

Bitcoin Improvement Proposals (BIPs):

Bitcoin is decentralized and open-source, which means that there's no centralized authority that determines protocol upgrades and that anyone can freely use, modify, and change the code. This doesn't mean that Bitcoin is governed anarchically. On the contrary, Bitcoin follows a governance model of collaboration. While Bitcoin transactions are immutable and preserved forever on the blockchain, the underlying protocol is being continually improved and upgraded.

Upgrades to Bitcoin's protocol are proposed and executed through BIPs. BIPs provide a standardized process for contributors to propose new ideas to the protocol, test them, and subject them to peer review. This system of checks and balances is intended to allow continual innovation on the protocol, while making sure that improvements are implemented through consensus and collaboration.

The Bitcoin code was originally written entirely by Satoshi Nakamoto as an experiment to validate that a decentralized peer-to-peer currency was actually possible. That meant that in the early days of Bitcoin, there was no standard for collaborating and developing the protocol. Satoshi authored most of the original code himself, along with subsequent updates and technical improvements. He solicited feedback from the Cryptography Mailing List, an internet email list for cryptographers, and eventually created the BitcoinTalk Forum. When someone reported a bug to Satoshi on the code base, Satoshi pushed an update to the Bitcoin protocol and told everyone on the network to upgrade their client. To survive, Bitcoin needed to develop processes that would make it less dependent on one individual, relying instead on a larger community of developers. In the early years, Satoshi had enlisted the help of Gavin Andresen, a developer who was active in the community. When Satoshi announced he was leaving the project in 2011, he handed over the reins to Andresen. Andresen didn't want to accept responsibility for the code completely on his own, so he enlisted the help of four other developers: Pieter Wuille, Wladimir van der Laan, Gregory Maxwell, and Jeff Garzik. These developers became known as the "Bitcoin Core developers," as they administered the development of the main Bitcoin Core client implementation. Historically, the Bitcoin Core developers have been responsible for the majority of development on the Bitcoin protocol. They maintain Bitcoin's codebase and are the only ones with the ability to push live code to the Bitcoin Core client. While hundreds of people have contributed code to Bitcoin over the years, only a dozen or so have ever had commit access to the code base. Core developers engage in a process of rough consensus to determine what is ultimately included.

The BIP process was established to open up discussion around Bitcoin's development process and make it more accessible by more members of the community. It was intended to formalize many of the processes already in use by Core developers. The BIP, a standard for proposing improvements to the Bitcoin Protocol, was proposed by Amir Taaki in 2011 in BIP 0001. Since the BIP process was established, there have been 191 contributors to the BIP Github repository. The goal of the BIP process is to allow anyone to propose improvements to the Bitcoin protocol, but also to thoroughly vet ideas for security and feasibility, before implementing any code that could threaten the stability of the network. The process is meant to allow the community to establish rough consensus around proposed ideas. Each BIP must move through several different stages before it can be implemented. To be implemented, a BIP must move from the draft stage, to proposed, to final. Along the way, a BIP can be rejected by the community, withdrawn, or replaced. The goal of the draft stage is to format new ideas for Bitcoin into a standardized BIP, and start soliciting feedback from the community. To move the Draft to proposed deems that the draft is complete, and includes a working implementation of the proposal in the draft.

When a BIP's status is changed to proposed, it's now ready to move from discussion to deployment in the actual Bitcoin protocol. To do this, each BIP needs to include specific criteria that outline how real-world adoption can be objectively established. A BIP needs to be implemented into the code through either a soft fork or a hard fork. A soft fork introduces a backward-compatible change to the protocol, meaning that nodes running the latest version of the software remain compatible with nodes running older versions. Hard forks introduce protocol changes that aren't backward-compatible which means that if a significant number of nodes don't upgrade their client to include the new software, the chain splits in two. As a result, hard forks are a much riskier way to implement BIPs. Soft-fork BIPs require activation by "a clear miner majority." The recommended guideline for establishing this majority is that 95% of nodes approve it by upgrading their software to include the BIP. Hard-fork BIPs, on the other hand, require adoption from the entire community. Given the difficulty of meeting the requirements of a hard-fork BIP, no BIPs have actually been implemented via a hard fork. Only when a BIP has been successfully implemented through a hard fork or a soft fork and implemented in the Bitcoin protocol is it considered "Final."