Global Journal of Computer Science and Technology: C
Software & Data Engineering
Volume 23 Issue 1 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Blockchain Challenges: Advantages and Algorithms

By Zeel B Dabhi & Aishwarya

Ajeenkya DY Patil University

Abstract- Cryptocurrency is the innovation that has changed the way of life most significantly over the past ten years. Bitcoins is a term that often comes up when discussing the blockchain system. Although they are not identical, Ethereum and Cryptocurrency nevertheless remain widely misunderstood. Innovative technologies had to be created as a result from rising degrees of globalization. These groundbreaking innovations improve the speed of international trade. There are many technical experiments; some of them were successful, whereas others died or required development. The decentralized ledger technology, its benefits, and methods for consensus are described on this article.

Keywords: the pros and disadvantages, and consensus method of the digital currency blockchain.

GJCST-C Classification: LCC: QA76.9.B58

Blockchain Challenges: Advantages and Algorithms

Zeel B Dabhi [α] & Aishwarya [σ]

Abstract- Cryptocurrency is the innovation that has changed the way of life most significantly over the past ten years. Bitcoins is a term that often comes up when discussing the blockchain system. Although they are not identical, Ethereum and Cryptocurrency nevertheless remain widely misunderstood. Innovative technologies had to be created as a result from rising degrees of globalization. These groundbreaking innovations improve the speed of international trade. There are many technical experiments; some of them were successful, whereas others died or required development. The decentralized ledger technology, its benefits, and methods for consensus are described on this article.

Keywords: the pros and disadvantages, and consensus method of the digital currency blockchain.

I. Introduction

Innovative innovations had to be created as a result of the rising degrees of globalization. These novel technologies improve the efficiency of international trade. Here are many technical experiments; a handful of them were successful, while others died or required development. But without the advent of blockchain technology, a number of significant turning points are being reached, particularly in terms of computational innovations. The techniques that were utilized to produce this research centered on review of literature, analyses of the most commonly quoted projects, pattern findings, readings of reports, analysis of advances in technology, and research of the priorities of the major IT firms.

Cryptocurrency is a decentralized, trustworthy, and challenging to utilize for unlawful type of record keeping. On the opposite hand, Cryptocurrency is a type of electronic money that conducts operations between peers to peers using an open database called the Blockchain, or distributed ledger. Blockchain-based solutions is used in a number of different industries, including Cryptocurrency and Hyperledger's and intelligent contracts. Thus, a wide range of possibilities can be made using the technology of blockchain. The distributed ledger called Blockchain is undoubtedly a new sort of store. Although it can address one of the major issues relating to banking, this type of technology is quite intriguing to people. Ethereum is an innovation that combines a number of various technologies and tools, including consensus, networks of peers, the use of encryption, and arithmetic.

II. Blockchain Technology

It is a sort of modern technology in which a computerized register is employed to track operations throughout a decentralized computing infrastructure in order to prevent the operations throughout the machines from being changed retrospectively. Here, every member in the shared ledger gathers the details of each deal the other person engages in. The site does feature a scheduling mechanism, but it provides no way to delete an operation through it one time it has been officially completed.

a) The definition of the Blockchain technology

Among the most commonly used descriptions of the Blockchain system, that was created by John & Alan Tapscott, who says it is "an infallible electronic register that records economic event that can be configured to store not only financial activities but nearly anything of significance" [1].

b) The structure of the Blockchain technology

The digital ledger is made up of pieces that are introduced to the channel in a straight line at scheduled times [1]. However, the date, purchase, and hashes are present in all Ethereum implementations. The data included in the blocks of data varies on the distributed network of Blockchain.

A single block includes the preceding item's digital digest (Fig. 1).

Since every piece of knowledge in the hash algorithm is created on its own, it is impossible to alter any of its components.

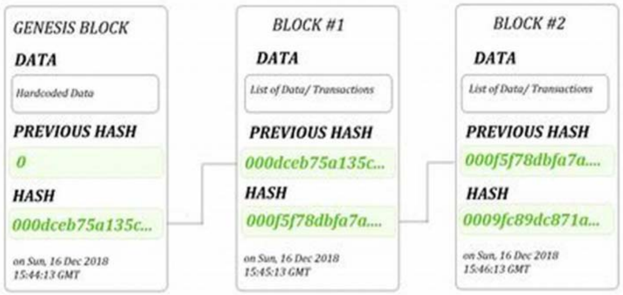


Fig. 1: The sequence of the hash value in the Blockchain

Author α: MCA DS, School of Engineering, Ajeenkya DY Patil University, Pune (MH). e-mail: zeel.dabhi@adypu.edu.in
Author σ: Ajeenkya DY Patil University, Pune (MH). e-mail: Aishwarya@inurture.co.in

The authentication procedure, including involves applying the personal key and license, is shown in Fig. 2. Verification begins after the authentication step is complete. (Fig. 3). If the resulting hash results are identical, the check is successful.

