standard for representing unique digital assets, most commonly the ERC-721 and ERC-1155 standards used on Ethereum. NFT can represent any digital content, such as artwork, music, game props, etc. Each NFT is unique and has unique properties and ownership. Unlike Bitcoin inscriptions, NFTs are designed to create and track unique digital assets on the blockchain and provide those assets with exact ownership and identity.

The main difference between Bitcoin Inscriptions and traditional NFTs is their design goals and uses. Bitcoin inscription is mainly used for Bitcoin transaction and ownership records, emphasizing the security and transparency of the Bitcoin network. Traditional NFTs focus on representing unique digital assets and providing exact records of ownership and identity.

2. Standards and Technology

The UTXO model of Bitcoin transactions and the consensus algorithm of the blockchain. Bitcoin Inscription uses cryptographic techniques such as hash functions and digital signatures to ensure that transactions are secure and tamper-proof.

Traditional NFTs use different standards and technologies, the most common being the ERC-721 and ERC-1155 standards on Ethereum. These standards define the basic functions and interaction methods of NFT, including the creation, transfer and ownership verification of NFT. Smart contract technology on Ethereum makes creating and managing NFTs more flexible and programmable. The difference between Bitcoin Inscription and traditional NFTs is not only their design goals and uses, but also the standards and technology they use. Bitcoin Inscription uses Bitcoin's scripting language and related encryption technology, while traditional NFT uses the ERC standard and smart contract technology on Ethereum.

3. Fungibility and uniqueness: Bitcoin inscriptions are fungible, that is, one Bitcoin inscription can be replaced by another Bitcoin inscription of the same amount, without substantial difference. Traditional NFTs are non-homogeneous. Each NFT is unique and has unique attributes and ownership. This means that each NFT has its own unique value and identity and cannot be simply replaced or interchanged.

	Fungibility (Bitcoin Inscription)	Non-fungibility (traditional NFT)
definition	They can be substituted for each other and there is no substantial difference.	Each NFT is unique and has unique properties and ownership.
exchange	Based on the quantity, there is no difference in the exchange between Bitcoin inscriptions.	Cannot simply be replaced or interchanged, each NFT has its own unique value and identity.
value	Mainly reflected in its quantity and market demand.	From its uniqueness, scarcity and the specific digital asset it represents.
Application scenarios	Mainly used as digital currency and store of value.	It has unique market value and appeal in the fields of digital art, collectibles and virtual assets.
storage	Up to 30GB.	Up to 300MB.

4. Market and Application: Bitcoin inscriptions are mainly used on the Bitcoin network to record Bitcoin transactions and ownership. Traditional NFTs are used on different blockchains and are widely used in the digital art market, gaming industry, virtual real estate and other fields. The uniqueness and irreplaceability of NFTs make them unique identifiers of digital assets, providing new opportunities for digital creators and collectors.

When it comes to the application scenarios of Bitcoin inscriptions and traditional NFTs, there is indeed more content worth extending. The following is a more detailed description of the application scenarios of Bitcoin Inscription and traditional NFT:

Bitcoin inscriptions are primarily used on the Bitcoin network to record Bitcoin transactions and ownership. It is part of Bitcoin and aims to provide a flexible programming language that enables users to create more complex transactions and

smart contracts. Bitcoin Inscription is designed to support the core functionality of Bitcoin as a decentralized digital currency and store of value.

Traditional NFTs are used on different blockchains and have wide applications in multiple fields. The most famous of these blockchains is Ethereum, which provides a decentralized platform that enables creators to create, issue and trade unique digital assets. Traditional NFT plays an important role in the digital art market, game industry, virtual real estate and other fields.

In the digital art market, traditional NFTs provide artists with a new way to create, sell and display digital artworks. Artists can convert their works into NFTs and ensure their uniqueness and irreplaceability via the blockchain while establishing a record of ownership for each work. This gives artists more creative freedom and the opportunity to communicate directly with collectors.

In the gaming industry, traditional NFT enables virtual items in games to have real ownership and value. Game developers can create unique virtual items and trade and transfer ownership through NFT. This provides players with more gaming experiences and financial incentives, while also creating new revenue streams for game developers.

In the field of virtual real estate, traditional NFT enables virtual land and real estate to have real ownership and value. Through NFT, users can purchase, own and trade land and real estate in the virtual world, which provides an important foundation and economic model for the development of virtual reality, metaverse and other fields.

5. The Bitcoin network is known for its strong security and decentralized features. Due to the security of the Bitcoin network, some projects and platforms have begun to store NFT ownership information on the Bitcoin blockchain, thus converting NFTs into the form of Bitcoin inscriptions.

A major advantage of this approach is the security of the Bitcoin network. The Bitcoin network is currently one of the largest blockchain networks. It has strong computing power and decentralization, making it highly secure and tamper-proof. Storing the NFT's ownership information on the Bitcoin network can rely on the security of the Bitcoin network to ensure the non-tamperability of the NFT and the reliability of ownership.

Another advantage is the fungibility of Bitcoin inscriptions. Converting NFTs into the form of Bitcoin inscriptions can make them more flexible in terms of trading and liquidity. Bitcoin Inscriptions can be traded just like Bitcoin, and due to the widespread acceptance and liquidity of the Bitcoin network, these NFTs can also be traded more easily on different platforms and markets. It is important to note that there are also some limitations and considerations when converting NFTs into Bitcoin inscriptions. Bitcoin Inscription has

a limited memory storage capacity of up to 30GB, which may limit the ability to store large NFTs. Additionally, Bitcoin Inscription is designed primarily to record Bitcoin transactions and ownership, rather than as a dedicated NFT platform. Therefore, there may be some technical and compatibility challenges that need to be addressed when converting NFTs into Bitcoin inscriptions.

