

BRC-20 TOKENS:

EXPLORING THE NEW ERA OF BITCOIN

September **2023**

CONTENTS

A Brief History of BRC-20	3
What is the difference between Ethereum's NFT and Ordinals?	4
Why the BRC-20 token standard was proposed:	5
Explanation of BRC-20	5
Differences and similarities between BRC-20 and ERC-20	7
Stakeholders in the BRC-20 Ecosystem Development	7
The main concerns about Ordinals and BRC-20	9
The Inevitable Momentum of BRC-20	10
BRC-20 in the Current Crypto Market	12
The Meme Movement	12
Market analysis of BRC-20	13
Ecosystem mapping	16
Exchange	16
Centralized Exchanges (CEX)	16
Decentralized Exchanges (DEX)	17
BRC-20 indexer	19
Decentralized Indexer - Trac	19
Wallet	21
Bitcoin Scaling Solution	23
On-chain Scaling	23
Off-chain State Channels	25
Layer 2 Solutions	27
Bitcoin DeFi Protocols	30
Bitcoin Cross-chain Bridge	30
Market Headwinds	31
Market tailwinds	33
Conclusion	34

A Brief History of BRC-20

Satoshi

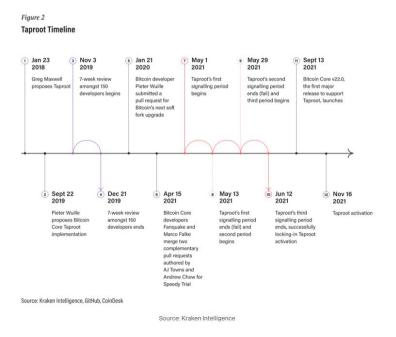
The smallest unit of Bitcoin is called a Satoshi. There are 100 million Satoshis in one Bitcoin. Satoshis act as the new carrier for BRC-20 tokens, allowing each Satoshi to be embedded with unique data inscriptions. Individual Satoshi's can now be bought, sold or traded.

SegWit (Segregated Witness)

Taproot and SegWit are technical upgrades to the Bitcoin network. These technical upgrades refer to modifications made to the Bitcoin consensus mechanism code.

SegWit reduces the impact of each transaction on block size, indirectly increasing the network's capacity. Taproot, building upon SegWit, standardizes data requirements for all transactions, enhancing privacy and efficiency, removing the size limit of witness data. It allows for inscriptions up to 4MB in size using Taproot scripts.

Together, they provide the technical feasibility for the emergence of BRC-20 by allowing more data to be attached to Bitcoin's block space.



Source: https://argoblockchain.com/articles/bitcoin-taproot-upgrade-explained

Ordinals

In early 2023, Bitcoin core contributor Casey Rodarmor released the Ordinals protocol.

Ordinals protocol refers to a scheme that assigns a unique number to every Satoshi (the smallest unit of Bitcoin) based on the order they were mined.

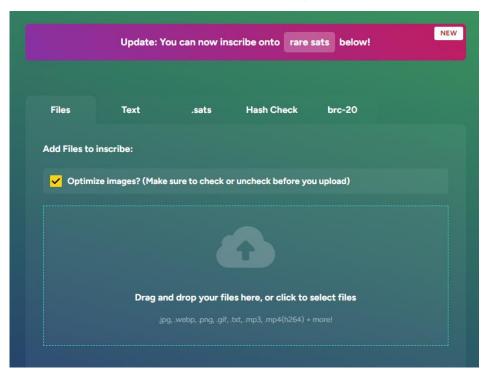
Once these satoshis are numbered and identified, users can inscribe the Satoshi with any arbitrary data they would like and upload it to the blockchain. This is equivalent to giving Bitcoin the native ability to create non-fungible tokens (NFTs).

Inscriptions

Inscriptions can contain various forms of information, including text, images, and videos less than 4MB.

This means that an individual Satoshi can be inscribed with any content, creating a unique Bitcoin-native digital artifact. Notably, BTC NFT collectibles include Bitcoin Frogs, Ordinal Punks, TwelveFold. According to the Ordinal Punks Sales bot on Twitter, an Ordinal Punk that was minted for 0.01 BTC was once sold for as much as 9.5 bitcoins, valued at over \$240,000.

You can visit ordinalsbot to upload (shown below) the images, videos, and other files you wish to inscribe onto an Ordinal. The whole process takes about 30-60 minutes.



Source:https://ordinalsbot.com/

What is the difference between Ethereum's NFT and Ordinals?

Nature of NFTs:

Ethereum's NFTs are unique digital assets in themselves, akin to a one-of-a-kind artwork or piece of writing.

Bitcoin's NFTs are created by attaching unique data to individual Satoshis, the smallest unit of Bitcoin.

Value Retention:

While Ethereum's NFTs can potentially become worthless if no one desires them, Bitcoin's NFTs will always retain value due to the inherent value of the underlying Satoshi. This Satoshi can also be used for network transaction fees.

Data Storage:

Unlike NFT systems built on smart contracts like Ethereum, all data inscribed with Ordinals is stored on-chain.

It does not rely on external storage like IPFS or AWS S3.

It's truly decentralized with high security and preserved on the benchmark blockchain like all Bitcoin transactions.

Why the BRC-20 token standard was proposed:

Since the Ordinals protocol can create Bitcoin NFTs by assigning different "attributes" to each Satoshi, it is also possible to create Bitcoin FTs, or fungible tokens, by specifying a uniform "format" and "attributes".

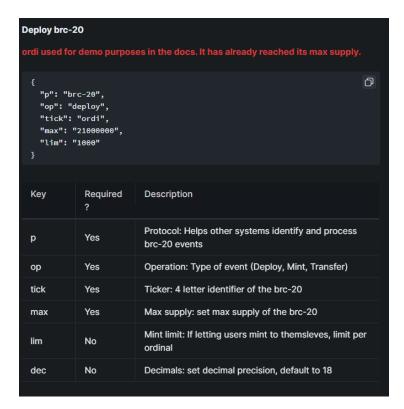
Recognizing this potential opportunity, domo@domodata proposed the BRC-20 standard, drawing inspiration from Ethereum's ERC-20 token standard. The BRC-20 standard provides a clear set of guidelines and protocols for creating, transferring, and managing Ordinal tokens on the Bitcoin network.

Explanation of BRC-20

BRC-20

BRC-20 tokens embed JavaScript Object Notation (JSON) into ordinal inscription to define and initialize token smart contract functionality. Hence, allowing users to deploy, mint, and transfer tokens on the Bitcoin network.

Key aspects of deployment include token name, total supply, and maximum minting amount per instance.



Source:https://docs.ordinals.com/inscriptions.html

Bitcoin network's experimental fungible token protocol, BRC-20, made its debut, and the first BRC-20 token - \$ordi was issued, with a total supply of 21 million (in homage to BTC). It was available on a first-come, first-served basis, for anyone to mint for free minus fees. All tokens were minted within 18 hours of deployment.

 Unlike ERC-20 tokens, BRC-20 tokens' ownership status is maintained offchain

Unlike ERC-20 tokens, whose ownership status is stored directly on the Ethereum blockchain, BRC-20 tokens' ownership status is maintained by indexers.

Why do we need indexers? If an inscription is merely a text document, what stops a bad actor from trying to deploy and mint \$ORDI once more?

