IJFEAT
INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

A CLOSER LOOK INTO THE WORLD OF BITCOIN MINING

Garima A. Chudiwale [1], Priyanka A. Kawale [2], Dnyaneshwari D. Rathod[3], Prof. A.P. Jadhao[4]
[1]*Student, Dept of CSE, J.D.I.E.T, Yavatmal, Maharashtra, India,* ***chudiwale.garima.gc@gmail.com***
[2]*Student, Dept of CSE, J.D.I.E.T, Yavatmal, Maharashtra, India,* ***priyakawale27@gmail.com***
[3]*Student, Dept of CSE, J.D.I.E.T, Yavatmal, Maharashtra, India,* ***dnyaneshwarirathod21@gmail.com***
[4]*Assistant Professor, Dept of CSE, J.D.I.E.T, Yavatmal, Maharashtra, India,****apjadhao@gmail.com***

ABSTRACT

Bitcoin is the most popular cryptocurrency today. The bedrock of the Bitcoin framework is mining. Bitcoin mining is decentralized. Anyone with an internet connection and the proper hardware can participate. Bitcoin mining is the mechanism to introduce Bitcoins into the system. It is the process of adding Bitcoin transaction records to the blockchain, which is a chain of blocks. Bitcoin miners use blockchain to authenticate Bitcoin transactions. It serves to both add transactions to the block chain and to release new Bitcoin. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The first participant who solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards incentivize mining and include both the transaction fees as well as the newly released Bitcoin.

Index Terms*: Cryptocurrency, Bitcoin mining, blockchain, peer-to-peer computing.*

1. INTRODUCTION

Bitcoin is a crypto currency and a digital payment system. The system is peer-to-peer, and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called a *blockchain*. Since the system works without a central repository or single administrator, Bitcoin is called the first decentralized digital currency. Besides being created as a reward for mining, Bitcoin can be exchanged for other currencies, products, and services in legal or black markets.

1.1 History

Bitcoin was created by Satoshi Nakamoto, who published the invention on 31 October 2008 to a cryptography mailing list in a research paper called "Bitcoin: A Peer-to-Peer Electronic Cash System". Nakamoto implemented Bitcoin as open source code and released in January 2009. The identity of Nakamoto remains unknown, though many have claimed to know it. In January 2009, the Bitcoin network came into existence with the release of the first open source Bitcoin client and the issuance of the first Bitcoins, with Satoshi Nakamoto mining the first block of Bitcoins ever, which had a reward of 50 Bitcoins. One of the first supporters, adopters, contributor to Bitcoin and receiver of the first Bitcoin transaction was programmer Hal Finney. In the early days, Nakamoto is estimated to have mined 1 million Bitcoins. Before disappearing from any involvement in Bitcoin, Nakamoto in a sense handed over the reins to developer Gavin Andresen.

1.2 Bitcoin Mining

Mining crypto-currency is done using a computer and it is scaled on hashes per second. Every time someone successfully solves a block and mines a coin, a new hash is created. The mining process will keep increasing in difficulty and as the data chunks become larger and processing it becomes more difficult, the resources used and cost will increase while the rewards diminish. The reward for mining used to be 50 Bitcoins per block while today it has been reduced to 12.5 per block. The supply of Bitcoins is fixed and the rewards have been programmed to halve every four years. Thus the mining process becomes less profitable as time goes on and the supply of Bitcoin slows down. Essentially, mining is a contest. Multiple miners are all working at the same time to find a hash. Computational problems that have been solved by miners are a certain “proof” that verifies that a certain miner has successfully mined a block. An eventual limit has been put on the total supply of Bitcoins. The announced limit is 21 million Bitcoins. During the process of mining the Bitcoin, evidence is added to the blockchain. Owners of Bitcoins use digital “wallets” to keep track of their own balance and for transaction purposes.

2. THE MINING PROCESS

Mining is a record-keeping service. Miners keep the blockchain consistent, complete, and unalterable by repeatedly verifying and collecting newly broadcast transactions into a new group of transactions called a *block*. Each block contains a cryptographic hash of the previous block, using the hashing algorithm, which links it to the previous block, thus giving the block chain its name.

