History of blockchain-Blockchain 1.0: Currency ☆

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

Contents

Abstract

Bitcoin is a cryptocurrency, which is not backed by any country's central bank or government. It can be traded for goods or services with vendors who accept bitcoins as payment. These bitcoins are the blocks of secure data. This data is transferred from one person to another and verifying the transaction, i.e., spending the money that requires high computing power to safely verify the individual transactions. The P2P network monitors and verifies the transfer of bitcoins between users. It can be used to book hotels, shopping, financial transactions, buy video games, etc. In this chapter, we describe the evolution of bitcoin cryptocurrency to evolution of blockchain and their usage in real-world entities.

☆ Introduction to blockchain.

Advances in Computers
ISSN 0065-2458
https://doi.org/10.1016/bs.adcom.2020.08.008

Chapter points

- In this chapter, we firstly discuss the bitcoin cryptocurrency and describes the working of bitcoin cryptocurrency. Then, we discuss the problems of double-spending and Byzantine General's Computing in bitcoin. After that, we discuss the evolution of blockchain from Bitcoin cryptocurrency.
- Here, we also discuss the fundamentals and potential impact of Blockchain in real-time world.

1. Bitcoin cryptocurrency

Bitcoin is a decentralized digital currency that enables instant payments to anyone, anywhere in the world. The primary concern of the bitcoin is a cross country payment transaction and other concern is that there is no need for a central authority or no government organization will have to control over it. It uses P2P technology and supports different level of securities so that the entire system becomes tamper-proof.

The two main operations of bitcoin cryptocurrency is as follows.

1. *Transaction management*: In this, everyone can transfer of bitcoins from one user to another. For example, anyone can buy something by utilizing the bitcoins make transfer of bitcoins from India to any other country.
2. *Money issuance*: It regulates the monetary base of bitcoins like economical aspects of a coin base of digital cryptocurrency whereas, in our banking system, there is a central authority that regulates the money inside the country.

Bitcoin cryptocurrency must be in controlled and in limited supply to have value. The value of bitcoin increases due to the following reasons.

- It is decentralized technology.
- It is limited in number (21 billion).
- It is P2P network.
- It can be anonymous.
- It is transparent in nature (open source).
- It is easy to buy and sell.
- It is irreversible (no-charge backs).
- It is difficult and expensive to hack.
- It has increased in value over 10,000 percent in a short period of time.

Traditionally, people deposit their money into a bank account. But now, they can store their currency into bitcoin wallets. It can store every transaction has to be done in the network. These transactions are verified by the bitcoin miners and get rewarded by bitcoin currency. Any malicious

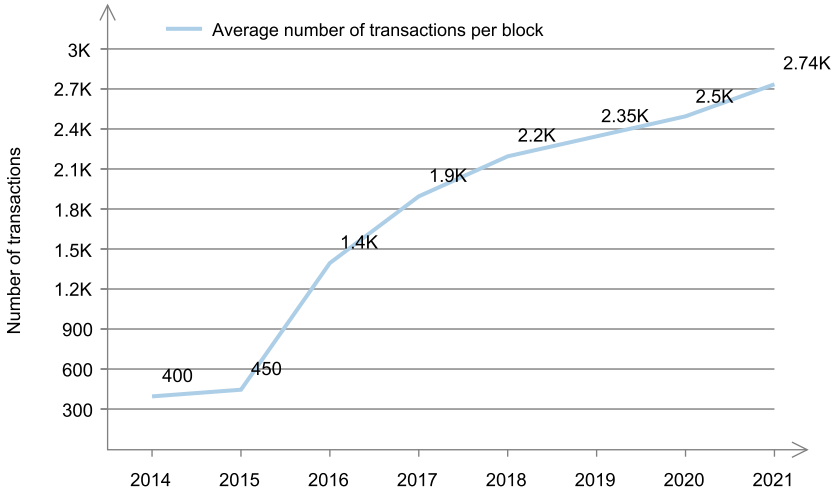

Fig. 1 Increase in average number of bitcoin transactions per block as per year advances.

currency needs to be rejected and only to accept the actual currency that is flowing through the network. According to the study as shown in Fig. 1, it has been observed that an average number of bitcoin transactions per block is increased as per years advance.

1.1 Creation of bitcoins

In bitcoin standard architecture, the creation of the block rate is adjusted after every 2016 blocks. This block creation takes 2 weeks of the period. After every 2016 blocks, there is readjustment for bitcoins that have been created from mining the blocks. So, this process still continues and to again manage the number of bitcoins generated from the mining blocks and is decreased geometrically.

For example, the number of bitcoins that are rewarded during the mining process gets decreased with a rate of 50 % after every 2,10,000 blocks creation. It approximately takes 4 years to complete this amount of blocks creation. From 2008 to 2012, when bitcoin cryptocurrency was developed by Satoshi Nakamoto, the block reward fees for one block is 50 bitcoins. After then, from 2012 to 2016 it gets reduced to 12.50 bitcoins per block which is again gradually decreased to 6.25 bitcoins per block for the next 4 years. In this way, the reward for mining the block will get close to 0. After some mathematical calculations, it has been found that when the number of bitcoins will reach up to 21 billion in the network, then further no reward will get to the miners from the system. So, by the time passes the

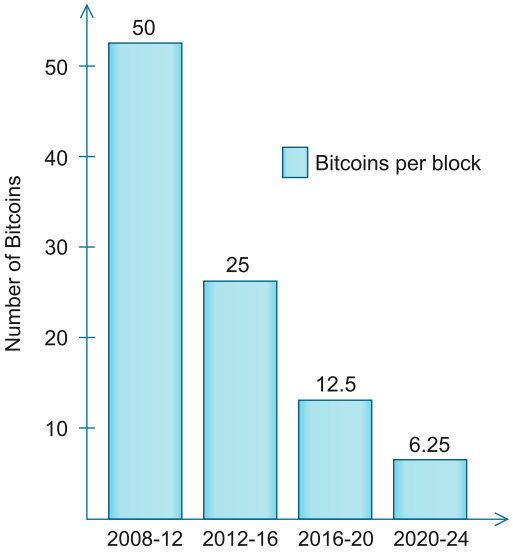

Fig. 2 Reduction in number of bitcoins per block can be seen as years advance.

