By Mohammad Shahidehpour, Mingyu Yan, Pandey Shikhar, Shay Bahramirad, and Aleksi Paaso

Blockchain for Peer-to-Peer Transactive Energy Trading in Networked Microgrids

©SHUTTERSTOCK/LUCKYSTEP

Providing an effective and decentralized strategy.

Digital Object Identifier 10.1109/MELE.2020.3026444
Date of current version: 30 November 2020

RENEWABLE ENERGY RESOURCES ARE KEY components of the sustainable social development that has been rapidly deployed in recent years. The proliferation of renewable energy resources promotes socioeconomic development in various parts of the world, and islandable

2325-5897/20©2020IEEE

microgrids (MGs) play an increasingly important role in such development. MGs represent a viable alternative to conventional bulk power transmission for addressing the vulnerabilities of long-distance power delivery from centralized generation units to distributed customer sites. A controllable MG equipped with on-site distributed energy resources (DERs), which could include distributed generators, energy storage, and economic demand responses, cultivates local resources to enhance the reliability, resilience, sustainability, security, and economics of local power systems.

The proliferation of DERs in power distribution systems also brings about operational challenges for distribution system operators (DSOs). Peer-to-peer (P2P) transactive energy trading, which allows networked MGs located in a community to trade flexible energy with each other, is regarded as an effective method to boost DER utilization. P2P transactive energy trading allows networked MGs to serve local utilities as controllable loads and provides a reliable means of accommodating variable DERs dispersed at various locations in a regional power distribution system.

The introduction of P2P transactive energy in a power distribution system allows for the decentralized and active operation of the local power system, thus benefitting from local, economically viable, environmentally sound, and abundant generation systems. Accordingly, decentralized management methods are required in the power system operation and control to accommodate decentralized P2P strategies. Blockchain provides an effective and decentralized strategy that can address the operational challenges introduced by the P2P transactive energy trading. Blockchain provides an immutable and distributed ledger to allow automatic P2P transactions among blockchain network participants that are independent of a central authority. The decentralized nature of blockchain provides a transparent and trustworthy environment for network participants to directly interact with each other and carry out P2P transactions in a secure manner. The introduction of blockchain to P2P transactive energy trading can increase the power system operation efficiency, reduce operational costs, and provide an automatic energy trading process for participating MGs.

This article proposes the use of blockchain technology in P2P transactive energy trading for delivering a secure and efficient level of distributed power generation in a networked MG. The proposed solution can address operational threats caused by the hosting of many DERs in active power distribution systems.

P2P Transactive Energy Trading Among Networked MGs

MGs, which can be operated in grid-connected or islanded mode, interconnect local DERs and are expected to play an important role in modern power distribution systems. MGs, which serve as controllable loads, can exchange energy and ancillary services to improve the sustainability, reliability, and resilience of the power distribution system operation and help reduce additional investments on distribution network upgrades.

Figure 1(a) and (b) illustrates the conventional and P2P transactive energy markets in the power distribution system for MG trading, respectively. In Figure 1(a), the MGs can exchange energy only with the DSO at a clearing energy price in a conventional market. For instance, the DSO can purchase surplus energy from one MG and sell it to other MGs. The clearing price for trading energy with the DSO may not incentivize MGs to utilize local DERs and apply a demand response. In Figure 1(b), P2P transactive energy trading allows MGs to communicate and exchange energy with each other at dynamic prices, which could differ from the market clearing price offered by the DSO. In P2P transactive energy trading, MGs determine their trading partners based on the market price and other criteria that reflect their specific objective values. For instance, certain MGs might prefer to exchange only clean energy, even if the exchange price is higher than that of market clearing. Here, the DSO is in charge only of the distribution network management. The DSO optimizes the network reconfiguration by switching the distribution lines to realize P2P transactive energy flows among participating MGs. Furthermore, the DSO provides instructions to MGs to adjust their energy trading strategies if energy trading results violate the distribution network security. For privacy concerns, each MG is treated as an equivalent load in the energy trading results provided to the DSO.

P2P transactive energy trading offers valuable solutions to address the technological and socioeconomic challenges in power distribution systems. One of the prime applications of the P2P transactive energy trading market will be in networked MGs in which participating MGs with various energy production and consumption profiles will cooperate based on the market signals for providing energy services in a power distribution network. Such cooperative energy trading alternatives will incentivize networked MGs to make full use of the local energy production to provide affordable energy prices for their respective customers. The application of P2P transactive energy trading allows MGs to better value local DERs since self-generating MGs will gain higher economic benefits from their DER investments. The DER investments in networked MGs will enhance the utilization of the renewable energy power distribution systems and promote sustainable development using P2P transactive energy trading markets. In addition, the P2P transactive energy market will promote the use of demand response when variable DERs cannot

