SURGE

Bitcoin Scalability

The Persistent Challenges of the Premier Cryptocurrency

July 2024

Table of Contents

Key Takeaways

Purpose Of The Report

This report addresses the critical scalability challenges faced by Bitcoin, aiming to provide a comprehensive understanding of its limitations and the need for innovative solutions to enhance its usability and adoption.

Outcome For The Reader

Readers will gain insight into the root causes of Bitcoin's scalability issues, their consequences, and the current efforts being made to overcome these obstacles. This report equips readers with a deeper understanding of Bitcoin's current state and future potential.

Summary of Points Covered

- **Scalability Conundrum:** Bitcoin's transaction processing capability is limited by its block size and block generation interval, leading to congestion and high transaction fees.
- **Network Congestion:** High demand for Bitcoin transactions results in slow processing times and increased fees, highlighting the need for scalability improvements.
- **Bitcoin Block Space:** The majority of Bitcoin blocks are nearly full, causing higher transaction costs and longer confirmation times compared to other blockchains.
- **Environmental Impact:** Bitcoin's substantial energy consumption and carbon footprint are significant concerns, driven by its increasing hash rate and reliance on non-renewable energy sources.
- **Mining Dynamics:** The diminishing block rewards pose a challenge for miners' profitability, raising questions about the future of Bitcoin's security and innovation.
- **Micropayment Limitations:** High transaction fees and long confirmation times make Bitcoin impractical for small transactions.
- **Smart Contract Constraints:** Bitcoin's limited programmability restricts its ability to support complex smart contracts and decentralized applications.
- **Dormant Bitcoin:** A significant portion of Bitcoin remains inactive due to limited utility compared to other utility tokens like Ethereum and Solana.
- **Innovations on the Horizon:** Layer-2 solutions, such as the Lightning Network, and advanced technologies like rollups offer promising paths to address Bitcoin's scalability and usability challenges, paving the way for its evolution.

The Bitcoin Paradox

Since the dawn of civilization, money has evolved to meet the changing needs of societies. From barter systems and precious metals to paper currency and digital transactions, the concept of money has continuously adapted to facilitate trade and economic growth. Each transformation has aimed to improve the efficiency, security, and accessibility of financial exchanges.

In this ongoing evolution, Bitcoin emerged in 2009 as a revolutionary form of digital currency, promising decentralization, transparency, and a new era of financial freedom. However, as Bitcoin gains prominence, it also faces significant challenges that threaten its potential to become a mainstream medium of exchange.

Bitcoin has promised a decentralized, transparent, and secure financial system, but it faces significant challenges that hinder its potential as a mainstream medium of exchange.

This report aims to provide a comprehensive examination of Bitcoin's scalability issues, focusing on its limited transaction processing capability, environmental impact, mining dynamics, and limitations in facilitating micropayments and supporting complex smart contracts. By delving into these root causes and consequences, we highlight the critical need for solutions to enhance Bitcoin's usability and adoption.

The Scalability Conundrum

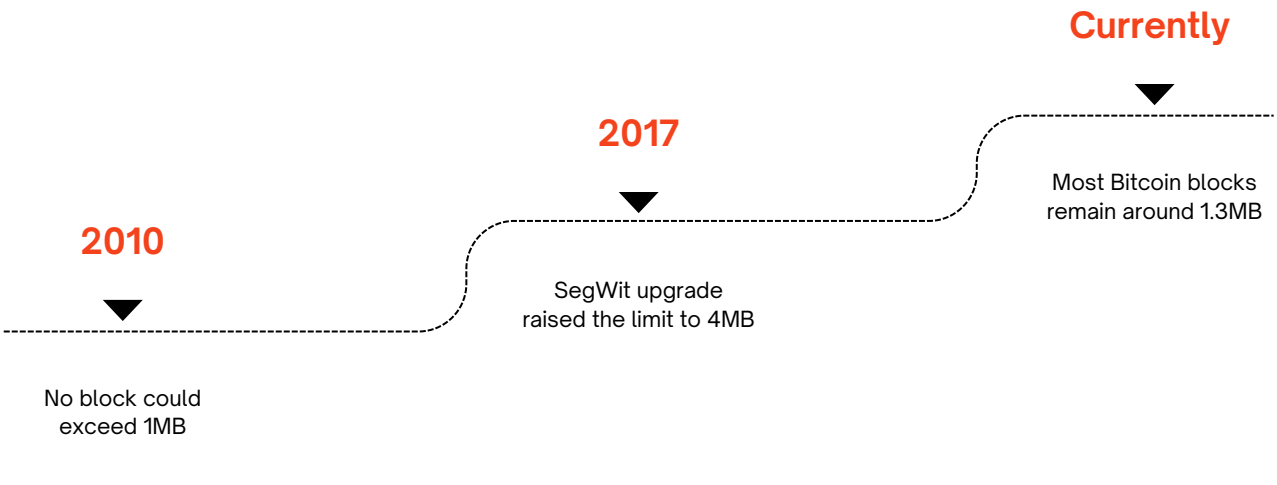
The Bitcoin Scaling Problem pertains to the challenge of increasing the Bitcoin network's transaction capacity effectively - so people start using it as money and efficiently - without incurring high transaction fees and wait times.

As Bitcoin usage grows, the existing block size limit of 1 megabyte becomes a bottleneck, resulting in slower transaction confirmations and higher fees. This issue arises from Bitcoin's decentralized structure, where each transaction must be recorded on every participant's computer, known as a full node.

The limited transaction processing capability of Bitcoin's blockchain, which ranges between 7 to 10 transactions per second, is due to the fixed interval of 10 minutes for block creation and the restricted number of transactions each block can handle.

The interval between block generations, set at 10 minutes, was established at Bitcoin's inception and is expected to remain unchanged. However, the maximum block size has been modified over time.

In 2010, Satoshi Nakamoto instituted a rule capping block sizes at 1MB. This limit was adjusted in 2017 with the SegWit upgrade, which introduced the concept of block weight, with a maximum of 4 million weight units (WU). This allows for a theoretical maximum block size of up to 4MB.



These constraints are in place to control the growth rate of the blockchain's size, which is why they are unlikely to be altered in the future.

One of the major consequences of these scalability constraints is network congestion.

Network Congestion

When demand is high, the base layer of Bitcoin's network can become congested, leading to slower transaction processing and higher fees.

Bitcoin's design prioritizes security and decentralization, often at the expense of scalability. This balance highlights the blockchain trilemma, where achieving decentralization, security, and scalability simultaneously is challenging. While Bitcoin's structure enhances its value, it makes the network less suitable for developing financial applications, unlike Ethereum.

