arrington
CAPITAL

Life After Taproot:

The Coming Age Of Narratives For Bitcoin Innovation & Governance

October 20, 2021

“The nature of Bitcoin is such that once version 0.1 was released, **the core design** was set in stone for the rest of its lifetime.

…I don't believe a second, compatible implementation of Bitcoin will ever be a good idea.”

-Satoshi Nakamoto

Disclosure

Arrington Capital and/or its affiliates (collectively “Arrington Capital”) has a financial interest in the success of the Bitcoin ecosystem. Arrington Capital currently owns BTC, and actively trades Bitcoin.

As of the publication date of this report, Arrington Capital, others that contributed to this report, are supporters of the Bitcoin Ecosystem and stand to realize gains through various manners of participation. All content in this report represents the opinions of Arrington Capital. Arrington Capital has obtained all information herein from third-party sources they believe to be accurate and reliable, including the Bitcoin Ecosystem. Third-party sources may not have been independently verified and its accuracy or completeness cannot be guaranteed and not be relied upon as such. Information is presented “as is”, without warranty of any kind – whether express or implied.

This document is for informational purposes only and is not intended as an official recommendation or confirmation of any transaction. The information contained herein does not take into account the particular investment objectives, regulatory status or financial circumstances of any specific person who may receive it. All market prices, data and other information are not warranted as to completeness or accuracy, are based upon selected public market data, and reflect prevailing conditions and Arrington Capital’s views as of this date, all of which are accordingly subject to change without notice. Arrington Capital has no obligation to continue offering reports regarding the project. Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances.

Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. This report’s estimated fundamental value only represents a best efforts estimate of the potential fundamental valuation of a specific token, and is not expressed as, or implied as, assessments of the quality of a token, a summary of past performance, or an actionable investment strategy for an investor.

This document does not in any way constitute an offer or solicitation of an offer to buy or sell any investment or token discussed herein.

The information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond Arrington Capital’s control. Investors should conduct independent due diligence, with assistance from professional financial, legal and tax experts, on all tokens discussed in this document and develop a stand-alone judgment of the relevant markets prior to making any investment decision.

By accepting this information the recipient agrees and acknowledges that no duty is owed to the recipient by Arrington Capital. The recipient expressly waives any claims arising out of the delivery of the information or the recipients use thereof or reliance thereon.

Executive Summary

Taproot is the first change to Bitcoin since 2017. It will introduce Schnorr signatures, Merkelized Alternative Script Trees (MAST) and a reformed scripting language known as Tapscript. Collectively, these upgrades will make the Bitcoin codebase simpler and unlock a number of new capabilities.

Taproot enables *key aggregation*: complex multi-sig transactions will now look like uni-sig transactions on-chain. Bitcoin thus becomes "more private", obscuring complex transaction types from blockchain sleuths. In addition, Taproot makes Bitcoin more efficient by unlocking *batch verification*: nodes more efficiently verify complex transaction types powered by Schnorr signatures. Finally, Tapscript enhances the capabilities of Schnorr while introducing opcodes that make future upgrades more flexible.

In summary, Taproot makes Bitcoin more private, scalable and secure. It is a non-contentious soft fork. An overwhelming majority of participants agree that Taproot improves Bitcoin. Beyond these technical contributions, Taproot could represent a turning point for narratives in Bitcoin innovation and governance.

We are more compelled by Taproot as a catalyst for Bitcoin governance than the idea that Taproot is a revolutionary technology. The upgrade makes marginal contributions to the protocol, but could more importantly catalyze the next major themes in Bitcoin politics. The post-Taproot era leaves behind the PTSD of 2017's Block Wars, highlighting the continued vibrancy of Bitcoin's political body.

As the crypto cycle progresses, the market has taken to the idea that Bitcoin is "stuck", outpaced by innovation elsewhere. Participants interpret post-2017 conservatism as stagnation. We have a fundamentally different take: that Bitcoin politics is more alive than ever before, and that Taproot debates capture this aliveness. Taproot's activation will be the culmination of four years of discussion following 2017. Despite being non-contentious, the upgrade has spurred a fresh discussion on how to digest 2017's lessons and juggle power between developers, miners and nodes going forward.

This post-Taproot era introduces new opportunities for Bitcoin evolution, but also highlights growing risks. As Bitcoin enters the sphere of nation state actors and powerful technologists, the network will face new pressures. We speculate that high-trust and well-resourced actors will lead fresh proposals for change that appear far more "reasonable" than the proposals in 2017's civil war. These could represent covert threats to Bitcoin's political stability. The debate between technical hardliners and progressive incumbents will likely intensify over the coming year, again shining a light on the robust nature of Bitcoin governance and potentially making the protocol more defensible in the long run.

The next set of debates about stability versus change will force hardliners to sharpen their defense of Bitcoin's non-negotiables, while motivating incumbents to pursue fresh and increasingly aggressive narratives about evolution.

Within this new chapter for Bitcoin, we think the network will slowly find its place in broader Layer 1 (L1) and Layer 2 (L2) developments, at some point defining its identity in the new "multi-chain" landscape. Taproot (in our view) doesn't introduce "Bitcoin-native DeFi" or "smart contracts on Bitcoin", but it will likely motivate burgeoning L1s and mobile, multi-chain developers to explore Bitcoin-centric innovation. This presents new opportunities as well as new risks – how the network digests these discussions will be an important signal going forward. At the same time, Taproot's contribution to the privacy of Lightning channels could further invigorate Bitcoin's L2 story, just as the Lightning network shows signs of a mainstream "breakout".

Contents

1 A Macro Thesis For Taproot

Taproot is the first change to the Bitcoin protocol since the Segwit upgrade in 2017. The upgrade encompasses three separate `Bitcoin Improvement Proposals (BIPs)`: `BIP340`, `BIP341` and `BIP342`.

1. `BIP340`[1] replaces Elliptic Curve Digital Signature Algorithm (ECDSA) with Schnorr Signatures
2. `BIP341`[2] introduces Merkelized Alternative Script Trees (MAST)
3. `BIP342`[3] reforms Bitcoin's scripting language through "Tapscript".

In aggregate, Taproot takes advantage of the capabilities unlocked by Schnorr, making new, complex transaction types possible on-chain. In subsequent sections, we cover how Taproot makes Bitcoin more private, secure and scalable.

Our thesis is less about Taproot as a technological leap and more focused on what a post-Taproot era could look like. Over the past year, the market has been lulled into a quiet skepticism toward Bitcoin. The market is captivated by a flurry of new narratives which characterize Bitcoin as the least innovative asset in crypto. Participants focus on the idea that there is Bitcoin – a community in stasis, stuck in an anti-innovation bronze age – and there is the rest of the market, the spearhead for mass adoption, fresh ideas and developer energy.

Bitcoin took the backseat to emerging forces in crypto macro. Ethereum arguably underwent its most important monetary pivot, embracing the ethos of "ultrasound money" and swinging at Bitcoin's leadership through `EIP1559`. As Ethereum challenged Bitcoin, the L1 wars demonstrated the fundamental portability of ecosystems and developers. The hunt for "fast DeFi" accelerated an interplay between L1 and L2, as new base layers pushed Ethereum to surmount its own scalability counter-attacks. The explosion of NFTs recast crypto as not just a financial asset class, but one that could fundamentally change popular culture.

Bitcoin underperformed all of these idiosyncratic and thematic trends. As a result, the market converged on a foregone conclusion that *Bitcoin is stuck*. The close-mindedness of Bitcoin would make this lag indefinite and even threaten to unseat its leadership in the long run.

In our view, this skepticism not only overlooks the continued vibrancy of Bitcoin governance, but could be discounting an upcoming turning point for the network: life after Taproot.

The Taproot upgrade will go into effect on or around November 16th: `Block 709,632`[4]. Four years in the making, Taproot is a non-contentious proposal, which leaves behind the scar tissue of the Block Wars[5] and shows the market that Bitcoin can evolve while still maintaining an ethos of extreme political stability.

A post-Taproot era could mark a new technical, political and cultural epoch for Bitcoin. Taproot digests the aftermath of the Block Wars, where the very idea of a soft fork brought back miserable memories of

[1] URL: https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki.

[2] URL: https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki.

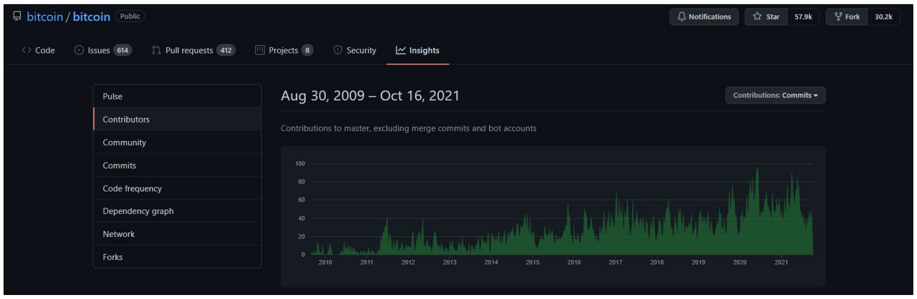
[3] URL: https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki.

[4] URL: https://bitcoinops.org/en/preparing-for-taproot/.

[5] We refer to the "Block Wars" as the debate about increasing the Bitcoin block size in 2017, which eventually culminated in the Segwit2x hard fork and the birth of the BCH child-chain. (URL: https://en.bitcoin.it/wiki/Block_size_limit_controversy)

2017 hostility. The Full Nodes claimed victory over the Miners, declaring Bitcoin Independence Day[6], but quickly thereafter retreated into a heightened guard of conservatism. The pace of technical discussions slowed, replacing evolvability with hardline stasis – all change could result in existential conflict.

We believe this conservatism will pay dividends as a necessary set up for the post-Taproot era. Critics who label Bitcoin "stagnant" are not only missing the vibrancy and evolution of the soft-fork design space since 2017, but the nuance of what innovation on Bitcoin means. Innovation is not radical experimentation; it is a cautious political juggle between networks who each have their own way of vetoing proposals – a perpetual power struggle between Miners, Developers and Full Nodes.



