The Electricity Journal 32 (2019) 58–72

Contents lists available at ScienceDirect

The Electricity Journal

journal homepage: www.elsevier.com/locate/tej

Blockchain for decentralized transactive energy management system in networked microgrids

Zhiyi Li[a], Shay Bahramirad[b], Aleksi Paaso[b], Mingyu Yan[a], Mohammad Shahidehpour[a,*]

[a] Robert W. Galvin Center for Electricity Innovation at Illinois Institute of Technology, Chicago, IL 60616, USA
[b] Commonwealth Edison, Chicago, IL 60640, USA

ARTICLE INFO

Keywords:
Blockchain
Networked microgrids
Transactive energy
Smart contracts
Decentralized energy management

ABSTRACT

The proliferation of distributed energy resources is reshaping the landscape of power distribution systems, including a network of autonomous microgrids. Networked microgrids transact energy for managing the efficiency, reliability, resilience, security, and sustainability of electric power services. This article offers a vision and analyzes a scheme developed for networked microgrids that utilizes blockchain technologies to optimize the financial and physical operations of power distribution systems. Blockchain provides a powerful and trustworthy path for launching distributed data storage and management, the article explores the possibility of customizing blockchain technologies to meet socioeconomic requirements of transactive energy management at the power distribution level. Then, a set of interoperable blockchains embedded with self-enforcing smart contracts is proposed to manage energy and financial flows among transacting microgrids in a credible manner. The article presents additional smart contract measures for securing optimal energy transactions between networked microgrids and the local distribution grid. It is concluded that blockchain technologies embedded in transactive energy will play a significant role in the evolution of traditional power distribution systems to active distribution networks.

1. Networked microgrids in power distribution systems

Technological and socioeconomic developments in distributed generation have promoted microgrids as promising alternatives to the traditional bulk power grid for electricity delivery. Principally, microgrids are small-scale self-controllable power systems that interconnect on-site generation resources and loads for striking a local balance of energy production and consumption. Each microgrid operates strategically for fulfilling the promise of boosting the survivability and the efficiency of electricity delivery. Normally, microgrids are connected to an adjoining power distribution system (i.e., main grid) so that they can optimize their energy management not only by taking full advantage of on-site resources but also by interacting actively with the main grid. When severe disruptions occur, microgrids isolate themselves from the main grid and function as self-contained islanded entities to sustain local and critical electricity services at a satisfactory level.

Geographically-close microgrids can be networked to broaden the merits of microgrids and eventually refine electricity service provisions across the power distribution system (Che et al., 2015). Networked microgrids can address inefficiencies and vulnerabilities especially in the face of emergencies that are embedded in the long-distance power delivery from central generating plants to dispersed customer sites. Networking microgrids can fundamentally challenge the way electric energy is generated, delivered, and consumed in a power distribution system. As microgrids are increasingly deployed and interlinked, a power distribution system is progressively becoming a network of autonomous microgrids that are capable of handling two-way flows of electricity and information (Li et al., 2017a). In Fig. 1, the IEEE 123-bus test system is portrayed as a system of seven networked microgrids, each accounting for the operation of a section of the local distribution feeder circuit.

These networked microgrids offer a highly scalable and flexible solution to environmental concerns and operational goals of power grid modernization. First, networked microgrids provide a credible means of accommodating distributed energy resources (DERs) scattered at diverse locations to supplement available resources in individual microgrids. Second, networked microgrids contribute to the system-wide efficiency and security in a power distribution system as they respond more efficiently to dynamic operating conditions caused by the variability of DER outputs. Third, networked microgrids are inherently more reliable than individual microgrids, since each networked microgrid offers reserves for their peers to reduce the probability of power outages

* Corresponding author.
E-mail address: ms@iit.edu (M. Shahidehpour).

https://doi.org/10.1016/j.tej.2019.03.008

Available online 06 April 2019

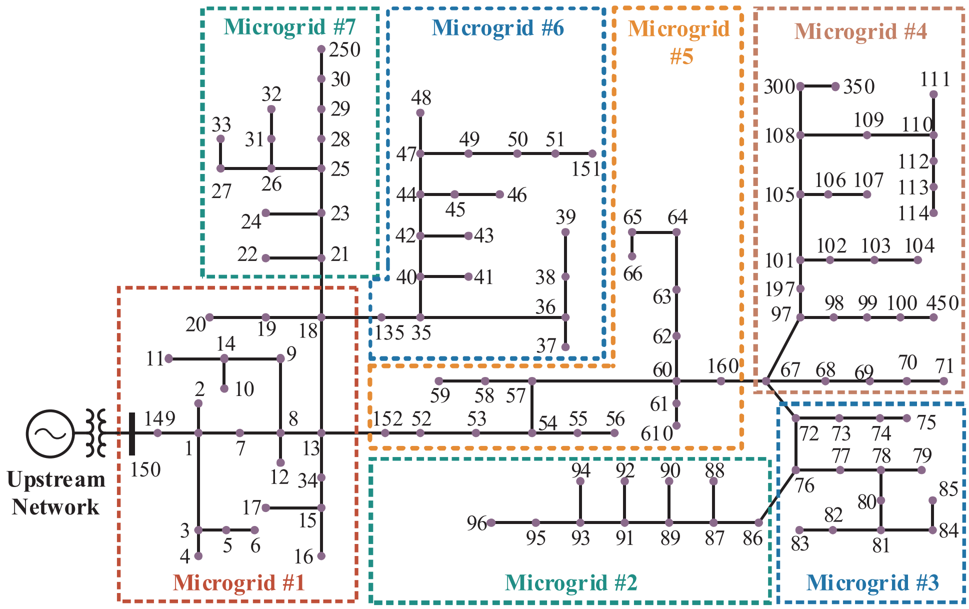

Fig. 1. Networked microgrids in the IEEE 123-bus test system.

in the utility network (Farzin et al., 2016). Last, networked microgrids are more likely to survive extreme event disruptions (e.g., natural disasters (Ma et al., 2018; Yuan et al., 2016), massive cyber or physical attacks (Li et al., 2016; Li et al., 2018)) and work collaboratively to expedite the restoration of electricity services (Liu et al., 2016). However, these provisions will also depend on the severity of extreme events and the degree of physical damages incurred by individual microgrids

Networked microgrids, operating as independent agents or functioning collaboratively, may also complicate distribution system operations. In particular, the emergence of two-way power flows has altered many traditional premises in power system protection and security analyses. Accordingly, conventional paradigms in energy management systems can hardly be met by the challenges arising from emergence of autonomous and interacting microgrids.

As microgrids are regarded as entities which participate increasingly in distribution system planning and operation, a natural evolution at the distribution level would be to provide market-based financial signals for incentivizing networked microgrids to share resources. Such financial signals will ultimately affect the way bulk power systems are planned and operated. In other words, energy transactions among networked microgrids with a myriad of flexible loads and intermittent generation resources become more appealing for managing the system-wide power balance. The applications of such energy transactions necessitate significant regulatory and technical changes in retail electricity market operations that have been historically characterized as regionally monopolistic. When competition is embedded in electricity retail markets, networked microgrids will exchange energy more flexibly with their peers, rather than interacting solely with the distribution grid at a fixed electricity rate using strategies such as rate design (Darghouth et al., 2011) or buy-all, sell-all (Distributed Generation Buy-All, Sell-All Program, 2019).

