thesis*

State of Bitcoin: 2023

Developments, Data, Insights, and the Future of BTC

The State of Bitcoin is a research report on major developments in the Bitcoin Ecosystem that took place in 2023. This piece was authored by a team of contributors: Jeremy Nation, Vaish Puri, Joey Campbell, Shaurya Singh, Matt Luongo, Hillary Adler, and Saul Hudson.

Special thanks to those who offered their expert feedback: Will Reeves, Gorkem, Brian Mahoney, Sean Medcalf, Harsharn Singh, Engin, Udi Wertheimer, and Eric Wall.

We'd love to hear your feedback on our direction via Twitter, Email, or in person if you see us around!

For press outreach please contact Saul Hudson
(saul@angle42.co)
If you're interested in contributing to Bitcoin or web3 technology, please get in touch at (contact@thesis.co)

Table of Contents

thesis* | DECEMBER, 2023

The State of Bitcoin

Introduction

When the world thinks of blockchains, the first thing that comes to mind is Bitcoin. While the past decade has seen countless developments and innovations in decentralized technology, from GameFi to DeFi to NFTs, Bitcoin remains the world's preeminent digital asset. Assessing its health, recent developments, and future indicators is therefore crucial to understanding the blockchain space as a whole. This report analyzes Bitcoin's activity over the past year using granular data and industry insights to closely examine where the network is today and where it is likely to be headed in the future.

A year that started in the grip of a long winter has seen prices surge above $40,000 – and still climbing. Underlying dynamics were positive, too, with first-time buyers entering the market in increasing numbers while veteran holders increased their positions. On the technical side, the year saw steps forward in scalability, usability, and mainstream adoption – albeit with important challenges remaining unsolved. Looking ahead, the likely approval of the first Bitcoin ETF stands to unleash a flood of new investment – meaning 2024 could be a crucial year in the long-term development of the decentralized economy.

Are ordinals intentionally breaking Bitcoin? Will DeFi exist on Bitcoin via protocols like Taproot Assets and BitVM, or are they just different implementations of things that have already been tried and haven't worked? Will there ever be a successful scaling solution for BTC? Read on for the answers and in-depth analysis, data, and insights into the State of Bitcoin in 2023.

Overview

Bitcoin continued to demonstrate its fundamental value in 2023. In a tough year for digital and traditional assets, the past twelve months have marked significant milestones in Bitcoin's steady rise, enhancing its functionalities and proving its legitimacy as a globally relevant asset and network.

Bitcoin can no longer be written off as a speculative vehicle for digital nonconformists. This year, builders and investors of all stripes worked to realize their visions atop its immutable foundation. The result has been a flowering of innovation that pushes Bitcoin's capabilities while aligning with its core ethos of decentralization and permissionless access.

Innovations like the Lightning Network and novel token standards demonstrate Bitcoin's evolving capabilities, which increasingly offer functionality that matches other popular networks without the centralized patches and workarounds that underpin many blockchain projects. Lightning enables instant, scalable transactions without ceding control to intermediaries. New asset protocols fuse Bitcoin's scarcity with versatile embedded metadata while avoiding congestion.

The Nostr integration merges Bitcoin's censorship resistance with a decentralized social sphere. Ordinals transform individual satoshis into unique programmable artifacts that confer ownership. Recursive scripts allow Bitcoin to host advanced logic and perpetually evolving structures rivaling decentralized application platforms. Taproot unlocks multi-asset transactions, mixing fungible value transfers with provable custody and issuance events. By matching feature sets without compromising core tenets, Bitcoin has proven itself more versatile than critics acknowledge without sacrificing its core ethos.

The developments stretch far beyond technical feats. River Financial and other services reimagine Bitcoin as an intuitive financial instrument while emphasizing security and self-custody. Gaming platforms like Zebedee pioneer new monetization models rewarding players and illuminating Bitcoin's benefits. Mainstream apps like Lolli and Fold offer cashback rewards in satoshis to normalize everyday usage. Finally, the likely approval of spot ETFs stands to unleash a flood of institutional capital as mainstream investors finally grasp Bitcoin's staying power.

The themes are clear – more builders, more use cases, strengthened legitimacy. This is a key time in the evolution of Bitcoin, which represents the frontier for open financial rails without centralized intermediaries. While innovations facilitate wider participation, Bitcoin cannot compromise on its commitment to decentralization, the ultimate hedge in a digital future where control, censorship, and manipulation are constant threats. As investment grows, the principles upholding trustlessness must endure.

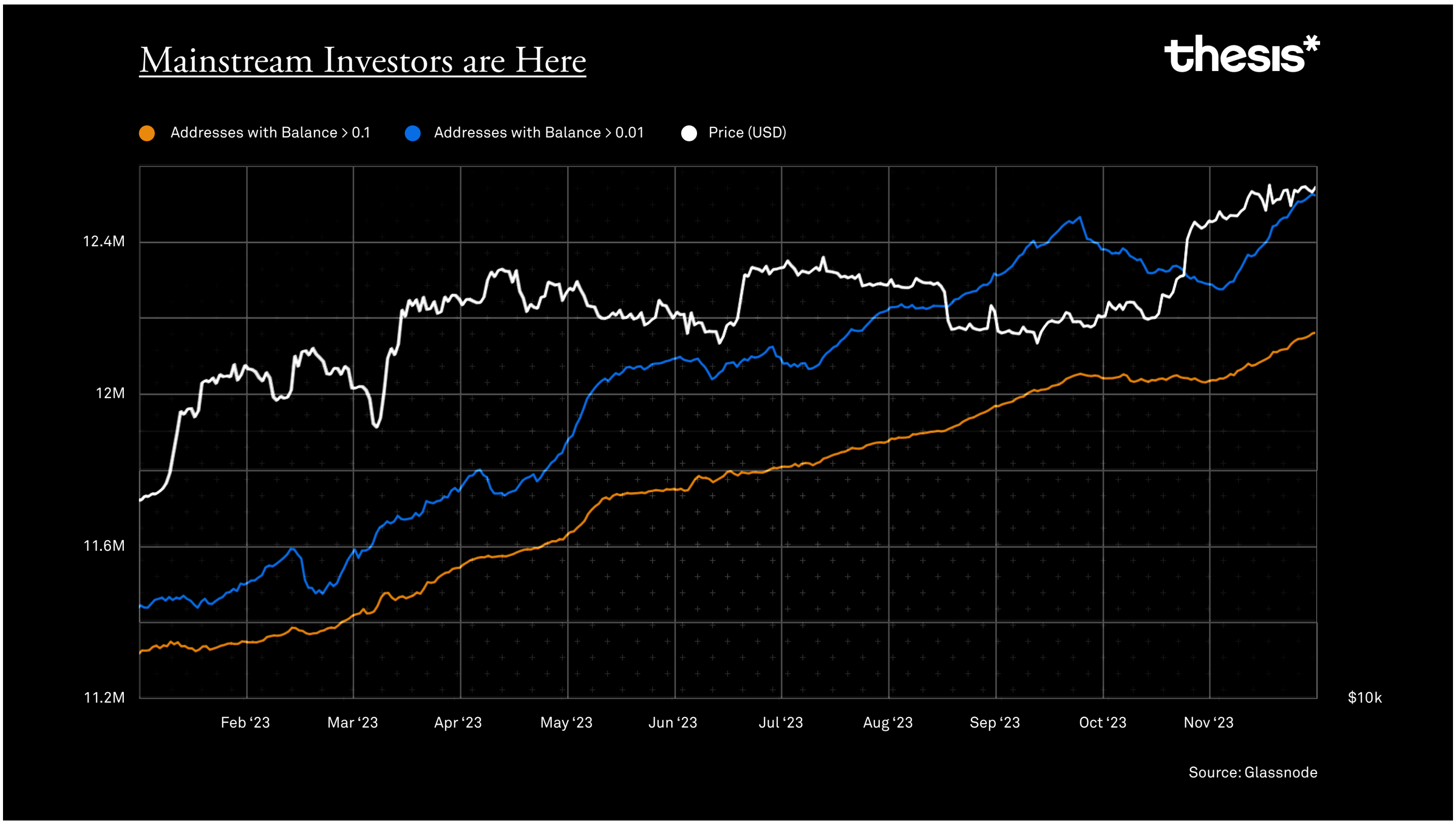
Now more than ever, the world needs sound, decentralized money. There are many challenges on the path ahead – technical, legal, socioeconomic – but with so much talent now striving to achieve this future, they are surmountable. Another cycle passes with Bitcoin in a stronger position both functionally and philosophically. The stage is set for exponential progress come 2024.

Confidence in Bitcoin Grew in 2023

Price tends to dominate headlines when it comes to the health of Bitcoin. But behind the market’s ups and downs, on-chain data reveals a compelling tale of expanding mainstream adoption and the resolute conviction of long-term holders.

Broader Participation from Mainstream Investors

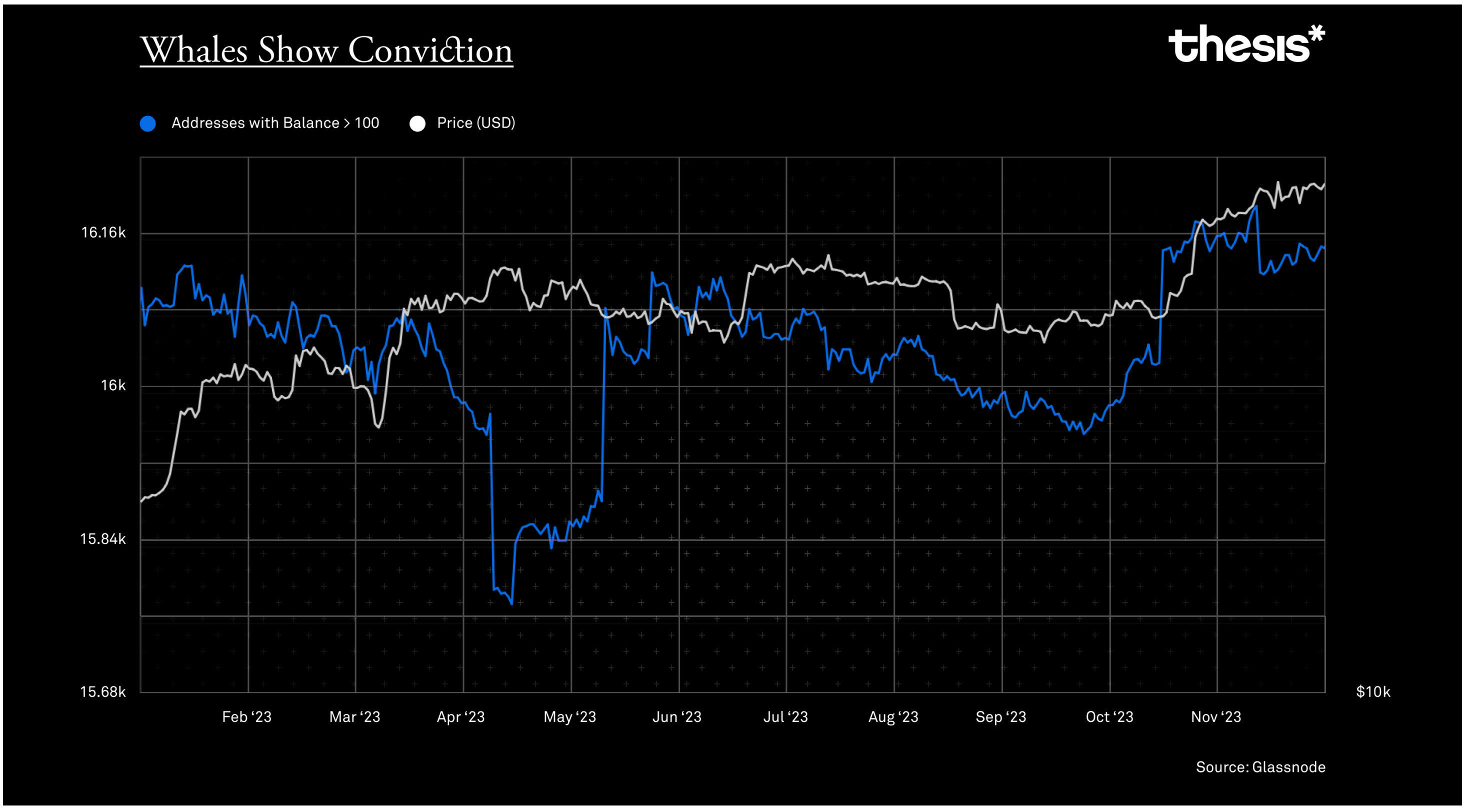
The number of addresses holding balances between 0.1 BTC and 0.01 BTC has gradually increased over the past year, indicating growing retail interest in Bitcoin as an attractive investment asset. With the performance of traditional markets uncertain amid continued high interest rates, mainstream investors have sought robust alternatives. Bitcoin's scarcity and programmatic monetary policy have always been prime ingredients for storing value securely.



Long-Term Holders Demonstrate Deep Conviction

At the same time as more and more new investors have entered the market, seasoned Bitcoiners have added to their positions during price dips and consolidations; their net position change correlates with market movements. As prices peaked, profit-taking also emerged. This divergence between holder behavior and market prices signals genuine, battle-tested conviction. Sustained accumulation often anticipates upward price trends, suggesting holders anticipate impending shifts.

Large holders – those with more than 100 BTC – drive shorter-term volatility, their trading activity reflected in fluctuating address counts. But this cohort regained yearly highs by Q4, hinting at renewed institutional interest even after mid-year uncertainty. The data illustrates Bitcoin's gravitational pull and staying power for those with experience.



Source: Glassnode

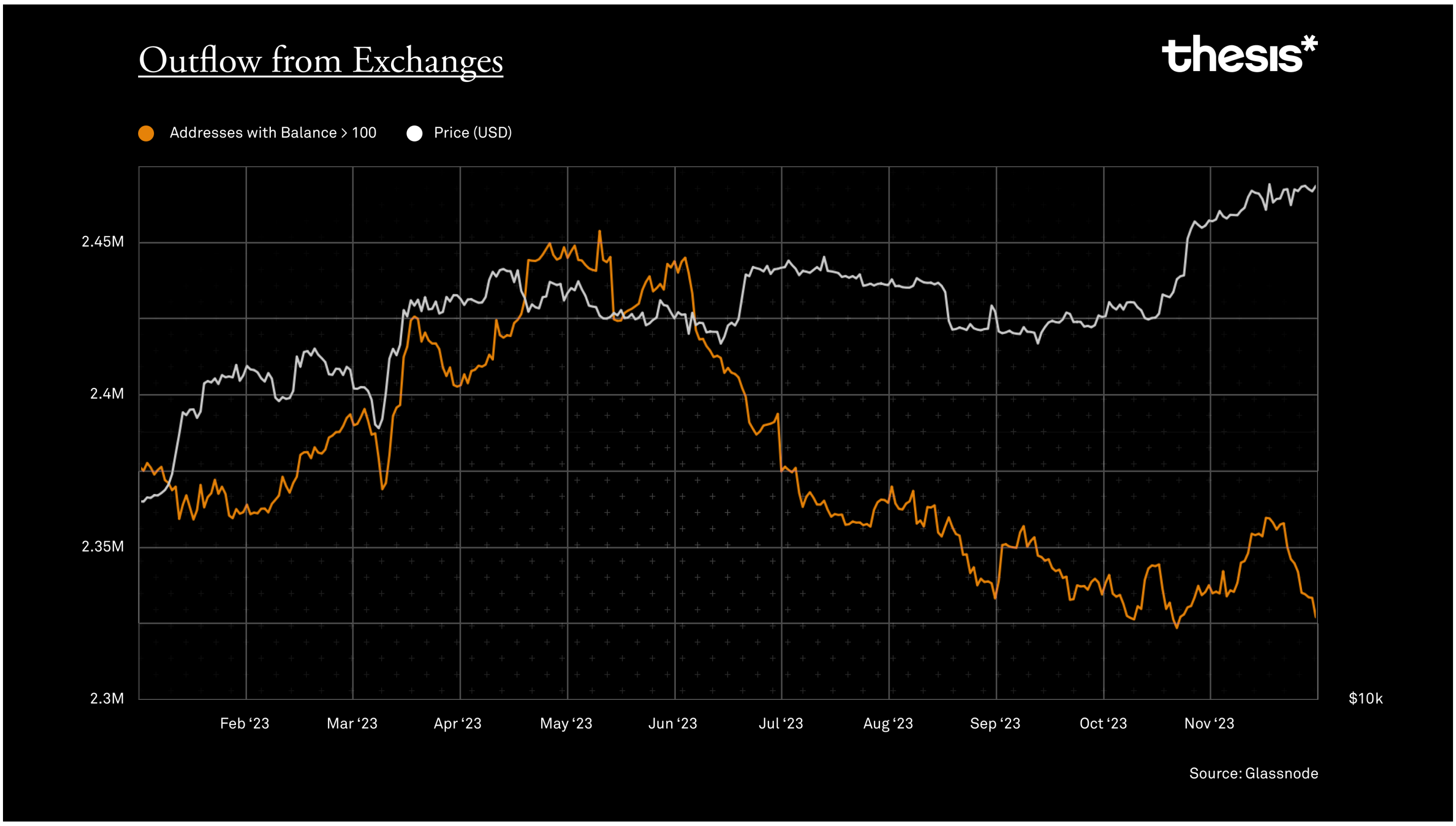
Exchanges Hemorrhage Assets While Investors Embrace Self-Custody

The contrast between declining exchange balances and rising self-custody paints a telling picture. Investors increasingly choose to take direct control of their coins rather than rely on intermediary platforms, undeterred by bearish macro winds. This accelerating migration squeezes exchange liquidity while enhancing the asymmetric upside of Bitcoin's supply dynamics' inelasticity.

Notably, the number of addresses withdrawing to self-custody continues to rise while exchange balances continue to decline1. This divergence, along with the net accumulation of long-term holders during price consolidations, signals enduring confidence in Bitcoin as an investment and store of value. Periods of heavy accumulation often precede significant price increases. The data illustrates two important concepts - the gravitas of holder conviction during volatile markets, and the merit of Bitcoin's inelastic supply curve. As larger entities consolidate Bitcoin supplies, the incentive to sell even at higher prices diminishes. This supply squeeze and heightening mainstream and institutional interest create the precursors necessary to propel periodic bull runs.

The wallet data constructs a compelling narrative: Increasing self-custody migration, accumulation by holders with high conviction, and demand from larger investors pave the road for the next wave of significant adoption. This macro backdrop offers a positive prognosis for Bitcoin's long-term investment thesis.

With robust demand intact despite downturns, the incentive to sell even at higher prices evaporates. Only high-conviction assets win mindshare through full market cycles. And nothing provokes conviction quite like self-custody - a pure signal of intent to allocate for the long term.



Source: Glassnode

Gathering Momentum for The Next Bull Cycle

If blockchain trails are leading indicators, Bitcoin stands poised to embark on its next major growth cycle. The key ingredients are there - expanding mainstream and institutional participation, long-time holders relentlessly accumulating, and an inexorable path to self-custody sparking inelasticity. Investor composition and holder behavior suggest momentum is building to propel Bitcoin through its next leg of adoption.

For long-term believers, Bitcoin's emerging narratives represent an early-stage opportunity. The foundations continue to grow stronger, edging closer to the asymptotic vision of decentralized money.

Scaling Bitcoin

In 2023, scaling Bitcoin to meet increasing demands remains a pivotal focus. While innovations like Lightning Network already push capabilities forward, 2023 sees new layer 2 protocols poised to unlock functionality without tradeoffs. These include sidechains parallel to Bitcoin with interoperable assets and features.

Bitcoin layers extend functionality and improve performance without changing the base layer, much like higher-level internet protocols augmenting TCP/IP. Examples range from fast payments via Lightning to sophisticated smart contracts in Stacks and RSK. Bitcoin emphasizes stability as a settlement base layer while encouraging innovation in the upper layers. The layers enable applications requiring fully expressive smart contracts, high throughput, and privacy by building on top of Bitcoin's durability.

This modularity mirrors Bitcoin's ethos — extending capabilities while minimizing trust. By keeping the base layer simple, permissionless access is preserved as the network becomes more versatile for different needs. Numerous layered protocols now strive to realize Bitcoin's versatility without compromising decentralization.

Technical Overview

At the core of ZK Rollups is the principle of transaction bundling, where multiple transactions are aggregated into a single transaction on the Bitcoin blockchain. This process is underpinned by the innovative use of zero-knowledge proofs, a cryptographic method that allows these bundled transactions to be validated without revealing their details. The essence of zero-knowledge proofs lies in their ability to establish the truthfulness of a statement while maintaining the confidentiality of the underlying data.

Sovereign and Starkware have emerged as leaders pushing zk rollup innovation on Bitcoin. Sovereign takes an opinionated full-stack approach with its SDK, compilers, and modular components for quickly building rollups. Starkware leverages its industry-tested Cairo language and STARK prover from deployment on Ethereum to enable programmability. Teams like Chainway and Kasar Labs have focused on crafting data availability solutions to anchor rollups to Bitcoin without protocol changes. They leverage Ordinals' inscription envelopes to graft rollup data into Bitcoin blocks while avoiding new opcodes.

Centralization Concerns and Decentralization Initiatives

Current iterations of zk rollups have given rise to concerns regarding centralization, primarily due to reliance on centralized sequencers. In many present implementations, a singular entity aggregates transactions, generates the validity proof, and submits the batched data to Bitcoin. This places considerable trust in the sequencer. Hybrid models may emerge long-term, combining multiple prover types based on use case needs.

