Cryptocurrency Network Forks, Explained

Author	josh
Date	2020-09-08 19:10:19

Overview

One of the beautiful features of open blockchains is their ability to "fork" in the event of an irreconcilable difference between community members. Many forks have happened in the short history of cryptos - Bitcoin to Bitcoin Cash and Ethereum to Ethereum Classic, to name two major ones. But what actually happens, technically, during at network fork? Does every fork have to be contentious? Lets look at what happens during a fork and some different types of forks.

Split, Split, Split - What Forks Mean

How a "Fork" Works

How does a fork actually occur on a cryptocurrency network? First, we need to explore and understand what a blockchain is and the role blockchains play in cryptocurrencies. A *blockchain* is a globally distributed ledger of transactions between parties. For a set period of time (dependent on the network), transactions are batched together to form a new *block* that is added to the chain. In Bitcoin, for example, new blocks are added approximately every ten minutes.

The important thing to note is that these blocks *must* follow an agreed upon set of rules to be included. Transactions must follow rules, the block reward for miners must be followed, proof of work must be valid, and more. All rules must be followed for the nodes on the network (miners and other full nodes) to recognize the block as valid and pass it around as part of the blockchain. If the block is invalid, then it is rejected.

So what happens when the community wants to change the rules that the software follows? This is when the fork happens! A fork happens when nodes start producing blocks that follow a *new set of protocol rules*. The blockchain diverges at this block into a *new* chain, with the same history as the old one up until that point.

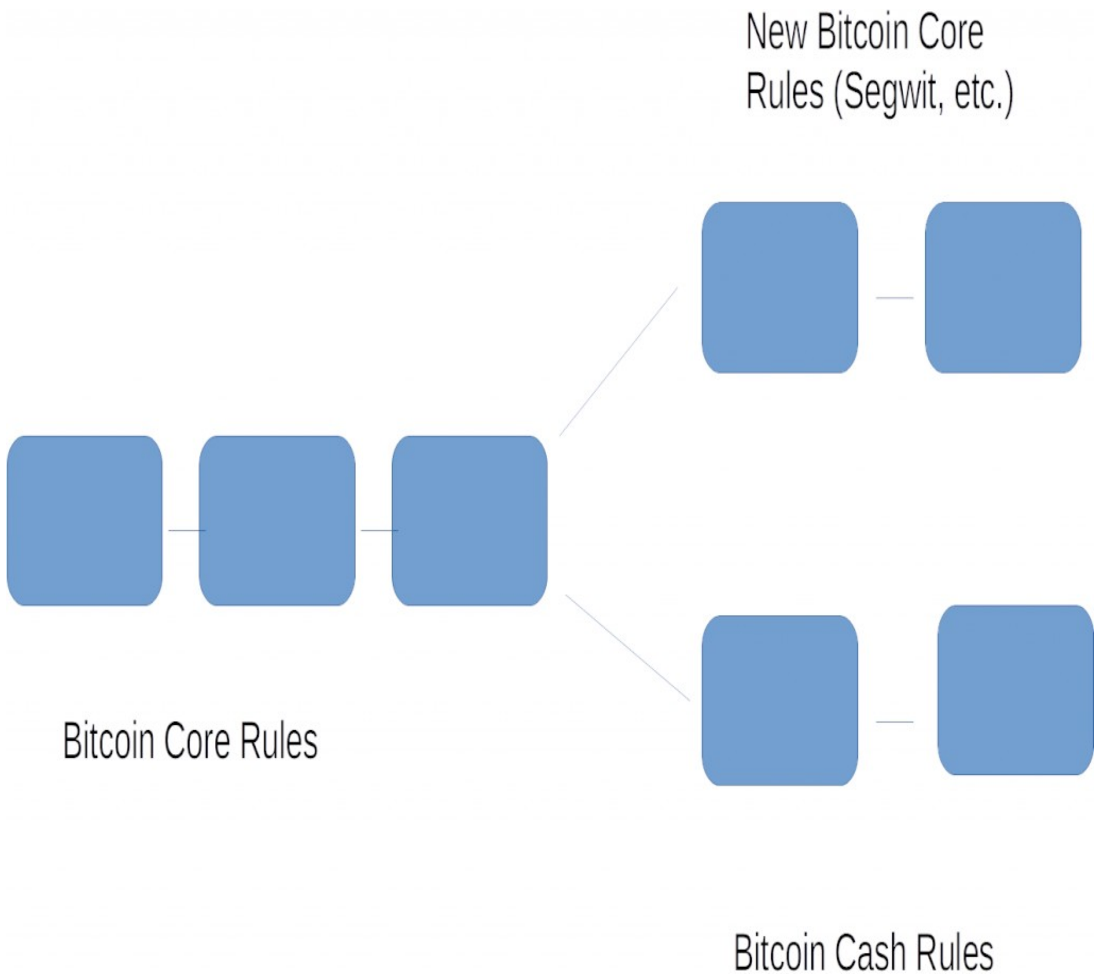
Let's look closer at some types of forks to help us understand this concept closer.

