ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 4, Issue - 6, November - December - 2018, Page No. 75 - 82

A Review in the field of Blockchain for Blockchain System

[1]Vaishali Sharma, Research Scholar, Dept. of Computer Science, Arya Institute of Engg. & Tech., Jaipur, Rajasthan, India

[2]Sayar Singh Shekhawat, Associate Professor, Dept. of Computer Science, Arya Institute of Engg. & Tech., Jaipur, Rajasthan, India

[3]Manish Choubisa, Assistant Professor, Dept. of Computer Science, Arya Institute of Engg. & Tech., Jaipur, Rajasthan, India

E-mail: [1]vaishali646@yahoo.com, [2]ssayarss@rediffmail.com, [3]ermanishchoubisa@gmail.com

Abstract

To know about Proof-of-Stack algorithm, weshould know about Blockchain. What is Blockchain and why we use Blockchain. Blockchain is a Method or Technology which is based on distributed databases. This technology offers advantages to both users or customers and service providers or programmers. The reason for the interest in Blockchain is that it provides security, obscurity and data integrity without any third party. Once you broadcast a message or transaction to the blockchain, it can't be erased. Bitcoin has developed as the most successful cryptographic currency in history. A blockchain is not a currency, It is a system for authenticating, tracking, clearance and recording the ownership of assets as they are traded.

Keywords: Blockchain, Database, Cryptographic, Data integrity, Bitcoin.

Introduction

Blockchain was introduced in 2008 in a technical document defining a new type of electronic money: Bitcoin. Subsequently, other cases of use of blockchain appeared. A blockchain is not a room at all. It is a system of authentication, tracking, disposal, settlement and registration of property ownership at the time they are traded.

The Blockchain method is used to validate transactions. In this case, first, the transactions are validated or we can say extracted by a method, called Proof-of-stack. After validating the transactions that are added to a string, we call that transaction a block and that block is added to a string, so let's call this Blockchain method.

Blockchain technology includes a sequence of transactions held in a network of servers called "nodes". Each node records a large book that reflects the ownership of the resources. The ledger is "distributed" because it is instantly maintained in all nodes of the network. The book contains complete and uninterrupted information of all transactions that date back to the beginning of the general ledger (the "chain"). Authorized transactions are added to the general ledger in sets or "blocks" using cryptographic approaches to confirm the integrity of the transaction. It is this record of transactions in blocks of the chain of transactions reflected in the ledger.

- How To Say Blockchain Is Secure

➢ *Block-based security plateforms*

The blockchain corrects fundamental security failures by eliminating the human factor from the algorithm, which is usually the weakest link. Blockchain technology provides end-to-end encryption and privacy. Blockchain technology can be used as a security shield.

B. *Confidentiality and security of conversations*

The decentralized blockchain network, which cannot be censored or controlled by a single source. There is a new decentralized chat application that uses Bitcoin Blockchain technology, called "XChat" and labeled "a new generation messaging application". We have other applications like ProtonMail and BitTorrent Bleep to protect and maintain our private information.

In the long run, blockchain can even replace legal contracts and contracts written with computer code thanks to its security and privacy function.

- Challenges

People lose control of their data as soon as they share it with online third parties. This presents three main challenges: information security, lack of control and transparency. The information can be stored in a dangerous manner and can be lost. People cannot remember the information they shared and they have no transparency about how their data is used.

A. *Transaction costs*

Blockchain will increase transaction costs. The reason for increasing the cost of the transaction is that it is necessary to keep all the old transaction blocks in the genesis block (ie the first block) in the current block.

- *Performance*

The Bitcoin network has a potential performance problem because it only processes one transaction per second (tps), with a theoretical maximum of 7 tps. The main developers say that this limit can be increased if necessary.

A.*Latency*

At this point, each Bitcoin transaction block takes 10 minutes to process, which means that the transaction can take at least 10 minutes to be confirmed. For sufficient security, you have to wait longer, about an hour, and for larger transfers you have to be even longer.

- *Scalability*

Many blockchain solutions require the storage of large transaction and data volumes and fast performance / transaction performance. Fully functional traditional blockchain batteries are relatively slow in this regard. Here are three approaches that are examined to improve scalability,one of them is Proof-of-Stack..