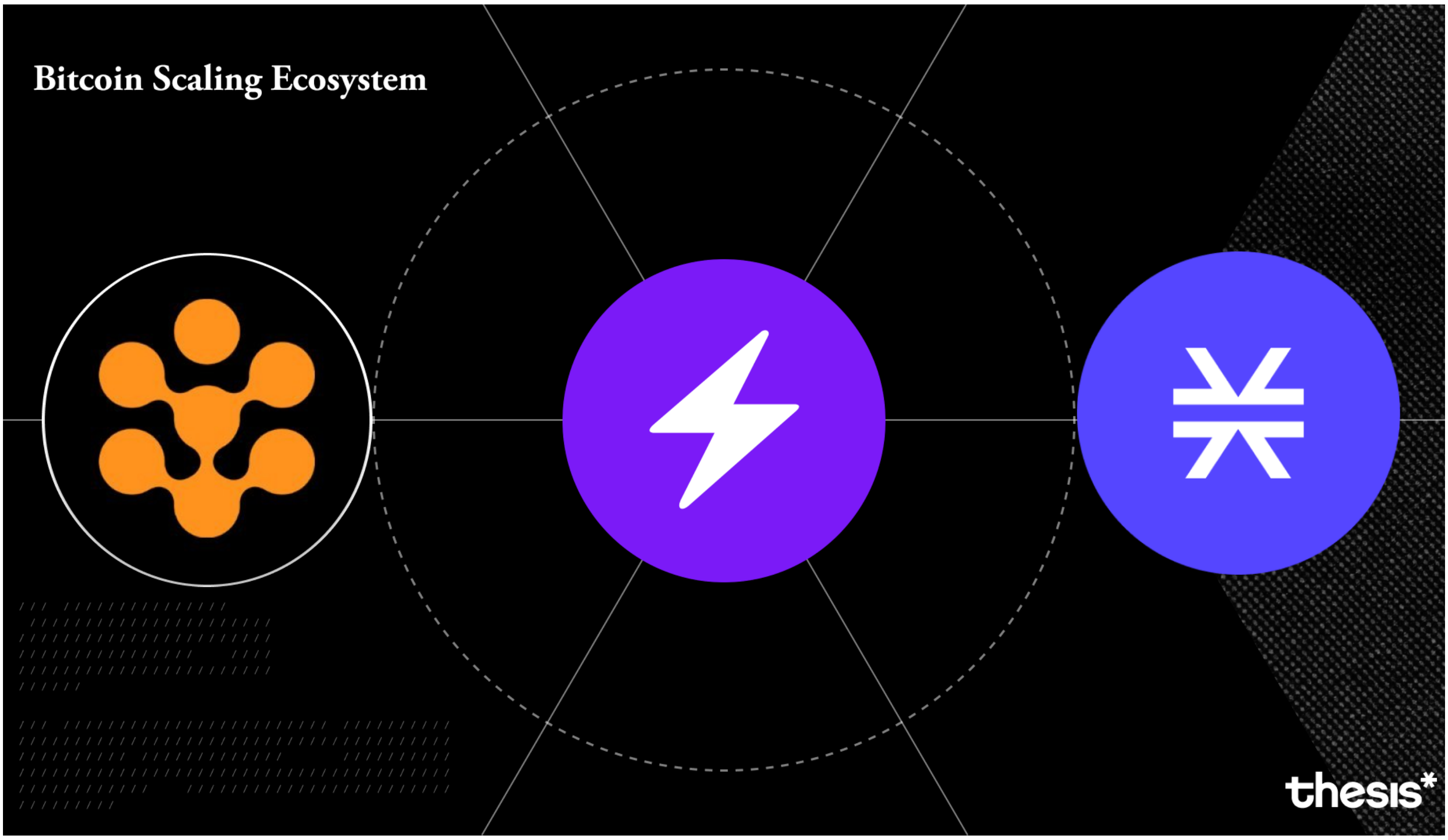
Recognizing this as incompatible with Bitcoin's ethos, there is a concerted effort toward decentralizing the sequencer role. The objective is distributing transaction gathering, proof generation and blocking submission responsibilities across multiple entities. This dilution of trusts aligns more closely with Bitcoin's decentralized architecture.

Several approaches have been proposed:

- Threshold schemes can divide power among a dynamic group of sequencer nodes based on stake or rotation.
- Computational proofs-of-work similar to Bitcoin mining determine participation.

For full decentralization, an eventual opcode could enable two-way movement of Sats and assets between Bitcoin’s base layer and zk rollups using validity proofs. This requires BTC mining nodes to parse the proofs directly, elevating functionality considerably without scaling back decentralization.

Bitcoin’s Layer 2 Landscape



Beyond zk rollups, other layer 2 technologies continue maturing. Two prominent examples are Stacks and Rootstock (RSK).

Rootstock

Rootstock leverages merged mining to achieve Bitcoin-level security assurances despite throughput exceeding the capacity of Bitcoin’s base layer.

Merged mining allows Bitcoin miners to simultaneously process and validate BTC and RSK transactions within the same block. In merged mining, a miner mines both the parent chain (larger blockchain, like Bitcoin) and the child chain (smaller blockchain, like RSK) at the same time. The miner assembles a block for both chains and performs valid work on both networks.
Rather than introduce redundant hash power, RSK transactions piggyback on Bitcoin's vast mining infrastructure. This is possible because both networks share the same proof-of-work algorithm - SHA-256. By extension, the collective hash power protecting Bitcoin protects RSK, preventing double spending or fraudulent manipulations.

The primary benefit of merged mining is its enhanced security to the child chain. By leveraging the computational power of a more robust parent chain, the smaller chain gains additional security against double-spending and 51% attacks. By harnessing Bitcoin's security, RSK achieves scaling, efficiency, and advanced functionality that would be impossible for Bitcoin natively while avoiding recourse to alternative consensus models with vague security tradeoffs.

In 2023, the RSK Infrastructure Framework (RIF) experienced significant advancements, including launching product development workshops and unveiling a new visual identity. These initiatives, alongside enhanced integrations with the Ethereum ecosystem, have played a key role in attracting more entrepreneurs to the RSK platform, which benefits from Bitcoin's robust security. Additionally, the project focused intently on elevating community comprehension of the network's security foundations. Monthly hashrate reports offered transparency into the mining industry's involvement via merged mining - detailing participation proportions of top Bitcoin mining pools securing RSK.[2]

IOV Labs, the entity behind RSK, has been actively working to foster the growth of the RSK ecosystem. In April 2023, IOV Labs announced significant advancements for RSK and RIF at a Consensus event.[3] These include launching a program offering product development workshops and a $2.5 million grant program for startups and developers to build DeFi applications on Rootstock.

However, despite these advancements, RSK has encountered certain challenges. RSK has struggled to garner significant user uptake beyond a small contingent of loyal supporters. The complexity and novelty of its merged mining mechanism also present risks.

These include the potential reluctance of Bitcoin miners to support the RSK network if the rewards do not outweigh the costs or if the rewards for merge mining are inconsistent or unreliable. If returns prove insufficient or unreliable, participation could falter. This creates a circular dilemma - miners secure the network, but maintaining a sufficient number of miners depends upon network usage. Breaking this feedback loop has stalled progress for previous merge-mined chains.

While network activity persists in raw BTC terms, the total value secured has deflated sharply from peaks in USD denominations. TVL peaked in 2021 at ~$229 million USD, though 2023 has seen a notable uptick relative to the past.[4] This bifurcation indicates that those committed to the network continue providing baseline support, with interest growing. However, translating this foundation into exponential growth has proven elusive so far.

RSK must still solve non-trivial incentive alignment puzzles connected to its pioneering security design. Miners must have enough upside to actively support RSK despite viewing it as a secondary priority. Solving these network bootstrapping challenges remains critical for RSK to reach its potential.

Stacks

Stacks is a Bitcoin layer-2 for smart contracts designed to bring decentralized applications and smart contract functionality to the Bitcoin ecosystem.

2023 marked a year of resurgence and expanded capabilities for Stacks amid broader excitement in Bitcoin innovation. While the layer-2 network contends with lingering adoption challenges, big-picture metrics affirm meaningful progress executing on Stacks' roadmap and vision.

Notably, Stacks' native token STX staged a powerful recovery in 2023 after prolonged bearishness. Prices rose over 50% to start Q1 and over 280% year-to-date, significantly outperforming Bitcoin and the wider market.[5] This constituted a remarkable reversal, cementing durable interest despite crypto winter headwinds.

Several crucial network upgrades shipped this year, including Stacks 2.1, which introduced decentralized mining and bridges to Bitcoin. These bridges enable protocols like sBTC to port Bitcoin liquidity into sophisticated Stacks applications incorporating features impossible on Bitcoin natively. The year also saw new blockchain tooling enter testing, like Clarity 2.1 and Hiro's contract deployment platform, priming additional functionality. Workstreams supporting major upgrades like Nakamoto and sBTC - introducing faster block times and decentralized bridges enabling Bitcoin liquidity flows, respectively - remained on track for planned developer releases.

Compared to 2022, renewed sprint processes increased contributor velocity by over 50% on key repositories.6 By the end of Q3, developer growth surpassed 1,100+ Stacks Developers, a 30% increase over Q2 ‘23.7 These efficiency gains accompanied community growth, with followers rising by 20%.

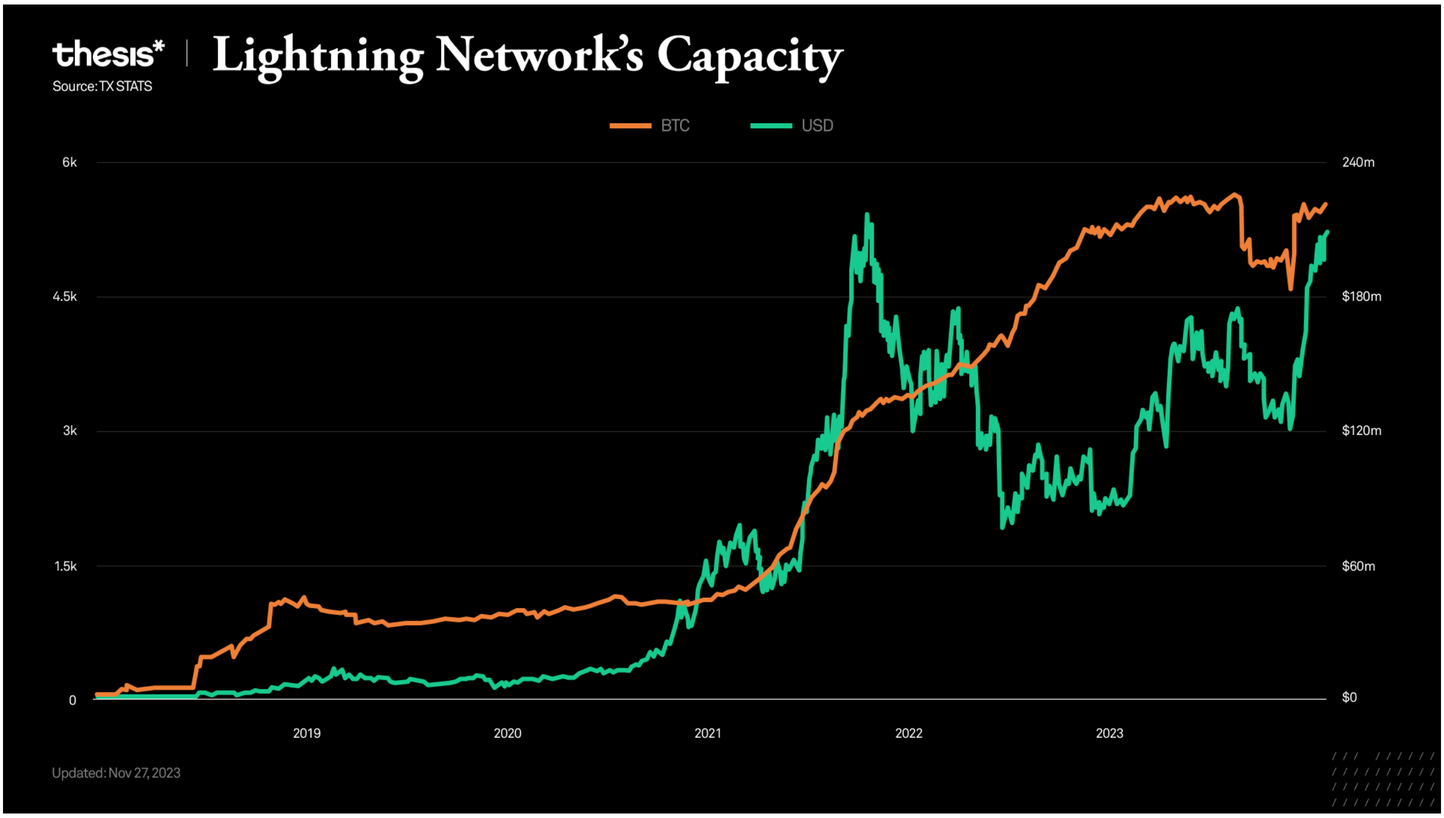
Ecosystem traction expanded steadily, albeit from a small base. Assets under management hit record highs in both USD and STX terms, reflecting growing DeFi participation. Non-fungible token and gaming projects like MetaBoy and Force Prime gained traction. BNS registrations exceeded 300,000 cumulative names, signaling persisting end-user interest.

Not all metrics kept pace, however. Daily active addresses, contract calls, and transaction volumes moderated after spiking earlier in 2023. The pullback implies fickle user retention beyond speculation. Bottlenecks like UX frictions, fees, and network effects likely still obstruct larger adoption.

From security to extensibility, Stacks made strides toward proactive posturing, anticipating likely inflection points for adoption. Public seed nodes launched across regions, eliminating centralization risks in query services while collecting node metrics to inform scaling. Formal auditing support commenced for projects, adding risk-proportionate diligence. While lagging adoption metrics moderately tempered enthusiasm, the year's developments constituted measured progress on multiple fronts. The still-nascent ecosystem contended with bootstrapping headwinds familiar to novel networks - incentivizing usage despite functionality preceding polished end-user experiences.

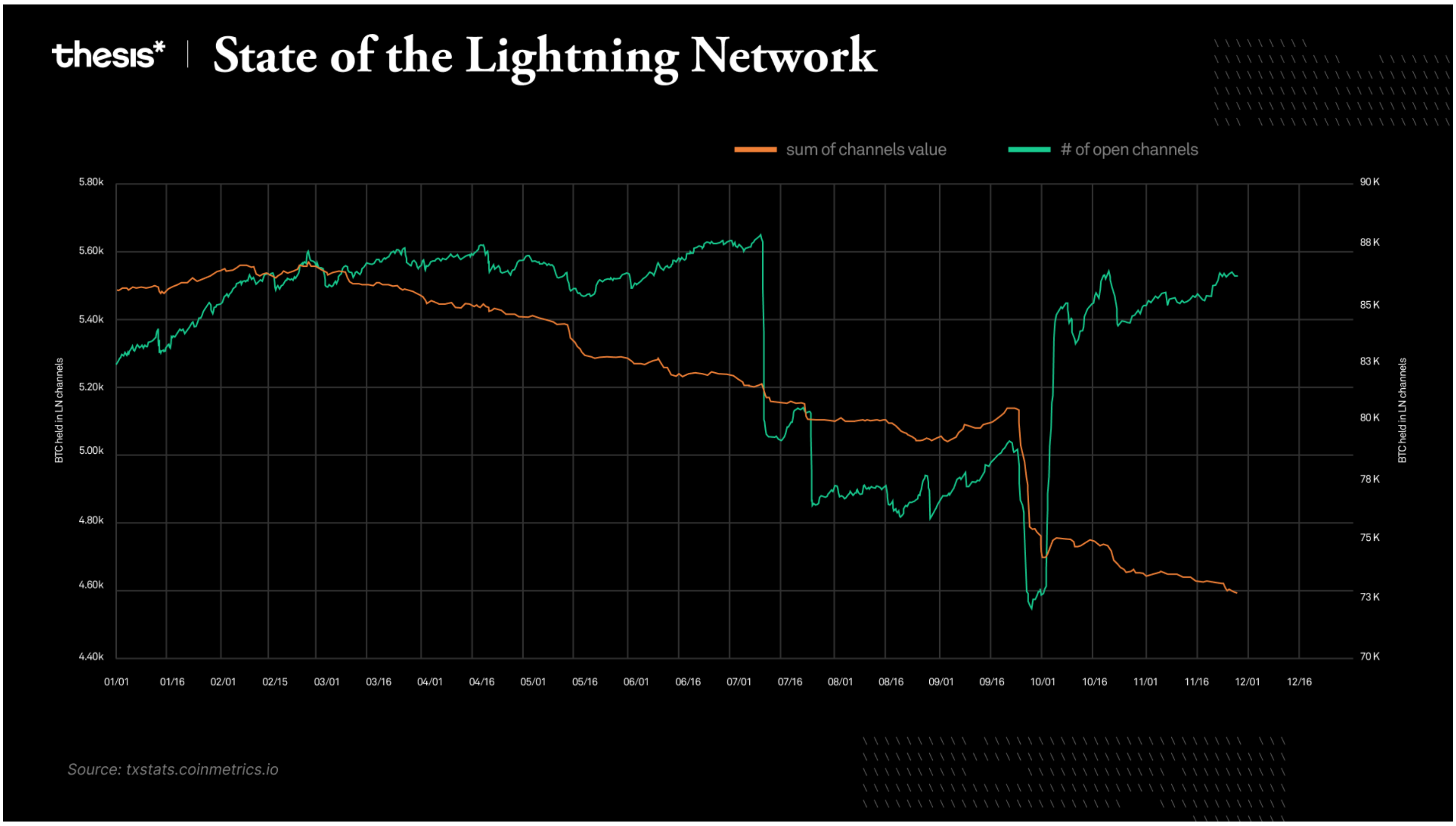
Lightning: Bitcoin's Scaling Solution Goes Mainstream

2023 saw over 5,400 BTC worth more than $230 million flowing through payment channels on the Lightning Network (LN). Capacity rocketed from August 2018’s 1 BTC to today’s robust liquidity pools. Supporting this growth were over 70 LN-enabled wallets offered by leading providers like BlueWallet, Muun, and Phoenix. Adoption ranged from citizens of inflation-ravaged countries to global corporations.



But what are Lightning channels? LN micropayment channels establish a relationship between two parties, enabling them to continuously update their balances without broadcasting every transaction to the blockchain. These channels function by deferring the broadcast of the cumulative balance between the two parties to a later date, effectively netting out the total balance in a single transaction. This approach allows for financial relationships to be trustless without the risk of counterparty default. Importantly, these micropayment channels use genuine Bitcoin transactions, but the choice is to delay broadcasting these transactions to the blockchain. This ensures that both parties can confirm their current balance on the blockchain while the actual payments within micropayment channels are exchanged off-chain.

In October 2023, the Lightning Network experienced a contraction in channel count and total value, suggesting a potential consolidation event or response to external market factors. The network's resilience was demonstrated by the subsequent recovery of both metrics. Over the year, despite fluctuations, there was an overall increase in channel value, indicating a growth in network capacity. The reduction in channel count, without a corresponding long-term decline in total value, implies a shift towards larger channels. This trend points to a concentration of liquidity in the network, potentially indicating a strategic shift in channel management or user behavior.



Source: txstats.coinmetrics.io

Infrastructure Hardens for Enterprise

Infrastructure Hardens for Enterprise
November marked another leap with Taproot Asset Protocol v0.2. Offering a toolkit to issue assets via LN and Bitcoin, customizable asset burning provides compliance controls for regulated businesses. Multiverse Trees enable transparent tracking of assets across sidechains, while configurable Proof Couriers relay validity records on-demand to prevent congestion. Load testing and forward-compatible data structures ensure rigorous functionality as LN steps onto the global stage.

- Costs plunge as issuance, transfer, and redemption are packed into single transactions.
- LN now cements versatility for enterprises, from tokenized securities to programmable contracts in restricted jurisdictions.
- Enhanced RPC calls grant detailed monitoring of proof relaying plus sophisticated asset lifecycle management.

Nostr Integration Opens P2P Economy

September brought decentralized social protocol Nostr's "NIP-57" upgrade. By introducing "Zap" notes representing Lightning invoice receipts, Nostr merged Bitcoin micropayments with social interactions. Content creators leveraged Zaps for tipping, while readers funded posts to unlock additional content and deter spam. The rapid uptake and usage of Zap payments, exceeding 50,000 by late 2023, demonstrate the increasing integration of Lightning Network solutions into broader applications.

This growth spotlighted scalability challenges still facing innovative Bitcoin infrastructure. Nostr Assets, which facilitates Taproot and Lightning transactions, paused deposits in late 2023 due to overwhelming demand. This firsthand encounter with capacity limitations underscores the tension between rising interest and capacity constraints Bitcoin's second layer stretches into uncharted territories.

Nevertheless, for a brief moment, Nostr combined decentralized networking with real P2P value transmission via Lightning's seamless interoperability. Companies like Peach and Noonesapp now leverage Nostr and cryptography to facilitate peer-to-peer exchange without centralized escrow reliance. The resulting framework is the antithesis to surveillance models like Worldcoin - instead emphasizing ethical information exchange backed by cypherpunks like Jack Dorsey.

The demand trajectory indicates Bitcoin's decentralized payment channels is likely to continue permeating communication and community building applications through relentless refinement.

