TEST Engineering & Management

July -August 2020
ISSN: 0193-4120 Page No. 6610-6618
.

A Deep Research on Application Level of Cryptography

Peddi Sai Pankaj[1],Rohit Yasashwi Bonthalakoti[2]

[1]Research Scholar , Department of Computer Science and Engineering,
Gandhi Institute of Technology and Management (GITAM), Visakhapatnam
[2]Research Scholar, Department of Computer Science and Engineering,
Gandhi Institute of Technology and Management (GITAM), Visakhapatnam

E-mail: peddi.pankaj@gmail.com, yasashwirohit@gmail.com

Article Info
Volume 83
Page Number: 6610-6618
Publication Issue:
July -August 2020

Article History
Article Received: *25 April 2020*
Revised: 29 May 2020
Accepted: 20 June 2020
Publication: *10 August 2020*

Abstract:
Block chain is a creative and operational model that can incorporate distributed data preserve, P2P (peer to peer) broadcast, concurrence models, digital encryption infrastructure and various computational components. Block chain is decentralized, information disclosure with secure outbound. In block chain digital encryption has a root level. The secured user's data/information and data transaction is a mandatory attribute for the main block chain promotion. The implementation of cryptography framework restricts and supports for future development of block chain. This research's ground plan is the block chain's infrastructure and building frameworks, with inclusion of all layers (application, contract, consensus and network). The fundamentals of encryption model is introduced in short like digital signature, hash model, asymmetric cryptosystem. The analysis is done in all applications of cryptography of block chain with all the layers (application, contract, consensus and network). This research reveals that cryptography runs over all the layers of block chain infrastructure. The available security issues of block chain are even analyzed and further research path is expected.

Keywords*:consensus, security, peer concurrence, cryptography, digital signature*

1. INTRODUCTION

Blockchain is decentralized and distributed database with the features non-tamperable, highly secured with reliable features. It incorporates Pear to peer (P2P) protocol, digitally encrypted model, smart contract, consensus infrastructure and more together. Leaving the service (maintenance mode of the existing root node and adopting the flow of collaborative maintenance with multiple uses to notice the data monitoring between multiple unknown parties, so protecting the trustworthiness and coherence of the information. The blockchain policy can be classified into private, public and alliance chains. Entire nodes in public chain can include or can withdraw on their own; but the private chain strictly moderates the selection of participating nodes; the alliance chain is collaboratively monitored and controlled with various participating firms. Bitcoin was introduced by Nakamoto in 2008[1], which was ultimately as successful case study of digital currency, and moreover this highly typical implementation of blockchain. Addition to this blockchain extended its standalone implementation value with many parameters and has shown its capability to change the society.

As an indicative of distributed and decentralized database, blockchain preserves all user's transactional details on the blockchain, which has huge needs for the security purposes and performance of blockchain. Blockchain is a P2P(peer to peer

July -August 2020
ISSN: 0193-4120 Page No. 6610-6618
.

network) with a decentralized infrastructure. There is no trust among the nodes and they won't trust each other and also no controlling (central) node. So, transactions with blockchain also required to make sure that secrets of transactional data and over unsecured channels and to manage the integrity of transactions. It's totally clear that cryptography engaged with most central place in the blockchain. In blockchain data consistency, protection of user's private data and transaction information [2] will be protected by cryptography. This research work is in brief Introduces the following cryptographic models:

1. Hash algorithms
2. Cryptographic techniques
3. Asymmetric encryption algorithm
4. Digital signature
5. Blockchain infrastructure
6. Bitcoin address
7. Digital currency trading

Other than above this work is extending how the cryptography model protects transactional details and privacy in blockchain in depth.

