Thursday, 19 March, 2020

The Bridge

Forks: A double-edged sword

Abstract

Forks give blockchain communities the capacity to change the rules as preferences may change or an update is proposed as a bug is fixed for instance. Some of these changes may be very profound and cannot be bridged with earlier versions or a part of the community may not endorse them. As a result, forks may lead to chain split, in other words, the creation of a new blockchain in addition to the old one.

Introduction

In earlier editions of the Bridge, we explored how mining[link1] works and consensus[link1] is employed in blockchains. In this edition, we venture into different types of forks, why they occur, and how they affect blockchains.

What is a fork?

Every blockchain is governed by a set of rules that are named consensus algorithms. A fork is a change in the underlying rules of a blockchain. The change in rules may or may not be backward compatible. These changes may or may not occur with every stakeholder's consensus.

What do forks really mean?

Due to its decentralised structure, blockchain borrows ideas from democracy. To make a change in the rules, or the laws, that govern the system, every eligible person is free to propose an initiative to improve or change some rules. If this initiative receives adequate (majority) backing by community, rules are updated and imposed to all others.

In some situations, the new rules do not please a part of the community in such a way that it wants to make secession. In the blockchain world, a secession is a chain split.

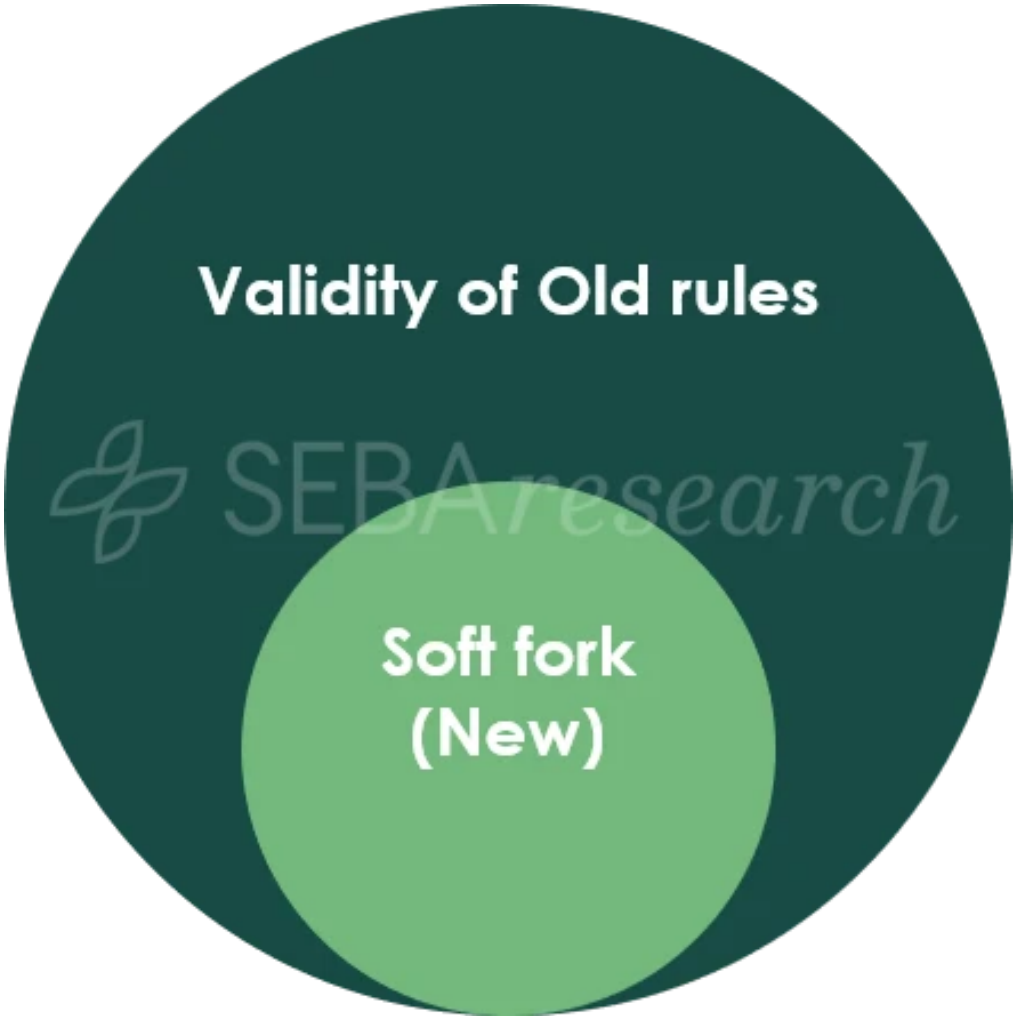
Forking is thus an important right given to the community to govern the system it is using. By granting this right, a blockchain with many users means that is has a strong support