This underscores the pivotal role of indexers in the BRC20 framework. If there's no on-chain mechanism generating an error on an already in use alert, then the responsibility falls on the BRC20 marketplace's indexer to discern whether \$ORDI is genuine or an imitation.

This necessitates a database designed to "read" and log all BRC20 transactional data to identify which inscription first "deployed" a fresh token label. The indexer has the duty to monitor which wallets produced the initial token batch up to its upper limit, pinpoint where the minting was halted, and verify if tokens being "moved" in the aftermarket can be linked back to these original wallets.

Without indexers a BRC20 market isn't possible, there's just the chaos of nearly indistinguishable text files.

```
{
    "p": "brc-20",
    "op": "deploy",
    "tick": "ordi",
    "max": "21000000",
    "lim": "1000"
}
```

Source:https://docs.ordinals.com/inscriptions.html

Currently, the existing trackers for these metaprotocols(eg. BRC20) are heavily centralized, which goes against the decentralized nature of cryptocurrencies like Bitcoin. **Trac solves this problem by providing a decentralized network** that allows anyone to connect, utilize, and earn from it. It is believed that Trac has 12 decentralized indexers at the moment. And we will explain further in the content below.

Differences and similarities between BRC-20 and ERC-20

Difference

Storage Mechanism: While both ERC-20 and BRC-20 token statuses are stored onchain, the way they are stored differs. ERC-20 tokens use Ethereum's smart contracts to record and manage token balances directly on the Ethereum blockchain. In contrast, BRC-20 tokens utilize the Ordinals protocol and JSON format inscriptions on the Bitcoin blockchain, but their ownership status and balances are interpreted and maintained by indexers.

Transfer Mechanism: Transfers of BRC-20 tokens must accompany a change in Bitcoin ownership, while transfers of ERC-20 tokens are based on smart contract function calls.

Centralization vs. Decentralization: The ownership status of BRC-20 is maintained off-chain, which might involve a certain degree of centralization. In contrast, ERC-20 is fully decentralized.

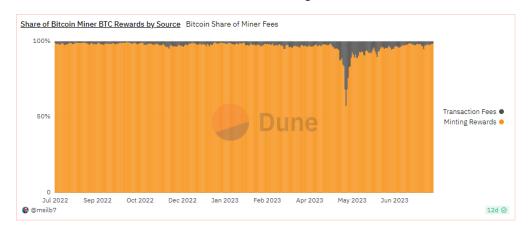
Similarities

Both aim to standardize the features and functions of tokens within their ecosystems. Both aim to ensure interoperability among various applications and platforms.

Stakeholders in the BRC-20 Ecosystem Development

Bitcoin Miners: The Direct Beneficiaries

Miners are overwhelmingly in favor of BRC-20's rise. The surge in BRC-20 transactions has led to a significant increase in transaction fees, which directly benefits miners. For instance, in a year where miners earned 5400 BTC from transaction fees, the introduction of BRC-20 has already contributed to over 1100 BTC in just a few months. This is a substantial increase especially when considering the overall declining block rewards due to Bitcoin's halving events. The spike in transaction fees due to BRC-20 activity, at its peak, accounted for 42% of the total miner rewards, a figure not seen since the Bitcoin bull run of December 2017. However, data from Dune Analytics indicates that, as of the writing of this article, the fee revenue has now fallen back to the 1-2% range.



Source:https://dune.com/msilb7/bitcoin-miner-fees-by-source

BTC Maxis are hostile towards BRC20

This group believes in the original vision of Bitcoin as primarily a peer-to-peer electronic cash system. They argue that Bitcoin should remain focused on its primary purpose: to serve as a decentralized medium of exchange without intermediaries.

They are concerned that innovations like BRC-20 might detract from this primary purpose, introducing inefficiencies and complexities that could hinder Bitcoin's broader adoption.

The BSV Community is experiencing a resurgence due to BRC-20

BSV is a cryptocurrency that emerged from a hard fork of Bitcoin Cash in 2018.

BSV and BTC have distinct paths. While BTC is seen as digital gold with its core as a value store, BSV aims to put everything on-chain. BSV believes in keeping transaction fees so low that users do not notice them, requiring continuous scaling. They hope to maintain the system's stability through a vast number of transactions.

Despite its ambitions, BSV's ecosystem didn't gain traction, and its on-chain data was dismal. During the craze for DeFi, NFTs, and new blockchains, BSV was gradually forgotten.

The BRC-20 boom has brought BSV back into the spotlight, mainly because many BRC-20 applications come from original BSV community developers.

Key BRC-20 projects and their BSV connections:

Unisat Wallet: The core wallet for BRC-20 was developed by a Chinese team that previously worked on the BSV ecosystem and developed the Sensible Contract for BSV.

Ordswap: The first BRC-20 trading platform. It was developed by a team that previously created RelayX, the first decentralized trading platform on the BSV network. Its founder was a former executive at OKCoin.

Ordinals Wallet: Behind this wallet is Twetch, a social application built on BSV. With the rise of the Ordinals protocol, Twetch began supporting BTC NFTs.

Mempool Mining Pool: Founded by core members of the BSV community.

CEX: The Trading Arenas are looking for new narratives

Cryptocurrency exchanges are platforms where users can buy, sell, or trade cryptocurrencies. They thrive on trading volumes and the diversity of trading pairs. Exchanges are likely supportive of BRC-20. In a market that's searching for narratives, BRC-20 provides a fresh trading opportunity.

Several major exchanges, including Gate.io, OKX, and MEXC Global, are supporting BRC-20 trading. Huobi is partnering with the top BRC-20 platform, Unisat, and many other exchanges are showing interest. Binance is developing an Ordinal NFT marketplace, suggesting potential BRC-20 integration. Binance's endorsement could significantly influence the market.

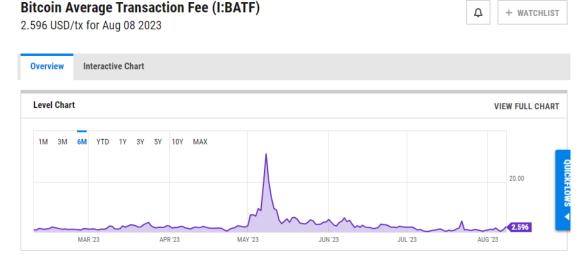
OKX Web3 Team's Support: BRC20 - Staking: In addition to the construction of basic infrastructure like trading tools, the support of the OKX Web3 wallet for the Bitcoin ecosystem goes deep into the protocol standard level. BRC-20S, an extended version of the BRC-20 protocol led by OKX, introduces equity operations such as deposits, minting, and withdrawals. Users can stake their own BRC-20 tokens and Bitcoin and receive corresponding rewards. In the words of the OKX community, "OKX is introducing the DeFi to BRC20".

The main concerns about Ordinals and BRC-20

There are views that BRC-20 goes against the mainstream narratives of **scalability**, **and low cost**.

Contradiction to Scalability

Block Space and Transaction Fees: One of the primary concerns is that Ordinals NFTs and BRC-20 tokens take up significant block space. This has led to increased transaction fees, making it costly for users in countries like Nigeria and El Salvador. For a network that aims to be a global payment system, high fees can be a deterrent.



Source:https://ycharts.com/indicators/bitcoin_average_transaction_fee

Network Integrity and "Spam": There's a sentiment among some Bitcoiners that these tokens and NFTs are "spamming" the network. They believe that Bitcoin's primary purpose is to be a store of value and medium of exchange, and these new additions detract from that.

