The Hash Idea for Blockchain Security

Ms.U.Sinthuja M.Sc.,M.Phil.,(Ph.D)[1]
Dr.K.Juliana Gnanaselvi M.Sc,M.Phil .,Ph.D[2]
Assistant Professor, Department of Computer Science,
Rathinam College of Arts and Science,Coimbatore, Tamilnadu,India
Sint@techie.com [1]
sunil.juliana@gmail.com[2]

Abstract: Blockchain is gaining traction and can be termed as one of the furthermost prevalent topics nowadays. Although critics question about its scalability, security, and sustainability, it has already transformed many individuals' lifestyle in some areas due to its inordinate influence on industries and businesses. Granting that the features of blockchain technology guarantee more reliable and expedient services, it is important to consider the security and privacy issues and challenges behind the innovative technology. In this paper hash function has discussed with algorithm to increase the security level.

Keywords: BitCoin, IoT, Hash Function, Denial of-Service

(Received July 12th, 2018/ Accepted November 25th, 2019)

1. INTRODUCTION

The blockchain is a public ledger which operates like a log by having a record of all business or other transactions in a chronological order which was operated by the user, and also secured by a fitting compromise mechanism and providing an absolute record. Satoshi Nakamoto published a brief but groundbreaking paper to a cryptography forum. In it he outlined a way to overcome the double-spend scenario – a problem which plagued previous cryptocurrency: "Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones behind it" (Nakamoto, 2008).

Its exceptional characteristics include immutability, irreversibility, decentralization, persistence and anonymity. With these advantages, it has found applications in almost all fields requiring data sharing among multiple parties but with secure authentication, namelessness and durability. It's a short of trending technology not only with bitcoin also called as cryptocurrency but also includes other fields like Payment processing and money transfers, Monitor supply chains, Retail loyalty rewards programs, Digital IDs, Data sharing, Copyright and royalty protection, Digital voting, Real estate, land, and auto title transfers and so on. It does not have limited accesses in few fields. The figure-1 depicts about the characteristic of Transactions & Smart Contracts which is a transaction is an exchange of assets that is managed under the entity service's rules.

Such rules are usually Operationalized through scripting languages (e.g. Bit coin's Forth) and are used for advanced transactions (such as escrow and multi-party signatures) to be performed. These rules also form the basis for smart contracts. Consensus & Trust In events surrounding nuclear disarmament near end of the cold war, President Regan made a Russian proverb famous: "trust, but verify."The same could be claimed for Blockchain. It is trusted by consensus as all parties must have identical copies of the Blockchain; but each participant is responsible for verifying it. Public and Private Blockchain can be classified as public, private or hybrid variants, depending on their application. Although across from these characteristics the Blockchain method is available with four core

characteristics known as Immutable – (permanent and tamper-proof), Decentralized – (networked copies), Consensus Driven– (trust verification), Transparent – (full transaction history) .

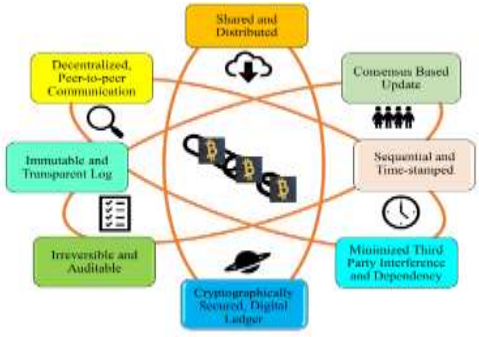

FIGURE-1. Blockchain Characteristics.

1.1. Blockchain Functionality:

Bitcoin exchange and transfer occur by means of a shared distributed ledger, which records the details of every transaction occurred among the network participants without involving any trusted centralized party. The single copy of the ledger resides in synchronization with all the complicated parties, thus dropping the risk of a single point of failure. Bitcoin works on Public Key Infrastructure (PKI) in the Blockchain for authenticating unnamed users and regulatory access. For source authentication and identification, each transaction is digitally signed by the owner with the private key. To keep a track of transactions occurring concurrently, multiple transactions are gathered together in a structure called a 'block' uniquely identified by its hash and timestamp. Validation of transactions and the block, among potentially distrusted users is done using a consensus mechanism, The working principle of Blockchain technology is quite significant for all users who have transact using it. Basically most famous personalities like Bill Gates and others are using bitcoin which was handled by chain of block (Blockchain) for their huge transactions. When a new transaction or an edit to an existing transaction comes in to a Blockchain, generally a majority of the nodes within a Blockchain implementation must execute algorithms to evaluate and verify the history of the individual Blockchain block that is proposed. If a majority of the nodes come to a consensus that the history and signature is valid, the new block of transactions is accepted into the ledger and a new block is added to the chain of transactions. If a majority does not concede to the addition or modification of the ledger entry, it is denied and not added to the chain.

