SRC101 – Feasible Domain Name Solution on Bitcoin Mainnet

bitnameservice@bitname.pro
bitname.pro

Abstract. This paper explores the feasibility of developing a domain name service (DNS) on the Bitcoin Mainnet using the SRC101 asset standard. Since the early attempts to bring additional functionalities to Bitcoin, including colored coins and metadata embedding, the Web3 ecosystem has witnessed a significant evolution. Despite innovations like Ordinals and Bitcoin Stamps, Bitcoin still lacks a native, consensus-backed domain name solution. The SRC101 standard aims to address this gap by leveraging Bitcoin's secure and immutable blockchain through a data-embedding approach facilitated by open-source indexers. This solution ensures compatibility with all Bitcoin address types, offers protocol-level paid minting, and enables bi-directional resolution between wallet addresses and domain assets. Additionally, SRC101 allows users to bind custom information to their domains and connects Bitcoin's ecosystem with other chains. This paper outlines the technical structure, essential functions, and potential use cases of SRC101 domains, proposing them as a foundational service for Bitcoin's Web3 ecosystem, with applications ranging from decentralized identities to cross-chain interoperability.

1. Introduction

Since the attempt of colored coins in 2013, builders in the Web3 world have been exploring additional functionalities on Bitcoin Mainnet. Whether by attaching metadata to Bitcoin to represent real-world assets like stocks, bonds, or real estate, or by using Counterparty's 2014 method of embedding data in Bitcoin's OP_RETURN field to enable token creation, asset transfer, and decentralized exchanges, these were pioneering attempts. However, in both economic investment and product development, we cannot overlook the importance of the "Timing Effect." Take Microsoft's 2004 launch of SPOT (Smart Personal Objects Technology) smartwatch, for instance: due to high costs, limited functionality, and insufficient market demand, SPOT was unsuccessful. However, with the spread of smartphones and advancements in network technology, software, and hardware, Apple's 2015 launch of the Apple Watch made it a leader in the modern smartwatch market. The same pattern has occurred in the Web3 world, where applications burst onto the scene in 2017, reaching a peak from 2020 to 2021. Through extreme market volatility, massive TVL, and trading volume, user numbers, funds, and consensus stabilized, with products like DEX, LEND, Oracle, and Name Service becoming recognized as "infrastructure."

Such attempts took shape on Bitcoin as early as 2013, but they came too soon; market acceptance often requires luck and timing, along with pre-existing and certified consensus.

This is what I believe drove the success of asset issuance protocols like Ordinal on Bitcoin Mainnet. Even in the unfavorable market conditions of 2023, Ordinal emerged, offering a Bitcoin Mainnet asset issuance solution using indexers and data embedding. This was followed by protocols like Bitcoin Stamps, BRC20, SRC20, and ARC20, which enabled a full suite of asset issuance from tokens to NFTs. Combining this with the mature development logic of NFT marketplaces, wallets, and order books established on Ethereum from 2017-2021, the market capitalization of Bitcoin Mainnet assets soon exceeded billions of dollars, accumulating consensus from developers to users.

This step was crucial; from November 2023, Bitcoin Mainnet assets finally achieved a first consensus, recognizing the assets issued through indexers and data embedding. At this point, we can begin developing application-level products based on such asset types. From among these infrastructural options, I selected what I believe to be the most feasible, sufficiently consensus-backed, and technically appropriate: a domain name service on Bitcoin Mainnet, for which I conducted an in-depth feasibility study.

2. Outline

Since the appearance of ENS in 2017 and its peak in 2021, Web3 name services' basic functions and user experiences have become widely recognized among participants, forming a stable consensus. The outcome is that every new chain since ENS has its own name service platform, such as SpaceID on BSC and Bonfida on Solana. However, the Bitcoin ecosystem lacks a consensus-backed, usable domain name service due to the absence of a name service carrier—namely, native NFTs and smart contracts to execute name service logic.

Given this context, I analyzed the functionalities required for a domain name service in two parts, then began research on feasible domain name solutions on Bitcoin Mainnet, resulting in the SRC101 standard.

Part 1: Determining Asset Class

Firstly, we need to select an asset form that the market has already accepted. As I mentioned in the introduction, Ordinal and similar Bitcoin Mainnet assets created a multi-billion dollar market in 2023, signaling market acceptance of assets issued through indexers and data embedding. When developing a name service solution based on the Bitcoin network, we must select an existing Layer 1 asset issuance protocol that meets the following conditions:

- Sufficient user and market consensus;
- Support for all Bitcoin address types;
- Data that is as secure and immutable as possible.

