Bailey, Andrew M., Troy Cross, Joshua Hendrickson, William Luther, Bradley Rettler, and Craig Warmke, 2026. "Bitcoin Works in Practice, but Does It Work in Theory?." *Journal of Private Enterprise*, 41(1): 89-97.

Bitcoin Works in Practice, but Does It Work in Theory?

Andrew M. Bailey*
Yale-NUS College/University of Notre Dame
United States of America

Troy Cross
Red College
United States of America

Joshua Hendrickson
University of Mississippi
United States of America

William Luther
Florida Atlantic University
United States of America

Bradley Rettler
University of Wyoming
United States of America

Craig Warmke
Northern Illinois University
United States of America

Abstract
Hinzen, John, and Saleh (2022) argue that the design of the bitcoin protocol results in a negative network effect. In their view, additional users create network congestion and settlement delays that discourage adoption. This is an interesting theoretical result, but it rests on faulty assumptions about how bitcoin actually works. In particular, the authors fundamentally misunderstand how bitcoin achieves consensus and how the entry and exit of miners affect the timing of new transaction blocks. The authors also ignore existing, widely implemented scaling solutions.

JEL Codes: E42
Keywords: bitcoin, network consensus, scaling of payments

* Murch, Micah Warren, and David Zell provided helpful comments and discussion.

I. Introduction

Millions use bitcoin as a speculative instrument, money, hedge, or safe-haven asset.[1] Dissidents and outsiders prize its censorship-resistance.[2] In fourteen years, it has grown into a network that hosts hundreds of billions of dollars in value. Despite competition from other cryptocurrency projects, it remains dominant along many dimensions.[3] Two countries have even adopted bitcoin as legal tender.[4] How far can this go? Are there technical limits to bitcoin adoption?[5]

Hinzen, John, and Saleh (henceforth HJS) argue in the affirmative.[6] Intriguingly, HJS contend that bitcoin's design engenders a *negative* network effect, whereby increased use of bitcoin for payments creates consensus delays, which in turn prolong time to settlement.[7] The result is taken to imply that *limited adoption* is an equilibrium outcome for bitcoin, meaning it will never serve as a widely used global payments system.

We show that HJS are mistaken. Their fundamental error lies in confusing how bitcoin *actually* achieves network consensus and how bitcoin *actually* scales with a purely theoretical—and factually incorrect—model. Whatever lessons may be derived from their model, they have little application to bitcoin.

II. The Argument

HJS's argument deploys three propositions. First, bitcoin payments require full network consensus for settlement. Second, the addition of miners to bitcoin's network prolongs time to settlement by delaying network consensus. Third, there is an upper bound on bitcoin payments, which derives from limits intrinsic to bitcoin's blockchain.[8]

The argument offered by HJS can be summarized as follows. Suppose use of bitcoin's blockchain for payments rises. As more users compete to have their transactions included in scarce

---

1 See, respectively, Baur, Hong, and Lee (2018), Hazlett and Luther (2019), Blau, Griffith, and Whitby (2021), and Bouri, Molnár, Azzi, Roubaud, and Hagfors (2017).

2 Bailey, et al. (2024).

3 Bailey and Warmke (2023).

4 Cross and Bailey (2023), Raskin (2021), Taylor (2022), BBC (2022).

5 The question here goes beyond familiar inquiries about bootstrapping, on which see Luther (2019).

6 Hinzen, John, and Saleh (2022).

7 On bitcoin's positive, but limited, network effects, see Luther (2016a, 2016b, 2018).

8 Hinzen, John, and Saleh (2022): 348.

blockspace, transaction fees rise (per proposition three). Rising fees incentivize entry of new miners enticed by the prospect of capturing those fees. And new miners slow down network consensus by increasing the likelihood of stale blocks or forks in the blockchain (per proposition two). In the absence of network consensus (per proposition one), payments are less likely to succeed, rendering the network less attractive for use. Thus, from its own design, bitcoin faces barriers to wide adoption.

The argument is straightforward. But all three assumptions are false. The bitcoin modeled by HJS bears little resemblance to bitcoin in reality.

