SEBA

September 2020

Are blockchains that safe?

How to attack them and how to prevent these attacks (Part 1)

The Bridge

Table of Contents

Authors

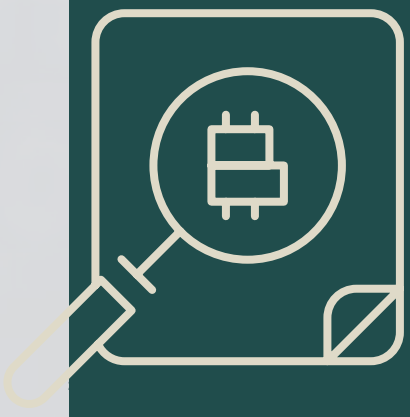
Yves Longchamp
Head of Research
SEBA Bank AG

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 outline:

- DDoS Attacks on blockchains can allow attackers access to associated networks such as Wallets and Exchanges
- Sybil Attacks run multiple malicious nodes on a network which can then refuse to allow new blocks from entering a blockchain
- 51% Attacks allow malicious entities to withhold majority control of a network and can use it to double spend.

Though the consensus mechanisms such as Proof of Stake (PoS) and Proof of Work (PoW) are designed to make blockchains secure, the open-source and censorship nature of blockchains make them an open target for different types of attacks. We explore three popular attacks in this article.

In this edition of Bridge, we explore some well-known attacks which are commonly used to compromise block-chain networks and discuss how consensus mechanisms such as Proof of Stake and Proof of Work may offer some (if limited) preventative measures to combat attacks.

1. Introduction

Examples of attacks to blockchains range from traditional and general threats that all network platforms face, to unique and specific attacks to blockchains. Before we go into depth about the types of attacks, we identify 4 elements of a blockchain which can face vulnerabilities:

- Blockchain nodes
- Smart contracts
- Consensus mechanisms
- Wallets

2. Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) takes place when a malicious user floods a server or network with requests and traffic. A DDoS attack intends to slow down or collapse a system. Any form of the online platform can be vulnerable to DDoS attacks including company websites and servers.

Specifically, within a blockchain, a DDoS attack can overload a blockchain with incoming bits of data which can force a blockchain to sever to further utilize its processing power. Through doing this, a blockchain server can lose connectivity to any crypto exchanges, online crypto wallets, or any other connected applications.

There are several high profile cases of attackers utilizing DDoS principals to gain access to crypto exchanges. Between November and December 2017, popular exchange Bitfinex had been successfully DDoS attacked 3 times where attackers shut down the exchange.

In both blockchain and non-blockchain focussed DDoS attacks, the overload of requests comes from either an individual or a small number of unique locations (which can be tracked through IP addresses).

How to prevent a DDoS attack on a blockchain?

Typically DDoS attacks are made possible through centralized features of a network such as a single point of connectivity to the internet. As a public blockchain is already a decentralized system linked to multiple nodes, a DDoS attack needs access to different nodes at the same time to inflict significant damage to the network.

The action of doing this makes the DDoS attack much more complex to pursue as well as considerably more time consuming compared to other methods of blockchain attacks.

In 2016 the Ethereum Blockchain became a victim of a DDoS attack which considerably increased the time it took in creating and verifying blocks. In response, the Ethereum development team made changes to their miner software in which gas limit targets were reduced[1] if the network experienced a similar attack where the creation of new blocks was taking a longer amount of time.

