ABCDE

The Past, Present and Future of Bitcoin Ecosystem

C0 Preface

Bitcoin has been in existence for over 15 years. Initially, it was positioned as a peer-to-peer payment system, separate from any “ecosystem." Discussions regarding Bitcoin's scalability have been widespread since Bitcoin lacks Turing-complete smart contracts. We’ve been hearing about debates and controversies on Block Size, Hard Forks, Lightning Networks for years. New attempts to expand the Bitcoin ecosystem have never stopped.

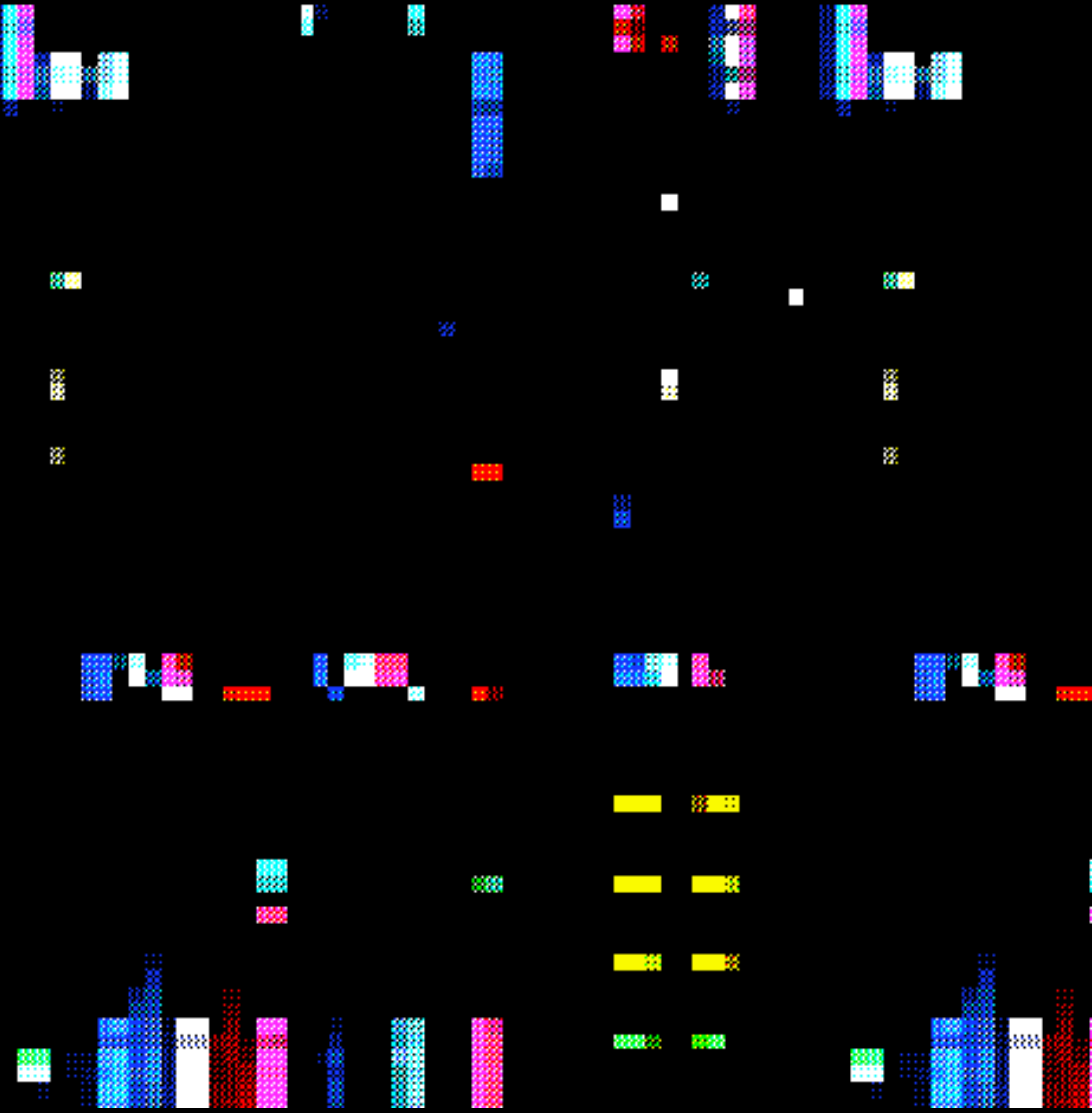
On March 8, 2023, Domodata introduced the concept of BRC20 and deployed $ORDI, which opened the Pandora's box of BTC. This led to the sudden appearance of numerous inscription assets on Bitcoin network, reminiscent of the Ethereum ICO in 2017. Assets like $ORDI and $SATS experienced exponential growth, with market cap exceeding $1 billion USD. The surge in the BRC 20 sector fueled continuous innovation and development across the entire Bitcoin ecosystem.

After the intense market attention, what lies ahead for the Bitcoin ecosystem? How did Bitcoin evolve from a peer-to-peer payment system to digital gold?

As we approach the end of 2023, on the eve of Bitcoin's halving, we present this report to reflect on Bitcoin's past, evaluate its current state, and look forward to its promising future.

This report is dedicated to all those who have contributed to the Bitcoin ecosystem.

> If you don’t believe me or don’t get it, I don’t have time to try to convince you, sorry.
>
> —— Satoshi Nakamoto



C1

The History of BTC: A Winding Path of Ecological Development

2018-2023 Bitcoin (BTC) Milestones: A Journey Through History

2008.11.01 Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System."

2009.01.03 Satoshi Nakamoto mined the genesis block on a small server in Helsinki, Finland: the first 50 bitcoins were created. A sentence is embedded in the genesis block from The Times stating, "The Chancellor is on the brink of a second bailout for banks," indicating both the time of the block and a critique of the banking crisis.

2009.01.12 Satoshi Nakamoto sent 10 bitcoins to developer Hal Finney, completing the first bitcoin transaction.

2010.05.21 Florida programmer Laszlo Hanyecz bought a pizza for 10,000 BTC, marking the first price of bitcoin at $0.0025/ BTC。

2010.07.17 Bitcoin exchange MT.GOX was founded in Tokyo.

2010.08.15 A bitcoin bug was discovered and exploited, generating over 184 billion bitcoins in a single transaction, which were sent to two addresses. This illegal transaction was quickly discovered and rectified.

2010.12.16 Pooled mining and the bitcoin mining pool got introduced.

2011.04.23 Satoshi Nakamoto sent his last email and disappeared completely. His email stated: "I've moved on to other things. Gavin and the others will take good care of Bitcoin."

2012.09.27 Bitcoin Foundation was established

2012.11.28 The block reward was halved for the first time, from 50 bitcoins every 10 minutes to 25. At the same time, the total number of bitcoins reached half of the total supply of 21 million.

2012.12.04 The Colored Coin whitepaper was released.

2013.08.15 MasterCoin ICO

2013.10.29 Canada launched the world's first Bitcoin ATM, manufactured by the American company Robocoin.

2013.12.05 The People's Bank of China and five other ministries issued a notice on preventing Bitcoin risk, triggering nearly a 30% drop in global Bitcoin prices.

2015.01 Coinbase became the first regulated Bitcoin exchange in the United States.

2015.09 The United States Commodity Futures Trading Commission (CFTC) rules that BTC is a commodity covered by the Commodity Exchange Act.

2016.07.10 Bitcoin halved for the second time. The reward per block drops from 25 to 12.5 bitcoins.

2016.08.03 Bitfinex, a well-known Bitcoin exchange overseas, lost bitcoins valued at over $60 million to a hack, causing the price to plummet by over 25%. Ultimately, all users on the platform shared the total asset loss of 36%, and Bitfinex issued debt tokens BFX for "debt-to-equity" conversion.

BITFINEX

2017.03.11 The U.S Securities and Exchange Commission (SEC) announced the rejection of the Bitcoin ETF, causing Bitcoin to drop by 10%. This was the first time a Bitcoin ETF proposal was rejected by the SEC.

2017.05.23 56 Bitcoin startups agreed to the Segwit2M (later changed to Segwit2x) compromise proposed by Barry Silbert, signing the New York Agreement.

2017.08.01 Bitcoin Cash was created from a hard fork of the original Bitcoin chain.

2017.08.24 Segregated Witness (SegWit) was officially activated.

2017.09.04 The People's Bank of China announced ICOs as illegal financial activities and suspends all domestic transactions, followed by the closure of all Bitcoin exchanges registered in the country.

2017.11.19 The price of Bitcoin surpassed $10,000 for the first time.

2017.12 BTC fostered the creation of 8 forked coins in December: SBTC, LBTC, BTP, GOD, BUM, Bitcoin Cash Plus, Bitcoin Silver, and Bitcoin X (Bitcoin Unlimited).

2017.12.11 The Chicago Options Exchange officially listed Bitcoin futures, which surged by more than 20% on the first trading day.

2018.01.01 RSK's main network went live.

2018.03.15 ⚡The Lightning Network released its first mainnet beta.

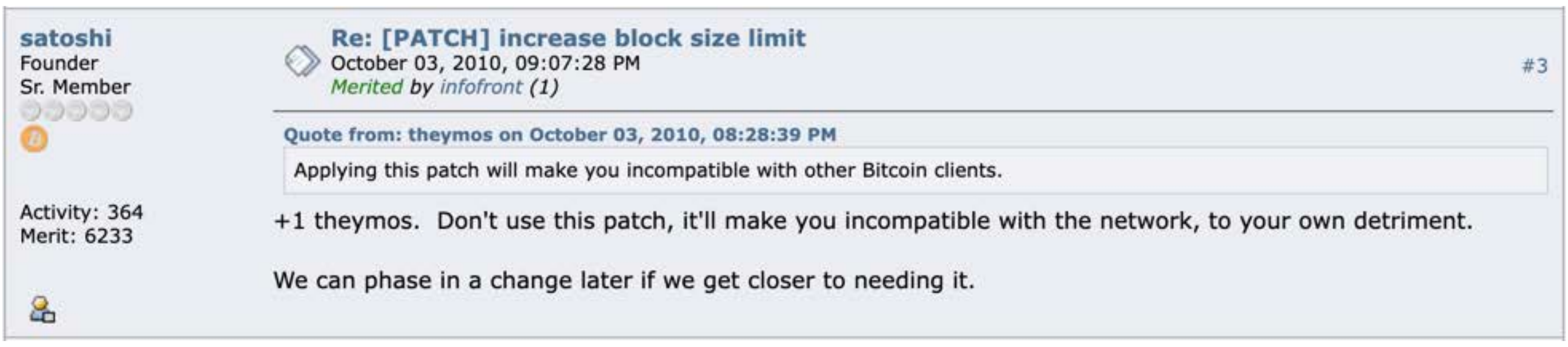
2018.09.27	Liquid Network went Live
2018.11.15	BSV forked
2019.09.23	Bakkt launched physically delivered Bitcoin futures contracts.
2020.03.12	Due to financial market panic, Bitcoin dropped more than 50% in one day.
2020.05.12	BTC halves for the third time, with the block reward now at 6.25 BTC.
2020.12.16	Bitcoin broke $20,000, setting a new all-time high.
2021.01.14	Stacks mainnet 2.0 went live.
2021.02.19	Bitcoin reached a market cap of $1 trillion for the first time.
2021.06.19	The Salvadoran Congress passed a bill making Bitcoin legal tender in the country, which came into effect 90 days later.
2021.11.16	Taproot upgrade officially went live.
2022.12.14	The Ordinals protocol was released.
2023.03.08	Domodata introduced the brc20 experiment and deploys $ORDI.
2023.10.19	Lightning Labs launched the first mainnet alpha version of Taproot Assets.

1.1 Should Bitcoin Be a Payment System or Digital Gold?

The debate on whether Bitcoin should function as a payment system or digital gold has been ongoing for quite some time. On June 17, 2010, Satoshi Nakamoto shared his thoughts on the Bitcoin forum:

"The design supports a tremendous variety of possible transaction types that I designed years ago. Escrow transactions, bonded contracts, third party arbitration, multi-party signature, etc. If Bitcoin catches on in a big way, these are things we'll want to explore in the future, but they all had to be designed at the beginning to make sure they would be possible later.”

Massive adoption and transaction volume imply more complex transaction instructions and larger transaction spaces. Between July and September 2010, Satoshi Nakamoto made multiple modifications to the BTC code, including the removal of two operation codes and disabling some functions of Bitcoin's programming language, Script. Initially, there was no limit on block size in BTC to accommodate the number of transactions within the same timeframe. However, when the early BTC price was very low, the cost of malicious transactions was also very low, leading to the need for a solution. On September 12, 2010, Satoshi Nakamoto presided over a soft fork, adding a limit that blocks could not exceed 1 MB. On October 4 of the same year, developer Jeff Garzik in his new client removed the limit introduced by Satoshi, which was opposed by the community and Satoshi himself. **Satoshi pointed out that this limit was temporary and could be raised in a controlled and gradual manner in the future to meet the need for expansion.**



satoshi
Founder
Sr. Member

Activity: 364
Merit: 6233

Re: [PATCH] increase block size limit
October 03, 2010, 09:07:28 PM
Merited by infofront (1)

#3

Quote from: theymos on October 03, 2010, 08:28:39 PM

> Applying this patch will make you incompatible with other Bitcoin clients.