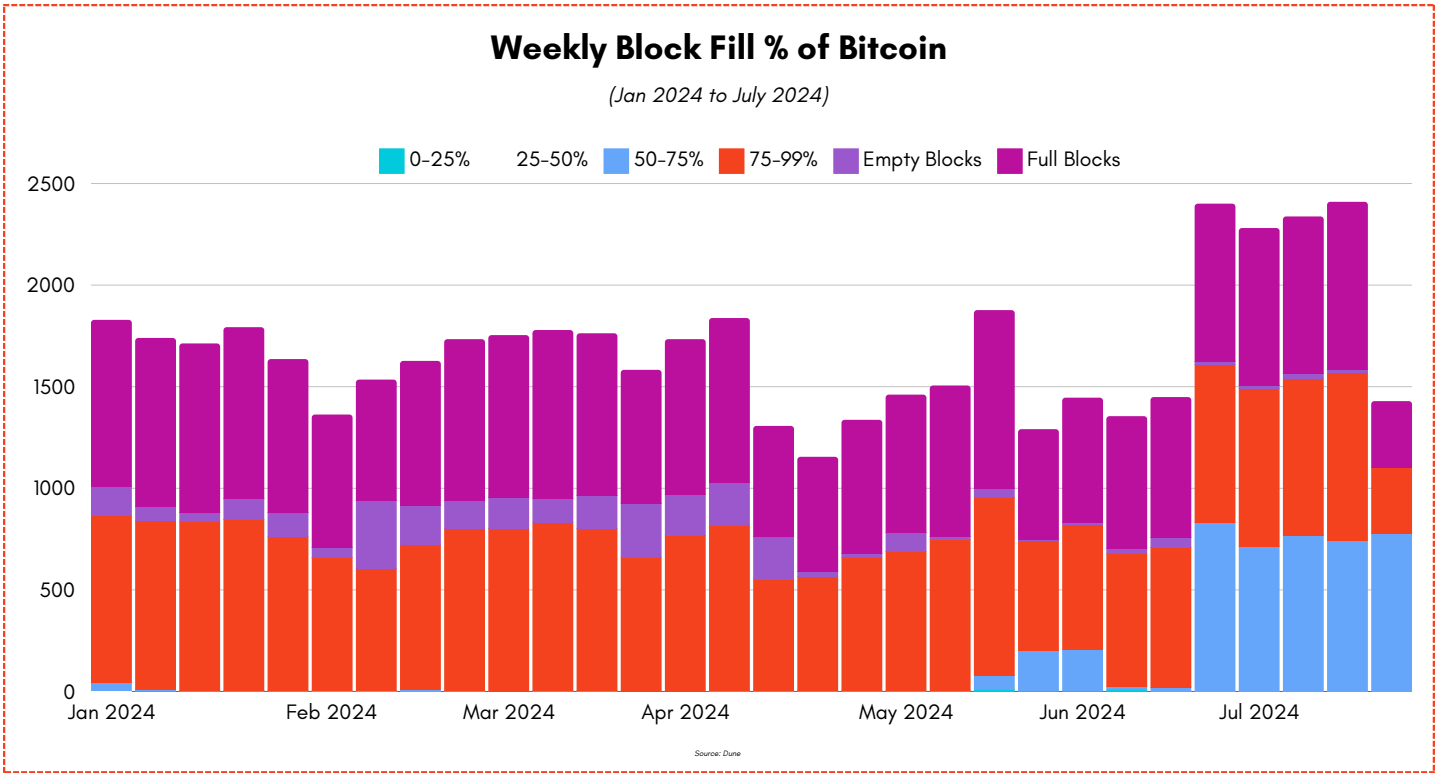
The Bitcoin community has contended with scalability issues for nearly a decade, with transaction fees soaring to tens of dollars during peak times. Currently, the demand for Bitcoin's block space is at an all-time high, spurred by innovations like Ordinals, Runes, and BRC-20s. As stated by Bankless,

1. Ordinals caused **Bitcoin fees to rise by up to 280%** year-to-date in December 2023.
2. Runes transactions comprise **68% of Bitcoin's total transactions** since its inception.

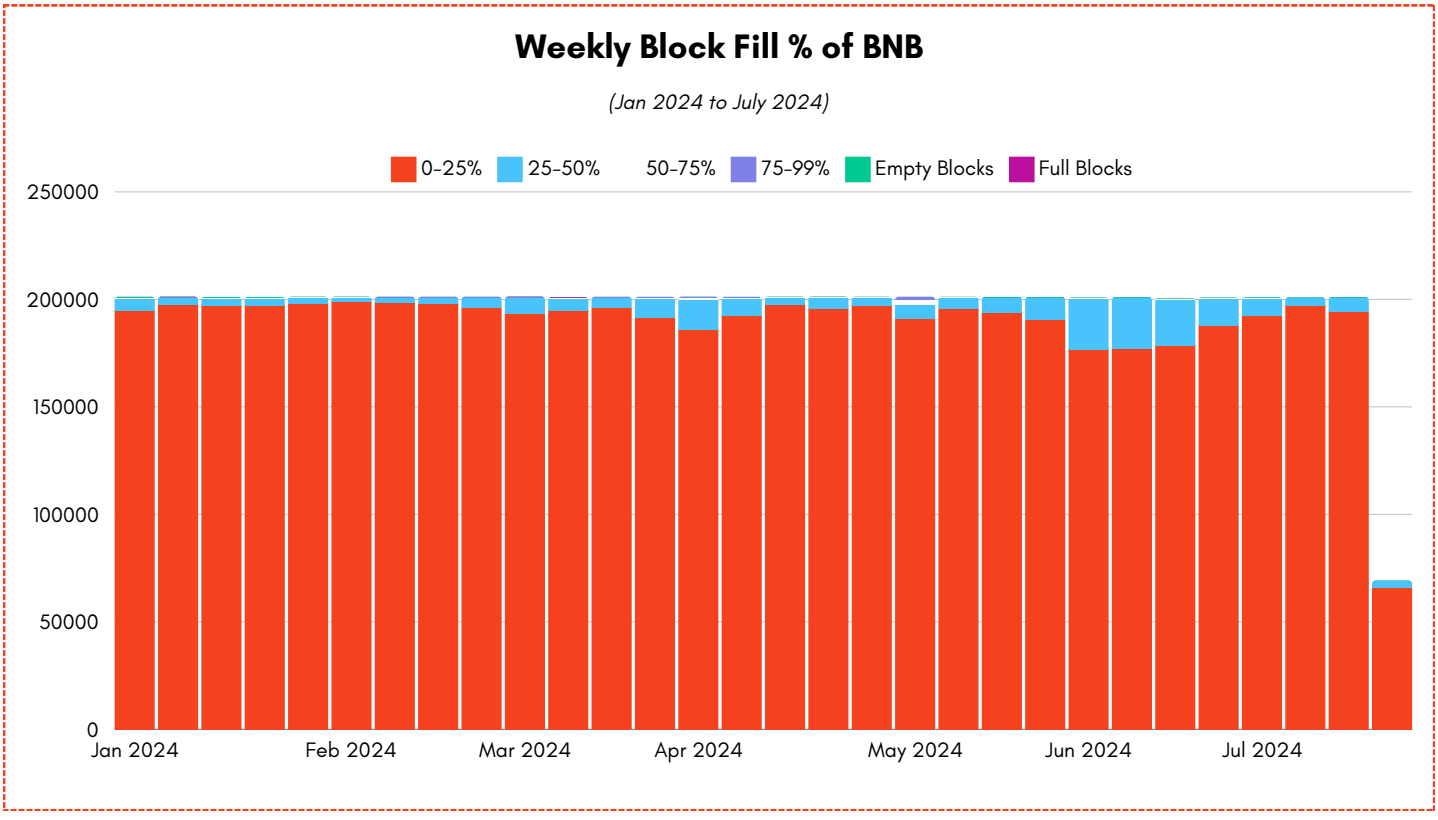
BRC-20s have intermittently caused spikes in Bitcoin transaction fees over the past year, at one point accounting for 74% of the block reward.

