EMERALD
DRIVEN BY RESEARCH

White Paper

June 2021

"Miners are the Sexy Plumber of Distributed Ledger Technology That Get a Bad Rap Because They Have a Few Cracks"

By: Steven E. Russell, Esq., MBA
Vice President & Portfolio Manager
Emerald Advisers, LLC

3175 Oregon Pike, Leola, Pennsylvania 17540
Tel: 717-396-1116 • Fax: 717-556-8895
www.teamemerald.com

“Miners are the Sexy Plumber of Distributed Ledger Technology That Get a Bad Rap Because They Have a Few Cracks”

Distributed Ledger Technology (DLT) is a resourceful invention where the information recorded on the ledger is kept in the shared database and can easily be verified, while not maintained by any one entity or in any one single location. It is a decentralized technology and there is no way for hackers to corrupt the information in any transaction connected to the process of identity verification.

DLT eliminates risks of data located centrally and has no single point of failure by various identical block across the network. DLT has been operable, in the form of cryptocurrencies, without failure since the invention of bitcoin, in 2008 based on public and private “keys”. Satoshi Nakamoto has introduced proof of work (PoW) to build a distributed trustless consensus and resolve the double-spend problem. Bitcoin’s innovation lies in its ability to coordinate trust and facilitate the transfer of value without relying on a centralized authority. We believe DLT, often referred to as blockchain technology, can disrupt almost every industry for its improvement in efficiency and security.

Mining is the process by which digital asset/blockchain transactions are validated, that requires significant micro processing and energy inputs. There are two primary algorithms, PoW (Proof-of-work) and PoS (Proof-of-stake) through which blockchain operates and are required for the security of the blockchain and these operations are conducted by “Miners”.

In this paper, we will discuss the job of the Miners as it applies to bitcoin, the cryptocurrency, and Bitcoin, the network.

Bitcoin Mining

Bitcoin’s innovation lies in its ability to coordinate trust and facilitate the transfer of value without relying on a centralized authority. Miners keep the blockchain consistent, complete, and unalterable by repeatedly grouping newly broadcast transactions into a block, which is then broadcast to the network and verified by nodes. Miners are paid in transaction fees for creating blocks of validated transactions and including them in the blockchain. Each block contains a cryptographic hash of the previous block, thus linking it to the previous block and creating the blockchain. The enabler in the process is proof-of-work mining, a mechanism that adds new bitcoin to the money supply and protects the network against nefarious actors attempting to spend the same bitcoin more than once. Through economic incentives, miners voluntarily secure the network by verifying “blocks” of transactions and appending them to Bitcoin’s public ledger. Specialized, dedicated hardware perform a function that proves that a miner has executed a costly computation. In exchange for providing the processing power that is critical to the network’s security, miners are rewarded with newly minted bitcoin and transaction fees.

How Mining Works

To understand how mining works, we will examine how bitcoin mining works as an example. To do so we will start by explaining what "nodes" are and what their role is in the mining process.

Node

Decentralized Ledger Technology, often referred to as blockchain, nodes are responsible for acting as a communication point that may perform different functions. Any computer or device that connects to the Bitcoin (reminder, Bitcoin with a capital "B" refers to the Bitcoin network) interface may be considered as a node in the sense that they communicate with each other. These nodes are also able to transmit information about transactions and blocks within the distributed network of computers by using the Bitcoin peer-to-peer protocol. However, each computer node is defined according to its particular functions, so there are different types of Bitcoin nodes.

"Full nodes" are the ones that really support and provide security to Bitcoin, and they are indispensable to the network. These nodes may also be referred to as fully validating nodes as they engage in the process of verifying transactions and blocks against the system's consensus rules. In addition, full nodes are able to relay new transactions and blocks to the blockchain. Usually, a full node downloads a copy of the Bitcoin blockchain with every block and transaction, but this is not a requirement to be considered a full node (a reduced copy of the blockchain may be used instead).

A "listening node" or "super node" is a full node that is publicly visible. It communicates and provides information to any other node that decides to establish a connection with it. Hence, a super node is a redistribution point that may act both as a data source and as a communication bridge.

