ISSN: 2096-3246
Volume 58, Issue 01, 2026

Comparative Analysis of Cryptographic Hash Functions in Blockchain and Their Possible Solutions

1st *Urvashi Chaudhary*
PhD Scholar, School *of Computer Science & Engineering,*
IFTM University, Moradabad, UP

2nd *Dr. Amit Bhatnagar*
Assistant Professor, School *of Computer Science & Engineering,*
IFTM University, Moradabad, UP

***Abstract*—As much as managing money is a part of our life, we are also more worried about security and safety. Blockchain tech is new but is efficient and able to drive expectations that it could lead to a new generation of applications. Essentially, blockchain is dependent on technology that encrypts digital data transfer. The success of any cryptocurrency lies in ensuring the privacy of the users and their transactions. The underlying data structure of the blockchain which supports scalability and security relies on hash functions. The hash function used by a blockchain to secure its operations can be tested against security criteria to evaluate its security. This text depicts the key elements of blockchain technology. In addition, it offers a short description of hash functions like Whirlpool, MD (Message Digest), RIPEMD, SHA (Secure Hash Algorithm), and BLAKE. The study comes to a conclusion after comparing the results. The simulation result shows that various cryptographic hash algorithms yield good results for different evaluation metrics such as frequency, throughput… etc.**

Keywords—blockchain technology, crypto currency, system security, message digest (MD), and secure hash algorithms (SHA) used in cryptographic applications.

I. Introduction

The idea of organizing data in a chain of encrypted blocks that are linked is not new. Stuart Haber et al. proposed this idea in 1991 to prevent tampering with digital data [1]. Blockchain, or distributed ledger technology, describes a chain of linked digital blocks that serve as a public ledger for transactions. Blockchain was used only for recording transactions related to digital currency. But later its application spread beyond finance and trade. Recently, the press has looked a lot at blockchain, which is the tech used to power many cryptos and is being marketed as a decentralized alternative that does not rely on a central trusted authority. A blockchain can be defined as a distributed append-only ledger that contains timestamped records, is tamper evident and secured by cryptography [2].

Blockchain enables the advantages of a peer-to-peer network, by relying on cryptographic systems to guarantee that every transaction participant abides by the agreement. One person cannot change the plan or record an activity without the consent of others. Organizations in different sectors can safely transact with one another thanks to this ability. Blockchain is the technology that ensures that events are stored in chronological order and they cannot be faked.

It is tremendously complicated to falsify records or reverse agreements since no single user is capable of changing the transaction history. Many of the industries are thinking of its adoption, and efforts are ongoing to figure out the best ways to implement.

Blockchain is peer-to-peer (P2P) networks that make use of cryptographic technologies that makes sure every party in an agreement sticks to their word. In the absence of another agreement, no participant may change a contemplated or recorded activity without the consent of all other parties involved. This capability allows businesses from various industries to transact safely with one another [3][1]. Because of its role in founding the digital currency bitcoin [4], blockchain technology has attracted much academic and commercial attention. The blockchain essentially serves as a ledger in the bitcoin system. Nonetheless, the public nature of blockchain transactions can be detrimental to their privacy. In contrast, conventional bankers generally keep records on a confidential basis. In a commercial and technological setting, this is less so where it is often clear who was involved in a transaction. Blockchain technology is widely recognized for its potential across multiple domains, particularly in enhancing privacy and security through applications such as risk control, data protection, and syste integrity. It also plays a significant role in digital currencies and financial services, including stock trading platforms, peer-to-peer markets, and crowdfunding systems. Beyond finance, blockchain is applied in reputation frameworks for research and online communities, as well as in the Internet of Things (IoT) to support secure e-business operations and data handling [1]. A key factor behind its rapid adoption is its versatility. Blockchain is being utilized in a broad range of sectors, including defense, education, identity verification, intellectual property management, mobile platforms, asset monitoring, healthcare, and a supply chain system. Its use further extends to industries such as agriculture, advertising, electroral processes, automotive systems, insurance, digital record-keeping, and law enforcement, particularly in applications that require reliable tracking of asset ownership and location. Blockchain technology utilizes the advantages present in peer-to-peer networks with cryptography so that every participant in the transaction can meet their terms. Until and unless all participants agree, no one can change an action or record. This allows firms in various sectors to transact with one another without worry. The sequence of events is maintained in blockchain technology and ensures the authenticity of the records. It is extremely hard to falsify the record or reverse agreements as the transaction history cannot be altered by a single user only. Consequently, several industries are considering the application of it, and measures are being taken to ascertain the best practices.

