Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, November 2021: 8216-8221

Methodization of Block Chain Cryptography Facts

Parul[1]
Research scholar
Baba MastnathUniversity, Rohtak
dparul79@gmail.com

Deepak Kumar[2]
Assistant Professor
Department of Computer Science,
Government college, Panchkula
dks.karnal@gmail.com

Dr .Pooja Vyas[3]
Assistant Professor
Department of management
Indira Gandhi University, Meerpur, Rewari, Haryana
pooja.vyas9@gmail.com

Abstract:

One of the disruptive technology is blackchainwhaich has verios applications in businesses. Cryptography is the basic of blockchain which provide dependable and protected reorganised solutions. Blockchain have multiple uses in different areas like medical, finance, enterprises, laws, internet of things, cyber security, construction of infrastructure which are studied broadly, but very limited research has been done in cryptography area. According to the litreture survey we have done there is no systematization of knowledge which properly elaborate the existing cryptographic concepts in blockchain and give idea about the future potential. This paper shows copmaparative analysis of already available cryptographic concepts which are used in blockchain. However there is lack of information and exact framework used to check viability of it like other plateforms to identify the blockages and improve the uses and plateforms. At the end we give suggestions for future scope and recommend a list different cryptographic concepts which have more versatile solutions in the area of blockchain applications problems and its solutions.

Keywords: Blockchain, cryptography, finance, framework.

I INTRODUCTION

The Fundamental core technology in Bitcoin is blockchain. It is a distributed ledger maintaining a continuously growing list of data records that are confirmed by all of the participating nodes. The data is verified in this public ledger in a form of blocks of valid transactions, and this public ledger is shared and available to all nodes. It is a powerful technology and also it faces so many research challenges. The main challenges is security and privacy, key management, scalability, analysis of new attacks, smart contract

management, and incremental introduction of new cryptographic features in existing blockchains. These challenges are available due to the network structure and the underlying consensus mechanisms and cryptographic schemes used within the blockchains. In this there are so many cryptographic concepts used such as signature schemes, zero- knowledge proofs, and commitment protocols. In order to improve the solutions in block chain , they have to find a new cryptographic concepts in research field. The majority of the ongoing research in Blockchain focuses on finding and identifying improvements to the current processes and routines, mostly in industries that rely on intermediaries, including banking, finance, real estate, insurance, legal system procedures, and healthcare. These blockchain enabled applications still need a proper way for choosing the cryptographic technique employed in their respective solution in order to meet the business requirements.This is the first systematization of knowledge that gives a complete picture of the existing cryptographic concepts related to blockchain. We have tried to depict most of the cryptographic concepts in the blockchain domain. Although there are various works about specific cryptographic concepts used in blockchain, there are only few works which merge all these atomic works and present them in a single paper. A recent work of Wang et al. [7] gives a comprehensive analysis of cryptographic primitives in blockchain. Their analysis presents the functionality and the usage of these primitives in blockchain. However, the study is based only on existing cryptocurrencies and it lacks many of the cryptographic protocols which are used in blockchain.

II.RELATED WORKS:

Nakamoto defined that build up a peer-to-peer decentralized electronic cash system called Bitcoin without any credit basis in 2008 [7], which has been proved to be stable but inefficient . In 2013, Vitalik et al. discussed that Ethereum [1], which has big progress compared with the Bitcoinblockchain. Ethereum has a turing-complete virtual machine to execute smart contracts. In 2015, IBM developed Fabric, executing smart contracts (chain cypher) in the docker [6]. In 2016, Onchain developed Antshareblockchain, using smart contracts to record the transferring of the digital asset. Antshareblockchain is reputed to handle 10,000 transactions per second. Qtum presented a smart-contract framework that aims for sociotechnical application suitability [10]. Different blockchain systems use different consensus protocols, code execution engines, and so on. Vukolic compares the execution efficiency of different consensus protocol including PoS and Pow [12]Idelberger et al. proposed logic-based smart contracts for blockchain systems [5]. Blockchain-based smart contracts have a wide range of applications. McCorry et al. proposed an open board voting system which maximizes the privacy of the voters [6].

