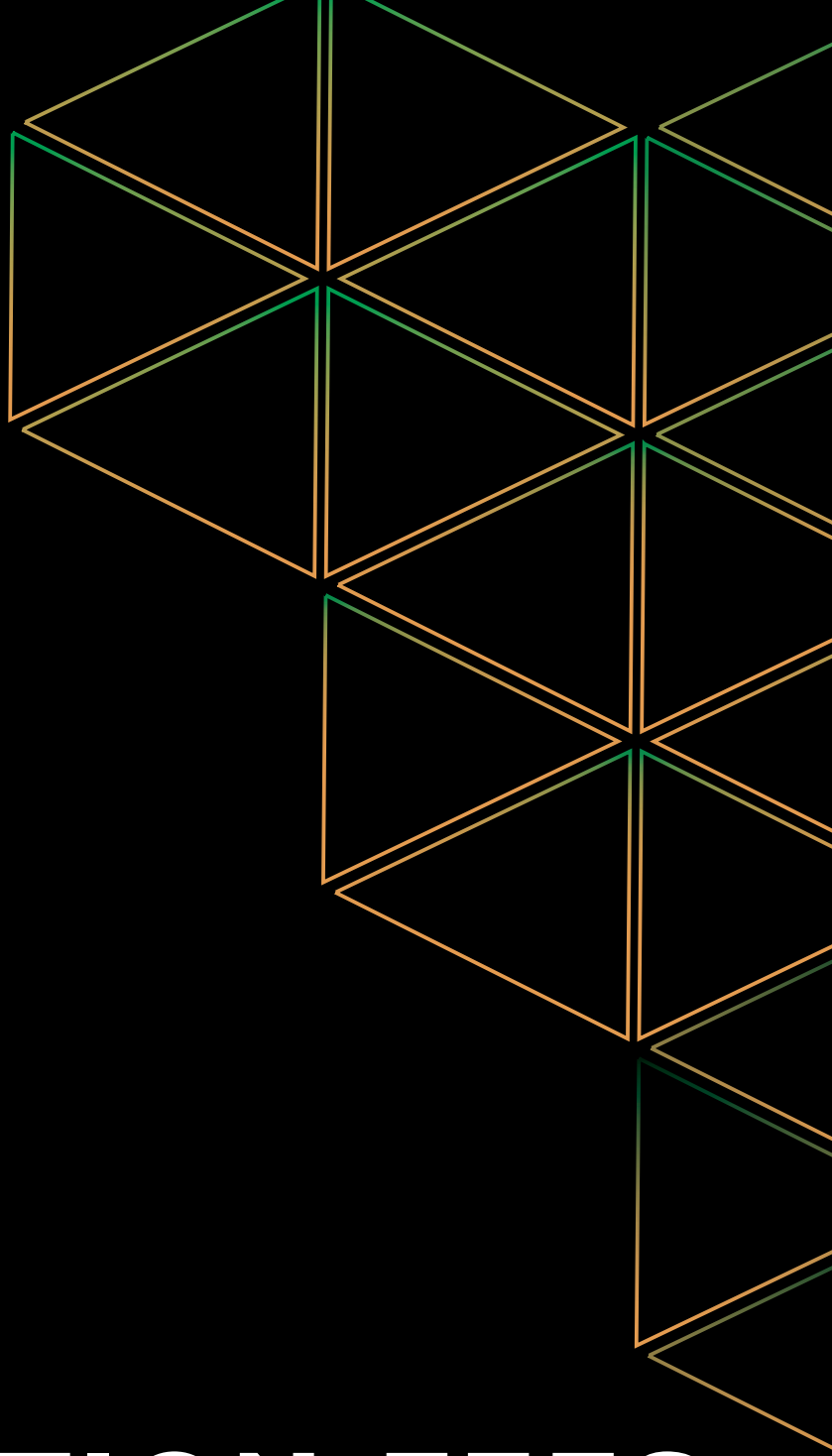


BITCOIN TRANSACTION FEES

THE FUTURE ECONOMICS OF BITCOIN SETTLEMENT FINALITY

Prepared By:

Joe Burnett, Head Analyst, Blockware Solutions
Pierre Rochard, VP of Research, Riot

SEPTEMBER 22

Table of contents

1. Executive Summary

The Bitcoin network's transaction fees and throughput are often cited as positive or negative catalysts for the value of BTC[1], depending on when and who you ask. The volatility of fees has led to the development of polarizing narratives, they are simultaneously characterized as being too high and too low.

For users of Bitcoin, its transaction fees represent an unpredictable cost, but a known benefit: global 24/7 digital final settlement of a highly liquid asset. Historically, Bitcoin's transaction fees have been a small part of miners' revenue relative to "minting" new BTC for the ledger, but long term these fees may become the primary source of miners' revenue.

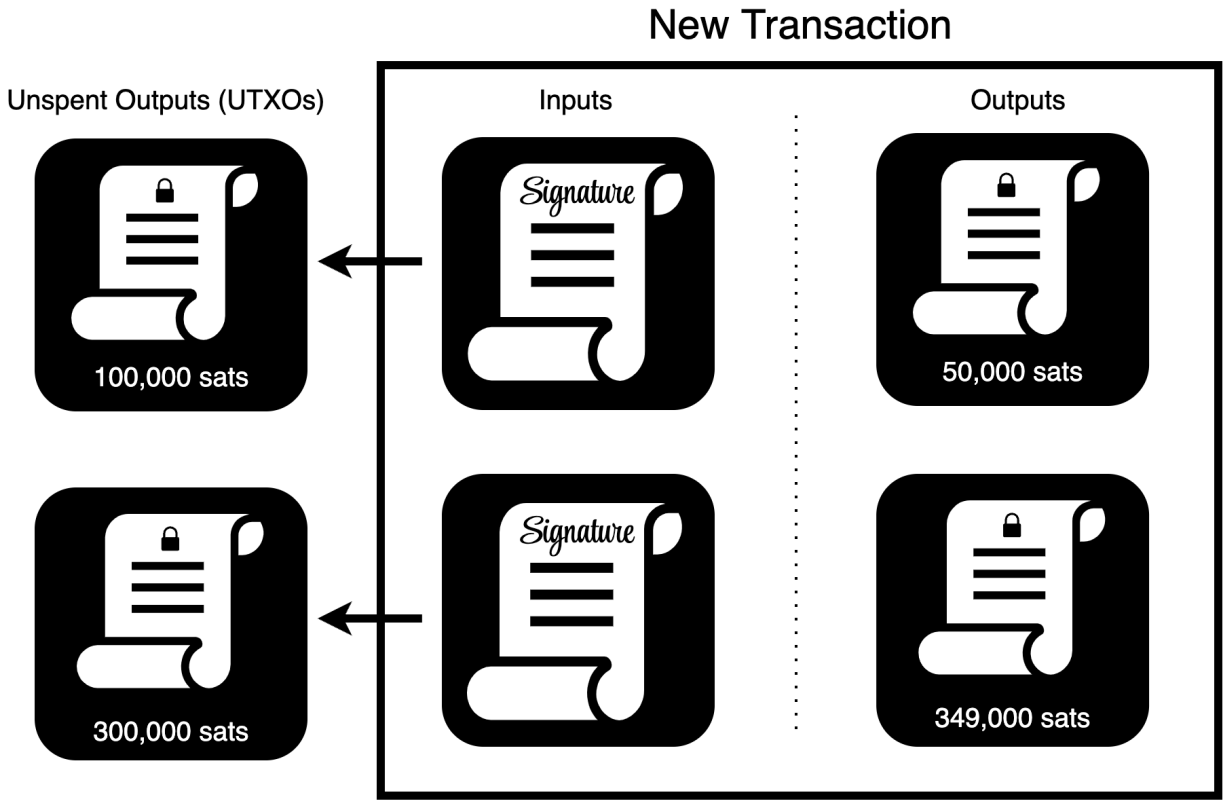
In this Blockware Intelligence Report, we describe:

- Who pays transaction fees and how fee rates are set
- Why high congestion fees are transitory
- How Bitcoin transactors could use fees to route around unreliable miners

[1]Throughout this report we will refer to the network or protocol as "Bitcoin" and its native asset as "BTC".

2. How Transaction Fees Work

When your wallet software creates a new transaction, it unlocks more BTC with inputs than it locks up in outputs[2]. This residual difference is the transaction fee offered to the first miner who includes the transaction in a block. The following example illustrates how 400,000 sats[3] of pre-existing outputs unlocked minus 399,000 sats locked in new outputs leaves a residual 1,000 sats for the transaction's fee earned by the miners.

