IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

# An Absolute Introduction and Overview of Modern Blockchain Technology

Atriya Patel, Arpit Patel, Queeny Jain, Manan Mehta, Apurva Patel

*Pandit Deendayal Energy University- PDEU, India*

A R T I C L E I N FO

***Keywords:***
Blockchain,
Decentralization,
Cryptography
Architecture

A B S T R A C T

In modern era blockchain technology has become favourite candidate to become the next big thing due to its vast applications and solid cryptographical fundamentals. Today blockchain is not just a database but a backbone of decentralized finance. Individual developers have discovered various applications of blockchain and successfully implemented it in current environment. In this paper we will discuss about architecture, components, applications, environmental impact and possible advancements in future of blockchain technology. This paper explains core fundamentals and specific use cases in simpler way which will be useful to understand for beginner level blockchain enthusiast and students.

## 1. Introduction

Blockchain is cryptography based decentralized, fast, secure and immutable network of database known as ledger which contains details of transaction and tracking of an asset. These assets can be physical or digital which possess any value. Using blockchain technology these assets can be tracked, maintained and even traded on a decentralized network. These features of blockchain made it interesting in many fields where data record has to be secured from others. Today governments in various sectors to multinational corporations are using blockchain technology to store immutable sensitive data to avoid the corruption and keep the track of items which are valuable to country. Also, blockchain is very secure due to transparent structure and participation of users in its maintenance. Finance related transactions and businesses requires high speed transaction data records and confirmations with very high accuracy which can be achieved by blockchain due to its cost effectiveness and atomic transaction confirmation rate.

### *1.1. Aim*

To provide brief information about blockchain and its components along with important use cases and analyse the scope of the technology in the upcoming future and other aspects such as security, cost efficiency, effect on global economy etc. and to come up with a conclusion.

### *1.2. Scope of this paper*

This paper contains important aspects relate to blockchain technology which provides in depth analysis of it. These aspects highlight the information and fact related to blockchain and covers the modern use cases currently trending on in world of internet. It also discusses the factors related to environmental impact and issues related to its security and market demand. Each aspect is analysed based on latest current situation of the blockchain technology in digital world and provided with good example. In world of modern computing blockchain technology's conurbation in cryptographic algorithm is remarkable due to its new innovative way to use existing algorithms which is also discussed in the report. This report also eliminates the myths about the blockchain and discusses the security issues related to cryptocurrencies which uses blockchain as its core element.

## 2. Detailed Overview and applications of the blockchain systems

This section highlights the various aspects related to blockchain technology which includes historical development, applications, specific use cases, technological and business challenges, policies and future market share prediction along with disadvantages related to environmental issues and expect on current banking-based finance sector, valuation analysis.

### *2.1. Historical development of the blockchain*

Following timeline highlights the evolution done in the blockchain technology in past three decades.

- **1990:** Concept of distributed computers were enlightened by mathematics with help of cryptography by Martin Hellman and Whitfield Diffie. Together they developed an algorithm named Diffie-Hellman which divides an encrypted key into a pair of public and private key.
- **1991:** Scott Stornetta along with Stuart Haber implemented and improved this algorithm using cryptography and deployed a secure chain of blocks on a computer network.
- **2008:** An anonymous man having identity Satoshi Nakamoto released a whitepaper of first ever crypto currency titled **Bitcoin: A Peer-to-Peer Electronic Cash System.**
- **2009:** Satoshi Nakamoto created Bitcoin and introduced the implementation of Blockchain concept to create a decentralized ledger maintained by people transparently.
- **2010:** Many Commercials and internet websites started accepting bitcoin as a cash less payment option. Governments noticed use of bitcoin for criminal activities.
- **2014:** Discovering the benefits of blockchain technology many government and organization projects started adopting blockchain technology to secure sensitive information and to keep a track of it and Blockchain 2.0 was introduced.
- **2015:** Smart contracts were introduced by Ethereum blockchain which was a first step towards Decentralized autonomous organizations. It also accelerated the finance and business-related transactions with improved security.
- **2017:** Using smart contracts many corporations started building their own network among Ethereum eco system and introduced a new market for Decentralized applications.
- **2018:** Many corporations started to provide a permissioned blockchain network solutions to businesses and finance firms.
- **2020:** Adoption of blockchain based cryptocurrencies among people accelerated at exponential rate and global cryptocurrency market passed market capitalization of 1.5 trillion $.

This timeline data points that blockchain have discovered many new use cases with cryptographic algorithms and along with blockchain many new algorithms in cryptography were also introduced and a new field in computer science and engineer were established which delt with blockchain technology.

