iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 8 **Issue:** VI **Month of publication:** June 2020

**DOI:** http://doi.org/10.22214/ijraset.2020.6329

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 8 Issue VI June 2020- Available at www.ijraset.com*

# Survey on Blockchain: Backbone of Cryptocurrency

Varsha I G[1], Prof. J .Nagesh Babu[2], Prof. Puneeth G J[3]
[1, 2, 3]*Dept. of Computer Science & Engineering, RYMEC, Ballari, Karnataka, India*

***Abstract:*** ***Technology like Blockchain is fast growing among other technologies that are now explored into various fields including services in finance, services in land holdings, department of health, academic organizations and many more. Crypto currency is a biggest shift towards assets online which is tradable. It is built with Blockchain as the backbone technology where trading takes place only online. Digital Wallets on computers or smartphones are used to store crypto currency. Using these digital wallets crypto currency transactions can be made. Every transaction is stored in a block that are chained together to form Blockchain. This paper, "Survey on Blockchain: backbone of Cryptocurrency", is a detailed survey on Blockchain and its applications.***

***Keywords: Blockchain, Cryptocurrency, Decentralization, Proof-of-Work (PoW), Consensus***

## I. INTRODUCTION

Before Internet, Banking System was completely based on manual work. Physical ledger books were used for book keeping of customer accounts, transactions, loans and the like.

With the advent of Internet, Banking System has now moved online. Book keeping physical ledger has become an online copy of records. Each bank will have its own website and the customers are given username and password which they can change later on. Using this username and password, they can login to the bank's website and perform any transactions.

The issue with the Banking System having moved online is that the customers are required to provide their identity while performing any transaction. This identity is used by the respective bank to authenticate the user and to maintain ledger. The provided identity may include customer name, account number, recipient's details, mobile number, and any identity card number.

But Internet is also full of hackers who look for any chance to collect the available information in transit and use it for illegal activities. The details provided by customers to perform transactions can be acquired by these hackers even when there is security in place and their accounts can be hacked. And hence banking online has become a major security concern even though there are many advantages of it.

To overcome this drawback, the idea of online currency known Crypto currency was introduced. Crypto currency uses strong cryptographic algorithms to monitor and secure the crypto currency transactions. Crypto currency is a decentralized system based on blockchain as against current banking system which is based on central banking system using centralized digital currency.

Crypto currency uses distributed ledger technology known as blockchain. Through blockchain all financial transactions are publically made visible.

Blockchain was first introduced with Bitcoin in the year 2009. From then on it has been explored in various applications including health, real estate, financial institutions, academia and many more.

Main aim of blockchain is to decentralize the transactions over the Internet. A blockchain will be constituted of list of blocks which will be chained together. Each block is made up of a bundle of transactions that are verified and placed together. The transactions that add up to a block are determined by the volume or size that is set for the block. Each of these transactions in a block is digitally signed by the sender node. Any participating computer / smartphone in the network is a node.

Few connected nodes in the network which are known as miners, use their powerful high-end machines and electrical energy to solve complex puzzles of cryptography to gather new transactions into the block and add newly created block to the ongoing chain of blocks thus creating a blockchain. Miner will then get a reward for his work.

Blockchain can either be a *Private or Public.* In Public blockchain also known as Permission less chain, any node can register itself and become a miner. In Private network also known as Permissioned, blockchain is private or confined to an organization and only chosen nodes can act as miners.

Following sections discuss some of the features and related work in the field of Blockchain.

©IJRASET: All Rights are Reserved

## II. BLOCKCHAIN AND ITS FEATURES

Blockchain has the following features associated with it:

*A.* Blockchain is a distributed ledger. Because it is distributed in nature, there is no question of a single system failure which can disrupt the whole system.
*B.* Blockchain is immutable in nature. For a block to be manipulated, all the copies of the chain in the entire network must be manipulated. There are many participating nodes and hence multiple copies exist. Therefore, it is virtually impossible to manipulate.
*C.* Transactions are completely secured since there is no involvement of any third party in the whole process.
*D.* Transactions are completely transparent in nature. The transaction that a sender sends to the receiver is recorded in the chain and everyone can view it.
*E.* Blockchain systems have higher reliability since data is available at different nodes in the network.
*F.* Blockchain systems are efficient over traditional databases.
*G.* Transaction time over the blockchain network is very low compared to traditional databases. No paper work or any regulations are involved.

## III. BLOCKCHAIN AND ITS ENTITIES

Following are the entities involved in a blockchain

*A.* Blockchain will have *User* who can initiate transactions. There is a pair of the Private and the Public that the user uses to encode and decode the transactions for verification.
*B.* Blockchain will have *Miner* who can add blocks to the blockchain after solving the difficult cryptographic puzzle.

## IV. BLOCKCHAIN AND ITS WORKING

Blockchain is based on a simple P2P network and works by simple broadcasting of transactions to the network in the following manner:

*A.* User will request for a transaction to be made.
*B.* Transaction after being signed by sender will be broadcast to peer-to-peer network. This network will consist of miners or nodes.
*C.* The transactions will be verified by the nodes in the network using a predefined network.
*D.* The transactions will then be grouped into block and added to the existing blockchain, and this completes the transaction.

## V. PRESENT BANKING SYSTEM

In the current Banking System, currency is regulated centrally by Central Bank of the country. This currency maintained by central authority is known as *Fiat currency*. In the days today, banking is in full swing moving towards digitalization. Gone are the days when people were supposed to go to banks to collect cash, make deposits or make any other transactions.

With the advent of ATMs people can now collect and deposit money without having to go to banks. Internet was accessible by most by mid 1990s. With this came online banking when people started to use their smartphones to carry out transactions online. People can now make payment to any service provider, book tickets online, and pay bills by means of digital banking.

Though digital banking comes with many advantages, it has a list of drawbacks to be addressed:

*1)* The prominent drawback is related to security of *customer information being transmitted* over Internet: users' login to the desired login page to perform any transaction providing details about their name, account number, mobile number and any other identity card number. This information being transmitted can be acquired by hackers who can crack security in place and use the information for illegal activities.
*2)* Fiat currency, the currency which is controlled by Central authority is considered to be stable. But it is exposed to economic recessions and it has been observed in the past. This creates the need to create, to develop and use cryptocurrency that is not going to be controlled or governed by any central system or governing body.
*3)* Another drawback is the *transaction fees* which is high and also varies for different types of transactions.
*4)* Also, *cross-border* transactions charge exchange fees rates.

In some cases, transactions may take days to get settled.

©IJRASET: All Rights are Reserved

## VI. BANKING WITH BLOCKCHAIN:

Drawbacks of current Banking System listed in the previous section makes the concept of Crypto currency as the future means of transacting over Internet.

Crypto currency uses strong cryptographic algorithms to monitor and secure the crypto currency transactions. Crypto currency is a decentralized system based on blockchain as against current banking system which is based on central banking system using centralized digital currency.

Some of the advantages of Crypto currency are listed below:

*A.* Crypto currencies are not under the control of any system or governing body such as a Central Bank. These cryptocurrencies are transactions available in blockchain which are virtually impossible to modify.

*B.* In crypto currency people do not share their identity information while performing transactions. So, security aspect provided by crypto currency is major plus.

*C.* Crypto currencies are easily available online for those who want to buy them.

*D.* Transactions through central banking system collect high transaction fees, whereas in crypto currency optional transaction that is collected is a very low.

*E.* Transaction settlement times in crypto currency is much faster compared to the transactions through central banking system.

