IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 44-49

A Review of Block chain Technology in Cryptography

Dr. (Mrs) RadhaPimpale
Asst. Professor, Department of Information Technology
Priyadarshini Bhagwati College of Engineering, Nagpur

Abstract: *The blockchain technology has great prospective in cryptography. It is facing a number of technical challenges such as authentication or authorization and security in cryptography. In this paper, review has been taken on Blockchain technology, which offers new tools for authentication and authorization in the digital world, it create new digital relationships. Blockchain is a technology to create and maintain a cryptographically secure, shared, and distributed ledger (a database) for transactions. Blockchain brings trust, accountability, and transparency to digital transactions. When we used block chain technology, A block contains a timestamp with reference to the previous block, the transactions and the computational problem that had to be solved before the block went on the Blockchain. Rigorous encryption and data distribution protocols on a network, can ensure that the information will remain safely and out of the reach of hackers.*

Keywords: *Block chain technology, digital transaction, Private Key, Public Key, Block*

I. Introduction

A Blockchain is a type of diary or spreadsheet containing information about transactions It is a diary that is almost impossible to forge. Each transaction generates a hash. Hash a program called a Hash function that turns text into a set of numbers and letters. A hash is a string of numbers and letters, produced by hash functions. A hash function is a mathematical function that takes a variable number of characters and converts it into a string with a fixed number of characters. Transactions are entered in the order in which they occurred. Order is very important. Even a small change in a string creates a completely new hash. The hash depends not only on the transaction but the previous transaction's hash. The Blockchain updates itself every 10 minutes. If someone change the record of each transaction. After each record, hash generated has been changed and inserted a hash generated from the record+last hash. So each entry depends on the previous. If a transaction is approved by a majority of the nodes then it is written into a block. Each block refers to the previous block and together make the Blockchain. A blockchain is a permanent, sequential list of transaction records distributed over a network. Each block in the chain contains a hash of the previous block, along with a timestamp and transaction data. When Hacker try to attack or manipulation, the blockchain naturally resistant attack. Blockchain technology is ideal for recording various types of transactions where data is sensitive or targeted by hackers for unauthorized duplication or other fraudulent activity. Bitcoin and other crypto currencies use blockchain technology to record transactions [6].

Some Most important terms in Blockchain Technology are:

Nodes Many records and transaction are converted into one page spreadsheet. Spreadsheets are distributed over many computers all over the world, are known as Nodes. Each node has a copy of the digital ledger or Blockchain. Each node checks the validity of each transaction.

Noncemeans to add a number after each record so generated hash ends with two zeros so no one can understand easily change the transaction. If a majority of nodes say that a transaction is valid then it is written into a block. If anyone change one entry, all the other computers will have the original hash. They would not allow the change to occur.

Block spreadsheet is called a block .The whole family of blocks is the Blockchain. Every node has a copy of the Blockchain. Once a block reaches a certain number of approved transactions then a new block is formed.

The Blockchain updates itself every ten minutes. It does so automatically. No master or central computer instructs the computers to do this. As soon as the spreadsheet or ledger or registry is updated, it can no longer be changed. Thus, it’s impossible to forge it. You can only add new entries to it. The registry is updated on all computers on the network at the same time.

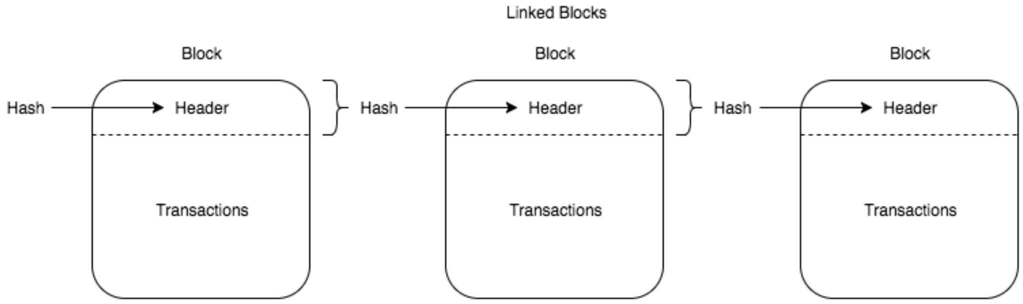
REQUIREMENT FOR THE TRANSACTION IN BLOCKCHAIN TECHNOLOGY

A Wallet To carry out a transaction you need two things: a wallet, which is basically an address, and a private key. A wallet is a string of numbers and letters, such as 18c177926650e5550973303c300e136f22673b74. This is an address that will appear in various blocks within the Blockchain as transactions take place. No visible records of who did what transaction with who, only the number of a wallet.