This article proposes a secure, scalable, and efficient solution using the blockchain for decentralizing the transactive energy management (corresponding to the electricity retail market) which is expected to address operational and financial challenges posed by the emergence of DER-based networked microgrids at the power distribution level. The remainder of the article is organized as follows. Section 2 explores the potential application of transactive principles to energy transactions in the electricity retail market where a set of networked microgrids are active market participants. Section 3 introduces the inherent properties of blockchain and points out that blockchain provides a powerful and trustworthy path for launching distributed data storage and management in the transactive energy system. Section 4 provides a deep insight into how the transactive energy system can utilize blockchain technologies to ensure the integrity, optimality, and privacy of market participation of individual microgrids. Section 5 presents the detailed process of transactive energy management that is dependent on interoperable blockchains. Section 6 further discusses the design and implementation of smart contracts for enhancing the cybersecurity of blockchain-based transactive energy management. Section 7 concludes the article and stresses the significance of transactive energy management in the evolution of power distribution systems.

2. Transactive energy system for networked microgrids

Transactive energy applications (Rahimi and Ipakchi, 2012; Khodayar et al., 2016) facilitate the dynamic balance of power generation and consumption in a power distribution system and address critical technical and financial management challenges posed by networked microgrids in the process of power grid modernization.

2.1. Transactive energy for power distribution systems

Transactive energy refers to direct energy exchanges in response to market-based energy generation values at the power distribution level, which allows networked microgrids to execute peer-to-peer energy transactions. Microgrids are considered aggregated prosumers (i.e., consumers with energy generation and storage capabilities) that can exchange energy at pre-specified rates with the utility network. This conventional top-down regulation scheme would impede the exploitation of operational flexibilities embodied in microgrids, which are networked for maximizing the benefits of on-site generation and load resources. Accordingly, alternative regulation schemes are needed for conducting energy trading by networked microgrids in more efficient, flexible and scalable manners.

Fig. 2 compares energy trading in four networked microgrids using conventional and transactive energy regulations. In Fig. 2(a), the four microgrids exchange power merely with the utility network at fixed electricity rates; the merits of localized renewable energy generation and demand-side management cannot be fully realized when the electricity rates are not appropriately adjusted. In Fig. 2(b), the four microgrids exchange energy with each other at market-based values; here,

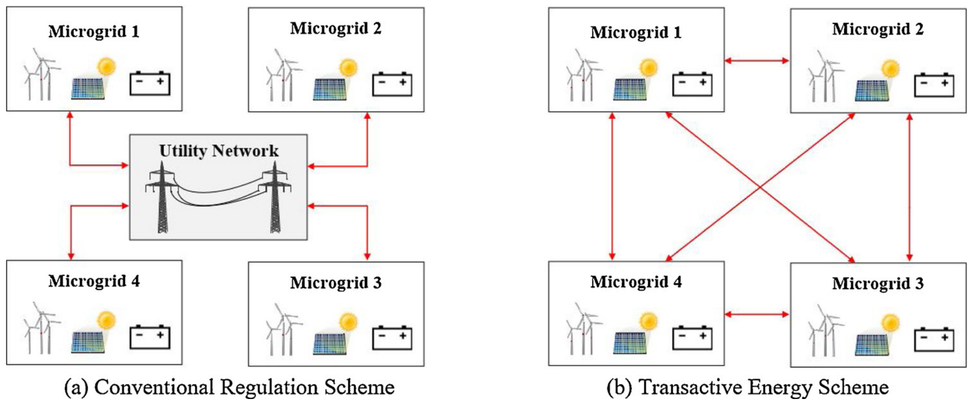

Fig. 2. Energy trading options in power distribution system.

microgrids maintain a dynamic power balance in their service territories with reduced dependency on the utility network; transactive energy would also satisfy pre-specified energy regulation objectives (e.g., power balancing, peak demand management, line congestion management) in microgrids through dynamic market signals.

Transactive energy provides a transformative solution to technological and socioeconomic challenges of the power grid modernization. The progress in establishing retail markets has been stagnant mostly due to regulatory concerns for incentivizing local generators and microgrids to collaborate with distribution utility companies on the management of modern power distribution systems. The power distribution system, operated by a distribution system operator (DSO), is experiencing a changing generation mix landscape where renewable energy resources are increasingly dominant. The adoption of transactive energy bestows additional opportunities for valuing and dispatching renewables-based DERs. Transactive energy is expected to catalyze innovative pricing schemes for compensating locational and temporal values of DERs in real time, incentivizing more investments in localized renewable energy generation. Accordingly, DERs will continue to grow and flourish in power distribution systems while providing tangible benefits to foster a sustainable future.

Transactive energy applications also expedite the development of demand response programs. When on-site generation resources are inadequate to supply local loads and power imports from external energy sources are expensive, microgrids tend to curtail non-critical loads for achieving a local power balance. Besides, real-time market signals enable networked microgrids to shift their real-time energy consumption for achieving a trade-off among multiple conflicting goals (e.g., comfort, convenience, savings on electricity usage).

2.2. Transactive energy management for networked microgrids

To close the gap between electricity wholesale and retail markets, DSO will apply transactive principles to set up a competitive energy trading system (denoted as transactive energy system) at the retail market level where networked microgrids become active market participants and interact to carry out energy transactions in a peer-to-peer manner. Accordingly, the transactive energy system enables networked microgrids to collaborate according to dynamic market signals in a quest for refining electricity services across the power distribution system (Wang and Huang, 2016). Such a collaboration contributes to more efficient use of on-site resources together with more affordable electricity rates for local customers and plays a particularly significant role in the wake of extreme events. When an extreme event occurs, networked microgrids with diversified generation and load profiles are incentivized to adapt their energy transactions to the changing environment in an effective and prompt manner for making their local electricity services more resilient to random disruptions.

However, significant differences between power transmission and distribution systems would make it impractical to operate the transactive energy system at the distribution level by directly mirroring the wholesale market mechanism. Power distribution systems normally feature a high ratio of power losses, radial network topology, three-phase unbalanced network configuration and numerous low-voltage buses. With an increasing level of DER penetration, the operation of power distribution systems would be further challenged by the variability of renewable energy. Accordingly, DSO needs to fulfil its role in transactive energy management to address operational challenges associated with peer-to-peer energy transactions among networked microgrids. On the one hand, DSO as a non-profit entity would lower the barrier to the non-discriminatory transactive energy system to increase the market participation and empower participants equally in the retail market. On the other hand, DSO is the independent intermediary that ties the network of microgrids with the utility network while meeting energy security requirements of localized energy transactions. DSO participates on behalf of networked microgrids in the wholesale market operation for maximizing the social welfare of the power distribution system. DSO would monitor and control the amount of energy exchange with the utility network to strike a balance between power generation and consumption with a guaranteed quality of electricity services at the power distribution system.

To ensure the scalability of transactive energy management, individual microgrids are allowed to exchange information and transactwith one another and with DSO in a decentralized manner. Furthermore, market participants are responsible for maintaining the stability and security of power distribution systems when participating in the transactive energy system. Fig. 3 illustrates a local power distribution system (which mimics the IIT-Bronzeville networked microgrids in Chicago (Shahidehpour et al., 2017)) for establishing a transactive energy system. Here, two adjacent microgrids have separate points of common couplings (controlled by switches S1 and S2, respectively) with the utility network; they are also tied directly by a dedicated power line (configured with switch S3) in parallel with existing distribution feeders. The three switches are remotely controlled by DSO for adapting the transactive energy system topology to economic incentives and at the same time mitigating energy security risks caused by the massive integration of DERs (e.g., voltage rises (Christakou et al., 2017), line congestions (Koutsoukis et al., 2017)).

