# Blockchain Technology: Applications and Future Trends

Remya.S.P
Lecturer, Department of Computer Science, N.S.S.College, Ottapalam
University of Calicut, Kerala, India.

***Abstract :*** Blockchain is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place in a secure, chronological, and immutable way. It can be used for the secure transfer of money, property, contracts, etc. without requiring a third-party intermediary such as bank or government. Blockchain is a software protocol, but it could not be run without the Internet. It is a decentralized distributed database of immutable records, where transactions are protected by strong cryptographic algorithmsA blockchain is a database that stores encrypted blocks of data then chains them together to form a chronological single-source-of-truth for the data. Digital assets are distributed instead of copied or transferred, creating an immutable record of an asset.The asset is decentralized, allowing full real-time access and transparency to the public. A transparent ledger of changes preserves integrity of the document, which creates trust in the asset. Blockchain's inherent security measures and public ledger make it a prime technology for almost every single sector. Blockchain is an especially promising and revolutionary technology because it helps reduce risk, stamps out fraud and brings transparency in a scaleable way for myriad uses. Blockchain has numerous benefits such as decentralisation, persistency, anonymity and auditability. Originally conceived as the basis of cryptocurrencies, aspects of blockchain technology have far-reaching potential in many other areas. There is a wide spectrum of blockchain applications ranging from cryptocurrency, financial services, risk management, internet of things (IoT) to public and social services. This paper presents an overview of blockchain technology ,it's architecture,applications ,challenges as well as recent trends in tackling the challenges**.**

***Keywords*** – **Blockchain, Bitcoin, Nodes, Blocks, Transacions, Cryptocurrency.**

## I. INTRODUCTION

A blockchain is a growing list of records, called blocks, which are linked using cryptography. Blockchain is a chain of blocks which contain information. Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database. Each time a block gets completed, a new block is generated.Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Blockchain has been in a lot of buzz these days. And that is mainly because it is backbone of the very famous cryptocurrency in the world - the Bitcoin. Many Governments and leading Banks have decided to bring many of their conventional transactions based on Blockchain concept. The applications and potential of this framework is huge and is considered to be changing the way transactions are made in various domains. A blockchain can be used for the secure transfer of money, property, contracts, etc. without requiring a third-party intermediary like bank or government. Blockchain is a software protocol, but it could not be run without the Internet (like SMTP used in email).
Digital assets are distributed instead of copied or transferred, creating an immutable record of an asset. The asset is decentralized, allowing full real-time access and transparency to the public. A transparent ledger of changes preserves integrity of the document, which creates trust in the asset. Blockchain's inherent security measures and public ledger make it a prime technology for almost every single sector.A simple analogy for understanding blockchain technology is a Google Doc. When we create a document and share it with a group of people, the document is distributed instead of copied or transferred. This creates a decentralized distribution chain that gives everyone access to the document at the same time. No one is locked out awaiting changes from another party, while all modifications to the doc are being recorded in real-time, making changes completely transparent. Blockchain is more complicated than a Google Doc, but the analogy is apt because it illustrates three critical ideas of the technology.

Blockchain technology has become popular because of the following.

- **Time reduction:** In the financial industry, blockchain can allow the quicker settlement of trades. It does not take a lengthy process for verification, settlement, and clearance. It is because of a single version of agreed-upon data available between all stakeholders.
- **Unchangeable transactions:** Blockchain register transactions in a chronological order which certifies the unalterability of all operations, means when a new block is added to the chain of ledgers, it cannot be removed or modified.
- Value: With blockchain, you can actually create value on a digital asset. The value can be controlled by that person who owns it. It enables a unique asset to be transferred over the internet without a middle centralized agent.
- Trust: Blockchain enables to securely assign ownership of a specific digital asset and be able to track who actually controls that asset at a time. In other words, blockchain creates a permanent, secure, unalterable record of who owns what. It uses advanced hash cryptography to preserve the integrity of the information.
- **Reliability:** Blockchain distributes their workload among thousands of different computers worldwide. It provides reliability because if you have everything localized in one location, it becomes a single point of failure. But, its decentralized network structure ensures that there is no single point of failure which could bring the entire system down.Blockchain certifies and verifies the identities of each interested parties. This removes double records, reducing rates and accelerates transactions.
- **Security:** Blockchain uses very advanced cryptography to make sure that the information is locked inside the blockchain. It uses Distributed Ledger Technology where each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.