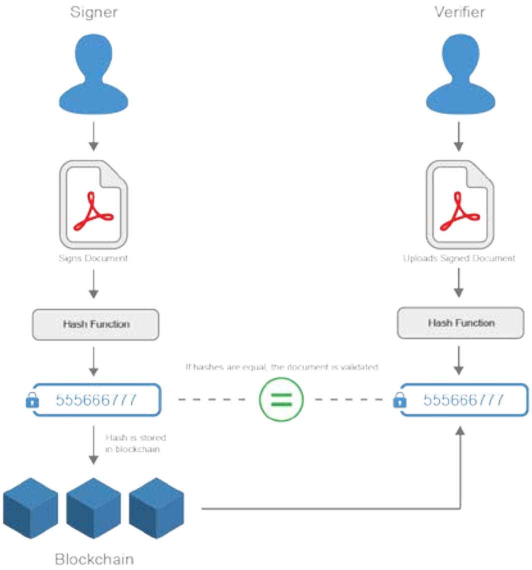


Fig. 2: The signing process in the Blockchain

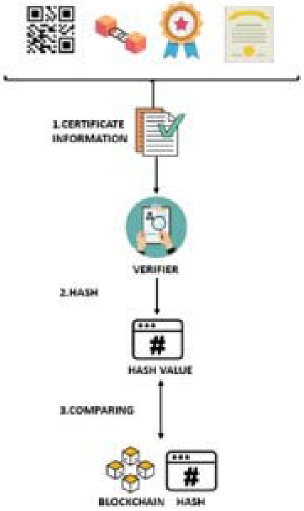


Fig. 3: The verification process in the Blockchain

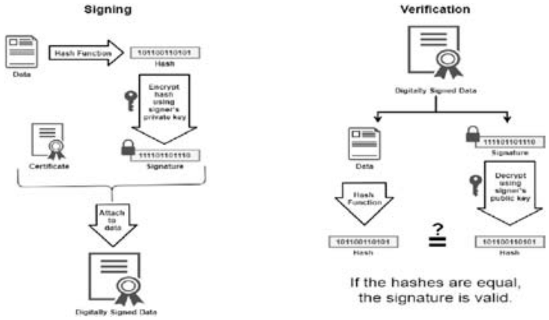


Fig. 4: The very simple shows, how blocks signing and verification processes work in the Blockchain

Fig. 5 illustrates the building block formation procedure. Every block in the current instance had the nonce, the Merkle shape, the date, the time, and the prior hashing value.

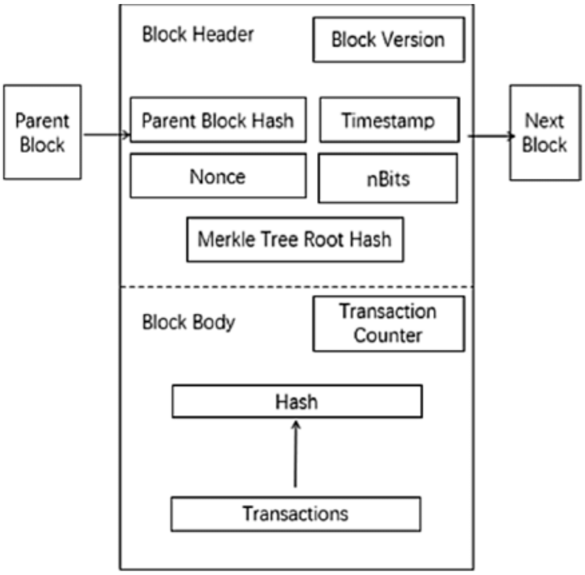


Fig. 5: The structure of the Blockchain

c) *What are the key components of blockchain technology?*

Distributed ledger:

➢ A distributed ledger is the shared database in the blockchain network that stores the transactions, such as a shared file that everyone in the team can edit. In most shared text editors, anyone with editing rights can delete the entire file. However, distributed ledger technologies have strict rules about who can edit and how to edit. You cannot delete entries once they have been recorded.

Smart contracts:

➢ Companies use smart contracts to self-manage business contracts without the need for an assisting third party. They are programs stored on the blockchain system that run automatically when predetermined conditions are met. They run if-then checks so that transactions can be completed confidently. For example, a logistics company can have a smart contract that automatically makes payment once goods have arrived at the port.

Public key cryptography:

➢ Public key cryptography is a security feature to uniquely identify participants in the blockchain network. This mechanism generates two sets of keys for network members. One key is a public key that is common to everyone in the network. The other is a private key that is unique to every member. The private and public keys work together to unlock the data in the ledger.

- For example, John and Jill are two members of the network. John records a transaction that is encrypted with his private key. Jill can decrypt it with her public key. This way, Jill is confident that John made the transaction. Jill's public key wouldn't have worked if John's private key had been tampered with.

III. Challenges

Additionally, blockchain science has applications in a number of commercial sectors. The medical field is one intriguing area where the blockchain technology is being used. Through the use of Ethereum for transferring costs via the digital currency, this meets everyone involved including medical facilities, medical facilities, and public health regulators by revealing consumers' expectations and maintaining the confidentiality of patients. If the public wanted to view the medical records of a person under the traditional framework, they'd have to fill out an inquiry form and send it to the registration location for permission. The details The buyer must pay an extra charge to the bookkeeper and get an invoice of payment after getting clearance. The receipt is subsequently presented by the details of the user to the registrations offices in order to get an electronic version of the medical records of the individual. But a patient's medical files. can be misplaced or copies made for nefarious intentions. Figure 6 illustrates the idea of a blockchain-based electronic medical record system.

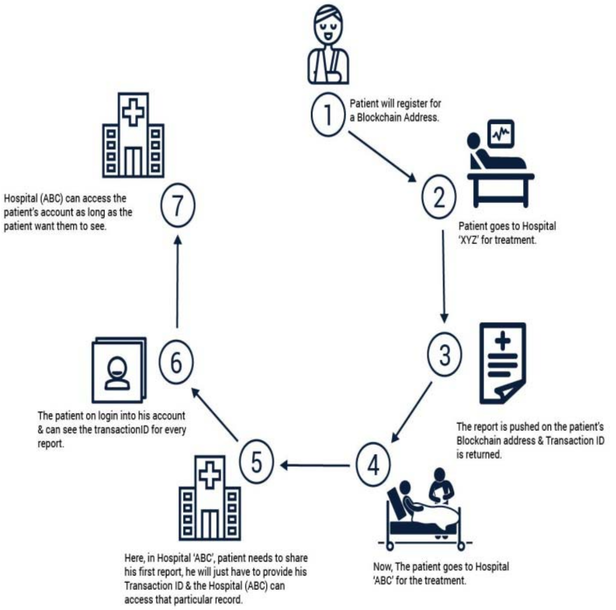

1
Patient will register for a Blockchain Address.
2
Patient goes to Hospital 'XYZ' for treatment.
3
The report is pushed on the patient's Blockchain address & Transaction ID is returned.
4
Now, The patient goes to Hospital 'ABC' for the treatment.
5
Here, in Hospital 'ABC', patient needs to share his first report, he will just have to provide his Transaction ID & the Hospital (ABC) can access that particular record.
6
The patient on login into his account & can see the transactionID for every report.
7
Hospital (ABC) can access the patient's account as long as the patient want them to see.