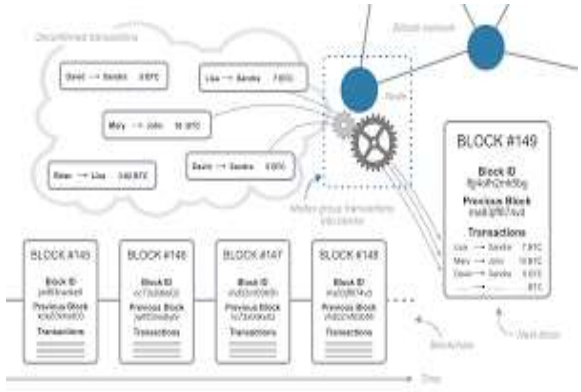

FIGURE-2: The working way of Blockchain

This distributed consensus model is what allows Blockchain to run as a distributed ledger without the need for some central, unifying authority saying what transactions are valid and (perhaps more importantly) which ones are not.

1.2. Classification of Blockchain:

Blockchain has been classified into three types as *Public, private and consortium.*

1.2.1Public Blockchain: A public Blockchaindelivers an open platform for people fromvarious organizations and backgrounds to join, transact and mine. There aren't any restrictions on any of these factors.Therefore, these are also called 'permission-less' block chains. Every user is having full rights to read/write transactions, and also to perform auditing in the Blockchain or review any part of the Blockchain at any time. The Blockchain is open and translucent and no such 'validate nodes'. All users can collect transactions and begin with the mining process to earn mining rewards. The availability of the copy of the entire Blockchain synchronized with all the nodes makes it immutable. With complete decentralization, the vastness of existing networks, and an open platform for anyone to join, consensus is achieved by any of the decentralized consensus mechanisms such as proof-of-work, proof of-stake,etc

1.2.2 Private Blockchain: It is a type of Blockchain system which is setup to enable private sharing and exchange of data among a group of individuals who comes under in a single organization or among multiple organizations with mining controlled by one organization or selective individuals. It is also called permission Blockchain since unknown users cannot get access to it, unless they receive a special invitation. Nodes' participation is decided either by a set of rules or by the network in-charge, to control access. This

inclines the network more towards centralization, while derogating the basic Blockchain features of complete decentralization, and openness as defined by Satoshi.

1.2.3 Consortium Blockchain: A consortium blockchain can be considered as a partially private and permission blockchain, where not a single organization but a set of pre-determined nodes are responsible for consensus and block validation. These nodes decide who can be part of the network and who can mine. For block validation, a multi-signature scheme is used, where block is considered valid, only if it signed by these nodes. Thus, it is a partially centralized system, owing to the control by some selected validate nodes, unlike the private blockchain which is completely centralized, and the publicblockchain which is completely decentralized. It is decided by the consortium whether read or write permissions would-be public or limited to the network participants. Also, the restriction of consensus to a set of nodes doesn't guarantee immutability and irreversibility, since control of the consortium by a majority can lead to tampering of the Blockchain.

2. RELATED WORK

The services discussed in [9] which include authentication , confidentiality, privacy and access control list (ACL), data and resource provenance, and integrity assurance of the blockchain. Give insights on the use of security services for current applications, to highlight the state of the art techniques that are currently used to provide these services, to describe their challenges , and to discuss how the blockchain technology can resolve these challenges. This paper [10] evaluated the security of blockchains specifically Bitcoin, Ethereum and Hyper ledger networks. Moreover, they overview several DLTs challenges and attacks scenarios. Furthermore, they have conducted a majority attack simulation visualizing the risk of a PoW consensus. Besides, we exploited the solidity language by performing a re-entrancy attack.

In this paper[11], author . In addition, blockchain can be applied beyond the Internet of Things (IoT) environment; its applications are expected to expand. Cloud computing has been dramatically adopted in all IT environments for its efficiency and availability. In this paper, they discuss the concept of blockchain technology and its hot research trends. In addition, they will study how to adapt blockchain security to cloud computing and its secure solutions in detail. In [12] the author shed light on the prevalence and nature of these incidents through a database structured using the STIX format. Apart from OPSEC-related incidents, author find that the nature of many incidents is specific to blockchain technology. Two categories stand out: smart contracts, and techno-economic protocol incentives. For smart contracts, we propose to use recent advances in software testing to find flaws before deployment. For protocols, they propose the PRESTO framework that allows us to compare different protocols within a five-dimensional framework.