- **Collaboration:** It allows each party to transact directly with each other without requiring a third-party intermediary.
- **Decentralized:** It is decentralized because there is no central authority supervising anything. There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

Blockchain technology can be integrated into multiple areas. The primary use of blockchains is as a distributed ledger for cryptocurrencies. It shows great promise across a wide range of business applications like Banking, Finance, Government, Healthcare, Insurance, Media and Entertainment, Retail, etc.

## II. HISTORY OF BLOCKCHAIN

The blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.[3] The identity of Satoshi Nakamoto remains unknown to date. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications[3][2] and blockchains that are readable by the public and are widely used by cryptocurrencies. The following is a brief timeline of some of the most important and notable events in the development of blockchain.

**2008**

- Satoshi Nakamoto, a pseudonym for a person or group, publishes "Bitcoin: A Peer to Peer Electronic Cash System"

**2009**

- The first successful Bitcoin (BTC) transaction occurs between computer scientist Hal Finney and the mysterious Satoshi Nakamoto.

**2016**

- Tech giant IBM announces a blockchain strategy for cloud-based business solutions.
- Government of Japan recognizes the legitimacy of blockchain and cryptocurrencies.

**2017**

- Bitcoin reaches $1,000/BTC for first time.
- Cryptocurrency market cap reaches $150 billion.
- JP Morgan CEO Jamie Dimon says he believes in blockchain as a future technology, giving the ledger system a vote-of-confidence from Wall Street.
- Bitcoin reaches its all-time high at $19,783.21/BTC.
- Dubai announces its government will be blockchain-powered by 2020.

**2018**

- Facebook commits to starting a blockchain group and also hints at the possibility of creating its own cryptocurrency.
- IBM develops a blockchain-based banking platform with large banks like Citi and Barclays signing on.

**2019**

- China's President Ji Xinping publicly embraces blockchain as China's central bank announces it is working on its own cryptocurrency
- Twitter & Square CEO Jack Dorsey announces that Square will be hiring blockchain engineers to work on the company's future crypto plans
- The New York Stock Exchange (NYSE) announces the creation of Bakkt - a digital wallet company that includes crypto trading

**2020**

- Bitcoin almost reaches $30,000 by the end of 2020
- PayPal announces it will allow users to buy, sell and hold cryptocurrencies
- The Bahamas becomes the world's first country to launch its central bank digital currency, fittingly known as the "Sand Dollar"
- Blockchain becomes a key player in the fight against COVID-19, mainly for securely storing medical research data and patient information

## III. BLOCKCHAIN VS BITCOIN

Satoshi Nakamoto introduced the bitcoin in the year 2008. Bitcoin is a cryptocurrency(virtual currency), or a digital currency that uses rules of cryptography for regulation and generation of units of currency. A Bitcoin fell under the scope of cryptocurrency and became the first and most valuable among them. It is commonly called decentralized digital currency.

A bitcoin is a type of digital assets which can be bought, sold, and transfer between the two parties securely over the internet. Bitcoin can be used to store values much like fine gold, silver, and some other type of investments. We can also use bitcoin to buy products and services as well as make payments and exchange values electronically.A bitcoin is different from other traditional currencies such as Dollar, Pound, and Euro, which can also be used to buy things and exchange values electronically. There are no physical coins for bitcoins or paper bills. When you send bitcoin to someone or used bitcoin to buy anything, you don?t need to use a bank, a credit card, or any other third-party. Instead, you can simply send bitcoin directly to another party over the internet with securely and almost instantly.