2. BLOCKCHAIN INFRASTRUCTURES:

As stated by Melanie Swan who is the founder of the blockchain science institute, blockchain has accomplished two difference phases:

1. Blockchain1.0(multi technology portfolio novelty indicated by bitcoin)
2. Blockchain2.0(transferred by digital assets indicated by Etherenum)

Classic applications of blockchain fundamentally incorporates following attributes:

1. Bitcoin
2. Etherenum
3. Hyperledgers

Altogether the developments are different but many similarities in overall infrastructure. As shown in below Table 1, blockchain can be divided into five layers:

1. Network layer
2. Consensus layer
3. Data layer
4. Contract layer
5. Application layer

Table1: Block chain structure

Layers	Bitcoin	Ethereum	Hyper ledger
Application layer	Bitcoin trading	Ethereum trading	Enterprise blockchain
Network layer	TCP-based P2P	TCP-based P2P	HTTP/2-based P2P
Contract layer	Script	Solidity/Script EVM	Go/Java Docker
Consensus layer	PoW	PoW/PoS	PBFT/SBFT
Data layer	Merkle tree	Merkle patricia tree	Merkle Bocket tree

The data layer block wise data structure to make sure that the integrity of storage. Every individual node in the network summarizes the data transactions received with the slot of time into a time stamped block and relates the block to current lengthy main blockchain for data storage. This layer implicates the main approaches of time stamp, hash algorithm, chain structure, block storage, Merkle tree etc.

July -August 2020
ISSN: 0193-4120 Page No. 6610-6618
.

The consensus layer integrates a consensus operation, which activates individual node to reach consensus on the expired time of block data in decentralized process [2]. The consensus operation mainly has pow, PoS, PBFT and SBFT. The intelligent contract is mainly incorporated in contract layer is fundamental programmable feature of blockchain. The digitalized program snippet which can automatically runs the contract terms preserved in blockchain in the mode of code and data sets. Intelligent contracts, operated by time or triggers, are executed by nodes in distributed ways. All related terms are coded with basically settled and initiated by digital signatures or other exterior data messages. The network layer incorporates various data broadcasting protocols and verification techniques. The blockchain is classical Peer to peer network. All nodes are connected with a planar topology without central nodes. Any node can leave the network at any moment of time and any two nodes can be freely connected. The P2P network protocol mainly used for broadcasting of data among nodes. The application layer incorporates Hyperledger and Etherenum etc. The principle policy of bitcoin is for digital currency transactions. Etherenum adds decentralized implementations on the basis of digital currency. And Hyperledger will not digital transactions basically with enterprise modes of blockchain implementations.

Hash and block structure:

The hash model is a task which maps a sequential messages of variable (any) length to a small fixed length value and identified by more sensitivity [3] , single direction and collision resistance. Basically Hash used to make sure the data integrity, which is to confirm the information has been illegitimate tampered with. While data under screening for changes, its hash value reflects accordingly. So, even if data is in unsafe boundaries, the integrity of data can be identified on the basis of hash value of data.

SHA is a kind of cryptographic model of hash function delivered by National Institute of Standards and Technology (NIST) with common features of cryptographic hash function. The SHA256 approach is a subset of SHA-2 cluster,

Which will generate generally 256-bit message dissolve. The algorithm's computational flow includes 2 stages: **Main loop and Preprocessing of message**. In the main loop phase, individual message block is handled by compression application, and result of last compression application is the hash value of the actual message. In preprocessing of message stage message length filled up , binary bit filled up will be handled over the information of any scale of length, and the resultant message will be divided into various 512-bit blocks.

RIEPEMD, a brief of RACE actual integrity inspection message, is a hash application approach implemented by the COSI R&D team of Leuven university of Belgium. RIPEMD-160 is the replacement and common version to RIPEMD[5]. As the SHA sequence applications, the fundamental step of approach is the complement of message, and the method of complement is similar to SHA sequence approach.

The basic process of algorithm is compression application, which is a recursive iterative loop, where individual loop contains 16 steps of applications. With various actual logic applications in individual loop, the handling of the application is splits

Into two separate cases, with 5 of two actual logic applications which are running with reverse order. Since entire 512-bit packets handing is finished, the end resulting of 160-bit result is the main hash value of the actual message.