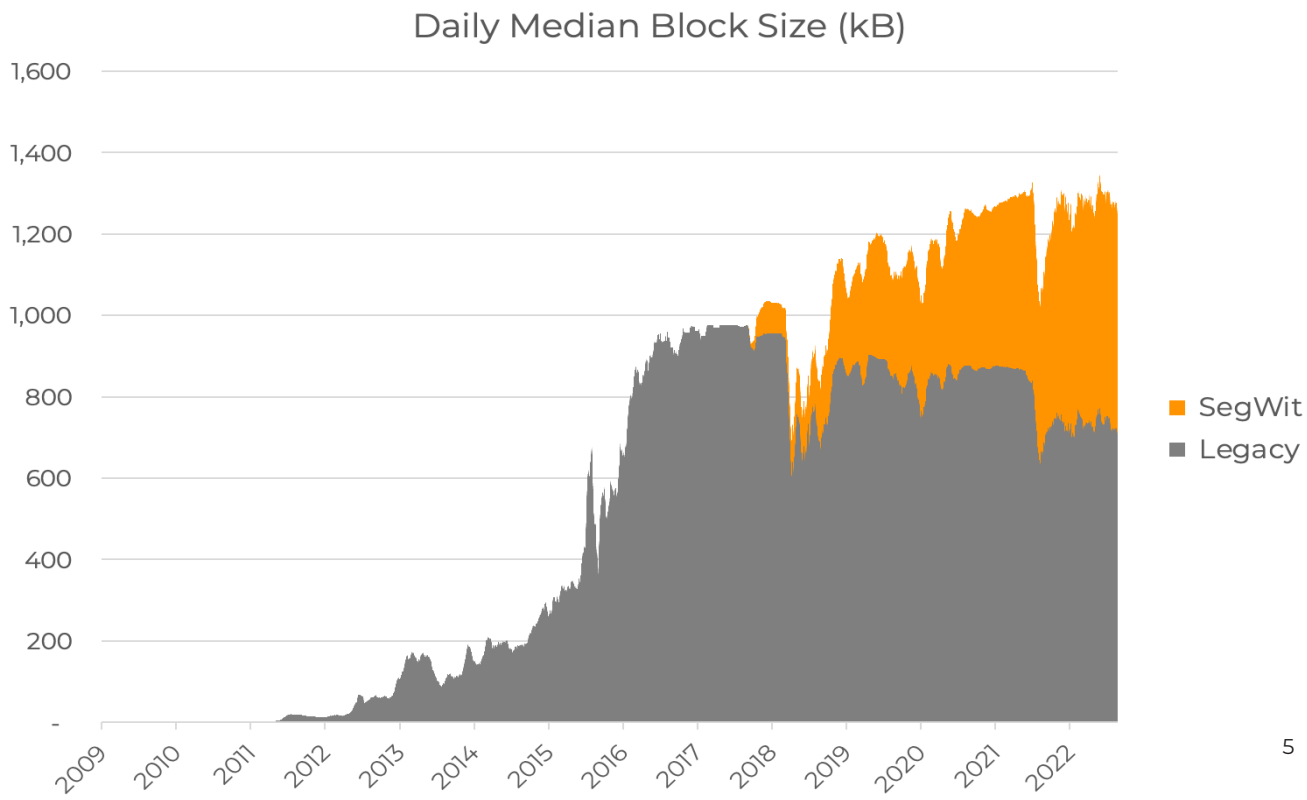


The number of inputs and outputs in a transaction varies widely depending on the nature of the wallet. It is common for exchange transactions to have dozens and even hundreds of outputs representing a 10-minute batch of withdrawals from their clients. The size of inputs and outputs varies depending on the kind of "script" or smart contract used to lock and unlock the sats.

[2] Rosenbaum, K. (2019). Grokking Bitcoin. Manning Publications Co.

[3] Just as 1 USD is divisible into a hundred cents, 1 BTC is divisible into 100,000,000 satoshis (sats).

To keep the cost of syncing and using a Bitcoin node reasonable, in 2010 Satoshi Nakamoto added a 1 megabyte (MB) block size limit to the Bitcoin node software's consensus rules. This protocol resource constraint means that nodes reject proposed blocks from miners if the blocks exceed the limit. In 2017 SegWit activation transformed the 1 MB limit into a 4 million weight-units (WU) limit, in effect doubling the supply of block space available to transactors[4].



5

The scarcity of block space means that the transaction fee is divided by the amount of data used to calculate a fee rate with units of satoshis per "virtual" byte (sats/vB).

A common transaction has two inputs and two outputs, taking up approximately 210 vB. Currently the lowest market fee rate is 1 sat/vB, so with the exchange rate at the time of writing a typical Bitcoin transaction often costs as little as $0.05 USD, a nickel. A transaction may be moving BTC worth billions of USD, but this valuable transaction pays the same total fee as any other identically data-sized transaction because the fee is proportional to the use of block space.

[4] Song, J. (2017, August 12). Understanding segwit block size. Medium. Retrieved September 1, 2022, from https://jimmysong.medium.com/understanding-segwit-block-size-fd901b87c9d4

[5] Bitcoin Block Size Chart. Bitcoin Visuals. (n.d.). Retrieved September 1, 2022, from https://bitcoinvisuals.com/chain-block-size

The sender's wallet creates the transaction, uses private keys to cryptographically sign the transaction, and broadcasts the transaction to the network of Bitcoin nodes. Each node uses the protocol's consensus rules to independently verify transactions they receive. If the transaction is valid, the node updates its view on the backlog of transactions waiting to be included in a block. This backlog, or queue, is called the "mempool" short for "memory pool".

When a mining pool wants to create a block to mine, it must first choose which transactions to include in the block. A rational miner would order the transactions to maximize total fee revenue, so blocks generally include the first 1 million vB of transactions paying the highest sats/vB fee rate. Transactors can compete to be at the top of the stack by paying a higher fee rate, so that they are included in the next block.

The market for block space has demand from a variety of consumers, examples include:

- short-term traders moving capital to or from an exchange
- point-of-sale or e-commerce payments for goods and services
- p2p transfers with friends or family, remittances
- long-term HODLers moving BTC to cold storage

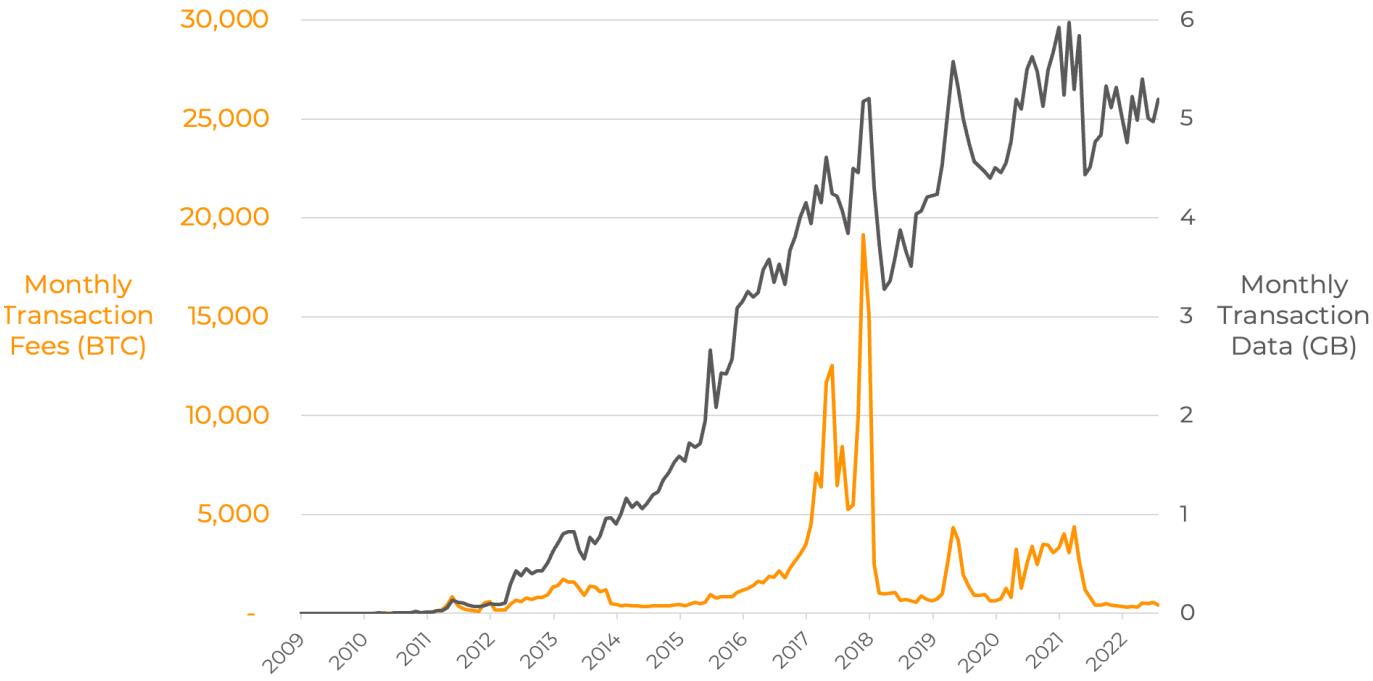
The supply of block space has a floor of zero, it's not unusual for miners to rationally propose a valid empty block because they started hashing the empty block immediately after just seeing a new valid block header; they can not yet include any transactions because they don't yet know which transactions were already included in the new block they are chaining to.