Contradiction to Low-cost

Inefficiency

BRC-20 tokens, in their current form, have been criticized for being inefficient. The use of JSON data for various functions is seen as bulky and not optimized for a blockchain environment.

Unfair minting practices

The combination of the "first-come, first-serve" approach for inscriptions and the miners' preference to prioritize transactions based on mining fees creates an inherent paradox. This system can lead to unfair minting practices. While the former encourages a race among users to secure unique inscriptions, the latter means that those willing to pay higher fees get prioritized, potentially sidelining genuine users or those who cannot afford high fees. This dual mechanism can inadvertently promote a

pay-to-win environment, undermining the decentralized and equitable principles of blockchain.

The Inevitable Momentum of BRC-20

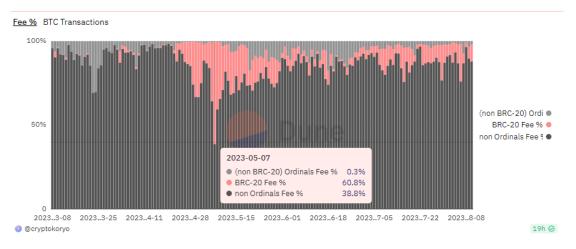
Despite the concerns raised, especially by Bitcoin Maximalists, the momentum behind BRC-20 seems unstoppable. Here's why:

BRC-20 Boosting Miners' Income

Miners' Revenue Challenge: Bitcoin undergoes a "halving" event every four years, reducing mining rewards by half. Once all 21 million bitcoins are mined, miners will only earn from transaction fees. If these fees don't cover mining costs, some miners might exit, compromising Bitcoin's security.

BRC-20 Boosting Miners' Income: Active BRC-20 transactions increase transaction fees, providing miners with additional income. This incentivizes miners to continue mining and ensures the security of the Bitcoin network.

On May 7th, transaction demand from Ordinals (including BRC-20 and non-BRC-20) even surpassed regular Bitcoin transaction fees. On May 8th, miners earned a significant \$17.4 million in transaction fees, marking it as the third-highest fee generation day in Bitcoin's history.



Source: https://dune.com/cryptokoryo/brc20

The Need for Layer 2 Solutions to unlock BTC's potential: However, the capacity and speed constraints of the BTC network have limited the growth of related transaction activities. If BTC had an L2 layer like the ETH ecosystem, creating more use cases and transaction fees, it could significantly boost the earnings of network miners and sustain the growth of its computational power.

It's hard to ban BRC-20 technically

One of the foundational reasons why BRC-20 is hard to stop lies in the technical nature of Bitcoin itself. Andrew Poelstra, one of the inventors of Taproot, has pointed out the inherent difficulty in preventing individuals from storing arbitrary data on the

blockchain. Given the decentralized and permissionless nature of Bitcoin, it's technically challenging to impose restrictions on what kind of data can be inscribed onto it.

For example, it is a challenge of distinguishing between "useful" data, like genuine transaction signatures, and "useless" data, such as NFTs. Any regulatory attempt targeting the latter might unintentionally affect the former. Furthermore, even if restrictions were in place, users could find workarounds, like embedding NFT data within "dummy signatures." Such methods might increase the user's storage costs but would allow them to sidestep imposed limitations.

Network Split Concerns

Implementing a hard fork to potentially curb or control the BRC-20 ecosystem is not a straightforward solution. As noted by Greenspan, while a hard fork is always feasible, it comes with the significant risk of splitting the network. Such a split would not only divide the community but could also undermine the stability and security of the Bitcoin network. Nobody wants to see the network divided, especially when the stakes are so high.

Decentralized Ethos

Trying to halt the development of the BRC-20 ecosystem would be a centralized move, which goes against the very spirit of Bitcoin. Bitcoin is a permissionless protocol. This means that as long as there's interest and utility, innovations like Ordinals and BRC-20 can emerge and thrive without needing approval from a central authority.

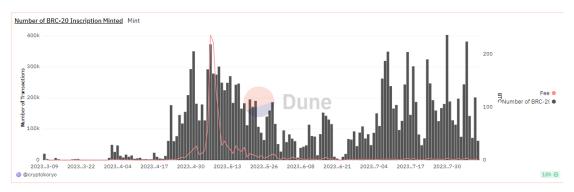
BRC-20 in the Current Crypto Market

The Meme Movement

Meme Effect

The FOMO (Fear of Missing Out) effect around BRC-20 tokens drew significant attention, leading to a surge in minting inscriptions visible on the Ordinals browser. In this initial phase, BRC-20 tokens, devoid of any practical value, were treated as memes and speculated upon by the community.

From the data, it's evident that after reaching the first minting peak in April, and following a two-month lull, the number of mints rapidly surged again in July and August, reaching a daily mint count of 403k.



Source: https://dune.com/cryptokoryo/brc20

However, from a negative perspective, BRC-20 has led to significant waste of block space and substantial expenditure on miner fees.

 The trajectory of the Blockchain ecosystem: From the BRC20 memecoins Catalyst to the flourishing of the BTC ecosystem

The cryptocurrency ecosystem has witnessed a recurring pattern where memecoins serve as a catalyst for broader adoption and subsequent infrastructure development. This trend is evident in various blockchain ecosystems:

Binance Smart Chain (BSC): The rise of the memecoin SafeMoon on BSC not only garnered massive attention but also played a pivotal role in BSC's rapid adoption in 2021. This influx of interest paved the way for developers to build a plethora of protocols on BSC, positioning it as a genuine competitor to Ethereum.

Solana: The Solana ecosystem, which faced challenges in its early days, was revitalized by the introduction of the BONK memecoin. Designed to support the Solana community, BONK boosted the adoption of Solana's native token, SOL, and attracted developers to its platform.

From 'Ordi' Meme Momentum to Bitcoin's Blossoming Ecosystem: Drawing parallels to the BRC-20 meme movement, the initial traction gained from the Ordi token can be seen as the starting point. While the current focus is predominantly on memes, history suggests that this will be followed by a surge in infrastructure and utility development. As witnessed in the aforementioned blockchains, the memedriven attention can attract a vast number of developers to the ecosystem. In the case of BRC-20, this could lead developers towards BTC-DeFi and BTC's layer-two networks.

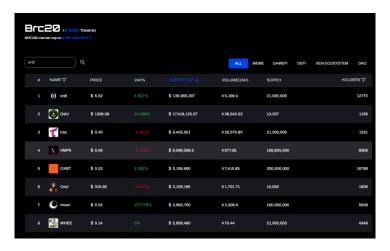
Expanding on this, Bitcoin's ecosystem has been evolving beyond just payments. Solutions like the Lightning Network are primarily focused on payments, while others, such as Stacks and Rootstock, serve as general-purpose smart contract layers. These platforms have paved the way for the development of various applications on Bitcoin.

The DeFi sector, which has predominantly been driven by Ethereum's smart contracts, is now seeing a gradual shift towards Bitcoin. Projects like Sovryn, ALEX, and Lend at Hodl Hodl are notable examples of Bitcoin's growing DeFi ecosystem.

