Mining process in Cryptocurrency using Blockchain Technology

Page content

Introduction

What is Cryptography?

Cryptography is a method of using encryption and decryption to secure communication in the presence of third parties who want to steal your data or eavesdrop on your conversation.

What is Cryptocurrency?

Digital or virtual currency that is meant to be a medium of exchanges.it is quite similar to real-world currency, except it does not have any physical body and it uses cryptography to work. Because cryptocurrencies operate independently and in a decentralized manner that mean without a bank or a central authority.

What is Blockchain?

Blockchain is a System of recording information in a way that makes it impossible to change once it written.so cannot hack or cheat this system.

And also blockchain is a digital ledger that keeps transcations duplicated and distributed across the entire network of computer system on blockchain.Each of block of the blockchain contains number of transactions and every time a new transaction occurs on the blockchain then a record of that trasaction is added to every participants ledger who in network.

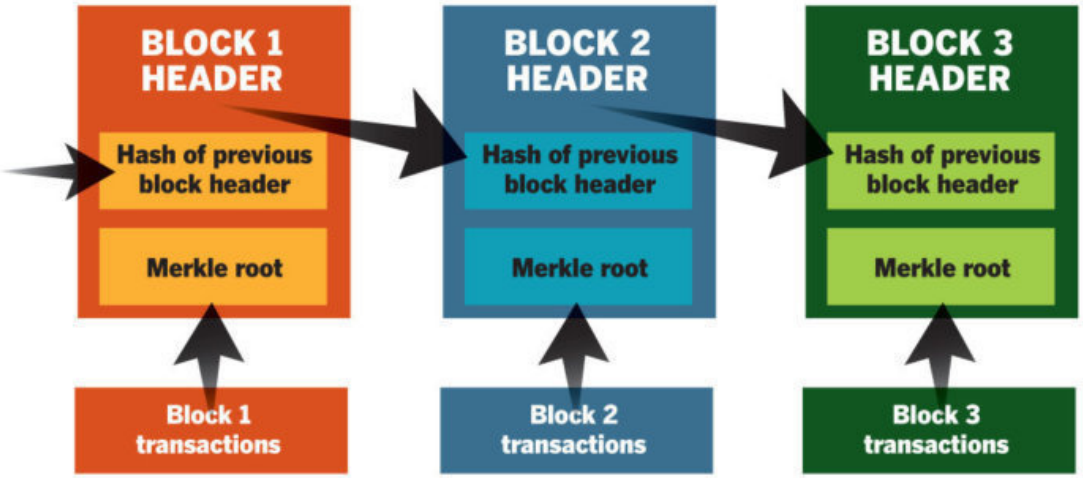
a blockchain is formed from a series of “blocks.” The blockchain software records each transaction during a block without the help of a 3rd party sort of a bank or payment processor. The blockchain algorithm automatically encrypts and authenticates the transaction, which is immediately visible to all users, minimizing the possibility of fraud. The terms of the transaction don't include any personal or identifying information.

Blockchain technology was invented to control bitcoin, the primary and best for cryptocurrency. Some newer platforms, like ethereum, employ a blockchain to provide a digital ecosystem for distributed computing, effectively using cryptocurrency to oil the works. In ethereum, blocks run what’s called a sensible contract to make sure that certain conditions are met before a service is rendered.