When a mining pool includes a transaction, they take its fee and add it to the outputs in a special transaction called the "coinbase". Unrelated to the exchange, the coinbase transaction is created by the mining pool to pay itself the block reward, which is the sum of the transaction fees plus the "subsidy", a quantity of new BTC allowed by the nodes' issuance schedule to transfer to the public ledger via the reward. The subsidy is the only way by which new BTC can be added to the ledger and it is cut in half after every 4 years worth of blocks. The mining pool pays out the total reward proportionally to its hash rate contributors.

3. Congestion and scaling

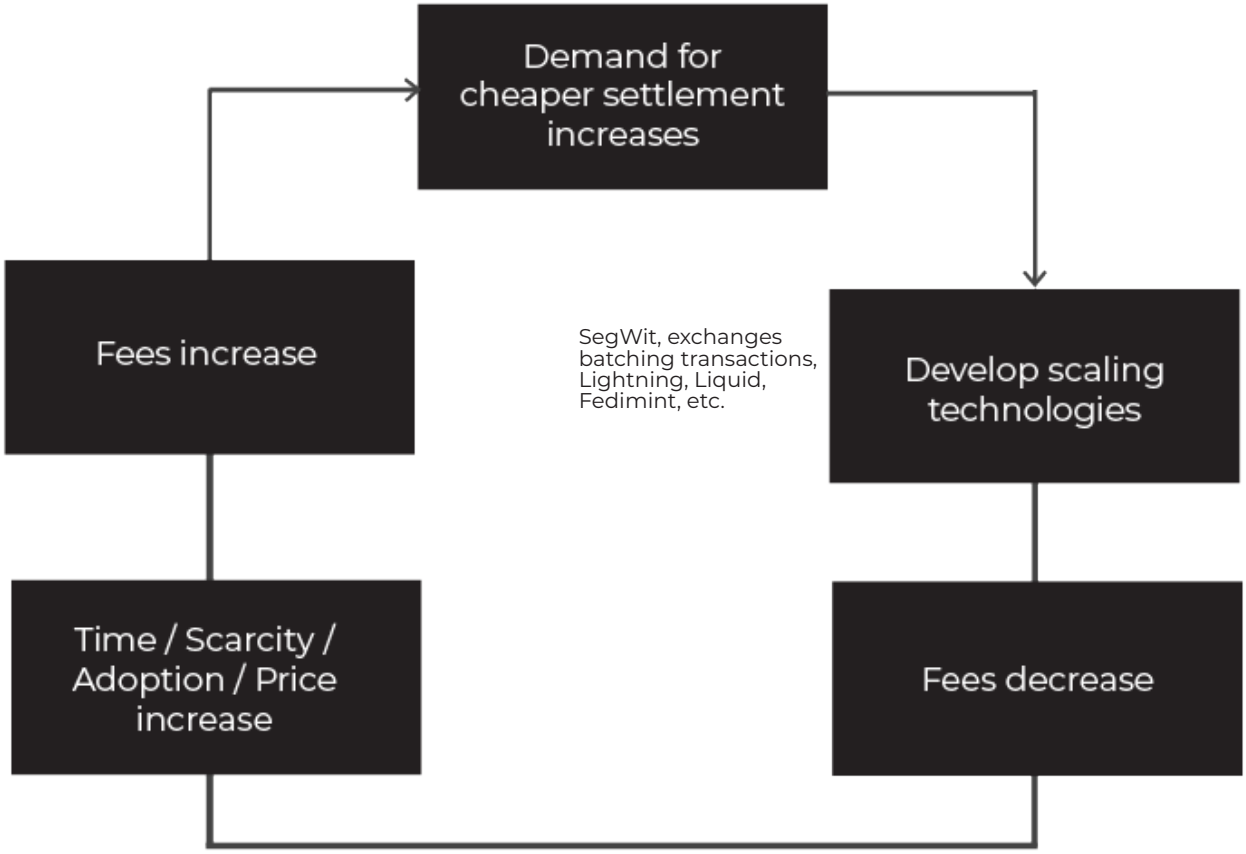
The first portion of this report focuses on Bitcoin's scalability and transaction fees that result from users simply transacting BTC, and the second portion of this report discusses how users would respond to settlement unreliability.

If we look at the history of transaction fee rates, they skyrocketed in the 2017 and 2020-2021 bull markets when demand was greater than the block size limit. Since mid-2021, fee rates have been very low while the network continues to process more than 5 GB of transactions per month.