Market analysis of BRC-20

Market

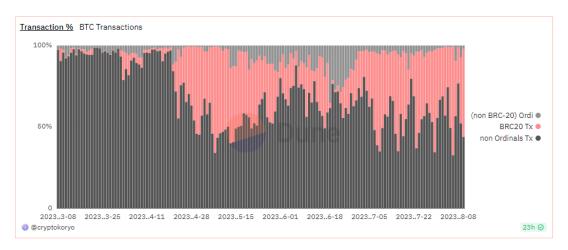
The total issuance of BRC20 Tokens is 37,528 Tokens. The market cap for BRC20 is \$301,358,115.277. The total value of BRC-20 tokens briefly surpassed the \$1 billion mark on May 9 but has since shrunk back down to \$300 million, a drop of nearly 70%.



Source:https://ordspace.org/brc20

BRC-20 transactions have been gaining and frequently surpassing non-ordinal transactions as a percentage of daily activity.

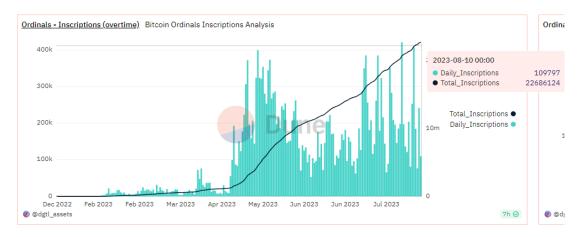
The highest proportion of non-ordinal transactions was 77% on April 25th, but it has been on a decline since then. On August 11th, the combined market capitalization of all BRC-20 tokens reached approximately 301 million. This is a significant increase from April 24th, when the total market cap was just around 17.5 million, marking a 17-fold growth in just four months.



Source: https://dune.com/cryptokoryo/brc20

Inscription

By August 11, 2023, the total number of inscriptions on Bitcoin exceeded 22.68 million, including various digital contents like images, texts, and videos. And it's worth noting that the 'text' type accounts for 94% of the total. Compared to the total of 380,000 inscriptions in March, there's been a growth of nearly 60 times.



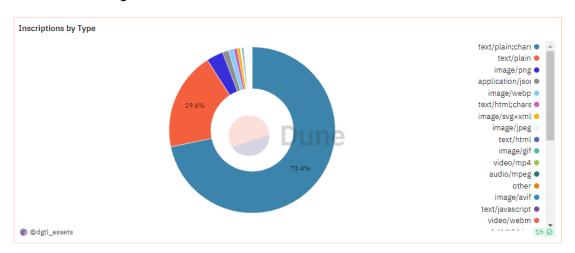
Source: https://dune.com/dgtl_assets/bitcoin-ordinals-analysis

As of August 11, the total fees in the Ordinals ecosystem surpassed 1894 BTC (equivalent to 55.82 million USD).



Source:https://dune.com/dgtl_assets/bitcoin-ordinals-analysis

Breaking down inscriptions by type as of August 11,Text inscriptions made up 73.4%, with over 21 million entries. Image inscriptions constituted less than 3%, with a count not exceeding 730,000.



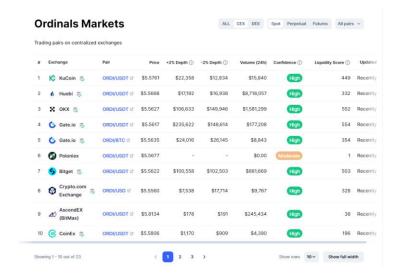
Source:https://dune.com/dgtl_assets/bitcoin-ordinals-analysis

Ecosystem mapping

Exchange

Centralized Exchanges (CEX)

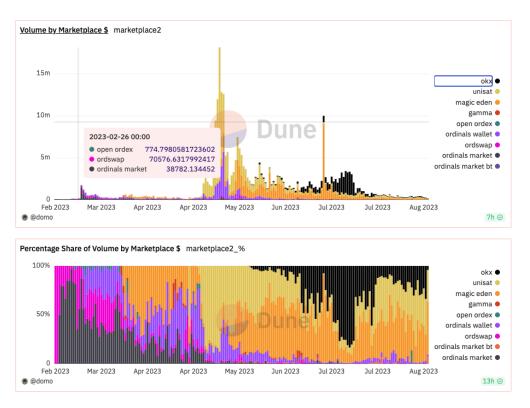
Currently, centralized exchanges such as Kucoin, Huobi, OKX, Gate support BRC-20 token trading, primarily for "ordi".



Source:https://coinmarketcap.com/currencies/ordinals/

OKX is the exchange most optimistic about the BRC20 ecosystem. They participated in the establishment of industry standards and introduced BRC20-S, endowing BRC20 tokens with staking capabilities.

Since OKX began supporting BRC-20 and Ordinals trading, it reached its peak on July 12th, with a market share of 83.3% and a trading volume of \$2.78 million. However, as the BRC20 market cooled down and the overall market trading volume dropped significantly, OKX's market share also plummeted to around 30%, with Magic Eden and Unisat continuously eroding its market share.

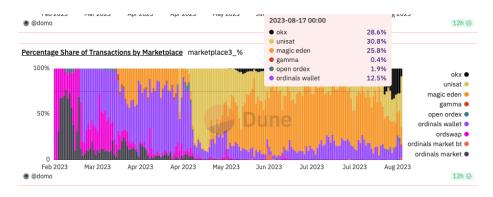


Source: https://dune.com/domo/ordinals-marketplaces

Decentralized Exchanges (DEX)

UniSat Marketplace

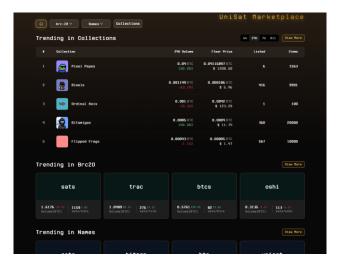
Unisat wallet emerged early as an open-source project and garnered support from the community. Unisat's open-source nature allowed users to verify its GitHub code, ensuring it wasn't a scam. Spontaneous user support gave Unisat a popularity boost, making it a shining star for a while. The booming BRC20 market quickly elevated Unisat to a top-tier exchange. Dune data showing Unisat has 64000 users, and a market share of about 25%, solidifying its mainstream status.



Source: https://dune.com/domo/ordinals-marketplaces

Unisat offers the cheapest transaction fee at 0.8%. Paired with its native wallet, it provides a very smooth user experience. Transaction network fees can be customized. The transaction page provides pricing in both BTC and USD, offering more detailed information.

UniSat Marketplace has implemented trustless transactions using the mature PSBT technology.

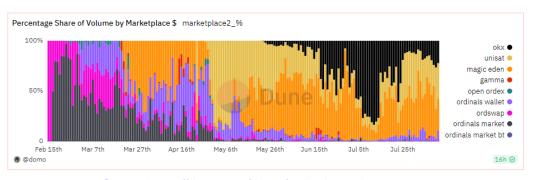


Source:https://unisat.io/market

The Marketplace interacts with wallets in a standardized manner; the seller's wallet signs to provide a sell order, and the buyer signs to place an order and complete the purchase. This is a fully decentralized transaction. The platform cannot intervene during the transaction process. Essentially, it's a peer-to-peer action between the trading parties, making it a secure transaction method.

MagicEden

MagicEden is undoubtedly a shining star in terms of data. Currently, MagicEden is the largest inscription trading market in the Ordinals ecosystem. Since June, its market share has primarily remained around 50% of the total market share.