E. *Big Data Store*

An innovative approach is to divide the blockchain process into two distinct levels: replication and linking. The latter has already been solved for large data warehouses that can evolve across large clusters of synchronized servers.

F. *confidentiality problem*

A problem with Blockchain's privacy is the problem with different addresses. For example, users of the bitcoin system can create any number of addresses and the searchers try to group all the addresses belonging to the same user. The goal is to find all the addresses included in the transaction belonging to the same user.

G. *Confidentiality issue*

A problem with distributed public books is highly speculative in nature, with a trade-off between network size and decentralization. Bitcoin Blockchain has a 51% chance of being attacked. A minor can have full control over most of the network, which is a serious problem.

Properties

Distributed consent and anonymity are two important characteristics of blockchain technology.

A blockchain efficiently records transactions between the parties in a distributed register. The data stored in a blockchain are immutable and immediately verifiable. A blockchain is a book of distributed transactions. The blockchain is a chain of blocks and each block represents a set of transactions. As a data structure, a blockchain has several interesting properties.

First of all, the blocks are probably immutable. This is possible because each block contains a hash or a digital summary of its contents, which can be used to verify the integrity of the transactions that contain it. Thus, the hash of a block depends on the hash of the previous block. This makes the whole history of the blockchain immutable, since the modification of the hash of any block n-i would also change the hash of block n. The blockchain itself does not depend on a central and reliable authority. On the contrary, it is distributed to all the nodes that participate in the network. Since no centralized authority can verify the validity of the blockchain, a block is added to the blockchain at regular intervals. For Bitcoin, this interval is determined by the difficulty of the Job Test function. The minor can not extract his transactions.

- Main Points In Blockchain

A. There is no customer protection in the blockchain.

B. Settlement in a blockchain is slow: the cost of settling a transaction in the blockchain is that all nodes in the network must reach an agreement for the transaction to be valid. It's a much slower process than having a bank to monitor the transaction in an instant.

C. Minors can be selfish: a child problem that finds empty blocks and validates them. There is also another problem known as Selfish Mines, a situation in which a data mining or mining group searches and validates a block and does not publish and distribute a valid solution to the rest of the network.

D. Size of the growing blockchain: the total size of the blockchain since January 2017 is 98 GB. At the same time, in 2016, the size was 50 GB. This is a problem because the reliability of a blockchain network depends on the number of blocks in the network and the size of these blocks all over the world.

E. Finally, the settlement in the blockchain will not be economic. This is not a mistake, but a characteristic.

Evolution of The Scale Blockchain

One of Blockchain's applications, Ethereum only makes 20 transactions per second, while another Bitcoin application handles 7 transactions per second. The only way to improve these numbers is to work on their scalability.

If we classify the main problems of scalability in cryptocurrencies, they would be:

Take some time to enter a transaction in the block.

Take the time to reach a consensus.

Suppose Ms. A wants to send 4 BTC to Ms. B, who will send this transaction information to minors, the younger one will put it in her block and the transaction will be considered complete. However, since the bitcoin gets slower and slower.

Furthermore, there is also the small issue of transaction fees. You see, when miners undermine a block, they become temporary dictators of that blockade. If you want your transaction to be completed, you will have to pay a toll to the responsible child. This "toll" is called a transaction fee. Solutions to Blockchain scalability problems:

The increase in the size of the block will only occur through the mechanism of hardfork, which can divide the community. The transition from the working test to the stack test. The work test is a requirement to define an expensive computerized calculation, also called mining.

A. Proof-of-stack

Proof-of-stack the creator of a new block is chosen deterministically, depending on its wealth, it is also defined as a stack. The Proof of Stack protocol will make the whole process of virtual data mining. In this we have validators instead of minors. The way it works is that, as a validator, you will first have to block a part of your ether like a stack. After that, you will begin to validate the blocks, which means that if you see blocks you think you can add to the blockchain, you can validate them by placing a bet. When and if the block is added, you will receive a reward proportional to the stack you have invested. If you bet on the wrong or malevolent block, the stack you have reversed will be eliminated. It makes the attack more difficult at 51% and makes the chain of blocks evolutiva introducing the concept of "Sharding".

