International Journal of Research in Engineering, Science and Management
Volume 4, Issue 7, July 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Applications of Blockchain in Cryptocurrency: Bitcoin and Dogecoin

K. Nagamani[1], R. Pruthu[2], Veluri Sai Teja[3*]
[1]*Professor, Department of Electronics and Telecommunication Engineering, RV College of Engineering, Bangalore, India*
[2,3]*UG Student, Department of Electronics and Telecommunication Engineering, RV College of Engineering, Bangalore, India*

***Abstract*: Blockchain is a secure way of storing information in a decentralized manner. It can also be viewed as another paradigm to store and record exchanges. In blockchain, blocks are connected with each other cryptographically with a specific intent to ensure that the contents are immutable thereby making the data stored impossible to tamper with. This emerging technology was developed in 2008 to lay foundation of digital money. This currency is a digital asset which is used to purchase, sell or transfer between two parties securely over the web electronically without involvement of third parties like banks, other types of organizations and government institutions. In this paper, we present a structured analysis of blockchain and compare cryptocurrencies like Bitcoin and Dogecoin. Also related cryptographic techniques, technological advantages and the process of mining is illustrated.**

***Keywords*: Blockchain, decentralization, public-ledger, mining, SHA-256, Scrypt, hash, cryptography.**

1. Introduction

A blockchain is an immutable and continual growing distributed public ledger system that keeps unerasable records of every transaction on multiple nodes connected together by a large network such as the internet. Hence, if any individual alters, deletes or appends some record, it will get reflected on all the nodes after synchronization and re-evaluation of the hash. Consequently, it can be said that blockchain is the core concept or the brain behind the creation of digital currencies. As it is distributed, cryptocurrency has no regulatory framework or supreme authority above it. This technology removes the barrier of mistrust that is present in traditional banking systems which involve government organizations, third party vendors and other financial institutions.

The four main features namely decentralization, tamper-proof, transparency and security make cryptocurrency far superior to fiat currency. Security is achieved by making use of cryptography techniques and algorithms such as SHA-256, Scrypt and hash functions.

2. Literature Review

An apt comparison between the cryptocurrency market with traditional financial markets, foreign exchange, and stock market is done [1]. Various developments of cryptocurrency were explored and their applications in a variety of fields such as financial transactions, capital management, and even non-monetary applications were discussed.

Blockchain as the offshoot for Bitcoin is given and the working on how the data is allocated in each block in a blockchain without any loss of data. [2] it is understood that the data is secure and is easily available for any user as the data is translucent yet secured by using few hashing techniques bitcoin application using blockchain infrastructure has gained attention with its reliability robustness and performance

Cryptocurrency mining is a process that makes sures the safety of the cryptocurrency system is not compromised. Mining for cryptocurrency has a lot of demands and if one wishes to mine a single cryptocurrency, high computational power as well as the time is required and the amount is awarded by giving a few coins known as PoW. [3] We see that most of the mining techniques focuses more into getting maximum outputs by using the computing capacity and also ensuring max performance to get optimum computing capacity.

The Internet-of- Things (IoT) scenario along with blockchain is examined in a general peer-to-peer approach which in turn could play a major role in the establishment of decentralized and data exhaustive software applications running on billions of devices addressing the concern of safeguarding the privacy of the users. The aim of this paper [4] is to understand whether blockchain and peer-to-peer approaches can be exploited to promote a decentralized public IoT ecosystem.

The Bitcoin currency's future scope can go up to such an extent that it can be considered as the universal coin acceptance. [5] There is a massive gap between the theoretical methods of implementation to the practical execution of bitcoin with respect to the decentralization of the framework, safety and how reliable a bitcoin can get in the coming years. There is a risk of security and feasible attacks are possible on the management of bitcoin. Bitcoin wallets are safe but up to what extent is questionable, this paper has come up with a solution named bitcoin core which is the safest means of storing the bitcoin and

*Corresponding author: velurisaiteja.te17@rvce.edu.in

blockchain rewriting is the only vulnerability of this wallet.

3. Cryptography Techniques Used in Bitcoin, Dogecoin and Mining

There are two techniques involved: 1) SHA algorithm 2) Scrypt algorithm.