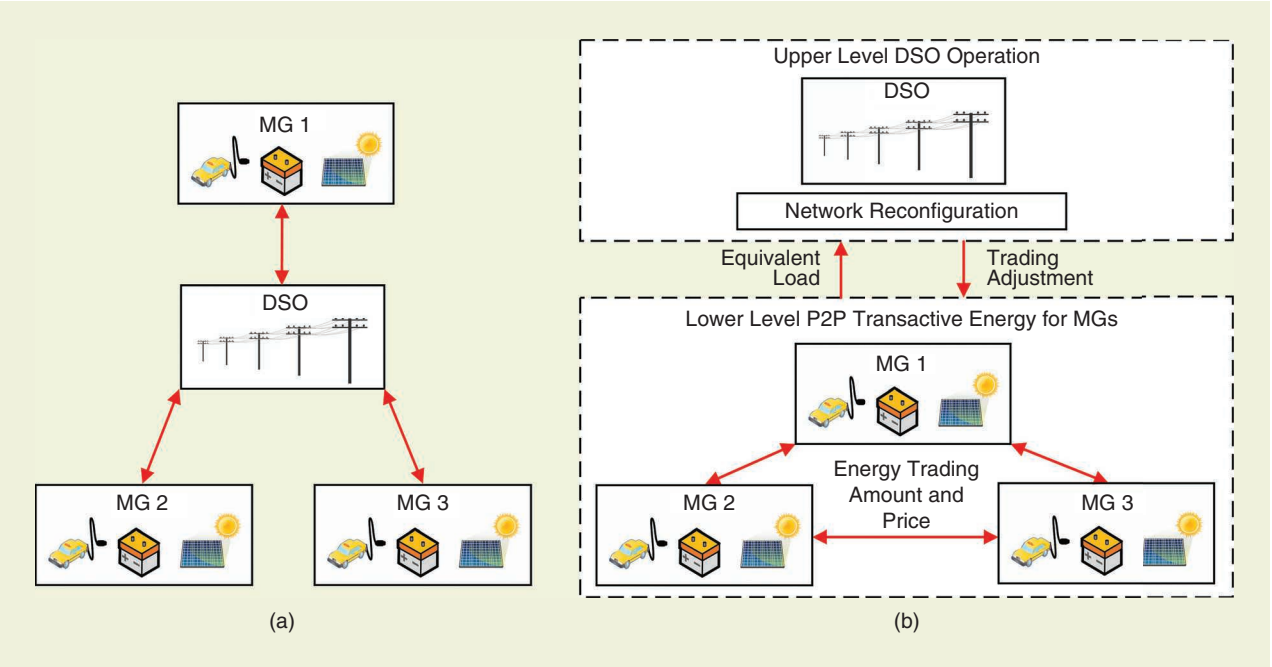

Figure 1. The conventional and P2P transactive energy trading in electricity markets. (a) The conventional market. (b) P2P transactive energy trading.

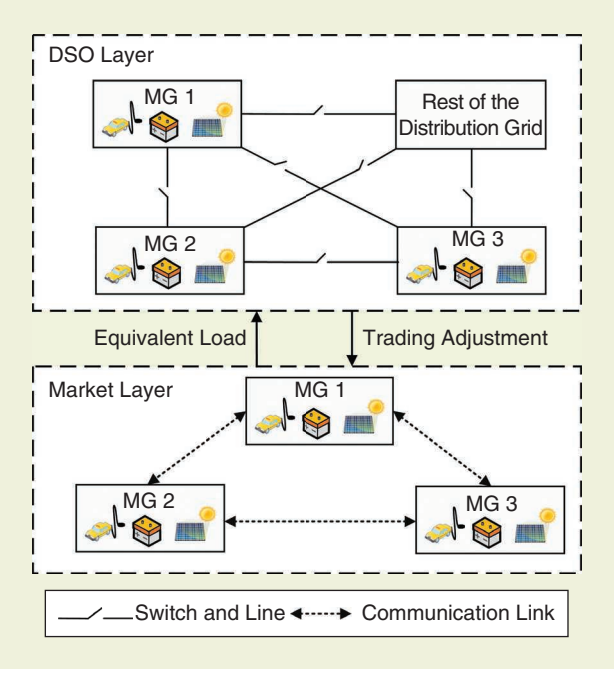

Figure 2. A sample of P2P transactive energy trading.

balance local loads and external power is expensive. MGs can adjust the use of noncritical loads to maintain the local power balance at the lowest cost in the P2P transactive energy market.

Figure 2 depicts the market and the network layers of the proposed P2P model in a power distribution network. MGs trade energy at the market layer in which the DSO is not involved since the DSO will not intervene in the P2P energy trading among MGs. In the P2P market model, the DSO serves as a nonprofit authority with the responsibility of narrowing the gap between the wholesale and retail markets for participating MGs. At the DSO layer, the DSO optimizes the network configuration for reasons pertaining to economics (e.g., reducing network losses) and network security (e.g., mitigating voltage violations and line congestions) by remotely controlling the line switches to adapt the power distribution network topology. In addition, the DSO, which is connected to the transmission grid, will participate in the bulk power market to make up the difference between MG power generation and consumption in the power distribution network.

Blockchain For P2P Trading

Introduction to Blockchain

Blockchain, which was first utilized in Bitcoin, is a decentralized, immutable, and shared digital ledger for recording transactions. Figure 3 compares a conventional centralized ledger without blockchain and a decentralized ledger with the introduction of blockchain. In Figure 3(a), the ledger is controlled only by one centralized authority (e.g., a bank or an enterprise), and participants will submit transactions to the central authority for any exchanges among participants. The submitted transactions will be executed after the central authority approves and records the submitted transactions on the ledger. In practice, the introduction of a central authority increases the intermediary costs, and it might occasionally be difficult to find a trusted central authority. A blockchain is a shared database that provides a secure and effective environment for decentralized data management. The introduction of a blockchain removes

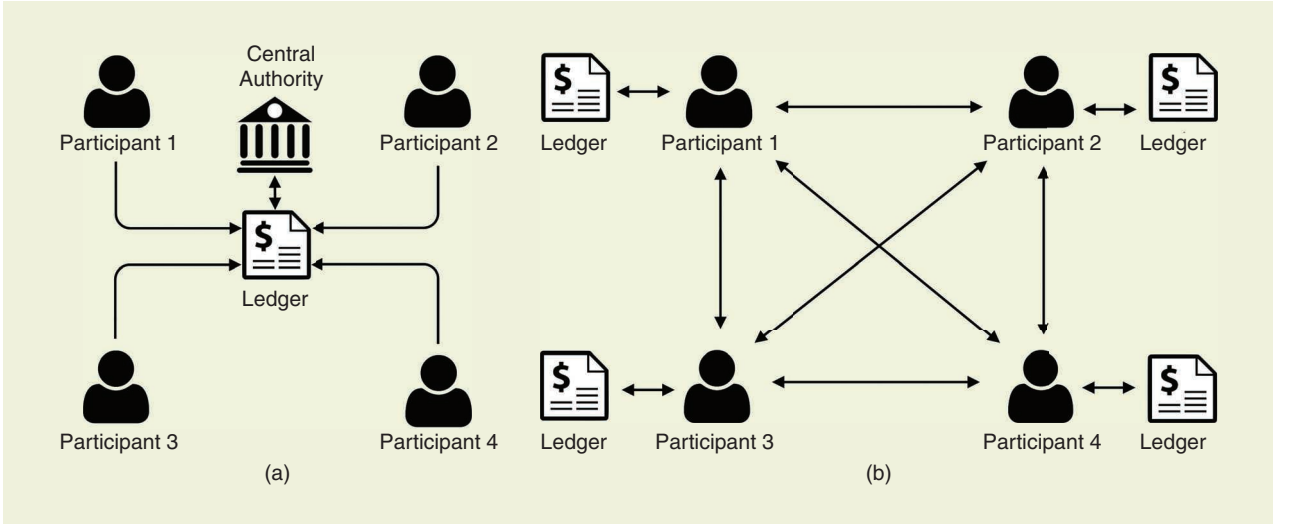

Figure 3. A comparison of a (a) conventional centralized ledger and (b) decentralized ledger.

the need for a central authority. In Figure 3(b), each participant in the blockchain network holds an individual ledger for recording each transaction, which is also sent to the other participants' ledgers for validation.