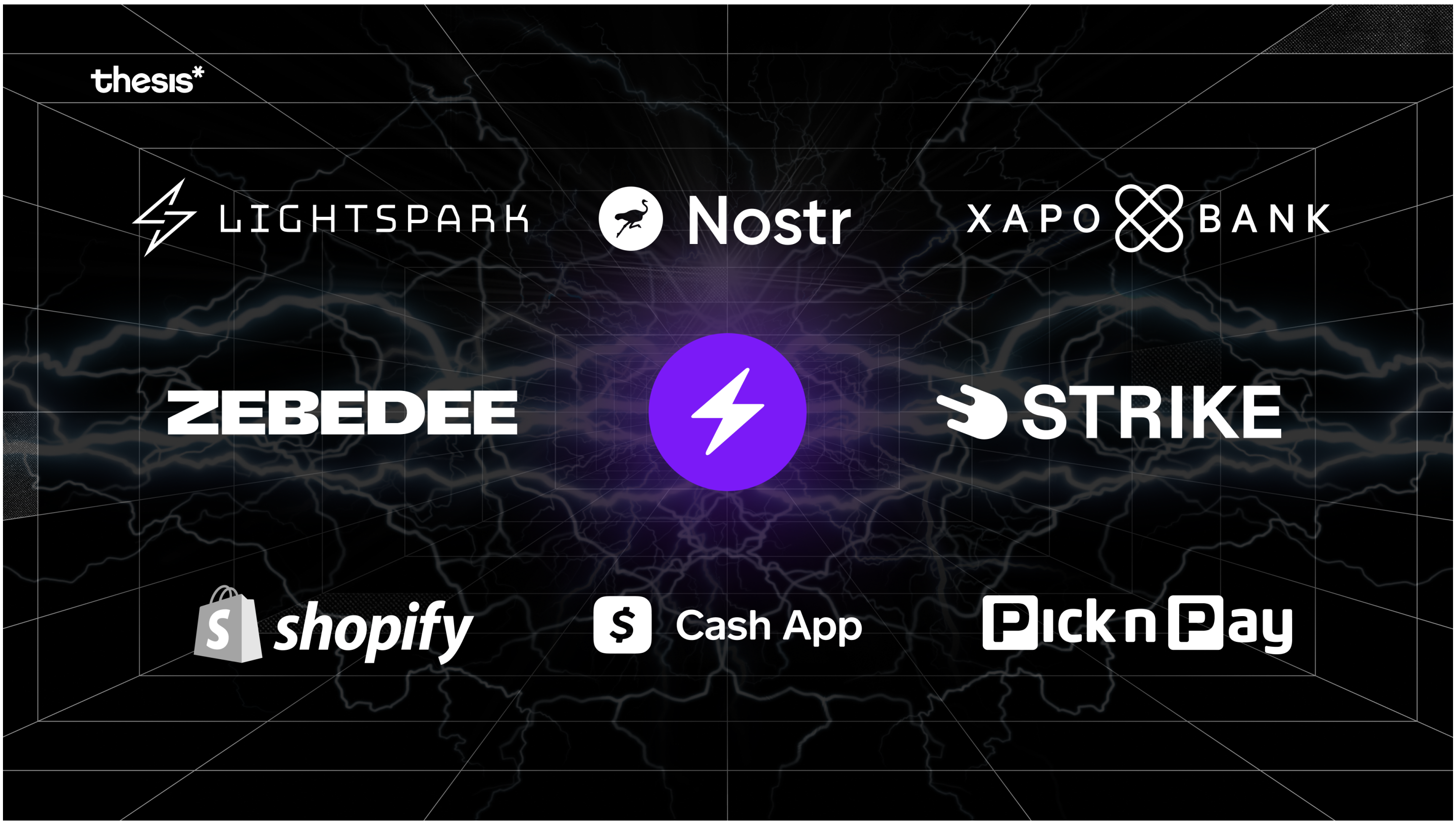
Retail Giants Stimulate Adoption

Major retailers expedited LN's consumer reach in 2023. Payment leader Stripe unlocked Lightning for corporations via its "Pay With Bitcoin" checkout button. Social giant Twitter integrated the tipping economy, letting users seamlessly reward quality content. In gaming, Zebedee brought fast Bitcoin transactions into multiplayer worlds like Minecraft and Fortnite

For Bitcoin converts, LN finally actualizes its promise as a scaling layer to support global adoption. By augmenting speed and reducing fees, Bitcoin moves from a clunky speculation vehicle to a fluid medium of exchange.

While volatility remains, enhanced real-world functionality primes Bitcoin as a globally recognized store of value and means of exchange.

Yet usability is half the battle. LN remains inaccessible without ramps into the legacy world. Hence, Stripe's checkout button resonates by easing conversion from bank accounts or cards. Though self-custodial and non-custodial solutions grew, exchanges still dominate LN access and liquidity for most users. More integrations across payments, e-commerce, and social media should steadily dissolve this friction.



The Custody Conundrum

Custodial services facing regulatory crackdowns contrast with non-custodial wallet breakthroughs on collaborative custody frontiers. Novel asset designs and scaling protocols signal functionality leaps if capacity barriers relent. Altogether, a narrative of measured headway despite setbacks persists across the Bitcoin landscape on both application and infrastructure planes. Miniscript and RGB constitute particularly promising extensions of Bitcoin's programmability.

Miniscript refers to a simplified scripting language for writing Bitcoin transaction logic to unlock funds.

It uses readable script building blocks while remaining highly flexible and customizable. Companies like AnchorWatch and Revault now leverage Miniscript for advanced wallet architectures, allowing collaborative multi-party custody and policy-based asset control. By expanding scripting capabilities beyond basic transfers, Miniscript unlocks the programmability of Bitcoin ownership configurations to match complex financial activities more seamlessly.

RGB refers to a new Bitcoin layer focused specifically on scalable smart contract functionality. It enables versatile dApps beyond payments and ownership like NFTs, tokens, and stablecoins while avoiding base-layer congestion. The development of RGB wallets like BitMask and myCitadel are gaining significant traction. Exchanges like Bitfinex now natively support RGB for launching Bitcoin-settled assets using its extended opcodes for embedding metadata. By moving data off the root Bitcoin blockchain, RGB constitutes a scaling platform granting developers leeway to experiment with Bitcoin in new paradigms like DeFi and digital collectibles

Meanwhile, the emergence of Chaumian E-Cash Protocols, such as Fedimint and Cashu, offer glimpses into potentially decisive scalability advancements. These protocols are supported by entities like Blockstream and provide scalable, instant settlements with minimal fees.

Looking Ahead with Tempered Optimism

Yet for all its progress, Lightning contends with acute growing pains belying its outward success. Episodes like exorbitant fees amid congestion reveal lingering scalability limitations. And core developer departures underscore ever-present technology risks that give pause. Additionally, approximately 90% of transactions occur through custodial wallets, reflecting UX obstacles in non-custodial usage - factors like continuous node oversight.[9] Lightning promises extraordinary potential but does not resemble a finished product.

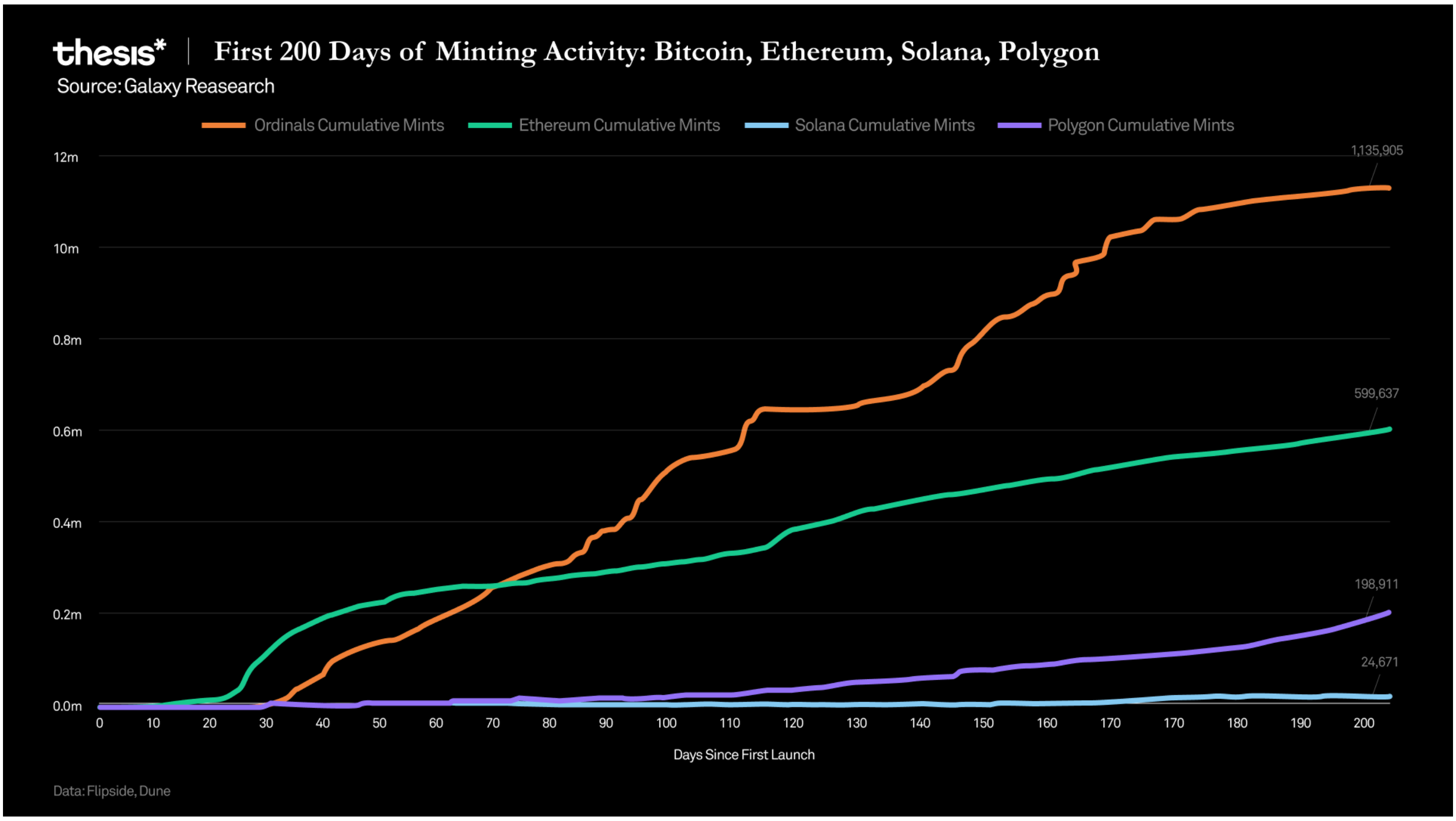
Nevertheless, writing off Bitcoin’s most ambitious innovation due to temporary turbulence proves shortsighted. Lightning has already unlocked life-changing utility for millions globally. Lightning appears poised to breach new thresholds with work underway on optimizations like Anyons and swarm settlements. Bitcoin’s very ethos rests on tireless iteration, transforming seemingly intractable challenges into catalysts for progress. Lightning’s setbacks may one day constitute launchpads if history holds course.

Ordinals: Artifacts Inscribed on Bitcoin

One technological innovation that has stood out amid Bitcoin’s evolution has been the emergence of Ordinals, which, turn individual satoshis into unique digital artifacts capable of holding rich data.Ordinals are instances of Bitcoin’s smallest subdivision that are inscribed with data such as text or images. Once inscribed, each satoshi becomes a unique digital asset.

The Ordinals Protocol, first proposed by protocol creator and developer Casey Rodarmor, was launched on January 21, 2023. It used the improvements brought by the 2021 Taproot upgrade, which enhanced Bitcoin's functionality and allowed for larger data attachments of up to 4MB per transaction. This technical advancement, which leverages Bitcoin's existing infrastructure, has opened up new possibilities for embedding richer data onto the blockchain while marking a departure from traditional digital assets and NFTs.

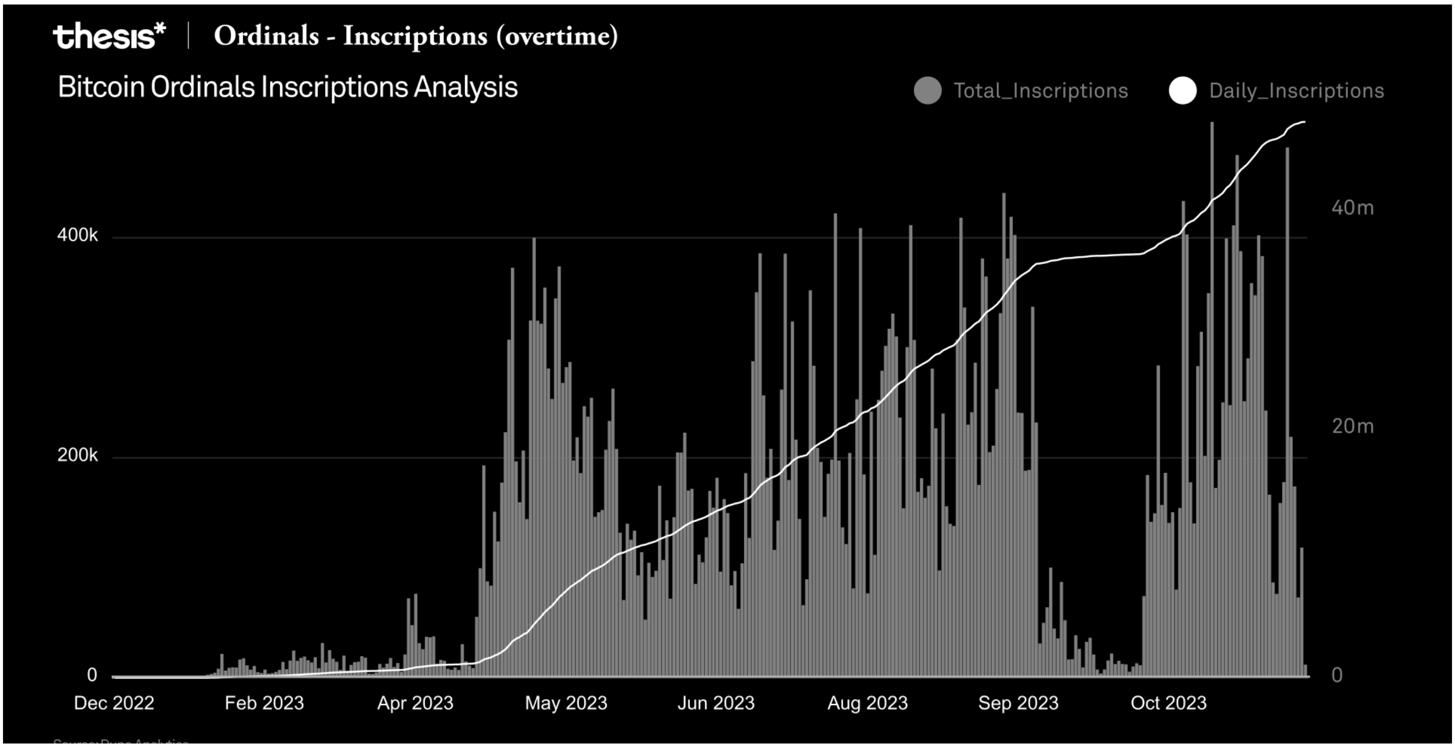
Growth was fast. In February, Yuga Labs announced the first-ever Bitcoin NFT collection based on ordinal inscriptions.


thesis* | First 200 Days of Minting Activity: Bitcoin, Ethereum, Solana, Polygon

Source: Galaxy Reasearch

Data: Flipside, Dune

By June, over 11 million Ordinals were inscribed on Bitcoin, with the peak volume occurring in May. The period from July to September saw a consistent increase in inscription volume, with plain text being the most popular type. Looking towards the end of 2023, projections indicate a trading volume of approximately $725 million for Ordinals.10



thesis* | Ordinals - Inscriptions (overtime)

Bitcoin Ordinals Inscriptions Analysis

Source: Dune Analytics

As ordinals took off, NFT sales fell by 8.7% from $4.2 billion in September 2021 to $3.8 billion in October 2023. The introduction of ordinals resulted in a spike in Bitcoin transaction fees and block size, with a staggering 45,074,477 inscriptions on the chain. November 12th, 2023 saw a daily record high of 505,345 bitcoin ordinal inscriptions.

Technical Deep Dive: Understanding the Ordinals Protocol

The Inscription Process

Several services exist to facilitate the creation of ordinals. To get started, a user must set up a Taproot-compatible wallet synced with the core Bitcoin chain and select the type of inscription they intend to create: either a singular ordinal or a collection. After this, users may load any image, text, code, document, video, or audio from their connected device to be inscribed. The recommended size of such uploads is less than 35kb to maintain optimal results.

Variables such as the uploaded file size and network congestion may impact fees related to inscription transactions. Finally, an unused recipient address must be specified for a newly created ordinal to be received.This system allows each satoshi in every transaction to be identified with a unique ordinal number, effectively creating a serial number for each satoshi, which can track the asset as it circulates.

Each satoshi receives a sequential number based on mining time, creating a range of ordinal numbers up to 2,100,000,000,000,000. This system introduces a rarity element based on the timing of mining and inscription.
Although services exist that allow ordinals to be created, the assets themselves do not rely on third-party services to store data. Unlike many NFTs, all information associated with each ordinal is permanently recorded on-chain. Such properties make it possible to build atop a foundation of preexisting ordinals via recursive protocols that retrieve data from existing inscriptions to generate new inscriptions.

Wallets That Support Ordinals

Ordinals Wallet: Launched on February 16, 2023, the Ordinals Wallet is a Bitcoin wallet designed to overcome the limitations of previous wallets. It supports holding, storing, viewing, transferring, sending, inscribing, buying, and selling Ordinals. Praised for its user-friendly interface, this wallet is a product of community funding.

Xverse Wallet: Xverse, a Bitcoin Web3 wallet, introduced its Bitcoin Ordinals service a day before the Ordinals Wallet. Xverse focuses on evolving as an advanced Bitcoin wallet with robust support for Ordinals. Users can interact with the blockchain without running a full node, purchase Bitcoin within the app for transactions, and inscribe Ordinals through Gamma, a Bitcoin Ordinal marketplace. Ordinals are visible in the user's NFT collection within about 30 minutes.

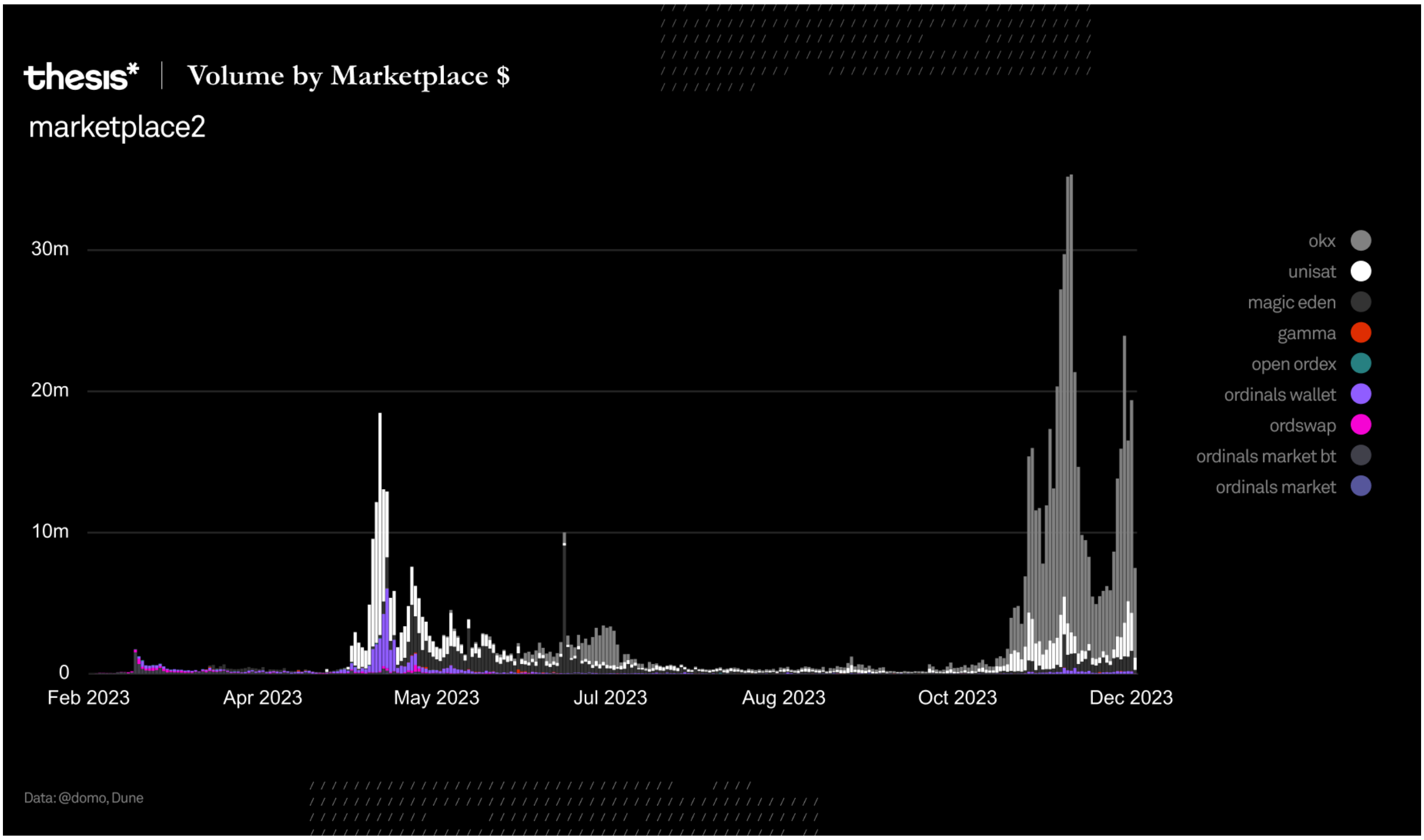
Hiro Wallet: Launching its Ordinal services on February 14, 2023, Hiro Wallet was a first mover. It enables secure storage, sending, and receiving of Bitcoin and quick creation and storage of Ordinal NFT inscriptions. Compatible with platforms like Gamma and OrdinalsBot, Hiro Wallet facilitates inscriptions directly in the web browser.

MetaMask: MetaMask can be linked to Generative XYZ to manage Bitcoin Taproot keys, which are essential for trades and authority over digital assets. It requires signature verification for Ordinal addresses and offers a key vault. Hardware wallets like Ledger and Trezor are compatible for enhanced security. MetaMask's Generative Marketplace allows exploration of Ordinals.