Part 2: Exploring and Developing Required Name Service Functions

Unlike many teams' enthusiasm for developing smart contracts on Bitcoin Mainnet, I prefer leveraging familiar and market-recognized structures to fulfill the necessary functions. This is because, as mentioned earlier, building consensus requires luck and time. Using an established structure, rather than completely novel technology, is advantageous in terms of product feasibility and versatility. Thanks to the "low-frequency interaction" nature of name service's on-chain interactions—unlike the high-frequency interactions of DeFi-type products—name service functions can be executed and parsed through the familiar "indexer + data embedding" method, utilizing the indexer's basic logic processing capabilities. Based on this premise, I summarized several essential features for a name service on the Bitcoin network, which include:

- Implementing protocol-level paid minting;
- One-to-one binding of wallet addresses and domain assets;
- Uploading custom information and binding it to domain assets;
- Other functionalities specific to the Bitcoin ecosystem, such as binding domain assets to both Bitcoin and other sidechain or Layer 2 addresses.

These features are achieved through "indexer + data embedding," i.e., uploading data to the Bitcoin mainnet and parsing it with open-source indexers

.

3. Structural Overview

The technical structure of the domain name service has been developed based on the SRC101 asset standard, as illustrated below. The execution logic is as follows:

- Bitcoin wallet holders (domain service users) embed data in the Bitcoin mainnet to mint assets, bind addresses, upload personal data, and fulfill other needs;
- Data is directly embedded (stored) in UTXOs to ensure data security and immutability;
- Open-source indexers supporting SRC101 parse and authenticate data on the Bitcoin chain, certifying both asset validity and wallet-address binding for domain names;
- The protocol provides an open-source API for SRC101 asset-related information, enabling ecosystem projects to utilize the domain and address bi-directional parsing function.

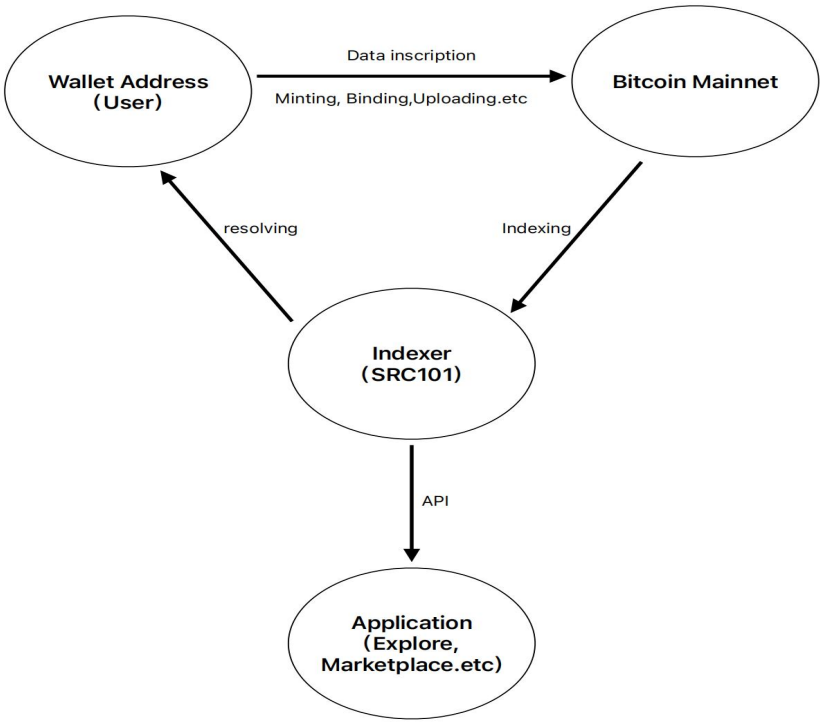
A. Wallet Address

The wallet address type is the Bitcoin mainnet address held by users of the Bitcoin domain name service implemented with the SRC101 asset standard. The data, stored directly

in UTXOs thanks to Bitcoin Stamps' underlying technical structure, supports all four existing Bitcoin address types (Legacy, Nested Segwit, Native Segwit, Taproot).

B. Bitcoin Mainnet

Through multi-signature, data embedded in UTXOs on the Bitcoin mainnet can be parsed by the indexer for domain-related information, including asset minting, address and domain binding, and personal data uploads. Embedding data directly in UTXOs ensures data security and immutability.



Bitcoin Domain Solution Using SRC101

C. Indexer

With official open-source support from Stampchain, indexers following Stampchain's standards (e.g., Openstamp, OKX) are synchronized to support the full Bitcoin Stamps and SRC ecosystem on a technical level. SRC101 asset information, including the core "wallet address and domain asset" bi-directional parsing function for name services, can be authenticated by multiple indexers and used by ecosystem projects.

D. Application

The official Stampchain open-source repository will expose APIs for SRC101 asset information, allowing Bitcoin ecosystem projects and partners to use it. Examples include:

■ Secondary markets supporting SRC101 asset trading;
■ Front-end SRC101 asset deployment and minting on third-party platforms;
■ Bitcoin wallets and explorers allowing wallet addresses to be parsed as bound domain names.