## VII. BLOCKCHAIN AND ITS RELATED WORK

### *A. Nakamoto, Satoshi. (2008): [1]*

Bitcoin, the first of Cryptocurrencies that was introduced by Santoshi Nakamoto in the year 2008. It was introduced with the help of peer-to-peer network system. This P2P system of network will eliminate double spending. Proof-of work, PoW, was made use by nodes connected in the network, that were known as miners to add new transactions to the public ledger. To resolve any conflicts in the network among the nodes, consensus algorithm was used. Nodes in the network use their high-end machine powers to keep the system alive by adding transactions.

Following is the summary of how the network works:

*1)* Newly initiated transactions will be sent to each the network node.

*2)* Every node that is participating then accumulates all the transactions into block, according to block size.

*3)* Nodes who are known as miners then start working on complex PoW for the new block.

*4)* The miner who gets the PoW solved sends the block to all the peer nodes in the system.

*5)* Rest of the nodes in the network check if each of the transaction contained in the block is valid and also check if the currency is not already spent; if all the transactions are valid, they will accept the block.

*6)* Nodes now prepare themselves to work on the next set of transactions that is going to be added to the block and hence blockchain. They will use hashing of the collected block as the hash of the preceding hash.

### *B. Ghimire, Suman, and Henry Selvaraj. (2018): [2]*

This paper is a detailed survey of various terms that are used in Bitcoin, created in 2008. It covers topics like blocks, blockchain, mining details used, proof of work etc. Following section discuss each one of them in detail.

*1)* *Blocks and Blockchain:* Blockchain was first introduced in 1991. This was made possible by member group of researchers and it was mainly supposed to timestamp documents on digital platform. Time stamped digital documents cannot be tempered. Blockchain is series of chains that are linked to each other by each block holding the hash of previous block.

*2)* *Mining:* Nodes known as miners are responsible for securing Bitcoin system. Miner can be node in the network. Several kinds of hardware's are tried and tested for mining blocks in the network. All this hardware requires high electric energy to mine a block. High end machines are used by miners to solve complex puzzles. Once solved the block will be attached to the blockchain and sent to all the nodes in the network. So, mining is basically solving complex puzzle known as PoW and add the block after solving PoW to the ongoing chain of blocks containing all the past transactions.

*3)* *Proof of Work:* The miners in the network do not work on individual transactions at a time. They collect newly initiated transactions into the block. The miners then try to mine this newly created block. The mining process of a block includes calculating the hash of this newly created block and incrementing the counter value. This counter is known as nonce. This nonce will be added in the block. The value of nonce will be started from the value 0 for every transaction and incremented for

©IJRASET: All Rights are Reserved

each unsuccessful hash that is calculated. Once the right hash is calculated for the newly created block, the successful miner will then be sending the newly framed block to rest of the nodes present in the network system after adding this newly created block to chain of ongoing blocks that contain all the previous transactions carried out till date. The speed with which the miner solves this hash depends upon the computational power he is possessing.

4) *Conclusion:* Bitcoin has been the talk of the town after its invention. In the recent days it has got great attention from the researchers all over the world, and many alternative currencies have emerged since then. Blockchain, the backbone of Bitcoin has been experimented in various other fields till today and is in full bloom because of its security.

*C. DeVries, Peter D. (2016): [3]*

In this paper, the analysis of Bitcoin is presented in terms of its strength, weakness, opportunity and threat. These four aspects tell whether Bitcoin can be a future drastic shift towards crypto currency.

1) *Strength:* Bitcoin has a great strength when looked from various perspectives. It is well secured against hackers; in that it is virtually impossible to alter the copies of blocks that spread across the network on various nodes. Moreover, Bitcoin and rest of crypto currencies are considered to be protected against economic crisis. They are not affected by any changes or restrictions imposed by the governing bodies in the country.
2) *Weakness:* When it comes to weakness, there are few weakness points in Bitcoin that are to be bared. The public ledger in the name blockchain is shared with everyone in the network, so it is exposed to attack, but quick access nature of the Bitcoin has prevented this from happening. And moreover, the network is not designed to handle high transaction rates because each block is made to be added every 10 minutes.
3) *Opportunity:* The transactions involving central core banking system is affected by the transaction fees it collects for each transaction that is made. For every transaction, the fees collected are high. And also, the transaction settlement can go up to days in central banking system. In crypto currency these transaction fees are eliminated and the sender can optionally provide any desired fees for the miner who gets to solve the puzzle. Also, in central banking system, each transaction is governed by many restrictions imposed by central authority. In the case of crypto currency simple P2P networks are used which will speed up the whole process. Moreover, there is no central authority to impose any restrictions. Because of these opportunities, the crypto currency is gaining more and more attention in the days.
4) *Threat:* Bitcoin is having a few road breakers to address. There are quite a few laws that say how Bitcoin for that matter how crypto currency needs to be accepted and used. Therefore, startup companies think before they try to enter the market of crypto currency. Today, there not only exist Bitcoin, but several competitors have entered the market. Several big companies are trying to enter the industry with their own crypto currency. So, Bitcoin will have its own difficulties facing these competitors with high face value in the market.

*D. Gazali, Haneffa Muchlis, Che Muhamad Hafiz Bin Che Ismail, and Tamrin Amboala. (2018): [4]*

This paper helps one understand the need to invest in crypto currency in the near future. The study shows that the attitude of people towards crypto currency is changing in the recent years. And also since crypto currency is tolerant to risks involved in financial economics people are thinking to invest in crypto currency. Lower transaction fees are one of the benefits users can get from using crypto currency. It only takes few minutes to transfer currency from sender to receiver as against the central banking system which can take many days for settlement. All these are the motivations that motivate people to invest in crypto currency in the near future. Based on these intentions, a model for conception is proposed in the paper.

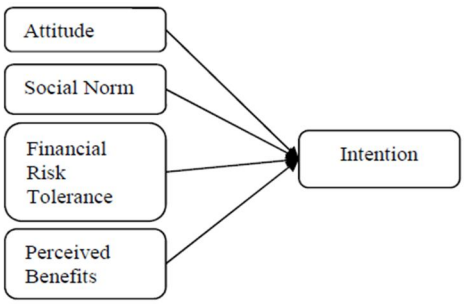



Fig1: The Conception Model

©IJRASET: All Rights are Reserved

*E. Alzahrani, Saeed, and Tugrul U. Daim. (2019): [5]*

The number of studies discussing the cryptocurrency adoption factors is low and there is lack of publications looking into the cryptocurrency from multidimensional view. This paper used Hierarchical Decision Model (HDM) to address multidimensional assessment of the adoption decision.

