Basics of blockchain☆

Shubhani Aggarwal and Neeraj Kumar
Thapar Institute of Engineering & Technology, Patiala, Punjab, India

Contents

Abstract

A blockchain is a distributed network, which can be used as a digital ledger as well as a mechanism that enables the secure transfer of assets without a central authority. Like the Internet is a technology that facilitates the digital flow of information, blockchain is a technology that facilitates the digital exchange of units of value. Anything from currencies to land titles to votes can be tokenized, stored, and exchanged on a blockchain network. In addition to the secure transfer of value, blockchain technology provides a permanent record of transactions and a single version of the truth called a network state, which is fully transparent in real-time for the benefit of all participants. In this chapter, we briefly describe the overview of blockchain and their characteristics that defines a blockchain is a prominent technology.

Chapter points

- In this chapter, we briefly discuss the centralized and distributed systems that is used in real-time applications.
- Here, we discuss the overview of blockchain and their characteristics. With this, we have also discussed the scope and motivation of blockchain.

☆ Introduction to blockchain.

Advances in Computers
ISSN 0065-2458
https://doi.org/10.1016/bs.adcom.2020.08.007

From the last few decades, the rapid advancements in information and communication technology (ICT) gives an exponential increase in the smart devices usage results in the demand of one of the most popular technologies called as the *Internet of things* (IoT). It refers to the ever-growing network of physical connected objects using the Internet. It consists of billions of interconnected objects to provide many services like e-healthcare, smart transportation, smart sensing, to name a few to the end-users. In such an environment, the bulk amount of data is being generated from these heterogeneous and graphically distributed devices. Michael Kanellos and Vernon Turner described the statistics in their report [1] that approximately 80 billion devices will be connected to the Internet by 2025. They also described that the total amount of digital data generated worldwide would be 4.4 Zettabytes in 2013 to 180 Zettabytes by 2025 as shown in Fig. 1. They also proved that currently connected devices per person is greater than the world population and is increasing exponentially as shown in Fig. 2.

From the above-mentioned facts, we found that the transmission of the huge amount of data and information to the core platform requires security and privacy as this whole information is shared using an open channel, i.e., Internet. In addition, it is also efficient for processing and storage of data at the cloud repository. However, the cloud systems are not found to be trustworthy as the global ecosystem has witnessed an exponential in the number of attacks in various applications like the financial system, supply chain management, healthcare, to name a few. Fig. 3 shows the growth trend of some of the recent attacks in various domains. To handle this situation, the dependability on cyber security mechanisms has increased manifold. There exist many

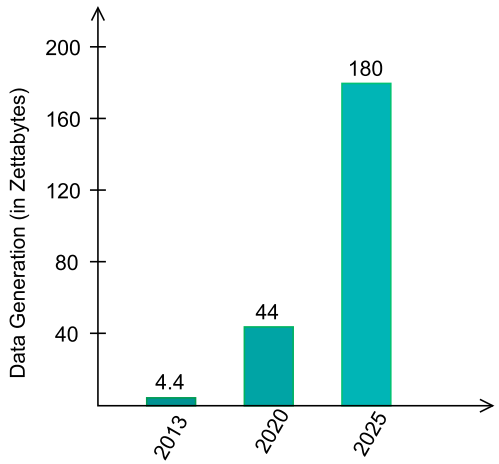

Fig. 1 Digital data generation from the smart devices.

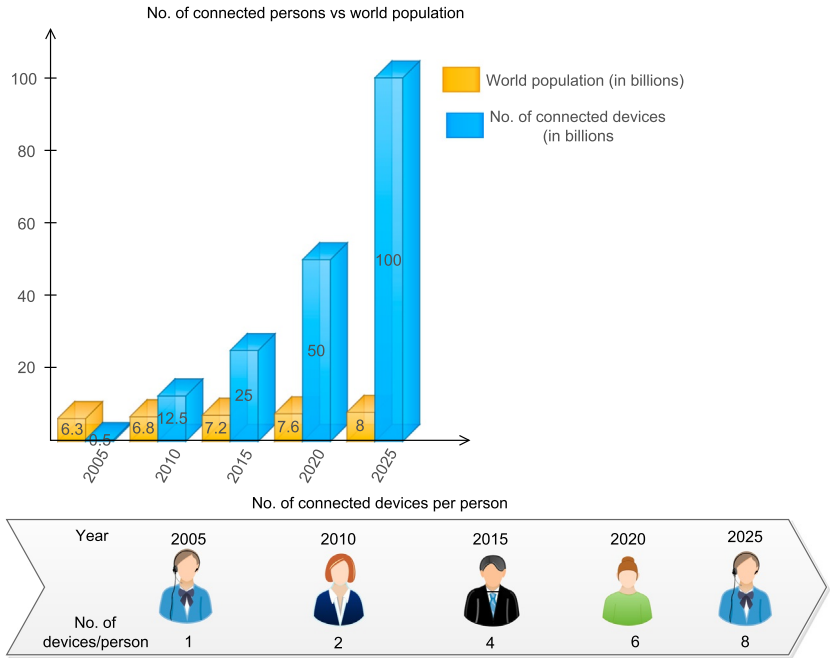

Fig. 2 No. of connected devices per person vs world population.

