SAT20 Protocol WhitePaper

SAT20 Protocol

Overview

SAT20 is a "**Satoshi Standard**" protocol for issuing and circulating BTC native assets, with its core feature being the binding of assets to satoshis and their free movement alongside satoshis. SatoshiNet is the native extension network of the BTC mainnet, based on Lightning channels and parallel BTC networks. Its purpose is to expand the liquidity of BTC's native assets. SatoshiNet is the implementation of the SAT20 protocol.

SatoshiNet

SatoshiNet is the native extension network of the BTC mainnet, built on Lightning channels and parallel BTC networks, providing a secure, fast, and cost-effective native circulation environment for BTC and the mainnet's native assets. SatoshiNet is an implementation example of the SAT20 protocol, constructed based on it.

Key Features of SatoshiNet:

1. **Native second-layer** extension network for BTC
2. **No bridge**: based on Lightning channels
3. **No new tokens**: all assets come from the BTC mainnet
4. **Same consensus**: same addresses, same network fees, same assets
5. Fast block times, low fees
6. Supports smart contracts

Asset Circulation Protocol (STP)

The SAT20 Asset Circulation Protocol, also known as the Satoshi Transcending Protocol (STP), is a protocol based on Lightning Network channels that defines the rules for the circulation of Satoshi assets.

Features of the Satoshi Transcending Protocol:

1. **BTC Native**: Inherits the Lightning Channel RSMC protocol, with asset security ensured by the BTC mainnet, giving users full control.
2. **Full Asset Support**: Supports native asset protocols on the BTC mainnet, such as Ordinals, Runes, BRC20, ORDX, and more.
3. **Dynamic Lightning Channel Technology**
4. **Simple Atomic Interface**:
    - Open and close channels
    - Lock and unlock assets
    - Splicing
    - Satoshi Swap
5. **Compatibility with Other Public Chains**

Asset Issuance Protocol (ORDX)

The SAT20 asset issuance protocol is an enhanced version of the Ordinals protocol. It is used to issue assets called SAT20 assets. These assets are bound to satoshis and inherit the properties of satoshis:

1. Satoshis are not destructible, so the assets are also non-destructible.
2. The data bound to satoshis is immutable, so once the assets are issued, they cannot be modified.
3. Wherever the satoshis are, the assets are also present, allowing assets to freely move across different networks alongside satoshis.
4. Assets belong to the owner of the satoshis, so when satoshis are transferred, the assets are transferred as well.
5. The non-fungible nature of satoshis determines the non-fungibility of assets, making them inherently SFT (Semi-Fungible Token) assets.
6. Satoshis can be bound to any data, including smart contracts, enabling assets to have a certain level of intelligence.

Vision

One sat, one world.

Everyone can enjoy the benefits of the BTC network.

Background

The term "satoshi" as the basic unit of BTC carries profound significance from its inception. If the BTC ecosystem truly represents the development trend of BTC, then an asset issuance and circulation protocol based on "sat" is an inevitable outcome that will emerge sooner or later within the BTC ecosystem.

First and foremost, SAT assets are the most natural way of issuing native assets on the BTC network without any adverse effects. During the minting phase, assets only require the inclusion of simple data on the BTC network. Subsequently, whether they are transferred or enter the second layer networks, no additional data needs to be written, ensuring no disruption to the mainnet. From another perspective, sats are users' assets, and SAT assets, through their association with sats, naturally belong to the users, with their security guaranteed by the mainnet. Therefore, SAT assets are the most natural and native form of asset issuance within the BTC ecosystem, regardless of how they are examined

.

Secondly, Sats-based assets are inherently aligned with BTC's technological evolution. No matter how BTC's technology develops or what second-layer networks emerge in the future, Sats-based assets will inevitably be part of that ecosystem, requiring no permission or additional operations. Sats assets will flow freely alongside the movement of Sats themselves into these networks. If BTC's first-layer smart contracts, such as BitVM, are successfully implemented, Sats-based assets can seamlessly interact with BitVM without any changes.

Finally, even if BTC doesn't yet have a native extension network, exploring and implementing a native BTC extension network that enables the free flow of Sats and fully unlocks their value is the mission of SAT20. Driven by this mission, we've created an extension network like the

SatoshiNet.

In conclusion, the SAT20 Sats Asset Protocol is an inevitable product of the BTC ecosystem's evolution. It represents the potential of the smallest unit of BTC, Satoshi, and highlights the uniqueness of BTC-based assets. As BTC technology progresses, the value of Sats will increasingly be recognized and fully utilized.

SatoshiNet

Overview

SatoshiNet is the native second-layer extension network of BTC, composed of Lightning Network channels (RSMC protocol) and a parallel BTC network.

SatoshiNet is native and based on the following core technologies:

1. **Assets are all from Layer 1**: SatoshiNet does not issue its own assets. All assets on SatoshiNet are derived from the BTC mainnet.
2. **Assets are secured by the BTC mainnet**: All assets on SatoshiNet are actually stored in Lightning channels, and the security of these channels is guaranteed by the BTC mainnet.
3. **Users retain control**: At any time, even if SatoshiNet shuts down, users can retrieve their assets without the need for any third-party involvement.
4. **Same consensus**: Same addresses, same assets, same network fees.

SatoshiNet represents a **new direction of evolution for the Lightning Network**. Unlike the original Lightning Network, which evolves into a network architecture using a combination of RSMC + HTLC protocols, SatoshiNet retains the RSMC protocol while abandoning HTLC. This allows the Lightning channel's full potential to be unlocked, transforming it into a bridge between Layer 1 and Layer 2 networks. At the same time, a parallel BTC network is used as

the second-layer network to record the transaction states of Lightning channels. This ensures that changes in Lightning channel states are traceable, auditable, and immutable as UTXO ledger records. Additionally, by activating OP_CAT and potentially more opcodes, SatoshiNet can evolve into a network supporting Turing-complete smart contracts. In this way, SatoshiNet allows the BTC ecosystem to compete with the ETH ecosystem.

SatoshiNet is developed on top of the BTC core code, and compared to the BTC mainnet, it mainly differs in the following aspects:

1. **Consensus Mechanism**: Proof of Stake (POS)
2. **Block Time**: 12 seconds
3. **Transaction Network Fees**: 10 satoshis
4. **Enhanced UTXO Model**: Supports explicit expression of any asset
5. **Supports Turing-complete Smart Contracts**: Activates OP_CAT and other instructions, turning Bitcoin scripts into Turing-complete scripts

SatoshiNet is also constantly evolving. All technologies that cannot be implemented on the mainnet can be realized on SatoshiNet. One day, it will even be able to connect to all other public chains through SatoshiNet, making the BTC mainnet truly the foundation of the value Internet.

SatoshiNet is also the ultimate goal of the SAT20 protocol, providing a secure, fast, and cost-effective native circulation environment for BTC and the native assets on the mainnet. SatoshiNet opens up entirely new possibilities for the development of the BTC ecosystem.

Native

The BTC mainnet does not support Turing-complete smart contracts, due to concerns over the risks that activating OP_CAT could introduce, which are perceived to far outweigh any potential benefits. This makes it virtually impossible to activate OP_CAT on the BTC mainnet. As a result, the development trajectory of the BTC ecosystem is fundamentally different from that of the ETH ecosystem.