With rising numbers of application deployed on blockchain, it is becoming important to secure data available on blockchain. Attackers are exploiting blockchain's distinctive features to launch different types

of attacks, which jeopardizes the information stored on the distributed ledger. Inferences from the IP address can link it to a Bitcoin address. Therefore, these attacks threaten the integrity of blockchain data and transferability of the currency. This association may assist the attackers in user monitoring, revealing their true identity, and tracking their IP address consistency [5].

Although the mining power (hash rate) is a key security feature of Bitcoin and other cryptocurrencies based on Nakamoto consensus, its distribution could reflect the market share of mining pools. If an attacker obtains control of more than fifty per cent of the hash rate of the entire blockchain network, the hacker will be able to erase all the transaction history, stop new transactions from being added to the new block and carry out double spending attacks. Even beneath this benchmark, endeavors like avaricious excavation and its alterations remain practicable [6]. Research studies on how concentrated is the mining power despite the security is vital are limited. Recent studies have researched centralization on the peer-to-peer layer, which revealed that over the long run, eight Bitcoin miners and five Ethereum miners had more than half of the total mining power jointly. As shown in figure 1, cryptocurrency mining is discussed.

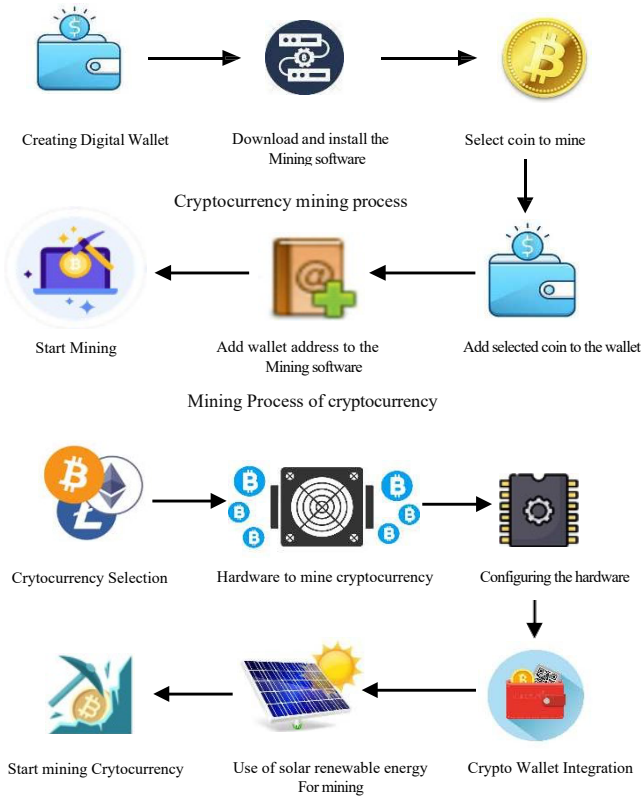


Fig. 1. Cryptocurrency mining process

A. Mining Pools

Miners join together to combine their resources, or hash power, in order to increase the chances of finding a block. Because the chance to successfully mine a block is proportional to the available computational power, the chances of a block being solved quickly increase by joining a mining pool. By splitting the work among many, these pools lower the risks of Bitcoin mining activity. The miner receives a fraction of the reward based on profit sharing. Nonetheless, miners tend to receive steady – if smaller – base returns, as transaction fees are not fully paid out, plus an extra fee to the pool operator to cover costs.

If miners want, they can switch to higher total hash rate pools. Research from Blockchain.info in July 2014, pooling calculated hash rates for existing mining pools, which revealed that GHash.IO and BTC Guild were the largest pools at the time. For Each mining pool differs in size, construction, and reward schemes. Bigger pools usually offer more stable and predictable earnings with less variance. Smaller pools might give less frequent but potentially larger rewards. Smaller pools also help limit the degree of centralization of hashing power through a broader distribution of miners.