## *2.2. Structure of a blockchain based DAO*

As a blockchain network is a shared and distributed among computers a working Blockchain structure do not require much manpower instead it requires Hardware power. As a blockchain is decentralized ledger it is highly depended on people maintaining and operating a nod of blockchain using computers. More the computers more powerful and secure the blockchain network is [1]. For example, a Decentralized Autonomous Organization (DAO) is a type of an organization which runs on a software code using specific instructions inserted by Smart Contracts based on blockchain. These organizations need just a few people to maintain it and hardware power to operate it is contributed by a group of users known as validators. A validator confirms the transaction with a specific validation method. if same transaction is confirmed by all other validators, then only the transaction is completed and delivered to user hence DAO is transparent and doesn't require much man power [1].

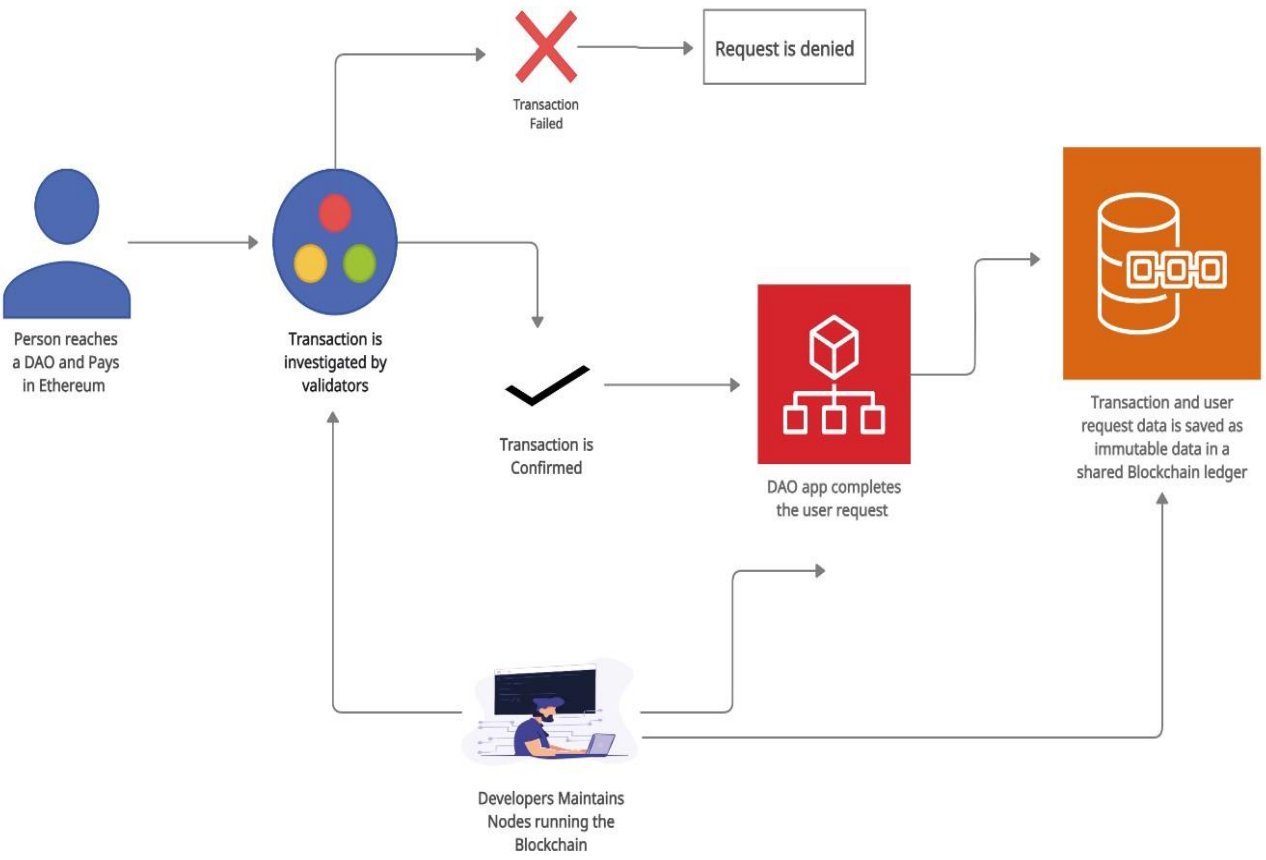


**Fig. 1.** Decentralized Autonomous Organization working process

Diagram above clears that how hardware plays an important part in a structure and operation of blockchain but to maintain the transparency and data inside blocks it's important to have humans for regulations. Many DAO pays people for regulating and becoming a validator of the blockchain. Higher the number of validators less the chances of error in verification occurs hence secure the blockchain becomes. This system is decentralized and more effective and secure compare to centralized organizations due to transparency and less involvement of sensitive bank details hence it also solves the issue of privacy on internet.

### *2.3. Detailed explanation of transactions made on blockchain*

When any type of request is made to a blockchain network it follows certain rules and verifies the request to store the data in the ledger. These requests can be a transaction, trade or any kind of information which is immutable. When the verification process is completed then only the requested data is written in the network [2]. This process is done across all the ledger repeatedly until a specific number of conformations are achieved.