For blockchain, hash applications are to process block's integrity and transaction check. In blockchain, the hash value of the data of previous block is preserved in each block's header, and user can validate the generated hash value with preserved hash value. This reveals the information of integrity of the previous block which is identified. Apart from this flow hash

July -August 2020
ISSN: 0193-4120 Page No. 6610-6618

application can generated private and public key pairs.

The hash pointer is structural data which carries, also with regular pointers, some information and secret passwords will be hashed linked with the information. A common pointer is to fetch information, and hash pointer is to checks that the data has been tampered [6]. Below shown in figure1, blockchain is a collection of listed hash pointers, each pointer which is connected with hash value. It is checked based on the hash value that data contains in the block is with changes, and make sure the Block information's integrity.

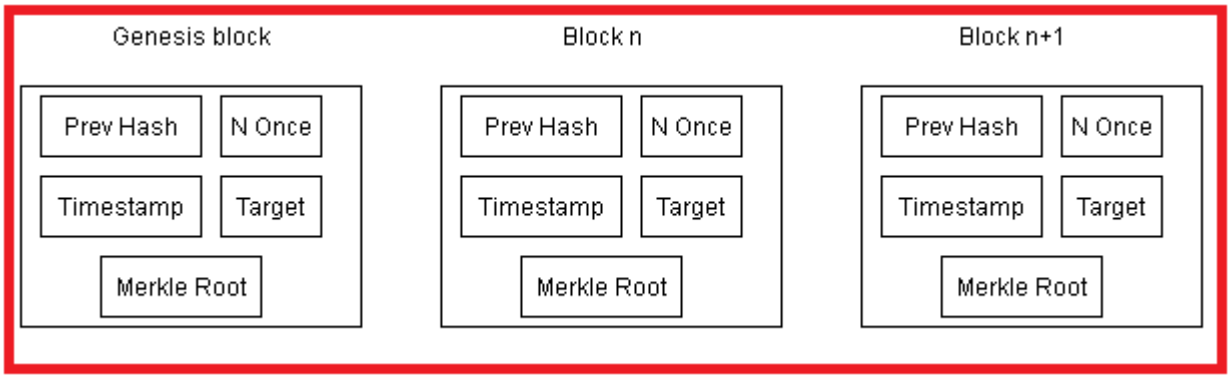

Figure1: Structure of block chain

Block chain's blocks holds all the data of entire network, mainly with block header which is framed as metadata and body of block with all transactional data [7]. The header integrates the previous block's has, the current block difficult target, and also current block's result of random numerical value, Merkle root and timestamp. The block accommodates a series of transactions to store the transaction data.

Previous Hash: The block is a segmented key of blockchain. This field is previous block's hash value of data information, and all blocks over the chain connected with sequential chain. This results the lengthy original chain from the making of block is Established at end. Individual block is not only contains previous block's location information, but also can have integrity check of the existing in current block based on the previous connected block hash value.

Nonce: Each block' header information contains random integer number with starting value as "0". The node which is running bitcoin mining code regularly performs SHA256 algorithm over the entire data of the block. When SHA256 value generated by current random number first it will not meet requirements, then with incremental of one unit of random number and SHA256 algorithm will be continued further. Till SHA256 value is less than the current block's SHA256 value, new block is framed and P2P networks connects that block for acceptance. So the process of new block generation is mainly information block generation which is of "Proof of **Work**".

Timestamp: The blockchain technology needs, that node should have a timestamp in current block header which specifies the framed time of block data. The main chain's blocks are organized in consecutive order. The timestamp is a solid proof of the existence of block, supports to frame a blockchain database which cannot be forged or tamper able.

Target: The target is create the computing capability of the whole network aggregately the difficulty situation needed to generate a complete block for every 10minutes slot. The target is planned automatically by blockchain network based on the outcomes of previous 2 weeks. The target is resolved by SHA256 value in the current block. This SHA256

July -August 2020
ISSN: 0193-4120 Page No. 6610-6618

value is the main control block has to dropped in the range of controllable target to change (decrease or increase) the target.