SHA algorithm: SHA stands for secure hash algorithm which was originally developed as SHA-1 algorithm. This algorithm takes any length of string and performs mathematical operation and gives out a hash function of 160 bits irrespective of the length of string that is given as an input. The complexity of this algorithm is less and hence it takes a smaller amount of time, to increase the complexity of the SHA-1 algorithm the NSA came up with another algorithm known as SHA-256, the SHA-256 takes any length of strings and produces the hash function of 64 bits. SHA-256 takes 512-bit blocks of data one at a time until the files are expanded, and if the message is exactly 512 bits in length, then the algorithm is run only once. The mathematical formulae used is SHA is as follows:

$$vwxyz = (z + Process\ P + G^{5}(v) + W[t] + K[t]):\ v, G^{30}(w), x, y \quad (1)$$

Where, vwxyz= The register of 5 variables u, v, x, y, z process P is logic operation and G^{t} is the circular right shift by t bits. W[t] is a 32-bit obtained from the current 32-bit sub-block. K[t] is an additive constant.

The values of W[t] are calculated as follows:

$$W[t] = s^{1}(W[t-16]\ XOR\ W[t-14]\ XOR\ W[t-8]\ XOR\ W[t-3]) \quad (2)$$

Scrypt algorithm: Scrypt is an algorithm that uses a similar mathematical function such as the SHA, but instead of computing the algorithm in the CPU the Scrypt algorithm is computed in the GPU hence it is much faster than the SHA. The Scrypt algorithm is used in mining of altcoins like Dogecoin. The Scrypt algorithm takes any length of strings and produces the hash function of 64 bits.

The Scrypt algorithm takes in few parameters and produces the derived key as output: K is the Scrypt (pass, salt, M, q, l, derived-key-length) The Scrypt arguments are: M – iterations count q –size of block l – parallelism factor (number of threads running in parallel) pass – input password salt – random bytes that are securely-generated derived-key-length -size of output in bytes. The Scrypt key derivation is obtained using the above equation and the memory required is as follows:

Memory required = 128 * M * q * l bytes

Example: 128 * M * q * l = 128 *2048 * 8 * 1 = 2 MB

Mining: Mining can be understood as the operation of updating the blockchain ledger transactions (in this case of Bitcoin/Dogecoin) encouraged by awarding a new coin as the PoW.

Individuals who undertake the process of mining are known as miners and their job is to solve a complex mathematical enigma in order to crack the cryptographic condition. The person who does this first receives the reward, thereby validating the transaction and adding a new block onto the blockchain.

This cryptographic puzzle to be solved has the preset condition that the number of leading zeros after solving the problem should be a fixed value. Currently the number of leading zeros to be obtained is 20 i.e., the hash to be calculated should begin with 20 zeros. The number of leading zeros represent the difficulty level of the blockchain.

Nonce: It is a 4 bytes (32 bits) number abbreviated as number used once. To make a particular block valid, miners have to pick an arbitrary number by hit and trial method for figuring out a correct nonce field to get leading zeros in a cryptographic hash generator.

4. Results and Analysis

For any input argument, the SHA-256 has a fixed output hash of 64 bits. Each bit is represented in its hexadecimal form so the total number of bits is 64*4 that is 256. As the complexity of SHA algorithm is increased by including more iterations /rounds, the length of hash value also increases.

SHA algorithm is implemented using the inbuilt libraries offered by Python and executed in PyCharm IDE. Scrypt is also executed in the same way.

Mining is implemented by invoking two user defined functions and passing the required arguments. The time taken to obtain the output is measured by importing the 'time' module.

Scrypt algorithm is a frequently used algorithm for upcoming cryptocurrencies as it is faster to compute as well as an easier algorithm in terms of understanding. SHA takes a lot of power consumption when compared to Scrypt algorithm and this can be a contributing factor for Scrypt algorithm to be much more popular than SHA. SHA is used in applications where there is a need for more security as it is the most complex algorithm used in blockchain development. Hence bitcoin wallets use SHA algorithm to protect the servers. For a miner using the SHA algorithm, high hash rates which go up to giga hashes per sec GH/s are necessary.