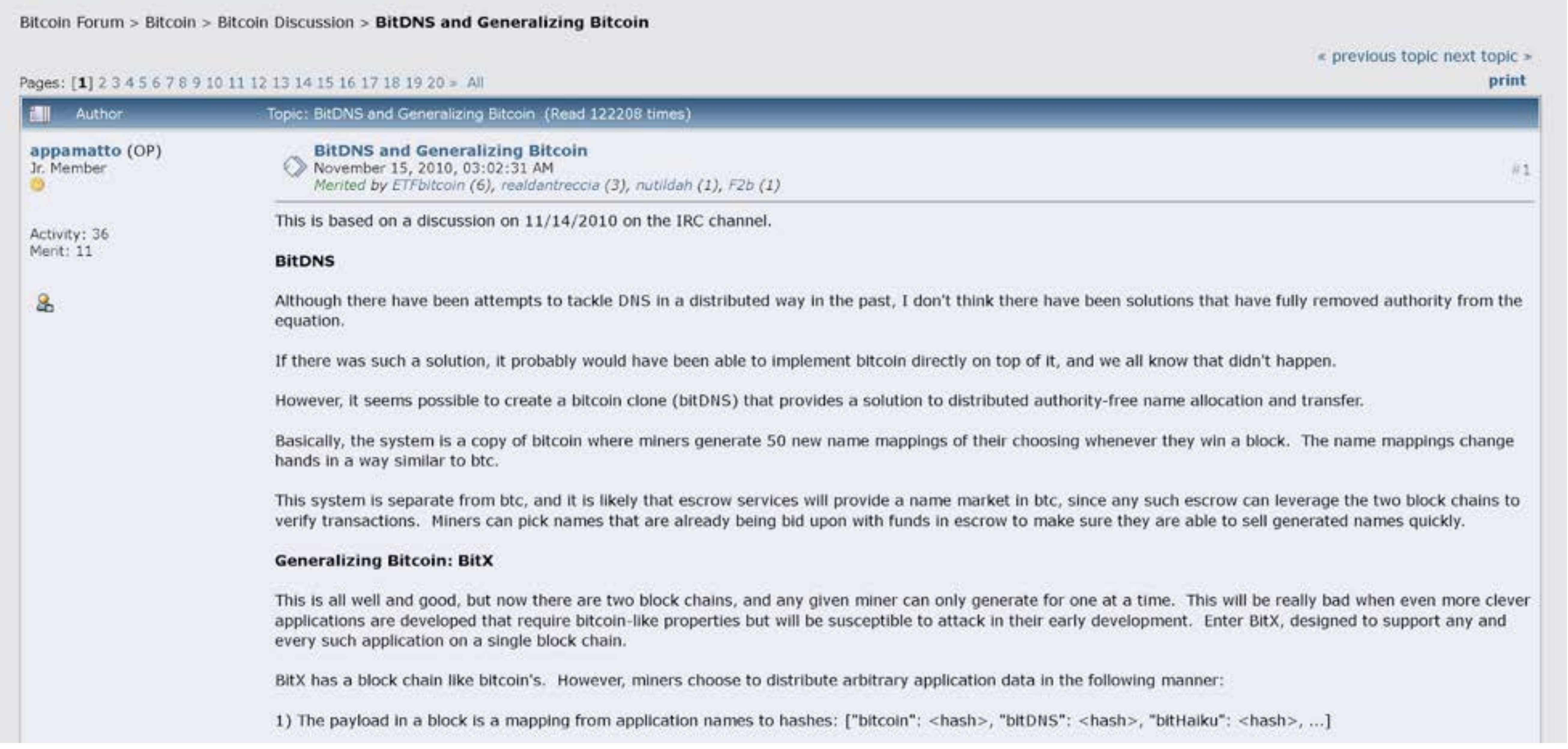
+1 theymos. Don't use this patch, it'll make you incompatible with the network, to your own detriment.

We can phase in a change later if we get closer to needing it.

Source： Bitcointalk

In December 2010, Satoshi Nakamoto, for reasons unknown, sent out his final public message and withdrew from the public eye. However, at that time, the issues surrounding BTC's positioning and scalability were still unresolved, and the 1MB limit set the stage for a series of subsequent debates.

During this period, discussions emerged on the Bitcointalk forum regarding Bitcoin applications beyond payments. For instance, in November 2010, Appamatto proposed the development of a decentralized domain name service on the Bitcoin network. However, this proposal did not gain recognition from early members, including Satoshi Nakamoto. Eventually, the proposed BitDNS evolved into Namecoin, marking the inception of the first altcoin in history.


Bitcoin Forum > Bitcoin > Bitcoin Discussion > BitDNS and Generalizing Bitcoin
« previous topic next topic »
Pages: [1] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 » All
print
Author
Topic: BitDNS and Generalizing Bitcoin (Read 122208 times)
appamatto (OP)
Jr. Member
Activity: 36
Merit: 11
#1

BitDNS and Generalizing Bitcoin
November 15, 2010, 03:02:31 AM
Merited by ETFbitcoin (6), realdantreccia (3), nutildah (1), F2b (1)

This is based on a discussion on 11/14/2010 on the IRC channel.

BitDNS

Although there have been attempts to tackle DNS in a distributed way in the past, I don't think there have been solutions that have fully removed authority from the equation.

If there was such a solution, it probably would have been able to implement bitcoin directly on top of it, and we all know that didn't happen.

However, it seems possible to create a bitcoin clone (bitDNS) that provides a solution to distributed authority-free name allocation and transfer.

Basically, the system is a copy of bitcoin where miners generate 50 new name mappings of their choosing whenever they win a block. The name mappings change hands in a way similar to btc.

This system is separate from btc, and it is likely that escrow services will provide a name market in btc, since any such escrow can leverage the two block chains to verify transactions. Miners can pick names that are already being bid upon with funds in escrow to make sure they are able to sell generated names quickly.

Generalizing Bitcoin: BitX

This is all well and good, but now there are two block chains, and any given miner can only generate for one at a time. This will be really bad when even more clever applications are developed that require bitcoin-like properties but will be susceptible to attack in their early development. Enter BitX, designed to support any and every such application on a single block chain.

BitX has a block chain like bitcoin's. However, miners choose to distribute arbitrary application data in the following manner:

1) The payload in a block is a mapping from application names to hashes: ["bitcoin": <hash>, "bitDNS": <hash>, "bitHaiku": <hash>, ...]

Source： Bitcointalk

1.2 Bitcoin 2.0: Asset Issuance

After Satoshi Nakamoto left, his successor, Gavin Andresen, took the lead in establishing Bitcoin Core and the Bitcoin Foundation. During this period, explorations of BTC's extensibility continued, particularly in the field of asset issuance.

- **Colored Coins**

Yoni Assia, CEO of eToro, was the first to propose the idea of colored coins in an article published on March 27, 2012. This idea evolved, and the concept of colored coins began to evolve and gain attention on forums such as Bitcointalk. Meni Rosenfeld eventually released a detailed whitepaper on colored coins on December 4, 2012. The concept of Colored coins is to represent a broader range of assets and values by adding special markings (i.e., Coloring) to specific parts of Bitcoin. Colored coins manifested in a series of entities, broadly classified into two categories:

Based on OP_RETURN: For example, Open Assets proposed by Flavien Charlon in 2013, utilizes OP_RETURN (introduced in Bitcoin v0.9.0, which can store a small amount of data on Bitcoin, initially limited to 40 bytes, later increased to 80 bytes). Operation codes are stored in the script and "colored" and traded through external reading. (This model is similar to how Ordinals relies on external indexing to determine asset legitimacy).

Not based on OP_RETURN: A typical example is the EPOBC Protocol proposed by ChromaWay in 2014. The extra information of EPOBC assets is stored in the nSequence field of Bitcoin transactions, and the category and legitimacy of each EPOBC asset need to be traced back to the genesis transaction to determine.

- **MasterCoin（Omin）**

On January 6, 2012, JR Willett introduced the concept of MasterCoin, which he referred to as "The Second Bitcoin Whitepaper." The project was officially launched through an ICO in July 2013 and managed to raise 5120 BTC (equivalent to $500,000). Unlike Colored Coins, MasterCoin implemented a comprehensive node layer that maintained a state model database by scanning the Bitcoin block.

This unique design allowed for more advanced functionalities, including the creation of new assets, decentralized exchanges, automated price feedback, and more. In 2014, Tether also launched a Stablecoin on Bitcoin through the Mastercoin protocol, the well-known Tether USD (OMNI).

- **Counterparty**

Counterparty was officially launched in 2014. It utilizes OP_RETURN to store data on the BTC network. Unlike colored coins, Counterparty represents assets not as UTXOs, but through OP_RETURN to indicate asset transfers. When an asset holder signs a transaction with specific data using the holding address, the asset is transferred. This approach allows Counterparty to serve as a platform for asset issuance, trading, and compatibility with Ethereum smart contracts.Moreover, some argue that Ethereum, Ripple, and BitShares also fall under the broader definition of "Bitcoin 2.0.”

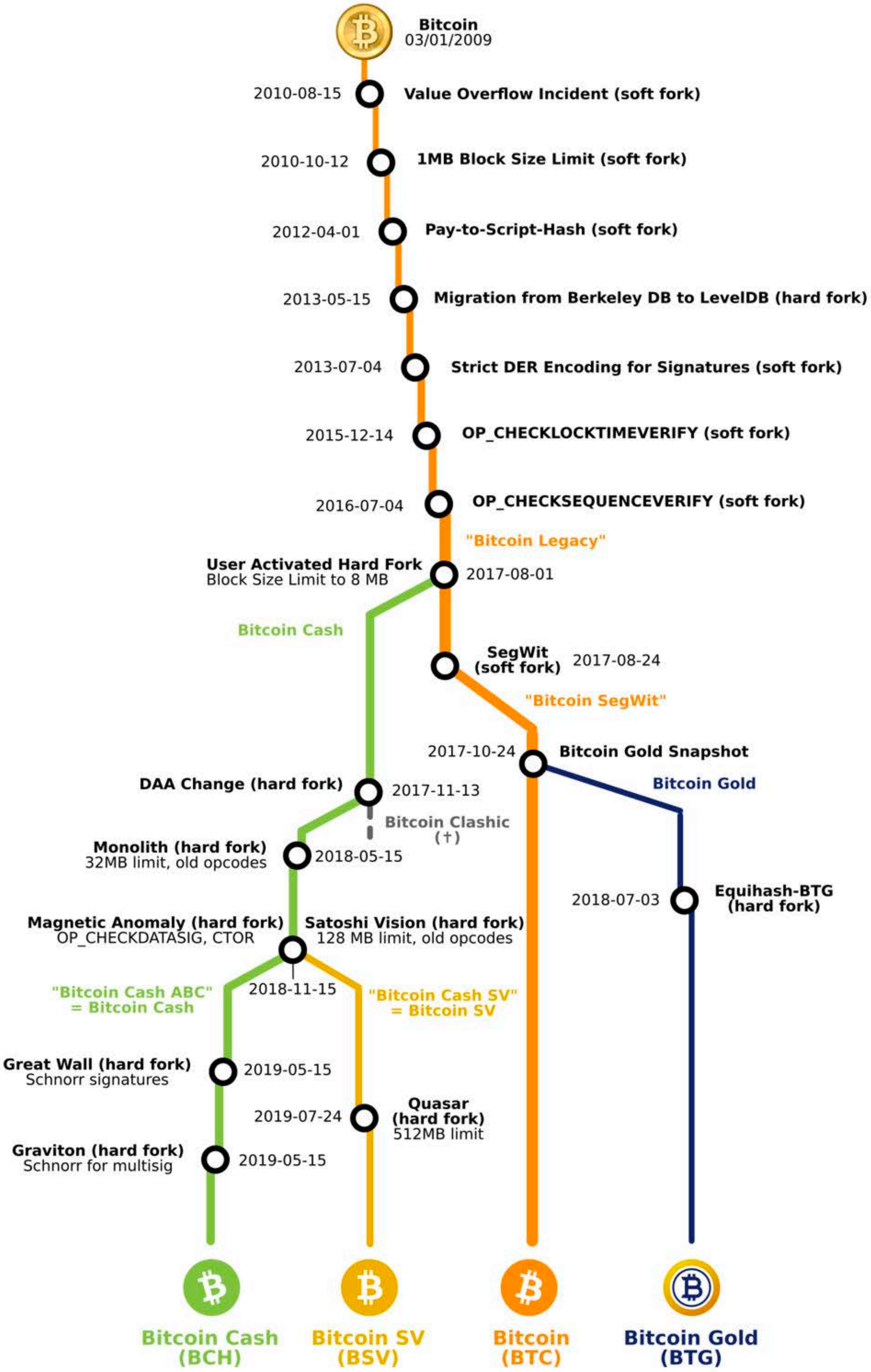
1.3 The Debate of Block Size and Hard Forks

As Bitcoin gained wider adoption, it faced increasingly serious issues such as network congestion and longer confirmation times. In 2015, Gavin Andresen and Mike Hearn proposed implementing the BIP-101 in the new version of BitcoinXT, aiming to increase the block size limit to 8 MB. However, core developers like Greg Maxell, Luke Jr, and Pieter Wuille opposed this idea, expressing concerns that it would raise barriers to running full nodes and have uncontrollable impacts. The debate expanded both in terms of the issues discussed and the number of participants involved.

