Applications of Cryptography in Blockchain

Saurya Pratap Singh and Ayush Pal
Pranveer Singh Institute of Technology, Kanpur

----------ABSTRACT----------

Blockchain is an innovative application model that integrates distributed data storage, peer-to-peer transmission, consensus mechanisms, digital encryption technology and other computer technologies. It is decentralized, secure, and Information disclosure. In blockchain, digital encryption technology has a core position. The security of user information and transaction data is a necessary condition for the promotion of blockchain. The development of cryptography and related technology promotes and restricts the further development of blockchain. This paper outlines the infrastructure of blockchain, including the data layer, network layer, consensus layer, contract layer and application layer. The principles of encryption technology are introduced briefly, such as hash function, asymmetric cryptosystem, and digital signature. The application of cryptography in all levels of blockchain is analyzed, including data layer, network layer, consensus layer, etc. It shows that cryptography runs through the whole blockchain system. The existing security problems of blockchain are analyzed, and the future research direction is expected.

Keywords:-**Blockchain, Hash, SHA-256, Cryptography, Encryption, Decryption**

I. INTRODUCTION

Security is an important requirement in protecting data against attacks. One of the most important methods for ensuring data security is cryptography. Cryptography is secret writing for data security protection. Cryptography protect data by changing plain text in to cipher text and this cipher text is decoded by only authorized receivers, who then convert the uncertain data into the original textual content. The two fundamental techniques for encrypting data are "symmetric cryptography"which generate the usage of the same key to encrypt/decode information and "asymmetric cryptography", which makes use of public and private keys to encrypt/decode information.

In blockchain we are now using an algorithm which is called SHA 256 for generating "hash number" SHA 256 is a cryptographic hash algorithm which does not use any key. So, there is no question of symmetric/asymmetric. In SHA 256 we give block no, nonce data of block and previous hash number as an input and output is our new hash number.

A. Common Terms Used in Cryptography & Blockchain:-

- ***Plain-text***: The original and understandable text. As an instance, let Alice need to transmit a "computer" message to Bob. Here, "computer" is the plaintext or the original message.
- ***Cipher-text***: The text that can't be understood by way of anybody or a gibberish text, example "E@$#£%"
- ***Encryption***: A process of changing plaintext into cipher text is called encryption. The manner of encipherment needs an encipherment algorithm and a key.
- ***Decryption***: A process of changing cipher text in to plain text is called decryption.
- **Key**: A key is character, number, or a special character. It is used at the time of decode on the ciphertext.

B. Purpose of cryptography in Blockchain

- ***Authentication***: The potential of a system to test the identity of new block in blockchain.
- ***Integrity***: Only real miner is allowed to add new block in blockchain.
- ***Access Control***: Only authorized miner is capable to get the reward of adding new block in blockchain.

In blockchain the block is attached by hash number and these hash number work like as linked list and generated by cryptography algorithm SHA 256, if somehow the hash is decodable then it is easy to hack a blockchain and add a duplicate block so that's why we are using a good cryptography algorithm for securing our hash.

II. ENCRYPTION ALGORITHMS WHICH ARE USED IN BLOCKCHAIN

This part clarifies numerous encryption algorithms to identify the best algorithm for blockchain on various parameters. Some common hashing algorithm includes MD5, SHA-1, SHA-2, SHA-256, and LANMAN.

a. ***MD5***: MD5 message-digest algorithm is the 5thversion of the message-Digest algorithm developed by Ron Rivest to produce a 128-bit message digest. MD5 is quite than other versions of the message digest, which the plaintext of 512-bit blocks, which is a set of four blocks, each of 32 bits. MD5 produce the message digest through five steps, i.e., padding, dividing length, dividing the input into 512-bit blocks, initial changing variable a process block and 4 rounds and using different constant in each of the iteration.

Use of MD5Algorithm

It was developed with the main motive of security as it takes an input of any size and produces an

output if a 128-bit hash value. To be considered cryptographically secure, MD5 should meet two requirements:

1.) It is impossible to generate two inputs that cannot produce the same hash function.
2.) It is impossible to generate a message having the same hash value.