On existing transactive platforms where blockchain technologies provide a trustworthy environment for all, participants may not be able to directly participate in the P2P transactive energy trading market due to physical constraints (e.g., power flow limits) and the cybersecurity requirements of the power distribution networks. Therefore, existing blockchain technologies should be adapted to be applicable to P2P transactive energy trading for providing efficient and reliable electricity services for participating MGs. Before we discuss blockchain applications to P2P transactive energy trading, we introduce a few common technologies that are utilized in existing blockchain applications.

Hash Function

A hash function is a type of cryptographic function that can map data of an arbitrary size to a fixed length of letters and numbers. The outputs (i.e., a fixed length for letters and numbers) provided by a hash function are defined as hash values. A hash function includes the following attributes: 1) it is complex and does not produce the same hash value for two different inputs and 2) it guarantees that the hash value is significantly changed even if the input data are changed slightly. An example of a hash function is demonstrated in Figure 4 to illustrate how a hash function converts the message into a fixed length of letters and numbers. Here, the lengths of the outputs are the same regardless of the lengths of the inputs. The hash function is widely used in data storage. The hash function characteristics help create vast storage savings, increase the efficiency of the system with a large sum of data, and ensure data security. Since any changes to the input data will change the hash value, any malicious attack to revise the data can be easily flagged by reviewing the hash value.

Merkle Tree

The data of each block are stored in a Merkle tree. Merkle trees use hash functions for efficient and secure storage and the verification of a large body of data. The Merkle tree structure helps verify the consistency and content of the data. Figure 5 shows the structure of a Merkle tree and how a Merkle tree works. Assume that the four transactions A, B, C, and D are recorded using a Merkle tree. These transactions are first encrypted using hash functions to form hashes A through D. Then, hash A and hash B are combined and encrypted into hash E. Finally, hash G is obtained, which is labeled as a Merkle root. The data stored in a Merkel tree can be easily tracked by referring to the hash value in the Merkle root. Since any change to the data stored in a Merkle tree will change the hash value in a Merkle root, any malicious attack to revise the Merkle tree data can be easily flagged by detecting the hash value in the Merkle root.

Asymmetric Cryptography

The blockchain network allows two participants to trade trustfully. Accordingly, the authentication and privacy of each message in a blockchain should be guaranteed. The

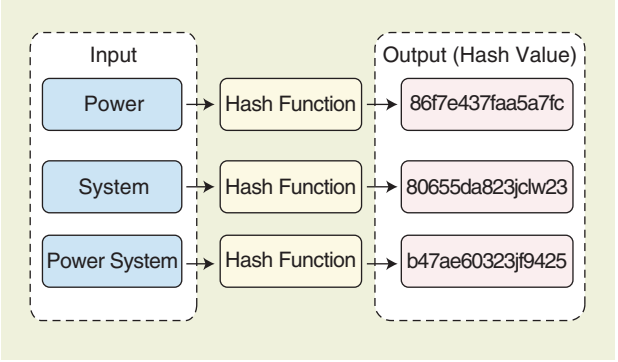

Figure 4. An example of the hash function.

asymmetric cryptography representing pairs of public and private keys in a blockchain ensures the message's authentication and privacy. Each participant applies public and private keys to encrypt and decrypt the data in the blockchain network. Both keys are a digital signature that is specific to a participant and provided before the participant submits any data to the blockchain; however, they have different functions. The public key, which is accessible by other participants, is a publishable identifier that allows each participant to be addressable in the blockchain network. The private key is kept secret.

Figure 6(a) and (b) depicts public and private keys for authentication and privacy, respectively. As for privacy, if participant 1 wants to send an encrypted message to participant 2 and does not want to reveal this message to the other participants, then participant 1 will use participant 2's public key to encrypt the message, representing a string of random numbers and letters. The encrypted message is sent to participant 2. After receiving the encrypted message, participant 2 decrypts the message using his or her private key. Privacy is, hence, guaranteed because the participants cannot decrypt and read the message without participant 2's private key. As for authentication, assume that participant 1 sends a message to participant 2 and wants to make sure that participant 2 knows this message is from participant 1. Participant 1 will encrypt this message into a string of random words and letters using his or her private key. Participant 2 receives the message and will use participant 1's public key to decrypt it. If the public and private keys do not match, participant 2 can see only a string of random words and letters. Therefore, authentication is maintained because nobody can impersonate participant 1 without participant 1's own private key to send messages to the other participants.

Blockchain Structure

A blockchain is a chain of data blocks, the structure of which is shown in Figure 7. Each data block for the blockchain data storage consists of two parts: the block header and the block body. In the block body, the data stored in the form of a Merkle tree will not be revealed because they are encrypted as fixed-length strings by using the hash function. The hash value of a Merkle root, which aggregates all of the encrypted data of a Merkle tree, is stored in the block header so that the data block can be tracked by referring to the Merkle root of the block header. Also, the block header stores the hash value of the Merkle root from the last block, which links all of the data blocks to form a chronologically ordered chain. Once the data block is added to the blockchain, any attempt to change the data in one data block will also change the hash value in the corresponding block header. Therefore, the blockchain structure is tamper proof because any attacks on the data block will be recognized immediately since the hash value of the revised block will not match the hash stored in the next data block.

In the blockchain network, every participant holding a blockchain would ensure that its blockchain is the same as those of other participants. A participant who stores data in the blockchain would formulate them as data blocks and propagate them to other participants randomly for validation. The updated blockchain, which is validated based on preset rules, will be added to the participant's own blockchains, and the data blocks are propagated randomly to other participants for validation. Once all blockchain network participants have verified the data blocks, the blockchain is updated.

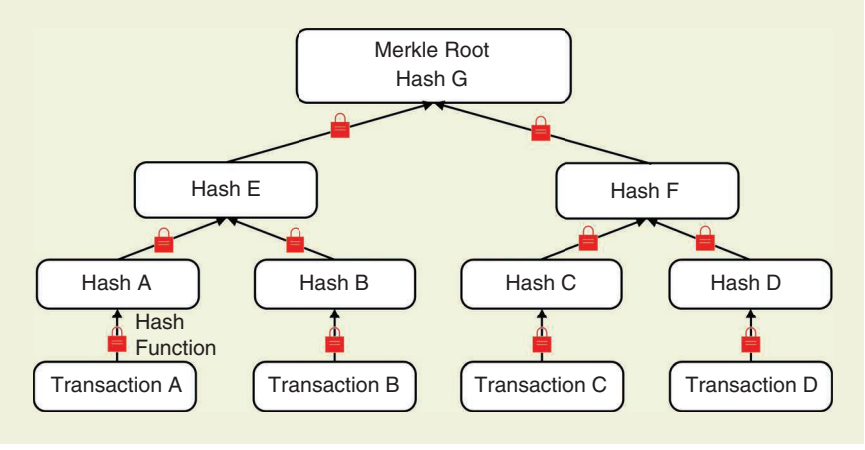

Figure 5. The structure of a Merkle tree.