III. Wrong on Scaling

Bitcoin's blockchain is a settlement—or base—layer.[9] Users submit transactions to the network. Then full nodes validate those transactions before miners compete to publish them to bitcoin's blockchain. When a miner has a candidate block of transactions, the full nodes must verify it before they each append the winning block to their own copy of the network's ledger—the blockchain.[10] A block is added approximately every ten minutes, with a total throughput of, at most, around seven settlements per second.[11]

HJS do not seem to realize that bitcoin payments and bitcoin transactions are not the same. While all bitcoin transactions follow the path described above, bitcoin payments often route through other networks, sidechains, and custodial payment systems that straddle bitcoin's blockchain. In doing so, these payments incur clearly defined trade-offs. They may achieve greater speed, privacy, or programmability, but with varying degrees of security. Most importantly, with respect to scaling, these off-chain systems enable users to get around bitcoin's base-layer transactions constraint.

---

[9] Limiting attention to the base layer, Luther and Stein Smith (2020) argue that final-settlement payments are neither centralized nor decentralized; they are distributed. See also Luther (2013, 2014, 2016c, 2020) and Luther and Olson (2015).

[10] For a convincing argument that miners are publishers and nodes are referees, see Warmke (2021).

[11] On these and other details about how bitcoin works, see Antonopoulos (2017), the standard technical manual on bitcoin's base settlement layer.

Consider the lightning network.[12] Lightning is an open-source, peer-to-peer payment network operating atop the bitcoin blockchain, much in the way that payment services like Visa and PayPal run atop the dollar base layer. Whereas final settlement for Visa and PayPal requires transferring physical cash or digital balances held at the Federal Reserve, final settlement for lightning takes place on the bitcoin blockchain. Lightning nodes stand in a mesh network, with each lightning node connected to some others by way of payment channels.[13] A sender need not have a direct payment channel to a target node. The sender only needs a path of channels to the recipient node. Lightning payments are fast, typically taking from mere milliseconds to a few seconds. They are also cheap, with typical fees of less than $0.01 per transaction.

Crucially, lightning payments do not require full consensus on the bitcoin network for finality. Lightning stands in stark contrast to the bitcoin base layer it sits atop in this regard. For an on-chain bitcoin transaction to settle, the entire network must recognize it as valid. For a lightning transaction to settle, only the lightning nodes involved must agree. Each payment channel on the lightning network requires one base-layer transaction to open and one base-layer transaction to close. But, once the payment channels exist, there is no technical constraint on the lightning network's transaction rate beyond familiar limits that restrict all internet traffic—the speed of light, latency and throughput for node connections, and so on.

With these details in hand, observe how bitcoin scales to accommodate more payments. While the main settlement layer has technical limits for bitcoin *transactions*, layers built on top of bitcoin, like lightning, have technical limits for *payments* that are well beyond those of Visa and Mastercard. Payments need only settle infrequently to the base layer, the bitcoin blockchain. These payment mechanisms, again, do not inherit bitcoin's intrinsic speed limit. The limit of around seven settlements per second noted above applies only to the bitcoin blockchain, not to the lightning payments layer, which can process thousands of payments per second.[14]

---

[12] The standard technical manual for lightning is Antonopoulos, Osuntokun, and Pickhardt (2021).

[13] For up-to-date statistics on lightning network nodes and channel capacity, see ML.com.

[14] There has been considerable controversy regarding the parameters that govern bitcoin's base settlement layer; see Bier (2021). The fundamental rationale for the current parameters, despite the speed limits they impose, is that a light base layer

A single on-chain bitcoin settlement can also include multiple inputs and outputs, which allows for scaling through payment *batching*. Users who need to make several payments can effectively send bitcoin to multiple destinations in one transaction. On the blockchain, this shows up as one transaction, though it would count as multiple transactions when using almost any other form of payment. This is significant because one on-chain transaction could be used to send bitcoin to hundreds of different people. The most obvious use case is when an exchange or other custodian processes dozens or even hundreds of bitcoin payments in just one blockchain settlement transaction. Here, as with bitcoin payments over lightning, there is no 1:1 relationship between on-chain transactions and actual payments, and so limits on the former do not impede the latter. Users can also perform collaborative settlements that mix and match inputs and outputs without the aid of any custodian in order to achieve better privacy and more efficient use of blockchain space, once again breaking any 1:1 link between on-chain transactions and payments.[15]

For the above reasons, proposition one is false. Not all bitcoin payments require full network consensus. The only agreement required to settle an off-chain payment is between the nodes involved. Other network nodes may not even see the payment, much less track and verify it on their own ledgers.