4. Asset Class Selection

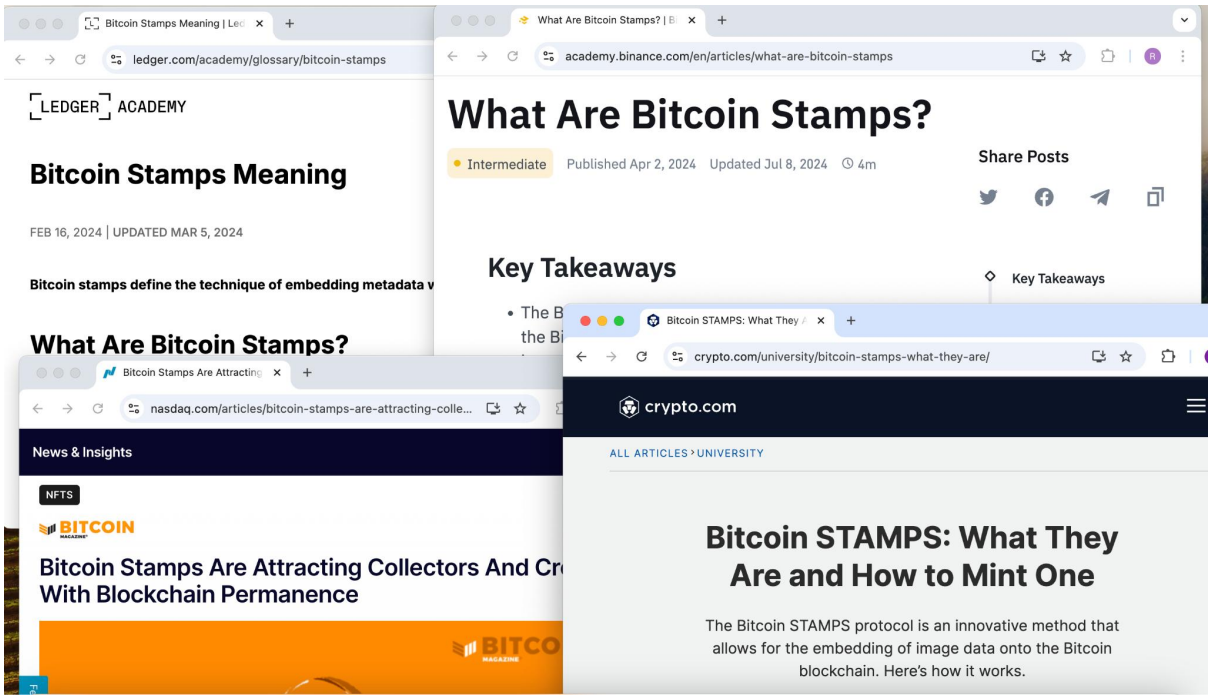
In designing a feasible name service on Bitcoin Mainnet, first principles thinking was applied to evaluate the standards to be used. The key question posed was, "What defines a simple, effective, and acceptable name service on Bitcoin Mainnet?" Based on this evaluation, three essential criteria for asset selection were established:

- Sufficient user and market consensus;
- Support for all Bitcoin address types;
- High data security and immutability.

A. Bitcoin Stamps and SRC

The enthusiasm for Ordinal inscriptions in 2023 brought new momentum to Bitcoin Mainnet. However, their greatest achievements, in my opinion, were twofold:

■ They provided a market-accepted mechanism for issuing Bitcoin Mainnet assets;
■ They established initial market consensus, essential for the Bitcoin Mainnet domain name service we aim to build.



Media and Exchange Coverage of Bitcoin Stamps

After assessing several mainstream protocols, we chose Bitcoin Stamps as the technical foundation. By November 2024, Bitcoin Stamps were widely regarded as "high-security,

immutable assets" and reported on by industry media, exchanges, and hardware wallets like Binance, Bitcoin Magazine, Cointelegraph, crypto.com, and Ledger. With over one million assets minted and a peak market cap of nearly $500 million, the technical compatibility and market consensus made Bitcoin Stamps the ideal foundation for developing the SRC101 standard.

B. Adaptability to All Bitcoin Address Types

Comparing applications on Bitcoin Mainnet to familiar Ethereum products, address type differences on Bitcoin introduce unique limitations on user experience. For instance, in 2023, users were required to use Taproot addresses (prefixed with "bc1p") for Ordinal. This address restriction is due to the Ordinal protocol design, which does not support "Nested Segwit" and "Native Segwit" addresses, while Legacy addresses are incompatible with Ordinal's storage methods introduced post-2017 soft fork.