Aug 30, 2009 – Oct 16, 2021

Contributions to master, excluding merge commits and bot accounts

Figure 1: Far from "dead", Bitcoin code development is the most active it has ever been. Total number of contributions to Bitcoin master repository[7].

We think the market is likely underpricing the vibrancy of Bitcoin governance, mistaking the fact that there have been no core changes for a sense of decay. Despite being non-contentious, Taproot has catalyzed a lengthy debate. For the most part, the debate has nothing to do with the upgrade – it is a heated back-and-forth about the meta-questions that underpin any change to Bitcoin. How should change be proposed and activated? Who should have the final say? If push comes to shove, do Miners or Nodes control the destiny of the network? Taproot's activation digests the nuances of Bitcoin governance while consolidating precedents from 2017: it turns the ugly civil war into something that helps Bitcoin going forward. Bitcoin can finally leave behind the PTSD of the Block Wars and embrace a new epoch of openness – closing one chapter and opening a new one – without forgetting the existential nature of technological utopianism.

Beyond what *Taproot could do* – which we will cover in this report – we think the real value is in *what Taproot could mean.* The upgrade could be a macro turning point for evolvability and innovation, merging the best of post-Segwit conservatism with the energy of new beginnings. It is a meta-upgrade, a chance to redefine what it means to contribute to Bitcoin, whether one is a Miner, Developer or Full Node. Taproot undermines the critique of Bitcoin as a slow and backward "boomer asset". It reframes the post-2017 era of hardline conservatism as a necessary prequel to the protocol's mainstream era, where it can cautiously embrace important changes without being hijacked by new and increasingly powerful participants.

Taproot could not come at a more important moment. Bitcoin is quickly progressing into the sphere of nation states, powerful technologists and international financiers. An unprecedented powerbase of new adopters have entered crypto. They could pose far more sophisticated and credible attacks than the chaotic band of OGs and miners in 2017. Just in the past year, some countries attacked Bitcoin and others waved Bitcoin as their flag of financial sovereignty – the polar scenes range from hashpower

[6] URL: https://coingeek.com/happy-bitcoin-independence-day-2020/.
[7] URL: https://github.com/bitcoin/bitcoin/graphs/contributor.

destruction in China to a ritualized presidential embrace in El Salvador.

Taproot is an important milestone for network defensibility, motivating new pressures on Bitcoin, and likely spurring more vigilance and engagement from its political core. The network is now interacting with the international political system in ways that are a step change from 2017. As Bitcoin becomes mainstream, there will be a greater push to tweak Bitcoin; *to keep Bitcoin with the times.* Well-capitalized actors could spend years accumulating social and economic capital within the Bitcoin community only to (knowingly or unknowingly) ally with adversaries, motivated by "reasonable" narratives like ESG, Scalability or DeFi. We think that without a new era of governance and political vibrancy, these attacks have higher odds of success. Taproot is thus not just a consolidation of Bitcoin's governance learnings after 2017, but a necessary step in Bitcoin antifragility, mobilizing the political process and better positioning the protocol against the next BCH-style civil war, likely far more credible, capitalized and covert.

Narratives for change are on the horizon. After the Block Wars, Bitcoiners had the luxury of walling off the protocol from the outside world, dismissing all change. In the post-Taproot era, we expect to see more soft fork proposals. Even if Taproot is a change around the periphery, going from zero change to activating Taproot is a large *rate of change* for Bitcoin. Its non-contentious nature will likely make the landscape for proposals less hostile going forward. This is captured by Taproot's activation path – converging on `Speedy Trial`, an iterative direction premised on the idea of "failing fast".

Is Bitcoin's soft fork design robust enough to prevent a new wave of child-chains that suck value away and destroy consensus while still embracing *good, non-contentious change* like Taproot? How will Bitcoin avoid another seductive Frankenstein moment? How can Bitcoin juggle the need to evolve without undermining its extreme political stability?

There is no clear answer to any of these open questions, but a healthy and robust environment for both formal `BIPs` and informal political debates is crucial to navigate them. Taproot has been the main expression of this political vibrancy since 2017.

Beyond this macro and cultural turning point, Taproot could also mark an end to Bitcoin isolationism within broader L1 and developer ecosystems. The L1 wars captured the malleability of "developer moats", establishing a multi-chain world beyond Ethereum. After Taproot, we can envision more L1s trying to interact with Bitcoin and unlock the "Bitcoin economy". If L1s can functionally add value to Bitcoin without threatening its security model, the Bitcoin "builder" ecosystem could grow rapidly. We are not convinced that Taproot *technically* lives up to the idea of "DeFi on Bitcoin" or "smart contracts on Bitcoin" – we see this as Bitcoiners making a similar mistake as Ethereans clinging to `EIP1559` as a way to compete against Bitcoin. Nonetheless, going from very little change to a major change could be a very strong signal for new engineers.

This potential interaction with the L1 narrative also aligns with the emergence of Bitcoin L2, rapidly finding product-market fit in Latin America. Taproot makes some incremental improvements to Lightning, making Lightning more private and possibly more palatable for mainstream, large-scale adoption. Ethereum has thus far built a rich ecosystem of L2s, and we don't think Bitcoin L2 is necessarily comparable (given that Bitcoin L1 is not highly programmable). There is nonetheless a Bitcoin-native L2 story worth exploring, one that again dispels the market's critique that there is "no innovation on Bitcoin".

2 Bitcoin's Public Forum: Debates In Soft Fork Design

We are particularly excited about Taproot because of how it has re-invigorated debates about soft fork design and highlighted the Socratic nature of Bitcoin governance. We think the market is underestimating the richness of today's soft fork design and `Bitcoin Improvement Proposals (BIPs)`. As demonstrated by Taproot, even a non-contentious proposal can elicit ferocious discussion and motivate the community to game out how any one direction could establish good or bad precedent in the future across all of Bitcoin's stakeholders.

`BIPs` are proposals put forward by Bitcoin developers to change Bitcoin's codebase. Once code is written, reviewed, tested, and merged, Bitcoin nodes decide if and how to activate the upgrade. Most debates about governance focus on how to determine if consensus has been reached, how to rely on miner and node signaling and how to manage node adoption after the upgrade has been approved (minority rights and backward compatibility).

2.1 Bitcoin As Decentralized Common Law

The back-and-forth behind `BIPs` is like a system of decentralized common law. The community iterates on *how to do an upgrade* and the outcome of this deliberation – from proposal to activation – creates precedent that can be referred to in the future. We saw this process of canonical, decentralized law-making in 2017. One of the network's most powerful fallbacks was strengthened by `BIP148`[8]: on August 1, Full Nodes signalled that they would move forward with Segwit *without* 95% miner signalling, countering norms established by other `BIPs`. This was a `User Activated Soft Fork`[9] `(UASF)` which established *forced signaling* as the network's ultimate insurance policy. Bitcoin users declared sovereignty over the network in an attempt to defend against undue miner and corporate influence, contrasting the idea of a `Miner Activated Soft Fork`[10] where miner signaling plays a stronger role.

`BIP148` was a powerful moment in Bitcoin history: it demonstrated that the Bitcoin Full Nodes could exercise the final say. It reminded Miners that they "work for the network", they don't "rule the network". Earlier in the year, the largest mining, corporations and exchanges in Bitcoin lobbied to double the size of Bitcoin blocks. `UASF`-advocates characterized this as a backdoor attempt to hijack Bitcoin, captured by the backdoor-nature of the "New York Agreement[11]" (NYA), when various powerbrokers gathered together to push for bigger blocks. In the end, `BIP148` was not just a decisive defeat to the NYA, but a reminder that at any point, the Full Nodes can "pull out the big guns" and pursue high-risk strategies to reassert user control.

The `UASF` camp is one contingent in Bitcoin politics. They take the hardline stance that while miner signalling can help drive the adoption of an upgrade and help with backward compatibility for nodes who haven't yet adopted the change, nodes should have the final say. They argue that miner signaling is more procedural than substantive, *that power does not ultimately rest with the miners.*

Other factions have criticized this approach as "playing chicken" with the network, viewing forced signalling like `BIP148` as high-risk[13]. It can splinter hashpower and reduce base layer security. These

[8] URL: https://github.com/bitcoin/bips/blob/master/bip-0148.mediawiki.

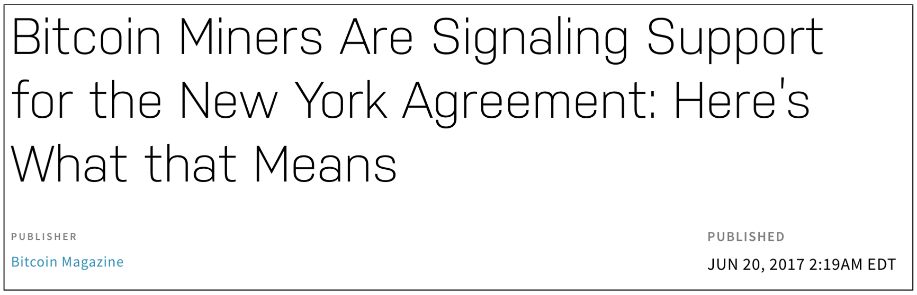
[9] URL: https://stephanlivera.com/episode/260/.

[10] URL: https://wiki.trezor.io/Soft_fork.

[11] URL: https://en.bitcoin.it/wiki/New_York_Agreement.

[12] URL: https://en.bitcoin.it/wiki/New_York_Agreement.

[13] URL: https://stephanlivera.com/episode/257/.



Bitcoin Miners Are Signaling Support for the New York Agreement: Here's What that Means

PUBLISHER
Bitcoin Magazine

PUBLISHED
JUN 20, 2017 2:19AM EDT

Figure 2: In May of 2017, over fifty of the largest miners, exchanges and financial institutions gathered to broker the "New York Agreement", collectively agreeing to double Bitcoin's block size[12].

camps are more likely to support the ethos of BIP9[14], which begins by surveying miner support, vetoing proposals if miner signalling doesn't reach 95% by the end of the expiration period.

