Clean Energy, 2021, 104–123

doi: 10.1093/ce/zkaa033
Homepage: https://academic.oup.com/ce

Review Article

Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: a review

Manish Kumar Thukral*

Manipal University Jaipur, Electrical Engineering Department, Jaipur, India

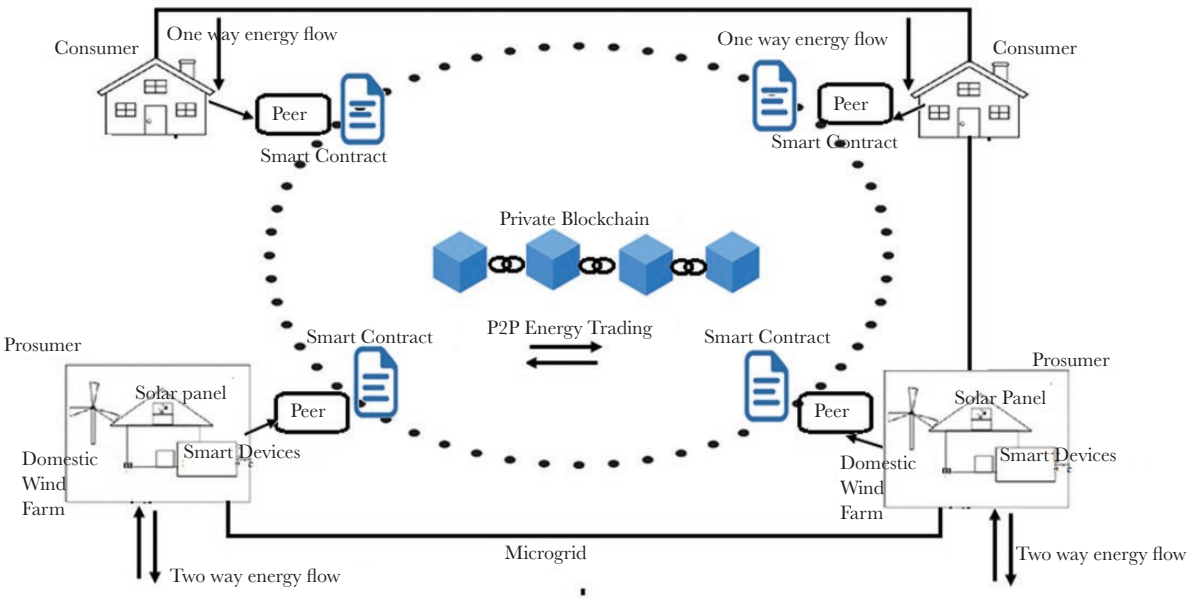
*Corresponding author. E-mail: manishkumarthukral1984@gmail.com

Abstract

Renewable-energy resources require overwhelming adoption by the common masses for safeguarding the environment from pollution. In this context, the prosumer is an important emerging concept. A prosumer in simple terms is the one who consumes as well as produces electricity and sells it either to the grid or to a neighbour. In the present scenario, peer-to-peer (P2P) energy trading is gaining momentum as a new vista of research that is viewed as a possible way for prosumers to sell energy to neighbours. Enabling P2P energy trading is the only method of making renewable-energy sources popular among the common masses. For making P2P energy trading successful, blockchain technology is sparking considerable interest among researchers. Combined with smart contracts, a blockchain provides secure tamper-proof records of transactions that are recorded in distributed ledgers that are immutable. This paper explores, using a thorough review of recently published research work, how the existing power sector is reshaping in the direction of P2P energy trading with the application of blockchain technology. Various challenges that are being faced by researchers in the implementation of blockchain technology in the energy sector are discussed. Further, this paper presents different start-ups that have emerged in the energy-sector domain that are using blockchain technology. To give insight into the application of blockchain technology in the energy sector, a case of the application of blockchain technology in P2P trading in electrical-vehicle charging is discussed. At the end, some possible areas of research in the application of blockchain technology in the energy sector are discussed.

Received: 23 August 2020; **Accepted:** 31 December 2020

Graphical Abstract



Keywords: blockchain; consensus algorithms; microgrid; peer-to-peer energy trading; distributed energy resources; electric-vehicle charging

Introduction

Non-renewable-energy resources like fossil fuels have been a prime source of fulfilling electrical-energy demand. Fossil fuels account for ~80% globally as a source of electric-energy production [1]. At the same time, conventional fossil-fuel-based energy sources are a major reason for environmental pollution and hence environmental degradation. To counter this problem, the integration of renewable-energy resources into existing energy systems is emerging as a prominent solution as far as the environmental aspect is concerned.

The advent of renewable-energy sources has brought into the picture a new class of participants that are prosumers in the electrical grid [2]. In the traditional grid, the end user had the option to be only a consumer and the flow of electric power was one-way, i.e. from utility to consumer. Now the traditional grid is changing drastically in the way in which consumers are becoming energy producers also and such consumers are termed prosumers. Prosumers are those who can consume as well as produce electrical energy. A few of the prime motives for end consumers to become prosumers are financial incentives, environmental awareness and low trust in energy suppliers [3]. With this emerged the concept of the microgrid, which integrates local renewable-energy sources and loads with the utility grid. A microgrid in the simple sense is a small-scale power system that can be controlled locally. Its major characteristic is that, besides integrating the on-site renewable-energy-generating source, it manages the balance between local load and power generation [4]. The microgrid technology is giving opportunities to prosumers to sell electricity to neighbours as well as to the grid and vice versa. The prospects of microgrids are so bright that, in future, it is possible that the traditional power-distribution system will be reshaped as interconnected autonomous microgrids. Microgrids have the capability of handling power flow in two directions, i.e. from the microgrid to the main grid and the main grid to the microgrid, to use its on-site generation most optimally. Microgrids can operate in an isolated manner that we call an islanding mode as opposed to its in-grid connected mode.

A transition from a traditional grid, which is centralized, to a decentralized grid and then to a distributed grid involving microgrids and prosumers is shown in Fig. 1 as discussed in [5]. In modern power systems, the energy flow is possible from the utility grid to the microgrid and from the microgrid to the utility grid through power-electronics interfaces like inverters.

This bidirectional flow of energy makes it feasible to buy and sell electrical energy to the utility grid. In Fig. 1, a distributed network is shown that allows energy flow between prosumers with the application of a local microgrid infrastructure. This configuration of prosumer-to-prosumer energy flow results in P2P energy trading, which has emerged as a new concept. It is defined as energy trading between prosumers, or between prosumers and consumers [6].

In [7], P2P energy trading is best summarized through Fig. 2. Here, the participants are considered prosumers with photovoltaic (PV) installations and battery-storage capacity available. It can be observed that, when the PV generation is more than the load requirement, part of the extra generation is sold to neighbours who have

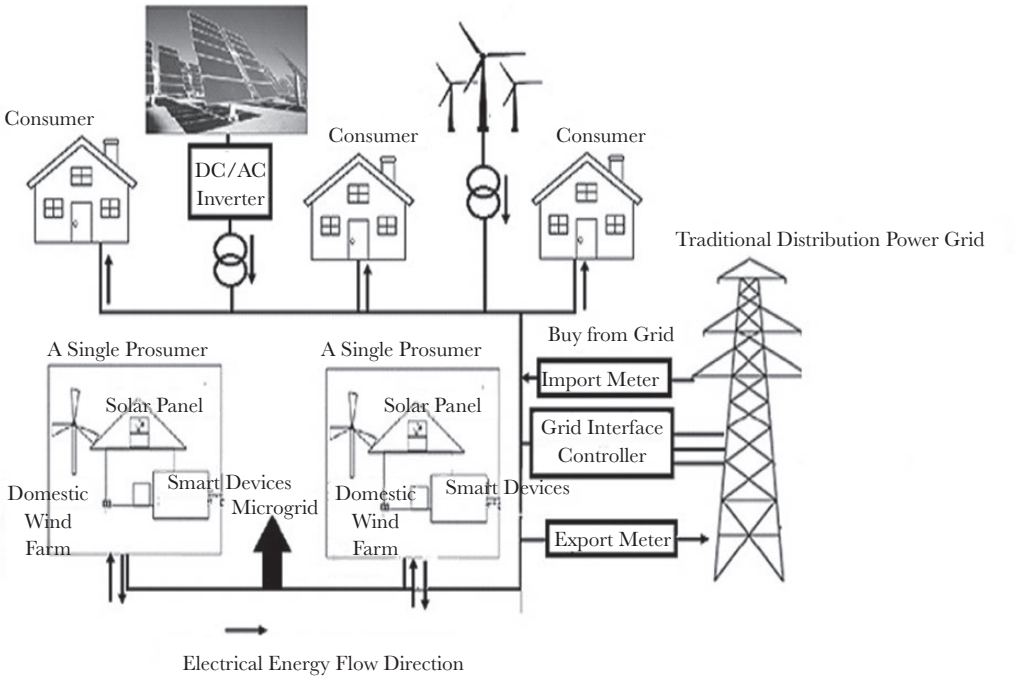


Fig. 1. Transition from central to distributed grid with a P2P network

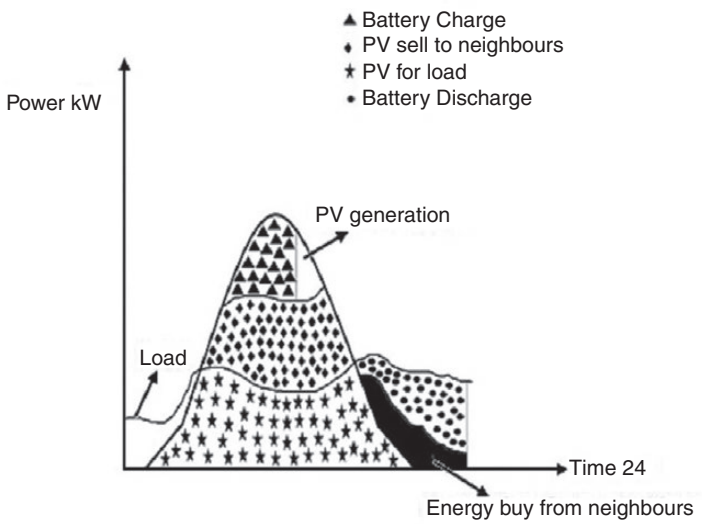


Fig. 2. P2P energy-sharing scenario

power requirements. Another part is used to charge the battery. In the evening hours when the PV generation goes below the load requirement, then part of the load requirement is filled through the battery and the rest is accomplished by buying energy from neighbours. The extra power can also be sold to the grid without any feed-in tariff scheme [8].

In energy trading in an islanding mode of the microgrid, P2P electricity cannot rely on a central authority [9]. This gives the opportunity for designing a blockchain-based energy-trading market. This has opened a gateway for end consumers to enter into local energy markets who otherwise had no option but to buy energy from a utility.

The blockchain is one of the emerging technologies in the world, as it is expected to redefine functioning and value creation in society.

A blockchain is an open distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way [10].

Major characteristics of a blockchain can be stated as follows:

- It is accessible to all, and therefore open.
- There is no central authority to maintain the ledger, which is why it is distributed among the participating parties with identical copies.

- It is scalable and quite fast in terms of transaction execution and recording, so it can be termed as efficient.
- The transactions recorded in a block are immutable, which means that they cannot be changed.