Fig. 6: The structure of the Blockchain

The Payment will indeed be put when such a data client asks a provider (a inpatient care facility) for a specific patient and the publisher approves. A main surgeon's and also the participant's consent are required before providing a participant's medical files to an info buyer so that just particular documents, such as medical files, are provided. The specifics of this procedure will be described in later study.

a) *Lack of adoption*

Ledgers work better and more efficiently when used by a large network of users. For instance, a cryptocurrency environment may require suppliers as well as users to sign up for such platform. On the opposite hand, according to APQC, only 29% of businesses are actively testing with or using cryptocurrency. Blockchain networks will continue inefficient & unmanageable without widespread usage.

There are certain signs, nevertheless, that its popularity of blockchain may grow. Businesses are progressively organising cooperative blockchain collaborations to address related issues and offer answers that can be helpful to everybody without sharing private data.

This reduces dependency on physical logs with adheres data set and helps to protect the integrity of the distribution network.

b) *The rising cost of blockchain implementation*

The key is making early stock assets. Costs related to execution may be too high for some businesses. Despite the fact that the majority of latest methods are free, hiring skilled software engineers who specialise in blockchains, paying licencing fees in the event that one wishes to switch to a for-profit program version, book keeping, and other costs all require a large investment. It is among the most significant challenges experienced for cryptocurrency.

c) *Scalability*

Durability is the key issue with it's own deployment. Cryptocurrency is not practical for sizable apps because, despite the fact that purchase networks could really control thousands and thousands of simultaneous transactions without experiencing any problems, atm machines for Crypto currency (about 3–7 exchanges per second) and Cryptocurrency (about 15-20 exchanges per moment) takes a long time.

d) *Security and privacy challenges*

Now, numerous organizations must abide by legal restrictions. With regards to important information, their clients have faith in them. Nevertheless, this information won't be completely private if it's all preserved on a public ledger. Here, blockchains in corporate or consortium settings may be used. Your personal data would still be protected, and you would only have access to what you needed.

Cybersecurity is a further essential component. Yet, only a small number of circumstances have robust processes that can deal with this. Even while blockchain-based apps, systems, and businesses are more secure than traditional pcs, criminals may still be able to access them.

He doesn't just want the authorities to safeguard our privacy. Ethereum ego IDs may enable us to gather and control our info. although there We've put in plenty of efforts towards creating new privacy procedures, including confirmation of negligible, but a new identity structure continues to be a long way off.

To learn whether cryptocurrency and Ml may be utilized for safe storage of information, visit the page on cryptocurrency and AI secure data handling. It is among the most significant challenges experienced for cryptocurrency.

e) Regulations

The very next aspect that you might run into trouble is with the lack of regulations. It is possible for fraud and price fixing to lead to a world economic catastrophe. As a reason, Cryptocurrency is the subject of a lot of unfavourable media coverage.

Although some nations have openly prohibited cryptocurrency, someone else has made vain attempts to control blockchain platform.

f) Criminal activities

The proliferation of bogus enterprises as well as other bad actors looking to take advantage of naive participants has been encouraged by the absence of strict regulations and indeed the notion that blockchains is still in its infancy. A number of prominent crypto trading scams have indeed occurred, along with the notorious Largest Cryptocurrency bitcoin hack in 2014 that almost brought out the entire sector.

g) Energy consumption

The fact that evidence of work, the most popular compromise technique, consumes a great deal of electricity seems to be another cause for concern. This makes it difficult for average users to access Distributed consensus networks, promotes the creation of big mining pools, inhibits decentralisation by pressuring users to join these pools, and creates global pollution.

h) 51% attacks

Block chain technology have an amazing feature. Certain are safer than in others. For instance, compared to centralised blockchain technologies, decentralised ledgers seem to be more susceptible to 51% attacks. For cryptocurrency traders who desire to hold financial funds on decentralised channels, this is what has created a few problems.

Several cryptocurrency platforms have been hampered by 51% assaults, wherein the criminals seize more than half of the channel's processing capacity. They take use of a flaw in decentralised systems that gives people access to over 51% of the processing capacity, giving them control over a chain. On systems that employ the concrete evidence paradigm, this frequently occurs. The architecture of blockchain technologies is distinct. Some are more secure than others. The decentralized blockchains, for example, are more vulnerable to 51% attacks than the centralized ones.

i) Low workforce availability

These nonfungible currency and Describe businesses have experienced a sharp increase in nonfungible assets & enterprises over the past year, which has caused problems in the labour market. As per current data, as startups and existing businesses search out best players, the demand for blockchain talent has surged by more than 300%.

j) Interoperability

One of the most important issues that must be addressed is interoperability, as this is one of the primary reasons businesses are yet hesitant to embrace blockchain technology. Most blockchains are maintained in isolation and do not communicate with other peer networks since they cannot transmit and receive data from a different blockchain-based system.

k) Lack of standardization

What standards does ethereum now follow? Despite the abundance of connectivity, there is no global standard. As a result of no global standard, there are issues with accessibility, rising costs, and complicated processes. Blockchain technology has no specific version, which discourages investment opportunities and entrepreneurs from getting involved entering the market.

l) Integration with legacy systems

Another issue is how to integrate blockchain solutions with an existing system. If a business chooses to use cryptocurrencies, they must typically entirely replace their outdated system or create a plan to properly connect the two techniques.

Additional problem is that businesses without software engineers limit access to the skill pool needed to take part in this undertaking. Reliance on an external source may make this issue worse. Yet, to implement the majority of market mechanisms, the business must commit a substantial amount of time and money.

m) Private key issues

In a decentralised environment, credentials that people hold in a centralised environment may have become exposed.

