Blockchain, Consensus algorithm

Ayoola ch

Andhra university (AU)

Abstract The Block chain or block chain can be defined as a public ledger in which all transactions are stored in the form of blocks, it is a chain in continuous growth in which new blocks are automatically added according to the number of transactions. In the block chain we will use cryptographic techniques such as digital signatures and different consent algorithms for user security and the consistency of the stored data. Consider any block chain that follows the following characteristics. They are transparency, invisibility, continuity and decentralization with these characteristics that a block chain can work efficiently and save costs. Because a Block chain is a growing list of public access records,each user has a public and private key to view and sign transactions without any intermediary and can also be used and applied in other fields such as smart contracts, Iot, organizations financial. Because a transaction cannot be manipulated once placed in the blockchain, organizations must be honest when creating and signing transactions. Althoughit has great potential for building a system of future transactions, it faces some difficulties.The main concern is archiving because the size of the block chain increases as the numberof transactions increases. In second place comes the loss of privacy in which the data are subject to losses and third comes the part of the algorithm. Here we cannot say which of allthe algorithms, for example, pow, which is a test of labor wasting electricity and the POS test of participation, which makes the rich richer in the phenomenon. Therefore, dependingon the application, it is necessary to use and implement our block chain accordingly.

Keywords Blockchain, Consensus algorithm, Challenges of Blockchain.

1. Introduction

The Block chain or block chain can be defined as a public ledger in which all transactions are stored in the form of blocks, it is a chain in continuous growth in which new blocks are automatically added according to the number of transactions. In the block chain we will use cryptographic techniques such as digital signatures and different consent algorithms for user security and the consistency of the stored data.

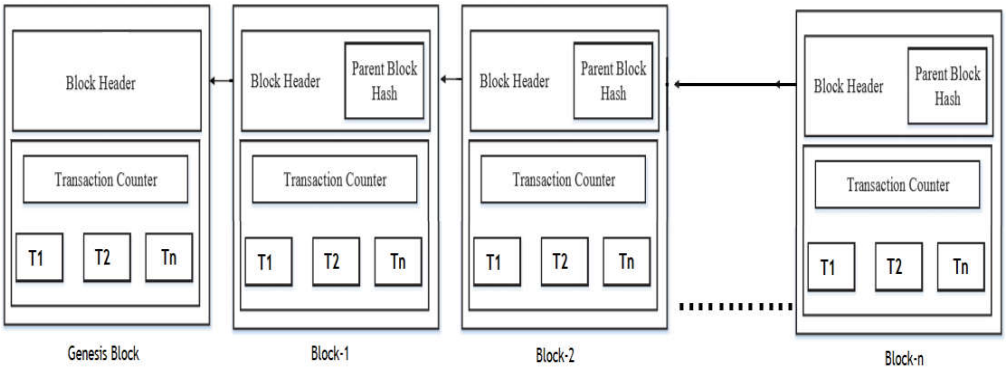
Consider any block chain that follows the following characteristics. They are transparency, invisibility, continuity and decentralization with these characteristics that a block chain can work efficiently and save costs.

Because a Block chain is a growing list of public access records, each user has a

public and private key to view and sign transactions without any intermediary and can also be used and applied in other fields such as smart contracts, Iot, organizations financial. Because a transaction cannot be manipulated once placed in the blockchain, organizations must be honest when creating and signing transactions.