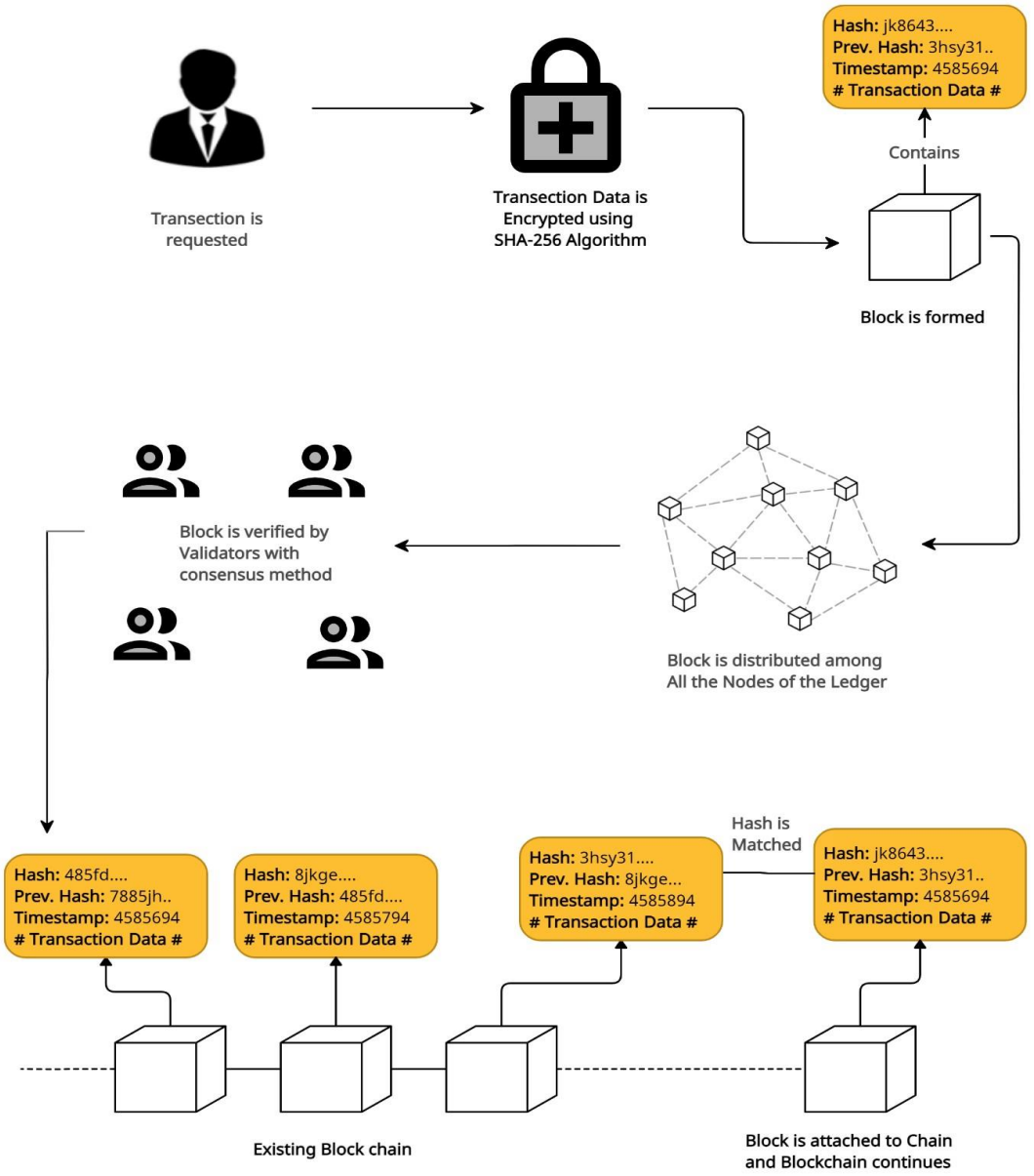


**Fig. 2.** Transaction completion process simplified

Here is a point wise explanation of Fig. 2. which explains the process of working of blockchain network

1. When a transaction is requested on blockchain. A block containing information about transaction along with timestamp and hash is formed.
2. The block contains information of transaction, Timestamp, Hash of previous bock and Hash of block itself, size of block.
3. Hash is a digital finger print of the block which is generated by cryptographic hash algorithm SHA-256. This is one way function type algorithm.
4. This block is sent to every node of the blockchain network to be verified by validators.
5. Each node in network is peer to peer which contains entire copy of blockchain data.
6. Now the previous hash of new block is matched with blockchains existing block and if the match is successive then verification process of block is said to be completed.
7. Once every Node in the network verifies the block by their own consensus method the block is joined with other existing blocks of chain and blockchain continues.
8. Now if some of the validators tries to corrupt or change the data inside their received block it can be noticed by other validators and they can eliminate the corrupt block and validator.
9. Once the block is added and transaction is completed validators receive their award.