The practice of converting NFTs into Bitcoin inscriptions may have certain advantages in some cases, especially in terms of security and liquidity. However, this does not mean that traditional NFTs will completely switch to Bitcoin Inscription, as the wide application of traditional NFTs on other blockchains and the demand in specific fields still exist. This depends on the specific project and application scenario, as well as different requirements for security, fungibility and functionality. There are obvious differences between Bitcoin inscriptions and traditional NFTs in terms of functions, uses, standards and market applications. Bitcoin inscriptions are mainly used for Bitcoin transactions and ownership records, while traditional NFTs are used to represent unique digital assets and have a wide range of applications in different fields.

Chapter 6 More Expansions of Lightning Network

Transactions on Bitcoin, especially those involving sequence numbers, have greatly benefited from previous Segwit protocol-level upgrades that reduced transaction weights and thus the overall fees for those transactions. However, Segwit was not originally designed for Ordinals—nor was Taproot, the Bitcoin upgrade that made the creation of Ordinals possible. The existence and proliferation of serial numbers on Bitcoin was made possible by unexpected reasons, but since their creation earlier this year, the Bitcoin development community has now come together to intentionally support such activity by building serial number-centric tools . When it comes to transactions and transfers of Bitcoin Inscriptions, the Lightning Network can be leveraged to optimize its performance and scalability. The Lightning Network is a second-layer solution built on top of the Bitcoin blockchain that enables fast, cheap, and private transactions by creating two-way payment channels and using multi-signatures. Here are a few aspects of how to leverage the Lightning Network to optimize Bitcoin Inscription:

Traditional NFT asset atomic state Atomic protocol

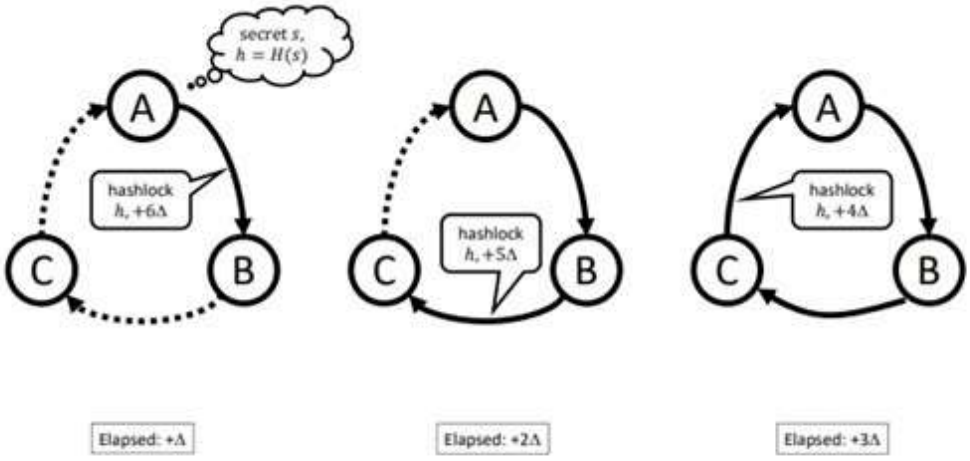
Traditional NFT asset deep pledge Sataking protocol

Traditional NFT asset fragments merge with Blockcypher protocol

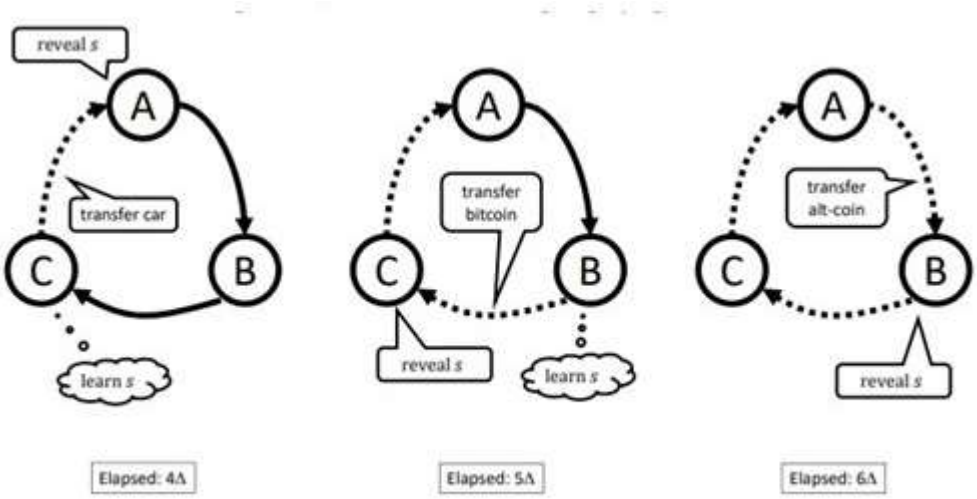
Traditional NFT asset atomic state Atomic protocol

Bitcoin Atomic Protocol is the fundamental protocol of Bitcoin and aims to realize atomic swap between different blockchains. The following details are mentioned in Brown University's Maurice Herlihy's 2022 paper Atomic Cross-Chain Swaps Solution: It allows for direct exchange between different blockchain networks without relying on third parties. trust or intermediary. The core idea of the Bitcoin Atomic Protocol is to ensure the security and reliability of exchanges through smart contracts and hash locking scripts. Both parties to the exchange create a locking script on their respective blockchains that contains a hashed locking condition. Both parties then share the hash in the locking