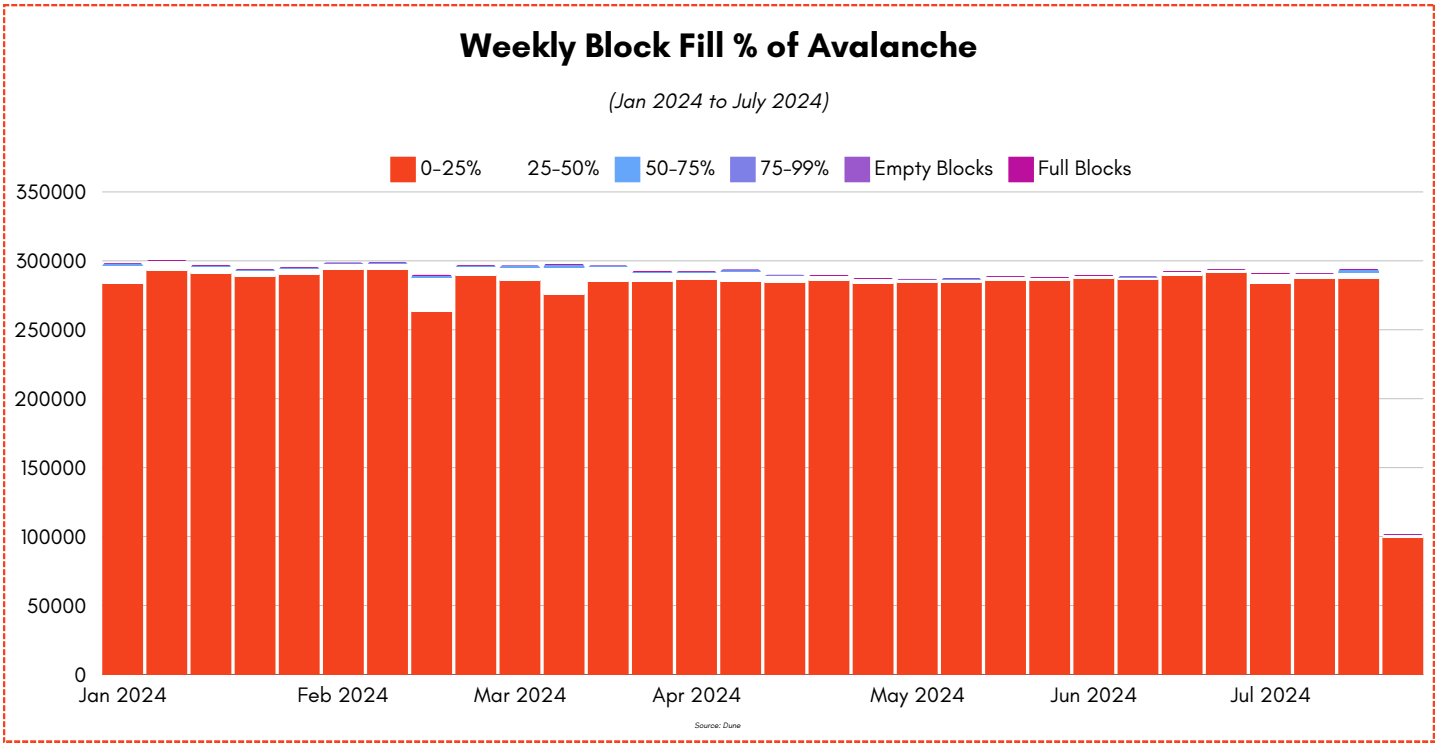
To better understand the impact of network congestion, we need to examine Bitcoin's block space utilization.

Bitcoin Block Space



Analyzing the weekly block space utilization data reveals that approximately 75-80% of the total blocks are filled to more than 3/4ths of their maximum capacity (2MB in this analysis). This indicates that the majority of blocks on the Bitcoin blockchain are nearly full, containing close to the maximum amount of data.



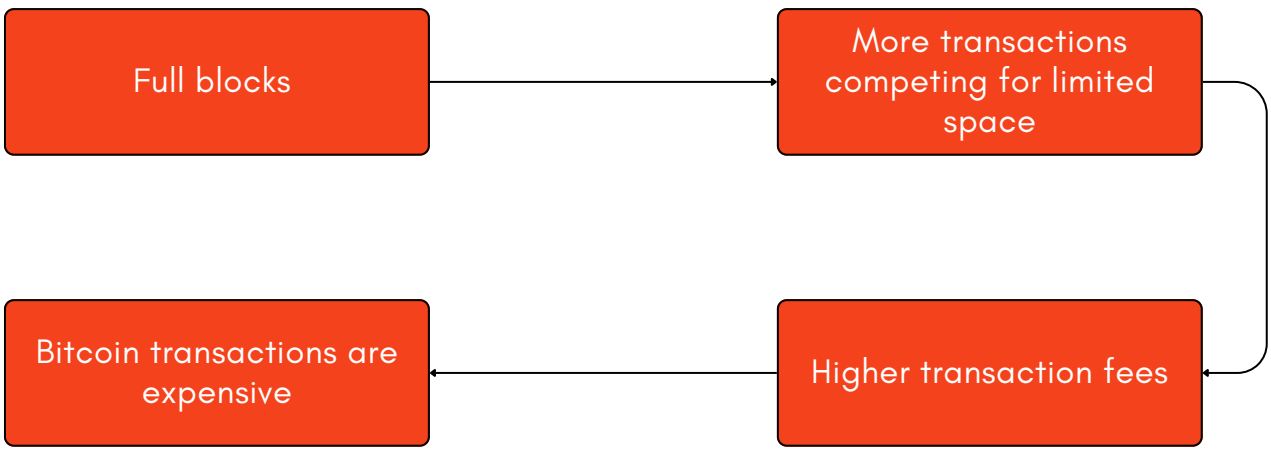


Compared with other fast and low-fee blockchains like BNB and Avalanche, we can observe that 95-99% of the blocks are filled to only less than a fraction of their maximum capacity resulting in empty blocks.