ETH has Turing-complete smart contracts, which allows the Layer 1 network to verify transaction data from Layer 2 networks. This makes it possible for the assets and transactions on ETH's Layer 2 networks to have their security ensured by the Layer 1 mainnet. However, this possibility does not exist in the BTC ecosystem. Simply put, the BTC mainnet is a "walled garden" that cannot accept external transaction or asset data. In other words, BTC's assets can only exist and be settled on the mainnet. Any asset or network that operates outside the mainnet for settlement is not considered part of BTC's native Layer 2 ecosystem. By this standard, the only truly native Layer 2 network for BTC is the Lightning Network.

However, the traditional Lightning Network does not support the native assets currently found on the BTC mainnet, such as Ordinals NFTs, BRC20 tokens, Runes, and others. This renders the Lightning Network as a native second-layer extension somewhat misnamed.

SatoshiNet represents an evolution of the traditional Lightning Network in a new direction. The traditional Lightning Network operates with a combination of RSMC + HTLC protocols, while SatoshiNet abandons HTLC in favor of RSMC + a parallel BTC network, creating a new generation of the Lightning Network. Compared to the traditional Lightning Network, SatoshiNet offers several advantages:

1. **Dynamic Lightning Channels**: Traditional Lightning channels are represented by a single UTXO, whereas the SatoshiNet Lightning channels use a set of UTXOs. These can be dynamically adjusted with splicing techniques to increase or decrease UTXOs or adjust the capacity of individual UTXOs.
2. **Supports BTC Native Assets**: While the traditional Lightning Network does not support mainstream asset issuance protocols on the BTC mainnet, such as Ordinals, ORDX, BRC20, and Runes, SatoshiNet supports all of these protocols.
3. **Lightweight Design**: Current popular Lightning Network versions, like LND, lack a lightweight version and cannot be compiled into WASM modules to run in browsers. However, SatoshiNet's Lightning channel modules can be compiled into WASM, allowing them to run in web browsers.

Beyond these differences, SatoshiNet's Lightning Network module fully inherits the RSMC protocol, which is the backbone of Lightning Network channel security. This protocol ensures that users can always broadcast commitment transactions to reclaim their assets, and it enables the construction of penalty transactions to deal with malicious counterparty behavior. These mechanisms are also implemented in SatoshiNet, ensuring the security of users' assets.

Moreover, SatoshiNet's features stem from its natural extension of the BTC mainnet:

1. **SatoshiNet's assets come from the mainnet**.
2. **SatoshiNet's addresses match those of the mainnet**, providing users with a seamless experience.
3. **SatoshiNet's network fees are paid in BTC**.
4. **SatoshiNet uses the same UTXO model**, as its code is derived from the BTC source code.

In conclusion, by inheriting the native characteristics of Lightning channels and maintaining consistency with the parallel BTC network, SatoshiNet is a truly native BTC extension network.

Safe

The security of SatoshiNet is ensured through the following mechanisms:

1. **Lightning channels based on RSMC contracts**: These are native extensions of the BTC mainnet and share the security of the BTC mainnet. This is the most fundamental aspect of security.
2. **SatoshiNet based on BTCD source code**: The security at the technical level is provided by BTC technology, ensuring the prevention of double-spending of assets.
3. **Assets and sats all from mainnet**: Every satoshi and asset on SatoshiNet originates from the BTC mainnet, providing asset-level security and preventing the creation or destruction of assets.
4. **Proof of Stake (POS) mechanism on SatoshiNet**: Economically ensures that there is

no incentive for malicious behavior among SatoshiNet nodes.

Ultimately, SatoshiNet combines these factors to ensure a robust and rock-solid security model. This security is based on the technology and consensus of the BTC mainnet. As long as the BTC mainnet's technology and consensus remain intact, every satoshi on SatoshiNet remains under the control of the user, and no one can take them away.

POS

SatoshiNet adopts a POS mechanism similar to the one used in the ETH network. Miners obtain mining qualifications by staking Pearl and are guided and supported in the development and growth of SatoshiNet by a non-profit foundation.

The BTC mainnet is already highly secure, and all assets on SatoshiNet originate from the mainnet, locked in Lightning channels with user control. Therefore, the decentralization requirements for SatoshiNet are not as stringent. By leveraging ETH's experience to build a POS consensus network, SatoshiNet can achieve an adequate level of decentralization while also addressing BTC mainnet's key shortcoming—efficiency. Moreover, due to the POS mechanism, SatoshiNet has minimal hardware requirements, further lowering the cost of maintaining the network and, in turn, reducing transaction network fees.

In summary, the POS consensus in SatoshiNet perfectly complements the POW consensus of the BTC mainnet. Both consensus mechanisms play their respective roles, providing a secure, stable, efficient, and cost-effective foundation for the BTC ecosystem.

Enhanced UTXO

In the Layer 1 network, a UTXO (Unspent Transaction Output) only represents the amount of satoshis (sats) without including additional data. However, when sats traverse to the second-layer network, their properties are fully encapsulated within the UTXO, significantly enhancing its capabilities.

The **enUTXO** will contain both the amount of sats and the asset information, greatly facilitating the circulation of sats and the validation of assets on the SatoshiNet. This not only prevents double-spending but also enables the possibility of supporting any asset type on SatoshiNet. Additionally, it allows for a clear and intuitive view of an asset's transaction history, improving transparency and traceability within the ecosystem.

Smart Contract

SatoshiNet supports two types of smart contracts:

1. **Template Contracts**: Directly embedded in the SatoshiNet source code through OP instructions to hard-code a contract.
2. **Turing-complete On-chain Smart Contracts**: Activated via the OP_CAT instruction, enabling Turing-complete on-chain smart contracts.

Liquidity Pool

The liquidity pool is a key module for keeping operational costs low on SatoshiNet. It reduces the likelihood of fees skyrocketing due to the dynamic adjustments of channels. The SatoshiNet Foundation is responsible for building a public liquidity pool that provides the basic liquidity needed for the network.

Additionally, the liquidity pool can also be operated by third parties.

Fundation

The SatoshiNet Foundation is a non-profit organization focused on advancing the development and technological innovation of the SatoshiNet ecosystem. Its mission is to support the research and development, education, promotion, and infrastructure building of the SatoshiNet platform.

Responsibilities

1. **R&D of SatoshiNet Technology**: Develop and innovate the underlying technology of SatoshiNet.
2. **Infrastructure Development and Expansion**: Build and expand the network infrastructure to ensure scalability and efficiency.
3. **Funding Open-Source Projects**: Provide financial support for open-source projects based on the SatoshiNet platform.
4. **Education and Promotion**: Promote and educate about SatoshiNet to foster adoption and growth.

Sources of Income

1. **Donations**: Funds donated by supporters and enthusiasts of the SatoshiNet ecosystem.
2. **Revenue Share from Core SatoshiNet Operations**: Income from activities such as mining and liquidity pools.
3. **Participation in Core SatoshiNet Operations**: Revenue generated by the foundation's own involvement in mining or liquidity pool operations.

Organizational Structure

1. **Executive Board**: Oversees the overall direction and decision-making of the foundation.
2. **Technical Team**: Responsible for the development and technical operations of the SatoshiNet platform.
3. **Operations Team**: Handles day-to-day operations, community management, and business development.
4. **Community and Education Team**: Focuses on outreach, education, and community-building efforts.

Management Model

1. **Decentralized Decision-Making**: Decisions are made through a decentralized process to ensure the broad participation of the community and stakeholders.

2. **Transparency and Openness**: The foundation operates with full transparency, regularly publishing financial statements and updates.