There is no absolute superiority between the two routes. Insisting on the small block route fails to address the core question: "How can low transaction volumes maintain sufficient incentives to ensure security after block rewards are reduced?" Moreover, increasing to 8 MB would not be the ultimate solution; choosing the path of larger blocks would likely lead to continuous expansion, introducing technical risks associated with infinite scaling and unpredictability. **Ultimately, the root of this debate lies in answering the question: "What is the vision for Bitcoin?"**

The debate led to a community split and subsequent hard forks in 2017. Besides BCH and BSV, over 50 new forked coins emerged within a year, as reported by BitMEX Research.

Main Consensus Forks of Bitcoin (2009 — 2019)

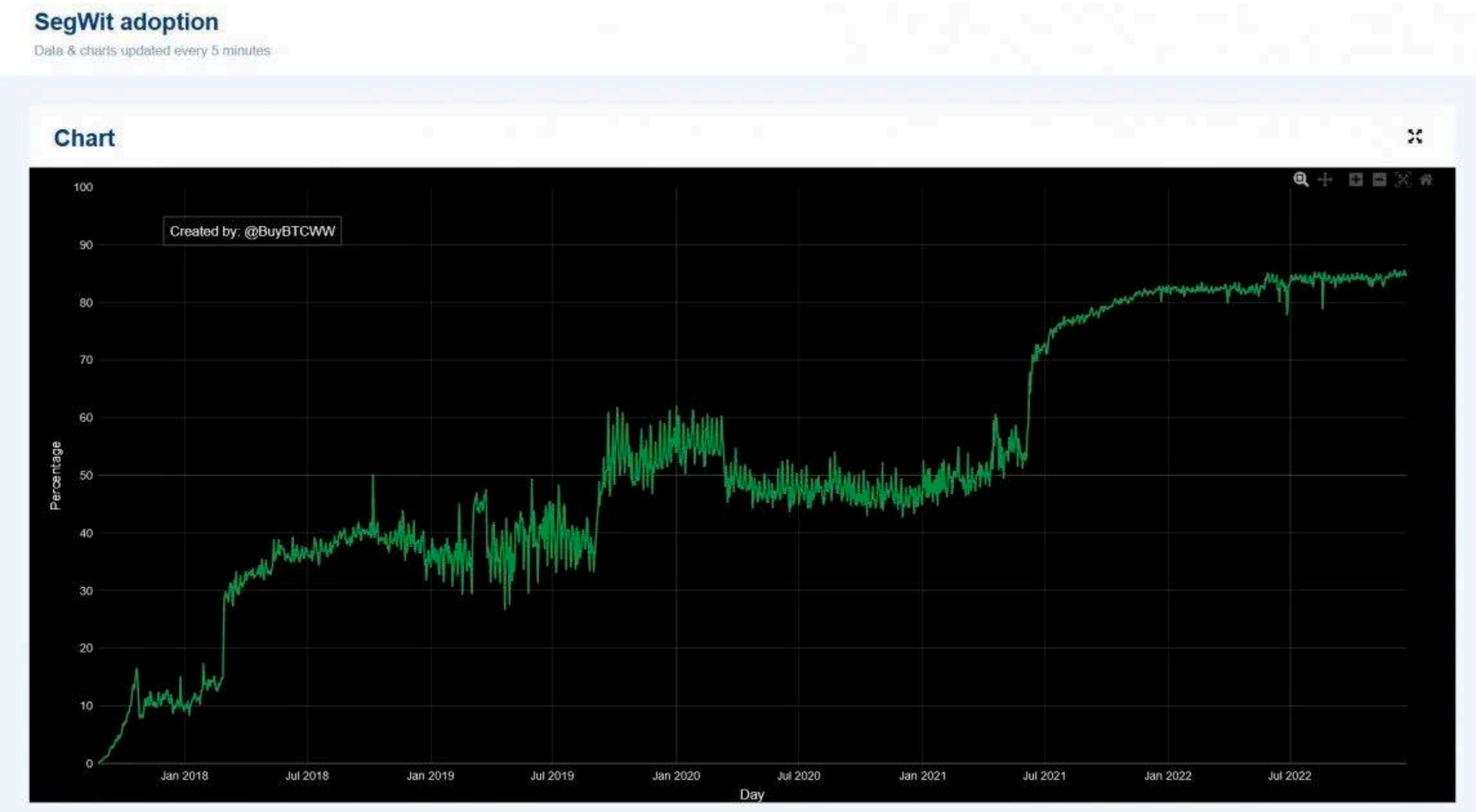


"Main Consensus Forks of Bitcoin" v3
@lugaxker / lugaxker#106;
Source: blog.bitmex.com/bitcoins-consensus-forks/

1.4 SegWit & Taproot

After the fork, the BTC chain gradually introduced a series of new technological proposals to improve scalability while maintaining the block size, among which SegWit and Taproot are the most important ones.

Segregated Witness (SegWit), as an alternative to directly increasing block size, was introduced concurrently with the BCH fork. SegWit divides a transaction into two parts, the first part contains the sending and receiving addresses, and the second part holds the transaction signatures or witness data, removing it from the main block but retaining the validation function. The removal of witness data allows for more transactions to be contained within the same block size, effectively increasing throughput. SegWit was introduced via a soft fork, and its adoption rate has steadily increased, exceeding 60% by 2020 and reaching 95% by December 2023.



Source: https://buybitcoinworldwide.com/stats/segwit-adoption/

In November 2021, a significant upgrade called Taproot was officially implemented as a soft fork. This upgrade combines BIP340, BIP341, and BIP342. BIP340 introduced Schnorr signatures, which can verify multiple transactions simultaneously, replacing the Elliptic Curve Digital Signature Algorithm (ECDSA). This expansion increases network capacity and speeds up batch transaction processing, enabling the deployment of complex smart contracts. BIP341 implemented Merkleized Abstract Syntax Trees (MAST) to optimize the storage of transaction data on the blockchain. Lastly, BIP342 (or Tapscript) adapted Bitcoin's scripting language to support Schnorr signatures and the implementation of Taproot.

It's worth noting that SegWit initially did not impose a limit on the length of the validation information, which allowed subsequent projects to circumvent the 1

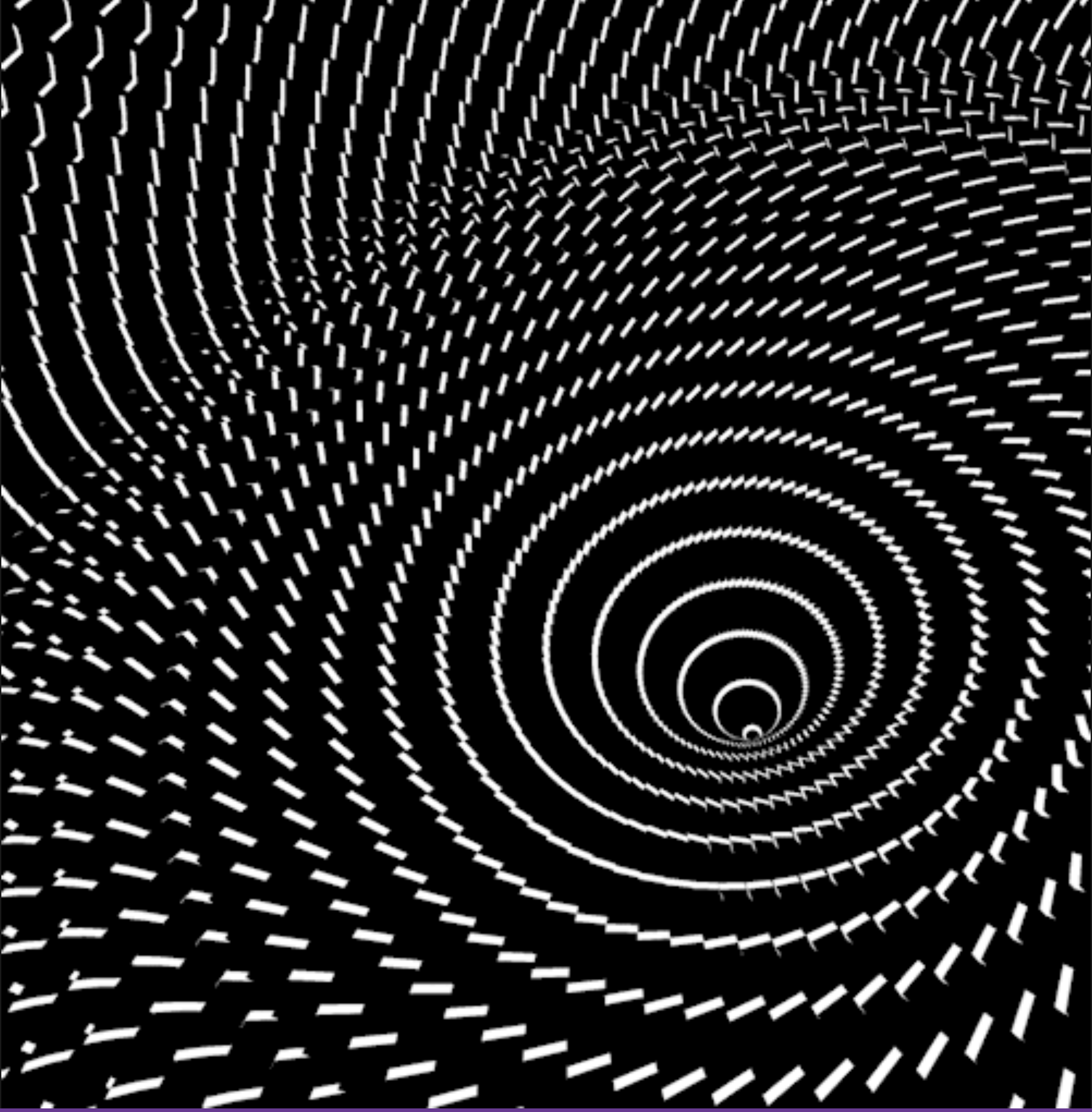
MB block size limit through the validation information method, laying the groundwork for the rise of Ordinals. There is controversy within the community about this approach. Some opponents believe that SegWit's failure to set a length limit was a "mistake," and therefore using validation information to transmit data is an improper "attack."

1.5 Early Exploration of Bitcoin Layer2

Following the resolution of the block size controversy, Bitcoin's Layer 2 solutions began to attract significant attention. The two most prominent options are the Lightning Network and Sidechains.

The Lightning Network was initially proposed in 2015 by Joseph Poon and Thaddeus Dryja. Its core concept involves locking a portion of Bitcoin within a multi-signature address, thus establishing a separate governance protocol. Transactions within the Lightning Network occur off-chain and are ultimately confirmed by the BTC network. In March 2018, Lightning Labs officially launched the Lightning Network on the Bitcoin mainnet, with notable applications such as Strike, Taro, and Lightspark.

Sidechains, on the other hand, aim to obtain or transfer Bitcoin from/to the Bitcoin network through transactions that are independent of the BTC network. The exploration of sidechain solutions began earlier, with Blockstream publishing the first technical paper on Bitcoin sidechain solutions in 2014, although the proposal was not fully implemented at the time. RSK released its whitepaper in 2015, and in January 2018, RSK successfully launched its fully functional mainnet. Later that year, in September, Blockstream launched the Liquid Network sidechain. Apart from RSK and Liquid Network, other sidechain solutions include Stacks, RootStocks, Drivechain, and more. Additionally, developers have also explored and experimented with approaches such as state channels and Roll-ups.



C2

BTC Ecosystem：Inscriptions Open Pandora's Box

Prior to the introduction of inscriptions, Bitcoin was not associated with the term "ecosystem" due to its inherent limitations in supporting Turing-complete smart contracts. The only ecosystems that could be considered, to some extent, were Lightning Network and Stacks. The primary focus revolved around solutions provided by "smart contract platforms," including ETH, L2, and various Alt L1s.

Unexpectedly, Ordinals disrupted the industry overnight with the concept of Inscriptions, attracting widespread attention. Ironically, the hype extended to other L1 & L2 chains such as Arbitrum and Solana. By the end of December, the majority of smart contract platforms had started to adopt inscriptions.

2.0 $ORDI Timeline

March 8: @domodata proposed the BRC20 experiment and deployed $ORDI.

March 9: $ORDI was fully minted, each at 5U.

March 10 to March 23: OTC(Over-the-counter) trading at around 0.03U.