Impact Of Full Blocks

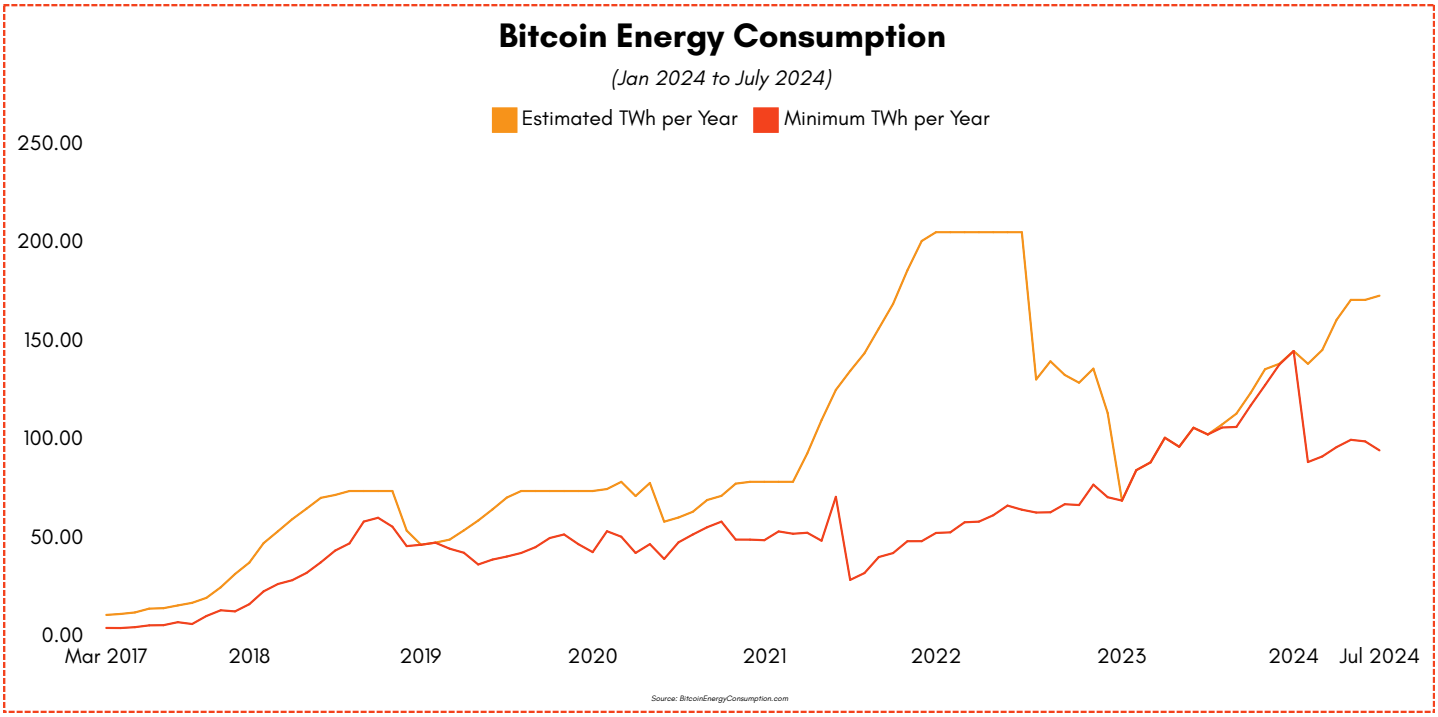
Higher Transaction Fees

As mentioned in this report, Ordinals caused Bitcoin fees to rise by up to 280% year-to-date in December 2023. We can observe the same in the graph below as the average transaction fee crossed $23:



Digital Gold's Carbon Footprint

The Environmental Paradox



Digiconomist reports that Bitcoin uses 550,000 times as much electricity per transaction as Visa.

A study published by the United Nations University and the journal Earth's Future found that during 2020-2021, the global Bitcoin mining network consumed 173.42 terawatt hours of electricity. If Bitcoin were considered a country, its energy consumption would rank 27th worldwide, surpassing that of Pakistan, which has a population exceeding 230 million.

This significant energy usage results in substantial greenhouse gas emissions.

The study revealed that Bitcoin mining activities generated 85.89 million metric tons of carbon dioxide equivalent (MTCO2E) from 2020 to 2021. This emission level is comparable to the carbon produced by consuming 9,665 gallons of gasoline or burning 96,210 pounds of coal annually, as per the U.S. Environmental Protection Agency's Greenhouse Gas Equivalencies Calculator.

The carbon footprint associated with Bitcoin mining was similar to burning 84 billion pounds of coal or operating 190 natural gas-fired power plants. To counterbalance this footprint, planting 3.9 billion trees would be necessary, covering an area almost as large as the Netherlands, Switzerland, or Denmark, or about 7% of the Amazon rainforest.

During this time, Bitcoin's water footprint equated to the volume required to fill over 660,000 Olympic-sized swimming pools, sufficient to meet the current domestic water needs of more than 300 million people in rural sub-Saharan Africa.

Bitcoin's energy consumption predominantly relies on non-renewable sources.

Researchers estimated that in 2022, 62% of the electricity used for Bitcoin mining globally was derived from fossil fuels, with coal power being the largest single contributor, based on data from the Cambridge Bitcoin Electricity Consumption Index (CBECI).

The e-waste generated by Bitcoin mining alone could surpass current global estimates.

Bitcoin's Defense

Despite Bitcoin's substantial electricity consumption, this cost is fundamental to its decentralization and security. The requirement for significant computational power and electricity helps prevent centralized control and ensures network integrity. Additionally, Bitcoin mining operations are increasingly adopting renewable energy sources to mitigate environmental impact.

Moreover, layer-2 scaling solutions promise to reduce Bitcoin's electricity consumption. By enabling off-chain transactions, these solutions can handle a higher volume of transactions with minimal on-chain interaction, thereby lowering the overall energy demand. This approach not only improves transaction speed and reduces costs but also enhances the sustainability of the Bitcoin network by decreasing its reliance on energy-intensive mining processes.

While traditional payment networks have significant costs associated with intermediation, such as extensive corporate structures and substantial resource expenditures, cryptocurrencies introduce different costs.

Accroding to Cato Institute, Mastercard, which handled 23% of the U.S. credit card market and 30% of the debit card market in 2016, employs over 13,000 people globally, incurring annual operating expenses of $5.4 billion in 2017. Visa, a larger competitor, had operating costs amounting to $6.2 billion.

Electricity prices vary globally, influencing miners to operate in countries where electricity is cheaper. For example, in China, which hosts approximately 80% of Bitcoin mining capacity, electricity costs 8.6 U.S. cents per kilowatt-hour, about half the average price in the U.S. Assuming an average electricity cost of 10 cents per kWh, the Bitcoin network's annual electricity consumption would amount to $7.3 billion, given current mining activities. This results in total annual operating costs for Bitcoin of approximately $10 to 12 billion.

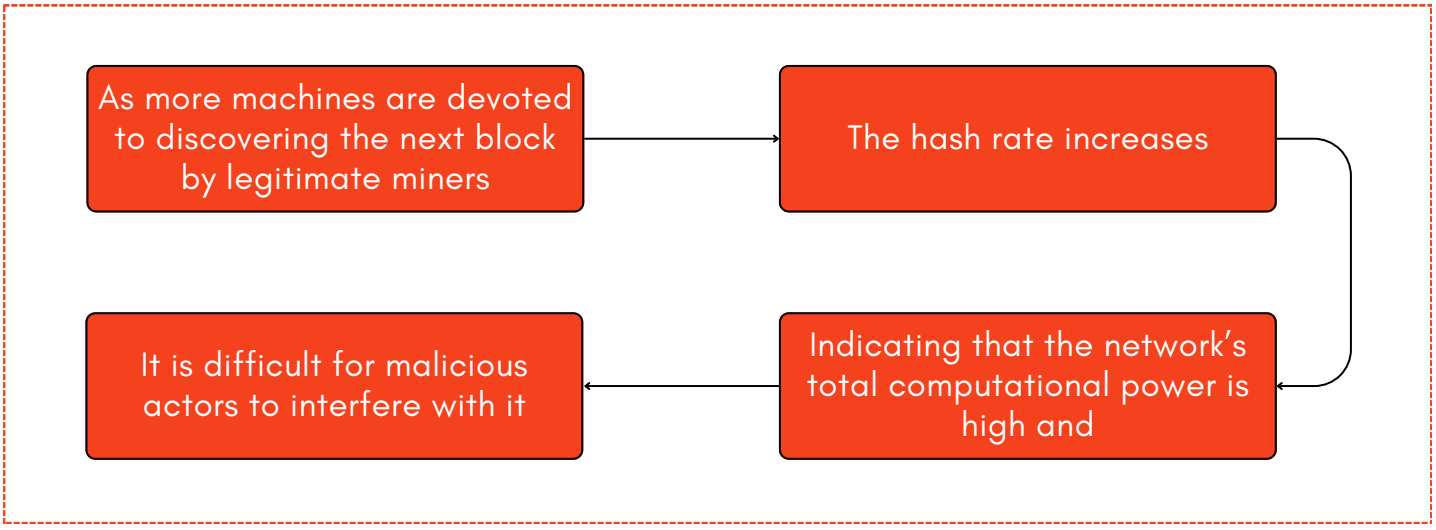
Bitcoin's Hash Rate

The hash rate of Bitcoin represents the total processing and computing power dedicated to the network through mining. This process, known as "hashing" a block, is essential for verifying the integrity of network transactions, and participants in this process are rewarded with Bitcoin.