After a wallet has been created, they allow access to all of its data. If stolen, it puts everyone wealth and personal information in danger. If the wallet is stolen or annihilated, access is permanently gone. That is one of the riskiest impediments for the cryptocurrency Destroyed. It is one of the most dangerous blockchain implementation challenges.

IV. Advantages

The blockchain technology's main benefit is that it is not regulated. What does it mean for our lifetimes? Merely expressed, there is no requirement for cooperation only with formal leader or a third party organisation. This suggests there's not a mediator in the design and that decisions are made by all owners of such virtual cash. A system software keeps a record of material, so must be adequately safeguarded as there's a danger that now the documentation may well be compromised if an institution works with other companies and might end up in the wrong hands due to misuse. There is a potential that the process of securing the data will be time-consuming and expensive. Using Btc Whenever transfers have been conducted It has the potential that its process of hiding the data will be time-consuming & expensive. When using Bitcoins Utilizing similar hardware is possible to be avoided because send or receive with Bitcoin generate their own evidence of legitimacy and power can enforce the restrictions. Moreover, it suggests that the actions might be verified and managed as a single The primary advantage of the distributed ledger tech is its decentralized nature. What is it significant to our lives? It is not needed to collaborate with the central administrator or an outside company, to put it simply. Every action taken is saved on the the distributed ledger, and the data in these records is accessible to all users and is unable to altered or removed. The Bitcoin's openness, constancy, and reliability are demonstrated by the outcomes resulting from this documentary.

- Each activity is recorded just on shared database, where the data is obtainable and cannot be changed or withdrawn. The outcomes of this film serve as evidence of the Blockchain's transparency, consistency, and dependability.
- Its Bitcoin relies on the belief of a number of people who are strangers to one another for its reliability. The key concept is that these are genuine, valuable interactions seen between unidentified parties. Since there might be additional provides valid and information, trust may be enhanced even more.
- When operations are approved and disseminated across the the distributed ledger, immutability is guaranteed. It isn't feasible to modify or remove an operation once it is linked with the Internet. It also hinges on the type of structure; if anything's centrally managed it might be modified or removed since a single individual makes a choice. But with a decentralized system, like the the distributed ledger, each purchase that is connected to the system gets duplicated to each computer in the community. This feature renders the public ledger technology impermeable and unbreakable. Data integrity is ensured when activities are authorised and spread throughout the public ledger. After an action has been uploaded to the web, it is impossible to change or delete it So it depends on the organization's system; if something is locally administered, it could have to be changed or eliminated because only one person can decide. And even though, in a decentralised system, such as the public blockchain, every buy linked towards the framework was mirrored across all of the computers with in group. The underlying blockchain has been rendered impenetrable and indestructible by this function.
- The Chain provides its clients with the ability to control every transaction and data point. Whenever a hacker has access to advanced technology, they can alter or delete the data on the Bitcoins It has enough processing power to change or erase every piece of content just on country's notebooks, along with the content of the electronic record, prior to the preceding batch is placed in. Should there be few Contrarily, with numerous notebooks, your connection seems to be more transparent and safer. Companies on the Ledger, that is, the technology, are much more susceptible to attack.
- The blockchain technology is designed to be able to detect any problems and, if necessary, correct them. Staying identifiable is a feature of the Cryptosystem. The interaction between technologies and the represent the data achieves a substantial degree of safety upon every user's admission towards the network. As a result, each Bitcoin user is given a unique identifier which is linked to the account. The reliable encoded lanyard is yet another element contributing toward the Channel's security.
- The year and day the document was created, as well as the person's ID. The present incarnation of mined includes its merkel's stem, it contains information on earlier buys and associated hashes. The component automatically returns that amount. In this case, it is impossible to alter any particular part of the hash function.
- That advantage is really the fast performance. It normally takes a lengthy time to finish and initiate a contribution further into banking institution. By using cryptocurrency technologies, the cleaning and initialising procedure can be completed in a fraction of the time—from around five days to just few seconds or less.

a) *Immutability*

Blockchain technology enables data integrity, making it hard to alter or change data that has already been committed. As a result, the cryptocurrency stops data manipulation on the internet.

Conventional data are not impervious to change. The CRUD approach makes it simple to erase and replace data, while the traditional database employs creation, access, update, and delete at the primary level to ensure proper application performance. Such information is vulnerable to modification by malicious employees or outside hackers. Blockchain supports immutability, meaning it is impossible to erase or replace recorded data. Therefore, the blockchain prevents data tampering within the network.

b) Transparency

Blockchain is decentralized, meaning any network member can verify data recorded into the blockchain. Therefore, the public can trust the network.

On the other hand, a traditional database is centralized and does not support transparency. Users cannot verify information whenever they want, and the administration makes a selected set of data public. Still, however, individuals cannot verify the data.

c) Censorship

Blockchain technology is free from censorship since it does not have control of any single party. Therefore, no single authority can interrupt the operation of the network.

Meanwhile, traditional databases have central authorities regulating the operation of the network, and the authority can exercise censorship. For instance, banks can suspend users' accounts.

d) Traceability

Blockchain creates an irreversible audit trail, allowing easy tracing of changes on the network.

The traditional database is neither transparent nor immutable; hence, no permanent trail is guaranteed.

e) Open

One of the major advantages of blockchain technology is that it is accessible to all means anyone can become a participant in the contribution to blockchain technology, one does not require any permission from anybody to join the distributed network.

f) Verifiable

Blockchain technology is used to store information in a decentralized manner so everyone can verify the correctness of the information by using zero-knowledge proof through which one party proves the correctness of data to another party without revealing anything about data

g) Permanent

Records or information which is stored using blockchain technology is permanent means one needs not worry about losing the data because duplicate copies are stored at each local node as it is a decentralized network that has a number of trustworthy nodes.

h) Free from Censorship

Blockchain technology is considered free from censorship as it does not have control of any single party rather it has the concept of trustworthy nodes for validation and consensus protocols that approve transactions by using smart contracts.

i) Tighter Security

Blockchain uses hashing techniques to store each transaction on a block that is connected to each other so it has tighter security. It uses SHA 256 hashing technique for storing transactions.

j) Immutability

Data cannot be tampered with in blockchain technology due to its decentralized structure so any change will be reflected in all the nodes so one cannot do fraud here, hence it can be claimed that transactions are tamper-proof.

k) Transparency

It makes histories of transactions transparent everywhere all the nodes in the network have a copy of the transaction in the network. If any changes occur in the transaction, it is visible to the other nodes.

l) Efficiency

Blockchain removes any third-party intervention between transactions and removes the mistake making the system efficient and faster. Settlement is made easier and smooth.

m) Cost Reduction

As blockchain needs no third man it reduces the cost for the businesses and gives trust to the other partner.