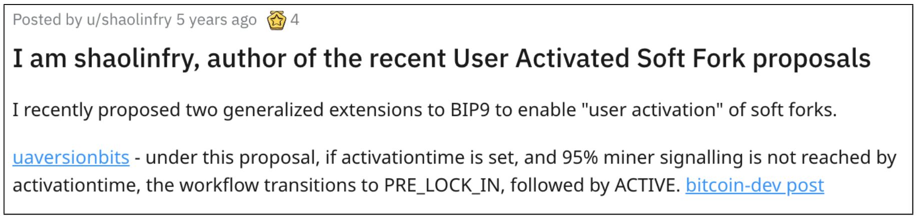
2.2 Miner Or Node Veto: True Or False?

The debate gets interesting when comparing BIP9's methodology to a particular variant of BIP8: BIP8 LOT = true. This also starts by surveying miner signalling. Where they differ is *what should happen if miner support is insufficient.* BIP9, more conciliary with Miners, states that the upgrade should be vetoed. BIP8 LOT = true states the case for Full Node self-sovereignty: the upgrade should pass anyway after a sufficient delay period.

BIP8, which resurfaces in the Taproot discussion, is arguably closer to 2017's radical UASF camp than the conciliatory BIP9 approach.

A distinct quality of Bitcoin governance is its fractured, decentralized nature. Documentation is scattered and procedure is uncodified. There is no Foundation or corporate entity to steer the ship and determine which BIP is or isn't authoritative. There is no "constitution" that states how governance should be done: there are different open-source proposals, but each upgrade will by definition induce a fresh round of discussion.

Beyond various BIPs, a rich discourse is scattered across obscure email lists, Bitcoiner forums and informal blog posts. 2017 highlights this point: UASF was born on Reddit, proposed by an anonymous developer named Shaolinfry[15].



Posted by u/shaolinfry 5 years ago 4

I am shaolinfry, author of the recent User Activated Soft Fork proposals

I recently proposed two generalized extensions to BIP9 to enable "user activation" of soft forks.

uaversionbits - under this proposal, if activationtime is set, and 95% miner signalling is not reached by activationtime, the workflow transitions to PRE_LOCK_IN, followed by ACTIVE. bitcoin-dev post

Figure 3: Shaolinfry's original UASF post[16].

This relatively unorganized literature is where contributors hash out the challenges of decentralized governance. We think the market doesn't appreciate this discussion partly because of how fragmented

[14] URL: https://en.bitcoin.it/wiki/BIP_0009.
[15] URL: https://www.reddit.com/r/Bitcoin/comments/5zsk45/i_am_shaolinfry_author_of_the_recent_user/.
[16] URL: https://www.reddit.com/r/Bitcoin/comments/5zsk45/i_am_shaolinfry_author_of_the_recent_user/.

and decentralized this discussion has become. Possibly in the aftermath of 2021's L1 wars, the market has become accustomed to the "benevolent dictatorship" approach to protocol governance[17].

One example of an informal governance proposal is Matt Corallo's `Modern Soft Fork Activation`[18], which tries to outline five "basic requirements" for soft fork design:

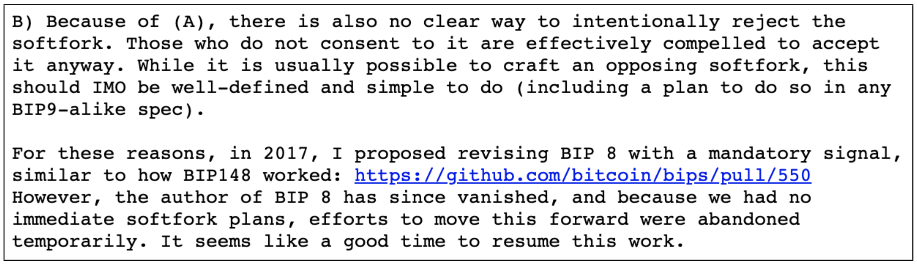
1. *Avoid activating in the face of significant, reasonable, and directed objection.*
2. *Avoid activating within a timeframe which does not make high node-level-adoption likely.*
3. *Don't (needlessly) lose hashpower to un-upgraded miners.*
4. *Use hashpower enforcement to de-risk the upgrade process, wherever possible.*
5. *Follow the will of the community, irrespective of individuals or unreasoned objection, but without ever overruling any reasonable objection.*

[bitcoin-dev] Modern Soft Fork Activation

Matt Corallo lf-lists at mattcorallo.com
Fri Jan 10 21:30:09 UTC 2020

Figure 4: Matt Corallo's "Modern Soft Fork Activation"[19].

Corallo is more aligned with the `BIP9` camp, which, as can be seen by the above principles, stresses the need to maintain network harmony and de-risk against chain splits. The difficulty lies in the realization of these principles. In the email trail that follows Corallo's original post, Bitcoiners respond with a host of countervailing principles, capturing the Socratic nature of Bitcoin politics. Luke Dashjr, prominent contributor to the 2017 `UASF`, argues against `BIP9` as well as "flag day soft forks[20]":



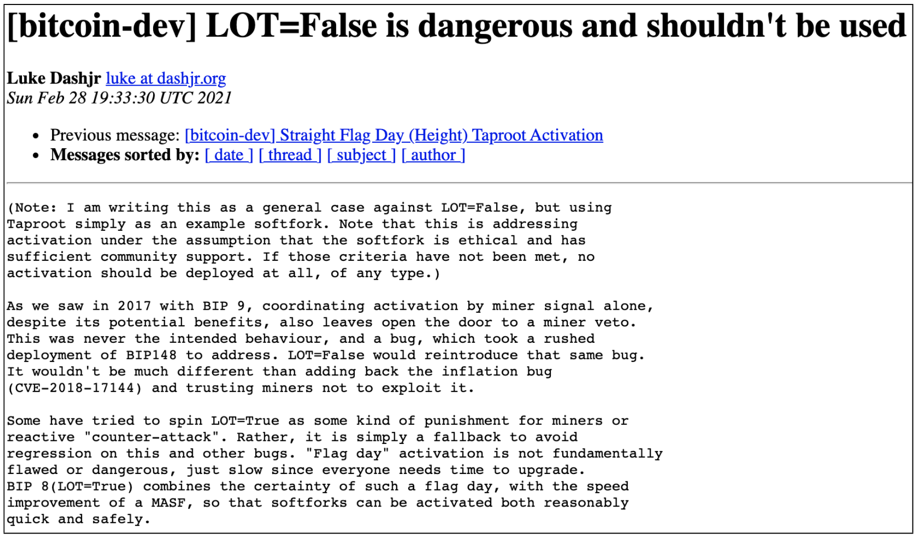
```
B) Because of (A), there is also no clear way to intentionally reject the
softfork. Those who do not consent to it are effectively compelled to accept
it anyway. While it is usually possible to craft an opposing softfork, this
should IMO be well-defined and simple to do (including a plan to do so in any
BIP9-alike spec).

For these reasons, in 2017, I proposed revising BIP 8 with a mandatory signal,
similar to how BIP148 worked: https://github.com/bitcoin/bips/pull/550
However, the author of BIP 8 has since vanished, and because we had no
immediate softfork plans, efforts to move this forward were abandoned
temporarily. It seems like a good time to resume this work.
```

Figure 5: Luke Dashjr's argument against `BIP9`[21].

We aren't taking a view on this exchange, but think the back-and-forth captures just how much progress has been made in Bitcoin soft fork design, even if it feels stagnant and slow to the rest of the market. *Taproot has spurred fresh and lengthy debate despite being an upgrade everyone agrees on.* In contrast, other networks often propose radical change – change which could represent a network's divergence from a multi-year ethos or vision previously defined – with very little contention, let alone heated debate.

[17] URL: https://arringtonxrpcapital.com/2021/07/19/illuminating-the-dark-age-of-blockchain-algorand/.
[18] URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2020-January/017547.html.
[19] URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2020-January/017547.html.
[20] URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2020-January/017551.html.
[21] URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2020-January/017551.html.

Dashjr's proposal to "revisit BIP8" with a mandatory signal is eventually expressed as "BIP8 TIME-LOT = TRUE" proposal, discussed in the next section. Like the UASF in 2017, this is a version of "forced signalling", putting mandatory pressure on Miners to upgrade and forcing their hand if they don't.



[bitcoin-dev] LOT=False is dangerous and shouldn't be used

Luke Dashjr luke at dashjr.org
Sun Feb 28 19:33:30 UTC 2021

- Previous message: [bitcoin-dev] Straight Flag Day (Height) Taproot Activation
- **Messages sorted by:** [date] [thread] [subject] [author]

```
(Note: I am writing this as a general case against LOT=False, but using
Taproot simply as an example softfork. Note that this is addressing
activation under the assumption that the softfork is ethical and has
sufficient community support. If those criteria have not been met, no
activation should be deployed at all, of any type.)

As we saw in 2017 with BIP 9, coordinating activation by miner signal alone,
despite its potential benefits, also leaves open the door to a miner veto.
This was never the intended behaviour, and a bug, which took a rushed
deployment of BIP148 to address. LOT=False would reintroduce that same bug.
It wouldn't be much different than adding back the inflation bug
(CVE-2018-17144) and trusting miners not to exploit it.

Some have tried to spin LOT=True as some kind of punishment for miners or
reactive "counter-attack". Rather, it is simply a fallback to avoid
regression on this and other bugs. "Flag day" activation is not fundamentally
flawed or dangerous, just slow since everyone needs time to upgrade.
BIP 8(LOT=True) combines the certainty of such a flag day, with the speed
improvement of a MASF, so that softforks can be activated both reasonably
quick and safely.
```

Figure 6: Using "Taproot simply as an example softfork", Luke Dashjr's makes the case that LOT=False is "dangerous"[22].

[22] URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2021-February/018498.html.

Table 1: Example BIP classifications.