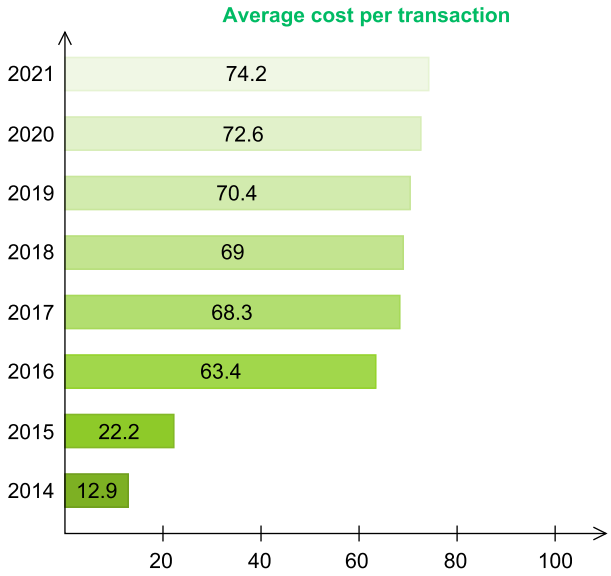

Fig. 3 Increase in the cost per transaction can be seen as years advance.

number of bitcoins per block will decrease and transaction fees will be increased. Over the past few years, a per year reduction in number of bitcoins per block and an increase in the cost per bitcoin transaction have been observed are as shown in Figs. 2 and 3.

1.2 Control of bitcoin network

Nobody controls the bitcoin network. It is controlled by their own bitcoin users across the globe. All the users are free to choose what software and version they want to use in the bitcoin network. It can work only when strong consensus agreement is present among all the users. By this, all users and developers have incentives irrespective of the security to the consensus agreement.

1.3 Bitcoin transaction system

From the user perspective view, bitcoin is nothing more than a personal wallet of the user and allows a user to send and receive bitcoins with each other. This is how it works for all users. Let us explain with example of *Alice* and *Bob*. All nodes in the network have their own digital wallets to store the bitcoin cryptocurrency on their computers. Basically, bitcoin wallets are public ledgers that provide access to all multiple bitcoin addresses. An address is a string of letters and numbers like "*KULP2589gcdg5UKUD*" and each address has its own balance of bitcoins. Now, *Bob* creates a new bitcoin address for accepting the bitcoin cryptocurrency from *Alice*. The scenario of bitcoin address is as shown in Fig. 4.

To verify the legitimate account user in the bitcoin network, the digital signatures with Public-key cryptography has been used. The bitcoin address represents a unique private or secret key and their corresponding public key

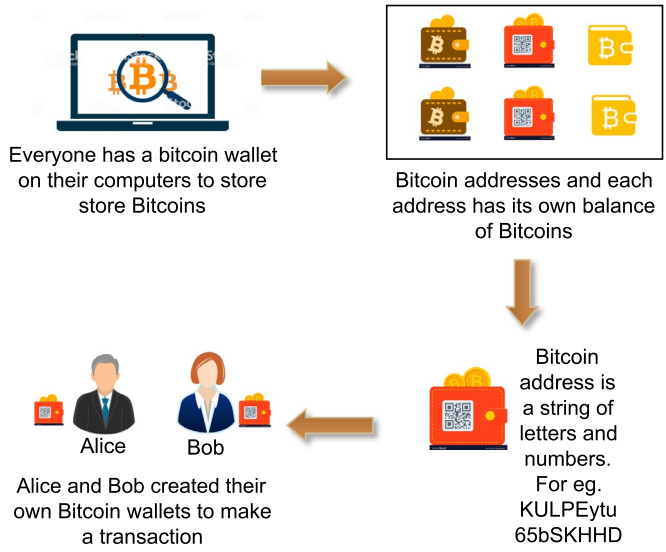

Fig. 4 Scenario of bitcoin address.

are stored in the bitcoin address. A *secret key* is used to sign a message for security and matching *public key* is used to verify the signed message it is valid or not. Now, to make a secure bitcoin transaction between *Alice* and *Bob*, *Alice* wants to transfer some amount of bitcoins to *Bob*. He holds his bitcoin address with a private key and broadcast this transaction to the blockchain network. Anyone on the network can use the public key of *Alice* to verify the transaction request, which is actually coming from the legitimate account user. By the use of digital signatures, we can provide authentication and integrity to the network. The scenario of the digital signatures is as shown in Fig. 5 and how it can be used in bitcoin system is as shown in Fig. 6.

The next step after the authenticity of the user is to verify the transactional data using cryptographic hash functions such as SHA-1 and SHA-2. These cryptographic primitives are used to secure data transmission between *Alice* and *Bob*. These hash functions transform the collection of data into an alphanumeric string with a fixed length called hash value and it is impossible for an adversary to predict the initial data that will create specific value. The transactional data, previous hash value, and the nonce (random number) create a new hash value that is completely different from

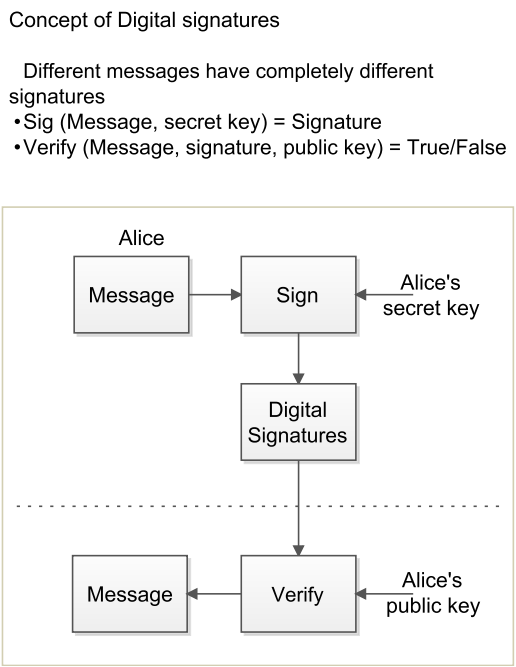

Fig. 5 The scenario of the digital signatures.