V. Disadvantages

Although the account individuals has advantages, additionally there are downsides or problems with such kind of technology as well. The main problem with Crypto currency is how much electricity it consumes. For a continuous registration to be maintained, power must be provided.

If a new block appears, it engages with the rest of the nodes simultaneously. On this basis, truth is generated. The show's hidden content are engaged on a variety of problems every moment during the day in an effort to check functioning. They are using a lot of CPU resources. Every node offers high levels of dependability, ensures quality support, and renders data stored on the decentralized system dissent & unchangeable for all time. Even while the digital ledger provides benefits, there are drawbacks or difficulties with this form of technology. The significant power use of the Ethereum is its biggest drawback. Power usage is required to maintain an ongoing register.

Such processes waste precious resources because every node must replicate the action. Bit coin Bit coin has expanded as a result of the addition of additional bits towards the network and rising computational demands. Not all nodes have the national resources offering. There really are two issues: the shorter logbook is the primary one since Both preservation and transparency of a Network are broken since the sites are unable to maintain the complete block chain; additionally, the Block chain shifts to a more centralised form of consent. A significant disadvantage of Ethereal is its excessive price. The average cost of the transfer is between $75 to $160, without electricity consumption taking up most of the costs [12]. One of the contributing factors to this situation has previously been highlighted. Additional reason is that it requires a substantial initial expenditure.

a) Speed and performance

Blockchain is considerably slower than the traditional database because blockchain technology carries out more operations. First, it performs signature verification, which involves signing transactions cryptographically. Blockchain also relies on a consensus mechanism to validate transactions. Some consensus mechanisms, such as proof of work, have a low transaction throughput. Finally, there is redundancy, where the network requires each node to play a crucial role in verifying and storing each transaction.

b) High implementation cost

Blockchain is costlier compared to a traditional database. Additionally, businesses need proper planning and execution to integrate blockchain into their process.

c) Data modification

Blockchain technology does not allow easy modification of data once recorded, and it requires rewriting the codes in all of the blocks, which is time-consuming and expensive. The downside of this feature is that it is hard to correct a mistake or make any necessary adjustments.

d) Scalability

It is one of the biggest drawbacks of blockchain technology as it cannot be scaled due to the fixed size of the block for storing information. The block size is 1 MB due to which it can hold only a couple of transactions on a single block.

e) Immaturity

Blockchain is only a couple-year-old technology so people do not have much confidence in it, they are not ready to invest in it yet several applications of blockchain are doing great in different industries but still it needs to win the confidence of even more people to be recognized for its complete utilization.

f) Energy Consuming

For verifying any transaction, a lot of energy is used so it becomes a problem according to the survey it is considered that 0.3 percent of the world's electricity had been used by 2018 in the verification of transactions done using blockchain technology.

g) Time-Consuming

To add the next block in the chain miners, need to compute nonce values many times so this is a time-consuming process and needs to be speed up to be used for industrial purposes.

h) Legal Formalities

In some countries, the use of blockchain technology applications is banned like cryptocurrency due to some environmental issues they are not promoting to use blockchain technology in the commercial sector.

i) Storage

Blockchain databases are stored on all the nodes of the network creates an issue with the storage, increasing number of transactions will require more storage.

j) Regulations

Blockchain faces challenges with some financial institution. Other aspects of technology will be required in order to adopt blockchain in wider aspect.

VI. Consensus Algorithms

Each participant of the decentralized network must agree on the validity of a payment, its participation or deletion first from log, along with the subsequent blocks to just be recorded. The issue at hand is what each of these people can concur here on proper scenario given the facts on the tape until they all reach consensus. Any crypto currencies organization needs to agree on the past of operations because distributed systems lack governance or confidence amongst information system.

→ *Objectives of Blockchain Consensus Mechanism:*

a) Unified Agreement

- One of the prime objectives of consensus mechanisms is attaining unified agreement.
- Unlike centralized systems where having a trust on authority is necessary, users can operate even without building trust in each other in a decentralized manner. The protocols embedded in the Distributed blockchain network ensures that the data involved in the process is true and accurate, and the status of the public ledger is up-to-date.

b) Align Economic Incentive

- When it comes to building a trustless system that regulates on its own, aligning the interests of participants in the network is a must.
- A consensus blockchain protocol, in this situation, offers rewards for good behavior and punishes the bad actors. This way, it ensures regulating economic incentives too.

c) *Fair & Equitable*

- ➢ Consensus mechanisms enable anyone to participate in the network and use the same basics. This way, it justifies the open-source and decentralization property of the blockchain system.

d) *Prevent Double Spending*

- ➢ Consensus mechanisms works on the basis of certain algorithms that ensures that only those transactions are included in the public transparent ledger which are verified and valid. This solves the traditional problem of double-spending,
- ➢ i.e., the problem of spending a digital currency twice.

e) *Fault Tolerant*

- ➢ Another characteristic of the Consensus method is that it ensures that the blockchain is fault-tolerant, consistent, and reliable. That means, the governed system would work indefinite times even in the case of failures and threats.
- ➢ Currently, there are a plethora of Blockchain consensus algorithms in the ecosystem and many more are heading to enter the marketplace. This makes it imperative for every Blockchain Development Company and enthusiastic Entrepreneur to be familiar with the factors that defines a good consensus protocol, and the possible effect of going with a poor one.

f) *The Bottom Line*

- ➢ Consensus mechanisms have become an essential aspect of distributed ledgers, databases, and blockchains because much of the world is becoming more digital. Ownership of physical assets is being tokenized on ledgers and blockchains, people without access to financial services have access through blockchains, and businesses need data security more than ever.
- ➢ Consensus mechanisms verify data inputs and outputs, which translates to automatically auditing the digital transactions that are common today—without human oversight or intervention. They create an environment where you don't need to trust that the other party in a transaction is honest because they ensure the information is unalterable and secure.