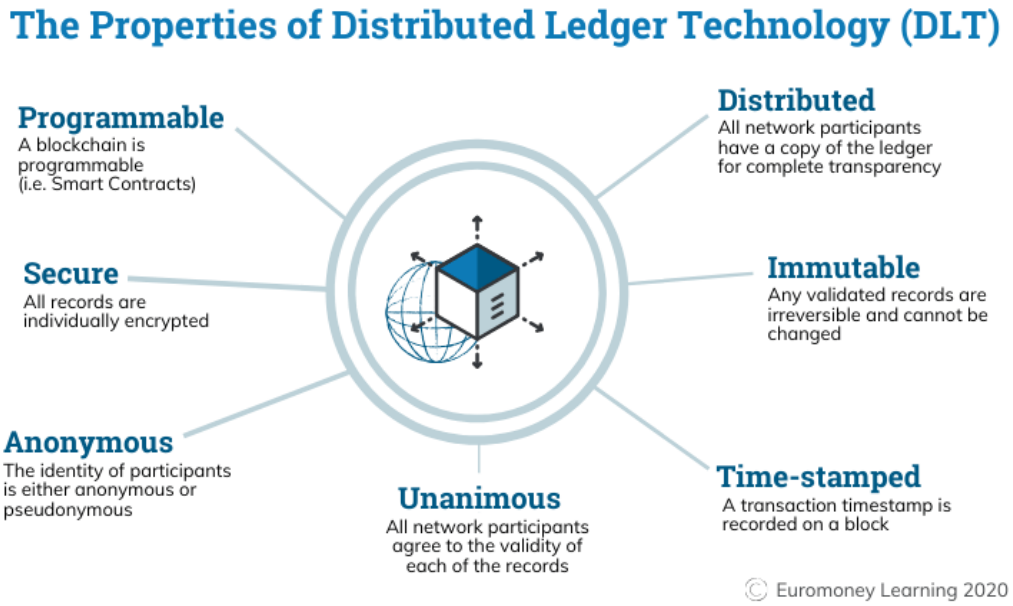
Every blockchain user has an equivalent copy of of the whole blockchain as everybody else. This makes it virtually impossible to manipulate: a hacker would need to harness computing power greater than that of each user to change the blockchain in her favor. Because of this ironclad security, major mainstream institutions like Citigroup and therefore the London stock market have embraced blockchain technology, within the hope of using it, for instance , to guard intellectual property or store investment records. Blockchains may even be employed by artists and musicians to secure their work and receive fair compensation from fans. It may not be long before artists forego

licensing their work to a publisher, who takes a cut, once they can register it on to a blockchain.

With blockchain technology, each page in a ledger of transactions forms a block. That block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain.



SIMPLIFIED BITCOIN BLOCK CHAIN



What are Minors?

Cryptocurrencies and currencies differ within the way that new coins/cash are generated and issued in their respective ecosystems. currencies are printed by government in response to a state authority's direct orders, while cryptocurrencies are issued by a blockchain network consistent with a group of predetermined algorithms. Blockchain networks that make tokens supported Proof of work schemes require mining, a classy process. In brief, participants use hardware to run algorithms on specific software to verify transactions on the blockchain, add those transactions to the general public ledger and in exchange receive the reward of a newly-created coin.

What means Cryptocurrency mining?

Cryptocurrency mining is the process in which transactions between users are verified and added to the blockchain public ledger (DLT). The mining process is also responsible for introducing new coins into the existing circulating supply and there is one of the key elements that allow cryptocurrencies to work as a peer-to-peer decentralized network, without the need for a third-party central authority.
Bitcoin is the most popular example of a mineable cryptocurrency, but it is worth noting that not all cryptocurrencies are mineable. Bitcoin mining is based on a consensus algorithm called Proof-of-Work (POW).

Hashing

Hash functions. Public and personal key cryptographic algorithms both involve transforming plaintext into ciphertext then back to plaintext. By contrast, a hash function is one-way encryption algorithm: once you've encrypted your plaintext, you can't ever recover it from the resulting ciphertext (referred to as a hash). This is a way that minors should recover that plain text.

This might make hash functions appear to be a somewhat pointless exercise. But the key to their usefulness is that, for any given hash function, no two plaintexts will produce an equivalent hash.
This makes hashing algorithms an excellent tool for ensuring data integrity. For instance, a message is often sent alongside its own hash. Upon receiving the message, you'll run an equivalent hashing algorithm on the message text; if the hash you produce is different from the one accompanying the message, you know the message has been modified in transit.
Hashing is additionally wont to make sure the confidentiality of passwords. Storing passwords as plaintext may be a big security no-no because that creates users susceptible to account and fraud within the wake of knowledge breaches (which sadly doesn't stop big players from doing it). If instead you store a hashed version of a user's password, hackers won't be able to decrypt it and use it elsewhere even if they do manage to breach your defenses. When a legitimate user logs in with their password, you'll just hash it and check against the hash you've got on file.