In order to be accepted by the rest of the network, a new block must contain a so-called *proof-of-work*. This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash, miners must try many different nonce before meeting the difficulty target. Every 2016 blocks, the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes. The proof-of-work system, alongside the chaining of blocks, makes modifications of the blockchain extremely hard, as an attacker must modify all subsequent blocks in order

for the modifications of one block to be accepted. As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called *confirmations* of the given block) increases.

A rough overview of the process to mine Bitcoins is:

a. New transactions are broadcast to all nodes.
b. Each miner node collects new transactions into a block.
c. Each miner node works on finding a proof-of-work code for its block.
d. When a node finds a proof-of-work, it broadcasts the block to all nodes.
e. Receiving nodes validate the transactions it holds and accept only if all are valid.
f. Nodes express their acceptance by moving to work on the next block, incorporating the hash of the accepted block.

2.1 Blockchain

A blockchain is a transaction database shared by all nodes participating in a system based on the Bitcoin protocol. A full copy of a currency's blockchain contains every transaction ever executed in the currency. With this information, one can find out how much value belonged to each address at any point in history. Every block contains a hash of the previous block. Each block is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated. The blockchain is the main innovation of Bitcoin.

A chain is valid if all of the blocks and transactions within it are valid, and only if it starts with the genesis block. For any block on the chain, there is only one path to the genesis block. Coming from the genesis block, however, there can be forks. One-block forks are created from time to time when two blocks are created just a few seconds apart. When that happens, generating nodes build onto whichever one of the blocks they received first. Whichever block ends up being included in the next block becomes part of the main chain because that chain is longer.

Blocks in shorter chains (or invalid chains) are not used for anything. When the Bitcoin client switches to another, longer chain, all valid transactions of the blocks inside the shorter chain are re-added to the pool of queued transactions and will be included in another block. The reward for the blocks on the shorter chain will not be present in the longest chain, so they will be practically lost. These blocks on the shorter chains are often called "*orphan*" blocks. This is because the generation transactions do not have a parent block in the longest chain, so these generation transactions show up as orphan in the list transactions. In reality, these blocks have a parent block, and might even have children. Because a block can only reference one previous block, it is impossible for two forked chains to merge.

In the fig 2.1 blocks in the main chain (black) are the longest series of blocks that go from the genesis block (green) to the current block. Purple blocks are blocks that are not in the longest chain and therefore not used.

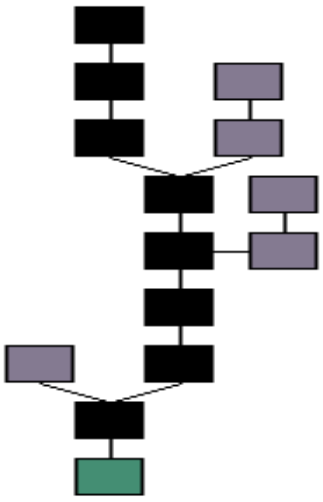

Figure 2.1: A blockchain showing Genesis Block and Orphan Blocks

2.2 Block

Transaction data is permanently recorded in files called blocks. They can be thought of as the individual pages of a city recorder's record book or a stock transaction ledger. Blocks are organized into a linear sequence over time (called block chain). New transactions are constantly being processes by miners into new blocks which are added to the end of the chain and can never be changed or removed once accepted by the network.

Each block mainly contains a record of some or all recent transactions, and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle - the answer to which is unique to each block. New blocks cannot be submitted to the network without the correct answer - the process of "mining" is essentially the process of competing to be the next to find the answer that "solves" the current block. The mathematical problem is extremely difficult to solve, buts it is very easy for the rest of the network to confirm that the solution is correct. There are multiple valid solutions for any given block - only one of the solutions needs to be found for the block to be solved.

Because there is a reward of brand new Bitcoins for solving each block, every block also contains a record of which Bitcoin addresses or scripts are entitled to receive the reward. This record is known as a generation transaction, or a coinbase transaction, and is always the first transaction appearing in every block. The number of Bitcoin generated per block started at 50 and is halved every 210,000 blocks (about four years) currently the reward is 12.5 BTC.

Bitcoin transactions are broadcast to the network by the sender, and all peers trying to solve blocks collect the transaction records and add them to the block they are working to solve. Miners get incentive to include transactions in their blocks because of attached transaction fees. Every 2016 blocks (solved in about two weeks), all Bitcoin clients compare the actual number created with this goal and modify the target by the percentage that it varied. The network comes to a consensus and automatically increases (or decreases) the difficulty of generating blocks.