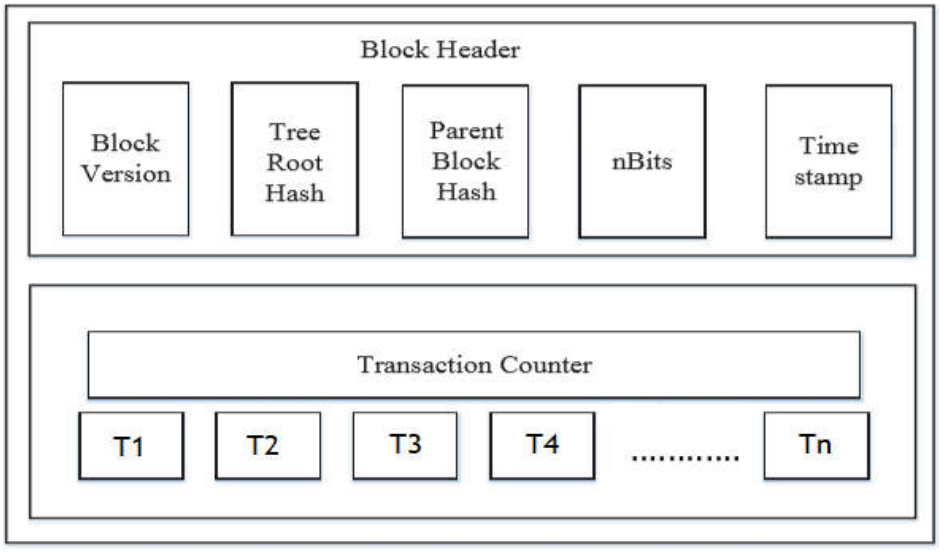
Although it has great potential for building a system of future transactions, it faces some difficulties. The main concern is archiving because the size of the block chain increases as the number of transactions increases. In second place comes the loss of privacy in which the data are subject to losses and third comes the part of the algorithm. Here we cannot say which of all the algorithms, for example, pow, which is a test of labor wasting electricity and the POS test of participation, which makes the rich richer in the phenomenon. Therefore, depending on the application, it is necessary to use and implement our block chain accordingly [1].

2. Architecture



The block chain is a sequence of blocks, in which a complete list of transactions is shown, such as the conventional public book. With a hash of the previous block contained in the block header, a block has only one main block. It should be noted that the first block of a block chain is called a genesis block that has no parent block [1].

Structure of Block



Block version: Set of validation rules to be followed

Tree root hash: Hash value of all the transactions in the block

Parent block hash: 256-bit hash value that points to the previous block.

n-Bits: threshold value of a valid block hash

Timestamp: current time at the creation of block

3. Characteristics of a Block chain

Generally speaking, block chain should have following characteristics.

1 Transparency

2 Invisibility

3 Continuance

4 De-centralization

3.1 Transparency

Provide complete transaction history. Because the block chain is an open file, each party can access and control transactions. This creates an origin in which it is possible to keep track of the useful life of the activities.

3.2 Invisibility

Each user can interact with the block chain with a generated address, which does not reveal the real identity of the user.

3.3 Continuance

Because each of the operations that extend through the network must be confirmed and recorded in the distributed through network blocks, it is almost impossible to manipulate. Furthermore, each block would be validated by other nodes and the transactions would be verified. Therefore, any manipulation can be easily detected.

3.4 Decentralized

In conventional centralized transaction systems, each transaction must be validated through the central trust agency, which translates into cost and performance bottlenecks in the central servers. In a different way, a transaction in the block chain network can be performed between any two pairs (P2P) without central agency authentication. In this way, the block chain can significantly reduce server costs, including the cost of development and the cost of the operation [2].

4. Categories of Block Chain Systems

Block chain systems can be roughly categorized into three types. They are:

4.1 Public block chain:

Block chains which are public allows anyone who wants to read, write or join a public block chain can do it. Public chains are decentralized, which means that no agent has control over the network, which guarantees that data cannot be changed once validated in the block chain. It simply means that anyone, anywhere, can use a public block chain to enter transactions and data as long as they are connected to the network.

Some well-known examples of are Bitcoin and Ethereum, with Bitcoin which is among the first Block chain applications to show that the value could move around the world without third parties such as banks or financial organizations.

4.2 Private block chain:

Blockchains which are private work similarly to public blockchains but with access controls that restrict those who are joining the network, which means it operates like a centralized database that limits access to certain users. These Block chains have one or multiple entities that have control over the network, relying on third-parties to transact. A well-known example is a Hyper ledger.

