Thursday, 21 November, 2019

The Bridge

Consensus: the truth seeker

Abstract

- *In the absence of any centralised authority, in decentralised systems there needs to be a way for everyone to come to an agreement.*
- *A consensus mechanism is the way in which different stakeholders in the blockchain ecosystem agree on a given state of the blockchain. Agreeing on its current state is a prerequisite for the functioning of a blockchain.*
- *There are several ways to achieve a consensus, but there cannot be a "one-size-fits-all" approach. Consensus mechanisms have different trade-offs, such as speed, security and decentralisation. As blockchains are built for a specific purpose, the consensus mechanism needs to be selected accordingly.*

The necessity of consensus mechanisms in decentralised systems

With the evolution of commerce, emails have replaced letter mail, databases have replaced physical ledgers, and so on. However, trust, the most fundamental factor in any transaction, remains the same. For two people to engage in a transactional contract, trust is essential – either in each other or in a third party possessing the power to enforce the contract. Public blockchains[1] such as Bitcoin have minimised the trust that needs to be placed in the other party by maintaining a decentralised, *single version of the truth*. And to do this, they need consensus mechanisms.

Consensus mechanisms are designed so that the incentives of the network and individuals are aligned to the maximum possible extent. In other words, each individual stakeholder, though selfish, is given an incentive to behave in a way that is good for the whole network.

We will now explore the Byzantine General's problem in order to gain a better understanding of the need for a consensus mechanism in decentralised systems.

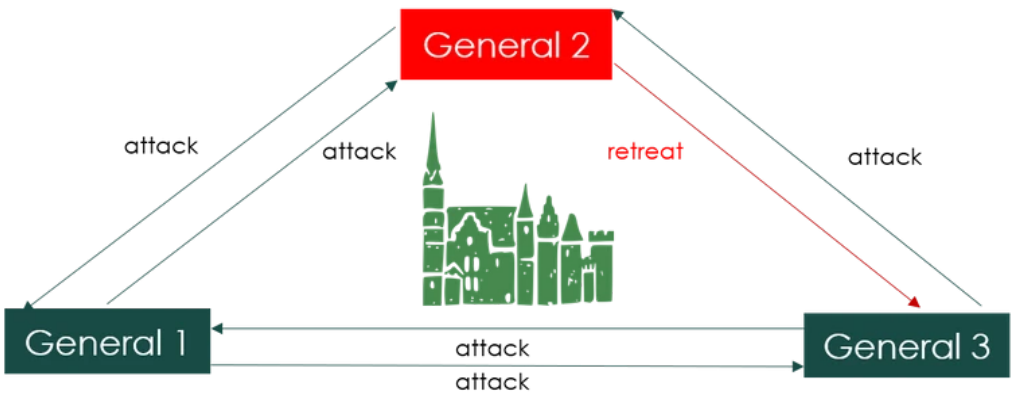
The Byzantine General's problem

This problem troubled computer scientists for a long time and remained unsolved until the Bitcoin protocol was released. According to the problem, the Eastern Roman Empire, or Byzantine Empire, has decided to capture a city that is offering fierce resistance. The three divisions of the Byzantine army, each led by a General, have encircled the city. Each division has two options: attack or retreat. Victory can be achieved only if all the Generals agree on a particular strategy, otherwise they will suffer a brutal defeat. The Generals must communicate with each other to ensure that everyone is in agreement. They can only communicate through messengers, and can only send their message once.

However, there are several potential problems. One or more Generals could be traitors. The messengers could be delayed, killed or compromised. With all these constraints, in a physical world it would be almost impossible for the Generals to reach a consensus and take the city. If you were one of the Generals, how would you act on any message if you didn't know whether the person who had sent it to you was trustworthy and whether the message had been intercepted?

In the above scenario where General 2 is a traitor, there is no way for General 3 to know whether to attack or retreat as he receives contradictory messages from the other Generals. Thus, a consensus cannot be reached, and the attack will not be successful (Exhibit 1).