March 23: UniSat launched the BRC20 market place, the price quickly rose up to 0.3U, but then the market was closed due to a double-spending problem.

April 27: UniSat relaunched the BRC20 trading market to a few particular users, the price of $ORDI rocketed to 1U and continued to rise.

May 5: Opensea announced support for Ordinals and BRC20. The market became FOMO, price reached 6U, various new BRC20s were hyped by various communities, like NALS,XING, OSHI, SHIB, etc.

May 8: $ORDI was listed on Gate.io, on the same day BTC's on-chain transaction fees accounted for 43.7% of miners' total income, after listing on Gate.io, the price surged from 9U to 20U.

May 9: $ORDI hit its peak at 28U, gate.io began to list various BRC20s like BANK, PIZA, as well as IRC20, DRC20, etc., diverting attentions from BRC20.

May 9 to May 12: As major holders sold off $ORDI and the overall market was sluggish, the price of $ORDI dropped to 7.5U. Market started to cool down.

May 12: OKX announced an official partnership with UniSat to jointly build BRC20 industry standards, a strong boost after which the price of $ORDI recovered, returning to 12U on the same day.

May 20: @OKX and @HuobiGlobal exchange listed $ORDI, the price rose from 12U to 15U, followed by a continuous decline for over four months.

September 11: The price fell below 3U, a dark day for $ORDI holders

October 18: UniSat released Brc20-swap, $ORDI began to recover. Since then, $ORDI started to take off.

November 3: The BRC20 ecosystem gained momentum, the price gradually rose to 6.2U, on the same day $SATS, another BRC 20 tokens, market value surpassed $ORDI.

November 7: Binance announced the listing of $ORDI, surging from 7.4U to 13.5U, beginning a comeback.

November 10 to December 1: Hovering around 20U.

December 2: $ORDI rose from 21.7U to 32U, surpassing the past ATH (all time high) in May.

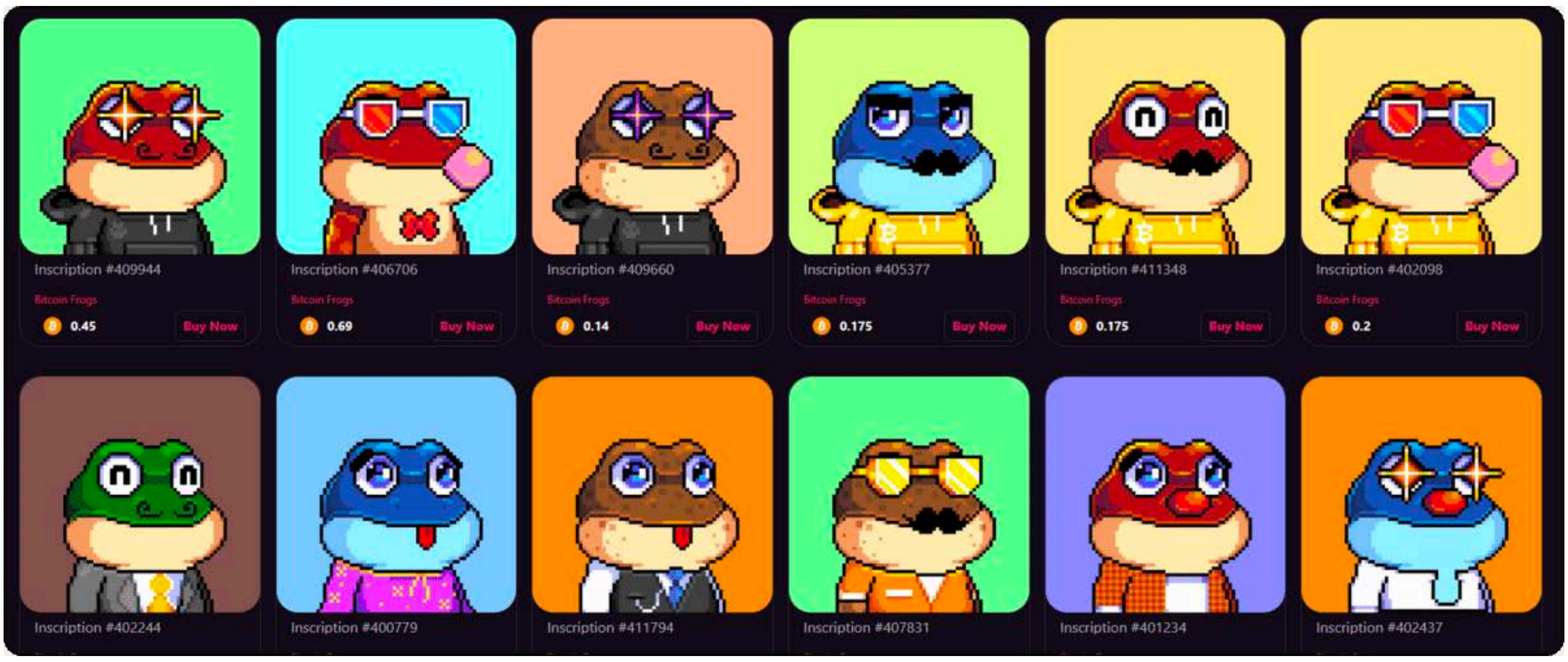
December 5: $ORDI rose to 69U, market value exceeded 1 billion US dollars.

2.1 Ordinals & BRC20

In summary, Ordinals are generally serve as protocol that utilizes BTC as a hard drive.

Thanks to the Taproot upgrade two years ago, the data volume limit for individual transactions in the segregated witness field was removed, allowing for a maximum data volume of 4M. This unintentionally gave BTC a "tamper-proof, permanent storage" quality, similar to Arweave.

Casey Rodarmor, the founder of Ordinal, was the one who opened Pandora's box. It is unlikely that he imagined the inscription ecosystem of BTC would evolve into what it is today when he created Ordinal.Ordinals are comparable to NFTs. However, unlike ETH or other public chains where NFT metadata is typically stored on IPFS or centralized servers, Ordinal's metadata is embedded in the transaction's Witness Data, as if it has been "inscribed" onto a specific Satoshi. This is where the term "Inscription" comes from.

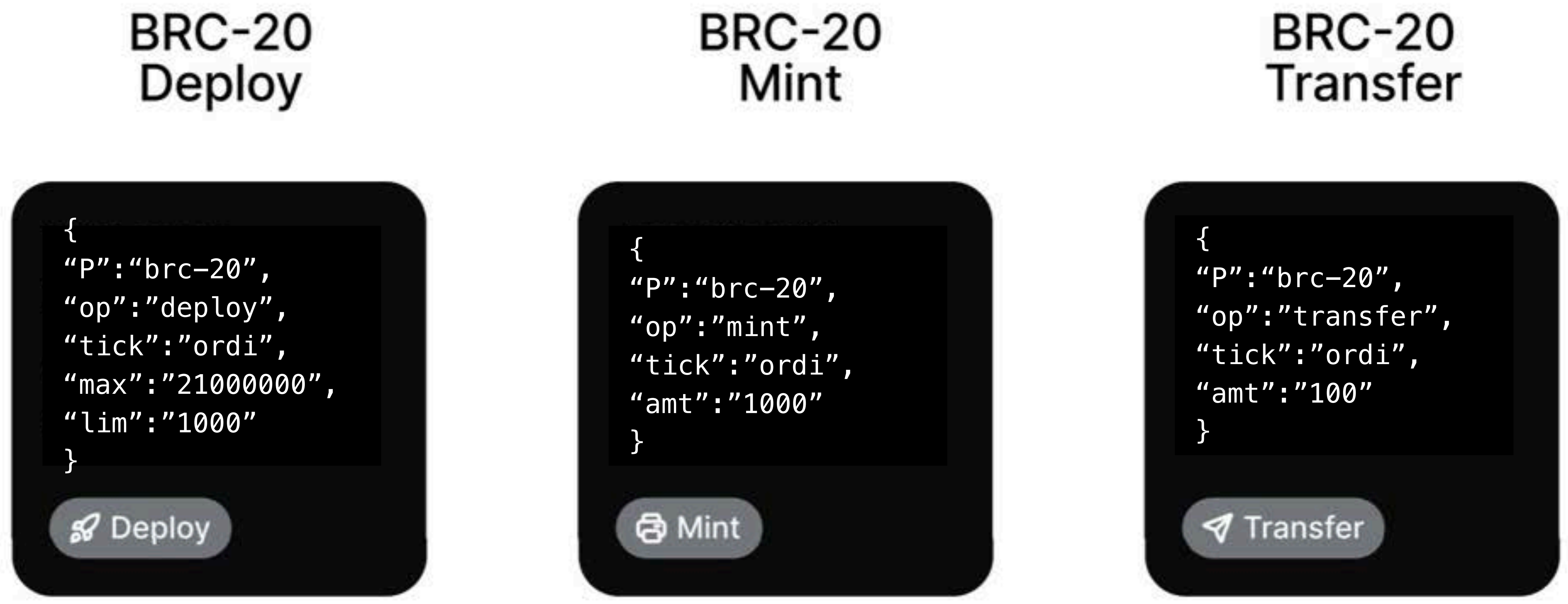


Source:BitcoinFrogs

Initially, Ordinal was characterized by its focus on the "hard drive" nature of Bitcoin's immutable and permanent storage. It allowed for metadata to support various content types such as text, images, videos, and more. Despite the 4MB size limit (which will become irrelevant with recursive inscriptions), BTC appeared to be the most suitable choice for an NFT platform. During this time, several ETH NFT clones, including BTC Punks and Apes, transitioned to BTC and gained popularity. Unexpectedly, Bitcoin Frogs emerged as the ultimate victor.

However, as the market evolved, it became clear that NFTs alone would not satisfy its demands. The non-fungible and illiquid nature of ordinals hindered the development of fungible tokens. This is where DOMO, a brilliant innovator, entered the scene. He leveraged the Ordinal protocol, which primarily focused on NFTs, and successfully simulated a fungible token mechanism similar to ERC20. This new token standard was named BRC-20.

Since Ordinal has no file format restrictions, a JSON file is also a viable option. With the help of three simple "operation codes" - Deploy, Mint, Transfer - BRC-20 was able to achieve a minting and transfer function similar to ERC-20, thanks to the help of an Indexer.



BRC-20 Deploy

```
{
“P”:“brc-20”,
“op”:”deploy”,
“tick”:”ordi”,
“max”:”21000000”,
“lim”:”1000”
}
```

BRC-20 Mint

```
{
“P”:“brc-20”,
“op”:”mint”,
“tick”:”ordi”,
“amt”:”1000”
}
```

BRC-20 Transfer

```
{
“P”:“brc-20”,
“op”:”transfer”,
“tick”:”ordi”,
“amt”:”100”
}
```

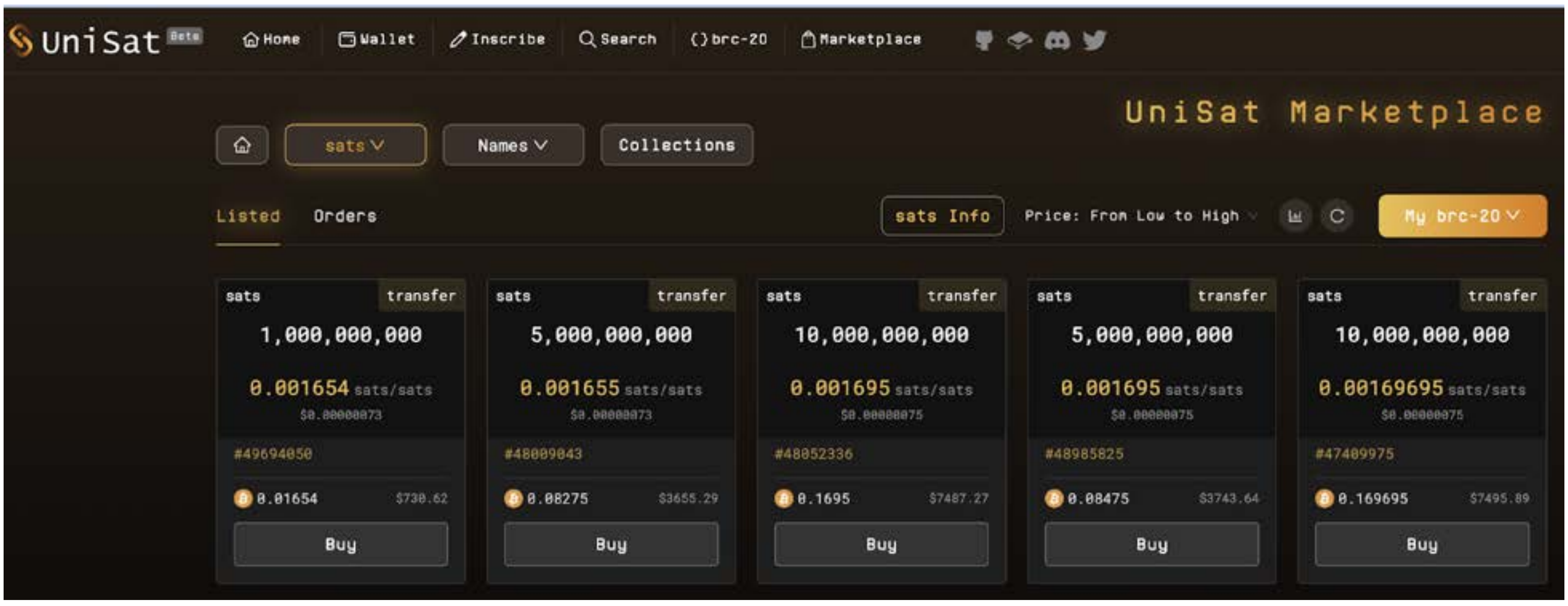
Indexers are now relatively centralized, providing the basic setup for searching all BRC20 on the Bitcoin chain. It indexes the amount of BRC20 tokens each person could hold based on the deploy, mint, and transfer operations.

