BRC20, a new dark horse in the digital currency market or a flash in the pan? What are its risks?

Beosin · Follow
7 min read · May 19

Recently, the focus of Bitcoin discussion seems to have shifted to the Bitcoin network, and BRC20 has also become a recent hot topic.

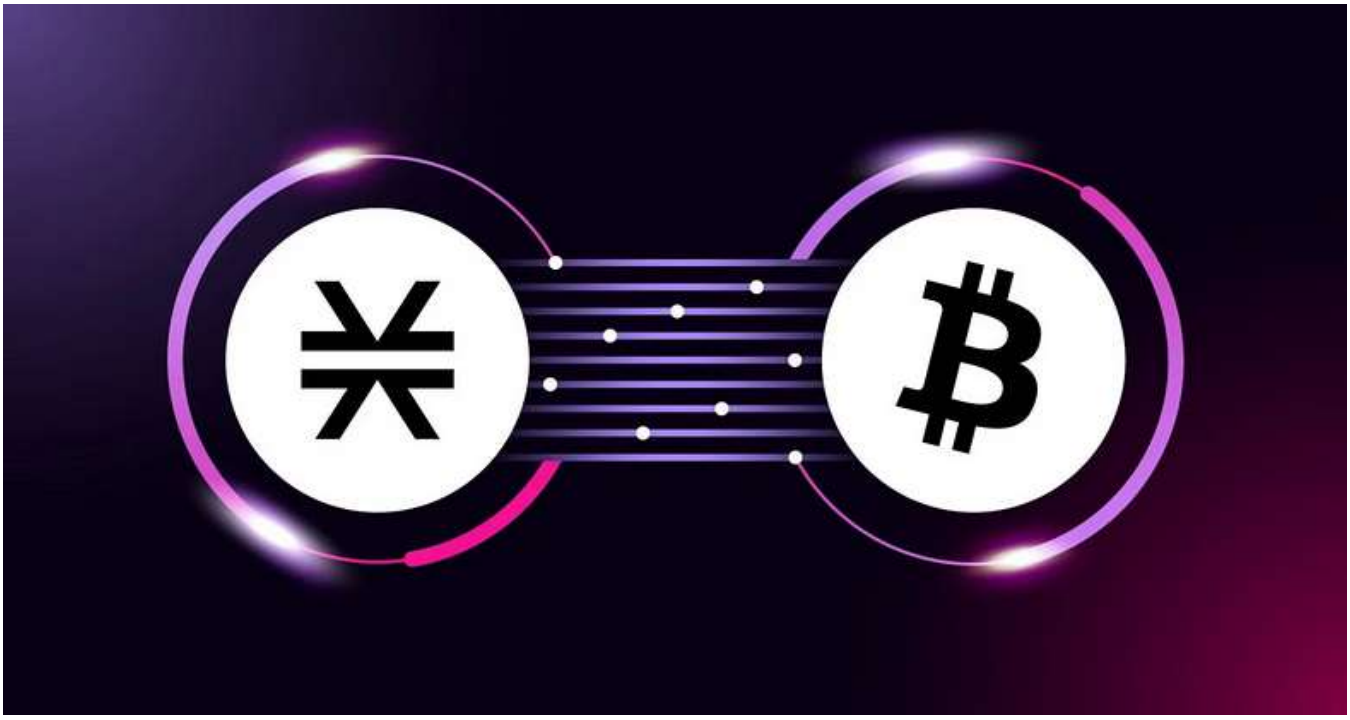
Everyone is discussing whether the emergence of the Bitcoin L2 scaling solution and the BRC20 standard brings more power and scalability to Bitcoin. But for now, the market is still too hyped. In this article, we will briefly introduce the Bitcoin L2 architecture, BRC20 related content and security views.

What is the Bitcoin L2 architecture?

In the blockchain, there is a triangle impossible to balance, that is security, decentralization and scalability, and when these three are introduced to a blockchain, only two of them can be chosen.

Bitcoin is a blockchain system that sacrifices scalability to maximize security and decentralization. Bitcoin's block time is around 10 minutes, while other common public chains such as Ethereum2.0 and Solana have a block time of seconds or even milliseconds. This shows that Bitcoin has made a huge sacrifice in efficiency, while security and decentralization are the highest, making a large number of blockchain participants have a great demand for Bitcoin's scalability.

Bitcoin Layer2 is an scalability solution to Bitcoin that addresses the lack of application scenarios and the relatively inefficient execution of Bitcoin. It aims to balance the above-mentioned triangle of scalability dimensions, such as the Stacks system.