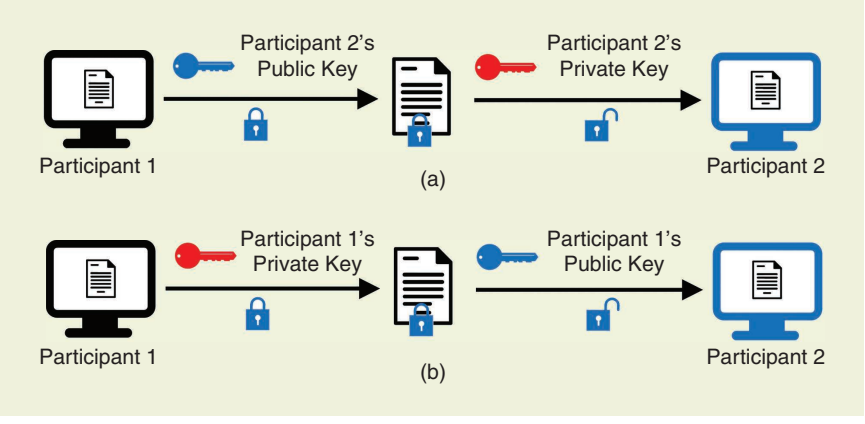

Figure 6. An example of public and private keys. (a) Privacy. (b) Authentication.

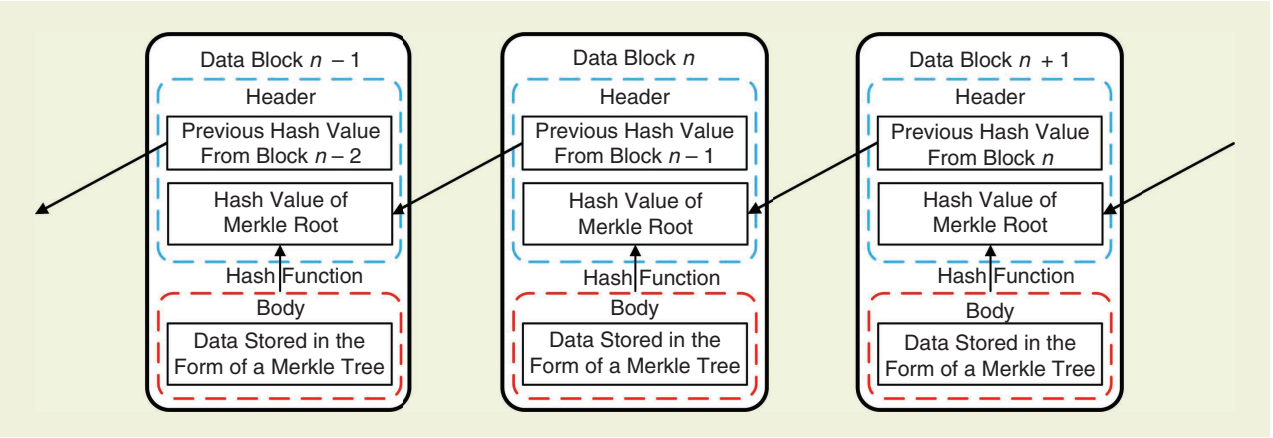

Figure 7. A blockchain formed by linking data blocks in sequence.

Smart Contract

A smart contract is a self-executing agreement embedded in a blockchain that contains a set of rules for participants' interactions, and the agreement is automatically executed when the predefined rules are satisfied. The functionality of smart contracts introduces immense opportunities for operational intelligence and enforces the market rules among distributed market participants. The deployment of smart contracts on the blockchain network is consistent with decentralized autonomous operations desired by P2P transactive energy trading. Smart contracts make it possible to develop and optimize automated and immutable applications in P2P transactive energy trading, including energy contract settlements in transactive energy markets.

Private Blockchain for Energy

The types of blockchain include the public blockchain and the private blockchain (also known as permissioned blockchain). Bitcoin is the most common transaction platform based on the public blockchain. Anonymous participants in such platforms can access and participate in transactions by adding a data block to the public blockchain without any trustworthiness or identity check. Because all of the participants in the public blockchain network operate without any central authority, a permissionless platform requires complicated consensus mechanisms [e.g., a proof-of-work (PoW) algorithm] to build a trusted environment for the participants. The utilization of such consensus mechanisms results in higher costs and lower speed for transactions, which hinders the use of the public blockchain for high-frequency P2P transactive energy trading.

In contrast to the public blockchain, the private blockchain is usually held and governed by a managing entity (e.g., the DSO in a power distribution system) that provides access to certified and trusted participants. A comparison of public and private blockchains is provided in Table 1. In the private blockchain, simple consensus mechanisms for data recording can be applied as participants have already declared a degree of manual trust. Accordingly, private blockchain transactions possess a much higher speed and much lower resource requirements. A proof of authority (PoA) consensus mechanism is utilized in the private blockchain for attaining a consistent consensus among participants on the data stored in the blockchain. In contrast to the public blockchain, only the authorized participants are authorized by the managing authority to validate the integrity of a new data block and add the data blocks to a blockchain. The authorized participants use their real identities to add the data block to the blockchain. By attaching their reputations to their identities, authorized participants declare the security and the authenticity of the data block as they are obliged to attach their identities to a negative reputation.

The Blockchain Initialization Process

This process is executed in private blockchains before the participants communicate with each other in the blockchain. The initialization process uses public and private keys to ensure that all of the participants are addressable in the blockchain, with a trustworthy environment for all participants. First, each blockchain participant should get permission from a blockchain managing entity who assigns each participant a public key. The public key

TABLE 1. A comparison of public and private blockchains.

Type of Blockchain	Public	Private
Participants	May result in malicious behavior	Identified and trusted participants
Consensus mechanisms	PoW (lower speed and higher energy consumption)	PoA (higher speed and lower energy consumption)
Transaction cost	High cost	Low cost
Applications	Public projects (i.e., cryptocurrency)	Organizations that require control of their data

TABLE 2. The participants' data.