Some nodes are "mining nodes", and are usually referred to as miners. A miner may choose to work alone, "solo miner," or in groups "pool miner". While the solo miners' full nodes make use of their own copy of the blockchain, pool miners work together, each one contributing to the computational resources known as "hashpower". In a mining pool, only the administrator of the pool is required to run a full node, which is referred to as a pool miner's full node. Miners validate outstanding transactions then enter them into blocks that the miners then add to the blockchain.

Miners validate transactions by solving a complex mathematical puzzle that is part of the bitcoin program, and including the answer in the block. To solve the puzzle the miner must find a number that, when combined with the data in the block and passed through a hash function. The hash function converts input data of any size into output data of a fixed length, produces a result that is within a certain range. The resulting number is called a "nonce", which is an abbreviation of "number used once." In the blockchain, the nonce is an integer between 0 and

4,294,967,296. Miners attempt to find this number by computer generated random guesses. The hash function makes it impossible to predict what the output will be. Miners apply the hash function with the guessed number and the data in the block. The resulting hash starts with a certain number of zeroes. There is no way of knowing which number will work, because two consecutive integers will give wildly varying results. There may be several nonces that produce the desired result, or there may be none. In that case, the miners keep trying but with a different block configuration. The first miner to get a resulting hash within the desired range announces its victory to the rest of the network. All the other miners immediately stop work on that block and start trying to figure out the mystery number for the next one. As a reward for its work, miners are paid in bitcoin. The difficulty of the calculation is adjusted frequently, so that it takes on average about 10 minutes to process a block. We believe the “difficulty adjustment” is key to the security of the Bitcoin network.

The Difficulty Adjustment

As the price of bitcoin rises, miners are increasingly incentivized to put more resources into their mining operations because successful mining results in bitcoin rewards thus creating the relationship between the price of bitcoin and the total worldwide mining incentive. The economic formula for miners is as follows:

(The miner’s hash rate/the-worldwide Bitcoin network hash rate) X (bitcoin price) X (global mining rewards) LESS (electricity cost per MWh) X (equipment efficiency J/TH) X (fixed corporate expenses)

At the time of writing, the reward is 6.25 bitcoins per block, which is worth around $40,000 in May of 2021.

The Bitcoin “hashrate” refers to the total computational power that is being used to mine and process Bitcoin transactions. Higher network hashrate implies greater security and growing hashrate is indicative of miner optimism and additional capital investment in computing power. Bitcoin’s hashrate recently reached an all-time high on April 6, 2021.

Hashrate is expressed as a number of hashes per second (h/s). A hash is an algorithm that converts an input of letters and numbers into an encrypted output of a fixed length. Given the size of the Bitcoin network, hashrate is typically expressed in terahash (TH/s) or petahash (PH/s) which represent 1 trillion and 1 quadrillion hashes, respectively. Hashrate is usually presented as a moving average to smooth out datasets and give a better picture of long-term network health. Determining the hashrate is not exact. There are too many miners operating to accurately determine how much computing power is being used. Instead, hashrate is estimated by taking the expected rate of finding a block and comparing it to the actual rate of finding a block given the current difficulty (a parameter of the Bitcoin network that measures how hard it is to construct a valid block). Although this is the industry standard, some are searching for more precise measurements employing statistical analyses. Hash rate is the number of calculations that your hardware can perform every second as it tries to crack the

mathematical problem described below. The higher your hash rate (compared to the current average hash rate), the more likely you are to solve a transaction block.

As the worldwide network hash rate increases, the Bitcoin protocol will automatically raise the difficulty of mining, such that the creation of new bitcoin, and the timing of transaction verification, does not accelerate beyond its preset schedule of about every 10 minutes. If bitcoin’s price falls, less efficient bitcoin miners rationally turn off their machines and the worldwide network hash rate decreases. As a result, the Bitcoin protocol will automatically reduce the difficulty of mining, such that the creation of new bitcoin, and the timing of transaction verification, does not decelerate below its preset schedule. Why 10 minutes? That is the amount of time that the bitcoin developers think is necessary for a steady and diminishing flow of new bitcoins until the maximum number of 21 million is reached (expected sometime in 2140).