## *2.4. Description of the different components of blockchain*

In this section we will discuss about components which are used in blockchain. These core components are responsible for working of the network across the scope. We will learn about components showed in Fig. 2.

1. **Ledger**
   It is a database which contains entire state of blockchain and transaction details. It is distributed among shared nodes

2. **Block**
   A block in blockchain records the transaction data which is yet to be confirmed. It stores the data in encrypted form along with other important details. Blocks together are joined each by other with digital chain of hash forms a blockchain. A block may contain following details inside it,

   1) Transaction Data
   2) Timestamp
   3) Hash (Digital Fingerprint)
   4) Hash of previous block
   5) Size of the block

3. **Node**
   A blockchain node is a one-way runtime program which allows user to create and develop services on distributed network and contribute to decentralized system. Every node within network transfers the details of blocks, transactions and contains a copy of entire ledger network in storage. These nodes are responsible for flow of data and validation of the block data. By using specific consensus method Node owners can become validators and can receive small income from transaction amount as a fee [2].

4. **Validators**
   Validators are the one who operates and maintains a node in a ledger. Validators are responsible for maintaining the quality and security of the ledger by verifying the blocks and attaching them safely to the blockchain network using consensus mechanism. If majority of validators hardware security is compromised then corrupt blocks will enter the network and it can cause the blockchain to collapse. Hence higher the validators higher the security of blockchain [2].

**5. Consensus**

A consensus protocol is a fault tolerant protocol which is used in blockchain systems to verify the blocks which is yet to be added in the chain. In order for nodes to verify the block majority of the Node owners must agree on decision of whether the block is authorized or not. There are two popular type of consensus mechanism [3],

1) **Proof of Work:** It requires huge computing power to solve a complex mathematical problem which applies brute force attack to SHA-256 algorithm encrypted block by matching various generated hash with hash of block [3]. If First X digits of generated hash matches with hash of block then block is mined and verified. Here block miner is awarded with a reward. X is difficulty index which can be adjusted according the need. There are many problems with this mechanism which is discussed in section 2.8.

2) **Proof of Stack:** In this mechanism people operating nodes must stack their earned reward for a specified time. During this time all validator's earnings are locked and if any how validator tries to validate a corrupt block his/her earnings will be liquidated and their node will be removed from network [3].

## *2.5. Technological and business challenges and possible solutions*

A growing number of companies have expressed their will to enter the blockchain arena. But after some number of years within which their focus was mainly on the advantages of blockchain in various areas, in terms of speed, costs, streamline operations and increased efficiency, their attention is now turned to the assorted challenges and bottlenecks that are preventing widespread adoption [4].

### *2.5.1. Challenges*

**1) Blockchain has a picture problem**

First of all, there's a reputation challenge. Blockchain continues to be abundantly connected to the crypto world within the mind of the many. which is seen as a world of bad actors, hackers, frauds and speculators.

**2) Corporates are scared of the disruptive character of blockchain**

There are organizations that don't just like the idea of blockchain and its disruptive character. for a few it's a nightmare thinking they're going to lose market share or will even become obsolete.

**3) Lack of scalability**

One major technology challenge of blockchain is said to the technical scalability of the network which may put a strain on the adoption process, especially for public blockchains. Legacy transaction networks are known for their ability to process thousands of transactions per second. Visa, as an example, is capable of processing quite 2000 transactions per second. The 2 largest blockchain networks, Bitcoin and Ethereum however are far behind when it involves transaction speeds. While the Bitcoin blockchain can process three to seven transactions per second, Ethereum can handle approximately 20 transactions during a second [4].

**4) Lack of standardization: limited interoperability**

The problem is that with such a large number of different networks, the blockchain space is in an exceedingly 'state of disarray' thanks to a scarcity of universal standards that may allow different networks to speak with one another.

5) **Integration with legacy systems**

And there's the challenge for corporates of the way to integrate blockchain with their legacy system(s). In most cases, if they plan to use blockchain, organization are required to completely restructure their previous system, or design some way to successfully integrate the 2 technologies.

6) **Lack of blockchain developers**

While the demand for qualified blockchain staff is increasing dramatically, the blockchain landscape suffers an acute shortage of an adequately trained and skilled /qualified people for developing and managing the complexity of peer-to-peer networks. Blockchain technology however demands additional qualification and knowhow.

7) **Blockchains is slow and cumbersome**

Due to their complexity and their encrypted, distributed nature, blockchains will be slow and cumbersome. Transactions can take ages to process, certainly compared to "traditional" payment systems like cash or debit cards.