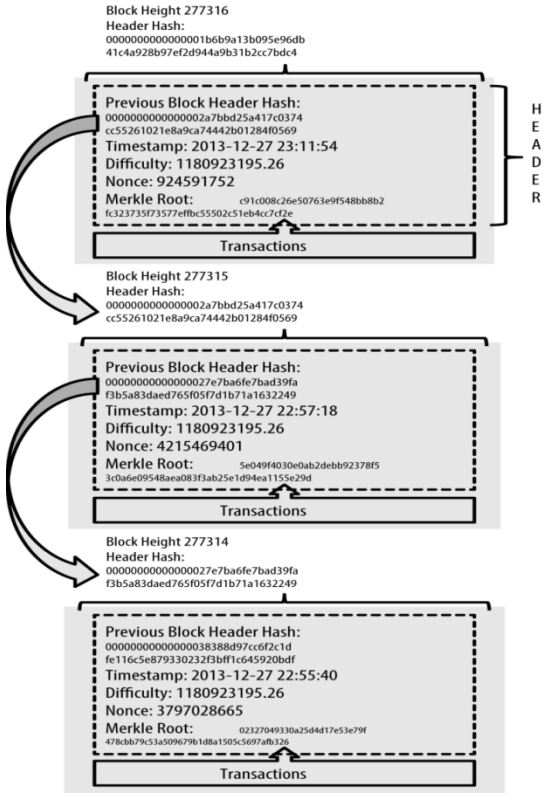

Figure 2.2: Blocks linked in a chain, by reference to the previous block header hash

2.3 Proof of work

A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Hashcash proofs of work are used in Bitcoin for block generation. In order for a block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block. The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes. Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block.

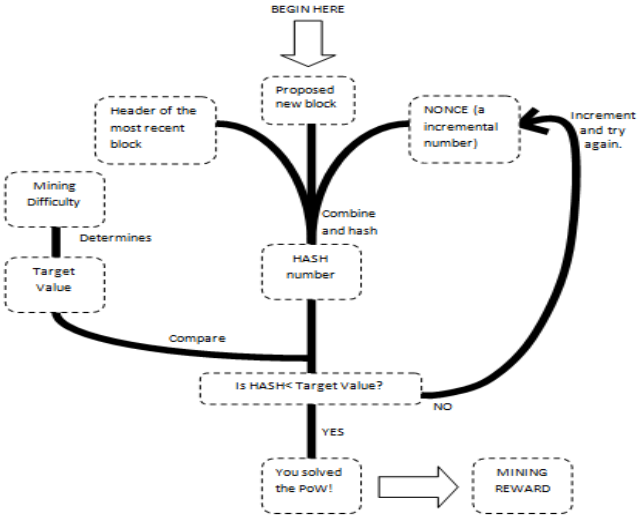

Figure 2.3: Steps to produce a Proof of Work.

For a block to be valid it must hash to a value less than the current target, this means that each block indicates that work has been done generating it. Each block contains the hash of the preceding block, thus each block has a chain of blocks that together contain a large amount of work. Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain. This protects the block chain from tampering.

3. BITCOIN MINING HARDWARE

Users have used various types of hardware over time to mine blocks.

3.1 CPU

Early Bitcoin client versions allowed users to use their CPUs to mine. The hashrate of the network grew such that the amount of Bitcoins produced by CPU mining became lower than the cost of power to operate a CPU. You might mine for decades using your laptop without earning a single coin. The option was therefore removed from the core Bitcoin client's user interface.

3.2 GPU

About a year and a half after the network started, it was discovered that high end graphics cards were much faster and efficient at Bitcoin mining and the landscape changed. CPU Bitcoin mining gave way to the GPU (Graphical Processing Unit). The massively parallel nature of some GPUs allowed increase in Bitcoin mining power while using far less power per unit of work. Trying different hashes repeatedly - the process behind Bitcoin mining - is a very repetitive task suitable for a GPU. The only decision making that must be made in Bitcoin mining is, "do I have a valid block" or "do I not". That's an excellent workload to run on a GPU.

