SEBA

October 2020

The Blockchain Trilemma

The Bridge

Redefining Finance for the New Economy

Table of Contents

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

Contact

research@seba.swiss

Executive summary

In this edition of The Bridge, we present an idea central to the design of any public blockchain: the blockchain trilemma. Trilemma refers to the fact that no blockchain has been able to optimise three qualities simultaneously, decentralisation, security, and scalability.

We discuss the advantages of each of the qualities, why they are desirable and their trade-offs. We illustrate the trilemma with live blockchain examples.

The blockchain trilemma refers to the idea that a public blockchain cannot reach the desired level of decentralisation, security, and scalability all at once.

In this edition of The Bridge, we introduce you to this trilemma and the consequences it has on high profile projects.

1. Introduction

Before diving into the dynamics of the trilemma, we broadly define what scalability, security, and decentralisation mean:

- Scalability is the ability of the blockchain to accommodate a higher volume of transactions
- Security is the ability to protect the data held on the blockchain from different attacks or blockchain's defence against double-spending
- Decentralisation is the redundancy in the network that makes sure fewer entities do not control the network

Blockchain trilemma or scalability trilemma is often just stated as a rule, which is not the case. It is not necessary that blockchain may never achieve optimum levels of decentralisation, security, and scalability. Before diving any further, we need to understand why or how this gets introduced in current public blockchains. We explain the tussle among the three qualities with the example of Bitcoin blockchain.

Bitcoin's breakthrough was that it solved the double-spending problem without a central entity. 'Without central entity' is a key here as double-spending is a trivial problem in centralised settings. The goal, always, was to facilitate the exchange of value between two parties with trust minimisation. Trust minimisation takes place when there are no centralised entities which meant that bitcoin relies on multiple miners (instead of one clearing house). Bitcoin introduces a delay in the form of blocks to ensure that the majority of the miners had sufficient time to verify transactions. It means that sacrificing speed was a conscious choice to ensure trust minimisation or decentralisation. The simplest way to increase speed or scalability is to reverse the decision of introducing time lag to ensure decentralisation. All other blockchains are built with bitcoin in their DNA in some shape or form.

2. The interplay among Scalability, Security, and Decentralisation

The network first needs to agree on the validity of the transaction to settle it. If the system has a large number of participants, the agreement may take time.
Therefore, given similar security parameters, we see that scalability is inversely proportional to decentralisation.

$$\text{scalability} \propto \frac{1}{\text{decentralisation}}$$

Now, assumes that two proof of work blockchains have the same degree of decentralisation and we can think of security as the hashrate of the blockchain. If the hashrate is higher, the confirmation time is lower, and scalability increases with security. Therefore, at constant decentralisation, scalability and security are proportional.

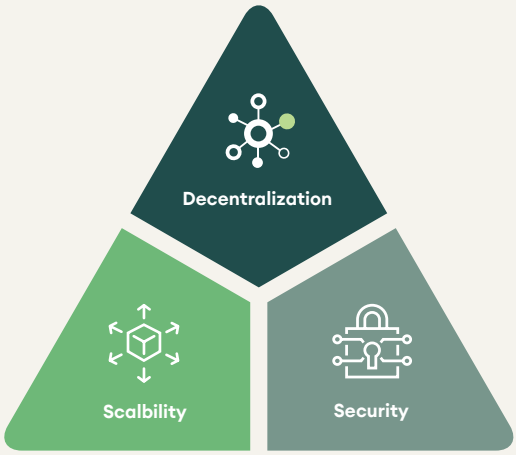
$$\text{scalability} \propto \text{security}$$

Thus, a blockchain cannot optimise for its three desired qualities simultaneously, and it must make trade-offs. through the use of multiple profiles. Specifically, with blockchains, Sybil Attacks are when

The most recent observation of trilemma at play was Ethereum. In the wake of the rise of Decentralised Finance (DeFi) applications this summer, the Ethereum platform usage surged. Ethereum cannot scale beyond a particular point. Therefore, increased demand pushed the transaction fees to the extent that it made prohibitive for some to interact with the blockchain. Increased fees on Ethereum is an illustration of the trilemma, where we could observe that Etehreum did not scale without giving up security or decentralisation. In the case of Ethereum, the emphasis was placed on decentralisation and security, limiting the number of transaction per second (scalability). Users paid a higher fee to incentivise miners to prioritise their transaction.

Ethereum and Bitcoin have preferred decentralisation and security over scalability. Ripple, a payment solution, prefers security and scalability over decentralisation. And EOS favours scalability at the cost of decentralisation and security.

Figure 1: The blockchain trilemma



Source: SEBA Bank AG

3.
Importance of each component in the trilemma

Decentralisation

Decentralised networks emphasise the ability of a blockchain to rely on a sufficiently large number of stakeholders. Decentralisation is observable on various levels: the number of miners, the number of full nodes, the geographical distribution, the number of active developers and so on. It is vital to note that not all blockchains are decentralised to the same extent. Decentralisation is a spectrum; it is not binary.