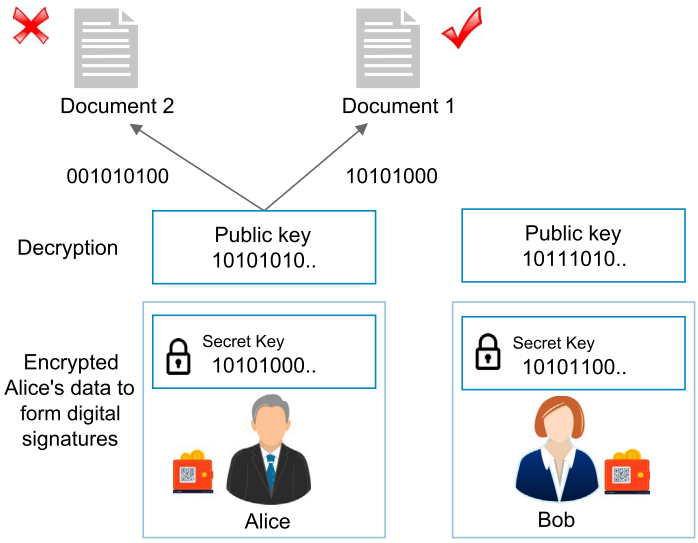

Fig. 6 Digital signatures used in bitcoin transaction system.

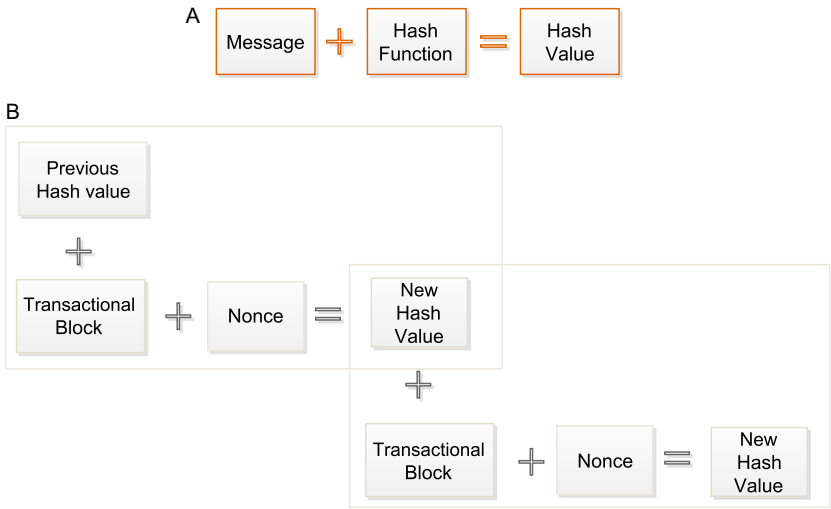

Fig. 7 (A) Cryptographic hash function. (B) The scenario of cryptographic hash function in bitcoin system.

other hash values. A little change in the input value will completely change the output hash value because each new value of hash contains information about previous hash value. The scenario of cryptographic hash function in bitcoin system is as shown in Fig. 7.

However, creating hashes is computationally important but in the bitcoin system, it must start with a certain number of zeroes like '*00000000000000…5876335859358*'. After creating the hash value, the transactional data is stored into the blocks where bitcoin miners calculate a new hash value for verification on the basis of present information (previous hash value, block, and nonce). The miners have no idea to predict which nonce will produce a correct hash value with a required number of zeroes. So, they will produce different hash value with different nonces until they reach on one that works. They use their maximum computational resources and power to find out the exact hash value during this process. After the mining process has been done, the first miner who finds the computational hash correctly get rewarded with bitcoin cryptocurrency in its wallet. The block is added into the blockchain network and each node of the network updates their local copies. As time passes, *Alice's* bitcoin transfer to *Bob* is done successfully and *Bob* receives the bitcoins. The bitcoin transaction between *Alice* and *Bob* is as shown in Fig. 8.

In this bitcoin transaction process, if anyone wants to modify the details then he or she would have to redo all the tasks and process as bitcoin miners did. Any little changes require or completely different nonce value. So, it is impossible for a hacker to hack transactional data that has to be done in the blockchain network.

1.4 Advantages of bitcoin cryptocurrency

The main advantages of bitcoin cryptocurrency over traditional systems are described as follows.

- *Payment freedom*: Bitcoin cryptocurrency is used for online purchases, payments, and investments. It is easily possible to send and receive bitcoins anywhere anytime in the world. There is no borders, bureaucracy, bank holidays, etc. to make payment transactions. It allows its users to be in full control of their currency. They can use their currency in their own way.
- *Choose our own fees*: In the bitcoin cryptocurrency system, there is no particular fees to send or receive bitcoins from anywhere at any time. In this, the transaction fee is not related to the number of bitcoins that are being sent or received by the users. However, it depends on how secure the transaction is? The more bitcoin transaction fee represents the high security and fast confirmation of the transaction.
- *Fewer risks of wholesaler*: Bitcoin transactions are irreversible, secure and do not contain personal information. It protects the wholesaler from frauds or fraudulent charge-backs. The net results of this currency are lower fees, larger markets, and fewer administrative costs than fiat currency.

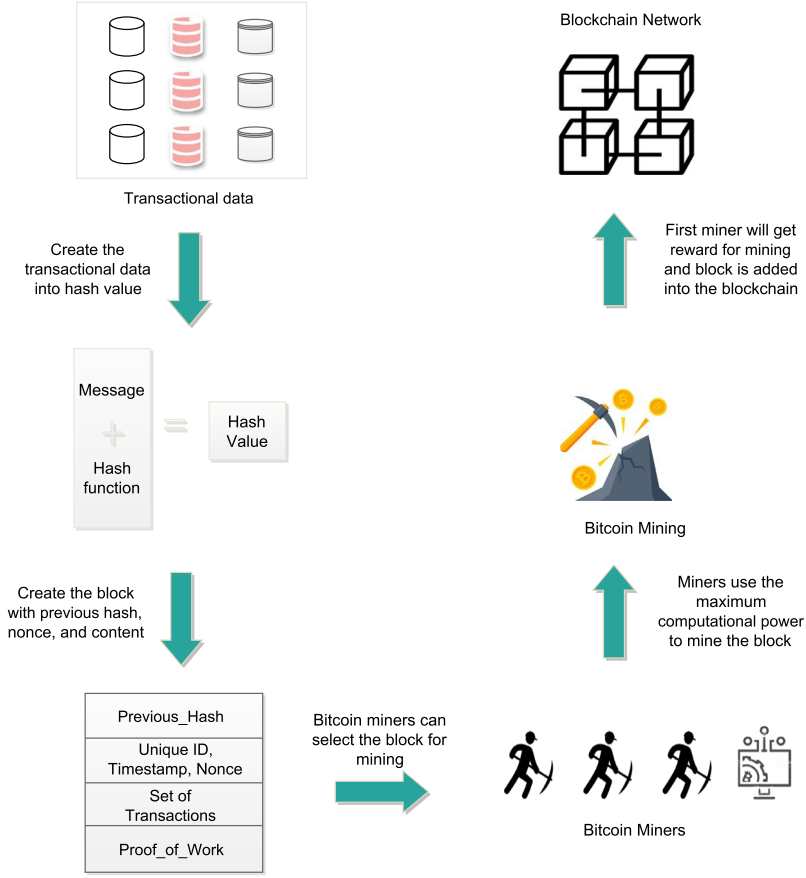

Fig. 8 Bitcoin transaction system.