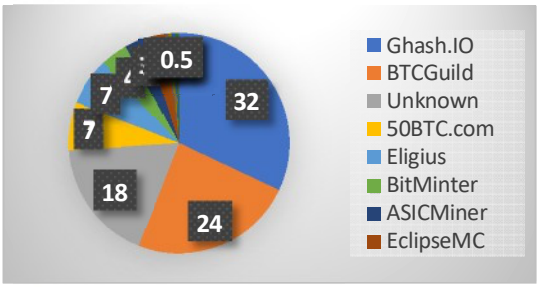


Fig.2 Mining pools

Bitcoin mining infrastructure is represented in figure 2. The mempool is a facility that temporarily stores a new transaction.The next step is to try to add this candidate block to the Bitcoin blockchain. Finding a number which, when hashed with SHA-256 as such, gives a hash with a value lesser than the target. The process of mining cryptocurrency consists of starting the mining process, adding a wallet address to the mining software, and linking the selected coin to the wallet. The blockchain architecture is shown in figure 3.

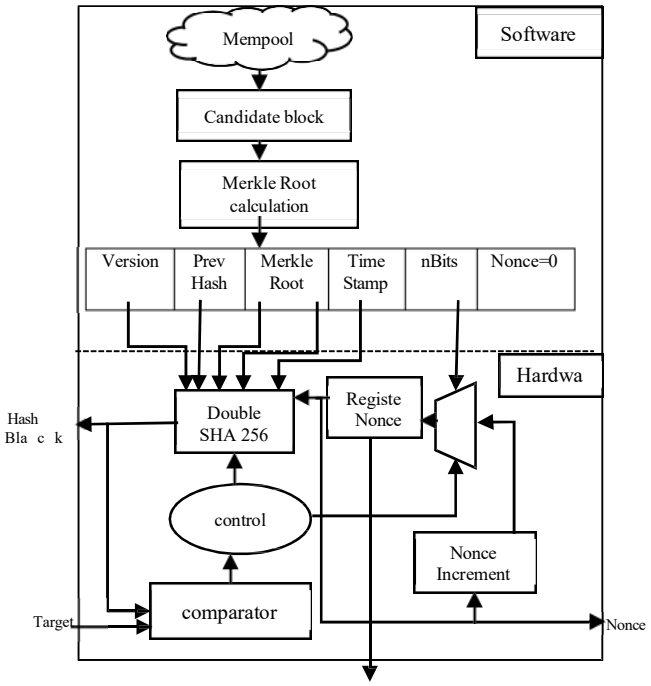


Fig. 3.Architecture of blockchain

The rest of the paper is organized in the following way – blockchain applications are discussed in section II, cryptocurrency, smart contracts, Hyperledger, etc. Section

III covers the literature review, while Section IV looks at cryptographic hash function. Section V compares state-of-the-art (SOTA) algorithms. To conclude the paper, Section VI will allow us to do so.

I. Applications of Blockchain

Aside from being used as a cryptocurrency, blockchain technology has other uses that can help reduce operational and administrative costs for businesses. The software is used in various sectors such as finance, healthcare and more looking for a safe, clear and efficient data storage.

A. Cryptocurrency

Bitcoin, introduced in 2009 by Satoshi Nakamoto, is built entirely on blockchain technology. Its underlying structure and transaction process are based on a distributed ledger, and it does not derive value from any physical asset. Transactions in this system occur directly between users without relying on intermediaries, using cryptographic methods for security. When a user initiates a transfer, the transaction is digitally signed with a private key and then shared across the network, where it is validated by other participants. A comparative overview of related systems is provided in Table I.

TABLE I. Systems of Cryptocurrencies

Cryptocurrency	Hash Algorithm	Year	Mining Method
Bitcoin	SHA-256 hashing function	2009	Proof-of-work(PoW)
Litecoin	Scrypt based hashing algorithm	2011	Proof-of-work(PoW)
Ripple	SHA-512 cryptographic function	2012	Proof-of-work(PoW)
Peercoin	SHA-256 hash function	2012	Proof-of-work(PoW)
Primecoin	Cunningham chain computation	2013	Proof-of-work(PoW)
Blackcoin	Scrypt hashing technique	2014	Proof-of-work(PoW)
Monero (XMR)	Ring signatures based privacy protocol	2014	Proof-of-work(PoW)
Ethereum (ETH)	Ethash algorithm	2015	Proof-of-work(PoW)

B. Smart Contract

A code can represent a transaction between the buyer and the seller. The contractual terms and the program can both be stored in a blockchain, which is a distributed ledger [8]. A smart contract is a self-executing piece of code that facilitates and enforces the exchange of digital asset between participants when predefined conditions are satisfied.The advantages of a smart contract are particularly proven in business collaborations. Agreements are coded into the contract and all parties are aware of what's to happen when the collaboration commences. Like humans, smart contracts function independently to automate through the execution of predetermined instructions and holding funds in escrow when needed. To enable smart contracts to run on a decentralized network, ETH was created as the native digital currency used within the Ethereum blockchain.