Reema Gupta et al proposed “Efficient Encryption Techniques in Cryptography Better Security Enhancement”. They proposed a study of Encryption techniques and discussed with their limitations and procedure. Huffman coding and B2G, G2B is used for encryption. They also discussed various transpositional techniques like Simple columnar, simple row, Route cipher, transposition [8]. Abhishek Joshi et al proposed “An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks” They proposed an efficient cryptographic scheme for text message Protection against Brute force and Cryptanalytic attacks. They show that this technique can also be used for most crucial applications where it requires a significant security of transmitted message and also there is no overhead on the transfer of message and the key when it is used with our proposed technique [9]. Ashraf Odeh et al “A Performance Evaluation of Common Encryption Techniques with Secure Watermark System (SWS)”. They demonstrate a fair comparison between the most common algorithms and with a novel method called Secured Watermark System (SWS) in data encryption field according to CPU time, packet size and power

consumption. They provide a comparison the most known algorithms used in encryption: AES (Rijndael), DES, Blowfish, and Secured Watermark System (SWS). They apply the same methodology on images and audio data [10]. Sushil Kumar Tripathi "An Efficient Block Cipher Encryption Technique Based on Cubical Method and Improved Key". They presented an efficient block cipher encryption technique based on improved key. Proposed EES method is based on block level symmetric encryption. The proposed EES method is based on improve cubes. They used a pair of binary inputs are contains by each cell. The Cube can able to provide a various number of combinations. The proposed EES algorithm, performed a series of bit transformations, by using of S-BOX, operation XOR, and operation AND [11].

III.BLOCK CHAIN AND ITS ARCHITECTURE:

The blockchain data structure is an ordered, back-linked list of blocks of transactions. Each and every block referred as a previous block, known as the parent block, through the "previous block hash" field in the block header. Each block comprises the hash of its parent inside its own header. It is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.There are four main types of blockchain networks: public blockchains, private blockchains, consortium blockchains and hybrid blockchains.

Four main types of block chain technology

	Public	Private	Hybrid	Consortium
Advantages	*Independence *Transparency *Trust	*Access control * Performance	*Access control * Performance *Scalability	*Access control *Scalability *Security
Disadvantages	*Performance *Scalability *Security	*Trust *Auditability	*Transparency *Upgrading	*Transparency
Use cases	*Cryptocurrency *Document validation	*Supply chain *Assetownersip	*Medical Records *Real estate	Research *Banking *Supply chain

It is a way to capture transactions in the form of blocks where blocks are linked through the cryptographic hash, hence forming a chain of blocks. Figure 1 shows the basic blockchain structure. Each block in the blockchain contains a block header and a representation of the transaction. For example, in Figure 1, each block consists of its hash, the hash of the previous block, a timestamp and some other block fields (e.g., version, nonce). This depends from the block design. Merkle root hash represents the set of transactions in the Merkle tree, and this representation of transactions varies according to the design of the blockchain implementation.

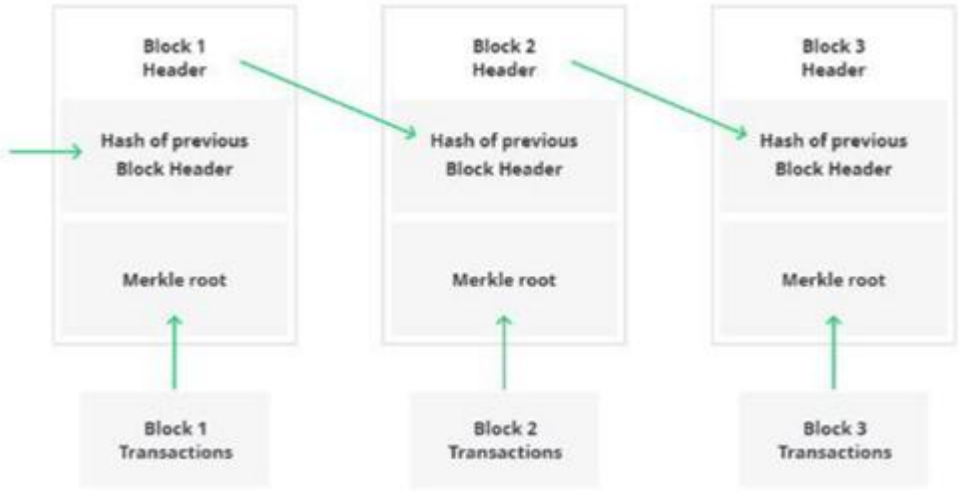

Figure 1: Basic Block chain Structure.

IV.PROPOSED FRAME WORK:

(i)**CRYPTOGRAPHIC HASH FUNCTION:**

A hash function H is a function which takes an input of an arbitrary size and maps it to a fixed size output. Cryptographic hash functions have some extra properties such as:

a) collision resistance - it is hard to find two inputs a and b such that H(a) = H(b);

b) preimage resistance - for a given output y it is hard to find an input a such that H(a) = y; and

c) second preimage resistance - for a given input a and output y = H(a) it is difficult to find a second input b such that H(b) = y. Cryptographic hash functions in blockchain are used for various purposes such as:

1) solving cryptographic puzzles (the Proof of Work (PoW) in Bitcoin [1]);

2) address generation (for public and private keys);

3) shortening the size of the public addresses;

4) message digests in signatures.