Most importantly, a blockchain allows P2P transactions in the most transparent manner and securely without involving centralized authority. One can trace the first application of this technology to Bitcoin, which is nothing but a P2P payment network that involves no central authority like banks [11].

The prime focus of the presented research work is to describe the current scenario of energy markets, the reasons why the current system does not support P2P transactions and how blockchain technology can make the P2P energy market possible. This paper is divided into various sections as follows. In Section 1, a brief description is given of blockchain technology and its various technical aspects. Section 2 gives a glimpse into the current scenario of energy markets and what are the basic requirements to set up a P2P energy market in a microgrid. How blockchain technology can be used to implement the P2P energy market in a microgrid through smart contract is explained in Section 3. Section 3 also provides details of the key challenges prevailing in blockchain technology for it to be fully applicable in the energy sector. In Section 4, the current scenario of blockchain-technology implementation in the energy sector is described. Section 5 discusses a case study of P2P energy transaction involving electrical vehicles (EVs). Finally, in Section 6, some possible future research directions in blockchain application in the energy sector are given.

1 Background of blockchain technology

Blockchain technology helps in making it possible to collaborate, coordinate and cooperate among various authoritative participants who do not trust each other to formulate a logical decision process. The way it does this is through decentralized computation and sharing information [12]. A blockchain is a decentralized, distributed public ledger that contains the transaction record. In a centralized system, there is a sole authority to coordinate whereas, in blockchain technology, there are multiple nodes, each acting as an authority, that are interconnected [13]. A blockchain is termed so because it is chain of blocks connected to each other through hash pointers. A single block contains a collection of records of transactions so, in one way, it is a ledger. One important aspect of this technology is that every node holds a copy of the ledger. It is ensured through synchronization that, when information is updated in a particular node's local copy, all other local copies are updated simultaneously. One can say that every local copy is identical.

Each block of a blockchain has two main components, i.e. a header and a body [14]. The block header comprises the block number, the hash value of the previous block, the hash value of the current block, the timestamp, the nonce and the address of the creator. The block body contains transactions. Fig. 3 shows a basic design of a block.

It can be observed from Fig. 3 that block 14 is chained to block 13 through the block hash of block number 13. The current block-hash value is calculated by finding the SHA256 cryptographic hash of the Merkle root and previous block hash used, as will be discussed below. A few basic block components are explained in the following section.

1.1 Hash

Hash functions are inevitable parts of blockchains. Hash functions are used for the encryption of data [15]. In the case of blockchains, the transactions are encrypted using hash functions. Hash functions map data of any size to a fixed data length. They are cryptographically secure because of two characteristics:

- Given data X, its hash value H(X) can be computed but, given hash value H(x), there exists no algorithm that can determine x. This is called a one-way property.
- For two different pieces of data, X_1 and X_2, their corresponding hash values $H(X_1)$ and $H(X_2)$ are entirely different, even with minute alteration. This property is also called the avalanche effect.

In the literature, X is termed as the message and H(X) is called the message digest. SHA256 is one of the commonly used hash functions in blockchain technology.

1.2 Merkle tree

The Merkle root is calculated from the Merkle tree—a concept that was introduced by Ralph Merkle in 1979

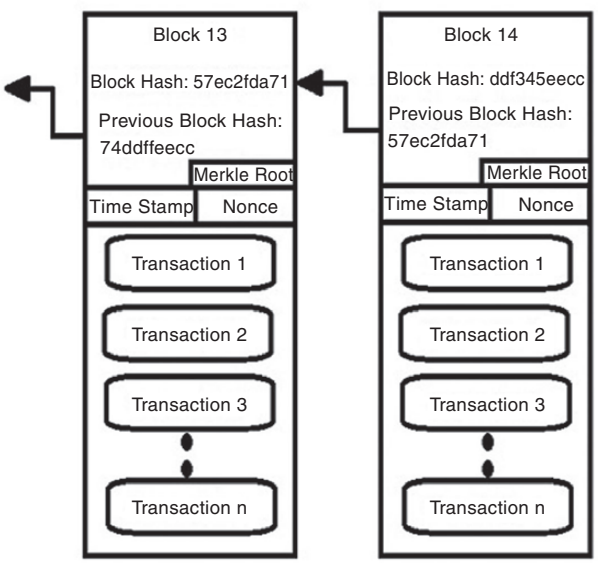


Fig. 3. Basic block design

[16]. The Merkle tree in one way is a foundational method of a block [17]. The Merkle tree can be explained by a tree-like structure, as shown in Fig. 4. In order to calculate the Merkle root, first the hash values of transactions T_1, T_2, T_3 and T_4 are calculated. These hash values are marked as leaves L_2, since the structure resembles the leaves of the tree. Then, the hash values of leaves L_2 are calculated to obtain leaves L_1 and finally the hash values H_0 and H_1 are calculated to obtain the hash root or Merkle root. The biggest advantage of the Merkle-tree structure is that, if an intruder tries to change any one of the transaction histories, then the Merkle root will change and finally the block hash will change. That will change the block hash of all the blocks. But, for successful tampering of the transaction record, the intruder is required to calculate the hash value with the difficulty level set in the blockchain and this is really computationally intensive. Since it is computationally intensive to calculate the hash values of all the blocks with a given level of difficulty, that is why we say that a blockchain provides immutable records and hence is secure.

1.3 Nonce

In a blockchain, there are certain authoritative participants who function as miners. The function of miners is to find the block hash with a certain level of difficulty. Mathematically, a miner has to solve a puzzle $H_K = \text{Hash}(H_{k-1}||T||\text{Nonce})$, where H_K is the block hash and H_{k-1} is the previous block hash, T is the Markle root and Nonce represents the random value number [18]. The nonce value is adjusted by the miner until a valid hash value is calculated for a new block being mined. For a hash value to be valid, it must satisfy the difficulty level defined by the blockchain network.

Blockchain technology is very promising to be applicable in electrical-energy marketing because of its characteristic of P2P transactions, which are secure, scalable and immutable.

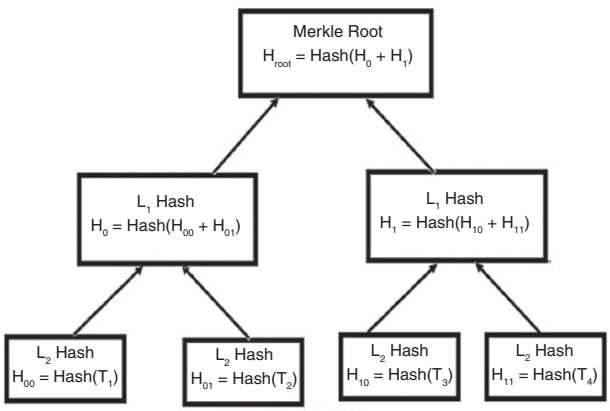


Fig. 4. Merkle tree

1.4 Types of blockchain-network architecture

A blockchain network can be of different types in terms of architecture, depending on its desired use. There are three types of blockchain architectures, i.e. permission-less, permissioned and consortium blockchains.

1.4.1 Public or permission-less blockchains

All the users who have access to the internet can join a public-blockchain network and therefore it is also named a permission-less blockchain. An apt example of a public-blockchain network is Bitcoin. In one sense, public blockchains are specific-purpose blockchains because they are mostly involved in cryptocurrency transactions. Here, there are many miners who are unknown to each other involved in the generation of blocks to solve a complex mathematical computation [19, 20].

1.4.2 Private or permissioned blockchains

As the name suggests, in this type of blockchain network, only restricted users are given access to the blockchain network. Permissioned blockchain networks, in contrast to permission-less blockchain networks, are generally in use in terms of the application domain. Such blockchain networks are implemented in a variety of domains ranging from different types of businesses and practices through the application of smart contracts. The concept of a smart contract will be discussed in a later part of the paper. The private blockchain is restricted to a single organization where members of the organization are its peers [21].

1.4.3 Consortium blockchains

In a consortium blockchain, many organizations come together and form a consortium or association. In this type of blockchain architecture, the members of any organizations who are in the consortium can read the distributed ledger, but writing in the ledger is only permitted to an authorized node in the particular organization [21, 22].

1.5 Consensus algorithms

A blockchain is primarily a distributed ledger. Each node in a blockchain maintains a copy of the ledger. So, it is of utmost importance that, in a distributed ledger, each copy of the ledger maintains a similar state of data. To achieve this, blockchain technology uses consensus algorithms. Another key aspect of consensus algorithms is that they prevent any malicious node from manipulating the data. A consensus mechanism decides how different distrusted nodes in a blockchain network come to an agreement to append a new block mined by miners [23].

1.5.1 Proof of work (PoW)

In a blockchain network, a miner collects the transactions from different nodes and validates them in the sense that the transactions are received from a valid node. Every miner constructs the block of transactions

that they receive. All the miners have a blockchain ledger copy with them. Consider that there are three miners depicted as Miner 1, Miner 2 and Miner 3, as shown in Fig. 5. All three miners are trying to mine a new block. Also, all three miners have existing updated blockchain copies with them. Miners are able to see through the existing blockchain that the last block has transactions T9, T10, T11 and T12. So, once the last block is committed to the blockchain, the miners are aware that they need not include these transactions in the new block that they are trying to mine. It is shown in Fig. 5 that Miner 1 is trying to mine a new block with transactions T13, T14, T15 and T17. It is interesting to see here that transaction T16 is missing simply because Miner 1 has not received that transaction. Similarly, Miner 2 is trying to mine a new block with transactions T13, T14 and T15 and Miner 3 is trying to mine a block with transactions T13, T14, T15 and T16. Now, all the miners are trying to mine a new block.

The term 'mining a block' was already explained in Section 1.3—it simply means solving a puzzle where a miner has to find the block-hash value H_K such that $H_K = \text{Hash}(H_K\text{-}1||T||\text{Nonce})$. So, all the miners are required to perform computational work to find the block-hash value that satisfies the nonce, which is the difficulty level set by the network. This example develops the notion of consensus, which means that a network poses a challenge to the nodes working as miners to solve the puzzle whose difficulty level is set by the network as per the nonce value. Considering this, when a miner solves the puzzle, it means that the miner has mined the block. Again, considering the example in Fig. 5, let us say that Miner 1 has mined the block first, then the miner propagates the mined block to all the nodes. When Miner 2 and Miner 3 receive the mined block from Miner 1, they stop mining the block containing the same transactions as contained in the block mined by Miner 1. Therefore, in one way, Miner 1 wins and the other two miners now start mining new blocks containing new sets of transactions. This is what we call a consensus algorithm based on which new block is added to the existing blockchain. This particular consensus algorithm, where a miner is required to solve a puzzle to mine a block, is called a PoW consensus algorithm [24–27]. It is named so because the miner must perform computationally intensive work to prove that it has mined a block. A PoW consensus algorithm is mainly used with permission-less blockchain networks.