Important Projects

- Ongoing and future initiatives will focus on advancing the core development of SatoshiNet, supporting community-driven projects, and enhancing the platform's reach.

Community and Culture

- Building a robust community around the SatoshiNet ecosystem, fostering collaboration, and cultivating a culture of innovation and openness.

Strategic Partnerships and Future Development

- The foundation will seek strategic partnerships to help expand the SatoshiNet ecosystem and ensure its long-term sustainability and success.

Note: The SatoshiNet Foundation is not led by SAT20Labs, nor is it a subsidiary of SAT20Labs. There is no hierarchical relationship between the two organizations. This document merely offers guidance on the development of the SatoshiNet Foundation.

Economic Model

The income sources of SatoshiNet are primarily divided into two parts: transaction packaging fees (network fees) and earnings from liquidity pool fund inflows and outflows. The SatoshiNet Foundation takes a commission from both income sources, starting at 20% in the early stages and gradually decreasing as the network develops.

1. Basic Assumptions

To better consider the revenue sources for both platform operators and liquidity pool participants, the following parameters are used:

- **Transaction packaging fee**: Fixed at 10 satoshis per transaction.
- **Daily transaction volume**:
    - **Guidance period**: Starting from zero and growing to 1,000 transactions per day, stabilizing the network and preparing for more projects to join.
    - **Development period**: Transaction volume grows from 1,000 to 100,000 transactions per day, with at least 10 active or large token projects joining.
    - **Mature period**: Transaction volume grows from 100,000 to 10 million transactions per day, with at least 100 active tokens traded.
    - **Explosive period**: Over 10 million transactions per day, with the most popular BTC ecosystem tokens being traded on SatoshiNet.

2. Mining Nodes

Mining nodes gain the right to mine by staking **Pearl** tokens.

- **Total network staking goal**: 50,000,000 Pearl (33% of total assets).
- **Mining node requirements**: The number of nodes required changes during each development phase.
- **Staking amount** is temporarily set at 1 million Pearl tokens.

Mining Revenue by Phase:

- **Guidance Period**: 3–5 nodes, no focus on economic profit.
- **Development Period**: 10–100 nodes. With daily transactions under 100,000, if there are 100 nodes, each node will mine 72 blocks per day. With 10 transactions per block, each block earns 100 satoshis, yielding daily earnings of 7,200 satoshis, and yearly earnings of about 0.02628 BTC ($2,628 USD).
- **Mature Period**: With 100 nodes, transaction volume increases by 10 times, resulting in annual earnings of $26,280 per node. At this stage, the required staking of Pearl might drop to 100,000 tokens.
- **Explosive Period**: In the ideal scenario, with 10 million transactions per day and 1,000

mining nodes each staking 100,000 Pearl tokens, liquidity is largely locked within the nodes. If the transaction volume can reach 100 million, the staking amount may drop to 10,000 Pearls.

3. Liquidity Pools

The liquidity pool provides the inflow and outflow of funds for SatoshiNet. The SatoshiNet Foundation manages two pools (BTC and Pearl). The funds required for these pools vary in different stages (exact calculations are not available yet). The revenue from these pools is controlled by the foundation, which is responsible for establishing and managing them. If funds come from third parties, the profits will be distributed according to the pool's fund share but will be subject to the foundation's commission.

4. Revenue Distribution Model

Principles:

- Those who provide services receive the profits.
- The foundation takes a percentage of the revenue for ecosystem development. The revenue share varies across different periods.
    - **Guidance Period**: No commission taken.
    - **Development Period**: 20% commission.
    - **Mature Period**: 10% commission.
    - **Explosive Period**: 1–5% commission, with a minimum guarantee of 1%.

Liquidity Pool Participant Earnings

- In the **Explosive Period**, with a daily transaction volume of 10 million transactions, 1% of the funds are expected to flow in and out of SatoshiNet. Funds entering the network are free of charge, but exiting the network incurs a service fee. The fixed service fee is 5,000 satoshis + 1% of the amount being withdrawn.
- Assuming an average of 10,000 transactions per day, each worth 1,000 USD (100,000 satoshis), a withdrawal transaction will incur 5,000 satoshis of fixed service fees + 10,000 satoshis of fund fees, totaling 15,000 satoshis. This generates a daily cost of

approximately 1.5 BTC.

- At this stage, with a liquidity pool size of 1,000 BTC, the annual revenue could be 182.5 BTC ($18.2 million), with an annual yield of **18.2%**. If a participant stakes $10,000, their annual earnings would be approximately **$1,820**.

Mining Node Earnings

- Mining nodes must pay a portion of their earnings to the foundation, up to 20%. Additionally, regular mining nodes need to pay core nodes a data service fee, up to 10%.
- The remaining earnings belong to the node operators themselves.

Explosive Period Example (10 million daily transactions and 1,000 nodes):

- **Revenue per node**: 10,000 transactions per day × 10 satoshis per transaction = 100,000 satoshis/day.
- **Annual earnings per node**: 100,000 satoshis/day × 365 = 0.365 BTC/year ($36,500).
    - Foundation share (5%) = $1,825.
    - Core node share (10%) = $3,650.
    - Node operator share (85%) = $31,625.

Node Costs:

- In the mature period, staking 100,000 Pearl tokens might cost $100,000 USD.
- Hardware and network costs per node are expected to be less than $3,000 per year.

Node ROI:

- In the mature period, the return on investment for a mining node would be approximately **30%**.

5. Dynamic Adjustment Mechanism

To balance platform earnings and participant attractiveness while adapting to market development, the following dynamic adjustments can be implemented:

1. **Foundation's Revenue Share**: Starting at 20%, gradually decreasing to a stable range of 1–5%.
2. **SatoshiNet Network Fee**: Currently 10 satoshis, but it could decrease as BTC prices

rise and transaction volumes increase. The fee may eventually drop to 1 satoshi per transaction.

Note: This is a proposal and should be reviewed and approved by the foundation before implementation.

Continuous Evolution

SatoshiNet is a continuously evolving system. From the very first day of its inception, it has been a product of constant evolution. It represents the evolution of the Lightning Channel protocol in a new direction, distinct from the traditional Lightning Network. SatoshiNet also embodies the continuous progression of mainnet technologies, providing a platform for the realization and development of various ideas and technologies that have historically led to BTC network forks, such as larger blocks, additional OP codes, faster block processing speeds, and more.

SatoshiNet can improve block production speed. Once a block is filled, it can be immediately packaged without delay. This allows block production to reach the maximum capacity of network throughput and the limits of local computation and verification. With the support of modern computer hardware, transmitting and verifying 4MB of data per second is a straightforward task. From this perspective, the network could easily handle 10,000 transactions per second or even more.

SatoshiNet can also plan for block size expansion if needed. As long as the network and hardware can keep up, blocks of 16MB or even larger are feasible.

SatoshiNet has the potential to activate various OP codes to enable Turing-complete smart contracts. This capability would pave the way for developing a native Layer 3 network or establishing connections to other blockchains. As a result, SatoshiNet would become a

mediator network connecting the BTC mainnet to external networks, enabling BTC to flow freely across all ecosystems and unleashing the full potential of BTC and native mainnet assets. The possibilities for innovation on SatoshiNet extend even further, particularly in applications and services built on the network. For example, SatoshiNet naturally supports BTC mainnet-based DID (Decentralized Identity). If it also adds a DA service, it could unlock limitless potential for imagination, allowing everyone to innovate and create in ways yet to be explored.