Private and Public Key The address of each particular wallet is also a public key. The private key is a string of random numbers, but unlike the address the private key must be kept secret. The system of two keys private and public kays is at the heart of encryption in cryptography, and its use long predates the existence of Blockchain [1].

Blockchain Architecture

The design of Blockchains are probabilistic systems. It comprises of network of computers called nodes. The nodes independently take decision about and concur upon the longest and most valid which "chain of blocks". After a block is created and set around the network, each node processes the block and decides where it fits into the current overarching blockchain ledger.



Within the context of a blockchain, there are a few different types of blocks.

Most blocks simply extend the current main blockchain. These are called "main branch blocks". Some blocks reference a parent block that is not at the current blockchain tip. These blocks are called "side branch blocks".Some blocks reference a parent block that is not known to the node processing the block. These are called "orphan blocks." Side branch might not currently exist in the main branch, but if more work is done on them (meaning other blocks are mined that reference them as a parent), there is the possibility that that a particular side branch will be reorganized into the main branch. This reorganization happens because the "main" branch of the blockchain is the one that has had the most work done on it. As new blocks are appended to the blockchain, it becomes increasingly difficult to "overwrite" existing blocks because the most valid chain is the one that has had the most work done on it [2].

Blocks

Blocks are data structures whose purpose is to bundle sets of transactions and be distributed to all nodes in the network. Blocks are created by miners(web users). Blocks contain a block header, which is the metadata that helps verify the validity of a block.

Typical block metadata contains:

Version - the current version of the block structure

Previous block header hash - the reference this block's parent block

Merkle root hash - a cryptographic hash of all of the transactions included in this block

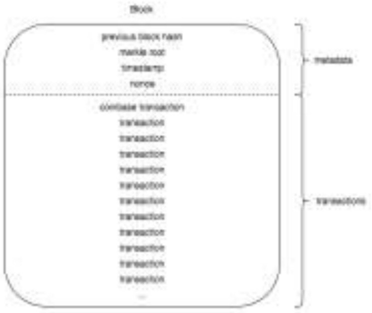
Time - the time that this block was created

nBits- the current difficulty that was used to create this block

Nonce ("number used once") - a random value that the creator of a block is allowed to manipulate however they so choose

These 6 fields constitute the block header. The rest of a block contains transactions that the miner has chosen to include in the block that they created.

Users create transactions and submit them to the network, where they sit in a pool waiting to be included in a block.



It's important to realize that each miner (and more generally, each user of a blockchain) is allowed to act however they want within this blockchain system. Consensus rules dictate that only valid changes to the blockchain will be accepted by everyone else. These results in a system that economically guarantees that only valid blocks will be worked on, submitted to the network, and accepted by the greater community [3].

II. Methodology

Blockchain Technology In Cryptography

In the case of blockchain technology, Authentication and authorization is most important for interactions in the digital world. Private key cryptography provides a powerful rights that fulfills authentication requirements. For Authorization it requires – needs a distributed, peer-to-peer network , broadcasting the correct transaction type and enough. This distributed network must also be committed to the transaction network’s record keeping and security. Authorizing transactions is a result of the entire network applying the rules upon which it was designed (the blockchain’s protocol).

Requirement of Blockchain technology

Requirement of Blockchain technology required for Authentication and authorization and digital transactions are

Cryptographic keys

A cryptographic key is a string of numbers and letters. Cryptographic keys are made by key generators or keygens. These keygens use very advanced mathematics involving prime numbers to create keys. Two people wish to transact over the internet. Each of them must holds a private key and a public key.

Digital Identity

The main purpose of this component of blockchain technology is to create a secure digital identity reference. Identity is based on possession of a combination of private and public cryptographic keys. The combination of these keys can be creating an extremely useful digital signature.

In turn, this digital signature provides strong control of ownership.

In blockchain, cryptography is primarily used for two purposes:

1. Securing the identity of the sender of transactions.
2. Ensuring the past records cannot be tampered with.

Blockchain technology utilizes cryptography as a means of protecting the identities of users, ensuring transactions are done safely and securing all information and storages of value. Therefore, anyone using blockchain can have complete confidence that once something is recorded on a blockchain, it is done so legitimately and in a manner that preserves security[7].

