

# Bitcoin Inscriptions: Foundations and Beyond

**Abstract**—Bitcoin inscription marks a pivotal moment in blockchain technology. This paper presents a primary exploration of Bitcoin inscriptions. We dive into the technological underpinnings and offer a detailed comparative analysis between Bitcoin inscriptions and NFTs on other blockchains. Further, we explore a wide range of use cases and significant opportunities for future innovation, including inscription derivative protocols, Bitcoin Layer2 solutions, and interoperability techniques.

**Index Terms**—Inscription, BRC-20, Ordinals, Bitcoin Layer2

## I. INTRODUCTION

When people mention blockchain, the first thing that comes to mind is Bitcoin [1]. Despite the past decade (an era also known as Web3 [2]) witnessing many innovations in numerous public blockchains such as Ethereum [3], BSC [4], and Solana [5] in terms of decentralization, scalability, security, and privacy, it is undeniable that Bitcoin remains the largest and most valuable cryptocurrency asset in the world [6]. The price trend (Fig.1) of Bitcoin from 2021 to the present shows that its price has experienced multiple significant rises and falls. Since reaching its historical peak of about \$69,000 in Oct 2021, the price of Bitcoin has been on a continuous decline. It was not until 2023 that Bitcoin welcomed a new round of “bull market”. In addition to market sentiment and economic environment factors, the technological development of Bitcoin is the key driver igniting this round of market enthusiasm.

The Ordinal protocol [7], crafted by Casey Rodarmor and launched on the Bitcoin mainnet in Jan, 2023, has opened new avenues for users to innovate within the Bitcoin blockchain. This is achieved through the creation of “inscriptions”, which function similarly to non-fungible tokens (NFTs) [8] found on other blockchains. Specifically, it is realized by adding non-transactional data (typically in JSON style) to Bitcoin transactions. These inscriptions can include a variety of data types, ranging from simple text to complex images or code. Following its launch, Bitcoin inscriptions quickly garnered significant attention in the cryptocurrency market. As of now, there have been over 55 million [9] Bitcoin inscriptions created, with text-based data types comprising over 95% of these inscriptions (Fig.2). Bitcoin inscriptions enhance the capabilities of Bitcoin, pushing the boundaries of what was once deemed impossible.

Previous studies have explored various aspects surrounding this new hype. Razi et al. [10] present a thorough overview of NFT (including Bitcoin NFT) and survey the current landscape of NFT applications across various domains. Wang et al. [11] delve into the surge of interest and activity surrounding BRC-20 tokens and critically examine the narratives of their hope and hype based on market sentiment. Louis [12] delves into the factors influencing transaction fees in the context



Figure 1: Bitcoin Price Trend from 2021 to Present (Jan. 2024)

of Bitcoin Ordinals and assesses their overall impact on the Bitcoin network. Yu et al. [13] present a detailed design of a lightweight bridge to facilitate communication and asset operation from the Bitcoin network to Ethereum blockchains. Kiraz et al. [14] introduce a novel mechanism for conducting NFT transactions on the Bitcoin blockchain. They propose an off-chain receipts method that allows for the certification of authenticity and ownership transfer of digital assets.

While these works have contributed elegant insights, our research distinguishes itself by offering a distinct perspective. We focus on providing a clear and comprehensive interpretation of the most fundamental aspects of inscriptions, delving deeper than the surface-level usage or construction discussed in prior works. We summarise contributions as follows:

- We provide the first technical paper dedicated to the topic of Bitcoin inscriptions (Sec.II), covering its necessary preliminary technologies, including SegWit, Schnorr Signatures, Taproot, Tapscript, and Ordinal Theory.
- We present Bitcoin inscriptions’ operational mechanisms (Sec.III), detailed by an examination of the working principles, a comparative analysis with conventional NFTs, and the potential use case built on Bitcoin inscriptions.
- We discuss challenges and opportunities from a forward-looking perspective (Sec.IV), identifying areas for future research and industry development. In particular, we emphasize the promising prospects of Bitcoin Layer2 and derivative protocols related to inscriptions, drawing parallels with their success in Ethereum ecosystems.

## II. PRELIMINARIES AND BACKGROUND

In this section, we provide technological underpinnings, including the Segregated Witness, Schnorr Signature, Taproot, Tapscript, and Ordinal Theory within the Bitcoin network.

**Segregated Witness.** SegWit [15] was proposed to address the scalability issue by changing the way transaction data is structured and stored in the blocks (cf. Fig.3). Firstly, a

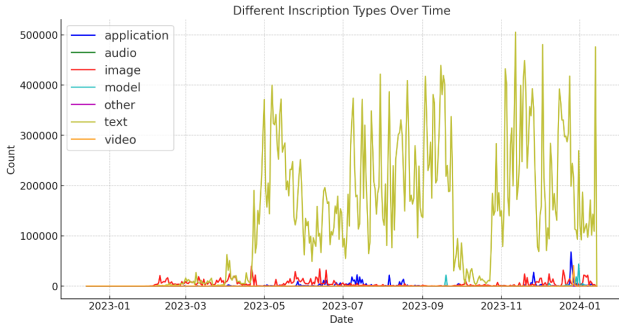


Figure 2: Different Inscription Types Over Time

SegWit transaction consists of two main components: the original transaction structure (without the signature) and a separate *witness* section containing the signatures and scripts. It is worth noting that the signature data is separated from the main transaction data. The witness information is still transmitted and stored in the blockchain but is no longer a part of the transaction's txid calculation. The txid is now calculated without including the witness data, effectively resolving the transaction malleability issue. This change means that the txid remains constant even if the signature data is altered. Secondly, SegWit introduces a new concept called *block weight*, which is a blend of the block's size with and without the witness data. The maximum block weight is set to 4MB, while the size of the non-witness data is still capped at 1MB [16]. This effectively allows for more transactions to be included in each block, improving the network's capacity.

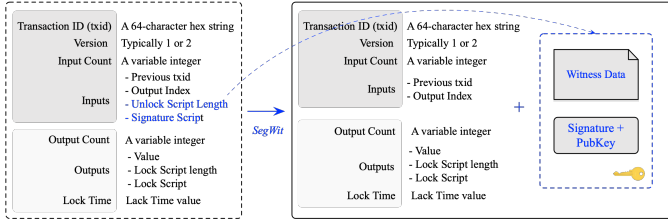


Figure 3: Bitcoin Transaction Data Structure (SegWit)

**Schnorr Signature.** The Schnorr signature [17] consists of three main algorithms: *key generation*, *signing*, and *verification* [18]. Key generation establishes a secure private-public key pair. The signing algorithm then creates a unique signature for each message, combining a random nonce, a hash function, and the private key. The verification algorithm checks the signature's validity against the message and public key. For example, key generation (Algorithm 1) initiates the Schnorr signature process. It involves generating a private key  $d$  and a public key  $Q$ . The private key is randomly selected from the set  $\mathbb{Z}_n^*$ , representing the group of integers modulo  $n$  (excluding zero), where  $n$  is the order of the elliptic curve. The public key  $Q$  is computed as the product of the private key  $d$  and the generator point  $G$  of the elliptic curve. The generator point  $G$  is a pre-defined point on the elliptic curve, known to all parties in the cryptographic system. The output is the pair  $(d, Q)$ .