Note: From a technical perspective, since SatoshiNet can serve as a native extension of the BTC mainnet, the same protocol could theoretically be applied to the ETH network. As long as the ETH network supports the interfaces of the Satoshi Transcending Protocol (STP), ETH could connect to the BTC mainnet via STP and Lightning Channels. This would allow BTC and BTC-native assets to flow into the ETH network. Alternatively, instead of connecting directly, would it be simpler to connect through SatoshiNet? This approach could also provide a level of buffering.

Additionally, could the reverse direction work? For example, enabling ETH to flow into the BTC mainnet for circulation?

Scenarios

SATSWAP

The Satoshi Swap Market is the first application on SatoshiNet, providing an efficient platform for exchanging assets within the network.

Stablecoin

On SatoshiNet, stablecoins not only serve their typical function but, to some extent, also help mitigate the high cost of adjusting the capacity of lightning channels.

Micropayment

SatoshiNet's low transaction fees make it naturally suitable for the development of various

micropayment applications, such as AI-based services.

DePIN

Many old smartphones from 7-8 years ago are equipped with quad-core CPUs, over 2GB of RAM, and at least 16GB of storage. These phones are capable of functioning as lightweight nodes, providing some computation and storage services. Additionally, these old phones consume very little power. If a large number of such devices are connected together, they could form a network with significant economies of scale.

Interestingly, SAT20 assets are solely tied to Satoshis, and while the quantity of Satoshis may be large, the storage and computation required to manage them are actually quite small. If each household uses an old smartphone as a lightweight node, it could form a decentralized indexing service network. This network would not only verify individual assets but also maintain the security of the entire network, provide storage and computational services, and distribute network data in a decentralized manner. Additionally, the network could perform tasks such as SVM execution, earning service fees in the process.

A decentralized BTC asset indexing service network built from old smartphones.

Asset Circulation Protocol: STP

Overview

The SAT20 Asset Circulation Protocol is a protocol that outlines how Satoshis (sats) can enter the BTC native Layer 2 network, how they can be traded and transferred within the Layer 2 network, and how they can be securely returned to the Layer 1 mainnet.

The SAT20 Asset Circulation Protocol is just a protocol and not a Layer 2 network itself. Currently, there is no existing Layer 2 network supported natively by BTC in the market. The BTC ecosystem needs a native Layer 2 network that allows BTC to freely circulate onto the Layer 2 network.

What is a BTC native Layer 2 network? We believe there is only one standard: complete user control. Users must have full control over the security of their assets without needing anyone's permission. They should be able to enter and exit the Layer 2 network at any time without compromising the security of their assets. The SAT20 Asset Circulation Protocol is designed to be compatible with all BTC native Layer 2 networks, whether existing or yet to emerge.

The core concepts of the SAT20 Asset Circulation Protocol include:

1. Sat Locking and Unlocking: Using Lightning Network channel technology, sats are locked on the mainnet. The battle-tested Lightning Network channel technology ensures the security of user assets.
2. Sat Transcending: Sats can transcend between Layer 1 and Layer 2, entirely controlled by the user.
3. Sat Swapping: Sats within the Layer 2 network gain remarkable liquidity through sat swapping.
4. RSMC: The core technology of the Lightning Network, ensuring that users have control over the assets in the channel.
5. Dynamic channel capacity adjustment technology: adjust the capacity of the lightning channel through Splicing technology.
6. Support mainstream asset issuance protocols on the mainnet: Ordinals, ORDX, Runes, BRC20, etc.

Protocol

The core of the STP is the Lightning Channel, and the main content of the protocol is to coordinate the flow of Satoshi assets between the Layer 1 and Layer 2 networks. The flow of assets essentially refers to the flow of asset ownership, as Satoshi and assets are locked on the mainnet, but the ownership is transferred to Layer 2 for circulation, ultimately needing to return to Layer 1 for final settlement.

The principle of the protocol is that the user is the initiator. Almost all actions must be initiated by the user, while the remote service node acts as an automated responder that complies

with the protocol and cooperates with the user's actions. This principle ensures that all operations reflect the user's intentions and maximizes the security of the user's funds.
Layer 1 is the mainnet, while Layer 2 can be any public chain supporting the Satoshi Transcending Protocol. In this example, we use the SatoshiNet.

Opening a Channel

This is the standard method of opening a Lightning Network channel. The user provides the funds to open the channel, and the remote service node automatically responds and assists in opening the channel. Once the channel is opened, according to the Lightning channel's RSMC protocol, the user holds the commitment transaction. This is the fundamental guarantee for the user's fund security. Even if the remote node does not respond, the user can broadcast the commitment transaction to reclaim their funds.

Likewise, the remote service node also holds the commitment transaction. Both parties are on equal footing.

At this point, the user can perform other actions to allocate ownership of the funds in the channel or adjust the channel's capacity. These actions will trigger updates to the commitment transaction. Both parties only hold the latest commitment transaction. If one party broadcasts an old commitment transaction, the other party can construct a corresponding penalty transaction to clear the output of the old commitment transaction, effectively sweeping all the funds in the channel to their address. This is the power granted to users by the RSMC protocol.

Another important function of the Satoshi Transcending Protocol is that, when opening a channel, the Satoshi assets in the channel are automatically Ascended to the SatoshiNet and corresponding UTXOs are generated on the SatoshiNet. This means the assets have transcended to the Layer 2 network.

Closing a Channel

The user can decide at any time to close the channel and reclaim their funds. There are two types of closure: negotiated closure and forced closure.

1. **Negotiated Closure**: Under normal circumstances, the remote node will be online and automatically support the user's closure request. The advantage of negotiated closure is that both parties can immediately spend their funds after the transaction is confirmed, with minimal fees.
2. **Forced Closure**: If the remote node is offline or permanently closed, the user can broadcast the latest commitment transaction to reclaim their funds. Unlike negotiated closure, the commitment transaction will first output the funds to an intermediate address, and the user will need to wait for a default CSVDelay (usually 144 blocks) before they can spend those outputs.

When executing the channel closure, the relevant assets on the Layer 2 network must perform a **Descend** operation, transferring the funds from Layer 2 back to Layer 1, ensuring that every Satoshi asset on the SatoshiNet is locked within the channel.

Unlocking and Locking

After opening the channel, the assets automatically transcend to Layer 2 but remain locked in the channel. It can be imagined that Layer 1 and Layer 2 are two reservoirs, and the channel connects these two reservoirs. The funds locked in the channel are in a critical state and need special operations to move them in or out of either network. The operations for entering or exiting Layer 2 are unlocking and locking, while operations for entering or exiting Layer 1 are splicing.

Unlocking and Locking are operations performed on Layer 2:

1. **Unlocking**: Release the funds from the channel to the user's address on the SatoshiNet. Afterward, the user can freely sign and use their assets, just like on the mainnet.

2. **Locking**: Lock the funds back into the channel. Note that the channel's capacity is fixed, so the unlocking and locking operations cannot change the channel's capacity. Whether or not the funds can be locked back into the channel depends on the channel's capacity.

Splicing

Splicing is a new protocol in the Lightning Network used to dynamically adjust channel capacity. However, the most widely used Lightning Network implementation, LND, has not yet implemented the splicing function. We use splicing technology to dynamically adjust the channel.