from the community and is stable.

What are the different types of forks?

A fork is called a *soft fork* if it is backward compatible, meaning that the changes allow nodes on the network govern themselves based on the previous set of rules. For example, when a phone pushes an operating system upgrade, not all the users need to upgrade to a newer version of the operating system. Older versions still work but users cannot take advantage of the feature upgrades in the newer version. Regarding soft forks, shown in figure 1, the new rules must ensure that old transactions are valid. Therefore, new transaction rules are a subset of old transaction rules. It essentially means that with new rules, the universe of valid transactions should strictly reduce. As new rules have to make sure that old rules are still valid, soft forks are difficult to design for developers. However, soft forks are more convenient for users as they are not forced to upgrade their software.

Figure 1: Soft forks



Source: SEBA research, https://vitalik.ca/general/2017/03/14/forks_and_markets.html

A *hard fork* is when old rules are no longer valid, and nodes must adapt to the new rules to participate in the new consensus. An analogy of hard fork is Play Station 4 versus Play Station 3. Users cannot play PS4 games on PS3 and vice-versa.

Hard forks can further be divided into *strictly expanding hard forks* and *bilateral hard forks*. Strictly expanding hard fork is where new rules are applicable in the old version but nodes with older version need to upgrade to validate new transactions.

Figure 2a: Strictly expanding hard fork

Source: SEBA research, https://vitalik.ca/general/2017/03/14/forks_and_markets.html

Bilateral forks are where old and new rules are not compatible with each other. Hard forks allow more flexibility to developers as they do not have to ensure compatibility of new rules with the old ones. Bilateral forks are also known as chain splits as the old and the new chains are no longer compatible with each other.

Figure 2b: Bilateral hard fork

Source: SEBA research, https://vitalik.ca/general/2017/03/14/forks_and_markets.html

An explanation of soft and hard forks using Bitcoin's example

Scaling[1] bitcoin has always been the point of contention among the bitcoin community. There were two groups with their ideologies as to how bitcoin should be scaled further. We will not cover the detailed arguments of both the sides here but the gist is that one wanted to increase the block size and the other wanted to do minimum changes at the base layer protocol and scale bitcoin by using layer two scaling solutions[2].

The group that was not in favour of increasing the block size of the base layer chain proposed a solution called Segregated Witness (SegWit). At a high level, SegWit increases the capacity of the block by segregating the transaction data from signature data. SegWit was launched by the bitcoin core as a soft fork. Therefore, nodes running on the previous version of the software could continue checking transactions. As of now the number of transactions in a block that use SegWit hovers around 55%[link1].

In August 2017, the group that was in favour of increasing the block size from 1MB to 8MB hard forked the original blockchain into a new blockchain called Bitcoin Cash (BCH). After the fork, bitcoin transactions were no longer compatible on the bitcoin cash blockchain. Till the fork, Bitcoin and Bitcoin Cash share the same history of the transaction.

Why forks take place?