Whenever you want to transfer money to someone over the internet, you need to use a service of third-party such as banks, a credit card, a PayPal, or some other type of money transfer services. The reason for using third-party is to ensure that you are transferring that money. In other words, you need to be able to verify that both parties have done what they need to do in real exchange.For example, Suppose you click on a photo that you want to send it to another person, so you can simply attach that photo to an email, type the receiver email address and send it. The other person will receive the photo, and you think it would end, but it is not. Now, we have two copies of photo, one is a simple email, and another is an original file which is still on my computer. Here, we send the copy of the file of the photo, not the original file. This issue is commonly known as the double-spend problem. The double-spend problem provides a challenge to determine whether a transaction is real or not. How you can send a bitcoin to someone over the internet without needing a bank or some other institution to certify the transfer took place. The answer arises in a global network of thousands of computers called a Bitcoin Network and a special type of decentralized laser technology called blockchain.

In Bitcoin, all the information related to the transaction is captured securely by using maths, protected cryptographically, and the data is stored and verified across the entire network of computers. In other words, instead of having a centralized database of the third-party such as banks to certify the transaction took place. Bitcoin uses blockchain technology across a decentralized network of computers to securely verify, confirm and record each transaction. Since data is stored in a decentralized manner across a wide network, there is no single point of failure. This makes blockchain more secure and less prone to fraud, tampering or general system failure than keeping them in a single centralized location.

Blockchain's most well-known use (and maybe most controversial) is in cryptocurrencies. Cryptocurrencies are digital currencies (or tokens), like Bitcoin, Ethereum or Litecoin, that can be used to buy goods and services. Cryptocurrencies are digital currencies that use blockchain technology to record and secure every transaction. A cryptocurrency (for example, Bitcoin) can be used as a digital form of cash to pay for everything from everyday items to larger purchases like cars and homes. Unlike cash, crypto uses blockchain to act as both a public ledger and an enhanced cryptographic security system, so online transactions are always recorded and secured. It can be bought using one of several digital wallets or trading platforms, then digitally transferred upon purchase of an item, with the blockchain recording the transaction and the new owner. The appeal of cryptocurrencies is that everything is recorded in a public ledger and secured using cryptography, making an irrefutable, timestamped and secure record of every payment. Here are some of the main reasons why everyone is suddenly taking notice of cryptocurrencies:

- Blockchain's security makes theft much harder since each cryptocurrency has its own irrefutable identifiable number that is attached to one owner.
- Crypto reduces the need for individualized currencies and central banks- With blockchain, crypto can be sent to anywhere and anyone in the world without the need for currency exchanging or without interference from central banks.
- Cryptocurrencies can make some people rich- Speculators have been driving up the price of crypto, especially Bitcoin, helping some early adopters to become billionaires. Whether this is actually a positive has yet to be seen, as some retractors believe that speculators do not have the long-term benefits of crypto in mind.
- More and more large corporations are coming around to the idea of a blockchain-based digital currency for payments. In February 2021, Tesla famously announced that it would invest $1.5 billion into Bitcoin and accept it as payment for their cars.

There are many legitimate arguments against blockchain-based digital currencies. First, crypto isn't a very regulated market. Many governments were quick to jump into crypto, but few have a staunch set of codified laws regarding it. Additionally, crypto is incredibly volatile due to those aforementioned speculators.

## IV. WORKING OF BLOCKCHAIN

Blockchain consists of three important concepts: blocks, nodes and miners.

### 4.1. Blocks

Every chain consists of multiple blocks and each block has three basic elements:

- The **data** in the block.

- A 32-bit whole number called a **nonce.** The nonce is randomly generated when a block is created, which then generates a block header hash.

- The **hash** is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

**4.2. Miners**

Miners create new blocks on the chain through a process called mining.In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens miners are said to have found the "golden nonce" and their block is added to the chain. Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology. Think of it is as "safety in math" since finding golden nonces requires an enormous amount of time and computing power.When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially.

**4.3. Nodes**

One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain. Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning. Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed. Each participant is given a unique alphanumeric identification number that shows their transactions. Combining public information with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users. Essentially, blockchains can be thought of as the scaleability of trust via technology.

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the “end” of the blockchain. If you take a look at Bitcoin’s blockchain, you’ll see that each block has a position on the chain, called a “height.” As of November 2020, the block’s height had reached 656,197 blocks so far.