Splicing is an operation executed on Layer 1:

1. **Splicing-in**: Add a new UTXO to the Lightning channel, increasing the channel's capacity. This operation is equivalent to "recharging" the channel, allowing any asset to enter as long as the indexer supports it.
2. **Splicing-out**: Output funds from the Lightning channel by removing part of the UTXO to a specified address. This operation is equivalent to withdrawing assets from the channel.

Similarly, when performing splicing, since the effect is akin to depositing/withdrawing assets from Layer 2, the involved assets must automatically complete Ascend/Descend operations to ensure that the assets on Layer 2 match the assets in the channel.

The above outlines the core technology of the Satoshi Transcending Protocol, which is fully based on Lightning channels and represents another native extension protocol within the BTC ecosystem.

SatSwap

Satoshi can be swapped between different UTXOs, which is the core of Satoshi's super liquidity on the second-layer network.

Satoshi locking, transcending, and swapping are the core technologies that enable secure movement of satoshi assets from layer-1 to layer-2 and facilitate their free circulation within the BTC native layer-2 network. This technology ensures the security of user funds while allowing satoshis and their associated assets to freely flow within the network.

RSMC

In the Lightning Network, RSMC (Revocable Sequence Maturity Contract) is a contract type used to ensure the security and reliability of Lightning Network channels. RSMC is a time-locked contract that allows participants to revoke or close a Lightning Network channel under specific conditions. Its design aims to prevent fraudulent activities and malicious actions, ensuring the security of transactions.

Assets are locked within the channel, and users hold commitment transactions while having the ability to construct penalty transactions to secure their assets. At any time, users can reclaim their funds without needing permission from any third party.

Dynamic Channel

Traditional Lightning Network channels consist of a single UTXO, while the Lightning channels in the Satoshi Transcending Protocol (STP) are composed of a set of UTXOs. These UTXOs can be dynamically added or removed using splicing technology, or the capacity of a specific UTXO can be adjusted. It is even possible to manage an entire Lightning channel using a multi-signature address. This flexibility is essential for transferring assets from the main network to the second-layer network.

1. Multiple UTXOs
2. Arbitrary addition or removal of UTXOs
3. Arbitrary adjustment of UTXO size

Full Assets

The Satoshi Transcending Protocol (STP) supports the native asset issuance protocols on the main Bitcoin network, including Ordinals, ORDX, Runes, BRC20, and others. In fact, as long as the asset issuance protocol is based on the UTXO model, it can be supported by the STP and

traded on the SatoshiNet.

Compitable

The Satoshi Transcending Protocol (STP) is an independent protocol that enables assets on the BTC mainnet—whether BTC, Ordinals, Runes, BRC20, ORDX, or others—to traverse to another network under the complete control of the user. As long as the network supports the atomic interface of STP (public chains that are UTXO-based natively support it, and public chains with smart contracts and support for asset issuance and destruction also support it).

The ability of STP comes from the RSMC protocol of Lightning channels. If we consider the BTC mainnet as a reservoir and other public chains, like ETH, as another reservoir, the role of STP is to connect these two reservoirs with a pipe (via the Lightning channel) and control the flow of assets into and out of this pipe. This entire process can be fully controlled by the user.

Asset Issuance Protocol: ORDX

Overview

The SAT20 Asset Issuance Protocol is a protocol for issuing various types of digital assets on the BTC mainnet. Its core is the **binding of satoshis**, hence the name "Sat Asset" (SAT20 ASSETS). Sat Assets have distinctive characteristics and are the world's first "**satoshi standard**" native BTC asset issuance protocol, where assets possess the properties of satoshis.

Basic Properties of SAT20 Assets

1. Satoshis are not destructible, so the assets are also non-destructible.
2. The data bound to satoshis is immutable, so once the assets are issued, they cannot be modified.
3. Wherever the satoshis are, the assets are also present, allowing assets to freely move across different networks alongside satoshis.
4. Assets belong to the owner of the satoshis, so when satoshis are transferred, the assets are transferred as well.
5. The non-fungible nature of satoshis determines the non-fungibility of assets, making them inherently SFT (Semi-Fungible Token) assets.

6. Satoshis can be bound to any data, including smart contracts, enabling assets to have a certain level of intelligence.

Basic Capabilities of SAT20 Assets

The issuance of SAT20 assets relies on two basic capabilities:

1. The ability to identify satoshis and track them.
2. The ability to read and write data on satoshis.

Core Principles of SAT20 Assets

SAT20 assets are built upon the two fundamental properties of satoshis, which are also the core principles of SAT20 assets:

1. The non-fungible nature of satoshis. The order of creation of satoshis determines their uniqueness and identifiability. Each satoshi can be encoded using a certain encoding scheme, serving as its identification that remains unchanged.
2. The non-destructible nature of satoshis. BTC operates on a ledger model that requires ledger balance. Satoshis, being inputs and outputs of the ledger, cannot be destroyed, as it would result in an imbalanced ledger.

Other Related Services

In addition, for convenient indexing and data manipulation of satoshis, some core services based on satoshis must be established:

1. Naming service. Based on satoshis, it facilitates memorability and propagation, serving as the foundation of IP (Intellectual Property) development and an essential core service for protocol evolution.
2. Data service. It enables the reading and writing of data bound to satoshis, where only the owner can write while anyone can read. In the future, income-generating services will require payment for accessing data.
3. Payment service. SAT20 supports running software compiled into the WASM (WebAssembly) format on a virtual machine (VM). When income-generating services

run other software packages on the VM, fees are charged, which are shared between node providers and software developers. The fees are low but not zero, denominated in satoshis.

The protocol's verification version was officially activated at height 827,307, and the official version is planned to be activated at height 845,000.

Protocol

The SAT20 asset issuance protocol only includes the "deploy" and "mint" instructions. There is no need for a "transfer" instruction.

Deploy

KEY	Required	Description
p	Yes	Protocol name: ordx
op	Yes	Instruction: deploy
tick	Yes	Ticker name: 3 to 16 characters (4 characters reserved for BRC-20)
lim	No	Token limit for each mint, default is 10,000. If minting a special token on a specific sat, the default is 1.
n	No	The number of tokens bound to each satoshi, 1 by default and the maximum is 65535. (v2)
selfmint	No	Proportion of self-minting (two decimal places). Only addresses holding the ticker are allowed to mint (parent-child inscription).
max	No	Total minting limit, a 64-bit integer.
block	No	Start and end heights for minting (start-end).
attr	No	Requirements for satoshi attributes, e.g., "rar=uncommon;trz=8", extensible.
des	No	Description content.

For example, a ticker for a fair launch:


```
{
    "p": "ordx",
```

```
    "op": "deploy",
    "tick": "satoshi",
    “block”: "830000-833144",
    "lim": "10000"
}
```

Or a ticker under the control of a project:

```
{
    "p": "ordx",
    "op": "deploy",
    "tick": "Gamever",
    "selfmint": "100%",
    "max": "1000000000",
    "lim": "10000"
}
```

Rules for deploying tickers:

1. The ticker name must not have been used before.
2. If the block parameter is provided, the deploy must be confirmed at a height greater than start height plus 1000. Tickers that violate these rules are considered invalid.

"attr" is an extensible attribute designed to filter out increasingly special satoshis. Currently supported attributes include:

1. rar: Rarity, as defined in Ordinals: common, uncommon, rare, epic, legendary, mythic.
2. trz: Trailing zeros, the number of zeros at the end of the satoshi's identifier, e.g., trz=8 indicates that the satoshi's identifier has 8 zeros at the end.
3. Custom attributes will be supported in the future.

mint

KEY	Required	Description
p	Yes	Protocol name: ordx
op	Yes	Instruction: mint
tick	Yes	Ticker name: 3 to 16 characters (4 characters reserved for BRC-20)
amt	No	Number of tokens to mint, default is equal to lim and cannot exceed lim.
sat	No	Serial number of the satoshi. For tickers with specified attributes, the minting requires satisfying the specified satoshi.