Features of Cryptocurrency

Why we use Cryptocurrency and Key features of Cryptocurrency

- **They only exist Digital Environment**

This means you can only access your currency through the internet from a computer or mobile device. Your cryptocurrency will not have a physical form like traditional currency at any point in time. In other words, you'll never be able to physically hold your cryptocurrency as you would your regular cash.

That being said, cryptocurrencies are still kept in wallets, digital ones to be exact. Cryptocurrency wallets use a software program that helps you spend and receive the currency online.

- **Operate with decentralized network**

There is no central server for most cryptocurrencies. They exist across a network of thousands of computers and devices. Cryptocurrencies are not controlled by one central authority like:

- The government
- Any one person
- Any group
- A bank
- Part of a Peer-To-Peer network

Cryptocurrency networks rely entirely on a peer-to-peer network. These peer-to-peer networks regulate transactions and ensure everything checks out. For users of cryptocurrencies, the decentralized network helps prevent fraud and government interference. It also helps create efficient transactions.

These networks operate through users passing cryptocurrencies directly to other users. As each exchange takes place, it gets regulated by others in the network. As mentioned above, it is never regulated by a central bank, government, or authority. After each transaction takes place, it gets recorded in the network's public ledger. This ledger is visible to every user of the network and is referred to as the blockchain.

- **Use Encryption**

Encrypted systems translate data into a code that is secure and can only be read by certain people who have the key that decodes it.

The process of converting this information into a secret code is known as cryptography. This method gets applied in each cryptocurrency exchange and is essential for making sure that the transactions are:

- Secure
- Anonymous
- Never controlled by one central authority
- Transaction are permanent Cannot be Undone

Cryptocurrency transactions get recorded on the network's ledger. This makes them irreversible, unchangeable, and permanent.

- **Guarantee anonymous transactions**

Most cryptocurrencies allow you to stay anonymous during transactions. Encrypted codes and other security measures conceal users' identities on the network.

- **Divisibility**

Bitcoin can be further divided into smaller units known as Satoshi. Satoshi is the smallest unit of Bitcoin. One hundred million Satoshi is equivalent to one Bitcoin.

- **Fast and Global**

The transactions are independent of their physical locations and are propagated and verified almost instantly over the distributed network.
Secure
Only the owner of the Bitcoin cryptocurrency has access to the private key so no one else can access and use it. Strong cryptographic algorithm(SHA 256) is used to encrypt the transactions and blockchain. The transactions are recorded on the distributed ledger known as blockchain and hence there is no possibility of any failure or probability of vulnerability. This makes transactions less prone to bugs, hacking and

system failure as information is decentralized on a distributed network which in turn makes Bitcoin cryptocurrency more secure.

- **No Permission Required**

In order to use Bitcoin cryptocurrency, users are not required to take consent from anyone. The users just need to download software for free. Thereafter, they can exchange Bitcoin cryptocurrency with others.

- **No Debt but Bearer**

The traditional money is generated by debt and the numbers on the account representing the debt. The Bitcoin cryptocurrency does not denote debts. They are money like any other physical assets.

- **Efficient**

Since, the Bitcoin cryptocurrency uses peer to peer database and there is no central authority for controlling and validating the flow of digital currency, the transactions are verified and validated on the blockchain. Moreover, any user having internet connection can exchange the Bitcoin currency across the world. Therefore, the cost of operating the digital currency, in particular Bitcoin cryptography is much lower than any other traditional currency exchanged through bank transfer.

- **Trustless**

Bitcoin cryptocurrency is based on “no trust” among the participant users because of the underlying decentralized network means no one has to trust anyone else in the network. The transactions are broadcasted over the distributed network and digital signatures are validated before being recorded on the blockchain. It is discarded if the validation fails otherwise added in the blockchain.