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block unless the majority reached a consensus to do so. That’s because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned time stamp. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Here’s why that’s important to security. Let’s say a hacker wants to alter the blockchain and steal Bitcoin from everyone else. If they were to alter their own single copy, it would no longer align with everyone else's copy. When everyone else cross-references their copies against each other, they would see this one copy stand out and that hacker's version of the chain would be cast away as illegitimate.

Succeeding with such a hack would require that the hacker simultaneously control and alter 51% of the copies of the blockchain so that their new copy becomes the majority copy and thus, the agreed-upon chain. Such an attack would also require an immense amount of money and resources as they would need to redo all of the blocks because they would now have different timestamps and hash codes.

Due to the size of Bitcoin’s network and how fast it is growing, the cost to pull off such a feat would probably be insurmountable. Not only would this be extremely expensive, but it would also likely be fruitless. Doing such a thing would not go unnoticed, as network members would see such drastic alterations to the blockchain. The network members would then fork off to a new version of the chain that has not been affected. This would cause the attacked version of Bitcoin to plummet in value, making the attack ultimately pointless as the bad actor has control of a worthless asset. The same would occur if the bad actor were to attack the new fork of Bitcoin. It is built this way so that taking part in the network is far more economically incentivized than attacking it.

## V. ADVANTAGES OF BLOCKCHAIN

**5.1. Accuracy of the Chain** - Transactions on the blockchain network are approved by a network of thousands of computers. This removes almost all human involvement in the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain. In order for that error to spread to the rest of the blockchain, it would need to be made by at least 51% of the network’s computers—a near impossibility for a large and growing network the size of Bitcoin’s.

**5.2. Settlement in real-time -** In the financial industry, blockchain can allowing the quicker settlement of trades. It does not take a lengthy process for verification, settlement, and clearance because a single version of agreed-upon data is available between all stack holders.

**5.3. Cost Reductions** - Typically, consumers pay a bank to verify a transaction, a notary to sign a document, or a minister to perform a marriage. Blockchain eliminates the need for third-party verification and, with it, their associated costs. Business owners incur a small fee whenever they accept payments using credit cards, for example, because banks and payment processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees.

**5.4**. **Decentralization** - Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. By spreading that information across a network, rather than storing it in one central database, blockchain becomes more difficult to tamper with. If a copy of the blockchain fell into the hands of a hacker, only a single copy of the information, rather than the entire network, would be compromised.

**5.5. Efficient Transactions** - Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Whereas financial institutions operate during business hours, five days a week, blockchain is working 24 hours a day, seven days a week, and 365 days a year. Transactions can be completed in as little as ten minutes and can be considered secure after just a few hours. This is particularly useful for cross-border trades, which usually take much longer because of time-zone issues and the fact that all parties must confirm payment processing.

**5.6**. **Private Transactions -** Many blockchain networks operate as public databases, meaning that anyone with an internet connection can view a list of the network's transaction history. Although users can access details about transactions, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like bitcoin are anonymous, when in fact they are only confidential. That is, when a user makes public transactions, their unique code called a public key, is recorded on the blockchain, rather than their personal information. If a person has made a Bitcoin purchase on an exchange that requires identification then the person's identity is still linked to their blockchain address, but a transaction, even when tied to a person's name, does not reveal any personal information.

**5.7. Secure Transactions** - Once a transaction is recorded, its authenticity must be verified by the blockchain network. Thousands of computers on the blockchain rush to confirm that the details of the purchase are correct. After a computer has validated the transaction, it is added to the blockchain block. Each block on the blockchain contains its own unique hash, along with the unique hash of the block before it. When the information on a block is edited in any way, that block's hashcode changes—however, the hash code on the block after it would not. This discrepancy makes it extremely difficult for information on the blockchain to be changed without notice.
Blockchain uses very advanced cryptography to make sure that the information which is going to lock inside the blockchain is secure against hacking attacks and fraud. It uses Distributed Ledger Technology where each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.

**5.8. Transparency** - Most blockchains are entirely open-source software. This means that anyone and everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. This also means that there is no real authority on who controls Bitcoin's code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile then Bitcoin can be updated.

**5.9. Immutability -** A blockchain register transactions in chronological order, which mean every transaction happens after the previous one. The chronological order certifies the unalterability of all operations in the blockchain. It means when a new block is added to the chain of ledgers, it cannot be removed or modified.