Just as any software needs regular maintenance and upgrades, blockchains also need regular upkeep. These upgrades are nothing but forks. Apart from regular maintenance, forks also take place when the community is divided as it was the case with Bitcoin and Bitcoin Cash. Accidental or unintentional forks take place when two different miners propose different valid blocks around the same time. The tie is resolved based on which branch has done more work. If that is the same, miners work on whichever block they received first, and the tie is resolved based on whichever branch is used to build the next block on.

Though such accidental forks are common and are resolved quickly, they can also be the evidence of an ongoing attack. Attackers may try to fork the blockchain to rewrite transactions. This fork monitor[link1] keeps an eye on possible contentious forks on BTC, BCH, and Bitcoin Satoshi Vision (BSV) blockchains.

Impact of blockchain forks

Soft forks are easy to deal with as there is backward compatibility. Hard forks that turn into splitting of the network often arise out of disagreements within the community and are detrimental for both the chains. Chain splits have an impact on the network itself as well as the stakeholders. Before assessing the impact of controversial forks, it is important to understand the different stakeholders in a blockchain ecosystem.

Table 1 shows different stakeholders and how contentious forks affect them

Table 1: Different stakeholders and chain split's impact on them

Stekeholder	Impact
Miners	Miners need to decide on which fork they will support. They have to consider on which chain they can maximise their revenue in the short and long term.
Hardware manufacturers	If there is change in mining algorithm, hardware manufactured for the old chain cannot support the newer chain. This new hardware has to manufactured for the new chain. Hardware manufacturers have to plan their manufacturing based on demand forecasts for both the chains
Developers	If the fork is due to debate related to development, as it was the case with Bitcoin Cash, human capital gets divided between two chains.
Exchanges / Marketplaces	Usually when there is a contentious hard fork, for every address controlled by public private key pair, is airdropeed with the same number of native tokens of new blockchain as the old one. For example if the address xyz123 had 0.1 BTC before the fork took place, it was also given 0.1 BCH after the fork. Exchanges have to build capabilities to ensure users get tokens allotted on the new blockchain.
Investors	Contentious splits are not without turmoil. This invites increased volatility and thus wild swings in price. If derivatives markets are developed, investors can make use of the volatility, but the uncertainty puts a downward pressure on price
Merchants	In case merchants decide to support the fork as well, they have built infrastructure to accept payments in new tokens as well
Wallet developers	Wallet infrastructure needs to be built and maintained to store tokens of the new blockchain

Impact on the network

As there is contention, some of the miners leave the older system in favour of a newer one and this results in a drop in hashrate. The drop in hashrate means the network is less secure and vulnerable to attacks. The second risk arising out of hashrate imbalance is that the chain with significantly higher hashrate can easily attack the chain with lower hashrate to reorg blocks to double-spend or censor transactions. This type of hostile takeover can turn catastrophic for blockchains. We will dive deeper into this type of attack in the next edition where we discuss different types of attacks on blockchains.

Conclusion

The distributed nature of the public blockchains allows them to split in case of disagreements. However, the freedom to separate comes with a cost. It is a double-edged sword. Such splits can prove to be catastrophic in terms of security. And though there is freedom, the network effects seem to stay only with a handful of blockchains. Therefore, it is in the best interest of the communities to resolve differences without causing a chain split.

[1] The capacity of bitcoin network to carry out the number of transactions per second is low. Efforts are ongoing to increase the throughput of bitcoin blockchain. This is commonly referred to as scaling.

[2] Layer two solutions are protocols being built on top of existing blockchain infrastructure to scale the base layer. A prominent example of layer two scaling is Lightning Network built on top of bitcoin.

Authors

Yves Longchamp
Head of Research
SEBA Bank AG

Saurabh Deshpande
Research Analyst
B&B Analytics Private Limited

Ujjwal Mehra
Research Analyst
B&B Analytics Private Limited

research@seba.swiss

Disclaimer

in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have officers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affiliated to such investment.

At any time, investment decisions (including whether to buy, sell or hold investments) made by SEBA and its employees may differ from or be contrary to the opinions expressed in SEBA research publications.