Exhibit 1: Difficulty in achieving a consensus when there is a traitor



Source: SEBA Research

Each General can be regarded as one of the nodes on the network. As the number of nodes increases, achieving a consensus becomes more complicated and less reliable. The solution to the problem lies in ensuring that all the Generals can agree on a strategy without relying on anything else. There are two critical elements within such a design:

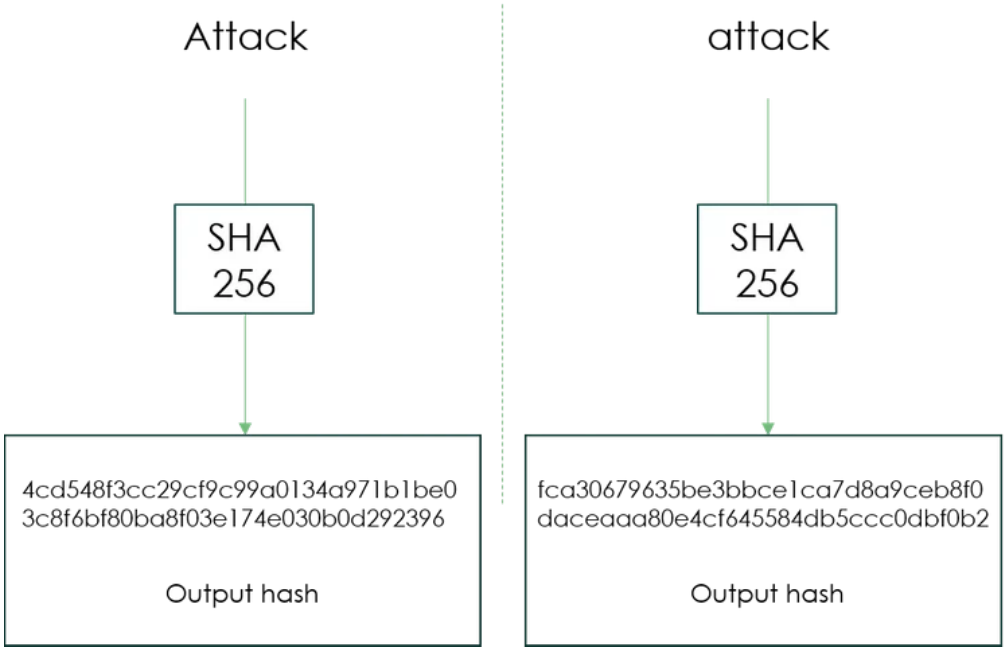
1. Encrypting the messages
2. Giving network participants an incentive: punishing cheating and/or rewarding good behaviour

Encryption using hash functions

The messages sent by the Generals need to be encrypted using hash functions to make them tamperproof. Hash functions are one-way functions that encrypt a message so that it becomes virtually impossible to obtain the original message from the output. We invite readers to check for themselves using the following link[link1].

SHA-256, for Secure Hash Algorithm variant 256, is used in the Bitcoin protocol. Regardless of the input text, the output is always a string of 64 digits. Minor changes in the original message cause massive differences in outputs (Exhibit 2). The hash of “attack” is completely different from the hash of “Attack”, even though the change in the original message appears to be trivial.

Exhibit 2: SHA-256 output



Source: SEBA Research

The use of hash functions gives the Byzantine Generals a higher degree of confidence in the messages they receive. To ensure that a message has not been tampered with, Generals add a random number along with the message. This random number is called *nonce*. Adding nonce provides extra security, as anyone who wishes to change the message must also change the nonce for the output to remain acceptable[2]. Only the Generals know what the acceptable output is. Therefore even minor tampering with the message will change the output and the recipient will know that there has been an attempt to change the message.

The role of incentives in consensus mechanisms

Using encryption alone does not fully solve the problem. A traitor General can still find a nonce that makes the output acceptable with a "retreat" message instead of "attack". So how can it be ensured that the General is acting in the best interests of the Empire? This is done by making misbehaviour costly for traitors. Different consensus algorithms have different methods of aligning incentives for network participants. Without this alignment, there is room for misbehaviour.

We will now present the two most widely used consensus mechanisms.

Proof of work (PoW)

What is PoW?