There are three notable terms in the BRC20 ecosystem:

- **ORDI** - the first BRC20 token, setting the benchmark for the entire token landscape. While it may be considered a meme due to its application attributes, being the first holds significance. Without ORDI, there would not have been the subsequent hundreds of BRC20 tokens, nor the various XRC20 tokens that emerged in the BTC ecosystem, or the token systems that expanded to other major public chains.

- **SATS** - Due to a six-month minting period and countless zeroes after the decimal point, it has a more decentralized structure compared to ORDI. Endowed by Unisat to be the first "useful" inscription for BRC-20 Swap fees, Sats once surpassed the market value of the leading ORDI, and showed a trend to compete with ORDI for the top spot. Regardless of the outcome, ORDI and SATS have become the top market-recognized inscriptions.

- **UniSat** - Currently the most essential infrastructure in the BRC20 ecosystem. From the earliest proxy services to wallets, Indexers to the marketplace, Modules UniSat became the foundation of today's inscription ecosystem.



sats transfer	sats transfer	sats transfer	sats transfer	sats transfer
1,000,000,000	5,000,000,000	10,000,000,000	5,000,000,000	10,000,000,000
0.001654 sats/sats	0.001655 sats/sats	0.001695 sats/sats	0.001695 sats/sats	0.00169695 sats/sats
$0.00000073	$0.00000073	$0.00000075	$0.00000075	$0.00000075
#49694050	#48009043	#48052336	#48985825	#47409975
0.01654	0.08275	0.1695	0.08475	0.169695
$730.62	$3655.29	$7487.27	$3743.64	$7495.89
Buy	Buy	Buy	Buy	Buy

Source: UniSat

It is interesting to note that Casey, the founder of Ordinals, does not appreciate the BRC-20 inscription. He believes it will fill the Bitcoin block space with "junk UTXOs," potentially impacting regular BTC transfers. However, the popularity of BRC-20 has grown so extensively that its progression cannot be halted, regardless of anyone's intentions. As Inscriptions continues, the market sees the emergence of more refined XRC-20 assets.

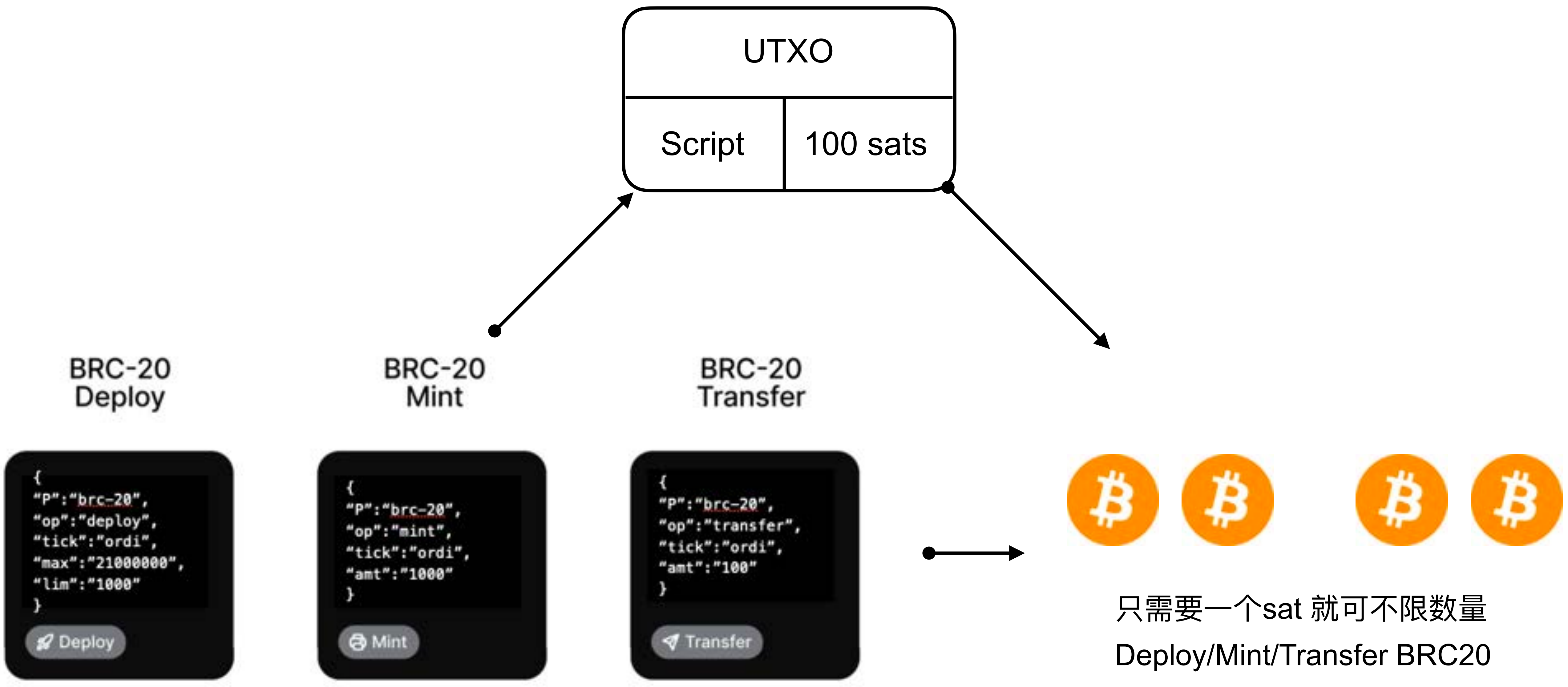
2.2 Atomicals: The Rising Star

If Ordinal in the BTC ecosystem is very much like BTC, then the one that resembles ETH is definitely the Atomicals protocol. Similar to BRC-20, the ARC-20 also supports the creation of various types of tokens on the Bitcoin blockchain. However, the fundamental design of ARC-20 and BRC-20 are not the same.

The ARC-20 fungible token standard brings colored coins to Bitcoin and uses each Satoshi in UTXO to represent ownership units of deployed tokens. UTXO itself can be combined in BTC transactions, making ARC20 tokens' programmability better'. **Theoretically, a swap between BTC and ARC20 could be achieved simply by swapping UTXO inputs and outputs.**

Unlike BRC20 which relies heavily on the indexer from minting to transferring, transactions of ARC20 are entirely dependent on BTC L1 (layer 1) UTXO and are completely independent of the indexer. Therefore, Atomicals avoid producing "junk UTXOs".

BRC20

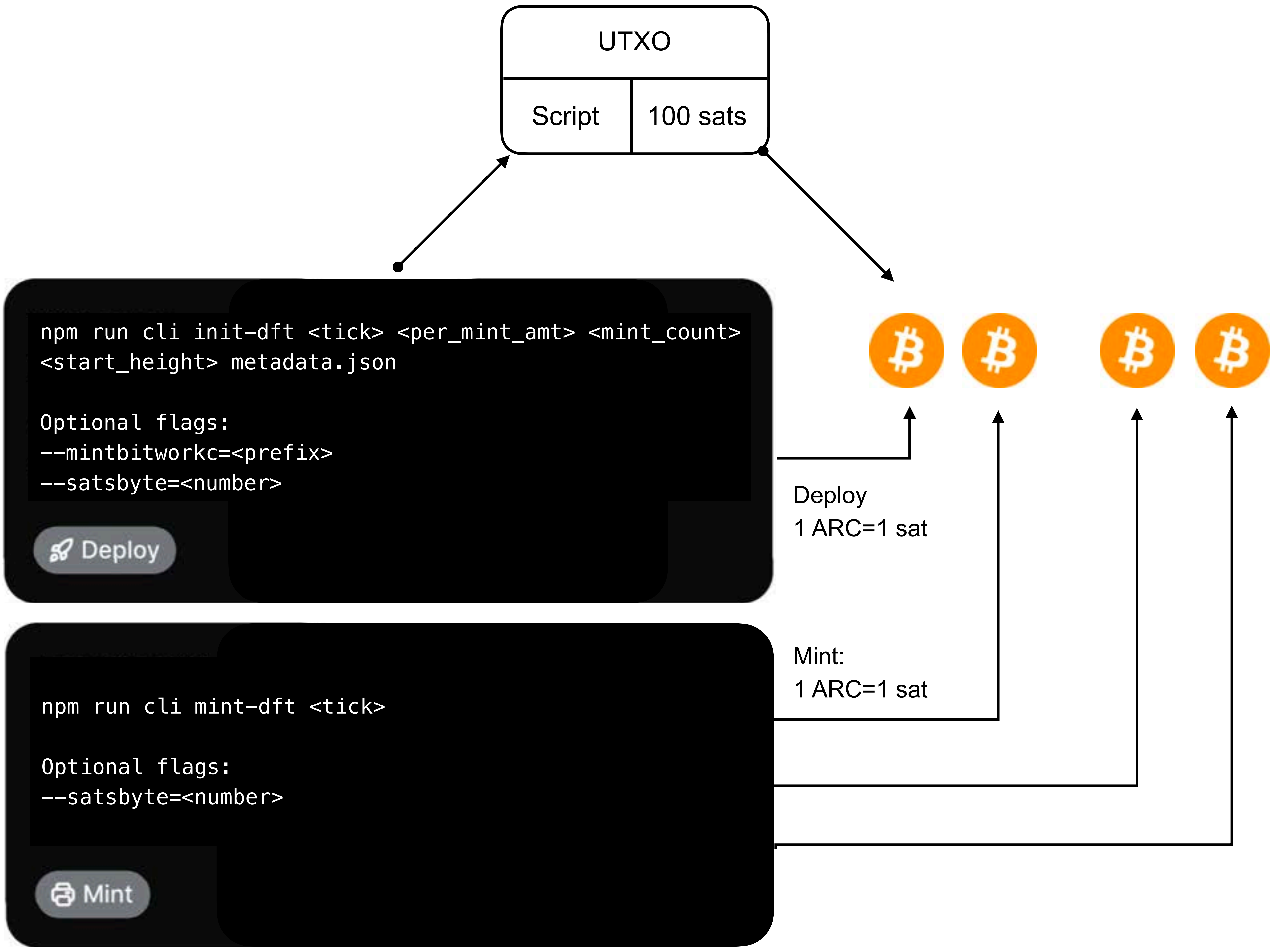


```
{
"P":"brc-20",
"op":"deploy",
"tick":"ordi",
"max":"21000000",
"lim":"1000"
}
```

```
{
"P":"brc-20",
"op":"mint",
"tick":"ordi",
"amt":"1000"
}
```

```
{
"P":"brc-20",
"op":"transfer",
"tick":"ordi",
"amt":"100"
}
```

ARC20



```
npm run cli init-dft <tick> <per_mint_amt> <mint_count>
<start_height> metadata.json

Optional flags:
--mintbitworkc=<prefix>
--satsbyte=<number>
```

```
npm run cli mint-dft <tick>

Optional flags:
--satsbyte=<number>
```

Of course, everything comes with a price. ARC20 brought higher asset issuance costs, and assets can easily be lost following the "spending" of UTXO. Another concern is its lagging infrastructure, which significantly lagged behind BRC20. (Fortunately, UniSat has already started supporting Atomical). Therefore, Atomical has a long way to go in catching up with Ordinal.

Lastly, there are some fun facts about Atomical:

The founder - Initially, many people viewed Atomical as a mere clone of Ordinal. However, upon joining the community, they quickly realized that it was far from being just another copy. Atomical boasted a lengthy development process, a determined founder, and an abundance of meticulously planned scenarios and features. It is truly a comprehensive protocol.In fact, some key opinion leaders (KOLs) went as far as comparing the anonymous founder of Atomicals to a young Steve Jobs, noting his rationality and vibe during multiple interviews. This enigmatic founder, with a Jobs-like style, sets the protocol apart.

Atomical's AVM - The ZeroSync team announced BitVM, a concept capable of computing anything on BTC. It's technically feasible but may take years to implement and is currently commercially unviable. Atomical's founder expressed enthusiasm and sees potential for their protocol. High hopes for AVM.