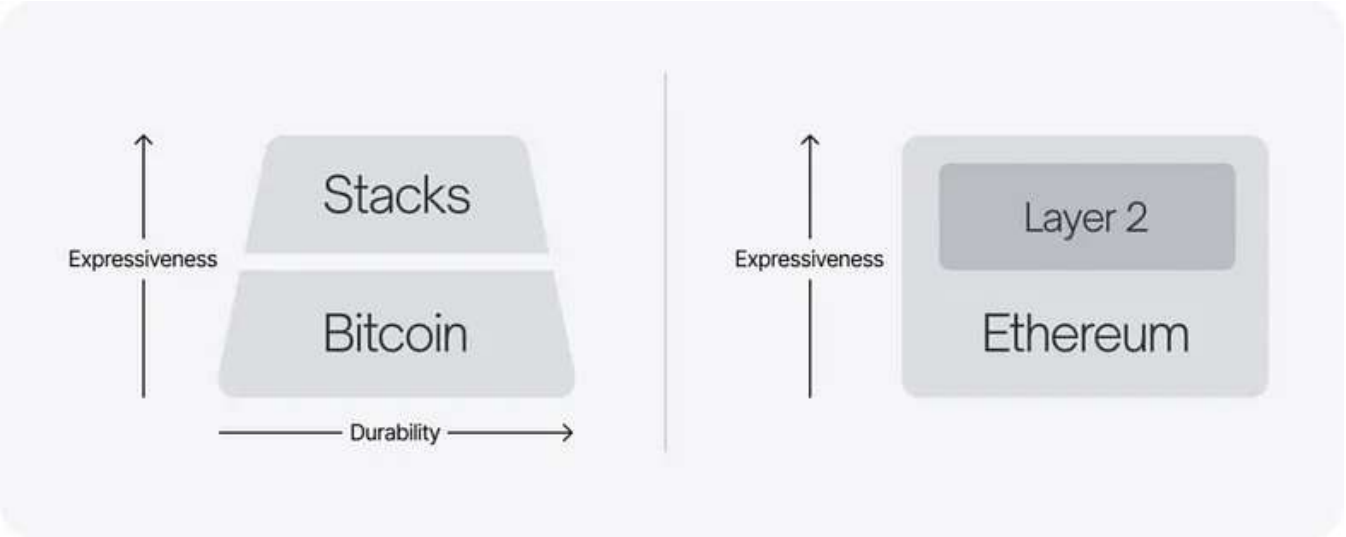


The Stacks system is a Bitcoin layer2 network supporting decentralized applications and smart contracts, connected to Bitcoin's blockchain system through a consensus mechanism spanning both chains, thus achieving both the security of Bitcoin and the rich application scenarios of smart contracts.

Stacks uses a pyramid approach, with the basic settlement layer (Bitcoin) at the bottom, then adding smart contracts and programmability on top of that (Stacks), and then adding scalability and velocity layers (Hiro's subnet) on top of that. By taking this layered approach, it not only gives Stacks the same rich functionality as public chains like ethereum, but also avoids a lot of drawbacks of these complex public chains.

Stacks is Bitcoin's Layer2. It has some unique properties such as its native token, which acts as an incentive mechanism to maintain the historical ledger of all its transactions and executions according to its own security scheme.

While Stacks adds additional functionality to Bitcoin, it does not change the content of Bitcoin itself due to its proof-of-transfer (POX) consensus mechanism. This is what separates Stacks from L2 scaling solutions on ethereum such as Polygon or Arbitrum. This keeps Bitcoin itself simple and secure, while other features and speed optimizations are implemented using other layers, so that even if other layers get damaged, it doesn't affect the base layer (Bitcoin).



What is BRC20?

To explain BRC20 clearly, it is important to first introduce Ordinals.

Ordinals is a system protocol that numbers the smallest unit of bitcoin (sats) by assigning a unique number to each sats. Moreover, Ordinals supports the ablity to write text, images, audio, video, etc to the sats, thus making each sats unique. This is similar to the familiar non-fungible token NFT on the Ethereum , and we call it Bitcoin NFT. Ordinals also assigns artificial rarity to these sats, and classifies the sats numbers into the following classes based on specific events in the Bitcoin network:

Common: not the first sat of its block;

Uncommon: the first sat of each block;

Rare: the first sat of each difficulty adjustment period;

Epic: the first sat of each halving period;

Legendary: the first sat of each cycle;

Mythic: the first sat of the Genesis block.

The founders of BRC20 came up with a different set of ideas based on the Ordinals protocol. Since the Ordinals protocol can create Bitcoin NFTs by assigning different “properties” to each sat, it is also possible to create Bitcoin FT by giving a uniform “format” and “properties “ , i.e., fungible tokens.