Source: https://dune.com/domo/ordinals-marketplaces

Magiceden's trading experience is most similar to OpenSea, covering NFTs, domain names, and BRC-20 comprehensively. Magicede offers the transaction fee at 2%.

MagicEden's open-source Msigner, launched on March 22nd, immediately adopted open-source, PSBT, and virtual UTXO technologies, quickly capturing a significant market share. MagicEden's launch pad has also become the preferred choice for most projects. MagicEden's creator center allows project founders to independently submit and manage project listings, enhancing efficiency.

BRC-20 indexer

A BRC20 index, like the **UniSat Indexer**, is a specialized database tracking the wallets and their respective BRC20 token balances. Indexers, the entities responsible for building and updating this database, play a crucial role given that the Bitcoin protocol doesn't inherently recognize deploy, mint, or transfer transactions of BRC20 tokens. Instead, it only perceives the transfer of satoshis between wallets, similar to standard Bitcoin transactions.

The responsibility falls on the indexer, such as UniSat, to verify the authenticity of tokens like \$ORDI, distinguishing genuine tokens from potential imitations. However, a significant concern arises from the BRC-20 ecosystem's dependence on these off-chain indexers. Their centralized nature poses vulnerabilities, emphasizing the pressing need for a decentralized solution for BRC20 indexing.

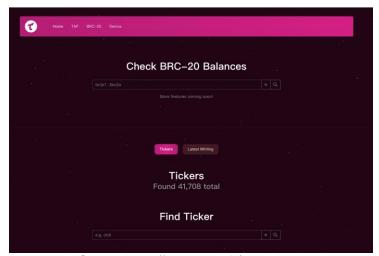
Decentralized Indexer - Trac

By using Trac, you can break free from the current system where your BRC-20 account is controlled by centralized trackers, thereby preserving your freedom. It solves this problem by providing a decentralized network.

Initially, Trac will focus on tracking the most popular metaprotocols, such as BRC-20, and provide comprehensive tracking services for them. This includes tracking BRC-20 balances, mints, and other relevant data. However, Trac also has plans to expand its tracking capabilities beyond BRC-20, with potential integration with other projects. Now they already provide public endpoints for various projects and protocols like Bitmaps, Handles, TAP and BRC-20 that everyone can use for free.

The core features of trac include:

- 1. Trac can display in real-time the issuance, circulation, holding addresses, transaction records, etc., of BRC-20 tokens and Ordinal NFTs, allowing users to understand the market situation of the tokens.
- 2. Trac allows users to view and verify the content inscribed on sat by entering the Ordinal serial number, including images, videos, texts, etc., enabling users to appreciate and identify digital artwork



Source:https://trac.network/brc20.html

The Trac team has also introduced a new protocol called **TAP**, which can be understood as an enhanced version of BRC-20. Previously, OKX introduced BRC-20s, bringing the staking function into the BRC-20 ecosystem. TAP is dedicated to building OrdFi, enhancing the liquidity of Ordinals and BRC20 assets and improving transaction efficiency through token staking, token swap, and batch transfers.

TAP tokens work in the exact same way as BRC-20 tokens. There are however a couple of minor modifications required for indexers:

	TAP	BRC-20
Allowed ticker lengths	3 and 5 to 32 (UTF16)	4 letters
Protocol	tap	brc-20
Deploy op	token-deploy	deploy
Mint op	token-mint	mint
Transfer op	token-transfer	transfer

Source:https://github.com/BennyTheDev/tap-protocol-specs

Within the TAP protocol, it offers more features compared to BRC20:

- token-send: This function allows for the mass-transfer of different tokens to multiple recipients in a single transaction. It's designed to enhance efficiency, especially when distributing tokens to many users simultaneously.
- token-swap: This function facilitates the exchange of one token for another.
 It's a crucial feature for decentralized exchanges and automated market makers within the TAP protocol ecosystem.
- token-stake: This function enables users to lock up or "stake" their tokens, often to participate in network security, governance, or to earn rewards.

Staking can also be used to create a form of collateral or to participate in DeFi protocols.

- token-unstake: As the counterpart to token-stake, this function allows users to retrieve or "unstake" their tokens from the staking mechanism.
- token-stake-reward: This function lets users claim rewards earned from staking their tokens. Rewards can be in the form of additional tokens or other incentives provided by the protocol or application.
- **token-batch**: This function is designed to process multiple token operations in a single transaction, enhancing efficiency and reducing costs.

The below example will send 10000 tap tokens to each address. Tokens and amounts can be mixed. There is no restriction on the amount of items (receivers).

Source:https://github.com/BennyTheDev/tap-protocol-specs

As a result, in the future, many will conduct transactions under the TAP protocol. Through monitoring tap inscriptions in memory pools, we can observe that an increasing number of people are adopting the TAP protocol.



Source:https://satosea.xyz/zh/hot_mints/tokens

Wallet

UniSat

UniSat Wallet, a leading service provider for Bitcoin Ordinals and BRC-20, has revealed its intention to secure funding at a valuation of \$50 million. As of the <u>article's</u> publication date, numerous investors have shown interest, with Binance Labs actively engaging in discussions with the UniSat team.

Data from Dune's panel indicates that UniSat Wallet has a significant presence in the current Bitcoin Ordinals trading market. It accounts for approximately 10% to 20% of the transaction volume and transaction times. Furthermore, the platform boasts around 60,000 unique users, marking its significant role in the market.

Recently, UniSat Wallet launched BRC20-swap, which is the industry's first-ever Ordinals native swap. This allows users to deploy new trading pairs and add liquidity to the Swap, similar to how they can deploy and mint a classic BRC-20.

Ordinals Wallet

A web-based wallet where users can create a new wallet or import it from UniSat, Hiro, or Xverse. Besides storing and viewing inscriptions, it also offers minting and trading services for Ordinals NFT and BRC-20.

Hiro Wallet

A popular wallet on the Stacks blockchain, now also a wallet for Bitcoin, NFTs, and Ordinals. Hiro Wallet recently introduced support for Ordinals. With Hiro, users can connect/interact with applications built on Bitcoin and manage assets built on Bitcoin L2s.

Xverse

Xverse is a leading Bitcoin Web3 wallet that supports Ordinals, NFTs, DeFi, and decentralized applications. Based in Hong Kong, Xverse aims to be a primary gateway to the Bitcoin ecosystem. It's recognized for pioneering support for Ledger hardware wallets with a focus on Ordinals.

Recently, Xverse successfully raised \$5 million in its seed funding round. The funding was led by Jump Crypto, with participation from several other investors and venture capital firms. The funds will accelerate the development of advanced features around DeFi, Stacks, Lightning, and other Bitcoin scalability solutions.

Soon, Xverse users will be able to replace their Bitcoin wallet addresses with .sats names which are human-readable names that are short and easy to remember.



Source:https://www.xverse.app/blog/what-are-sats-names

OKX Web3 Wallet

The first multi-chain wallet on the APP side to support the Ordinals market.

Bitcoin Scaling Solution

On-chain Scaling

SegWit (Segregated Witness): A technical improvement proposal for the Bitcoin network that increases its processing speed by moving transaction signature data out of the transaction record, thus reducing the size of transaction data.

Taproot: A new script language upgrade designed to enhance the privacy and security of the Bitcoin network while reducing transaction fees.

Schnorr Signatures: A new signature scheme that allows the Bitcoin network to process more transactions without increasing the size of transaction data.