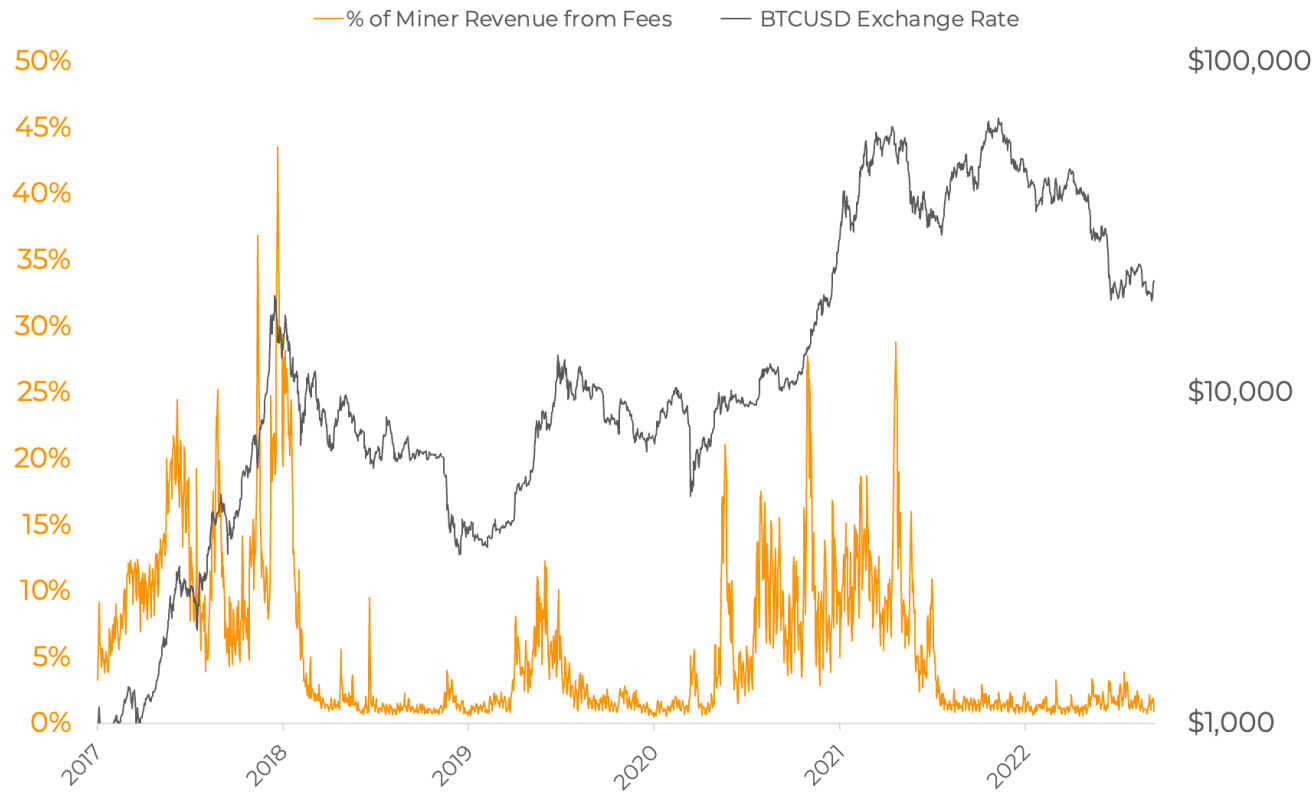


Bitcoin Scaling Cycle

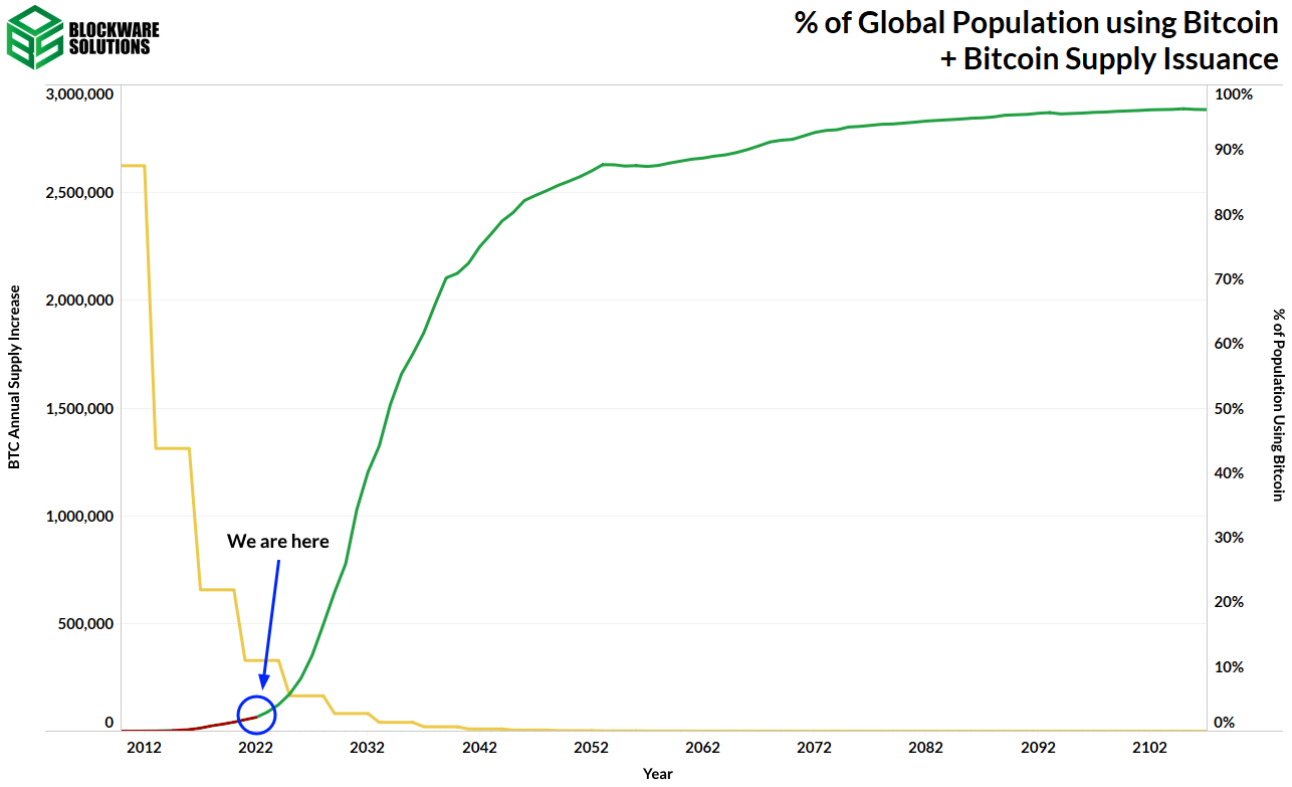
Bitcoin's scaling solutions are not perfectly timed to coincide with waves of new adoption, so Bitcoin will likely continue to see transitory fee spikes as it did in 2013, 2017, and 2020. High fees bring pressure to more efficiently use block space by adopting new scaling technologies. These cost-saving measures enable an increase in total throughput for Bitcoin settlements without significantly increasing the cost of running a Bitcoin node. Low-cost nodes empower users to use their own software's consensus rules to verify all transactions and blocks without trusting a third party. Low-cost system verification secures Bitcoin's decentralization.



Bitcoin will continue to go through scaling cycles. As exponentially more users begin using Bitcoin and holding their own private keys, they are all competing for a fixed amount of block space roughly every 10 minutes. During sudden bursts of adoption, fees paid to miners explode relative to the block subsidy earned by miners.



Interestingly, global Bitcoin adoption is still a small fraction of the total global population. Bitcoin still has magnitudes more worth of individuals to onboard and they are likely all going to be competing to add their transactions to Bitcoin's scarce block space.

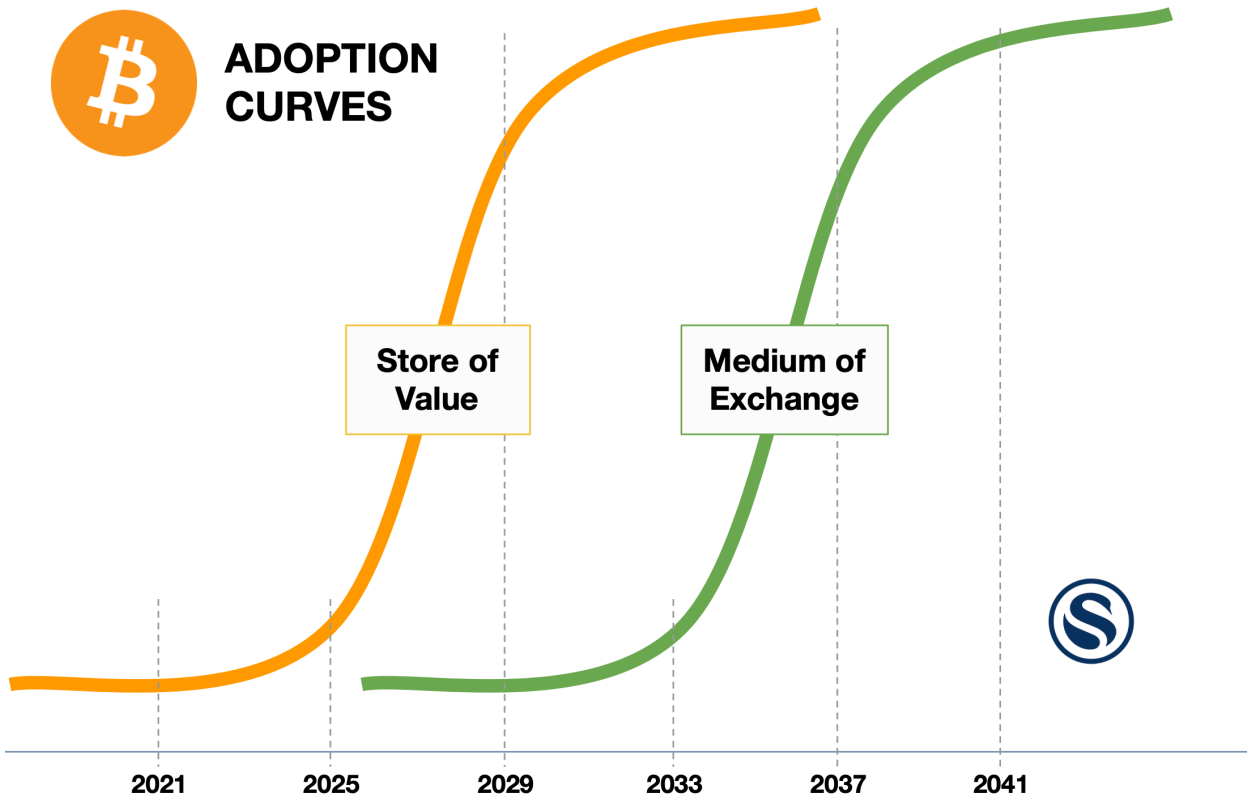


[6]

Using Glassnode data, Blockware previously estimated that ~ 32 million entities currently store wealth on the Bitcoin blockchain. Virtually all of these 32 million are using BTC as a store of value and not as a medium of exchange. What happens when there are 7 billion entities using it as a store of value? That is a 218.75x increase in entities competing for the same amount of block space.

On top of the billions of potential future Bitcoin users looking to use Bitcoin to store a large amount of their wealth, it is possible that one day Bitcoin itself may also be used as a payments tool or a medium of exchange. This would be the period where transaction throughput really starts to get tested and transaction fees would likely soar. Users may adopt second and third-layer scaling solutions for day-to-day spending to save money on fees.

[6] Blockware Solutions. (2022, June 8). Bitcoin User Adoption. Retrieved September 1, 2022, from https://www.blockwaresolutions.com/research-and-publications/bitcoin-user-adoption-report



[7]

Bitcoin users may go from 1-5 transactions per year to 1-5+ transactions per day as more and more individuals begin using Bitcoin as a medium of exchange. With 7 billion people using Bitcoin as a medium of exchange, throughput would have to increase by 79,843.75x instead of just 218.75x for the store of value use case.