Traditional Currencies Vs Cryptocurrencies

- **Anonymity**

Bitcoin, Ethereum, Litecoin, and lots more are cryptocurrencies. US Dollars, Pounds, euros, etc. are fiat currencies. The main difference between them is, the normal currency may be a centralized system and bitcoins are decentralized one and peer-peer systems. Hence there are not any central authorities to manage rules and regulations on a bitcoin transaction. But a standard currency is strictly regulated by the governmental authorities. Both the bitcoins and currency have values which can be used for buying and selling of goods in the market.

- **Flexibility**

With traditional currency functioning for five days every week and die to transaction restriction, there's an opportunity of freezing of currency. There is no limit within the number of currencies, being printed, and hence when there's inadequate currency, it'll affect the buyers and sellers, leading to inflation. But because the bitcoins have a maximum limit of 21 million bitcoins to be mined.

- **No fraudulent activity**

If you would like to transact with a standard currency system, the users need to provide personal details like name, address, telephone number , and much more. So, with the web technology, the malicious user are going to be ready to hack the account details of the normal currency system easily. Traditional currency can suffer from double-spending, where an equivalent money is employed for quite one transaction.
In the case of bitcoins, every transaction is recorded as blocks during a blockchain, which may be a large public ledger. A transaction are going to be stored as blocks, which contains transaction history, time of the transaction, and hash code of the previous block. This will be moved to

the memory pool, from where the miners want to solve the complex mathematical problem of 16-bit hashing digits to one bitcoin.
After verification, the miners generate a hash code for that block then encrypt them with an asymmetric encryption algorithm. After the block is given an encrypted hash code, it'll be added to the transaction chain. Once the blocks are added to the blockchain, the blocks can't be altered by any malicious users.
As every block structure has the hash code for previous blocks, the alteration will be known to all the users in the blockchain. If the malicious user tries to access the block, the hash code becomes more complex, and therefore the input can't be retrieved. The transactions are public, where every bitcoin user will realize the transaction details, but the user identity will never be disclosed to anyone, thus maintaining anonymity.

- **Reduced cost**

In a traditional banking industry, for creating a normal transaction, it will take 2-3 working days, and therefore the transaction fees are going to be high. Also international transactions, the transaction fee will be very higher and fee is depends with value of the transaction, and it will take more days to complete the transaction. But in a Cryptocurrency system like bitcoins, there is no transaction fee for making a national transaction or it was very small fees and not depend on transaction value. The transaction also will happen in seconds or within 24 hours, as a bitcoin system function 24 x 7. For making a world transaction, a transaction fee are minimum.

In the future, there's an opportunity of merging cryptocurrencies and therefore the banking industry, which can impose rules and regulations. But still, the normal banking industry are going to be pushed to adopt to blockchain technology, when such merging happens. So, even with frequent fluctuations within the bitcoin system, many of us wish to take a position in bitcoins thanks to speed transactions and reduced costs. Bitcoins are often exchanged with any currencies, saving time and

money at an equivalent time. so developing countries are taking steps for adopting blockchain in their business.