Participants	Public Key	Private Key	Bids (Ether)
1	0x929aB5a6bFf983bC888953664886D01666803D9f	3e3x692uf93gyeuu	—
2	0x8dA5ad34728805c60aE7d1B4f0fD0145ce75782B	u32hfas89dh43165	30
3	0x509e76C694D84D74A8736332B1c822045c7cE5A6	43u28jhfas9438f8	20
4	0x1A4545135756CC8Fe5301E50c2E1d2E4A7741880	3c318d9914606339	25

serves as a publishable address in the blockchain. Next, each participant is authenticated by selecting a private key as a digital signature before communicating with the other participants. The pairs of public and private keys are stored in a participants' blockchain, which provides a tamper-proof attribute for these keys.

An Example of a Blockchain Application

This section provides a simple example of an auction that applies smart contracts to blockchain technology. Assume that there are four participants, 1, 2, 3, and 4, in the market. Participant 1 intends to sell a painting in an auction using smart contracts. The following rules are preset in smart contracts: 1) Participant 1 is the seller. 2) Participants 2, 3, and 4 can bid to buy the painting. 3) The highest bidder wins. Here, we use the Go Ethereum (Geth), which is a blockchain development platform. In Table 2, the Geth platform provides each participant with a unique public key, and each participant sets up a private key that is privately held.

Assume that participant 2 submits a bid at 30 Ether (a cryptocurrency used in Geth). Here, Participant 2 provides his private key as a digital signature. The participants' bids are listed in Table 3, where participant 2 is declared the winner because of their highest bid. Accordingly, the smart contract will transfer 30 Ether from participant 2 to participant 1. In this case, the participants held an auction without a third party (e.g., an auctioneer), and the smart contract automated the contract settlement process.

Blockchain For P2P Transactive Energy Trading in Networked MGs

The combination of a private blockchain and a PoA consensus method is applicable to the P2P transactive energy market for the following reasons: First, compared with a public blockchain, adding a data block is faster and embedded at a lower cost in the private blockchain. Participants in the private blockchain can easily trade with each other by adding data blocks to a blockchain. Second, the set of participants in the P2P transactive energy market is usually fixed (e.g., local MGs in a power distribution system). Accordingly, the DSO can easily determine the authorized MGs by using the PoA consensus method.

TABLE 3. The results of the auction.

Participant	Bidding Price (Ether)	Winner
1	—	—
2	30	✓
3	20	✗
4	25	✗

Two-Level Blockchain for P2P Transactive Energy Trading

Figure 8 illustrates the proposed two-level application of a blockchain applied to the P2P transactive energy trading depicted in Figure 2. We consider that each MG is managed by a MG master controller (MGMC). In Figure 8(a), each MGMC at the lower level manages its respective on-site DERs and demands and determines the optimal DER schedule for maximizing its payoff by selling power to the other MGMCs. In addition, the MGMCs provide strategic offers/bids for P2P energy trading with the other MGMCs. Once the energy trading among the MGMCs is completed, each MGMC submits its surplus/deficiency information to the DSO. For privacy concerns, each MG is represented as an equivalent source/load to the DSO. At the upper level of the power system, the DSO shoulders the responsibility of managing the grid and reconfiguring the power distribution network for enhancing the local network security and facilitating the P2P energy trading among the MGMCs. The DSO will subsequently request that the MGMCs adjust their trading schedule if the proposed MGMC's P2P energy trading schedule violates the DSO's distribution network security.

Figure 8(b) depicts a blockchain consisting of two blockchain systems. At the lower level, there is an MGMC blockchain that uses smart contracts to trade energy with each other. Additionally, the MGMC blockchain manages on-site DERs in each MG, which then submit the data blocks to the MGMC blockchain and execute the smart contracts sent from the MGMCs. In essence, the first blockchain performs two functions, including the P2P trades among MGs, and the trade within each MG that could occur among their respective components (e.g., buildings, batteries, generation resources, charging stations, and so on). The second blockchain in Figure 8(b), which is referred to as the DSO blockchain, is set up for distribution network management. The upper level cloud data center includes the DSO's operation for managing the distribution grid. The DSO blockchain collects the data blocks provided by the MGMC blockchains and sends the smart contracts to the MGMC blockchains. The two blockchain systems in Figure 8(b) store the data blocks and smart contracts.

The Blockchain Initialization Process

Figure 9 shows the initialization process for both MGMC and DSO blockchains. When using the private blockchain, it is mandatory for the participating MGMCs to register with and receive authorization from the DSO prior to interacting with the other MGMC and DSO blockchains. Such requirements prevent unauthorized MGMCs from participating in the blockchain system and thus ensure the networked MG security. The DSO authorizes the MGMCs by assigning a public key to each one as a unique publishable address that is accessible by other MGMCs and the DSO. In addition, each MGMC will set a private key as its digital signature, which is submitted for authentication before any interactions with other MGMC and DSO blockchains. These pairs of public and private keys are stored in both the MGMC and DSO blockchains, which provide a tamper-proof fabric for these keys. To protect the privacy of each MGMC, the DSO assigns each MGMC with an anonym that conceals the MGMC's identity. These MGMCs execute the anonymous P2P transactive energy trading, which effectively avoids linking the energy trading patterns and financial gains to the MGMCs' actual identities.

Lower-Level P2P Transactive Energy Among MGs

The MGMC blockchain performs two functions. Figure 10 illustrates the first function for the interaction between

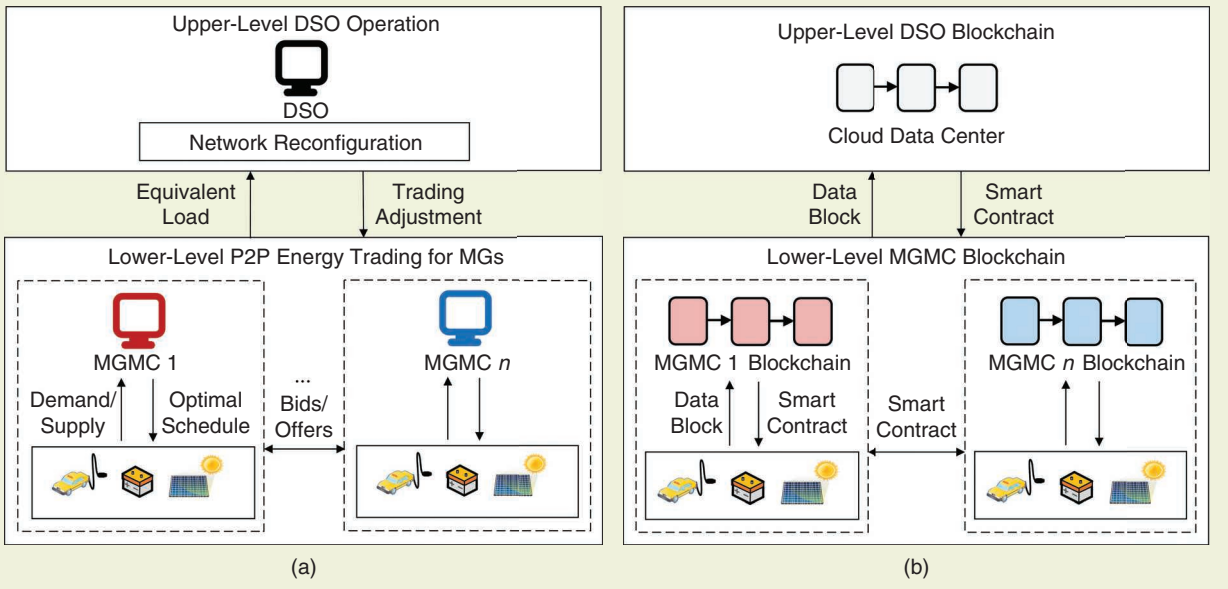

Figure 8. A blockchain framework for P2P transactive energy trading in networked MGs. (a) The power system. (b) The blockchain system.