OKX Wallet: OKX Wallet, supporting Bitcoin Ordinals, integrates with the Taproot upgrade for easy viewing and transferring of ordinals. It offers cross-chain interoperability across more than 50 chains, simplifying the user experience. In addition to supporting the purchase of BRC-20 tokens, OKX Wallet highlights the BRC20-S standard for staking BRC-20 tokens, an open-source protocol available for developer adoption.

Ordinals Markets

Trading volumes across various Bitcoin Ordinals marketplaces, including OKX, Unisat, Magic Eden, and Gamma, showed substantial growth throughout the year.



- Overall Trading Volume: Dune Analytics data indicates an overall volume of $794,330,265 in the Bitcoin Ordinals marketplace.
- Total Number of Trades: 1,173,402 trades across these marketplaces in 2023.
- Unique Users: The cumulative count of unique users engaging with these platforms was reported to be 253,379.
- Individual High-Value Transactions: High-value transactions on marketplaces like OKX and Ordinals Wallet exceeded $1 million in some cases.

Technical Foundations: SegWit and Taproot

The Segregated Witness (SegWit) upgrade in 2017 laid the foundation for Ordinals, as it introduced the concept of witness data, which reduced the block space occupied by each transaction and enhanced the network's processing capacity. The 2021 Taproot upgrade further enhanced this capability by introducing new script features and removing the size limit on a transaction's witness data, enabling storing data up to 4MB on BTC.

Impact on Bitcoin's Architecture

The Ordinals Protocol introduced a new use case for Bitcoin, enabling the creation of immutable, ownable, permissionless, and uncensorable digital artifacts that reside fully on the Bitcoin blockchain with no need for a sidechain or separate token.

This development has led to discussions around the use and scalability of the Bitcoin blockchain as it introduces new types of data and transactions, potentially impacting the network's efficiency and operational costs.

Pros of the Ordinals Protocol

- Attracts New Users: Ordinals introduce NFT-like assets to Bitcoin, potentially attracting new users such as collectors and artists interested in digital assets and NFT trading. Users who previously ignored Bitcoin due to the lack of collectible offerings may respond to this and drive demand for Bitcoin as they pay inscription fees and trade these assets.

- Market Demand: The uptake in inscriptions demonstrates market interest in this new use of block space. If such transactions were inefficient or valueless, they would likely be priced out, but their popularity indicates a strong market demand.

- Increased Fees for Miners: The Ordinals Protocol generates additional fees for miners, potentially benefiting Bitcoin's security model, especially as block subsidies diminish. High-value transactions, like the sale of Ordinal Punks, illustrate this potential for revenue.

- Accelerating Second-Layer Adoption: The increased transaction fees and block space usage could drive the adoption and development of second-layer solutions like the Lightning Network, helping scale the Bitcoin network.

- Driving Taproot Adoption: The launch of Ordinals has led to a rise in Taproot transactions, accelerating the adoption of this upgrade, which offers more compact transactions and enhanced privacy.

Cons of the Ordinals Protocol

- Increased Costs for Block Space: Including additional non-financial data in blocks increases fees and makes it harder for node operators to run full nodes. This could lead to more demanding technical requirements and potential centralization of full nodes verifying the chain.

- Speculation and Market Distortion: Ordinals could divert capital into trading these assets rather than storing value in Bitcoin. This could affect the perception of Bitcoin as a serious investment.

- Impact on Satoshi Fungibility: By creating non-fungible attributes for satoshis, Ordinals could challenge the ethos built around Bitcoin's use case as ultra-sound money. The differentiation between inscribed and standard satoshis could create a dual market, potentially impacting the fungibility of Bitcoin

- Additional Tracking and Privacy Concerns: The data associated with Ordinals could make on-chain behavior easier to track, raising privacy concerns. Bitcoin users who value anonymity might find this aspect of Ordinals contrary to their privacy goals.

- Risk of Data Pruning: There's a possibility that Bitcoin nodes could prune inscription data, raising concerns about the permanence of these digital assets. Although this case is extremely unlikely it does introduce a potential vulnerability in an aspect of the decentralized nature of Bitcoin.

Concerns in Ordinals Numbering

Although the Ordinals Protocol introduced a novel system for indexing digital assets on the Bitcoin blockchain, its indexing of those assets sparked significant controversy regarding its numbering schema.

Managing the index for Ordinals isn't straightforward, which has led to improperly indexed inscriptions known as "cursed ordinals." These instances add complexity and create bugs within the system.

Discrepancies in the indexing process, such as minting multiple inscriptions in a transaction or committing multiple inscriptions to the same satoshi, can produce such anomalies. These cursed ordinals are ascribed negative numbers, complicating the ability to discern the creation order and adding to the system's complexity.

A strategy that could streamline the Ordinal codebase, proposed by Rodarmor, would “bless” such cursed ordinals, and fold them back into the protocol’s main sequence. However, doing so would also re-number all existing ordinals.

Rodarmor’s plan would make inscription numbers permanently unstable, departing from the initial intention behind inscription numbers, but would also retroactively forgive all prior and future cursed ordinals.

Support for the change is not universal. The existing numbering system underpins several Ordinals projects, and many collectors have made acquisitions based on the perception of value as attributed to low-indexed assets. For example, collections like "Hell Raiders" could lose their iconic positioning due to re-indexing. Still, many support Rodarmor's plan for its potential to reconcile issues with the protocol’s current indexing schema and ensure its adaptability.

A potential compromise involves preserving impacted Ordinals via a snapshot or allowing users to reinscribe their unique numbers. This could address concerns about renumbering while minimizing the impact on the system.

Recursive Ordinals: A Solution to Concatenation

June 2023 saw the introduction of Recursive ordinals, marking an important move towards advanced data interaction for the protocol.

Recursive ordinals take advantage of how ordinal data is stored, enabling complex on-chain software operations by daisy-chaining data calls. This method enables developers to circumvent the 4MB limit imposed by standard ordinals.

With more interconnected on-chain data sources, recursive ordinals allow for the establishment of more intricately interconnected data sources with the potential to significantly enhance storage efficiency while reducing transactional costs.

The recursive ordinal protocol allows developers to host extensive files, be they applications, or even video games, directly on the Bitcoin network. This opens up opportunities for more advanced applications, such as permissionless smart contracts that dwell in the blockchain's immutable storage layer.

Recursive ordinals therefore represent a critical step towards enabling more sophisticated DeFi architectures within the Bitcoin ecosystem. While the technology initially addresses file concatenation issues, the potential also extends to more advanced applications and operations requiring logic, rules, and algorithms.

Developers may use the foundation of recursive ordinals to engineer immutable decentralized platforms, such as DEXs, or stablecoins, whose frameworks permanently live on Bitcoin. Such developments align with ongoing efforts to integrate the Ethereum Virtual Machine and Solidity into the Bitcoin network, exemplified by developers' deployment of Uniswap and Optimism contracts, potentially signaling a shift to a more developer-inclusive Bitcoin ecosystem.

As with the ordinals protocol, community response to recursive ordinals is somewhat mixed. Some fear that the fact that such protocols are maintained and altered by a somewhat centralized developer group is in conflict with the ethos of Bitcoin. Others eager to explore the possibilities of recursive ordinals have welcomed processes that promise to reduce storage duplication and transaction costs.

Ordinals Use Cases

- Collections: Taproot Wizards, ORD Rocks, and Bitcoin Punks are among the most well-known collections at the time of writing. Yuga Labs' forthcoming generative art collection TwelveFold is also poised to become one of the more popular collections.

- Marketplaces: OpenOrdex is one of the most fascinating marketplaces, as it is fully open-source and strictly uses decentralized tools to enable trading. Specifically, OpenOrdex uses partially-signed bitcoin transactions (PSBTs) to enable the trustless listing and purchasing of inscriptions.

- Explorers: OpenOrdex, Gamma, and Ordinals.com are research tools to analyze Ordinal/inscription activity. Explorers also provide data on transaction ID, address, output value, weight, sat number, and location.

- Inscriptions as a service: The complexity of minting an Ordinal introduced inscriptions as a service to help collectors create collections. OrdinalsBot, OrdSwap, Gamma, Bitcoin Bandits, and Luxor mining are among some of the popular inscriptions as a service provider. These services handle every step of Ordinal creation.

- Wallets: Bitcoin wallets currently lack sat selection functionality, which is an essential feature to send Ordinals to other addresses. Although sat selection is unavailable, wallets that offer UTXO selection like Sparrow wallet, Electrum, and Xverse are widely used by Ordinal collectors.

Spotlight on Taproot Wizards: Pioneers of Ordinals

Taproot Wizards Inscription #1

thesis*
taprootwizards.com
MAGIC internet JPEGS
Join us

Taproot Wizards (TW) is a unique Bitcoin NFT project that has been an important (and controversial) voice within the ordinal community. Led by an independent developer and Bitcoin advocate, TW introduced a collection of 2,121 wizard-themed Ordinals. The project gained attention for its avant-garde art and paid homage to the iconic Bitcoin Wizard. TW contributed to the growth of Bitcoin NFT sales and promoted the adoption of Bitcoin's Lightning Network. It inspired artists, developers, and collectors to explore new possibilities within the Bitcoin ecosystem, driving further interest in the Ordinals market.

Luxor Mining made headlines by mining the largest Bitcoin block to date on February 1, reaching 3.96 MB in size, nearly hitting the 4 MB block size limit of Bitcoin. This block included a non-fungible token (NFT) named Taproot Wizards, which plays on the "magic internet money" meme. The transaction fees for this NFT were around $209. This event took place amidst a heated debate within the Bitcoin community about the legitimacy and appropriateness of utilizing the blockchain for ordinals, with some arguing that they are spam and should be removed, while others, including Luxor, believe they have a place within the Bitcoin ecosystem.[11]

Protocol Overview: Introduction to the BRC-20

The BRC-20 protocol on the Bitcoin blockchain enables the creation and management of ordinals with enhanced functionality. It also leverages the Ordinals protocol, however, BRC-20 tokens are a type of ordinal inscription that includes JSON data, allowing for seamless transfer and interaction of tokens representing various assets or utilities alongside Bitcoin.

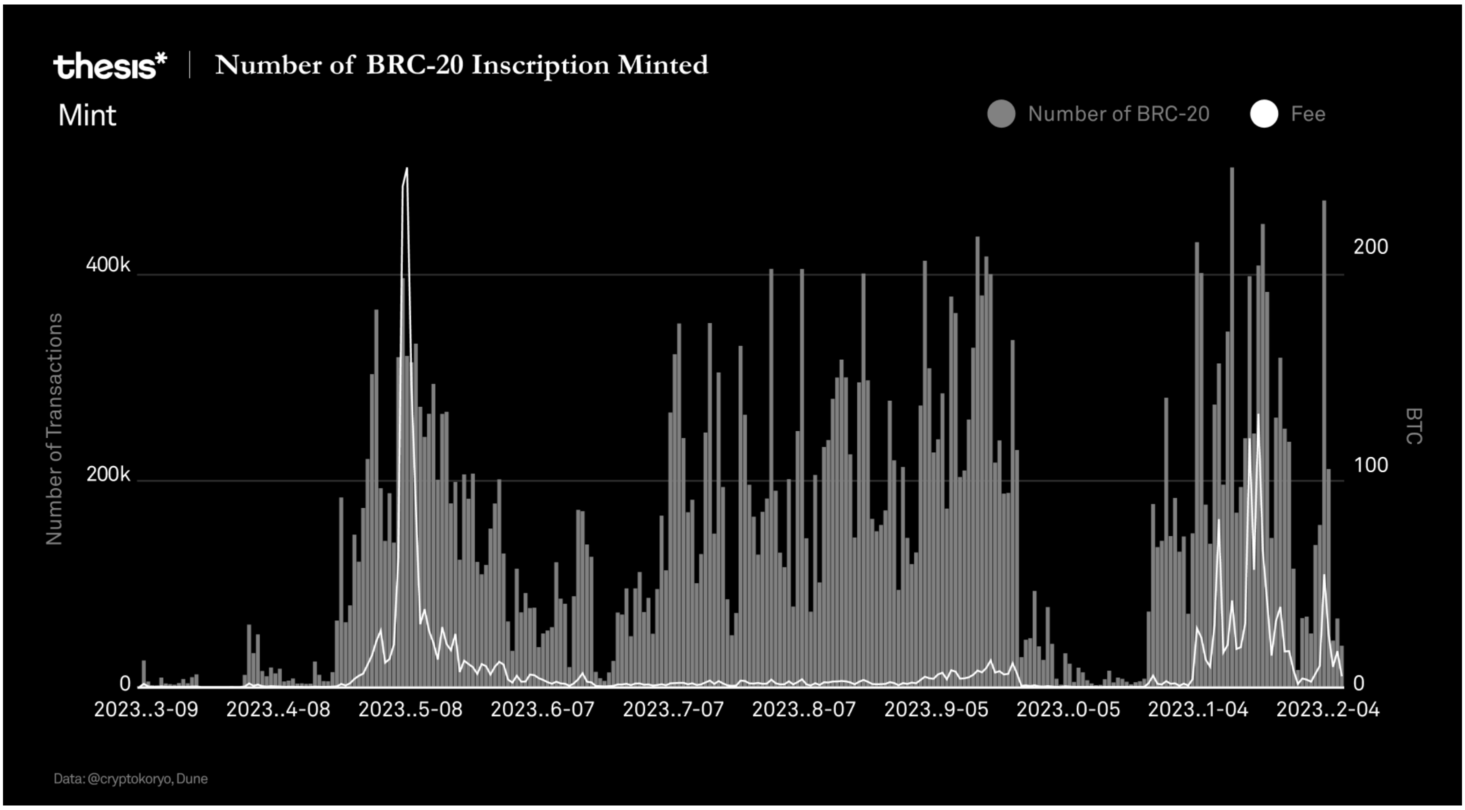
By supporting ordinals, the BRC-20 protocol enhances the functionality of tokenization within the Bitcoin network. The BRC-20 standard while evolving, provides a framework for developers to create arbitrary tokens on the Bitcoin network, opening up a wide range of possibilities for programmable assets.

BRC-20 Trends

The first token contract to be deployed was for the $ORDI token with a limit of 1K tokens per mint and 21M max supply (paying homage to Bitcoin's max supply). In less than a day, all 21M $ORDI tokens had been minted, and other tokens soon emerged. According to data from brc-20.io, $ORDI has been the leading the way as the highest valued BRC-20, with a market cap of $1.4B as of writing.[12] The initial pump in BRC-20s ended with a significant drop from May 9th-11th, going from $990 million to $379 million, representing a 62% decline.

The BRC-20 market is heavily influenced by the capitalization of the ORDI token, which accounts for over 80% of the trading volumes. The importance of the ORDI token in this market means that price fluctuations directly impact the market cap of BRC-20 tokens.

Regardless of the factors driving volatility among BRC-20 tokens, data indicates that the ecosystem surrounding the inscription of such assets remains robust, with activity rising after a relative lull between May and July 2023, and with a more recent spike in activity following a trough between late September 2023 and to late October 2023. Notably, the number of BRC-20 tokens inscribed reached a new all time high in November 2023, with over 492,000 tokens minted.



Key Findings

- Innovative Use of Blockchain Technology: The Ordinals Protocols, by leveraging the Taproot upgrade, has enabled the embedding of rich data onto the Bitcoin blockchain, thereby diversifying the kinds of assets Bitcoin can natively support.

- Enhanced Market Potential: Ordinals have attracted new users and market demand, showcasing the Bitcoin blockchain's expanded capabilities. This has included the creation of unique digital assets, sparking interest in digital collectibles and artworks across Bitcoin, and driving increased demand for block space.

- Emergence of Recursive Ordinals: The introduction of recursive ordinals marks a significant advancement, enabling complex software operations and circumventing the 4MB limit of standards imposed by standard ordinals. This opens up the possibilities for more intricately interconnected data sources, enhancing storage efficiency, and reducing transaction costs.

- Potential for DeFi Architectures: Recursive ordinals have paved the way for sophisticated DeFi architectures built on Bitcoin. They extend the possibilities beyond simple file concatenation, allowing for the creation of decentralized platforms that require complex logic and algorithms.

Future Developments and Impact

Looking forward, ordinals and recursive ordinals are likely to continue to impact the Bitcoin ecosystem. The potential to host extensive files, such as applications or video games directly on-chain allows for numerous innovative use cases. As developers explore the potential to integrate complex structures on Bitcoin, such as the Ethereum Virtual Machine and Solidity, it may shift the dynamic of maximalism in the ecosystem.

However such evolutions do not come without challenges. Controversy over the numbering schema and the centralization concerns in maintaining and submitting changes to the protocol settings highlight the delicate balance between innovation and adherence to the decentralized tenets upon which Bitcoin, and networks like it, were founded.

Moreover, the impact of Ordinals on transaction fees, block space utilization, and the overall scalability of the Bitcoin blockchain remains a topic of ongoing discussion. As the market for ordinals matures and more platforms emerge to fill that space, we may yet see a clearer image of how these new entries in the digital artifact pantheon integrate with the broader Bitcoin ecosystem, and that of interconnected Web3 platforms.

So, while the full potential and long-term implications of ordinals and recursive ordinals have yet to unfold, these novel innovations represent a milestone in the evolution of Bitcoin. As the ecosystem continues to change and adapt, we can expect to see further developments that continue to harness the unique capabilities of ordinals, and which may potentially reshape the very landscape of blockchain technology, and digital assets.

Taproot Assets: Making Bitcoin a Multi-Asset Network

Mid-October, Lightning Labs announced the Alpha version of “Taproot Assets”, a meta-protocol allowing arbitrary assets to be issued and managed on the Bitcoin blockchain.13 Through Taproot Assets, fungible and non-fungible tokens can be created, with the asset’s metadata stored in an existing UTXO. With Taproot v0.3, builders have all the foundational tools to make Bitcoin a multi-asset network.

Taproot Assets natively integrates with Lightning Network, enabling cheap and fast transactions with these arbitrary assets. Ryan Gentry, head of business development at Lightning Labs, said that this will start a new era for Bitcoin, where a “myriad of global currencies [are] issued as Taproot Assets, and the world's foreign exchange transactions [are] settled instantly over the Lightning Network.”13

But how will this affect Bitcoin? As usual, there is a stark divide between supporters of the development and those with concerns about its implications. Will there be a similar fee spike as we have seen with Ordinals and BRC-20s? Will this bring some regulatory scrutiny to Lightning Network as various assets are brought to the Bitcoin network?

Under the Hood of Taproot Asset Protocol (TAP)

Taproot Assets is a Taproot-powered protocol, relying on how data is stored after the Taproot upgrade to the network, just like BRC-20s.14 However, compared to BRC-20s and other fungible token protocols on Bitcoin, such as RBG, Taproot Assets rely on “universes” to keep track of token ownership information. The concept of universes is expanded on further below.

The process of creating Taproot Assets is technical, but in short, a specialized merkle tree, known as a ‘Merkle Sum, Sparse Merkle Tree (MS-SMT)’, and Taptweak, are used to create information for an asset.15 The three important elements in the creation process are the outpoint spent to mint the asset, an asset tag of the minter’s choice (e.g., a hash of a brand name), and meta information associated with the asset--links, images, or documents.

This is stored in a 32-bit asset ID, and the UTXO is the unique identifier for the newly created asset:

```
asset_id = sha256(genesis_outpoint || asset_tag || asset_meta)
```

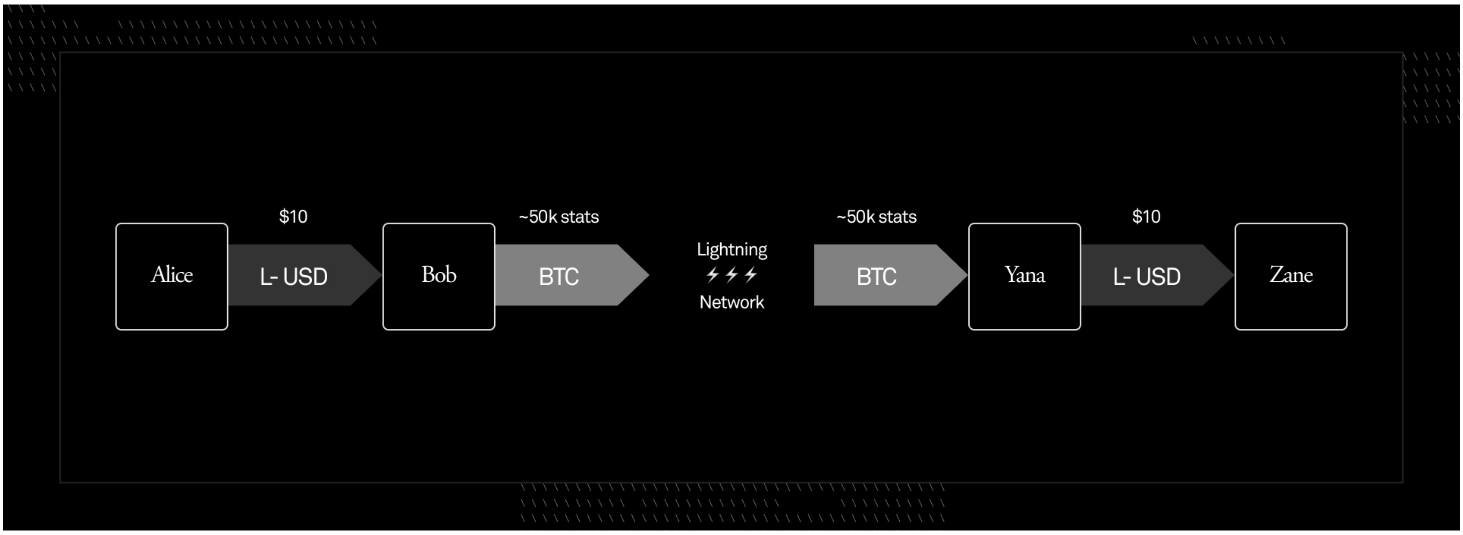
Transacting with Taproot Assets

Once created, Taproot Assets can be transferred on the Bitcoin blockchain or via channels directly on the Lightning Network. Compared to other fungible tokens on the Bitcoin blockchain, Taproot Assets improve chain efficiency by enabling multiple asset actions (mint, send, receive) in a single on-chain transaction, reducing congestion and fees. This is contrary to BRC-20, which also enables arbitrary asset creation, but significantly congests the Bitcoin network and spikes fees (which peaked at an all time high of $30 during the initial ordinal frenzy.16

The most compelling use for Taproot Assets is its compatibility with Lightning Network (LN.) Although the assets are issued on the Bitcoin blockchain, bridging to LN to benefit from the lower transaction cost and faster transactions will bring expanded utility to the assets. In the future, direct deployment to Lightning Channels will also be possible.