4.3 Consortium block chain:

Consortium block chain is partly private. This type of block chain has same advantages as that of a private block chain, but operate under the leadership of a group instead of a single owner. This platform would be great for organizational collaboration. Imagine central banks coordinating their activities based on international rules of finance. Or the United Nations outsourcing their transactional ledger and voting system to block chain, allowing each country to represent a verifying node in the network.

We compare these three types of block chain from different perspectives.

Property	*Public blockchain*	*Consortium blockchain*	*Private blockchain*
Consensus determination	All miners	Selected set of nodes	One organisation
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralised	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

5. Types of Consensus Algorithms and their Benefits and Problems

Consensus mechanisms are the ways to guarantee a mutual agreement on a data value and the state of this as the layout of all data. With block chains, consensus mechanisms guarantee that each node in the network has a copy of the same ledger. And, as expected, different consensus mechanisms impact the security, and the framework of the cryptographic protocol in different ways.

Consensus mechanisms come in a number of forms and won't bring about the same result for every transaction, or block chain network, where they are used.

And because it's so quick in the process, it's hard to say what consensus mechanisms will be the most popular for implementing. Creating consensus mechanisms involves the study of mechanism design, which is a two-step process:

- Considering the desired outcome.
- Work backward to create a game that credits players to fulfill that outcome.

5.1 Proof of Elapsed Time (PoET)

The Proof of Elapsed Time is consensus mechanism operates in a similar fashion. For beginners, PoET is used on a permitted block chain, meaning that every node in the system must be identifiable, and accepted in the network. Just like, in the class, all students know each other, and everyone had to be enrolled in the course to take the final exam.

But with PoET, the "timer" is different for each node. Every participant in the network is assigned a random amount of time to wait, and the first participant to finish waiting gets to commit to the next block in the block chain. Difference from Proof of Stake: By requiring each node to "rest", PoET is believed to be more energy efficient than PoS [3].

5.2 Proof of Authority (PoA)

Block chains are cutting edge technology, but they have their boundaries. Like most of the systems, block chains have trade-offs. Vitalik Buterin refers this situation as the 'Scalability Trilema', identifying three desired attributes of blockchains:

Scalable- Is the Block chain Scalable?

Decentralized- Is the Block chain decentralized?

Secure- Is the Block chain Secure?

Unlike Proof of Stake algorithm where nodes stake financial value, Proof of Authority consensus rewards the actual identities of the nodes in the system. It's a turn on PoS consensus that speaks a risk of how a stake can be valued by members in a network.

By identifying validators, PoA algorithm becomes inherently centralized. Therefore, it's best suited for private block chains and consortiums [3].

5.3 Proof of Capacity

After revising multiple consensus algorithms, we have discovered a pattern: Most of the lesser known types of algorithms are considered to be better than Proof of Work or Proof of Stake.

The more number of seats, the better. That is the essence of PoC. Here the shortest solution to the mining algorithm is stored in advance and it grants the rights to mine the next block. In our comparison, that "solution" is liken to the student who lives close to the school and probably doesn't need to go in bus [3].

Advantages:

- **Efficient**—Less energy used than Bitcoin transactions.
- **Cheap**—No need for specialized mining software.
- **Distributed**—Excess storage space is more accessible.

PoC in action: the free space on the hard drive is used to mine coins with the solutions planned in advance.

5.4 Proof of Burn

Also known as an un-spendable address, eater addresses are on the receiving end of all proof of burn transactions. They are storage cells for coins surrendered through proof of burn consensus.

Because addresses are generated randomly, it is believed that nobody not even miners can determine the private key. So, by the name coins are effectively eaten. More burnt coins = greater odds of being selected. However, rewards decline over time, meaning that you'll need to burn tokens every now and then to continue receiving block rewards at about the same rate.

Pros: As we have mentioned, proof of burn algorithm sets you back in the short term. The possibility for larger gains in the future could incentivize users to remain involved in the transaction, thereby preserving the functionality of the network.
Cons: It is comparable to Plinko where burning the empty coins does not guarantee that you are can mine future blocks. And also similar to proof of stake, the process favours them who can commit more principal, tilting the chances in their favour.
PoB in action: Slim coin uses proof of burn as a consensus algorithm, and its counterpart uses proof of burn to "seed" tokens. Seeding is a way to bootstrap one coin by burning another. With Counterpart, users can transfer Bitcoin to an consumer address and can receive XCP tokens in return [3].