It may happen that two miners may mine the block at the same time and this creates what we call a fork [28]. The generation of blocks can be concurrent in a blockchain because many miners are trying to mine blocks simultaneously and therefore the phenomenon of forking is inevitable [29]. To consider the forking phenomenon in a blockchain, see Fig. 6. The blockchain in Fig. 6 starts with block 1. Now, let us say that block 2 and block 3 are generated simultaneously by two miners at instance T2. So, as such, both should be accepted. Now, the miner who has generated block 2 connects it with block 1 and a miner who has generated block 3 connects it to block 1. Both miners propagate their blockchain to the network. The nodes that are receiving the blockchain view this as a fork where one chain consists of block 1 and block 2 connected together and another chain consists of block 1 and block 3 connected together. In this situation, let us say another three blocks, i.e. block 4, block 5 and block 6, are mined together by other three miners at instance T3. Now, the question arises as to which chain these miners should connect to the newly mined blocks, as both the chains are of the same length. In such a condition, where both the chains are of the same length, the miners choose the chain arbitrarily and connect their blocks as shown in Fig. 6. Now, let us say a single block 7 is mined at instant T4. Here, we have three chains that are of the same length. So, the miner who has mined block 7 can randomly choose any chain and connect block 7. In Fig. 6, it is shown that block 7 is connected to the chain consisting of block 1, block 2 and block 5. Finally, consider the instance T5 in which a single block is mined, i.e. block 8 as shown in Fig. 6. Here, as per the distributed-consensus protocol, the miner must select the longest chain to connect the mined block. Therefore, as shown in Fig. 6, it is shown that block 8 is connected to the longest chain out of the three chains available. The chains available at instance T5 are:

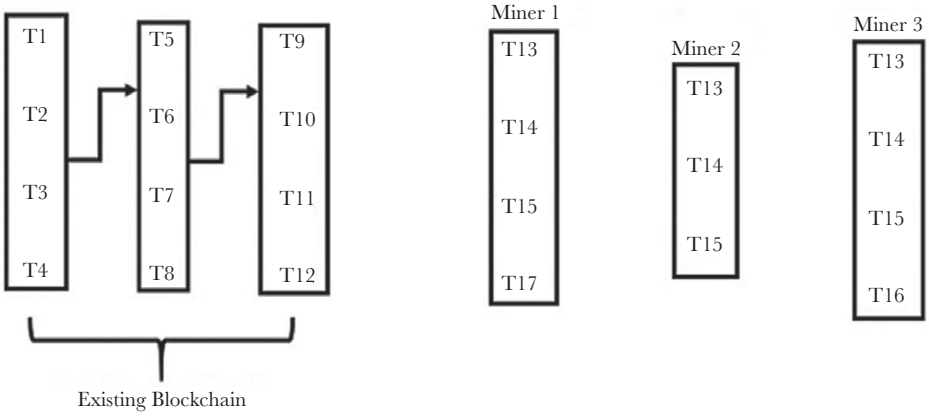


Fig. 5. Mining process

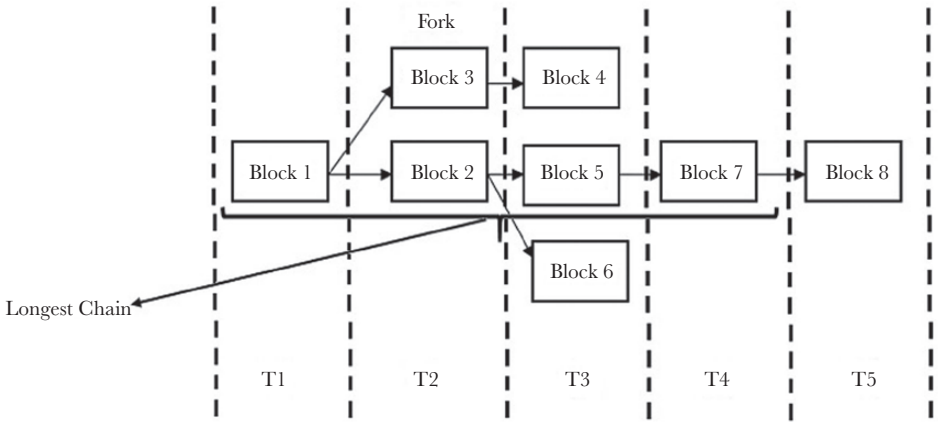


Fig. 6. Forking phenomenon

Chain 1 consisting of block 1, block 3 and block 4;
Chain 2 consisting of block 1, block 2, block 5 and block 7;
Chain 3 consisting of block 1, block 2 and block 6.

1.5.2 *Proof of stake (PoS)*

One of the main drawbacks in the PoW consensus algorithm is the high computational power required. Because of this, the transaction throughput per second (TPS) is very low. Another adverse effect of the PoW consensus algorithm is its large energy consumption [18, 30]. In the PoS consensus algorithm, the miners are required to solve the puzzle to mine the block, as in the case of PoW, but the basic difference is that, in PoS, the difficulty level is different for different miners [31]. In the case of the PoW consensus algorithm, a node having higher computational power wins and is selected for new block generation. In the case of PoS, a node is selected for a new block generation based on its stake, i.e. having higher coinage. One can understand the PoS consensus algorithm in such a way that the puzzle that a node needs to solve must fulfil the condition SHA256(timestamp, previous hash....) < target*coin [18]. This condition simply means that the SHA256 cryptographic hash of the timestamp, previous block hash, etc. generated by the node must be less than the product of the target nonce set by the network and the coins held by the node. One can observe that the larger the coin held by the node, the easier it will be to solve the puzzle, as the product will reduce the difficulty level of the puzzle. This in turn reduces the computational power required and hence saves energy also. This type of consensus algorithm is used in permissioned blockchains for increasing transaction TPS, since security is not much of an issue. This is so because participating nodes are known.

1.5.3 *Proof of capacity (PoC)*

In PoW, many nodes simultaneously solve computationally intensive puzzles to mine a block. This causes a large consumption of electrical energy in a collective manner. In the PoW algorithm, a miner keeps on changing the nonce value to find the hash value that satisfies the difficulty level set by the network. In the PoC algorithm, the participating node finds all possible solutions using a shabal algorithm well in advance and stores them in disk space to mine a block [30]. This process of storing the random solutions in disk space is called plotting. A participating node having large disk space can store a higher number of solutions and this has a better probability to mine a block. The major advantage of PoC over the PoW algorithm is that, here, the mining speed is considerably increased because the miner is having the possible solutions in advance. Another advantage is that only those nodes that have a good amount of disk space to store solutions are selected to mine the block. In this way, energy consumption is reduced as compared to PoW as a whole [30, 31].

1.5.4 *Proof of authority (PoA)*

In the PoW consensus algorithm, the nodes having a high computational infrastructure may gain a monopoly to validate the transactions for earning a large share of the profits. Also, in the case of the PoS consensus algorithm, those who can put their coin at stake have the privilege to be selected as miners. In the PoA consensus algorithm, validators are randomly selected from participating nodes in the blockchain network, as in the case of PoS. But the main difference is that the selected validators need not put either coin or storage capacity at stake to be selected as validators. The only thing that validators need to ensure is to validate the blocks honestly and gain reputation points to be selected next time. The validators with higher reputation points have a better probability of getting selected as validators and are thus incentivized for validating a block [30].

1.6 Scalability issue in blockchains

The transactions in a blockchain are required to go through a validation process. Unless a transaction is not added by a miner in a block and the valid block is not generated by the miner containing that transaction, the same is not considered valid. There is a processing fee charged in a

blockchain for validation of the transaction. Now, as the number of transactions increases, the processing fee also increases, because high computational power is needed. Bitcoin can handle three to four transactions per second with block size of only 1 MB and, on average, takes 10 minutes to mine a block [32]. Such low speed is a serious limitation for high-frequency trading applications of a blockchain. But, in the real world, the blockchain transaction capability is required to be improved so that it can handle a good number of transactions. This will help customers not to face delays in their transaction execution. Similarly, Ethereum has the capability to handle 15 transactions per second, which is again low. Scalability issues are required to be addressed if the blockchain is to be adapted in financial institutions. One solution is to increase the block size because this will help by including more transactions in a block and hence the validation speed will increase. In this context, Bitcoin cash increased its block size from 1 MB when it started to 32 MB in 2018 [32]. As the block size is increased, although more transactions can be added and mined together, this would require higher bandwidth to propagate the block. Increased numbers of users in blockchains have increased scalability problems. Two main concerns in scalability are transaction throughput and transaction-confirmation delay. Researchers have periodically had the common view that there exists a blockchain trilemma in which decentralization, security and scalability cannot exist together perfectly. It means that, when we are trying to improve security, scalability deteriorates [33].

1.6.1 IOTAs and DAGs

In order to overcome the difficulties faced in the Bitcoin blockchain related to the low throughout and intensive energy consumption involved in mining a block, mathematician Serguei Popov came up with a solution in the form of a cryptocurrency ledger named the IOTA [34]. The IOTA is based on a directed acyclic graph (DAG)-based distributed ledger known as Tangle [35, 36]. A DAG is a part of graph theory. This class of graph is named so because it is directed and acyclic. As shown in Fig. 7, DAG has vertices shown as a square and edges shown as arrows.

This graph has directions on the edges and no cycles in the graph. Here, there is no direct path from any vertex back to itself [37, 38]. In one sense, Tangle is a directed data structure based on DAG in which vertices are representations of transactions. Whenever a new transaction is issued, it is required to approve two other transactions that have never been approved by any other transactions. Referring to Fig. 7, transaction 4 is a newly issued transaction and it approves transaction 2 and transaction 3. After transaction 4 validates the other two transactions, it adds two edges. A transaction that has never been approved is called a tip. In Fig. 7, transaction 4 is a tip. This is the main difference between blockchain and Tangle technology. In the Bitcoin blockchain, miners have to solve a complicated puzzle to mine a block that consists of ~500 transactions.

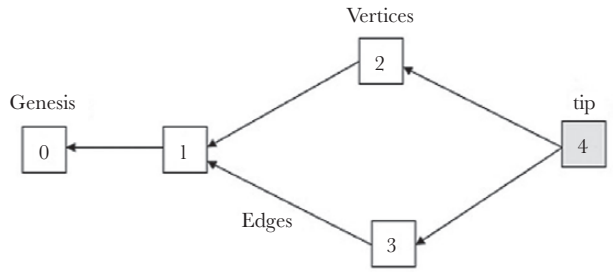


Fig. 7. Directed acyclic graph (DAG)

This process takes a lot of time and consumes a lot of power also. Eventually, a block containing a particular set of transactions is validated after a miner has mined a block and transactions get approved. In the case of Tangle, many transactions are approved simultaneously with minimum computational efforts, therefore consuming less time. Each transaction must approve two transactions by validating it through the Tangle history. In Tangle history, the approver must check the links starting from the tip to the genesis vertex. A genesis vertex is the beginning of the Tangle or DAG that contains all the tokens that are issued to the nodes participating in the transactions [34]. For example, in Fig. 7, the vertex marked as 0 is the genesis. Let us say the genesis transaction issued 20 IOTAs (cryptocurrency in the IOTA platform) at the beginning of the Tangle. Let us say that vertex 0 issued 5, 10, 3 and 2 IOTAs to vertex 1, 2, 3 and 4, respectively. So, vertex 4, which is a tip, can verify the transaction made by vertex 2 by checking the IOTAs issued by the genesis vertex to vertex 2 and other transactions made by vertex 2 through its transaction bundle. Similarly, tip 4 validates the transaction of vertex 3. Once tip 4 validates the transaction of vertex 2 and vertex 3, then it must solve a simple PoW puzzle that is nothing but a cryptographic hash of bundle hash and transaction-branch hash with a few other parameters [39]. The main aim of introducing a simple PoW solution is to avoid spam. Once the tip confirms transaction 2 and transaction 3, then tip 4 itself awaits new incoming transactions to approve it. For the sake of simplicity, only one tip is shown in Fig. 7 but, in real time, there are numerous tips. A new incoming transaction selects tips based on the Markov Chain Monte Carlo tip-selection algorithm [40].