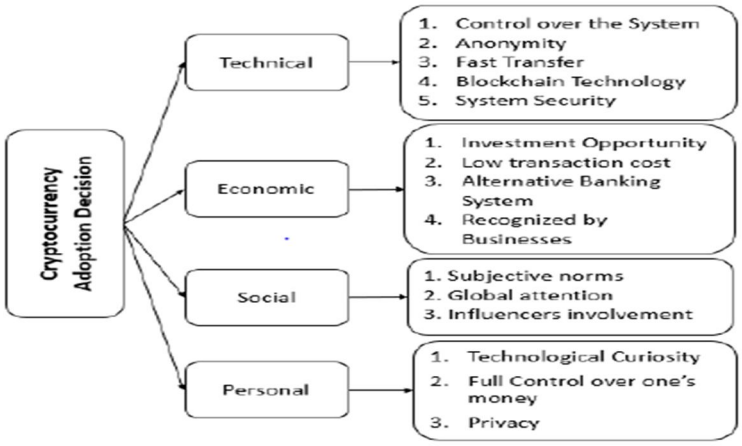



Fig2: HDM

*F. Lee, Jong-Hyouk. (2019: [6]*

This paper compares various crypto currencies for anonymity. Anonymous is the nature of crypto currency that removes the need to provide identity information of the sender and the receiver. Anonymous crypto currency crypto currency provides the following features:

1) *Privacy:* Crypto currency ensures that the sender, receiver and transaction currency details are not modified by any dishonest nodes in the network.
2) *Not Traceable:* Crypto currency ensures that the currency that is sent by the sender and the receiver are virtually not possible to traceable and also cannot be linked with the previous transaction details.
3) *Interchangeability:* Crypto currency makes sure that all the coins are indistinguishable and thus they are interchangeable.

| | Bitcoin | Dash | Monero | Verge | PIVX | Zcash |
|---|---|---|---|---|---|---|
| Origin | - | Bitcoin | Bytecoin | Bitcoin | Dash | Bitcoin |
| Release | January 2009 | January 2014 | April 2014 | October 2014 | February 2016 | October 2016 |
| Consensus algorithm | PoW | PoW | PoW | PoW | PoS | PoW |
| Hardware mineable | Yes | Yes | Yes | Yes | No | Yes |
| Block time | 600 s | 150 s | 120 s | 30 s | 60 s | 150 s |
| Rich list | Yes | Yes | No | Yes | Yes | No |
| Master node | No | Yes | No | No | Yes | No |
| Sender address hidden | No | Yes | Yes | No | Yes | Yes |
| Receiver address hidden | No | Yes | Yes | No | Yes | Yes |
| Sent amount hidden | No | No | Yes | No | No | Yes |
| IP addresses hidden | No | No | No | Yes | No | No |
| Privacy | No | No | Yes | No | No | Yes |
| Untraceability | No | No | Yes | No | No | Yes |
| Fungibility | No | No | Yes | No | No | Yes |

Fig3: Comparisons of Crypto Currencies

©IJRASET: All Rights are Reserved

*G. Balaskas, Anastasios, and Virginia NL Franqueira. (2018): [7]*

This paper examines various analytical tools based on blockchain. It gives a detailed report based on the analysis carried out in different environment. Each analytical tool is examined to check their effectiveness in investigating crimes in cyber security.

| Thematic Taxonomy | Features | Tools |
|---|---|---|
| *Analysis of Relationships* | Transaction Graph Utilised for Address Clustering | • BitIodine<br>• Blockchain.info<br>• BitConduite |
| | Wallet Explorer Proprietary Database | • Chainalysis<br>• Elliptic |
| *Analysis of Metadata* | OP_RETURN | • OpReturnTool |
| *Analysis of Money Flows* | Transaction Graph Utilised for Address Clustering | • BitConduite<br>• BitConeView |
| | Address Tagging | • Blockchain.info<br>• Bitcointalk.org |
| *Analysis of User Behaviour* | Profile Rules | • Blockchain Inspector |
| | Risk Assessment | • Chainalysis |
| *Analysis of Transaction Fees* | Transaction Graph | • Blockchain.info<br>• Coindesk.com<br>• BitConeView<br>• BlockSci |
| | Exchange Rate | • Blockchain.info<br>• Coindesk.com<br>• BlockSci |
| *Analysis of Market / Wallets* | Transaction Graph | • Blockexplorer.com |
| | Trade Data | • Bitcoincharts.com |

Fig4: Analysis of Analytical tools based on blockchain

*H. Patel, Raj, Akhil Sethia, and Shyam Patil. (2018): [8]*

Blockchain as a technology has evolved greatly over part few years. It can completely eliminate the need to have third party system monitoring the currency. Blockchain has given rise to a new business online where people can make revenue out of it. Blockchain in crypto currency enables the development global currency that can be accepted by all the governing bodies across the globe. Many industries are coming forward to experiment with blockchain in fields that not only includes finance but also health; real estate etc. ruling out the need for third party authority to monitor transactions and the currency, blockchain brings new reformation to the financial industry. Blockchain will be completely dominant in the financial organization. It also eliminates the need to store huge amount of data and also reduces paper work and removes any other regulations. Internet of things is gaining huge popularity for connecting all the objects to the Internet. But it has issue with organizing its huge data that is produced by various sources. Blockchain can provide a way for such a huge volume of data to be stored and analyzed properly and further security is provided to all the stored data.

Blockchain can give a new phase to the Internet era which would benefit many across the globe. Blockchain However, Blockchain will provide more security and privacy to Internet in the future days. Along with the benefits that the Blockchain provides to various other base technologies, it can have its own issues and problems that get needed to be addressed. There must be proper laws that must be implemented to regulate its proper usage. With all the issues addressed, Blockchain can be next major revolution after Internet in the recent future dominating all the areas of domain.

*I. Lucas, Bouvarel, and Rafael V. Páez. (2019): [9]*

This paper discusses two most commonly used algorithms for consensus that will be used with blockchain technology.

1) *Proof of Work:* This algorithm for consensus is based on solving a complex puzzle that is based on cryptography. Whichever node will be able to solve the puzzle will be able to add the newly created block for the end of the ongoing chain in the network. The puzzle will be a complex problem that involves calculating the hash of the block that will need to be added to the chain repeatedly until desired output is obtained. On receiving a new set of transactions, the nodes that are participating in the network jump to solve puzzle so that they will be able to add the newly created block for the end of the chain. However, only one node which resolves the puzzle first will get a chance to add the block for the chain, rest of the participating nodes in the network system, will agree to the new chain and accept it after verifying the transactions. The winner node will get a reward in terms of crypto currency for solving the puzzle. Solving this puzzle cannot be done by using normal system it requires high end machines with properly equipped hardware and also it consumes more CPU power and electric energy.

©IJRASET: All Rights are Reserved

2) *Proof of Stack:* The PoS consensus algorithm is based on the amount of crypto currency that a miner holds in the network. The more the crpto currency held by the node, the more is the chance of him getting the right to add the newly created block to the chain. But this system is biased towards the miners who hold more currency in the network.

| Criteria | PoW | PoS |
|---|---|---|
| Energy efficiency | No | Yes |
| Modern hardware | Very important | No need |
| Forking | When two nodes find the suitable nonce at the same time | Very Difficult |
| Double spending attack | Yes | Difficult |
| Block creating speed | Low, depends on variant | Fast |
| Pool mining | Yes, but it can be prevented | Yes, and it is difficult to prevent |
| Example | Bitcoin | Nextcoin |

Fig5: Comparison PoW and PoS

*J. Hazari, Shihab Shahriar, and Qusay H. Mahmoud. (2019): [10]*

For each set of the new transactions that arrive, each miner in the network collects the arrived transactions into new block later try on solving the complex cryptographic hash for the block so as obtain the right to add the block to the chain at the end.

The identical information used by all the miners in the network is crypto currency index, previous blocks' hash value and the time created.

The nonce value chosen by each miner may be different, so that the work performed by each miner will be different.

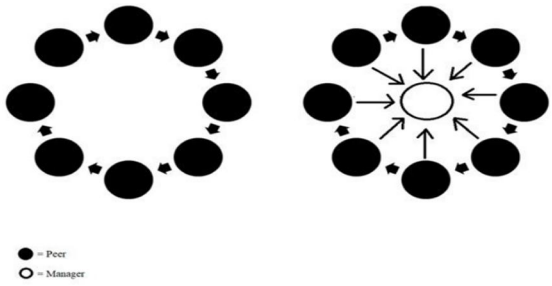
This paper proposes a method to appoint a new manager every time a new block is created. The job of manager is to provide a nonce accordingly that the miners will not be using the same nonce for block.