For example: { "p": "ordx", "op": "mint", "tick": "satoshi" }

Each time minting occurs, the following rule checks must be performed:

1. The protocol must be "ordx".
2. The operation must be "mint".
3. The ticker must have been deployed previously.
4. The "amt" must be less than or equal to the "lim" specified in the deploy.
5. If the deploy includes "selfmint":

- Only addresses holding the ticker can mint (parent-child inscription).
- The total minted amount, including the current mint, must not exceed max*selfmint.

1. If the deploy includes "max": The total minted amount, including the current mint, must not exceed max.
2. If the deploy includes "block": The block height for the current minting must be within the specified range.
3. If the deploy includes "attr": During minting, the specified satoshi must meet the following attribute requirements:
    - If "rar" attribute is provided, check if the satoshi falls under that rarity.
    - If "trz" attribute is provided, check if the satoshi's identifier has enough trailing zeros.
    - If custom attributes are provided, check according to the defined rules.

If the above rules are not met, the current minting is considered invalid.

Protocol v2.0

The SAT20 asset issuance protocol, ORDX, will continue to evolve based on the needs of the BTC ecosystem while maintaining compatibility with previous versions.

This upgrade primarily aims to enhance the circulation of Satoshi assets on Layer 2 networks, while making the protocol more streamlined and user-friendly.

Key Updates:

Data Writing Method

The data writing method in the ORDX protocol has been upgraded from the original inscription method to the OP_RETURN data method.

New Instructions

Version 2.0 primarily supports the destruction and swapping instructions for Ordinals NFTs. These two instructions have permanent effects and are initiated by the owner to either permanently destroy the corresponding Ordinals NFT or transfer it to another Satoshi.

Data Format:

```
OP_RETURN | MAGIC_NUMBER | CT_TYPE | CONTENT

MAGIC_NUMBER = OP_16

CT_DESTROY = OP_4

CT_SWAP = OP_5
```

Destroy Content:

```
Satoshi | Inscription Number
```

Swap Content:

```
assetName | (start, end) | (start, end)
```

Note: The range of the input Satoshis must be controllable by the user. However, the output Satoshis are not necessarily under the user's control, meaning remote swaps are possible,

allowing the binding asset of the Satoshis to be sent to another party. If the UTXO contains multiple ranges for the asset, each range requires a separate OP_RETURN execution. The format for assetName is: protocol:type:tickername (For NFTs, use inscription_number).

Exploring New Features

The stake/unstake operation is similar to deploy, but with the added requirement of staking specified assets to issue corresponding new assets. This can simplify the management of staked assets. This operation instruction must be used with a SatoshiNet channel to take effect. Assets issued via staking are not bound to Satoshis.

```
assetName | amt
```

Notes:

Please note that the above new features are still in the exploratory phase and have not yet been officially implemented.

Numbering of SAT: Ordinal

SAT20 strictly assigns ordinal numbers to satoshis based on their order of creation, ensuring a **one-to-one correspondence between ordinal numbers and satoshis, with a continuous increase**. This means that within the valid range, each ordinal number corresponds to a satoshi, and each satoshi corresponds to an ordinal number. This strict one-to-one relationship is permanent. The basic principles of ordinal numbers are as follows:

1. The ordinal number of the first satoshi is 0.
2. The numbering follows the order of creation without any gaps.
3. Satoshis are transferred in a first-in, first-out manner.
4. In reward transactions, the rewarded satoshis are the first inputs, followed by other transactions' satoshis as fees in sequential order.
5. The rewarded quantity matches the actual reward quantity exactly.

The ordinal number theory of SAT20 is derived from the Ordinals protocol, but there are fundamental differences between them:

1. The Ordinals protocol considers satoshis to be destroyable, and in fact, 2,895,502,904 satoshis have already been destroyed within the Ordinals ordinal number theory

system before block 840000. This result can be confirmed by querying the Ordinals website (https://ordinals.com/status).

2. The Ordinals protocol assigns ordinal numbers to satoshis based on theory, resulting in many ordinal numbers that do not have actual satoshis corresponding to them. For example, at height 840,000, which is the fourth halving, the first satoshi of the block, called "epic," has the ordinal number 1,968,750,000,000,000. This might give the impression that 19,687,500 BTC have already been issued. However, in reality, before this height, there were slightly less than 19,687,497.2 BTC in circulation, as there were many reward blocks that were not fully claimed. Therefore, in the Ordinals ordinal number theory, for the epic satoshi with the ordinal number 1,968,750,000,000,000 at the fourth halving, there are many ordinal numbers before it that do not have corresponding satoshis.

SAT20 does not directly adopt the ordinal number theory of the Ordinals protocol, mainly because we consider satoshis to be non-destructible. This fundamental difference from the ordinal number theory of the Ordinals protocol makes it impossible for us to develop SAT20 assets based on the Ordinals ordinal number theory. Fortunately, the ordinal number theory of Ordinals has officially entered the BIP process. We look forward to the satoshis having a formal numbering rule as soon as possible, and we hope that the numbering of satoshis will better align with the fundamental principles of BTC and be based on the actual situation. Once there is a standardized scheme for satoshi numbering, we will respond promptly to the standard satoshi numbering rules, which will not affect the security of SAT20 assets.

Furthermore, SAT20 fully supports Ordinals NFTs because Ordinals NFTs are assets bound to satoshis, which align with the definition of SAT20 assets. In other words, Ordinals NFTs are also a type of SAT20 asset.

(Note: The Ordinals theory now has an official BIP number and has entered the consideration process. The possibility of the Ordinals theory becoming a BTC standard is very high. Ultimately, the encoding scheme used by the Ordinals theory will become the encoding scheme for SAT20. For more details, please refer to: https://github.com/bitcoin/bips/pull/1408)

Read and Write of SAT: Inscribe

The technique of writing data on satoshis is called inscription ("inscribe," derived from the Ordinals protocol).

Currently, there are several ways to write data on the BTC mainnet:

1. UTXO: This method is used for data writing in protocols like SRC20.
2. Segregated Witness (SegWit): This method, such as the one used in the Ordinals protocol, involves writing data in the SegWit area.
3. OP_RETURN: This method, as used in protocols like Runes, involves writing data in the OP_RETURN field.

SAT20 supports multiple methods for data inscription on satoshis, with the goal of minimizing any impact on the security of the BTC network. Currently, SAT20 adopts the inscription technology of the Ordinals protocol.

In the future, SAT20 will expand its support for additional data writing methods based on practical needs and circumstances.

Asset Issuance Models

There are three main modes for issuing SAT20 assets, primarily adjusted based on the following three parameters:

1. selfmint: Proportion of self-minting, must be set along with the max parameter.
2. max: Total supply of the token.
3. block: Block height range for minting.

Project-led Mode

For projects led by the issuer, two modes are available:

1. Complete Control selfmint: 100% max: 64-bit integer, must be set. block: Optional parameter, can be set or not.

In this mode, only the address holding the deploy NFT can mint tokens, and the assets will be fully controlled by the project. Stablecoins, for example, are typically minted by the project team.