In Fig. 3, each microgrid is deployed with a microgrid master controller (MC) for centrally monitoring and controlling on-site resources in various operating conditions. DSO would balance the generation with consumption according to the outcome of the transactive energy system by exchanging energy with the utility network. The two MCs and DSO interact through dedicated telecommunication channels for making energy trading decisions in accordance with their operational and environmental goals (e.g., lower cost, congestion, emission). Given a particular distribution system topology, the two microgrids can exchange energy with the utility network via their points of common

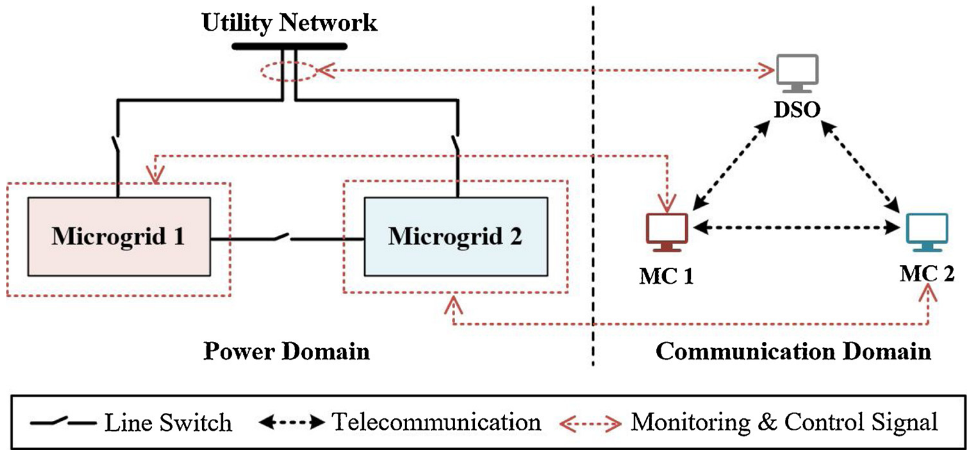

Fig. 3. Networked microgrids for enabling transactive energy.

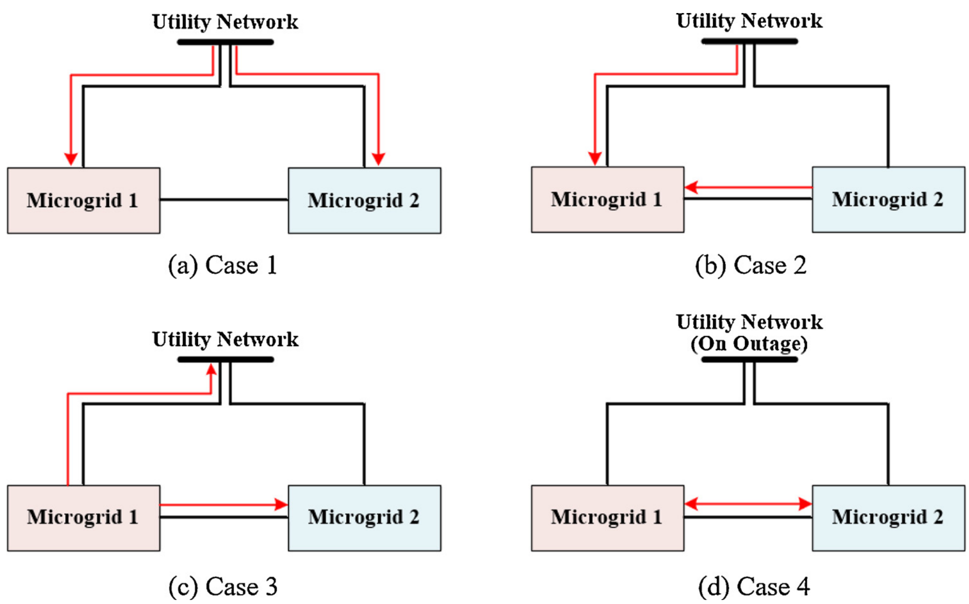

Fig. 4. Energy transactions among networked microgrids.

couplings and/or directly with each other via the dedicated power line. Fig. 4 presents four typical cases where each microgrid participates actively in transactive energy. In Fig. 4(a), both microgrids lack sufficient on-site renewable energy generation and request DSO to import the energy balance from the utility network. In Fig. 4(b), Microgrid 2 has an excess generation supply and Microgrid 1 has a supply deficiency. So, Microgrid 2 transacts energy with Microgrid 1 and DSO imports energy from the utility network for balancing the power deficit. An opposing case is shown in Fig. 4(c). In Fig. 4(d), only the two microgrids are transacting energy once the utility network is on outage.

2.3. Blockchain-based transactive energy system

The operation of the transactive energy system could face an overwhelming degree of complexity in sustaining market participant objectives. As the transactive energy system affords the joint responsibility of managing energy and market, energy flows and financial transactions across the distribution system need to be trustworthy and transparent to all participants.

In each microgrid, MC is the central source of communication, coordination, and management in microgrid operations. MC gains fine-grained visibility and control over various generation and load resources distributed on the microgrid and makes timely decisions on exchanging energy in the transactive energy system. Meanwhile, DSO itself participates in the localized energy trading as a surrogate prosumer representing interactions with the wholesale market. DSO provides strategic financial signals (commonly determined by economic incentives) for the local transactive system to interact with the wholesale market. The lowered threshold for access to the transactive energy system introduces challenges in the establishment of trust among market participants. In particular, the transactive energy system needs to be protected adequately from the careless or malicious trading behavior of networked microgrids, which would otherwise hamper the integrity of retail market operations and even destabilize physical system operations. Privacy leakage is another common concern in transactive energy management. Market participants should avoid exposing their sensitive commercial information (e.g., production cost coefficients of local generation) and critical operation information (e.g., operating states and security margin of local generation) to their peers. Market participants will be instructed to exchange non-critical information (e.g., available generation capacity, marginal generation cost) for driving their local operating conditions toward a common goal of the transactive energy system.

To enhance the transparency and trustworthiness of decentralized transactive energy management (without a central intermediary), we propose a highly secure and scalable transactive energy system

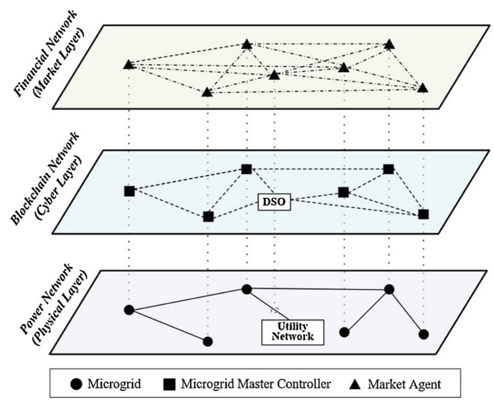

Fig. 5. Blockchain-based transactive energy system in networked microgrids.

structure as shown in Fig. 5. The proposed transactive energy system consists of three functional layers: physical layer representing the power distribution infrastructure, including a network of microgrids and the adjoining utility network for electricity generation, delivery, consumption and storage; cyber layer representing the information and communication infrastructure, including a host of communication, computing, and control devices for data exchanges, peer discovery, and automated control; and a market layer representing the financial network, including a variety of retail market agents that interact and compete for optimal peer-to-peer energy transactions. The cyber layer facilitates the participation of networked microgrids in the competitive retail market and underpins the interplay between physical and market layers as follows: the cyber layer collects and aggregates real-time operating conditions of the physical layer for decision making on energy trading at the market layer; on the other hand, the cyber layer automates and enforces the execution of energy transactions determined by the market layer in the actual operation of power distribution infrastructure at the physical layer.