Recursive Inscriptions: In June 2023, the ordinals community introduced recursive inscriptions, which is a method that allows on-chain software to run entirely on Bitcoin's blockchain.

This approach overcomes the rigid 4MB boundary. It retrieves data from current inscriptions and integrates it into subsequent ones. By connecting data via a sequence of calls, developers can operate software entirely within the chain. Video games, movies, or complex software could reach gigabytes of data. Such an innovation greatly enhances the potential for interoperability on the Bitcoin network. Projects like OnChainMonkey have already utilized recursive inscriptions to create 3D art. Using recursion, they inscribed various data packages as ordinals on Bitcoin, enabling them to create stunning 3D art under 1KB in size by making calls to those packages.



Source: OnchainMonkey Twitter

What's more, NES games can be developed and run on the Bitcoin network through Recursive Inscription. Due to the data size constraints of individual Bitcoin transactions, the game data is split into smaller chunks. Each chunk is then inscribed onto the Bitcoin blockchain in a series of transactions.

Through the method of recursive inscription, these chunks of data are linked or "daisy-chained" together. This allows for the retrieval and reconstruction of the entire game data from the series of linked transactions.

So, the inscription id for JSNES and its license is: 3a4575b2a8fe6e7968146f290d494c2346d40ff692314050babcaa7268347f4bi0

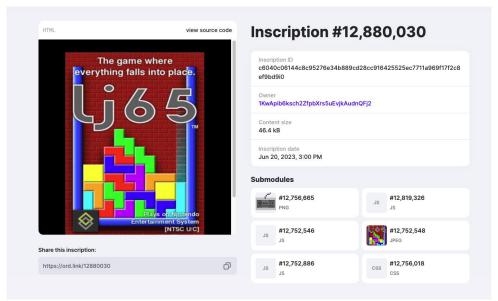
the inscription id for the application code I wrote is: $\underline{89aaae01a47dd2d26f13513a797d99612db4b504412bbb2ac94e0c39e1c80369i0}$

the inscription id for the UI stylesheet is: f90c74f6a2f4cf6ba73312b444596c4f34641d72ba9dda049d26751ee1a908e8i0

and lastly, a cute little "favicon" asset for the browser tab: $\underline{0e377734f883a5abd9a89478facc028b747d6766a11de4effc2990fc8bc81d4ci0}$

Source: How to put NES games on Bitcoin with recursive Ordinal inscriptions.

With the game data stored and linked on the Bitcoin blockchain, specialized software or emulators can retrieve this data, reassemble the game, and run it just like the original NES game. You can play right now on the Ordinals protocol with its indexers.



Source: Game Preview

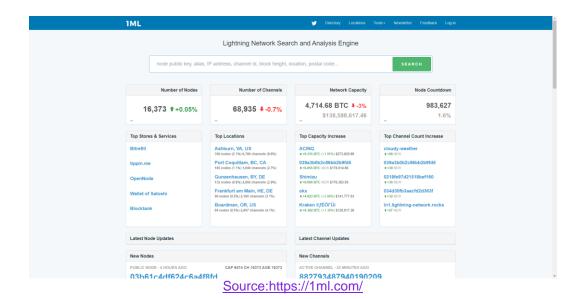
This innovative approach not only showcases the versatility of the Bitcoin network beyond simple financial transactions but also breathes new life into classic NES games by preserving and executing them on a decentralized platform.

Off-chain State Channels

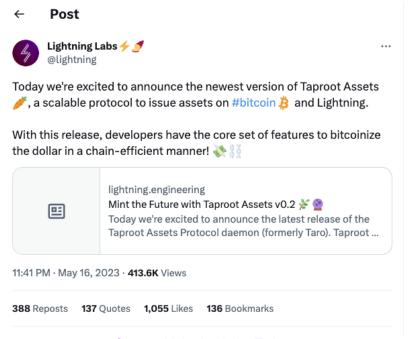
A second-layer network protocol based on Bitcoin, designed to speed up transactions and reduce fees by establishing multiple "channels". Representative projects include **Lightning Network**, **RGB**, **OmniLabs**, **and others**.

Lightning Network: The Lightning Network, often referred to as Lightning or LN, is a
scalability solution built on the Bitcoin network. It facilitates instant micro-payments,
reduces transaction fees, and eliminates the risks associated with entrusting funds to
third-party platforms.

As of Aug 13, 2023, according to 1ML data, the Bitcoin Lightning Network's capacity stands at 4714.68 BTC, valued at \$138 million, with 16,373 nodes and 68935 channels.



The Lightning Network, in response to the on-chain congestion caused by BRC20, introduced the Taproot Assets Protocol. In fact, exchanges like Binance and Coinbase are swiftly moving toward Lightning integration, and the popularity of the BRC-20 standard is only adding to demand for L2s.



Source: Lightning Labs Twitter

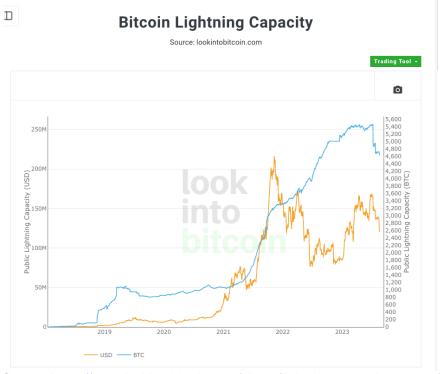
This protocol offers four main advantages:

- 1. It utilizes taproot to enhance both privacy and scalability.
- 2. Assets can be deposited directly into Lightning channels.
- 3. These assets can then be transferred across the existing Lightning Network for fast, high-volume, and low-fee transactions.

Furthermore, this approach capitalizes on existing networks, such as wallets, exchanges, and merchants, eliminating the need to establish a new ecosystem.

The anonymous developer behind BRC-20, Domos commended Taproot Assets as a more efficient method for minting new Bitcoin assets compared to techniques like JavaScript Object Notation (JSON).

However, there doesn't seem to be a direct correlation between the capacity of the Lightning Network and the activity of BRC-20. From May to July 2023, the BRC-20 ecosystem experienced its most prosperous phase. Yet, during this period, the capacity of the Lightning Network did not show significant growth. This might indicate that people were not using the Lightning Network for minting and trading BRC-20 tokens. According to the team, Taproot Assets is currently available on a test network, with main network support "coming soon".



Source: https://www.lookintobitcoin.com/charts/lightning-network-capacity/

Layer 2 Solutions

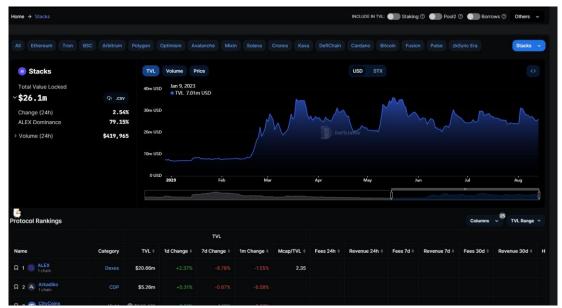
Connects the Bitcoin with other faster blockchain networks, securely recording transaction results on the Bitcoin. Representative projects include **RSK and Stacks**.

• Stacks: Pioneering Bitcoin's Layer 2 Development

Stacks Labs is currently the most well-known Bitcoin Layer 2 project. It enables the creation of smart contracts and decentralized applications. It aims to expand the Bitcoin economy by introducing new functionalities.