**Taproot and Tapscript.** In comparison, BIP-341's Taproot

### Algorithm 1 Key generation

**Require:** Generator point  $G$ , order of the curve  $n$

**Ensure:** Private key  $d$ , Public key  $Q$

- 1:  $d \leftarrow$  randomly choose from  $\mathbb{Z}_n^*$
- 2:  $Q \leftarrow d \cdot G$
- 3: **return**  $(d, Q)$

[19] allows for the compression of data in inscription transactions, reducing their size and improving scalability. BIP-342 [20] enables batch verification of signatures, which is crucial for multi-signature transactions often used in inscriptions. To further illustrate the working principle of BIP-341 and BIP-342, we consider a situation where a Bitcoin address is controlled by three parties: A, B, and C. We created a Taproot output address that allows for flexible spending conditions using MAST and Tapscript (shown in Fig.4). The spending conditions are as follows: (i) *any two of the three parties (A, B, C) can jointly spend the funds*; and (ii) *if the funds are not moved for a year, party A can unilaterally spend them (a time-lock condition)*. Initially, the parties aggregate their individual public keys ( $pk_A, pk_B, pk_C$ ) to form a single Schnorr Internal public key  $P$ . This aggregate key, alongside the Merkle root derived from two hashed scripts (Script1 adds up the valid signatures and ensures that at least two signatures are provided; Script2 uses OP\_CheckSequenceVerify to enforce the time-lock, ensuring the script can only be executed after a year. Then it checks the signature from A), and forms the Taproot output. When it's time to spend, the parties can opt for a key-path spend using  $P$  for a private transaction, or a script-path spend, revealing the chosen script and its corresponding Merkle proof to fulfill specific conditions.

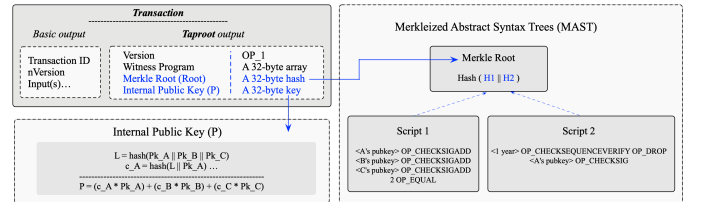


Figure 4: Taproot and Tapscript

**The Ordinal Theory.** Bitcoin Ordinal Theory [21] introduces the uniqueness within the Bitcoin ecosystem. It revolves around the idea of assigning distinct identities to individual satoshis (sats), the smallest unit of Bitcoin (100 millionths of a Bitcoin) [1], allowing for their precise tracking and utilization in various applications. Satoshis are numbered in the order they are mined, and this numbering is maintained as they are transferred from transaction inputs to outputs, adhering to a first-in-first-out principle. Ordinal numbers are essentially a numbering scheme for satoshis, allowing each satoshi to be tracked and transferred as an individual entity.

### III. UNDERSTANDING BITCOIN INSCRIPTIONS

This section offers a comprehensive understanding of Bitcoin inscriptions, illustrating the history of Bitcoin-related

NFTs, technical working principles, a comparative analysis distinguishing Bitcoin inscriptions from NFTs on platforms like Ethereum, and the exploration of use cases.

### A. Working Principle

The following diagram (Fig.5) illustrates the process of inscribing data onto the Bitcoin blockchain and associating it with a specific ordinal (satoshi).

The working principle is as follows: Firstly, the data intended for inscription is first prepared in a suitable format. This often involves encoding the data into a byte string that can be embedded in a Bitcoin transaction. The data is typically accompanied by a MIME type [22] that specifies the nature and format of the content (e.g., image/jpeg, text/plain), ensuring compatibility with web standards. This alignment with web standards means that inscription content can be retrieved and rendered by standard web browsers, similar to how they handle regular web content served from a server.

Inscription content is encapsulated within a structure known as an “envelope”, which uses Bitcoin taproot script-path spend script [21] opcodes OP\_FALSE, OP\_IF, ..., OP\_ENDIF. Taproot scripts benefit from the witness discount [23] introduced by SegWit, which reduces the size and cost of storing witness data compared to other transaction data.

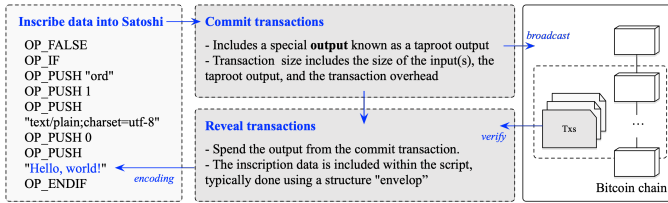


Figure 5: Working Principle of Bitcoin Inscriptions

Creating the inscription transaction has two phases. In the first phase (called *commit transaction*), a taproot output is created, which commits to a script containing the inscription content. This script is constructed in such a way that it cryptographically references the data without revealing it. The transaction is then broadcast and included in a block on the blockchain. In the second phase, a subsequent transaction (*reveal transaction*) is made to spend the output from the commit phase. This spending transaction includes the actual inscription data within its script. When confirmed, inscription data becomes permanently recorded on-chain.

Finally, the unique ordinal number of the selected satoshi is tracked through these transactions. As ordinals follow a first-in-first-out principle, such ordinal number is effectively transferred from the input satoshi to the output satoshi (namely, the commit transaction) and then to the inscribed satoshi (the reveal transaction).

### B. Differences Between Bitcoin Inscriptions and Other NFTs

Bitcoin inscriptions and NFTs on other blockchains (majorly, EVM-compatible platforms) represent two distinct approaches. This comparative analysis aims to discuss the funda-

mental differences between these two paradigms, highlighting their unique characteristics and implications.

**Protocol and description method.** Bitcoin inscriptions operate on the Ordinal protocol, embedding data directly into individual satoshis, and are described as digital assets, ordinals, or inscriptions. In contrast, NFTs on platforms like Ethereum utilize standards such as ERC-721 [24] or ERC-1155 [25], and are commonly referred to as NFTs. This fundamental difference in protocol form shapes the inherent properties and possibilities of each asset type.

**Storage and immutability.** Bitcoin inscriptions are entirely stored on-chain, ensuring complete immutability and permanence. Once an inscription is embedded in the Bitcoin blockchain, it becomes unalterable. This method ensures the durability of the inscribed content, with the cost of inscriptions being proportional to the content’s size. On the other hand, NFTs on other blockchains often rely on off-chain storage solutions like IPFS [26] and Arweave [27], introducing potential challenges in content availability and permanence. The degree of immutability for these NFTs can vary, with some being alterable or deletable by the contract owner. This variability necessitates a thorough audit of the contract code to ascertain the immutability of an NFT. The auditing process can be complex and technically demanding.

**Minting and trading.** Minting Bitcoin inscriptions currently requires a node or third-party services, and the trading of these inscriptions occurs through NFT marketplaces. Other NFTs can often be minted directly through web interfaces and are also traded on NFT marketplaces. However, the integration of Bitcoin inscriptions with other platforms is challenging due to Bitcoin’s scripting limitations, while NFTs on programmable blockchains offer more seamless integration.

**Scarcity.** Bitcoin inscriptions are inherently limited by the nature of the Bitcoin blockchain. Since they are directly tied to individual satoshis, their scarcity is intrinsically linked to the total supply of Bitcoin, which is capped at 21 million coins. This finite supply of satoshis imposes a natural limit on the number of possible inscriptions. On platforms like Ethereum, the creation of NFTs is often governed by smart contracts that allow for flexible minting policies. Creators can generate large quantities of NFTs with minimal cost, which can potentially lead to a saturation of the market. While some NFT projects on other blockchains impose a cap on the number of tokens, others do not, allowing for an unlimited supply. This flexibility means that the scarcity of NFTs on these platforms can vary significantly from one project to another.

**Royalty models.** Bitcoin inscriptions do not inherently support on-chain royalty models. This means that when a Bitcoin inscription is transferred or sold, there is no automatic mechanism within the Bitcoin blockchain to provide a percentage of the sale back to the original creator. Many NFTs on platforms like Ethereum utilize smart contracts that can include on-chain royalty models. These contracts automatically enforce that a certain percentage of every secondary sale of the NFT is paid to the original creator. The presence of on-chain



royalty models offers ongoing compensation for creators but introduces complexity and standardization challenges.