Merkle Root: The Merkle tree is binary structured format with hash function to verify the integrity of huge data instantly. As shown below in figure2 this tree generally incorporates with transactional database for all the blocks, the block header's root hash and all branches block(s) data to underlying with block header, finally it will be framed with tree structure. SHA256 hash function is will be used by bitcoin, to pass 2 SHA256 has applications on main data of exact length, 256-bit binary digitsfor unified recognition and storage.

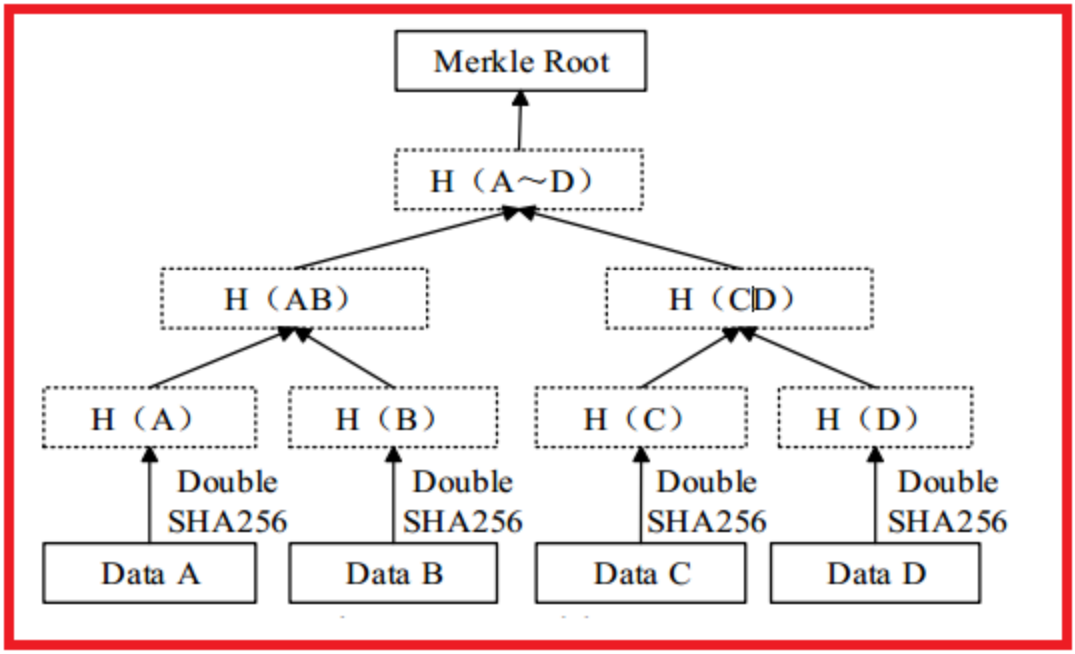

Figure 2: Merkle tree

Transaction list: This list contains more details of transaction records, encapsulating the time of each transaction, unique number of transaction, amount of bitcoin, payer and other related information. In data block, individual bitcoin is marked and received altogether, so individual bitcoin can be detected.

Bitcoin and public key structure: The basic features of cryptography are symmetric and asymmetric encryption. Mainly asymmetric encryption called as public key encryption, which can resolve the issue of instant distribution of symmetric encryption. In asymmetric encryption algorithm, the decryption and encryption keys are different they called as private and public key, respectively. The random number approach will be used to generate the private key, irreversible approach is used to generate and calculate the public key. The main advantage of asymmetric encryption is that we can have separate private and public keys, which can be broadcast over unsecured resources. But asymmetric encryption is with low processing speed and very less encryption capability, and it is mandatory to make sure the security for this asymmetric encryption application based on computational (mathematical) issues.

Elliptic Curves cryptography is most commonly used cryptographic technique in public key encryption models. The difficulty of elliptic curve discrete approach issue[8] is main aspect for security. The secp256k1 in elliptic curve is the algorithm used in public key encryption.Secp256k1 depends on elliptic curve over limited field. Due to its unique construction, its effective implementation can attain 30% of

July -August 2020
ISSN: 0193-4120 Page No. 6610-6618

enhancement over other curves. Possibility of backdoors can be effectively avoided by the constant of secp256k1.