BIP Type	Layer	Type	Description	Veto Power
BIP8	NA (Activation procedure)	Informational	Version bits with lock-in by height	Nodes or Miners
BIP9	NA (Activation procedure)	Informational	Version bits with timeout and delay	Miners
BIP148	Consensus (soft fork)	Standard	Mandatory activation of SegWit deployment	Nodes
BIP340	NA (signature scheme)	Standard	Schnorr Signatures for secp256k1	NA
BIP341	NA (spending rules)	Standard	Taproot: SegWit version 1 spending rules	NA
BIP342	NA (Taproot scripts)	Standard	Validation of Taproot scripts	NA

3 Taproot's Activation Path

We have scratched the surface on Bitcoin's philosophical debates and how they have been renewed by Taproot. In this section, we look at Taproot's specific activation path and discussion. Since the activation path has now been settled, we have the luxury of hindsight, allowing us to speculate on the implications of the chosen direction.

Taproot's development began four years ago, initially proposed by core developer Gregory Maxwell in January 2018[23]. In September 2019, Pieter Wuille (also a core developer) proposed implementing Taproot into Bitcoin Core[24]. This proposal was reviewed and tested by 150 developers between November and December of 2019[25].

3.1 Speedy Trial + BIP8 LOT = False

Taproot was eventually proposed through a variant of `BIP8` with a `Speedy Trial` overlay. `Speedy Trial`[26] overlays on top of `BIP8` (or any other chosen proposal) and gives miners a chance to signal readiness on a shorter timeframe. Rather than giving them a year to flag support as otherwise proposed, `Speedy Trial` does the following: if within the first 3 months of the proposal, miners signal 90% readiness, Taproot goes into effect 3 months after the end of this initial period. In effect, `Speedy Trial` means that Taproot can go live 6 months after being proposed.

Taproot's first two-week signalling period began on May 1st, 2021[27] and didn't gain miner majority. A second period began immediately following (May 14th[28]), also suffering the same fate. On the third signalling period, Taproot reached the 90% signalling threshold on June 12th, 2021 (`Block 687,284`), thus officially locking in the upgrade for November 2021.

A few different camps emerged during the activation debate. How much time should miners have to signal readiness? What is the appropriate threshold requirement to determine a miner super-majority? If miners don't signal in the given period, should Taproot go through anyway, or should a fresh signalling period begin, restarting the process? Who should have final veto power over the activation process?

3.2 The BIP8 Debate Returns: Taproot's Controversy

The structure of `BIP8` proposals is almost identical to `BIP9`, but includes the "`lockinontimeout`" (`LOT`) option. It can be assigned "true" or "false" values, which each take a different view on miner signaling[29]:

- When set to "true", even if the miner signalling threshold isn't reached before the expiration of the final signalling period, *the change will go forward anyway.* This is the idea of forced signalling discussed previously. Instead of failing, `LOT` will force Taproot activation. Full Nodes running the activation process reject blocks produced by miners that have not signalled readiness. By rejecting

[23] URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html.

[24] URL: https://github.com/bitcoin/bitcoin/pull/19997.

[25] URL: https://github.com/bitcoin/bitcoin/pull/19997.

[26] URL: https://www.coindesk.com/tech/2021/03/18/speedy-trial-taproot-activation-on-bitcoin-could-still-include-a-safety-net/.

[27] URL: https://taprootactivation.com/.

[28] URL: https://taprootactivation.com/.

[29] URL: https://bitcoinmagazine.com/technical/lottrue-or-lotfalse-this-is-the-last-hurdle-before-taproot-activation.

these blocks, the chain will reach the signalling threshold even if it means forcing delinquent miners off of the network.

LOT is designed to trigger a UASF (similar to how SegWit was ultimately activated), assigning decision power to the Full Nodes if miners disagree or are apathetic.

- When set to "false", if miner signalling is below the required threshold before the activation period, nothing will happen. The status quo is maintained, similar to a regular Miner Activated Soft Fork. In "false", miners have the ultimate veto power as they can perpetually delay soft fork activation.

The LOT = true camp argues that forced signalling enshrines community consensus on-chain and gives control of the network to the Full Nodes. Full Nodes decide to upgrade their software and force miners to comply. The LOT = false camp argues that this could splinter hashrate and create unnecessary network division.

In our view, the strongest credible critiques of the "self-sovereign" UASF approach are as follows: (1) if there was an undiscovered critical flaw in Taproot (undiscovered before consensus on "LOT = true"), the network could eventually be forced to hard fork to fix the bug, forcing nodes and miners to forgo the canonical chain and upgrade their software again. (2) What if there is no consensus amongst Full Nodes on the assigned value of "LOT"? This could also lead to a hard fork: if the majority of miners signal for "LOT = false", the "LOT = false" network continues to run the old software, now with a fraction of the mining power.

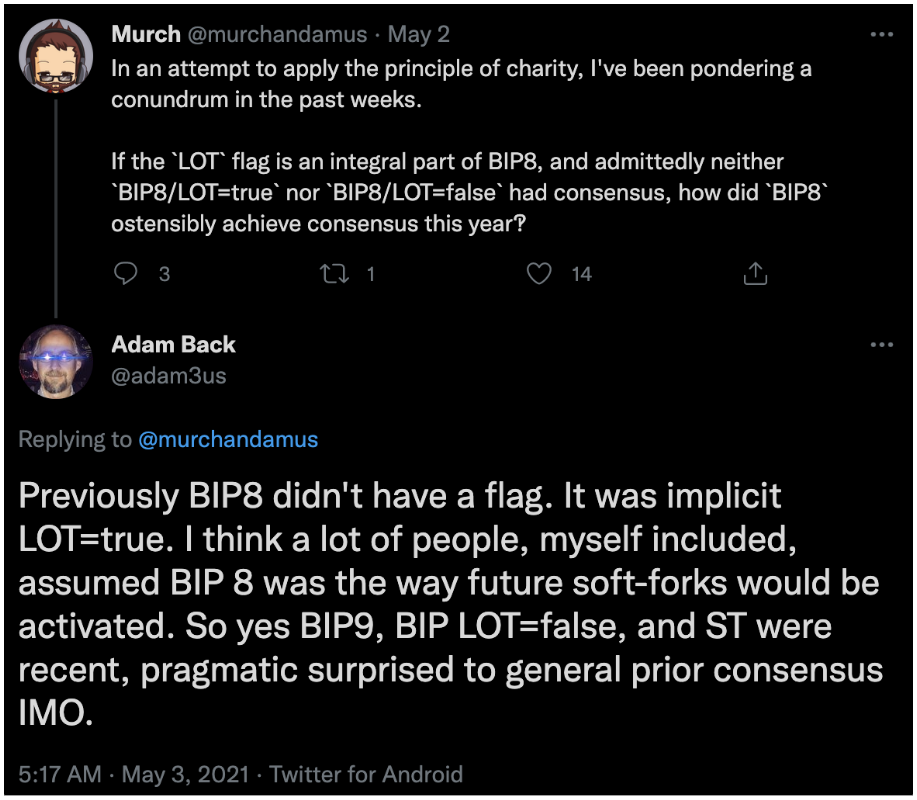
LOT = true advocates counter (1) by stressing the extent of Taproot's existing code review. The community hasn't found a bug after auditing the code for years. They counter (2) by stressing the need for Full Nodes to have final veto rights over the network. Even if hashrate splinters, difficulty will adjust and new miners will join the original network. If miners leave, difficulty adjusts and hashrate rebounds. Miners are pragmatic economic actors who will return if there is money to be made. **If nodes leave or are mistreated (by, say, erosion of their veto rights), Bitcoin security suffers irreparably – and it can't simply bounce back (as hashrate does after a difficulty adjustment). Breaking the trust of the Full Nodes can irreparably damage Bitcoin.**

3.3 The Pros & Cons Of Speedy Trial

The idea behind Speedy Trial is that Taproot activation can either quickly succeed or quickly fail without compromising safety. In a sense, Speedy Trial is agnostic to the BIP8 debate. It simply brings the timeline forward. It doesn't necessarily take a stance on the LOT = true or LOT = false question of forced signaling. If Speedy Trial works, there is no need to go with other proposals (like BIP8 or BIP9); if it doesn't, then these other lengthier activation paths continue.

The goal of any soft fork is that new rules are enforced by a large part of the economy. If there isn't enough adoption, the network can splinter and create direct losses to transaction receivers and larger indirect losses to holders due to reduced confidence in Bitcoin safety. In the past, developers have navigated user adoption by creating a delay between the release of the new software and the date that the software starts tracking which blocks signal activation. Speedy Trial replaces most of that upfront delay with a backend delay. No matter how fast Taproot meets the activation threshold, there are six months between the start of signalling and rule enforcement.

[30] URL: https://twitter.com/murchandamus/status/1388990419623628801.



Murch @murchandamus · May 2

In an attempt to apply the principle of charity, I've been pondering a conundrum in the past weeks.

If the `LOT` flag is an integral part of BIP8, and admittedly neither `BIP8/LOT=true` nor `BIP8/LOT=false` had consensus, how did `BIP8` ostensibly achieve consensus this year?

Adam Back
@adam3us

Replying to @murchandamus

Previously BIP8 didn't have a flag. It was implicit LOT=true. I think a lot of people, myself included, assumed BIP 8 was the way future soft-forks would be activated. So yes BIP9, BIP LOT=false, and ST were recent, pragmatic surprised to general prior consensus IMO.

5:17 AM · May 3, 2021 · Twitter for Android

Figure 7: A Twitter exchange between Adam Back and a Bitcoin engineer on LOT = true versus LOT = false[30].

Advocates for Speedy Trial argue that it improves the proposal process. If it fails fast, the community can incorporate new data (reasons for the failure) into subsequent proposals. In some sense, it also puts pressure on miners to signal (in the spirit of BIP8 LOT = true) without "playing chicken" and threatening a UASF. There is no *mandatory signalling*, although such signalling is encouraged. One other benefit is that, if signalling is fast (in theory, if the threshold is reached on day one from the first initial period), the market could have up to 6 months to prepare for activation. This gives developers, users, holders and any other relevant organization ample time to prepare for the change, improving adoption of the upgrade.