**5.10. User Pseudonymity** - It is a state where the user has a consistent identifier which is not the real name of the user. The real identities are only available to administrators. It allows users to communicate with others in a generally anonymous way. It helps to maintain user privacy and enables free transactions without any security worries. In the blockchain, your pseudonym is the address to which you receive Bitcoin. Every transaction which involves that address is stored permanently in the blockchain. If your address is linked to your identity, every transaction will be linked to you. It is always good to every time use a new address for each transaction to avoid the transactions being linked to a common owner.

Blockchains of the future are also looking for solutions to not only be a unit of account for wealth storage, but also to store medical records, property rights, and a variety of other legal contracts.

## VI. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Blockchain is a term constantly raised when we talk about how technology has changed the way we live. For a good reason, blockchain fundamentally transforms our way of life in a multitude of areas. Blockchain is a remarkable revolution in digital ledger systems with a vast range of use cases possibilities.

### 6.1. Peer to Peer Digital Cash System

Perhaps the most famous blockchain application can send and receive payments. Because blockchain technology begins in cryptocurrency, this makes sense. Using blockchain technology, you can securely and directly transfer funds to anybody in the world at ultra-low rates. There are no Intermediaries to slow the transfer of funds between several banks or charge outrageous transaction fees.

### 6.2. Capital Market

For capital markets, blockchain unlocks easier, cheaper, and faster access to capital. It reduces the barriers to issuance and enables peer-to-peer trading, faster and more transparent settlement and clearing, reduced costs, decreased counterparty risks, and streamlined auditing and compliance

### 6.3. Internet-of-Things Network

A great opportunity awaits the developer team who can make IoT data move faster by combining it with blockchain technology. By 2022, the IoT market is set to generate $2.48 billion in revenue. More and more technology companies are looking for ways to build a share of this market. The result is that cases of business use blockchain enter the landscape now.Blockchain offers digitization of assets with IoT sensors so that organizations can label their assets and provide a transparent tracking system. Digitization enables to identify the location and condition of items. The blockchain can store, manage, protect and transfer all this information.

### 6.4. Smart Contracts

Smart contracts are another application area of blockchain technology. Smart contracts are the latest digital technology for self-executing agreements recorded to a blockchain. The term ' smart contract' was first coined in 1993, but it has become a worthy term since the launch of the Ethereum project in 2013. Ethereum is the most known and developed smart contract blockchain platform.These contracts remove the intermediary by resolving problems related to trust so that agreements between two parties can be made more efficiently. We've already written a smart contracts in-depth guide and entered into details about its use cases. Blockchain use cases in smart contracts category include:

- Smart contracts in insurance
- Supply chain management
- Financial data recording and management
- Copyright management
- Clinical trial tracking
- Property ownership transfer

### 6.5. Personal Identity Protection

Digital IDs (Passports, Personal IDs, Marriage Certificates)

The blockchain could make record-keeping more reliable by encrypting these personal identification IDs and allowing citizens to access this information. With blockchain technology, individuals can be in control of their digital data and the way in which it is utilized by different parties.

### 6.6. Finance

Financial services struggle with archaic operational processes, slow payment settlements, limited transparency, and security vulnerabilities. Blockchain enhances the efficient digitization of financial instruments, which increases liquidity, lowers cost of capital, and reduces counterparty risk

### 6.7. Wills and Inheritances (Smart Property)

Digital wills and signatures are a convenient way to create testaments, they are at the risk of fraud. Individuals can benefit from blockchain technology to prevent tampering of their wills. Testators can distribute their assets to inheritors via a crypto-will network that can be accessed by related parties. This can be built in the form of a smart contract that can be automatically executed after the death of the testator.Slock, an internet-of-things platform of Ethereum, uses this application to enable customers to rent apartments by activating an smart lock once the contractual agreements have been agreed on by both parties.The Ledger will store and exchange these smart keys once the contract has been confirmed. It is also a registering and management system for property rights that enables smart contracts to double records or smart keys when lost. Developing property intelligence reduces your risk of doubtful fraud, mediation and business circumstances.