Type	First Seen	BTC Supply*	Use*	Encoding	Prefix	Characters
P2PK	Jan 2009	9% (1.7M)	Obsolete			
P2PKH	Jan 2009	43% (8.3M)	Decreasing	Base58	1	26 – 34
P2MS	Jan 2012	Negligible	Obsolete			
P2SH	Apr 2012	24% (4.6M)	Decreasing	Base58	3	34
P2WPKH	Aug 2017	20% (3.8M)	Increasing	Bech32	bc1q	42
P2WSH	Aug 2017	4% (0.8M)	Increasing	Bech32	bc1q	62
P2TR	Nov 2021	0.1% (0.02M)	Increasing	Bech32m	bc1p	62

* Data in these columns are subject to change.

In cases involving fungible tokens or NFT minting, address restrictions affect compatibility rather than necessity. However, for name services closely tied to wallet addresses, full address-type compatibility is not optional—it's a requirement. Due to Bitcoin's development trajectory and community culture, Taproot addresses account for only about 5% of all Bitcoin addresses and holdings, while the remaining 95% is spread across other types. Therefore, when developing domain products for Bitcoin users, we must choose technology compatible with all Bitcoin address types to maximize potential user coverage across the Bitcoin ecosystem. In the "indexer + data embedding" models currently available, only Bitcoin Stamps meet these requirements.

C. Security and Immutability

Security is paramount when releasing a new asset type. In late 2023, Bitcoin core developer Luke Dashjr highlighted potential security risks with Ordinals, noting that Ordinals rely on Bitcoin's serialization data structure. If nodes or miners fail to recognize a Satoshi's serialized position, NFT data could be lost or corrupted. This reliance on serialization

exposes Ordinals to consensus dependency risks, especially when protocol changes may jeopardize on-chain data integrity.

In contrast, Bitcoin Stamps avoid serialization dependency by storing data in the scriptPubKey of an unspendable UTXO using the OP_RETURN opcode, rather than in the scriptSig. This means that Stamps data is stored directly within the UTXO set and is not subject to the risks associated with serialization order changes. Since the data is embedded in an unspendable UTXO, it remains secure and immutable on the blockchain, providing a stable foundation for new standards and assets developed on top of them.

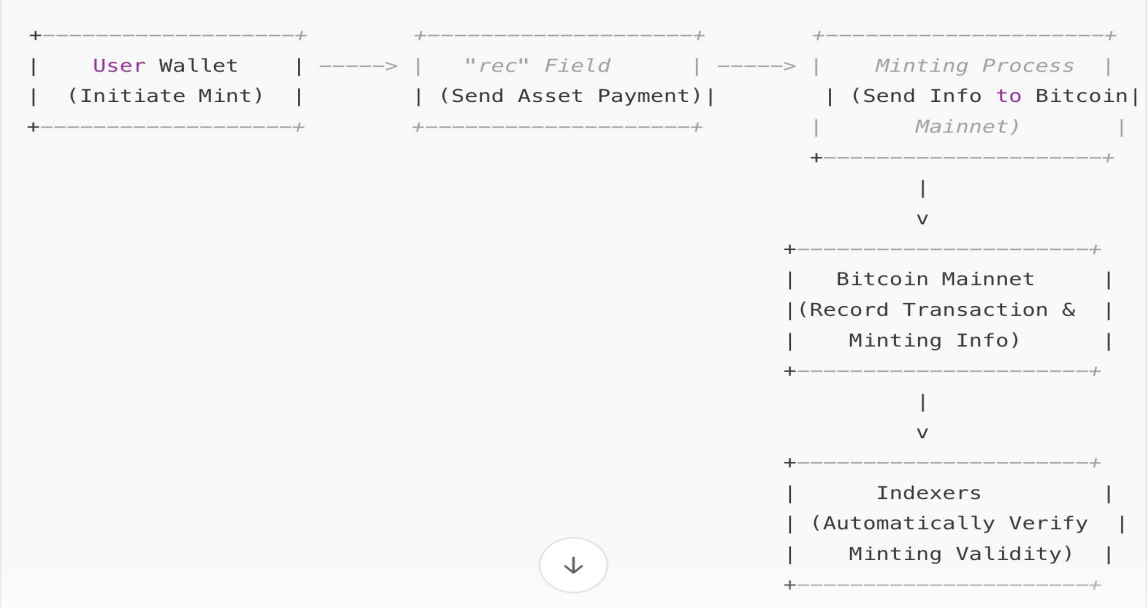
5. Essential Functions of SRC101

After finalizing the asset type, we considered the essential functions for a domain name service, specifically whether these functions could be achieved on Bitcoin Mainnet through an “indexer + data embedding” approach. Given the absence of smart contracts on Bitcoin, the indexer, as a data verification and archiving terminal, cannot perform complex computations. This makes it unsuitable for high-frequency interaction projects, mainly DeFi, but adequate for low-frequency interaction use cases like name services. Based on these requirements, SRC101 defines the following functions using “indexer + data embedding”:

- Protocol-level paid minting;
- One-to-one binding of wallet addresses and domain assets;
- Uploading custom information and binding it to domain assets;
- Bitcoin ecosystem-specific functions, such as binding domain assets to Bitcoin and other sidechain or L2 addresses.