How does the protocol adjust to make discovering the nonce more difficult or easier? To explain how the Bitcoin protocol adjusts, imagine that the product of two prime numbers is a certain three-digit number and the miners are asked to guess the two prime numbers. We remind you that a property of prime numbers is that the product of two primes is uniquely the product of those specific two primes. There is no closed-form solution to find the three-digit number and thus, miners must randomly guess until you figure it out. Since the product of the primes, in our example, is only three digits, miners would probably be able to guess the two primes quickly. However, suppose miners are told that the product was five digits? How about ten digits? How about twenty digits? The Difficulty Adjustment is akin to adjusting the number of digits of the product of the primes as a function of how much mining power is on-line at any given time. The more miners, the greater the number of digits of the product of the primes. The fewer miners, the smaller the number of digits such that, even if all commercial Bitcoin miners, and their combined super-computing power, suddenly went off-line overnight, individuals mining on laptops at home would keep the entire global Bitcoin network just as secure.

The Difficulty Adjustment has now been continuously tested for almost thirteen years. The total network power volatility is what requires the Bitcoin protocol to continually adjust the mining difficulty, akin to continually adjusting the number of digits of the product of the two primes. The amount of energy the Bitcoin network consumes is the sum total of the energy consumption of all the mining machines that secure the network.

Bitcoin mining is the only profitable use of energy in human history that does not need to be located near human settlement to operate. The long-term implications of this are world changing and hiding in plain sight. The problem of energy has never been its scarcity, but only our ability to channel it geographically where humans live. Bitcoin mining can be located anywhere. Because of satellite and wireless internet communication, remote areas with moving water or other renewable energy sources can monetize their natural resource by creating clean energy and using it to mine Bitcoin. The Bitcoin network can make isolated renewable energy sources all over the world that are currently not utilized because they would be cost prohibitive to connect to electric grids close enough to residential or industrial areas monetize able. In doing so, the Bitcoin network can fundamentally change the economics of energy by introducing a highly profitable use of electricity that is location independent.

While Bitcoin mining uses a substantial amount of energy, a good percentage comes from renewable energy. According to a 2020 study carried out by the Cambridge Centre for Alternative Finance (CCAF), 39% of total energy for Bitcoin mining came from renewable sources in 2019 (compared to 28% in 2018) with 76% of miners using renewable sources as part of their energy mix. This upward trend and meaningful renewable energy penetration should be encouraging.

Investing in Miners

Due to the diminishing flow of new bitcoin, 21 million, the reward for validating transactions will continue to decrease significantly over time. However, if bitcoin prices sustain at current levels or move higher, the reward versus the cost of mining will likely remain hugely profitable. Additionally, transaction fees are becoming a larger part of digital asset transaction validation as newly mined bitcoin dwindles.

From an investment perspective, mining revenue reached an all-time high in March 2021 due to rising total fees as well as the bitcoin price. Increasing revenue could lead to a couple of things. The first is more external industry investment, which in turn leads to improvements across all facets of Bitcoin mining. Second, increased miner income means miners are flush with cash reserves, which could be utilized to improve miner efficiencies, grow footprint, expand clean energy use capabilities and/or allow miners to hold their bitcoin on balance sheet.

Important Disclosure

This report is furnished for the use of Emerald Advisers, LLC, its affiliates and its clients and does not constitute the provision of investment, legal or tax advice to any person. It is not prepared with respect to the specific investment objectives, financial situation or particular needs of any specific person. The information contained in this report was obtained from sources deemed reliable. Such information is not guaranteed as to its accuracy, timeliness or completeness by Emerald. Any opinions contained in this report represent the judgment of the authors as of the publication date. The information contained in this report and the opinions expressed herein are subject to change without notice. Past performance is no guarantee of future results. Neither the information in this report nor any opinion expressed herein constitutes an offer nor recommendation to buy or sell any security or financial instrument. Accounts managed by Emerald's affiliated advisory firms may take positions from time to time in securities discussed in its reports.