Based on data from Defi Llama, along the rise of BRC20, there has been a significant increase in funds on Stacks recently. Over the past 30 days (from February 1st to August 20nd), the Total Value Locked (TVL) has risen from \$7.56 million to \$21.5

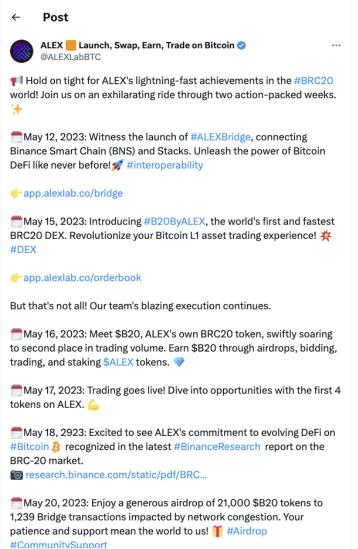
million, marking a 184% growth. The most notable growth is seen in the DEX ALEX, which experienced a 120% increase in TVL over the past 6 months.



Source: https://defillama.com/chain/Stacks?tvl=true

To embrace the growth of the BRC20 ecosystem, Stacks has been tirelessly building and delivering. They introduced the ALEX Bridge, linking BNBChain with Stacks, followed by the debut of B20, the premier and swiftest BRC20 DEX. Alongside, they launched \$B20, ALEX's proprietary BRC20 token, which quickly climbed to the second spot in trading volume.

Soon after, Stacks facilitated permissionless listings for new tokens on B20. Recently, they presented their BRC20 Launchpad. Now, just a few weeks post-launch, B20 hosts 22 distinct BRC20 tokens for trading.



Source:https://twitter.com/ALEXLabBTC/status/1663616813567975425?s=20

Stacks is set to undergo **the Nakamoto upgrade** in Q4 of 2023, introducing five crucial features.

- Of utmost significance is the feature that ensures Stacks transactions are secured by the Bitcoin network. This enhancement not only bolsters the security and reliability of Stacks transactions but also positions it as a genuine Layer 2 solution rather than an independent sidechain with its own state.
- Furthermore, the introduction of decentralized, two-way Bitcoin pegging (sBTC) could potentially unlock a "Bitcoin DeFi market" worth hundreds of billions of dollars.
- Lastly, with block times reduced to 4-5 seconds and support for programming languages from other networks, such as Solidity, the network performance is greatly enhanced. This not only lowers the barrier to entry for developers but also sets the stage for an explosive growth in ecosystem projects.

Bitcoin DeFi Protocols

- Stacks DeFi protocols
 - Some Bitcoin applications created with Stacks' L2 clarity smart contracts.
 - a. Lending out \$BTC to earn yield: The Zest protocol is a decentralized finance application that allows users to lend their Bitcoin to borrowers. In return, lenders earn yield in \$BTC. The process is secured by a smart contract that ensures borrowers repay the loan with interest within a set timeframe.
 - b. **Borrowing a stablecoin:** Arkadiko offers users the ability to use their Bitcoin (in the form of xBTC) to either swap or use as collateral to borrow a stablecoin. This provides financial benefits to a broader audience, especially in regions with unstable fiat currencies.
 - c. In-game items and trading: Project Indigo is a game that uses smart contracts to give players legal ownership of in-game items. These items can be traded on an automated marketplace, allowing players to monetize their ingame assets.
 - d. ALEX Lab: ALEX Lab stands out as the premier DeFi application within the Stacks ecosystem, boasting a comprehensive suite of features. The platform is often dubbed the "Bitcoin Uniswap" due to its comprehensive suite of decentralized financial (DeFi) services built on the Bitcoin network via Stacks. ALEX Lab stands out with its diverse offerings. These include a launchpad for liquidity provision for new projects, fixed-term and fixed-rate lending and borrowing services without liquidation risks, an advanced orderbook Decentralized Exchange (DEX) that supports limit orders and facilitates NFT auctions, and attractive yield farming opportunities.



Source:https://docs.alexlab.co/

Oshi Finance: The mission of Oshi Finance is to be the first Bitcoin liquidity pool
protocol using BOSS (Bitcoin Operational Standardized System). Think of it as a
virtual machine that facilitates code execution, Web2 API integration, and
decentralized data indexing. With BOSS, Bitcoin can directly interface with off-chain
JSON data, essentially connecting Bitcoin to the broader internet.
BOSS introduces "smart inscriptions," akin to Ethereum's smart contracts, into the
Bitcoin Ordinals ecosystem. The liquidity pool protocol from Oshi Finance (\$OSHI) is
one of endless possibilities.

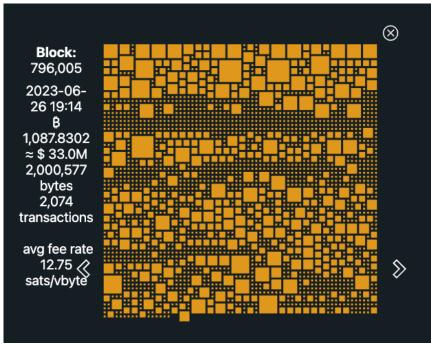
Bitcoin Cross-chain Bridge

To unleash the liquidity of BTC, besides BTC L2, we can also achieve it through cross-chain bridges from BTC to other ecosystems.

VMPX: Bridging Bitcoin and Ethereum/X1 blockchains
 VMPX is designed to act as a bridge liquidity token, connecting the Bitcoin and Ethereum/X1 blockchains. The token exists in two forms: as a BRC-20 token on the Bitcoin side and as an ERC-20 token on the Ethereum side, both with a total supply of 108,624,000 tokens.

The primary goal of VMPX is to enable smooth swaps between BRC-20 and ERC-20 tokens across the Bitcoin-Ethereum bridge. Additionally, VMPX tokens can be converted to XN native coins on the X1 blockchain through a smart contract. Interoperability: VMPX is crucial for enhancing interoperability and expanding opportunities for users across the Bitcoin, Ethereum, and X1 blockchain ecosystems.

Bitmap bridges Bitcoin with the metaverse: Bitmap Theory is a novel concept that bridges Bitcoin with the metaverse. It allows users to claim ownership of a Bitcoin block by inscribing it on a Satoshi, the smallest unit of Bitcoin. Once a block is inscribed, it can potentially be integrated into a metaverse. The theory suggests that platforms could convert block data into 3D spaces, granting block owners the privilege to construct within these digital realms. This would enable block owners to actively contribute to the metaverse, creating dynamic, community-centric spaces. The image below represents the city block landscape mapped out from Bitcoin block 796005 using Bitmap Theory.



https://bitfeed.live/block/height/796005

Market Headwinds

Underdeveloped Infrastructure

The BRC-20 token, as an emerging token standard on the Bitcoin network, has garnered attention for its innovation and potential. However, its underdeveloped infrastructure could pose significant challenges to its future growth. Firstly, given that BRC-20 is still in its nascent stages, its market activity and user engagement remain relatively limited. Furthermore, since BRC-20 tokens lack social consensus could result in certain parties not acknowledging specific tokens. In summary, while BRC-20 tokens introduce new opportunities to the Bitcoin ecosystem, their fragile infrastructure might constrain their long-term market appeal and stability, undoubtedly representing potential market headwinds in the future.