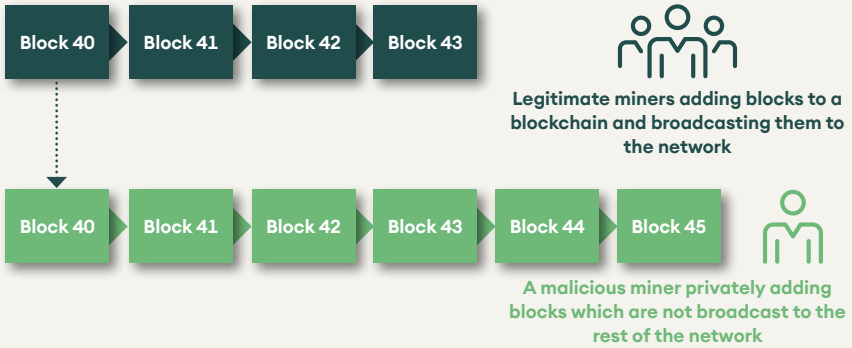
DDoS attacks are prevented through further decentralisation of a network. Not only would this reduce the capacity of a DDoS attack but also offer bandwidth to other specific servers facing attacks without compromising the whole chain. Even if certain nodes are compromised, taken offline, or disrupted, the blockchain can still operate and validate transactions. The disrupted nodes can recover and re-sync with unaffected nodes.

[1] Ethereum blockchain charges gas fee for every operation. Gas limit is the total gas that can be spent for one block. As the gas limit is decreased, number of operations per block gets limited thereby disallowing spam requests

3.
51% Attack

As referenced earlier in this article and in previous editions of The Bridge, a crucial feature of what makes a blockchain secure, lies within the decentralization and the ability of nodes to reach consensus. For example, the Proof of Work algorithm which is used by the Bitcoin blockchain forces all participants of the network to follow the same rules and protocols when miners are introducing new blocks, verified by nodes. The decentralized element of block-chain ensures there is no individual or centralized entity from influencing the activities of the blockchain outside of the PoW consensus. In a typical Blockchain network, new coins/tokens are unlocked through computers/miners that compete against each other in finding nonces that fit hashing problems. Once a miner successfully inputs the correct hashing combination and it is verified by the nodes and propagated throughout the network.

Figure 1: A demonstration of a 51% attack on a blockchain



Source: SEBA Bank AG

In January 2020, the Bitcoin Gold blockchain was the target of a 51% hack resulted in attackers double-spending over USD 85,000 worth of Bitcoin Gold. It speculated that attackers were able to obtain mining power through the online mining power market place "NiceHash". Currently, NiceHash allows users to rent mining power for over 33 major blockchain algorithms.

A 51% attack takes place where a malicious individual or a group takes control of over 50% of a blockchain network hash rate. In having control of 51% of the hash rate, attackers can influence other blocks that hold their transactions.

Figure 1 shows how a 51% attack takes place. Let's say that the attacker has their transactions in the legitimate chain wherein they send transactions to exchanges, merchants etc. based on which they receive services. For example, assume that block 40 has a transaction of token A sent to an exchange and as soon as the deposit is confirmed, the attacker converts token A to say ETH. Meanwhile, the attacker is mining blocks with their hashpower. In the private chain, the attacker sends the same transaction in block 40 to themselves instead of the exchange. As the attacker's chain is longer (implying more work done), the network has to accept the new chain. In the new chain, token A never went to the exchange. Thus, the attacker has token A as well as ETH. The farther back the attacker goes in the chain, the higher is the damage. And the number of blocks that can be re-written by the attacker depends on the hashpower they have compared to the network. Key incentives for attackers to conduct 51% attacks include the possibility of "double spending". Double spending takes place where a malicious entity controls more than 51% of the hashing power and can create a copy of a transaction and add it to a blockchain. This erases earlier transactions on the network as if they never took place.

This, in turn, means attackers can spend their tokens multiple times through erasing other blocks.

Over the past few years, there have been a few 51% attacks. In the past 3 months, attackers have been able to fraudulently steal over USD 8 million worth of ETC. The latest Ethereum Classic 51% attack in which attackers were able to 'reorganize' over 7,000 blocks. This was the third 51% attack the blockchain had faced in recent times and the ETC blockchain is now trialling a strategy to stabilize the networks decreasing hash rate to avoid future attacks. Other major attacks include:

- Ethereum Classic 51% attack in 2019 causing a loss of USDm 1.1
- Verge 51% attack in 2018 causing a loss of USDm 1.75
- Verge was later attacked (51% attack) 2018 resulting in a loss of USDm 1.1

Conclusion

So far, the EU did not provide its single financial services market a regulation addressing crypto-assets and crypto-finance. The situation is now changing. However, the move may demand regulatory adjustments in countries that have already implemented comprehensive regulations. The resultant necessary adaptations should be kept to the minimum. The forthcoming single market regulation will allow member states to efficiently manage the opportunities and challenges associated with crypto-assets and cryptofinance.