**Integration and energy consumption.** Bitcoin inscriptions benefit from direct integration into the largest and most established cryptocurrency market, with immediate access to a vast and liquid market, but it is difficult to integrate into other platforms due to Bitcoin’s scripting limitations. On the other hand, their energy consumption is high due to Bitcoin’s Proof of Work consensus. In contrast, NFTs on other blockchains are confined to specific ecosystems with varying energy footprints based on the consensus algorithm of the platform.

**Advantages and disadvantages.** Bitcoin inscriptions offer the advantages of scarcity and the characteristics of luxury goods. However, they face challenges such as slow block speed, complexities in minting and trading, and a complex wallet setup. Other NFTs enjoy a mainstream mode and a high user base but may lack unique features or recognition, potentially leading to market saturation.

#### C. Use Cases

**Token Standard for Fungible Tokens on Bitcoin.** On March 8, 2023, an anonymous developer named domodata launched the BRC-20 [28]. The BRC-20 token standard represents an experimental approach to creating fungible tokens using ordinal inscriptions. This standard is akin to Ethereum’s ERC-20 [29] but is uniquely tailored for the Bitcoin network [11]. ORDI [30] is the first BRC-20 token issued on the Bitcoin network, with a total supply of 21,000,000 tokens. Unlike Ethereum’s ERC-20 tokens, ORDI is not a smart contract token. It operates without the support of underlying technology, project teams, real-world project applications, or defined use cases. The valuation of ORDI is essentially driven by community consensus and the dynamics of market interest (also known as the meme coins [31]). Creating a new meme coin comes at no cost; each one faces competition from other, more ‘meaningful’ meme coins. For instance, another BRC-20 token, SATS [32], competes in this space. Each Bitcoin can be divided into 100 million satoshis, and this BRC-20 token named SATS has set its total supply at 21 trillion, mirroring the maximum number of 21 trillion satoshis.

**Digital art&collectibles.** Bitcoin inscriptions can offer artists and collectors an innovative approach to creating and trading digital works. It leverages the capability to inscribe digital assets directly onto individual satoshis on Bitcoin, ensuring each piece’s authenticity and permanence. A notable example of this is the creation of Ordinal Punks [33], which draw inspiration from the iconic CryptoPunks [34] on Ethereum. These pixel-art characters, each with unique features and levels of rarity, are inscribed onto satoshis, turning them into highly desirable collectibles within the digital art sphere. Furthermore, writers and poets are finding a new medium for their work through Bitcoin inscriptions. Entire poems or short stories can be inscribed onto satoshis, creating a unique form of literary art. For instance, a poem by Ana Maria Caballero sold for 0.28 Bitcoin (equiv. \$11,430) at Sotheby’s [35], one of the world’s most famous auction houses.

**Gaming assets.** Leveraging the immutable nature of the Bitcoin blockchain, gaming assets inscribed as ordinals provide players with ownership of unique in-game items, characters, or even entire game worlds. The “Pizza Ninjas” gaming project [36] intertwines the thrill of gaming with the world of digital collectibles. Each Pizza Ninja character is not only a playable asset but also a piece of art. By inscribing these unique characters and narratives onto Bitcoin, the project ensures the rarity and ownership of every in-game element.

**Record of messages.** The use of Bitcoin inscriptions for creating an immutable record of messages is another feasible application. Inscribing messages can serve as proof of existence for documents or intellectual property. By embedding a hash of the document or a reference to the work in a Bitcoin transaction, creators can prove the existence of their work at a specific point in time. In some scenarios where the integrity of communication is crucial, such as in legal contexts, this way ensures that the content of the communication remains unaltered and verifiable.

## IV. OUR DISCUSSION

### A. Challenges

**Blockchain bloat.** It refers to the increase in the size of the blockchain due to the accumulation of data over time [37]. In the context of Bitcoin inscriptions, blockchain bloat is exacerbated by the addition of non-financial data embedded directly into the blockchain. As the blockchain grows in size, the storage requirements for nodes also increase. In addition, new nodes or nodes catching up to the blockchain state may experience slower synchronization times due to the larger amount of data that needs to be verified. Moreover, larger block sizes can impact the efficiency of the network and potentially undermine the decentralized nature of Bitcoin.

**Limited smart contracts and compatibility.** It refers to Bitcoin’s inherent design, which prioritizes security and simplicity over complex programmability. Unlike platforms like Ethereum, which are designed to support a wide range of decentralized applications through smart contracts, Bitcoin’s scripting language is more restricted. This limitation impacts the blockchain’s ability to support complex transactions and scalable applications, particularly those requiring intricate logic and interactions, such as DeFi protocols [38].

**Security threats.** The United States National Vulnerability Database (NVD) has identified a significant cybersecurity risk associated with the Ordinals protocol [39]. The vulnerability allows for bypassing the datacarrier limit by disguising data as code in certain versions of Bitcoin Core and Bitcoin Knots. This exploit has been utilized by inscriptions, leading to the addition of substantial non-transactional data to the blockchain. Moreover, with the rising popularity of Bitcoin inscriptions, this ecosystem has attracted various types of scams. For example, scammers construct JSON fields for transferring inscriptions and encode them as hex for users to inscribe [40]. This can result in the theft of users’ inscriptions.

Additionally, on trading platforms, users often encounter numerous inscriptions with the same name, making it challenging to identify authentic ones.

**User-friendliness.** Although minting and transferring Bitcoin inscriptions can be done directly on Bitcoin, for many users, especially those not deeply familiar with blockchain technology, accessing and interacting with Bitcoin inscriptions may require specialized wallets and marketplaces. Most Ethereum users utilize wallets and tools optimized for interacting with ERC standards, which may not be compatible with Bitcoin inscriptions. This necessitates the use of Bitcoin-specialized wallets (e.g., Gamma.io [41], Ordinals Wallet [42]) or third-party services (e.g., UniSat [43], Magic Eden [44]), which is a significant educational gap for users transitioning from Ethereum to Bitcoin inscriptions. In addition, users accustomed to Ethereum’s transaction speed and fee structure may find Bitcoin’s inscription system less efficient and economical.

**Increased transaction costs.** Bitcoin transaction costs are usually influenced by several factors, such as the size of transactions, network congestion, and priority of transactions [45]. Inscriptions often involve embedding additional data into a Bitcoin transaction. The larger and more complex this data, the more space it occupies in a block, driving up transaction fees. As inscriptions become more popular, they contribute to network congestion, further elevating the costs. Therefore, users might become more selective in creating inscriptions due to higher fees. Cost barriers will lead users to perceive inscribing on Bitcoin as most appropriate for artworks that are either small in size or of high value.

## B. Opportunities

**Inscription derivative protocols.** After the surge in popularity of Bitcoin inscriptions, the trend quickly spread to other public blockchains, leading to the emergence of numerous inscription derivative protocols and imitation projects. These innovative projects and protocols have further enriched the inscription ecosystem. We categorize mainstream inscription protocols based on their respective public blockchains, analyzing and comparing the inscription protocols on each chain.

As discussed above, the BRC-20 protocol faces limitations with only four-letter tokens and susceptibility to front-running attacks. To improve BRC-20, ARC-20 [46] removes the four-character limit, allowing for more diverse gameplay. A unique project within this framework is “Realm” [47], where each registered entity is a prefix text, ultimately owning the pricing rights to all suffixes. Rune [48], proposed by Ordinals founder Casey, is designed to issue Fungible tokens by inserting token data directly into UTXO scripts. Rune’s implementation is similar to ARC20, while it includes the token quantity in the script data, making it more legitimate. In addition, RGB [49] represents an ultimate scaling solution, turning smart contract states into concise proofs inscribed in BTC UTXO output scripts. RGB offers low transaction costs and high scalability. It is considered a Layer2 for BTC, leveraging BTC’s security for smart contracts.