1. Partial Control selfmint: A value less than 100%, such as 10%. max: 64-bit integer, must be set. block: Must be set, and the starting block should be at least 1,000 blocks after

the deployment confirmation.

In this mode, the address holding the deploy NFT can mint tokens, but not exceeding the set proportion. Any excess minting is considered invalid. Other addresses can participate in minting following the rules of a fair launch.

Fair Launch

selfmint: Not set. max: 64-bit integer, optional. block: Must be set, and the starting block should be at least 1,000 blocks after the deployment confirmation.

This mode is primarily community-led, focusing on fair minting by community members, controlled by the block parameter. The deployment confirmation block must be at least 1,000 blocks before the starting block; otherwise, the ticker is considered invalid. If a max limit is set and the total supply reaches that limit before the end block is reached, further minting is considered invalid. Once the end block is reached, minting is no longer possible, even if the max limit has not been reached.

Unrestricted Mode

selfmint: Not set. max: Optional. block: Not set.

In this mode, minting is not restricted by the parameters mentioned above, but rather by other factors specified by the project team. For example, it may require minting to continue on a specific rare satoshi or ticker.

Through these mode settings, we aim to provide projects with complete flexibility and allow participants to clearly understand the type of project they are engaging with.

SAT Objects

In traditional software, digital objects are cheap and infinitely replicable. These ordinary and inexpensive digital objects, combined with algorithms, have built the entire software world we have today, including the traditional internet. In the process of evolving from the traditional internet to the next generation internet, a completely different kind of digital object has emerged as the foundation for building the next generation internet. These new digital objects are non-replicable, possess unique value, and have an owner. These are the core attributes of this new type of digital object.

These new digital objects have inherent value and ownership. Counterfeit copies are worthless,

and there is no doubt about who the creator is: "first is first." If the use of their content brings benefits, it is clear who will receive those benefits. These digital objects come with their own value, rights, ownership, and inherent programmability. They provide the best underlying foundation for a value network and serve as the optimal medium for unleashing creativity.

The basic unit of BTC, the satoshi, is precisely such a valuable and meaningful digital object. We call it a "satoshi object." It cannot be created out of thin air, and it can never be destroyed. If it belongs to you, it cannot be taken away. It is the first digital object in history to possess such memorable attributes. Its potential is limitless. The admiration we have for it, which words cannot fully express, is owed to Satoshi Nakamoto's ingenious conception.

The unique attributes of "satoshi objects" – value, uniqueness, ownership, and programmability – will spark remarkable innovations on the BTC mainnet and layer-2 networks. We have boundless optimism and active participation in exploring their possibilities.

Name Service (SNS)

Satoshis are the foundation of our entire protocol ecosystem, and their ordinal numbers can be considered as indices of satoshis. However, the ordinal numbers are 64-bit integers, which are too long and not easy to remember. In order to quickly index each satoshi, it is necessary to develop a name service based on satoshis, allowing users to remember satoshis that hold significant meaning to them. The relationship between ordinal numbers and names is similar to the relationship between IP addresses and domain names. The SAT20 Name Service is a completely decentralized, BTC-based name service that is available to everyone on a fair basis and is not controlled by any third party.

The core of the name service is that each name is unique, and there are no sub-namespace. This avoids the possibility of fraud. Each name is an NFT (Non-Fungible Token) that is engraved on a satoshi. A Satoshi has only one name, and the name and Satoshi are also in one-to-one correspondence. Names are bound to satoshis, so whoever owns the satoshi also owns the name. When a satoshi is transferred, the name is transferred along with it. Names are also a type of sat asset.

Naming Rules

1. The first instance of a name is valid.
2. Names use UTF-8 characters.
3. Case-insensitive. All names/namespaces will be indexed in lowercase.
4. No spaces are allowed in names.
5. No punctuation marks are allowed in names. (Names with periods are from other name protocols.)
6. Name length starts from 3 bytes, but 4-byte names are temporarily prohibited from registration.

Note: The 4-byte names are reserved for BRC20 tickers. 1-2 byte names are for internal protocol use only and are prohibited from registration at the protocol level. They will never be opened for registration to prevent unnecessary speculation.

Combination Rules

Names can be combined to form a special meaning. The protocol establishes the following basic rules:

1. Names are combined using the "@" symbol, such as Alice@sat20.
2. Both parties need to sign and agree to the combination, meaning that the combination represents a contractual relationship.
3. The latter name, such as "sat20," belongs to a higher-level organizational form, such as a company or club.

Compatibility

The SAT20 Name Service is compatible with the major name services currently on the BTC network. For example, taking .btc as an example, a name like 1.btc will be treated as a whole, rather than splitting it into the name "1" and the namespace ".btc". As our development progresses, we plan to be compatible with these name services (read-only, without support for minting):

1. .btc
2. .x
3. Others

Note that names with a "." and names without a "." are different names. For example, 123.btc and 123 are two independent names with no relationship to each other.

Monopolistic Resources

Names are core resources and also assets. For example, the name "Pearl" as a ticker name is a name automatically held by the address that deployed the ticker. If a name has already been registered, other people cannot deploy a ticker for that name. By registering a name, one automatically gains all the permissions associated with that name, and the SAT20 protocol maintains these permissions.

Royalties

The owner of a resource will automatically receive royalties based on a configurable tax rate when the resource is used. The resource owner automatically receives royalty income.

D-Indexer

Indexers can connect with each other to form a decentralized network. This network is crucial for the BTC ecosystem and enables user nodes to operate effectively. Even smartphones can become nodes within this network. The core functionalities of this decentralized network will be gradually revealed.

[Scenarios]

FT

Each token is bound to a satoshi. Here are some examples:

The Oriental Peral


```
{
   "p": "ordx",
   "op": "deploy",
   "tick": "Pearl",
   "block": "828200-828800",
   "lim": "10000",
   "des": "The Oriental Pearl."
}
```

Fair minting for this token, which is the first token of the sat20 protocol and a meme coin with no real value, started around February 1st, 2024, and ended around February 5th, 2024 (based on the block heights 828200-828800). Please note that this token is for experimental purposes only, and it is not valuable. Avoid FOMO (Fear Of Missing Out).

We can also mint FT on rare satoshis as part of our planned experiments:

Miner's Jades


```
{
  "p": "ordx",
  "op": "deploy",
  "tick": "Jades",
  "lim": "1",
  "attr": "rar=uncommon",
  "des": "Miner's Jades."
}
```


Only the first satoshi of each block can be successfully minted, and it is estimated that each Jade token will be worth 1 BTC.

Digital Golds


```
{
  "p": "ordx",
  "op": "deploy",
  "tick": "Golds",
  "lim": "1",
  "attr": "trz=8",
  "des": "The first satoshi in a BTC"
}
```


Only the first satoshi of each BTC can be successfully minted. The serial number of this satoshi ends with eight zeros. This means that each token is worth one BTC.

NFT

Up to this point, the Ordinals protocol has been the most outstanding protocol for issuing NFTs on the BTC mainnet. However, it lacks efficient management for collections. Now, SAT20 inherits the minting capabilities of Ordinals NFTs and enhances the capabilities of NFTs and collection management. Here is a brief overview:

1. Collection Management using Tickers: SAT20 utilizes tickers to manage NFT collections. Each minting result represents a valid minting within that ticker's collection. The indexer provides comprehensive data support for ticker management.
2. Customizable Minting Conditions: SAT20 allows for the customization of minting conditions directly applicable to NFT minting. This enables project owners to set additional conditions for NFT minting. For example, minting can be limited to a specific block height, specify the amount of satoshis included in each NFT, or even set requirements for specific attributes or rare satoshis to be included in the NFT.
3. Possibility for Further Changes to NFTs: Previously, NFTs minted under the Ordinals protocol remained static and unchangeable after minting. However, SAT20 introduces the possibility for further changes and evolution of NFTs. When the underlying satoshis that constitute the NFT undergo changes, the NFT itself can also undergo subsequent transformations.