One can easily observe from the discussion that the IOTA overcomes the low-transaction-throughput problem in Bitcoin since a number of tips approve transactions simultaneously. One interesting point to note here is that, in the case of the Bitcoin blockchain, as the number of nodes participating in issuing the transactions increases, the speed of transaction approval reduces. In the case of IOTAs, the scenario is just the opposite; here, with an increase in the number of nodes issuing new transactions, the speed of transaction validation increases. Another advantage of IOTAs is low energy consumption, as the puzzle involved in PoW here is very simple as compared to that in the Bitcoin blockchain.

1.7 Security and privacy issues in blockchains

In recent times, blockchain technology has gained interest among businesses as well the academic community, as it can provide a decentralized platform for data records that is immutable without the involvement of a centralized authority. In spite of the overwhelming response to its adoption, blockchain technology has yet to overcome various privacy and security issues. Few of the concerning issues, such as transaction linkability, blockchain wallet theft, security threats because of quantum computing, Bitcoin address tracing through P2P network traffic analysis and compliance with regulations, have been tackled in a firm manner. Researchers have started giving thought to these issues, as this causes limitations over user anonymity, confidentiality and control over his/her data. All these privacy and security issues are discussed one by one as follows.

1.7.1 *Privacy threat through transaction linkability*

It has been reported in the literature that transactions can be linked to get the user's identity through blockchain analysis. The users commit to transactions in the blockchain network by signing in through a private key. The validators use a public key to validate the authentication of the user who has signed the transaction in the blockchain. Although, in a blockchain, a user can create a number of public-key addresses, in a blockchain using transaction-graphs analysis, an intruder may know the user's identity [41]. Apart from blockchain-transaction-graph analysis, another way of leaking the privacy of the user has been reported through web cookies when users perform web payment via cryptocurrencies [42].

1.7.2 *Privacy leakage through P2P network traffic analysis*

In a blockchain, nodes communicate for transaction operation through a P2P overlay network. To hide the node or user's identity, a blockchain never stores the IP address used in the P2P overlay network. It might be possible for an intruder to do mapping of IP addresses and Bitcoin addresses through P2P IP address network analysis and using statistical analysis of aggregated transaction data [43].

1.7.3 *Theft attack on a blockchain wallet*

To perform a transaction, a user must use his private key as a digital signature. The private key in one sense authenticates the person's identity. Therefore, the security of the private key is a very important aspect of blockchain-based financial transaction systems. Often, a user has a wallet, which we call a blockchain wallet and which contains the private key and the public-key transaction-history information of a user. In one sense, the wallet is a file that stores all this information hosted by the user device [44]. But there are published works that report attacks on wallets [44, 45]. This requires urgent attention to design a secure wallet-key-management scheme.

1.7.4 *Attacks on Ethereum smart contracts*

A smart contract in the Ethereum platform has fields and functions, and is much like the JavaScript language. A detailed explanation of smart contracts is given in Section 3.1. Whenever a user calls a function in a smart contract that involves the state change of a variable, the user must pay some transaction fee to the miners and the execution fee in the form of gas. Now, a programming language like Solidity has an exception feature that is used to throw an error in case some conditions are not met in the execution of the function. The exceptions are implemented using functions like assert and require. In the case that an exception is thrown, then the execution of the function called by the user stops but, at the same time, the user must pay an execution fee.

1.7.5 *Non-erasable data in blockchains*

An overall requirement for the privacy of a system is that it should provide confidentiality and control. For confidentiality in blockchains, the data must be encrypted and this condition is fulfilled in a blockchain, as the data that are stored are always encrypted. To fulfil the second requirement of privacy, a user must have the liberty to erase any data that they may think is a threat to revealing his/her identity. This is a challenge in blockchains because a blockchain is immutable. Digital identifiers, which are considered as the personal data of a user, are written in the ledger of a blockchain. To be in compliance with the general data-protection regulation (GDPR), personal data like digital identifiers, encrypted personal data or any hashed personal data should not be stored in the chain of the blockchain network. This is one way of providing the user with the right of erasure of personal data.

1.7.6 *Quantum-computing threat to blockchains*

Quantum computing gets its name because it uses quantum phenomena like superposition and entanglement to perform computations. The computers that use quantum-computation techniques are known as quantum computers [46].

A blockchain uses one-way hash functions like SHA256 to create digital signatures, which blockchain users apply. Hash functions are also used to generate the block hash of a block that is to be mined and to link blocks of a blockchain. It is well known that, with conventional computers, it is practically impossible to calculate the reverse of a hash function. This is the reason why hash functions are known as one-way functions. But, with the advent of quantum-computing technology, it is expected that public-key cryptography algorithms like RSA (Rivest, Shamir, Adleman) [47], ECDSA (Elliptic Curve Digital Signature) [48], ECDH (Elliptic Curve Diffie-Hellman) [49] and one-way hash functions are at risk of being breakable [50]. The computing speed of quantum computing is very high as compared to that of classical computing. It is shown in [51] that an RSA algorithm can be broken using Shor's prime factorization

algorithm within a few hours, which otherwise would have taken years to break with traditional computing techniques. Researchers have also estimated that, with the use of quantum-computing-based algorithms, especially Grover's algorithm, hashes can be generated very fast and hence the blockchain can be recreated, which is again a threat to blockchain security [50].

1.7.7 Security issues in blockchain integration with constrained devices

Blockchain technology, like cloud computing, will play a big role in the implementation of the internet of things (IoT) in the future. This is so because blockchains would be able to provide data provenance, which is a vital issue in the IoT paradigm. But IoT devices have limited capabilities, such as memory, processor and battery. With these limitations, a pertinent question that will arise is how to store the crypto-key pair in IoT devices, which is a very essential aspect in blockchain transaction operations. Again, with limited processor speed and computational capabilities, how would key management protocols be executed by IoT devices [52, 53]? If these issues are not resolved, then, again, a security threat would always be there in the case of integrating constrained devices with blockchain technology.

1.7.8 Blockchain interoperability

A variety of blockchain platforms like Ethereum, Hyperledger Fabric, Corda, multichain, Ripple or Quorum are employed, depending on the requirements. One of the prime aspects of choosing a particular blockchain platform is a security requirement. There are different security requirements, such as full anonymity, which we also call zero knowledge proof; mixer services for anonymous cryptocurrency transfer, such as Zpay, Zcash, Monero, etc.; blockchain wallets on mobile devices; and capability to implement smart contracts. Such diverse requirements require different types of blockchain applications. In this context, a challenging issue is to integrate different blockchain platforms for exchanging data, exchanging software artefacts and transferring cryptocurrencies in different blockchain platforms. The main issue in blockchain interoperability is security, which should not be compromised when two different blockchains are integrated. This is because one blockchain application may have higher standards of security using mixer services and others may not have the same standards. Likewise, if we are trying to integrate a blockchain application used in electrical-energy trading with one used for IoT, then the constraint of the hardware capability of IoT devices will be a problem [54].

1.8 Impact of regulations on blockchain technology

The regulations imposed by legal authorities sometimes drive technology into an odd position. One can quote the example of the dispute between the Federal Bureau of Investigation (FBI) in the USA and Apple on encryption in 2016. This dispute started after the FBI recovered an iPhone from one of the terrorists who was shot down by police in December 2015 in San Bernardino, California. The FBI was unable to unlock the password of the iPhone. Eventually, the FBI asked Apple to come up with a new version of the iPhone operating system (iOS) in which it could be installed in the random access memory of the iPhone so that features could be weakened [55]. Apple immediately declined the order from the FBI to come up with any such software, as it was against the policy of the company. As per policy, the company was not allowed to design any software that could undermine the security features of the product. Finally, the dispute went to court. This is an apt example in which a legal authority wanted a company to change its technological features, which could adversely affect the company's product.

In this context, one can say that a regulation such as the GDPR is in direct conflict with blockchain policy. As per the GDPR guidelines, a service provider must collect only enough personal data that are sufficient for the intended purpose. As per Article 17 of the GDPR, an individual may ask for erasure of his/her personal data if its use is no longer required by a company for any processing [56]. The blocks of a blockchain contain transactional data that are personal data as per the scope of the GDPR. Article 17 of the GDPR is in direct conflict with blockchains because, in blockchains, data are immutable but the GDPR guidelines require giving liberty to the user to rectify or erase their data [57]. To erase the data from a blockchain, the chain must be broken. If a blockchain application tries to abide by this regulation, it will directly challenge the fundamental essence of blockchain technology and finally customer trust will be adversely affected.

Another conflicting regulation of the GDPR is Article 25, which requires privacy by default. As per this article, a technology must be designed such that it inherently embodies privacy characteristics. It is well known that a blockchain is transparent and tamper-proof in nature. So, anyone having access to blocks can easily document the transactions and values associated with them. Therefore, the open-to-the-public nature of blockchain pseudo-anonymous data is in direct contradiction to Article 25 of the GDPR [56].

Article 4 of the GDPR emphasizes assigning a data controller who would be responsible and accountable for implementing all technical and organizational measures for ensuring the protection of personal data [56]. Now, this article is again in direct contradiction to blockchain technology, which ensures the elimination of any third party to ensure trust management. This is a unique selling point of blockchain technology, which ensures that no third party would manage the system [56]. Obeying the GDPR regulations is essential to blockchain technology for its widespread acceptance and the energy sector is no different from it. If the conflicting points between the GDPR and blockchains persist, then this would adversely affect the aim of developing decentralized energy marketing also.

1.9 Impact of gas fees on smart-contract-based trade

In the Ethereum blockchain platform, a fee is required to be paid for every transaction made or a smart contract executed by a user. This fee to be paid by the user is known as the gas fee. The prime reason for a user to pay a gas fee is because every transaction is required to go through a process of validation and a mining process, which requires electrical-energy consumption. For this electrical-energy consumption, miners charge a gas fee. Charging a gas fee is good for preventing denial-of-service attacks in blockchain networks [58]. A gas fee is decided by miners in the network. Now, if the gas limit set in the smart contract is low, then the miners may ignore executing the smart contract or deploying the smart contract on the blockchain. Another problem is that a miner may stop executing a smart contract when the gas limit is low or the operation runs out of gas. One can understand considering an example that there is a smart contract that is to add two numbers and the gas requirement to validate the execution is 100 gas. Let us say that the sender has set a gas limit of 90 gas, i.e. the sender is ready to pay a maximum of 90 gas for the execution or validation of the smart contract to a miner. In this scenario, the miner will do computation worth 90 gas. In this case, the operation has run out of gas so the miner will charge the user 90 gas for the computation that it has performed and revert the contract to its original state [59]. The state variables of the contract will be in the original state, i.e. they will retain the same value as was there before execution. So, in this example, the user who tried to end a transaction in the form of smart-contract execution had to pay a gas fee without getting a smart contract executed because of running out of gas. Such problems will incur losses for users. This is an adverse side of charging a gas fee on the Ethereum blockchain network. Such situations would discourage participants from using the blockchain platform and encourage them to look for other platforms. Sometimes, there are situations in which a transaction to be made by a user is less than the gas fee charged by the miners. Again, such conditions would not be helpful for users to go for blockchain platforms.