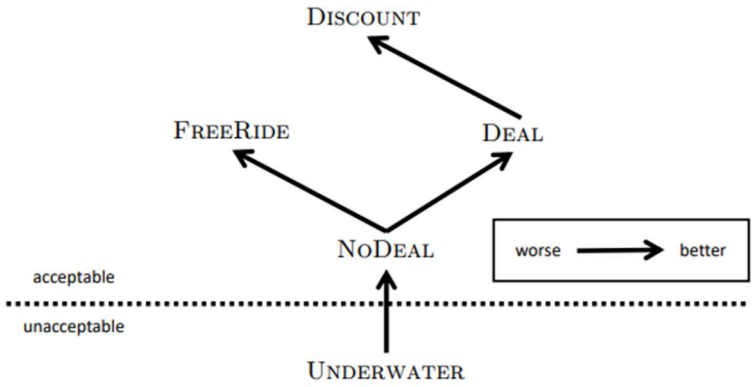
script with the other party. Next, both parties can unlock the other party's lock script and complete the exchange. An important application of the Bitcoin Atomic Protocol is atomic swaps between Bitcoin and other blockchains. For example, the Bitcoin Atomic Protocol can be used to perform atomic swaps between Bitcoin and Ethereum, enabling asset swaps between Bitcoin and Ethereum without the need to trust or rely on a centralized exchange. The Bitcoin Atomic Protocol is a technical solution that requires the cooperation and support of both parties to implement. The blockchain networks of both parties need to have corresponding smart contract functions and the ability to support atomic swaps. In addition, due to the different designs and characteristics of different blockchains, implementing atomic swaps may require solving some technical and compatibility challenges. Therefore, in the native Bitcoin protocol, multiple upgrades of the Segregated Witness protocol cannot fully solve the possibility of cross-chain interaction of existing traditional assets.



The Atomic Cross-Chain Exchange Protocol is a distributed coordination task that enables multiple parties to exchange assets across different blockchains, such as exchanging Ethereum NFT assets for Bitcoin Inscription assets. The protocol guarantees several important properties:

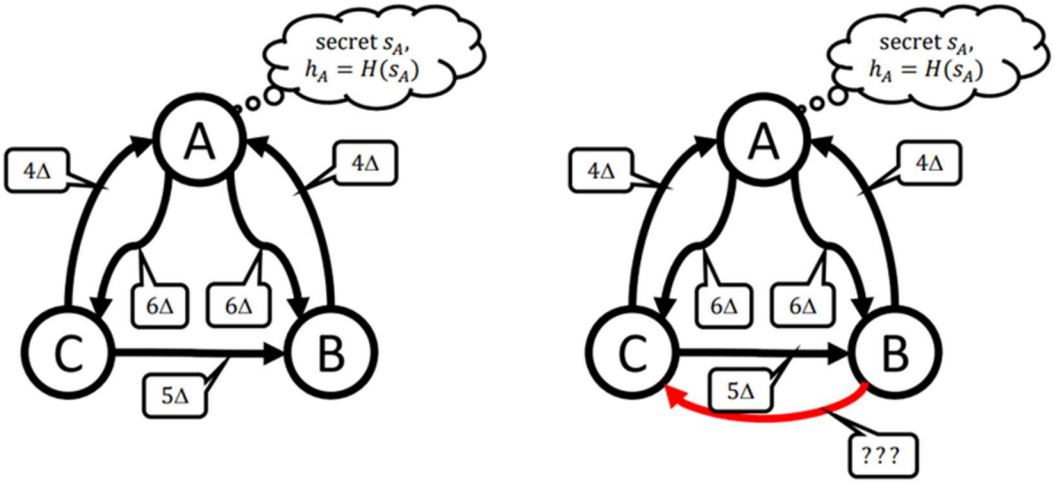


1. If all parties adhere to the agreement, all exchanges will occur: If all parties adhere to the agreement, the exchange of assets will occur as expected.

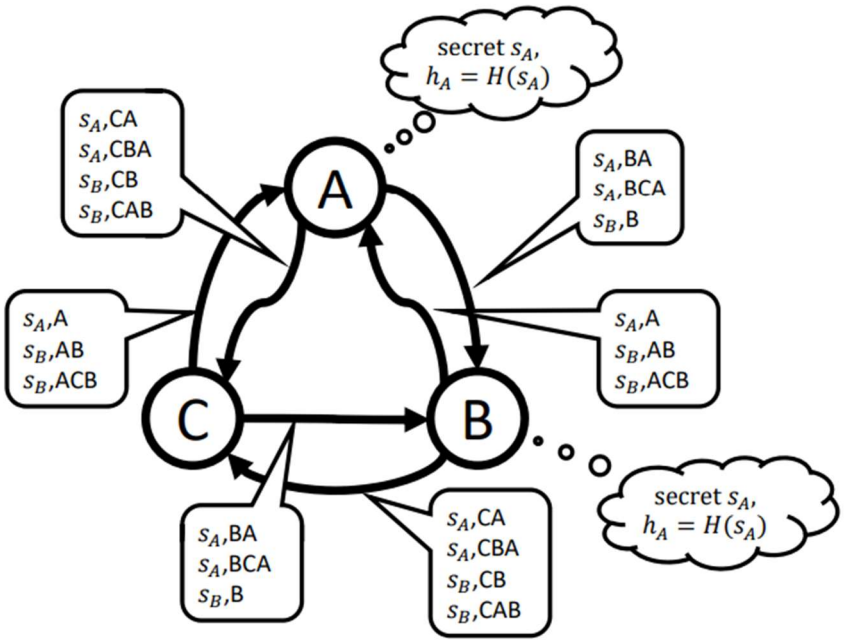


2. If the coalition deviates from the agreement, the parties that adhere to the agreement will not end up worse off: If a group of parties deviates from the agreement, the parties that adhere to the agreement will not be worse off.

All parties involved will not suffer any negative consequences.



3. No coalition has an incentive to deviate from the agreement: The agreement is designed in such a way that neither group has an incentive to deviate from the agreed-upon rules.



To model cross-chain exchanges, a directed graph D is used, where the vertices represent the parties involved and the arcs represent the proposed transfer of assets. For any pair (D, L), where D = (V, A) is a strongly connected directed graph, L⊂ V is the set of feedback vertices of D, providing an atomic cross-chain exchange protocol. Parties in

the feedback vertex set L generate hash-locked secrets that are used in the hash-time-locked contract.