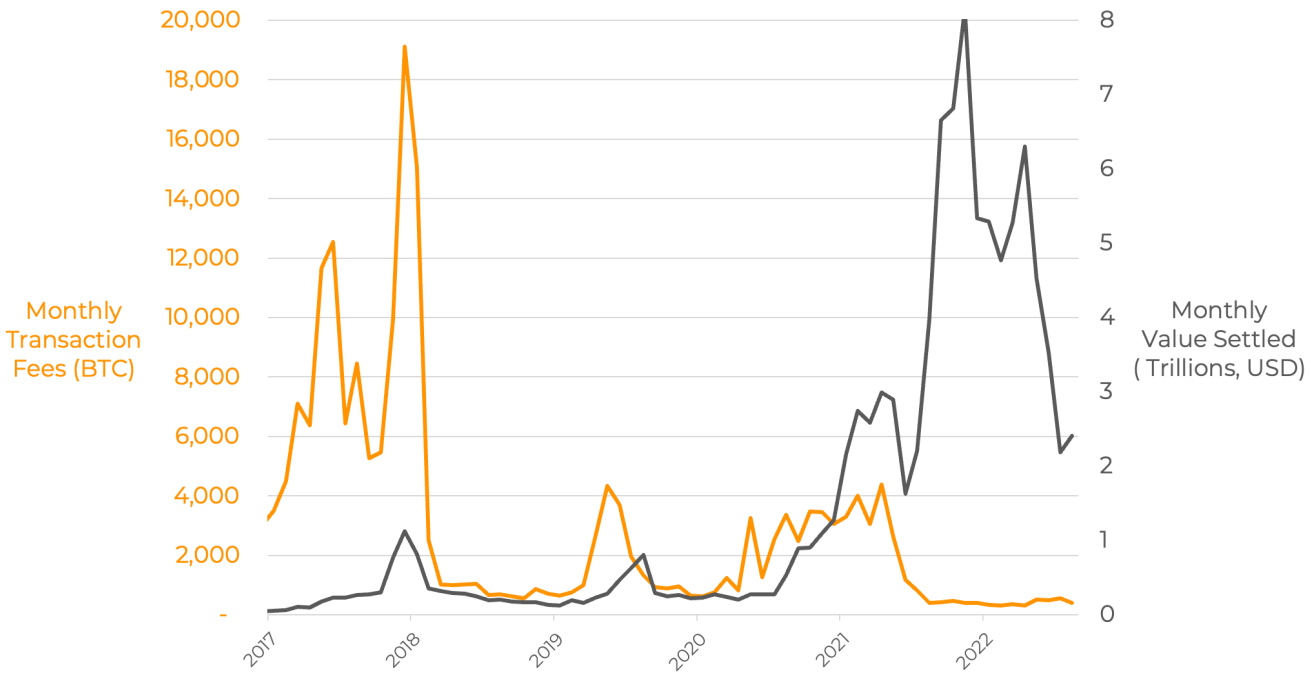
As mentioned above, this increase in throughput may incentivize the adoption of second and third-layer scaling solutions (Lightning, Fedimint, etc.). However, all of these scaling solutions are still anchored to the first layer (i.e. opening, closing, and rebalancing Lightning channels), and they always will rely on the Bitcoin blockchain to be secure and permissionless. High-value transactions to and from cold storage will also likely be done on the first layer to minimize uncertainty.

Transitory high on-chain fees will likely continue to motivate the development of more scaling solutions, many of which may be completely unknown today. However, for throughput to increase by 79,843.75x in the next ~ 20 years, there will likely be periods of high on-chain fees with each wave of adoption. With each halving of the block subsidy, the importance of transaction fees for miner revenue increases. If we take 350 BTC to 3,500 BTC as the range of monthly transaction fee revenue for miners, we would expect fees to be a greater source of revenue than the subsidy between the years 2032 and 2048.

[7] Klippsten, C. (2021, November 17). Twitter. Retrieved September 1, 2022, from https://twitter.com/coryklippsten/status/1461102945685192717

4. Settlement Finality

During periods of low fees the skeptics of Bitcoin have sounded the alarm that the finality, or "security", of transactions is at risk of being undermined. This assertion is surprising because Bitcoin settlements are widely viewed as being irreversible[8]. Even with very low transaction fees, Bitcoin has reliably settled trillions of dollars worth of transactions monthly without needing any trusted third parties.



However, Bitcoin detractors argue, “it may work fine now with the block subsidy (monetary inflation), but post-subsidy the chain will be ‘insecure’ due to little incentive to mine.” Many Bitcoiners have responded to this by broadly saying “fees will [eventually] begin to consistently represent a healthy portion of the block reward”[9] or “we will figure this out later if it ever actually becomes a problem.”

The next part of this research piece is going to take a different approach to this subject, and it is important for both Bitcoin users and miners to take it into consideration.

[8] Morton, H., & Narvasa, H. (2014, August). The Emergence of Bitcoin. National Conference of State Legislatures. Retrieved September 1, 2022, from https://www.ncsl.org/research/financial-services-and-commerce/the-emergence-of-bitcoin.aspx

[9] Held, D. (2021, February 12). Bitcoin's security is fine. Medium. Retrieved September 1, 2022, from https://danhedl.medium.com/bitcoins-security-is-fine-93391d9b61a8

Finality, not "security"

Bitcoin's security and consensus rules are defined by private key storage and nodes respectively, not miners.

No matter how much or how little hash rate is on the network, miners cannot force your node to accept more than 21M BTC, raise node cost constraints like the block size limit, create a valid new transaction that steals your BTC, or alter other fundamental consensus rules.

This is why the Blocksize War from 2015-2017 was so important.[10] It affirmed that Bitcoin's core consensus rules can be immutable and enforced by individual users (node operators), not large companies, exchanges, miners, developers, or any government.

Bitcoin is a Schelling point on an existing consensus rule set.[11] The first one was set by Satoshi Nakamoto with his initial release in 2009. Changes can occur, but you need users to opt-in. Users of node software converged on prioritizing cautious changes that do not materially increase their long term bandwidth, compute, memory, or storage costs. The result is decentralization: where anyone has the ability to run free open source software, a full node that at low cost verifies and validates the history of the entire ledger including their own transactions.

To maximize security and decentralization, it is necessary to avoid "forced" or "automatic" software upgrades, so new software versions must compete against old software versions by proving themselves to either be more useful while maintaining backward compatibility or needed for survival.

Unreliable Miners

At the end of the day, miners have the ability to only do one thing: propose blocks that nodes (who set the consensus rules) verify, accept, and use to update the ledger.

Since miners cannot change key consensus rules, malicious or unreliable miners can only censor specific transactions they do not want to include in their own blocks. They can get creative with this, but all attacks stem from only being able to censor transactions in the longest proof of work chain.

[10] Bier, J. (2021). The Blocksize War: The battle for control over Bitcoin's protocol rules. Independently published.

[11] Rochard, P. (2018, July 8). Bitcoin governance. Medium. Retrieved September 1, 2022, from https://pierre-rochard.medium.com/bitcoin-governance-37e86299470f

The costs of accumulating hashrate for an attack, like building hosting facilities, manufacturing ASICs, or purchasing electricity are not relevant for attackers who have the power to seize these assets or hijack them with a cyber-attack. Of course, miners have an incentive to protect themselves against these uncertainties, but they are fundamentally unquantifiable contingencies.

There are three key attacks that miners can perform. One is an economic attack (potential to profit) and the other two attacks are either accidents or attempts to destroy confidence in Bitcoin's settlement assurances.

1.) Double spend their own coins (economic attack)

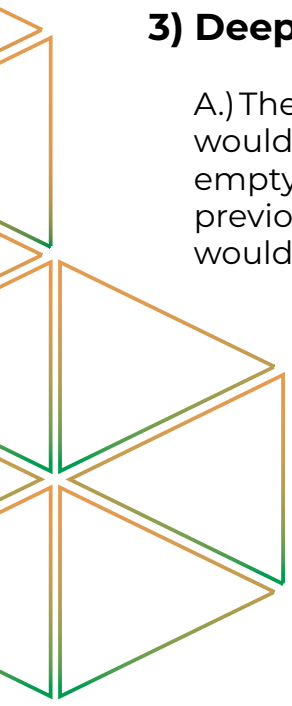
A.) The attacker would spend their BTC to a receiver's address, and at the same time, begin mining a chain with that original transaction sent back to themselves. The receiver initially sees the transaction confirm until the attacker later releases the longer chain without the original transaction. The receiver no longer has the BTC and the attacker keeps the original BTC.