For other blockchains, DRC-20 [50] on Dogecoin is similar to BRC-20 but popular due to low transaction costs and strong meme appeal. Ethscriptions protocol [51] on the Ethereum chain introduced “dumb contracts”, bringing functionality and practicality. ASC-20 [52], BSC-20 [53], PRC-20 [54] on other EVM-compatible chains also enable inscription and index building for projects like AVAL, BNBS, and POLS. SOLs [55] on Solana began in November 2023, with a total of 21,000,000 inscriptions. The main focus is on NFTs, with indexing based on image or file hashes. SFNs [56] is recognized as the first inscription on the EOS chain. It adopts the AtomicAsset standard [57], which provides a powerful feature set while minimizing unnecessary complexity and focusing on RAM efficiency. In addition, MRC-20 [58] powered by the Move blockchain offers an efficient and user-friendly approach to token management. APT-20 [59] is an experimental token standard that facilitates the creation and transfer of fungible tokens through the Ordinals protocol on the Aptos blockchain.

**Bitcoin Layer2 solution.** BTC Layer2 is a layer above the BTC network, primarily aimed at solving issues of insufficient transaction throughput, high transaction costs, and scalability challenges in the BTC network [60]. In simple terms, Layer1 refers to the Bitcoin public chain. To address the throughput issues of the BTC network and avoid high fees, transactions can be processed on Layer2 and then the results returned to Layer1, thereby reducing network pressure on the Bitcoin network. As the volume of inscription transactions on the Bitcoin network continues to grow, maintaining the stability of the settlement layer (Layer1) while encouraging innovation in the upper layer (Layer2) is the current and future main direction of development.

The core concept of ZK Rollups [61] is to bundle multiple transactions into a single transaction on the Bitcoin blockchain. This process uses zero-knowledge proofs to verify bundled transactions without exposing details. The current versions have raised concerns about centralization, as they primarily rely on centralized sequencers. In many existing implementations, a single entity is responsible for aggregating transactions, generating validity proofs, and submitting batch data to the Bitcoin network. This places considerable trust in the sequencers. A hybrid model combining multiple types of provers to accommodate different use cases may emerge. For example, a threshold scheme [62] can distribute power to a dynamic group of sorting nodes based on equity or rotation; an opcode scheme [63] can enable bidirectional transfer of Sats and assets between the Bitcoin base layer and ZK rollups.

In addition to ZK rollups, other Layer2 technologies are also maturing. Two notable examples are Rootstock and Stacks. Rootstock (RSK) uses merged mining to ensure security comparable to Bitcoin and achieves expansion, efficiency, and advanced functionalities [64]. Merged mining allows Bitcoin miners to process and validate BTC and RSK transactions within the same block. In this mode, miners can mine simultaneously on the parent chain (larger blockchains like Bitcoin) and the child chain (smaller blockchains like RSK).

By leveraging the computational power of the more powerful parent chain, the smaller chain gains additional security. Despite progress, RSK still faces challenges. RSK has difficulty attracting enough users, and the complexity and novelty of its merged mining mechanism also pose risks. Stacks is a Layer2 smart contract protocol designed specifically for Bitcoin, aiming to bring decentralized applications and smart contract functionalities to the Bitcoin ecosystem [65]. Stacks introduces decentralized mining/bridging with Bitcoin. However, bottlenecks such as user experience, fees, and network effects may still be barriers to its broader adoption.

The payment channels on the Lightning Network (LN) circulated over 5400 BTC, valued at over 230 million USD [66]. LN micropayment channels establish a relationship between two parties, allowing them to continuously adjust balances without broadcasting each transaction to the blockchain [67]. This method delays broadcasting the total balance between the two parties to a future point in time, effectively processing the total balance in one transaction. This approach allows financial relationships to exist without trust in the other party, free from the risk of default. The Taproot asset protocol [68], announced in Nov 2023, further supports asset issuance through LN and provides customizable asset destruction features. Although high-fee events caused by network congestion have exposed LN’s ongoing scalability limitations, LN solutions are expected to continue to be integrated into a wider range of applications as decentralized payment channels.

**Interoperability for Bitcoin inscriptions.** Bitcoin inscriptions currently face limitations in interoperability and lack effective liquidity mechanisms. Establishing the infrastructure to provide liquidity for Bitcoin inscriptions, such as interoperability mechanisms [69], is one of the key directions to propel the development of the Bitcoin inscription ecosystem. Interoperability techniques allow Bitcoin inscriptions to be traded or utilized in various blockchains. This opens up a larger market for these assets, as they can be accessed by users on different blockchain platforms, not just those on the Bitcoin network.

In 2023, Ordinals Market and Bitcoin Miladys jointly released the BRC721E standard [70]. This standard enables the migration of verifiable ERC721 NFTs from Ethereum to Bitcoin Ordinals. During the bridging of NFTs, BRC721E encodes NFT data directly into a burn transaction. This burn transaction also acts as a request for a Bitcoin chain inscription, specifying a Bitcoin address to receive the inscription. It’s important to note that the burn transaction is irreversible, which means that currently, it’s not possible to convert an Ordinal back into an ERC-721 NFT. Therefore, we consider this reversibility a potential research direction for the future.

In addition, several cross-chain bridging protocols support the transfer of BRC-20 assets across chains, such as MultiBit [71], TeleportDAO [72], and SoBit Bridge [73]. MultiBit is a cross-chain protocol between BRC20 and ERC20. It enables the transfer of tokens between BRC20 and ERC20. Similar to MultiBit, TeleportDAO has established a cross-chain Ordinals market, supporting the transfer and trading of assets between

BTC and Polygon. SoBit Bridge allows users to transfer their BRC20 assets to Solana, enabling the creation of equivalent tokens on the Solana blockchain. Additionally, Allins [74] is a decentralized exchange that employs an automated market maker [75] method to establish asset liquidity for inscriptions. Allins encapsulates the inscription scripts of different chains in its unique virtual machine and continuously updates assets through an indexer. Leveraging smart contract-based liquidity pools, users can buy and trade inscriptions via AMM and earn income from inscription assets in the Farming market.

Table I: Bitcoin-related Standards

Standard and Proposal	Proposal Full Title	Blockchain Platform	Year
BIP 114	Merkelized Abstract Syntax Tree	Bitcoin	2016
BIP 141	Segregated Witness (Consensus layer)	Bitcoin	2017
BIP 340	Schnorr Signatures for secp256k1	Bitcoin	2020
BIP 341	Taproot: SegWit Version 1 Spending Rules	Bitcoin	2020
BIP 342	Tapscript	Bitcoin	2021
Ordinal	Ordinal Protocol Documentation	Bitcoin	2023
BRC-721E	BRC-721E Token Standard	Bitcoin	2023
Rune	Rune Issuance Tool	Bitcoin	2023
RGB	RGB Blueprint: Scalable & Confidential Smart Contracts	Bitcoin	2023
ARC-20	ARC-20 Tokens - Atomicals Guidebook	Bitcoin	2023
DRC-20	DRC-20 Standard	Bitcoin	2023
Ethscriptions	Introducing Ethscriptions	Ethereum	2023
ASC-20	Overview - ASC-20 AVAX Market	Avalanche	2023
BSC-20	Understanding BNB Chain Inscriptions	BSC	2023
PRC-20	PRC-20 Contract	Polygon	2023
AtomicAsset	AtomicAssets Smart Contract Repository	EOS	2023
SPL-20	Unlocking the Future: Inscriptions on Solana	Solana	2023
MRC-20	What’s Going On With MOVE: Smart Inscription (MRC20)	Move	2023
APT-20	APT-20 Protocol	Aptos	2023

**Conclusion.** In this paper, we present an exploration of Bitcoin inscriptions, dissecting their technological roots. We compare Bitcoin inscriptions with traditional NFTs, revealing unique characteristics and broad use cases. Despite several challenges, we still highlight significant opportunities provided by Bitcoin inscriptions, especially for derivative protocols, Layer2 solutions, and interoperability techniques.