A. Protocol-Level Paid Minting

In designing a typical domain name project, the first necessity for Bitcoin Mainnet “projects” is a transparent and reasonable fee model. This is rooted in a subtle discomfort I felt towards the Bitcoin Mainnet ecosystem last year. Due to the lack of smart contracts, tokens are distributed through "compulsory free and fair minting." If project founders or developers wish to profit from their assets, they must either rely on third-party platforms for custody trading and auctions or pre-mint and distribute tokens in "under-the-table" deals. As a result, most benefits are reaped by third-party platforms providing asset circulation channels, which dampens the enthusiasm for asset issuance projects (like NFT and fundraising).



Protocal-Level Paid Minting Overview

A healthy ecosystem needs quality assets first, followed by compatible platforms, but this is currently reversed. Asset issuance projects need a protocol-level cost recovery channel to minimize path loss, and domain projects fall into this category. Therefore, we attempted to establish the first protocol-level paid minting standard on Bitcoin Mainnet.

DEPLOY

```
{
  "p": "src-101", //(string)protocol standard name for bitname service
  "root": "btc", //(string)root domain
  "op": "deploy", //(string)function name
  "name": "Bitname", //(string)collection name
  "lim": "10", //(uint64)A maximum of 10 mint op are allowed op in each transaction. If there are more than 10 mint op in 1 transaction, it's regarded as an invalid transction, all op will be failed.
  "owner": "bc1q34eaj4rz9yxupzxwza2epvt3qv2nvcc0ujqqpl", //(string)owner address
  "rec": [
  "bc1q7rwd4cgdvcmrxm27xfy6504jwkllge3dda04ww",
  "bc1q2xexmuqmf20u5yuqcyryqprgyvap9l2wqe3lh9",
  "bc1q7epcly9u55yut5k7ykmlcyrp87knt8gxd7knnt"
  ], //(string[])recipient address to receive mint fees, can include multi addresses in an array of string. Either will be valid in transaction verification. Pay mint fees to either of these is OK.
  "tick": "BNS", //(string)
  "pri": {"0":45000,"1":-1,"2":-1,"3":900000,"4":225000}, //json object. The key is the length number of domain. These fee must be paid to "rec". Value is price in sats for each "idua". Allowed max count of this json key-value pair is 10. "-1" means it isn't mintable. 900000 is for 3 characters, 225000 is for 4 characters and 45000 is the default price for these unlisted legnth(>=5).
  "desc": "Bitname Service powered by BTC stamp.", //(string)description for the collection.
  "mintstart": "1706866958", // Unix timestamps in Milliseconds. Mint is available from this time.
  "mintend": "18446744073709551615", // Maximum Unix timestamps
  "wla": "03f86fde54dde75b1f63a5ecbf5bbf4ed5f83fee4f35437631ac605c04a8d5f15e", //Public key of admin address for whitelist data signature.
  "imglp":"https://img.bitname.pro/img/", //Image url link prefix.The full link should be "imglp"+"tokenid"(utf8)+"."+"root"+"."+imgf"
  "imgf":"png", //image format
  "idua": "999"//(string)"idua" is minimum duration. That means the actual duration = (Ceiling(dua/idua))*idua. The price will be (Ceiling(dua/idua))*pri.
}
```