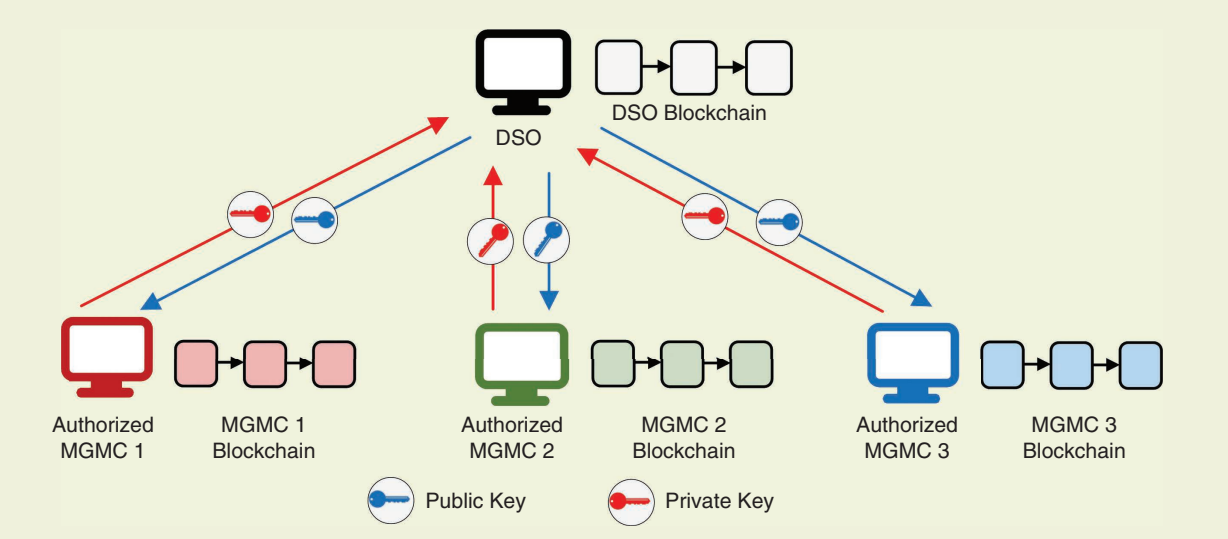

Figure 9. A blockchain based transactive energy initialization process.

the DERs and the MGMC. In Figure 10(a), the DERs submit their demand/supply data to the MGMC, which manages the DER outputs and demands for maximizing its own payoff. Each MGMC maximizes its payoff function by optimizing on-site DERs, with the consideration of operation constraints of the DERs. Accordingly, the MGMCs will obtain the DER demand/surplus after solving the optimization problem and further send the optimal schedule to each DER. In Figure 10(b), the blockchain system represents the interaction between the DERs and MGMC. The DERs formulate demand/supply data as data blocks and submit them to the MGMC. The MGMC formulates the optimal schedule as a smart contract in the blockchain system and delivers this contract to all of the DERs for scheduling.

Cybersecurity is critically important when considering the interaction between DERs and the MGMC since there are often no special information protection measures available for the DER data. Because the DERs may not have a password to access, or built-in protection, they are easily attacked and controlled by external attackers. In Figure 10(b), the hash function ensures security, where any malicious attack by external attackers for revising the data block and smart contract can be easily detected. Furthermore, the tamper-proof characteristics of the data stored in the MGMC blockchain protect the integrity of the DER data.

Figure 11 shows the second function of the MGMC blockchain that allows the MGMCs to trade energy with each other through P2P energy trading. In Figure 11(a), the MGMCs are categorized as sellers and buyers according to their energy surplus and deficiency. The sellers will provide offers (i.e., their energy surplus quantity and price), while the buyers provide bids (i.e., their energy demand quantity and price). The MGMC state (i.e., the seller or buyer) could change according to the trading price signal. For instance, the MGMCs with energy storage tend to sell their stored energy when the energy price is high and buy energy and store it when the energy price is low. In P2P energy trading, sellers will compete to maximize their profits, while buyers will compete to minimize their purchase cost.

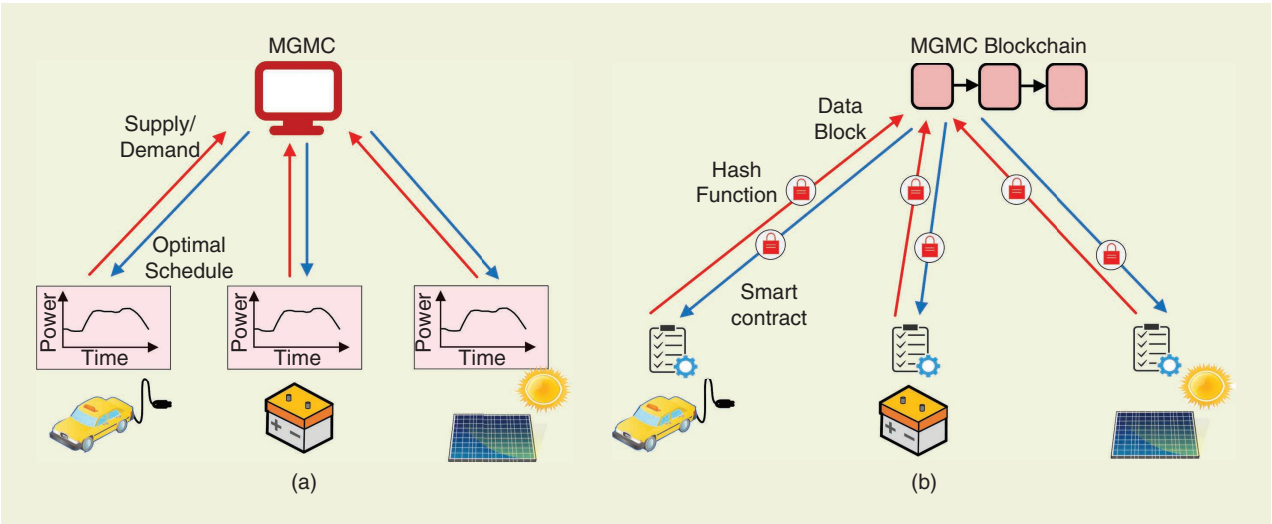

Figure 10. The interactions between DERs and MGMC in a single MG. (a) The power system. (b) The blockchain system.