One of the main arguments[31] against Speedy Trial is that it could encourage false signaling. Miners could signal readiness to rules that their nodes don't actually support. Since it only gives them a maximum of three months to signal support, they could end up locking in Taproot only to fail to upgrade by the activation date several months later. Unprepared miners would lose money and users could face long reorgs, with unupgraded nodes and SPV lite clients also losing money. Speedy Trial advocates argue that the issue of false signalling is possible with any other proposal which could similarly create miner losses.

There are several important implications of this debate. In the context of an extremely non-contentious proposal, the community embraced the LOT = false approach and rejected forced signaling. We don't think this is necessarily a defeat to the 2017 UASF movement. It doesn't mean that LOT = true couldn't be employed for future upgrades if there was greater tension between miners and users. Unlike

[31] URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2021-March/018584.html.

2017, Taproot creates no conflict of interest between miners and users, and so (one could argue) that the extreme stance of self-sovereign Full Node veto was less imperative.

The adoption of `Speedy Trial` also shows a willingness to adopt non-contentious upgrades as quickly as possible within the constraints of the system. Given how much time Taproot has had in the market and the extent of its review process, `Speedy Trial` made sense. It's unclear that `Speedy Trial` will be adopted in more contentious upgrades or where there is less time for developer review. Regardless, it arguably involves the least friction and has the most optionality for both users and miners – demonstrating the community's openness to adopt mutually beneficial changes, come to consensus and – if governance fails – fall back on other more stringent `BIPs`.

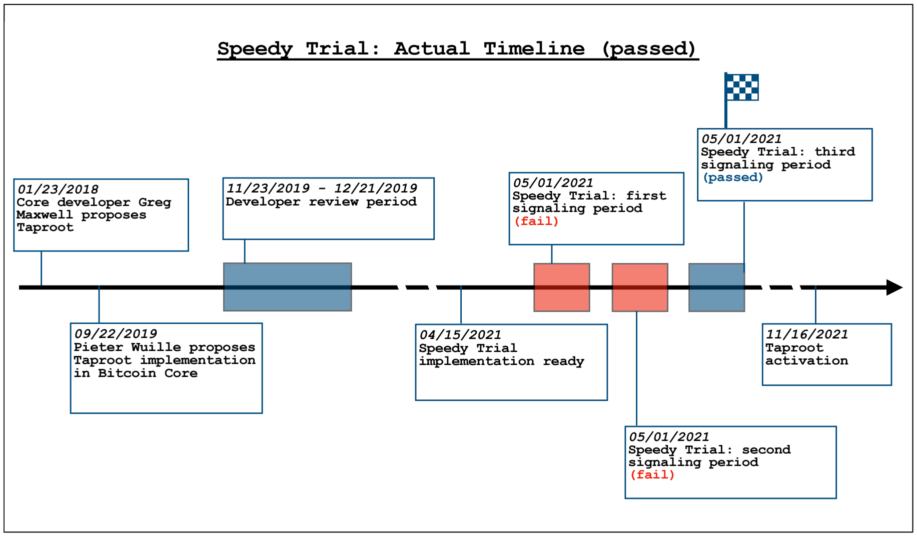

Speedy Trial: Actual Timeline (passed)
01/23/2018 Core developer Greg Maxwell proposes Taproot
09/22/2019 Pieter Wuille proposes Taproot implementation in Bitcoin Core
11/23/2019 - 12/21/2019 Developer review period
04/15/2021 Speedy Trial implementation ready
05/01/2021 Speedy Trial: first signaling period (fail)
05/01/2021 Speedy Trial: second signaling period (fail)
05/01/2021 Speedy Trial: third signaling period (passed)
11/16/2021 Taproot activation

Figure 8: Visualizing Taproot activation path and the four-year road to `Speedy Trial`.

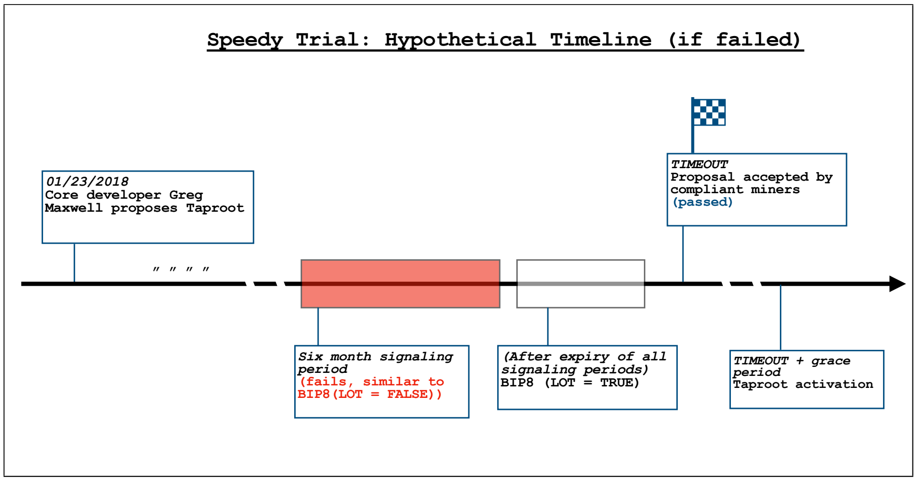

Speedy Trial: Hypothetical Timeline (if failed)
01/23/2018 Core developer Greg Maxwell proposes Taproot
Six month signaling period (fails, similar to BIP8(LOT = FALSE))
(After expiry of all signaling periods) BIP8 (LOT = TRUE)
TIMEOUT Proposal accepted by compliant miners (passed)
TIMEOUT + grace period Taproot activation

Figure 9: Visualizing a hypothetical timeline for Taproot if `Speedy Trial` had failed, where `LOT = False` would have likely been employed. This timeline also captures a hypothetical world where `LOT = True` was employed.

4 Taproot's Technical Contributions: What Taproot Is & What Taproot Isn't

Taproot is an incremental improvement that makes Bitcoin more scalable, private and secure. It improves the periphery of Bitcoin today while setting up the protocol for continued upgrades.

As mentioned previously, Taproot involves three separate BIPs: BIPs 340, 341 and 342.

1. **BIP340** replaces the legacy Elliptic Curve Digital Signature Algorithm (ECDSA) with Schnorr Signatures, a cryptographic scheme which makes complicated Bitcoin transactions simpler and more secure.

2. **BIP341** builds on the SegWit upgrade and improves Bitcoin privacy while lowering transaction fees, updating Bitcoin Script to include Schnorr Signatures. This BIP introduces MAST, which allows users to lock outputs to multiple scripts.

3. **BIP342** makes future upgrades easier by reforming Bitcoin's scripting language and introducing "Tapscript". This allows Bitcoin nodes to create and validate Pay-to-Taproot (P2TR) outputs, upgrading the opcodes that evaluate scripts. Tapscript changes how signatures are evaluated and takes advantage of the efficiency of Schnorr Signatures. In addition, BIP342 adds new null opcodes called OP_SUCCESS that allows Tapscript to be flexibly upgraded in the future.

4.1 Schnorr Season

The transition from ECDSA to Schnorr Signatures improves computation, storage and privacy capabilities. It is important to note that Satoshi likely used ECDSA because it wasn't patented at the time. It was also widely used in commercial encryption and implemented in OpenSSL, an open-source cryptography library that Satoshi leaned on in the early days of Bitcoin.

Taproot advocates believe that Schnorr signatures are *more provably secure* and help make complicated transactions possible while simplifying Bitcoin cryptography. Schnorr signatures have existed for decades, but the patent – heavily guarded by inventor Claus Schnorr – only expired in 2008[32].

Schnorr signatures enable *key and signature aggregation.* Before Taproot, a digital signature would involve the following: (1) a single public key, (2) a signed message and (3) a signature asserting that the public key owner signed the given message. If three parties wanted to sign the same message (a multi-sig), the proof needed to contain three public keys and signatures. Each node must thus perform signature verification three times, storing each set of signatures and keys.

With Schnorr, the same three parties can now combine their three public keys, form a single public key and sign the same message from each of their private keys. All of this comes together to form one single signature, valid as the aggregated public key. Multi-sig transactions can now *look like* uni-sig transactions. Not only does this make Bitcoin more scalable, it creates a new privacy layer: sleuths can't decipher complex multi-sigs through blockchain heuristics since they all look like uni-sig transactions.

Key aggregation unlocks *batch verification.* Instead of verifying every transaction and signature in a block – one-by-one – nodes can verify transactions in batches. The signatures of separate keys are equivalent to the signature of an aggregated key, known as linear verification. This reduces the time and computation required to verify a transaction with many inputs.

[32] URL: https://patents.google.com/patent/US4995082.

Taproot's introduction of a reformed Bitcoin script type called Tapscript opens up new and complex transaction types. Tapscript enables P2TR, which lets users send coins to either a Schnorr public key or the Merkle root of a variety of other scripts. Using this new script type, users can create UTXOs that can now be unlocked and spent by either the owner of the private key or anyone who can satisfy the requirements of a script within the Merkle tree.

When bitcoin is sent to a P2TR output, it is locked to a single public key. Now that this public key is an aggregation of some public key and a public key formed from the Merkle root of other script types, any of the alternative scripts in the Merkle tree can be used to spend the output. This design allows users to choose between complex, arbitrary scripts or simple pay-to-public-key functionality at the time of spending – rather than at the time of receiving. This is why Taproot improves Bitcoin privacy: *multisig outputs, single sig outputs and other complex smart contracts all look the same.*

4.2 Summarizing The Benefits Of Taproot

In summary, there are three main benefits to the Taproot `BIPs`:

1. *Space Savings*: Most Taproot (P2TR) outputs consume less space on the blockchain than normal P2PKH outputs, but are slightly larger than P2WPKH outputs. This is because P2TR outputs lock bitcoin directly to a public key, not the hash of the public key. This makes sending to Taproot outputs slightly more expensive, as public keys take up more space than public key hashes. However, spending Taproot outputs is significantly cheaper because the public key is included in the `scriptPubKey` and thus does not need to be included in the Script Witness. Taproot also defined the encoding scheme for Schnorr public keys and signatures, making them shorter than their ECDSA counterparts, further saving fees.