## REFERENCES

- [1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
- [2] Qin Wang, Rujia Li, et al. Exploring Web3 from the view of blockchain. *arXiv preprint arXiv:2206.08821*, 2022.
- [3] Vitalik Buterin. Ethereum white paper. <https://ethereum.org/en/whitepaper/>, 2013.
- [4] Binance. Binance smart chain: Whitepaper. <https://research.binance.com/en/projects/binance-smart-chain>, 2020.
- [5] Anatoly Yakovenko. Solana: A new architecture for a high-performance blockchain v0.8.13. <https://solana.com/solana-whitepaper.pdf>, 2018.
- [6] CoinDesk. Bitcoin price — BTC price index and live chart. <https://www.coindesk.com/price/bitcoin/>, 2024. Accessed: January 16, 2024.
- [7] Ordinal Protocol. Ordinal protocol documentation, 2023. Accessed: January 16, 2024.
- [8] Qin Wang et al. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*, 2021.
- [9] Glassnode. BTC: Ordinals and inscriptions - glassnode studio. [https://studio.glassnode.com/dashboards/4d64f74b-fdb5-4487-4f86-08d193e34ed0?referrer=use\\_case](https://studio.glassnode.com/dashboards/4d64f74b-fdb5-4487-4f86-08d193e34ed0?referrer=use_case), 2024. Accessed: January 16, 2024.
- [10] Qaiser Razi, Aryan Devrani, Harshal Abhyankar, GSS Chalapathi, Vikas Hassija, and Mohsen Guizani. Non-fungible tokens (NFTs)-survey of current applications, evolution and future directions. *IEEE Open Journal of the Communications Society*, 2023.
- [11] Qin Wang and Guangsheng Yu. Understanding BRC-20: Hope or hype. Available at SSRN 4590451, 2023.
- [12] Louis Bertucci. Bitcoin Ordinals: Determinants and impact on total transaction fees. Available at SSRN 4486127, 2023.
- [13] Guangsheng Yu et al. Bridging BRC-20 to Ethereum. *arXiv preprint arXiv:2310.10065*, 2023.
- [14] Mehmet Sabir Kiraz, Enrique Larraia, and Owen Vaughan. NFT trades in Bitcoin with off-chain receipts. *Cryptology ePrint Archive*, 2023.
- [15] Pieter Wuille et al. BIP-141: Segregated witness (consensus layer). <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>, 2017. Accessed: January 16, 2024.
- [16] Amritraj Singh, Reza M Parizi, Meng Han, Ali Dehghantanha, Hadis Karimipour, and Kim-Kwang Raymond Choo. Public blockchains scalability: An examination of sharding and segregated witness. *Blockchain Cybersecurity, Trust and Privacy*, pages 203–232, 2020.
- [17] Pieter Wuille, Jonas Nick, and Tim Ruffing. BIP-340: Schnorr signatures for secp256k1. <https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki>, 2020. Accessed: January 16, 2024.
- [18] Gregory Neven, Nigel P Smart, and Bogdan Warinschi. Hash function requirements for schnorr signatures. *Journal of Mathematical Cryptology*, 3(1):69–87, 2009.
- [19] Bitcoin Community. BIP 341: Taproot. <https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki>, 2021. Accessed: January 16, 2024.
- [20] Bitcoin Community. BIP 342: Tapscript. <https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki>, 2021. Accessed: January 16, 2024.
- [21] Ordinal Theory Authors. Ordinal theory handbook. <https://docs.ordinals.com/>, 2024. Accessed: January 16, 2024.
- [22] Yakov Shafranovich. Common format and MIME type for comma-separated values (CSV) files. Technical report, 2005.
- [23] Pieter Wuille, Jonas Nick, and Anthony Towns. BIP-341: Taproot: Segwit version 1 spending rules. <https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki>, 2020. Accessed: January 16, 2024.
- [24] Ethereum Community. ERC-721: Non-fungible token standard. <https://eips.ethereum.org/EIPS/eip-721>, 2018. Accessed: January 16, 2024.
- [25] Ethereum Community. ERC-1155: Multi token standard. <https://eips.ethereum.org/EIPS/eip-1155>, 2018. Accessed: January 16, 2024.
- [26] Juan Benet. IPFS - content addressed, versioned, P2P file system. <https://arxiv.org/abs/1407.3561>, 2014. Accessed: January 16, 2024.
- [27] Arweave Team. Arweave whitepaper. <https://whitepaper.io/document/627/arweave-whitepaper>, 2018. Accessed: January 16, 2024.
- [28] Domo. BRC-20 experiment. <https://domo-2.gitbook.io/brc-20-experiment/>, 2023. Accessed: January 16, 2024.
- [29] Ethereum Community. ERC-20: Token standard. <https://eips.ethereum.org/EIPS/eip-20>, 2015. Accessed: January 26, 2024.
- [30] Crypto.com. Ordinals price — ORD price, USD converter, Charts — Crypto.com. <https://crypto.com/price/ordinals>, 2023.
- [31] Imran Yousaf, Linh Pham, and John W Goodell. The connectedness between meme tokens, meme stocks, and other asset classes: Evidence from a quantile connectedness approach. *Journal of International Financial Markets, Institutions and Money*, 82:101694, 2023.
- [32] Cointelegraph. Why are Bitcoin Ordinal inscription tokens ORD, SATS crashing? <https://cointelegraph.com/news/why-are-bitcoin-ordinal-inscription-tokens-ordi-sats-crashing>, 2024. Accessed: January 16, 2024.
- [33] Magic Eden. Bitcoin Punks on Magic Eden, 2023. Accessed: January 16, 2024.
- [34] Larva Labs. Cryptopunks, 2023. Accessed: January 16, 2024.
- [35] Ana Maria Caballero. Bitcoin Ordinals inscription marks first individual poem sale by Sotheby's. *Decrypt.co*, 2024.
- [36] Ninjalerts. Bitcoin Ordinals Pizza Ninjas, 2023. Accessed: January 16, 2024.
- [37] MD Soharab Hossain Sohan, Minhaz Mahmud, MA Baten Sikder, Fakir Sharif Hossain, and Md Rakibul Hasan. Increasing throughput and reducing storage bloating problem using IPFS and dual-blockchain method. In *International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pages 732–736. IEEE, 2021.
- [38] Erya Jiang, Bo Qin, et al. Decentralized finance (DeFi): A survey. *arXiv preprint arXiv:2308.05282*, 2023.
- [39] National Vulnerability Database. CVE-2023-50428: Vulnerability in Bitcoin Core and Bitcoin knots. <https://nvd.nist.gov/vuln/detail/CVE-2023-50428>, 2023. Accessed: January 16, 2024.
- [40] GoPlus Security. GoPlus security reminder: Beware of inscription scams. <https://goplussecurity.medium.com/goplus-security-reminder-beware-of-inscription-scams-13eb5cf7d066>, December 2023. Accessed: January 16, 2024.
- [41] Gamma. Gamma — find & buy Bitcoin Ordinals and NFTs. <https://gamma.io/>, 2023. Accessed: January 16, 2024.
- [42] Ordinals Wallet Team. Ordinals wallet. <https://ordinalswallet.com/>, 2023. Accessed: January 16, 2024.
- [43] UniSat Wallet Team. UniSat wallet. <https://unisat.io/>, 2023. Accessed: January 16, 2024.
- [44] Magic Eden. Magic eden - NFT marketplace. <https://magiceden.io/>, 2023. Accessed: January 16, 2024.
- [45] David Easley, Maureen O'Hara, and Soumya Basu. From mining to markets: The evolution of Bitcoin transaction fees. *Journal of Financial Economics*, 134(1):91–109, 2019.
- [46] Atomicals Team. ARC20 tokens - atomicals guidebook. <https://docs.atomicals.xyz/arc20-tokens>, 2023. Accessed: January 16, 2024.
- [47] Realm Team. Realm - the people's Metaverse. <https://www.realm.art/>, 2023. Accessed: January 16, 2024.
- [48] Luminex. Luminex introduces Rune issuance tool: Seamless effortless rune token creation on Bitcoin. <https://www.blog.luminex.io/luminex-introduces-rune-issuance-tool-seamless-effortless-rune-token-creation-on-bitcoin/>, 2023. Accessed: January 16, 2024.
- [49] RGB Team. RGB blueprint: Scalable & confidential smart contracts for Bitcoin & Lightning Network. <https://rgb-org.github.io/>, 2023. Accessed: January 16, 2024.
- [50] DRC-20 Development Team. DRC-20 standard. <https://docs.drc-20.org/>, 2023. Accessed: January 16, 2024.
- [51] Etherscriptions Team. Introducing etherscriptions. <https://docs.etherscriptions.com/overview/introducing-etherscriptions>, 2023. Accessed: January 16, 2024.
- [52] ASC-20 AVAX MARKET Team. Overview - ASC-20 AVAX market. <https://docs.avaxmarket.xyz/introduction/overview>, 2023. Accessed: January 16, 2024.
- [53] Gate Learn. Understanding BNB chain inscriptions: BRC-20, BSC-20, BNBS-20 explained. <https://www.gate.io/learn/articles/understanding-bnb-chain-inscriptions/1473>, 2023. Accessed: January 16, 2024.
- [54] PlatON Team. PRC-20 contract. [https://platonnetwork.github.io/docs/en/PRC20\\_contract/](https://platonnetwork.github.io/docs/en/PRC20_contract/), 2023. Accessed: January 16, 2024.
- [55] Magic Eden. Unlocking the future: Inscriptions on Solana. <https://help.magiceden.io/en/articles/8615097-unlocking-the-future-inscriptions-on-solana>, 2023. Accessed: January 16, 2024.
- [56] SFNs Team. SFNs inscription launches on DefiBOX: Conversion tutorial. <https://sfns.notion.site/sfns/SFNs-Inscription-Launches-on-DefiBOX-Conversion-Tutorial-7791aa315c584a5bae3e7848623eb491>, 2023. Accessed: January 16, 2024.
- [57] Pink Network X. Atomicassets smart contract repository. <https://github.com/pinknetworkx/atomicassets-contract>, 2023.
- [58] CoinLive. What's going on with MOVE: Smart inscription (MRC20). <https://www.coinlive.com/news/what-s-going-on-with-move-smart-inscription-mrc20>, 2023. Accessed: January 16, 2024.
- [59] APT-20 Development Team. APT-20 protocol. <https://apt-20.com/>, 2023. Accessed: January 16, 2024.