### 6.8. Cloud Storage

Cloud storage is another application company that can use it. Storj, but, is one such company in beta testing at the time of this article offering secure cloud storage while reducing its dependence.Users can store traditional cloud 300 times over excess hard drive spaceAs the world spends $22 billion more on cloud storage alone, this could open up revenue streams for average users while reducing data storage costs for businesses and personal users.

### 6.9. Healthcare and the Life Sciences

Blockchain-based healthcare solutions will enable faster, more efficient, and more secure medical data management and medical supply tracking. This could significantly improve patient care, facilitate the advancement to medical discoveries, and ensure the authenticity of drugs circulating global markets.

### 6.10. Retail and e-Commerce

For internal and external auditing purposes, Metro Group, the fourth largest retailer in the world, is required to archive all point of sale data. While Metro used to rely on a single provider, it recently moved to a more flexible model, where the data can be re-saved from a variety of cloud providers. This gives them much more freedom and the ability to negotiate prices.The blockchain can also help retailers to offer gift cards and loyalty programs, which make the process cheaper and safer, cut off intermediaries and use the unique verification capabilities of blockchain.. Smart technology may incorporate tangible or intangible assets such as cars, houses or cookers, or a company's patent, title, or share.

### 6.11. Advertising

Like it or not, advertisers know a lot about us. We sell our personal details to advertisers who send their ads, often without even realizing what we did. Blockchain obstructs this by establishing a secure data point where only you can access your encrypted personal data.On the advertising side, platforms such as ClearCoin and MetaX use blockchain technology to deliver secure, transparent advertising transactions to customers worldwide. By managing the purchase and sale of ads via the blockchain platform, these companies provide all parties with a stable, market-driven economic foundation as well as efficient and secure transactions, accurate, real-time data reporting and a dramatic reduction in ad fraud.

### 6.12. Intellectual Rights

The distribution and transparency of royalties are key issues in debates over intellectual property. By creating a comprehensive, precise and decentralized music rights database, blockchain and smart contract technology. Provides transparent, real-time transfer of fees to artists and distribution to all participants in the label.

### 6.13. Notaries

Blockchain technology can also be used as a convenient and affordable notary service. For example, applications like Uproov a smartphone multimedia platform can be detected immediately following an image, video or sound recording by the user. Meanwhile, stampd.io could actually prove that digital creation is owned.

### 6.14. e-Voting Systems

The reliability of the voting process has been a problem since the beginning of democracy. Stalin secretary claimed that Stain famously said “It’s not the people who vote that count, it’s the people who count the votes”.Blockchain technology can decentralize the voting process so that elections can happen securely with transparency. In a decentralized system, there is no single point of weakness. This creates a system that is more robust.FollowMyVote is a start-up that uses blockchain technology to ensure a transparent online voting platform. Individuals who are eligible, receive a token that allows them to vote only once and each vote is stored as a node in the blockchain.

### 6.15. Media and Entertainment

Piracy, fraud, and intellectual property theft of digital items cost the entertainment industry an estimated $71 billion annually. Blockchain technology can track the life cycle of any content, which has the potential to protect digital content, and facilitate the distribution of authentic digital collectibles

## VII. CHALLENGES IN BLOCKCHAIN TECHNOLOGY

Blockchain technology has enormous potential in creating trustless, decentralized applications. But it is not perfect. There are certain barriers which make the blockchain technology not the right choice and unusable for mainstream application. We can see the limitations of blockchain technology in the following image.

### 7.1. Lack of Awareness

There is a lot of discussion about blockchain, but people do not know the true value of blockchain and how they could implement it in different situations.

### 7.2. Limited availability of technical talent

Today, there are a lot of developers available who can do a lot of different things in every field. But in the blockchain technology, there are not so many developers available who have specialized expertise in blockchain technology. Hence, the lack of developers is a hindrance to developing anything on the blockchain.

### 7.3. Immutable

In immutable, we cannot make any **modifications** to any of the records. It is very helpful if you want to keep the **integrity** of a record and make sure that nobody ever tampers with it. But immutability also has a drawback.We can understand this, in the case, when you want to make any revisions, or want to go back and make any reversals. For example, you have processed payment and need to go back and make an amendment to change that payment.