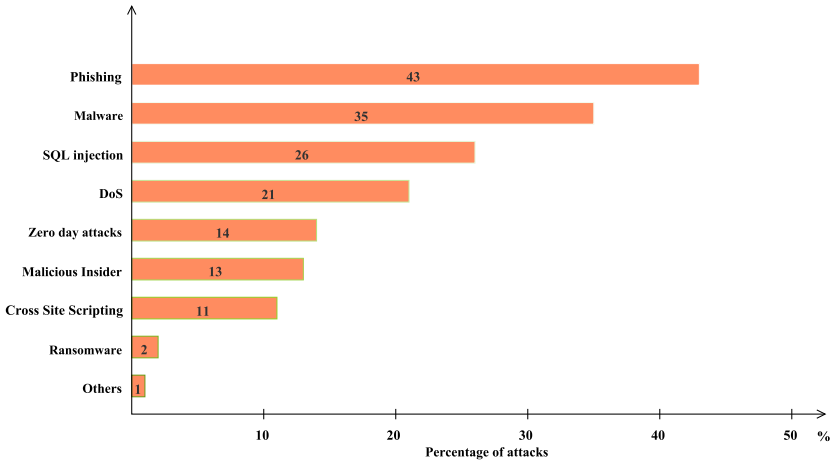

Fig. 3 Cyber attacks.

solutions to handle different type of cyber attacks on these applications [2]. However, the need of ubiquitous services in various applications on the move creates hurdles in front of the existing security solutions for many attacks such as replay attack, distributed denial-of-service (DDoS), data modification, eavesdropping. Therefore, to tackle these attacks in a distributed

environment, blockchain technology can be an effective solution due to its properties of easy transactions tracing, immutability, and decentralization.

1. Overview of blockchain

From the past few years, there has been an exponential increase in the usage of ICT for quick, efficient, and secure data exchange among different devices across the globe. With the emergence of the Internet, digital transformations between different entities emerged which results in data and information interchange among them. This interchanging is done through online transactions such as financial transactions for making payment and receive funds from different users. This entire communication and transactional system is validated using a trusted third party (TTP) system as shown in Fig. 4. This TTP system not only guarantees the safe and secure data delivery but also ensures the accurate updates in multiple accounts at the same time. However, there are a number of issues and challenges while accessing and sharing the information over the open channel [3]. For example, with the single TTP network controller, there are number of questions to be answered such as (1) What if the TTP becomes a fraud and cannot be trusted? (2) What if this party is hacked by a hacker or attacker gets hold of all the data which may act as a single point of failure? (3) Each time a TTP is used which may occur additional delay in a communication network? (4) The authenticity and validation of each transaction are very important.

Moreover, the existing traditional mechanisms heavily rely on TTP, i.e., the centralized network, where anonymity and privacy leakage are the major concerns. For this reason, it is important to have decentralized/distributed and secure system which can execute contracts and can handle transactions during the communication among devices. To tackle these issues, a secure communication technique is required, which can provide data security, integrity, authentication, non-repudiation, and confidentiality while transmitting the data generated by the various smart devices [4].

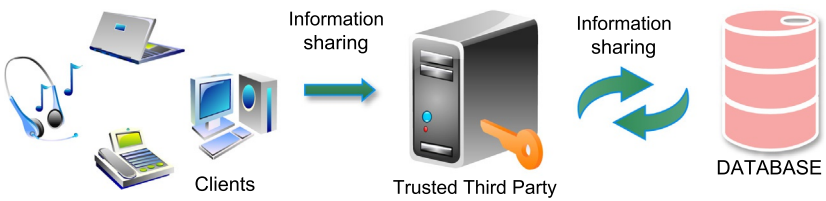

Fig. 4 Scenario of trusted third party system.

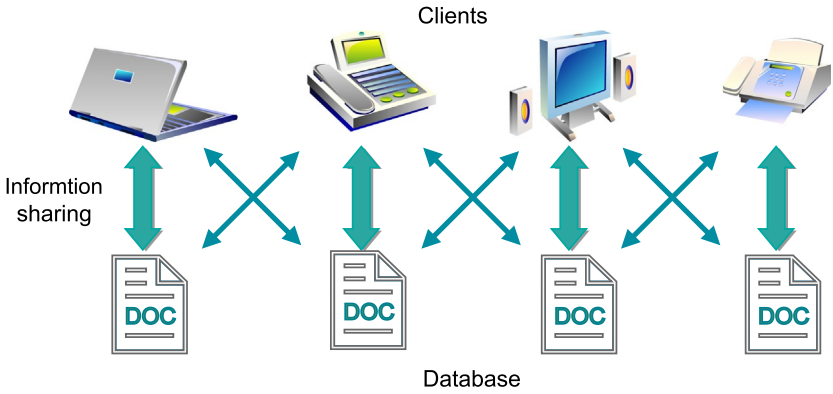

Fig. 5 Scenario of distributed system.