2.3. Rune & BRC100

- **Rune**

Casey, the founder of Ordinal, has always been dissatisfied with BRC-20 but was unable to do much about it. Taking inspiration from the Atomincal protocol (a blind guess since Atomical was released first), Casey introduced the Rune protocol for issuing Fungible Tokens-like inscriptions.

At the core level, Rune and Atomical are very similar. Both protocols write Token ID, output, and quantity information in the UTXO script, leaving the transfer to be handled by BTC Layer 1, and they are not heavily reliant on Indexer.The main difference is that Rune includes the specific number of Tokens in the script data, rather than following the 1 sat=1 token model. This allows for higher precision compared to ARC20, but also adds complexity and limits the ease of leveraging BTC UTXO composability like ARC20 does.

Interestingly, Casey's Rune protocol started as just an "idea" without a specific product. However, the founder of TRAC preemptively developed the first usable protocol based on this idea and released the pipe inscription.

Subsequently, a project called Rune Alpha emerged, introducing the Cook inscription. At first, everyone assumed it was Casey's project, but to their surprise, he denied any involvement. Despite the denial, market enthusiasm had already been ignited, resulting in sustained hype surrounding Cook's inscription.

- **BRC100**

BRC100 claims to function as an application protocol. It follows Ordinal Theory like BRC 20 but adds more concepts such as protocol inheritance, application nesting, state machine, models, and decentralized governance.

These improvements may enable the Bitcoin blockchain to support the development of native decentralized applications like AMM DEXs, lending platforms, SocialFi, GameFi in the future. The protocol is still under development. Please refer to the details to see the current status: https://docs.brc100.org/

2.4. SRC20 & BRC420

- **SRC20**

SRC20 was born out of the BTC Stamps protocol, which is a direct competitor rather than a derivative of Ordinal. There is an informative image available online that effectively highlights the distinctions between BTC Stamps and Ordinal.

BRC-20 VS SRC-20
BRC-20
data is stored in witness data, may be erased after a hard fork.
SRC-20
data is stored in spendable data transactions, cannot be erased.

In a direct comparison, Ordinal stores data in the segregated witness field, while BTC Stamps stores data in BTC transaction outputs.Naturally, within BTC Stamps, SRC20 is the Fungible Token version corresponding to BRC20.

The advantage of SRC20 over BRC20 is evident - the data stored in the segregated witness field is at risk of being "pruned" by full nodes, whereas transaction outputs are not. This makes SRC20 or BTC Stamps a definitively "permanent" protocol.

However, the downside is also clear - SRC20 is expensive. While BRC20 minting costs range from 3-5 USD, SRC20 can cost around 30-50 USD, representing a significant cost differential of 5-10 times.

Overall, SRC20 appears to be more favored by developers in the West, as it is pursued to counter the Eastern BRC20 ecosystem.

- **BRC420**

BRC420 is a "BTC Metaverse protocol" introduced by the Recursiverse team (https://twitter.com/rcsvio?lang=en). Unlike previous asset issuance protocols, BRC420 focuses more on the application layer and is known for its complexity.

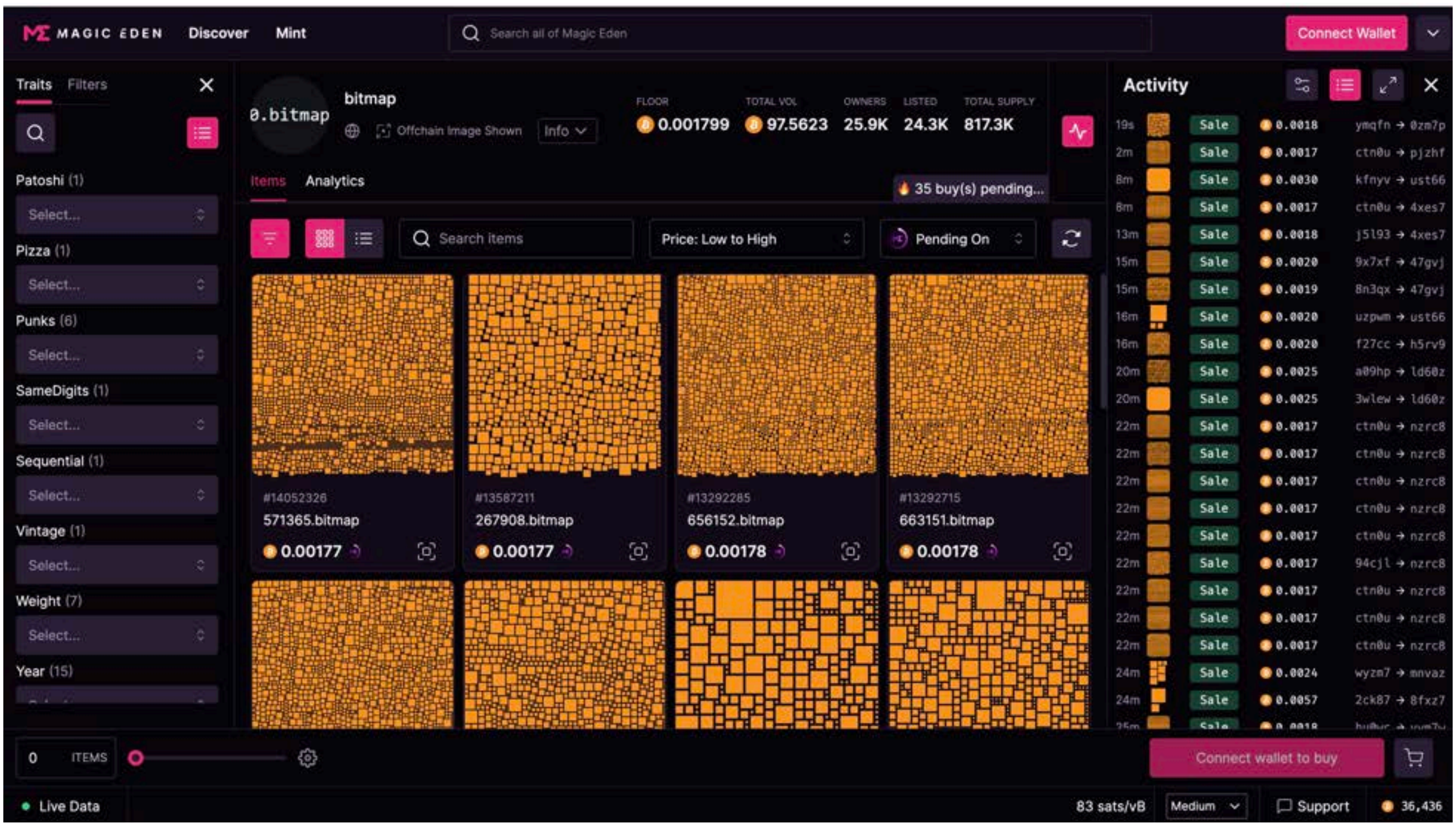
BRC420 introduces three interesting innovations:

A. New Assets Types: BRC420 has introduced more complex asset formats using recursion, which involves combining multiple inscriptions to create intricate inscriptions. This allows for the creation of various metaverse inscriptions, such as game characters, game DLC, HTML scripts, music, videos, and more. The ultimate goal is to achieve "on-chain inscription modularization."

B. On-Chain Royalties: By enabling recursive module assets' mutual calls, on-chain assets can encompass everything from characters and pets to entire game scripts, virtual machines, or even large AI models. Implementing a fair and automated royalty system can incentivize a thriving developer ecosystem, fostering the creation of more valuable modules on the chain.

C. Bitmap: The concept of Bitmap is fascinating and advanced. It can be seen as a BTC-based Sandbox land but with even greater native capabilities.
Each .bitmap inscription corresponds to a block on Bitcoin, with the number increasing in sync with the blocks. Currently, there are over 810,000 Bitmaps,

with an annual addition of 50,000. With more than 20,000 unique holder addresses, it ranks second only after ORDI and SATS.



0.bitmap bitmap

Offchain Image Shown

FLOOR	TOTAL VOL	OWNERS	LISTED	TOTAL SUPPLY
0.001799	97.5623	25.9K	24.3K	817.3K

35 buy(s) pending...

#14052326	#13587211	#13292285	#13292715
571365.bitmap	267908.bitmap	656152.bitmap	663151.bitmap
0.00177	0.00177	0.00178	0.00178

0 ITEMS

Activity

19s	Sale	0.0018	ymqfn → 0zm7p
2m	Sale	0.0017	ctn0u → pjzhf
8m	Sale	0.0030	kfnyv → ust66
8m	Sale	0.0017	ctn0u → 4xes7
13m	Sale	0.0018	j5l93 → 4xes7
15m	Sale	0.0020	9x7xf → 47gvj
15m	Sale	0.0019	8n3qx → 47gvj
16m	Sale	0.0020	uzpwm → ust66
16m	Sale	0.0020	f27cc → h5rv9
20m	Sale	0.0025	a09hp → ld60z
20m	Sale	0.0025	3wlew → ld60z
22m	Sale	0.0017	ctn0u → nzrc8
22m	Sale	0.0017	ctn0u → nzrc8
22m	Sale	0.0017	ctn0u → nzrc8
22m	Sale	0.0017	ctn0u → nzrc8
22m	Sale	0.0017	ctn0u → nzrc8
22m	Sale	0.0017	94cjl → nzrc8
22m	Sale	0.0017	ctn0u → nzrc8
22m	Sale	0.0017	ctn0u → nzrc8
22m	Sale	0.0017	ctn0u → nzrc8
24m	Sale	0.0024	wyzm7 → mnvaz
24m	Sale	0.0057	2ck87 → 8fxz7

83 sats/vB

36,436

Although BRC420 does not own Bitmap, it holds the title of being its biggest promoter and dominates over 95% of the browser traffic. With more than a hundred teams issuing assets on BRC420, it has become an application protocol intricately linked to Bitmap.

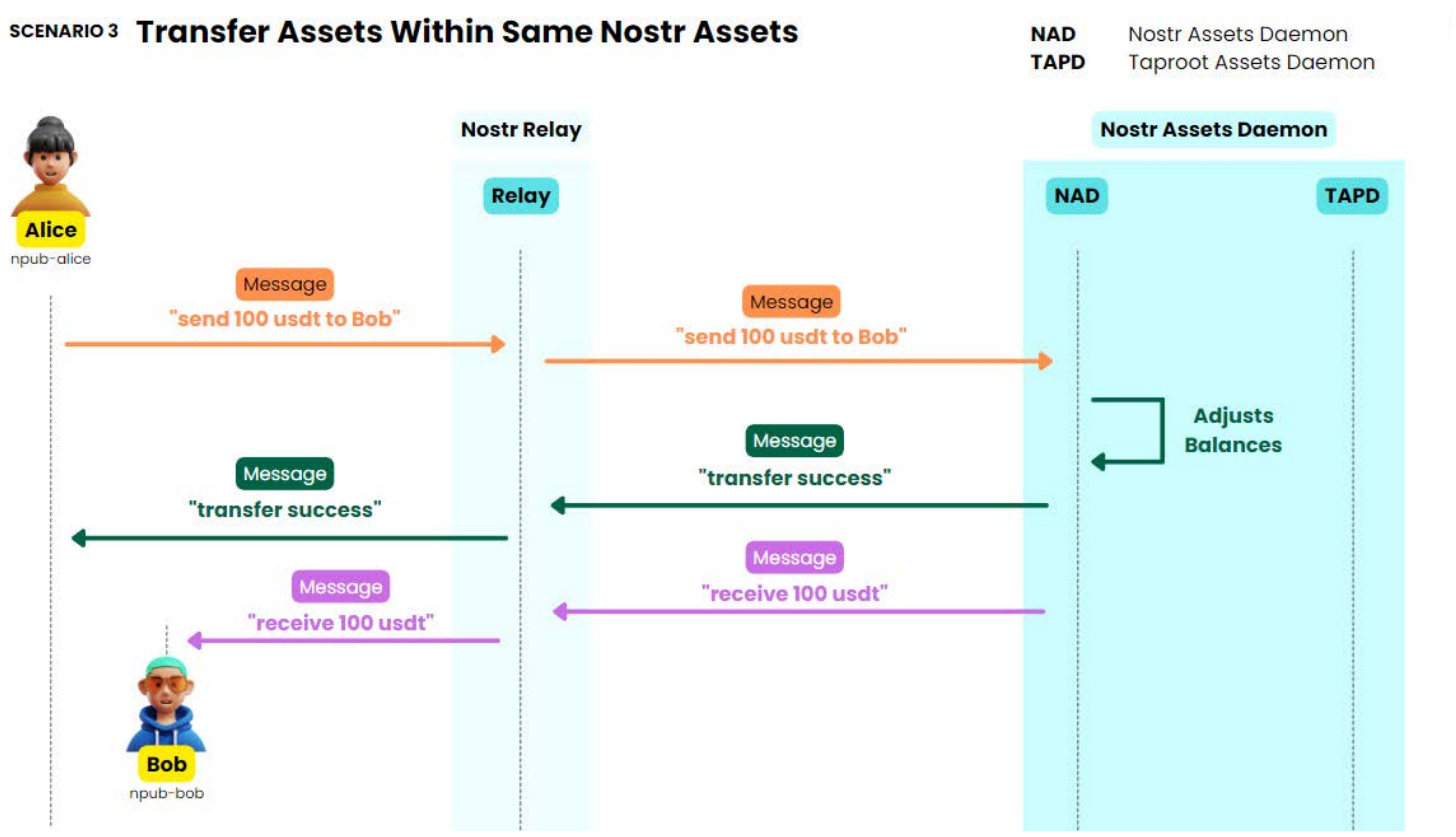
2.4. Taproot Asset & RGB

These two technological solutions are considered strong contenders for BTC's long-term scaling solutions, known as Client Side Validation.