It is worth noting that this protocol is only possible if the graph D is strongly connected and L is the set of feedback vertices. If D is not strongly connected or L is not a set of feedback vertices, it is not feasible to construct such a protocol. The time complexity of this protocol is O(diam(D)), where diam(D) represents the diameter of graph D. The space complexity is $O(|A|^2)$, which refers to the number of bits stored on all graphs involving blockchain assets, namely inscription assets.

In Bitcoin NFT cross-chain technology, enabling Lightning Network, cross-chain exchange is represented by a directed graph D = (V, A), where each vertex V in the graph represents the party participating in the exchange, and each arc A in the graph Represents a proposed transfer of assets through a shared channel. It should be noted that BitTrust assumes that D is connected, because a disconnected directed graph can be viewed as multiple independent exchanges. In game theory terms, exchange D can be viewed as a cooperative game in which all participants adhere to the agreement and asset transfers on each arc occur. Each possible outcome is given by the subgraph E = (V, A'), where A' is the set of triggered arcs in D. A proposed transition $(u, v) \in A$ occurs if it is also in A'. In short, BitTrust can say that arc (u, v) was triggered. A protocol is a strategy for playing the game, a set of rules that determine the actions each participant takes at different stages of the game. When simulating real-life situations, exchanges involving secret control by multiple parties are collaborative. Parties can form miners' alliances, also known as mining pools, which commit to a common strategy.

It is assumed that the directed graph of blockchain exchanges is constructed by a market clearing service, which may communicate with the parties through its own blockchain. The clearing service is not considered a trusted party because parties can check the clearing service's responses for consistency. That is, if the NOSTR protocol or the new protocol is not enabled, the mining fee may be higher and higher.

In this case, each party creates a secret s and a corresponding hash lock h = H(s). They will send their hash lock to the clearing service along with a quote describing the exchange they are willing to make. The clearing service will collate these proposals and publish the exchanged directed graph D = (V, A), where V is the set of vertices and A is the set of arcs. The clearing service also determines a vector $L \subset V$, serves as the leader of the feedback vertex set. These leader vectors include the hash locks h0, ..., h`, and the start time T of the exchange, which is at least Δ in the future.

At this stage, participants can evaluate whether they are willing to participate in the exchange based on information about the directed graph and feedback vertex set published by the clearing service. They can examine the structure of the directed graph and the leader of the feedback vertex set, and verify that the clearing service is processing what they quoted.

If the participants decide to participate in the exchange, they will perform corresponding operations according to the provisions of the agreement. This may involve generating and exchanging hash lock secrets, performing cross-chain asset transfers, and verifying the correctness of the transaction after the exchange is completed.

Hash key paths for bi-bootstrapping directed graph arcs

This contract includes functions such as asset transfer, initial exchange, redemption and refund. The contract's constructor is used to initialize assets and lock time. The initiateSwap function is used to initiate exchange, the redeem function is used to redeem assets, and the refund function is used to refund. During the redemption and refund process, the contract verifies that the provided secret matches the pre-stored hash and checks that the lock time has elapsed. The Atomic Cross-Chain Swap Protocol provides a safe and reliable method for parties to exchange assets across different blockchains. It ensures that exchanges occur as expected, protects parties adhering to the agreement from negative outcomes, and discourages deviations from agreed-upon rules. The feasibility of this protocol depends on the characteristics of the directed graph representing the exchange and the presence of a set of feedback vertices.

The Lightning Network is a second-layer protocol based on Bitcoin designed to provide fast, low-cost transaction and payment solutions. By establishing a two-way payment channel, it allows participants to conduct multiple transactions within the channel without recording each transaction on the blockchain. This can greatly improve the efficiency and scalability of transactions.

In cross-chain exchanges, the Lightning Network can be used as the basis for implementing atomic swaps. Participants can establish cross-chain payment channels through the Lightning Network, allowing them to exchange assets safely. By using Hash Time Lock Contracts (HTLC) and multi-signature transactions, the Lightning Network provides a mechanism to ensure the security and reliability of assets during cross-chain exchanges.

Traditional NFT assets deep pledge STAKING protocol

Provides a deep pledge mechanism for traditional NFT assets and liquidity within the industry or between tokens, allowing holders to obtain more asset returns. Implement fast, low-cost transaction and payment solutions based on the Lightning Network. Ensure the security and reliability of assets through the use of hash time lock contracts and multi-signature transaction mechanisms. Implementation steps:

1. Create a traditional NFT asset deep pledge contract: Design a smart contract in which the rules and conditions of deep pledge are defined. The contract should include the following functions: users can lock their traditional NFT assets in the contract for pledge. The contract records the amount and period of assets pledged by

each user, which is the timestamp technology solution of the Bitcoin Lightning Network (Bitcoin timestamp). Users can unstake and withdraw their assets at any time.

2. Integrate the Lightning Network: Use the Lightning Network as the underlying protocol to provide fast, low-cost transaction and payment functions for the deep staking protocol. By establishing a two-way payment channel, participants can conduct multiple transactions within the channel without recording each transaction on the blockchain.

3. Implement cross-chain payment channels: Participants can use the Lightning Network to establish cross-chain payment channels to achieve cross-chain asset exchange. By using hash time-lock contracts and multi-signature transactions, asset security and reliability are ensured during cross-chain exchanges.

4. Design an asset return mechanism: Based on the quantity and term of pledged NFT assets, design an economic return mechanism so that pledgers can obtain more asset returns. Rewards can be issued to stakers in the form of currency or other exchangeable assets.On the Ethereum protocol, there is an NFT card with a market price of $1,000, called the NFT product STAKING protocol. If user Bob chooses not to participate in STAKING or only holds Ethereum, he will not be able to earn any income or be displayed on this blockchain. However, on the Bitcoin network, user Bob can gain more attention. In addition to considering mining fees and market fluctuations, user Bob can obtain higher regular income by participating in the STAKING protocol. In addition, user Alice can transfer, replace, lend, mortgage, etc. use user Bob's NFT within a reasonable range with authorization. If it is a reverse operation, the name is Inscription Asset Pledge NFT, but Ethereum does not create a corresponding feedback mechanism.