Managers chosen for each new block will be different. Manager should also be providing the hash of the transactions of the particular block in addition to providing the nonce.

In normal crypto currency system, the all different nodes will be either directly hooked to each one or through the other node. In the system that is proposed here, in this paper, each node will be connected to every other node in the network; in addition they will also be connected to the Manager.

Genesis block in the system will be created in normal way, where every node will compete to solve the puzzle and add the block.

The node that gets to solve the puzzle and the block to the chain first, will be chosen as a Manager for the next block in the system of network and procedure is followed for the remainder of the chain.




*K. i Munoz, Jordi Zayuelas, Jose Suarez-Varela, and Pere Barlet-Ros., (2019): [11]*

Crypto currency became a major technological twist by the end of 2017 and starting of 2018. Many people started to take part in the network as miners to append the blocks for the end of the chain. But this also attracted cyber criminals. They started to attack other systems in the network. These cyber criminals started to infect other machines in the network and started to use these machines to mine crypto currency without spending any amount to purchase the machines. This situation is known as crypto jacking. This crypto jacking has become a major problem in the field of cyber security and needs to be addressed. This crypto jacking has negative impact on the infected machines and can reduce their life expectancy. So it is necessary to detect all such dishonest miners in the network.

©IJRASET: All Rights are Reserved

Miners having little computational power often come together to form a mining pool. Upon solving the cryptographic hash of the puzzle, they divide the received reward between them. This pool of miners can be detected by scanning the IP addresses list from the known crypto currency mining pools or they can also be detected by going through the DNS queries posted by such pool of miners. Theses 2 methods of detecting the mining pools work only when they are connected to the servers that are known.
Another method is, DPI can be used to check through the traffic and identify some of the commonly and well-known signatures in these mining pools. But performing DPI is not feasible in the real time network traffic, because it is very expensive and requires proper administering infrastructures. And also, miners can bypass all these by trying to connect to the server using Virtual Private Networks.
This problem can be addressed by using machine learning based solution that is based on NetFlow/ IPFIX. It can be used to measure flow level traffic of mining in the network and detect dishonest miners.

*L. Baek, Hyochang, et al. (2019): [12]*
The main motto behind this paper is to study wallets implementing crypto currency that carry out anomalous transactions and to detect any suspicious transaction being made.
The overview of steps carried out in the paper is shown below in the diagram.

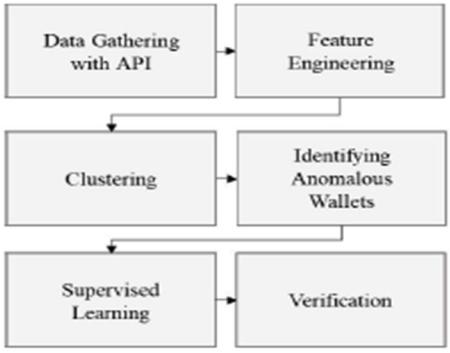



Fig6: Anomaly detection for crypto currency

*1)* The API in python is responsible for collecting all the data of crypto currency.
*2)* The features are then extracted from the data collected using some of the preprocessing techniques.
*3)* The unsupervised learning method then performs the clustering the data based on the features extracted.
*4)* Each cluster is identified by a different wallet and is given names (labels) accordingly.
*5)* RF technology is then performed to distinguish between the anomalous transactions and is finally verified.

Features that were identified from the data collected are:
*a)* The average of the value of difference between value of the difference between the earlier and the preceding transaction.
*b)* The variance value of the above feature is computed.
*c)* The standard deviation calculated from the amount that is added to the wallet.
*d)* The standard deviation of the amount withdrawn from the wallet is computed.
*e)* The average value of the amount that is transacted from the wallet is taken to consideration.
*f)* The difference between the earlier transaction and the transaction the follows is computed.
*g)* The balance available in the wallet is taken into consideration.

*M. Scholar, P. G.: [13]*
Crypto currency has provided a great opportunity and offers many challenges to the current financial organization.
College fees payment is one of the types of transactions involved in current system. Many different ways can be used to pay the fees. It can be either cash, cheque, credit card, debit card or any other means. But this type of transaction has to go through intermediaries to transfer money from sender to receiver.
This paper proposes a system that will be on technology which is blockchain which is proposed to fulfill the need to pay college fees directly to the college without going through any intermediaries.

©IJRASET: All Rights are Reserved

This system makes use of digital ID using which the sender can track all his information. Smart cards are used to secure transactions. In this way student can pay fees to the college directly without going through intermediaries that includes banks and other organizations. In this way fees payment has been made secure, fast and requires no extra amount to be paid for the intermediaries in the form of transaction fees. Following diagram shows the proposed system:

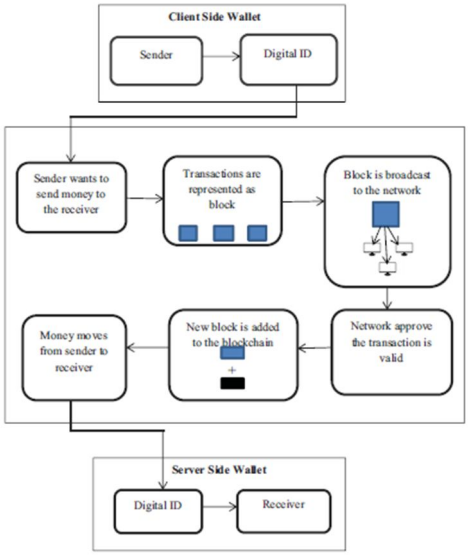



Fig7: College Fees System

*N. Yu, Shitang, et al. (2018): [14]*

On a daily basis more and more devices are getting attached to the Internet. All the devices together that are connected to the Internet are known as Internet of Things (IoT). Huge volume of data is produced by these devices that are connected together on a daily basis. This data is useful and can yield great amount of useful information. This big data is really big and difficult to manage. Processing this data requires a necessary platform so as to efficiently transfer and use the valuable information provided by the data so as to improve performance of the concerned industry.

Traditional database system is not capable of holding this huge data in of its currently available data types. So, there is a need to shift from the current traditional database system to another system which facilitates processing of this massive amount of data.

This paper tries to address this issue with big data using blockchain and smart contract technology. This enables the intelligent devices shift towards data-oriented platforms from traditional databases.

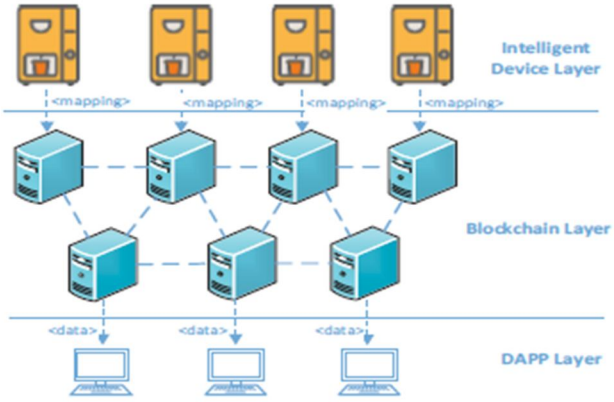



Fig8: blockchain model for IoT

Technologies used are

*1)* Distributed network architecture.
*2)* IoT Device Nodes mapping system.
*3)* PBFT-DPOC algorithm for consensus

©IJRASET: All Rights are Reserved

*O. Latifi, Sobhan, Yunpeng Zhang, and Liang- Chieh Cheng. (2019): [15]*

Real Estate (RE) investment is one of the fields where money can be invested safely. It ensures security to investors in that it is not concerned with inflation in money. Not only experts but anyone can make investment in real estate and can benefit from it.