3. PROPOSED WORK

The need for blockchain based identity authentication is particularly salient in the internet age. While there exists somewhat defective systems for founding personal identity in the physical world, in the form of Social Security numbers, state liquor identification cards, drivers' licenses and even passports or national identity cards, there is no equivalent system for securing either online authentication of our personal identities or the identity of digital entities. Facebook accounts, now often used as login for different digital applications, and media access control (MAC) addresses, may come close, yet both can hardly function as trustworthy forms of identification when they can be changed at will.

Secure Communications The personal keys are exchanged over *DTLS channels* between the key server, the resource servers, and the clients. Authentication between the resource servers and the key server is achieved on the basis of certificates and between the clients and the key server, through a challenge-response.

Data Security Conventional models of data security rely on creating harder and harder "walls" – adding multiple factors to authentication for access and stronger encryption. They typically rely on the same fundamental concept: once you enter the system, you can access the data. Compartmentalization is typically minimal. Edward Snowden used a combination of social engineering and a low-tech "spider" to crawl over 1.7 million documents. 8 With Blockchain, there exists the potential to "scatter the stack", rendering the cost of any one breach or combination of breaches much lower.

Decentralized Security Underlying all of the above applications of Blockchain technology is the importance of the data being securely held – in the sense that it cannot be tampered with. Data protection and privacy is another aspect of data security. The decentralized nature of Blockchain may initially appear to be at odds with privacy; this is indeed a valid concern however there are some developments to reunite the two.

3.1. Hash Function:

Blockchain platforms available across have developed various security features to handle the transaction anonymity and security. Hyper ledger Fabric does the provisioning for identity management

as well as transaction authentication via certificate authority (CA). Ethereum platform supports transaction authentication using transaction signing mechanism where transaction can be signed by an author using the secured key (private key). Ethereum in conjunction with Java Web3J provides API to perform transaction signing where the author signs the transaction with his own secret key and generates transaction hash.

```
RawTransaction rawTxn = RawTransaction.createEtherTransaction (param1, param2,…,));
BytesignedMessage = TransactionEncoder.signMessage(rawTxn, privateKey/credentials);
```

Once signed, transaction can be executed and hash can be generated. Also making this transaction hash secure is the key for transaction authentication process. The smart contract to share the hash with intended recipient. Before sharing the hash in a smart contract has been added one more security layer to hash the transaction, by encrypting it using Java crypto AES encryption utility. This ensures added level of data security to transaction hash.

```
Cipher aesCipher = Cipher.getInstance ("AES");
aesCipher.init (Cipher.ENCRYPT_MODE, secretKey);
ByteEncryptedTxnHash = aesCipher.doFinal (transactionHash);
```

The encrypted transaction hashes (hash of hash) then push to a smart contract which has been permission for intended recipients. The intended recipient will be authenticated first and later they will be provided access to the transaction hash.

Authentication Hash Algorithm

```
contract GetTransactionHashForAuthenticUser
{
address[]intendedRcptAddrs=[0x45df89ghf6dft4n5kl56rt, 0xgh234g78jk90sdf4ghh23];
address ownerAddr= 0x87eaf79c12e96a3dc6f53426c;
function fetchTransactionHash()
 public return (string)
{
uint i = 0;
for(i = 0; i < addrs.length; ++i)
if(msg.sender == addrs[i])
// Return stored hash of hash for authenticated user.
return "hashOfHash";
else
return "You are not an authorized user";
}
}
```

Once intended user is authenticated and gets the required hash from the above contract, then using steps given below, he can obtain the exact transaction hash and later decode/decrypt the signed transaction.The secret key can be generated using Java crypto API and shared with intended user in an offline process. After decrypting the transaction hash the user need to decode the signed transaction for authentication. Once the user decode the signed transaction can get the sender and receiver addresses for transaction verification.