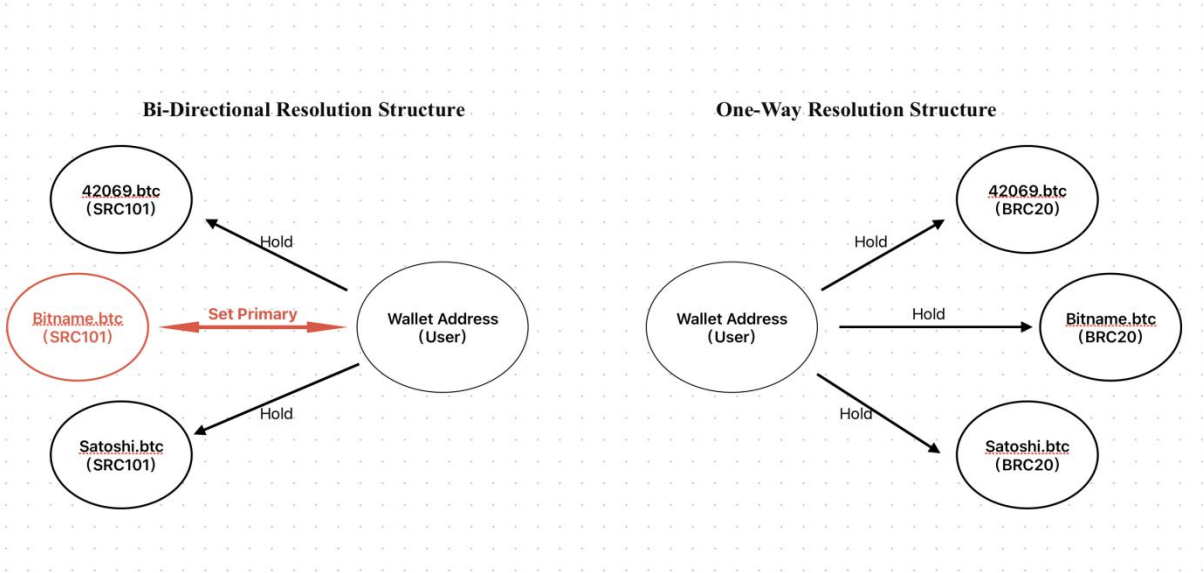
“rec” field overview

We added an “rec” field to allow for paid asset minting by specifying the required token amount and wallet address for minting SRC101 assets. Indexers verify that the specified

wallet address and token amount meet the requirements for a valid minted asset. The entire process is recorded on Bitcoin's mainnet, with no third-party platform involvement, maximizing asset issuer benefits.

B. One-to-One Binding of Wallet Addresses and Domain Assets

After ensuring the project's basic operational feasibility, I began focusing on the fundamental function of a domain name service: the one-to-one binding between wallet addresses and domain assets, enabling bi-directional resolution. This means that a search for a specific domain should reveal the associated wallet address, and conversely, a search for a wallet address should return the bound domain name. Bi-directional resolution is essential for both usability and distinguishing our approach from existing Bitcoin mainnet domain assets, such as BRC20-based inscriptions, which use a one-way resolution model. In these existing models, resolution is typically based on the holding state of the asset, where the domain name can be tracked back to a wallet address, but there is no actual binding relationship. As a result, it's only possible to perform a one-way resolution. For example, if a wallet holds 100 domain names, the one-way resolution system can identify the wallet from a domain search, but it cannot resolve the wallet address to any of the domain names. This limitation fundamentally fails to meet the standard of a fully functional domain service.



Bi-Directional Resolution vs. One-Way Resolution

In SRC101, we introduced a "prim" field to allow users to bind their wallet addresses to a domain, uploading the data to the Bitcoin mainnet. Open-source indexers then verify this binding transaction, enabling partners to retrieve address-to-domain relationships through the indexer's API for bi-directional parsing. This decentralized and automated binding mechanism is transparent, as the data is stored on-chain and parsed by an open-source indexer.

SETRECORD

```
{
  "p": "src-101", //(string)protocol standard name
  "op": "setrecord", //(string)function name
  "hash": "38091b803f794e50dcc10a9091becaf4f65d35d3ef9e71cfa90c7936af50757e", //(hash256)txid of the deploy transaction, without
"0x" at the beginning
  "tokenid": "c3VwZXJib3k=", //(string)Base64 to UTF8: c3VwZXJib3k= -> superboy.Maximum length of `tokenid` base64 string is
128.
  "type": "address", //(string)Currently two kinds of record types are supported, txt and address
  "data":{
  "btc": "bc1q7epcly9u55yut5k7ykmlcyrp87knt8gxd7knnt",
  "eth":
"7748baa6434fd17e4901e2049acad30fac188398e235e92efcd9ab90dfd67c602b4c6a50f0f62a6d3fa6d6a46abe6c1ae141f8f3322b7266fe9611a029dd7a9
71c"
  },//(Object of string value, can include multi key-value pairs)record data, this is an example to bind with both btc and eth
address.
  "prim": "true" //"true" makes this btc domain as a primary one to bind with this address.It can be true only when "btc"
address is set in "data". If you don't need this, make it as "false".
}
```

"prim" field overview

C. Uploading Custom Information and Binding it to Domain Assets

After establishing the basic one-to-one wallet and domain asset binding, we considered other essential functions for a domain service. ENS remains an excellent model in blockchain domain services, and I believe custom information upload and binding to domain assets without third-party platforms directly through on-chain data scanning and parsing is beneficial. This feature could enhance Bitcoin's domain system's expandability for social networks, identity systems, and other applications.

```
{
  "p": "src-101", //(string)protocol standard name
  "op": "setrecord", //(string)function name
  "hash": "38091b803f794e50dcc10a9091becaf4f65d35d3ef9e71cfa90c7936af50757e", //(hash256)txid of the deploy transaction, without
"0x" at the beginning
  "tokenid": "c3VwZXJib3k=", //(string)Base64 to UTF8: c3VwZXJib3k= -> superboy.
  "type": "txt", //(string)Currently two kinds of record types are supported: txt and address
  "data":
  {
  "twitter": "BitnameService",
  "github": "stampchain-io",
  "telegram": "BitcoinStamps"
  },//(Object of string value, can include multi key-value pairs)record data
  "prim": "false" //"true" makes this btc domain as a primary one to bind with this address.It can be true only when "btc"
address is set in "data". If you don't need this, make it as "false".
}
```