The way business is carried out with RE is complicated, costly, non-transparent and highly inefficient. Real estate investments are dominated by some institutions or the rich people in today's market. In addition to this problem with the current system, it is also difficult for real estate business to improve upon its current core system which is efficient and user friendly for fresh users.

Commercially people involved in the system are facing difficulties with old technology which is obsolete, and also data sharing is the biggest issue.

Also, cash flow and transaction data processing is problematic with current real estate system. Only people with experience can operate the system which is a major drawback.

To overcome these issues, the system based on technology known as blockchain and smart contract is proposed in this paper. Combination of these two technologies provides for a secure and easy investment in the field of real estate even for common people.

The ideal method as offered in the paper is:

*1)* Firstly, an ICO- initial coin offerings, is made into the system. Investors are then invited to invest into the system. The money collected from ICO is used to buy real estate assets.

*2)* The assets that are brought are then tokenized. These tokens will be associated with certain values and given to the investors. The price value of the tokens can be changed over time.

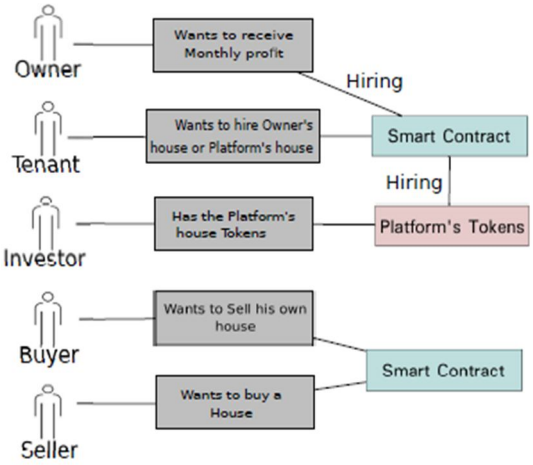



Fig9: entities in real estate

*P. Kuzlu, Murat, et al. (2019): [16]*

This paper focuses on one in every of the foremost blockchain frameworks that is open source known as Hyperledger Fabric. The performance of a blockchain platform which is impacted by network workload is evaluated in terms of: (a) throughput, i.e., successful transactions per second; (b) latency, i.e., response time per transaction in seconds; and (c) scalability, i.e., number of participants serviceable by the platform.

The AWS EC2 instance comprising of 16 CPUs, 3.0 GHz Intel processors and 32GB RAM is used as testing condition to evaluate the blockchain framework.

In conclusion, with the given test environment it was discovered that the blockchain network is capable of supporting up to 200 transactions per second. It was discovered that this transaction rate was supported without much of latency i.e. the response time taken for each transaction per second. It was identified and tested many times that blockchain network could be able to support up to 1, 00,000 number of transactions in a second at 200 transactions per second. 1, 00,000 transactions per second means 1 lakh participants can participate in the system at the same time. In the experiment conducted it was observed that the average response time for query was less than 0.01 and average response time for open transaction requests is less than 0.16. But it was also studied and observed that simultaneous transactions had greater impact on the response time per second and the number of transactions that were executed per second.

©IJRASET: All Rights are Reserved

*Q. Kolekar, Sachin M., et al. (2018): [17]*

This paper is a survey on various elements that constitutes that blockchain. Concepts discussed are:

*1)* Public blockchain
*2)* Private blockchain
*3)* Distributed Ledger
*4)* Consensus
*5)* Proof of Work
*6)* Proof of Stake
*7)* Mining
*8)* Block
*9)* Chain

Detection system for intrusion and detection system for network are discussed in detail throughout this paper.

*R. Kshetri, Nir, and Jeffrey Voas. (2018): [18]*

Blockchain is an emerging technology and it has been tested in e-voting. The main thought behind e- voting which is based on blockchain system is making use of online currency. Each voter in voting enabled by blockchain will be made available with digital wallet. The digital wallet will contain credentials for the user. Each user will be provided with one digital coin. Using the digital coin, the user can vote only once. Once the user makes the vote his single digital currency will be transferred to the digital wallet of the candidate. However, even after making the vote the user can change their voting decision before the predefined deadline to vote for another candidate. Bad access to voter and frauds are the major concern in the current voting system. These drawbacks are addressed by the voting system enabled by the blockchain. Since all the voting are made through the system that is based on blockchain, all the voting will be visible to public and hence cannot be altered without others knowing and hence difficult to manipulate. Also, each vote will be wrapped within the block and blocks are connected together through hashes. So, changing a block would require one to change all the subsequent blocks which is difficult. The online voting system has each vote that is attached to the user digital wallet address and the vote that is cast, so it becomes immutable system for anyone to hack.

This system has been tested by various startup companies across the globe and it has been observed to be performing with great performance and good user rating and experience.

*S. Homayoun, Sajad, et al. (2019): [19]*

This paper proposes a system enabled by blockchain for malware detection. This system is used to detect any Framework (B2MDF) to detect malign mobile applications that are present in mobile application store. The system based on blockchain for detection of malware uses internal and external permissioned blockchains. These two permissioned blockchains form a dual private blockchain. Consortium blockchain is used for the final decision. Feature extraction is used to extract features from the permissioned blockchain. Detection engines are used. These engines are supplied with the extracted features. The detection system determines if the application is malign based on the extracted features. The consortium blockchain is used. This blockchain provides the output, the final end result by analyzing output from all the detection engines.

*T. Wutthikarn, Ruksudaporn, and Yan Guang Hui. (2018): [20]*

This paper has proposed a framework for sharing patient's dental health care from one hospital to another and allows for recognizing each patient to facilitate subsequent treatments. The entities that participate in the workflow include Participants: Patient, Dentist and Clinic. Assets: Prescription and Contract. Functions and Transactions: Treatment Interview, Treatment Plan, Treatment Fee, Treatment Receive along with transaction id and timestamp.

Fig10: Work sequence for dental application

©IJRASET: All Rights are Reserved

*U. Chowdhury, Mohammad Jabed Morshed, et al. (2018): [21]*

Technology like Blockchain has become the backbone of Cryptocurrency and it is in full bloom in the recent years. As opposed to the traditional database, blockchains store data in distributed nodes in the network. This paper surveyed various scenarios to understand the differences between blockchain technology and traditional database.

| Problem | Blockchain | Traditional Database | Preferred |
|---|---|---|---|
| Trust | No third party | Central trusted party | Blockchain |
| Data Confidentiality | All nodes can see data | Only central authority | Database |
| Fault Tolerant | All nodes have data | Only central authority | Blockchain |
| Performance | Takes time | Immediate action | Database |
| Redundant Data | All nodes have data | Only central authority | Blockchain |
| Security Featues | Cryptographic hash functions used | Basic access control mechanism used | Blockchain |

*V. Raghuwanshi, Sandeep, R. K. Pateria, and R. P. Singh. (2009): [22]*

Mathematical modeling system that is used in verifying the payment integrity and order details of digital purchase is proposed in this paper. External party verification system is used. This external system uses mainly 2 kinds of information from buyer also the merchant and integrity are verified between them.

Following are sequence of steps that gets executed during transaction:

*1)* The buyer gets the digital certificate after opening an account.
*2)* Similarly, merchant will get his digital certificates.
*3)* Buyer will open the web site owned by merchant and order details will be placed by the buyer.
*4)* Merchant will verify the buyer using buyer's signature which is digital through the help of organization used for payment.
*5)* Organization for payment would check the integrity for the order with the help of the proposed protocol model and authorizes buyer.
*6)* Merchant then check list all the purchases and the order are confirmed.