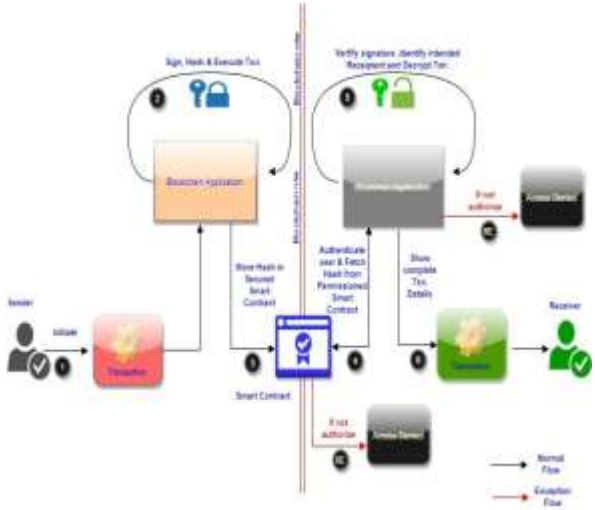

FIGURE-3: Hash Function Process

```
Cipher aesCipher = Cipher.getInstance("AES");
aesCipher.init(Cipher.DECRYPT_MODE, secretKey);
byte [] bytePlainText = aesCipher.doFinal(byteCipherText);
return new String(bytePlainText);
```

Here to keep the transaction decodes process as a part of solidity smart contract where the algorithm used solidity **ecrecover** function to recover the transaction to get the owner of the transaction. If owner/sender and receiver from decode process is valid then we can assume that transaction is authenticated. Solidity **ecrecover** function call looks like this:

```
ecrecover (txnHash, uint8(v), r, s);
```

The user can obtain r, s and v values using Java web3j API from transaction signature as follows:

```
Transaction tx = new Transaction (rawtxHashHexByteArray);
java.math.BigInteger rInitial = tx.getSignature ().r;
java.math.BigInteger sInitial = tx.getSignature ().s;
byte vInitial = tx.getSignature().v
```

Based on r, s and v value pass to a smart contract function ecrecover, it will return you transaction owner/sender address. The above entire process ensures transaction authentication and security by sharing the transaction hash in a secured way with additional security mechanism (hash of hash) for robust transaction processing.

4. CONCLUSION AND FUTURE WORK

This paper has dealt with Blockchain basic and characteristics of different applications. Secondly the classification of the model which has been divided based on some criteria. Final focus is recommended hash function for secured block chain. The Future research may be extending with any other security algorithm like AES, DES, Digital Signature other security considerations and so forth.

REFERENCES:

1. Applications karim sultan1 , umar ruhi1 and rubina lakhani conceptualizing blockchains: characteristics & applications 11th iadis international conference information systems 2018. Https://arxiv.org/pdf/1806.03693

2. Data Insertion in Bitcoin's Blockchain Andrew Sward, Ivy Vecna, Forrest Stonedahl,,ISSN 2379-5980 (online) DOI 10.5915/LEDGER.2018.101 https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx

3. Applications of Blockchain Technology beyond Cryptocurrency Mahdi H. Miraz , Maaruf Ali- Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.

4. Don Tapscott and Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 1st ed. New York, USA: Penguin Publishing Group, 2016.

5. Maaruf Ali and Mahdi H. Miraz, "Recent Advances in Cloud Computing Applications and Services," International
Journal on Cloud Computing (IJCC), vol. 1, no. 1, pp. 1-12, February 2014, Available:http://asdfjournals.com/ijcc/ijcc-issues/ijcc-v1i1y2014/ijcc-001html-v1i1y2014/

6. Xueping Liang et al., "ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," in Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid '17), Madrid, Spain, May 14 - 17, 2017, pp. 468-477,
Available:https://dl.acm.org/citation.cfmid=3101176&CFID=994896989&CFTOKEN=44228545

7. Mahdi H. Miraz, Maaruf Ali, Peter Excell, and Picking Rich, "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," in the Proceedings of the Fifth International IEEE Conference on Internet Technologies and Applications (ITA 15), Wrexham, UK, 2015, pp. 219 – 224, Available:http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7317398

8. IoTChain: A Blockchain Security Architecture forthe Internet of ThingsOlivier Alphand, , Michele Amoretti, Timothy Claeys, Simone Dall'Asta,Gianluigi Ferrari,Franck Rousseau, Bernard Tourancheau, Luca Veltri, Andrzej DudaDepartment of Engineering and Architecture, University of Parma, ItalyUniv. Grenoble Alpes, CNRS, Grenoble INP, LIG, F-38000 Grenoble, France

9.Tara Salman et al "Security Services Using Blockchains: A State of the Art Survey" n: DOI 10.1109/COMST.2018.2863956,
IEEE.https://arxiv.org/ftp/arxiv/papers/1810/1810.08735.pdf

10. Joanna Moubarak et al," On Blockchain Security and Relevant Attacks" 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)

11. Jin Ho Park et al "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions" Symmetry 2017, 9, 164; doi:10.3390/sym9080164.

12. Vincent Chia et al "Rethinking Blockchain Security", issued on : april 2019 https://www.reddit.com/r/Bitcoin/comments/28242v/eligius falls victim to blocksolution withholding