At a high level, transacting with Taproot Assets on LN is trivial; there is no need to opt-in as a routing channel for these payments. Bitcoin can provide liquidity for payments denominated in various assets. Thus routing node operators are incentivized to help route Taproot Assets to earn more routing fees paid in satoshis.

The below example shows a scenario where L-USD transfers (Lightning Network USD, a Taproots Asset stablecoin) can be paid with BTC and ultimately settled as Taproot Asset, in this case, L-USD. This is made possible by edge liquidity: LN nodes willing to swap their value to BTC and back, allowing you to pay any LN invoice with Taproot Assets or receive any asset by issuing a standard Lightning invoice.



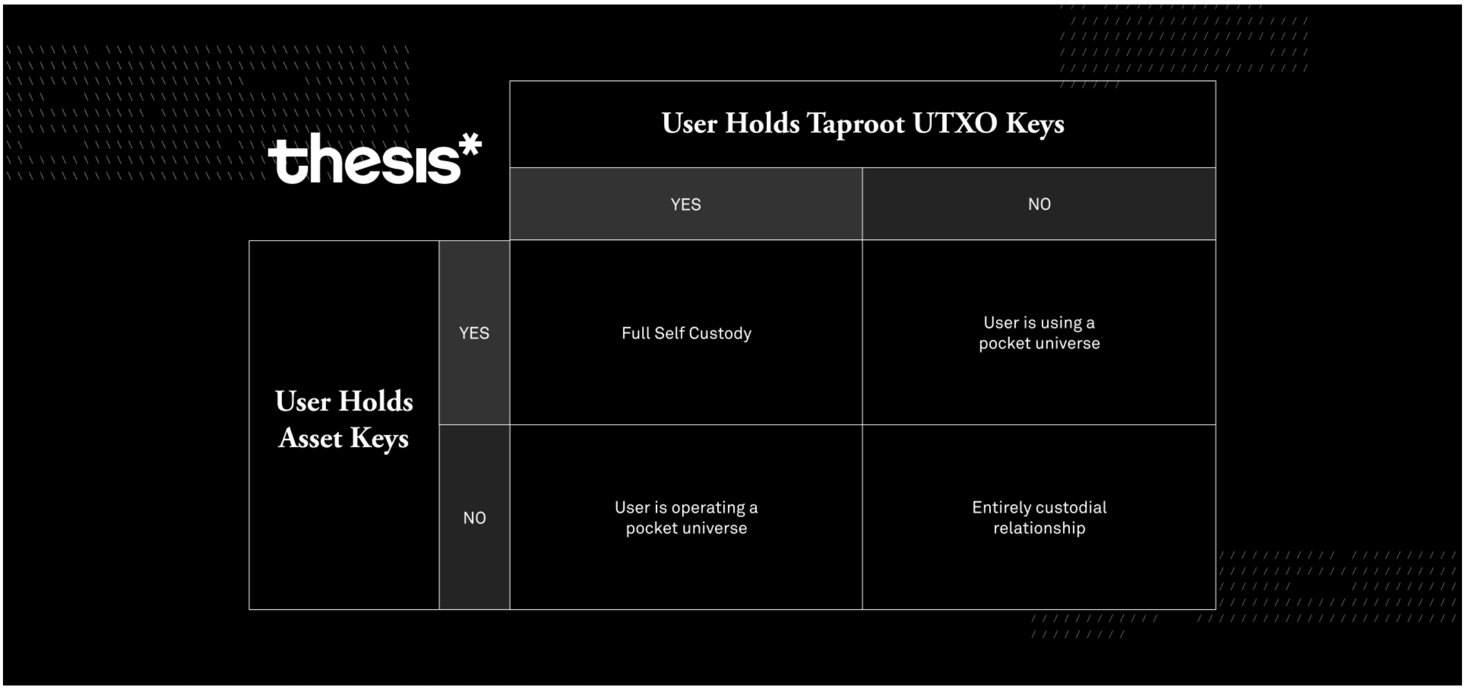
Notice that the intermediary transactions do not route the stablecoin itself – there is no need to opt-in, the transactions can be routed so long as there is available BTC liquidity. An invoice ultimately settled in Taproot Assets can be paid by BTC or any other asset, and anyone with a Taproot Assets balance can pay any Lightning invoice.17

Custody and Ownership of Tokens

As mentioned above, the custody and ownership of Taproot Assets differs from other fungible tokens on Bitcoin.

A Taproot Assets universe is a repository of assets and their proofs, essentially a full node for specific assets, providing historical data for validation. The universe will have all relevant information for the token, such as issuance, recent transfers, quantity, and more, but the information can only be released at the discretion of the "universe operator." Thus, compared to a blockchain explorer, the Taproot universe is much more private.

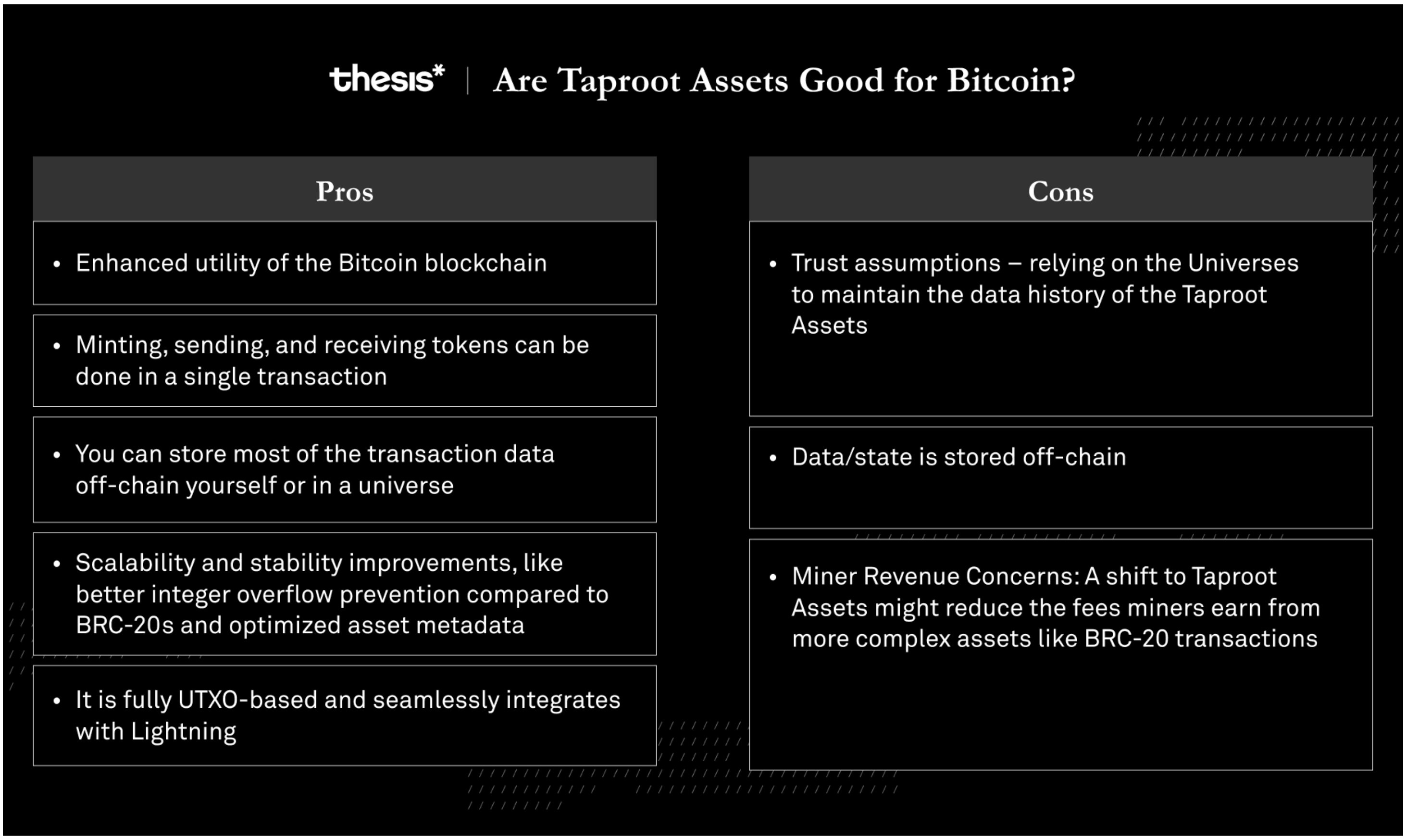
The pocket universe is a way to collectively store Taproot Assets and use TAP (Taproot Assets Protocol,) without giving up ownership of assets. A pocket universe controls the Taproot key to a UTXO, but not the keys to the (possibly multiple) Taproot Assets held in that UTXO. Asset holders can use the pocket universe to batch their transactions efficiently.



		User Holds Taproot UTXO Keys	
		YES	NO
User Holds Asset Keys	YES	Full Self Custody	User is using a pocket universe
	NO	User is operating a pocket universe	Entirely custodial relationship

Pros and Cons of Taproot Assets

At a general level, we can look at how Taproot Assets might be beneficial to Bitcoin, and understand some of the positives and negatives to the upgrade.



thesis* | Are Taproot Assets Good for Bitcoin?

Pros	Cons
• Enhanced utility of the Bitcoin blockchain	• Trust assumptions – relying on the Universes to maintain the data history of the Taproot Assets
• Minting, sending, and receiving tokens can be done in a single transaction	• Data/state is stored off-chain
• You can store most of the transaction data off-chain yourself or in a universe	• Miner Revenue Concerns: A shift to Taproot Assets might reduce the fees miners earn from more complex assets like BRC-20 transactions
• Scalability and stability improvements, like better integer overflow prevention compared to BRC-20s and optimized asset metadata	
• It is fully UTXO-based and seamlessly integrates with Lightning	

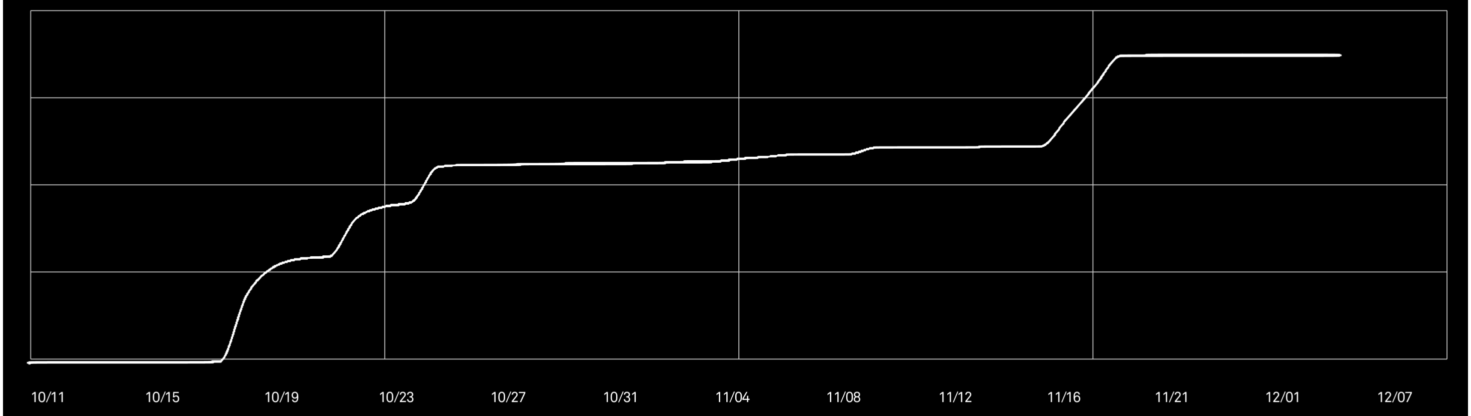
The Numbers

The current transaction and value data for Taproot Assets on Bitcoin is minimal. Although there have been nearly 65,000 unique asset mints on the network, the protocol is in its very first implementation phase, and thus these are largely experimental.

Given the explosion we have seen in BRC-20s this year, it will be interesting to follow whether Taproot Assets can find similar demand. Once there is support for direct deployment to lightning channels, we expect to see more activity and use of the TAP.

Taproot Assets Universe

64,664 Asset Mints



Source: Terminal.Lightning

Why Taproot Assets on Bitcoin: Is This Needed?

Everything above sounds great, but how does this solve a problem in Bitcoin? Swapping between arbitrary assets on bitcoin is currently price-prohibitive, as seen in BRC-20s. There is a demand to have non-BTC assets to transact within a secure and trustless way on the Bitcoin blockchain, this is evident by the fact that DeFi and different blockchain ecosystems thrive as multi-asset networks.

Bringing Taproot Assets to Lightning Network brings the vision of bitcoin as a global payment network to life. Imagine an entity that creates a new stable asset, L-USD, with $1M in USDC in custody. If you have the L-USD tokens, you can send BTC and L-USD to Lightning Network in a single transaction and begin trading and swapping your L-USD assets for minimal cost and at high speeds. Any DeFi-style transaction, which has processed billions in volume on other networks, is now possible on Lightning Network thanks to Taproot Assets.

It doesn't matter if you are simply a spot BTC holder or a dedicated user of DeFi, Bitcoin is expanding its use-cases via TAP, and with the expansion in use-cases, new users and demand will flow to the network. At the end of the day: Bitcoin needs to enable a fair, accessible, and non-biased financial system, and the TAP is a step in that direction.

Consumer-Facing Bitcoin Applications

Consumer applications are one of the most important onboarding tools for newcomers in crypto. Centralized exchanges serve as an entry point for buying the asset, but the consumer-facing application is what most users will be using at the end of the day. Regardless of where you land on the “BTC is money” conversation, there is no doubt that consumer applications play an important role in engraining bitcoin into our lives. Simple ways to save, buy, and transact in BTC, available via mobile phone, is a sure-fire way to increase the adoption of BTC as an asset and form of money.

2023 saw a significant growth of interest in the diverse uses of BTC. These applications, varying from rewards programs to financial services, are more than mere functionalities; they represent a crucial shift in how Bitcoin is integrated into everyday life. Financial services are solidifying bitcoin as a practical savings vehicle. Gaming platforms are innovatively incorporating Bitcoin, transforming gameplay into opportunities for bitcoin acquisition. Privacy-focused wallets emphasize the importance of security and anonymity in the digital space.

Each of these applications contributes to the unfolding story of Bitcoin – a narrative of practicality, diversity, and user-centric innovation. They are leveraging Bitcoin's capabilities and actively broadening its appeal and usage, making it accessible to a wider audience.

These consumer apps can be broadly categorized into the below sectors, each representing a unique aspect of Bitcoin's growing influence and versatility in the digital world. This exploration seeks to delve into these categories, uncovering how they contribute to Bitcoin's global adoption, navigate their distinct challenges, and collectively drive the evolution of Bitcoin in our interconnected digital era.

Bitcoin Rewards and Cashback

One of Thesis’s portfolio companies, Fold, offers a simple way for users to buy and earn bitcoin on everyday purchases with their cashback debit card.

Despite a slew of competitors in the space, Fold offers the cheapest place to buy BTC when looking at fees and spreads, and these even take into account Coinbase.18

The product saw several key updates in 2023:

- New Features: Introduction of Bitcoin Buying with Round-Ups, allowing users to round up purchases to the nearest dollar for bitcoin purchases, and instant withdrawals from Fold to cold storage.
- Enhanced Gaming Experience: Guarantee of 1% back on every purchase for Spin+ users, alongside the opportunity to win up to a whole bitcoin on the new Spinwheel.
- Account Funding Updates: Introduction of a 1.5% fee for instant debit transfers and forthcoming instant ACH transfers with lower fees.
- Expanded Bitcoin Integration: Implementation of Bitcoin's Lightning Network for faster transactions across the Fold ecosystem.

Lolli: Provides Bitcoin rewards for shopping at partner retailers online. With over 25,000 stores with eligible rewards, the product has seen rapid adoption.

- Expansion to Retail Locations: Transition from a web-only app to being available in over 900 retail locations across the U.S., significantly broadening its user reach.
- Strategic Partnerships: Collaboration with major retailers like Safeway, a subsidiary of Albertson, marking Lolli's expansion into retail alongside web services.
- User Rewards: Users receive a 3-5% return on purchases, aligning with the mission to integrate Bitcoin into daily lives and make it accessible to the masses.
- Diverse User Base: Approximately 40% of Lolli's users are new to buying cryptocurrency, indicating its role in introducing Bitcoin to a wider audience

SatsBack: A platform offering Bitcoin rewards for shopping at various online stores.

- Launch of Satsback v2: A relaunch with a new version, connecting to 10,000 online stores offering cashback in bitcoin through the Lightning Network and a browser extension to enhance the shopping experience.

- Focus on European Markets: Targeting specific European markets including The Netherlands, Germany, Poland, the UK, France, and Belgium, while lowering the barrier of entry to the Bitcoin ecosystem for beginners.
- Connections with Major Brands: Partnerships with prominent brands like Booking and Nike.

Shopping and Services with Bitcoin

Bitrefill: Allows users to buy gift cards, mobile phone top-ups, and everyday purchases with BTC.

- Expansion in 2023: Bitrefill, a Swedish startup, expanded its services to the U.S. in 2023. Known for offering gift cards and mobile top-ups for cryptocurrency users, it introduced a new service called Pay Bill.
- Pay Bill Features: This service allows users to pay various bills, including credit card, utilities, auto loans, healthcare, mortgage, social security, property taxes, and even funeral services using cryptocurrencies like Bitcoin, Ethereum, Litecoin, Dogecoin, DASH, and Tether (USDT).
- Growth and Partnerships: Initially launched in El Salvador after Bitcoin became legal tender there, Pay Bill has grown rapidly. Bitrefill partnered with Arcus Financial, a regulated payments platform, for its U.S. launch.

OpenBazaar: A decentralized marketplace where users can buy and sell goods and services directly with bitcoin.

- Revival in 2023: After shutting down in 2020 due to funding issues, OpenBazaar announced its comeback in 2023. The decentralized marketplace platform, previously known for allowing users to buy and sell goods and services directly with Bitcoin, is being rebuilt.
- Updates and Development: OpenBazaar's website indicates the upcoming launch of "openbazaar 3.0." The platform's CEO, Brian Hoffman, has been working on a new implementation of OpenBazaar in the Rust programming language, which is gaining popularity in the Bitcoin community.

Bitcoin-Focused Financial Services

River Financial: A financial service specializing in Bitcoin, offering buying, selling, and managing Bitcoin investments.

- Significant Funding: Raised $35 million in a Series B round, backed by Kingsway Capital and Peter Thiel, indicating robust growth and confidence in their services.
- River Lightning Integration: Launched an API for easier access to the Lightning Network, enhancing Bitcoin transaction efficiency.
- Comprehensive Services:
  - Bitcoin-Only Exchange: Focused approach for heightened security and ease of use.
  - Security: Implements offline cold storage and 2FA, using military-grade technology.
  - Private Client Service: Personalized assistance for larger Bitcoin transactions.
  - River Mining: Offers Bitcoin mining hardware purchase and hosting services.
  - Recurring Bitcoin Purchases: Fee-free, automatic Bitcoin investment options.
  - App Accessibility: iOS app for managing Bitcoin purchases and mining; no Android app yet.
- Regional Availability: Operational in 48 U.S. states, excluding Nevada and New York.

Swan Bitcoin: Focuses on Bitcoin savings plans, allowing users to buy Bitcoin automatically and regularly.

- Operational Changes in Texas: Temporarily paused Bitcoin purchasing due to regulatory processes, with plans to resume in Q1 of 2024.
- Custodian Transition: Switched to BitGo Trust Company and Fortress Trust for improved client asset management.

Strike: A financial app that allows users to send and receive money globally, with an option to convert payments to Bitcoin.

- Global Expansion: Extended service to over 65 countries, reaching an estimated 3 billion people worldwide.
- Enhanced App Features:
  - USDT Support: Integrated support for USDT (Tether)【52†source】.
  - Lightning Wallet Functionality: Enabled Bitcoin transactions via dollar-equivalent channels.

Bitcoin Gaming and Entertainment

Zebedee: Provides a platform for Bitcoin gaming, enabling gamers to earn Bitcoin through in-game activities.

- 2023 Developments: Zebedee has introduced a significant feature in its app, allowing users to instantly send money to various jurisdictions, including the Philippines and Brazil, at minimal costs using Bitcoin's Lightning Network. This feature connects Zebedee accounts to bitcoin payment firms like Pouch and Bipa, enhancing the gaming and payment experience.
- Open Source Bitcoin Initiative: Additionally, Zebedee launched the "No Big Deal" (NBD) nonprofit organization, aiming to advance open-source Bitcoin development. NBD's launch included several projects dealing with hosted channels on the Lightning Network, facilitating faster and cheaper bitcoin transactions.

Privacy and Security Focused

Wasabi Wallet: A privacy-focused Bitcoin wallet that implements CoinJoin for transaction anonymization.

- Latest Developments:
    - Version 2.0.4 Release: Wasabi Wallet has released version 2.0.4, incorporating highly requested features and performance optimizations. These enhancements notably speed up wallet load times and resolve transactions stuck in the mempool, significantly benefiting privacy-focused Bitcoin users.
    - Coin Control Reintroduction**: Version 2.0.3 was released earlier in the year, bringing back the Coin Control feature. This update provides optional insight and control over the wallet's Smart Coin Selection Algorithm, enhancing user control for sending transactions.