Symmetric Key Cryptography

In Symmetric Key Cryptography, encryption has been performed at sender side and decryption performed at receiving side , it is named as symmetric cryptography due to same key is used for encryption and decryption.

Asymmetric cryptography

Asymmetric cryptography or public cryptography in this key pair is used public key, the public key may be public address, can be compared to an email address and private key and private key to password ,blockchains accomplish this with public key cryptography. This cryptographic techniques ensure that the source of transactions is legitimate and that hackers can not steal a users funds for example cryptocurrencies like Bitcoin and Ethereum [7].

Public Key Cryptography is a cryptographic system that relies on a pair of keys, a private key which is kept secret and a public key which is broadcast out to the network. This system helps ensure the authenticity and integrity of a message by relying on advanced cryptographic techniques.

Digital Signatures

Digital signatures are quite similar to actual signatures on a document. For the authentication of document public key of the user and authentic Digital signatures are check. Digital signatures depend on two functions:

Sign(Message, Private Key)->Signature

Given the message we want to sign and a private key, this function produces a unique digital signature for the message.

Verify (Message, Public Key, Signature) -> True/False

Given the message we want to verify, the signature and the public key, this function gives a binary output depending on whether the signature is authentic

Once the transaction is signed by the owner, the transaction is sent to the memory pool where it sits to be processed by miners. The miners use the sender's public key to ensure that the digital signature is authentic so that a hacker cannot spend a user's funds without their consent. If the ownership and digital signature check out, they include the transaction in the next block, and the money is sent from one wallet to another.

Proof of Work

The other major use of cryptography in the Bitcoin protocol is in computing the proof of work function. Miners rely on computing the "SHA256 Hash Function" for a lot of inputs until they find the nonce for a given block before adding it to the blockchain. The difficulty of the mining process is changed by how many zeroes the hash must begin with to be added to the blockchain. This is a unique system as it adjusts higher or lower depending on how many people are mining at any given time. It also makes it computationally in feasible for an attack vendor to go and edit transactions that are already recorded on the blockchain.

Hashing

Hashing is a cryptographic method of converting any kind of data into a string of characters into fixed size hash value, it providing security through encryption, hashing creates a more efficient store of data. The same input must always generate the same output. Regardless of how many times you put the data through the hashing algorithm, it must consistently produce the same hash with identical characters in the string.

The input cannot be deduced or calculated using the output. There should be no way to reverse the hashing process to see the original data set.Any change in the input must produce an entirely different output. Even changing the case of one character in a data set should create a hash that is significantly different. The hash should be of a fixed number of characters, regardless the size or type of data used as an input[10].

III. Performance Evaluation

Innovative Uses For Blockchain Technology

As more people join the worldwide web and technology continues to develop, more data gets produced and more hackers will attempt to steal or corrupt that data. The technology behind blockchain is versatile and incredibly useful for the future of the Internet, allowing users to better secure their data. Innovative uses for blockchain technology are already incryptocurrencies and can be especially useful to boost cyber security.

Application Of Blockchain Technology

1. Blockchain Technology work as a smart contracts, it define the rules and penalties around a specific agreement in like traditional way. The contracts are coded so that they are discharged on the fulfillment of specific criteria.
2. Blockchain Technology work A warranty claim by settling warranty by smart contracts using Blockchain that will inevitably make the process a lot easier.
3. Derivatives are used in stock exchanges and are concerned with the values of assets. Using smart contracts, peer-to-peer trading will become a usual operation, resulting in a complete revolution in stock trading.
4. Insurance claims Blockchain technology, you could just submit your insurance claim online and receive an instant automatic payout
5. Identity verification Using the decentralization of Blockchains, the verification of online identity will be much quicker
6. Data storage is tamper-proof and incorruptible when backed by Blockchain.
7. The Internet of Things (IoT) is the network of physical devices, vehicles and other items embedded with software, actuators, sensors, software and network connectivity, connected to the Internet. All of those

features enable such objects to collect and exchange data. Blockchain and its smart contracts are ideal for this.