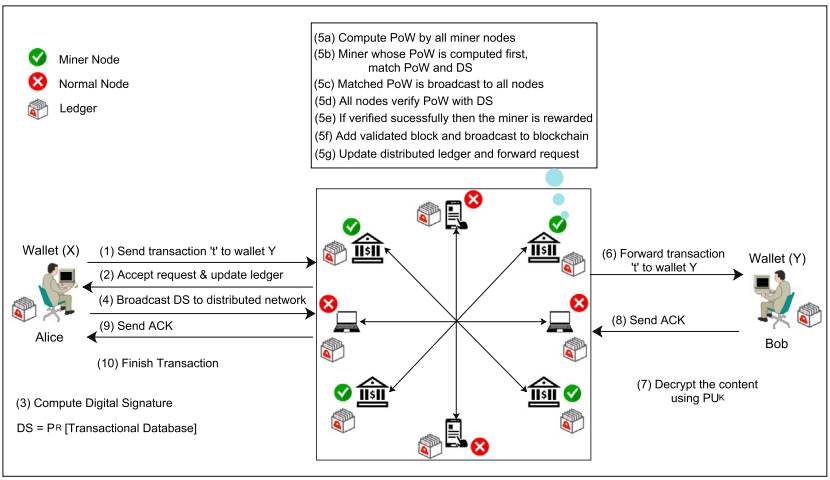

Fig. 6 Bitcoin transaction volume.

The solution to all these problems can be provided by distributed ledger technology called *BLOCKCHAIN* as shown in Fig 5. It was invented by Satoshi Nakamoto by introducing the first-ever decentralized crypto-currency called "Bitcoin" [5, 6]. The popularity of bitcoin is evident in the bitcoin transaction volume, which is presented in Fig. 6. It is a distributed network having the potential for creating and using smart contract in IoT-based smart applications to ensure security and to remove a single point of failure. In these smart applications, there can be many network attacks as depicted in Fig. 7. To defend against the attacks such as DDoS, malware, server message block, brute force, etc., blockchain technology is one of

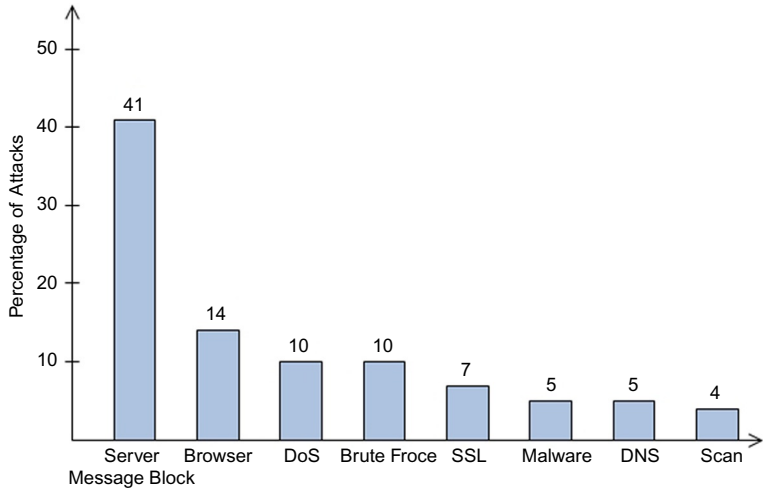

Fig. 7 Network attacks.

the possible solutions. It ensures security and privacy to the system and provides the properties such as scalability, edibility, reliability, authorization, identity management, data integrity, confidentiality, nonrepudiation, authentication, and accountability.

In the recent past, there came a few pioneering technologies. Also, previously discarded technologies get a fresh life because of a dazzling array of distinct improvisations in the information technology (IT) infrastructures domain and also due to the steady emergence of integrated and insightful platforms. Artificial intelligence (AI) with a bombardment of a heavily improved machine learning and deep learning (ML/DL) algorithms is garnering a lot of attraction and attention these days. With a host of digitization and edge technologies gaining uninhibited prominence and dominance, the aspects of extreme connectivity and deeper integration among digitized entities and devices are seeing the reality. The IoT and cyber-physical systems (CPS) concepts are traversing through surging popularity these days. Another highly visible trend is to club together multiple proven technologies to present new and clustered technology. The blockchain technology is a neat combination of several pioneering technologies and this blended paradigm is being pronounced as one of the most significant technologies capable of making solid and spectacular impacts.

Blockchain is a part of a distributed software system which is one of the most popular technologies of security of the modern era. To handle the security, blockchain technology can be used, which is based on the concept

of the cryptocurrency system. It provides secrecy and privacy to the users using cryptographic primitives to authenticate the communication among the nodes. It is a chain of*digital signatures* comprising of nodes which are connected to each other in a mesh topology.

The most important feature of blockchain is that it is a decentralized computation and information sharing platform that enables multiple authoritative domains to combine and come to a common platform for providing security and privacy for different transactions. These multiple domains can coordinate, cooperate, and collaborate to develop applications at business intelligence process. In this way, this technology can be useful for rational decision-making in management and engineering applications [7].