C. Hyperledger

Hyperledger is a blockchain framework that requires a modular architecture with a variable component that allows the ease of scaling for an organization's needs. It is managed by the Linux Foundation and it aims to provide a powerful technology platform which decreases the level of complexity when it comes to enterprise blockchain affairs and its deployment. The Hyperledger consists of many blockchain frameworks in its collaboration network. This is comprised of private and permissioned blockchain infrastructures that can use smart contracts via the use of enterprise industries. Compatibility with major industries such as automotive and banking is a possibility with this framework. The use of Linux OS has allowed its cooperation with use of major non-blockchain and node systems. This often uses various Linux system services and APIs. Hyperledger is an open-source global collaboration with many cross-industry associations. Members and contributors from organizations and businesses consist of its project team. The use of power big clouds allows their project to develop blockchain solutions. With the help of contributors, they are the architect of Industrial blockchain landscape.

Hyperledger fabric standard and architecture inspires various installations and uses with its sub-projects. All of which use various Linux systems and its structure. Structured participation in consensus phases through replicated state machines is a standard method. Wherein a machine Hyperledger is a collaborative project (an open-source platform governed by the Linux Foundation) which has seen contributions from the likes of finance, supply chain, IoT, manufacturing, and IT experts [9]. Hyperledger does not feature any native cryptocurrency and only authorized users can participate in the network. These functions are known as chaincode. Similar to smart contracts, they are deployed within the network to carry out transactions. When the user needs to invoke the chaincode on a specified channel, a transaction is sent to Hyperledger Fabric. The Hyperledger Fabric architecture consists of three components peer nodes, client applications, and ordering nodes. Furthermore, the anonymity of transaction participants in the network is ensured through isolation channels.

D. Other Applications

In addition to smart contracts and cryptocurrency, trade finance, health care, academic systems, IoT, insurance, supply chain management, voting systems, international payments weren't the only industries taking note of other application areas for blockchains.

III. Literature of review

Gundaboina et al. (2022) argue cryptocurrencies have gained attention in the quest for blockchain-based finance sustainability as they are mostly run by renewable energy. In the essence of time, the researcher's objective was to assess the Blockchain application practicing Crypto Currency in diachronic perspective. There is currently limited research estimating the volume of renewable energy needed to consistently operate such a mine. The authors investigates Solar Energy As a Sustainable & Performance Effect of overclocking and undervolting on dogecoin miner performance. their research paper relates to Sustainable Power. The researchers collected the data using different types of Graphic Processing Units (GPUs) and non-lite hash rate (LHR) hardware. This software can both mine and store your dogecoin in a wallet similar to your USB wallet. According to the research, mining Dogecoin with solar energy uses about 2000 watts on overclocking and about 1700 watts on undervolting. The research also points to important questions about whether all cryptocurrency mining can be carried out using renewable energy and what hardware configurations would be needed. The method could also reduce e-waste and encourage sustainability.

The study shows that miners can enhance their

performance without harming the environment by optimizing their GPU usages and using green energy that provides them with power-efficient and less e-waste [10].

Jones, Goodkind, and Berrens (2022) Bitcoin (BTC) is the most widely used proof-of-work cryptocurrency whose miners consume a substantial amount of energy. The paper assesses the economic cost of climate damage. The authors outline three criteria to identify when climate-related damages might become untenable; Bitcoin mining fails under all three of their criteria. The climate damage of Bitcoin increased for the years 2016 to 2020 each year with industry maturation. Moreover, for some periods, the environmental cost of creating each Bitcoin exceeded its market price. The climate impact of producing one dollar of Bitcoin value was around 35 cents. This damage is less than that caused by beef production and crude oil combustion. Blockchain technology's energy consumption must be curbed by proper governance People generally refer to Bitcoin as "digital gold". But, it is more like "digital crude" when it comes to environmental impact [11].

According to Sun et. al (2022), Bitcoin mining plays a key role in sustaining the entire network and acts as the primary intermediary between digital currency systems and the real world. Network security, cryptoasset, and environmental impact are part of their research. Using bottom-up monitoring methods and geographical analysis, they investigate the worldwide spread of Bitcoin mining activities. The decentralized nature of the Bitcoin network means that mining operations are dispersed across more than 6,000 geographic units within 139 countries and regions in the world. According to our estimates, despite the global dispersion of energy production, there is a high concentration of computational power in regions with better access to renewable energy resources.