5.5 Delegated Proof of Stake (DPoS)

DPoS is a twist on Proof of Stake consensus that relies upon a group of agents to validate blocks on behalf of all participating nodes in the network. There are typically 22 to 98 delegates elected in networks using this algorithm. It will be easier for them to gather themselves and allot slots in which each delegate will publish their block when less parties are involved.
Pros: Scalable, energy efficient, cheap transactions.
Cons: Partially centralized (Scalability Trilemma).
DPoS in action: BitShares, EOS, and Steemit all use Delegated Proof of Stake [3].

5.6 Byzantine Fault Tolerance

Here a group of generals or validators are called to confirm that the information delivered to them is authentic.

BZFT in action: We came across two types of algorithms. They are:

Practical Byzantine Fault Tolerance: Used by Hyperledger Fabric, PBFT uses less than 20 pre-selected validators to determine consensus for the network.

Federated Byzantine Agreement: Here each node general is called to establish truth for each of their respective chains.

Pros: Low transaction cost, high throughput, network scalability.

Cons: Centralized, permissioned [3].

5.7 Proof of Importance

As we've seen, different consensus algorithms can be integrated into a decentralized network in order to reward users to follow a particular set of rules. And there isn't a one for all each mechanism has its own set of advantages and disadvantages which have varying degrees of success depending upon the action. Proof of Importance recognizes that other factors can considered when defining what nodes provide the most value to a network. For example, Proof of Stake gives too much power to those with higher stakes in that only a smaller percentage of total capital could be committed to the network, which may not encourage others to participate. Here the nodes which are clustered weighs heavily.

Improvements on Proof of Stake:

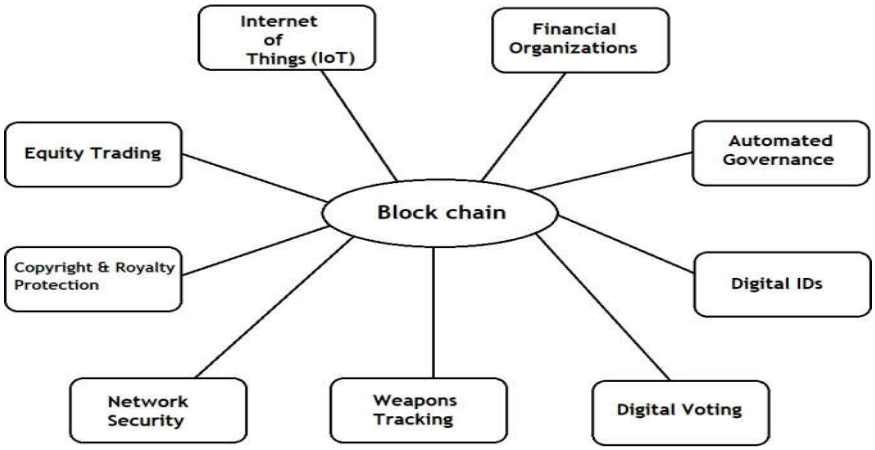
Less chance of being notice: Traditional staking requires the members to commit their positions and no value is being transferred throughout the network. Net transfers provide a better grade to those who operate in circulation. The marginal cost of creating a block is always zero, which means that users can continue validating blocks with PoS even in the event of a fork. That risks to drain off users away from the most popular network as time progresses [3].

Comparison of Consensus Algorithms:

Property	*PoW*	*PoS*	*PBFT*	*DPOS*	*Ripple*	*Tendermint*
Node identity management	Open	Open	Permissioned	Open	Open	Permissioned
Energy saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	< 25% computing power	< 51% stake	< 33.3% faulty replicas	< 51% validators	< 20% faulty nodes in UNL	< 33.3% byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

6. Applications

Block chain can be considered as the vision of developers who believed that the current banking system had faults. Particularly they viewed banks as third-parties and transaction fees as a unnecessary thing, and they mocked at the idea that payment validation and settlement could take up to five business days over the boundaries. So with the help of block chain, real-time transactions are possible even across borders, while banks are out of their traditional process, apparently reducing the transaction fees [4].