2 Current scenario in the energy market

The current wholesale-electricity market on the distribution side does not support P2P electricity trading for prosumers. The reasons outlined in [8] are as follows:

- The wholesale-electricity market sets a minimum-capacity barrier to become a participant in trading. The prosumers are small-scale power-generating units and are therefore not allowed in the wholesale-power market.
- In the present scenario, the independent system operators (ISOs) collect bids from the large-scale power-generation participants and then, depending on the market-clearance price, dispatch the electricity accordingly. Now, small-scale power-generating prosumers are very large in number and managing the electricity-trading market is not feasible for the ISO.
- The wholesale-electricity market is based on the centralized structure in which participants are limited. If prosumers, who are large in number, are allowed to participate, then there is a high chance of cyberattacks in the central system. This will cause significant monetary losses.
- The prosumers are not rewarded with the money instantaneously for energy that they have sold back to the grid [60].
- The 'net-metering' approach does not permit the prosumers to sell the energy at the price that they want to and allows only a fixed reward for energy sold.

2.1 Electricity-trade models

With the advent of time, various economic sectors have seen a transition in the form of liberalization and the electricity market is no different in this respect. Earlier, there was a monopoly in electricity generation, transmission and distribution, but liberalization brought competition. This helped customers to gain an advantage in terms of the flexibility to switch over to different electricity suppliers who offered a reduced price per unit. In a broader sense, the electricity-trade model can be broadly divided into a centralized market and a decentralized market. A power pool is an example of a centralized market, which primarily includes a day-ahead market in which a uniform-price auction is used to clear the market price. A power-purchase agreement is an example of a decentralized market, in which two parties can independently enter into a contract for electricity trading. Nowadays, a new emerging electricity-trade model is the coalition formation in which various distributed energy resources form a coalition and enter an electricity-trading mechanism. A brief discussion of these models is given below.

2.1.1 Coalition formation for electricity-market trading

In the coalition form of trading model, different distributed energy resources such as solar power planta, wind power planta, combined heat and power, energy-storage systems and flexible loads act as a single entity or form a coalition and participate in an electrical-energy market. A virtual power plant (VPP) energy-management system with the help of information and communication technology represents this coalition for participating in electricity marketing through an auction process. These virtual power plants are also called microgrid aggregators. Financial power-purchase agreements, future contracts and day-ahead markets are a few ways through which the VPP can participate in electricity trading by placing bids. In the VPP model, a manager is appointed who carefully examines the distributed energy resources, technical capacities and bids of other VPPs, and then forms the coalition to make a bid. Every member of the

coalition announces their minimum bid to the VPP manager and the VPP manager accordingly formulates the coalition bid. The minimum coalition bid decided by the VPP manager is the highest minimum bid announced by the coalition members. After a particular VPP wins, then a contract is signed between the VPP manager and the coalition members to supply the amount of power bid for the given time duration [61].

2.1.2 *Power-purchase agreement*

A power-purchase agreement is a bilateral contract in which there is a negotiation between two parties (load and power suppliers like VPPs) directly to exchange power. Such a contract is laid under a certain set of conditions such as the time of power supply and the duration, price, and MW amount. The power-purchase agreement is of two types: future and forwarded contracts. In future contracts, the supplier and the load trade in an exchange and are not bound to the agreement. Both parties can continuously trade until the delivery time of the power. In a forward contract, the load and the power supplier like a VPP negotiate directly without going to a power-exchange market and they agree upon the price, the amount of power delivery and the time of delivery, which remains fixed until the delivery time [62].

2.1.3 *Day-ahead electricity market*

The buyer sets the quantity needed for the next day and this might be made up of 5-minute intervals. The buyer is usually a grid-management agency. These agencies have a forecast of the power needed in each 5-minute block for the next 24 hours. These agencies accept the bids for a certain amount of power at certain prices from different generating units for each of these 5-minute increments throughout the day. These bids will be done regionally, as there are transmission constraints. The bids from sellers contain the amount of electricity and price. Based on a uniform-price auction, the market is cleared.

2.1.4 *Uniform-price sealed-bid auction*

Day-ahead electricity markets use uniform-price sealed-bid auctions. In this auction method, the auctioneer collects the sealed bids from the electricity supplier and electricity buyers for each period as decided in the day-ahead market (it can be 5- or 15-minute intervals). The sealed bid from the supplier and the buyer side contains the amount of electricity, minimum price sought, time of delivery and duration. After collecting the sealed bids, the auctioneer plots the cumulative-supply and cumulative-demand curves, as shown in Fig. 8. In the cumulative-supply curve, the auctioneer sorts the bids from low to high. Similarly, the auctioneer sorts the bids from high to low in the case of the cumulative-demand curve. After this, both the curves are drawn on a single graph and the point of intersection of the two curves is obtained, as shown in Fig. 9, which is marked as the market-clearing price (MCP). This point of

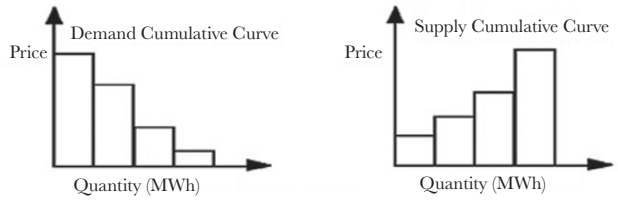


Fig. 8. Demand and supply cumulative curve

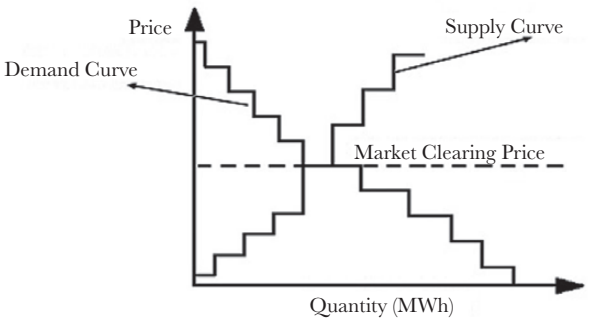


Fig. 9. Uniform-price sealed-bid auction

intersection is also known as a market-equilibrium point because, at this point, the power supply equals the power demand. Now, the auctioneer will clear all the supply-side bids that are less than this MCP and similarly all demand-side bids are cleared that are equal to or higher than the MCP. This auction scheme is called 'uniform-price' simply because all the sellers who have bid for a price lower than the market-clearing price will be paid a uniformly equal amount, which is nothing but the MCP [63].

2.1.5 *Comparison*

A bilateral contract has the advantage that an electricity supplier fixes the price of the power to be sold to the customer in a forward-contract scheme. Because of this, the supplier may avoid the risk of price fluctuation that exists in a real-time market. But the disadvantage is that the grid balance is adversely affected in such a scenario. In the case of a pool market under a day-ahead scheme, the grid balancing is better as compared to that in a bilateral contract, but the price-fluctuation risk is always there with the supplier. In real-time electricity markets, grid balancing is better as compared to forward bilateral contracts and day-ahead markets [64].

2.2 Basic requirements to set up P2P-based energy markets

It is necessary to understand the basic requirements for setting up a microgrid P2P energy market, which is well explained in [65]. Their requirements are categorized into seven components:

- *Microgrid set-up:* In order to design a feasible P2P microgrid market, there has to be a sufficient number of interested participants who want to trade energy. Out

of these, there should be prosumers who may have renewable generation capacity such as PV-based. While setting up a microgrid system, it should be decided whether the traditional grid will be used for energy exchange or whether a separate transmission line will be installed.

- *Grid connection:* The microgrid must have the capability to work in islanding mode or in synchronization with a traditional grid. To achieve synchronization, a microgrid must have a common point of coupling with the traditional grid, which is maintained at the same level of voltage as the main grid. This would help the local prosumers to sell the energy not only to peers, but also to the main grid when in surplus or to buy from the grid when in deficiency.
- *Information system:* An efficient information and communication technology is required for all the participants to get the real-time energy-pricing information so that they can have a fair platform on which to buy or sell energy. This is a very vital component and, if not given due attention, then microgrid energy trading will collapse.
- *Market mechanism:* This component focuses on what would be the energy-bidding modus operandi in the case of the P2P energy market. This must be clearly laid down before making microgrid energy marketing operational.
- *Pricing mechanism:* For a profitable microgrid energy market, the pricing mechanism must be such that, when the energy generation is surplus, this should lower the energy price and, when in deficiency, the pricing must increase.
- *Energy-management trading system:* This part of the microgrid energy market collects the real-time demand and supply of its market participants and accordingly plans for bidding for the energy.
- *Regulations:* Traditional electricity regulations do not allow P2P electricity trading. Therefore, while setting up microgrid energy trading, it will be necessary to plan how consensus can be reached on a common platform with the existing regulations.

3 Blockchains as a possible solution for setting up P2P electricity trading

Blockchain technology has proven to be proficient for P2P transactions in terms of security, transparency and the immutable recording of transactions. This characteristic of blockchain technology makes it a fit candidate to for implementing P2P trading in the electricity market.

The problems stated in Section 2 can easily be solved using blockchain-based P2P electricity trading that would provide distributed-ledger technology. Blockchains can provide scalability to many participants, and security and safety from cyberattacks, as no central server is involved. P2P energy trading mostly faces double-spending attack, data integrity, denial-of-service (DOS) attack and privacy attack as the main cybersecurity issues [66].

Blockchain-based P2P energy-trading systems are safe from double spending. In a double-spending attack, a user can spend a digital asset more than once. Because of consensus algorithms like PoW, a double-spending attack is prevented in blockchains.

The data-diddling attack is a serious issue in cybersecurity in P2P energy trading where an attacker can compromise data integrity and can alter the data. A blockchain, because of its immutable ledger by virtue of cryptographically hashed block linkage, is safe from attack on the data integrity [67].

In P2P energy trading, the participating prosumers and consumers are required to communicate with each other for negotiating energy prices and payment transactions. Such a scenario invites intruders for DOS attack to puncture the P2P energy-trading communication by blocking availability. Blockchain technology inherently provides safety from DOS attacks. This is so because users must pay a gas fee for every transaction. So, any intruder trying to launch a DOS attack will have to pay a huge amount of gas fees [68]. Apart from that, each transaction undergoes validation before being executed, which provides a second layer of protection from DOS attack.

Privacy attacks on P2P energy trading have been a serious concern. This is because the participants are required to frequently make transactions for buying and selling energy. This process would reveal the identity of prosumers or consumers on a conventional digital platform, which they may not want. In blockchain technology, cryptographic public keys are the means to identify users and not names or other identifications. This provides anonymity to the users and therefore privacy [69].

Energy trading on the distribution side is an active research area. In this direction, work has been reported in which different business models for P2P electricity trading have been proposed [65]. One business model includes collective pricing from the seller and buyer using a blockchain platform [65].

One important fact to be considered is that a blockchain set-up requires paying the miners' fees for performing PoW that participants must bear. Despite the operating cost involved in using blockchain technology, still it is lower than the charges to be paid to brokers and agents [70]. Although blockchain technology is envisaged as a promising solution for the successful implementation of P2P energy trading, there are several issues that are required to be addressed.

The basic application of blockchain technology in energy trading in a P2P system is to record the following as a transaction in blocks [71]:

- energy generated by prosumers;
- bid price asked by the prosumers;
- energy demand raised by the consumer or prosumer and maximum price at which they want to buy.

