Thursday, 19 December, 2019

The Bridge

Mining: the essence of proof of work

Abstract

Mining is essential to blockchain ecosystems that use the proof-of-work consensus mechanism[link1]. Bitcoin, the most popular crypto-currency, runs on a proof-of-work blockchain.

Crypto-assets mining is similar to traditional mining in many respects, as it ultimately leads to an increase in supply. There are nonetheless important differences. Crypto miners validate transactions and add new blocks to the blockchain. The more productive they become, the more difficult it is to mine the next block.

In this article, we also present the kinds of mathematical puzzles miners solve, how they perform this task and finally how the mining technology has evolved over time.

What is mining?

Crypto asset mining is analogous to real-world mining. New bitcoins are discovered through a process of mining in the same way as raw materials are discovered in the process of mining. Traditional mining requires manual labour or machine power; bitcoin mining requires computational power. As a result, both raw material and bitcoin mining have an operational cost associated with them. Finally, as with raw materials, the bitcoin supply is also finite, i.e., the more one mines, the scarcer bitcoin gets.

However, bitcoin miners act as the network's transaction validators in addition to suppliers[1] of new bitcoins. Miners verify all the transactions before including them in a block and then adding the latter to the blockchain. As miners are free to enter or exit the market, they act as decentralised clearinghouses.

The miner's primary role is to validate transactions, bundle the transactions into a block and then append them to the blockchain. By verifying transactions and adding new blocks to the blockchain, miners earn block rewards denominated in crypto-currencies such as bitcoins for the work done[2]. These block rewards generate new crypto-currencies in the network according to a predetermined supply function. In the case of bitcoin, the current

supply function assigns a block reward of 12.5 bitcoins for each block added to the blockchain.

Now that we have an initial idea of how mining operates in the bitcoin network, let us dig deeper into how the mining process works.

Using a game of dice to understand the mining process

Imagine a game where players must simultaneously roll five dices with the aim of obtaining a total of digits below a certain number, N. The player who obtains the number below N first wins the game. The expected time of a game is 10 minutes, which means there is a winner every 10 minutes on average. If players find ways to increase the number of throws per minutes (productivity increases), the expected time of the game becomes shorter than 10 minutes. The difficulty must increase in order to bring the expected game time back to 10 minutes. It can be done by choosing a smaller number N or adding another dice to the mix and resetting N to a different value. As the probability of finding the new number decreases, the expected number of throws to win increases. Consequently, the expected game time once again becomes 10 minutes.

In comparison with the bitcoin network, the dice throwing players are the miners. The number of throws per unit time is equivalent to the computational power (measured in *hash rate*). The number N is similar to the network *difficulty* in bitcoin mining. A bitcoin block is created approximately every 10 minutes (this is hardcoded in the bitcoin's code, and is similar to the rules of a game). With every new block, new bitcoins are issued as a reward to the successful miner; this is how new bitcoins enter the circulating supply.

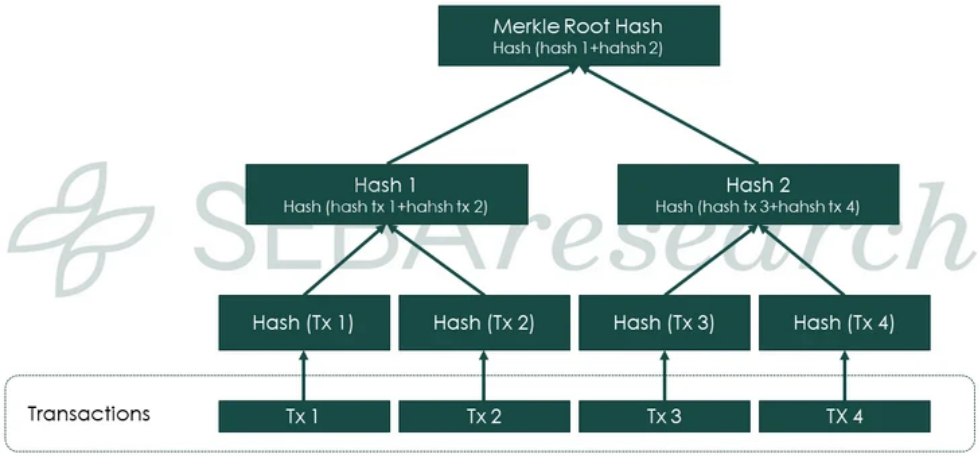
One might question why transactions are kept in blocks, and this is where the challenge lies. To avoid double-spending, it is essential to order transactions chronologically. As there is no synchronous clock in the world, it is not possible to order transactions based on one clock. Therefore, to resort to some other mechanism, transactions are bundled together in blocks, and then blocks are used to order transactions. Every block points to the previously accepted block by the network, and this is why the database is called a "blockchain".

Step-by-step guide to mining a transaction

Understanding how transactions take place in the bitcoin network provides an insight into how mining actually works.