Block chain technology can be integrated into multiple areas. The primary use of block chains as of now is as a distributed ledger for cryptocurrencies, most notably bitcoin. There are a few more domains where block chain can be used. They are:

6.1 Internet of things

Internet of things (IoT), one of the most encouraging information and communication technologies (ICT), is coming into light. Networking giant Cisco Systems may be working on a block chain-based application system that would monitor these networks. The IoT describes wirelessly connected devices that can send and receive data without user interference. Such an application could determine the trustworthiness of devices on a network and can potentially improve the IoT sector [4].

6.2 Financial Organizations

Many of the industry's methods are overdue for an upgrade or in some cases they need to be replaced completely in order to withstand new volumes and

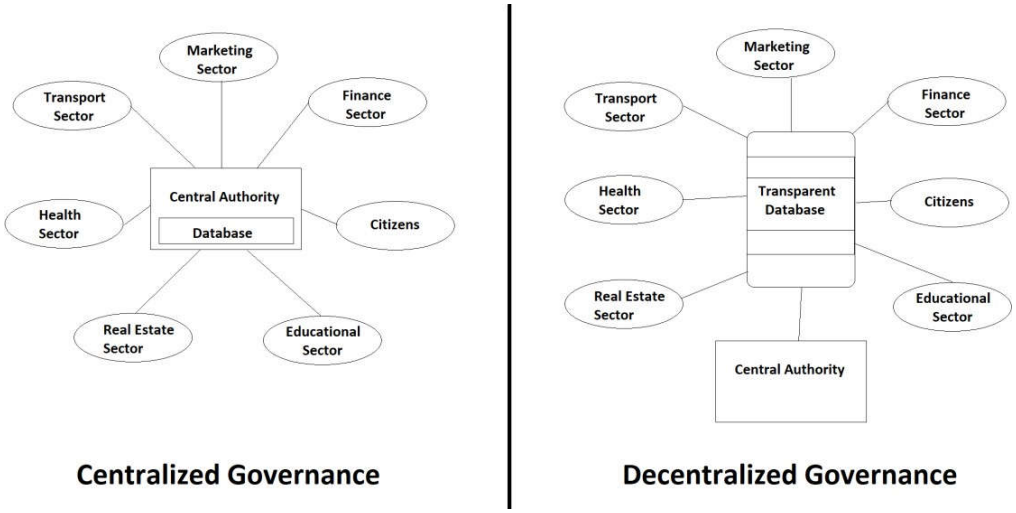
unknown security threats. Block chain is invincible and recoverable as there will be no existence of centralized version of this information.

Transfers aided by central authorities such as banks and clearinghouses have not changed in the last 150 years. An international transfer can take up to five days to settle, causing problems like credit risk, exchange rate risk. Not only that the industry needs to reduce heavy transaction fees and transaction times. So with the help of Block chain we can make these transfers visible and fast which other technology cannot.

In the future, people will make a lot of smaller payments. That's going to increase economic activity which makes a larger amount with smaller amounts, higher volumes and a demand for technology that will be supported [4].

6.3 Automated Governance

In the financial sector, each institution maintains its own records on its own ledger system and reports data frequently to the authorities by following compliance rules. So in the whole market, large duplication of efforts, lack of transparency and unavoidable conflicts can arise. These problems are associated with large costs and risks making the system inefficient [4].



Block chain technologies can provide a transparent and secured environment where transaction records are made accessible to both industry and regulators creating an environment where both market players and regulators have access to trusted auditable data by releasing companies from compliance duties and risks. Block chain technologies bring these following main elements:

a) Access to auditable data which are verified and hard to tamper with, creating time-stamped, immutable and historical records.

b) Constitution of a transparent, inter-operable environment where rules can be implemented, enforced and adapted by monitoring their effects in real-time and by using feedback from the participants.
c) Provision of instruments to monitor and quantify both the reliability and reputation of users.
d) Creation of a platform where rules can be encoded within the system – enabling automated review via audit software and.
e) Create a unique source of truth approved by the community via consensus.