8. Archiving and file storage Google Drive, Dropbox, etc. have thoroughly developed the electronic archiving of documents with the use of centralized methods. Decentralized cloud storage solutions available, such as Storj, Sia, Ethereum Swarm and so on are available for file storage.
1. The protection of intellectual property Blockchain will offer much greater protection of intellectual property an application called Ascribe, using Blockchain, gives this protection.
2. Crime Law breakers have to hide and camouflage the money gained from their exploits. Currently this is done with fake bank accounts, gambling, and offshore companies, among other stratagems. There are a lot of concerns regarding the transparency of cryptocurrency transactions. But, all of the necessary regulatory elements, such as identifying parties and information, records of transactions and even enforcement can exist in the cryptocurrency system.
9. Social media Social media organizations are able to freely use the personal data of their clients. This helps them make billions of dollars. Using Blockchain smart contracts, users of social media will be enabled to sell their personal data, if they so desire.
10. Blockchain technology is have capability to manage data. Relational databases, which orient information in updatable tables of columns and rows, are the technical foundation of many services we use today[3]
11. The use of smart contracts in elections and polls -Elections and polls could be greatly improved with smart contracts. There are various apps such as Blockchain Voting Machine, Follow My Vote and TIVI.

Advantage Of Using Blockchain Technology In Cryptography

1. Blockchain Technology is secure technology, it itself does not get hacked. A Blockchain technology being decentralized, This means that hackers can attack a single point in the hope of gaining access. As such, these hacks have given rise to calls for decentralized exchanges and it is only a matter of time before these become the main platforms allowing people to trade cryptocurrencies.
2. Security has got most important aspect to people in blockchain technology. Private keys are more secure as they are considerably longer. user must use different password for each account, they should used strong complex password for each account including numbers and symbols and different cases.
3. The distribution and decentralization potential of blockchain technology.
3. Blockchain technology provides one of the best tools we currently have to protect data from hackers, preventing potential fraud and decreasing the chance of data being stolen or compromised.
4. Complex structure provides blockchain technology with the ability to be the most secure form of storing and sharing information online that we’ve discovered so far.
5. Guardtime using blockchain technology to keep important data safe. Guardtime’s system works in such a way that it’s always able to detect when a change has been made to the data and is constantly verifying the changes. This ensures that there is no discrete way to tamper with blocks in the chain and the data remains uncompromised.
6. Preventing Distributed Denial of Service (DDoS) attacks Blockchain technology prevent denial of services attacks due to partially decentralization, Hackers can use several techniques to instigate an attack on centralized part of DNS (the one which stores the main bulk of data) and continue crashing one website after another. essentially sending myriads of junk requests to a website, increasing traffic until the site can no longer keep up with the requests.
7. Blockchain play a major role in the roll out of IoT, it provide ways of guarding against hackers. Because it is built for decentralized control, a security scheme based on it should be scalable enough to cover the rapid growth of the IoT.

Limitations And Vulnerability Of Blockchain Technology

In order to operate blockchain network in full potential, Robustness of network system requires for Blockchain network for widely distributed grid of nodes. The network’s nodes will no longer be decentralized in the full sense of the word.

IV. Conclusion

In this paper, we present a comprehensive overview on blockchain. We first give an overview of blockchain technologies, blockchain architecture in blockchain Technology. We discussed the typical cryptographic techniques used in blockchain such as cryptographic keys, digital signature, proof of work, digital signature most important hasing techniques. Furthermore, we listed some application, advantage in blockchain development and Limitations and vulnerability.

References

[1]. https://www.coindesk.com/information/how-does-blockchain-technology-work

[2]. https://www.pluralsight.com/guides/blockchain-architecture

[3]. https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

[4]. Zibin Zheng[1], Shaoan Xie[1], Hongning Dai[2], Xiangping Chen[4], and Huaimin Wang[3], "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE 6th International Congress on Big Data, 978-1-5386-1996-4/17 $31.00 © 2017 IEEE, DOI 10.1109/BigDataCongress.2017.85

[5]. https://jaxenter.com/cryptographic-hashing-secure-blockchain-149464.html

[6]. https://www.edx.org/learn/blockchain-cryptography

[7]. https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/blockchain-cryptography-explained

[8]. Olivier Boireau," Securing the blockchain against hackers" ,Network Security, Volume 2018, Issue

[9]. https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/

[10]. https://blog.bankex.org/essentials-of-blockchain-cryptography-c60180f14b7f

[11]. Satoshi Nakamoto," Bitcoin: A Peer-to-Peer Electronic Cash System"