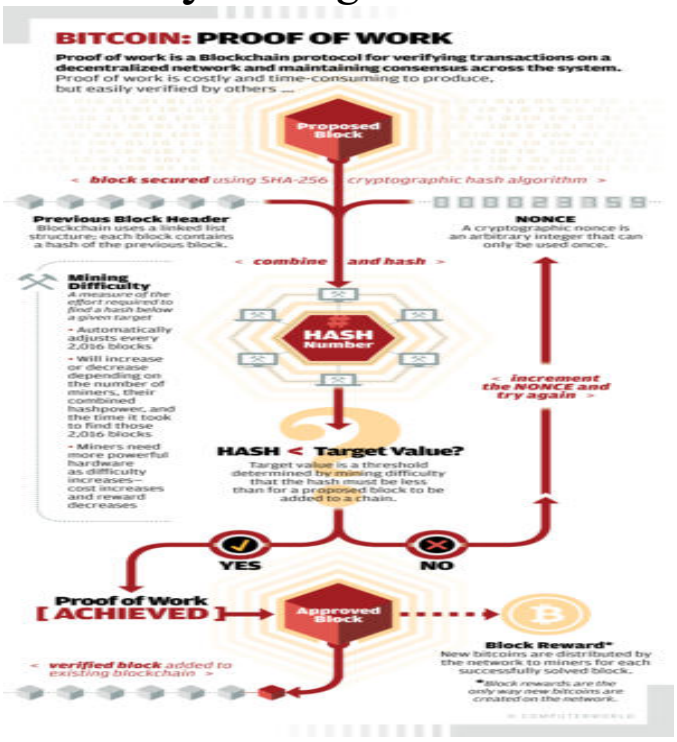
Benefits of Cryptocurrency

With cryptocurrency, the transaction cost is low to nothing at all—unlike, for example, the fee for transferring money from a digital wallet to a bank account. You can make transactions at any time of the day or night, and there are no limits on purchases and withdrawals. And anyone is free to use cryptocurrency, unlike setting up a bank account, which requires documentation and other paperwork.

International cryptocurrency transactions are faster than wire transfers too. Wire transfers take about half a day for the money to be moved from one place to another. With cryptocurrencies, transactions take only a matter of minutes or even seconds.

Cryptocurrency Mining and Process

What is Cryptocurrency mining?