We utilize state-of-the-art blockchain technologies (as will be detailed in Section 3) to secure and automate interactions among MCs and DSO at the cyber layer. The blockchain-based secure database is shared across the data storage and exchange network of MCs and DSO (denoted as the blockchain network) to audit the integrity and validity of energy flows at the physical layer and financial transactions at the market layer. Accordingly, MCs and DSO would require powerful computers with adequate data storage capabilities for maintaining an ever-growing blockchain-based database. It would also be necessary to deploy cybersecurity measures on MCs and DSO so that a significantly high level of trustworthiness of MCs and DSO is guaranteed when they participate in the blockchain network (Jin et al., 2017). Hence, participants in the transactive energy system would have stronger capabilities to make credible decisions on energy transactions without violating energy security requirements.

3. Blockchain technologies for secure data management

Blockchain, which was originally developed for the cryptocurrency Bitcoin (Nakamoto, 2008), has acted as the core technology that underpins a multitude of trustless peer-to-peer financial services (Underwood, 2016). In the context of transactive energy management, blockchain would also offer additional opportunities for reconciling privacy and manipulation concerns. In particular, blockchain would transform the ways participants share information and monetize their market participation in a transactive energy system.

3.1. Blockchain as shared distributed database

Operating states in a transactive energy system are recorded in blockchain to keep track of energy trading among transacting microgrids in a trustless environment. Conventionally, each transacting microgrid would maintain a local database for recording local operating states, as MC communicated with DSO (trusted central intermediary) for validating the recorded data as illustrated in Fig. 6(a). This separately-maintained data storage and management scheme, which is subject to inefficiencies in validation process and cyberattacks, can hardly support the desired scalability and trustworthiness of transactive energy management. Blockchain, which is a shared chronological database, avoids data storage and management tampers in the transactive energy system. In Fig. 6(b), the four microgrids use blockchain to collectively maintain a shared database in a decentralized manner that would not require a trusted central intermediary. The new operating states are packaged into additional data blocks at the end of the blockchain by a chosen miner (e.g., Microgrid 1 in this case). Once recorded in blockchain, these operating states can no longer be altered as all four microgrids have reached a consensus. Each microgrid keeps a copy of the blockchain in its local settings for recording and reading local operating states.

Blockchain maintains a continuously growing list of data records secured by cryptographic signatures (Swan, 2015). Fig. 7 shows the blockchain structure where data block is the fundamental unit for data storage. Each block records data in the form of a Merkle tree (Li et al., 2014) which is encrypted by a hash function (e.g., SHA-256 (Gilbert and Handschuh, 2003)) to produce a fixed-length string without

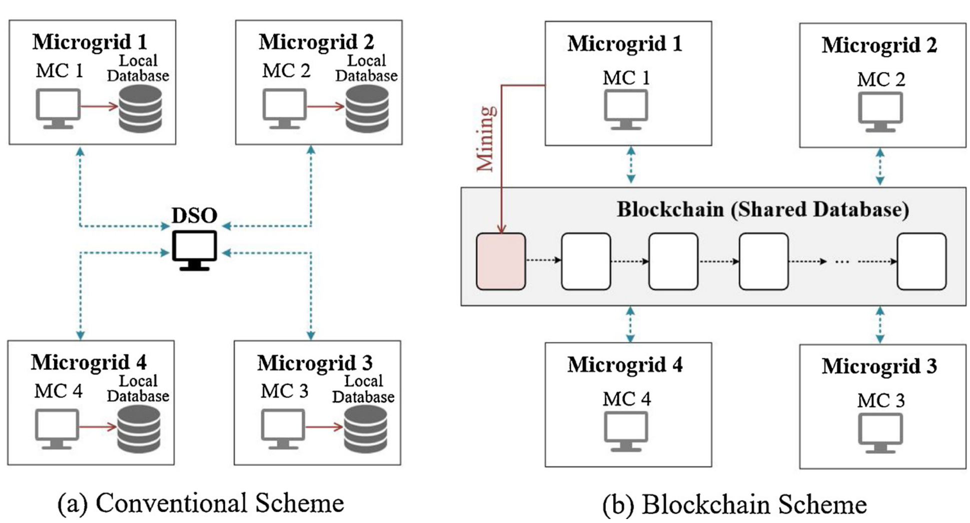

Fig. 6. Data storage and management schemes for transacting microgrids.

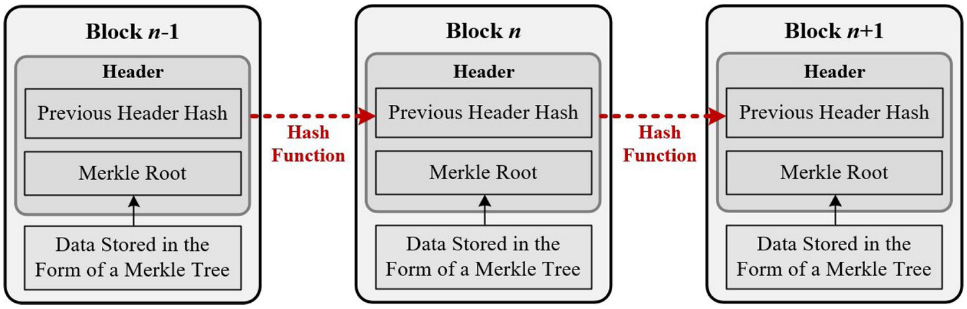

Fig. 7. Blockchain formed by sequential data blocks.

revealing any clue associated with the original data. In the Merkle tree, whose bottom nodes (i.e., leaf nodes) correspond to the recorded contents, hashes of children nodes are combined to form hashes of their parent node at the upper layer as the iterative process terminates at the top node (i.e., root node). Since the root node aggregates the encrypted information of other nodes in the Merkle tree, the header of each data block would only contain the root node for keeping track of the contents intended to be recorded. Moreover, each data block can be uniquely identified by the hash generated over the header of the previous block. Therefore, data blocks are linked by reference to their previous blocks, which form a chronological chain in a cyber-secure manner.

The blockchain-based database is replicated and distributed throughout the blockchain network for sharing and synchronizing data records among MCs and DSO. All nodes in the blockchain network would provide their consensus whenever a set of new data would be stored in the blockchain-based database. A chosen node (i.e., miner) would then be in charge of packaging the data into an encrypted block, adding them to the end of the current blockchain, and broadcasting such a state change in the blockchain network. Each node continuously receives the information on any state changes, verifies the changes based on pre-specified mechanisms, implements the changes on its own copy of blockchain if validated, and communicates with peers randomly for notifying the validated changes. Accordingly, all nodes in the blockchain network will hold an up-to-date copy of blockchain.

3.2. Cryptographic techniques in blockchain applications

As implemented with cryptographically-secure techniques, data records in the form of blockchain are guaranteed to be immutable, verifiable, and auditable. The one-way hash function guarantees in theory that it is computationally impractical to modify data records in the blockchain network due to the interlinking nature of hashes. Any tampering with a local copy of blockchain can be easily detected by only checking the last data block. Any changes in the original content of an existing block would result in significant and uncorrelated changes in cryptographic identifications of target blocks along with all subsequent blocks (e.g., hashes in their headers). Recall that blockchain is a distributed database jointly maintained by all nodes in the blockchain network (i.e., MCs and DSO). Even if attackers manage to change, falsify, or delete the content of a block in a copy of blockchain by regenerating all the related cryptographic identifications, their suspicious behavior can be easily flagged and identified by the difference with a commonly-acknowledged copy of blockchain that is maintained by other nodes in the blockchain network.