Hash Time Lock Contract (HTLC) and multi-signature transactions ensure the security and reliability of asset exchange. Implement appropriate security audits and code reviews to ensure the security of the contract and the Lightning Network. Provide user support and monitoring mechanisms to promptly resolve potential problems and risks.

user experience:

BitTrust provides a user-friendly interface and operation process for in-depth staking of traditional NFT assets so that users can easily pledge. Real-time pledge and return information allows users to understand the status and returns of their pledged assets at

any time. In order to optimize transaction speed and cost, the Lightning Network is integrated as the underlying protocol to provide a fast, low-cost transaction and payment experience. BitTrust’s protocol uses hash time-locked contracts and multi-signature transactions to ensure the security and reliability of cross-chain asset exchanges. In addition, the return mechanism is designed and optimized to enable pledgers to obtain more asset returns. By providing a user-friendly interface and optimizing the transaction experience, BitTrust aims to improve the utilization value and user experience of traditional NFT assets. Best of all, everything is simpler and the miner fees are lower.

Traditional NFT asset fragments merge with Blockcypher protocol

1. Fragmentation algorithm: Design a fragmentation algorithm to divide traditional NFT assets into multiple fragments. This algorithm can be designed according to different needs and properties, such as splitting proportionally or splitting according to specific rules.Fragmentation methods for converting NFTs into Bitcoin inscriptions include proportional splitting, attribute-based splitting, random splitting, rule-based splitting, and function-based splitting. These algorithms can be customized based on needs and the characteristics of the asset to ensure that fragments are accurately split and assembled when converted into Bitcoin inscriptions. Proration is the proportional allocation to each shard based on the value or attributes of the asset, ensuring that each shard represents the same proportion or value. Splitting by attributes is the process of splitting an asset into pieces with similar attributes based on its specific attributes. Random partitioning creates shards by randomly selecting parts or attributes of an asset, increasing the diversity and unpredictability of the shards. Rule-based segmentation is the segmentation of assets into fragments based on predefined or user-defined rules. Different parts of an asset can be split into fragments based on rules or into a specific number of fragments based on user-specified rules. Function-based segmentation is dividing an asset into fragments based on its function or purpose so that when combined, the fragments can be selected and assembled as needed. These fragmentation algorithms provide multiple ways to convert NFT assets into fragments of Bitcoin inscriptions, and can be customized based on specific needs and asset characteristics.

2. Smart contract development:

The process when using smart contract platforms (such as Ethereum) to develop contracts to handle fragmented NFT assets

The Lightning Network allows users to establish payment channels off-chain, allowing for fast transactions and payments without recording each transaction on the blockchain. This can greatly increase transaction speed and reduce transaction fees. The contract can integrate the Lightning Network payment function, allowing users to use the Lightning Network to pay for fragmented NFT assets. This way, when users buy or exchange shards, real-time, low-cost payments can be made through the Lightning Network. The Lightning Network uses multi-signature-based payment channels to ensure the security and reliability of payments. Contracts can use these security mechanisms to ensure that the payment process of fragmented NFT assets is trustworthy and safe. When a transaction is completed or the payment channel is no longer needed, the contract can settle and close the payment channel through integration with the Lightning Network. This will ensure the correct allocation of funds and the proper closing of payment channels.

3. Blockchain interaction:

Utilize blockchain interaction protocols (such as Ethereum’s Web3.js library) to interact with smart contracts. In this way, communication and data transmission with smart contracts can be achieved to submit fragmented NFT assets and perform merge operations. Interact with smart contracts through blockchain interaction protocols, such as Ethereum's Web3.js library, and implement communication and data transmission with the contract to submit fragmented NFT assets and perform merge operations. At the same time, if you want to join the Bitcoin Lightning Network, use the corresponding Bitcoin Lightning Network library to interact with the Lightning Network.

Here is an example showing how to use Web3.js to interact with smart contracts and integrate with the Bitcoin Lightning Network:

Interact with smart contracts using Web3.js:

- First, users need to configure the Web3.js library to connect to the Ethereum network and communicate with smart contracts.

- Users can then use the methods provided by Web3.js to call the functions of the smart contract to submit fragmented NFT assets and perform merge operations. This can include calling the contract's receive fragmented NFT asset fragment function, merge fragment function, etc.

4. Integrate Bitcoin Lightning Network:

- In order to integrate with the Bitcoin Lightning Network, users need to use an appropriate Bitcoin Lightning Network library, such as LND (Lightning Network Daemon) or c-lightning. Through blockchain interaction protocols (such as Ethereum's Web3.js library), users can interact with smart contracts and implement communication and data transmission with the contract to submit fragmented NFT assets and perform merge operations. At the same time, if users want to join the Bitcoin Lightning Network, they can use the corresponding Bitcoin Lightning Network library to interact with the Lightning Network. Shows how to use Web3.js to interact with smart contracts and integrate with the Bitcoin Lightning Network: Interacting with smart contracts using Web3.js: The Web3.js library needs to be configured to connect to the Ethereum network and communicate with smart contracts. You can use the methods provided by Web3.js to call the functions of the smart contract to submit fragmented NFT assets and perform merge operations. This can include calling the contract's receive fragmented NFT asset fragment function, merge fragment function, etc. In order to integrate with the Bitcoin Lightning Network, an appropriate Bitcoin Lightning Network library needs to be used, such as Lightning Network Daemon or c-lightning. Use the API provided by this library to create and manage payment channels for the Bitcoin Lightning Network and make Lightning Network payments. In the smart contract, Web3.js is used to communicate with the Bitcoin Lightning Network library to perform payment operations for fragmented NFT assets. This could include using the Bitcoin Lightning Network for payments when shards are merged, and ensuring the security and reliability of payments.