2. *Privacy Benefits*: By introducing Schnorr signatures and key aggregation, multisig contracts no longer look different from single signature contracts, providing privacy to Taproot users. Taproot also introduces significant privacy benefits through the integration of MAST. As discussed above, Taproot allows bitcoin to be locked to many scripts at once. However, when spending bitcoin from a Taproot output, the spender need not reveal every possible script that could have unlocked the bitcoin: only the script they actually used. In the majority of cases, Taproot users will likely use the pay-to-public-key option, but users will now have optionality for private transactions.

3. *Security Upgrades*: In academic cryptography, Schnorr signatures are considered more secure than ECDSA. They are provably secure with fewer assumptions. Like all elliptic curve cryptography schemes, both ECDSA and Schnorr rely on the assumption that the Discrete Logarithm Problem is hard (i.e. practically intractable). However, ECDSA relies on additional assumptions to guarantee its security. There have been no examples of ECDSA being systematically compromised (the postulate remains unchallenged). Schnorr signatures also eliminate signature malleability (recall SegWit) present in ECDSA signatures. While transaction malleability was solved by the SegWit upgrade, malleable signatures persisted as part of ECDSA, now remedied by Taproot.

Taproot makes Bitcoin better. It makes complicated transactions easier to achieve, while improving privacy and scalability. It opens the door for future upgrades that continue to build on Taproot's innovations. It creates a richer environment for conditional spends, giving users more flexibility with how they plan, protect and spend their money.

4.3 Programmable Bitcoin: What Taproot Isn't

What Taproot isn't is a wide overhaul of Bitcoin programmability. There are still no smart contract functionalities on Bitcoin L1 after Taproot. Some media coverage has characterized Taproot as Bitcoin-native DeFi or "smart contracts" on Bitcoin[33]". From our perspective, Taproot does not live up to this narrative, nor was it designed to. It opens up new possibilities for conditional transaction types, both cheaper and more expressive, making Bitcoin fundamentally *better*, but "DeFi" on Bitcoin would require a much more contentious change to L1 Script.

We also don't believe that Taproot will enable "DeFi on Lightning", although it will make Lightning incrementally better. It will improve user experience, reduce transaction costs and add a privacy buffer to Lightning channels, masking on-chain fingerprints through `BIP340`. Before Taproot, sleuths could trivially identify when a Lightning channel was closed as a simple 2/2 multisig. After Taproot, signatures can be aggregated beforehand and thus the fingerprint of a Lightning channel is now indistinguishable from a simple payment. We believe that this is an important step toward making Lightning mainstream-ready, especially as institutions and sovereign nations embrace Bitcoin – but it is not "DeFi on Lightning".

[33] URL: https://www.cnbc.com/2021/06/12/bitcoin-taproot-upgrade-what-it-means.html.

5 Digesting Block War PTSD: Taproot As Healing

5.1 The Return Of "Blockchain, Not Bitcoin"

As we progress into the crypto cycle, critics contrast Bitcoin's attitude toward change against other protocols, concluding that while it may have been first, it is stuck in an age of complacency. It is the MySpace of crypto. The market sees ossification as a negative, aspiring for technological idealism; the drive to experiment and iterate. Inevitably, both new and old participants arrive at a familiar but recurring narrative: "Blockchain, Not Bitcoin".

The problem with this approach is that it mistakes Bitcoin's value proposition. Bitcoin is fundamentally an economic innovation, not a technical one. *Bitcoin value is its ossification.* It is a haven for stability amidst the dynamism of the world. It is calcified by design – the most obvious and compelling feature of this status being a fixed money supply of 21 million. This extreme stability shows up elsewhere, often subtly, from veto-rights between participants, the staunch separation between Full Nodes and Miners and a pre-programmed inflation schedule (the "Halvings").

With that said, calcification has challenges. It may be the most enduring property, but with extreme stability comes a paradox: capital that comes for stability can eventually seek change. Each subsequent wave of mainstream adopters put Bitcoin deeper into the world, a world that is changing all the time, a world that begins demanding a similar evolvability from the protocol.

The question then becomes – possibly Bitcoin's defining challenge – how can it keep pace with the world and adapt to new pressures, but remain Bitcoin? How can Bitcoin stay Bitcoin, embracing technical progress while guarding against the danger of "constant innovation"?

5.2 The Swings Between Progress & Stability

Bitcoin has always swung between this paranoia toward change and openness to evolution. In the early days, it changed all the time, at the pace of a public forum and curated email chain. In more recent times, Bitcoin has settled on a conservative ethos, rejecting most change as the path to fresh hostilities.

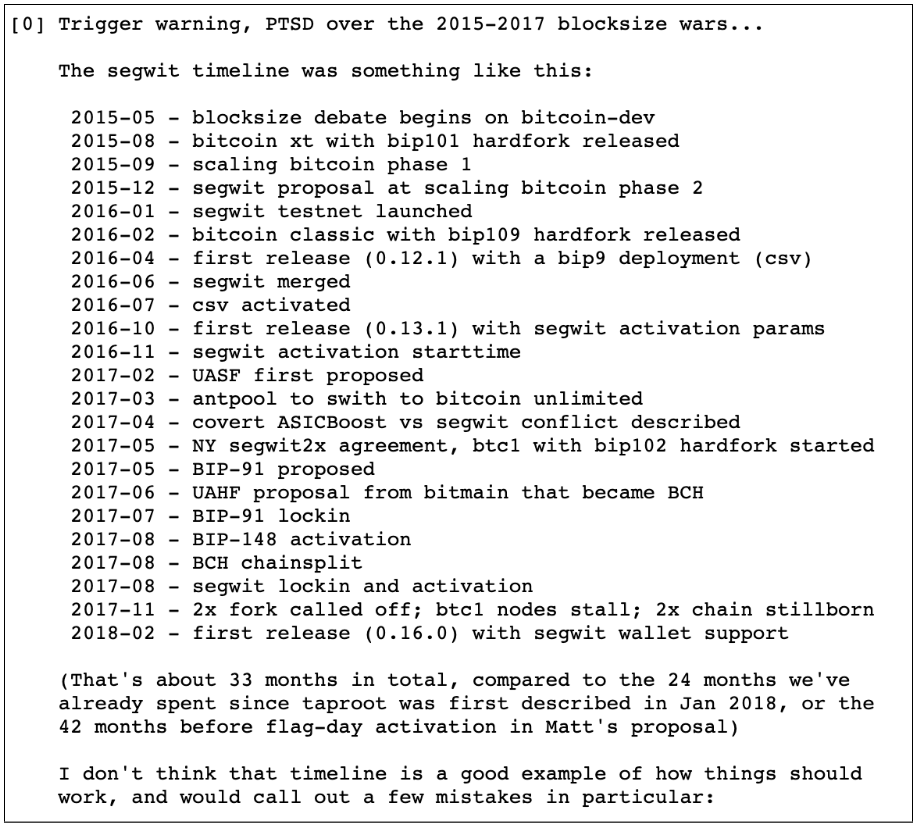
We argue that today's hyper-conservatism is part of 2017's legacy. The Block Wars motivated a natural but heightened conservatism. All soft forks could lead to hard forks. The sectarian war – a war about whether Miners or Nodes governed the network – created the conditions for technical conservatives to rule for years to come. They became the guardians of the network, guardians against change. Any change to Bitcoin – even if peripheral – brought back memories of this power struggle. The Frankenstein child-chain – the BCH network – eventually experienced its own cannibalization event in 2018 in the BSV Wars[34], vindicating this hardliner ethos: *the ethos that technical progressivism is how the network eventually dies.*

This technical conservatism is a feature of Bitcoin. If iteration damages extreme stability, it likely damages the protocol beyond the marginal benefits of new innovation. Conservatism is part of the immune system. On the other hand, like any political system, Bitcoin inevitably swings between stability and evolution, experiencing new periods of excitement and eagerness.

As a potential turning point, Taproot could be the beginning of a new openness. The first upgrade since 2017, and being non-contentious, it alleviates the fear that all change is a catalyst for sectarianism. It

[34] URL: https://www.europeanbusinessreview.com/btc-bch-and-bsv-how-are-they-different/.

gives Bitcoiners – and the market – a moment to sigh, to feel relief, and to finally digest the self-serving splinters of the past. It allows Bitcoin to process and move beyond Block War PTSD.



```
[0] Trigger warning, PTSD over the 2015-2017 blocksize wars...

    The segwit timeline was something like this:

     2015-05 - blocksize debate begins on bitcoin-dev
     2015-08 - bitcoin xt with bip101 hardfork released
     2015-09 - scaling bitcoin phase 1
     2015-12 - segwit proposal at scaling bitcoin phase 2
     2016-01 - segwit testnet launched
     2016-02 - bitcoin classic with bip109 hardfork released
     2016-04 - first release (0.12.1) with a bip9 deployment (csv)
     2016-06 - segwit merged
     2016-07 - csv activated
     2016-10 - first release (0.13.1) with segwit activation params
     2016-11 - segwit activation starttime
     2017-02 - UASF first proposed
     2017-03 - antpool to swith to bitcoin unlimited
     2017-04 - covert ASICBoost vs segwit conflict described
     2017-05 - NY segwit2x agreement, btc1 with bip102 hardfork started
     2017-05 - BIP-91 proposed
     2017-06 - UAHF proposal from bitmain that became BCH
     2017-07 - BIP-91 lockin
     2017-08 - BIP-148 activation
     2017-08 - BCH chainsplit
     2017-08 - segwit lockin and activation
     2017-11 - 2x fork called off; btc1 nodes stall; 2x chain stillborn
     2018-02 - first release (0.16.0) with segwit wallet support

    (That's about 33 months in total, compared to the 24 months we've
    already spent since taproot was first described in Jan 2018, or the
    42 months before flag-day activation in Matt's proposal)

    I don't think that timeline is a good example of how things should
    work, and would call out a few mistakes in particular:
```

Figure 10: Anthony Towns: "Trigger warning, PTSD over the 2015-2017 blocksize wars..."[35].