All these data are transmitted by smart meters with a time interval of usually 15 minutes. This gives a fair platform on which prosumers and consumers can trade electricity without intermediate agents. The load profile, PV-generation status and battery-charge status are maintained through the smart meter. The smart meter, which is blockchain-enabled, uses this status for the buying and selling of electric energy from neighbours as per the blockchain framework and the execution of smart contracts embedded in the smart meters. Therefore, to implement blockchain technology for a P2P energy market in a microgrid, smart meters would be indispensable, as they would have smart contracts embedded in them and they will transmit the data, as already mentioned. In this context, it is very important to understand smart contracts.

3.1 Smart contracts

The term 'smart contract' was first coined by a cryptographer in 1996 named Nick Szabo [72]. As such, the first application of blockchain technology was Bitcoin but, by using smart contracts, the blockchain application can be further extended to solve other types of real-world problems. A smart contract is a computer program that implements real-world contractual agreements between two parties. A smart contract is realized with the help of a programming language like Solidity. It includes an execution condition and logics for a business application. These execution conditions are automatically executed when a transaction is made by a client and if the transaction meets the conditions [72]. Once a smart contract is executed, then only the data are written in the blockchain. A copy of the smart contract, which is immutable, remains with each peer [73]. Most of the permissioned blockchains use smart contracts. In a permissioned blockchain, the participants are already known, unlike in a permission-less blockchain such as Bitcoin, in which anyone can participate [74].

Smart contracts have advantages as follows:

- Smart contracts facilitate the transaction of assets other than value or cryptocurrency.
- Smart contracts allow specification of rules for the operation of the blockchain.
- A smart contract facilitates the implementation of policies for transfer of assets in the decentralized network.
- A smart contract also adds programmability and intelligence to the blockchain.

In terms of P2P energy marketing, each peer would have a smart contract in the smart meter implemented in its renewable-energy-generation infrastructure. The smart contracts would execute the transactions and transfer the energy between peers based on contract conditions. In a nutshell, to implement P2P energy marketing, there must be smart contracts enabled by smart meters.

Ethereum Remix Integrated Development Environment (IDE) is one of the platforms on which to design, code, deploy and execute smart contracts. This platform is open-source and available on a web interface [75]. One snapshot of this platform is shown in Fig. 10, where a simple, smart-contract code is shown for the addition of two numbers. One thing that should be noted is that the Ethereum Remix IDE platform updates from time to time, so the snapshot shown in Fig. 10 may not be the same as would be seen by the reader later on.

3.2 Challenges for blockchain-technology implementation in the energy sector

Blockchain technology is still in an initial stage and it will take some time for it to mature. In this context, there are still many hurdles that must be resolved for the successful implementation of blockchain technology in the energy sector. In [5], such possible challenges are grouped into five categories, which are as follows:

- *Technical challenges:* PoW is considered as the first consensus algorithm to be used in blockchain technology. Due to the high computational requirement for mining a block, this algorithm demands high electricity expenditure. One of the major advantages of a microgrid is that the local renewable sources supply the majority of their electricity generated to the local loads. This helps in reducing the power loss that is incurred in long-distance transmission. But this advantage is lost when a PoW consensus algorithm-based energy market is designed for the microgrid, as this algorithm requires high electrical-power consumption for performing computations. Another important technical issue is the speed of transaction execution, which, in the case of an existing blockchain-implementation platform like Ethereum, is ~12–30 transactions per second [76]. This limitation is a hindrance towards increasing the scalability of a P2P network.
- *Economical challenges:* As of now, the regulations do not allow P2P electricity trading and hence the market mechanism for such a case does not exist. Therefore, this would require new market rules and mechanisms [77]. Designing smart contracts that integrate consumers, prosumers and the utility grid requires a new thinking process, as the energy market for P2P trading would be dynamic.
- *Social challenges:* The willingness of prosumers and consumers to participate in the blockchain network for P2P energy trading is an important issue because the blockchain is a new technology and is yet to mature. Thus, building confidence among stakeholders in adopting this new technology is a very important issue [78].
- *Environmental challenges:* One of the prime objectives of P2P energy trading fuelled by blockchain technology is to reduce environmental pollution because of fossil-fuel-based generation. Also, global warming is a serious issue, as it is adversely affecting environmental health. Encouraging energy procurement among consumers

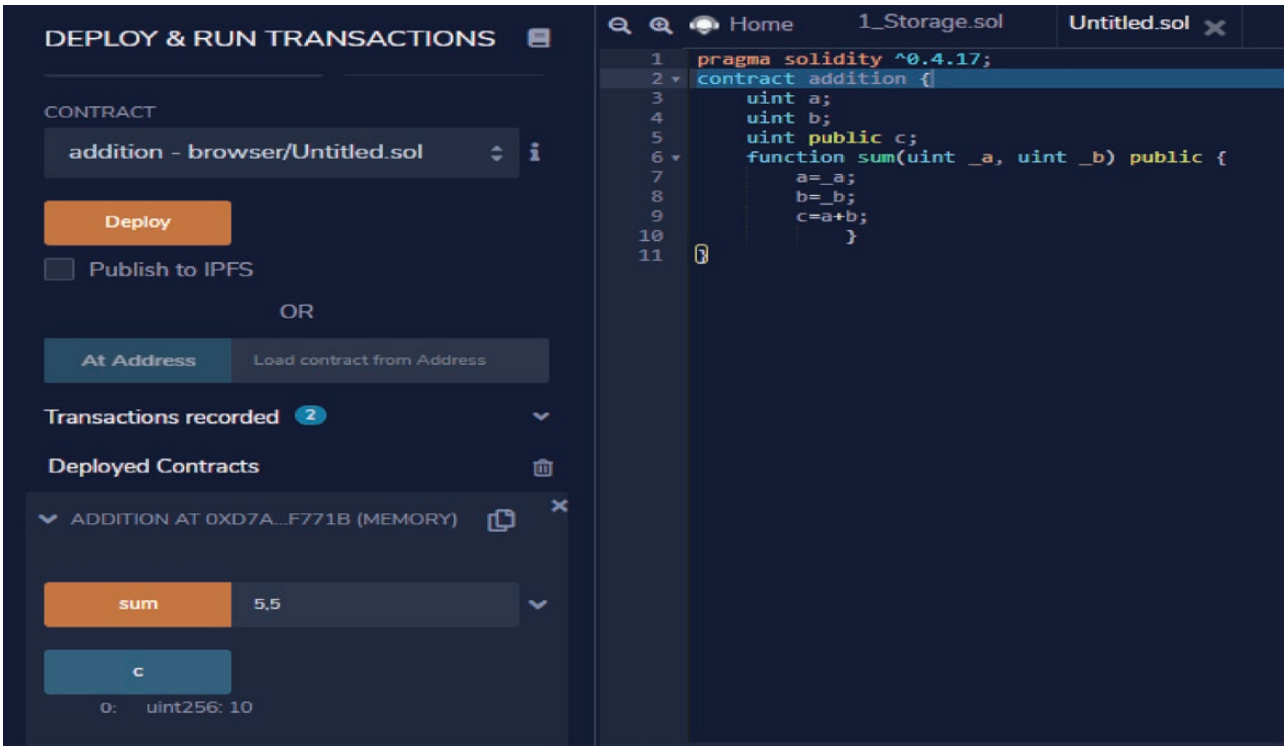


Fig. 10. Remix Integrated Development Environment

from renewable-energy-resources-based generation, even at a higher price than from the grid, may be a challenging task. For this, consumers need to be educated on the environmental effects and positive impacts of renewable-energy resources [79].

- *Institutional challenges:* The existing electricity regulations in most countries do not have a provision for allowing P2P electricity trading. In this direction, it will be required to amend the laws to accommodate P2P energy trading [80].

4 Present status of blockchain-technology application in the electrical-energy sector

Decentralized energy trading is one of the major areas that are being strengthened by blockchain technology [81]. Other areas very much relevant to the energy sector include metering, billing and security, grid management and e-mobility, which are next to energy marketing [81]. To put more emphasis on blockchain-technology application in the electrical-energy sector, various application areas of the electrical-energy sector using this technology are discussed below.

4.1 Blockchain-based P2P energy trading in microgrids

In [82], an energy-trading platform is proposed based on a consortium blockchain. The prosumers and consumers use energy-storage devices for the exchange of energy. In the event of energy exchange as trading conditions are met, ERC20 tokens are generated and exchanged as trading currency using smart contracts employed in the private blockchain.

In [67], a decentralized energy-trading architecture for smart grids is developed. One of the prime missions of a smart grid is to engage the distributed energy-generation resources into energy trading. In the present scenario, financial infrastructure renders account management, payments relating to different processes and security to third parties. This is a centralized mechanism in which a third party holds the entire data related to accounts and transactions. The existing smart grid is no different from this mechanism when it comes to providing energy-trading architecture to distributed energy generators and this is what we call centralized energy trading [67]. A centralized-energy-trading system can suffer from a single-point failure, which hinders the entire process of energy trading. This may be because of a cyberattack or other type of physical-infrastructure failure. To counter this problem, a decentralized energy-trading system called PriWatt was developed in [67] using blockchain technology. The transactions are stored in a decentralized manner in different nodes, which can be prosumers or consumers in the blockchain.

4.2 Blockchain-based real-time implementation of a demand–response event

Using blockchain-based smart contracts, demand–response events in real time are implemented in [83]. With the introduction of information and communication technology

(ICT), the traditional power grid is transforming into a smart grid. In a smart grid, unlike in a traditional power system, there is two-way communication between consumers and power generators. One of the burning issues in smart grids is the participation of consumers in a demand–response programme. It is no longer possible for centralized authorities for grid management since the introduction of distributed energy prosumers. Using blockchain-based smart contracts, it is possible to implement real-time demand–response events [83]. Hence, real-time demand–response implementation has emerged as a very important application for blockchains in the energy sector.

4.3 Blockchains for implementing an optimal power flow (OPF) algorithm

In [84], a bilateral trading mechanism is developed in a microgrid in which the physical constraints are respected using an OPF. The OPF problem is solved using alternating-direction methods of a multiplied algorithm (ADMM). Here, blockchain technology is used for solving part of the ADMM algorithm through smart contracts and exchanging information between different nodes that are prosumers.

4.4 Blockchains for implementing ancillary services in a microgrid

Another important application for blockchain technology that has come into picture in recent times is to provide ancillary services to the grid. Ancillary services are the operations required in the grid apart from electricity generation and transmission to maintain the grid stability [85]. Ancillary services are of different types, such as the injection of reactive and real power, frequency control, voltage control, etc. In the context of these renewable-energy sources (RESs) such as solar and wind, power-generation sources can be used as ancillary service providers [86]. In [86], it is reported that RESs are being used as ancillary service providers for frequency regulation, as conventional sources have a lower ramp-up time. Likewise, energy-storage devices can provide ancillary services [87]. In this direction, work has been reported in [88] in which a blockchain platform has been used to incentivize the PV generators who provide ancillary services in terms of voltage regulation.

4.5 Blockchain-enabled safe operation of a power-distribution network having EV load

Advancement of EV technology has provided a promising solution to counter environmental pollution. At the same time, it is expected that the huge penetration of the EV-charging load will pose a serious threat to power-system distribution-network operations if the load distribution among charging stations is not done in a justified manner. In this direction, work has been reported in [89] in which a blockchain-based fair EV-charging load distribution is done among charging stations such that the distribution network operates to permissible limits. Apart from this, a blockchain is used for implementing double-auction mechanisms to help the charging station to get maximum incentives under the limited charging rights.