The key pair in bitcoin application contains unique public key derived from the private key. The key pair is framed from the public key encryption. In the deposit link of transaction, the recipient's address by public key, which is bitcoin address, called as payee [9]. As shown in below figure 3, the private key is numeric value, generally random selection, and the public key is generated with private key encryption by multiplication of elliptic curve. Single entry encryption hash function is used to frame the bitcoin address via public key.

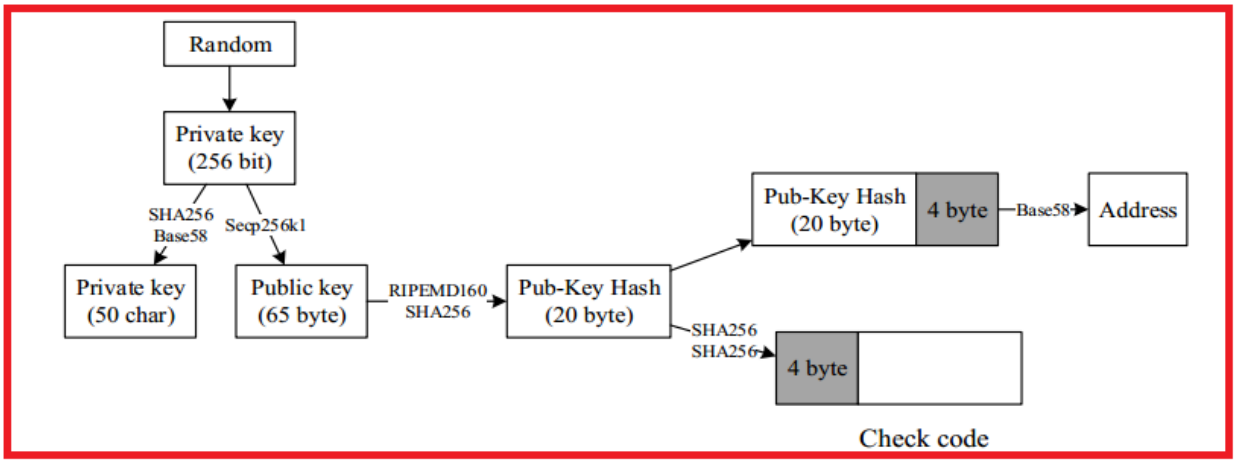

Figure 3: bitcoin address generation flow

Bitcoin selects the private key in the scale 1 to 2(256) and it is mandatory to make sure that selected result is not repeatable and unpredictable. Bitcoin system uses random number generator of the OS (operating system) to generate 256 bits random number as the private key, and it multiplies the generated random key (k) by the specified generation point G over the curve to generate neighboring point on curve. I.e. the equivalent public key K. The elliptic curve depends on discrete approach. The relation among k and K is standard, but with single operation i.e. K is framed from k, and k is difficult to framed from K. The framing of currency addresses uses different approaches on different programs.

Bitcoin uses SHA256 and RIPEMD160 multiple hashes to acquire bitcoin address; Ethereum uses Keccak256 approach to frame Ethrereum address [10]. In bitcoin public key K is the input, and from that SHA256 hash value calculated. Repeated calculation of RIPEMID160 hash value to obtain 160-bit number as public key hash. At the end , the public key hash is Base58 encoded format used to frame a bitcoin address. Base58 is most popular to use in encoded format, it's not only for bitcoin, but also for various crypto currencies, which merges powerful compression, easily readable, fast in error diagnosis. An error check code (4-byte) will be added to encode the data for efficient check for errors in transcription. Bitcoin uses Base58 inspect in Base58 encoding.

Digital signature and currency trade:

Digital signature generally contains two parts as algorithms:

1. **Signature**
2. **Verification**

Signature algorithm generates a digital signature over message, generally signature

controlled by signature key, this signature key is kept as secret and will be controlled by signer (signature creator). Verification algorithm is to monitor the digital signature of message, and the message can be confirmed according to signature more effectively. Verification algorithm will be controlled by verification key, but this algorithm and verification key are public, so it is easy to verify the signature by any person.

