A softfork is a change to the bitcoin protocol wherein only previously valid [blocks](https://bitcoin.org/en/glossary/block)/transactions are made invalid. Since old [nodes](https://bitcoin.org/en/glossary/node) will recognise the new [blocks](https://bitcoin.org/en/glossary/block) as valid, a softfork is backward-compatible.

A **softfork** is a change to the bitcoin protocol wherein only previously valid blocks/transactions are made invalid. Since old nodes will recognize the new blocks as valid, a softfork is backward-compatible. When a majority of miners upgrade to enforce new rules, it is called a **miner-activated softfork** (MASF). When full nodes coordinate to enforce new rules, without support from miners, it is called a **user-activated softfork** (UASF).

New transaction types can often be added as softforks, requiring only that the participants (sender and receiver) and miners understand the new transaction type. This is done by having the new transaction appear to older clients as a "pay-to-anybody" transaction (of a special form), and getting the miners to agree to reject blocks including these transaction unless the transaction validates under the new rules. This is how [pay to script hash](https://en.bitcoin.it/wiki/Pay_to_script_hash) and [Segregated Witness](https://en.bitcoin.it/wiki/Segregated_Witness) were added to Bitcoin.

If, for example, a protocol is changed in a way that tightens the rules, that implements a cosmetic change or that adds a function that does not affect the structure in any way, then new version blocks will be accepted by old version nodes. Not the other way around, though: the newer, "tighter" version would reject old version blocks.

In bitcoin, ideally old-version miners would realize that their blocks were rejected, and would upgrade. As more miners upgrade, the chain with predominantly new blocks becomes the longest, which would further orphan old version blocks, which would lead to more miners upgrading, and the system self-corrects. Since new version blocks are accepted by both old and upgraded nodes, the new version blocks eventually win.

For instance, say the community decided to reduce the block size to 0.5MB from the current limit of 1MB. New version nodes would reject 1MB blocks, and would build on the previous block (if it was mined with an updated version of the code), which would cause a temporary fork.

This is a soft fork, and it's already happened several times. Initially, Bitcoin didn't have a block size limit. Introducing the limit of 1MB was done through a soft fork, since the new rule was "stricter" than the old one. The pay-to-script-hash function, which enhances the code without changing the structure, was also successfully added through a soft fork. This type of amendment generally requires only the majority of miners to upgrade, which makes it more feasible and less disruptive.

Soft forks do not carry the double-spend risk that plagues hard forks, since merchants and users running old nodes will read both new and old version blocks.

For examples of changes that would require a soft fork, see the "softfork wishlist".

Com um [**Soft fork**](http://www.criptomoedasfacil.com/tag/soft-fork), somente os mineradores terão que atualizar a plataforma, ou então eles vão acabar na blockchain perdedora. Usuários e comerciantes podem continuar executando nodos antigos, que agora aceitarão os blocos mais recentes que os mineradores encontrarem.

Softforks procuram preservar o código original, fazendo com que pequenas mudanças no código, sejam implementadas no projeto original, todas elas, aceitas pela comunidade de desenvolvedores, nodos, usuários e mineradores.

As novas regras permitem que um novo [**subconjunto**](https://pt.wikipedia.org/wiki/Subconjunto) derivado dos blocos válidos anteriormente, faça parte da cadeia de blocos original.

Portanto, todos os novos blocos são considerados válidos pela versão mais recente além de também serem validados por quem roda a versão antiga.

Bom, para algo acontecer alguém tem que tomar a decisão e no caso das criptomoedas isso não é diferente. Para que uma atualização entre em vigor, ela deve passar antes no consenso da comunidade, ou seja, a grande maioria dos usuários devem votar e decidir se tal atualização deve ser aplicada ou não. Essa votação é feita através do próprio sistema do bitcoin e pode levar alguns minutos ou até várias semanas. Não se preocupe se você nunca votou, normalmente esse processo é feito pelos mineradores, e os usuários comuns, aqueles que apenas usam a moeda como forma de pagamento ou coisas do tipo, não passam por esse processo.

Como acontece frequentemente com aplicativos de celular, algumas atualizações são feitas sem que você precise baixar uma nova versão do aplicativo. Esse é o mesmo processo da soft fork: o sistema de uma criptomoeda é aprimorado para uma versão melhor, mas pode ser que o usuário nem note — as atualizações são feitas mantendo o sistema compatível com a versão anterior. As soft forks podem ser uma correção de pequenas falhas que não comprometem a moeda ou uma melhoria em algum processo interno.

It’s possible for anybody to submit a BIP, which stands for Bitcoin Improvement Proposal, and contribute to the development of Bitcoin. A BIP proposes an update to the Bitcoin code- which can be either the Bitcoin protocol itself or its documentation.