Fragment verification and merging process:

When dealing with fragmented NFT assets, here are more details on the fragment verification and merging process:

Fragment verification:

Validity verification of fragments: Before merging, the validity of each fragment needs to be verified to ensure that only legal fragments can be merged. This can be accomplished by checking the fragment's digital signature, hash value, or other verification mechanism. Contracts can use corresponding verification algorithms to verify the integrity and authenticity of fragments. Integrity verification of fragments: In addition to verifying the validity of fragments, it is also necessary to verify the integrity of fragments. This means making sure there aren't any missing or damaged pieces. The integrity of a fragment can be verified by comparing its location information with the total number of fragments. Fragment location recording: During the merging process, the location information of each fragment needs to be recorded so that the fragments can be positioned and assembled correctly. This can be achieved by storing the location information of the shards in the state variables of the smart contract. For example, you can use an array or map to store location information for each fragment.

Merge Process: Merge Rules and Conditions: During the merge process, merge rules and conditions need to be defined to determine when a merge operation can occur. This can include specifying the minimum number of shards required for a merge, ordering requirements for specific shards, etc. According to the rules and conditions, the merge operation can only be carried out if the requirements are met.

Merging algorithm and processing: The merging process can be a simple assembly operation, combining the fragments into a complete NFT asset in a specific order. In addition, the merging process can also be calculated and processed according to specific algorithms, such as calculation based on the attributes of the fragments, application of encryption algorithms, etc. The combined complete NFT asset can be created and recorded through the issuance function of the smart contract. By conducting fragment verification and merging processes, users can assemble fragmented NFT assets into a complete NFT, which is recorded and managed in smart contracts. In this way, users can obtain ownership of fragmented assets by purchasing or exchanging this complete NFT.

User interface and interaction: Design a user-friendly interface and interaction method to enable users to conveniently submit fragmented NFT assets and perform merge operations. This can be a web application or mobile application that provides easy-to-use forms and buttons to upload fragments and perform merge operations.

Privacy and security, operational interactivity

Bitcoin uses public and private key encryption algorithms to ensure the security and privacy of transactions. Every Bitcoin user has a public and private key pair associated with their Bitcoin address. A private key is a user's personal key used to sign transactions and prove ownership. The public key is the public address generated from the private key and is used to receive coins and verify transactions. This encryption algorithm ensures that only the holder of the private key can sign and operate the transaction, thus protecting the security and privacy of the transaction. Public and private key encryption: Bitcoin uses public and private key encryption algorithms to ensure the security and privacy of transactions. Every Bitcoin user has a public and private key pair associated with their Bitcoin address. A private key is a user's personal key used to sign transactions and prove ownership. The public key is the public address generated from the private key and is used to receive coins and verify transactions. This encryption algorithm ensures that only the holder of the private key can sign and operate the transaction, thus protecting the security and privacy of the transaction.

Anonymity of Bitcoin addresses: Bitcoin addresses are generated from public keys rather than identifiers directly linked to the user's identity information. This makes Bitcoin transactions somewhat anonymous, as transactions cannot be directly linked to a specific personal identity. However, it is important to note that by analyzing transaction patterns and other metadata, it may be possible to infer information associated with a specific address.

Mechanism to prevent tampering: Bitcoin's blockchain is a public ledger that cannot be tampered with. Each block contains the hash value of the previous block, forming a chain of linked blocks. This hash chaining mechanism ensures the integrity and security of the blockchain, as any tampering with the data of one block will cause the hash value of that block and all subsequent blocks to change. In addition, Bitcoin's consensus algorithm (such as proof of work) and distributed node network further enhance Bitcoin's security, making it very difficult to attack and tamper with Bitcoin's blockchain.

The following is a comparison table about the development of Ordinals NFT and traditional NFT:

Features	Bitcoin inscription	Traditional NFT
Deployment chain	BTC is the main POW public chain	ETH is the main POS public chain
Technical features	The inscription cannot be tampered with	Smart Contracts - Hardly Modifiable
Quantity	Limited, more rare	unlimited
Worry	Lightning Network Might Just Be a Temporary Solution	Public chain specificity issue
Create	Relatively complex and requires specific protocols or tools	Relatively simple, using smart contracts
Trade	Through specific protocols or tools	Direct access to smart contracts and markets
Storage	Pure on-chain storage requires specific tools	Use external storage such as IPFS
Development and customization	Limited, requires specific tools and Lightning protocol	Flexible, using programming languages like Solidity

Solutions based on decentralized exchanges typically involve depositing Bitcoin into the exchange's wallet and conducting fault-tolerant transactions within the exchange. This approach increases transaction speed and reduces transaction fees. To further combine

the Lightning Network to solve the problem of Bitcoin inscription, the following steps can be taken: Users deposit Bitcoin into a Lightning Network wallet on a centralized exchange. These wallets support the creation and management of Lightning Network channels. Users open Lightning Network channels and make payments within the exchange. These payments are made within the exchange, allowing for fast, low-cost transactions. Users can close Lightning Network channels within the exchange. When a user wishes to withdraw Bitcoin to their blockchain wallet, they can choose to close the Lightning Network channel and withdraw the Bitcoin to their blockchain address.

pay

BitTrust is a platform that provides directional domain name pointing services to the Bitcoin community, aiming to simplify the management and use of Bitcoin inscription transaction addresses for users.

On the BitTrust platform, combining with the Lightning Network can provide a faster and lower-cost transaction experience. Users can choose to associate a domain name with a Lightning Network channel when registering it. This way, when someone wants to send funds to a user, they can pay by entering the registered domain name instead of having to enter a complicated Bitcoin address. The specific steps are as follows:

1. Users can deposit Bitcoin into a Lightning Network wallet associated with a domain name. These wallets support the creation and management of Lightning Network channels.

2 When someone wants to send funds to a user, they can pay using the registered domain name. Payments will be made via Lightning Network channels, thus enabling fast, low-cost transactions.

3 Users can choose to close Lightning Network channels at any time and withdraw Bitcoins to their blockchain address. This can be done by managing the relevant settings on the BitTrust platform.