Proposition three is also false. The settlement layer's transaction limits do not restrict the flow of payments, which can take place on off-chain. Off-chain payment channels can process a nearly infinite amount of payments with just two on-chain transactions: one to open and one to close the channel. In this way, lightning payments bypass the consensus bottlenecks intrinsic to the bitcoin base layer. Batched payments similarly facilitate routing around those bottlenecks.

IV. Wrong on Mining and Consensus

There is an even bigger problem with HJS's argument: It misconstrues how the bitcoin network achieves consensus and falsely claims that the addition of new miners slows down that process.

According to HJS, "The mining network's free entry condition then implies that additional miners enter the network. The resulting

---

permits anyone to operate a network node at low cost. This in turn enables a widely distributed payments network that is difficult to censor or control, bitcoin's most fundamental value proposition.

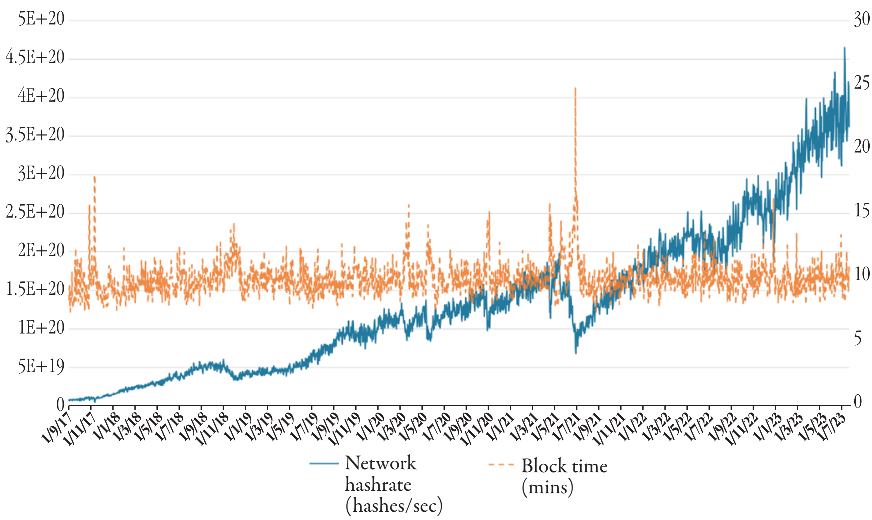
[15] For the latest on bitcoin privacy techniques along these lines, see Ficsór, Kogman, Ontivero, and Sere (2021). See also Hendrickson and Luther (2022).

network expansion exacerbates network delay which, due to the need for consensus, prolongs expected user wait times."[16]

Note that this second proposition makes an empirical prediction about block times (i.e., how long it takes for the network to achieve consensus on its latest batch of transactions). Were it correct, we would expect to see any addition of new mining (and, thereby, the increase in hashrate—the cycles of an algorithm per second—across the network) to result in longer block times.

In fact, we have not observed longer block times as hashrate has increased over time. Consider the last five years, for example. In this time, hashrate has increased by orders of magnitude.[17] In the same period, the network continued to publish a block around every ten minutes. Nor have we seen that a drop in hashrate—that is, a loss in mining—leads to faster network consensus, and shorter block times, as HJS imply. In fact, the opposite happened in historic fashion with China's April 2021 ban on bitcoin mining. At that time, the associated historic drop in hashrate led to a temporary *increase* in block time. Again, this is precisely the opposite of what one would expect from HJS's model.

Figure 1. Network hashrate and block time, 2017–23[18]



[16] Hinzen, John, and Saleh (2022): 348.
[17] Bitcoin miners together computed around 7,572,423,973,014,190,000 hashes per second on September 1, 2017, and around 363,000,000,000,000,000,000 hashes per second on July 21, 2023; see figure 1.
[18] Figure 1 is the authors' work, with data drawn from BitInfoCharts.com.