6.4 Digital ID's

More than 1 billion people are facing identity challenges. Microsoft NASDAQ is looking to working on that problem to change that. It is creating digital IDs within its Authentication application which is currently used by millions of people all over the world and also would give users a new way to control their digital identities in this online world. This would allow people in underprivileged regions to access financial services [4].

6.5 Digital Voting

Block chain offers the ability to vote digitally with the help of biometrics, but it's transparent enough that any regulators can see if something is being changed / updated on the network. It combines the ease of digital voting with immutability which is the unchanging and a secured nature of block chain to make your vote count [4].

6.6 Weapons Tracking

One of the hot-button topics on any news channel is weapons liability. Block chain could create a transparent and unchanging registry network that allows law enforcement and the federal government to track weapon ownership, as well as also by keeping a record of weapons sold privately [4].

6.7 Network Security

Block chain technology provides us with the best tools to protect our data from hackers, preventing fraud and decreasing the chance of data being compromised.

In order to destroy or corrupt a complete block chain, the hacker must have to destroy the data stored on every and every user's computer in a network. This

could be millions of computers, with each one storing a copy of some part or all of the data. Even in case of a hacker bringing down a block chain, undamaged computers, also known as “nodes”, would continue running to verify and keep record of all the data which is on the network. The impossibility of taking down a whole chain increases along with the amount of users participating in a network. Bigger block chain networks with more number of users have an infinitely lower risk of getting hacked because of the complex network.

This complex structure provides block chain technology with the ability to be the most secured form of storing and sharing information online. That’s why innovators have begun applying the technology in different sectors to prevent fraud and safeguard the data [4].

6.8 Copyright and Royalty Protection

In a world with growing internet access, copyright and ownership laws on music and other digital content has become negligible. With block chain, those copyright laws would be made strict for digital downloads, ensuring the artist or creator of the content being purchased gets their fair share. The block chain would also provide real-time and transparent protection to musicians and content creators for securing their content online [4].

6.9 Equity Trading

At some point, block chain could challenge or replace current trading platforms to buy or sell stocks. Because block chain networks validate and settle transactions so quickly, it could eliminate the huge wait time which is encounter by investors when selling stocks and seeking access to their funds for the purpose of reinvestment or withdrawal [4].

7. Challenges

There are false passes in any technological revolution. Some people in the block chain industry have pointed out that block chain has become overhyped but in reality, the technology has its limitations and is inappropriate for many digital interactions [1].

But through research and development we have known the current issues and limitations of block chains. There are three types of challenges currently the block chain network is facing. They are:

1. Leakage of Privacy
2. Scalability Factor and
3. Un-authorised Mining

7.1 Leakage of Privacy:

Users believed that block chain gives better privacy when handling sensitive data. In block chain users could only generate address instead of their identity. In 2013 Meikle john and in 2016 Kosba showed that block chain cannot guarantee the transnational privacy. Recent study shows that bitcoin transactions are linked together to an account address to reveal the identity of user. but Elliptic Curve Diffie- Hellman- Merkle(ECDHM) can be used to overcome this problem. It will deal with public and private key by exchanging shared secrets between two people by securing message transaction over the un-secured internet [1].

7.2 Scalability Factor:

The amount of transactions are increasing day by day. Most of the companies were suggesting block chain for their transaction process. All transaction have to be stored and it must be validated. The capacity of the block will be very small. Some transaction must be delayed due to high transaction fee. So the large block size will lead to reduce the growing speed. Therefore scalability is a problem. There are some methods to avoid the scalability problem in block chain. They are:

1. Storage Optimization of block chain
2. Redesigning block chain

Storage Optimization of block chain:

The old transaction records are removed by the network and a database named account tree is used to hold the balance of all non-empty addresses. In this way, nodes do not need to store all transactions to check whether a transaction is valid or not. Besides lightweight client could also help fix this problem. In 2014 a novel scheme named VerSum was proposed to provide another way allowing light weight clients to exist. VerSum allows light weight clients to outsource expensive

computations over large inputs. It guarantees that the computation result is accurate by comparing results from multiple servers.