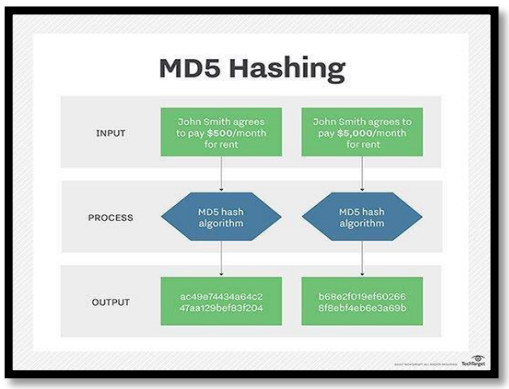

Fig.1. Showing MD5 hashing

b. ***SHA1***:- SHA1: SHA1 or SECURE HASH ALGORITHM 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. This hash value is known as a message digest. This message digest is usually then rendered as a hexadecimal number which is 40 digits long. It is a U.S. Federal Information Processing Standard and was designed by the United Sate National Security Agency.
SHA-1 is now considered insecure since 2005. Major tech giants browsers like Microsoft, Goggle, Apple and Mozilla have stopped accepting SHA-1 SSL certificates by 2017.[2]

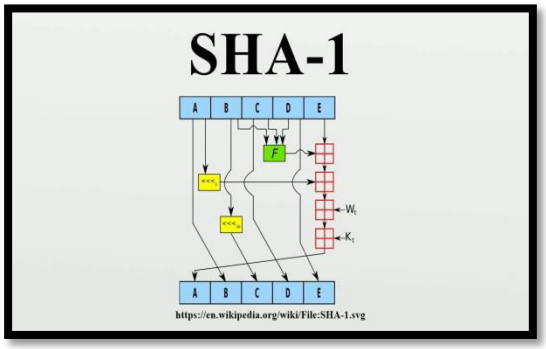

Fig. 2. Showing hashing procedure of SHA1

c. ***SHA2***:- Secure Hash Algorithm 2 is a set of cryptographic hash functions designed by the United States National Security agency and first published in 2001.SHA-2 hash six different variants, which differ in proportion with the bit size for encrypting data.

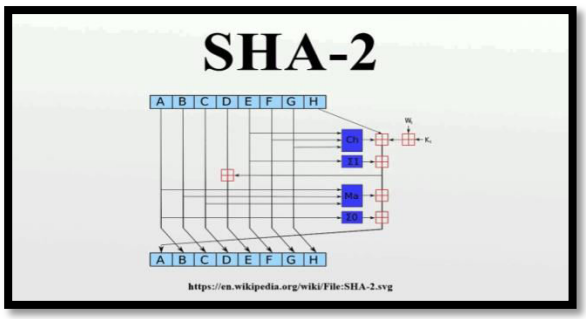

Fig. 3. Showing hashing procedure of SHA2

SHA-2 provide better prevention against collision, meaning the same input data always has a different hash value.SHA-2 uses from 64 to 80 rounds of cryptography operations, and it is commonly used to validate and sign digital certificates and documents.

d. ***SHA-256***:- The SHA-256 algorithm is one of the flavours of SHA-2 (Secure Hash Algorithm 2). SHA-256 is a patented cryptographic hash function that outputs a value that is 256 that is 256 bits long.

What is hashing? In encryption, data is transformed into a secure format that is unreadable unless the recipient hashes a key. In its encryption form, the data may be of unlimited size, often just as long as when unencrypted. In hashing, by contrast, data of arbitrary size is mapped to data of fixed size. For example, a 512-bit string of data would be transformed into a 256-bit string though SHA-256 hashing.

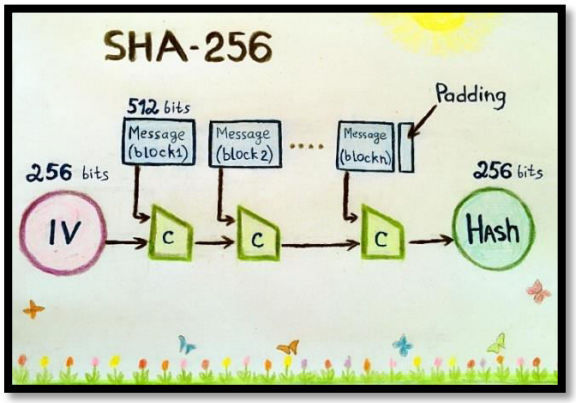

Fig. 4. Showing hashing procedure of SHA256

How secure is SHA-256?