One notable solution is the Nostr Asset Protocol within Taproot Assets. Despite common misconceptions, Nostr Asset and Nostr, the decentralized social networking message protocol, are not the same. Nostr Asset does not utilize the Nostr protocol to issue assets. Instead, it functions as an application on Nostr, leveraging Nostr messages to manage custodial wallets.

This allows users to send and receive Taproot Asset assets through Nostr's public and private keys at the protocol layer. The project team has faced controversy regarding the name for some time.

In the first half of next year, Taproot Assets will undergo integration testing with the Lightning Network. If successful, we can anticipate more Taproot Asset issuances and new applications on the Lightning Network side within the next 6-12 months.



SCENARIO 3 Transfer Assets Within Same Nostr Assets

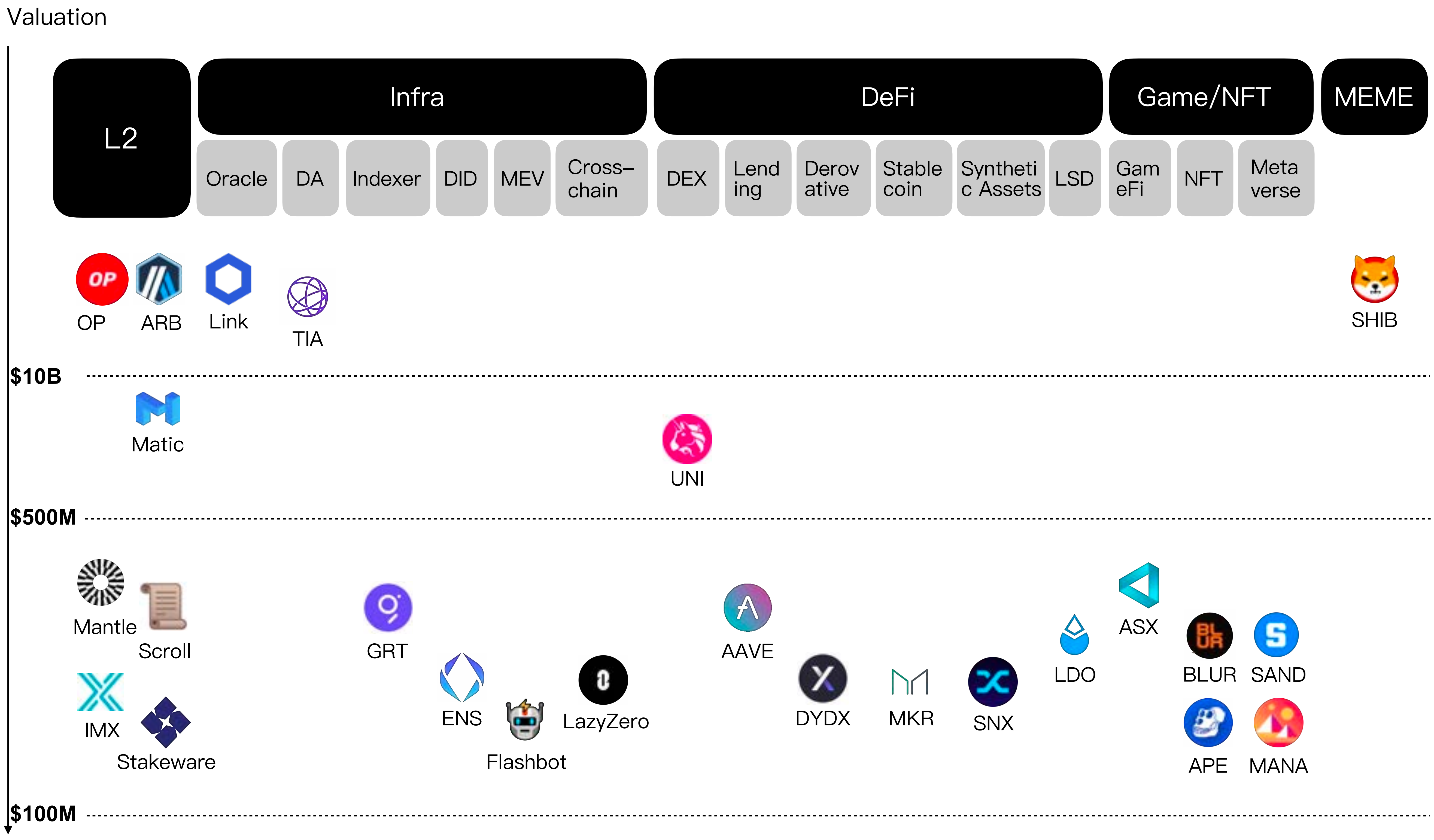
NAD Nostr Assets Daemon
TAPD Taproot Assets Daemon

Although RGB has missed out on the current hot BTC ecosystem, it remains one of the best scaling solutions for BTC in the long run. Its support for smart contracts gives it an edge in scalability and flexibility over Taproot, especially with Tether's interest in issuing USDT on RGB. The number of teams developing on RGB far exceeds those working on Taproot Assets.

However, discussions with several RGB and Taproot developers reveal that RGB currently faces significant technical challenges in integrating with the Lightning Network. As a result, the Liquid sidechain may serve as a "temporary choice" for RGB in the short term. Founder Maxim is even considering launching a new Layer 1 to host RGB. From a standpoint of legitimacy, the Lightning Network is undoubtedly the best choice. However, whether the technical compatibility issues can be overcome is a question that only time can answer.

C3

The Future of Bitcoin: Stepping into a Golden Age



As we envision the future of the Bitcoin ecosystem, we can anticipate thrilling innovations and transformations in numerous critical domains. It has the potential to emulate the achievements seen in the Ethereum ecosystem over the past few years.

1. Layer 2 Solution

Bitcoin network's Layer 2 solutions aim to tackle network congestion and high transaction fees. For instance, BSquared, an EVM Compatible Layer2, offers an off-chain transaction platform supporting Turing-complete smart contracts. This enhances transaction efficiency and reduces costs. By integrating Zero-Knowledge Proofs (ZKP) technology with Bitcoin's Taproot, these solutions also ensure improved transaction privacy and security. In fact, this project can achieve transaction costs that are 50 times cheaper and speeds 300 times faster than BTC. The team actively encourages developers to build various DeFi and NFT platforms on the chain, with the ultimate goal of developing Bitcoin into a dynamic platform. Additionally, Bitmap and Babylon are also working on their own Layer 2 services. Bitmap, leveraging its strong community and influence in asset protocols on Layer 1, possesses a significant advantage in the Layer 2 ecosystem. Similarly, Babylon can tap into the massive traffic generated by BTC collateral to empower the construction of Layer 2.

2. Asset Issuance and Trading

In the future Bitcoin ecosystem, we can expect to see the emergence of more asset issuance and trading platforms. These platforms will enable users to create and trade various digital assets. In this regard, Bitmap has introduced the BRC420 protocol, which takes a different approach compared to protocols like Ordinals.

The BRC-420 protocol creatively combines multiple inscriptions into a complex inscription, deviating from the traditional 'single inscription' method. This means that users can create chain assets ranging from character images or pets to complete game scripts, virtual machines, or even large AI models. Developers can then purchase these assets or pay royalties for their use.

The BRC-420 protocol consists of two parts. The first part is the Metaverse Standard, which defines an open format for assets in the metaverse. The second part is the Royalty Standard, which establishes a blockchain protocol for the creator economy.

3. Stablecoins

Stablecoins play a crucial role in the Bitcoin ecosystem by offering a stable digital asset to mitigate volatility. This enhances Bitcoin's utility as a reliable store of value.

BitSmileyDAO offers peer-to-peer lending based on BRC20, as well as insurance and CDS derivatives built upon this lending. Additionally, they have established partnerships with several BTC Layer2 platforms to provide Stablecoins and DeFi ecosystem products. BitUSD's over-collateralized mechanism is similar to MakerDAO.

At the coinage level, users can collateralize BTC by either using Wrapped BTC on the cooperative Layer2 or bridging BTC using BitSmiley's official bridge. This allows them to mint bitUSD. BitSmiley fills a critical gap in the current BTC ecosystem with its 'inscriptions form Stablecoin' and opens new doors in BTC DeFi with its lending, insurance, and CDS derivative solutions. It has quickly become an indispensable key component project in the BTC ecosystem.

4. Lending & Borrowing

As Bitcoin popularity grows, lending platforms will expand services for Bitcoin holders, including borrowing and earning interest. This will further financialize Bitcoin and attract traditional financial institutions.

Babylon allows Bitcoin holders to stake their idle Bitcoins. This not only enhances the security of Proof-of-Stake (PoS) chains but also enables users to earn profits in the process. Babylon proposes a Bitcoin staking protocol that eliminates the need to bridge to a PoS chain, ensuring full and reducible security guarantees for the chain. Additionally, the protocol supports rapid unbonding, maximizing liquidity for Bitcoin holders. Its modular plug-in design makes it compatible with various PoS consensus algorithms, providing a solid foundation for building resettable protocols.

5. Bridging

In the future, cross-chain technology in the Bitcoin ecosystem will mature, enabling interoperability between different blockchains. This will enhance the synergy of the blockchain ecosystem, facilitating cooperation and interaction between projects. To explore DeFi applications in the Bitcoin network, BTC assets can be efficiently brought into public chains like Ethereum with smart contract functionality.

Polyhedra Network introduces a Bitcoin cross-chain messaging protocol based on zkBridge, improving the interoperability of the Bitcoin network. This innovation enables secure interaction between the Bitcoin network and other blockchain networks. The protocol represents a major advancement in blockchain technology, opening up possibilities for interactions between Bitcoin and various blockchains.

6. Applications

The future holds great potential for applications built on Bitcoin, spanning across various domains. These decentralized applications will offer users more reliable solutions due to Bitcoin's security and immutability. Among these applications, Bitmask stands out as the most popular and flagship wallet used on RGB. It features an in-built Marketplace (Coming Soon) that enables the trading of RGB assets. Furthermore, the team plans to launch the launchpad section in the next phase. RGB, being a 'native scaling' solution, is technically and logically the most compatible with BTC. Notably, RGB V0.1 has been officially released for half a year, with V0.11 Alpha set to be released soon. As a result, the RGB ecosystem is expected to gain momentum within the next six months, aligning perfectly with Bitcoin's halving event.