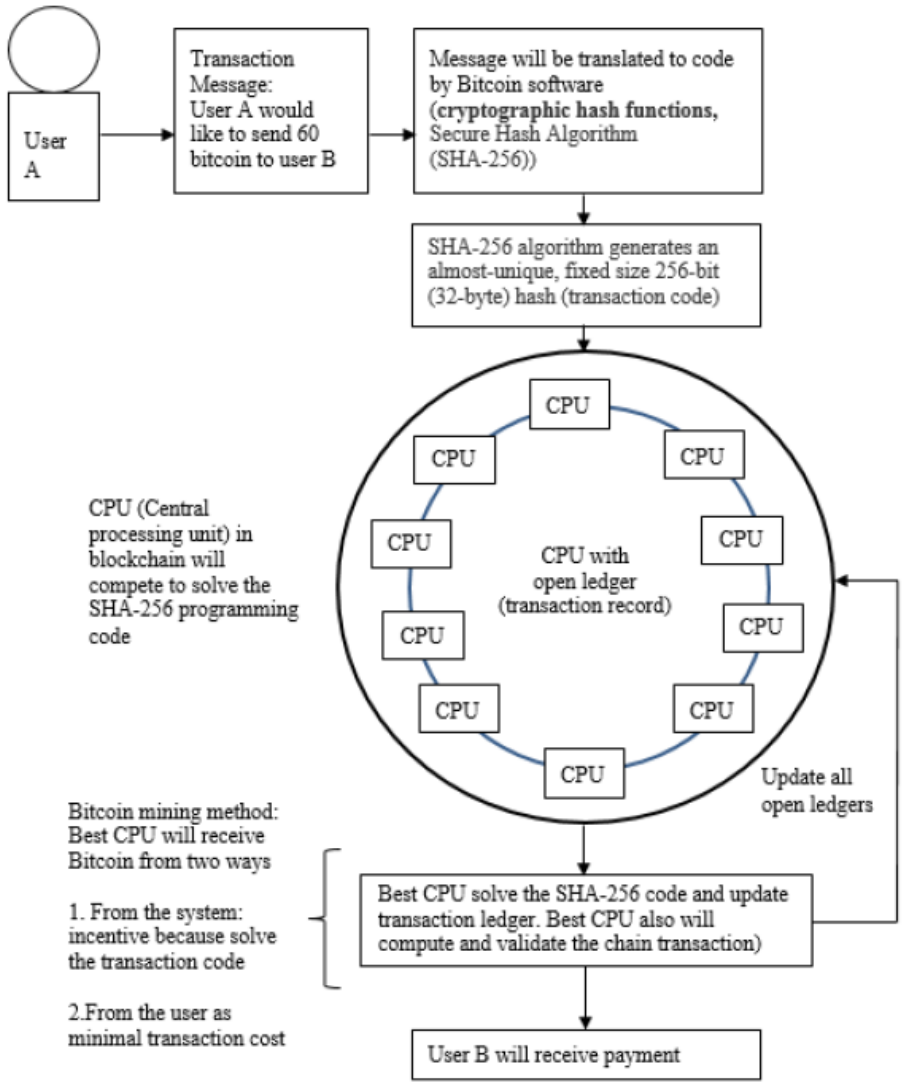
Explain of Mining process

The Bitcoin software runs on a powerful computer called node. It also helps in transmitting the information over the distributed network. The transactions are propagated over the network through nodes which are known to it, which in turn will spread it further. In this way, the transactions are spread very quickly over the network. Some of the nodes can act as mining nodes and are called miners. The job of the miners is to group all outstanding transactions together as a block. The block will then be appended to the blockchain.
The miners crack the complex mathematical puzzle which is part of the Bitcoin program. The miner tries to find a number known as nonce. This number will be combined with the data in the block. It will then be passed through the hash function. If it produces a result that should falls within a certain range. It is much difficult to guess the number, Moreover, the two consecutive numbers can have entirely different hash values. The only way to find the correct nonce is to keep trying until we get the desired output.
So, miner once finds the desired output; the miner communicates it to all other nodes in the network. Then rest of the miners stop working on that block. The miner who finds the desired output gets the reward in terms of certain Bitcoin.

Lot of mining nodes are trying to find the block and contending for the reward. It is just a matter of luck. More the computational power a node has, more is the probability to solve the problem puzzle and get the reward. More computational power leads to more consumption of electricity and hence the cost increases.

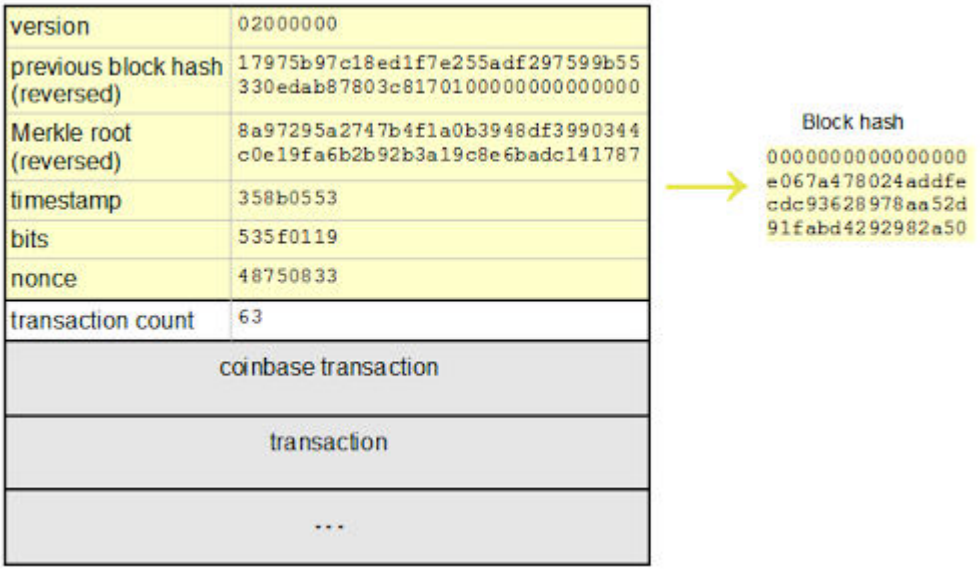
The mining is the process of finding the valid block. Anyone who has access to internet can become a miner. It is no one's job to delegate the authority for this task as it is using decentralized distributed network. A preventive mechanism is required to stop dominating one ruling party.