Hype Risks Associated with BRC-20

The current BRC-20 tokens are in a very early stage, and their speculative value far exceeds their actual value. According to data from the chaineye tool, the current number of users participating in BRC-20 is about 100k. Actual user numbers are much lower than the associated hype. Many BRC-20 tokens have poor liquidity and are illiquid. Therefore, users need to control their FOMO and be wary of the BRC-20 hype bubble.



Source:https://chaineye.tools/ord

BRC20's Regional Concentration in Asia

One potential challenge that BRC20 might face in the future is its perceived regional concentration. The majority of BRC20 projects seem to be predominantly driven by Chinese teams and investors. This localized dominance suggests that BRC20 has not yet achieved a global reach, potentially missing out on the influence and participation of international opinion leaders and major institutions. Such a regional

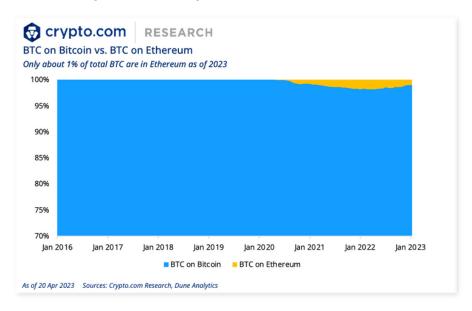
focus could limit BRC20's broader adoption and acceptance in the global crypto community.

Market Tailwinds

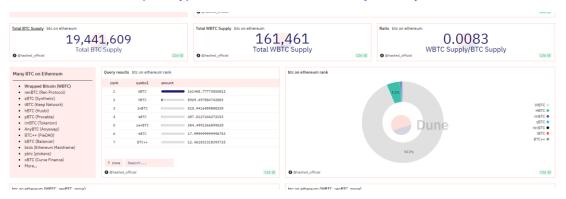
• Unparalleled Capital Reservoir of Bitcoin

Bitcoin remains the leading cryptocurrency in terms of market cap. This dominance ensures that any development or innovation on its platform, like BRC-20, garners significant attention and adoption potential.

Currently, Bitcoin's market capitalization exceeds USD\$570B, with over USD\$4.74B of Bitcoin bridged to Ethereum, providing them with liquidity. For the Bitcoin ecosystem, there's a naturally strong financial foundation. The challenge is how to revitalize and leverage these existing assets.



Source: https://crypto.com/research/bitcoin-ecosystem-layer2-defi-nft



Source: https://dune.com/hashed_official/btc-on-ethereum

BTC Halving Approaches: A Surge in Interest for Layer 2 Solutions

As the anticipated Bitcoin halving event is projected for May 2024, it remains one of the most watched events in the crypto market. With the halving drawing closer, investments will increasingly focus on Bitcoin. However, given its vast market capitalization, investing in Bitcoin might only yield market Beta returns. Layer 2 projects, which aim to unlock BTC's liquidity and expand its application layer, could potentially become the primary targets for investors seeking Alpha returns.

• Price in Satoshi: Capturing Ecological Value for Bitcoin's Renaissance

Ethereum's growth was fueled by activities priced in its currency \$ETH, when an asset becomes a standard for pricing, it gains intrinsic value and demand. Historically, Bitcoin has been underutilized in terms of its transactional capabilities. Many people, especially newcomers to the cryptocurrency world, rarely transact or even hold Bitcoin. However, the BRC-20 concept and Ordinals protocol have sparked increased Bitcoin blockchain activity. The rise of BRC-20, combined with future developments like the Lightning Network, suggests a shift towards Bitcoin transactions being priced in "Satoshis." If everyone were to adopt a Bitcoin wallet and transactions were commonly priced in Satoshis, it would be a significant boon for Bitcoin's ecosystem.

Conclusion

BRC-20 was initiated as an experiment, aiming to test if Ordinals could foster the development of fungible tokens on Bitcoin. With its simplicity and flexibility, BRC-20 has achieved the ease of token deployment and pioneered a new market worth hundreds of millions of dollars.

The rise of the BRC-20 ecosystem has spurred the development of BTC Layer2 technologies. It's essential to keep a close eye on the progress of core projects, such as Alex Labs and Oshi Finance, mentioned in this article. Additionally, the emergence of cross-chain bridges that facilitate liquidity interoperability between BTC and other blockchain ecosystems is a noteworthy development to monitor.

As the industry evolves, we are witnessing a surge of innovative startups. For instance, Bitmap is bridging the gap between Bitcoin and the metaverse, while Recursive Inscription bypasses the 4MB capacity limit, offering a broader scope for imagination and application. With the upcoming Bitcoin halving cycle next year, it becomes even more crucial to closely monitor the ecosystem's growth and adaptability. This event could potentially influence the trajectory of BRC-20 and its associated projects.

However, it's crucial to recognize the current issues with BRC-20. Its functionality is overly simplistic, limiting developers from performing more complex operations. The token transfer mechanism is inefficient, leading to significant block wastage,

unnecessary costs, and network congestion. Its reliance on centralized indexers also poses security risks.

In conclusion, BRC-20, as the beginning of an experiment, has undoubtedly unlocked the Pandora's box of the Bitcoin ecosystem. Its potential is vast, but so are the challenges ahead. As stakeholders, it's imperative to stay informed, adaptive, and prepared for the evolving landscape.

References:

- a. Ordinals turned Bitcoin into a worse version of Ethereum: Can we fix it?
- b. It Started With a Meme Accelerating Growth and Adoption in Web 3.0
- c. <u>Bitcoin's Expanding Ecosystem: Layer-2, DeFi, NFT</u>
- d. Layer 2 | Lightning Network MIT Digital Currency Initiative
- e. Bitcoin Developer Introduces New Layer 2 Protocol
- f. ITrend Research by LD Capital Stacks, layer2 network of Bitcoin
- g. VMPX websites
- h. Recursive inscriptions: Your essential guide to the future of Bitcoin smart contracts

Disclosure:

This document was produced by the Aves Lair team and is meant for informational purposes only. It should not be taken as financial predictions, investment guidance, or an endorsement or solicitation for any financial instruments, cryptocurrencies, or investment approaches. The terminology and perspectives shared aim to foster comprehension and the ethical growth of the industry, and they shouldn't be seen as conclusive legal opinions or representations of Aves Lair. The views presented are those of the author as of the indicated date and may evolve based on changing circumstances. While efforts have been made to source information from reliable and comprehensive resources, Aves Lair Research does not guarantee its accuracy or completeness. Consequently, Aves Lair does not accept liability for any errors, omissions, or negligence that might arise from this content.

This document might include forward-looking statements that are speculative and not strictly historical. There's no assurance that any predictions or forecasts will materialize. Readers should use this information at their own discretion. It's crucial to understand that this content is neither a direct investment recommendation nor an invitation to buy or sell any securities, cryptocurrencies, or adopt a specific investment strategy. Moreover, no financial instruments or cryptocurrencies will be offered or sold in any region where such actions would breach local laws. All investments come with risks.

1 AVES LAIR

About Aves Lair:

Aves Lair is a hybrid venture fund and accelerator focused on supporting visionary and ambitious founders at the seed-stage and early-stage of companies in the Web3 and crypto space. Our mission is to nurture cutting-edge applications and technology for a decentralized internet and economy where users control their own data, identity and digital assets.

www.aveslair.com