In addition, the study shows that the location of mining activities changes with economic and regulatory changes [12].

The paper investigates the factors influencing the decisions of global miners to undertake cryptocurrency mining, with electricity cost being the key factor. The discussion around the use of renewable energy to minimise the environmental impact of Bitcoin mining has gained traction. The energy modelling of the International Energy Agency incorporates many dimensions, including energy prices; energy generation; weather; regulatory obstacles; human capital; and research and development and innovation R&D&I

They build a modified environment performance index using linear regression after accounting for these environment and social variables upon the environment performance indexEPI.

Through the recalculated EPI, they now show the link between sustainability issues and the practice of cryptocurrency mining.

According to the Environmental Performance Index (EPI), Germany and Denmark emerge as the most favorable locations for Bitcoin mining. Of the ten leading countries, eight are European-including Denmark, Germany, The United Kingdom, Finland, Austria, and Switzerland-while only two are based in Asia [13].Table II summarizes the relevant systematic review studies associated with this work.

IV. Cryptographic Hash Functions

Many cryptographic hash functions are built using the Merkle–Damgård approach, either developed independently or derived from block cipher designs. These functions are broadly categorized into two types: unkeyed and keyed. Unkeyed hash functions, often referred to as Manipulation Detection Codes (MDCs), require only the input message, whereas keyed hash functions take both a message and a secret key as inputs. The keyed variants are commonly known as Message Authentication Codes (MACs). In general usage, the term "hash function" typically refers to the unkeyed form [21].

Well-known examples of cryptographic hash families include the MD series and the SHA series, both specifically developed for security applications. Another notable example is the Whirlpool algorithm, which is constructed using a block cipher. A number of widely used cryptographic hash techniques are outlined below.

A. Message Digest (MD)

All message digest (MD) algorithms were devised by Ron Rivest. Attention-grabbing instances include MD2,

MD4, MD5. The MD2 algorithm is a hash function that was proposed in 1989. This algorithm processes message blocks of length 128 bits. The hash function has a moderate memory requirement. It produces a digest of the original message that has a length of 128 bits. Nonetheless, its shortcomings include pre-image vulnerabilities. In the year 1990 MD4 created to process message blocks at the operating mode of 512 bits to create 128 bits of hash output. Even though it is faster, it has weak collision resistance which makes finding collisions easier. MD5, a type of MD4, is a popular hashing algorithm. It additionally runs on 512-bit blocks and produces a message digest of 128-bits. Even though MD5 is vulnerable to collision and pre-image attacks and not recommended for use, a lot of people still use it as a checksum to verify that content has not changed.

B. Secure Hash Algorithms (SHA)

The secure hash algorithm, commonly referred to as the Secure Hash Standard (SHS), was designed by the National Institute of Standards and Technology (NIST) and formally released as part of the Federal Information Processing Standard under FIPS 180.

Version SHA-0 operates on 160-bit blocks and has a weak collision resistance, with collisions being readily achievable. Structured similarly to MD5, SHA-1 is another one of the advanced versions that produces 160-bit hashes.

SHA-2 represents a family of hashing algorithms, with SHA-256 and SHA-512 being the most widely used variants. In SHA-256, data is handled in 512-bit chunks to generate a 256-bit hash value, whereas SHA-512 works on 1024-bit blocks and produces a 512-bit output. Because known attacks typically operate on reduced or weaker variants, the complete hash functions are not subject to known attacks. Both the MD5 and SHA algorithms are derived from MD4. The attributes of MD and SHA can be compared in terms of block size, key length, cryptanalysis, number of iterations, total computation steps and so on.

SHA is typically regarded as more secure than MD5. Specifically, recovering the original message would require roughly (2^{160}) operations for SHA but

(2^{128}) for MD5. Also, the digest is longer 160 bits for SHA while it is only 128 bits for MD5. MD5 only requires 64 iterations, making it faster than SHA, which requires 80 iterations to compute a hash.

The resource requirements for padding and fingerprint generation are similar for both algorithms. For this reason, one can use SHA when security is a priority. And MD5 can be used whenever speed is more important.

C. Whirlpool

The compression mechanism in this context is derived from a block cipher. Unlike methods that operate on individual bits, a block cipher processes an entire block of data at once using a cryptographic key and algorithm, producing encrypted output.