8) **Lack of awareness and understanding**

The main challenge for corporates related to blockchain, especially the tiny and medium ones, could be a lack of awareness of the technology and a widespread lack of understanding of how it works. Many companies don't understand what blockchain is or what they'll do. This includes a lot to try to with the dominance of technicians within the blockchain area and an excessive amount of technology approach.

9) **Productivity paradox**

And there's the so-called blockchain paradox. The speed and effectiveness with which blockchain networks can execute peer-to-peer transactions comes at a high aggregate cost, which is bigger for a few varieties of blockchain than others. This inefficiency arises because each node performs the identical tasks as every other node on its own copy of the info in an effort to be the primary to seek out an answer.

10) **Lack of regulatory clarity and good governance**

There is also the shortage of regulatory clarity regarding the underlying blockchain technology, which may be a significant roadblock for mass adoption. Regulations have always struggled to stay up with advances in technology. this can be also the case with blockchain. One among the challenges of the blockchain approach (which was also one in every of its original motivations) is that it reduces oversight.

11) **Blockchain interoperability**

As more organizations begin adopting blockchain, there's an inclination for several organizations to develop their own systems with varying characteristics (governance rules, blockchain technology versions, consensus models, etc.). These separate blockchains don't work together, and there's currently no universal standard to enable different networks to speak with one another.

12) **Security and privacy challenges**

And what to consider the assorted security and privacy challenges. While cryptocurrencies offer pseudonymity, many potential applications of the blockchain require smart transactions and contracts to be indisputably linked to known identities, and thus raise important questions about privacy and of the safety of the information stored and accessible on the shared ledger.

13) **Blockchain has an environmental cost**

And finally, but not least important the massive energy consumption is another blockchain adoption challenge. the bulk of blockchains present within the market consume a high amount of energy.

Most of the blockchain technology follow bitcoins infrastructure and use Proof of Proof-of-work (PoW) as consensus mechanism for validating transactions. These protocols require users to unravel complex mathematical puzzles, and need tremendous computing power to verify and process transactions and to secure the network.

#### *2.5.2. Possible solutions*

As we can notice blockchain is still in developing phase and have lot of challenges, but many private companies such as IBM have determined to overcome these challenges and develop a perfect ledger. As blockchain is open-source developers across countries are contributing their innovative ideas and updating it on regular bases. To eliminate problem of energy and environment Proof of stack algorithm was introduced which is successfully adopted by many new blockchain companies one of them is Algorand (MIT's own blockchain). This Algorand blockchain is 1000 times faster than Bitcoin's traditional blockchain and its first of its kind which introduced atomic transfer. To solve the problem of energy mass adoption of solar roofs to mine bitcoin is spreading all across world as a trend. But due to these there were serious supply shortage of Graphic cards and Solar panels in 2020. Once every bitcoin is mined then only people will stop these activities. In many countries' governments are forcefully shutting down these farms due to report of heavy theft of electricity and hardware [4].

### *2.6. Specific use cases of the blockchain*

#### *2.6.1. Real world use cases*

- Secure sharing of medical data
- NFT marketplaces
- Music royalties tracking
- Cross-border payments
- Real-time IoT operating systems
- Personal identity security
- Anti-money laundering tracking system
- Supply chain and logistics monitoring
- Voting mechanism
- Advertising insights
- Original content creation
- Cryptocurrency exchange
- Real estate processing platform

#### *2.6.2. Corporation associated with blockchain*

1) **BurstIQ (Healthcare):** With BurstIQ's blockchain-enabled contracts, patients and doctors can securely exchange sensitive medical information. Smart contracts determine which data can be shared, and can show detailed health plans tailored to the needs of each patient.

2) **Mediachain(Music):** With Mediachain, artists can agree to higher royalties and actually receive payments in full and on time by entering into a decentralized, transparent contract. In April 2017, Spotify acquired Mediachain.

3) **Propy (Real estate):** Propy is a global real estate marketplace with a decentralized title registry system. The online marketplace uses blockchain to make title issuance instantaneous and even offers properties that can be purchased using cryptocurrency.

4) **OPSkins(Gaming):** Fintech Gamers looking to buy rare skins, accessories and even emotes can use Bitcoin as a method of payment at the OPSkins online marketplace. Sellers receive the bitcoin in their virtual wallet and either choose to keep the cryptocurrency or exchange it for cash. OPSkins processes more than two million virtual transactions a week.

5) **Filament (Internet of Things):** Hardware, Software Filament creates software and microchip hardware that lets connected devices operate on blockchain. The Reno-based company's products encrypt ledger data, distribute real-time information to other blockchain-connected machines and allow for the monetization of those machines based on timestamps.

6) **CIVIC (Identity Security):** Fintech Civic is a blockchain-based ecosystem that gives individuals insights into who has their information. The company's users enter into smart contracts, where they decide who can share their personal information and how much. If the contract is broken or an unauthorized source tries to access private data, the individual is immediately alerted.