Why is Hash Rate Important?

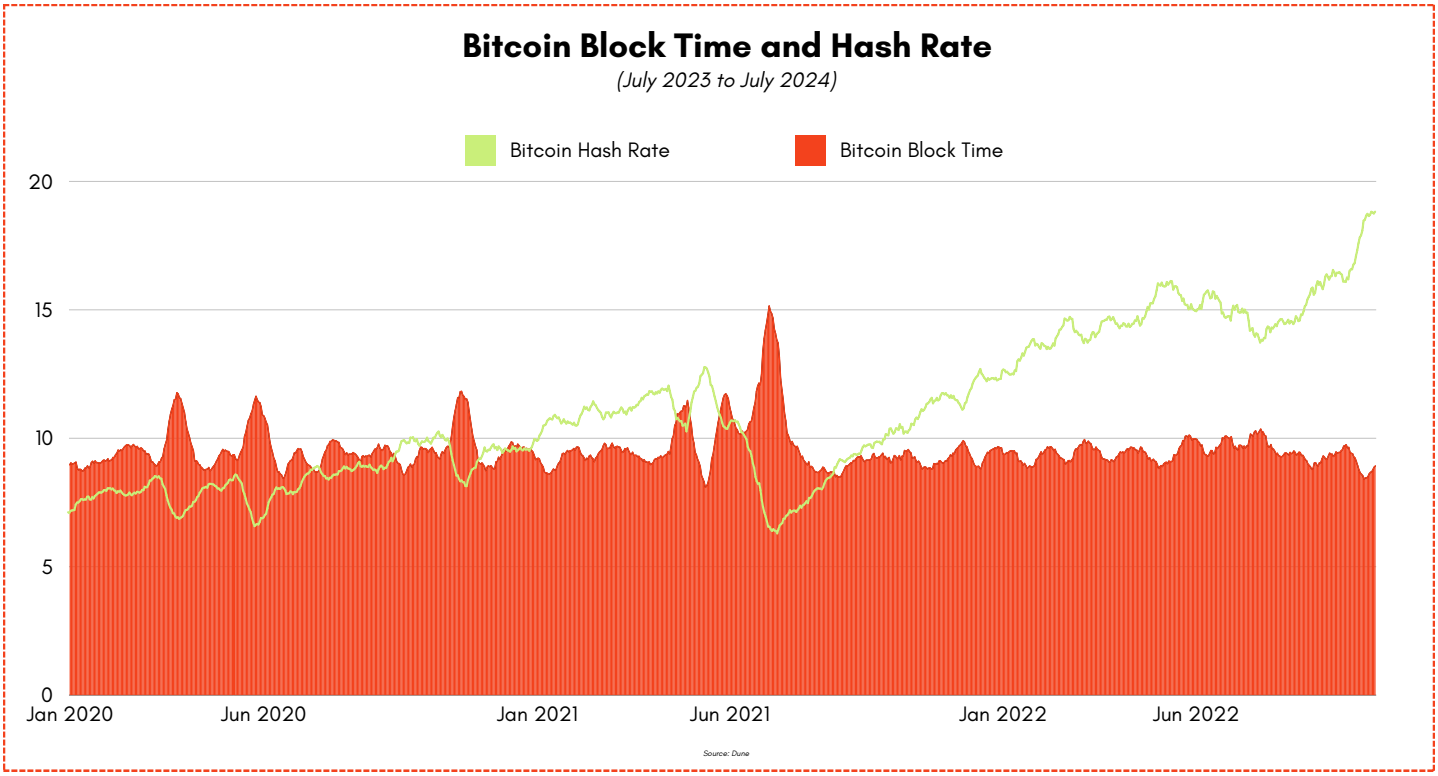
The hash rate is a crucial indicator of a blockchain network's resilience, particularly its security.

What then occurs if Bitcoin's hash rate increases?



The Environmental Concern Of Increasing Hashrate

Bitcoin's hash rate has been on an upward trend since its inception and will continue to rise. It has reached all-time high levels, indicating that the computational power required for mining Bitcoin is greater than ever before.



The increasing hash rate of Bitcoin is environmentally concerning for several reasons:

1. **Higher Energy Consumption:**
A higher hash rate indicates more computational power is being used to mine Bitcoin. This translates to increased energy consumption as miners deploy more and more powerful hardware to stay competitive. The energy requirements of Bitcoin mining are substantial and growing, leading to greater overall energy usage.

2. **Carbon Footprint:**
Much of the energy used in Bitcoin mining comes from fossil fuels, which contribute to carbon emissions and global warming. The higher the hash rate, the more energy is consumed, and if this energy is derived from non-renewable sources, the environmental impact is significant.