The distributed system would stop functioning immediately if someone produces and blowouts counterfeit transactions.
miners are competing with each other to find the desired solution, which is based on the cryptographic puzzle. Once the desired solution is found, the miner adds the block to the blockchain. The miner in turn is rewarded by certain number of Bitcoins. Bitcoin can be generated if and only of the miner solves the cryptographic puzzle. The difficulty of solving the puzzle increases and the reward in term of Bitcoin decreases over the period. The number of Bitcoin that can be generated in a given amount of time cannot exceed a specific amount. The more the hardware capability to solve the puzzle, the more will be the cost of mining block.



How mining works on Bitcoin

Bitcoin Mining requires a task that is very tricky to perform, but easy to verify. Bitcoin mining uses cryptography it uses a hash function called double SHA-256. A hash takes a portion of data as input and shrinks it down into a smaller hash value (in this case 256 bits). With a cryptographic hash, there's no way to get a hash value you want without trying a whole lot of inputs. But once you find an input that gives the value you want, it's easy for anyone to authenticate the hash. Thus, cryptographic hashing becomes a good way to apply the Bitcoin "proof-of-work".
In more detail, to mine a block, you first collect the new transactions into a block. Then you hash the block to form a 256-bit block hash value. If the hash starts with sufficient zeros, the block has been successfully mined and is sent into the Bitcoin network and the hash becomes the identifier for the block. Most of the time the hash isn't successful, so you alter the block to some extent and try again, over and over billions of times.
About each 10 minutes somebody will successfully mine a block, and the procedure starts over.



Above fig shows the structure of a precise block, and how it is hashed. The yellow part is the block header, and it is followed by the transactions that go into the block. The first transaction is the special Coinbase transaction that grants the mining reward to the miner. The remaining transactions are normal Bitcoin transactions moving bitcoins around. If the hash of the header starts with enough zeros, the block is successfully mined. For the block below, the hash is successful: 00000000000000000e067a478024addfecdc93628978aa52d91fabd4292982a50 and the block became block #286819 in the blockchain. The block header contains a handful of fields that illustrate the block. The first field in the block is the protocol version. It is followed by the hash of the preceding block in the blockchain, which ensures all the blocks form a continuous sequence in the blockchain. The next field is the Merkle root, a special hash of all the transactions in the block. This is also a key part of Bitcoin security, since it ensures that transactions cannot be altered once they are component of a block. Next is a timestamp of the block, followed by the mining complexity value bits. Finally, the nonce is a random value that is incremented on each hash attempt to give a new hash value. The difficult part of mining is finding a nonce that works.

Steps to Mining

The nodes which participate in the mining process are known as miners. These nodes execute the following steps:

1. The miner collects all transactions broadcasted over the distributed network.
2. The transactions are checked and verified. They are also checked whether there have been spent previously or not.
3. The most recent block on the longest path is selected on the blockchain. The path which has accrued maximum computational power is the longest path.

4. The miner solves the Proof of Work and the solution is broadcasted to all the nodes in the network. The above steps are repeated. Any transaction not included in the block are saved for next cycle.

The miner tries to find a block whose SHA256 lies below the target value. The miner calculates several hashes keeping block intact. Following steps are used to find the Proof of Work.

1. Set the nonce value to user's choice
2. Compute the hash of block header
3. Reverse the byte order of the computed hash.

Check whether it lies below the target value. The process is repeated until the valid solution is found.

Conclusion and Future

Future of Cryptocurrency

The world is clearly divided when it comes to cryptocurrencies. On one side are supporters such as Bill Gates, Richard Branson, who say that cryptocurrencies are better than regular currencies. The other side are people such as Warren Buffet, Paul Krugman, and Robert Shiller, who are against it.

In the future, there's going to be a conflict between regulation and anonymity. Since several cryptocurrencies have been linked with terrorist attacks, governments would want to regulate how cryptocurrencies work. On the other hand, the main emphasis of cryptocurrencies is to ensure that users remain anonymous.