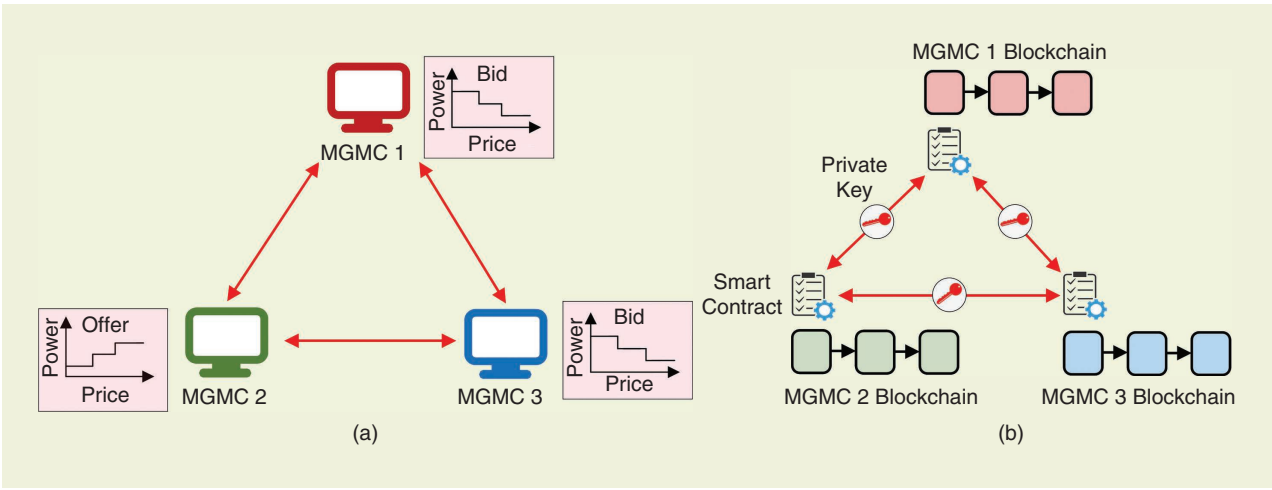

Figure 11. The P2P energy trading process among MGs. (a) The power system. (b) The blockchain system.

For privacy concerns, MGMCs do not want to reveal their proprietary information (e.g., DER generation quantities and costs) to other MGMCs. Therefore, a distributed approach is developed for MGMCs to attain optimal energy trading results while protecting their privacy. Using the distributed approach, the MGMCs will strategically bargain for adjusting their bids/offers until they reach optimal energy trading results (i.e., energy quantity and price). The distributed approach will offer the following attributes: 1) A converging and distributed bargaining process among participating MGMCs must be attainable; otherwise, the MGMCs do not have an incentive to bargain. 2) A stable outcome should be available in the bargaining process in which the MGMCs will not find a more economically preferable outcome.

Therefore, an iterative distributed approach is designed as follows. First, the MGMCs that want to trade with others publish their bids/offers. Second, the MGMCs choose their favored bids/offers published by the other MGMCs. If the published bids/offers are not acceptable, the participating MGMCs may not choose any of them. The MGMCs adjust their bids/offers according to the P2P energy trading results. For instance, if the selling MGMCs receive a supply bid that is higher than their surplus energy, the selling MGMCs could increase their energy prices for making a higher payoff. The procedures will be terminated when all of the MGMCs are satisfied with the energy trading results. Accordingly, the competitive behavior among buyers and sellers is modeled by a noncooperative multileader, multifollower Stackelberg game, where the MGMCs optimize the energy trading quantity and price by solving the game problem.

Figure 11 illustrates the use of blockchain in the proposed P2P energy trading process among MGMCs. In practice, the participating MGMCs may lack a sufficient market knowledge to quickly submit reasonable bids/offers in a dynamic energy market. Therefore, it is a great challenge to implement a viable procedure for the MGMCs to attend the P2P energy trading market. The introduction of blockchain and smart contracts makes it possible to automate energy trading interactions for the MGMCs in a dependable and secure fashion. In Figure 11(a), the MGMCs exchange bids/offers with each other in power systems.

However, in Figure 11(b), the MGMCs use smart contracts to achieve automatic energy trading in the blockchain. Each MGMC publishes a smart contract through its MGMC blockchain and provides the smart contract a unique address, to which other smart contracts can have access. In addition, the MGMCs will preset their rules in a smart contract (e.g., the selling energy price cannot be lower than US$10/MW). Accordingly, smart contracts will be triggered and executed automatically for participating MGMCs in the P2P transactive energy trading. The smart contracts will read the data (e.g., the available DER outputs) stored in the MGMC blockchains and automatically calculate bids/offers according to the preset rules in the smart contracts. Subsequently, the smart contracts will be encrypted with their private keys as digital signatures to communicate with one another for energy trading.

When individual smart contracts receive bids/offers from other smart contracts, they will automatically calculate the corresponding energy trading results. If the results do not meet the preset expectations in the smart contracts, the smart contracts will upgrade their bids/offers and communicate them to the other smart contracts for energy trading. For instance, if the MGMC is scheduled to sell less energy than expected, owing to high energy prices, the smart contract will automatically reduce its energy price for selling more energy. If the proposed P2P energy trading results have met the preset expectations of the MGMCs in their smart contracts, the smart contracts will terminate the energy trading process and publish the optimal P2P energy trading results. Then, the smart contracts will automatically execute market settlements based on the P2P energy trading results. The energy trading results will be recorded by the MGMC blockchains, which provide tamper-proof characteristics for these results to the participating MGMCs.

Upper Level DSO Blockchain

Figure 12 depicts the upper-level DSO blockchain for the transactive energy management in networked MGs. At the upper-level DSO blockchain, the DSO uses the MGMC trading results to determine the distribution network reconfiguration. In Figure 12, each MGMC submits its equivalent load/source data blocks to the DSO for privacy concerns. The MGMCs encrypt the data blocks with their privacy keys to indicate the sources of their data blocks, which are recognized and stored by the DSO using the MGMCs' public key. Accordingly, the DSO applies the optimal power flow model for the distribution network reconfiguration to facilitate the P2P energy trading transactions.