2) Allow nobody to transact by mining empty blocks (non-economic attack)

A.) The attacker would continuously broadcast empty blocks to prevent any users from transacting. Since the attacker would have > 50% of all hash power, honest miners would never be able to mine a block that gets built on, as the attacker would be able to reorg out non-empty blocks that other miners might attempt to produce. This is a non-economic attack because the attacker would have to purchase or steal mining rigs, mining infrastructure, and energy to earn nothing. The moment the attacker stops burning resources, honest miners can continue operating normally.

3) Deep reorgs (non-economic attack)

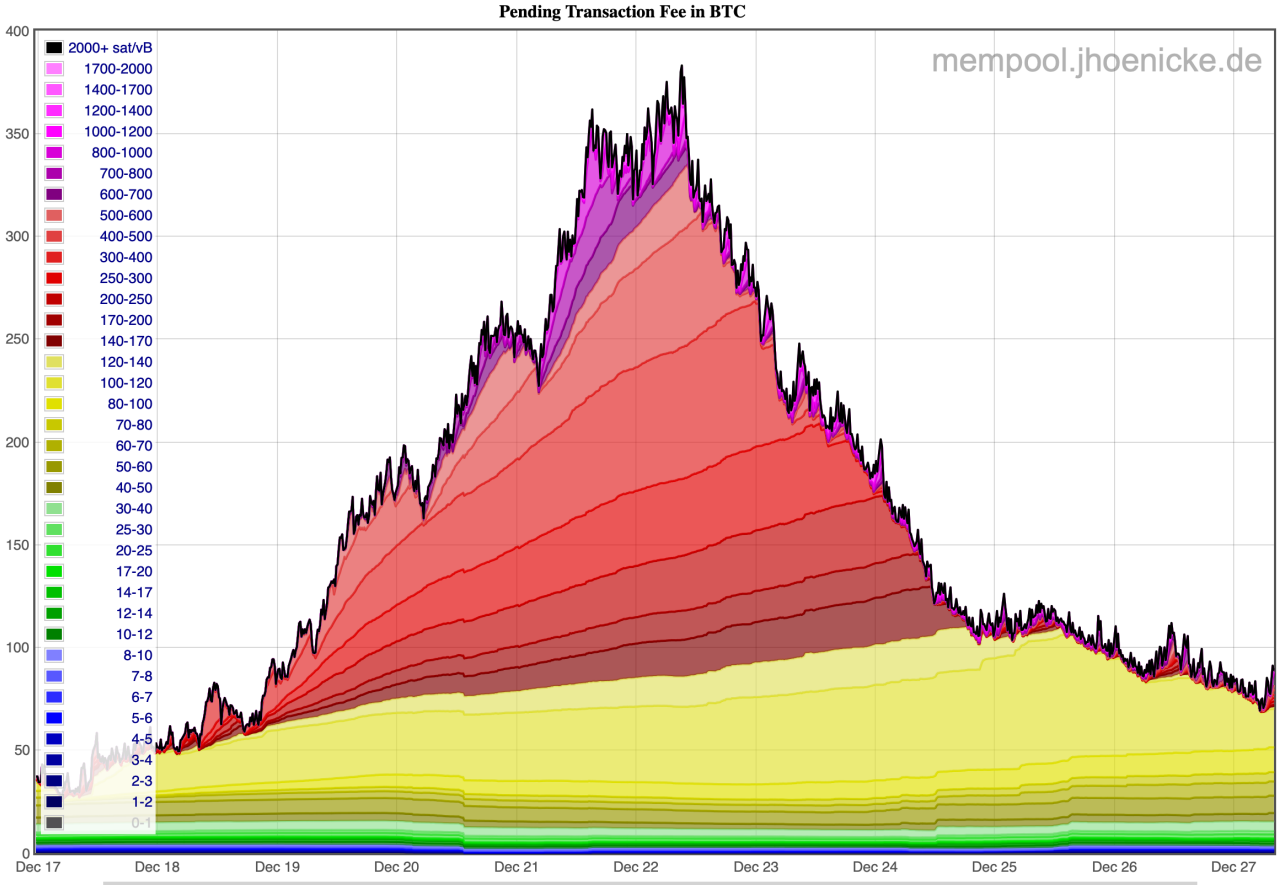
A.) The attacker would silently begin mining a chain of empty blocks. The attacker would wait for a large number of blocks to be mined, and later broadcast the empty longer chain of blocks, removing transactions that users thought previously confirmed. Again, this is a non-economic attack because the attacker would burn resources for nothing in return.



Bitcoin is antifragile

Fees will soar if needed

Are empty blocks being mined? The mempool will fill with Bitcoin transactors raising fees, competing with each other to get in the next block. This is not theoretical either. We have seen what happens when demand exceeds block space supply (see Bitcoin's mempool from December 2017 below).



Under an empty block attack, it is in the self-interest of Bitcoin users to raise their transactions' fees to get into the next block. The more empty blocks (the longer the attack lasts), the more pending transactions in the mempool. Transaction fees could soar from 1 sat/vbyte to 1,000+ sats/vbyte. The reward for one block could go from close to 0 BTC to 10+ BTC assuming the current maximum block size of 1,000,000 vbytes.

The system is antifragile, and an empty block attack would be met by an endless market-based counterattack of high transaction fees. And knowledge of this counterattack would likely deter the attacker from this attack in the first place.

This solves an ongoing empty block attack, but what if the attacker mines a chain in secret for 24 hours and later broadcasts a longer empty chain to the network that all nodes still consider valid? All previous transactions that had confirmations in the last 24 hours now have zero confirmations according to the longest proof of work chain and go back to the mempool.

This attack will also be countered in a similar way. All previous transactors (senders or receivers) will use CPFP (child pays for parent) or RBF (replace by fee) to increase the transaction fees to get their transactions confirmed as soon as they desire.

For example, if someone sent you 100 BTC, it received 23 confirmations, you thought it was settled, but then an attacker broadcasts an empty chain (reorg) without your transaction. This would be devastating, as you are now out of the 100 BTC you thought you had, right? Well not exactly, you could CPFP that now unconfirmed transaction with a much higher fee to get it at the top of the (now very clogged) mempool. You again could raise your fee to 1,000+ sats/vbyte or whatever it takes to get into the next honest block.

Note that the point of fees rising is to incentivize miners to get plugged in. Machines that may only be profitable during certain times of the day when electricity is free or negative now are running at nearly any cost because their future revenue increased by 1,000x or more. The amount of honest hash rate soars with increases in fees eventually overwhelming the attacker.

Some may argue that an empty block attack could also be an economic (profitable) attack. Before broadcasting a string of empty blocks, the attacker would open a large short position on Bitcoin anticipating that the price would collapse due to the attack. However, in previous 51% attacks on Bitcoin Gold[12] and BitcoinSV[13], the price didn't immediately collapse during or after the attack. While these 51% attacks were double spends and not empty blocks, they highlight that a 51% attack may not damage the price of the asset. In fact, during the attack, it would not be clear what the price would be since nobody could move coins (empty blocks). Existing coins stuck on exchanges could potentially still trade, but there's no guarantee that the price would fall, especially since all users know the attack eventually will end as the attacker won't burn resources forever. The moment fees become high enough to bring on additional hash rate or the attacker gives up, the attack fails.

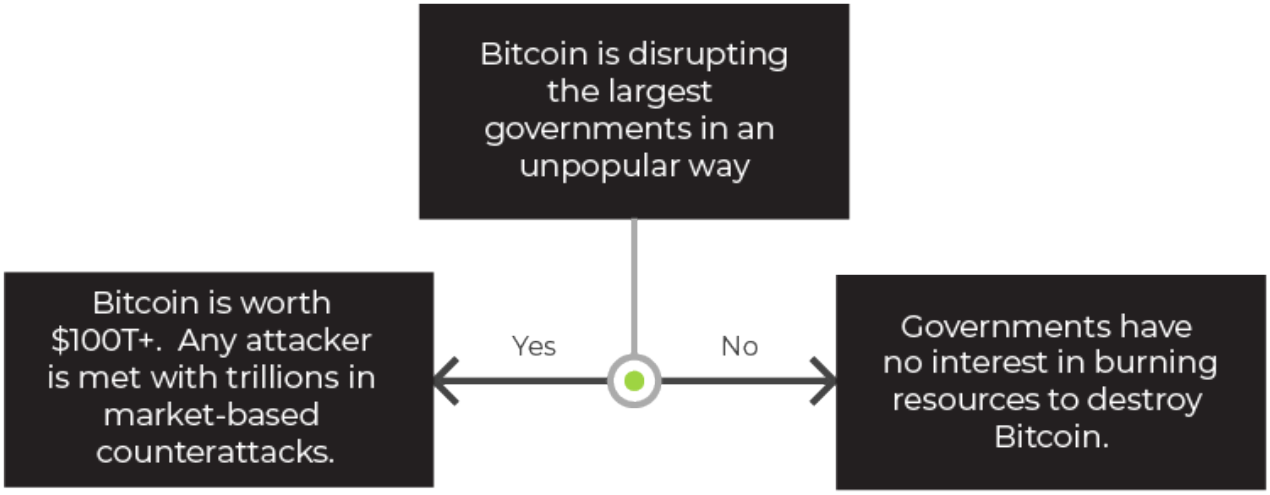
[12] Martin, J. (2020, January 27). Bitcoin gold blockchain hit by 51% attack leading to $70k double spend. Cointelegraph. Retrieved September 1, 2022, from https://cointelegraph.com/news/bitcoin-gold-blockchain-hit-by-51-attack-leading-to-70k-double-spend

[13] Avan-Nomayo, O. (2021, August 7). Bitcoin SV rocked by three 51% attacks in as many months. Cointelegraph. Retrieved September 1, 2022, from https://cointelegraph.com/news/bitcoin-sv-rocked-by-three-51-attacks-in-as-many-months

Conclusion: The Bitcoin network's dynamic fee market could make it resilient against adversaries.