The POS will make the block chain much faster because it is much easier to control who has more batteries and then see who has more hashes. This makes consent much easier.

POS facilitates the implementation of Sharding. POS miners will not receive block commissions and will only be able to win a transaction fee.

G. *Sharding*

The biggest problem that Ethereum faces is the speed of transaction verification. Each complete node in the network must download and save the entire chain of blocks. What is

different is that it breaks a transaction and splits it into the network. The knots work side by side in individual fragments. This, in turn, reduces the total time spent. Why cannot we block the first blocks?

The main reason why we can not remove the old blocks is that each new block is based on data from the previous block. The system is designed in such a way that when everyone has to accept that all data is correct. Each block contains a pointer to the previous block and the block that follows. The problem will be solved by a process called fragmentation that means dividing the database, so that each node does not have to keep the entire blockchain.

Blockchain Prunning

If the size of the Bitcoin blocks should be changed or not, and if so, at what size?

What happens with the bitcoin nodes of the network?

Prune blockchain can be the answer to all these questions, even if there are always disadvantages in this proposal. Pruning refers to the elimination of unnecessary information from the chain of blocks when it is no longer necessary.

Blockchain itself can not be pruned. Each block is checked by shredding all its data and a random combination to find a hash that has a number of zeros to the left. If you have even deleted a small block of data from a block, the resulting hash will be modified. Since it is very likely that the new hash does not meet the difficulty requirements, the work test would have been destroyed. I should create a new block to take its place. Therefore, you will also have to re-create the entire

next block, since the parent hash (think of it as a fingerprint) is included in its secondary block, that is, if the parent changes, the entire blockchain becomes invalid .

Now it is possible to store diplomas and personal data in Ethereum according to the GDPR. Lexing Legal Opinion analyzes compliance with the BCDiploma solution. The General Data Protection Regulation (GDPR) of the EU will come into effect on May 25, 2018.

The GDPR is extraterritorial and applies to all companies that own or process data for residents of the EU.

Due to the unalterable character of the block chain, once the data is "written" into a chain of blocks, it can not be deleted or modified. The inalterability and decentralization not only mean that the registration is indelible, but, above all, must be shared by all users. If the right to be forgotten is exercised, one must expect to go against the same principle of the inalterability of the chain of blocks. The data of each node in the block chain must be deleted, as well as its history, which is neither desirable nor possible. For players and users of blockchain technology, it is increasingly urgent to find answers to this question

Single address function:

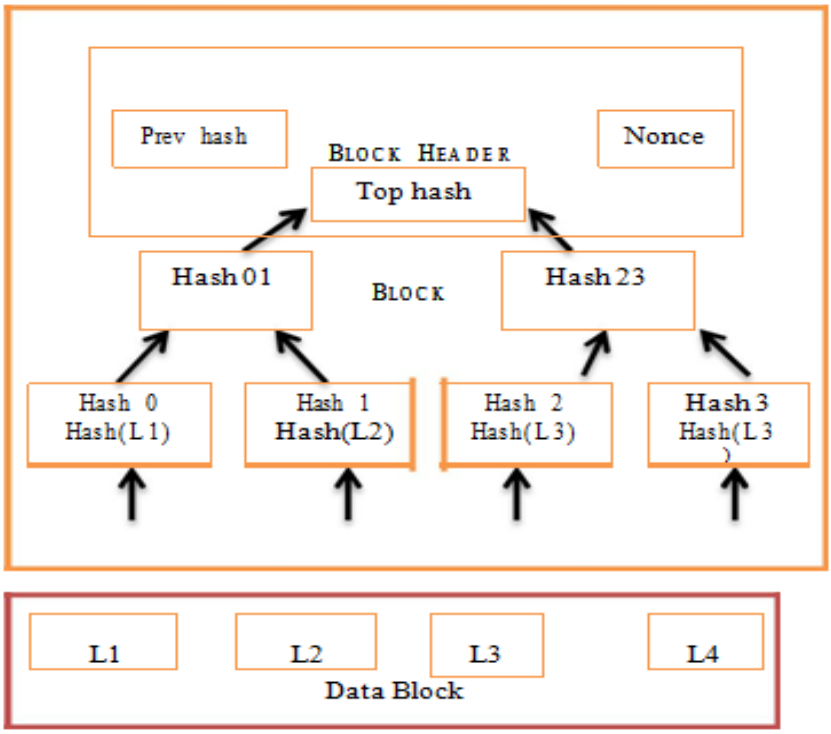
1. An input for an individual output.