SHA-256 is one of the most secure hashing functions on the market. That why we use it in blockchain. The US government requires its agency to protect certain sensitive information using SHA-256. Three properties make SHA-256 so secure.

1. It is almost impossible to reconstruct the initial data from the hash value. A brute force attack

would need to make 2^256 attempts to generate the initial data.

2. Having two messages with the same hash value (called a collision) is extremely unlikely. With A minor change to the original data alters the hash value so much that it's not apparent the new hash value is derived from similar data; this known as the avalanche effect.

3. LAN Manager Hash (LANMAN Hash): The LAN manager hash (LAMAN hash) is an encryption mechanism implemented my Microsoft prior to its release of NTLM. The LANMAN hash was advertised as a one-way hash that would allow end users to enter their credentials at a workstation, which would, in turn, encrypt said credentials via the LANMAN hash.
It turns out that the LANMAN hash is not true one-way hash. First, regardless of how the end user entered his password, the LANMAN hash would covert the characters into uppercase.

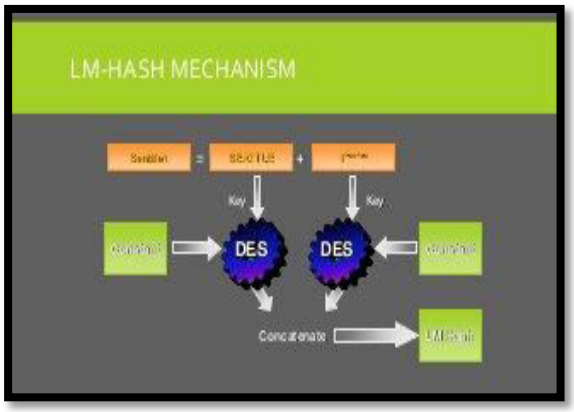

Fig. 5. Showing LM Hash mechanism

Now we know the fundamental of MD5 and SHA-2. Let's compare them. First of all, MD5 produce 128-bithashes. SHA-2 contains subversion that can produce hashes of different lengths. The most common is SHA-256. Secondly, the SHA-2 is more secure than MD5, especially in term of collision resistance. Therefore, the MD5 isn't recommended for Blockchain technology. Moreover, there are fewer reported attack on SHA-2 than onMD5. The MD5 is considered to be cryptographically broken and can be attacked by average computer. In term of speed, the MD5 is slightly faster than SHA-2. Therefore, the MD5 is often used as check sum for verifying files integrity.

III. COMPARISION OF THE HASHING ALGORITHMS

- *SHA-1 vs. SHA-2 vs. SHA-256*:-As we discussed, SHA is an acronym for Secure Hash Algorithm, so while SHA2 is the successor to SHA1, it's a completely different algorithm, or rather set of algorithms, not a variation on the original. SHA1 was developed by the US government and is closer in nature to MD5. It creates message digests, 160-bit (20-byte) hash values that are represented by 40-digit long hexadecimal strings. SHA2 was also developed by the US government, specifically the NSA, and is actually a family of algorithms, six different hash functions that produce digest/hash values of varying lengths: 224, 256, 384 or 512. "The variety of SHA-2hashes can lead to a bit of confusion, as websites and authors express them differently. If you see "SHA-2," "SHA-256" or "SHA-256bit," those names are referring to the same thing. If you see "SHA-224," "SHA-384," or"SHA-512," those are referring to the alternate bit-lengths of SHA-2. You may also see some sites being more explicit and writing out both the algorithm and bit-length, such as "SHA-2 384."[5][2]

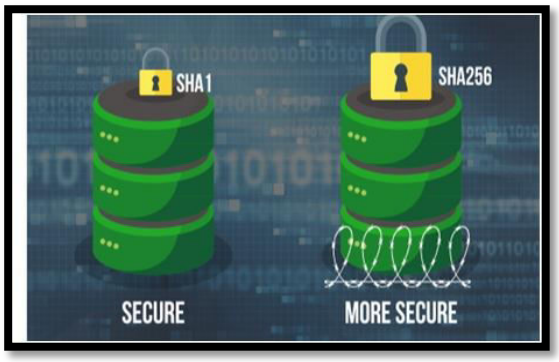

Fig. 6. Showing comparative security status

The basic difference betweenSHA1 vs. SHA256 or SHA1 vs. SHA2 is the length of the key used to encrypt the data transferred online. SHA1 uses 160-bitlong key to encrypt data while SHA256 uses 256-bit long key to encrypt data. SHA2 is a family of algorithms developed by the US government to secure the data online. SHA2 uses keys of varying lengths, including224, 256, 384, and 512 to encrypt the data. SHA512 uses a 512-bit key for the purpose of encryption [1][4].