Attack paradox

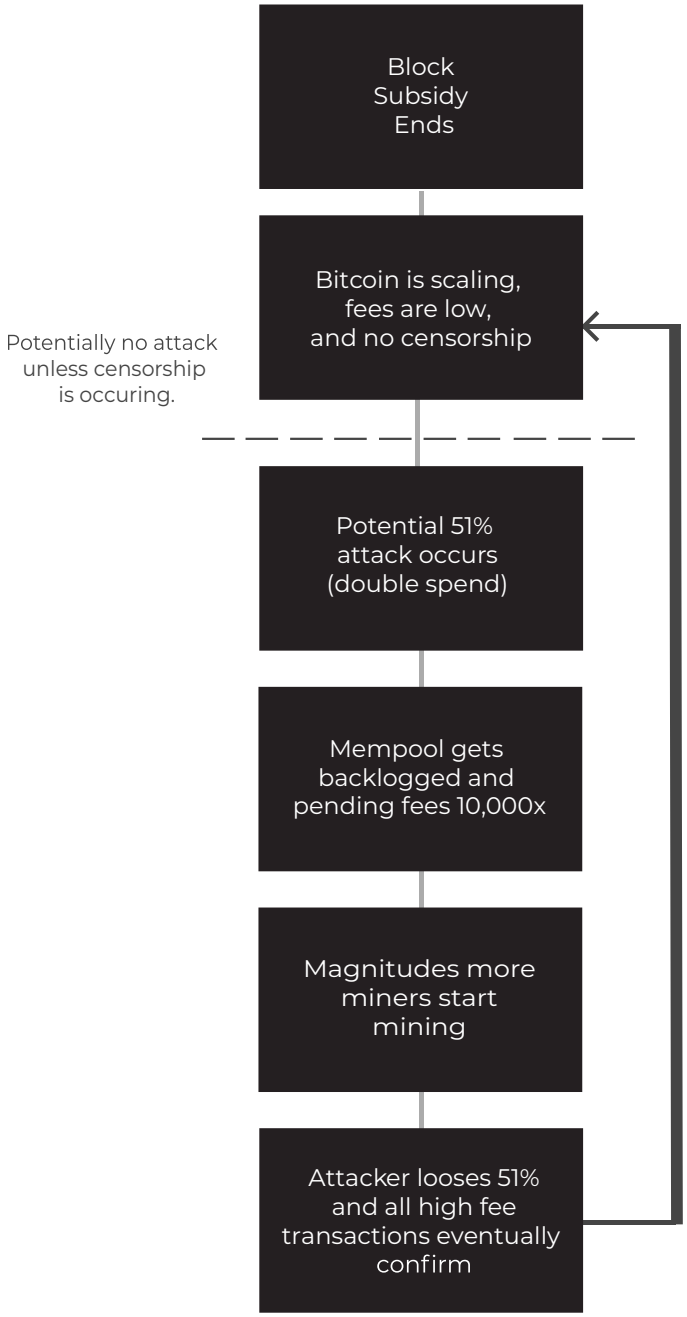
For this attack to be attempted, an entity with nearly endless amounts of resources needs to have a strong desire to try to destroy Bitcoin for no economic incentive. By only proposing empty blocks and preventing users from transacting on the network, this entity would simply be burning resources and energy. The larger Bitcoin is, the more resources the entity needs to burn.



If Bitcoin is “small” and not severely disrupting its monetary competitors, the benefits of an attack would be insufficient to justify the effort or cost.

If Bitcoin is large ($100T+) and is severely disrupting its monetary competitors, they likely won’t be able to successfully attack. Any attack would be met with the natural market-based counterattack of high fees as explained above. If multiple bad actors are trying to attack at the same time, each one has an incentive to "defect" by being the first to include high-fee censored transactions, this is a geopolitical Prisoner's Dilemma.

Market-Based Feedback Loop



Waiting out attackers

Last, if an attack has not occurred, but receivers of BTC fear one may occur, they can wait for more confirmations to have more confidence that their transaction has settled.

This isn't theoretical either. This is exactly what happened with BCH, BSV, and other altcoins.

There are still transactions being broadcast and confirmed, and users are buying and selling coins on these networks on multiple exchanges even though the "security" or settlement finality on these networks is far less certain than BTC.

A great example is a transaction that occurred on BCH on July 17th, 2022. The transaction moved 113,356 BCH ($12.4M). At the time, the block reward was only ~ $800 (5x less than the current average transaction fees per block on BTC).

It is potentially profitable to perform a double spend, and here is how you could do it:

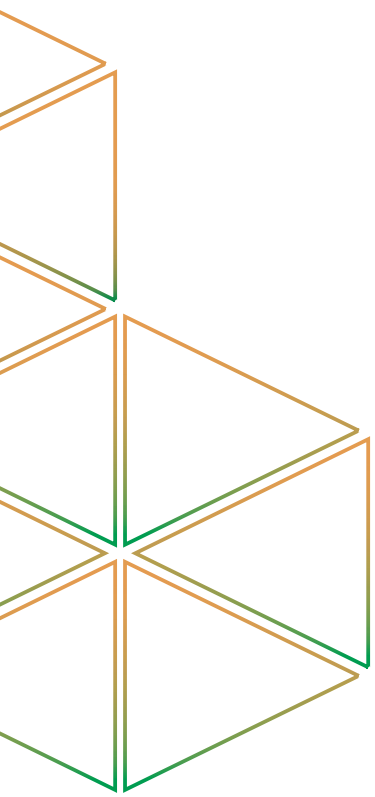
1. Send 113,356 BCH to an exchange.
2. Start 51% attacking the network silently by mining a chain without that transaction.
3. Sell the BCH for BTC.
4. Send the BTC off the exchange.
5. Broadcast your new longer chain that doesn't include the original BCH transaction to the exchange.
6. The attacker now has BTC, and the longest valid BCH chain now says the attacker has the original BCH as well.
7. The exchange has been double spent on, and they are now out of $12.4M.