- *Security and control*: Bitcoin transactions are full control under the bitcoin users. So, it is impossible for a hacker to hack or to force unwanted changes in this transaction. It can be made without any personal information of the user which provides strong protection against identity theft.
- *Transparent and neutral*: All the bitcoin transactions are passed through the blockchain network where every node can verify the transaction and use in a real-time. There is no individual control and manipulation on the bitcoin protocol because it is secured by cryptography. This allows the core of bitcoin to be trusted for being neutral, tamper-proof, and transparent.

After the study of the advantages of the bitcoin cryptocurrency, there is a number of disadvantages that needs to be resolved for ongoing development. Many people are still aware of this cryptocurrency and their software and

tools are still in active development with some incomplete features. These features and services are being developed to make the bitcoin more secure and accessible to masses. Most of the bitcoin-based companies are new and small in number in the process of maturing.

2. Double-spending problem

Double-spending is a problem in which the same digital currency can be spent more than once. At the same time, it is an instance in which the transaction uses the same input as another transaction that has already been broadcast on the network. This is the major flaw present in the digital cryptocurrency. The bitcoin system is designed to prevent double-spending in a decentralized environment where there is no central authority to interfere with the disputes. However, as bitcoin cryptocurrency is neither physical money nor transmitted via centralized database, it raises challenges on preventing this issue. In this system, a ledger of each node is the most important concept. It is used to record the transactions and contain information of how much amount of currency each account still has.

To understand the concept, let us take an example as shown in Fig. 9. Suppose *Alice* wants to pay some currency to *Bob* in bitcoin cryptocurrency. This transaction will be sent to the P2P network and be recorded in the ledgers of the network as a type of verification process that takes some time to complete. That means, during verification time *Alice* might be able to send another payment to *Charlie* using same bitcoin currency token that was spent

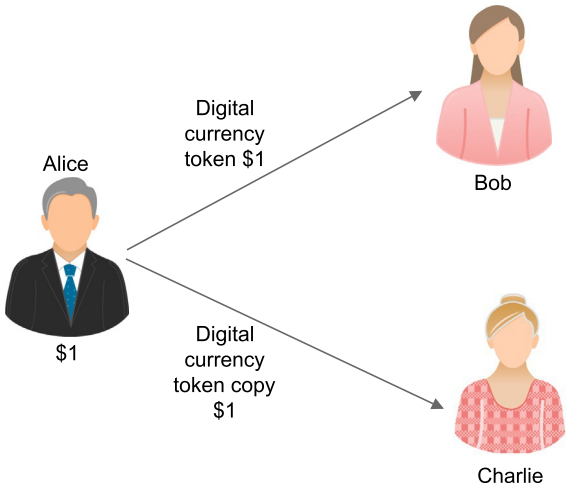

Fig. 9 Double-spending problem.

in the *Alice-Bob* transaction. It means, one bitcoin token being paid twice. This problem is called double-spending problem.

2.1 Bitcoin prevents the double-spending problem

Fig. 10 shows the trading of cryptocurrency between a *buyer* and a *seller*. The *buyer* advised the miners to make a bitcoin payment to *seller* while the *seller* delivers the service to the *buyer* simultaneously. The*buyer* can make secret

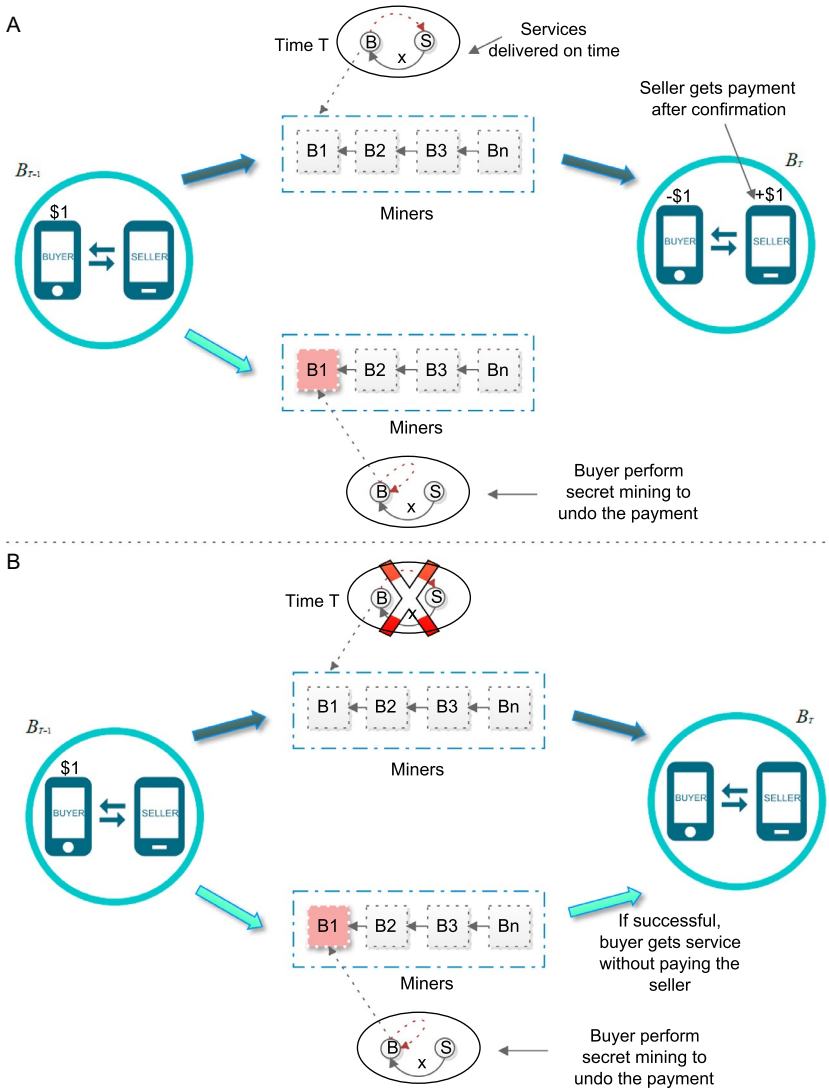

Fig. 10 (A) Double-spending attempt fails. (B) Double-spending attempt accepts.

mining for an alternative history where the funds are not transferred. The outcome of the transaction depends on which the payment transaction is incorporated into the network first. If the payment transaction is incorporated, then the double-spending attempt fails and the *seller* receives the payment. If the transaction is accepted, then double-spending attempt accepts and the *seller* selling the service to the *buyer* without paying.