Redesigning block chain:

The conventional block is de-coupled into two parts: key block for leader election and micro block to store transactions. Miners are competing to become a leader. The leader would be responsible for micro block generation until a new leader appears. Bitcoin also extended the longest chain strategy where only key blocks count and micro blocks carry no weight. In this approach, block chain is redesigned [1].

7.3 Unauthorized Mining:

Here, the miner does not follow the normal process of creating a block. He mines the block continuously maintaining its track but fails to publish it on the network. The attacker only publishes the chain of the transaction to increase the amount of revenue earned. From the attack, the miner gains more than the stipulated portion of the mining power.

It is considered that un-authorized mining attacks approximately 25% of Bitcoin's whole network. The exposure of Bitcoin's system to attacks increases drastically when pooling forces the individuals to stop mining. Though optimizations are not considered any form of attacks, the process of pooling increases the chances of an attack on its Block chain [5].

8. Future Enhancements and Scope

8.1 Standardizing and Blockchain Testing

When users want to combine block chain into business, they have to know which block chain suits their requirements. So block chain testing mechanism needs to be done to test different block chains. Block chain testing is categorized into two phases: standardization phase and testing phase.

In standardization phase, all criteria is to be made and agreed. When a block chain is created, it could be tested with the agreed criteria to make sure if the block chain works fine as claimed. As for testing phase, block chain testing needs to be performed with different criteria. For example, a user who is in charge of online

retail business cares about the throughput of the block chain, so the examination needs to test the average time from a user sending a transaction to the transaction being packed into the block chain and capacity for a block chain block [5].

8.2 Eliminating Centralization in Block Chain:

Even though block chain is a de-centralized type of architecture, miners are centralized in the mining pool which means all the miners form together as a group or creating a pool leading to centralization in block chain. Till now, almost 50% of the hashing power in the network is owned by only 5 mining pools. Apart from that a review published on un-authorized mining showed that mining pools with over 25% of total computing power could get more revenue than a fair share. New and rational miners would be easily attracted into the selfish pool and finally, the pool could easily exceed 51% of the total power. As the block chain is intended to serve all organizations, these type of grouping and forming centralization is a big no [5].

8.3 Big Data Analytics:

As Big data has to deal with huge data-sets, having the right infrastructure is the challenge that most organizations come across. Additionally, the volume of transactional information that is to be stored within ledgers becomes huge over a period of time. Conventional cloud storage providers do not serve as a cost-effective alternative for storing such voluminous information for the business. Also, there may be a need for maintaining multiple copies at different locations, which puts an additional burden on resources. Here, block chain solution serves as a more viable option as it makes data storage more economical [5].

8.4 Network Security:

Network Security is the key concern that has led to the increasing adoption of block chain technology in banking and other industry verticals as well. The reason is that being a decentralized system, it requires multiple signatures of authorized users at every level of access. Moreover, any updates in block chain-based data resource can be tracked and verified. Industries such as retail and healthcare are relying on this innovative technology to secure their crucial records and minimize the risks of leaks and hacking [5].

8.5 Educational Institutions:

Normally in any organization or institution records of all their transactions are stored in media such as books and ledgers in offices and certificates and soft copies in colleges. So this media can be accessed easily and is prone to data manipulation. This is the main disadvantage of current record keeping formats. Not only losing the originality of the data there also exists a problem in storing those records. Storage of large sets of data and accessing them becomes a tedious task both in paper and digital format because the incoming data needs to be organized continuously and need to be maintained securely. So currently we are facing three problems for record keeping. They are:

1. Data Manipulation
2. Storage of Data
3. Data Accessing

So to overcome those problems we will implement a new idea with the help of block chain.