3.3 FPGA

FPGA **(**Field-Programmable Gate Arrays) are microprocessors that can be programmed for a specific purpose. FPGA mining is a very efficient and fast way to mine. FPGAs typically consume very small amounts of power with relatively high hash ratings, making them more viable and efficient than GPU mining. FPGA is attached to computers using a convenient USB connection. The FPGA Bitcoin mining hardware landscape gave way to specially manufactured hardware dedicated to mining Bitcoins. It made concentrated mining farms possible for the first time and the Bitcoin mining industry was born.

3.4 ASIC

The Bitcoin mining world is now solidly in the Application Specific Integrated Circuit (ASIC) era. An ASIC is a chip designed specifically to do one thing and one thing only. An ASIC designed to mine Bitcoins can only mine Bitcoins and will only ever mine Bitcoins. The inflexibility of an ASIC is offset by the fact that it offers a 100x increase in hashing power while reducing power consumption compared to all the previous technologies. This makes power consumption on an ASIC device the single most important factor of any ASIC product, as the expected useful lifetime of an ASIC mining device is longer than the entire history of Bitcoin mining. Mining profitability is also dictated by the exchange rate, but

under all circumstances the more power efficient the mining device, the more profitable it is.

4. ADVANTAGES

4.1 Security and control

Bitcoin users are in full control of their transactions. Bitcoin payments can be made without personal information tied to the transaction. This offers strong protection against identity theft.

4.2 Payment freedom

It is possible to send and receive Bitcoins anywhere in the world at any time. No bank holidays. No borders. No bureaucracy.

4.3 Choose your own fees

There is no fee to receive Bitcoins, and many wallets let you control how large a fee to pay when spending. Higher fees can encourage faster confirmation of your transactions.

4.4 Transparent and neutral

All information concerning the Bitcoin money supply itself is readily available on the block chain for anybody to verify and use in real-time. No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent and predictable.

5. DISADVANTAGES

5.1 Degree of acceptance

Many people are still unaware of Bitcoin. Every day, more businesses accept Bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects.

5.2 Volatility

The total value of Bitcoins in circulation and the number of businesses using Bitcoin are still very small. Therefore, relatively small events, trades, or business activities can significantly affect the price.

5.3 Ongoing development

New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. Some of these are still not ready for everyone. Most Bitcoin businesses are new and still offer no insurance.

5.4 Black Market Activity May Damage Reputation

Despite high-visibility prosecutions, Bitcoin remains attractive to criminals and gray market participants. If shady uses for Bitcoin outweigh legitimate ones over time, and the authorities can't effectively put a stop to the shenanigans, the entire system faces marginalization.

6. CONCLUSION

Bitcoin is a rare case where practice seems to be ahead of theory. Bitcoin has emerged as the most successful cryptographic currency in history. Within few years of its quiet launch in 2009, Bitcoin grew to comprise billions of dollars of economic value. Many people are still unaware of Bitcoin, the list remains small and still needs to grow in order to benefit from network effects. Bitcoin mining is a record-keeping service which is fully decentralized. The supply of Bitcoins comes from "mining", a process which involves computing complex algorithm with increased difficulty over time, making it more expensive and resource intensive and thus less profitable as time go by. Not only that technology has evolved from initial CPU/GPU/FPGA mining to highly specialize low nanometer ASIC miners, but also the whole structure of the market has shifted. This has already changed within the years and mining has moved more and more from a short term quick profit game to a slower, patient and more steady industry where only the most efficient operations have a chance to yield high profit within an extended frame. This trend will clearly continue and the development of newer technology gets more and more expensive.

REFERENCES

[1] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, in IEEE Symposium on Security and Privacy, 2015.

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, in 2009.

[3] Fergal Reid, Martin Harrigan, An Analysis of Anonymity in the Bitcoin System, in IEEE 2011.

[4] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten, Have a snack- pay with Bitcoins, in IEEE P2P, 2013.

[5] A. Gervais, G. O. Karame, D. Gruber, and S. Capkun, on the Privacy Provisions of Bloom Filters in Lightweight Bitcoin clients, in ACSAC, 2015.

[6] Web- Available at- https://en.Bitcoin.it/wiki/Mining.

[7] Web- Available at- https://en.wikipedia.org/wiki/Bitcoin.