In Figure 12, if there are any network violations, the DSO will submit the prescribed transactive market trading adjustments to each MGMC to revise the P2P energy trading results accordingly. Here, the P2P energy trading adjustment request is formulated as a smart contract, which is first stored in the DSO blockchain and then submitted to the MGMC blockchains. The DSO will encrypt each MGMC's smart contract with their public key to ensure the privacy of the smart contracts. The smart contract will be self-executable in the MGMC blockchain to apply the necessary revisions in the P2P transactive energy trading results. This iterative process between the upper- and lower-level blockchain will continue until the network security is maintained as part of the calculation of the optimal P2P energy trading in the networked MGs.

Conclusion

With the increasing penetration of DERs, power distribution systems are undergoing a significant transformation from conventional inactive distribution systems

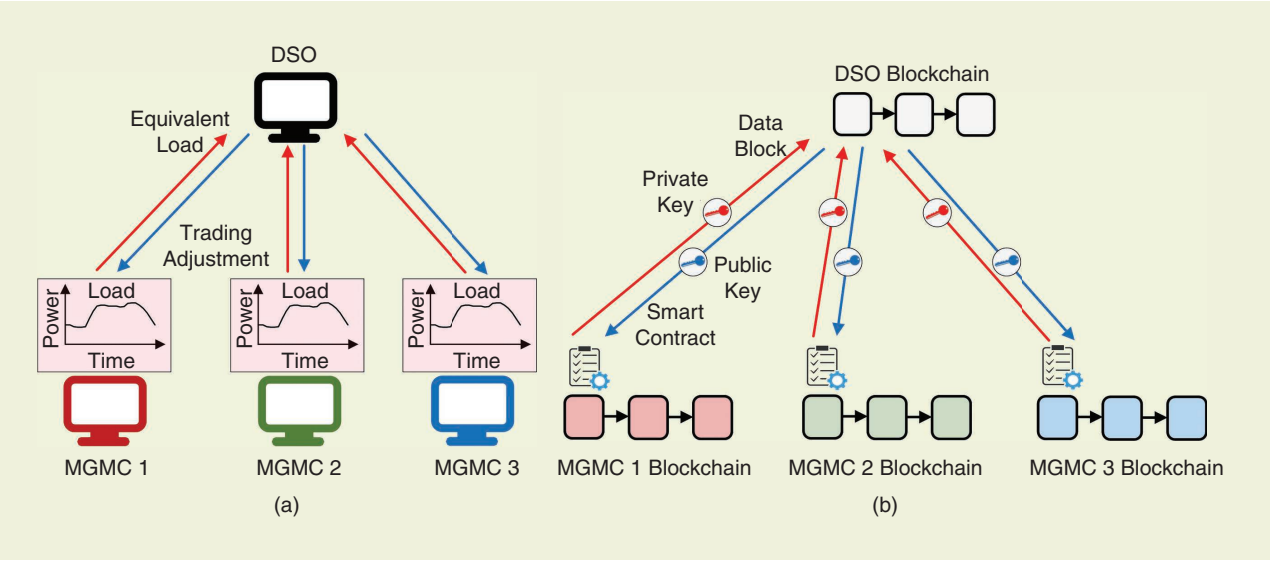

Figure 12. An upper-level DSO blockchain for networked MG transactive energy management. (a) The power system. (b) The blockchain system.

into active distribution systems. Transactive energy, which allows MGs to trade energy in a P2P fashion, opens the door to autonomous electricity retail markets and establishes a new business and operational method for local power generation, delivery, and consumption. By actively participating in the P2P transactive energy trading market, networked MGs provide a promising alternative to improve the operational performance of power distribution systems.

P2P transactive energy trading can benefit from blockchain technology by offering robust, transparent, and tamper-proof alternatives to electricity market participants. In this article, blockchain was introduced as a secure technology for energy trading. In particular, blockchain has offered a viable solution for empowering networked MGs to play a more active role in P2P transactive energy trading. We proposed a two-level blockchain for P2P transactive energy trading, which paves the way for flexible energy trading among networked MGs. The solution encourages MGs to participate more proactively in energy trading and take full advantage of environmentally friendly and economically viable DERs in power distribution systems. The introduction of blockchain provides a secure and trustworthy alternative by using cryptography and smart contracts for networked MGs, which can trade energy in an automatic mode for enhancing the reliability, resilience, economics, and sustainability of the electricity services offered by local power distribution systems.

In the future, networked community MGs will evolve into networked energy hubs (featuring linked electricity, natural gas, heat, water, and transportation infrastructures), which will govern the optimal supply and consumption of different types of energy in local districts. The proposed blockchain management system is capable of providing a trustworthy market environment to automate the secure delivery of multienergy transactions in our communities.

For Further Reading

Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked microgrids for enhancing the power system resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1289–1310, 2017. doi: 10.1109/JPROC.2017.2685558.

M. Shahidehpour, Z. Li, S. Bahramirad, Z. Li, and W. Tian, "Networked microgrids: Exploring the possibilities of the IIT-Bronzeville grid," *IEEE Power Energy Mag.*, vol. 15, no. 4, pp. 63–71, July–Aug. 2017. doi: 10.1109/MPE.2017.2688599.

Y. Wang, Z. Huang, M. Shahidehpour, L. L. Lai, Z. Wang, and Q. Zhu, "Reconfigurable distribution network for managing transactive energy in a multi-microgrid system," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1286–1295, Mar. 2020. doi: 10.1109/TSG.2019.2935565.

Z. Li, S. Bahramirad, A. Paaso, M. Yan, and M. Shahidehpour, "Blockchain for decentralized transactive energy management system in networked microgrids," *Electr. J.*, vol. 32, no. 4, pp. 58–72, May 2019. doi: 10.1016/j.tej.2019.03.008.

M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019. doi: 10.1016/j.rser.2018.10.014.

Biographies

Mohammad Shahidehpour (ms@iit.edu) is with the Robert W. Galvin Center for Electricity Innovation at the Illinois Institute of Technology, Chicago.

Mingyu Yan (myan9@iit.edu) is with the Robert W. Galvin Center for Electricity Innovation at the Illinois Institute of Technology, Chicago.

Pandey Shikhar (shikhar.pandey@comed.com) is with ComEd, Chicago.

Shay Bahramirad (shay.bahramirad@comed.com) is with ComEd, Chicago.

Aleksi Paaso (esa.paaso@comed.com) is with ComEd, Chicago.