- [60] Cosimo Sguanci, Roberto Spatafora, and Andrea Mario Vergani. Layer2 blockchain scaling: A survey. *arXiv preprint arXiv:2107.10881*, 2021.
- [61] Ray Neiheiser, Gustavo Inácio, Luciana Rech, Carlos Montez, Miguel Matos, and Luís Rodrigues. Practical limitations of Ethereum’s Layer2. *IEEE Access*, 11:8651–8662, 2023.
- [62] Louis Tremblay Thibault, Tom Sarry, and Abdelhakim Senhaji Hafid. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access*, 2022.
- [63] Patrick McCorry, Chris Buckland, Bennet Yee, and Dawn Song. SoK: Validating bridges as a scaling solution for blockchains. *Cryptology ePrint Archive*, 2021.
- [64] Sergio Demian Lerner. Rsk. *RootStock Core Team, White Paper*, 2015.
- [65] Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. SoK: Layer-two blockchain protocols. In *International Conference on Financial Cryptography and Data Security (FC)*, pages 201–226. Springer, 2020.
- [66] CoinTelegraph. The state of the Bitcoin lightning network in 2023. <https://cointelegraph.com/news/the-state-of-the-bitcoin-lightning-network-in-2023>, 2023. Accessed: January 16, 2024.
- [67] Joseph Poon and Thaddeus Dryja. The Bitcoin lightning network: Scalable off-chain instant payments. 2016.
- [68] Lightning Labs. Taproot assets - the builder’s guide to the LND galaxy. <https://docs.lightning.engineering/the-lightning-network/taproot-assets>, 2023. Accessed: January 16, 2024.
- [69] Gang Wang, Qin Wang, and Shipping Chen. Exploring blockchains interoperability: A systematic survey. *ACM Computing Surveys*, 2023.
- [70] Maticz. BRC-721E token standard. <https://maticz.com/brc-721e-token-standard>, 2023. Accessed: January 16, 2024.
- [71] MultiBit Exchange. Multibit documentation. <https://docs.multibit.exchange/multibit/>, 2023. Accessed: January 16, 2024.
- [72] TeleportDAO. TeleportDAO documentation. <https://docs.teleportdao.xyz/teleportdao/introduction>, 2023. Accessed: January 16, 2024.
- [73] SoBitBridge. SoBit: Bridging BRC-20 and Solana. *Medium*, 2023.
- [74] Allins. Allins: Swap, trade and earn effortlessly on the leading multi-chain inscription amm, 2023. Accessed: January 16, 2024.
- [75] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. *ACM Computing Surveys*, 55(11):1–50, 2023.
- [76] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 1:36–63, 2001.
- [77] Anubha Jain and Emmanuel S Pilli. SoK: Digital signatures and Taproot transactions in Bitcoin. In *International Conference on Information Systems Security*, pages 360–379. Springer, 2023.
- [78] Bitcoin Community. BIP 114: Merkelized Abstract Syntax Tree. <https://bips.xyz/114>, 2016. Accessed: January 16, 2024.
- [79] Harry A Kalodner, Miles Carlsten, Paul M Ellenbogen, Joseph Bonneau, and Arvind Narayanan. An empirical study of namecoin and lessons for decentralized namespace design. In *WEIS*, pages 1–23, 2015.
- [80] Meni Rosenfeld et al. Overview of colored coins. *White Paper, Bitcoin. co. il*, 41:94, 2012.
- [81] Counterparty. Counterparty - pioneering peer-to-peer finance. <https://counterparty.io/>, 2014. Accessed: January 16, 2024.
- [82] Spells of Genesis Team. Spells of genesis. <https://spellsofgenesis.com/>, 2015. Accessed: January 26, 2024.
- [83] Rare Pepes Team. Rare Pepes NFT tools & community. <https://rarepepes.com/>, 2016. Accessed: January 26, 2024.

## APPENDIX A

### TECHNOLOGICAL UNDERPINNINGS SUPPLEMENTARY

#### A. Segregated Witness

The Bitcoin network consistently verifies a new block approximately every 10 to 15 minutes, with each block encompassing a specific number of transactions [1]. Consequently, the size of these blocks directly influences the number of transactions that can be confirmed within each block. Segregated Witness, commonly known as SegWit, represents one of the key protocol upgrades [15] addressing scalability and transaction malleability issues.

Before SegWit, Bitcoin transactions included a component called the *signature* data within the transaction structure. This data, crucial for the verification of transactions, contributed to two primary issues: scalability and transaction malleability. Specifically, each Bitcoin block has a size limit (originally set to 1MB), which constrains the number of transactions that can be processed in each block. The inclusion of signature data within transactions consumed significant space, limiting the overall transaction throughput of the network. In addition, the transaction ID (txid) was generated by hashing the entire transaction data, including the signature. Since signatures could be altered without invalidating the transaction, the txid could also be changed, leading to potential issues in tracking and confirming transactions.

SegWit can bring advantages for Bitcoin inscriptions:

- *Increased inscription transactions*: SegWit increases the number of transactions that can fit into a block by changing how data is counted towards the block size limit. This indirectly benefits Bitcoin inscriptions by allowing more space for these types of transactions, which can sometimes be data-heavy.
- *Enhanced transaction efficiency*: By optimizing the space within each block, SegWit makes the Bitcoin network more efficient. This efficiency can be beneficial for Bitcoin inscriptions, as it potentially leads to faster confirmation times and lower fees.
- *Enhanced transaction security*: For Bitcoin inscriptions, which may rely on unaltered transaction IDs for their operation, SegWit ensures that the modification of the signature part does not affect the transaction ID. It is crucial for maintaining the integrity of inscription transaction references.