By integrating the Lightning Network into the BitTrust platform, users can enjoy a faster, lower-cost transaction experience while still maintaining domain resolvability and user-friendliness.

trade

As a Lightning Network supporter, BitTrust understands your concern for transaction convenience. In addition to using Bitcoin for payment, BitTrust also recognizes that decentralized exchanges under the Lightning Network can provide users with the same convenient trading experience.

The Lightning Network is a second-layer scaling solution designed to increase Bitcoin's scalability and transaction speed. It enables fast, low-cost transactions by establishing payment channels outside of the blockchain. Decentralized exchanges are platforms built on the Lightning Network that allow users to trade in a decentralized manner.

Trading on a decentralized exchange has the following advantages:

1. Transaction Speed: Decentralized exchanges leverage the lightning network's fast transaction characteristics, allowing users to complete transactions at nearly instantaneous speeds. This means you can buy and sell faster and get faster transaction confirmations compared to traditional centralized exchanges.

2. Low Cost: Decentralized exchanges typically have low transaction fees due to the low-cost nature of the Lightning Network. You can trade in a more economical way and save some money.

3. User Control: Decentralized exchanges allow users to directly control their funds without having to store them in the exchange's wallet. This means you have greater control over your assets and reduces the risk of an exchange being hacked or malfunctioning.

4. Decentralized characteristics: Decentralized exchanges are based on blockchain technology and have decentralized characteristics. This means that the exchange does not rely on a single central institution, but is jointly maintained and managed by multiple nodes in the network. This provides greater security and censorship resistance.

Decentralized exchanges can provide users with a convenient trading experience similar to centralized exchanges under the Lightning Network, while retaining the advantages of decentralization. They combine the speed and low-cost features of the Lightning Network with the security and user control of decentralized transactions. BitTrust will continue to pay attention to and support the development of decentralized exchanges and provide users with integrations with these platforms so that they can obtain a more convenient trading experience when using BitTrust's domain name services.

Chapter 7 Incentive Mechanism

Bitcoin Inscription’s incentive mechanism has some similarities to Bitcoin’s incentive mechanism. The following is a discussion about the incentive mechanism of Bitcoin Inscription:

1. Creation fee: In Bitcoin Inscription, creation usually requires payment of a certain fee. This fee can be used to pay transaction fees to incentivize verification nodes to verify and record transactions. The size of the fee can vary based on network congestion and how much the user is willing to pay.

2. Transaction fees: Similar to creation, transactions also require certain fees. This fee is intended to incentivize validator nodes to verify and record transactions. Similar to Bitcoin transactions, the size of transaction fees depends on network congestion and how much users are willing to pay.

3. Incentive verification nodes: The incentive mechanism of Bitcoin Inscription also involves verification nodes. Validation nodes are responsible for validating and recording transactions and maintaining the Bitcoin Inscription blockchain. These verification nodes compete to create new blocks by participating in consensus algorithms (such as proof of work) and receive corresponding rewards.

4. Reward mechanism for participants: Users participating in the Bitcoin Inscription ecosystem can receive rewards in different ways. For example, if a user creates a popular piece, they can earn money from sales. In addition, users can earn rewards by participating in community activities, providing technical support, or participating in the development and promotion of Inscriptions.

It should be noted that the specific Bitcoin Inscription incentive mechanism may vary depending on the platform and protocol. Different platforms and protocols may adopt

different fee structures, verification node reward mechanisms, and participant reward mechanisms. Therefore, when participating in Bitcoin Inscription, users should understand and abide by the rules and mechanisms of the corresponding platform and protocol.

In addition, Bitcoin Inscription’s incentive mechanism is also constantly developing and innovating. Over time, new mechanisms and models may emerge to provide better incentives and rewards, as well as a better participation experience.

Chapter 8 Community Governance

Bitcoin’s Lightning community governance model is a decentralized model designed to facilitate the process of developer collaboration, upgrade decisions, and network improvements. The following is a general overview of Bitcoin’s community governance model:

1. Developer collaboration: Bitcoin’s developer community is an open and diverse community composed of developers from around the world. Developers communicate and collaborate through mailing lists, social media, developer forums, and more. This open collaboration model allows anyone to participate in the development and improvement of Bitcoin.

2. Upgrade decision: Bitcoin’s upgrade decision is a complex process that involves extensive discussion and consensus. In the Bitcoin community, upgrade proposals are proposed by developers or other community members and are subject to extensive review and discussion. Community members can provide input, provide technical analysis and testing, and debate the strengths and weaknesses of proposals. Ultimately, upgrade decisions are typically made by consensus rather than by a centralized entity or individual.

3. Network improvement process: Bitcoin network improvements are usually carried out in the form of BIP (Bitcoin Improvement Proposal). BIP is a standardized proposal format used to describe and discuss improvements to Bitcoin. BIP can propose new features, fix bugs, improve performance, etc. Once a BIP is proposed, community members can review, discuss, and test it. If BIP is widely supported, it could be accepted and implemented into Bitcoin's protocol.

4. Landing page for a decentralized exchange solution: When designing a landing page for a decentralized exchange solution, here are some key elements and suggestions to help the platform effectively communicate its message and capture the interest of visitors: The platform emphasizes core benefits: Prominence This solution has core advantages over traditional centralized exchanges, such as faster transaction speed, low cost, and user control over funds, etc. Use concise and clear language and a catchy title to pique your visitors’ interest and let them quickly understand why they should choose decentralized exchanges. Provide a clear interface display so that visitors can understand how the user interface of the decentralized trading solution works. Diagrams, screenshots, or demo videos can be used to demonstrate transaction processes and operational interfaces. Highlight the solution's security and privacy measures. Explain how to ensure the security of user funds through blockchain

technology and cryptography, and emphasize the importance of users mastering their own private keys and funds. Highlight the premium user experience and convenience provided by the solution. Explain how to enable fast, low-cost transactions through the Lightning Network or other technologies, and provide a seamless user interface and operation process. Introducing the community support and ecosystem this decentralized trading solution relies on. Describe whether there is a developer community, technical support and partner network, and other ecosystems relevant to the solution. Provide a clear sign-up or download entry point on your landing page so visitors can start using the solution immediately. Make sure the registration or download process is simple and clear, and provide necessary guidance and assistance. Display trust and security-related logos such as security certificates, user reviews, or partner logos at the bottom of the page or in other appropriate locations. This will help increase visitor trust and reliability in the solution. Provide clear contact and support channels so visitors can get help or advice. This can include email addresses, live chat support, or social media links. Make sure your landing page has a responsive design that adapts to different devices and screen sizes. This will ensure that your visitors have a great browsing experience whether they are on a desktop, tablet or mobile device.