F (4) = abcd, then f (3) or f (2) cannot be abcd

We cannot find the input value of the output value G (abcd) = 4 <- this should not be possible

What is a Merkle tree?

A binary tree in which all leaf nodes and all nodes are given leaf nodes are combined hash results from its two children.



Exploitation of the blockchain

The chain of mining blocks is the process by which transactions are checked and added to the public ledger, known as blocks of blocks, as well as the means by which new cryptocurrencies are released. Anyone with access to the Internet and appropriate equipment can participate in the mining industry. The extraction process consists of compiling recent block transactions and attempting to solve an enigma that is difficult to solve. The participant who solves the puzzle places the next block in the blockchain and claims the prize.

The bonuses, which encourage extraction, are both the transaction costs associated with the transactions compiled in the block, and the newly issued bitcoins. The amount of new cryptocurrencies published with each extracted block is called "block reward".

Attack 51%

The 51% attack belongs to an attack on a chain of blocks (usually bitcoin, for which this attack is hypothetical) by a group of miners who control more than 50% of the mining power of the network or of the computing power. Attackers could prevent new transactions from obtaining confirmations, which would allow them to block payments between some or all users. They could also reverse completed transactions while checking the network, which means they could double the currency. It is almost certain that they could not create a new currency or modify the old blocks, so a 51% attack would probably not directly destroy bitcoins or any other currency based on chains of blocks, even if it turned out to be very harmful.

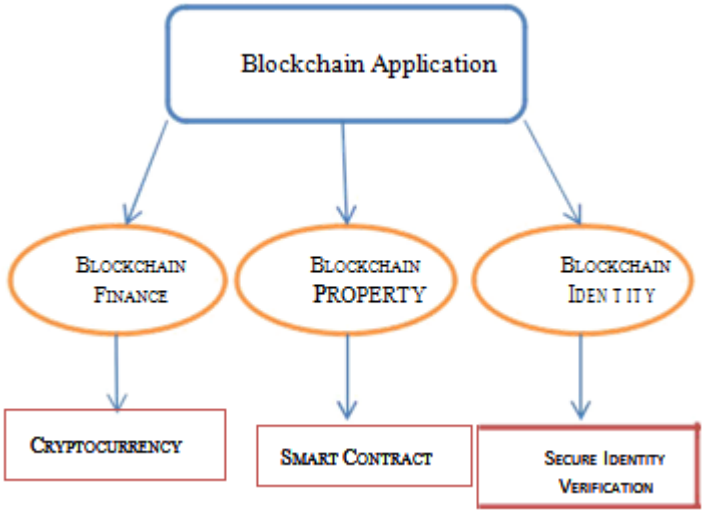
Double Expenditure Problem

The risk that a digital currency can be spent twice. Double spending is a unique problem for digital currencies, since digital information can be reproduced relatively easily. Physical currencies do not have this problem because they can not be duplicated easily and the parties involved in a transaction can immediately verify the good faith of the physical currency. With digital currency, there is a risk that the owner can make a copy of the digital form and send it to a merchant or other party while retaining the original. Initially, it was a problem with Bitcoin, the most popular digital currency or "cryptocurrency", as it is a decentralized currency without a central agency verifying that it is only spent once. However, Bitcoin has a mechanism based on transaction records to verify the authenticity of each transaction and avoid double counting.

Bitcoin requires that all transactions, without error, be included in a public transaction log called "blockchain". This mechanism ensures that the part that spends the bitcoins actually owns them and also avoids double counting and other frauds. The chain of verified transaction blocks accumulates as more transactions are added. Transactions with Bitcoin take a long time to be verified, since the process requires numerous complex obstacles and algorithms that consume a large amount of computing power. Therefore, it is extremely difficult to duplicate or falsify the blockchain due to the enormous amount of computing power required to do so.

Blockchain Applications

The term "Blockchain" caused huge sketches in the tech community.