#### B. Schnorr Signature

The Schnorr signature scheme was proposed by Bitcoin core developer Pieter Wuille via Bitcoin Improvement Proposal (BIP)-340 [17] in January 2020. The proposal includes the Taproot/Schnorr soft fork upgrade [23] to replace the Elliptic Curve Digital Signature Algorithm (ECDSA) [76] employed in Bitcoin’s digital signature mechanism. The details of the signing and validation are as follows.

*Signing procedure.* Signing (Algorithm 2) is responsible for creating a digital signature for a given message. It starts by selecting a random nonce  $k$  from  $\mathbb{Z}_n^*$ . This nonce is a random number that ensures the uniqueness of each signature, even for repeated signings of the same message. The algorithm computes a point  $R$  on the elliptic curve by multiplying  $k$  with the generator point  $G$ . Subsequently, it calculates a hash value  $e$  using a cryptographic hash function, taking as input the concatenation of  $R$ , the public key  $Q$ , and the message  $m$ . The signature component  $s$  is then computed as  $(k - e \cdot d) \bmod n$ , where  $d$  is the private key. The resulting signature for the message  $m$  is the pair  $(R, s)$ .

*Signature validation.* Verification (Algorithm 3) determines the validity of a given signature for a message. It requires the public key  $Q$ , the message  $m$ , and the signature  $(R, s)$  as



---

**Algorithm 2** Signing

---

**Require:** Private key  $d$ , message  $m$

**Ensure:** Signature  $(R, s)$

- 1:  $k \leftarrow$  randomly choose from  $\mathbb{Z}_n^*$
  - 2:  $R \leftarrow k \cdot G$
  - 3:  $e \leftarrow \text{Hash}(R \parallel Q \parallel m)$
  - 4:  $s \leftarrow (k - e \cdot d) \bmod n$
  - 5: **return**  $(R, s)$
- 

inputs. The algorithm first computes the hash value  $e$  similarly to the signing algorithm. It then calculates a verification point  $V$  on the elliptic curve, which is the sum of  $s \cdot G$  and  $e \cdot Q$ . The signature is deemed valid if and only if this verification point  $V$  equals the point  $R$  in the signature. If  $V = R$ , the algorithm returns *True*, indicating the signature is valid. Otherwise, it returns *False*, indicating the signature is invalid.

---

**Algorithm 3** Verification

---

**Require:** Public key  $Q$ , message  $m$ , signature  $(R, s)$

**Ensure:** Validation result

- 1:  $e \leftarrow \text{Hash}(R \parallel Q \parallel m)$
  - 2:  $V \leftarrow (s \cdot G) + (e \cdot Q)$
  - 3: **if**  $V = R$  **then**
  - 4:     **return** *True* {The signature is valid}
  - 5: **else**
  - 6:     **return** *False* {The signature is invalid}
  - 7: **end if**
- 

Employing Schnorr signatures is particularly important to Bitcoin inscription technology for several reasons that align well with the cryptocurrency’s goals of security, efficiency, and privacy. Here are the key reasons:

- *Efficient data embedding:* Schnorr signatures, known for their efficiency in terms of size, enable more data to be embedded within a transaction while minimizing the space it occupies on the blockchain [77]. This efficiency is crucial for inscription technology, which involves embedding additional data (like digital artifacts) on the blockchain. The compact nature of Schnorr signatures allows for more inscriptions without significantly increasing the size of the blockchain.
- *Enhanced privacy:* Inscriptions can potentially expose more transaction details. Schnorr signatures help mitigate privacy concerns by making multi-signature transactions indistinguishable from single-signature ones. This feature is vital to maintaining user privacy, especially when inscriptions involve multiple parties.
- *Scalability and throughput:* The reduced size and increased efficiency of Schnorr signatures directly contribute to Bitcoin’s scalability. By allowing more transactions (and thus more inscriptions) to be included in each block, Schnorr signatures can improve the overall throughput of the Bitcoin network. This is particularly important as the volume of transactions, including those

with inscriptions, continues to grow.

- *Flexibility for complex transactions:* Schnorr signatures offer greater flexibility for complex transactions, which is beneficial for advanced inscription use cases. They enable sophisticated scripting possibilities, which can be used to create more intricate types of inscriptions and digital artifacts on Bitcoin.

### C. Taproot and Tapscript

BIP-341 [19], commonly known as Taproot, is an enhancement to BIP-340. The core idea is to combine the strengths of *Merkelized abstract syntax trees* MAST [78] and *Schnorr signatures* by committing a single Schnorr public key in the output that can represent both a single public key spend and a complex script spend. It introduces a new Taproot output (SegWit version 1) that includes a signature, a control block, and a script path. Moreover, it also specifies the rules for spending the Taproot output, which can be either a key-path spend (using a single signature) or a script-path spend (using the scripts committed to in the MAST structure). It achieves privacy and efficiency by allowing users to mask complex smart contracts as standard single-signature transactions.

Tapscript proposed in BIP-342 [20] introduces improvements to the Bitcoin scripting language, particularly focusing on the integration of Schnorr signatures and used for Taproot script-path spends. The primary motivation behind BIP-342 is to address certain limitations within the existing Bitcoin scripting system, especially in terms of compatibility with the semantics of certain opcodes. BIP-342 modifies the signature opcodes OP\_CHECKSIG and OP\_CHECKSIGVERIFY to verify Schnorr signatures as specified in BIP-340. It presents a new opcode, OP\_CHECKSIGADD, which facilitates the establishment of multi-signature policies that can be verified in batches. This enhancement significantly boosts the efficiency and scalability of transactions involving multiple signatures.

### D. Ordinal Theory

**Numbering scheme for satoshis.** Ordinal numbers can be represented in several distinct formats [21]. Taking Inscription #34,595,802 as a case in point.

- *Integer notation:* The ordinal number assigned according to the order in which the satoshi was mined. E.g., 1938930000000000.
- *Decimal notation:* Combines the block height at which the satoshi was mined with the offset of the satoshi within the block. E.g., 792288.0.
- *Degree notation:* A unique representation that makes the rarity of a satoshi easy to see at a glance. E.g., 0°162288'0''0'''.
- *Percentile notation:* The satoshi’s position in Bitcoin’s supply is expressed as a percentage. E.g., 92.33000010156304%.
- *Name:* An encoding of the ordinal number using characters a through z. E.g., acqgzfkezav.

**Rarity system.** Ordinal Theory introduces a system of rarity based on periodic events in Bitcoin, such as blocks, difficulty

adjustments, halvings, and cycles. This system categorizes satoxis into different rarity levels like common, uncommon, rare, epic, legendary, and mythic [21].

Bitcoin experiences regular events that vary in frequency, creating a natural framework for categorizing rarity, including:

- *Blocks*: New blocks are mined about every 10 minutes.
- *Difficulty adjustments*: Occurring every 2016 blocks or roughly every two weeks. The network adjusts the difficulty level required for block acceptance in response to hash rate fluctuations.
- *Halvings*: Approximately every four years, or every 210,000 blocks, the number of new satoxis generated per block is halved.
- *Cycles*: A special event, known as a conjunction, happens every six halvings, approximately every 24 years<sup>1</sup>, where halvings and difficulty adjustments align. The period between these conjunctions is termed a cycle, with the next one anticipated around 2032.

Based on these events, satoxis can be classified into different levels of rarity:

- *Common*: Any satoshi that isn't the first in its block.
- *Uncommon*: The first satoshi in each block.
- *Rare*: The first satoshi in each difficulty adjustment period.
- *Epic*: The first satoshi in each halving epoch.
- *Legendary*: The first satoshi in each cycle.
- *Mythic*: The very first satoshi from the genesis block.