Stablecoins and CBDCs have continued to dominate the developments in the digital regulatory space during the last few weeks.

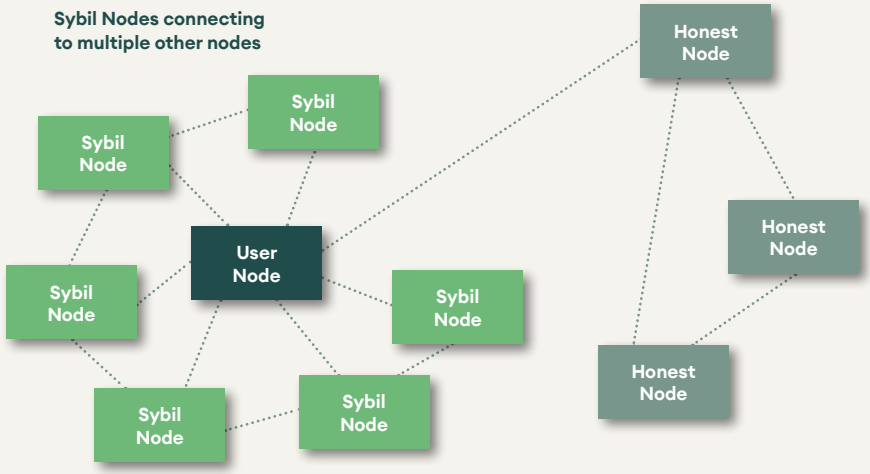
How to prevent a 51% attack?

Blockchains that use a PoW consensus algorithm are vulnerable to 51% attacks because the network is open for anyone to mine, including attackers. The lower the hash rate the blockchain the easier it is for an attacker to gain a majority advantage. Popular blockchains such as Bitcoin or Ethereum (both run PoW) have a very low vulnerability risk to 51% attack as gaining 50% of their networks would require an unrealistic amount of computational and energy resources. In sum, the higher the hashrate, the more difficult it is to perform a 51% attack.

4.
Sybil Attacks

Sybil Attacks manipulate online systems where one user attempts to overpower a network through the use of multiple profiles. Specifically, with blockchains, Sybil Attacks are when a user attempts to run multiple nodes on a blockchain network.

Figure 2: Illustration of a Sybil Attack, connecting to a Node and masking uncorrupted nodes



Source: SEBA Bank AG

A successful Sybil attack on a blockchain can force a network into influencing other nodes (if they can create enough nodes). Through controlling nodes, the Sybil attackers can refuse to transmit blocks which effectively prevents users from adding data to the network. It is important to add that Sybil attacks can lead to a malicious user (or users) to control the majority of a blockchain network. In doing this they can conduct a 51% attack where they could manipulate transactions and even force to double spend.

How to prevent a Sybil Attack?

Though consensus algorithms do not prevent Sybil attacks, they make it difficult and impractical for the attacker to carry out such an attack. For example, running full mining nodes on bitcoin network demands the attacker to possess significant hashpower which means the cost of an attack is high, and the expected rewards of a Sybil attack may not compensate for this cost. Therefore, it is in the best interest of an attacker to keep mining honestly.

Outside of PoW and PoS consensus algorithms, blockchains can prevent Sybil attacks through direct validation and indirect validation of new and existing members. Direct validation would allow existing members of a blockchain to verify new members joining a network, whereas indirect validation would allow existing members of a blockchain to provide authorisation rights to other members.

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