Hard Forks (That Create New Currencies)

The first and most prominent example of forks are *hard forks* that create new cryptocurrencies. These are sometimes referred to as *contentious hard forks*. A prime example of this is the creation of Bitcoin Cash from the Bitcoin chain.

In August 2017, a sizeable contingent of the Bitcoin community was unhappy with changes (or lack thereof) from the Bitcoin Core development team. Bitcoin Core is a reference implementation of a Bitcoin node that *defines the Bitcoin protocol rules*. The Bitcoin Cash community wishes to increase the block size and reintroduce some Bitcoin scripting functionality, among other things. And so, the Bitcoin Cash community introduced new node software implementations such as Bitcoin ABC and Bitcoin unlimited that followed this desired ruleset.

At the time of the split, nodes and miners running Bitcoin Cash implementations such as ABC started creating new blocks that followed their ruleset, while Bitcoin Core clients continued with their ruleset. This created a divergence in the blockchain known as a *hard fork*.



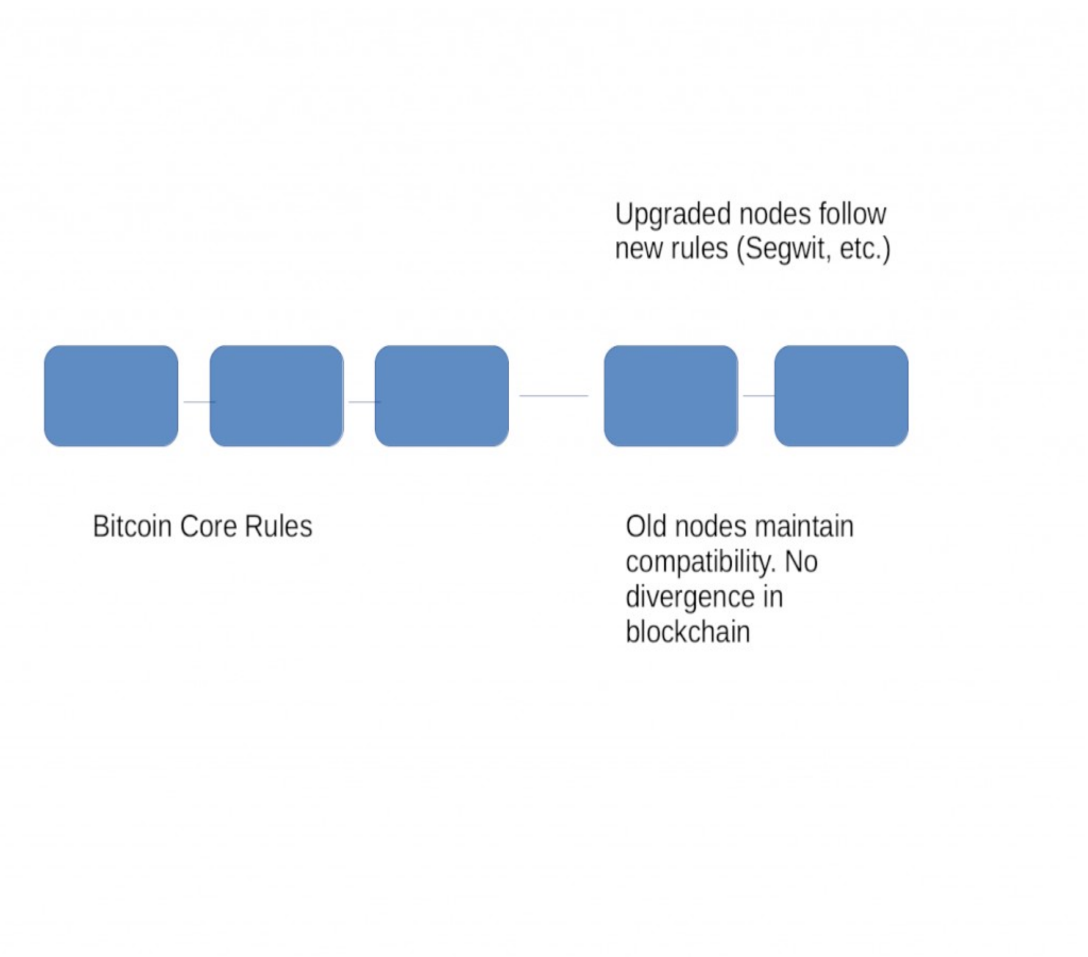
The Bitcoin Cash Hard Fork

Soft Forks

There are also "soft forks". Unlike hard forks, these don't require following a new software version or upgrading to continue using the network as new blocks are added.

A prime example of this is the Bitcoin Segwit ruleset for transactions. Bitcoin Core developer Luke Dashjr figured out how to implement this change to the network without requiring old nodes to upgrade to continue following the Bitcoin chain. Upgraded nodes will recognize and enforce the rules for segwit transactions. Old nodes, however, simply ignore segwit transactions as "anyone can spend" transactions without having to understand the segwit rules.

Soft forks are useful for backward compatibility, which can ultimately make it easier for individuals and companies to continue using cryptocurrencies without constant upgrades. However, it's much easier to rapidly iterate and add new features using hard forks, with much less complexity than soft forks require.


Upgraded nodes follow new rules (Segwit, etc.)
Bitcoin Core Rules
Old nodes maintain compatibility. No divergence in blockchain