3. Byzantine Generals' problem

Byzantine Generals' is a problem that symbolizes the difficulty of having a coordinated conversation when nontrusted parties are involved. They must agree on the single strategy to avoid complete failure but somewhere involved parties are corrupt and sharing false information.

Let us explain with the help of an example. On each side of the enemy city, there are two armies present to attack at the same time. But the city is strong enough to safe by itself against one of the armies attacks but not so strong to defend against both the armies at the same time. If they do not attack at the same time, they lose the enemy city's attack. So, the Generals' of both the armies must agree on the same time of when to attack. They can communicate with each other by sending a messenger through the enemy city. There is no other way to communicate with each other. By this, *General A* send the message "*Hey General B, we are going to attack this city on Monday. Can we count on you with us on this attack?*" The messenger then walks through the enemy city and delivers the message to *General B*. *General B* responds back to the *General A* with a message "*No, we can not do attack on Monday. We will not free on that day. So, what about Friday? If we attack on Friday, will you join us on Friday to attack?*" Then, again the messenger walks through the city and delivers the message to General again and so on. However, during message delivery, here is the attacker, where the messenger could potentially get caught and replaced by the fake-news messenger in the city. The fake-news messenger tries to change with the other General to attack the city at the wrong time. So, In this scenario, there is no way to check that the delivered message is authentic or not in a trust-less environment, which is called the Byzantine Generals problem. The scenario of this problem is as shown in Fig. 11.

3.1 Solution of Byzantine Generals with proof-of-work

PoW consensus mechanism has been used to solve the Byzantine Generals problem as it achieves a majority agreement without any involvement of

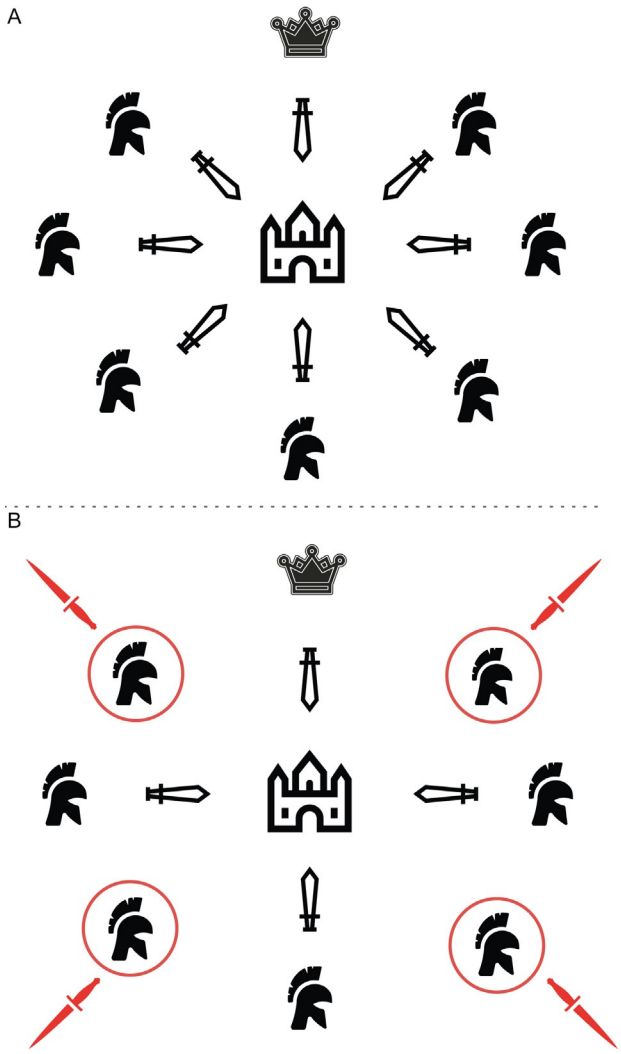

Fig. 11 (A) Coordinated attack = victory. (B) Uncoordinated attack = defeat.

central authority and in-spite the use of untrusted or unknown parties. It is the original blockchain mechanism that enables the user on the network to reach a trusty consensus. It is essentially an answer to a complex mathematical problem. It takes a lot of time and work to create but make the validate process easy for others. It allows the distributed and uncoordinated Generals to come to a consensus agreement as under.

1. The Generals agree on the first plan that has been accepted as a plan by all Generals.
2. A number of Generals solve the PoW problem, creating a block, and broadcast it to the network so that all Generals have received it.
3. Each General verifies the block and works on solving the next PoW problem so that their plan add it to the previous information.
4. Each time General solves the PoW problem, a block is generated, and the chain begins to grow.

Fig. 12 shows the consensus between armies using PoW. By this consensus mechanism in Byzantine Generals problem, the Generals can arrive at a state where they know when to attack the city and can estimate their chances of successfully doing so. In this way, they can prevent different messages and signals coming from many Generals to attack being sent simultaneously. This mechanism also prevents the system from malicious actors, i.e., traitors that destroy the network by changing the message with historic messages. In this mechanism, every information is stored in the ledgers as the hash values. This value is stored as a previous hash in every new block. So, a little change to an earlier block will fully change the hash value of all the successive blocks. This would take a huge amount of computing power that ensures the ledger is secure and tamper-proof.