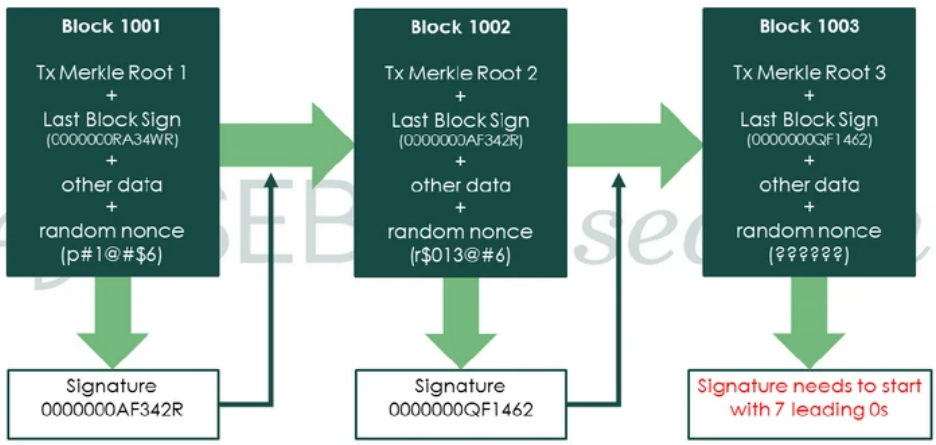
1. A user authorises sending bitcoin from their wallet[3]. The wallet application broadcasts the transaction to the network.
2. All unconfirmed transactions are pooled together as they wait to be placed in blocks. This collection of unconfirmed transactions is called a memory pool or mempool.
3. Miners pick transactions from the mempool, verify them, hash[4] them into what is called a Merkle root (exhibit 1), which is then added into the candidate block[5] along with the hash of the previous block and other data[6].
4. This is where the process of generating a signature begins (exhibit 2). The signature is created by guessing a nonce[7] through trial and error[8] in order to generate a required signature for their transaction block. In other words, to obtain the required signature, miners need to keep hashing the block header with different nonces (at a hash rate speed of billions per second) until one of the miners produces a valid signature, i.e., a signature with a specific number of zeros at the beginning (the number of zeros sets the difficulty).
5. When a miner finds the eligible signature for their block, they immediately broadcast the block to all the nodes on the network.
6. All other nodes will check if the hash is valid, and if so, they add the block to their copy of the blockchain and move on to mining the next block.
7. After a new block is added to the network, miners restart the mining process for the next block.

Exhibit 1: Merkle tree



Source: SEBA Research

Exhibit 2: Block addition process



Source: SEBA Research

Difficulty adjustment

Though there are similarities between bitcoin and commodity mining, there are certain differences as well. The most significant difference is the fixed rate of supply of bitcoins. If the efficiency of traditional mining equipment increases, then the mining rate also

increases, and thus the estimated supply schedule is disrupted. However, if bitcoin mining becomes more efficient due to improvements in mining equipment, the network automatically increases the difficulty to mine bitcoins and vice versa. The issuing of bitcoins is therefore adjusted in line with efficiency improvements so that on average 12.5 bitcoins are added every ten minutes.

As efficiency improves, the hash rate increases and blocks are found quicker than expected. The issuing of new bitcoins needs to be controlled so as to stick to bitcoin's predetermined supply schedule. Hence, the difficulty needs to be adjusted as the hash rate changes.

The mining difficulty is adjusted every 2,016 blocks, or roughly every two weeks[9]. It is adjusted in a manner that constantly keeps the average time it takes to mine a block at 10 minutes. If 2,016 blocks are mined in less than 14 days, the difficulty increases; if it takes more than 14 days to mine 2,016 blocks, then the difficulty decreases.

Development of bitcoin mining

In the early days, the hash rate of the bitcoin network was only a fraction of its current level. Mining on laptops with a good Graphics Processing Unit (GPU) was profitable as the processing power requirement was very low. As public interest in bitcoin grew, companies started building dedicated hardware to mine bitcoins, called Application Specific Integrated Circuits (ASICs). When compared to high-end laptops, ASICs are far more efficient in mining bitcoins as they have thousands of integrated circuits[10] that run the hashing algorithm in parallel at incredible speeds. A typical mining rig has thousands of ASICs running in parallel.

Mining pools - The block reward is given to the miner who discovers the signature first, while individual miners with a low hash rate may not be able to find a block. Therefore, to solve this problem, individuals with low processing power pool their mining resources. These setups are known as mining pools. Whenever the network accepts a mining pool's block, the bitcoin reward is shared among the individuals based on their resource contribution to the pool. Anybody can join a mining pool. It doesn't matter whether you have a single small mining machine or a warehouse of thousands of mining rigs.

Conclusion

The mining process is the backbone of any proof-of-work based blockchain network. It is one of the key elements that keeps the network up and running. Miners perform two critical functions for the network: they clear and settle the transactions and supply new bitcoins to the network.

In recent times, as the bitcoin price has increased from a few cents to several thousand dollars, mining has turned into an industrial-scale operation with many big companies operating mining farms. This has increased the safety in the system, as safety and difficulty go hand in hand, and has raised questions about the energy wastage caused by mining activities. An alternative to proof-of-work and mining is proof-of-stake and staking. We will explore this topic in the next edition of the Bridge.

[1] They generate new bitcoins according to a predetermined supply function.

[2] To be complete, they also receive the transaction fees. These are however very low in comparison to the block reward.

[3] A wallet contains users' keys. These keys are used to access users' bitcoins in the blockchain

[4] A hash is a string and/or number generated from an input. The resulting string or number is a fixed length, and will vary widely with small variations in input.

[5] This is a block that a miner tries to mine in order to receive the block reward.

[6] A block comprises the previous block hash, Merkle root hash, timestamp, difficulty, size, nonce, version and transactions.

[7] A nonce is a variable input that is fed into the bitcoin's hash function.

[8] Contrary to popular belief, miners don't solve blocks by solving complicated maths problems. They do so by sheer brute force, checking trillions of nonces per second.

[9] Expected block time = 10 min. This translates to 144 blocks per day and 2,016 blocks every 14 days.

[10] Integrated circuits are small electronic circuits designed on one chip to perform a dedicated function.

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

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.