Distributed data storage eliminates the threat of single-point-of-failure in the blockchain network in contrast to conventional database architectures coordinated by a trusted central intermediary (see Fig. 6(a)). The blockchain network with inherent redundancy is so fault-tolerant that faulty communication links, caused by denial-of-service attack (Moore et al., 2006), or compromised MCs, caused by man-in-the-middle attack (Callegati et al., 2009), can hardly change the universal agreement on the blockchain network state (represented by an authentic copy of blockchain). Accordingly, the blockchain network gains strong self-healing capabilities for ensuring the authenticity of recorded contents as long as a certain number of MCs (which depends on the consensus protocol) are trustworthy.

Blockchain is further protected by asymmetric cryptography. Each DSO and MC maintains a pair of public and private keys to interact with other nodes in the blockchain network for the purposes of encrypting and decrypting data records in transactive energy management. The public key as a publishable identifier makes sure that the pertinent market participant is addressable in the blockchain network, and all other market participants can access the public key. Conversely, the private key is only held by the participant, which can seldom be identified based on the prior knowledge of the public key. Each participant uses its private key as a digital signature to approve any new data that are to be recorded on blockchain. Then, other market participants can validate the data authorization via the participant's public key before the miner adds it to blockchain. In addition, each participant can share sensitive data with any other participant by using the target participant's public key to encrypt the data block; the target participant can decrypt the data record with its own private key. Hence, the blockchain network maintains a publicly verifiable and auditable proof of transactive energy system operations, in which market participants would interact faithfully even in the event of a previous mistrust.

3.3. Smart contracts in blockchain applications

Smart contracts are considered the silver bullet for automating effective and secure interactions among market participants in the blockchain-based transactive energy system. Fundamentally, smart contracts are a set of pre-defined rules implemented as blockchain-based self-executable scripts (Bhargavan et al., 2016). Each smart contract that is designated with a unique address in the blockchain network can function automatically according to clearly-defined specifications (e.g., participants to be involved, events or times to take effect). Smart contracts offer a great potential for developing specialized applications that operate autonomously and immutably for optimizing the transactive energy management, when all nodes in the blockchain network have access to a cryptographically verifiable trace pertinent to the execution of these applications. In this sense, the blockchain network serves as a dependable solution to tackle data storage and exchange challenges in the transactive energy system, where smart contracts are operated as self-enforcing programs for automating transactive energy management (Papadimitriou, 2003). Smart contracts can even be coordinated with other off-blockchain resources (e.g., solver, cloud, Internet) for completing complicated, cost-effective and dependable tasks that emerge in the transactive energy management. Hence, the transactive energy system should take full advantage of smart contracts to instill operational intelligence in the retail market and enforce market rules to trustless transacting microgrids.

Examples of blockchain development frameworks, which support smart contracts, include Ethereum (Wood, 2014) and Hyperledger Fabric (Hyperledger Fabric - Hyperledger, 2019). Similar to ordinary data records residing in blockchain, the logic of smart contracts is strictly enforced by the blockchain network with immutable and irreversible executions. A smart contract, which is executed after being addressed, processes inputs and provides outputs automatically with completely auditable and predictable behavior. The state of the blockchain network is then updated after the execution when smart contract outputs are replicated among MCs and DSO.

4. Application of blockchain technologies in transactive energy systems

Transactive platforms that use blockchain have unique advantages for the efficient and trustworthy execution of local energy transactions (Christidis and Devetsikiotis, 2016; Dorri et al., 2017). However, constrained by the physical properties of power distribution systems, transactive energy management poses strict domain-specific requirements and challenges to the utilization of blockchain technologies. Efforts should thus be invested into making blockchain technologies adaptable to the transactive energy system so that the market participation of networked microgrids and DSO can be recorded automatically and immutably with efficient, sustainable, reliable, and resilient electricity services guaranteed.

4.1. Permissioned blockchain for facilitating transactive energy management

Bitcoin (Nakamoto, 2008) and Ethereum (Wood, 2014) allow user's access without checking its trustworthiness. Such a permissionless (public) characteristic, however, bundles blockchain applications with complex consensus mechanisms (e.g., proof-of-work algorithm (Gervais et al., 2016)) to provide a trusted environment for anonymous users. Design limitations on consensus mechanisms commonly render the addition of new data blocks expensive (in terms of resource consumption) and slow (in terms of computation speed), which hinders public blockchain applications to practical scenarios with high-frequency data recording requirements.

Permissioned (private) blockchain only grants access to verified users with significantly less technology-specific restrictions on data recording. As all users are presumed trustworthy, permissioned blockchain commonly resorts to simple, lightweight consensus mechanisms (e.g., practical Byzantine fault-tolerant algorithm (Androulaki et al., 2018)) instead of energy-intensive, computationally-cumbersome consensus mechanisms. Accordingly, users of permissioned blockchain validate and record data blocks more swiftly with fewer resources. Permissioned blockchain is thus more cost-effective than permissionless blockchain for implementing data storage and exchange applications in the transactive energy system, primarily due to the regulated nature of power systems and strict time requirements on recording operating states. Hence, all the following blockchain applications are pertinent to permissioned blockchain if not specifically mentioned.

The electricity market is more monopolistic than other free markets, which usually set high entry barriers for security considerations. In that regard, potential market participants in the transactive energy system would need to be verified and authorized by a regulatory authority (i.e., DSO) before carrying out decentralized energy transactions. DSO may even automate the permission-issuing functionality via smart contracts in blockchain so as to safeguard the retail market entry without single-point-of-failure concerns. All the permissible market participants are granted access to the blockchain network where they can audit the recorded contents to detect anomalies and frauds in processing the transactive energy system.

To limit financial and physical impacts of careless or malicious market participants, each participant is associated with a reputation score that directly reflects the trustworthiness of its historical electricity trading. After every commonly-acknowledged period, all market participants are assigned an equal reputation score. If a participant's behavior is found to be suspicious according to the complete tracing of transactive energy management, which could be caused by cyberattacks or malicious collusions, the participant would be penalized by lowering its reputation score. In particular, a participant's faulty or compromised energy trading activities, which could be the result of a failure to fulfill energy transfer obligations, would lead to an unfair market equilibrium with reduced social welfare and even the destabilization of the power distribution system. For instance, a significant difference between scheduled and actual power production (or consumption) in a transacting microgrid would lead to unexpected frequency and/or voltage oscillations, with an impact on the distribution system security. When a participant's reputation score is lower than a certain threshold, the participant will be temporally banned from participating in the transactive energy system.

Moreover, networked microgrids transacting in the retail market may be required to deposit a considerable amount of currencies (or cryptocurrencies) as collateral at the beginning of every reputation assignment cycle. At the end of each cycle, all the deposited currencies (or cryptocurrencies) will be returned to market participants in proportion to their final credit scores. Thus, a reduced reputation score would lead to a sizeable reduction in a participant's revenue. That is, the risk of faulty or compromised energy trading activities is expected to be effectively managed, as market participants risk their revenue and reputation for interacting with each other.

Since the set of transacting microgrids is fixed and known in each round of transactive energy management, efficient consensus mechanisms are designed and implemented for facilitating fast and reliable data recording and sharing in the blockchain network. For instance, the following two mechanisms can be deployed by market participants to reach a consensus on the miner for permissioned blockchain: DSO as a single permission-issuing authority can directly serve as the miner; alternatively, a temporary miner could be selected randomly among a small group of transacting microgrids with reputation scores among the top 20% when a microgrid's probability of winning the selection is proportional to its reputation score. In addition, a full knowledge on transacting microgrids' identities eases the development and enforcement of smart contracts that boost the integrity and trustworthiness of automated interactions in the transactive energy system.