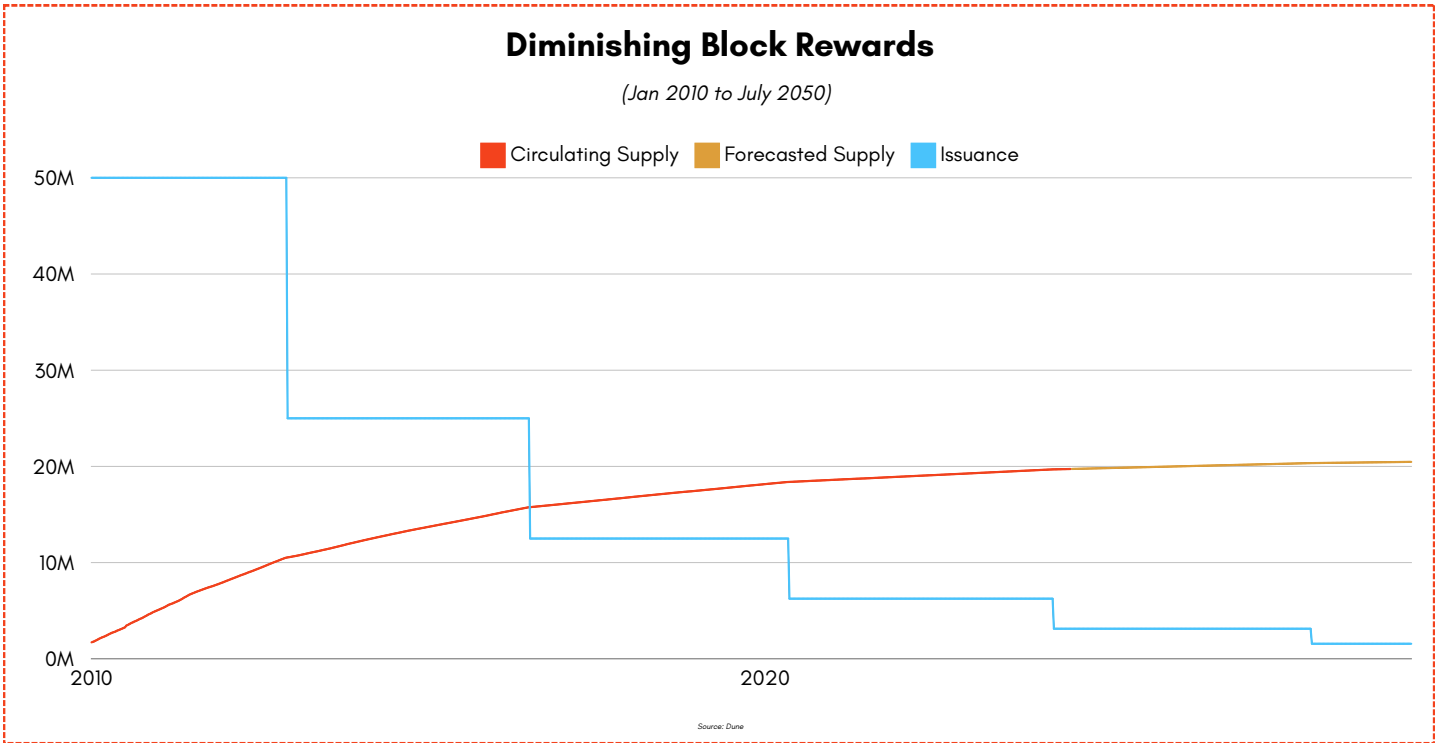
Mining For Profits

When The Gold Rush Slows Down

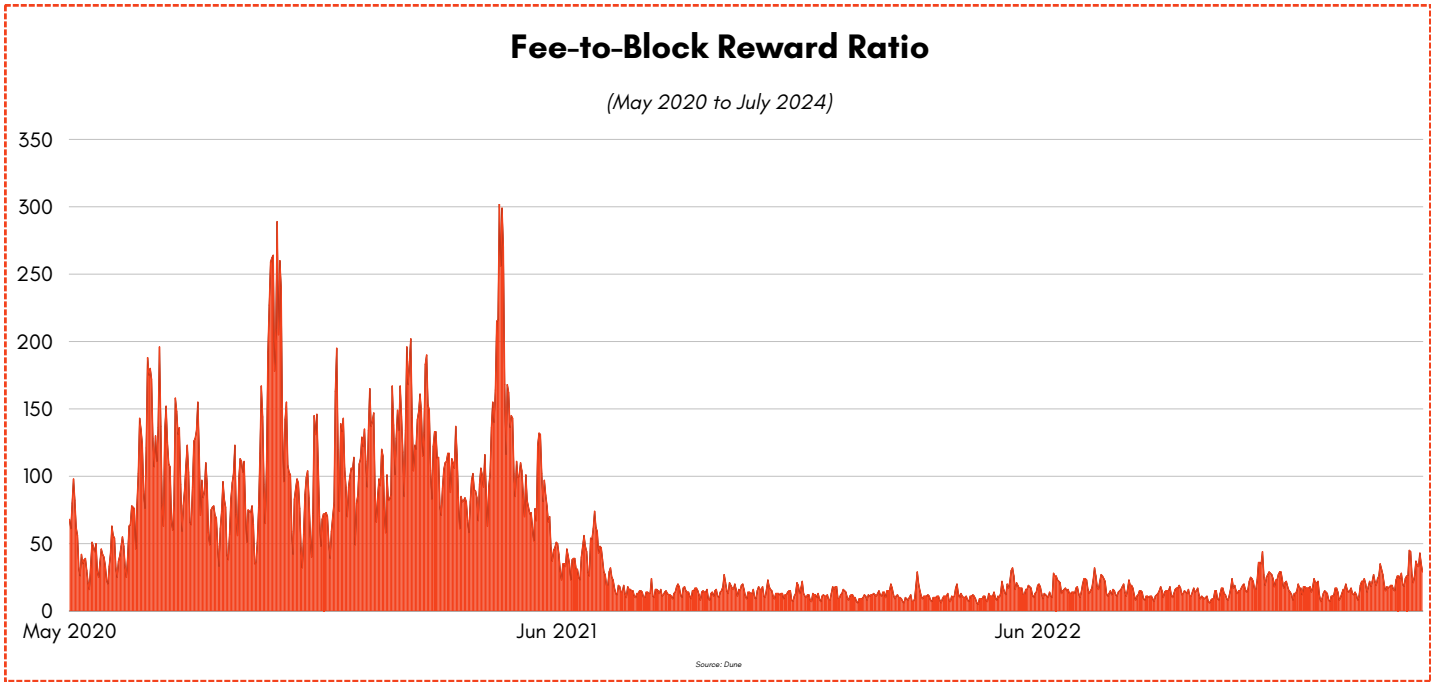
What Is The Bitcoin Block Reward?

A Block Reward consists of a predetermined amount of newly minted Bitcoin along with the total transaction fees from a mining node's candidate block. The first mining node to successfully validate and add its block to the blockchain receives this reward, a process that occurs approximately every 10 minutes.

As of now, the Bitcoin block reward includes 3.125 newly generated coins per block. This quantity is regulated by a halving event that happens roughly every four years. The halving event reduces the number of newly generated Bitcoins by half, aiming to restrict the issuance of new Bitcoins until the total supply reaches 21 million.



As clearly shown in this graph, the block rewards will continue to diminish until all Bitcoin is mined, at which point the rewards will be zero.



Currently, block rewards amount to a total of 95-98% of the total miner's revenue on average once the total global supply has reached approximately 21 Million, the show is over for miners earning Bitcoin from a block reward.

Despite this, Bitcoin transactions will continue to be collected, blocks will be processed on the blockchain, and miners will be compensated through the market value of transaction fees. But will these transaction fees be enough to sustain the miners and the security of the network? And as the digital gold rush slows down, what will be the fate of innovation on Bitcoin?

Multiple teams are innovating and building to prevent this potential stagnation, aiming to bring more usage to Bitcoin by scaling it via rollups, state channels, and side-chains. These advancements could pave the way for a vibrant Bitcoin-driven economy, ensuring the network's relevance and utility beyond the era of block rewards.

Small Change, Big Issues

The Micropayment Dilemma

Bitcoin was originally introduced as a peer-to-peer decentralized digital currency which could be used for payments between two parties without the need for governmental and centralized institutions but today, it is majorly used as a store of value sitting idly in cold storages and wallets.

Bitcoin in its current form isn't suitable for micropayments for several key reasons:

High Transaction Fees

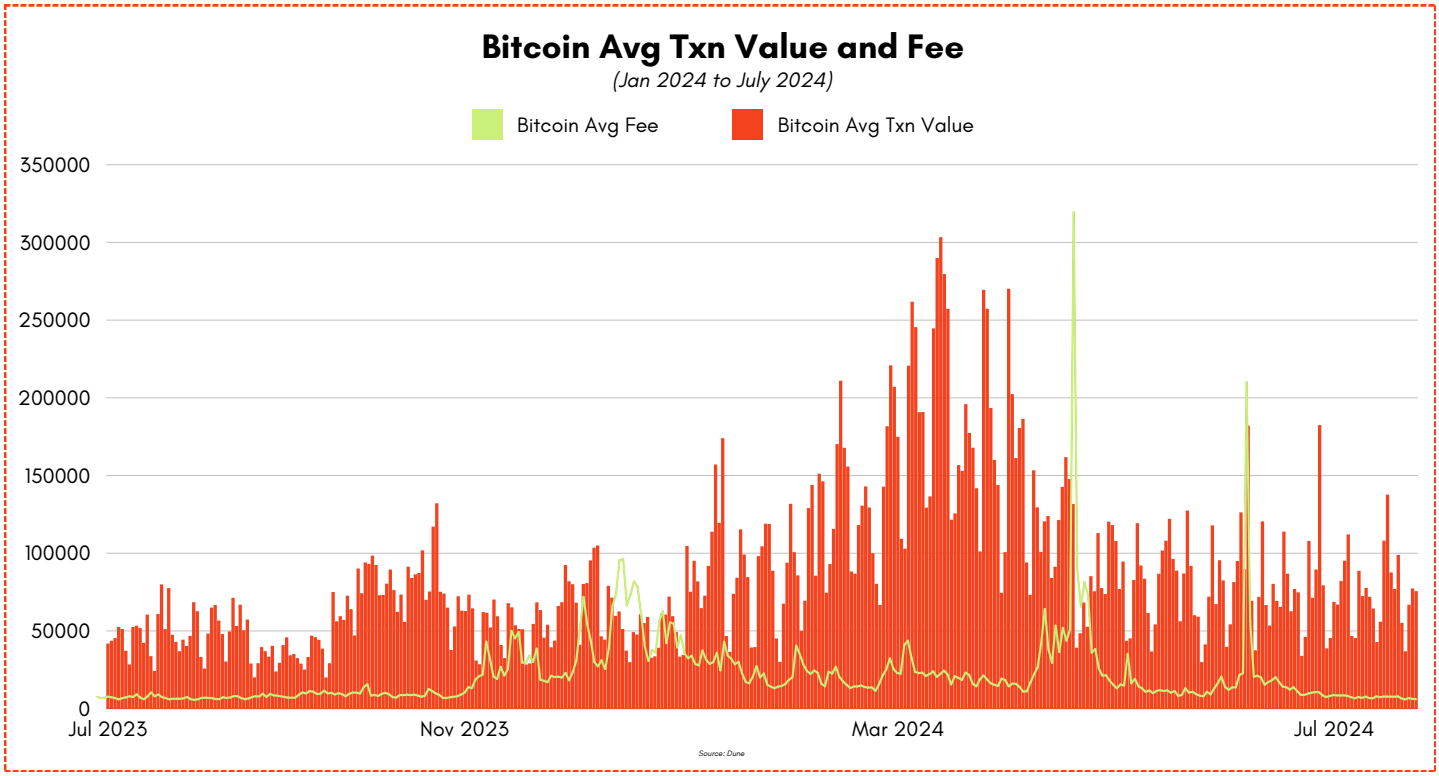
Bitcoin transaction fees can be quite high, especially during periods of network congestion. For small transactions, the fees can often exceed the value of the transaction itself, making it impractical for micropayments.

Transaction Confirmation Times

Bitcoin transactions require confirmation from the network, which can take from several minutes to over an hour. For micropayments, where speed and convenience are crucial, these delays are a significant drawback.

Price Volatility

The value of Bitcoin can fluctuate significantly within short periods. This volatility makes it challenging to use Bitcoin for small, everyday transactions, as the value of the payment can change quickly.



As evident from the above data, the average transaction fee for Bitcoin is approximately $1 and the average transaction value is upwards of $50k.

Now imagine buying a $1 candy for $2 using Bitcoin every day for a week. By the end of the week, you would have actually spent $14 instead of $7.

The Struggle With Programmability

Bitcoin's smart contracts are created using a language called Script, which has limited programmability because it is not Turing-complete.

Turing completeness refers to the ability of a programming language or machine to solve any computational problem given sufficient memory and time.

Since Script lacks Turing completeness, deploying complex smart contracts on Bitcoin is challenging. But this is an intentional piece of design by the creator(s) Satoshi Nakamoto. Bitcoin was intentionally designed to be Turing incomplete, meaning that its scripting language does not support logical loops and conditionals. This limitation reduces Bitcoin's ability to handle complex transactions and contracts.

As a result, smart contracts are often associated with other smart contract compatible and usable blockchains like **Ethereum** and **Solana**, which have more advanced scripting capabilities. Bitcoin's limited scripting language restricts what can be achieved on its base blockchain.

In contrast, **Ethereum** allows for extensive flexibility in writing decentralized applications (dApps), as developers can write smart contracts from scratch without inherent limitations. On Bitcoin, smart contract primitives are gradually added as needed, once they are proven useful and secure.

For instance, the opcodes OP_CHECKLOCKTIMEVERIFY (CLTV) and OP_CHECKSEQUENCEVERIFY (CSV) were incorporated into Bitcoin to support the Lightning Network, which is crucial for scaling Bitcoin payments.

However, sophisticated smart-contract-based applications like Uniswap and Maker cannot be built on the Bitcoin blockchain today due to the absence of necessary tools in Bitcoin Script.

