SN Computer Science (2021) 2:30
https://doi.org/10.1007/s42979-020-00366-x

SURVEY ARTICLE

A Detailed Review on Blockchain and Its Applications

Akash Raj Khettry[1] · Karthik R. Patil[1] · Abhilash C. Basavaraju[1]

Received: 24 September 2020 / Accepted: 4 October 2020 / Published online: 11 January 2021

Abstract
In the recent past, there has been a huge concern for secured storage of records, and transactions between varied parties and applications. Using the concept of cryptography, and its increase in popularity in the current generation we here describe the concept of blockchain technology that helps provide solutions to the above issues. It describes the design and functionality of blockchain technology. It gives a brief insight into the types of blockchain used in various industries. In this paper, we also promote the need for the decentralized network over a centralized one which is an important aspect. There are various consensus algorithms used to develop an application, we are giving a comparison between various approaches to decide the best suited algorithm for the required application. Furthermore, we provide a detailed analysis on the various applications of blockchain with use case. We also present an insight into the future advancements in the field of blockchain.

Keywords Blockchain · Centralization · Distributed · Consensus · Decentralization · Ledger · Node · Transaction · Mining · Bitcoin

Introduction

Blockchain is considered to be a public ledger where all the transactions are stored securely in structures called blocks where each block is connected as a chain. The chain gets appended when new blocks are added to it [15]. Each block has a hash which is a function of the previous block [18]. The transactions in the ledger are verified by consensus by the participants. Information once entered into the block cannot be erased [12]. The characteristics of blockchain include decentralization, persistency, anonymity and auditability. It has several core technologies integrated to it like cryptographic hash, digital signature and distributed consensus mechanism. Since it takes place in a decentralized fashion and adopts cryptographic technologies, it is immutable and can greatly save the cost involved in developing the application and improves efficiency. [15] It also avoids a single point of failure. Blockchain technology uses smart contracts which are basically computer programs that can execute contract terms automatically.

When the smart contracts meet a predefined condition, the parties involved can make payments in a transparent manner automatically [12]. Bitcoin is one of blockhain's most famous applications, apart from it, blockchain can be applied in financial services like online payments, remittance, digital assets and other fields including agriculture, intelligent transportation, identity management, mobile crowd sensing, security, internet of energy, industry 4.0 and supply chain management [15, 16].

There were many generations of blockchain that were produced—the first generation such as Bitcoin that acted as a public ledger to cryptographically store financial transactions. These provided a platform to store transactions, which is of great value in today's world. The second generation of blockchain provides a general structure of public blockchain used to store computational results. The third generation of blockchain introduces us to the concept of smart contracts, which are automatically executable computer programs. The fourth generation, tells us about the concept of multi-chains

This article is part of the topical collection "Advances in Computational Approaches for Artificial Intelligence, Image Processing, IoT and Cloud Applications" guest edited by Bhanu Prakash K N and M. Shivakumar.

✉ Akash Raj Khettry
akashrajkhettry5@gmail.com

✉ Karthik R. Patil
karthikpatil097@gmail.com

Abhilash C. Basavaraju
abhilashcb@jssateb.ac.in

[1] Department of CSE, JSS Academy of Technical Education Bangalore, Bangalore, India

while the fifth generation introduces us to Blockchain-as-a-Service (BaaS) where companies have invested a lot on the development of blockchain technology which has a variety of applications [21].

The blockchain includes decentralization. In the conventional technology, each transaction is stored in a centralized node and all validation takes place through this central trusted agency. Whereas in the case of blockchain, each transaction takes place between two peers without any kind of authentication by a central agency, thus reducing the cost on the servers also. Transparency—the data stored on the blockchain is transparent to each node, to view and to update the data. Open source—blockchain is an open source technology, which means anyone can use it to develop applications of their choice. Autonomy—every block can transfer and update the data on each other block. Immutable—the contents of the block are stored forever and it cannot be changed under any circumstances. Anonymity—it has solved the problem between nodes and thus every transaction is anonymous [8].

Blockchain Technology Has the Following Advantages

1. The blocks that are arranged in a chain are immutable, which means they cannot be altered or tampered by any means.
2. It is a distributed system, which implies that a copy of the ledger is available with all the members.
3. Blockchain technology is not centralized, that is, it does not depend on a centralized server [9].

