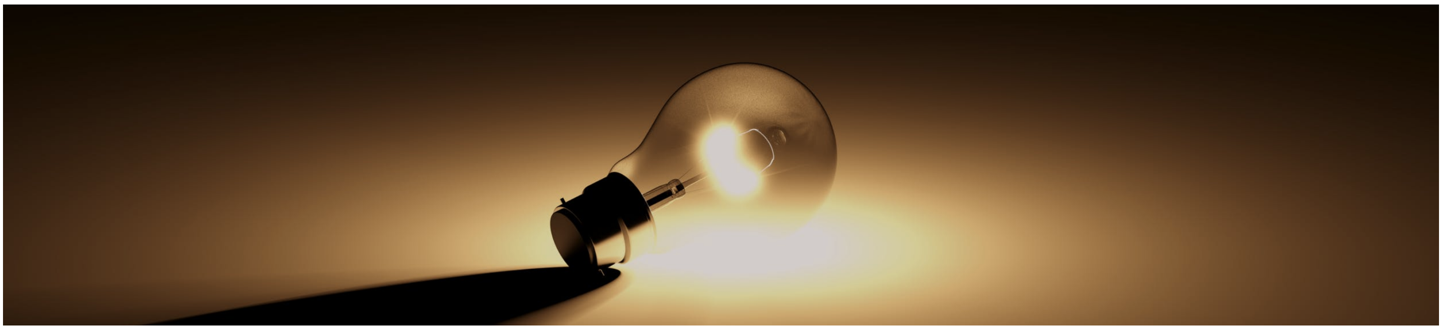
A Look at Innovation in Bitcoin's Technology Stack

Lucas Nuzzi
Dec 3 · 11 min read



Bitcoin has come a long way over the past ten years. Relative to the first iteration of its software, the quality and reliability of current implementations has remarkably improved. Rapidly and organically, Bitcoin was able to lure a legion of developers to dedicate thousands of hours to improve, and at times revamp, most of its underlying codebase.

Nevertheless, Bitcoin is still the same. Much like a constitution, the core set of consensus rules that define its monetary properties, such as its algorithmic inflation and hard-coded supply, remain unchanged. Time and time again, factions have attempted to change these core properties, but all hostile takeovers thus far have failed. It's often a painful process, but one that highlights and solidifies two of Bitcoin's biggest virtues:

1. **No single party can dictate how Bitcoin evolves**
2. **The lack of centralized control protects Bitcoin's monetary properties**

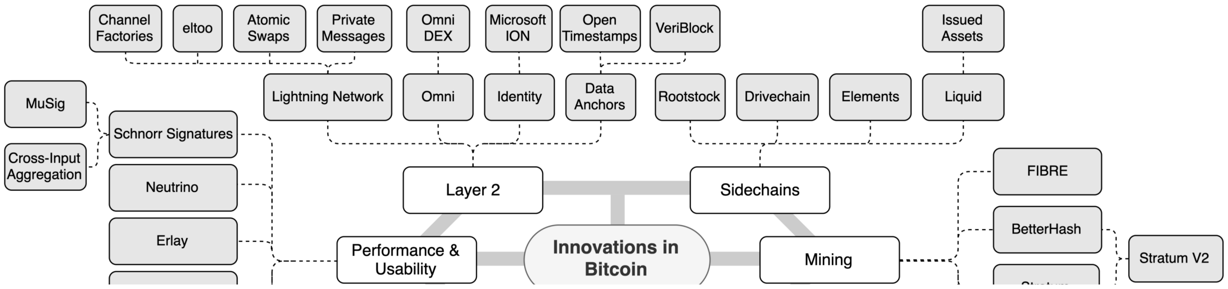
Interestingly, these are the rules that attract cypherpunks and institutional investors alike. These are the rules that make bitcoin an unprecedented type of money. However, these are also the rules that make developing software atop Bitcoin more challenging than any other digital asset. In essence, Bitcoin’s constitution awards developers a limited toolkit so that they can’t infringe upon its monetary policy. There’s too much at stake to *move fast and break things*.