## *2.7. Present condition in market and future prediction*

The global blockchain market size is expected to grow from USD 3.0 billion in 2020 to USD 39.7 billion by 2025, at an impressive Compound Annual Growth Rate (CAGR) of 67.3% during 2020–2025. The increasing need for simplifying the business processes and need for supply chain management applications integrated with the blockchain technology will drive the overall blockchain market.

Private blockchain type is estimated to carry the biggest market size in 2020. A non-public blockchain could be a shared database or ledger that's secured by traditional security techniques, like limited user rights. Generally, security is provided to a personal blockchain using private keys that are known only to the related organization. A non-public blockchain could be a category of the blockchain technology, where write permissions are kept centralized to one organization. Read permissions may additionally be restricted supported the organization's usability. A personal blockchain provides more opportunities to businesses in terms of leveraging the blockchain technology for business-to-business use cases. Based on organization size, the SMEs segment to grow at the next rate within the blockchain market during the forecast period

The SMEs segment is projected to grow at the next CAGR during the forecast period, thanks to the requirement for streamlining the business processes cost-effectively across SMEs. The adoption of the blockchain technology is currently within the experimentation introduce most of the SMEs; however, the adoption rate within the SMEs segment is anticipated to extend significantly within the coming years, due to the low infrastructure costs and transparency.

The banking and financial services application area is anticipated to carry the most important market size within the blockchain market during the forecast period. The banking and financial services application area has realized the importance of the blockchain technology which helps secure transactions for purchasers. The blockchain technology within the banking and financial services is anticipated to experience ascension worldwide, thanks to various factors, like high compatibility with the financial services industry ecosystem, rising cryptocurrencies and Initial Coin Offerings (ICOs), rapid transactions, and reduced total cost of ownership.

### *2.7.1. A look into future of blockchain technology*

1) **Economy and Finance Will Lead Blockchain Application**
Unlike other traditional businesses, the banking and finance industries did not introduce radical transformation to their processes for adopting blockchain technology. After it had been successfully applied for the cryptocurrency, financial institutions begin seriously considering blockchain adoption for traditional banking operations [5].

2) **Blockchain Integration into Government Agencies**
The idea of the distributed ledger is additionally very attractive to government authorities that should administrate very large quantities of knowledge. Currently, each agency has its separate database, in order that

they must constantly require information about residents from one another. However, the implementation of blockchain technologies for effective data management will improve the functioning of such agencies [5].

3) **Law Integration into Smart Contracts**

Besides cryptocurrency, blockchain technology benefits us with another convenient possibility, like "smart contracts." The idea of smart contracts is its automatic execution when conditions are met. As an example, delivering goods after payment is received. However, other conditions of contracts should even be automatically regulated. Thus, Insurers AIG is now piloting a blockchain system that permits creating complex insurance policies [5].

Blockchain within the future will revolutionize business processes in many industries, but its adoption requires time and efforts. Nevertheless, within the near future, we will expect that governments will finally accept blockchain benefits and start to use it for improving financial and public services. Though some blockchain start-ups might fail, people would get more experience and knowledge on the way to use this technology. Blockchain will stimulate people to accumulate new skills, while traditional business would most likely completely reconsider their processes. All in all, by 2020, we are able to see more samples of successful implementation of blockchain technology.

## *2.8. Environmental impact*

Among all the use cases of blockchain, cryptocurrency is the most popular among the internet. These crypto currencies use blockchain technology as their core component in order to record the data of transaction and trades. Bitcoin is most powerful cryptocurrency by market capitalization among them. Bitcoin market capitalization is 1 trillion $ which is higher than GDP of many small counties combined. To maintain the Bitcoin networks blockchain it requires huge amount of hardware power which run on electricity [6].

Bitcoin uses proof of work algorithm to verify the transactions which occurs across the ledger. When the transaction is verified by miner (validator) they are rewarded in bitcoin. This process of verification requires a powerful GPU power in order to apply brute force attack and a successive result can take 100s of years to be matched with the hash which is not economical. Hence people across world had started to collect the GPUs in bulk and use their combined power for verification. This process is called Bitcoin farming which is very power consuming and have very harmful effect on environment. It is estimated that at current situation a Bitcoin network consumes 133.68 TW-hour of energy per year which is higher than total energy consumption of European counties. Production of this much amount of energy is harmful to environment. A single transaction of Bitcoin leaves 549.74 kg $CO_2$ of carbon footprint which is equivalent of watching 91,624 hours of YouTube video [6].