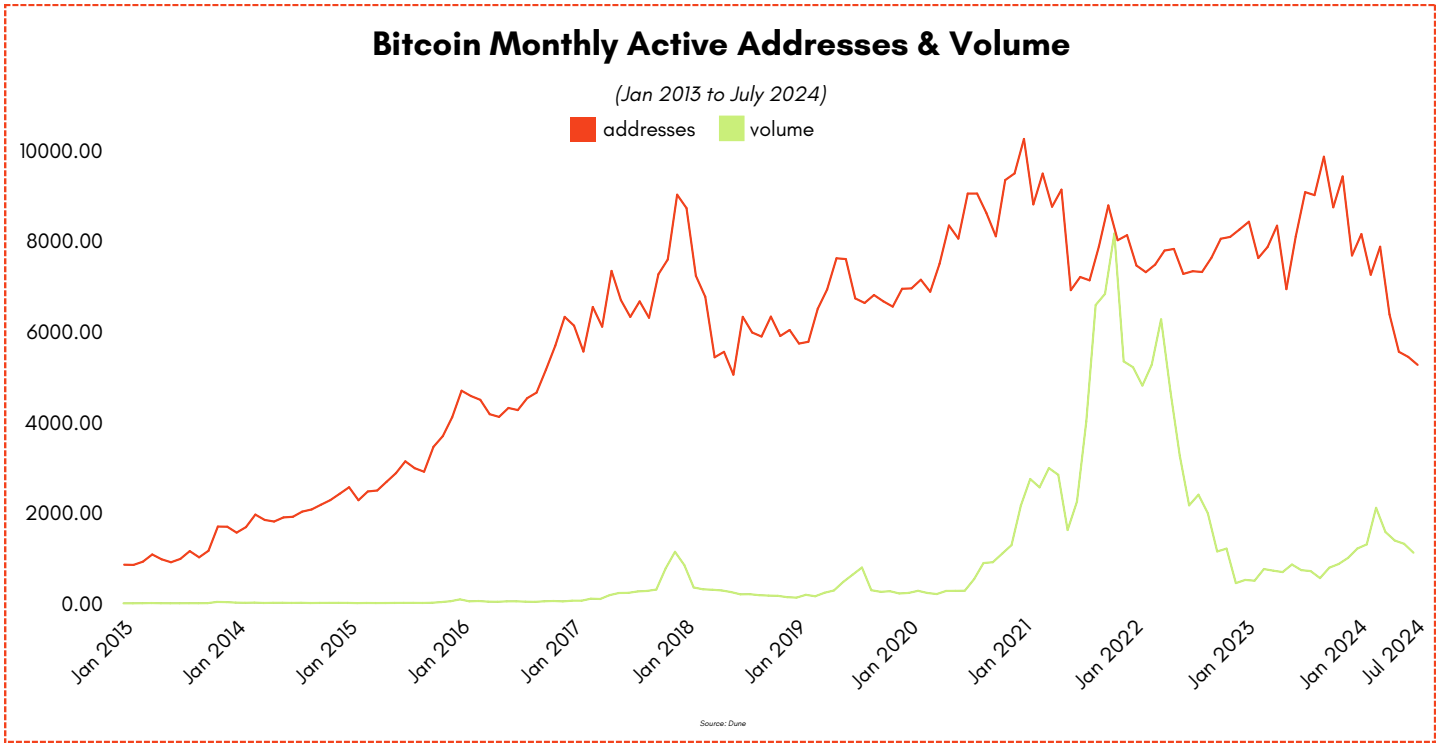
Unintended Consequences

Dormancy and Declining Activity in the Bitcoin Network

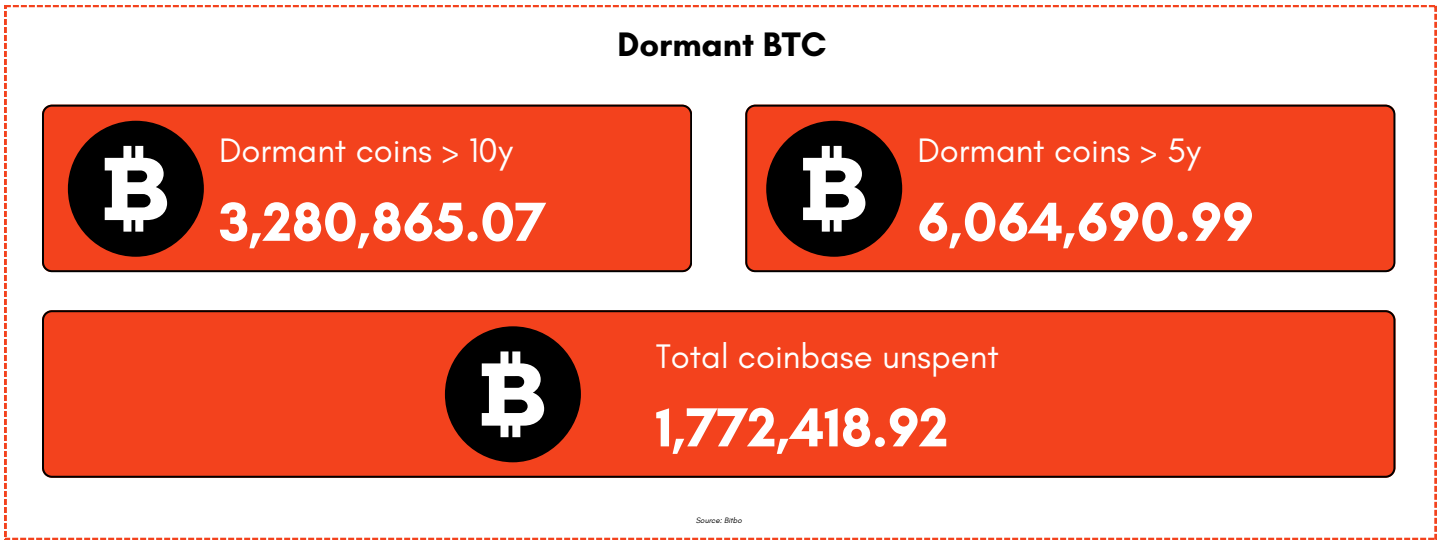
Decreasing Active Addresses & On-chain Volume

One of the most noticeable effects of Bitcoin's inherent problems is the decline in the number of active addresses and the on-chain transaction volume. Over the past few years, the network has seen a significant drop in user engagement, correlating with the growing severity of the aforementioned problems. This decline underscores the urgent need for solutions to address Bitcoin's scalability, environmental, and usability challenges to revitalize its ecosystem.

The graph below illustrates the declining trend in active Bitcoin addresses and on-chain transaction volume.



Dormant Bitcoin



If we take a look at the data from Bitbo, 3,280,865.07 BTC are dormant for more than 10 years and 6,064,690.99 BTC has remained dormant for more than 5 years.

The majority of the BTC sitting dormant in cold wallets for all these years is because users cannot utilitise them along with reason that many holders view Bitcoin as a long-term store of value, similar to gold, and engage in deliberate long-term holding as a strategy. Additionally, some dormant Bitcoin may be lost or inaccessible, not necessarily unused by choice.

In contrast, other utility tokens like Ethereum (ETH) and Solana (SOL) offer multiple use cases that incentivize active participation and utilization.

Ethereum and Solana, for instance, can be used not only for payments but also for earning yield through DeFi platforms, staking to support network security, and participating in a wide range of dApps. This multifaceted utility drives constant demand and activity, contributing to a vibrant and dynamic ecosystem. The ability to earn rewards and participate in different blockchain activities encourages users to actively engage with the network, rather than simply holding their tokens passively.

The comparison highlights a significant drawback for Bitcoin: its lack of broader utility beyond being a store of value. As a result, a substantial portion of Bitcoin remains dormant, while utility tokens like ETH and SOL continue to foster active and diverse use, driving continuous engagement and growth within their respective ecosystems. This difference in utility underscores the need for Bitcoin to evolve and address its limitations to maintain relevance in an increasingly versatile and utility-driven blockchain landscape.

Innovations On The Horizon

Paving the Way for Bitcoin's Evolution

Let's be honest, Bitcoin faces challenges. But the Bitcoin community has made efforts to overcome these challenges.

The development and implementation of layer-2 solutions like sidechains, state channels (lightning network), and advanced technologies like rollups and rollups as a service (RaaS), are paving the way for a more scalable and efficient Bitcoin network. These innovations aim to unlock a layer of innovation on Bitcoin.

As these solutions continue to evolve and gain adoption, there is an optimistic outlook for Bitcoin's future, where it can achieve greater scalability and utility while maintaining its core principles of security and decentralization.

With continued innovation and community support, Bitcoin can solidify its role as a cornerstone of the global financial system.

Bibliography

- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System
- Bitcoin Core. (2017). Segregated Witness (SegWit). Bitcoin Core Documentation.
- Bankless, The Curious Case of Bitcoin L2s
- Lorenzo Protocol, The Definitive Guide To Bitcoin Smart Contracts
- Argo Blockchain, Explaining The Bitcoin Block Reward
- Dune Analytics, @blockintel.
- Dune Analytics, @21co.
- Dune Analytics, @decrypto_space.
- Bitbo, Dormant Bitcoin Statistics. Bitbo.
- Lightning Network Documentation.
- Digiconomist. (2023). Bitcoin Energy Consumption Index. Digiconomist.
- United Nations University and Earth's Future. (2021). Study on Bitcoin's Environmental Impact.
- U.S. Environmental Protection Agency's Greenhouse Gas Equivalencies Calculator. EPA.
- Cambridge Bitcoin Electricity Consumption Index (CBECI). CBECI.
- Cato Institute. (2018). Analysis of Payment Networks' Operating Costs. Cato Institute.

PYOR

Supercharging Bitcoin Rollups of Tomorrow

A modular Bitcoin Rollup-as-a-Service with a Decentralised verifier network

Check out at → surge.build

This report is created by **PYOR** a digital assets data company for institutional investors and hedge funds.
Our investors include – Castle Island Ventures, Hash3 Capital, Coinbase Ventures, and Balaji Srinivasan, among others.