[35] URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2020-January/017553.html.

6 The Testing Ground For Covert Warfare: Taproot As Preparation

The nature of attacks on Bitcoin is evolving with the network. What was a credible threat in 2017 would today look like a cluster of chaotic OGs and ragtag miners clasping for power. The next credible attacks will look extremely different, likely led by new, high-trust and well-resourced entrants.

Post-Taproot innovation narratives could motivate these attacks, but also encourage the old guard to sharpen its defense. Powerful technologists, financiers and politicians are now in Bitcoin's orbit. They are a powerbase that Bitcoin's diverse stakeholders don't yet understand.

As Bitcoin becomes a mainstream asset and includes more powerful and diverse stakeholders, these attempts at change become increasingly likely. We could envision a tail scenario where powerful technologists gradually monopolize Bitcoin tooling, build trust within the developer community and incrementally re-shape consensus about `BIP` methodology. These actors could slowly crowd out the hardliner, self-sovereign Full Node types – captured by `UASF` maximalism – instead empowering more "conciliatory" philosophies for governance.

In the end, it is the same power struggle as 2017: the swing between corporate and miner interests and Full Node sovereignty. Yet, in our view, these more "covert" attacks will be unlike 2017's: they will look reasonable and necessary. They could take the form of popular mainstream narratives like ESG, Bitcoin DeFi or Medium of Exchange (MoE) scalability. The institutionalization of Bitcoin will inevitably motivate, finance and mobilize a new BCH-style struggle, except that it won't feel like a *direct* attack.

6.1 Becoming Antifragile: Can Bitcoin Survive A Hidden Enemy?

To defend the network from covert warfare, Bitcoiners need to stay dynamic and politically engaged. Extreme close-mindedness served the network after 2017, but – alone – it will make Bitcoiners look unreasonable and "out of touch" going forward. Hardliners who blindly dismiss change without engaging in the rigors of governance will embolden their enemies, now more palatable to mainstream audiences and likely more popular than the Big Block coalition.

This is why we think Taproot is a major turning point. It drives new pressures toward the network. ***That we can now have any change will embolden actors who want more change***. Taproot will mobilize technological progressives. At the same time, it will force hardliners to sharpen Bitcoin's Socratic fallbacks, strengthening their defense of the network's non-negotiables. The outcome of this back-and-forth, we believe, is fundamentally positive, shining a light on the vitality of Bitcoin's political process.

In our view, there is no network with a governance layer as complex and defensible as Bitcoin's. The critique of relative "stagnation" fails to capture Bitcoin's ongoing web of developer contribution and stakeholder dialogue. We think these debates in soft fork design are just getting started and will likely heat up in the coming year.

The post-Taproot era will present new opportunities and risks. How Bitcoin's diverse stakeholders react, organize and adapt to this new environment will be a critical signal for the network's antifragility, as it enters its next phase.

In 2017, the Full Nodes organized the impossible: they defeated the largest mining pools, exchanges and financial institutions. Anonymous Redditers had more sway than industrial actors. The challenge going forward is different. Can the network evolve and embrace peripheral change that unquestionably makes Bitcoin better – *non-contentious changes like Taproot* – but stay sufficiently paranoid about the next trojan horse, likely proposed with a strong technical rationale? Can the community continue to pioneer low-risk change without accidentally (or by corporate persuasion) accepting high-risk change?

We don't have a good answer, but think that some of the market's assumption that *Bitcoin is stuck* overlooks this system-wide complexity. Instead of seeing Bitcoin as a nuanced political body that dances between technical progressives and defensive hardliners, the market sees a stale and close-minded asset decaying in the past. The market clings to the "toxicity" of Bitcoin governance without appreciating the role it plays in the context of Bitcoin as a political system. We believe that the value of Bitcoin governance will become better appreciated in years to come, especially if the network faces a new wave of highly-credible adversaries – and survives.

7 L1 & L2 Innovation Narratives In Post-Taproot Bitcoin

Our thesis is that Taproot is less important as a direct catalyst for innovation and more important as a turning point for innovation and governance stories. Even if Taproot is a relatively benign change, the dramatic rate of change opens the door for more soft forks.

With that said, there are a few *direct* innovation narratives that could emerge and position Bitcoin within broader crypto trends. Whether or not these narratives have legs in the long term is unclear to us, but we think they will surface, pushed as a counterattack against the idea that "there is no innovation on Bitcoin".

7.1 Bitcoin's Entrance Into Multi-Chain L1

The L1 wars captured the malleability of "developer moats". DeFi protocols emerged beyond Ethereum, bootstrapping liquidity and crossing international borders to find new talent. With the exception of wrapped BTC (WBTC), a purely centralized solution, Bitcoin did not participate in this trend.

While Taproot does not directly create the conditions for cross-chain expressiveness and portability (this would require a fundamental change to Bitcoin Script), its fresh attitude toward change could encourage burgeoning L1s to interact with Bitcoin around the edges. Up until now, there has been no clear reason for L1s and Bitcoin to form alliances, but this could change. Especially in a world where Ethereum has embraced a new monetary identity – captured by the sentiment around `EIP1559` as "ultrasound money" – the barbell between Bitcoin and non-ETH L1s has some (at a first glance) strategic rationale ("the enemy of my enemy is my friend").

Fast L1s which "nod at the king" could find product-market fit amongst Bitcoin holders and users. If they preserve decentralization and tip their hats to help Bitcoin, Bitcoiners may become marginally more open to "crypto" innovation. In a sense, some L1s could become "BD arms" for Bitcoin adoption – likely a win for these chains, given that they aren't trying to compete with Bitcoin as money. We have already seen some signs of this during this cycle, including Algorand's attempt to build infrastructure that underpins the Chivo Wallet in El Salvador[36], Blockstack's attempt to position itself as a "Layer 1.5" that can bridge Bitcoin with other chains[37] and Sovryn's attempt to build money markets and "DeFi for Bitcoin" through the RSK sidechain[38].

One scenario is that L1s with their own scripting language try to become intermediate side-chains for Bitcoin, where they can theoretically bootstrap the Bitcoin-native user experience. These L1s may aspire to bridge Bitcoin into the wider L1 universe, arguing that they can help Bitcoin leave behind its current isolationism and embrace crypto internationalism.

There are short and long term considerations in this Bitcoin and multi-chain L1 interplay. One question Bitcoiners will likely ask is how these L1s help or hurt Bitcoin security. Do they genuinely help expand the Bitcoin economy without compromising its core value set or do they extract away the fees that would otherwise go to miners? Every L1 will claim to "help Bitcoin", but how will the Bitcoin ecosystem assess the long term risk and reward of these proposals?

We don't have a strong view on this theme, but think that it will also likely heat up in the post-Taproot era. One challenge for attempts at creating Bitcoin-based financial products – both on Bitcoin or through

[36] URL: https://www.siliconrepublic.com/enterprise/el-salvador-bitcoin-digital-wallet-chivo-offline.
[37] URL: https://decrypt.co/82019/bitcoin-defi-thing-says-stacks-founder-muneeb-ali.
[38] URL: https://defiprime.com/sovryn.

other L1s as sidechains – is the same challenge for Ethereum monetary policy: is it worth competing on somebody else's territory? Ethereum (and other L1s) are unquestionably ahead of Bitcoin as composable and expressive financial platforms and it's not necessarily clear that DeFi-type products are part of Bitcoin's ethos to begin with.

There is always the risk that Bitcoin tries to embrace DeFi, fails, and that this energy was otherwise put to better use where Bitcoin is already thriving. Nonetheless, we are eager to follow these experiments and watch how they attempt to position Bitcoin growth within broader L1 trends.

7.2 Bitcoin's Emerging Environment For L2 Innovation: Lightning Strikes

As we discussed earlier, Taproot helps make Lightning more private and scalable. While it may not seem relevant today with Lightning adoption in its infancy, increased privacy could be critical, especially if Lightning is adopted into mainstream applications.

By every relevant metric, Lightning is entering its first phase of exponential growth. The most compelling use case is El Salvador's recent adoption of Lightning for remittances. It was recently reported that based on a single day's activity, remittances through the Chivo wallet accounted for close to 5% of the country's GDP on an annualized basis[39]. As part of its push to bootstrap the country's adoption of Bitcoin for remittances, El Salvador established a $150m fund which supports the free conversion of Bitcoin into dollars[40].

Lightning growth has a longer arc beyond just this Latin American uptick. In 2019, the number of unique Lightning channels roughly doubled, growing from a base of 15,939 to 27,900. As of October 17th 2021, there are now 73,715 unique Lightning channels[41]. This is a strong gauge for Lightning adoption as these channels represent new nodes connecting to Bitcoin L2.

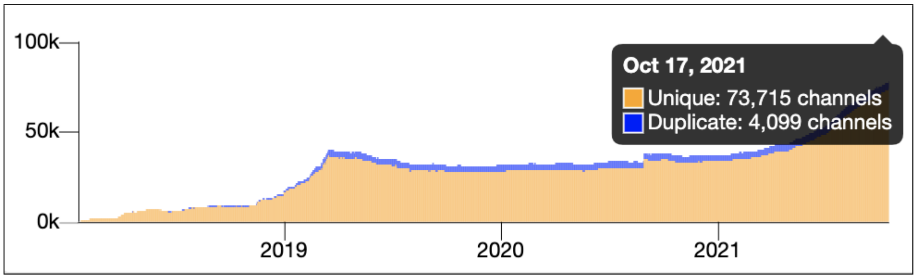


Figure 11: Lightning's multi-year growth trajectory, captured by the growth in unique Lightning channels[42].