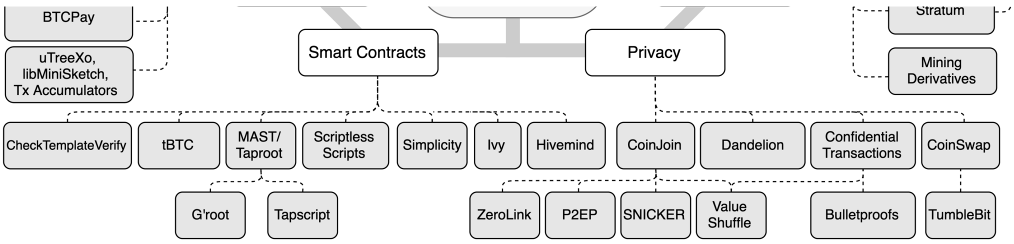
That means innovation in Bitcoin requires creativity, patience, and perhaps most importantly, ego-minimization. After all, the fundamental rules embedded in Bitcoin’s constitution ultimately supersede technology. This is why Silicon Valley has had a hard time understanding Bitcoin’s value proposition, it’s not just a technology, financial instrument, or consumer application; it’s an entire monetary system *supported* by technology. Changing Bitcoin’s constitution requires a quasi-political process that can infringe upon its monetary properties, therefore, technological innovation is implemented as modules.

As often pointed out, Bitcoin’s modular approach to innovation is analogous to the evolution of the Internet’s protocol suite, whereby layers of different protocols specialized in specific functions. Emails were handled by SMTP, files by FTP, web pages by HTTP, user addressing by IP and packet routing by TCP. Over the years, each of these protocols evolved to provide the full experience you’re having this very second.

In Spencer Bogart’s excellent post on the emerging Bitcoin technology stack, he makes the case that **we are now witnessing the beginning of Bitcoin’s own protocol suite**. As it turned out, the inflexibility of Bitcoin’s core layer gave birth to several additional protocols that specialize in various applications, like Lightning’s BOLT standard for payment channels. Innovation is both vibrant and (relatively) safe, as this modular approach minimizes systemic monetary risks.

So much is happening at the many layers of Bitcoin’s technology stack, it can be incredibly difficult to keep track of emerging solutions. The diagram below is an attempt to map all relatively new initiatives and showcase a more complete picture of Bitcoin’s technology stack. It is not exhaustive, and it does not signal any endorsement for specific initiatives. It is, nevertheless, impressive to see that innovation is being pushed on all fronts; from *layer 2* technologies, to emerging smart contract solutions:

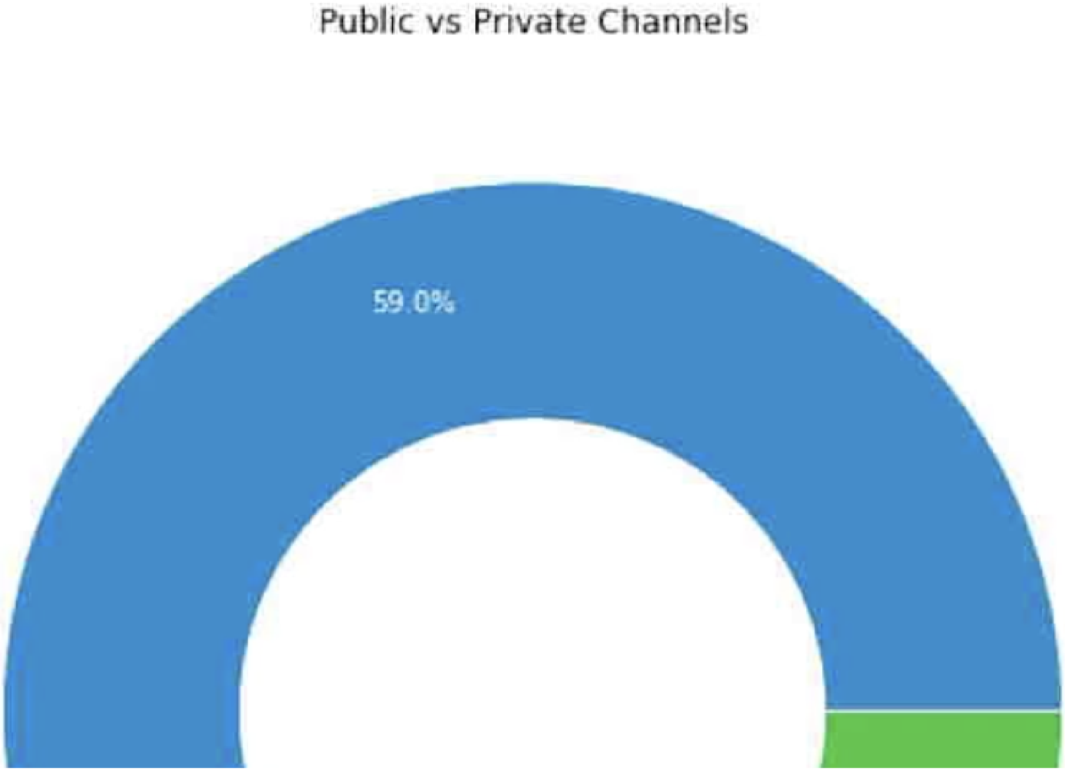


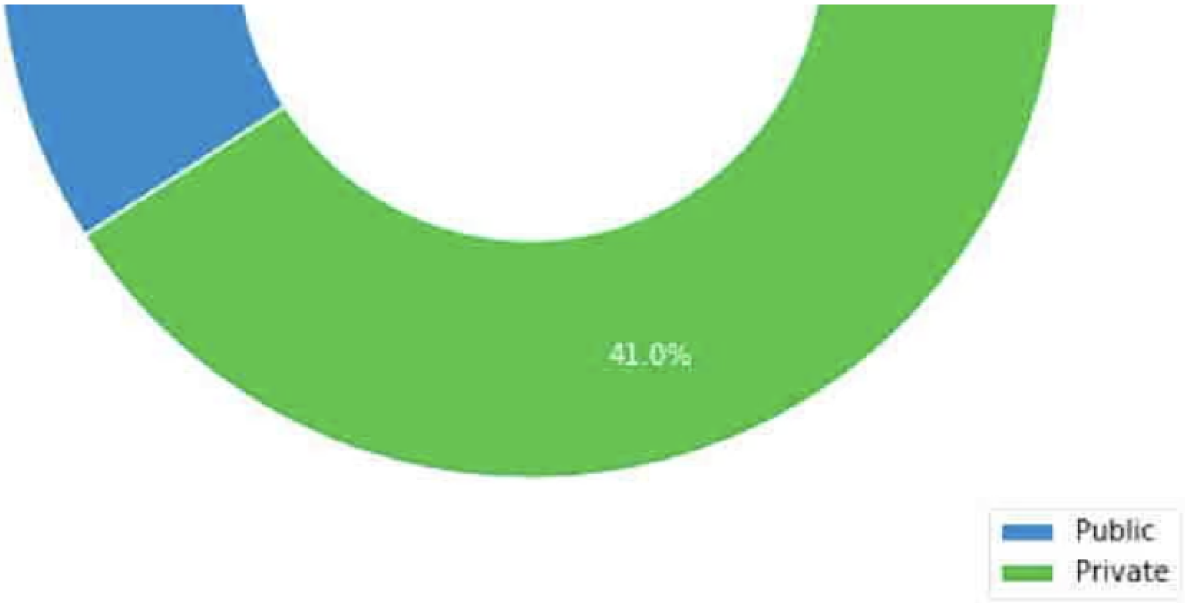


Layer 2

There has been a lot of talk lately about the rate of adoption of the Lightning Network; Bitcoin's most prominent *layer 2* technology. Critics often point at an apparent decline in the number of channels and total BTC locked in Lightning; two metrics frequently used to evaluate user adoption. Although the community has converged on such metrics, it is important to point out that they are fundamentally flawed given the way Lightning works under the hood.