The Whirlpool hash algorithm, created by incent Rijmen and Paulo Barret processes data in 512-bit segments and produces a 512-bit output digest. Owing ti its relatively large digest size compared to many other hashing methods, it offers a lower likelihood of hash collisions. Because its digest size is larger than that of many other hash algorithms, the probability of collisions is reduced. This larger output size also enhances its resistance to common cryptographic attacks, thereby providing an additional layer of security.

TABLE II. HOW THE CURRENT STUDY VARIES FROM PREVIOUS SYSTEMATIC REVIEWS

Title	Authors	Year	Findings
Survey System Using Blockchain for Scientific Research [14]	Salim Eray ÇELİK, Vildan Özkır	2021	This study uses SWOT analysis to compare blockchain-based survey systems with traditional centralized systems. It evaluates different blockchain models and concludes that blockchain provides improved anonymity, transparency, and security.
Blockchain Analysis of the Bitcoin Market [15]	Igor Makarov, Antoinette Schoar	2021	The study analyzes Bitcoin transaction records and ownership patterns, highlighting that exchanges account for about 75% of transactions, while other activities such as illegal transactions and mining rewards form a smaller portion.
Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey [16]	Naveed Ahmad et al.	2021	Provides a detailed overview of blockchain architecture and applications across multiple domains such as healthcare, banking, supply chain, and education, including different permission models.
Mining Process in Cryptocurrency Using Blockchain: Bitcoin a Case Study [17]	Ahmad Abdullah Aljabr, Avinash Sharma, Kailash Kumar	2019	Demonstrates secure and efficient transaction processing using blockchain, reducing fraud and eliminating the need for third-party intermediaries.
Economic Issues in Bitcoin Mining and Blockchain Research [18]	Shuai Wang et al.	2018	Introduces an ACP-based framework to analyze economic challenges in Bitcoin mining and blockchain ecosystems, supporting future research directions.
Bitcoin Mining: A Case Study [19]	Prashant Ankalkoti	2017	Explains Bitcoin mining as a decentralized process where miners validate transactions and are rewarded, highlighting its accessibility and global adoption.
Bitcoin: The Case Against Strict Regulation [20]	Michael Sherlock	2017	Emphasizes balanced regulation to maintain efficiency, low transaction costs, and strong security for users.

D. RIPEMD (RACE Integrity Primitives Evaluation Message Digest)

The RIPEMD family of cryptographic hash functions was developed by the COSIC research group at Katholieke Universiteit Leuven, drawing inspiration from the structure of the MD4 algorithm to achieve improved speed and security. RIPEMD-160, one of the most widely used variants, produces a hash digest of 160 bits (20 bytes).

E. BLAKE

The BLAKE hash function was proposed by Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C.W. Phan as part of the NIST hash function competition. It is based on the ChaCha stream cipher developed by Daniel J. Bernstein. In this approach, each round of the ChaCha algorithm involves XOR operations applied to duplicated tuples of the input block along with round constants, forming the basis of the hashing process.

V. Comparative Results

In this section, we evaluate the simulation result to analyze the efficiency of various cryptographic hash algorithms. SHA-1, SHA-2, SHA-256, and MD5. The algorithms would be compared on a few important parameters. We will see important parameters indicating the performance of the algorithms. The following comparison table shows how different members of hash function families perform with respect to these measures.

TABLE III.Analysis of Contrast in Results

Implementation	Frequency (MHz)	Throughput (Mbps)
SHA-1 [22]	42.9	119
SHA-2 [23]	218.2	1719
MD5 [24]	42.9	146
SHA-256 [25]	172.0	88064
SHA-512 [26]	133	1660

The operating frequency (in MHz), clock rate, and data throughpuy (in Mbps) for several widely used hash functions-such as SHA-512, SHA-256, MD5, SHA-1, and SHA-1 are presented in Table III. The table does not specify how often SHA-1 is used, but the chip runs at a clock frequency of 42.9 MHz and has a throughput of 119 Mbps. SHA-2 algorithm shows a clock rate of 218.2 MHz and a throughput of 1719 Mbps. The throughput is 146 Mbps and the clock speed for the MD5 algorithm is 42.9 MHz. The SHA-256 algorithm works with a clock speed of 172.0 MHz, while the throughput of the SHA-256 algorithm is 88064 Mbps which is more compared to the throughput of 1660 Mbps of SHA-512 which works with a clock speed of 133 MHz. Typically, when the implementation frequency and clock speed are high, it indicates that the hash algorithm is faster. However, throughput depends on implementation.