2. Traditional centralized systems

In a traditional system, the way of sharing the documents is by using the document file. For example *Alice* wants to share the document with Bob. Firstly, *Alice* writes down all the content inside the document then she will share the document to *Bob*. After that, *Bob* updates the document according to the needs and share the document again to her. So, this was the traditional way of coordination and cooperation between *Alice* and Bob when they want to read or write the document. The scenario of sharing between *Alice and Bob* is as shown in Fig. 8.

The particular scenario is as shown in Fig. 8, there are many problems. The first fundamental problem of this architecture is that *Alice and Bob* both are not able to edit the document simultaneously. The replaceable architecture of Fig. 8 is as shown in Fig. 9. In this architecture, a shared document platform has been used. Here, *Alice and Bob* both can write or read the document simultaneously. But, this architecture is still centralized and have some major drawbacks as follows. The first drawback of this system is that it may have single point of failure. The second drawback is that if something happens or server crash down, then the entire information or data get lost.

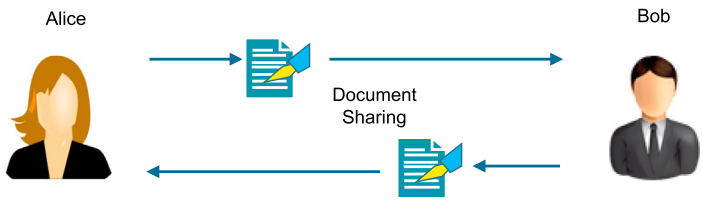

Fig. 8 Traditional way of sharing the document 1.

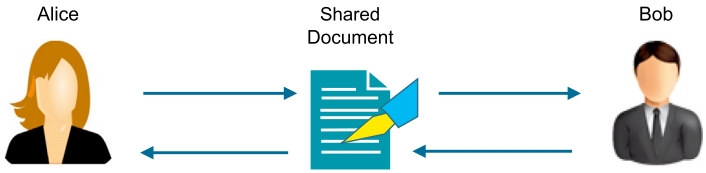

Fig. 9 Traditional way of sharing the document 2.

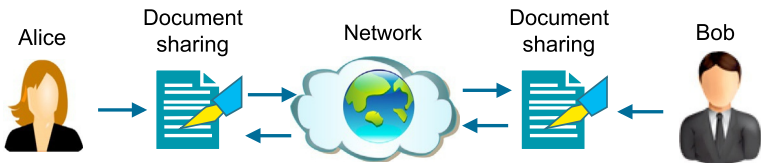

Fig. 10 Sharing the document using blockchain network.

From the aforementioned reasons, researchers move from the centralized platform to a distributed platform that provides scalability and reliability as shown in Fig. 10.

3. Types of systems

There are three types of systems, i.e., centralized, decentralized, and distributed systems that are used in real-time applications. Their description is described in the following sections

3.1 Centralized system

In the case of centralized architecture (see Fig. 11), there is a central coordination system in which each node is connected to that system and whatever they want to share the information will be shared by that system. In this system, there is a problem if central coordination system fails (single point of failure) than all of these individual nodes will get disconnected and the network becomes shut down.

3.2 Decentralized system

In the case of the decentralization system (see Fig. 12), there is a number of coordinators instead of single and all the coordinators and their individual nodes are cooperative with each other. If any particular or multiple nodes fail then they can connect to the other coordinators or to the other individual nodes. They can share their information or perform the tasks using available coordinators. In this architecture, if a simultaneous failure of nodes

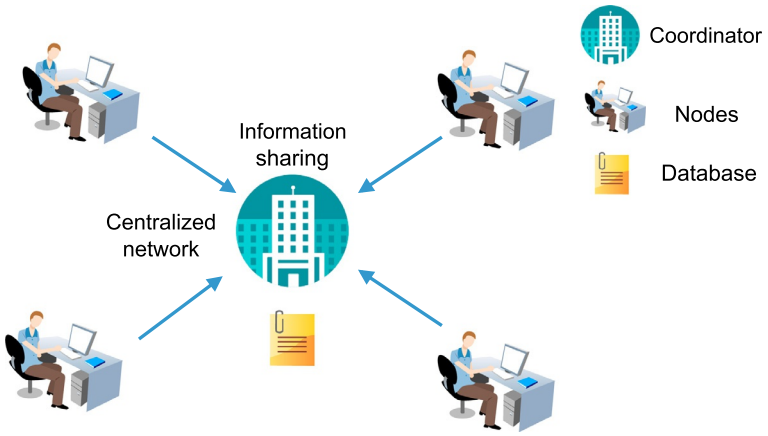

Fig. 11 Centralized architecture.