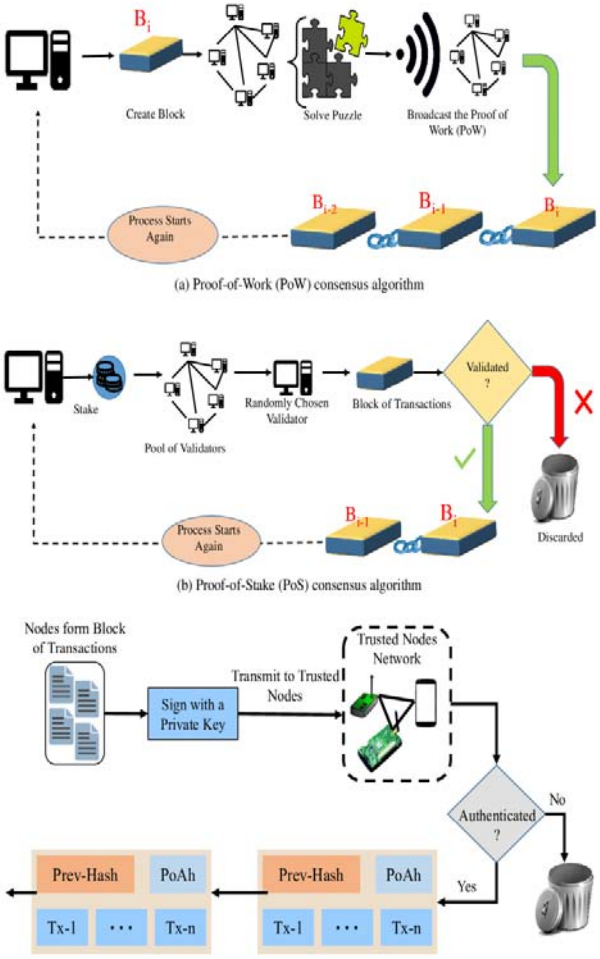
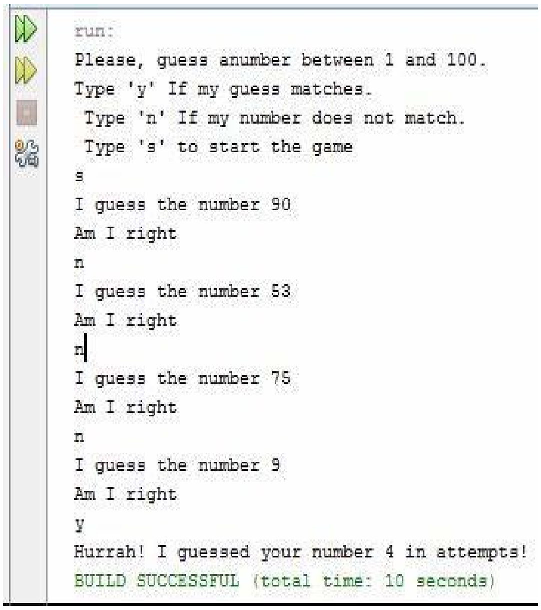


Fig. 7: Various consensus algorithms which can be used in a blockchain technology.

g) *Proof of work*

- There will be proof of promise soon. This system composed of crypto currencies uses the early acceptance process known as confirmation of labour. The argument for such working notion is founded on the notion that every organisation in some kind of a node hierarchy competes to figure out the right hashing value in order to add a new transactions to the block chain and get the payment, as seen in image 8.
- There are numerous unique sorts of employment certification in literature. Demonstrating work is a great method to negotiate an agreement, but it has a major economic disadvantage. Costly computer-based labor evaluation. This motivates us to propose fresh agreement strategies to deal with the evidentiary labor.



```
run:
Please, guess anumber between 1 and 100.
Type 'y' If my guess matches.
 Type 'n' If my number does not match.
 Type 's' to start the game
s
I guess the number 90
Am I right
n
I guess the number 53
Am I right
n
I guess the number 75
Am I right
n
I guess the number 9
Am I right
y
Hurrah! I guessed your number 4 in attempts!
BUILD SUCCESSFUL (total time: 10 seconds)
```

Fig. 8: Proof of Work consensus pseudo code

h) *Proof of stake*

- Ledgers use the proof of stake (Pops) consensus process. It establishes which individual or persons authenticate brand-new transactional chunks yet are rewarded by being rewarded successfully. Undeservedly, crypto currency seems to have a notoriety for just being difficult to understand and impregnable. proof of stake consensus algorithm there is less computation performed.

1. Delegated Proof of Stake (DPoS)

- One decision matrix is delegation to demonstrate stake. The primary concept behind it is that the shareholders should be allowed to choose a manager who will support you and possibly pass along other benefits as well. These leadership can indeed be elected or removed at multiple times over time, and they create bricks since round form instead of in a sequence.
- In Dopes, the miners stake their coin and vote for a particular number of delegates, in a way that, the more they invest, the more precedence they receive. They get rewards in terms of coins or transaction fees.
- In DPoS, there are 21-100 delegates charged periodically and assigned to deliver their blocks. Having fewer delegates allows for an efficient organization to design time slots for publishing blocks in the network. In case of, insufficient, invalid, or missing block publishing, the miners vote them out to be replaced with other selected delegates.
- As DPoS works on the stake-weighted voting system, it has become one of the fastest growing and adapted blockchain consensus models.