A new system has to be designed which will overcome all the problems which are mentioned above. So with the help of block chain technology we can implement a new type of peer-to-peer record keeping system with the addition of crypto-graphical methods like digital signatures which guarantees transparency, data security and easy storage of the records for college management system for educational institutions which will guarantee no manipulation at any point of time. Since digital signatures are created by hashing technique and uses public and private keys, the transactions which are created by owner cannot be modified by third parties.

Thus, Block chain uses a Consensus mechanism which is a fault tolerant mechanism which is used to achieve the necessary agreement on a single data value over a system. So we can implement a new type of management system for colleges/ educational institutions where all the problems of traditional methods of record keeping are overcome [6].

8.6 Smart Contracts

A smart contract is a computer program that controls the transfer of digital currencies between two parties under some certain conditions. A smart contract not

only defines the rules and penalties related to an agreement in the same way that a traditional contract does, but it can also automatically enforce those obligations.
In 2008, the cryptocurrency bitcoin was developed via a block chain platform comprised of a digital and distributed ledger that tracks monetary transactions. This technology enabled the development of smart contract code that is used to enter all the terms of the contract into the block chain.

There are several potential business advantages when using smart contracts.

- Cost-efficiency.
- Processing speed.
- Autonomy.
- Reliability

There are numerous potential disadvantages to smart contracts, as well. A lack of international regulations focusing on block chain, cryptocurrencies and smart contracts makes these technologies difficult to monitor in the global economy.
Smart contracts are also complicated to implement. They are also impossible to change, and while this is considered a security-related advantage, the parties cannot make any changes to the smart contract agreement or incorporate new details without developing a new contract [6].

8.7 Block chain as Industry 4.0:

Industry 4.0 can be described as the current trend of data automation and exchange in the creation of latest technologies in our society. Industry 4.0 is merely a confirmation that technology had developed greatly since the 19th century, marking the commencement of mass production.

This is a trend marked by extensive industrial automation, development of Internet of Things (IoT), and the increase of high-bandwidth mobile networks.
The blockchain is regarded as an improvement or originality capable of holding the key to cybersecurity risk management for Industry 4.0. Blockchain technology is generally connected with cryptocurrencies such as Bitcoin, even though it has a lot of other use cases, like in Industry 4.0 cybersecurity.

Blockchain technology will work in industry 4.0 because it is able to do much more than mere confirmation and tracking of records [7].

Likely Uses of Blockchain Technology within Industry 4.0

- Recognizing and Authenticating IoT devices which are remotely connected through the block chain.
- Time and Date is added and hashed with the transaction to confirm the timestamp in order to avoid manipulation.
- Mass Production with multiple customizations

Since Industry 4.0 is referred to as cyber physical systems they use internet as a medium to exchange the work transactions or working procedures which is again insecure. A hacker can break into the data stream and can alter the working procedures of machines. So block chain is a must in Industry 4.0 [7].

9. Conclusion

Block chain is an emerging topic this year and it will also support many applications. Block chain will give Better security for transactions of any value. This block chain technology is mainly proposed to handle bitcoin transactions. It will also provide better security to Smart contracts, Ethereum and distributed ledgers. Best suited and mostly used application of block chain bitcoin. The transaction rate of block chain is fast and cheap than any other application and also provides a better security to sensitive data. Since Block chain is transparent and immutable the benefits and applications are more.

10. References

[1]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ‘‘An overview of blockchain technology: Architecture, consensus, and future trends,’’ in Proc. IEEE Int. Congr. Big Data (BigData Congr.), Jun. 2017, pp. 557–564. [Online]. Available: http://ieeexplore.ieee.org/document/ 8029379/

[2]. S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3]. https://medium.com/coinmonks/blockchain-consensus-algorithms-an-early-days-overview-2973f0cf49c6

[4]. https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx

[5] https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf

[6] https://www.cognizant.com/whitepapers/blockchain-goes-to-school-codex3775.pdf

[7] https://en.wikipedia.org/wiki/Industry_4.0