Advantages of decentralised networks

- Decentralisation allows maintaining consensus without mandating users to trust a single entity
- Decentralisation is desirable because it increases the robustness of the system. It makes the network resistant to censorship and thus allows anyone to use the network uplifting the property rights

Disadvantages and difficulties of decentralised networks

- Decentralisation introduces delay and slows down the network
- It is expensive as it introduces redundancy and thus not desirable for all the applications

Conclusion

We have explored the blockchain trilemma that refers to the idea that a blockchain cannot reach all the three desired qualities (security, decentralisation, and scalability) all at once. Using examples, we presented diverse existing blockchains and showed how their design choice affects the other parameters in the trilemma. Finally, we introduced a few promising solutions.

Scalability

The scalability refers to the capacity a blockchain system to support the growth in size (more users, more use cases and ultimately more transactions), to deal with mass adoption without compromising performance. It essentially boils down to reducing the settlement time of a transaction to increase TPS (transactions per second) or the throughput of the chain.

How can the scalability of a blockchain increase? There are two ways (or a combination of these two ways):

- Reduce the number of entities vetting the transactions (compromise on the decentralisation)
- Reduce the block time, which demands reducing difficulty of the network (compromise on the security)

Advantages of a scalability focussed network

- Allows the network to support a high volume of transactions
- Can be useful in applications where security is not a prime focus, for example, social messaging applications

Disadvantages of a scalability focussed network

- As we mentioned above, the scalability could come at the cost of security
- As a network scales the consensus mechanism will also need to scale which could come at the cost of centralisation

Security

Security is the ability of a blockchain to maintain irrevocability of transactions. It does so by forcing network participants to expend resources to earn rewards. The more resources network participants spend, the more secure the blockchain.

In a recent Ethereum Classic (ETC) attack, the attacker re-organised over 4,000 blocks[1], and the attacker managed to double spend ETC worth close to USDmn 2. Why was the attacker successful? Because the cost to acquire more than 51% of the entire network's hashpower was insignificant compared to the stolen value. In short, the wealth in those 4,000 blocks far outstripped the resources deployed by network participants.

Advantages of a security focussed blockchain

- Enables large value transfers which are quicker and cheaper than traditional value transfers
- The security of public blockchains comes from network participants. Higher security implies higher network effects which are not easy to replicate

Disadvantage with security focussed networks

- Requires more resources, i.e. more investment

4. Promising Solutions

It is no secret that the current scalability of blockchains such as Bitcoin and Ethereum is a limitation. Developers are approaching the problem from various angles. Bitcoin cash's increased block size was an attempt at increasing scalability of bitcoin. However, there is no evidence of its gaining popularity. Bitcoin is attempting to solve it by adding a layer on top of the existing blockchain layer. The idea is the layer two solution will conduct bundle multiple transactions together and query the base layer blockchain only from time to time. Ethereum is taking a somewhat hybrid approach where sharding will scale base layer blockchain, and the community expects different layer two solutions to increase the throughput further. None of the scalability solutions is perfect yet. We will have to wait to find out which of the mentioned solutions works the best.

[1] Block re-organisation means that the same block was mined again with different contents (transactions)

Disclaimer

This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head once and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial investment or to participate in any particular investment. strategy. This document is for distribution only under such circumstances as may be permitted by applicable law. It 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 any locality, state, country or other jurisdiction 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.

No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document, except with respect to information concerning SEBA. The information is not intended to be a complete statement or summary of the financial investments, markets or developments referred to in the document. SEBA does not undertake to update or keep current the information. Any statements contained in this document attributed to a third party represent SEBA's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Any prices stated in this document are for information purposes only and do not represent valuations for individual investments. There is no representation that any transaction can or could have been elected at those prices, and any prices do not necessarily reflect SEBA's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by SEBA or any other source may yield substantially different results.

Nothing in this document constitutes a representation that any investment strategy or investment is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgment in making their investment decisions. Financial investments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Certain services and products are subject to legal restrictions and cannot be offered on an unrestricted basis to certain investors. Recipients are therefore asked to consult the restrictions relating to investments, products or services for further information. Furthermore, recipients may consult their legal/tax advisors should they require any clarifcations. SEBA and any of its directors or employees may be entitled at any time to hold long or short positions in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have offcers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affliated 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 diffcult 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 specifc 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 affliate 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 andfinancial 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 declned 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 offce 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 GBP 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 GBP 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 GBP 5 million share capital / net assets requirement is reduced to GBP 500,000); (ii) a partnership or unincorporated association with net assets of at least GBP 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 GBP 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.

SEBA

SEBA Bank AG
Kolinplatz 15 • 6300 Zug • Switzerland • www.seba.swiss • info@seba.swiss