A soft fork, with no divergence in the blockchain

Chain Splits

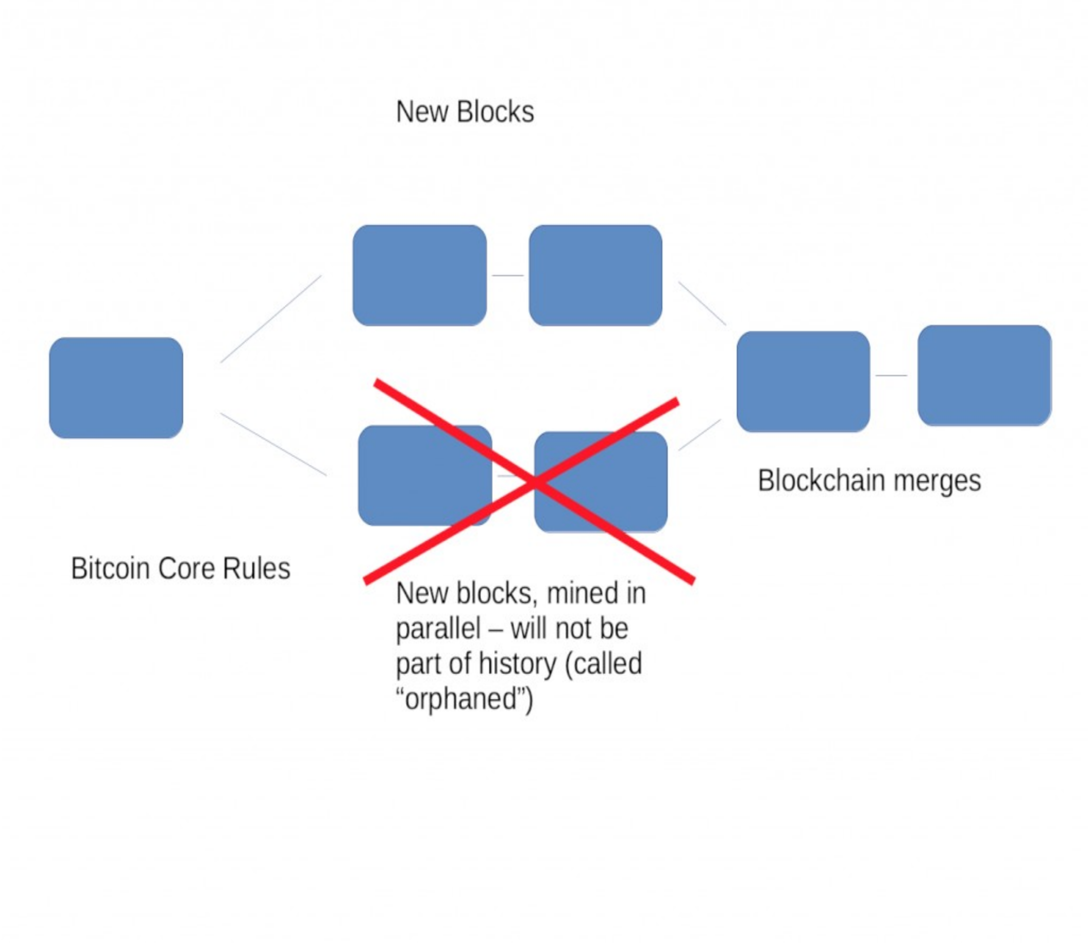
It's also important to note that not all hard forks result in the creation of new cryptocurrencies. In fact, most hard forks do not!

Hard forks can occur on a single cryptocurrencies' chain in two ways. The first is when two miners are working to create two different blockchains that ultimately re-converge. Miners ultimately follow what is called the longest proof-of-work chain. Sometimes, miners in different parts of the world may create 2-3 blocks that are different than 2-3 blocks added somewhere else. However, these minor forks usually resolve themselves within a few blocks.

This sometimes happens due to software upgrades that don't change the ruleset, but result in software bugs. In Bitcoin, a change from BerkelyDB to LevelDB cause a sustained chain split. BerkelyDB was unable to handle larger but valid blocks, and so could not follow the chain that

LevelDB nodes were running. Ultimately the community was able to quickly respond and fix old nodes or get users to upgrade.

As well, hard forks occur when the community agrees to upgrade the software for a new ruleset. This does diverge the blockchain as new nodes follow blocks with the new rules, but the old chain simply ends as users no longer follow the old rules. This can be used for rapid development and the introduction of new features with less complexity.


New Blocks
Blockchain merges
Bitcoin Core Rules
New blocks, mined in parallel – will not be part of history (called “orphaned”)

A chain split, resulting in orphaned blocks but no new currency

Forks...Not So Scary After All

With some understanding, we can see that blockchain forks aren't necessarily a bad thing at all. Splits in the community, while contentious, are a feature of the open-source ecosystem. Sometimes, it's possible to create soft forks that don't require users to upgrade to introduce new features. And finally, hard forks can and due occur due to software bugs or the intentional introduction of new rules on one cryptocurrency chain. Forks are a part of the system that happen, and aren't necessarily indicative of problems or community contention.