Samourai Wallet: Another privacy-enhanced Bitcoin wallet offering robust security features.

- Key Updates:
    - Sentinel Update v5.0.0: This significant update introduced a comprehensive redesign and overhaul of the Sentinel, offering a new way to interact and manage public keys.
    - Wallet Update 0.99.98i: This update laid the foundation for the Sentinel watch-only app update and introduced several new features, marking a significant step in the wallet's evolution.
    - Dojo 1.21.0 Release: This release featured multiple updates, including improvements to Tor, BTC-RPC Explorer, MariaDB, Fulcrum, and Nginx, along with the introduction of a new feature.

- Wallet Update 0.99.98h: Focused on a range of stability improvements and bug fixes, this update also brought new tools and enhancements to the wallet, further fortifying its security and functionality.

Contribution to Bitcoin's Global Adoption

Bitcoin has come a long way since its inception in 2009. Over the years, various companies have contributed to Bitcoin's growth and adoption, making it more accessible, practical, and versatile than ever before.

Applications like Fold, Lolli, and Bitrefill are democratizing Bitcoin accessibility, making it more accessible and usable for everyday consumers. By offering Bitcoin rewards for common activities like shopping and purchasing gift cards, they integrate Bitcoin into daily life, encouraging broader adoption among those who may not typically engage with cryptocurrencies.

Services like River Financial, Swan Bitcoin, and Strike are expanding Bitcoin's financial utility by transforming it from a speculative investment to a practical financial tool. They provide platforms for regular Bitcoin investment, global money transfers, and even bill payments, showcasing Bitcoin's versatility as both an asset and a currency.

Lightnite and Zebedee are pioneers in integrating Bitcoin into the gaming industry. By allowing players to earn Bitcoin through gameplay, they're creating a new avenue for Bitcoin acquisition and bringing it into a popular and fast-growing sector, appealing to a younger, tech-savvy audience.

Privacy-focused wallets like Wasabi Wallet and Samourai Wallet enhance Bitcoin's privacy and security features. They make Bitcoin safer and more attractive for users who prioritize data protection and anonymity by providing robust privacy features.

Tippin.me facilitates microtransactions and tipping by leveraging Bitcoin's Lightning Network to enable small, instant payments. This demonstrates Bitcoin's flexibility in transaction sizes and encourages its use in new, innovative contexts such as online content creation and social media.

Navigating the Challenges: The Road Ahead

As novel applications like Fold and Bitrefill grow, they face real-world hurdles like scalability and network congestion. These challenges can lead to slower transactions and higher fees during peak times, impacting the overall user experience.

For financial services such as River Financial and Strike, the evolving regulatory landscape presents its own complexities. Staying compliant and adapting to new rules is a constant challenge that could significantly affect their operation and growth.

Gaming platforms Lightnite and Zebedee are at the forefront of integrating Bitcoin into the gaming industry. Their challenge lies in attracting traditional gamers to this new model, requiring a mix of innovative gaming experiences and effective education about Bitcoin's role in gaming.

Privacy-focused wallets like Wasabi and Samourai Wallet are continuously working to stay ahead of evolving cyber threats. Their ongoing commitment to maintaining high levels of security and privacy is crucial in a landscape where data protection is paramount.

Finally, the inherent volatility of Bitcoin presents a unique challenge for applications that rely on its stability for transactions and rewards. Fluctuating Bitcoin prices can influence the perceived value of rewards and affect user trust and long-term engagement with these applications.

Fold: A Case Study in Bitcoin Rewards and User Adoption

User Engagement and Growth

Fold's journey in the Bitcoin rewards space is marked by rapid user adoption and extensive participation. As the platform approaches a significant milestone of one million users, it highlights the burgeoning interest in cryptocurrency rewards and the growth of the Bitcoin economy.

The initial phase saw over 250,000 individuals eagerly joining the waitlist. Additionally, the early adoption of the Fold Card program by 20,000 users demonstrated the willingness of consumers to engage with new financial products, especially those offering innovative rewards in Bitcoin.

Transaction Volumes and Bitcoin Rewards

Since its launch in November 2020, Fold has seen high transaction volumes, with nearly $1.5B transacted on the platform. This substantial figure signifies users' trust and reliance in Fold for their financial transactions and Bitcoin investments. The platform's success in transaction volumes strongly indicates the increasing normalization of Bitcoin in everyday financial dealings.

Moreover, the collective earning of over 65 billion satoshis by users through the app is a testament to the app's effectiveness in promoting Bitcoin stacking. The reward structure, offering between 1% to 20% returns on purchases, not only incentivizes the use of Bitcoin but also positions it favorably against traditional payment methods. This rewarding user experience is crucial in driving the adoption of Bitcoin for regular transactions, making it an attractive alternative to traditional currencies.

Implications for Bitcoin Adoption

The rapid growth in user numbers and high transaction volumes indicate a shift in consumer behavior towards embracing Bitcoin in everyday transactions. This adoption is not limited to seasoned cryptocurrency enthusiasts but extends to a broader audience, indicating the potential for Bitcoin to become a more integrated part of the financial system.

In conclusion, Fold's popularity is only a microcosm of the larger trend of Bitcoin adoption, which exemplifies how innovative platforms can leverage the unique qualities of cryptocurrencies to offer novel solutions and rewards, thereby driving wider acceptance and integration of digital currencies into everyday life.

A Cross-Chain BTC: Bringing bitcoin the Asset Beyond Bitcoin the Network

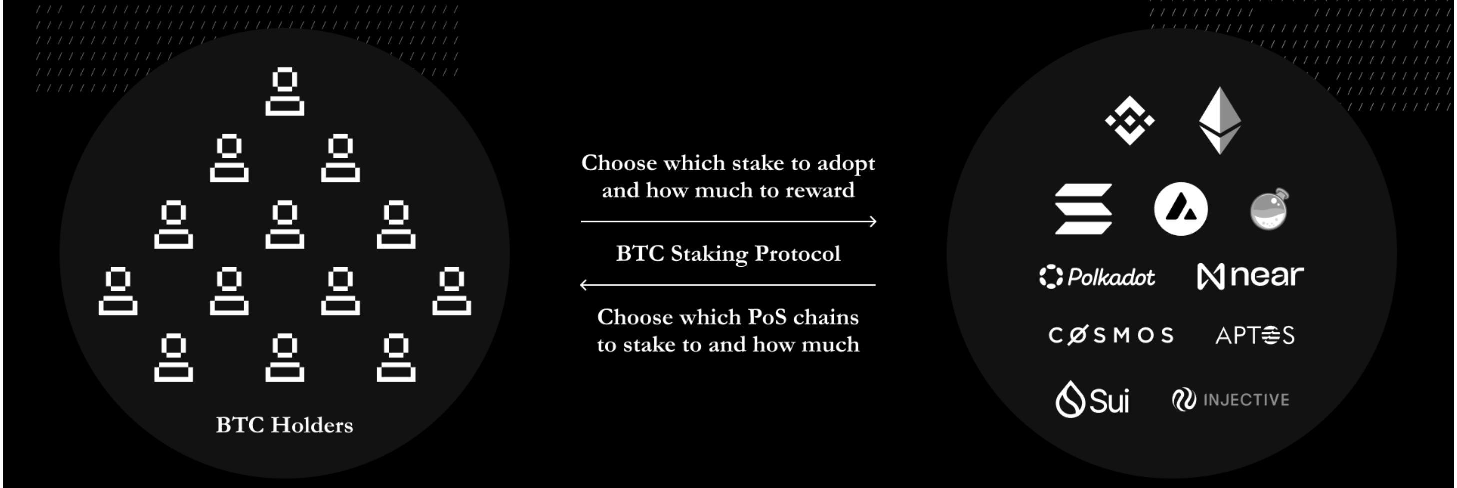
Staking Bitcoin/Yield on BTC

One of the biggest crypto trends in the past few years has been the proliferation of staking assets. Initially seen in proof-of-stake blockchain networks such as Peercoin, the concept has proliferated through crypto and is popular in DeFi, where users can stake their assets for a percentage of fee distribution, token emissions, and more.

This concept of staking for an extra yield has become so popularized that many crypto market participants have difficulty accepting anything that does not generate a yield for them. While this concept of yield has resulted in many unsustainable protocol designs and requires giving up asset custody, specific solutions are being built to bring yield to BTC in a safe and ethos-aligned manner.

Babylon is creating a way to enable BTC to help secure various POS chains without requiring BTC to be bridged yet still providing the POS chain with slashing guarantees. This is done by remote staking, where the staked bitcoins are locked in a contract on the Bitcoin chain and then slash the stake when there is a protocol violation on the consumer PoS chain, similar to shared security solutions such as EigenLayer for Ethereum or Cosmos' mesh security.

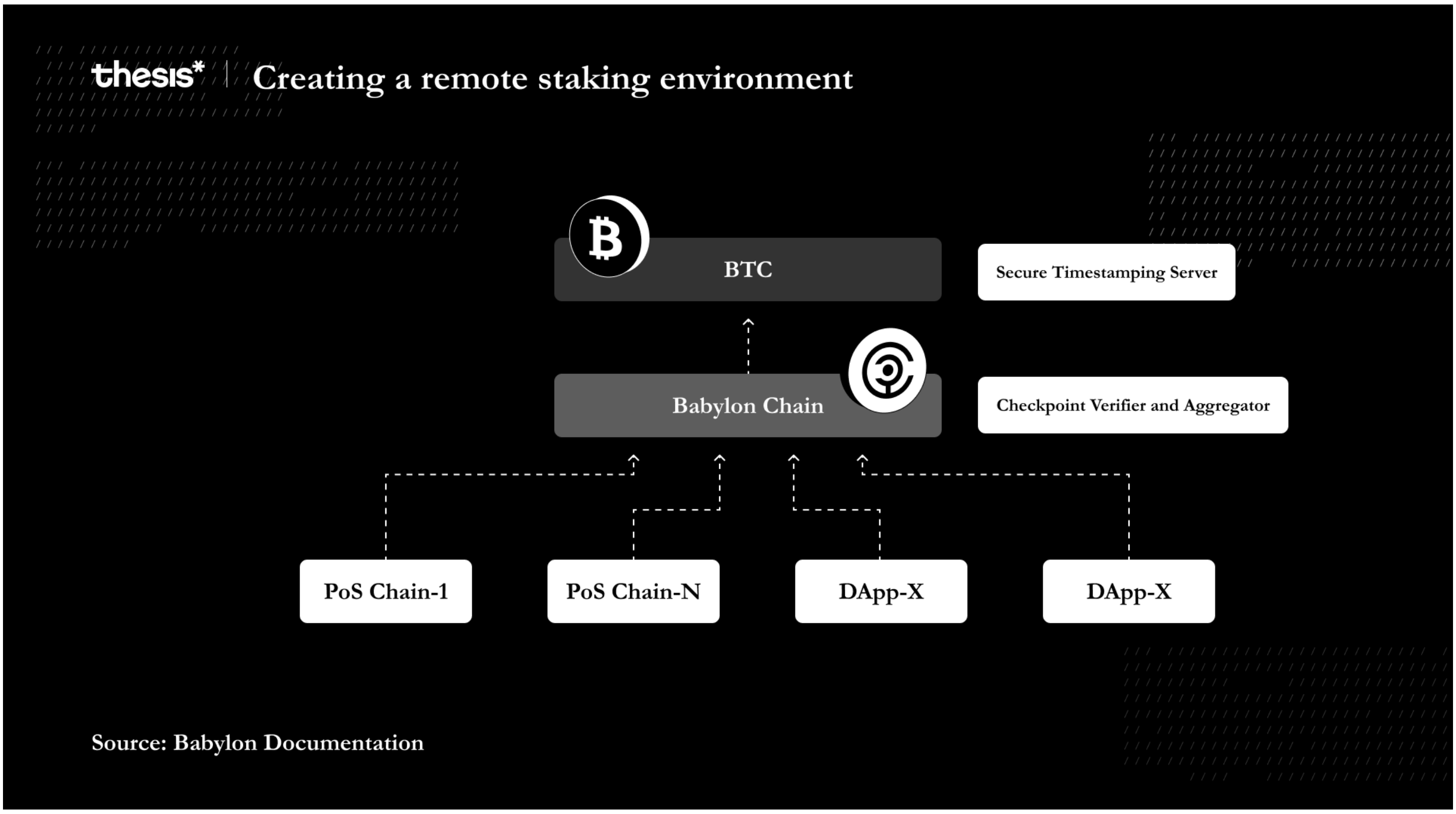
thesis* | Bitcoin Staking is a two-sided market place


BTC Holders
Choose which stake to adopt and how much to reward
BTC Staking Protocol
Choose which PoS chains to stake to and how much
Polkadot
near
COSMOS
APTOS
Sui
INJECTIVE

Source: Babylon Whitepaper

Since Bitcoin does not have smart contract functionality, Babylon can create a remote staking environment through advanced cryptography, consensus protocol innovations, and optimized use of the Bitcoin scripting language. Key features of the Babylon are:

- Bitcoin timestamping helps synchronize the PoS chain with the Bitcoin network and enables fast unlocking of the staked bitcoins.
- Extractable one-time signature (EOTS) allows the staked bitcoins to be slashed in the event of a malicious staker.


thesis*
Creating a remote staking environment
BTC
Secure Timestamping Server
Babylon Chain
Checkpoint Verifier and Aggregator
PoS Chain-1
PoS Chain-N
DApp-X
DApp-X

Source: Babylon Documentation

The concept of native BTC staking on Bitcoin to secure other PoS chains is valuable for various reasons. Firstly, the function to stake BTC is completely siloed within the Bitcoin network. Not only does this eliminate the bridging risk of BTC, which often involves custodians and other trusted third parties, but it also maintains the demand within the Bitcoin network, which can help boost fees paid to network miners. Of course, this also generates a new way to earn on BTC, improving its viability as an asset and store of value. And finally, the PoS chains that are inheriting security from Bitcoin benefit from the most valuable and decentralized cryptocurrency in the world. For example, ATOM, which helps secure the Cosmos network, has a market cap of ~$3B. This means it would only require 3.5% of BTC to be staked and securing the Cosmos network to double its economic security.

As the PoS chains all have significantly lower market capitalizations than Bitcoin, the added economic security is a massive value add for Babylon and native BTC staking.

Bitcoin Wrappers

Helping proliferate BTC in various DeFi ecosystems, we have seen forms of BTC wrappers become increasingly popular. The architecture varies significantly between each type of wrapper, but the underlying premise is that BTC is locked/stored in one location, and minted elsewhere. This helps transport wealth held on the Bitcoin blockchain into different ecosystems for various uses. Below, we'll look at some of the popular wrapper options today.

Avalanche's BTC.b

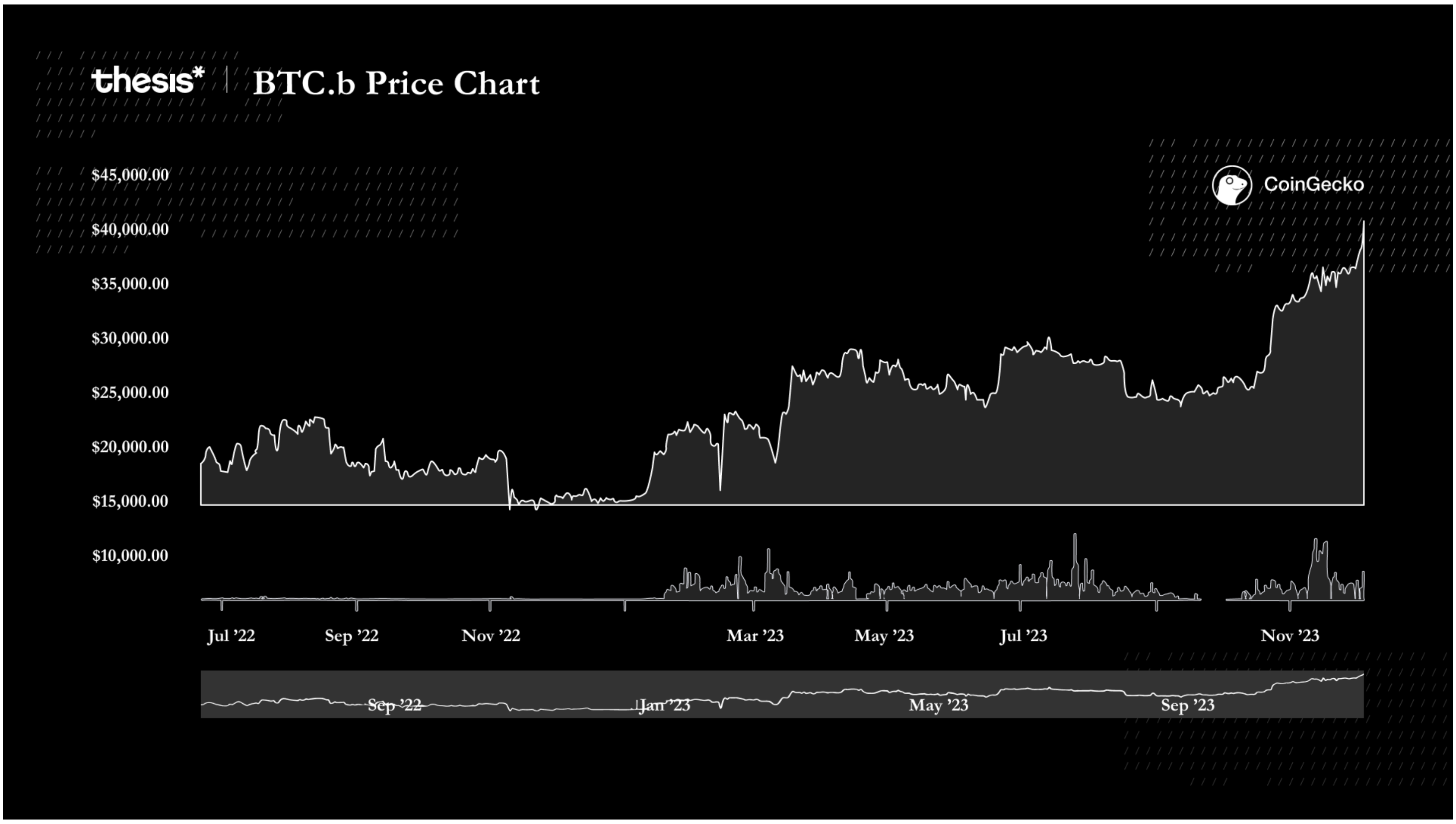
BTC.b is an ERC-20 representative of Bitcoin Avalanche in the ecosystem, specifically dwelling on the Avalanche C chain, which is a facet of the Avalanche blockchain ecosystem devoted to running EVM-compatible smart contracts.

The Avalanche Bridge employs a highly secure method with its C-Chain, involving a master key split into parts and distributed among 8 Bridge Nodes. These nodes use secure communication to verify identities and encrypt their share of the key, ensuring robust security throughout the system.

To wrap BTC on the bridge, users must initiate a transfer on the Bitcoin Network, sending their bitcoin to a specified bridge address controlled by the enclave. Once the transaction is confirmed on the Bitcoin Network, the Bridge Nodes indexes it.

Secure hardware in the enclave processes the transaction, and an equivalent amount of BTC.b, directly representative of what is locked in the bridge, is minted on the Avalanche C-Chain by the SGX application. Anytime users want to convert BTC.b back to BTC, they can send a transaction on the Avalanche C-Chain that burns the specified amount of BTC.b tokens. The Bridge Nodes index this transaction as in the case of wrapping, and the enclave processes it to send the equivalent amount of native BTC back to the user's wallet on the Bitcoin network.

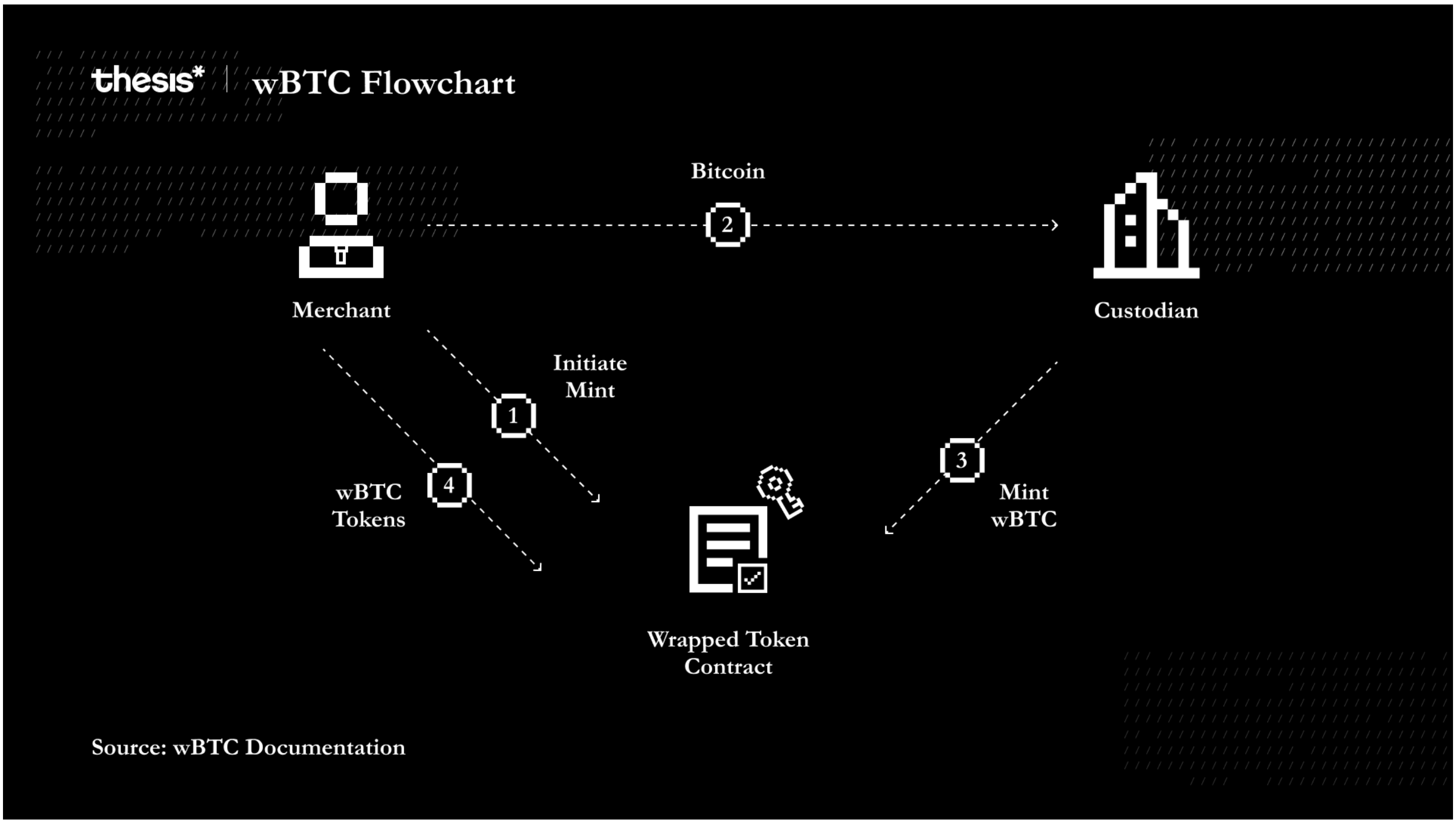
Demand for BTC.b is reflected by market activity, which shows a current market cap of $152.4M with a 24-hour trading volume of roughly $14.2M as of December 4, 2023. In addition, several trading volume spikes occurred throughout November 2023, BTC. BTC.b is traded across various decentralized exchanges, such as Uniswap V3 (Arbitrum One), Dexalot,and Trader Joe V2.1 (Avalanche), which allow users to swap BTC.b against other cryptocurrencies and stablecoins such as USDC.



wBTC

Short for wrapped bitcoin, wBTC is an ERC-20 token representing bitcoin on the Ethereum blockchain. It is another means by which BTC is linked to Ethereum, backed by a bridging process that pins wBTC and the BTC backing it as one-to-one pairs.