2. Leased Proof of Stake (LPoS)

- LPoS operates on Waves' blockchain platform and is an advanced version of PoS.
- In LPoS, users lease crypto tokens to the node that wants to act as a block producer for the network. A node with the maximum number of staked tokens is more likely to be selected for the next block generation as well as receive rewards.
- It also helps users with smaller tokens who might not have been eligible for participating as the blockchain creator in the traditional proof of Stake process in pooling their assets while enhancing their chances of receiving network transaction fees' share.
- The leased proof of stake consensus algorithm is best for networks with high high-technical requirements for operating full nodes capable of verifying and validating transactions.

i) *Delegated proof of stake*

Delegated proof of stake is another consensus algorithm. Its idea main about the stakeholders able to select a leader who votes for them and potentially passes some rewards as well. These leaders can be voted in or out at different times and they produce blocks in around robin fashions so they do not get to put them all in a row.

1. Leased Proof-Of-Stake (LPoS)

- The leasing stake evidence is also another variation on the traditional evidence of stake. Its Wave propagation network exposed us to the based on block chain technology consensus method. Similar to every other system for block chains, Waters wants to make sure to provide a better catch with less electricity usage.
- There were several restrictions on staking in the original proof of stake. Those with a little number of coins might never truly take part in the staking. The infrastructure is capable of being managed to keep by a small number of people who have more currencies to donate...

j) Proof of activity

Proof of activity consensus algorithm is proposed, it is a hybrid approach that includes proof of work and proof of stake. It starts with a proof of work allowing minors to mine empty template without any transactions then it switched to proof of stake where validators select a block to sign and rewards get split between both proof of work minor and the stake.

k) Proof of authority

The Evidence of Activity electricity usage was also resolved by this protocol. Di Gooseneck faucet . the faucet et al. presented an official proof or unanimity, with the idea focusing on auditors or credentials that are approved or public identity, requiring them to manage what is known as an authorities station.

l) Proof of space or proof of capacity

The distinction between several work evidence and then this methodology is that here, the network node reserves a certain amount of storage or storage in to resolve challenging phrases in so it can get towards the ability to add another transaction, as opposed to the use of computational power or calculation power. It is a wise strategy to apply proof of work in more depth with additional resources.

m) Proof of importance

It is a more comprehensive variant of stake verification, with the premise that could for ought to be included in addition towards the serious risk or number of coins. The drawback of it is the energy wastage it causes.

It overcomes Transaction processing restrictions by giving priority to miners according to the amounts of transactions matching to each denomination. There in context of Poi, the greater the number of payments between and within a user's crypto currency, the greater the likelihood that even these users will be awarded crypto currency coal mines.

n) Proof of burn

It is a more comprehensive variant of stake evidence, with the premise that some measures will be factored in in addition towards the serious risk or number of bit coins. The drawback that it brings is the environmental wastage it causes.

1. The Pros and Cons of the Proof-of-Burn Algorithm

- The main objective of burning the coins is to find out the strength. We are aware that lengthy players constantly keep coins for a very long time so as to benefit.
- By providing less strong currency with huge commitment, our system benefits such protracted stakeholders. Besides which, this improves decentralization and develops a more equitably spread networks.

2. Practical byzantine fault tolerance

A useful bureaucratic fault detection technique addresses the problem of hostile nodes within a network. The dispersed network device may well be enabled to reach an accord regardless of certain nodes that are failing or delivering false info because the virtual pad uses a replicate technique to accommodate bureaucratic defects.

- PBFT makes an effort to offer a robust logic replicating that functions even in the existence of malicious nodes.
- A primary node (or the leader) and numerous subsidiary nodes are successively arranged in micro services with bet (or the backups). Any eligible node in the system has the ability to switch form intermediate to major in the case of a major node failure. All trustworthy locations can participate using the majority rule.

3. Delegated Byzantine Fault Tolerance (dBFT)

- Daft is a consensus method that offers outstanding fraud protection. The mining are given the duty of voting for the members but are not contingent on our participation quantities, which is somewhat similar to the Dopes approach. The only requirements for becoming a deputy yourself are the appropriate tools, biometric identification, and 10,000 GAS.
- Genuine voting is used by identification to choose the consensus algorithm, this enhances the method and cuts down on condition that makes for payments. The chosen team of auditors then generates new blocks using the BFT process.

o) Ripple

Inside one bigger system, the ripples protocol performs well. It can make use of the existence of reliable thread. Instead of operating in a competition fashion, it operates cooperatively; the nodes collaborate to determine the authenticity and sequence of events with in channel.