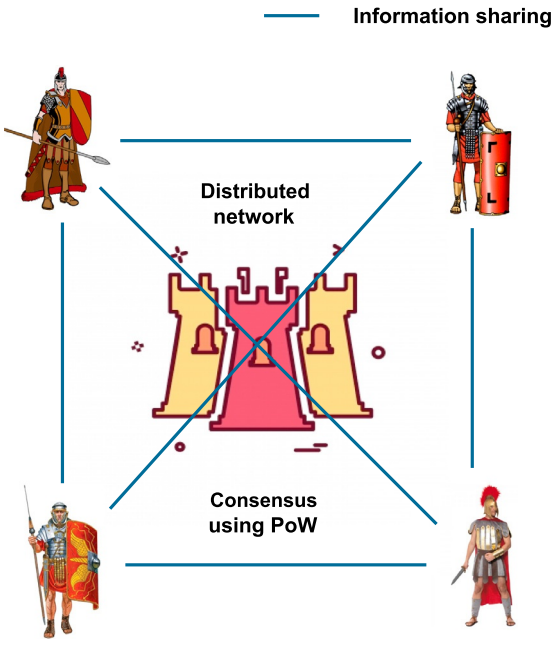

Fig. 12 Solving the Byzantine Generals problem using PoW.

4. Evolution of blockchain

From January 2009, blockchain technology has been developing and emerging. In the beginning, the blockchain technology supporting bitcoin that produced the following properties.

- Decentralization of the bitcoin cryptocurrency and financial transactions.
- Decentralization of the data storage using a distributed database.
- Eliminates the central authority that verify the transactions in a centralized system.
- Support for tamper-proof data and transparency in a P2P network.
- Introduces the PoW concept which makes the blockchain technology more unique because it combines with high computational power by the use of nodes connected to the network. These nodes verify the transactions and secure the public ledger.

4.1 Understanding blockchain technology

The blockchain is a time-stamped series of an immutable record of data that is distributed and managed by a cluster of computers. Each of these blocks is combined together using cryptographic primitives to make a secure chain. As it is a decentralized system, there is no third-party validator to manage all the records and data information at blockchain network. So, it is a shared immutable public ledger that is open and accessible for everyone to see. Hence, the data present on the blockchain is transparent in nature and everyone can be involved for their accountable reasons. The understanding of blockchain is as shown in Fig. 13.

The blockchain technology is a simple yet creative way of transmitting the information among the nodes of the network in a fully automated and secure manner. The nodes of the network create a block that contains transaction information. Then, this block is verified by thousands maybe millions of distributed computer nodes around the network. The verified block is then added to the chain across the network by creating a unique record with a unique history. The main advantage of the blockchain is that if falsifying a single record then, the entire chain of blockchain is false in millions of instances which is impossible in practice. It carries no transaction cost but has high infrastructure cost. It can not use only for making transactions but also replace bitcoin models and processes that rely on charging a payment for a transaction. For example, The gig economy hub Fivver charges $0.5 on five transactions between the buyer and the seller services. Bitcoin itself use

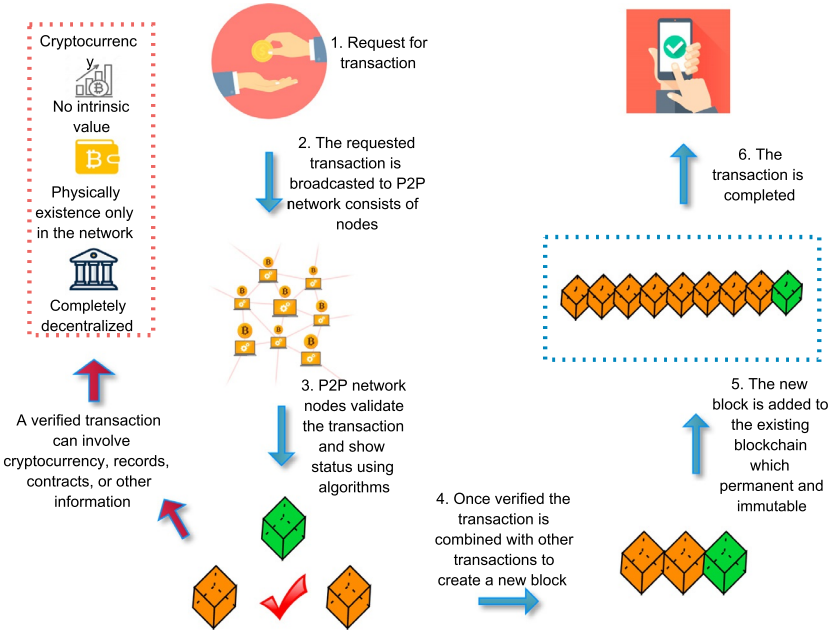

Fig. 13 Understanding blockchain.

this model to make the transaction secure but it can also be used in other ways. The main reasons why blockchain has gained popularity are as follows.

- It is not kept by only one single entity means there is no involvement of the third-party validator that may leads to a single point of failure.
- The data stored on the blocks of the blockchain is cryptographically secured.
- It is immutable in nature so no one can tamper the data that is inside the blockchain.
- It is transparent in nature so anyone can track the data if they want to.

5. Fundamentals of blockchain

The three main properties of blockchain technology that helped it to gain recognition all over the world are as follows.

1. *Decentralization*: Before bitcoin cryptocurrency, all the users were used to centralized services that depend on the third-party validator. The centralized system stores all type of data and information. The user would interact with this system whatever information and data they want to use it or required at any-time. For example, Banks, that stores all the

Fig. 14 The centralized system.

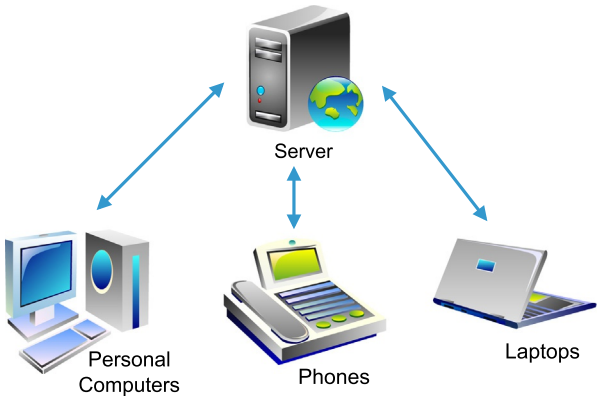

Fig. 15 The client–server model.

currency and money in a centralized way. The only way to pay someone is by going through banks as shown in Fig. 14.

The other example is the client–server model as shown in Fig. 15 in which when someone is searching on the Google then, he or she sends a query to server who gets back at you after few seconds with relevant information. Hence, there are some vulnerabilities in a centralized system that are mentioned below.

- In a centralized system, all the data and information is stored in one place where anyone can attack or change the data.
- If the centralized system goes through some software up-gradations then, it would halt the entire system.
- If in between the centralized system shut-down then, no one will be able to do a task or to access information.
- If the centralized system is malicious or corrupted then, all the data inside it will be compromised.