Anyone with passing familiarity with the bitcoin protocol knows exactly why the secular rise in hashrate over the last five years has not resulted in a secular drop in block time: the difficulty adjustment. Every 2,016 blocks (roughly every two weeks at ten minutes per block), the bitcoin network adjusts the difficulty to win the competition to publish a block. Every 2,016 blocks, the software looks at how quickly the previous 2,016 blocks were published and sets the difficulty level for the next 2,016 blocks. When blocks arrive substantially quicker than every ten minutes, the network raises the difficulty. When blocks arrive substantially slower than every ten minutes, the network lowers the difficulty. At times of rapid increase or decrease of hash rate, blocks can come more or less often than every ten minutes. But that only ever happens for about two weeks (2,016 blocks); at that point, the difficulty adjusts.

What's more, consider stale blocks (i.e., valid blocks excluded from the blockchain when network nodes fall out of consensus). From January 2020 to September 2022, for example, just forty-four stale blocks were visible to one well-connected node run by researchers.[19] And this rarity is exactly as one should expect: Mining a bitcoin block is *expensive* (on the order of tens to hundreds of thousands of US dollars). Miners would discontinue or dial down operations were stale blocks much more frequent. We can empirically verify that an increase in hashrate does not substantially increase the incidence of stale blocks.

Proposition two is false. HJS misstate the relationship between increased hashrate and network consensus. The addition of miners to bitcoin's network does not prolong time to settlement by delaying network consensus, nor does the addition of miners to bitcoin's network increase the frequency of stale blocks.

V. Conclusion

HJS's argument establishes the following already well-known fact: Even with tweaked parameters, bitcoin's blockchain does not scale well for on-chain payments. This has been known since soon after bitcoin's creation. The current parameters allow for ten-minute block

---

[19] See https://forkmonitor.info/feeds/stale_candidates/btc.rss. Since some stale blocks fail to propagate across the entire network, there can be slight variations in visibility of stale blocks from node to node. Across that interval, for comparison, there were over 138,000 ordinary (non-stale) blocks recognized by all nodes.

times, with each block typically containing between 1 and 4 MB of data—roughly 1,800 to 4,200 transactions (which, again, is not the same as 1,800 to 4,200 payments) every ten minutes. At these parameters, the authors concede, the probability of forking is near zero. What the mathematics predicts is supported empirically; forks do happen, but very infrequently.

HJS further claim that a dramatic increase in transaction volume would cause frequent forks, no consensus, and an unusable network. But they are tilting at windmills: Bitcoin scales through off-chain payments, not by increasing throughput at the base layer.[20] Off-chain protocols afford more scalability precisely because they do not require consensus of the entire network. Hence, the limited-adoption thesis HJS advance should be interpreted only in the strictest terms: As the number of would-be bitcoin users approaches infinity, the proportion that will successfully transact on the base layer approaches zero. Given the current bitcoin parameters, this should surprise no one; the quotient of any fixed number and a denominator going to infinity goes to zero.

Bitcoin has many fascinating lessons for interdisciplinary researchers willing to put in the work.[21] Responsible research on bitcoin should attend to the actual characteristics of the protocol and scaling solutions that have been proposed or adopted. In doing so, it might aid in better understanding those scaling efforts, their effects, and their limits.[22] HJS fall far short of this ideal.

References

Antonopoulos, Andreas M. 2017. *Mastering Bitcoin*. 2nd ed. Boston: O'Reilly.

Antonopoulos, Andreas M., Olaoluwa Osuntokun, and René Pickhardt. 2021. *Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments*. 1st ed. Boston: O'Reilly.

Bailey, Andrew M. and Bradley Rettler and Craig Warmke. 2024. *Resistance Money: A Philosophical Case for Bitcoin*. Routledge.

Bailey, Andrew M. and Craig Warmke. 2023. "Bitcoin Is King." In *Cryptocurrency: Concepts, Technology, and Issues*, ed. J. Liebowitz, 175–97. Taylor & Francis.

BBC. 2022. "Bitcoin Becomes Official Currency in Central African Republic" *BBC News*.