### 7.4. Key Management

As we know, blockchain is built on cryptography, which implies that there are different keys, such as public keys and private keys. When you are dealing with a private key, then you are also running the risk that somebody may lose access to your private key. It happens a lot in the early days when bitcoin wasn't worth that much. People would just collect a lot of bitcoin, and then suddenly forgot what the key was, and those may be worth millions of dollars today.

### 7.5. Scalability

Blockchain like bitcoin has consensus mechanisms which require every participating node to verify the transaction. It limits the number of transactions a blockchain network can process. So bitcoin was not developed to do the large scale volumes of transactions that many of the other institutions are doing. Currently, bitcoin can process a maximum of seven transactions per second.

### 7.6. Consensus Mechanism

In the blockchain, we know that a block can be created in every 10 minutes. It is because every transaction made must ensure that every block in the blockchain network must reach a common consensus. Depending on the network size and the number of blocks or nodes involved in a blockchain, the back-and-forth communications involved to attain a consensus can consume a considerable amount of time and resources.

## VIII. CONCLUSION

A Blockchain is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, chronological, and immutable way. It can be used for the secure transfer of money, property, contracts, etc. without requiring a third-party intermediary like bank or government.Blockchain is the backbone of the most famous cryptocurrency named Bitcoin. It is a peer to peer electronic cash system and a decentralized network which allows users to make transactions directly without the involvement of third-party to manage the exchange of funds. Security of data is always matters. Encryption is a process of converting information or data into a code to prevent unauthorized access. It helps organizations to keep their data secure(i.e., prevent unauthorized access). In this technique, the data is encoded or changed into an unreadable format up to some extent before it is sent out of a network by the sender. The only receiver can understand how to decode the same. In Blockchain technology, this approach is very useful because it makes the overall security and authenticity of blocks and help to keep them secure.

First proposed as a research project in 1991, blockchain is comfortably settling into its late twenties. Like most millennials its age, blockchain has seen its fair share of public scrutiny over the last two decades, with businesses around the world speculating about what the technology is capable of and where it's headed in the years to come.With many practical applications for the technology already being implemented and explored, blockchain is finally making a name for itself at age twenty-seven, in no small part because of bitcoin and cryptocurrency. As a buzzword on the tongue of every investor in the nation, blockchain stands to make business and government operations more accurate, efficient, secure, and cheap with fewer middlemen.

## IX. REFERENCES


[1] Catalini, Christian; Gans, Joshua S ,"Some Simple Economics of the Blockchain", 6 March 2020
[2] Tapscott, Don; Tapscott, Alex, "Here's Why Blockchains Will Change the World", 16 November 2016.
[3] Bheemaiah, Kariappa "Block Chain 2.0: The Renaissance of Money" 14 November 2016.
[4] Androulaki E, Karame GO, Roeschlin M, Scherer T, Capkun S (2013) Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security. Springer, Heidelberg
[5] Antonopoulos A "Bitcoin security model: trust by computation".30 Nov 2016
[6] Atzori M "Blockchain technology and decentralized governance: Is the state still necessary?" 2015
[7] Barber S, Boyen X, Shi E, Uzun E "Bitter to better—how to make bitcoin a better currency". International Conference on Financial Cryptography and Data Security. Springer, Heidelberg 2012
[8] Bonneau J, Narayanan A, Miller A, Clark J, Kroll JA, Felten EW Mixcoin: "Anonymity for Bitcoin with accountable mixes. In International Conference on Financial Cryptography and Data Security." Springer, Heidelberg 2014
[9] Buterin V A next-generation smart contract and decentralized application platform. White Paper 2014
[10] Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Gun Sirer E, Song D, Wattenhofer R On scaling decentralized blockchains. 3rd Workshop on Bitcoin Research (BITCOIN), Barbados 2016
[11] Crosby M, Nachiappan Pattanayak P, Verma S, Kalyanaraman V "Blockchain technology: Beyond bitcoin Application" 2016
[12] Zheng Z, Xie S, Dai HN, Wang H (2016) Blockchain Challenges and Opportunities: A Survey. Work Pap
[13] Zyskind G, Nathan O, Pentland A (2015) Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), IEEE