*W. He, Yongqiang, Yanrong Shi, and Aixiang He. (2010): [24]*

The three main online systems used for payment are as follows: e- card for credit, e-cash and e-check are discussed in this paper along with their respective application environment.

The traditional payment system is the weak part in the development of electronic commerce system; market still relies on traditional payment system even when online payment has advanced. Development of market is further affected by security, credit and other issues. Technological advancement has made these online systems to flourish and be more useful to people. They are used in almost all platforms for making payment in a secured manner. e-card for credit, e-cash and e-check are becoming more and more popular with people. As these technologies are used more and more, it becomes urgent need to do lot of research in these areas and develop versatile systems.

*X. El Haddad, Ghada, Esma Aïmeur, and Hicham Hage. (2018): [24]*

Customers will have to send their individual information along with financial information through Internet in order to purchase or pay for a service. Online payment has three concerns that need to be addressed: Trust, Security and Financial Fears. These three factors are surveyed in this paper. The work in this paper developed a research model that defines several features that affect the people's online payment decision making.

©IJRASET: All Rights are Reserved

Some of the hypotheses that were drawn from the research model are as follows:

*1)* Display of security signs on the website
*2)* The website ease of use
*3)* The website information quality

*Y. Wang, Zhiran. (2011): [25]*

Considering the drawbacks of existing online payment system, this paper has developed cloud computing based online payment system that has organizational, technical and business process.

*1) Organization Structure Includes*
*a)* Bank information center,
*b)* Financial permissioned cloud,
*c)* Industry systems,
*d)* Logistics systems and
*e)* Government systems

*2) Technical Structure Includes*
*a)* Physical layer,
*b)* Virtualization resource layer,
*c)* Service resource layer and
*d)* User resource layer

*Z. Ebadi, Zahra. (2007): [26]*

In order to address the ever-growing customer needs, the Banking system is looking for a future way to improve customer's experience with banking system and to make it more convenient. This paper proposes the features and architecture of Centralized system operation and process up gradation through automating with the help of central banking system applications and Internet Protocol driven networks.

Banks are now able to provide online delivery systems or applications like Internet Banking system, Telephonic system also Automated Teller Machines with the help of Core banking solution.

*AA. Xue, Tengfei, et al (2018): [27]*

In Proof of Work (PoW) based blockchain implementation enormous amount of energy is spent in solving the difficult puzzle. PoW also requires expensive mining equipment.

In this paper a new consensus protocol "Proof-of-Contribution (PoC)" for cryptocurrency is proposed. It is built on existing protocol used for Bitcoin. Energy usage for mining process is reduced by Poc algorithm by means of providing reward.

PoC is based on Pow and PoS. Honesty of miners is represented in terms of successful times. It then is used as trump in adjusting the difficulty level in mining process of PoC. Poc is good towards obedient miners and the miners will get difficulty rewards when they no more get mining reward for mining as well as regular mining fee that will be boosting to miners. PoC also penalizes malicious behavior.

*BB. Nakahara, Ryoya, and Hiroyuki Inaba. (2018): [28]*

PoW is the backbone algorithm for consensus which is implemented in Bitcoin. It prevents double spending but encourages mining pool to centralize computing power in the network. This leads to "majority attack" issue. To overcome this problem, a Fair PoW algorithm is proposed in this paper.

In Fair PoW consensus algorithm:

*1)* Miner is evaluated based on the computational power that he possesses number of blocks that are going to be generated by miner and conditions for mining.
*2)* Based on evaluated power, he/ she can adjust difficulty rating.
*3)* All these parameters will be included in the participating transaction that is sent to rest of the nodes in the network.
*4)* Rest of the nodes then verifies the block using these parameters.

©IJRASET: All Rights are Reserved

| Sl. No | Author | Work/ Result/ Method used | Comments |
|---|---|---|---|
| 1. | Satoshi Nakamoto | This is the first research work done on crypto currency using blockchain as the underlying technology. Proof of Work is used as consensus algorithm. | Crypto currency can efficiently replace traditional Internet Banking if implemented securely. |
| 2. | Suman Ghimire,<br>Dr. Henry Selvaraj | This paper is a survey of various terms used in Bitcoin. It includes block, block chains, mining details and proof of work. | Mining concept and Proof of Work explained in detail. |
| 3. | Peter D. DeVries | SWOT analysis of Bitcoin is presented. Highlights the facts that could make Bitcoin a future of Internet- connected global markets. | Helps understand the weakness in Blockchain technology and design accordingly. |
| 4. | Haneffa Muchlis Gazali,<br>Che Muhamad Hafiz Bin Che Ismail,<br>Tamrin Amboala | Survey on "why to invest in crypto currency is made". Study shows that financial tolerance to risk and these benefits lead to investing in crypto currency. | Financial tolerance to risk is the key to invest in crypto currency. |
| 5. | Jong-Hyouk Lee | This paper is a survey on anonymity of various crypto currency that exists in market. It checks for consensus algorithm used, block time, sender and receiver address hidden and so forth. | Anonymity of the user of crypto currency is explained in detail and it is motivation behind crypto currency. |
| 6. | Raj Patel,<br>Akhil Sethia,<br>Shyam Patil | Features of blockchain: Immutable, Privacy, No one point of failure, Efficiency and transparency are discussed. Working of blockchain is discussed in detail. Consensus algorithm: PoW and Pos are explained in great detail. | Blockchain is efficient because it is immutable and highly secured. |
| 7. | Bouvarel Lucas,<br>Paez Rafael V | Consensus algorithm PoW and PoS are discussed with criteria such as energy efficiency, block creating speed, double spending attack, modern hardware etc. | Proof of Work and Proof of Stake are the two main consensus algorithm used. |
| 8. | Shitang Yu,<br>Kun Lv,<br>Zhou Shao,<br>Yingcheng Guo,<br>Jun Zou,<br>Bo Zhang | Highly performaning system based on blockchain is proposed for Internet of things devices. | Blockchain can be a backbone of IoT devices. |
| 9. | Sobhan Latif,<br>Yunpeng Zhang,<br>Liang-Chieh Cheng | Real- Estate investment made efficient and easy by introducing blockchain technology that harnesses smart contracts. | Real – Estate can be backed by Blockchain technology. |
| 10. | Murat Kuzlu1,<br>Manisa ipattanasomporn,<br>Levent Gurses,<br>Saifur Rahman2 | Evaluates how the blockchain is impacted by workload framework- Hyper ledger Fabric. The result shows that it supports 200tps with up to 1,00,000 participants. | Blockchain is impacted by more number of transactions per second. |
| 11. | Nir Kshetri,<br>Jeffrey Voas | In blockchain enabled voting system, votes are cast using computer or otherwise smartphone. Encrypted keys and tamperproof personal IPs are used. Blockchain identifies each cast vote to individual voter and establish permanent immutable records. | e- voting based on blockchain is implemented and tested. |
| 12. | Sajad Homayoun,<br>Ali Dehghantanha,<br>Reza M. Parizi,<br>Kim-Kwang Raymond Choo | System based on blockchain is used in malign detection system to detect malign mobile apps in mobile application stores. Uses private blockchains, detection engines and consortium algorithm. | Malign mobile applications can be detected using blockchain technology. |
| 13. | Ruksudaporn Wutthikarn,<br>Yan Guang Hui | Uses hyperledger blockchain framework. Enables sharing patient's dental characteristic between one hospital to another, allows identification of each patient for follow up treatments. | Dental hospital system based on blockchain is implemented. |