4.6 Companies and investments involved

Blockchain technology is gaining momentum in terms of its application in the power sector such that, around the world, as many as 189 companies are involved in this direction [90]. The investments are huge from companies seeing the prospects of this technology. Leading blockchain companies have invested ~466 million USD [90]. Most of the companies in this technology started during 2016–18 and this is the sign of the early stage of this technology. One interesting fact is that Germany, the Netherlands and the USA are three leading countries working on this technology. Some of the companies that have invested in blockchain-based energy-sector applications are shown in Supplementary Table 1 (see the online Supplementary Data).

4.7 Blockchain platforms used in the electrical-energy sector

In [81], it is reported that ~50% of the total blockchain-based electrical-energy start-ups are using the Ethereum platform to design blockchain-based solutions, followed by Hyperledger fabric, Tendermint, Interbit and other platforms. Similarly, 55% of the total blockchain-use cases in the energy sector are using PoW consensus algorithms followed by PoA, PoC and others.

5 Case of blockchain-application use in the EV-charging energy market

The EV is projected to be an integral component of the intelligent grid in the future [91–93]. It is projected that, by connecting EVs with blockchain technology, the most optimal charging opportunities can be given to customers [91]. In this direction, a blockchain protocol has been designed in [94], in which an EV sends its charging signals to a blockchain. Various charging stations are connected in the form of a blockchain consortium. The protocol proposed in [91] consists of the following steps:

- The EV places its charging request, identifying itself with a unique id β generated by a public-key infrastructure. The charging request includes a unique id β, the amount of energy required e, the time frame T within which energy is required and finally the geographical region R. The charging-request parameters {β,e,T,R} are placed in the blockchain. Since all the charging stations are connected in the blockchain consortium, the charging request is visible to all the charging stations.

- In response to the charging-request signal from the EV, the charging stations send their offers in the form of four parameters {i,R,T,B), where i is the address id of the charging station, R is the region in which the charging station is located, T is the time frame offered by the charging station in which the vehicle will be charged and B is the bidding offer. The offers from different charging stations are placed in the blockchain and hence are visible to all the charging stations. In this way, the charging stations keep updating their charging offers to win the bid.
- The bid offers placed on the blockchain are accessible to the EV. The EV can select the most appropriate bid offer in terms of the lowest bid with the minimum time frame required for charging along with the nearest charging station. Once the EV decides on the best suitable charging station, then it sends a hashed commitment H(β,i,r), where r is the random number. This hashed commitment, which is placed on the blockchain, is visible to all but, since it is hashed, the decision taken by the EV is not revealed.
- Finally, the EV reaches the charging station selected. The charging station asks for the parameters β, i and r from the EV, calculates its hash and then compares the hashed commitment obtained from the one placed in the blockchain.

In [94], a trivial method of an EV-charging protocol has been designed using blockchain technology. But, in real practice, the stress on the power grid must be taken into consideration while designing the blockchain protocol, as the penetration of EVs into the grid can cause voltage instability and hence added operational cost. In this direction, a blockchain-based EV-charging scheme has been proposed in [95] in which minimization of power-fluctuation level P_{PFL} has also been taken into account so as to maintain voltage stability. The objective function considered in [95] is:

$$\min P_{PFL} \tag{1}$$

where,

$$P_{PFL} = \sum_{t=1}^{T} ||P_{total}(t) - P_{total}(t-1)|| \tag{2}$$

In Equation (2), $P_{total}(t)$ is the total power demand at hour t and $P_{total}(t-1)$ is the total power demand at $t-1$ hours. The total power demand is given as:

$$P_{total}(t) = P_{residential}(t) + P_{EV}(t) \tag{3}$$

where $P_{total}(t)$ is the total load, $P_{residential}(t)$ is the load of the home without considering the load of the EV and $P_{EV}(t)$ is the EV load. The total load demand is subjected to the condition that it should be less than the substation power capacity P_{sub} after the addition of the transmission losses $\zeta(t)$, as shown in Equation (4):

$$P_{total}(t) + \zeta(t) \leq P_{sub} \tag{4}$$

Also, while satisfying the Equation (4) condition, the bus-voltages level $V(t)$ must be between the minimum value V_{min} and maximum value V_{max}, as shown in Equation (5):

$$V_{min} \leq V(t) \leq V_{max} \tag{5}$$

The EV power demand in Equation (3) $P_{EV}(t)$ in the span of 24 hours T for given number I of EVs connected in the grid is given as:

$$\sum_{t=1}^{T} P_{EV}(t) = \sum_{t=1}^{T} \sum_{i+1}^{I} (SOC_{exp}(i) \pm SOC_{ini}(i)) \tag{6}$$

In Equation (6), $SOC_{exp}(i)$ is the expected state of charge by the i^{th} EV and $SOC_{ini}(i)$ is the initial state of charge of the i^{th} EV. While fulfilling the objective function (1), it is to be kept in mind that the expected state of charge must not exceed the maximum capacity P_{max} of the battery, as given by the following equation:

$$SOC_{exp} \leq P_{max} \tag{7}$$

So, first, by using the blockchain protocol, the power demand of EVs is recorded in the blockchain and the matching bids. Later, using the data collected from the blockchain, a suitable optimization technique is applied to fulfil the objective in Equation (1) subject to the conditions of Equations (4), (5) and (7). If the conditions are met, then the orders are finalized or else the orders are not met and the next bid is floated by the bidders.

6 Open areas of research

A few of the open areas of research in which blockchains can be applied in the energy sector are as follows:

- Designing a computationally efficient consensus algorithm that requires less electrical-energy consumption and has good execution speed in terms of transactions per second.
- Designing a new P2P electricity-marketing framework that is supported by blockchain technology.
- Designing smart contracts for P2P trading that also take into consideration environmental laws and targets that would be new in their own way.
- Designing an intercountry system of renewable-based electricity trading involving prosumers or small-scale generating entities using blockchain technologies.
- In renewable-energy resources such as solar or wind generation, whenever excess energy is generated relative to the load requirement, a common practice is to curtail the generation. This is done because the grid balance between demand and supply has to be maintained. This is a wasted energy-generation opportunity. To avoid the curtailing of generation, a smart contract can be designed and deployed in smart meters to divert excess energy generated by solar or wind to energy-storage devices. Similarly, the smart contract should divert the energy from storage devices to consumers whenever there is a deficiency in generation.
- Many companies such as Sun Exchange or ImpactPPA are involved in financing renewable-energy resources. But the outcome is not visible, which is required

to check the impact on climate change. For this, a crowdfunding system based on blockchains can be designed for financing the renewable-energy resources in potential areas. This would accelerate the deployment of renewable-energy resources and hence the generation of green energy.
- Designing a blockchain platform to collect the data from smart meters and storing them for load forecasting, energy management, etc.
- Dynamic demand-side management using blockchain technology.

7 Conclusion

The presented research work is an attempt to address the issue of P2P energy-market implementation with the help of blockchain technology. A thorough review of various published work has been done to analyse the current scenario prevailing in the energy market and how blockchain technology can be used in this direction. Blockchain technology is in its nascent stage of development, but the expectation is very high and therefore this paper also outlines the limitations of blockchain technology in its present state.

Blockchain technology has gained significant momentum in recent times because of the number of industries that are investing in it. In this direction, some initiatives taken by different industries are reviewed. At the end, some of the possible research directions are also discussed.

It is expected that the presented work will encourage readers to pursue research work in the application of blockchains in the energy sector.

Supplementary data

Supplementary data is available at *Clean Energy* online.

Conflict of Interest

None declared.

References

[1] Noor S, Yang W, Guo M, *et al*. Energy demand side management within micro-grid networks enhanced by blockchain. *Applied Energy*, 2018, 228:1385–1398.

[2] Wang S, Taha AF, Wang J, *et al*. Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019, 49:1612–1623.

[3] Hirsch A, Parag Y, Guerrero J. Microgrids: a review of technologies, key drivers, and outstanding issues. *Renewable and Sustainable Energy Reviews*, 2018, 90:402–411.

[4] Li Z, Bahramirad S, Paaso A, *et al*. Blockchain for decentralized transactive energy management system in networked microgrids. *The Electricity Journal*, 2019, 32:58–72.

[5] Ahl A, Yarime M, Tanaka K, *et al*. Review of blockchain-based distributed energy: implications for institutional development. *Renewable and Sustainable Energy Reviews*, 2019, 107:200–211.

[6] Peck ME, Wagman D. Energy trading for fun and profit buy your neighbour's rooftop solar power or sell your own-it'll all be on a blockchain. *IEEE Spectrum*, 2017, 54:56–61.

[7] Long C, Wu J, Zhou Y, *et al*. Peer-to-peer energy sharing through a two-stage aggregated battery control in a community microgrid. *Applied Energy*, 2018, 226:261–276.

[8] Luo F, Dong ZY, Liang G, *et al*. A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain. *IEEE Transactions on Power Systems*, 2018, 34:4097–4108.

[9] Sanseverino ER, Di Silvestre ML, Gallo P, *et al*. The blockchain in microgrids for transacting energy and attributing losses. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, England, 21 June 2017, 925–930.

[10] Iansiti M, Lakhani KR. The truth about blockchain. *Harvard Business Review*, 2017, 95:118–127.

[11] Feld S, Schönfeld M, Werner M. Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective. *Procedia Computer Science*, 2014, 32:1121–1126.

[12] Wattenhofer R. *The Science of the Blockchain*. 1st edn. California: CreateSpace Independent Publishing Platform, 2016.

[13] Mohanta BK, Jena D, Panda SS, *et al*. Blockchain technology: a survey on applications and security privacy challenges. *Internet of Things*, 2019, 8:100–107.

[14] Pal O, Alam B, Thakur V, *et al*. Key management for blockchain technology. *ICT Express*, 2019, 1:1–5.

[15] Menezes AJ, Van Oorschot PC, Vanstone SA. *Handbook of Applied Cryptography*. 1st edn. Boca Raton: CRC press, 1997.

[16] Chen YC, Chou YP, Chou YC. An image authentication scheme using Merkle tree mechanisms. *Future Internet*, 2019, 11:1–18.

[17] Xu J, Wei L, Zhang Y, *et al*. Dynamic fully homomorphic encryption-based Merkle tree for lightweight streaming authenticated data structures. *Journal of Network and Computer Applications*, 2018, 107:113–124.

[18] Zhang S, Lee JH. Analysis of the main consensus protocols of blockchain. *ICT Express*, 2020, 6:93–97.

[19] Helliar CV, Crawford L, Rocca L, *et al*. Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, 2020, 54:1–15.

[20] Carvalho A. A permissioned blockchain-based implementation of LMSR prediction markets. *Decision Support Systems*, 2020, 130:1–50.

[21] Zhang R, Xue R, Liu L. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 2019, 52:1–34.

[22] Yuen TH. PAChain: private, authenticated & auditable consortium blockchain and its implementation. *Future Generation Computer Systems*, 2020, 112:913–929.

[23] Gao S, Yu T, Zhu J, *et al*. T-PBFT: an EigenTrust-based practical Byzantine fault tolerance consensus algorithm. *China Communications*, 2019, 16:111–123.

[24] Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics*, 2019, 36:55–81.

[25] Kumar G, Saha R, Rai MK. Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. *IEEE Internet of Things Journal*, 2019, 6:6835–6842.