One of the most underrated virtues of the Lightning Network is its straightforward privacy properties. Since Lightning does not rely on global validation of all state changes (i.e. its own blockchain), users can transact privately over using additional techniques and network overlays, like Tor. At this point, we can estimate the percentage of private usage of the Lightning network by analyzing the number of channel opening transactions on-chain, and comparing that to the number of public channels off-chain. **Christian Decker estimates that 41% of Lightning channels are private:**





Source: Christian Decker

Activity happening within these channels is not captured by popular Lightning explorers. As such, **an increase in private usage of Lightning results in a decrease in what can be publicly measured**, leading observers to erroneously conclude that adoption is down. While it is true that Lightning must overcome substantial usability barriers before it can enjoy wide adoption, we must stop using misleading metrics to make assertions about the current state of the network. As Decker pointed out in his talk at the latest Lightning Conference in Berlin, even the above estimate of private vs. public channels is flawed, as the adoption of Schnorr signatures will make channel-opening transactions indistinguishable from regular transactions.

Another interesting recent development in the field of layer 2 privacy was the creation of WhatSat, a private messaging system atop Lightning. This project is a modification of the Lightning deamon which allows for relayers of private messages (the messengers that connect the entities communicating) to be compensated for their services via micropayments. This decentralized, censorship-and-spam-resistant chat was enabled by innovations in LND itself, such as recent improvements in the lightning-onion, Lightning’s own onion routing protocol.

The growth of *Lapps*, or Lightning Applications, demonstrate the wide applicability of these innovations when it comes to consumer applications, from a Lightning-powered cloud computing VPS to an image hosting service that shares ad revenue via microtransactions. And that’s just layer 2 innovation within Lightning. More generally, we define *Layer 2* as a suite of applications that use Bitcoin’s base layer as a *court* where exogenous events are reconciled and disputes are settled. As such, the theme of *data* *anchoring* on Bitcoin's blockchain is much broader, with companies like Microsoft pioneering a decentralized ID system atop Bitcoin. Such initiatives increase the demand for on-chain reconciliation and are instrumental for the long-term development of a Bitcoin fee market.

Smart Contracts

There are also a number of projects attempting to bring back expressive smart contract functionality to Bitcoin in a safe and responsible way. This is a significant development, because starting in 2010, several of the original Bitcoin opcodes (the operations that determine what Bitcoin is able to compute) were removed from the protocol. This came after a series of terrifying bugs were unveiled, which led Satoshi himself to disable some of the functionality of Script, Bitcoin's programming language.

Over the years, it became crystal clear that there are non-trivial security risks that accompany highly-expressive smart contract functionality. The common rule of thumb is that the more functionality is introduced to a virtual machine (the collective verification mechanism that processes opcodes), the more unpredictable its programs will be. More recently, however, we have seen new approaches to smart contract architecture in Bitcoin that can minimize unpredictability, but also provide vast functionality.

The devise of a new approach to Bitcoin smart contracts called Merkleized Abstract Syntax Trees (MAST) has ignited a new wave of supporting technologies that attempt to optimize the trade-offs between security and functionality. Most prominently is Taproot, an elegant implementation of the MAST structure that enables an entire application to be expressed as a Merkle Tree, whereby each branch of the tree represents a different execution outcome. Along with Taproot will come a programming language called Tapscript, which can be used to more easily express the spend conditions associated with each branch of the Merkle Tree.

Another interesting innovation that has recently resurfaced is a new architecture for the implementation of covenants, or spend conditions, on Bitcoin transactions. Originally proposed as a thought experiment by Greg Maxwell back in 2013, covenants are an approach to limit the way balances can be spent, even as their custody changes. Although the idea has existed for nearly seven years, covenants were impractical to be implemented before the advent of Taproot. Now, a new opcode called OP_CHECKTEMPLATEVERIFY (formerly known as OP_SECURETHEBAG) is leveraging this new technology to potentially enable covenants to be safely implemented in Bitcoin.