BRC20 writes unified JSON text data to Satoshi via the Ordinals protocol. This text data is the ledger of the BRC20 tokens, and can be used to parse out token holdings and

transfers. The main contents are as follows:

{

“p”: “brc-20”.

“op”: “deploy”.

“tick”: “ordi”.

“max”: “21000000”.

“lim”: “1000”

}

{

“p”: “brc-20”.

“op”: “mint”.

“tick”: “ordi”.

“amt”: “1000”

}

{

“p”: “brc-20”.

“op”: “transfer”.

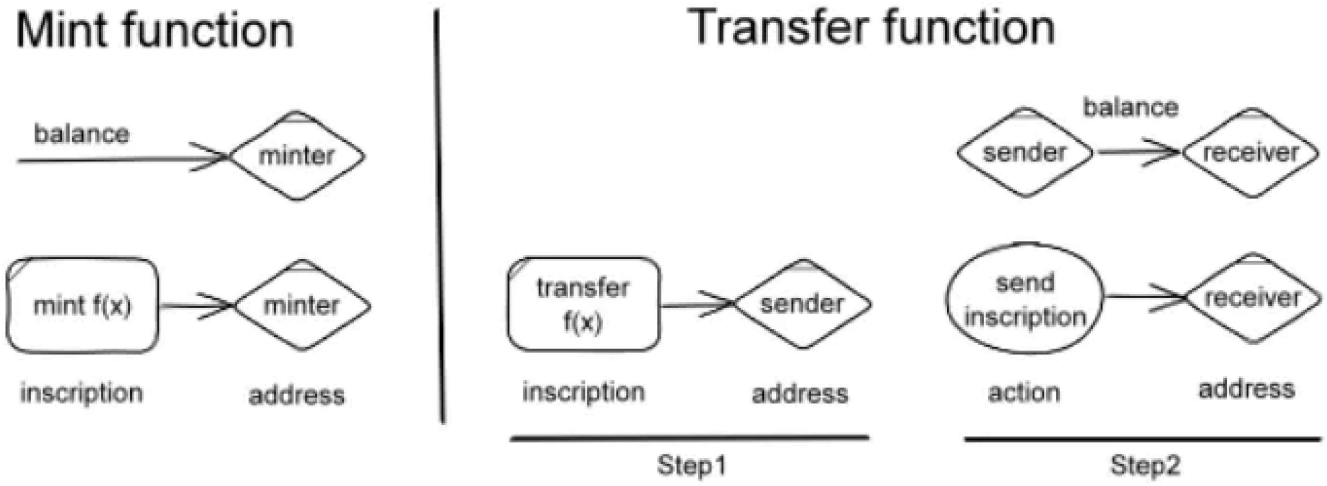
“tick”: “ordi”.

“amt”: “1000”.

}

The above are the three standards of BRC20, where the op field indicates **the operation to be performed, including deploy, mint and transfer, tick indicates the name of the token to be operated, max indicates the total**

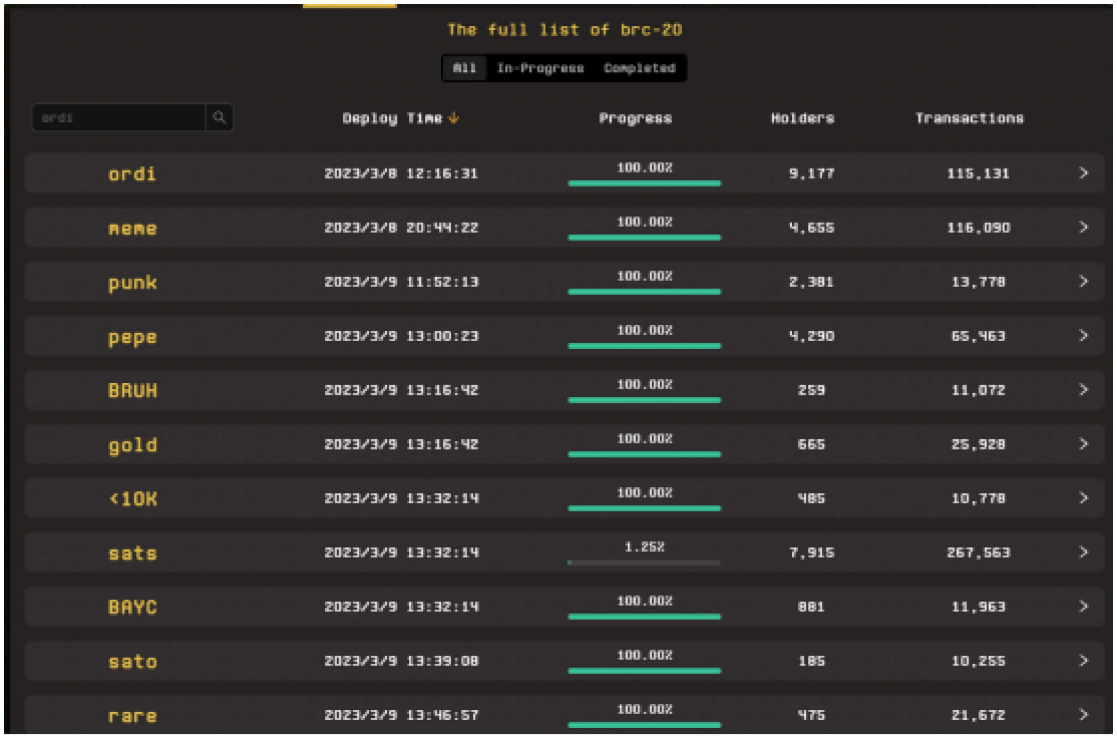
number of tokens issued, lim indicates the maximum number of coins minted per token, amt indicates the amount of tokens to be operated. In the transfer standard, there are also fields such as “to”, but this is not required. The transfer is done by sending the inscription to the target address to achieve the balance change, as shown in the figure below.