©IJRASET: All Rights are Reserved

| | | | |
|---|---|---|---|
| 14. | Mohammad Jabed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, Jun Han, Paul Sarda | Compares issues such as Trust building, data Confidentiality, tolerance to Fault, Performance, Redundant data and Security between traditional database and blockchain. | Comparison between traditional database and Blockchain technology. |
| 15. | Sandeep Raghuwanshi, Prof. R. K. Pateria, Prof. R. P. Singh | Mathematical modeling system to verify payment integrity or order details of online purchases. | Online purchases are verified through mathematical model. |
| 16. | Yongqiang He, Yanrong Shi, Aixiang He | The three digital payment modes e- card, e- cash and e-check are discussed along with their application environments, | Traditional online payment systems are discussed |
| 17. | Ghada El Haddad, Esma Aïmeur, Hicham Hage | Three important aspects of online payment Trust, Security and Financial fears are surveyed. | Online payment systems are verified for Trust, Security and Financial risk. |
| 18. | Zhiran Wang | Cloud based digital payment system is proposed in this system. | Cloud based digital payment system is proposed in this system and verified. |
| 19. | Zahra Ebadi | Features and architecture of centralized core operations and automation of process using core banking applications and IP- based network are proposed in this paper. | Centralized banking system is investigated. |
| 20. | Tengfei Xue, Yuyu Yuan, Zahir Ahmed, Krishna Moniz, Ganyuan Cao, Cong Wang | Proof-of-Contribution which is based on PoW and PoS is proposed. | Consensus algorithm based on PoW and PoS is developed. |
| 21. | Ryoya NAKAHARA, Hiroyuki INABA | PoW is used in Bitcoin. It encourages mining pool to centralize computing power in the network. This leads to “majority attack” issue. To overcome this Fair PoW that evaluates power of computing on every node that alters difficulty of generating a block is proposed | PoW used in Bitcoin is discussed for its stability. |

Table: Blockchain survey papers

## VIII. CONCLUSION

Blockchain as technology was first introduced in the year 2009 with Bitcoin. Since then it has evolved to a large scope and now being explored in various applications.

Surveying various papers related to crypto currency has led to the conclusion that blockchain is the technology that can be basis for crypto currency.

Proof of Work and Proof of Stake are the two consensus algorithms that are tried and tested in many projects and they are working in a secured manner.

Proof of Contribution which is a combination of PoW and PoS is proposed in some papers and it combines benefits of both PoW and PoS and works much faster than the individual algorithms.

With the security provided by blockchain technology, this is tested on various platforms including Internet of Things, e-voting, Real Estate business, Medical systems and most importantly financial sector.

Cryptocurrency is a major invention in the field of banking and each day the trust, security and transparency of it is being tested. Going forward major technological shift towards blockchain can be expected.

## REFERENCES

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[2] Ghimire, Suman, and Henry Selvaraj. "A Survey on Bitcoin Cryptocurrency and its Mining." 2018 26th International Conference on Systems Engineering (ICSEng). IEEE, 2018.
[3] DeVries, Peter D. "An Analysis of Cryptocurrency, Bitcoin, and the Future." International Journal of Business Management and Commerce 1.2 (2016): 1-9.
[4] Gazali, Haneffa Muchlis, Che Muhamad Hafiz Bin Che Ismail, and Tamrin Amboala. "Exploring the Intention to Invest in Cryptocurrency: The Case of Bitcoin." 2018 International Conference on Information and Communication Technology for the Muslim World (ICT4M). IEEE, 2018.