- ***SHA vs. MD5***: Now we know the fundamental of MD5 and SHA-2. Let's compare them. First of all, MD5 produce 128-bithashes. SHA-2 contains subversion that can produce hashes of different lengths. The most common is SHA-256. Secondly, the SHA-2 is more secure than MD5, especially in term of collision resistance. Therefore, the MD5 isn't recommended for Blockchain technology. Moreover, there are fewer reported attack on SHA-2 than on MD5. The MD5 is considered to be cryptographically broken and can be attacked by average computer. In term of speed, the MD5 is slightly faster than SHA-2. Therefore, the MD5 is often used as check sum for verifying files integrity.[2]

IV. CONCLUSION

We discussed the MD5, SHA-1, SHA-2, SHA-256 algorithm in details and then we compared them the conclusion is that SHA-2 does better than MD5 in most cases, especially regarding security, that's why we use SHA-2 in place of MD5 but there is another advance version of SHA which is SHA-256and now this is very secure than other previous version, so start using it in our new technology Blockchain for producing hash number for blocks.

V. FUTURE SCOPE of SHA-256

So, based on the assumption that a supercomputer can manage 15 trillion sha256 hashes per second (roughly what the Bitcoin network itself can manage) it would take 65 billion years, assuming computing power stagnated at this very second. If you factor in Moore's Law, which can be used to measure the general increase in computing power over time, it would be roughly 60 years (though there is no guarantee that Moore's law will remain in act for 60years). The study of cryptography & allied areas is essential in the development of various security protocols [7-15], wireless communication scenarios [16-21] and plenty of network security related applications [22-26].

REFERENCES

[1] Johnson Brad and Gossels Jonathan. The ssl handshake,2001.http://www.system experts.com/tutors/The_SSL_Handshake_V1.5f.pdf .

[2] Jones Eastlake. US Secure Hash Algorithm 1 (SHA1), 2001. http://www.ietf. org/rfc/rfc3174.txt.

[3] University of Tours-France. Channel coding and error detection, 2001. http://www. rfai.li.univ-tours.fr/ramel/fr/codage_canal.pdf.

[4] RSA Laboratories. Rsa laboratories' frequently asked questions about today's cryptography, version 4.1, 2000. http://www.rsasecurity.com/rsalabs/faq/ 2-3-1.html

[5] Rivest Ron. RFC-1321 The MD5 Message-Digest Algorithm, 1992. http://www. ietf.org/rfc/rfc1321.txt.

[6] Ahmed, S., & Broek, N. t. (2017). Food supply: Blockchain could boost food security (brief article)

[7]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6,
DOI: 10.1680/jnaen.18.00006

[8]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451, DOI: 10.1080/09720529.2019.1692450

[9]. A. Chaturvedi, N. Srivastava, V. Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38,
DOI: 10.5120/ijca2015906060

[10]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9,
DOI: https://doi.org/10.1007/s11277-020-08008-4

[11]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720,
DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[12]. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5,
DOI: 10.1109/CICT48419.2019.9066168

[13]. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5,
DOI: 10.1109/UPCON.2018.8596905

[14]. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7,
DOI: 10.5120/cae2017652680

[15]. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6,
DOI: https://doi.org/10.48550/arXiv.2203.12606

[16]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86,
DOI: 10.1109/UPCON.2016.7894629

[17]. V. Shukla, A. Chaturvedi, N. Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21,
DOI: 10.5120/cae2015651903

[18]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39,
DOI: 10.5120/ijca2015906437

[19]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419,
DOI: 10.35940/ijrte.B1503.078219

[20]. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

[21]. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36,
DOI: 10.5120/cae2017652716

[22]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

[23]. V. Shukla, A. Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

[24]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI: https://doi.org/10.1080/09720529.2021.1932902

[25]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

[26]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI: https://doi.org/10.1080/09720529.2021.1932908