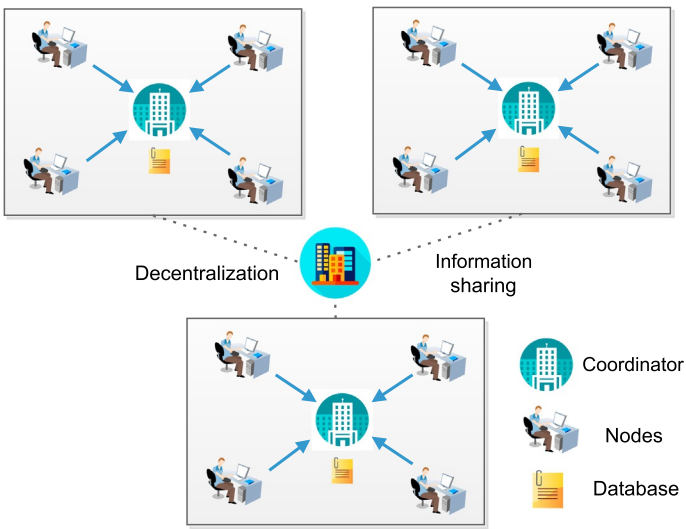

Fig. 12 Decentralized architecture.

occur then individual nodes may not be able to cooperate with each other and the network gets disconnected. So, to solve the problem of a decentralized system, distributed architecture comes into the picture.

3.3 Distributed system

In a distributed architecture (see Fig. 13), there is no need for a central authority. In this system architecture, each node is connected and coordinated with every node. They can collectively share the information and

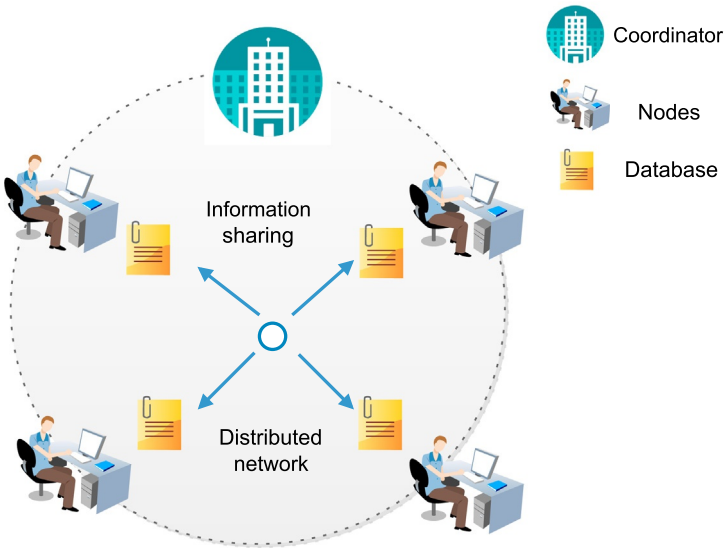

Fig. 13 Distributed architecture.

worked together. In this, if any single or multiple nodes fails then other nodes can share their information or perform the operation using coordination and cooperation.

So, from the aforementioned facts it is clear that, blockchain is a platform which helps us to provide a decentralized and distributed platform where we can share the information among others in a trusty manner. Using this technology, both *Bob and Alice* can edit or update the document simultaneously. The main advantage of this technology is that it does not rely on the centralized system. So, by definition, we can say that blockchain is a platform that provides consistency in the database. It also supports whatever information *Alice* and *Bob* are writing individually on the document, they get synchronized over the network.

4. Scope of the blockchain

Blockchain, a relatively recent technological trend, is a decentralized and chain of cryptographic blocks linked together to form a P2P network which is distributed in nature [8, 9]. This technology can be leveraged to achieve authorization, accountability, authentication (AAA), integrity, security, privacy, confidentiality and nonrepudiation for real-time applications which may not be provided by the centralized systems effectively and efficiently [10–14].

It is a technology which is the combination of three technologies: public-key cryptography, P2P network, and the program. It has shown its revolution in terms of digital cryptocurrency that removes the requirement of an intermediatory expert in the field of registration and distribution. It has also provided the most popular product, i.e., Bitcoin which is a type of cryptocurrency and work as a public ledger for all the transactions done on the network. It has resolved the problems like double-spending, unauthorized accessing, etc. and thus improves the security and privacy of the network. An incredible scope of this technology has been observed in various application like smart grid, voting system, financial system, supply chain management, etc. [15]. Incorporating blockchain with digital transactions gives many benefits such as time and money can be saved which is used for validating and processing the transactions. Its function on a distributed database makes the operation smoothly, ensuring tight security, and made it safe from the cyber attacks. It is one of the most consistent technologies when it requires to keep track of the digital properties. It also has the abilities to add distinct features like security and privacy in the company's structure.

The future scope of the blockchain technology in different sectors is described as under.

1. *Blockchain in digital advertising*: Presently, digital advertising faces a lot of problems such as fraud domain, lack of transparency, data tampering, etc. Due to the issues, incentives are not affiliated but blockchain has provided a solution to ensure transparent, tamper-proof data to the network as it executes trust in a trustless environment.
2. *Cyber security*: The blockchain data is stored in the public ledgers which is verified and encrypted using cryptographic primitives. So, the data and information cannot to be tampered or attacked without any involvement of central authority.
3. *No single point of failure*: It is a decentralized technology in which each node is connected to every node without any involvement of the third party which may act as a single point of failure. It provides a public ledger that consists of verifiable and validated transaction data which lowers the risk of data modification and trust issues on the network.
4. *Supply chain management*: It record all the information or data into the public distributed ledgers and supervise them more transparently. It also helps to minimize human errors and time delays. It is also used to monitor costs, employment, and releases at each point of the supply chain.