"data" field overview

With SRC101's "data" field, asset holders can upload information like X accounts, Discord IDs, email addresses, personal websites, or personal messages to the Bitcoin mainnet. Since individual upload fields belong to each unique SRC101 domain asset, indexers can parse personalized content for each domain. Without smart contracts, this approach establishes an all-on-chain personal information and domain asset system on Bitcoin.

D. Ecosystem-Specific Functions

After incorporating the basic functions of traditional domain projects, we developed features specific to the Bitcoin ecosystem. The 2023 Ordinal boom added momentum to the Bitcoin ecosystem, where over 70 Bitcoin Layer 2 solutions have emerged. Many Bitcoin L2s function more like projects—specifically DeFi projects—than traditional EVM-compatible chains. Due to Bitcoin's lack of smart contracts, these L2s attempt to provide BTC assets

with liquidity or restake options by adopting a chain form. Regarding domain names, each Bitcoin L2 has its own domain project, but even top L2s like Arbitrum and Optimism see limited market interest in domain assets. However, Bitcoin L2s, especially those functioning as projects, face a challenging outlook.

Could we, while considering the uniqueness of the Bitcoin ecosystem, build a system that links all BTC-related ecosystems through SRC101-based mainnet domain assets? This would create a “one domain to link the entire BTC ecosystem” state.

SETRECORD

```
{
  "p": "src-101", //(string)protocol standard name
  "op": "setrecord", //(string)function name
  "hash": "38091b803f794e50dcc10a9091becaf4f65d35d3ef9e71cfa90c7936af50757e", //(hash256)txid of the deploy transaction, without "0x" at the beginning
  "tokenid": "c3VwZXJib3k=", //(string)Base64 to UTF8: c3VwZXJib3k= -> superboy.Maximum length of `tokenid` base64 string is 128.
  "type": "address", //(string)Currently two kinds of record types are supported, txt and address
  "data":{
  "btc": "bc1q7epcly9u55yut5k7ykmlcyrp87knt8gxd7knnt",
  "eth": "7748baa6434fd17e4901e2049acad30fac188398e235e92efcd9ab90dfd67c602b4c6a50f0f62a6d3fa6d6a46abe6c1ae141f8f3322b7266fe9611a029dd7a971c"
  },//(Object of string value, can include multi key-value pairs)record data, this is an example to bind with both btc and eth address.
  "prim": "true" //"true" makes this btc domain as a primary one to bind with this address.It can be true only when "btc" address is set in "data". If you don't need this, make it as "false".
}
```

“eth” field overview

The `SETRECORD` transaction signer must be the same as "owner", otherwise it will not be considered as a valid SRC-101 transaction.

`data` is a Json object of string value, it can include multi key-value pairs.

When `type` is "address", `data` MUST include address type. Currently we only support `btc` and `eth` address types and only can set single value as record under each address type. For `btc`, the value MUST be a valid btc address. For `eth`, the value MUST be a result of signed msg following EIP191. The message to sign is the input UTXO hash for `setrecord` transaction. For example:

```
UTXO: 3409229f61face039da6bfc947252f506f379e41e3ef4a7d0cf9006b0afce695
UTXO as Message to keccak256: d7f2304806700771ad69624987a51c1c0dc2ee7884fe75428bc3e02cb6921070
Then sign it with aimed eth address:
7748baa6434fd17e4901e2049acad30fac188398e235e92efcd9ab90dfd67c602b4c6a50f0f62a6d3fa6d6a46abe6c1ae141f8f3322b7266fe9611a029dd7a971c
Signer address can be recovered by keccak256 message hash and signature:
2CA7447310b9588D9112Ee68D83dAeD4D17e5719
```

“eth” field overview

We added an “eth” field to the SRC101 standard, enabling Bitcoin wallet users to verify ownership of EVM wallets and upload both Bitcoin and EVM addresses to the Bitcoin mainnet for indexer verification. Ecosystem partners can use the indexer’s API to parse bound information across chains, strengthening BTC L2 consensus legitimacy while enhancing SRC101’s value.

6. Use Cases for SRC101 domains

After overcoming technical hurdles, SRC101 domain assets offer a comprehensive decentralized name service on Bitcoin Mainnet for the first time. This can serve as foundational infrastructure for the Bitcoin ecosystem's further expansion and potential.