At first glance, covenants are incredibly useful in the context of lending (and perhaps bitcoin-based derivatives) as they enable the creation of policies like clawbacks to be attached to specific BTC balances. But their potential impact on the usability of Bitcoin goes vastly beyond lending. Covenants can allow for the implementation of things like Bitcoin Vaults, which, in the context of custody, provide the equivalent of a second private key that allows a party that has been hacked to "freeze" stolen funds. There are so many other applications of this technology, like Non-Interactive Payment Channels, Congestion Controlled Transactions, CoinJoins, it truly deserves a standalone post. For more on this, check out Jeremy Rubin's BIP draft.

It is important to note that Schnorr signatures are the technological primitive that make all of these new approaches to smart contracts possible. After Schnorr activates, even edgier techniques being can be theorized, such as Scriptless Scripts, which could enable fully private and scalable Bitcoin smart contracts to be represented as digital signatures (as opposed to opcodes). Similarly, Discreet Log Contracts also employ the idea of representing a smart contract's execution outcome as a digital signature for better privacy and scalability. Together, these new approaches may enable novel smart contract applications to be built atop Bitcoin and Schnorr is the basis of it.

Mining

There have also been some interesting developments in mining protocols, especially those used by mining pool constituents. Even though the issue of centralization in Bitcoin mining is often wildly exaggerated, it is true that there are power structures retained by mining pool operators that can be further decentralized. Namely, pool operators can decide which transactions will be mined by all pool constituents, which grants them considerable power. Over time, some operators have abused this power by censoring transactions, mining empty blocks and reallocating hashing output to other networks without the authorization of constituents.

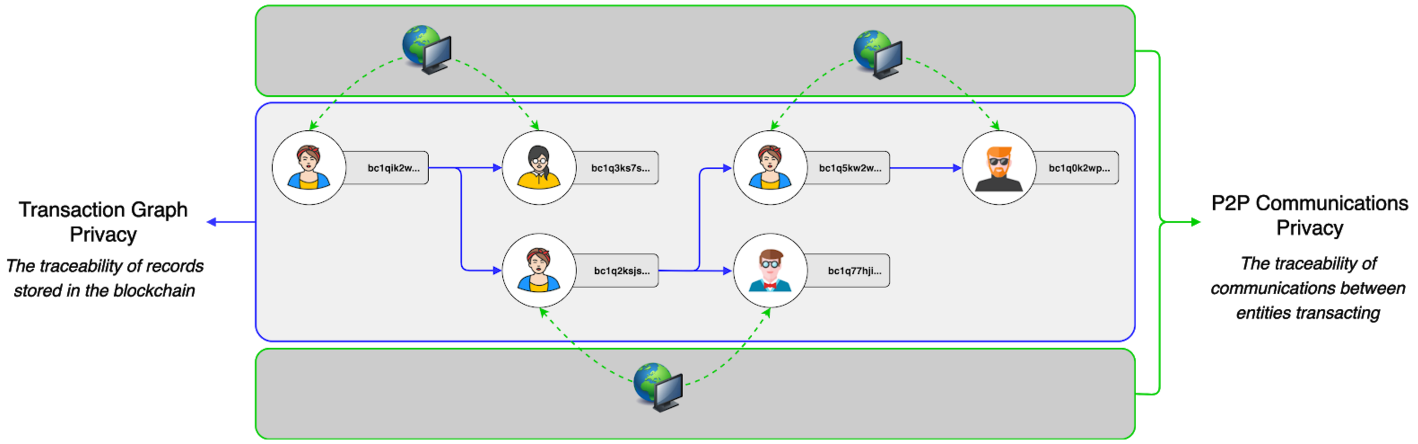
Thankfully, there are technologies that are attempting to flip that power structure upside down. One of the most substantial changes coming to Bitcoin mining is the second version of Stratum, the most popular protocol used in mining pools. Stratum V2 is a complete overhaul that implements BetterHash, a secondary protocol that enables mining pool constituents to decide the composition of the block they will mine and not the other way around. Stratum V2 also implements several optimizations, and allows mining pool constituents to better communicate and coordinate.

Another interesting development in the mining industry that should contribute to more stability is reignited interest in hashrate and difficulty derivatives. These can be particularly useful for mining operations that wish to hedge against hashrate fluctuations and difficulty readjustments. While these derivatives have yet to be productized, this marks an interesting evolution in the industrialization of Bitcoin mining.