BRC20 has a “first-come, first-served” mechanism, so **after a BRC20 token is deployed, no tokens with the same name can be deployed again. Even if a token with the same name is deployed, the off-chain ledger platform will consider the second deployment illegal and not record it because it has already recorded the previously deployed token with the same name during the resolution process.** The same principle applies to the management of the mint limit.

The above example is the ordi token which has been extremely hot recently. It is a BRC20 experimental token launched by the creators of BRC20, the first bitcoin inscription token, with a mintage of 21 million pieces. This can be minted at first by paying a miner’s fee, up to 1000 pieces can be minted each time. Although the token was a BRC20 experimental token, being the first BRC20 token attracted a large number of investors, making ordi once exceed $100 per unit with a huge price fluctuation. And, because ordi uses an order book approach instead of a trading pair approach, which is a kind of transaction where the token holder puts up an order for sale and the price is customized by the seller, this results in non-uniform caculation of token’s price , and the uniform valid price cannot be checked on different platforms.

The current number of BRC20 tokens deployed is over 20,000, which can be viewed through the unisat website. （https://unisat.io/brc20）



What are the security risks of BRC20 related issues?

At present, although the BRC20 token is concerned and recognized by a large number of users, it is, after all, only a piece of json file without any practical value or business application scenario as support, and is a product that uses the popularity and traffic of BTC to attract investors. And BRC20 tokens cannot be used and managed as easily as BTC, it needs a separate wallet for management. Ordinary users need to learn to use a third-party tools if they want to participate in BRC20 investment, and these third-party tools generally require a threshold, such as Unisat, which requires nearly $200 sats to enter for the first time, which greatly increases the complexity and participation threshold for users.

Although BRC20 has received a lot of attention in recent times, it still has some risk points, including:

1 Bubble risk: The token price may be overvalued due to the hype and speculation in the BRC20 token market.

2 Security risk: Like other blockchain technologies, BRC20 tokens may be subject to hacking attacks.

3 Lack of regulation: The lack of regulation of blockchain technology and the cryptocurrency market may lead to some unscrupulous individuals using BRC20 tokens for fraudulent and illegal activities.

Expanded reading: Ape in altcoins but fall into a honeypot. What you should pay attention to in the meme season?

BRC20 is prone to make users have the illusion that BRC20 is a token created using the security of Bitcoin and will be as safe and stable as Bitcoin. But in fact it is not the same as BTC, BTC's security is based on encryption and consensus algorithm, which has been running relatively stable for a long time and has stood the test of time. While BRC20 is bound to BTC using the Ordinals protocol, the Ordinals protocol has only been running for a short period of time and is still in the initial stages of development, where there may be some security risks that have not yet been discovered.

For example, Ordinals protocol supports writing text, images, audio, video and even code to the Bitcoin network, is this process safe and will there be any injection risks? The above describes its numbering of sats, with each number being artificially graded. When the time comes for some special bitcoin blocks, there may be miners who steal and roll back blocks in order to grab the right to bookmark the special blocks, thus giving themselves a high grade sats number, which could have security implications for the bitcoin consensus if the miner's computing power is at an advantage. These are all security risk points that deserve extra attention.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, South Korea, Japan and other 10+ countries. With the mission of "Securing

Blockchain Ecosystem”, Beosin provides “All-in-one” blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance. You are welcome to contact us.