Types of Blockchain

There are three categories of blockchain technologies:

1. Public blockchain: Each and every record is publicly viewable in this kind of blockchain. Everybody can participate in the process of consensus. Everyone can not only check but also verify the transactions [7]. A public blockchain is both readable and writable for everybody in the globe. Cryptocurrencies are based on public blockchain [4, 9]. Ethereum and Bitcoin are both examples of public blockchain which is depicted in Fig. 1 [8].
2. Consortium blockchain: This type of blockchain signifies that the node which has the authority could be selected previously. It generally possesses partnerships such as business-to-business. This type of blockchain contains data that include private or open, and could be viewed as partially decentralized [8]. Only a set of nodes that are selected previously would take part in a consortium blockchain's consensus process which is depicted in Fig. 2 [7]. Some of the consortium blockchains include R3CEV and Hyperledger [8].
3. Private blockchain: The nodes that belong to a particular organization will be permitted to participate in the consensus process. A private blockchain is considered as a network that is centralized, due to the fact that only a single organization controls it fully. The consortium blockchain built by many firms is partly decentralized as it would select a small fraction of nodes to ascertain the consensus which is depicted in Fig. 3. A private blockchain imposes limitations on who could interact with or read the blockchain. Private blockchains are also recognized as being permissioned, where only particular

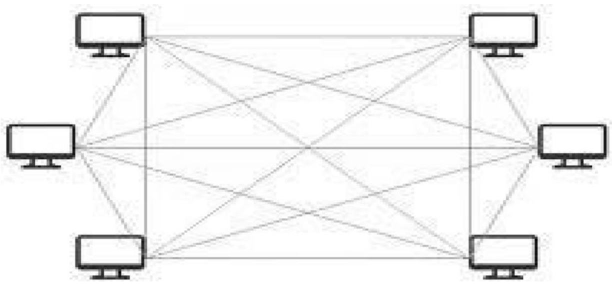

Fig. 1 Public blockchain

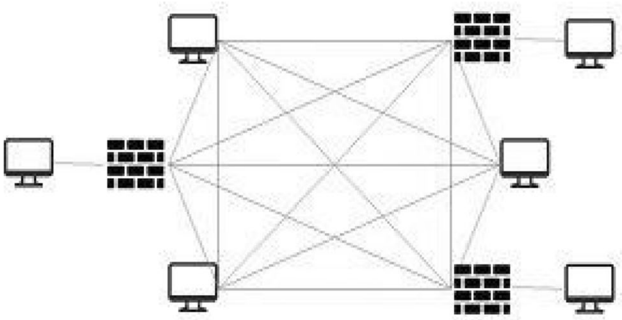

Fig. 2 Consortium blockchain

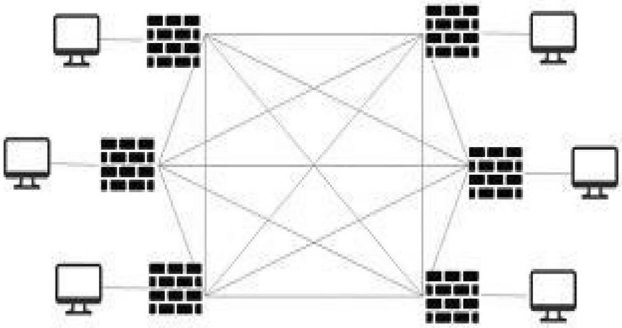

Fig. 3 Private blockchain

nodes that might interact with the blockchain can be provided access [4, 9].

The comparison of the three different types of blockchain:

- **Consensus determination** All nodes could be engaged in the consensus process in case of a public blockchain. A particular group of nodes are accountable for the validation of the block in the consortium blockchain. On the other hand, only a single firm fully controls the private blockchain, and the final consensus is determined by the firm.
- **Read permission** The transactions are publicly viewable in case of a public blockchain. On the other hand, it depends on the case of a consortium blockchain or a private blockchain.
- **Immutability** In a public blockchain, due to the fact that the records are cached on a huge amount of participants, it is not possible to manipulate transactions. In contrast, transactions in a consortium blockchain or a private blockchain could easily be manipulated as there are only a restricted number of participants.
- **Efficiency** In the public blockchain network, it takes a long time to promulgate blocks and transactions due to the fact that there are a huge amount of nodes. As a consequence, transaction performance is restricted and it has high latency. Efficiency could be increased in case of private and consortium blockchain, with fewer validators.
- **Centralized** The three types of blockchain have a key dissimilarity. The private blockchain is completely centralized as it is governed by a single organization, while, the public blockchain is decentralized. On the other hand, the consortium blockchain is partly centralized.
- **Consensus process** The public blockchain's consensus process could be joined by anybody. Unlike the public blockchain, both the consortium and the private block chain are permissioned.