In cryptocurrency model in which blockchain is underlying model, the owner of digital currency hashes the data of the previous transaction's order of digital currency and address of next owner. The data signed with its internal private key is added at end of the transaction sequential list and sent to receiver. The receiver has to verify the received information to show the information of previous owner, and then checks with the owner of transaction. Individual transaction in blockchain saves the previous, current and next owner of the currency. So the entire process of currency can tracked back, efficiently avoiding repayment, wrong transactions and other exiting issues [11].

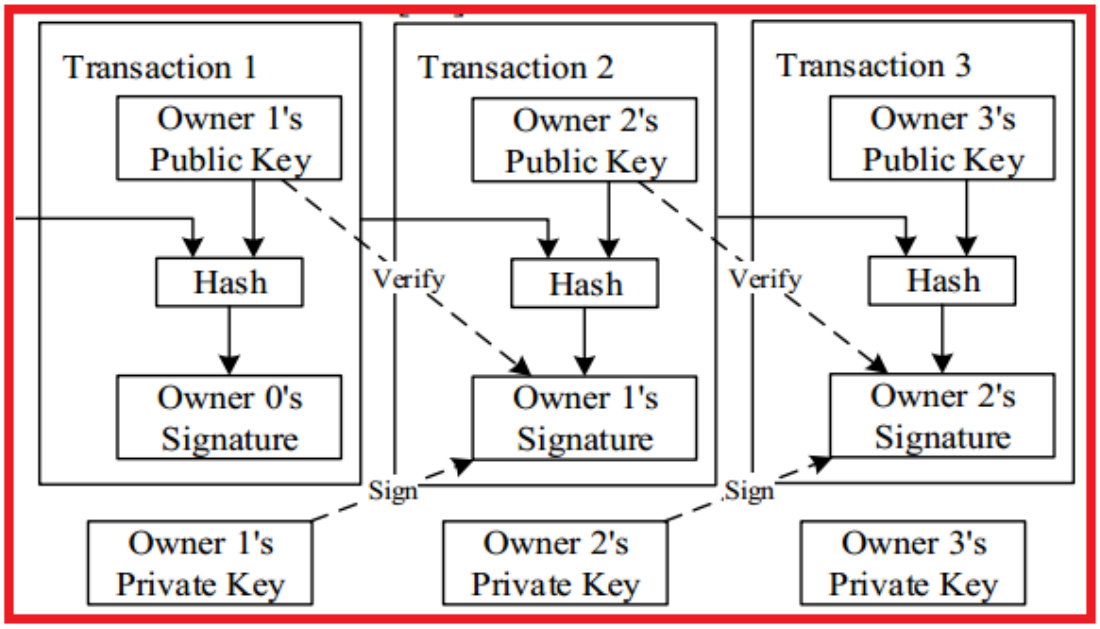

Figure 4: Signing and verification of transaction

As mentioned in figure 4, user2 doing payment transaction to user3 .When user 2 needs to transact n bitcoins to user 3, the source and amount of initially digitally noted on transaction slip. The n bitcoins of user 2 from the user 1, to completethe entire payment transaction of the user 2 to user 3, it is mandatory to record source of bitcoin, the digital signature and amountfor transaction of the user 2.

The authentication of transaction action, the signature is primarily completed by the payer. The payer of the transaction initially hashes the transacted data information of past transaction to get its hash value. The payer encrypts the hash with its own private key. The encrypted information is sent to receiver at the same time as the signature of previous transacted message and data. After getting the information, the recipient will check for the legality of the transaction and utilize same hash functionas the past step to generate entire hash summary from the received transacted data. Finally payer's public key is to decrypt theadded signature of past step to get another hash value. By tracing two summaries, the expiry of order can be ensured. If the 2contents are similar, the receiver can confirm about order is valid or not.