5. *Beyond the world of computing*: Currently, most of the countries are developing their blockchain strategies for usage in the future. But still, there are many issues such as security and privacy in various sectors like finance where blockchain can be used to address various problems like data modification. It can also be used to generate a database for medical purpose, to manage insurance policies, etc.
6. *Internet of things and networking*: The different companies such as IBM, Samsung, etc. are utilizing blockchain technology to create a new distributed network of IoT devices. It will improve the requirement of central authority to manage the central database among all communicating parties.
7. *Cloud storage*: Data stored on the central cloud storage can be exposed to hacking, loss of data or human error. With this technology, it is possible to make cloud storage more protected and robust against various type of attacks.

5. Characteristics of blockchain

In this section, we discuss the main features of blockchain technology. These features provide major benefits in most of the applications due to the properties discussed below (Fig. 14).

1. *Immutability*: Immutability means something that cannot be altered or changed. To create the immutability, ledgers is one of the main values of blockchain technology. All the centralized systems and database can be corrupted and requires a TTP to ensure integrity. But, the blockchain-based decentralized database provides transparency and tamper-proof data.
2. *Decentralization*: In a traditional centralized system, each transaction needs to be validated through TTP which may act as a single point of failure. In contrast to this, the decentralized-based blockchain system provides a trustless environment between the different nodes who do not trust each other. These nodes can coordinate and cooperate with each other in a rational decision-making process.
3. *Digital*: All the information on the blockchain is stored as digital that eliminates the need for manual documentation. This digital information is stored in the blocks of the blockchain.
4. *Distributed ledger*: The indistinguishable copies of all the information are shared on the blockchain. A public and distributed ledgers store every information about a transaction and the participant. So, every node can act as verifiers of the ledger. Each node can participate individually

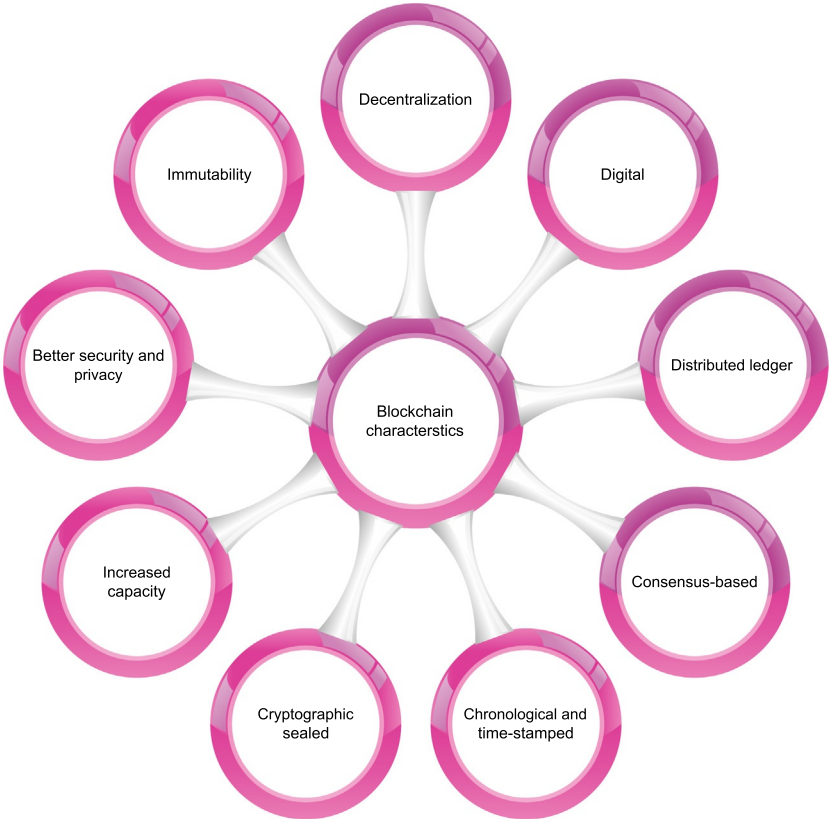

Fig. 14 Characteristics of Blockchain.

and validate the transaction independently without any involvement of central authority. If any node fails, the remaining nodes can continue to operate and ensure no disruption.

5. *Consensus-based*: In simple words, the consensus is a decision-making process for a group of nodes that are active on the network. Here, the nodes can come to an agreement as fast as possible because when million of nodes are validating a transaction, a consensus-based agreement is necessary for the system. The transaction on the blockchain can be executed only if all the nodes on the network anonymously approve it.
6. *Chronological and time-stamped*: Blockchain is a chain of blocks each being a repository that stores information pertaining to a transaction and also links to the previous block in the same transaction. These connected blocks form a chronological chain by providing a stream of the underlying transactions.