By incorporating these enhancements, SAT20 improves upon the minting and management of NFT collections, offering greater flexibility and possibilities for customization and evolution of NFTs.

SFT

The essence of SAT20 lies in SFT, where FT or NFT is just one of its manifestations. The nature of SAT20's SFT stems from two aspects:

1. The base asset, satoshis, is inherently non-fungible, which can be reflected through the numbering of satoshis.
2. Satoshis can also be bound to different data, which brings unlimited possibilities for the use of SFT.

We illustrate the attributes of SAT20's SFT through the following examples:

Pizza

SFT minted based on rare satoshis that showcases the characteristics of graphic representation. The quantity and attributes of satoshis determine the visual style of the pizza, such as a pile of pizzas, a single pizza, or a fraction of a pizza. The toppings can also change based on different satoshi attributes.

Stablecoins

Issuing multiple sets of stablecoins with different denominations, such as $1, $10, $100, $1000, etc. Each set can mint multiple NFTs as needed, with each satoshi representing a coin. Minting stablecoins on satoshis and allowing satoshis to flow to Layer 2 networks serve as transaction media, reducing the demand for a large amount of BTC on Layer 2 networks

.

RWA (Real-World Assets)

Taking real estate as an example, a Ticker can be issued for a building, and each room can be represented as an NFT. This NFT can be further divided into multiple fractions, facilitating trading and circulation.

Game Equipment

Game equipment can be continuously adjusted by the attributes of the satoshis that constitute the NFT, effectively activating trading.

Summary

SFT possesses infinite potential, and Ethereum's ERC3525 is a good example of this. It demonstrates the various possibilities and applications of SFT in the blockchain ecosystem.

DID

Based on the SAT20 Name Service, the following characteristics are achieved for DIDs (Decentralized Identifiers):

1. Uniqueness: Each DID is unique and non-duplicative to ensure the uniqueness of the identifier. The uniqueness of DIDs is supported by the protocol at the underlying level.
2. Decentralization: DIDs are not reliant on central authorities or intermediaries for verification or management. Instead, participants have autonomous control and verification. The individual who holds the satoshi with the corresponding name is the owner of the DID.
3. Verifiability: DIDs have verifiability and can be validated through cryptographic proofs to demonstrate ownership and control. This aligns with the previous point.
4. Persistence: DIDs should have a persistent lifecycle and not be invalidated due to certain changes or expiration. Satoshis are indestructible, and data inscribed on satoshis is also immutable.

In summary, the SAT20 Name Service enables the implementation of DIDs with the characteristics of uniqueness, decentralization, verifiability, and persistence. The nature of satoshis ensures the longevity and immutability of the associated data.

DeIP

DeIP (Decentralized Intellectual Property) is a decentralized network based on BTC that possesses the following fundamental attributes:

1. Decentralization: Creators who submit their works on the BTC network automatically obtain DeIP.
2. Intellectual Property Protection: Similar to open-source software, learning and personal use do not require payment, but commercial usage requires fees.
3. Decentralized Intermediation: DeIP authorization, verification, and management are achieved through smart contracts, distributed ledgers, or other decentralized technologies.
4. Verifiability: Data is inscribed on satoshis, and the individual who holds the satoshi is the owner of the corresponding DeIP.

In simple terms, data recorded on the blockchain automatically becomes a digital asset with

intellectual property rights. Commercial usage that generates income using someone else's digital asset requires payment of fees.

Roadmap

SAT20 is just the beginning of our efforts to build the BTC ecosystem. Throughout this development process, we adhere to the following principles, which we believe reflect future trends:

1. Asset Issuance on the BTC Mainnet: There will be an increasing number of assets issued on the BTC mainnet.
2. Asset Trading on Layer 2 Networks: Infinite liquidity while ensuring assets remain under users' control, offering security, cost-effectiveness, and speed.
3. The BTC network will become the foundation of the digital world, leading to a "one sat, one world" future.

SAT20 Asset Issuance Protocol (ORDX Protocol)

The development of the asset issuance protocol will be completed in the first half of 2024.

SAT20 Asset Circulation Protocol (Satoshi Transcending Protocol)

A protocol that allows BTC (Satoshi) to circulate freely. We hope to complete the prototype development of the Transcend Protocol in 2025Q1 and run it on SatoshiNet.

Native Extension Network: SatoshiNet

SatoshiNet is a modified BTC network based on BTCD source code. It is the first native extension network of the BTC mainnet based on the Satoshi Transcending Protocol (STP). Any technology that benefits BTC development can be experimented with on this network. SatoshiNet is expected to officially launch in Q2 2025.

Satoshi Swap Market: SatSwap Market

SatSwap Market is a decentralized exchange (DEX) on the SatoshiNet, developed and operated by ordx.market, providing asset trading services for the SatoshiNet. ordx.market is a professional platform in the BTC ecosystem that offers complete services for asset minting,

browsing, trading, and management. It supports all major assets in the BTC ecosystem, as well as both Layer 1 and Layer 2 networks. In the future, it will connect more ecosystems and public chains with SatoshiNet as the central hub. SatSwap Market is expected to launch alongside SatoshiNet in Q2 2025.

Open Source

To ensure efficient early-stage development, we will initially keep the project closed source. However, we plan to gradually open and eventually fully open-source the entire SAT20 project. Through community management, SAT20 will evolve into a fully decentralized project that can incorporate any BTC-native technologies, such as BTC native smart contracts or any future BTC-native layer 2 networks. We aim to promote mass adoption of SAT20 within the BTC ecosystem through open-source, permissionless collaboration and contribute to the prosperity of the BTC ecosystem. We welcome teams interested in SAT20 to join us in building a world of satoshis.

Plan:

1. Provide installation packages to assist collaborating teams in setting up their own service nodes (starting from June 2024).
2. Gradually open-source the project, releasing one module at a time as they mature (beginning in Q4 2024):
    - Indexer
    - Name service
    - SatoshiNet
    - STP
3. Explore community management models and continue the development of SAT20 (promoting community governance after open-sourcing, making Pearl the governance token for proposals, voting, etc.).

Donate

We do not issue any tokens to raise funds. Instead, we rely on service fees collected through our website to support the project's development. If you would like to contribute to the

project's growth, please consider making a donation! The donation address is: bc1ppejz29yxpz66yzkaxh6dek8pzsm8aajne6p4qak0xhxphkwzqnmsw45sur

The received donations will be used to fund the maintenance and further development of the project, as well as cover the hosting fees for sat20.org.

Thank you for your donation!

About

We are a group of technology optimists, a technical team focused on the BTC ecosystem, and we are solely dedicated to protocol development. We do not issue any assets nor have an official community. Any assets issued using the SAT20 protocol are community-driven initiatives. We are willing to provide technical support to the community as long as it aligns with the principles of the SAT20 protocol and falls within our capabilities. We are committed to continuously building the SAT20 ecosystem.

Links

- GitHub
- Twitter
- office website