Due to the fact that anybody could connect to the public blockchain, it could entice several active communities and users. There are several public blockchains emerging every day. Several business applications involve the usage of consortium blockchain. Many business consortium blockchain frameworks are currently being developed by hyperledger. Tools have been provided by Ethereum for building the consortium blockchains [7].

The following table depicts the comparison of the types of blockchain (Table 1) [7].

Centralization and Decentralization

Centralization is defined as a process in which the authority to make decisions lies in the hands of a few. All decisions are made by those who are regarded as the center of the organization [blockchain 1]. This authority can manipulate the entire system which includes updating databases, softwares, etc. The financial systems work in a centralized manner. A central authority acts as a single point of failure in the case of a centralized system. There are two types of centralized systems—one is an alternative service provider like bank and online payments, the other is the monopoly service provider such as governments and courts within a jurisdiction. The failure in the case of an alternative providers affects only the users and the users may shift to other providers, whereas decentralization is independent of any central authority and works independently [21]. Blockchain is a decentralized ledger. Centralization and decentralization in the case of a blockchain depend on the number of participants on the ledger. In the case of a decentralized network, anyone can participate and transact on the ledger.

Bitcoin is an example of a decentralized blockchain. It uses the concept of proof-of-work to maintain the integrity of the ledger. It also uses proof-of-work to regulate the rate at which new blocks are generated. Here every user in the network has a copy of a ledger that stores information about all the transactions occurring in the network. Since every user has a copy of the ledger, it is also considered to be distributed ledger. Bitcoin downloads every transaction and block, verifies them against their consensus rules and helps in providing the required functionality to process the transactions. Fully decentralized systems include permissionless

Table 1 Comparisons among public, consortium and private blockchain

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

blockchains such as Ethereum and Bitcoin [21]. Here users can join the network at any time, validate transactions and mine blocks.

However, decentralization has its own set of disadvantages.

- Though decentralized currency exists now, it may cease to exist in future. People have initially started showing interest on bitcoins, but if this system fails all the investors start facing heavy loses.
- Since the process is decentralized, transactions take place anonymously which might force the government to intervene in future. In such cases, centralized network is preferred as the identity of the participants are known. Thus, only credible and reputable participants are allowed to post on the ledger in the case of a centralized network, which is a pitfall for the decentralized process.
- Other risks include security as decentralized currency uses wallets. Every minute detail lost will lead to a loss in our investment made, and since it is a virtual investment, all the money invested is lost. Wallets can also be hacked and misused [10].

Decentralized applications: The present blockchain applications still use smart contracts, whose users run their programs on a local system in order to complete their application. Thus, the final blockchain application should be a dApp that is completely hosted by a peer-to-peer blockchain system. dApps require no governance and maintenance from the developers and thus operate without human intervention, forming Decentralized Autonomous Organization (DAO). Bitcoin is an example of a DAO. dApps have the following properties.

1. dApps should have their codes open sourced so that audits, if any from third parties become possible.
2. Tokens act as internal currency support that runs an ecosystem for a particular dApp.
3. There should be consensus among decentralized nodes.
4. A fully decentralized system has no central point of failure as all the components will be hosted on a blockchain [22].

Architecture and Working

A blockchain has a series of blocks that are connected to each other that store a complete list of records of transactions like a public ledger. Each block in the network points back to its previous block called the *parent* block, via a reference that is the parent's hash value. The Ethereum block also stores the hashes of the children of the block's ancestor (*uncle blocks*). The first block generated is called the *genesis block* and does not have a block of parents [15]. Blocks in the network are encrypted in a cascaded manner, which is the result obtained on encrypting the previous block is used in encrypting the current block. Thus, any changes made to any of the blocks leads to different encryption results [4].