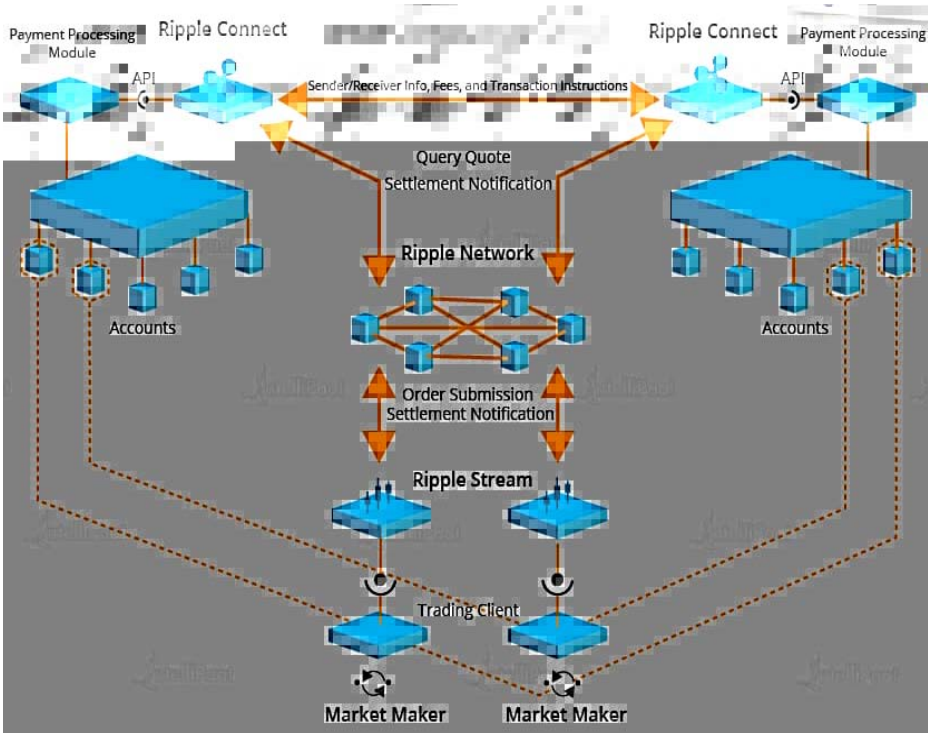


Fig. 8: Ripple Blockchain

p) *Proof of Elapsed Time (PoET)*

- Among the top voting systems is Poet. This specific technique is primarily utilized in public block chains block chain networks, whereby networking access requires authorization. Those authorization systems must choose ballot or oil rights policies.
- The Poet techniques employ a specific strategy for masking openness over the entire system to guarantee that everything operates as planned. Since the networks required identity before allowing a user to engage the mining, the Approval methods also guarantee a secure entrance into in the platform.

→ *Properties of a Good Blockchain Consensus Mechanism:-*

1. Safety

- Together all stations in a competent consensus algorithm have able to produce outcomes that seem to be legitimate in accordance with the program's requirements.

Inclusive

- A strong consensual smart contract makes sure that each specific system node gets involved in the election system.

Participatory

- A decent convention on Ethereal entails a system in which all sites engage and help to maintaining datasets. updating databases on Blockchain is called a good consensus model.

Egalitarian

- Giving each ballot obtained first from network similar worth and importance seems to be another quality of a successful process.

→ *Consequences of Choosing a Bad Consensus Protocol:*

2. Blockchain Forks

- Using a subpar consensus mechanism technique makes the network more susceptible. Ethereal conflicts are but one weakness that block chain enthusiasts and developers must deal with. In simpler terms, a crypto currency splitting occurs when one or so more chains split off into another one or more.
- In the video that is posted below, a thorough explanation of block chain forks and their varieties is provided. In the video that is posted beneath, a comprehensive description of crypto currency forks and their varieties is provided.
- That whenever a fork in the Ethereal happens, the app comes to operate erratically, leading to two or more diverging nodes forward.

3. Poor Performance

- That whenever a poor block chains method is taken into account, whether the node malfunctions or experiences net division. As a result, the software's latencies grows and the operation of transmitting letters amongst servers takes longer, lowering its level of play.

4. Consensus Failure

- Majority failures is a result of using a poor trust model in your company strategy. In this case, a small percentage of nodes refuse to engage inside any transaction, and without their voting, the agreement is unable to produce the intended and correct results.

VII. Conclusion

It is clear that crypto currency has several benefits and applications, including the capacity to operate in a decentralized mentor net devoid of a centralized government and to send money over the globe more cheaply. Digital medical records using block chains. It will take into account how a foreign entity can utilize or seek a child's health history from a medical facility or other body while violating the participant's right to privacy.

Crypto currency is dependable and unbreakable due to its benefits, including visibility, confidence, extra copies of activities, and a decentralized database. The aforementioned threats might only affect how the system functions, not the innovation itself.

We examined lightning network in this study and underlined the most recent research on

In this survey, we presented a survey of blockchain technology and highlighted the latest studies in blockchain and consensus algorithms.

Given the number and complexity of these blockchain issues, it would be unrealistic to think they are not major roadblocks to its adoption. In general, though, many of blockchain's greatest obstacles reflect growing pains typical with any new technology. Blockchain advocates will need to persuade their organizations to take similar risks, establish comparable relationships, and make similar trade-offs in other business areas to make a business case for adoption.

Acknowlegment

We would like to thank our Professor Aishwarya, for his invaluable guidance and support throughout the research process. His expertise and insights were instrumental in shaping the direction and focus of our research. We are also grateful to the MCA Data Science at Ajeenkya DY Patil Universityfor providing us with the resources and support we needed to complete this project.

References Références Referencias

1. Julija Golosova, Andrejs Romanovs., the Advantages and Disadvantages of the Blockchain Technology, November 2018.
2. Pinyaphat Tasatanattakool, Chian Techapanupreeda, Blockchain: Challenges and Applications, · January 2018.
3. Stefan Forsstrom, Blockchain Research Report, December 2018.
4. Samar Al-Saqqa, Blockchain Technology Consensus Algorithms and Applications: A Survey, 30 December 2019.
5. Soliman Soliman, Yao Xu, Yifei Shen, blockchain technology, | April 2019.
6. Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin pdf. 2008
7. Popov, Serguei. "A probabilistic analysis of the nxt forging algorithm." Ledger. 2016.
8. Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An over□view of blockchain technology: Architecture, consensus, and future trends." In IEEE International Congress on Big Data. 2017.
9. Blockchain, April. 10, 2020
10. R Bhme, N Christin, B Edelman, Bitcoin: Economics, technology, and governance, 2015.
11. M Iansiti, KR Lakhani, The truth about blockchain, 2017.
12. M Crosby, P Pattanayak, S Verma, V Kalyan Raman, Blockchain technology: Beyond bitcoin, 2016.
13. "History of bitcoin," Nov 2018. Available: https://en.wikipedia.org/wiki/History of bit coin.
14. CNNMoney, What is Bitcoin, [online] http://money.cnn.com/infographic/technology/what-is-Bitcoin/.
15. Vitalik Buterin, Ethereum and The Decentralized Future, April 2015.
16. Christian C., Elli A., Angelo De Caro, Andreas K., Mike O., Simon S., Alessandro S., Marko V,. et al, Blockchain, cryptography, and consensus, June 2017.
17. Ripple, Ripple Net, [online], https://ripple.com.
18. Eray Eliaçık, Blockchain challenges, May 30 2017.