7. MEV

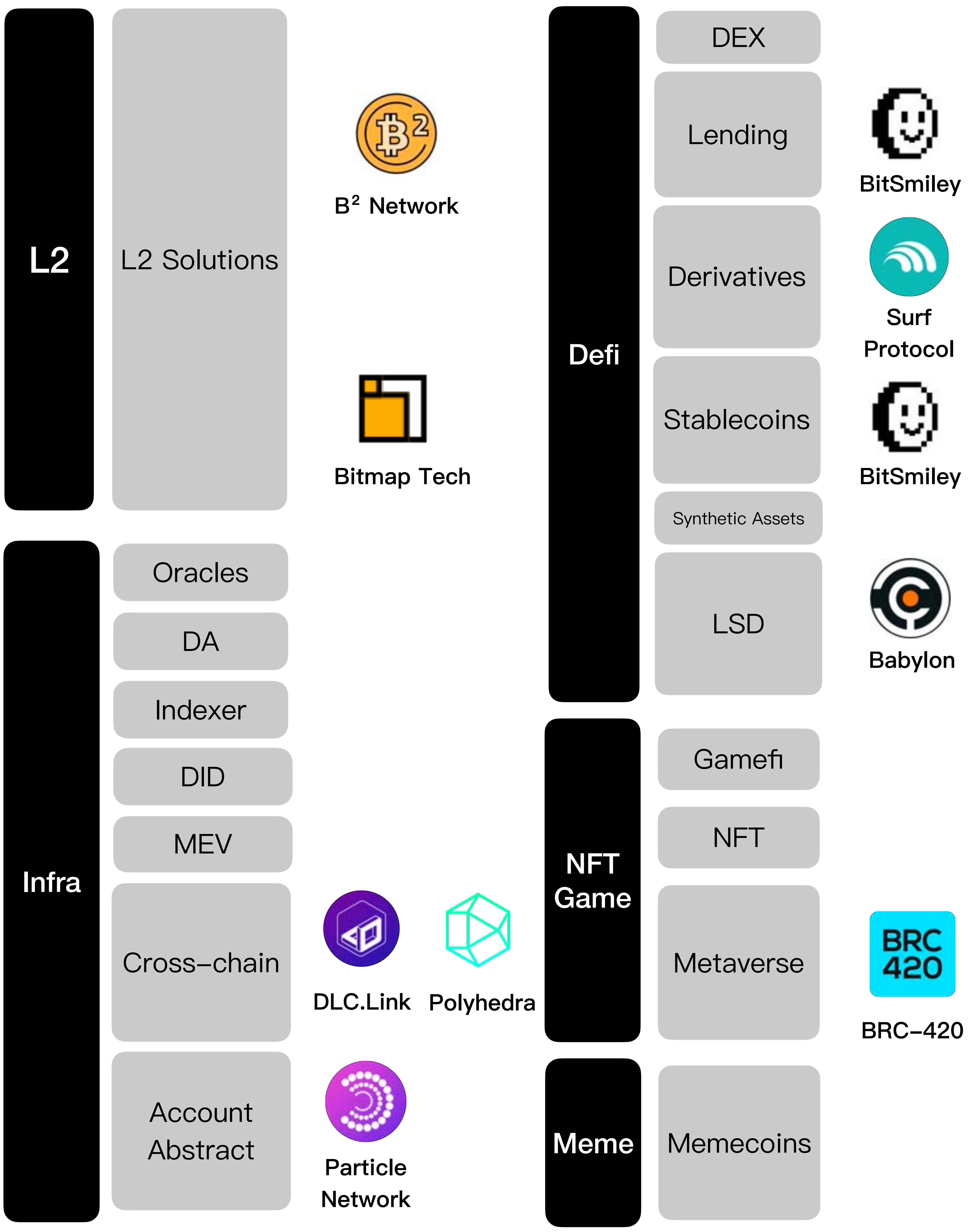
MEV, a characteristic of the Proof-of-Work (PoW) mechanism, has theoretical applicability to Bitcoin. During the BRC20 hype, a Bitcoin OG created an MEV machine called 'Sophon' to protect BTC from dust attacks through inscriptions. 'Sophon' utilizes a front-running strategy to swiftly deploy tokens with the same name, setting the supply to 1, and ensuring priority deployment by paying high gas fees. This effectively prevents others from deploying tokens with the same name. The introduction of Sophon led to a rapid fluctuation in the number of BRC-20 tokens, serving as an experiment in BTC MEV.

In practice, Bitcoin transactions primarily involve simple Bitcoin transfers, resulting in relatively limited opportunities for MEV. However, with the introduction of more complex transactions such as Taproot or Layer 2 solutions, the potential for MEV may increase. This is especially relevant after all Bitcoins are mined, as MEV could potentially become a new source of mining income. Currently, there are no economic incentives for miners to actively seek MEV, but we can anticipate the emergence of ecosystem projects like Flashbots on BTC Layer 2 in the near future.

These innovations and transformations will shape the future of the Bitcoin ecosystem, making it more usable, scalable, and applicable. This vision is not merely a preliminary imagination but a hopeful prospect. The actual development in the future will benefit from continuous technological progress, collaborative cooperation within the community, and the market's ongoing demand for innovation.

Portfolio Overview

ABCDE Capital (BTC Eco) Portfolio



L2
L2 Solutions
B² Network
Bitmap Tech

Infra
Oracles
DA
Indexer
DID
MEV
Cross–chain
DLC.Link
Polyhedra
Account Abstract
Particle Network

Defi
DEX
Lending
BitSmiley
Derivatives
Surf Protocol
Stablecoins
BitSmiley
Synthetic Assets
LSD
Babylon

NFT Game
Gamefi
NFT
Metaverse
BRC–420

Meme
Memecoins

About Us

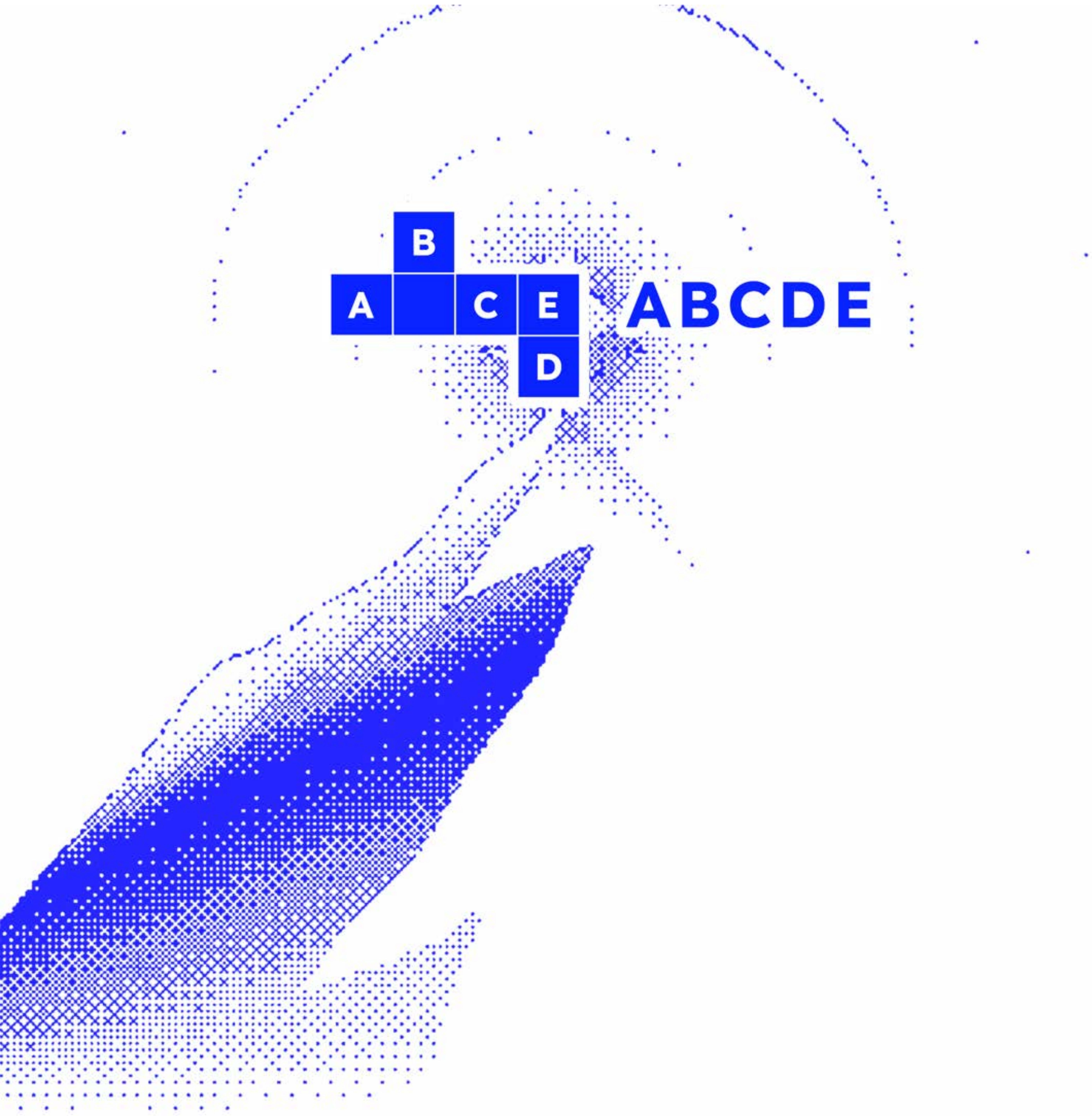
ABCDE is a 400m fund co-founded by Huobi cofounder Du Jun and former Internet&crypto founder BMAN. Before ABCDE, we have built multi-billion dollar companies in Crypto from the ground up, including HongKong listed companies with crypto licenses(01611.HK), exchanges(Huobi), SAAS companies(ChainUP.com), media(CoinTime.com), and developers platforms(BeWater.xyz).

Twitter: @ABCDELabs

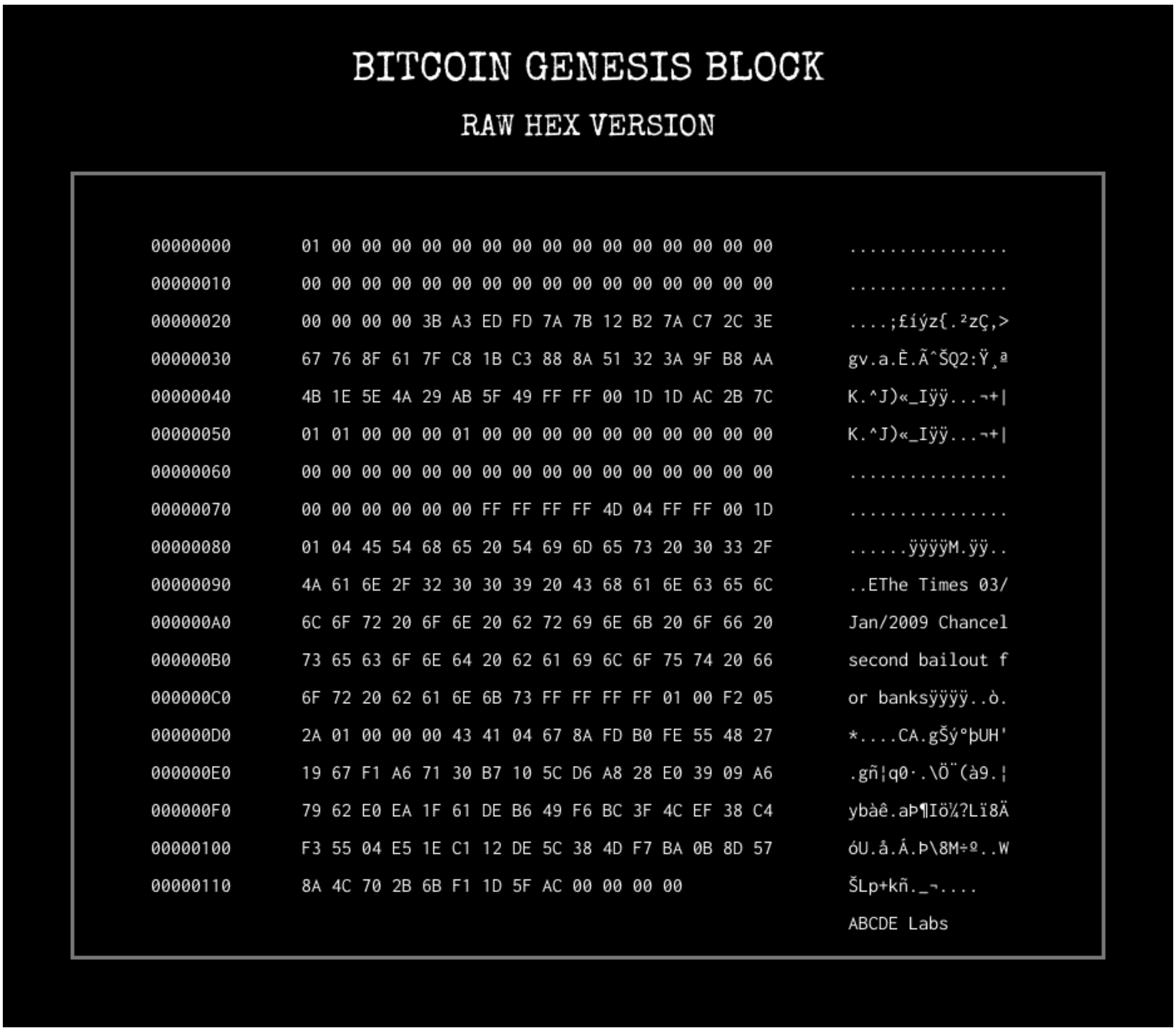
Email: b@ABCDE.com

Medium: @ABCDE

Website: https://www.abcde.com/



Thanks for Reading!



BITCOIN GENESIS BLOCK

RAW HEX VERSION

```
00000000    01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00000010    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00000020    00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E    ....;£íýz{.²zÇ,>
00000030    67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA    gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040    4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C    K.^J)«_Iÿÿ...¬+|
00000050    01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00    K.^J)«_Iÿÿ...¬+|
00000060    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00000070    00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D    ................
00000080    01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F    ......ÿÿÿÿM.ÿÿ..
00000090    4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C    ..EThe Times 03/
000000A0    6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20    Jan/2009 Chancel
000000B0    73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66    second bailout f
000000C0    6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05    or banksÿÿÿÿ..ò.
000000D0    2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27    *....CA.gŠý°þUH'
000000E0    19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6    .gñ¦q0·.\Ö¨(à9.¦
000000F0    79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4    ybàê.aÞ¶Iö¼?Lï8Ä
00000100    F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57    óU.å.Á.Þ\8M÷º..W
00000110    8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00             ŠLp+kñ._¬....
                                                                ABCDE Labs
```

Visit the ABCDE office with this report to collect a limited edition of Bitcoin print.
(Limited 100 pieces)

Report published by ABCDE Labs in 2024