7. *Cryptographically sealed*: The blocks in the blockchain are created and combined together using cryptographic primitives in the chain. So, it is very difficult to edit, delete or update the already created blocks and it on the blockchain network. Thereby, creating digital assets ensures a high level of robustness and trust. Also, it is known as *failure-resistant*, because, if the failure of a large number of nodes in the network, then blockchain remains available and eliminates the problem of a single point of failure.
8. *Increased capacity*: This feature of the blockchain technology increases the capacity of the entire network. Because there are thousands of computer which are working together as a whole in the blockchain network and have great power than a few computers worked in the centralized system.
9. *Better security and privacy*: Blockchain provides better security and privacy to the network than a centralized system because there is no single point of failure to shut down the whole network. It also provides privacy because every information on the blockchain is hashed cryptographically that acts as a firewall for attacks.

6. Key motivations for blockchain

Many technical, business, and use cases are emerging for experimenting with and embracing the blockchain technology, which is seen largely as a disruptive one by many. Today banks play a very vital role in facilitating financial transactions. Banks provide much-needed trust when we exchange money with our friends and colleagues across the world. But this model is very expensive and slow. These intermediary-based financial transactions stifle the innovation culture. The centralized computing model being adopted by banks comes in the way of exploiting the distinct benefits of distributed and decentralized computing. If the centralized database gets broken, then all kinds of customer, confidential, and corporate data get stolen. This model is vulnerable to DDoS attacks. Hence, the brewing trend is that we need trust but at the same time, we want to discard banks and other intermediaries forthwith. Employing banks makes the whole process a bit complicated. For legal transactions, lawyers and judges play that intermediary role. Contract documents are being made and used for eliminating any kind of confusion and cheatings. Precisely speaking, trust and formal contracts have been the predominant ways and means for all

kinds of transactions. Unfortunately, both trust and contract are not optimal solutions. The blockchain technology offers a third option, which is affordable, inventive, fast, and secure.

Second, we are heading toward the connected era. We are being bombarded with a dazzling array of slim and sleek, trendy and handy devices. These embedded and networked devices come handy in producing next-generation services and applications not only for business houses but also for common people. That is, we are on the verge of entering into the era of the IoT and cyber-physical systems (CPS). The well-known challenge and concern here is the security, safety, and privacy of IoT devices and data. The traditional security solution approaches are found incompetent in guaranteeing the utmost security due to the participation of resource-constrained devices. Any everyday environment stuffed and equipped with intelligent sensors and actuators is typically dynamic and liable for instability. Herein, the arrival of the blockchain paradigm is being applauded. That is, futuristic environments (personal, industrial, social, and professional) are going to be not only smart but also secure and safe.

Finally, suppose you are a retailer souring from over 100 different fast. Moving consumer goods (FMCG) companies, including over 10,000 stock keeping units, in one store, and your B2B transactions amount to over 1000 high transactions a day. Now, these 1000 transactions are just from one store. You may have ten or more stores. Each of these transactions gets recorded on a combination of paper and digital methods. Now the problem here is that your purchase department can under-report transactions and bill you for the ordered quantity. So, while your stock shows the right amount, your store shelves are never stacked up after a sale. This presents a problem because it hurts the top line and bottom-line revenues. Further on, there can also be price changes very often being made by the FMCG company. That details cannot be recorded by the retailer.

Now enter blockchain, assuming that the retailer has moved all transactions digitally, which creates blocks of each transaction like Vendor A supplied X, Vendor B supplied Y and Vendor C supplied YY and in the process the system ropes in the finance and the purchasing team together with each receipt generated. Now each transaction becomes part of a block and gets recorded in the ledger of all parties involved. Any changes made to a price or purchase agreement, another block gets added, which has to be verified by all parties. The algorithm secures each block of transactions and it cannot be tampered with because all parties have the keys to make the transactions legitimate. The technology brings transparency and traceability.

Newer technologies, architectural patterns, and tools are forthcoming in order to assist deeper and decisive automation in business operations. Also, disruptive applications can be realized through fresh technology-inspired approaches and algorithms. Decentralized applications (DApps) and smart contracts are being demanded these days. Blockchain has shown the initial exuberance and the innate strength to set up and sustain DApps across multiple industry verticals. There are a number of distinct advantages of distributed databases and decentralized applications. IT, business, and device services can do certain actions automatically through smart contracts. That is, contract logic gets embedded inside the application and service code in order to automate the contractual obligations. Thus, eliminating third-party involvement through automation is the core strength of this new technological paradigm. Several other business verticals are keenly experimenting and exploring to gain something new out of this concept.