4.2. Impact of power delivery characteristics on blockchain applications

Electricity is distinguished from other market commodities by its physical characteristics. As power flows conform to physical laws (e.g., Kirchhoff's laws), technical constraints would limit the flexibility and scalability of energy exchange among transacting microgrids. Accordingly, the decentralized management of energy transactions at the retail market level could be more complicated than peer-to-peer transactions of other market commodities, which could subject the design and the implementation of blockchain-based transactive energy models to domain-specific limitations and constraints in addition to common market rules. Although peer-to-peer transactions are promising, blockchain applications to power systems could be limited by physical constraints. Only when working in concert with physical properties of power distribution systems can blockchain technologies maximize their potential to realize benefits of the transactive energy system. A constrained physical network can make the participants' delivery of traded assets more cumbersome (as illustrated by two cases in Fig. 8). In fact, a line flow is restricted by thermal or stability requirements, which can potentially lead to a power flow congestion. As shown in Fig. 8(a), two microgrids reach an agreement for transacting 20 kW from Microgrid 1 to Microgrid 2 at a certain price. However, the constrained transfer is only 10 kW, even though Microgrid 1 has adequate on-site generation resources.

In addition, the monetization of distribution power loss which is closely tied with individual transactions would also have to be resolved. In Fig. 8(b), the transaction is reduced by 0.5 kW when considering

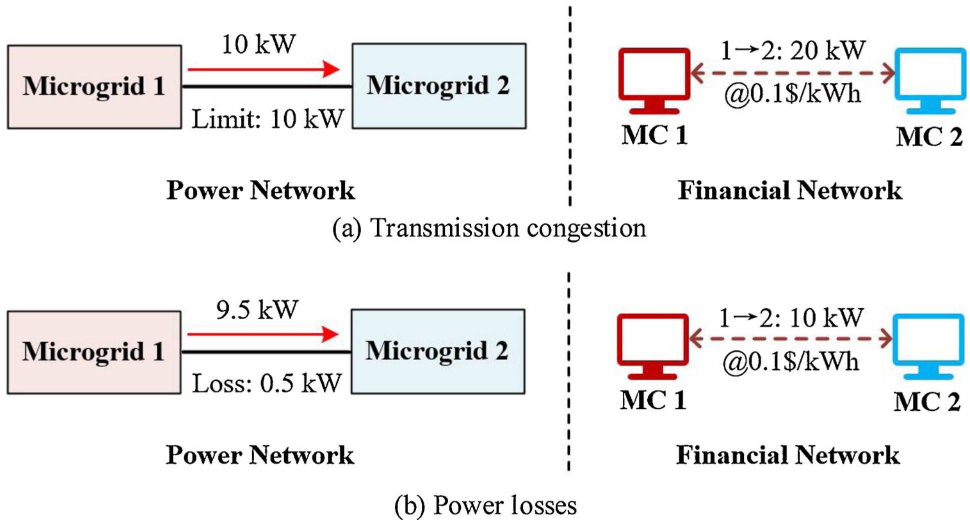

Fig. 8. Physical characteristics of energy trading.

power losses. It would be difficult to calculate individual transaction losses, due to nonlinear power network operations, when such losses are attributed to multiple transactions. The transaction loss calculation becomes more challenging when real-time operating conditions (reactive flows and voltage profiles) are taken into consideration. In practice, the slack bus would be compensating power losses in real time as the power delivery network bridges the gap between power production and consumption. The utility network (interacting with DSO) or a microgrid with adequate energy resources (e.g., storage) could serve as slack bus.

In Fig. 9, Microgrids 1 and 3 transact energy with Microgrids 4 and 2, respectively. Microgrid 3 serves as the slack bus which supplies the extra 5.9 kW for offsetting losses along the four lines; the extra energy supplied by Microgrid 3 would be monetized by the other three microgrids. However, as depicted in Fig. 9, there is no actual flow from Microgrid 1–4, and the energy to Microgrid 4 is supplied only by Microgrid 3, when Microgrid 1 partially supplies Microgrid 2. Such an inconsistency between actual flows and pre-signed energy transactions further complicates the attribution and monetization of power losses. Although the transactive market is designed with plug-and-play capabilities that enable the trading among specific networked microgrids, it is imperative to satisfy power network constraints for maintaining efficient and secure electricity services.

In Fig. 10, Microgrids 1 and 3 participate in the transactive market while the other two microgrids function as self-sustained entities; Microgrid 3 serves as the slack bus to supply losses. When the lines that interconnect Microgrids 2 and 4 to the other two microgrids are disconnected, the power transfer from Microgrid 1–3 via a 30 kW line will be constrained; the local power network of Microgrids 2 and 4 should maintain a connection with the remaining power distribution system as long as they manage to utilize on-site resources for maintaining a local power balance. Hence, Microgrid 3 will fully supply Microgrid 1 via two parallel paths (i.e., Microgrids 2 and 4 are the enablers of such transfer).

4.3. Existing blockchain applications in power distribution systems

In addition to emerging research on the applications of blockchain technologies in power systems (Basden and Cottrell, 2017; Aitzhan and Svetinovic, 2016; Zizzo et al., 2018), there have already been several industrial pilot projects focusing on peer-to-peer electricity markets. The most well-known peer-to-peer transactions of renewable energy occurred in Brooklyn, New York in April 2016, when residents employed the blockchain platform developed by LO3 Energy (LO3 Energy: The Future of Energy, Blockchain, Transactive Grids, Microgrids, Energy Trading, 2019) to trade with their neighbors the excess power locally generated by solar panels in a decentralized and automatic fashion (Papadimitriou, 2003). Similarly, Power Ledger has implemented the peer-to-peer electricity trading system to transact the excess solar energy flexibly and automatically based on the proprietary blockchain platform and existing electricity meters (PowerLedger Token Generation Event, 2019; Power Ledger & Clean Energy

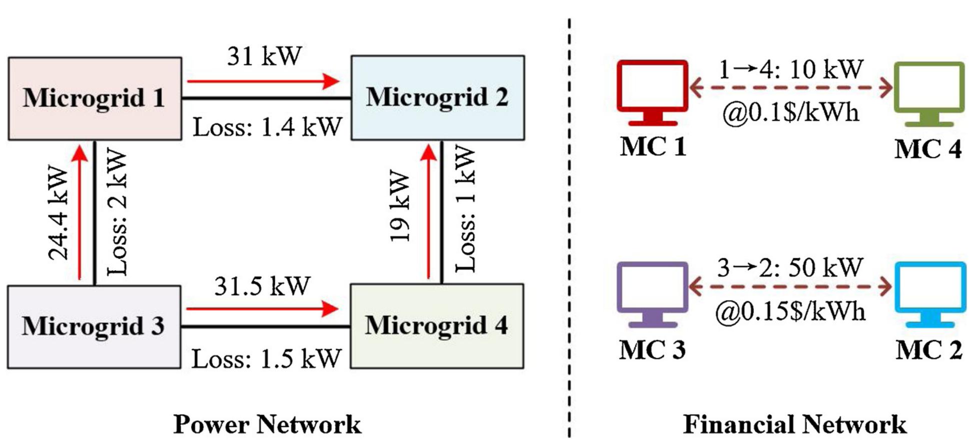

Fig. 9. Microgrid as a slack bus for compensating power losses.