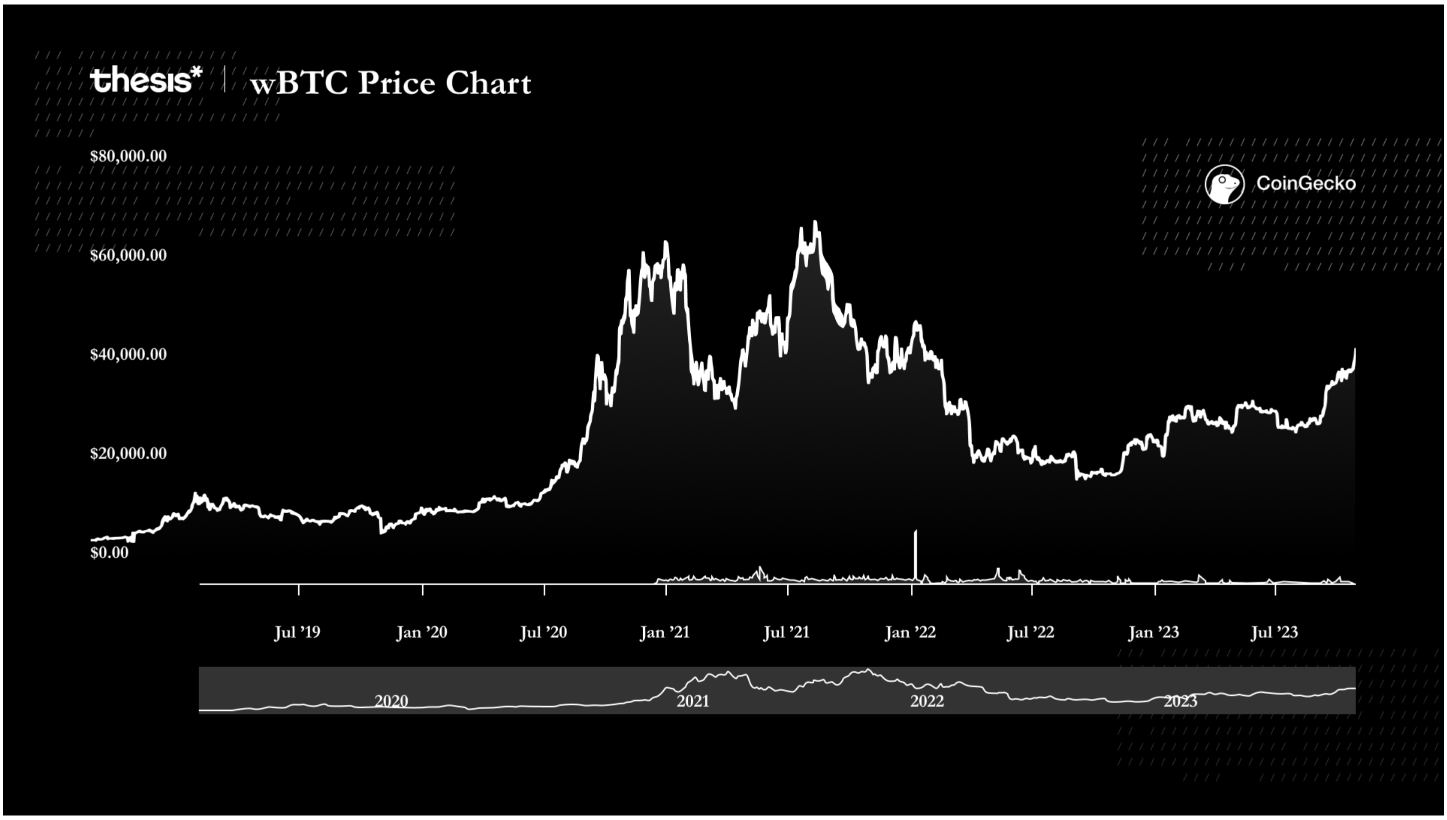
To create wBTC, users must deposit bitcoin with a designated custodian responsible for maintaining custody of the bitcoin. The custodians are typically regulated financial institutions or entities that adhere to fintech industry best practices but represent an interface with a centralized institution. Due to this facet of wBTC’s protocol, it is not a genuinely decentralized form of BTC on Ethereum.



Source: wBTC Documentation

Custodians initiate the creation of wBTC upon receiving BTC from a user, in collaboration with entities and merchants authorized to mint wBTC tokens that use smart contracts on the Ethereum blockchain that are configured to issue wBTC tokens at a 1 to 1 ratio with deposited BTC. wBTC tokens are distributed to a user's Ethereum wallet address upon mint.

Merchants similarly facilitate the unwrapping of wBTC, wherein a user sends the amount of wBTC they wish to convert back to BTC to a merchant who, in collaboration with the custodian, burns corresponding wBTC tokens so that the custodian may relinquish the equivalent amount of BTC back to the user's Bitcoin address.
System authenticity is maintained via regularly held audits from third-party firms and analyzing on-chain data.Demand for wBTC is reflected by market activity, which shows a current market cap of roughly $6.7B, with a 24-hour trading volume of just under $239M in the last 24 hours as of Dec 4, 2023. Around October 24, 2023 volume spiked to $639M, and again on Nov 9, 2023, to $560M.



Threshold and tBTC

tBTC, developed by Threshold, is a tokenized version of Bitcoin on the Ethereum blockchain. It is designed to enable Bitcoin's integration into other blockchains, including Ethereum and Solana. This integration facilitates Bitcoin's participation in decentralized finance (DeFi) applications.

tBTC operates on a decentralized model, utilizing a network of users and smart contracts. This structure allows it to function without centralized control, aligning with the decentralized principles of the Bitcoin network.

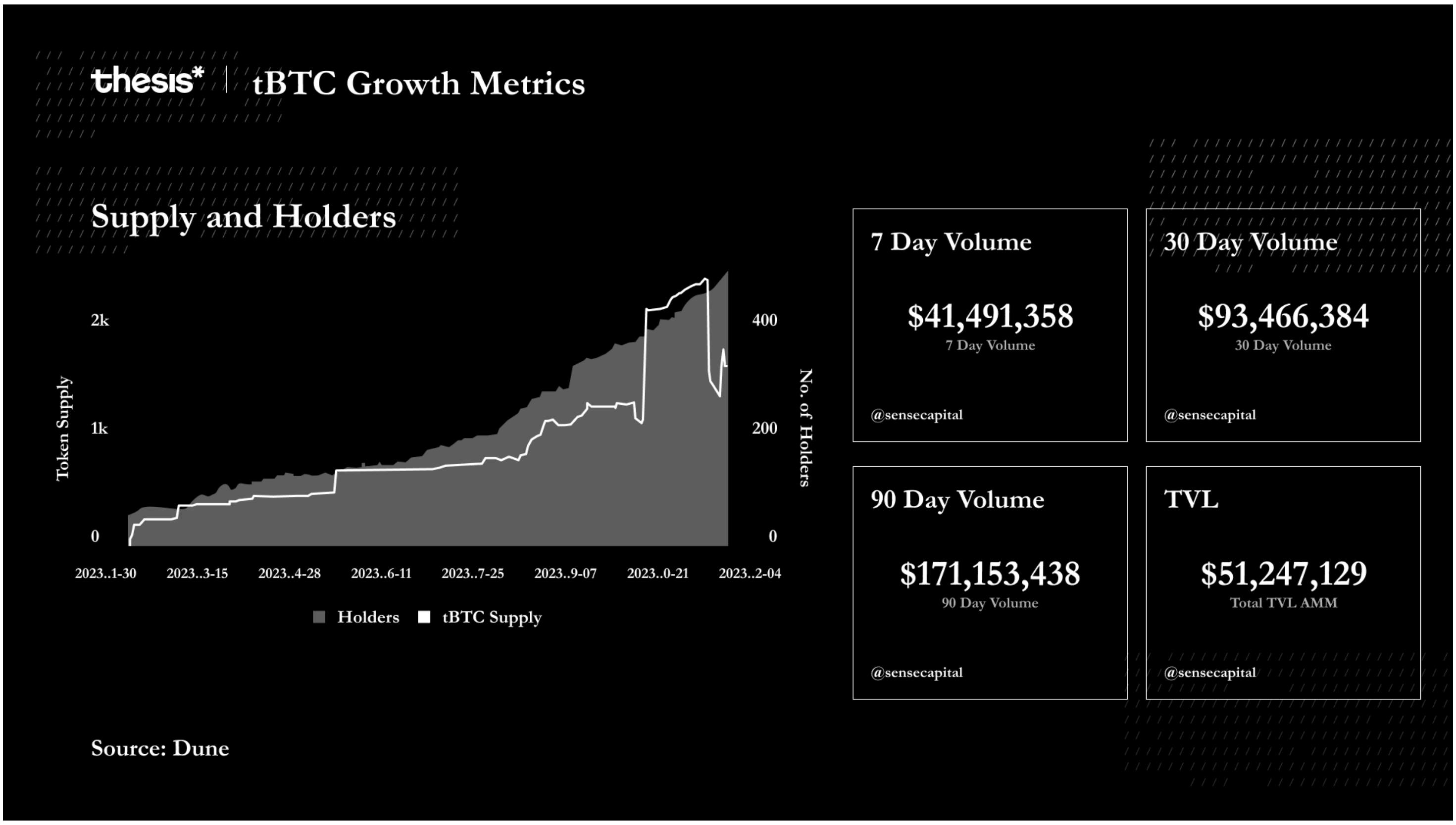
Unlike other forms of Bitcoin wrapped bitcoin, tBTC features a comprehensive SDK that supports its integration into various DeFi platforms. The SDK is designed to enhance the accessibility of tBTC in the broader DeFi landscape.

tBTC is designed to maintain user anonymity, operating without the need for Know Your Customer (KYC) protocols. This approach preserves user privacy and autonomy, consistent with the core principles of blockchain technology.

tBTC has been integrated into multiple blockchain networks, such as Ethereum, Solana, Optimism, Arbitrum, and Polygon.

This interoperability allows Bitcoin holders to engage seamlessly across different blockchain ecosystems.

Following its introduction, tBTC experienced a resurgence in its total value locked (TVL), indicating its adoption and utilization in the DeFi sector. Along with TVL growth, the number of holders of tBTC has been in a slow and steady uptrend all year, clearly demonstrating its market demand and value compared to some of the products that exist today.



thesis* | tBTC Growth Metrics

Supply and Holders

7 Day Volume

$41,491,358
7 Day Volume

@sensecapital

30 Day Volume

$93,466,384
30 Day Volume

@sensecapital

90 Day Volume

$171,153,438
90 Day Volume

@sensecapital

TVL

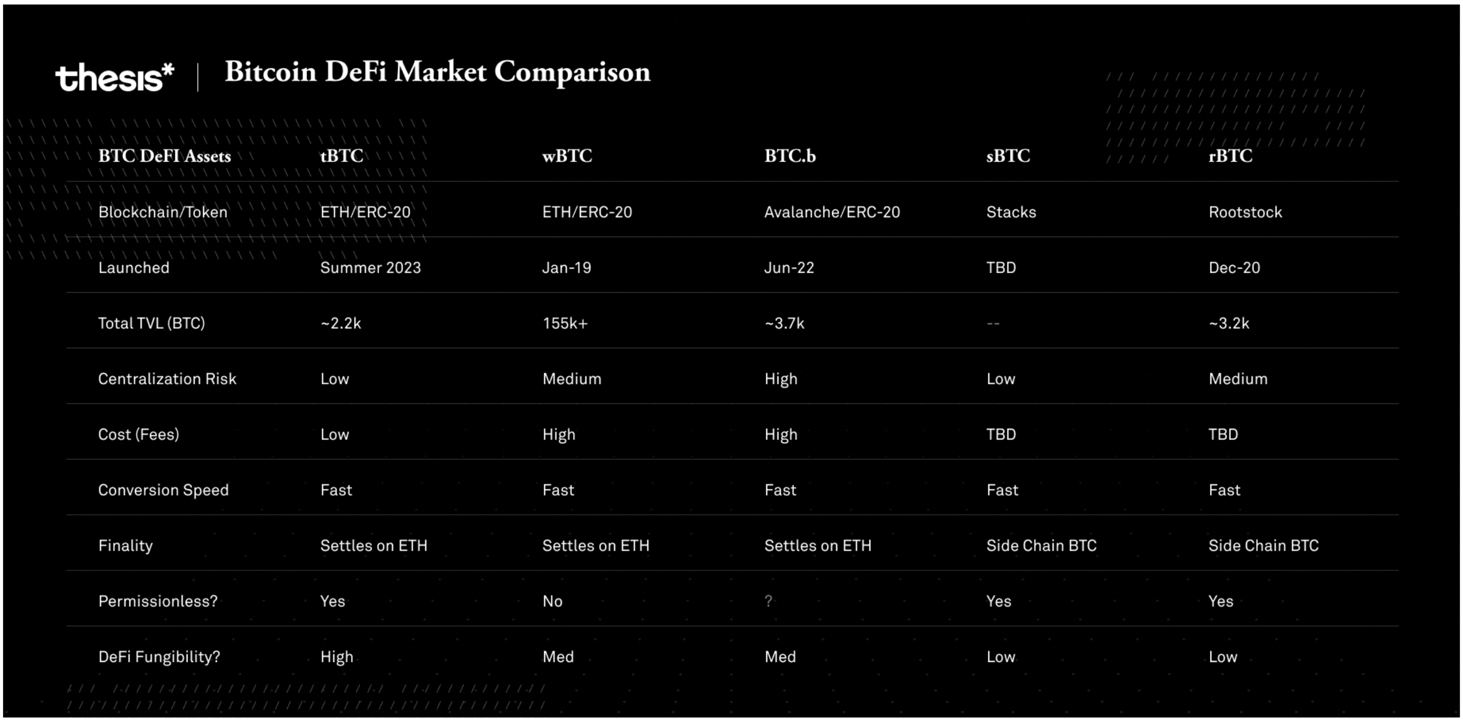
$51,247,129
Total TVL AMM

@sensecapital

Source: Dune

Threshold has formed partnerships to enhance the cross-chain functionality of tBTC, notably with Wormhole. These collaborations have expanded tBTC's presence across over 20 blockchain ecosystems.

Below is a comprehensive list of various BTC DeFi assets that dives into how exactly these BTC wrappers differentiate from one another. It will be worth while to keep an eye on which of the other BTC DeFi assets can begin to disrupt wBTC, which has been the clear first mover and gathered majority share of the market



thesis* | Bitcoin DeFi Market Comparison

BTC DeFI Assets	tBTC	wBTC	BTC.b	sBTC	rBTC
Blockchain/Token	ETH/ERC-20	ETH/ERC-20	Avalanche/ERC-20	Stacks	Rootstock
Launched	Summer 2023	Jan-19	Jun-22	TBD	Dec-20
Total TVL (BTC)	~2.2k	155k+	~3.7k	--	~3.2k
Centralization Risk	Low	Medium	High	Low	Medium
Cost (Fees)	Low	High	High	TBD	TBD
Conversion Speed	Fast	Fast	Fast	Fast	Fast
Finality	Settles on ETH	Settles on ETH	Settles on ETH	Side Chain BTC	Side Chain BTC
Permissionless?	Yes	No	?	Yes	Yes
DeFi Fungibility?	High	Med	Med	Low	Low

A Bitcoin ETF: What Institutional Adoption Means for Bitcoin and Regulatory Developments for BTC

2023 marks a historic year for bitcoin within U.S. financial markets. While the year began with a sour taste and leftover fear from the FTX blow-up, there has been growing confidence that bitcoin is here to stay and poised to make a serious impact within the traditional equity markets.

Although regulatory scrutiny regarding crypto from Gary Gensler and the SEC has been rampant, bitcoin has thrived. Now, with multiple ETF filings from the largest asset managers in the world, it is all but certain that approval is imminent and the SEC's crackdown is over. As the GBTC discount shrinks and inflows for BTC pick up, the institutional demand is already showing for BTC. But beyond the conceptual narrative of "institutional money flowing in," what does this mean for bitcoin the asset?

Bitcoin was originally crafted as an idea against power, against those controlling the financial markets. A way for the common person to free themselves without permission or oversight from anyone and under any circumstances. Thus, it is no surprise to see some split decisions about the impact of an ETF.

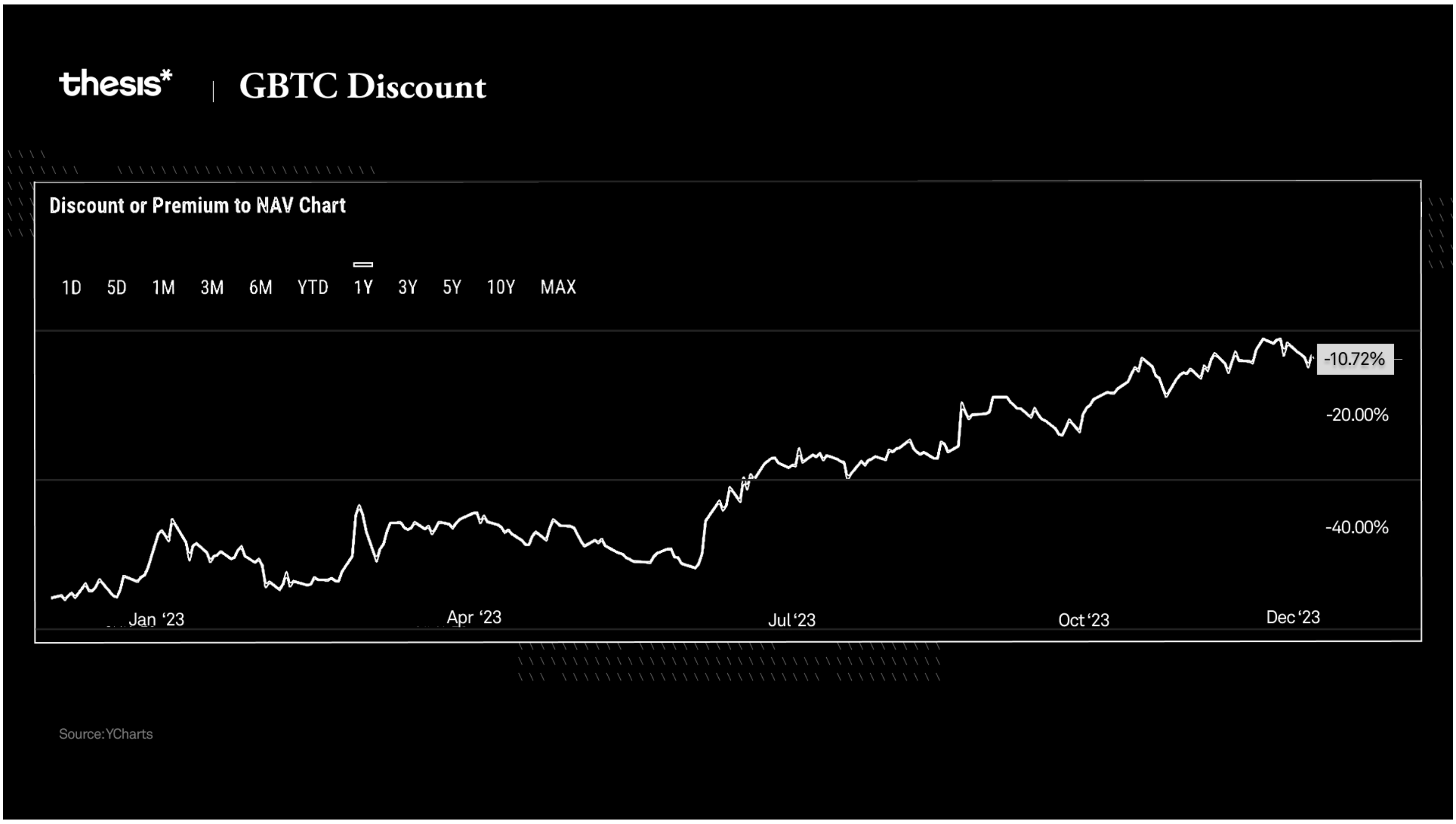
Doesn’t this go against the ethos of bitcoin? Why are we celebrating the institutions owning the people’s coin?