So, from the above-mentioned reasons are the causes that change the entire system from centralized to decentralized. In the decentralized system, everyone owns the information by itself in the network. If someone wants to interact with a particular node then, he or she can directly

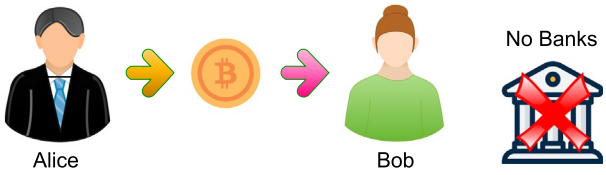

Fig. 16 Transaction without central authority.

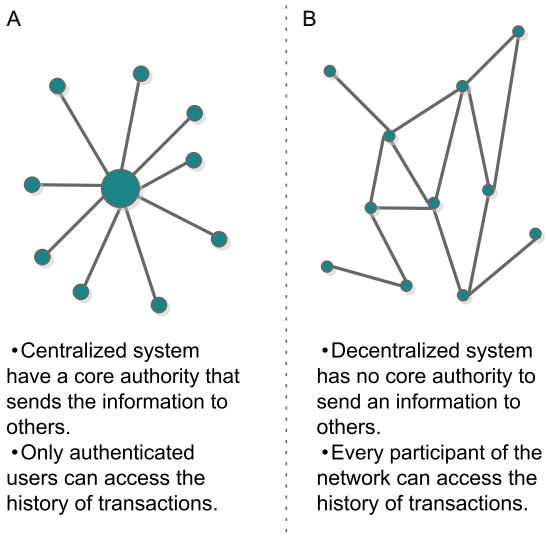

Fig. 17 The new networks. (A) Centralized system; (B) Decentralized system.

interact with that node without going through a third-party validator. In this, we are the only one for the charge of our cryptocurrency. Anyone can send or receive currency from anybody without the involvement of third-party as shown in Fig. 16. The new networks instead of using centralized system is as shown in Fig. 17.

2. *Transparency*: The most important and interesting concept in blockchain technology is transparency. In the system, a person's personal information is hidden using complex cryptographic primitives and is only represented by their public address. For example, Fig. 18 shows the person's transaction history and Fig. 19 shows the detail information of person in which their personal information (address) is secured by hash cryptography.
3. *Immutability*: It means that once something has been written or done into the blockchain, it can not be tampered or changed because it is secured by a cryptographic hash function. In this context, the transaction is taken as an input and run through a hashing algorithm (SHA-256) which gives an output of a fixed length as shown in Fig. 20. Even, a small change in

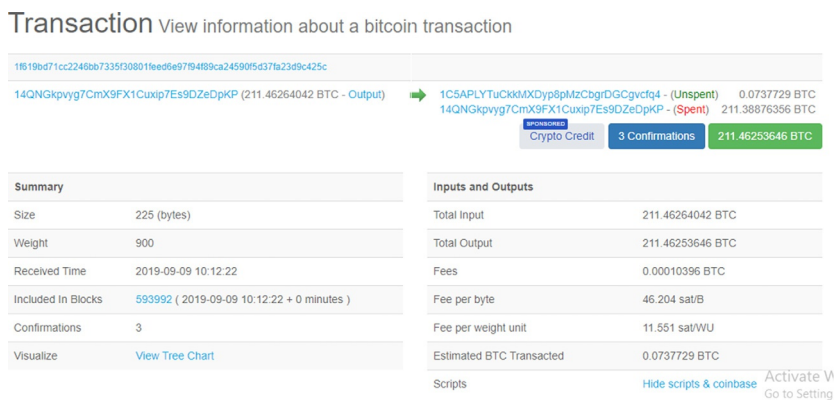

Fig. 18 Transaction history.

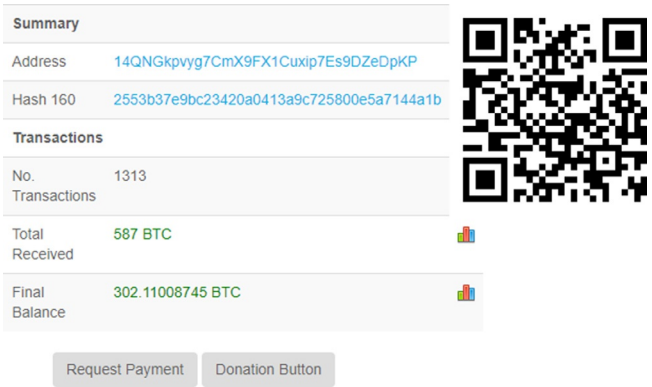

Fig. 19 The detail information of person's transaction.

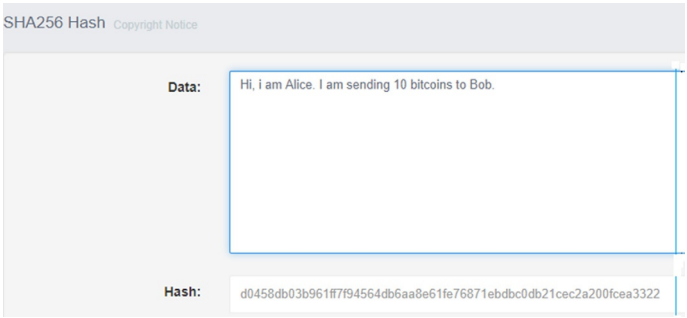

Fig. 20 Cryptographic hash function 1.

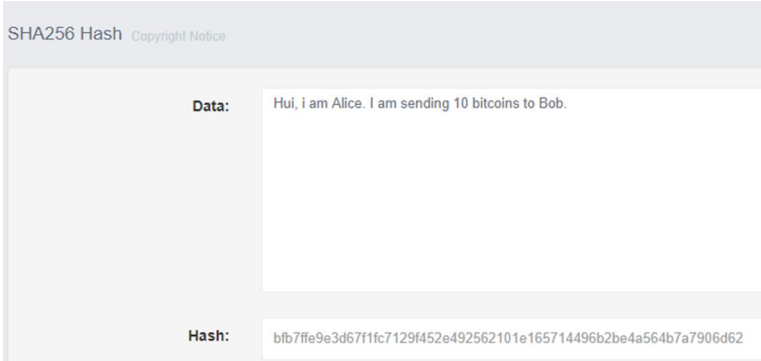

Fig. 21 Cryptographic hash function 2.

the input data that directly reflects the output value. For example, the Fig. 21 shows a small change in the letter "*Hi*" to "*Hui*" that reflects the full hash value of the output. Because of this property, it has been used in blockchain technology. In this technology, a link list is formed that contains data and a hash pointer which directs to a previous hash and creating a chain called blockchain.