Futurists believe that by the year 2030, cryptocurrencies will occupy 25 percent of national currencies, which means a significant chunk of the world would start believing in cryptocurrency as a mode of transaction. It's going to be increasingly accepted by merchants and customers, and it will continue to have a volatile nature, which means prices will continue to fluctuate, as they have been doing for the past few years.

References

1. Tseng, L., 2017. Bitcoin's Consistency Property. *Proceedings of the IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp.219–220.

2. Viswam, A. and Darsan, G., 2017. An Efficient Bitcoin Fraud Detection in Social Media Networks. *Proceedings of the International Conference on Circuits Power and Computing Technologies (ICCPCT)*, pp.1–4.

3. Fraser, J.G. and Bouridane, A., 2017. Have the Security Flaws Surrounding BITCOIN Effected the Currency's Value? *Proceedings of the Seventh International Conference on Emerging Security Technologies (EST)*, pp.50–55.

4. Mehrzad, M. and Mirzayi, S., 2017. Bitcoin, an SWOT Analysis. *Proceedings of the Seventh International Conference on Computer and Knowledge Engineering (ICCKE 2017)*, October 26–27; Ferdowsi University of Mashhad. pp.205–210.

5. Desai, A., Hariya, M., Wagle, Y. and Deshpande, S., 2017. Buyer's Protection in Bitcoin. *Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017*, pp.713–715.

6. Zhu, J., Liu, P. and He, L., 2017. Mining Information on Bitcoin Network Data. *Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp.999–1003.

7. Liu, Y., Li, R., Liu, X., Wang, J., Zhang, L., Tang, C. and Kang, H., 2017. An Efficient Method to Enhance Bitcoin Wallet Security. *Proceedings of the 11th IEEE International Conference on Anti-Counterfeiting, Security, and Identification (ASID)*, Xiamen. pp.26–29.

8. Zhu, F., Chen, W., Wang, Y., Lin, P., Li, T., Cao, X. and Yuan, L., 2017. Trust Your Wallet: A New Online Wallet Architecture for Bitcoin. *Proceedings of the International Conference on Progress in Informatics and Computing (PIC)*, Nanjing. pp.307–311.

9. Qin, R., Yuan, Y., Wang, S. and Wang, F., 2018. Economic Issues in Bitcoin Mining and Blockchain Research. *Proceedings of the IEEE Intelligent Vehicles Symposium (IV) Changshu*, June 26–30; Suzhou, China. pp.268–273.

10. Soni, A. and Maheshwari, S., 2018. A Survey of Attacks on the Bitcoin System. *Proceedings of the IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, pp.1–5.

11. Beerliova-Trubiniova, Z., Hirt, M. and Riser, M., 2007. Efficient by zantine agreement with faulty minority. *Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security*, Springer-Verlag. pp.393–409.

12. Bentov, I., Lee, C., Mizrahi, A. and Rosenfeld, M., 2014. Proof of activity: Extending bitcoin's proof of work via proof of stake. *ACM SIGMETRICS Performance Evaluation Review, 42*(3), pp.34–37.

13. Biryukov, A., Khovratovich, D. and Pustogarov, I., 2014. Deanonymisation of Clients in Bitcoin p2p Network. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pp.15–29.

14. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A. and Felten, E.W., 2015. Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *Proceedings of the IEEE Symposium on Security and Privacy*, pp.104–121.

15. Vallois, V. and Guenane, F.A., 2017. Bitcoin Transaction: From the Creation to Validation, a Protocol Overview. *Proceedings of the First Cyber Security in Networking Conference (CSNet'17) 1570383518*, pp.1–7.

16. David Easley, D., O'Hara, M. and Basu, S., 2019. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, *134*(1), pp.91–109.

17. Ankalkoti, P. and Santhosh, S.G., 2017. A relative study on bitcoin mining. *Imperial Journal of Interdisciplinary Research (IJIR), 3*(5), pp.1757–1761.