Fig. 4. Frequency comparison graph of different algorithms

Figure 4 is a bar graph showing the different frequency values (MHz) of the various cryptographic hash algorithms. Along the horizontal axis, the algorithms are represented, while along the vertical axis, the corresponding frequency values of the algorithms are represented in this graph. The SHA-2 algorithm achieves higher frequency values than other hash functions, as is obvious from the chart. The maximum frequency recorded is 218.2 MHz

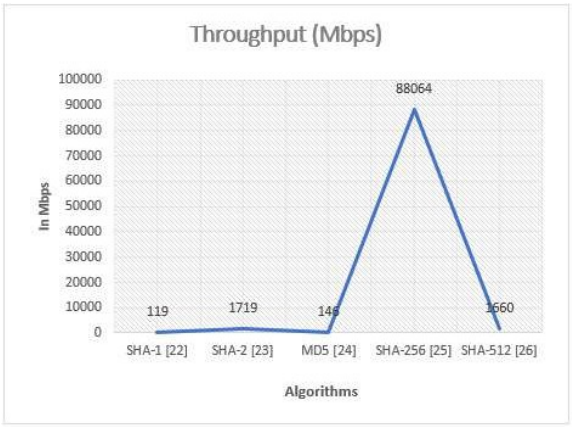


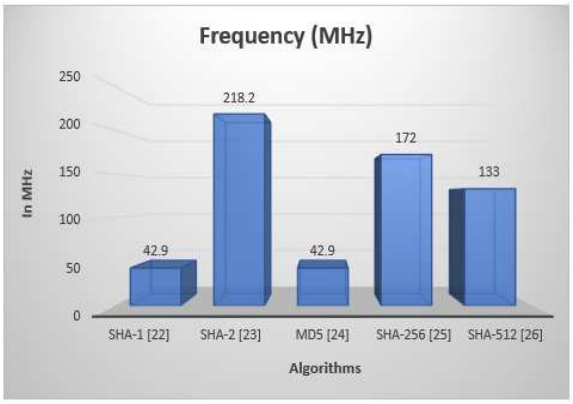
Fig. 5. Throughput comparison graph of different algorithms

The throughput of different cryptographic hash algorithms is compared in Figure 5. It offers a sense of their performance. Throughput refers to the amount of data processed by an algorithm in a given time period. For hash functions, this is usually measured in bits per second. The graph has throughput (Mbps) on Y axis and the various algorithms being compared on X axis. This comparison is a useful guide for choosing suitable hash algorithms for different applications. Based on my evaluation, SHA-256 has the highest throughput value of 88064 Mbps as compared to the other algorithms.

VI. Conclusion and Future Work

Blockchain security is primarily reliant on cryptographic hash algorithms. Through the generation of fixed-length hash values that are unique to each input, these algorithms facilitate the creation of tamper-proof digital ledgers, which are crucial for the functioning of blockchains. Research work on the development and improvement of hash algorithms is ongoing. Robustness and accuracy of hash algorithms directly influence the security of blockchain networks. Cryptographic hash algorithms such as SHA-512, SHA-256, MD5, SHA-2 and SHA-1 has analyzed in the blockchain security and compared. Choosing the best algorithm for a particular application is only possible with a good understanding of their characteristics and behaviour.

All of these hash algorithms performed well on metrics including frequency and throughput, while SHA-2 and especially SHA-256 perform better than the rest. Even with all these advances, hash algorithms resistant to quantum computing attack, scalability and energy consumption challenges need to be researched more as blockchain adoption continues to grow. As a whole, further development and fine-tuning of the cryptographic hash



algorithms to boost efficiency and security in a blockchain are a necessity.

References

[1] X. Y. Huaqun Guo, "A survey on blockchain technology and its security," sciencedirect, vol. 3, no. 2, 2022, doi: https://doi.org/10.1016/j.bcra.2022.100067.

[2] W. Chen, S. S. Zhiying Xu, and J. Z. Yang Zhao, "A Survey of Blockchain Applications in Different Domains," Int. Conf. blockchain Technol. Appl., 2018, doi: https://doi.org/10.1145/3301403.3301407.

[3] M. N. M. Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," IEEE Access, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[4] A. A. A. Ahmed G. Gad, Diana T. Mosa, Laith Abualigah, "Emerging Trends in Blockchain Technology and Applications: A Review and Outlook," sciencedirect, vol. 34, no. 9, pp. 6719–6742, 2022, doi: https://doi.org/10.1016/j.jksuci.2022.03.007.