6. Potential impact of blockchain

The various number of identified use cases show that the potential applications of the blockchain-based framework have been recommended for virtually all stages of the chain value [1]. Blockchain, the distributed ledger technology (DLT), continues to expand in various field of applications such as banking sector, insurance services, IoT, governance, etc. It improves privacy and confidentiality, enhances user safety, and provides a high level of care services to customers [2]. It gives Internet users the ability to authenticate digital information. It provides revolutionary change in new business applications that are described as under.

1. *Cryptocurrencies*: At present, cryptocurrency is the most important use-case in blockchain technology. Using this technology, hundreds of cryptocurrencies like bitcoin, litecoin, ethereum, etc. exist. The secured nature of smart contracts helps to make cryptocurrency transactions without the involvement of any central authority. All these transactions are authorized by blockchain network nodes. So, the increasing demand for famous cryptocurrencies will help to attract the crowd toward blockchain technology.

2. *Smart contracts*: DLT provides simple codes for smart contracts that will execute when sufficient conditions are met. At the current development level of blockchain technology, smart contracts can be programmed to perform or to develop various type of applications, functions, and programs. For this, Ethereum has been used which is an open-source blockchain project. This platform has the potential to take advantage of the usefulness of blockchain technology in a trust-less environment.
3. *Authentication/notary services*: The secured and protected nature of smart contracts in blockchain technology gives online notary services to the customers. These smart contracts can be used by people to authorize, authenticate, and accountable the other people's actions as a part of the evidence. With this technology, it is also possible to check the authentication and authorization of a document or a file.
4. *Crowdfunding*: This is the important concern in blockchain technology because the use of digital cryptocurrencies start-up companies can crowdfund or collect money from the public for their upcoming journey in an early stage [3]. For example, Kickstarter and Gofundme are companies that doing advance work for P2P economy. Regardless, decentralized autonomous organization (DAO) suggests that blockchain has the potential to guide in "*a new paradigm of economic cooperation*."
5. *Governance*: The transparent and public-accessible nature of DLT would bring full transparency in several applications like day-to-day governance operations, online voting system, hiring of personnel, providing identities, hospitality management, etc. [4]. The secured nature of smart contracts in Ethereum-based platform gives high-security by automating the process in blockchain technology. This means governance provides transparency and ensure smoothness to digital assets, equity or information.
6. *Internet-of-things*: With the generation and development of IoT, blockchain technology can be used to keep track of individual history by maintaining the record of data transmission between devices, web-services, and end-users. This technology would be useful in IoT applications as a security and privacy purpose because the transactions recorded in blockchain are secured by cryptographic primitives. So, it is very difficult for hackers to manipulate the information that exchanges between the devices and end-users.
7. *Transport sharing*: There is a classic and standard case to utilize blockchain technology for transport sharing or ride-sharing. During transport

sharing, people make payments to each other using cryptocurrencies that do not need any central authority to deal between them [5].

8. *Energy sharing*: Blockchain technology empowers the buying and selling of the renewable energy generated by microgrids. The automatic nature of Ethereum-based smart contracts redistributes the energy when solar panel makes excess amount of energy. Using these smart contracts, the microgrids can consume or contribute their energy to and from the grids easily [6]. They can make their payments in a P2P network using cryptocurrencies. For example, A "*transactive grid*," Brooklyn, working with the distribution of energy outfit called "*intelligent grid*" in an IoT functionality environment.
9. *Data storage*: The decentralized way to store and share the files using blockchain technology provides security and privacy from getting hacked or lost. Using this technology, it is possible to generate a network infrastructure that stores unalterable data at the nodes and remove duplicated files from the network. It is also used to obtain public address of network nodes for accessing storage facilities to search a file in the blockchain network.
10. *Financial services*: Blockchain technology can be applied for banking and insurance operations between the participating nodes without requiring the intervention of third-party validator. The transactions are based on the level of trust between the network nodes in a particular blockchain. The participating nodes may pay premiums in the form of cryptocurrencies and insurance policy can be concerned in the form of smart contracts. They may act as a validator or authenticator for claim. So, blockchain services can be very helpful in financial services.

References

[1] A. Kumari, R. Gupta, S. Tanwar, N. Kumar, Blockchain and AI amalgamation for energy cloud management: challenges, solutions, and future directions. J. Parallel Distrib. Comput. (2020). https://doi.org/10.1016/j.jpdc.2020.05.004.

[2] D. He, K.-K.R. Choo, N. Kumar, A. Castiglione, IEEE access special section editorial: research challenges and opportunities in security and privacy of Blockchain technologies, IEEE Access 6 (2018) 72033–72036.

[3] C. Lin, D. He, S. Zeadally, N. Kumar, K.-K.R. Choo, SecBCS: a secure and privacy-preserving blockchain-based crowdsourcing system, Sci. China Inf. Sci. 63 (3) (2020) 1–14.

[4] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, Blohost: Blockchain enabled smart tourism and hospitality management, in: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS) IEEE, 2019, pp. 1–5.

[5] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, J. Ma, Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles Ad-Hoc network, IEEE Trans. Vehicular Technol. 68 (11) (2019) 11309–11322.
[6] A. Miglani, N. Kumar, V. Chamola, S. Zeadally, Blockchain for Internet of energy management: review, solutions, and challenges. Comput. Commun. 151 (2020) 395–418, https://doi.org/10.1016/j.comcom.2020.01.014.

About the authors

Neeraj Kumar received his Ph.D. in CSE from SMVD University, Katra (Jammu and KashmirJ & K), India, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as an Associate Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, Patiala (Punjab.), India since 2014. Dr. Neeraj is an internationally renowned researcher in the areas of VANET & CPS Smart Grid & IoT Mobile Cloud computing & Big Data and Cryptography. He has published more than 150 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, and Taylor and & Francis.

Shubhani Aggarwal is pursuing Ph.D. from Thapar Institute of Engineering and & Technology (Deemed to be University), Patiala, Punjab, India. She received the B.Tech degree in Computer Science and Engineering from Punjabi University, Patiala, Punjab, India, in 2015, and the M.E. 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.