Simplifying Wallet Addresses: SRC101 allows users to replace lengthy Bitcoin addresses with memorable domains (e.g., "bitname.btc"). When integrated with wallets, this simplifies user transactions.

Decentralized Bitcoin Ecosystem Identity: SRC101 domain assets can serve as decentralized identity markers. Users can bind them to social media, personal information, or DApps, replacing wallet addresses with bound domains in browsers, marketplaces, and other applications for a unified DID.

Cross-Chain Identity Matrix: With SRC101's EVM linkage feature, users can establish a BTC mainnet-centric identity matrix, linking Bitcoin with all BTC ecosystems. This cross-chain identity matrix allows users to display multi-chain information, creating a more complete decentralized identity.

Domain-Centric Personal On-Chain Data Analysis: The strong association between domains and wallet addresses, combined with SRC101's cross-chain compatibility, enables personal full-chain data collection. This allows for user preference analysis and specific data parsing.

Identity Authentication in Multiple Scenarios: SRC101's decentralized Bitcoin blockchain name service can verify user identity and data integrity in various applications, such as social media authentication, email signature validation, medical record protection, and public record certification. It can also mitigate on-chain and off-chain data manipulation, fake accounts, phishing, and more, supporting secure and reliable digital identity verification.

7. Conclusion

The idea of building a decentralized domain name service on Bitcoin Mainnet has taken a significant step toward reality with the SRC101 asset standard. By leveraging Bitcoin's existing consensus and data-embedding mechanisms, we've designed a solution that offers not only security and immutability but also scalability for the growing Web3 ecosystem. This service aligns with Bitcoin's core principles of decentralization and transparency while introducing new functionality that enhances Bitcoin's utility beyond being a store of value.

With the market already showing acceptance of Bitcoin-based assets, particularly through innovations like Bitcoin Stamps, SRC101 is positioned as a foundational component of a broader ecosystem that could transform how users interact with Bitcoin. The introduction of protocol-level paid minting, bi-directional address-domain binding, and cross-chain

interoperability all point to a future where Bitcoin can play a larger role in identity, asset ownership, and decentralized applications.

Looking forward, the SRC101 standard holds the potential to catalyze a wave of innovation in the Bitcoin ecosystem, expanding its use cases and broadening its impact across the digital economy. As this technology matures, it will be exciting to see how the community, developers, and partners continue to drive the adoption and further development of this solution.

Reference

(1) **Nakamoto, Satoshi**. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008, https://bitcoin.org/bitcoin.pdf. Accessed 23 Sept. 2024.

(2) **Buterin, Vitalik**. "A Next-Generation Smart Contract and Decentralized Application Platform." 2013, https://ethereum.org/whitepaper. Accessed 23 Sept. 2024.

(3) **Bartoletti, Massimo, Bryn Bellomy, and Livio Pompianu**. "A journey into bitcoin metadata." Journal of Grid Computing 17 (2019): 3-22.

(4) **Bartoletti, Massimo, and Livio Pompianu**. "An analysis of Bitcoin OP_RETURN metadata." Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers 21. Springer International Publishing, 2017.

(5) **Ito, Kensuke, Kyohei Shibano, and Gento Mogi**. "Bubble prediction of non-fungible tokens (NFTs): An empirical investigation." arXiv preprint arXiv:2203.12587 (2022).

(6) **Li, Ningran, et al. "Bitcoin inscriptions**: Foundations and beyond." arXiv preprint arXiv:2401.17581 (2024).

(7) **Liao, Guofu, et al**. "Programming on Bitcoin: A Survey of Layer 1 and Layer 2 Technologies in Bitcoin Ecosystem." arXiv preprint arXiv:2409.19622 (2024).

(8) **Muzammil, Muhammad, et al**. "Typosquatting 3.0: Characterizing Squatting in Blockchain Naming Systems." arXiv preprint arXiv:2411.00352 (2024).

(9) **MicroStrategy**. "DID-BTC Specification." 2023, https://microstrategy.github.io/did-btc-spec/. Accessed 23 Sept. 2024.

(10) **Ordinals**. "ord." GitHub, 2022, https://github.com/ordinals/ord. Accessed 23 Sept. 2024.

(11) **StampChain.** "stampchain-io." GitHub, 2023, https://github.com/stampchain-io. Accessed 23 Sept. 2024.

(12) **Ethereum Name Service.** "ENS Documentation." 2023, https://docs.ens.domains/. Accessed 23 Sept. 2024.

(13) **Unchained Capital**. "Bitcoin Address Types Compared." Unchained Capital Blog, 27 Oct. 2023, https://unchained.com/blog/bitcoin-address-types-compared/. Accessed 23 Sept. 2024.

(14) **Bertucci, Louis**. "Bitcoin ordinals: Determinants and impact on total transaction fees." Available at SSRN 4486127 (2023).