Network capacity has similarly skyrocketed this year, tripling from a base of roughly 1,000 BTC in January to over 3,000 BTC in October, with the pace of growth accelerating in August[43]. While the idea of network capacity is not comparable to DeFi Total Value Locked ("TVL"), given that they serve fundamentally different use cases, Lightning could be in the early innings of parabolic growth akin to

[39] URL: https://www.cnbc.com/2021/10/07/one-month-on-el-salvadors-bitcoin-use-grows-but-headaches-persist.html.

[40] URL: https://www.theblockcrypto.com/linked/116200/el-salvador-approves-150-million-trust-fund-to-support-bitcoin-ambitions.

[41] URL: https://bitcoinvisuals.com/lightning.

[42] URL: https://bitcoinvisuals.com/lightning.

[43] URL: https://www.lookintobitcoin.com/charts/lightning-network-capacity/.

DeFi's ETH-denominated growth in the second half of 2020[44].

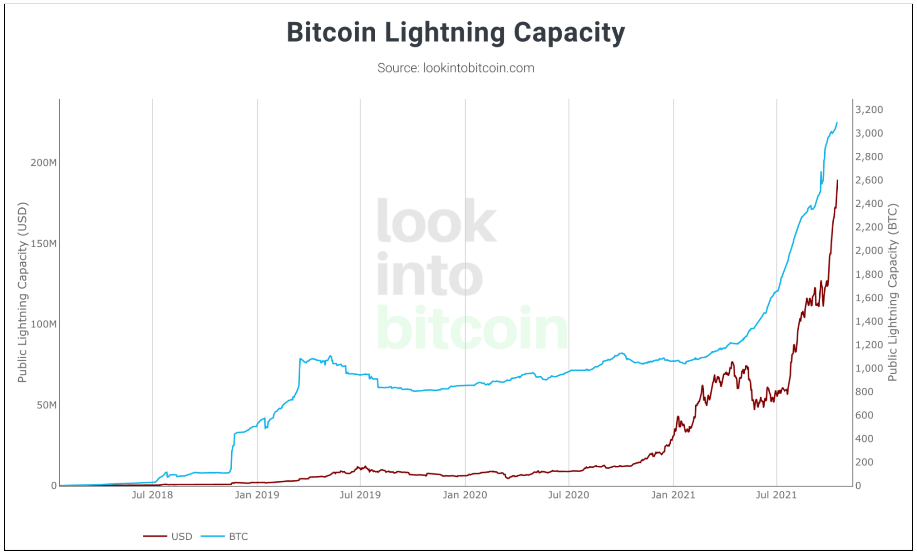


Figure 12: BTC and USD-denominated Lighting Capacity, capturing Lightning's exponential growth in the second half of 2021[45].

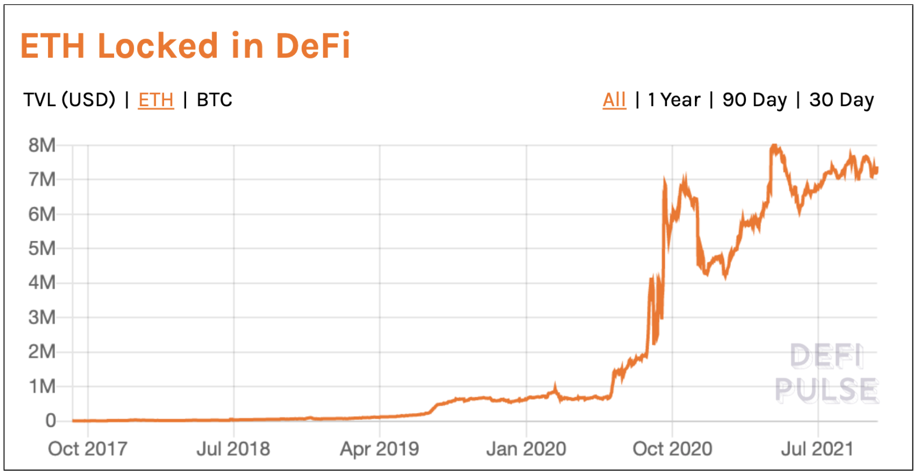


Figure 13: ETH DeFi's "breakout" moment in the second half of 2020. While Lightning capacity is not comparable to DeFi, we hypothesize that Lightning could be in a similar phase of exponential adoption[46].

The developer experience and tooling around Lightning is also nascent but rapidly maturing. Led by Matt Corallo, a major contributor to the BIP discussion from previous sections, Square Crypto is building a Lightning Development Kit (LDK). The LDK empowers wallet and app developers who want to create "custom experiences" on Lightning through a Rust-based development environment, language bindings and demo apps[47]. It makes it easier to add Lightning support to existing wallets, support

[44] URL: https://defipulse.com/.
[45] URL: https://www.lookintobitcoin.com/charts/lightning-network-capacity/.
[46] URL: https://defipulse.com/.
[47] URL: https://medium.com/@squarecrypto/what-were-building-lightning-development-kit-1ed58b0cab06.

multi-application processes and create simpler UIs for wallets deciding on UX, security and privacy tradeoffs.

Strike is also building an API and mobile application for users to plug into the Lightning network without interfering with Bitcoin. Instead of buying Bitcoin to take advantage of Lightning's instant settlement layer, users can plug into Lightning directly with fiat currency. The Strike API is how Twitter will create Tipping functionality[48]. In theory, Strike could not only become the way that any Web2 merchant, marketplace or developer interfaces with Lightning, but also the way that Lightning penetrates mass applications like social media or online gaming. This makes Lightning an Internet-native Visa competitor, one where anyone using the network can transact globally with practically no fees and instant finality. Strike launched in El Salvador in March following the initial introduction of pro-Bitcoin legislation and quickly became the country's most-downloaded mobile application[49].

Another company dedicated to Lightning innovation is Breeze, focused on improving mobile accessibility to Lightning and allowing users to "create channels on the fly[50]". With Breeze, users can run Lightning nodes from their mobile device, using one-click solutions to become merchants. Breeze recently launched a product called "Podcasting 2.0", focused on payments for podcasters – "Streaming Sats[51]". Like the Strike API and Tipping integration, this is yet another example of how Bitcoin L2 can penetrate Web2, arguably positioning Bitcoin to slowly craft its own "Web3" narrative (albeit fundamentally different from Ethereum's).

While most of the market has focused on the rapid innovations in Ethereum L2, the climate for Bitcoin L2 is evolving extremely quickly. We are eager to follow Bitcoin L2 post-Taproot and monitor the relationship between new privacy capabilities and the pace of Lightning adoption. Do users care about the ability to create multi-party channels with less on-chain footprint, now enabled by Schnorr? Do these privacy features help the value proposition for escrow-focused companies like Strike? If the El Salvadorian Lightning experiment succeeds, will better privacy make similar adoption more likely for other, possibly larger nation states?

We hypothesize that most Bitcoin innovations will live on L2. Bitcoin could theoretically become a Visa competitor, with new products that revitalize Bitcoin's capabilities as a MoE. Post-Taproot friendliness toward innovation could accelerate the rush of capital and developer interest into the Bitcoin L2 market.

This emerging L2 environment demonstrates that Bitcoin can dynamically shift between narratives without changing the base layer. The Block Wars forced users to choose one identity: Store of Value (SoV) or Medium of Exchange (MoE). It was one or the other; small blocks or big blocks, Bitcoin or Bitcoin Cash. Increasingly, users and developers will have optionality between both, optionality that grows if more countries adopt the El Salvadorian playbook, or if existing Bitcoin holders become more open to spending their coins given the improved tooling, experience and – courtesy of Taproot – privacy.

[48] URL: https://blog.twitter.com/en_us/topics/product/2021/bringing-tips-to-everyone.

[49] URL: https://www.businesswire.com/news/home/20210605005045/en/Strike-Drives-Bitcoin-Forward-as-El-Salvador-Becomes-World%5C%E2%5C%80%5C%99s-First-Country-to-Adopt-Bitcoin-as-Legal-Tender.

[50] URL: https://medium.com/breez-technology/podcasts-on-breez-streaming-sats-for-streaming-ideas-d9361ae8a627.

[51] URL: https://stephanlivera.com/episode/264/.

Conclusion

In 2021 Bitcoin became a political asset. The Chinese government attacked the network while a Latin American sovereign embraced it with open arms. The political exiling of Chinese hashpower demonstrated how quickly nation states can try to reshape the network. In this case, the change was fundamentally positive: the network bounced back, hashpower migrated to friendlier jurisdictions and Bitcoin security became more dispersed and decentralized.

In the US Bitcoin's politicization has taken a more ambiguous path, but one that continues to push toward mainstream adoption. Bitcoin's political narrative is no longer the utopian dream of the cypherpunks: it is part of an international political conversation, slowly adopted by burgeoning politicians who recognize the network's growth trajectory. In the context of both crypto L1 and L2 narratives as well as international politics, Bitcoin is slowly leaving behind its first decade of isolationism.

As Bitcoin becomes a political asset, the vibrancy of Bitcoin governance becomes increasingly important. Can Bitcoin survive a hidden enemy; a sophisticated coalition of technologists, political ideologies and developers, who can now lobby for change through compelling mainstream pressures?

On the other hand, how can Bitcoin adapt to these dangerous pressures – survive them – but stay open-minded toward improvements at the margin like Taproot? Can post-Taproot Bitcoin embrace non-contentious and peripheral evolution? Can Bitcoin say yes to change that makes Bitcoin better, but still refuse to lower its shield against the slippery slope of technological utopianism?

While the market today arguably underappreciates the value and complexity of Bitcoin's governance and innovation narratives, we think that is about to change. The next several years of Bitcoin could represent a new chapter in the swing between innovation and extreme stability, leaving behind the legacy of 2017's civil war and inviting new macro forces onto the network.

As technical progressives gain better footing, hardliners will need to sharpen their arguments. They will need to continually revisit the archives of Bitcoin politics. Rather than dismiss change without engaging the political process, Bitcoin's defense will require continued revitalization. Stakeholders must remain vigilant and engaged, revisiting the Socratic process behind the formal BIPs as well as the vast literature of informal and often ferocious debates.

***Authors**: Ninos Mansor, Omar Yehia, Ninor Mansor*