Blockchain Financing

The original and proven application of blockchain-bitcoin. The world has characterized the need of cryptocurrencies, the innovative engineers of talnet made the needs for new blockchain financial application for technology.

My Money Using Blockchain

Bitcoin is the example of Money based on blockchain. Cryptocurrencies offer people around the world instant, safe, and smooth money. Blockchains provide a permanent registry store for each cryptocurrency transaction performed. Block-based cryptocurrencies work because only verified transactions can be stored in the block chain. In current systems, users must rely on a central authority to ensure that money and payment transfers are not compromised. Obsolete technologies that block the previous payment method of payment without providing a trusted environment, so that it is no longer necessary to use a third party to transfer payments by creating a person for the peer-to-peer relationship ,

Blockchain Financial Services

Blockchain Financial Services redefines the existing footprints of our current capital market infrastructure. Sectors in the sector that have significant activity range from liquidation and back-end regulation to the general architecture of the capital markets. In some of these cases, distributed accounting systems need not be fully decentralized and more financial institutions are planning to create their own blockchain.

Block Chain Property Intelligent and Autonomous Property

The Smart property allows you to review, schedule, and exchange properties of physical and non-physical properties in the block chain. Physical examples of smart products include vehicles, phones and homes that can be activated, deactivated, monitored and managed.

Blockchain Internet-of-Things

Blockchain technology is the ideal engine for a relatively new concept in our new connected world: the Internet of Things. Internet Internet spending is expected to exceed $ 1 billion over the next few years. This opportunity will be offered to Blockchain Internet of Things to intervene and deliver the final system to track the unique history of billions of smart devices being released in the coming years.

Blockchain Act

Programmable and Self-Leading Contracts

In the block chain law applications, smart contracts are controlled in the chain block, which allows programmable, self-executable and self-forgiving contracts. The Blockchain Act also incorporates the idea of "Corporate Smart", which includes concepts such as Decentralized Autonomous Companies (DAC) or the Decentralized Autonomous Corporation (DAO).

Music Blockchain

Blockchain's application is music applications that permits a shift in a way that artists can control their musical functions or tasks. From ownership to rights and rights payments, blockchain technology applications enable artists to expand ownership of their work for the first time.

Block of Real Estate

Blockchain technology will inevitably become a fundamental pillar of the real estate sector. In a sector based primarily on paper documents, the chain of building blocks allows unprecedented improvements in document archiving and archiving. Using blockchain applications in some methods or some tasks like payment, and security can also reduce error, increase financial privacy, accelerate transactions and internationalize markets.

Blockchain Identity Secure and Secure Identity Check

Blockchain identification applications provide verification, authorization, and identity management without modification, resulting in significant efficiency and fraud reduction.

Digital Blockchain Identity

Blockchain technology is the ideal engine for improving digital identities. As digital identities emerge as an inevitable part of our networked world, the way we protect our online information is under control. Blockchain-based identity systems can provide a solution to this problem with advanced cryptography and distributed MASTER BOOKS.

References

1. Satoshi Nakamoto. “Bitcoin: A Peer-to-PeerElectronic Cash System” www.bitcoin.org
2. Matthew Vilim, HenryDuwe, Rakesh Kumar.“Approximate Bitcoin Mining”.Ieeexplore.ieee..org/document/7544340/
3. Ariel Ekblaw*, Asaph Azaria*, John D. Halamka,MD†, Andrew Lippman. “A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data”.
4. J.D. Bruce. “Purely P2P Crypto-Currency With FiniteMini-Blockchain”.
5. Marco A. Santori, Craig A. DeRidder and James M.Grosser .“Blockchain Basics: A Primer”.
6. Robert Courtneidge “Bitcoin and BlockchainTechnology Update: Research Paper”.
7. BitFury Group. “Digital Assets on PublicBlockchains”.
8. Michael Crosby, Google, Nachiappan, Yahoo,Pradhan Pattanayak, Yahoo, Sanjeev Verma,Samsung Research America, VigneshKalyanaraman,Fairchild Semiconductor “BlockChain TechnologyBeyond Bitcoin”.
9. Updated Bitcoin Information:http://www.weusecoins.com/.
10. Official Bitcoin Forums: https://bitcointalk.org/