[20] The mistake here—supposing that bitcoin scales only by increasing transaction throughput at the base layer—is repeated in Malik et al. (2022). As with HJS, their argument fails to find a real-world target. For bitcoin, like traditional payment systems, scales in layers, not merely by clogging the base settlement network with more transactions.

[21] Ray (forthcoming).

[22] Sztorc (2022) is exemplary.

Bier, Jonathan. 2021. *The Blocksize War: The Battle over Who Controls Bitcoin's Protocol Rules*.

Blau, Benjamin M., Todd G. Griffith, and Ryan J. Whitby. 2021. "Inflation and Bitcoin: A Descriptive Time-Series Analysis." *Economics Letters*, 203: 109848.

Baur, Dirk G. and KiHoon Hong, and Adrian D. Lee. 2018. "Bitcoin: Medium of Exchange or Speculative Asset?" *Journal of International Financial Markets, Institutions and Money*, 54: 177–89.

Bouri, Elie and Peter Molnár, Georges Azzi, David Roubaud, and Lars Ivar Hagfors. 2017. "On the Hedge and Safe Haven Properties of Bitcoin: Is It Really More than a Diversifier?" *Finance Research Letters*, 20: 192–98.

Cross, Troy and Andrew M. Bailey. 2023. "Carbon-Neutral Bitcoin Adoption for Nation States." In *Financial Cryptography and Data Security*, ed. S. Matsuo et al., 55–65. Springer.

Ficsór, Ádám and Yuval Kogman, Lucas Ontivero, and István András Sere. 2021. "WabiSabi: Centrally Coordinated CoinJoins with Variable Amounts." *Cryptology ePrint Archive*.

Hazlett, Peter K., and Luther, William J. 2019. "Is Bitcoin Money? And What That Means." *Quarterly Review of Economics and Finance*, 77: 144–49.

Hendrickson, Joshua R., and Luther, William J. 2022. "Cash, Crime, and Cryptocurrencies." *Quarterly Review of Economics and Finance*, 85: 200–207.

Hinzen, Franz J., Kose John, and Fahad Saleh. 2022. "Bitcoin's Limited Adoption Problem" *Journal of Financial Economics*, 144: 347–69.

Luther, William J. 2013. "Friedman Versus Hayek on Private Outside Monies: New Evidence for the Debate." *Economic Affairs*, 33(1): 127–35.

Luther, William J. 2014. "Synthesizing State and Spontaneous Order Theories of Money." *Advances in Austrian Economics*, 18: 161–78.

Luther, William J. 2016a. "Bitcoin and the Future of Digital Payments." *Independent Review*, 20(3): 397–404.

Luther, William J. 2016b. "Cryptocurrencies, Network Effects, and Switching Costs." *Contemporary Economic Policy*, 34(3): 553–71.

Luther, William J. 2016c. "Mises and the Moderns on the Inessentiality of Money in Equilibrium." *Review of Austrian Economics*, 29(1): 1–13.

Luther, William J. 2018. "Is Bitcoin Intrinsically Worthless?" *Journal of Private Enterprise*, 33(1): 31–45.

Luther, William J. 2019. "Getting Off the Ground: The Case of Bitcoin" *Journal of Institutional Economics*, 15(2): 189–205.

Luther, William J. 2020. "Four Principles for a Base Money Regime." *Cato Journal*, 40(2): 533–45.

Luther, William J., and Stein Smith, Sean. 2020. "Is Bitcoin a Decentralized Payment Mechanism?" *Journal of Institutional Economics*, 16(4): 433–44.

Malik N, Aseri M, Singh PV, and Srinivasan K. 2022. "Why Bitcoin Will Fail to Scale?" *Management Science*, 68(10): 7065–7791.

Raskin, Max. 2021, June 15. "A Global First: Bitcoin as National Currency." *Wall Street Journal*.

Ray, Korok. Forthcoming. "Bitcoin and the Academy." *Journal of Investing*.

Sztorc, Paul. 2022. "Lightning Network—Fundamental Limitations."

Taylor, Luke. 2022. "The World's First Bitcoin Republic." *New Scientist*, 253: 14.

Warmke, Craig. 2021. "What Is Bitcoin?" *Inquiry*, 1–43.