[5] S. Ghimire and H. Selvaraj, "A survey on bitcoin cryptocurrency and its mining," 26th Int. Conf. Syst. Eng. ICSEng 2018 - Proc., no. December, 2019, doi: 10.1109/ICSENG.2018.8638208.

[6] M. Romiti, A. Judmayer, A. Zamyatin, and B. Haslhofer, "A Deep Dive into Bitcoin Mining Pools: An Empirical Analysis of Mining Shares," Res. Gate, no. June, 2019.

[7] A. H. Dyhrberg, S. Foley, and J. Svec, "How investible is Bitcoin? Analyzing the liquidity and transaction costs of Bitcoin markets," Econ. Lett., 2018, doi: 10.1016/j.econlet.2018.07.032.

[8] L. W. Cong and Z. He, "Blockchain Disruption and Smart Contracts," Review of Financial Studies. 2019, doi: 10.1093/rfs/hhz007.

[9] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," Bus. Horiz., 2019, doi: 10.1016/j.bushor.2019.01.009.

[10] L. Gundaboina et al., "Mining Cryptocurrency-Based Security Using Renewable Energy as Source," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/4808703.

[11] B. A. Jones, A. L. Goodkind, and R. P. Berrens, "Economic estimation of Bitcoin mining's climate damages demonstrates closer resemblance to digital crude than digital gold," Sci. Rep., vol. 12, no. 1, pp. 1–10, 2022, doi: 10.1038/s41598-022-18686-8.

[12] W. Sun, H. Jin, F. Jin, L. Kong, Y. Peng, and Z. Dai, "Spatial analysis of global Bitcoin mining," Sci. Rep., vol. 12, no. 1, pp. 1–12, 2022, doi:

10.1038/s41598-022-14987-0.

[13] S. L. Náñez Alonso, J. Jorge-vázquez, M. Á. Echarte Fernández, and R. F. Reier Forradellas, “Cryptocurrency mining from an economic and environmental perspective. Analysis of the most and least sustainable countries,” Energies, 2021, doi: 10.3390/en14144254.

[14] S. Eray and V. Özkır, “Survey System Using Blockchain for Scientific Research,” Quantrade J. Complex Syst. Soc. Sci., vol. 3, no. 2, pp. 45–67, 2021.

[15] I. Makarov and A. Schoar, “Blockchain Analysis of the Bitcoin Market,” SSRN Electron. J., 2021, doi: 10.2139/ssrn.3949206.

[16] S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, “Research and applied perspective to blockchain technology: A comprehensive survey,” Appl. Sci., 2021, doi: 10.3390/app11146252.

[17] A. A. Aljabr, A. Sharma, and K. Kumar, “Mining process in cryptocurrency using blockchain technology: Bitcoin as a case study,” J. Comput. Theor. Nanosci., 2019, doi: 10.1166/jctn.2019.8515.

[18] R. Qin, Y. Yuan, S. Wang, and F. Y. Wang, “Economic Issues in Bitcoin Mining and Blockchain Research,” 2018, doi: 10.1109/IVS.2018.8500377.

[19] P. Ankalkoti, “Bitcoin Mining : A Case Study,” pp. 1–5.

[20] M. Sherlock, “BitCoin: The Case against Strict Regulation,” Bank. Financ. Law Rev., 2017.

[21] W. Macharia, “Cryptographic Hash Functions,” 2021.

[22] S. Wanzhong, G. Hongpeng, H. Huilei, and D. Zibin, “Design and optimized implementation of the SHA-2(256, 384, 512) hash algorithms,” 2007, doi: 10.1109/ICASIC.2007.4415766.

[23] U. Malik, R. Shahid, M. Shahid, K. Rogawski, and K. Gaj, “Use of Embedded FPGA Resources in Implementations of Five Round Three SHA-3 Candidates,” 2011.

[24] L. V. T. Duong, N. T. T. Thuy, and L. D. Khai, “A fast approach for bitcoin blockchain cryptocurrency mining system,” Integration, 2020, doi: 10.1016/j.vlsi.2020.05.003.

[25] J. Fu, S. Qiao, Y. Huang, X. Si, B. Li, and C. Yuan, “A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA,” Secur. Commun. Networks, 2020, doi: 10.1155/2020/8876317.

[26] M. D. Rote, N. Vijendran, and D. Selvakumar, “High performance SHA-2 core using the Round Pipelined Technique,” 2016, doi: 10.1109/CONECCT.2015.7383912.