For example, Inscription [#34,595,802](#) is rare. We can use degree notation to highlight the rarity straightforwardly.

$$1^{\circ}1'0''0'''$$

1°	Second <i>cycle</i>
1'	Not the first block in <i>halving epoch</i>
0''	First block in difficulty <i>adjustment period</i>
0'''	First sat in <i>block</i>

Overall, the Ordinal theory allows for the creation of unique, non-fungible assets directly on the Bitcoin blockchain. By assigning distinct identities to individual satoxis, it becomes possible to attach specific data or digital artifacts to these satoxis, effectively turning them into unique digital assets. Additionally, each satoshi can be tracked through its transaction history. This level of traceability is crucial for establishing the provenance and ownership history of inscribed assets.

## APPENDIX B BITCOIN INSCRIPTIONS

**Historical Overview.** Bitcoin (2009) laid the groundwork for blockchain technology, but initially, it was focused on cryptocurrency rather than NFTs. Namecoin in 2011 [79] was a pioneering project that forked from Bitcoin. It focused on using blockchain technology for decentralized domain name

registration, representing an early exploration of blockchain's potential beyond currency. Its limitations included limited adoption and being overshadowed by Bitcoin's growth.

Table II: Historical Overview of Bitcoin Inscriptions

Year	Milestone	Description	Limitations
2011	Namecoin	Early fork of Bitcoin for decentralized domain name registration.	Limited adoption and overshadowed by Bitcoin's growth.
2012	Colored Coins	Early asset representation method on Bitcoin.	Inefficient, capacity constraints.
2014	Counterparty	Platform for Bitcoin-based unique tokens.	Bitcoin's transaction speed and fee limitations.
2015	Spells of Genesis	Blockchain game using Counterparty for assets.	Limited mainstream adoption, platform constraints.
2016	Rare Pepe	Digital assets based on Pepe meme via Counterparty.	Niche appeal, technical limitations.
2023	Bitcoin Ordinals	Advancements for digital artifacts on Bitcoin.	Network congestion, content permanence issues.

One of the earliest concepts related to NFTs on Bitcoin was "Colored Coins" [80] in 2012. Colored Coins implemented a method known as "metadata injection" to incorporate additional metadata. This process utilized the scriptSig field within a transaction's input script. However, this approach was inefficient and faced limitations because it was not designed for storing extensive metadata, leading to scalability issues.

In 2014, Counterparty [81] emerged as a significant development, building on the Bitcoin blockchain to enable the creation of unique tokens and digital assets. This platform expanded the possibilities for asset representation and transfer on Bitcoin. However, it was limited by Bitcoin's transaction speed and fee structure. The reliance on Bitcoin's blockchain meant that Counterparty transactions were subject to the same congestion and high fees during peak times. Spells of Genesis [82] proposed in 2015, one of the first games to integrate blockchain technology, utilized Counterparty to create in-game assets as tradable tokens. While it represented a novel blend of gaming and blockchain, the game's dependence on the Counterparty platform inherited its limitations.

In 2016, Rare Pepe [83] brought a unique cultural twist to blockchain tokens. Using Counterparty, it allowed the creation and trading of digital assets based on the popular Pepe the Frog meme, showcasing the diverse potential of blockchain assets. However, it was constrained by the niche appeal of its meme-based assets and the technical limitations of the Counterparty platform. The project's success was more within the crypto community than in broader markets. More recently, the concept of Bitcoin NFTs has seen a resurgence with the introduction of Bitcoin Ordinals [21]. This approach involves assigning unique ordinal numbers to individual satoxis, enabling them to be used as distinct, trackable assets akin to

<sup>1</sup>The LCM is the smallest number that is a multiple of 2016 and 210,000.:

$$1260,000 = \text{LCM}(2016, 210,000)$$

NFTs. This has opened up new possibilities for creating and trading digital artifacts directly on the Bitcoin blockchain. Despite this, Bitcoin NFTs are still in their nascent stages. Challenges include potential network congestion due to increased data from inscriptions and the permanence of content issues (more discussions refer to Sec.IV).

Table III: Bitcoin Inscriptions vs. NFTs on Other Blockchains

Aspect	Bitcoin Inscriptions	Other NFTs
<b>Description Method</b>	Digital Asset, Inscription, Ordinal	NFT
<b>Protocol Form</b>	Ordinal Protocol	ERC-721, ERC-1155, etc
<b>Storage Method</b>	Entirely stored on-chain	Stored on IPFS or Arweave, not 100% on-chain
<b>Immutability</b>	Inherent	Variable
<b>Minting</b>	Not possible without a node, only via third-party services	Mostly can directly interact with the webpage
<b>Trading Method</b>	NFT Marketplace	NFT Marketplace
<b>Scarcity</b>	Limited by Bitcoin usage	Potentially less scarce
<b>Royalty Models</b>	None	Common, with challenges
<b>Integration</b>	Difficult due to Bitcoin's scripting limitations	Easier due to programmable smart contracts
<b>Energy Consumption</b>	High due to Proof of Work consensus	Depends on the consensus algorithm of the platform
<b>Advantages</b>	Scarcity, characteristics of luxury goods	Mainstream NFT mode, high user base
<b>Disadvantages</b>	1. Slow block speed, not suitable for bulk minting. 2. Difficulties in minting and trading. 3. Complex wallet entry	No special gimmicks or fame, easily overlooked

**BRC-20.** BRC-20 requires users to fill in various parts according to a standardized JSON format, with the specifications as:

- *'p': protocol type.* This is a mandatory keyword that defines the operation, helping other systems identify and process BRC-20 events.
- *'op': event type.* This is a mandatory keyword that defines the type of event, whether it's deploy, mint, or transfer. For example, the content of 'op' as 'transfer' means the event type is a transfer.
- *'tick': BRC-20 token identifier.* This is a mandatory keyword that defines the name (4 letters) of the BRC-20 token. In this case, the content of 'tick' as 'ORDI' means the BRC-20 token being transferred is \$ORDI.
- *'amt': the amount of BRC-20 token being transferred.* This is a mandatory keyword that defines how many BRC-20 tokens will be transferred.














- *'max': maximum supply.* This is a mandatory keyword that defines the maximum supply of the BRC-20 token.
- *'lim': the maximum number of BRC-20 tokens that a single inscription can accommodate.* This is an optional keyword that defines how many BRC-20 tokens a user can obtain from minting a single inscription. If set to 1000, minting a single inscription can obtain a maximum of 1000 BRC-20 tokens.

## APPENDIX C

### SUMMARISED TABLES FOR QUICK REFERENCE

We present Table III that outlines the fundamental differences, Table IV that details existing derivative protocols, and Table I compiling a list of Bitcoin-related standards discussed in this paper, providing a quick reference for readers.

Table IV: Inscription Derivative Protocols

Icon	Protocol	Chain	Feature Description
	BRC20 [28]	BTC	First Bitcoin-based inscription protocol
	ARC20 [46]	BTC	Removes the four-character limit
	Rune [48]	BTC	Embeds token data in Bitcoin's UTXO
	RGB [49]	BTC	Converts smart contract states into concise proofs
	DRC20 [50]	Doge	Similar to BRC-20, popular for low costs
	Etherscription [51]	ETH	Introduces "dumb contracts"
	ASC20 [52]	Avax	EVM-compatible chain protocol
	BSC20 [53]	BSC	EVM-compatible chain protocol
	PRC20 [54]	Polygon	EVM-compatible chain protocol
	AtomicAsset [57]	EOS	Efficient and powerful feature sets
	SPL20 [55]	Solana	NFTs with indexing based on file hashes
	MRC20 [58]	Move	User-friendly approach to token management
	APT20 [59]	Aptos	Based on Ordinals protocol