Chapter 9 Global Development Roadmap

Phase One: Technology R&D and Product Verification

- Establish a core team in New York State, including blockchain developers, cryptography experts and business development experts.

- Conduct market research and competitive analysis to determine the positioning and competitive advantages of the company's products in the local market in New York State.

- Carry out research and development of lightning technology solutions, establish a core technical team, and conduct prototype development and testing.

- Conduct internal testing and validation to ensure product performance and scalability.

- Seeking local early-stage investments and partners in New York State to support the company's growth and expansion.

Phase Two: Product Launch and Marketing

- Improve the functionality of Lightning Technology Solutions and make improvements and optimizations based on feedback from New York State users.

- Conduct local marketing activities in New York State, including attending the New York State Blockchain Summit, hosting seminars and social media promotions.

- Establish cooperative relationships with local businesses and partners in New York State to expand user and customer base.

- Provide local user training and support in New York State to ensure that users can fully understand and use the company's lightning technology solutions.

- Collect local user feedback and data in New York State to continuously improve products and services and improve user satisfaction.

The third stage: ecosystem construction and partner expansion

- Promote the construction of the ecosystem in New York State and attract local developers and partners in New York State to join the company's ecosystem.

- Provide developer tools and resources to facilitate the development and integration of third-party applications native to New York State.

- Cooperate with local industry organizations and standards-setting bodies in New York State to promote the development and adoption of local blockchain industry standards in New York State.

- Seeking local strategic partners in New York State to expand the company's influence and scope of cooperation in different local industries and markets in New York State.

- Promote local community governance and participation in New York State and promote the participation and contributions of local users and community members in New York State.

Phase Four: Innovation and Expansion

- Continue to carry out technological innovation of lightning technology solutions and explore new blockchain application scenarios and solutions.

- Expand product lines and launch new products and services based on lightning technology to meet the needs of different local industries and users in New York State.

- Expand the local market in New York State, establish cooperative relationships with local enterprises in New York State, and enter the international market.

- Strengthen the R&D team and talent pool to maintain technological leadership.

- Continuously improve corporate governance and operations to ensure the company's sustainable development and growth in New York State.

Chapter 10 Literature Search and Note Sources

[1] D. J. Abraham, A. Blum, and T. Sandholm. "Clearing algorithms for barter exchange markets: Enabling nationwide kidney exchanges." In Proceedings of the 8th ACM Conference on Electronic Commerce, EC '07, pages 295–304, New York, NY, USA, 2007. ACM.

[2] J. Bang-Jensen and G. Gutin. "Digraphs: Theory, Algorithms, and Applications." Monographs in Mathematics. Springer, 2001.

[3] A. Becker and D. Geiger. "Optimization of Pearl's method of conditioning and greedy-like approximation algorithms for the vertex feedback set problem." Artificial Intelligence, 83(1):167–188, 1996.

[4] bitcoinwiki. "Atomic cross-chain trading." https://en.bitcoin.it/wiki/Atomic cross-chain trading. As of 9 January 2018.

[5] bitcoinwiki. "Hashed timelock contracts." https://en.bitcoin.it/wiki/Hashed Timelock Contracts. As of 8 January 2018.

[6] S. Bowe and D. Hopwood. "Hashed time-locked contract transactions." https://github.com/bitcoin/bips/blob/master/bip-0199.mediawiki. As of 9 January 2018.

[7] V. Buterin. "On sharding blockchains." https://github.com/ethereum/wiki/wiki/Sharding-FAQ. As of 8 January 2018.

[8] C. Decker and R. Wattenhofer. "A fast and scalable payment network with bitcoin duplex micropayment channels." In A. Pelc and A. A. Schwarzmann, editors,

Stabilization, Safety, and Security of Distributed Systems, pages 3–18, Cham, 2015. Springer International Publishing.

[9] DeCred. "Decred cross-chain atomic swapping." https://github.com/decred/atomicswap. As of 8 January 2018.

[10] J. P. Dickerson, D. F. Manlove, B. Plaut, T. Sandholm, and J. Trimble. "Position-indexed formulations for kidney exchange." CoRR, abs/1606.01623, 2016.

[11] M. K. Franklin and G. Tsudik. "Secure group barter: Multi-party fair exchange with semi-trusted neutral parties." In Financial Cryptography, 1998.

[12] M. Green and I. Miers. "Bolt: Anonymous payment channels for decentralized currencies." Cryptology ePrint Archive, Report 2016/701, 2016. https://eprint.iacr.org/2016/701.

[13] Z. Jia, P. Tang, R. Wang, and H. Zhang. "Efficient near-optimal algorithms for barter exchange." In Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems, AAMAS '17, pages 362–370, Richland, SC, 2017. International Foundation for Autonomous Agents and Multiagent Systems.

[14] R. M. Kaplan. "An improved algorithm for multi-way trading for exchange and barter." Electronic Commerce Research and Applications, 10(1):67–74, 2011. Special Section: Service Innovation in E-Commerce.

[15] R. M. Karp. "Reducibility among combinatorial problems." In Proceedings of a symposium on the Complexity of Computer Computations, held March 20-22, 1972, at the IBM Thomas J. Watson Research