A Block Is Composed of Two Parts: Block Header and Block Body

Block header is subdivided into

1. Block version: It contains the rules for validation to be followed.
2. Parent block hash: The parent block is referenced by the child block using a 256-bit hash value.
3. Merkle tree root hash: Each transaction in a block contains a hash value, which will be stored in the header with the help of the Merkle tree function.
4. Timestamp: current timestamp in seconds.
5. Nonce: A 4-bit field that starts at zero and increases for each calculation [15].

The body of the blockchain network is mainly composed of transactions and transaction counter. Each block has a limit on the total transactions it can hold, depending on the block size and the size of each transaction. It uses the concept of cryptography to validate the transaction authentication.

The algorithm to check whether is a block a valid or not is as follows:

1. The parent block is checked by the current block for validity.
2. The current block should be checked if its timestamp is greater than the previous block but less than 2 h into the future.
3. The block's proof-of-work is checked for validity.
4. S[0] is the state towards the end of the previous block.
5. Let TX be the transition for n transitions. For i in $0\ldots i-1$, set $S[i+1]=APPLY(S[i],TX[i])$. The application exits and returns false on encountering an error.
6. Set register $S[n]$ to be the state of the block and return True [13] (Fig. 4).

Digital Signature

A user on the network owns a pair of public key and private key. The user uses the public key to sign the transactions. The transactions signed digitally using the private key are distributed throughout the network and are then accessed by public keys, which is made available to everyone in the network. There are two phases involved in digital signature: a signing phase and a verification phase [15].

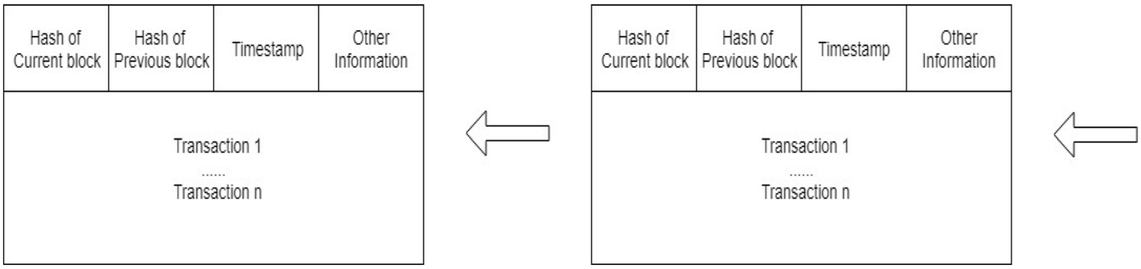

Fig. 4 Structure of blockchain (each of the panels in the figure, correspond to a block)

Working

Blockchain works as follows:

1. The sender node keeps a track of all the new data which are received, records it and transmits it over the entire network.
2. The received data are validated by the receiving node; if yes, the data are stored onto a block.
3. All the receiving nodes execute consensus algorithms to the block.
4. The block gets appended to the chain after executing the consensus algorithm thus leading to an increase in the length of the network [8].

The working of blockchain can be explained using the concept of bitcoin:

Bitcoin uses the concept of cryptography instead of entirely trusting a third party. The digital signature concept was thus used. The sender uses his private key to encrypt the data and the receiver uses his public key, the receiving person must know both the digital signature and private key. All the peer nodes are aware of the activities which take place. All the transactions have to be endorsed and validated before it is incorporated into the public ledger. First, if the sender has the right to send it, the validator must know. Second, it is the duty of the valuators to cross check and verify if the sender has enough amount of money to legit transactions. The transactions in the case of blockchain are not ordered; thus, there are more chances of double spending that can be eliminated using the blockchain technology. In this technology, all transactions are arranged in the form of a linear chain that is linked to each other. Each block stores the previous block's hash. Thus, transactions are stored in a secure manner using the blockchain technology [9].

Consensus Algorithm

Consensus is roughly defined as agreement between various parties. This term comes into existence since the beginning of war, where a few generals preferred to attack while a few preferred to retreat. Therefore, they had to come with an agreement, otherwise the mission is more likely to fail if only a few generals are ready for the war.