July -August 2020
ISSN: 0193-4120 Page No. 6610-6618
.

Blockchain consensus operation: The consensus operation is to identify the nodes in blockchain network and used to finalize transaction information, thereby makes sure of each block's consistency. The old bitcoin used Proof of work operation. This operation depends fully on node computational capability to make sure the moderated accountable mode for bitcoin network for distributed model. The Proof of work operation depends on computational capability among nodes to make sure the security and consistency of whole block chain's network data. Individual node needs to depend on capability to resolve the SHA256 computational issue, i.e. to identify valid and suitable random number Nonce, so that actual SHA256 hash numerical value of the block header's actual data is smaller than the current setting value of difficult target in header of block: ***H(n||h)<=t.***

H is hash function of SHA256; ***n*** is Nonce's random number; ***h*** is header data of block, moreover addition of hash of previous block, root Merkle so on; ***t*** is target difficult, the smaller the ***t*** value, the more efficient ***n*** value is discovered; The node which is identified first can be generated with accounting rights of fresh block. The consensus application of PoW in blockchain is given below:

1. ***Each fresh transaction is transmitted to all available nodes in block chain's network.***
2. ***To construct a new block, individual node gathers all transactions in past since the past block was generated, and computes the Merkle root of the header on current transactions. Raising Nonce of block header from 0 to 1, till the 2-times of SHA256 hash value of header are less than or equal to sets of values of the target.***
3. ***The entire network nodes contributes in computation at same time. If individual node identifies the perfect random number, that node will get new block's bill rights and rewards in mining of blockchain, and transmits the block to whole network.***
4. ***After getting new block, neighboring nodes checks the timeline (validity) of transaction and random number Nonce of the block. If it is perfect, the block is included in local blockchain, and preceding block will be built on the basis of this block.***

3. CONCLUSION:

This entire research introduced the major application of cryptography in blockchain and analyzes the current issues. Primarily, beginning from blockchain application, the blockchain application is moderated. Secondly, the introduction of cryptographic infrastructure is introduced to extend the blockchain. At end, existing security issues in blockchain are categorized. This shows the whole digital encryption technology runs with blockchain application and is core infrastructure of blockchain application. This research emphasizes that research on cryptography plays major role in implementation of blockchain, and propagates the further research path of blockchain application.

4. REFERENCES

[1] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Consulted., 165: 55-61.

[2] Zhu, Y., Gan, G.H., Deng, D. (2016) Security Research in Key Technologies

July -August 2020
ISSN: 0193-4120 Page No. 6610-6618
.

of Blockchain.Information Security Research., 12: 1090-1097.

[3] Liu, X.F. (2017) Research on blockchain performance improvement of Byzantine fault-tolerantconsensus algorithm based on dynamic authorization. Zhejiang University.

[4] Wang, X., Lai, X., Feng, D. (2005) Cryptanalysis of the Hash Functions MD4 and RIPEMD.Advances in Eurocrypt., 3494: 1-18.

[5] Shen, Y., Wang, G. (2017) Improved preimage attacks on RIPEMD-160 and SHA-160. KsiiTransactions on Internet & Information Systems., 12: 727-746.

[6] Wang, H.Q., Wu, T. (2017) Cryptography in Blockchain. Journal of Nanjing University of Postsand Telecommunications., 37: 61-67.

[7] Yuan, Y., Wang, F. (2016) Current Status and Prospects of Blockchain Technology
Development. Acta Automatica Sinica., 42: 481-494.

[8] Miyaji, A. (1994) Elliptic Curves Suitable for Cryptosystems. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences., 77: 98-105.

[9] He, P., Yu, G., Zhang, Y.F. (2017) Prospective review of blockchain technology and application.Computer Science., 44: 1-7.

[10] Zhai, S.P., Li, Z.Z. (2018) The data block chain of the key technologies Consistency. ComputerTechnology and Development., 8: 1-6.

[11] An, Q.W. (2017) Research and application of key technologies for decentralized transactionsbased on blockchain. Donghua University.