Also, there are other crypto currencies also which uses Proof of work mechanism which increases the global energy demand and hence indirectly harmful resources are added to environment. The carbon footprints these transactions left behind increases the pollution growth and hardware waste increases the E-waste. Many governments across countries are reportedly disallowing the Bitcoin mining to save the environment. However, to avoid the conflicts with governments and to keep their mining operations going on Bitcoin enthusiasts have started to use solar and other renewable energy sources to run the huge Bitcoin farms. But these steps don't solve the problem related to E waste and supply shortage of hardware caused by miners [7].

These can be solved by Proof of stack mechanism which was discussed earlier in section 2.4. Proof of stack can reduce the energy consumption of blockchain network by 99% compared to same blockchain which uses Proof of work mechanism. Realizing the effect of blockchain on environment, founder of Ethereum blockchain have decided to move entire blockchain to the Proof of stack mechanism and it would be named Ethereum 2.0 which will be released at end of 2021.

### *2.9. Probable advancements in future*

The Blockchain is a solution to many problems today. Whether it's security or smart transfer of data, Blockchain promises to solve many problems. The future may ask to secure every system even more with quantum computers. It reduces the risk of data tampering and hacking as well. Blockchains are primarily decentralized structures, so the usage of these systems is also based on decentralized technologies.

1) **Smart Contracts:** The smart contract is a digital form of contract with a programmable architecture. With a smart contract, the details of the contract can be stored in the Blockchain block. It is also useful for tracking assets for the long-term. Smart contracts are also vital to the relationship with consumers.
2) **Web Servers:** The security of data in a web server is very important. A web server has two parts: API and Data. Each block in the server serves as a node and joins the request response cycle.
3) **Banking:** The process of encash a cheque and updating the statement usually takes hours. With Blockchain technology, the process can be completed in just ten minutes. The time needed is the same as the time needed to add a block to the Blockchain.
4) **Cryptocurrency:** Blockchain applications in Bitcoin and other cryptocurrencies are well-known.
5) **Healthcare:** Healthcare professionals can use blockchain to secure patient records. The information will be more secure.
6) **Records:** Property records should use Blockchain with Smart Contracts. This will uphold the statements to all the parties.
7) **Voting:** Using Blockchain in Voting will indulge in the safety of counting and misinterpretation.
8) **Digital Marketing:** With easy Consumer-market relations and secured way of data transfer, Blockchain has a great opportunity in Digital markets too.

### *2.10. Competitors and threats for existence*

#### *2.10.1. Competitors*

Many companies with centralized ledgers have developed more powerful and efficient blockchain ledger compared to existing classic ledgers. These new ledgers can make atomic transactions which takes fraction of seconds to transfer data which is very fast than existing blockchains transaction rate. Also, these new ledgers are environment friendly and secure. Following companies have successfully developed this kind of blockchain ledgers with their own technique**.**

**1)** **Coinbase:** Coinbase is a crypto exchange platform which also develops an online platform that allows merchants, consumers, and traders to transact with digital currency.

**2)** **Hedera Hashgraph:** Hedera Hashgraph is a company that develops a consensus data structure alternative to blockchain.

**3)** **Cosmos Network:** Cosmos Network is developing a network of block chains whose purpose is to allow many sovereign and easy-to-develop block chains to scale and interoperate with each other.

**4)** **Polkadot Network:** Polkadot Network offers a heterogeneous multi-chain technology.

**5)** **Circle:** Circle is a global crypto finance company.

These companies provide services worldwide and increasing their partners along. It's predictable that these projects can replace the traditional slow blockchain in future.

### *2.10.2. Threats for existence*

Quantum computers contains qubits which can set their state to 0 and 1 at same time of instance which indirectly opens observation to many possibilities at once rather than checking it by 0 and 1 differently. Quantum computer can act as a brute force machine which works 1012 times faster than world's most powerful computer. It takes average 3 minutes to mine a bitcoin but a quantum computer can mine entire 21 million bitcoins within 3 years which can impact its valuation. A person operating on quantum computer can overpower hash rate of all other validators combined and can insert corrupt blocks into blockchain and can break it also [8].

Using these behaviours of quantum computing many existing cryptographic algorithms can also become vulnerable to brute force attacks. Trillions of dollars of financial details are encrypted using modern cryptographic algorithm. If quantum computers successfully achieve quantum supremacy, then these details will be jeopardized and we can witness a global economic depression. But scientist is assuming that before age of quantum supremacy arrives there will be quantum algorithm-based encryptions available which will be protected from hacks from quantum computers.

## *2.11. Long term policies for blockchain and decentralized finance*

The question is why is there so much hype around Blockchain. The answer is trust and security. There have been attempts in the past to create digital money but they have failed, the prevailing issue was trust and ethical concerns. Blockchain is the specific type of database that quickly solved the problem. Most of the common databases like SQL have someone in charge who can change the entries, but in blockchain, it's run by the people who use it. Blockchain is unarguably a revolutionary technology because of its decentralized nature, transparency and security. It has also eased the process of global transactions to a greater extent.