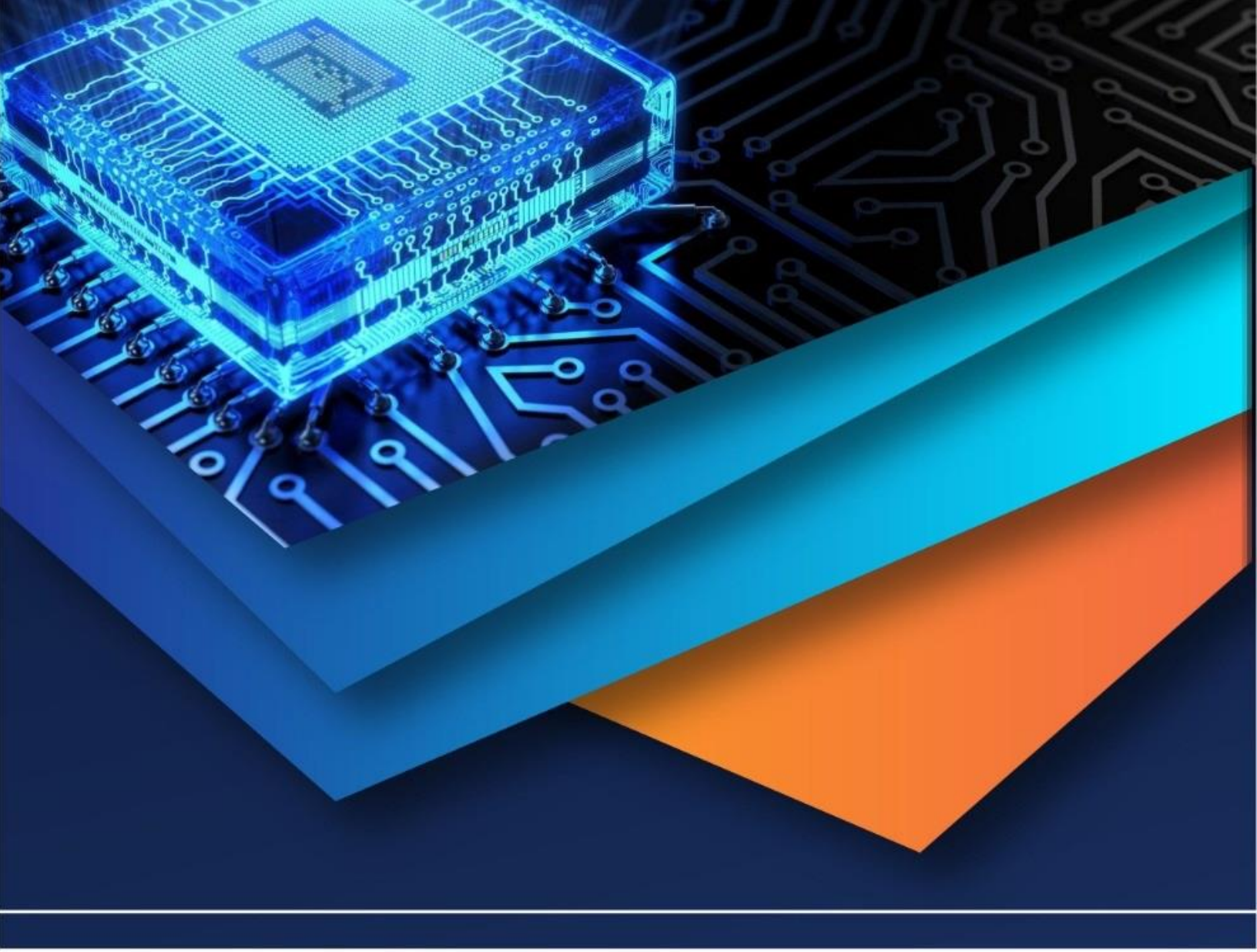
©IJRASET: All Rights are Reserved

[5] Alzahrani, Saeed, and Tugrul U. Daim. "Evaluation of the Cryptocurrency Adoption Decision Using Hierarchical Decision Modeling (HDM)." 2019 Portland International Conference on Management of Engineering and Technology (PICMET). IEEE, 2019.
[6] Lee, Jong-Hyouk. "Rise of Anonymous Cryptocurrencies: Brief Introduction." IEEE Consumer Electronics Magazine 8.5 (2019): 20-25.
[7] Balaskas, Anastasios, and Virginia NL Franqueira. "Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges." 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2018.
[8] Patel, Raj, Akhil Sethia, and Shyam Patil. "Blockchain–Future of Decentralized Systems." 2018 International Conference on Computing, Power and Communication Technologies (GUCON). IEEE, 2018.
[9] Lucas, Bouvarel, and Rafael V. Páez. "Consensus Algorithm for a Private Blockchain." 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC). IEEE, 2019.
[10] Hazari, Shihab Shahriar, and Qusay H. Mahmoud. "A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems." 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2019.
[11] i Muñoz, Jordi Zayuelas, José Suárez-Varela, and Pere Barlet-Ros. "Detecting cryptocurrency miners with NetFlow/IPFIX network measurements." 2019 IEEE International Symposium on Measurements & Networking (M&N). IEEE, 2019.
[12] Baek, Hyochang, et al. "A Model for Detecting Cryptocurrency Transactions with Discernible Purpose." 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, 2019.
[13] Scholar, P. G. "College Fees Transaction Using Hash Functions of Blockchain Model."
[14] Yu, Shitang, et al. "A high performance blockchain platform for intelligent devices." 2018 1st IEEE international conference on hot information-centric networking (HotICN). IEEE, 2018.
[15] Latifi, Sobhan, Yunpeng Zhang, and Liang-Chieh Cheng. "Blockchain-Based Real Estate Market: One Method for Applying Blockchain Technology in Commercial Real Estate Market." 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019.
[16] Kuzlu, Murat, et al. "Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability." 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019.
[17] Kolekar, Sachin M., et al. "Review paper on untwist blockchain: A data handling process of blockchain systems." 2018 International Conference on Information, Communication, Engineering and Technology (ICICET). IEEE, 2018.
[18] Kshetri, Nir, and Jeffrey Voas. "Blockchain-enabled e-voting." IEEE Software 35.4 (2018): 95-99.
[19] Homayoun, Sajad, et al. "A blockchain-based framework for detecting malicious mobile applications in app stores." 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). IEEE, 2019.
[20] Wutthikarn, Ruksudaporn, and Yan Guang Hui. "Prototype of Blockchain in Dental care service application based on Hyperledger Composer in Hyperledger Fabric framework." 2018 22nd International Computer Science and Engineering Conference (ICSEC). IEEE, 2018.
[21] Chowdhury, Mohammad Jabed Morshed, et al. "Blockchain versus database: a critical analysis." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.
[22] Raghuwanshi, Sandeep, R. K. Pateria, and R. P. Singh. "A new protocol model for verification of payment order information integrity in online E payment system." 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC). IEEE, 2009.
[23] He, Yongqiang, Yanrong Shi, and Aixiang He. "Research on online payment mode of e-commerce." 2010 IEEE International Conference on Software Engineering and Service Sciences. IEEE, 2010.
[24] El Haddad, Ghada, Esma Aïmeur, and Hicham Hage. "Understanding trust, privacy and financial fears in online payment." 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE, 2018.
[25] Wang, Zhiran. "Research on cloud computing-based online payment mode." 2011 Third International Conference on Multimedia Information Networking and Security. IEEE, 2011.
[26] Ebadi, Zahra. "Advance banking system features with emphasis on Core banking." The 9th International Conference on Advanced Communication Technology. Vol. 1. IEEE, 2007.
[27] Xue, Tengfei, et al. "Proof of contribution: A modification of proof of work to increase mining efficiency." 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 1. IEEE, 2018.
[28] Nakahara, Ryoya, and Hiroyuki Inaba. "Proposal of Fair Proof-of-Work System Based on Rating of User's Computing Power." 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE). IEEE, 2018.
[29] "Indian Banks": information about how banking has evolved in India over time https://en.wikipedia.org/wiki/Banking_in_India
[30] "Internet Banking": information about how online banking is carried out https://en.wikipedia.org/wiki/Online_banking
[31] "Bitcoin Developer Guide": information needed to understand Bitcoin and start building Bitcoin based applications https://bitcoin.org/en/developer-documentation
[32] "Bitcoin: A peer-to-peer Electronic cash system" https://bitcoin.org/en/bitcoin-paper
[33] "Cryptography" or "Cryptology": An idea about Cryptography and its process https://en.wikipedia.org/wiki/Cryptography
[34] "What is Blockchain technology and how it works" https://blockgeeks.com/guides/what-is- blockchain-technology/
[35] "Computer security, cyber security or information technology security" https://en.wikipedia.org/wiki/Computer_security
[36] Hu, Yao-Chieh, Ting-Ting Lee, and Chungsang Lam. "A Risk Redistribution Standard for Practical Cryptocurrency Payment." 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). IEEE, 2019.
[37] Selvi, S. Sharmila Deva, et al. "Splitting and Aggregating Signatures in Cryptocurrency Protocols." 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). IEEE, 2019
[38] Giang-Truong Nguyen and Kyungbaek Kim," A Survey about Consensus Algorithms Used in Blockchain", 2018
[39] M. Milutinovic, H. Wu, W. He and M. Kanwa, "Proof of Luck: an Efficient Blockchain Consensus Algorithm", 2017
[40] J. Bohr and M. Bashir, "Who Uses Bitcoin?," in 2014 Twelfth Annual Conference on Privacy, Security and Trust (PST), 2014, pp. 94–101.

©IJRASET: All Rights are Reserved

[41] L. H. White, “The Market for Cryptocurrencies,” Hofstra Law Rev., vol. 35, no. 2, pp. 383–402, 2015.
[42] Bitcoin Mining Software ”https://www.bitcoinmining. com/bitcoin-mining-software/”. Accessed August 16, 2018
[43] Blockchain Charts ”https://www.blockchain.com/charts”. Accessed August 19, 2018
[44] Scherer, Mattias. “Performance And Scalability Of Blockchain Networks And Smart Contracts.” Umea University, 2017, http://www.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf. Accessed 15 May 2018.
[45] "Cryptocurrency Transaction Speeds: The Complete Review". The Daily Hodl, 2018, https://dailyhodl.com/2018/04/27/cryptocurrencytransaction- speeds-the-complete-review. Accessed 3 Nov 2018.
[46] FLEXCUBE Universal Banking Solution, http://www.iflexsolutions.com/iflex/pdf/website/ /Flexcube.pdf, http://www.iflexsolutions.com/iflex/solutions/PrivateBankingsolutions.aspx.
[47] Taking Core Banking to the Next Level http://www.tietoenator.com/.
[48] S. King and S. Nadal, “PPcoin: peer-to-peer cryptocurrency with proof-of-stake,” 2012 [Online]. Available: https://decred.org/research/king2012.pdf.
[49] Litecoin," [Online]. Available: https://github.com/litecoin-project.
[50] "Ethash," 24 July 2017. [Online]. Available: https://github.com/ethereum/wiki/wiki/Ethash
[51] Weller, "Bitcoin is soaring - here's what the cryptocurrency is all about," 25 May 2017. [Online]. Available: https://www.businessinsider.in/Bitcoin-is-soaring-heres-
[52] Block Headers," bitcoin.org, 7 December 2017. [Online]. Available: https://bitcoin.org/en/developer-reference#block-headers
[53] Roop Gill, ”CEX. IO Slow to Repond as Fears of 51% Attack Spread”, 2014, https://www.coindesk.com/cex-io-response-fears-of-51-attack-spread/
[54] “Majority attack”, https://en.bitcoin.it/wiki/Majority attack

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)