Reaching consensus in a distributed network, like blockchain is a challenge. There is no central node present to ensure that there are identical ledgers on the distributed node. So, there should be some protocol to ensure the nodes are consistent. Thus, consensus plays a major role here [7]. A foolproof consensus mechanism is required to maintain the coherence and sanity of data. The consensus mechanisms in blockchain help to eliminate the problem of double spending and byzantine general's problem [12]. A few of the consensus algorithms are explained below:

1. **Proof-of-work (PoW)** It requires all the network nodes to actively use brute force to solve cryptographic puzzles. This can used in the case of the Bitcoin network. In a decentralized network like blockchain, the transactions have to be recorded be someone. The easiest way is to select someone in random. But, this cannot be done as it is more prone to attacks. Thus, a node has to prove itself that it is not going to attack the network while publishing a block a transactions. In PoW, each node calculates the block header's hash value. The header contains nonce values and the miner would often change nonce to obtain different hash values. The calculated value should be equal to or smaller than this value. The node on reaching a target value would immediately broadcast it to other nodes and those nodes check the

correctness of the hash value. Upon validation, other miners append this new block onto the blockchain. The procedure followed by PoW is called mining and the nodes calculating the hash values are named miners. In PoW, the chain that becomes longer is considered to be an authentic one. Miners continue to mine their blocks until a branch longer than the previous one is found. Miners perform plenty of calculations in PoW, thus wasting a lot of resources.

2. **Proof-of-stake (PoS)** In PoS, the amount of money they have, proves their ownership. It is a common convection that people who own more money are less likely to attack the network. The single richest person has the power to dominate the network. Thus, many solutions have been proposed, for decision-making. Blockchain uses the concept of randomization to predict the next generator. PoS is more effective and saves a lot of energy when compared to PoW [7]. The main idea behind PoS is that it is difficult to acquire digital currency than it is difficult to acquire computing equipment [12].
3. **Practical byzantine fault tolerance (PBFT)** Here the participants in the network know each other and are able to distinguish as to which one is important and which is not. Hyperledger Fabric uses PBFT as its consensus algorithm. A new block is round and a primary would be selected according to the following rules. The whole process of PBFT is divided into three phases, namely pre-prepared, prepared and commit. A node enters into the next node only if two-third of the total nodes vote in favor of the node [7]. The node sends its request to all other nodes in the network. PBFT is required to suit the needs of certain organizations like bank, payroll systems or supply chain [12].

Table 2 depicts the comparison of blockchain consensus algorithm [12].

Consensus Algorithm Comparison

Different consensus algorithms can be compared accordingly:

- Node identity management—Knowing the identity of each miner in the network and selecting a primary in each round is necessary for the PBFT. POW and POS nodes are free to join the network.
- Energy saving—In PoS and PoW, miners have to perform hash on the block header to obtain the target value. There

Table 2 Comparison of blockchain consensus algorithms

Algorithm	Pros	Cons
Proof-of-work	Considered very secure as less prone to Sybil attacks	Quite slow at the moment, only one block added in 10 min
	51% of the pools computing power	Driven by rewards assigned to solving the hash, may run into problems as rewards dwindle
	Miners get rewards as Bitcoins	Consumes lot of electricity
	Prevents unlawful forking of the chain	Decisions are not final till six blocks are confirmed
Proof-of-stake	Less wasteful in terms of energy consumption	Miners are encouraged to hold on to their stake rather than converting it into at currency
	Less chance of hardware centralization	Economic penalties for fraudulent attempts
	Potentially faster than proof-of-work protocol	
	Possibly reduced possibility of selfish mining attack	
Practical byzantine fault tolerance	Can tolerate 1/3rd of the nodes to be faulty or adversarial	Parties must agree to the exact participation of groups
	Fast and efficient	Comes at the cost of anonymity
	Trust is decoupled from resource ownership, so small group can keep a powerful organization in check	

Table 3 Typical consensus algorithm comparison

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

is no mining involved in the consensus process in PBFT, so it saves energy.

- Tolerated power of adversary—The threshold for gaining control over the network is 51 percent of hash power. However, in the case of PoW, miners can gain revenue by 25% of the hashing power. PBFW handles one-third of the faulty nodes (Table 3) [7].

Applications

Currently, the currency used throughout the globe is mainly fiat currency or a government-assured currency, such as US dollar. These currencies are not financed by any holdings [14]. Bitcoin is a type of cryptocurrency that does not fall into the abovementioned category of currencies. Cryptocurrency is a medium of exchange that secures transactions using cryptography. The disadvantages of cryptocurrency include reduced price stability as there is no intervention by the government and have a penurious reserve of value in comparison with the traditional fiat currencies. However, cryptocurrencies provide an efficient medium of exchange both in terms of speed and cost, as it incorporates blockchain technology. There are several cryptocurrencies that have been developed and are used for specific purposes, out of which, the one that is highly successful and is used widely is bitcoin [15]. The fiat currency is used to measure the value of cryptocurrency [12].