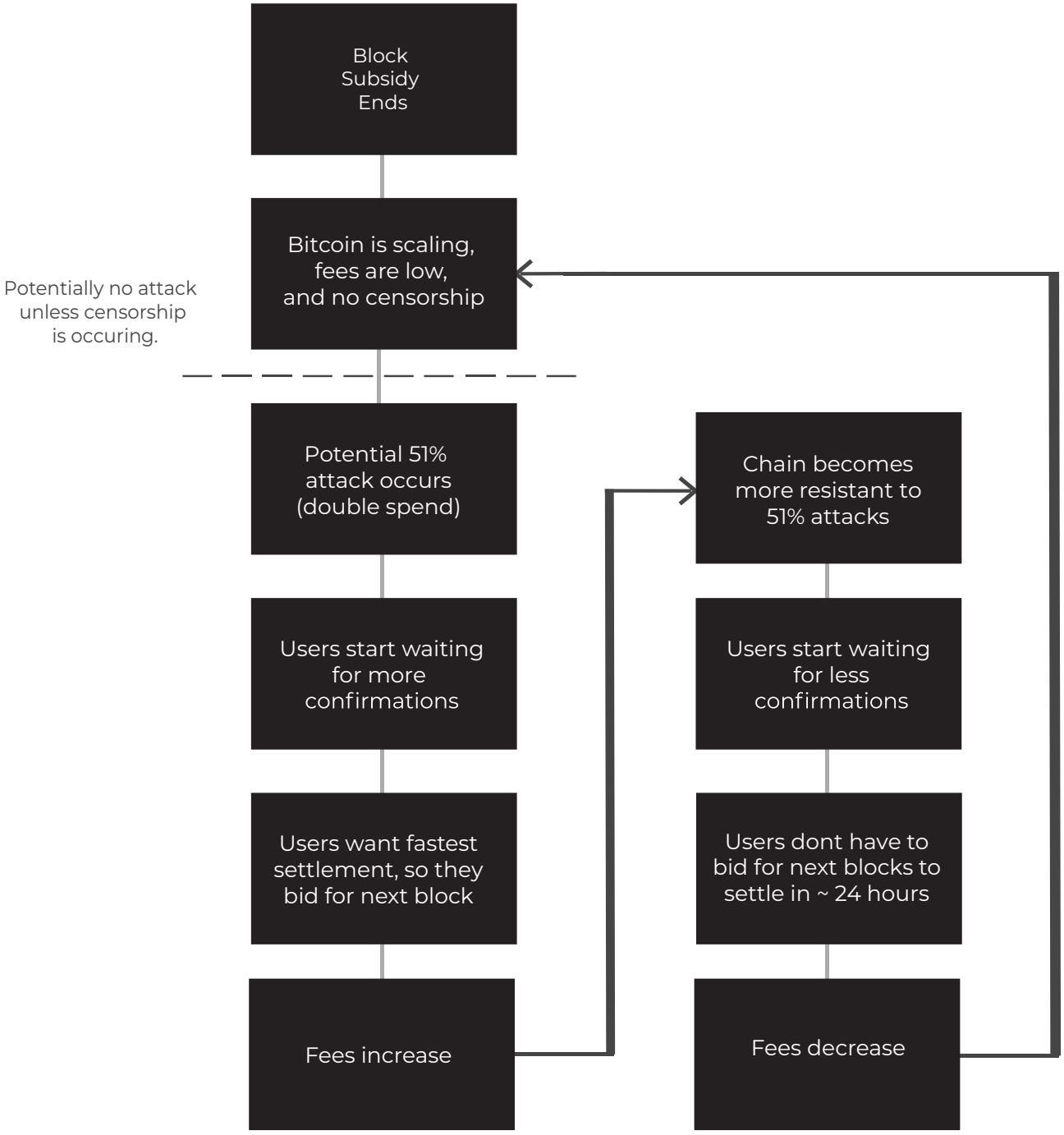
This can happen today and the economic incentive appears to be there for it, but it rarely occurs. Why?

Exchanges and other users now require more confirmations to consider a transaction settled. Some exchanges require 100 confirmations for BCH, which is still less than 24 hours, but it does protect them from double spending by increasing the amount of work, time, and energy that would need to be consumed to perform a 51% attack and reverse a transaction. In conclusion, waiting for enough confirmations increases the assurance of settlement.

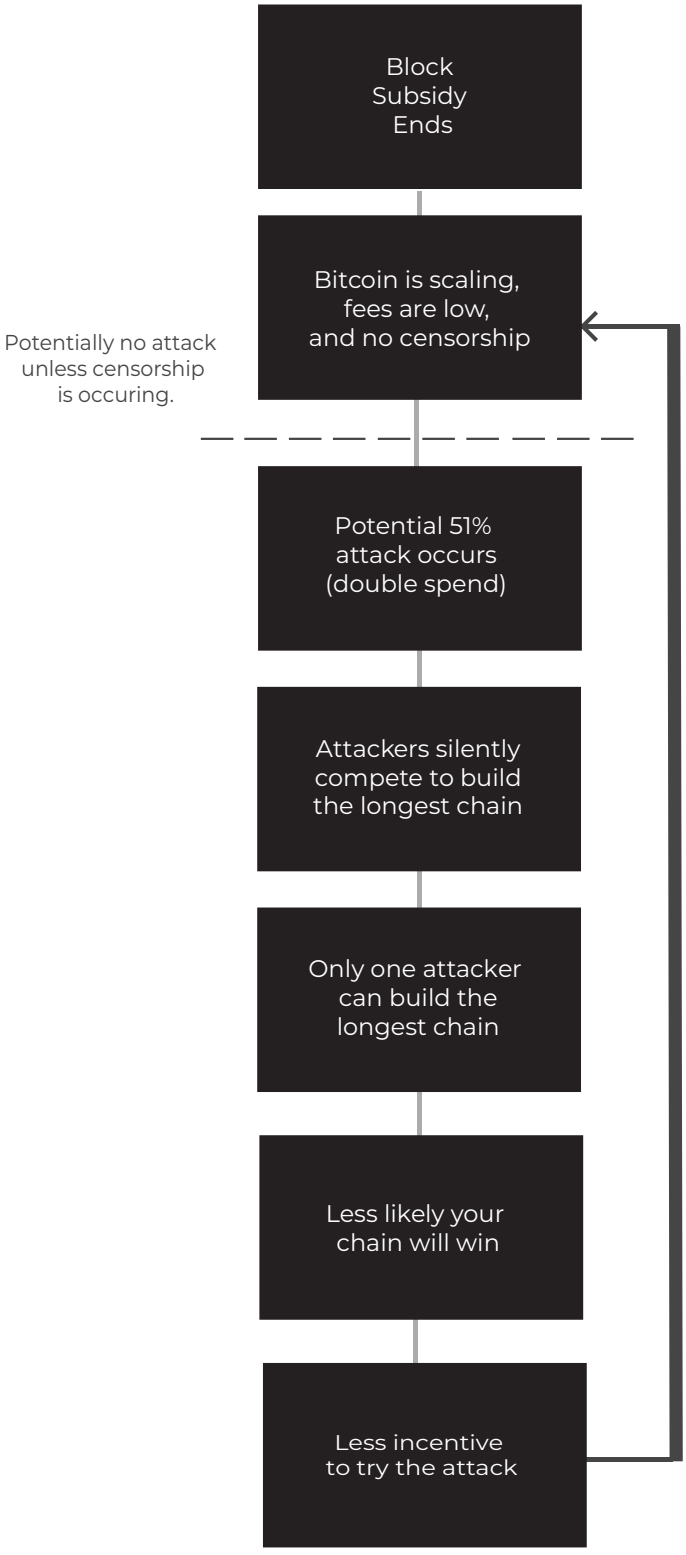
Additionally, with the double spends, the attackers would still owe all their victims money, so they would have to find new victims for the next attack, the attacker would have to be pseudonymous and victims would have to be of high enough value to bother. It is unlikely to be a scalable attack.

On top of that, if users or exchanges deem it critical to wait for a significant number of confirmations to be settled, transactors may be willing to pay the highest fee it takes to get into the next block to avoid waiting even longer than at least the number of required confirmations. Meaning that if the exchange requires 100 confirmations (~ 16.7 hours), and users are in a rush to get their transaction settled, they want those confirmations to start coming in as quickly as possible. They may be willing to pay a high enough fee to get into the very next block. Of course, these higher fees may lead to more users feeling more confident in settlement finality for fewer confirmations, so the market would find a natural equilibrium if there are any issues to begin with.





Yet another example is that if many users are attempting to double spend by 51% attacking the network, all attackers end up competing with each other making it more difficult for each one to be successful. This means that if the chain is actually insecure and double spends are happening (unlikely), double spends would be local only to the entity with more hash power than everyone else. In this example, the other 51% attackers will fail.



Last, most individuals that have the capital to double spend by performing a 51% attack don't have the incentive to do it. They likely own significant BCH, BSV, or BTC. They may not want to potentially damage the integrity of the network that they own a significant amount of.

In short, there's an argument that double spending should already be occurring on blockchains, especially weaker ones. However, they rarely occur in reality due to a variety of reasons just explained, and **these attacks can be mitigated by requiring more confirmations** to enable more confidence in transaction settlement.

In an absolute worst-case scenario, waiting a day (144 confirmations) or a week (1,008 confirmations) for final settlement without relying on any third parties would be highly valuable. Today, Visa and ACH finality is measured in weeks and months and reversals are much easier than purchasing and running a majority of Bitcoin's hash rate. Furthermore, if on-chain transactions are only being used for long-term cold storage and Lightning channels, long delays are not a significant problem for users.

5. Conclusion

In the long run, the market may naturally find an equilibrium for on-chain fees. It could reach a point where there is not much more demand for scaling technology and fees are high enough to avoid censorship after X blocks. When will this occur? Impossible to know, but it's safe to say that Bitcoin's long-term "security" is probable and that miners will likely experience more scaling cycles where they earn a significant amount of transaction fees as Bitcoin adoption accelerates and the use of it as a medium exchange begins.