While that position is valid, it is important to understand the logical implications of a BTC ETF, and unanimous acceptance of BTC as an investible asset. BTC can serve multiple purposes with the launching of ETFs. Yes, an important value proposition of bitcoin is digital, borderless money. But another use case, potentially completely separated from the digital money aspect of BTC, is a store of value. Some people want to use bitcoin to improve their portfolio risk/return metrics or add higher beta exposure. ETF approval is not a failure of the original principles of bitcoin, but instead an enabler of a new narrative, a new use case. BTC is the millennial's gold, and ETFs will open the door for anyone in the US to access through their retirement and brokerage accounts.

Current demand for the ETF can be examined by financial products available in the equity markets. According to research from Galaxy, institutional funds currently hold 842k BTC (~$22B).[19] However the investment products today do not provide efficient exposure to BTC. Take, for example, BITO, the iShares Bitcoin Futures ETF, which has a significant performance drag compared to vanilla BTC. In addition to tracking error, the current state of BTC products have downsides such as high fees and lower liquidity. Despite these downsides, we still see interest and investment from institutions.

The same report from Galaxy shows an addressable market of $48.3T, based on current wealth management assets under management by broker-dealers, banks, and registered investment advisors (also excluding family offices with a market of $15T.)[20] Rather than pick through the exact details of that number, the bottom line is that the flows coming in when an ETF is approved will bring a flow of capital into BTC unlike anything before. YTD fund flows on BTC just recently eclipsed $1.5B, meaning it only takes .003% of the addressable market to double the yearly flows into BTC.[21]

A significant player in the ‘regulated BTC’ market is Grayscale’s bitcoin trust, GBTC, which has had a remarkable year, up 240% from $8. At the end of November, Grayscale filed for an amendment to their current GBTC to make the redemption and creation more efficient and collect management fees more frequently.[22]



Source: YCharts

Demand for this asset being front run by currently available traditional equity market instruments, like BITO, the iShares BTC futures ETF reaching an ATH in AUM at the end of November.22

Bitcoin's Ascendancy to a Store of Value

Given the scope of activity surrounding the establishment of a spot ETF fund, the perception of bitcoin has transformed from a speculative digital asset to a more recognized potential store of value. This is highlighted by BlackRock CEO Larry Fink, whose remarks surrounding rallies related to rumors of spot bitcoin ETF approvals signal a growing consensus that the digital asset sector presents a "flight to quality" for traditional financial houses amid times of geopolitical and economic uncertainty.23

This sentiment, adjacent to a surge in institutional appetite for bitcoin as a modern day equivalent to "digital gold" may be reflective of a shifting investment paradigm where digital assets are increasingly considered a part of a diversified investment portfolio. Indeed, Fink's advocacy of bitcoin as an alternative to gold to hedge against inflation is further bolstered by his assertion that bitcoin is mature enough to serve as a safe haven asset.24 25

Analysts at JP Morgan speculate that bitcoin could continue to track gold higher over the next year, up to $45,000, despite the speculative nature of the asset, which has pro traders and commodities analysts on the fence.[26]In turn, the banking crisis and regulator changes continue to reinforce bitcoin's position as a refuge outside of traditional finance, say JP Morgan analysts. Amid bailouts and times of economic stress, bitcoin's appeal can be considered somewhat equivalent to that of gold.[26]

However even as retail and crypto native investors adopt the narrative for bitcoin as a digital gold equivalent, institutional investors have taken a more cautious approach, with some choosing to reduce exposure to bitcoin as an asset class. So, although it is gaining traction, the institutional sphere has yet to fully accept the idea of bitcoin as a form of digital gold.

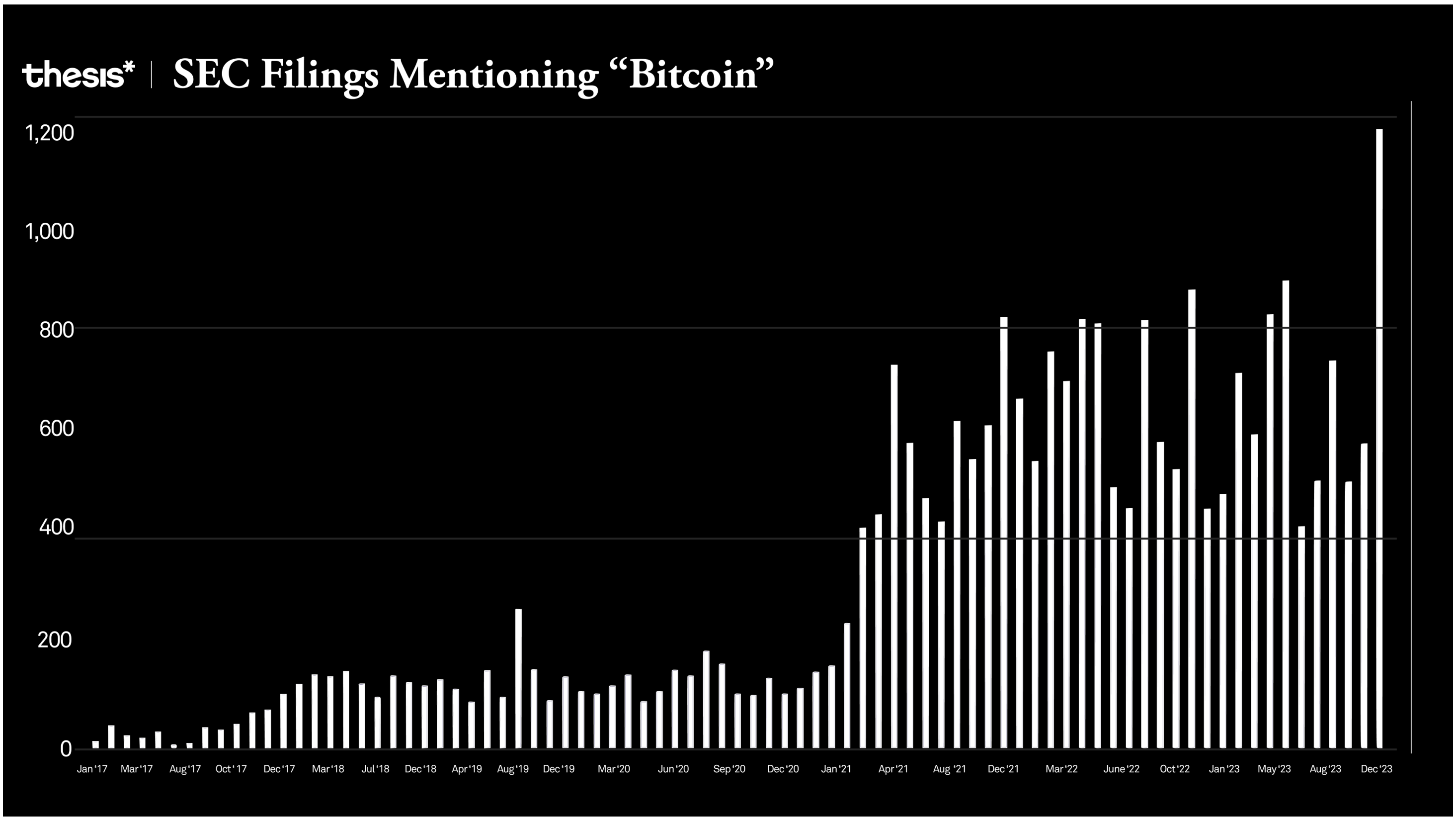
Market Impact and Regulatory Environment

Anticipation that a spot bitcoin ETF will receive approval remains high despite the SEC's historic caution, with over 30 applications rejected over concerns surrounding investor protection. Demand for a bitcoin ETF, which would open up a conduit for retail and institutional investors, remains high. A Glassnodes study suggests that anticipation of a spot bitcoin ETF approval contributed to the asset's 28% month-over-month increase in October, a recovery generally spread among crypto assets.[27]

Meanwhile, the month saw a tightening in the available trading supply of bitcoin, as long-term holders ascended to a new all-time high of 76%, indicating that over two-thirds of the circulating supply have not transacted in at least 5 months.[27]

Similar to establishing gold ETFs, a spot bitcoin ETF is expected to lead to a significant appreciation of bitcoin's price. However, it is of note that the market size for such instruments remains unknown.

The bullishness that BTC will not go away goes beyond the echo chamber of crypto Twitter. Data from the block suggest that November marked the month with the highest count of filings with the SEC that mentioned "bitcoin," well above any previous month.



Despite this sudden bullishness within the U.S., the global approach to Bitcoin regulation is far from uniform, with countries adopting divergent strategies that reflect a spectrum ranging from enthusiastic acceptance to outright prohibition.

Jurisdictions with Welcoming Approaches

El Salvador: Pioneering Bitcoin Integration

- In a groundbreaking move, El Salvador embraced Bitcoin as a legal tender in September 2021, marking a historic moment in the evolution of cryptocurrency.
- The government mandated businesses to accept Bitcoin as a form of payment, while citizens were provided with the Chivo wallet, a government-backed digital wallet, for conducting transactions.
- Notably, El Salvador granted a capital gains tax exemption on Bitcoin transactions, fostering an environment conducive to cryptocurrency adoption.[28]

United States: A Regulatory Landscape in Flux

- In the United States, regulatory developments are underway, with the Securities and Exchange Commission (SEC) considering Bitcoin as a commodity, while contemplating the possibility of regulating it as a security.

- The Commodity Futures Trading Commission (CFTC) oversees Bitcoin futures contracts, and the Financial Crimes Enforcement Network (FinCEN) applies anti-money laundering (AML) and know-your-customer (KYC) regulations to cryptocurrency transactions.29

European Union: Crafting a Unified Framework

- Within the European Union, the European Central Bank (ECB) recognizes Bitcoin as a currency and is actively exploring regulatory frameworks.
- The Markets in Crypto Assets (MiCA) regulation is currently in development, aiming to harmonize crypto regulations across EU member states.30

Jurisdictions with Strict Approaches:

China: A Forceful Prohibition

- China took a decisive stance in 2021 by banning financial institutions from dealing in Bitcoin.
- The ban extended to prohibit banks and financial institutions from offering cryptocurrency services, accompanied by a crackdown on cryptocurrency mining operations.31

India: Navigating Regulatory Uncertainty

- India has witnessed regulatory uncertainty, with the Reserve Bank of India (RBI) expressing concerns about cryptocurrencies and imposing a ban on banks dealing with them.
- The government is currently deliberating on a cryptocurrency bill, which may lead to a ban or establish a regulatory framework.32

Russia: A Mixed Regulatory Landscape

- Russia has adopted a mixed approach, recognizing cryptocurrencies as non-legal tender but allowing ownership and trading.
- Both mining and trading activities are subject to registration with authorities, and the country remains open to potential future regulatory measures.33

The divergence in regulatory approaches to Bitcoin across various nations and jurisdictions underscores the inherent complexities and challenges associated with the general global adoption of the asset and decentralized cryptocurrencies.

The lack of a unified, standardized regulatory framework fosters uncertainty for users and businesses operating in the cryptocurrency space and hampers the potential for a cohesive and integrated global financial system.

This disparate treatment of Bitcoin can lead to regulatory arbitrage, wherein users and businesses might seek out jurisdictions with more favorable regulations, potentially undermining the intent of regulations put in place by other nations. Moreover, the absence of a common approach increases the difficulty of international cooperation and coordination in addressing fraud, money laundering, and market manipulation. That is not to say that the result will be a cohesive and ubiquitous treatment of digital currencies, but the closer the world's regulatory bodies can get to be on the same page, the more welcoming of an environment for innovation while still protecting the public from abuse in the markets.

Conclusion

As a spot bitcoin ETF is widely anticipated, 2023 marks a seminal moment in bitcoin's integration into U.S. financial markets, challenging pre-existing norms and opening new avenues for institutional investment. Once set up, a spot bitcoin ETF is expected to signal a paradigm shift as a step towards acknowledging bitcoin as a mainstream global asset.

The SEC, which has typically held a hard stance on such matters, is softening its views, potentially paving the way for broader acceptance of bitcoin, particularly among now sidelined traditional financial market players.

Involvement by major players such as BlackRock and Grayscale filing for spot bitcoin ETFs underscores the asset's capacity to move out of a niche digital currency to a reputable investment class, a perception echoed by industry leaders and analysts who increasingly see bitcoin as a viable alternative to traditional assets.

BitVM: Computing Anything on Bitcoin

Many of this paper's points have extensively covered the technological developments surrounding the Bitcoin blockchain. Scalability solutions, new forms of assets, and metadata stored in bitcoin transactions are all changing how the Bitcoin network works. Many users likely did not expect these developments to occur at such a breakneck pace and create the impact they have in such a short amount of time. While some will continue to argue that these innovations are disruptive to the core principles of Bitcoin, the debate is, as usual, nuanced and all angles should be carefully considered.

Another critical development in this area is the BitVM, proposed by Robin Linus, a Bitcoin developer responsible for various projects, such as ZeroSync. BitVM proposes a new way to process smart contracts on Bitcoin, improving functionality and providing a way for more complex transactions. This architecture behaves similarly to a rollup on the Ethereum network, where transaction computation is completed off-chain and only confirmations are done on the base layer. While off-chain computation is necessary to have this level of functionality on Bitcoin, some argue that the transaction load on the base layer will still be significant.[34]

An important distinction of BitVM is that it requires no soft fork of the Bitcoin network, meaning it can be utilized today. Versus something like the Taproot protocol, which took years of testing and development to ensure its safety and functionality, BitVM can be tested immediately, which will likely help lead to a faster adoption cycle.

Anonymous developer Super Testnet believes the project is “the most exciting discovery in the history of Bitcoin script.” While it may sound like a hyperbole, BitVM's impact should not be discounted.[35]

The important function to understand with BitVM is its prover-verifier structure, which behaves similarly to an optimistic rollup on the Ethereum network. Off-chain, some parties can do the computations for a given transaction and post the proof of those transactions on Bitcoin. Another party denoted the “verifier”, checks the transaction for validity. The prover can be penalized for making a false claim if there is any dispute.

For example, take the above structure of wrapped bitcoin assets, such as wBTC or tBTC.

The application of BitVM can help minimize trust in creating a wrapper asset. Everyone in the group knows the central party creating the wrapped bitcoin asset cannot lie when proving a transaction, or the verifier can earn the bond posted by the prover. A protocol that helps minimize trust in the Bitcoin ecosystem should objectively be viewed as a massive win.

The main innovation that BitVM and Robert Linus have discovered to achieve this type of trust minimization is the trustless transfer the state from one Bitcoin transaction to another via bit value commitments. Because of the incentive to not lose their deposit by getting slashed, a BitVM prover performs every computation step within a given set of rules to prove the state change.

This same concept of minimized trust in the wrapped bitcoin custodians can be extended into different applications, such as improving a two-way bridge's security. To paint it with a broad brush, BitVM can enable complex applications such as exchanges, derivatives, prediction markets, games, and more. Any sort of substantial development is still plenty of time away. And the big innovation needed to cement the positive impact of BitVM is a 1:N, multi-party scheme, versus what BitVM currently is, a 1:1, two-party scheme. This would make it so anyone could become a verifier in the prover-verifier construct.

Expectedly, the takes on BitVM are not all positive. Dan Robinson of Paradigm says the excitement is overblown and should not be getting the attention it deserves.[36] The main critique is the two-party scheme, and both parties must be able to inherit significant computation off-chain.

Eric Wall said it well: the fact that this type of transaction computation can even be possible on Bitcoin is nothing short of amazing.[37] It proves yet again that Bitcoin has many paths yet to be explored. BitVM can be experimented with today, again, requiring no adjustments to the network. The practicality of BitVM is currently a big question mark, but thanks to the fact that it can be developed on and tested today, it won’t be long until we start to see some examples of applications using the script.

Conclusion and Look Ahead to 2024: What's in Store for the Future of Bitcoin?

Bitcoin's continued growth has seen a continued trend of increased participation from both retail and institutional investors, driven by its scarcity and codified monetary policy. Such factors have significantly boosted Bitcoin's legitimacy as an investment asset.

Technological advancements in scaling solutions have greatly enhanced the transaction capabilities of Bitcoin, enabling fast, scalable transactions, and encouraging broader utility in everyday transactions and even in gaming platforms.

Likewise, the introduction of Ordinals has altered the nature of Bitcoin transactions by turning individual satoshis into unique digital assets via the inscription process, and sparking significant market interest. Recursive ordinals further enhance Bitcoin's functionality by enabling complex on-chain software operations.

Other technical Innovations, like Babylon's remote staking concept, are creating new avenues for earning yield on BTC in a safe and ethos-aligned manner, facilitating its viability as both an asset and a store of value.

There remains a notable shift towards self-custody, observable via investors increasingly taking direct control over their Bitcoin holdings, and thereby enhancing the asset's supply dynamics and asymmetric upside. The shift towards self-custody is significant as it reflects a maturation of the investor mindset in the Bitcoin ecosystem. By taking direct control of their assets, investors not only enhance their security and autonomy but also contribute to a change in the market dynamics of Bitcoin, potentially influencing its value and stability.

Growth in consumer applications like Fold, Lolli, and Bitrefill has also played a significant role in taking fundamental steps towards embedding Bitcoin into daily life, broadening its appeal and usage among a wider audience.

For the same consumers, privacy-focused wallets like Wasabi and Samourai Wallet continue to enhance Bitcoin's privacy features, catering to users who prioritize data protection and anonymity.

With these advancements, Bitcoin still faces obstacles surrounding scalability, network congestion, regulatory complexities, and inherent market volatility, all of which pose hurdles for the continuous integration of Bitcoin into mainstream finance and other sectors.

Although challenges persist, the foundational strength and the diverse applications of Bitcoin suggest a promising trajectory for its continued evolution and integration into various facets of global economics and finance.

Citations

1www.coindesk.com/markets/2023/10/26/bitcoin-primed-for-supply-shock-as-exchange-balance-drops-to-5-year-low-analyst-says/#:~:text=The%20level%20of%20available%20bitcoin.

2https://2784460.fs1.hubspotusercontent-na1.net/hubfs/2784460/Content%20Report/Rootstock%20Bitcoin%20Mining%20Report%20Oct%202023.pdf

3coincodex.com/article/26289/iovlabs-announces-key-developments-for-rif-and-rootstock-at-consensus-2023/

4https://defillama.com/chain/RSK?devsCommits=false&developers=false&stables=false&tvl=true

5https://coinmarketcap.com/currencies/stacks/

6https://defillama.com/chain/RSK?devsCommits=false&developers=true&stables=false&tvl=true

7https://stacksfoundation.notion.site/Q3-23-Foundation-OKRS-Published-1c6b4d37ec3a4e48bf282691189bdd8c

8https://cointelegraph.com/news/bitcoin-core-developer-antoine-riard-steps-back-lightning-network-dilemma

9https://zapalytics.com/

10https://dune.com/domo/ordinals-marketplaces

11https://bitcoinops.org/en/podcast/2023/02/16/

12http://brc-20.io/

13https://lightning.engineering/posts/2023-10-18-taproot-assets-v0.3/

14https://argoblockchain.com/articles/bitcoin-taproot-upgrade-explained

15https://docs.lightning.engineering/the-lightning-network/taproot-assets/taproot-assets-protocol#asset-proof

16https://ycharts.com/indicators/bitcoin_average_transaction_fee

17https://bitcoinops.org/en/podcast/2023/09/14/

18https://twitter.com/btcpricetool/status/1730646181376823430

19https://www.galaxy.com/insights/research/sizing-the-market-for-a-bitcoin-etf/

20https://www.galaxy.com/insights/research/sizing-the-market-for-a-bitcoin-etf/

21https://jbutterfill.medium.com/volume-159-digital-asset-fund-flows-weekly-report-0103828f4a3d

22https://www.sec.gov/Archives/edgar/data/1588489/000095017023066760/gbtc_pre_14a_v2.htm

22https://ycharts.com/companies/BITO/assets_under_management

23https://www.coindesk.com/business/2023/10/17/blackrock-ceo-larry-fink-seeing-client-demand-for-crypto-around-the-world/

24https://bitcoinmagazine.com/business/blackrock-ceo-larry-fink-says-bitcoin-is-an-international-asset#

25https://dailyhodl.com/2023/10/18/blackrock-ceo-larry-fink-says-bitcoin-and-crypto-will-play-a-role-in-investors-flight-to-quality/

26https://www.dlnews.com/articles/markets/bitcoin-as-digital-gold-narrative-returns-for-crypto-natives/

26https://studio.glassnode.com/workbench/da038c46-94e7-45e4-63e3-4ecfa5d1b7e9?&utm_source=gn_insights&utm_medium=insights_woc&utm_campaign=woc_16_2023

27https://insights.glassnode.com/finance-bridge-spot-btc-etf-impact/

27https://studio.glassnode.com/workbench/fc950f4d-fa78-479d-5030-8873c6e6bd5c

28https://www.ft.com/content/7b5b1cc4-50bb-437f-aa16-f106d2dbc1c7

29https://www.forbes.com/advisor/investing/cryptocurrency/sec-crypto-regulation/

30https://www.ft.com/content/50388307-08a8-4330-be8e-ff17f41e8e13

31https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/

32https://rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1196

33https://cryptoslate.com/russia-to-legalize-crypto-as-means-of-payment/

34https://twitter.com/roasbeef/status/1711455467569020969

35https://twitter.com/super_testnet/status/1711410131701756023

36https://twitter.com/danrobinson/status/1711531283212562877

37https://twitter.com/ercwl/status/1712052792779505925