Privacy

After our report on Schnorr signatures, some privacy-coin advocates were outraged by the suggestion that *sufficient* privacy may be optionally achieved in Bitcoin at some point. Although this suggestion may challenge theses around the long-term value proposition of privacy assets, there are a host of emerging protocols that can bring better privacy into Bitcoin. Although it is likely that privacy in Bitcoin will continue to be more of an art than a science, there have been interesting innovations on this front that are worth highlighting.

Before we delve into specific privacy innovations, it's important to highlight that the biggest impediment to private transactions across digital assets is the fact that most solutions are half-baked. Privacy assets that focus on transaction-graph privacy often neglect network-level privacy, and vice versa. Both vectors suffer from a lack of maturity and usage, which makes transactions easier to de-anonymize via statistical traceability analysis at either the P2P network layer or the blockchain layer.


Transaction Graph Privacy
The traceability of records stored in the blockchain
bc1qik2w...
bc1q3ks7s...
bc1q5kw2w...
bc1q0k2wp...
bc1q2ksjs...
bc1q77hji...
P2P Communications Privacy
The traceability of communications between entities transacting

Thankfully, there are several projects pushing boundaries on both fronts.

When it comes to transaction-graph privacy, solutions like P2EP and CheckTemplateVerify are interesting because **privacy becomes a by-product of efficiency.** As novel approaches to CoinJoin, these solutions can increase the adoption of private transactions by users that are solely motivated by lower transaction fees. Although privacy guarantees are still suboptimal under a CoinJoin model, unshielded sent amounts can still be beneficial, as they preserve the auditability of Bitcoin’s supply and free float.

If lower transaction fees become a motivator and lead to an increase in Bitcoin’s anonymity set (the % of UTXOs that are CoinJoin outputs), de-anonymization via statistical clustering analysis will become even more subjective than it already is. Some blockchain analysis companies have been able to trick law enforcement agencies into believing an assigned probability that a UTXO belongs to a specific user, but the underlying model is already extremely nuanced and fragile. If the majority of UTXOs become CoinJoin outputs, that might break existing approaches to clustering.

Before that can happen, there’s a tremendous amount of work that needs to be done on the usability front so that all Bitcoin users, tech savy or not, have equal access to privacy mechanisms. Beyond P2EP and CheckTemplateVerify, a recent development in usability was the proposal of SNICKER (Simple Non-Interactive CoinJoin with Keys for Encryption Reused), a novel way to generate CoinJoins with untrusted peers. SNICKER combines several technologies to grant users access to CoinJoin transactions without having to trust or interact with their peers.

Progress is also noticeable in protocols that aim to improve the privacy and efficiency of P2P communications. Over the course of 2019, the privacy-preserving network protocol Dandelion was successfully tested across multiple cryptonetworks. Even though privacy in transaction propagation is not a silver bullet when it comes to the full spectrum of P2P communication, protocols like Dandelion can still meaningfully increase user privacy by hiding the originating IP address of a nodes broadcasting a transaction.

A final development in Bitcoin’s networking stack worth highlighting is a new transaction relay protocol called Erlay. Although still at a very early development stage, Erlay is an important innovation because it can considerably reduce the bandwidth requirements of running a Bitcoin full node. If implemented, Erlay’s efficiency gains can enable users to participate in transaction relay, which is bandwidth intensive, and continuously validate the chain, especially in countries where Internet Service Providers impose caps on bandwidth.

The Tip of the Iceberg

It is incredibly difficult to track all the innovation happening in Bitcoin, and this post is just a scratch on the surface. This brings us to the key takeaway of this piece: Bitcoin, in its totality, is a constantly evolving suite of protocols. The modular approach to innovation described here is important, as it plays a key role in minimizing politicism in the evolution of Bitcoin and protects its fundamental monetary properties. Remember this article the next time someone claims Bitcoin is a static technology.

Connect with DAR

If you would like to learn more about DAR, click here to reach out. For our free daily newsletter chocked full of the highest quality crypto news and information, sign up here.

Blockchain Bitcoin Lightning Network Mining