An expansion of the blockchain technology to transmit things apart from *crypto currency* was recommended by Zyskind et al. [16]. The system that was proposed involves transactions that contain instructions for sharing, storing and queuing data. There are a large number of mobile applications that have full access to the data that belongs to the user, such as photos, messages, contacts and various other types of idiosyncratic data. The system's architecture presented by Zyskind et al. [16] incorporates blockchain and an offline storage mechanism to supervise permissions explicitly for every line entity, instead of providing unlimited complete access permissions. Any cloud or offline storage can be used to restrict the quantity of data gathered in the blockchain, which might lead to a third party dependency, but would provide an additionally scalable solution. Organizations might opt for a technology upgrade to acquire an increasingly reliable data privacy solution, for their respective data [12].

Blockchain technology can also introduce many transformations in the field of education. The application of blockchain technology has been proposed by Sharples and Dominguez [17], which furnishes an effortlessly sharable, verifiable and persistent record of educational rewards and records. Also, it discusses the likelihood of having an—*Educational Reputation Currency*—that is shared originally on the basis of any existing metric to the participating institutes. Then this currency could be forwarded consecutively in the blockchain and is granted to enhance the prestige of the learner. A restriction here is the way in which we can control the creation of such a reputable currency. For example, when a particular block is adjoined to the blockchain, as in the case of a Bitcoin blockchain, Bitcoins are generated. The appended Bitcoins will be granted to the block node. The Bitcoin algorithm also defines the quantity of Bitcoins created. Each appended block adjoins 25 bitcoins to the account of the winning node. Utilizing external reputation of educational organizations by third parties can create a bias and participants might question fairness. Sony and the University of Nicosia have successfully implemented blockchain to award educational certificates [12, 18, 19].

Recently, there has a digital transformation in *healthcare* with many healthcare machineries, hospitals, doctors storing the respective records of the patients digitally. The medical data being digitized not only provide effortless retrieval, but also sharing on the basis of need for improvising decision-making on the basis of previous medical cases and is very important for maintaining records legally. However, the process of digitization of medical data provides a huge risk of violation of the patient's privacy. A Healthcare Data Gateway (HDG) that incorporates blockchain technology was recommended. To ensure that the medical data are not altered by the physician, patient or anybody else, a private blockchain cloud is deployed in the system. The nature of medical data is diverse, that it can include video data, textual data, numeric data, image data, etc. A data model was proposed that is based on Indicator Centric Schema (ICS) to eradicate the complexity involved in storing different types of data. A single table is used in this model to organize the patient's entire data and incorporates simple fields like category, type, value, indicator, timestamp. The indicator, requestor, purpose, timestamp and retention duration can be included in a Purpose Centric Access Control model that can be incorporated in the ICS. A blockchain application requiring storage of different kinds of data may also use this type of model. The frequently and not frequently accessed data may be classified into different blocks of the blockchain. A system, called MeDShare has been presented that uses the blockchain technology, for dispensing the medical data amongst various cloud. The proposed system also provides auditing, provenance and data access control. MeDShare blocks malicious users and also uses smart contracts for detecting the behavior of data from its access patterns [12].

It has long been a challenge to build a secure electronic *voting system* that provides the privacy and fairness of current voting schemes while ensuring the flexibility and transparency offered by electronic systems. Blockchain can be used as a service to implement shared electronic voting systems that enhance security and reduce the cost of holding a countrywide election. An electronic voting system based on blockchain that uses smart contracts to provide cost-effective and secure election while ensuring privacy for voters was proposed. It is certain that blockchain technology offers a new opportunity to surmount the constraints and barriers to the adoption of electronic voting systems that ensure the safety and integrity of elections and lay the ground for transparency. You can send many transactions per second on the blockchain, by utilizing an Ethereum private blockchain, and using every aspect of the smart contract to lighten the load on the blockchain. For larger countries, certain additional measures would be required to provide higher transaction throughput per second [18].