The most popular cryptographic hash functions used in blockchains are SHA-2 [19] (especially the variant SHA256 - a variant that produces outputs of 256 bits), and some of the well analysed hash functions from the NIST SHA-3 competition and standardization. A characteristic way how cryptographic hash functions are used in blockchain designs is in a form of a mode of operation, i.e., a grouping of several requests of a same or different hash functions. For example, in Bitcoin [1], SHA256 is used twice and that creation is called SHA256d, i.e., SHA256d(message) = SHA256(SHA256(message)). (1)

In this Phase the main thing is to provide the data security in toll gate. Here it is better to provide the data for security with the help of rfid tag and then include the cryptographic functions such as encryption and decryption by using different algorithms. After securing the data, then the process is ready to send to the database with the help of block chain technology. In this technology, the blocks are combined with the next block and also the previous hash function is to be the next hash function for the block header. For example, if the last record will be deleted or any changes will be hacked by the hackers in the database. If

any small changes will be noted, the block header will give the wrong output for the whole database. It easily validates the hash functions of the datas stored in to the database.
The performance comparison was provided based on different file size, key size, file type, encryption time and decryption time. The encryption time is measured by the start and the end time of the encryption process. We processed each file 100 times and measured the average execution time to have a better result. It was detected that the execution time increased linearly due to the increase of packet size. The experiment was carried out by varying different key sizes for different algorithms. In most cases, the execution time was increasing due to the increase in key size. Decryption time is considered as well for the performance comparison. It is measured by the decryption algorithm execution start and stop time.

VI CONCLUSION:

To identify the different research problems and directions their main gaol is to propose a systematic study of cryptographic concepts.There are so many research challenges and problems raised in block chain the cryptographers can choose the particular domainfor particular area, They can easily enabled the solutions of blockchain in the current transitions. Academic and industrial research is focused on making blockchain cost efficient in terms of computational power, memory requirements and security. Many existing cryptographic concepts have been embraced for blockchain use. This paper systematizes the current state-of-the-art knowledge of existing cryptographic concepts used in the blockchain. It also gives a brief description of the used cryptographic concept and points to the available blockchain models that are using that concept. The paper also identifies some concepts which have not yet been used in blockchain but can be beneficial if applied in the blockchain. Apart from existing cryptographic concepts, the paper also presents the basic building blocks of blockchain and how these building blocks are dependent on each other.

REFERENCES:

1. VitalikButerin et al. 2013. Ethereum white paper. (2013).
2. Christian Cachin. 2016. Architecture of the Hyperledgerblockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers\
3. Patrick Dai, Neil Mahi, Jordan Earls, and Alex Norta. 2017. Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform. (2017).
4. Christian Decker and Roger Wattenhofer. 2013. Information propagation in the bitcoin network. In International Conference on Peer-to-Peer Computing (P2P). IEEE, 1–10.
5. Florian Idelberger, Guido Governatori, RégisRiveret, and Giovanni Sartor. 2016. Evaluation of logic-based smart contracts for blockchain systems. In International Symposium on Rules and Rule Markup Languages for the Semantic Web. Springer, 167–183.
6. Patrick McCorry, Siamak F Shahandashti, and FengHao. 2017. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. IACR Cryptology ePrint Archive (2017), 110.
7. Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).
8. Marko Vukolić. 2015. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International Workshop on Open Problems in Network Security. Springer, 112–125
9. Reema Gupta “Efficient Encryption Techniques In Cryptography Better Security Enhancement” Volume 4, Issue 5, May 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.comAvailable:https://www.ijarcsse.com/docs/papers/Volume_4/5_May2014/V4I5-0450.pdf
10. Abhishek Joshi a*, Mohammad Wazid b, R. H. Goudarc “An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks” Available online at www.sciencedirect.comInternational Conference on Intelligent Computing, Communication& Convergence (ICCC-2014) Conference Organized by Inter science Institute of Management and Technology,

Bhubaneswar, Odisha, India Available:
http://www.science direct.com/science/article/pii/S1877050915007036

11. Ashraf Odeh, ShadiR.Masadeh, Ahmad Azzazi "A Performance Evaluation of Common Encryption Techniques with Secure Watermark System (SWS)" International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015. Available: http://a irccse.org /journal/ nsa/7315nsa03.pdf
12. Sushil Kumar Tripathi "An Efficient Block Cipher Encryption Technique Based on Cubical Method and Improved Key" Imperial Journal of Interdisciplinary Research (IJIR)Vol2, Issue-6, 2016ISSN: 2454-1362, Available: http://www. Imperia ljournals.com/index.php/IJIR/article/view/836