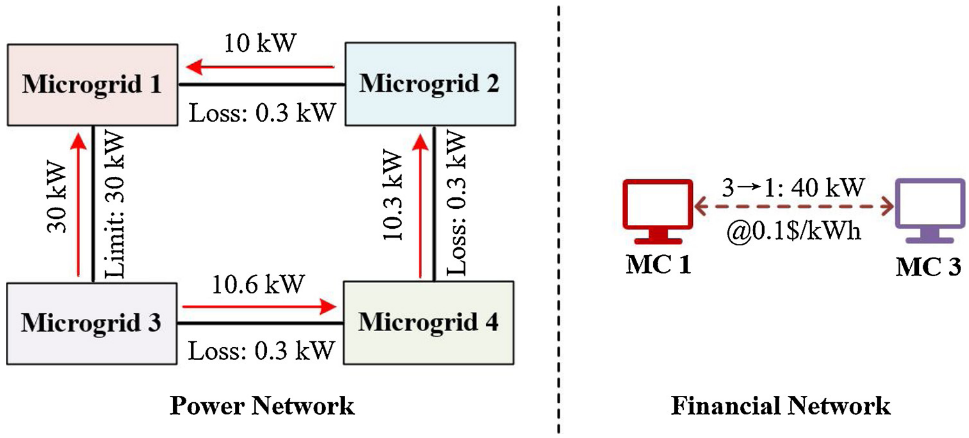

Fig. 10. Enforcement of microgrid connections for improving transaction security.

Blockchain Network Partner With Northwestern University For First Commercial Deployment In United States, 2019).

There is also a trend to extend the concept of blockchain-based intelligent energy systems beyond its implementation of decentralized energy trading at the building level. (Grid Singularity (2019)) applies blockchain technologies to a unified energy management platform that hosts a wide range of smart grid applications from electricity trading optimization for improving prosumers' earnings to field device monitoring for prolonging the equipment life. The Energy Web Foundation (The Energy Web Blockchain, 2019) builds a blockchain-based industry platform to meet a variety of regulatory, operational, and market needs in the energy sector with the ultimate goal of boosting the DER penetration. Also, cryptocurrencies specific to power systems are introduced to incentivize the DER investment at customer sites. NRGCoin (NRGcoin, Smart Contract for green energy, 2019) and (SolarCoin (2019)) are two cryptocurrencies designed for rewarding renewable energy generation. Users obtain cryptocurrencies for feeding the local renewable energy back to the utility grid (e.g., $1 SolarCoin for 1 MW h of renewable energy generation) and monetize them in an open currency exchange market.

The examples demonstrate that blockchain technologies can accelerate the transition to more decentralized and decarbonized power systems. However, additional research would be needed to explore the scalability and practicality of these technologies for optimizing and securing the transactive energy system.

5. Transactive energy management process based on blockchain technologies

The decentralized blockchain framework for transactive energy management is detailed in this section. A set of interoperable blockchains are the epitome of coupled management of energy and financial flows, while the execution of self-enforcing smart contracts attempts to replace uncertainty with transparency in the management process. The proposed framework merges the merits of DSO-centric top-down regulation and bottom-up microgrid automation process, which removes barriers to presenting more decentralized and secure operations of a power distribution system.

5.1. Interoperable blockchains for transactive energy management

Fig. 11 shows a blockchain-based framework for the transactive energy system, which follows the wholesale market experience. The transactive energy management is divided into four stages. At the first stage (market initialization), DSO configures the underlying power network for energy transactions and adjusts the list of networked microgrids which can physically participate in energy trading (according to their reputation scores). At the second stage (energy trading), market participants submit generation offers and consumption bids (including DSO which exchanges energy with the utility network) for market clearing (transaction prices and quantities). At the third stage (state estimation), market participants exchange their on-site information (operating states at participants' physical boundaries) for estimating the system operating state for energy transfers in the constrained power network. At the last stage (market settlement), market participants settle committed transactions for any differences between the committed generation and actual energy transfers.

Transactive energy management at four stages in the proposed framework involves a heterogeneity of data originated from various sources, including networked microgrid properties (e.g., topological relation) validated and published by DSO at the first stage; Market participants' bids and offers submitted periodically and the corresponding market clearing results at the second stage; real-time metering data collected by smart meters, phasor measurement units (PMUs)) and the corresponding state estimation results at the third stage. Finally, market participants' payments and revenues along with financial settlement anomalies (if any) are managed at the fourth stage. The creation and maintenance of records using such heterogeneous data could be problematic when they are generated in multiple timescales and used in transactive energy management on a single blockchain. Instead, multiple blockchains working in tandem are designed and deployed for automating the transactive energy management and securing a complete log of market operations.

In Fig. 11, the proposed framework utilizes four permissioned blockchains, each belonging to a class of data used for a specific purpose. These blockchains embedded with specially-designed smart contracts achieve distinct objectives requested by the transactive energy management. The market initialization blockchain considers power network configuration and market rules (e.g., access control) for energy transactions; the energy trading, state estimation, and market settlement blockchains are responsible for storing transactional, operational, and financial information involved in the subsequent management process, respectively. Collectively, the four blockchains provide transformative solutions to the decentralized coordination between non-trusting market participants, the sharing and the storage of energy and financial flows as well as the enforcement and payment of energy transactions.

Given that each blockchain provides an interface for the others to interoperate, the operations of these four blockchains are closely coordinated in the following manner. The market initialization blockchain requests reputation scores of transacting microgrids from the market settlement blockchain for screening out these non-eligible ones in the market; the energy trading and statement blockchains obtain the pseudonym of each transacting microgrid along with the power

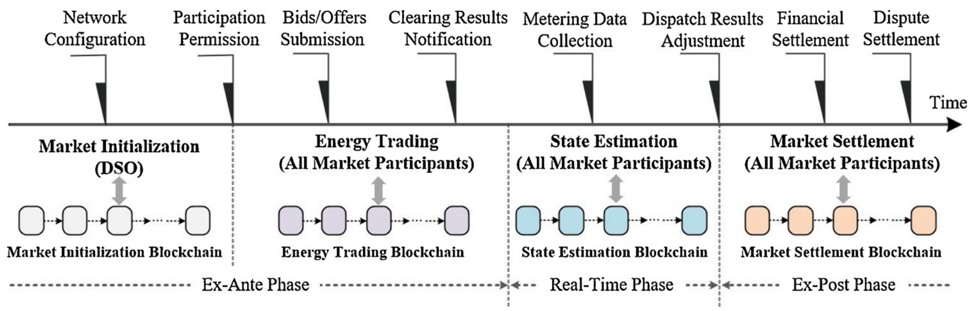

Fig. 11. Blockchain-based transactive energy management framework.

network configuration from the market initialization blockchain for determining scheduled and actual energy transfers, respectively, and also poll participants' reputation scores recorded on the market settlement blockchain for determining the miner in charge of blockchain extensions; the market settlement blockchain asks the energy trading and state estimation blockchains for scheduled and actual amounts of energy transactions, respectively, in order to determine each participant's payment or revenue as well as the change in its reputation score.

5.2. Blockchain operations in the ex-ante phase

5.2.1. Market initialization process

As the power network underpins energy transactions in networked microgrids, a deterministic (fixed) network configuration facilitates the transactive market clearing and contributes to the overall efficiency and security of electricity services. In each round of transactive energy management, DSO strategically determines and subsequently fixes the network configuration using the experts' knowledge or machine learning techniques applied to historical configurations, while meeting the following considerations: excluding network components with forced and planned outages; ensuring the quality of electricity services (e.g., proper frequency and voltage profiles); and maximizing environmental and economic benefits (e.g., reduced power losses).