[26] Hölbl M, Kompara M, Kamišalić A, *et al*. A systematic review of the use of blockchain in healthcare. *Symmetry*, 2018, 10:1–22.
[27] Knirsch F, Unterweger A, Engel D. Implementing a blockchain from scratch: why, how, and what we learned. *EURASIP Journal on Information Security*, 2019, 2:1–14.
[28] Ghosh A, Gupta S, Dua A, *et al*. Security of cryptocurrencies in blockchain technology: state-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, 2020, 163:1–35.
[29] Reyna A, Martín C, Chen J, *et al*. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 2018, 88:173–190.
[30] Cao B, Zhang Z, Feng D, *et al*. Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digital Communications and Networks*, 2020, 1:1–6.
[31] Nguyen CT, Hoang DT, Nguyen DN, *et al*. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access*, 2019, 7:85727–85745.
[32] Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 2016, 18:2084–2123.
[33] The blockchain trilemma. Medium. https://medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3 (10 October 2020, date last accessed).
[34] Silvano WF, Marcelino R. Iota tangle: a cryptocurrency to communicate Internet of Things data. *Future Generation Computer Systems*, 2020, 112:307–319.
[35] Brogan J, Baskaran I, Ramachandran N. Authenticating health activity data using distributed ledger technologies. *Computational and Structural Biotechnology Journal*, 2018, 16:257–266.
[36] Son B, Lee J, Jang H. A scalable IoT protocol via an efficient DAG-based distributed ledger consensus. *Sustainability*, 2020, 12:1–11.
[37] Kotilevets ID, Ivanova IA, Romanov IO, *et al*. Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions. *IFAC-PapersOnLine*, 2018, 51:693–696.
[38] Divya M, Biradar NB. IOTA-next generation block chain. *International Journal of Engineering and Computer Science*, 2018, 7:23823–23826.
[39] Zichichi M, Ferretti S, D'Angelo G. A framework based on distributed ledger technologies for data management and services in intelligent transportation systems. *IEEE Access*, 2020, 8:100384–100402.
[40] Ferraro P, Shorten R, King C. On the stability of unverified transactions in a DAG-based distributed ledger. *IEEE Transactions on Automatic Control*, 2019, 65:3772–3783.
[41] Motamed AP, Bahrak B. Quantitative analysis of cryptocurrencies transaction graph. *Applied Network Science*, 2019, 4:1–21.
[42] Live Bitcoin News. Cookies, Online Trackers and the Blockchain - You Privacy is at Risk Part 1. https://www.livebitcoinnews.com/cookies-online-trackers-blockchain-privacy-risk-part-1/ (10 October 2020, date last accessed).
[43] Koshy D. *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*. 1st edn. *M.S. thesis*. University Park, Pennsylvania: The Pennsylvania State University, 2013.
[44] He S, Wu Q, Luo X, *et al*. A social-network-based cryptocurrency wallet-management scheme. *IEEE Access*, 2018, 6:7654–7663.
[45] Er-Rajy L, El Kiram My A, El Ghazouani MO, *et al*. Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures. *Journal of Internet Banking and Commerce*, 2017, 22:1–29.
[46] Gyongyosi L, Imre S. A survey on quantum computing technology. *Computer Science Review*, 2019, 31:51–71.
[47] Boneh D, Durfee G. Cryptanalysis of RSA with private key d less than N/sup 0.292. *IEEE Transactions on Information Theory*, 2000, 46:1339–1349.
[48] Caelli WJ, Dawson EP, Rea SA. PKI, elliptic curve cryptography, and digital signatures. *Computers & Security*, 1999, 18:47–66.
[49] Kumar M, Iqbal A, Kumar P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. *Signal Processing*, 2016, 125:187–202.
[50] Fernández-Caramès TM, Fraga-Lamas P. Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, 2020, 8:21091–21116.
[51] Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 1999, 41:303–332.
[52] Reyna A, Martín C, Chen J, *et al*. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 2018, 88:173–190.
[53] Salimitari M, Chatterjee M, Fallah YP. A Survey on consensus methods in blockchain for resource-constrained IoT networks. *Internet of Things*, 2020, 11:1–19.
[54] The Challenges of Blockchain Interoperability. PrimaFelicitas. https://www.primafelicitas.com/the-challenges-of-blockchain-interoperability/#:~:text=What%20is%20Blockchain%20Interoperability%3F,make%20cross%2Dchain%20transactions%20seamlessly (8 October 2020, date last accessed).
[55] Hack M. The implications of Apple's battle with the FBI. *Network Security*, 2016, 2016:8–10.
[56] De Hert P, Papakonstantinou V, Malgieri G, *et al*. The right to data portability in the GDPR: towards user-centric interoperability of digital services. *Computer Law & Security Review*, 2018, 34:193–203.
[57] Truong NB, Sun K, Lee GM, *et al*. Gdpr-compliant personal data management: a blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, 2019, 15:1746–1761.
[58] Gas(Ethereum). Investopedia. https://www.investopedia.com/terms/g/gas-Ethereum.asp (5 October 2020, date last accessed).
[59] Blockgeeks. What is Ethereum Gas?. https://blockgeeks.com/guides/Ethereum-gas/ (9 October 2020, date last accessed).
[60] Cali U, Fifield A. Towards the decentralized revolution in energy systems using blockchain technology. *International Journal of Smart Grid and Clean Energy*, 2019, 8:245–256.
[61] Jafari M, Foroud AA. A medium/long-term auction-based coalition-forming model for a virtual power plant based on stochastic programming. *International Journal of Electrical Power & Energy Systems*, 2020, 118:1–16.
[62] El Khatib S, Galiana FD. Negotiating bilateral contracts in electricity markets. *IEEE Transactions on Power Systems*, 2007, 22:553–562.
[63] Shah D, Chatterjee S. A comprehensive review on day-ahead electricity market and important features of world's major electric power exchanges. *International Transactions on Electrical Energy Systems*, 2020, 1:1–39.
[64] Barroso LA, Cavalcanti TH, Giesbertz P, *et al*. Classification of electricity market models worldwide. In: International Symposium CIGRE/IEEE PES, 2005, New Orleans, USA, 5–7 October 2005, 9–13.

[65] Mengelkamp E, Gärttner J, Rock K, *et al*. Designing microgrid energy markets: a case study: the Brooklyn Microgrid. *Applied Energy,* 2018, 210:870–880.
[66] Yahaya AS, Javaid N, Alzahrani FA, *et al*. Blockchain based sustainable local energy trading considering home energy management and demurrage mechanism. *Sustainability,* 2020, 12:1–28.
[67] Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing,* 2016, 15:840–852.
[68] Singh R, Tanwar S, Sharma TP. Utilization of blockchain for mitigating the distributed denial of service attacks. *Security and Privacy,* 2020, 3:1–13.
[69] Abdella J, Shuaib K. Peer to peer distributed energy trading in smart grids: a survey. *Energies,* 2018, 11:1–22.
[70] Dang C, Zhang J, Kwong CP, *et al*. Demand side load management for big industrial energy users under blockchain-based peer-to-peer electricity market. *IEEE Transactions on Smart Grid,* 2019, 10:6426–6435.
[71] Musleh AS, Yao G, Muyeen SM. Blockchain applications in smart grid–review and frameworks. *IEEE Access,* 2019, 7:86746–86757.
[72] Lu Y. The blockchain: state-of-the-art and research challenges. *Journal of Industrial Information Integration,* 2019, 15:80–90.
[73] Yu L, Tsai WT, Li G, *et al*. Smart-contract execution with concurrent block building. In: 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE) 2017, San Francisco, USA, 6–7 April 2017, 160–167.
[74] Zheng Z, Xie S, Dai H, *et al*. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress), Honolulu, USA, 25–30 June 2017, 557–564.
[75] Remix-Ethereum IDE. https://remix.Ethereum.org (26 September 2020, date last accessed).
[76] Ethereum Watch. Any truth to EOS investor claim that the blockchain now handles 5000 transactions per second? https://Ethereum.medianewsonline.com/2018/07/24/any-truth-to-eos-investor-claim-that-the-blockchain-now-handles-5000-transactions-per-second/ (26 September 2020, date last accessed).
[77] Zhou Y, Wu J, Long C. Evaluation of peer-to-peer energy sharing mechanisms based on a multiagent simulation framework. *Applied Energy,* 2018, 222:993–1022.
[78] Long Y, Wang Y, Pan C. Incentive mechanism of micro-grid project development. *Sustainability,* 2018, 10:163.
[79] Khaqqi KN, Sikorski JJ, Hadinoto K, *et al*. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Applied Energy,* 2018, 209:8–19.
[80] Green J, Newman P. Citizen utilities: the emerging power paradigm. *Energy Policy,* 2017, 105:283–293.
[81] Andoni M, Robu V, Flynn D, *et al*. Blockchain technology in the energy sector: a systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews,* 2019, 100:143–174.
[82] Pee SJ, Kang ES, Song JG, *et al*. Blockchain based smart energy trading platform using smart contract. In: 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Okinawa, Japan, 11–13 February 2019, 322–325.
[83] Pop C, Cioara T, Antal M, *et al*. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors,* 2018, 18: 1–22.
[84] van Leeuwen G, AlSkaif T, Gibescu M, *et al*. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. *Applied Energy,* 2020, 263:1–13.
[85] Kumar A, Meena NK, Singh AR, *et al*. Strategic integration of battery energy storage systems with the provision of distributed ancillary services in active distribution systems. *Applied Energy,* 2019, 253:1–16.
[86] Banshwar A, Sharma NK, Sood YR, *et al*. Renewable energy sources as a new participant in ancillary service markets. *Energy Strategy Reviews,* 2017, 18:106–120.
[87] Opathella C, Elkasrawy A, Mohamed AA, *et al*. Optimal scheduling of merchant-owned energy storage systems with multiple ancillary services. *IEEE Open Access Journal of Power and Energy,* 2019, 7:31–40.
[88] Di Silvestre ML, Gallo P, Ippolito MG, *et al*. Ancillary services in the energy blockchain for microgrids. *IEEE Transactions on Industry Applications,* 2019, 55:7310–7319.
[89] Jin R, Zhang X, Wang Z, *et al*. Blockchain-enabled charging right trading among EV charging stations. *Energies,* 2019, 12:1–22.
[90] IRENA. *Innovation landscape brief: Blockchain*. Abu Dhabi: International Renewable Energy Agency, 2019. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Sep/IRENA_Blockchain_2019.pdf?la=en&hash=FAE6EBFE616C1F0511BEAA6F2B8ABCDE44209C1F (3 October 2020, date last accessed).
[91] Mwasilu F, Justo JJ, Kim EK, *et al*. Electric vehicles and smart grid interaction: a review on vehicle to grid and renewable energy sources integration. *Renewable and Sustainable Energy Review,* 2014, 34:501–516.
[92] Thukral MK. Design and Simulink implementation of electrical vehicle charging using wireless power transfer technology. In: Optical and Wireless Technologies 2020, Jaipur, India, 16–17 March 2019, 631–640.
[93] Tripathi RS, Thukral MK. Switching angles computation of multi-level inverter for electrical vehicle application. In: 2019 Global Conference for Advancement in Technology (GCAT), Bangalore, India, 18–19 October 2019, 1–5.
[94] Knirsch F, Unterweger A, Engel D. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Computer Science-Research and Development,* 2018, 33:71–79.
[95] Liu C, Chai KK, Zhang X, *et al*. Adaptive blockchain-based electric vehicle participation scheme in smart grid platform. *IEEE Access,* 2018, 6:25657–25665.