References

[1] Forbes, 2016, Available: https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/ (accessed 26 July 2019).
[2] R. Iqbal, F. Doctor, B. More, S. Mahmud, U. Yousuf, Big data analytics and computat. ional intelligence for cyber-physical systems: recent trends and state of the art applications, Futur. Gener. Comput. Syst. 105 (2017) 766–778..
[3] D. Puthal, S.P. Mohanty, P. Nanda, U. Choppali, Building security perimeters to protect network systems against cyber threats [future directions], IEEE Consumer Electron. Mag. 6 (4) (2017) 24–27.
[4] N. Komninos, E. Philippou, A. Pitsillides, Survey in smart grid and smart home security: issues, challenges and countermeasures, IEEE Commun. Surv. Tutorials 16 (4) (2014) 1933–1954.
[5] R. Grinberg, Bitcoin: an innovative alternative digital currency, Hast. Sci. Technol. Law J. 4 (2012) 159.
[6] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Working Paper, 2008.
[7] Q. Feng, D. He, S. Zeadally, M.K. Khan, N. Kumar, A survey on privacy protection in blockchain system, J. Netw. Comput. Appl. 126 (2019) 45–58.
[8] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, Y.-X. Yang, A secure cryptocurrency scheme based on post-quantum blockchain, IEEE Access 6 (2018) 27205–27213.
[9] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, C. Yang, The blockchain as a decentralized security framework [future directions], IEEE Consumer Electron. Mag. 7 (2) (2018) 18–21.
[10] N. Kshetri, J. Voas, Blockchain in developing countries, IT Professional 20 (2) (2018) 11–14.
[11] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaría, To blockchain or not to blockchain: that is the question, IT Professional 20 (2) (2018) 62–74.
[12] A. Anjum, M. Sporny, A. Sill, Blockchain standards for compliance and trust, IEEE Cloud Comput. 4 (4) (2017) 84–90.

[13] A. Jindal, G.S. Aujla, N. Kumar, SURVIVOR: a blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment, Comput. Netw. 153 (2019) 36–48.
[14] A.N. Mencias, D. Dillenberger, P. Novotny, F. Toth, T.E. Morris, V. Paprotski, J. Dayka, T. Visegrady, B. O'Farrell, J. Lang, An optimized blockchain solution for the IBM z14, IBM J. Res. Dev. 62 (2/3) (2018) 4-1.
[15] S.V. Akram, P.K. Malik, R. Singh, G. Anita, S. Tanwar, Adoption of blockchain technology in various realms: opportunities and challenges. Security Privacy (2020). https://doi.org/10.1002/spy2.109.

About the authors

Shubhani Aggarwal is pursuing PhD from Thapar Institute of Engineering & Technology (Deemed to be University), Patiala, Punjab, India. She received the BTech degree in Computer Science and Engineering from Punjabi University, Patiala, Punjab, India, in 2015, and the ME degree in Computer Science from Panjab University, Chandigarh, India, in 2017. She has many research interests in the area of Blockchain, cryptography, Internet of Drones, and information security.

Neeraj Kumar received his PhD in CSE from Shri Mata Vaishno Devi University, Katra (Jammu and Kashmir), India in 2009, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as a Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology (Deemed to be University), Patiala (Punjab), India. He has published more than 400 technical research papers in top-cited journals such as IEEE TKDE, IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCE, IEEE TII, IEEE TVT, IEEE ITS, IEEE SG, IEEE Netw., IEEE Comm., IEEE WC, IEEE IoTJ, IEEE SJ, Computer Networks, Information sciences, FGCS, JNCA, JPDC, and ComCom. He has guided many research scholars leading to PhD and ME/MTech.

His research is supported by funding from UGC, DST, CSIR, and TCS. His research areas are Network Management, IoT, Big Data Analytics, Deep Learning, and Cybersecurity. He is serving as editor of the following journals of repute: ACM Computing Survey, ACM·IEEE Transactions on Sustainable Computing, IEEE·IEEE Systems Journal, IEEE·IEEE Network Magazine, IEE·IEEE Communication Magazine, IEE·Journal of Networks and Computer Applications, Elsevier Computer Communication, Elsevier International Journal of Communication Systems, Wiley. Also, he has been a guest editor of various international journals of repute such as IEEE Access, IEEE ITS, Elsevier CEE, IEEE Communication Magazine, IEEE Network Magazine, Computer Networks, Elsevier, Future Generation Computer Systems, Elsevier, Journal of Medical Systems, Springer, Computer and Electrical Engineering, Elsevier, Mobile Information Systems, International Journal of Ad Hoc and Ubiquitous Computing, Telecommunication Systems, Springer, and Journal of Supercomputing, Springer. He has also edited/authored 10 books with international/national publishers like IET, Springer, Elsevier, CRC: Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions (ISBN-13: 978-1-78561-898-7), Machine Learning for Cognitive IoT, CRC Press, Blockchain, Big Data and IoT, Blockchain Technologies Across Industrial Vertical, Elsevier, Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms and Solutions (ISBN: 978-981-13-8759-3), Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019) (ISBN 978-981-15-3369-3). One of the edited text-book entitled, "Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms, and Solutions" published in Springer in 2019 is having 3.5 million downloads till June 6, 2020. It attracts attention of the researchers across the globe (https://www.springer.com/in/book/9789811387586). He has been a workshop chair at IEEE Globecom 2018 and IEEE ICC 2019 and TPC Chair and member for various international conferences such as IEEE MASS 2020 and IEEE MSN 2020. He is a senior member of the IEEE. He has more than 12,321 citations to his credit with current h-index of 60 (September 2020). He has won the best papers award from IEEE Systems Journal and ICC 2018, Kansas City in 2018. He has been listed in the highly cited researcher of 2019 list of Web of Science (WoS). In India, he is listed in top 10 position among highly cited researchers list. He is an adjunct professor at Asia University, Taiwan, King Abdul Aziz University, Jeddah, Saudi Arabia, and Charles Darwin University, Australia.