Some investments may not be readily realizable since the market is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be difficult to quantify. Investing in digital assets including cryptocurrencies as well as in futures and options is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may under certain circumstances occur. The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. Tax treatment depends on the individual circumstances and may be subject to change in the future.

SEBA does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specific investor's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of individual investors and we would recommend that you take financial and/or tax advice as to the implications (including tax) prior to investing. Neither SEBA nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information provided in the document.

This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this document.

Research will initiate, update and cease coverage solely at the discretion of SEBA. The information contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. SEBA may use research input provided by analysts employed by its affiliate B&B Analytics Private Limited, Mumbai. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information The compensation of the analyst who prepared this document is determined exclusively by SEBA.

Austria: SEBA is not licensed to conduct banking and financial activities in Austria nor is SEBA supervised by the Austrian Financial Market Authority (Finanzmarktaufsicht), to which this document has not been submitted for approval. France: SEBA is not licensed to conduct banking and financial activities in France nor is SEBA supervised by French banking and financial authorities. Italy: SEBA is not licensed to conduct banking and financial activities in Italy nor is SEBA supervised by the Bank of Italy (Banca d'Italia) and the Italian Financial Markets Supervisory Authority (CONSOB - Commissione Nazionale per le Società e la Borsa), to which this document has not been submitted for approval. Germany: SEBA is not licensed to conduct banking and financial activities in Germany nor is SEBA supervised by the German Federal Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), to which this document has not been submitted for approval. Hong-Kong: SEBA is not licensed to conduct banking and financial activities in Hong-Kong nor is SEBA supervised by banking and financial authorities in Hong-Kong, to which this document has not been submitted for approval. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Hong-Kong where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not "professional investors" within the meaning of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and any rules made thereunder (the "SFO"). Netherlands: This publication has been produced by SEBA, which is not authorised to provide regulated services in the Netherlands. Portugal: SEBA is not licensed to conduct banking and financial activities in Portugal nor is SEBA supervised by the Portuguese regulators Bank of Portugal "Banco de Portugal" and Portuguese Securities Exchange Commission "Comissao do Mercado de Valores Mobiliarios". Singapore: SEBA is not licensed to conduct banking and financial activities in SIngapore nor is SEBA supervised by banking and financial authorities in Singapore, to which this document has not been submitted for approval. This document was provided to you as a result of a request received by SEBA from you and/or persons entitled to make the request on your behalf. Should you have received the document erroneously, SEBA asks that you kindly destroy/delete it and inform SEBA immediately. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Singapore where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not accredited investors, expert investors or institutional investors as defined in section 4A of the Securities and Futures Act (Cap. 289 of Singapore) ("SFA"). UK: This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head office and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product.

SEBA is not an authorised person for purposes of the Financial Services and Markets Act (FSMA), and accordingly, any information if deemed a financial promotion is provided only to persons in the UK reasonably believed to be of a kind to whom promotions may be communicated by an unauthorised person pursuant to an exemption under the FSMA (Financial Promotion) Order 2005 (the "FPO"). Such persons include: (a) persons having professional experience in matters relating to investments ("Investment Professionals") and (b) high net worth bodies corporate, partnerships, unincorporated associations, trusts, etc. falling within Article 49 of the FPO ("High Net Worth Businesses"). High Net Worth Businesses include: (i) a corporation which has called-up share capital or net assets of at least £5 million or is a member of a group in which includes a company with called-up share capital or net assets of at least £5 million (but where the corporation has more than 20 shareholders or it is a subsidiary of a company with more than 20 shareholders, the £5 million share capital / net assets requirement is reduced to £500,000); (ii) a partnership or unincorporated association with net assets of at least £5 million and (iii) a trustee of a trust which has had gross assets (i.e. total assets held before deduction of any liabilities) of at least £10 million at any time within the year preceding the promotion. Any

financial promotion information is available only to such persons, and persons of any other description in the UK may not rely on the information in it. Most of the protections provided by the UK regulatory system, and compensation under the UK Financial Services Compensation Scheme, will not be available.