There are some disadvantages regarding Blockchain too, which are listed below,

1) **Large Energy Consumption:** In a particular year the power consumption of Bitcoin miners was alone more than per-capita power consumption of 159 individual countries

2) **Maintenance Cost:** Because of high energy consumption and requirement of storage, the cost of maintenance becomes high.

3) **Uncertain Regulatory Status:** Since blockchain is decentralized it becomes hurdle for cryptocurrencies to get accepted by pre-existing financial institutions.

4) **Transaction Delays:** One of the major drawbacks of blockchain is that they usually take a long time to register transaction.

5) **Volatility:** The blockchains are decentralized and hence are extremely volatile, it is very common for Bitcoin price to fluctuate over 20% in a day.

6) Doesn't guarantee full transparency

7) **Unavoidable security flaw:** Since Blockchain is decentralized entity, it becomes necessary for transactions to propagate between the nodes in peer-to-peer fashion. The verification and generation of these signatures is computationally complex.

Cryptocurrencies continues to ride waves of public interest and market volatility. The policy making needs to focus on:

1) The intersection of crypto-currency and the traditional financial system.
2) Consumer Protection
3) Financial Stability
4) Public Security

Decentralized nature of Blockchain works both favour and against of Blockchain. If we consider the example Bitcoin, the miners need computational power so high that Bitcoin mines consume more energy than the whole country of Ecuador. The energy consumption is so high that some mines are now sited near Arctic Circle to cut down on cooling costs. These problems have held back what could have been a revolutionary technology.

## 3. Summary

We started with introduction as our first chapter and later discussed different core components of blockchain and learned why adoption rate of blockchain is accelerating due to its cost effectiveness, security and transparency. We learned about smart contracts which are used by many DAO with association of blockchain ecosystem. We knew about challenges and problems with blockchain technology. Due to decentralization regulations on smart contracts-based applications conflicts with governments of different nations. As DAO eliminates banks for payment many banks describe this system as a threat to finances. We also came to know about different use cases like NFTs, cryptocurrencies and a solution to record immutable data. Interest of people in NFTs have taken it to all new heights and it already attracted many huge personalities. We also discussed negative impact of blockchain based technologies on environment which is a huge concern noticing current state of global warming and pollutions in same section we also discussed solution to few of problems related to environmental impact in which proof of stack closeness mechanism will play a huge role. We discovered possible advancements in blockchain and discussed its integration with internet of things to setup a global ledger which can be contributed by everyone just by using internet. In chapter-3 we discussed learning we obtained from writing this paper, which was based on architecture, use cases, challenges and innovation all these together provided a good understanding of a fact about the blockchain technology.

## 4. Conclusion

Blockchain is very promising for future and can be very useful in creation of transparent systems. It seems challenges related to blockchain will be solved in near time with innovation and interest taken by many individual and corporate developers. It can also be useful to improve current cryptographic algorithms just like past. But in current scenario imagining a big picture of future and use cases it is understandable that it is still in development and innovative phase. Hence for medium sized projects which don't need regular updates on technology and is stable blockchain is very good component is to be used in them.

## 5. References

[1] S. K. Madhusudan Singh, “Blockchain technology for decentralized autonomous organizations,” in *Advances in Computers*, vol. 124, Seoul, Elsevier, 2019, pp. 115-140.

[2] A. Lewis, The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology That Powers Them, 2018.

[3] M. J. M. C. M. A. H. Md Sadek Ferdous, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *Journal of Network and Computer Applications*, vol. 182, no. 10848045, p. 103035, 2021.

[4] A. S. A. A. F. B. A. A. I. V. M. E. C. S. G. D. Yassine Himeur, "Blockchain-based recommender systems: Applications, challenges and future opportunities," *Computer Science Review*, vol. 43, no. 15740137, p. 100439, 2 2022.

[5] M. Swan, Blockchain: Blueprint for a New Economy, 1st ed., O'Reilly Media, Inc., 2015.

[6] A. O. M. F. M. L. E. A. Elisa Di Febo, “From Bitcoin to carbon allowances: An asymmetric extreme risk spillover,” *Journal of Environmental Management*, vol. 298, no. 03014797, p. 113384, 2021.

[7] C. S. Alex de Vries, "Bitcoin's growing e-waste problem," *Resources, Conservation and Recycling*, vol. 175, no. 09213449, p. 105901, 12 2021.

[8] C. A. P.-D. Joseph J. Kearney, "Vulnerability of blockchain technologies to quantum attacks," *Array*, vol. 10, no. 25900056, p. 100065, 7 2021.

[9] L. J. Liebi, “Antony Lewis: The basics of bitcoins and blockchains,” *Financial Markets and Portfolio Management*, vol. 35, no. 1934-4554, pp. 145-147, 2021.