If the BIP is met by general community approval, it can be pushed out with the next update of the Bitcoin Core Client. At this point, nodes and miners are able to decide whether they want to update their software to the next version or not.

Most Bitcoin software changes aren’t critically important, so they don’t require a significant amount of attention. In many cases, it’s not essential for users to update their software. In some cases, however, software changes are so important that they require everybody to update their client at the same time in order for the network to continue to function.

UASF stands for User Activated Soft Fork. It’s a mechanism where the activation time of a soft fork occurs on a specified date enforced by full nodes, a concept sometimes referred to as the economic majority. A UASF requires a lot of industry support and coordination, which is good practice for eventual hard forks which requires even more industry coordination. In the past, a UASF was successfully carried out to activate the P2SH soft fork (BIP16).

What is a MASF?

MASF stands for Miner Activated Soft Fork. It’s a mechanism by which miners trigger activation of soft forks when a majority signals the readiness to upgrade. This allows for a faster activation time for the soft fork, leaving full nodes to upgrade at their leisure. This method is a tradeoff, because it puts trust in the hash power actually enforcing the new rules. If they do not, it can cause various invalid chains on the network. For example, this was the case with BIP66, when hashpower indicated they had upgraded when in fact more than 50% had not. The other tradeoff is that the method allows a small number of hash power to veto activation of the soft fork for everyone on the network. Overall, if everyone cooperates, this method is very convenient and has been used to successfully activate multiple soft forks in the past such as BIP65 CLTV and BIP112 CSV.

What is BIP148?

BIP148 is a UASF that is designed to cause the existing SegWit MASF deployment to cause activation in all existing SegWit capable node software (which currently is 80% of the network nodes). How does BIP148 Work? From August 1st, 2017, miners are required to signal readiness for SegWit by creating blocks with the version bit 1. This will cause all SegWit ready nodes, which make up over 80% of the network, to activate and begin enforcement. Link for reference: luke.dashjr.org/programs/bitcoin/files/charts/segwit.html. Miners must also check blocks prior to their own and ensure that they also signal for SegWit, and only build on those blocks.

Soft Forks

A soft fork is an updated version of the protocol which is backward compatible with previous versions whereby older versions of the Bitcoin software will recognize new blocks. Conducting a soft fork of the Bitcoin software is less challenging on the network as only a majority of node users need to upgrade. All nodes, whether updated or not will continue to recognize new blocks and maintain compatibility on the Blockchain.

What Could Go Wrong?

The soft fork could become the shortest chain and shunned off by the network when it is supported by only a minority of hash power in the network. Or, it can act like a hard fork, and one chain can be dislodged.

Past Successes Of Soft Forks

Soft forks have been the most commonly used option to upgrade the Bitcoin Blockchain so far because of their capability of lowering the risk of splitting the network. Software upgrades like BIP 66 – which dealt with signature validation – and P2SH – which altered bitcoin’s address formatting – are past examples of successful soft forks.

Soft forks have been used on the Bitcoin and Ethereum blockchains, among others, to implement new and upgraded functionalities that are backwards compatible.

SegWit is a “soft fork” (a backwards compatible code change) that has been implemented on some cryptocurrencies (such as Litecoin). It is a scaling solution meant to solve Bitcoin’s blockchain size limitations by allowing more transactions to be added in each block thereby increasing Bitcoin transaction speeds. The trick involves splitting a transaction into two segments, moving the unlocking signature (“witness” data) from the original segment to a “witness” segment (see details on how SegWit works here). It is up to Bitcoin users, including entities like Coinbase, to embrace SegWit. As more entities embrace SegWit, Bitcoin transaction speeds will become faster.

--Azul: Bitcoin.org

--Vermelho: BitcoinWiki

--Verde: Medium

Referencias:

1 <https://bitcoin.org/en/glossary/soft-fork>

2 https://medium.com/@elombrozo/forks-signaling-and-activation-d60b6abda49a

3 https://bitcoin.org/en/developer-guide#consensus-rule-changes

4 https://www.techtudo.com.br/noticias/2017/12/atualizacoes-na-bitcoin-o-que-sao-e-como-acontecem-os-forks.ghtml

5 https://bitcoinexchangeguide.com/bitcoin-blockchain-forks-history/

6 http://www.uasf.co/

7 https://guiadobitcoin.com.br/o-que-sao-e-por-que-acontecem-os-forks-do-bitcoin-entenda-de-uma-vez-em-nosso-guia-completo/

8 https://www.criptomoedasfacil.com/o-que-e-fork-qual-a-diferenca-entre-softfork-e-hardfork/

9 https://bcmy.io/blog/what-does-a-hard-fork-or-soft-fork-mean-for-bitcoin-and-ethereum/

10 https://cryptocurrencyfacts.com/segwit-and-the-lightning-network-explained/