Future Enhancements

Blockchain provides a secured storage of records which cannot be altered or tampered. One such application is the storage of medical and educational records. A person might have various educational and medical records that need to be provided at various organizations for various purposes such as documentation, verification, and validation. Storing all these records on a single block which is dedicated for a single person provides an efficient way of maintaining records. Since several blocks are connected to one another, the hash value of the preceding block is stored in the next block and any changes made lead to the change in the hash value, thus securing the block. To share the contents of the block, each user has to just send the link of the block to any user requesting to view the contents of the block. Thus, it provides an easier and faster way for people to access records which contain details of each user that can be shared in a secured manner. Also, all countries across the globe maintain a unique identification for each of its citizen. A person's identification also includes their biometrics like thumb impression, iris pattern etc. This can be stored safely on a block which is dedicated to one specific individual. The contents of the block can be accessed only by the concerned authority and cannot be tampered in any manner. Hence, this provides increased confidentiality and security.

Conclusion

Blockchain, a decentralized ledger technology, has found its applications in various fields such as cryptocurrency that includes Ethereum and Bitcoin. The use of Bitcoin in the digital market has grown enormously due to its increasing value and has made transactions secure and verifiable. It is accepted widely for transactions over the internet across the globe. All transactions which take place are secured and stored in a network called the blockchain. It is a form of distributed database which stores transactions. Since it is decentralized, it is not controlled by a single organization. It uses the concept of cryptography through which it has achieved the trust of several users. There are various consensus algorithms which can be applied to a variety of applications. Among them, PBFT is adapted by most of the industries owing to its better performance as compared to other algorithms. Today, enormous research is being carried out in the field of Blockchain Technology which has brought about a radical change in the functioning of healthcare, finance, banking, education, cyber security, etc. Although there are certain drawbacks in the field of blockchain, we cannot deny the fact that blockchain would bring a potential change in the field of technology.

Compliance with Ethical Standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Angela R, Liana B: The issue of competing currencies. Case study. Bitcoin 2014
2. Michael Crosby N, Pradhan Pattanayak SV, Vignesh K: Blockchain Technology-Beyond Bitcoin; 2015
3. Christian C: Architecture of the Hyperledger Blockchain Fabric; 2016
4. Wei-Tek T, Robert B, Yan Z, Lian Y: A system view of financial blockchains; 2016
5. Ariel E, Asaph A, John DH, Andrew L: A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data; 2016
6. Josep LR, Victor T-P, Andrés F, Denisa Gibov ic Hornyák O, Lutz M, Francesc M: A survey of blockchain technologies for open innovation (2017)
7. Zibin Z, Shaoan X, Hongning D, Xiangping C, Huaimin W: An overview of blockchain technology: architecture, consensus, and future trends; 2017
8. Iuon-Chang L, Iuon-Chang L, Tzu-Chun L: A survey of blockchain security issues and challenges; 2017
9. Rishav C, Rajdeep C: An overview of the emerging technology: blockchain; 2017
10. Akanksha K, Archana C, Chinmay E, Deepti T, Syed A: Blockchain–Literature Survey; 2017
11. Stefan S, Ronny S: Blockchain technology as an enabler of service systems: a structured literature review; 2017
12. Supriya TA, Vrushali K: Blockchain and its applications—a detailed survey; 2017
13. Vitalik B: A next generation smart contract and decentralized application platform
14. Charles S, Feniosky P: Blockchain for cities—a systematic literature review; 2018
15. Zibin Z, Shaoan X, Hong-Ning D, Xiangping C, Huaimin W: Blockchain challenges and opportunities: a survey; 2018

16. Mohamed Amine F, Makhlouf D, Mithun M, Abdelouahid D, Leandros M, Helge J: Blockchain technologies for the internet of things: research issues and challenges; 2018
17. Quoc Khanh N, Quang Vang D: Blockchain technology for the advancement of the future; 2018
18. Friðrik ÞH, Gunnlaugur KH, Mohammad H, Gísli H: Blockchain-based E-voting system; 2018
19. Mahdi HM, Maaruf A: Applications of blockchain technology beyond cryptocurrency; 2018
20. Tanesh K,Vidhya R, Ijaz A, An B, Erkki H, Mika Y: Blockchain utilization in healthcare: key requirements and challenges; 2018
21. Fahad A, Ibrahim E, Kumudu SM, Dharmendra S, Abbas J: Blockchain in IoT security: a survey; 2018
22. Wei C, Zehua W, Jason BE, Zhen H, Chen F, Victor CML: Decentralized applications: the blockchain-empowered software system; 2018

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.