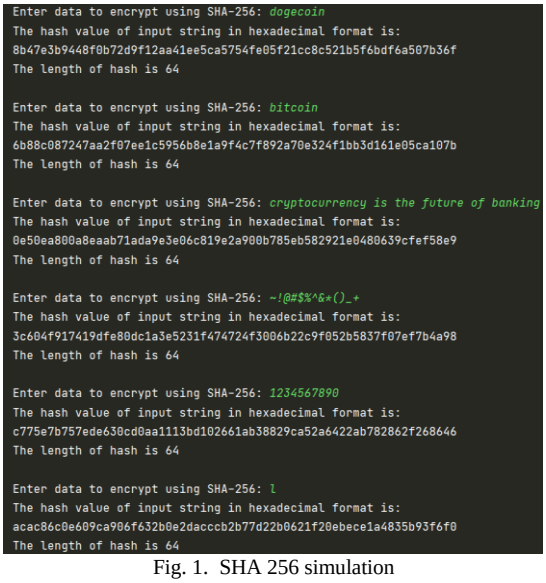

Fig. 1. SHA 256 simulation

Also, the mining process depends on the difficulty level as shown below. Increasing the number of leading zeros exhibits that the system/mining configuration takes a substantial proportion of time to solve the puzzle. The value of nonce is incremented till the first 'n' bits of hash is not equal to the number of leading zeros.

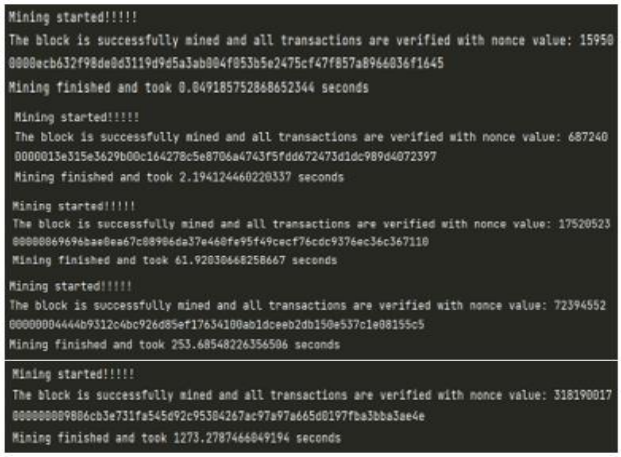

Fig. 2. Simulation of mining process with increasing number of leading zeros ranging from 4 to 8 each representing a particular difficulty level

Table 1
Results

Number of leading zeros	Nonce value generated	Time taken(s)
4	15,950	0.04918
5	687,240	2.19412
6	17,520,523	61.9203
7	72,394,552	253.68548
8	318,190,017	1273.27874

Table 1 depicts the nonce value generated for each level of difficulty. It is inferred that the time taken to generate the nonce increases exponentially according to the number of leading zeros.

5. Conclusion

This paper compares the cryptographic algorithms employed in Bitcoin and Dogecoin along with the functioning of the mining process and the generation of nonce value needed to validate the transaction to be shown as proof-of-work through a piece of code.

The concept of cryptocurrencies, despite being developed recently, is a subject that has an increasing surveillance. An increasing number of charities, other organizations and businesses are accepting cryptocurrency remittances ranging from e-retailers to sports franchises to law firms. Some large multinational companies, such as Twitch, Tesla etc. are beginning to take receipt of Bitcoins. Many other alternative currencies were developed after Bitcoin and are known as altcoins. Some of them face identical problems while others have an upper hand when compared to Bitcoin. It is quite difficult to anticipate which of these will succeed, but we can consider Bitcoin as a relative success in terms of its usage and the news volume that it generates. Further, recent inflationary and banking crises across the globe have spotlighted some of the key threats inherent to fiat currency. This creates extra opportunities for decentralized digital currencies.

References

[1] J. Liang, L. Li, W. Chen and D. Zeng, "Towards an Understanding of Cryptocurrency: A Comparative Analysis of Cryptocurrency, Foreign Exchange, and Stock," 2019 *IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2019, pp. 137-139.

[2] Baygin N, Baygin M., and Karakose M. (2019). Blockchain Technology: Applications, Benefits and Challenges.1st *International Informatics and Software Engineering Conference.*

[3] P. V. Sukharev and D. S. Silnov, "Asynchronous Mining of Ethereum Cryptocurrency," 2018 *IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies"* (IT & QM & IS), 2018, pp. 731-735.

[4] Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. 2016 *IEEE/ACS 13th International Conference of Computer Systems and Applications* (AICCSA).

[5] P. K. Kaushal, A. Bagga and R. Sobti, "Evolution of bitcoin and security risk in bitcoin wallets," 2017 *International Conference on Computer, Communications and Electronics (Comptelix)*, 2017, pp. 172-177.