Satoshi Nakamoto developed PoW in order to achieve a consensus on the Bitcoin network. The consensus process can be broken down into two steps: proposing the current network state – the single truth – and accepting the current network state. Proof of work makes it expensive to propose the current state of the network. In Bitcoin's consensus mechanism, the *miners* are the ones who propose the existing state of network, along with the right nonce to enforce trust in the system. Finding the right nonce is very unusual and can only be done by brute force. Therefore, discovering the correct nonce is expensive. However, checking the nonce is very easy. Miners are paid if their proposition is accepted by the network. As it is easy to check the combination between the nonce and the current network state proposed by the miners, there is little incentive for them to submit the wrong state. Consequently, it is in the best interests of the miners to submit the correct state every time: the single truth.

Incentive alignment in PoW using the Byzantine Empire analogy

If the Byzantine Empire were to employ PoW, they would have to promise the spoils from the city to the Generals if the attack succeeded. If the attack failed, the Generals would not receive anything. To compel the Generals to act in the best interests of the Empire, the following additions must be made to the design;

- ✓ Generals need to invest significant capital to set up the messaging system
- ✓ The generation of each message must be expensive

Generals need rewards to recover the costs they have incurred to set up the messaging system. As they are rewarded only when the attack is successful, they are compelled to work towards making the attack successful.

Advantages

- ✓ Most secure consensus algorithm
- ✓ Miners cannot hoard coins as they need to sell them to cover their operational costs

Disadvantages

- ✓ Inefficient in terms of energy – brute force is used
- ✓ Longer transaction time – the right nonce is only found after trial and error
- ✓ High fixed and operational costs

Examples of crypto-assets using PoW: Bitcoin, Ethereum (plans to migrate to proof of stake), Ethereum Classic, Monero, Zcash.

Proof of stake (PoS)

What is PoS?

In a proof of stake consensus, validators or forgers have the same functions as the miners in PoW. The mechanism is different, however. To participate in the consensus, validators have to stake a minimum amount in the blockchain's native token to be selected to validate a block and earn transaction fees.

Incentive alignment in PoS using the Byzantine analogy

If the Byzantine Empire were to implement PoS, there would have to be a condition according to which anyone aspiring to be a General would have a significant stake in the Empire. If they do not act in the best interests of the Empire, any loss in the Empire's value would also hurt their possessions. The best strategy for the Generals is therefore to act in the interests of the Empire.

Unlike PoW, with a PoS consensus there is no race among the users to find the next block. A user needs to own a stake in the network to be regarded as a validator, which forces users to put as much effort as possible into the game. Validators are chosen randomly. Two

common ways to select a block forger are the Coin Age Selection[3] and the Randomised Block Selection[4] processes.

Advantages:

- Efficient in terms of energy
- Shorter transaction time
- No need to buy expensive mining equipment

Disadvantages:

- As a validator is selected before the block has been proposed, transaction manipulation is possible through bribing
- The lack of operational costs represents an incentive for re-staking, which may lead to hoarding
- "Nothing at stake[link1] problem[5]". Simply having nothing at stake means that there is no variable cost associated with voting on the legitimacy of the block, so it is possible for validators to vote on multiple blocks at a time and receive rewards for the one that is accepted by the network.

Example of crypto-assets using PoS: Algorand, Cosmos, Binance Coin, Qtum.

Conclusion

The need to place trust in others has long been the status quo of the financial world. In a decentralised ecosystem, the consensus mechanism plays an important role in resolving the trust issue to a large extent. By aligning an individual's incentives to those of the network, consensus mechanisms enable a single truth to emerge, creating trust in the system.

However, no consensus mechanism is perfect as there must be trade-offs between elements such as speed, decentralisation and security. The consensus to be employed

depends on the design goal of the blockchain. Understanding the consensus mechanism of a blockchain forms the bedrock for discerning what that blockchain can and cannot do.

[1] Public blockchains are open to everyone, while private blockchains are by invitation.

[2] Acceptable output defines certain standards for the output. For example, in the case of Bitcoin, it represents a certain number of 0s at the beginning of the hash value.

[3] A validator is selected based on the age of the coins staked

[4] A forger is selected based on the combination of various parameters such as stakes, age, recentness etc.

[5] A detailed explanation of the "nothing at stake problem" is beyond the scope of this document.

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

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 effected 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 clarifications. 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 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.