It is mandatory for individual microgrids to register with DSO prior to participating in the transactive energy system. In order to preserve the market participants' privacy, DSO assigns each transacting microgrid with a randomly-generated pseudonym that temporarily obfuscates the microgrid's identity. These microgrids perform pseudonymous trading, which effectively reduces the possibility of linking exposed trading patterns and financial gains to individual microgrids' identities. Additionally, each transacting microgrid' pseudonym is unbundled from its reputation score which is recorded along with its actual identity to conceal the actual identities when making the reputation score public for mining purposes.

Fig. 12 shows the process of market initialization based on blockchain technologies. DSO appends the market initialization blockchain for broadcasting initial market settings, and microgrids access the blockchain for attaining pseudonyms and topological locations. Note that the shared information is secured by asymmetric cryptography when DSO encrypts sensitive settings pertinent to each transacting microgrid by using the microgrid's public key. The microgrid then uses its private key to perform decryption. In Fig. 12, each microgrid is informed about its pseudonym (e.g., $0 \times 8f1$ for Microgrid 1) and its location in the pseudonym-based power network at the end of the market initialization process.

5.2.2. Energy trading process

DSO provides market participants with economic signals to aggregate networked microgrids in the electricity wholesale market for minimizing the energy transaction costs. Each market participant considers the price signal and the historical market data corresponding to other market participants' behavior to calculate its bidding strategy and provide it to DSO, which clears the market for achieving a transactional consensus. All submitted bids and offers, regarded as static during the clearing process, are stored in the energy trading blockchain to avoid tampering.

Fig. 13 illustrates the bidding process in blockchain, where the DSO's trade with the bulk power system is neglected for the ease of representation (i.e., energy transactions correspond to the three microgrids). Each participant approves its bidding strategy by using its private key before interacting with the blockchain. Considering the potential asynchronization in practical applications, market participants could resort to a two-step approach (Hahn et al., 2017) for submitting bids and offers. More specifically, market participants submit encrypted bids and offers separately at the first step and continue to decrypt the submitted bids and offers after a pre-defined period at the

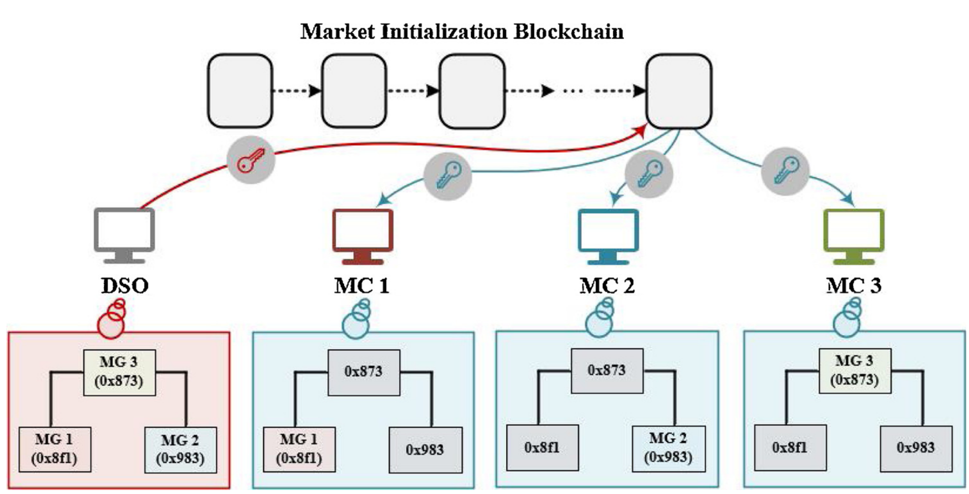

Fig. 12. Blockchain-enabled market initialization process.

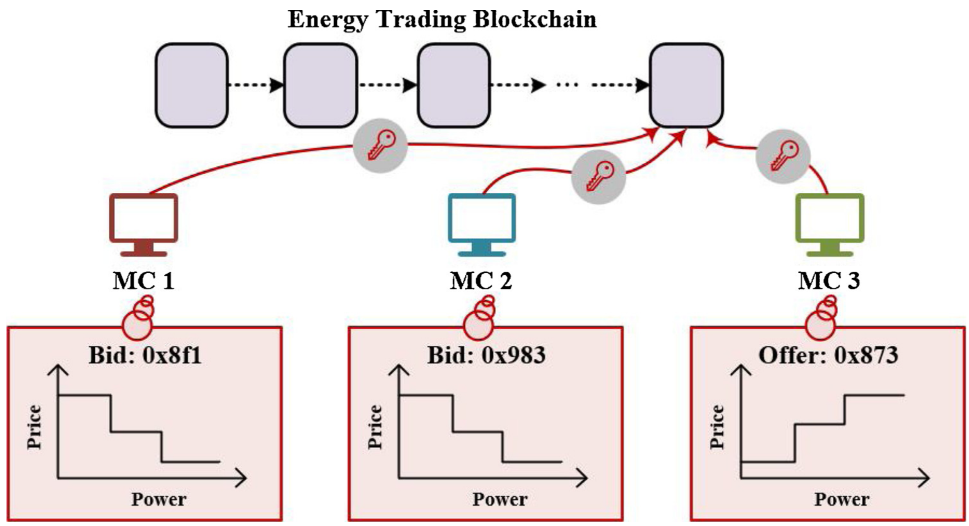

Fig. 13. Blockchain for the market bidding process.

second step. Even though the participants do not reveal their bids and offers simultaneously at the second step, the risk of exposing bids and offers to individual's peers ahead of time is effectively reduced as bids and offers stored in the blockchain at the first step cannot be modified.

Once all bids and offers are collected and revealed, DSO determines quantities and prices for energy trades in a decentralized manner considering the network operation constraints. The market clearing process is formulated as a decentralized security-constrained optimal power flow (DSCOPF) problem (Liu et al., 2017; Feng et al., 2018). The solution process features individual participant's decentralized and autonomous decisions in an iterative process which is presented as follows. Each microgrid solves a local DSCOPF problem at each iteration and the results are passed on to smart contracts that execute the aggregation step (e.g., return the average value of any coupling variable collected from neighboring microgrids) for evolving locally optimal decisions to a global equilibrium for scheduled energy transfers. Upon convergence, each participant receives the energy price specific to its location, which is principally the marginal cost to serve an incremental unit of power demand at that location. Eventually, all quantities and prices of scheduled energy transfers are recorded on the energy trading blockchain. Fig. 14 illustrates the blockchain for the market clearing process, when the three microgrids interact via smart contracts for achieving the decentralized energy coordination with a consensus on scheduled energy transfers.

5.3. Blockchain operations in the real-time phase

During the period when committed energy transactions are carried out, each market participant is required to continuously collect field device measurements (including a host of advanced wireless sensors, smart meters, and PMUs) and share the measured or estimated operating states at the boundary of its physical territory via the state estimation blockchain. Since the blockchain keeps track of operating states, the risk of data integrity attacks (e.g., falsify and mislead power system operations) is effectively reduced during the data sharing process. Besides, the sharing of boundary operating states contributes to the consensus on actual energy transfers, when market participants collaborate on the decentralized state estimation (DSE) (Tai et al., 2013; Minot et al., 2015) using smart contracts.

The DSE procedure is iterated as follows. Each participant relies on

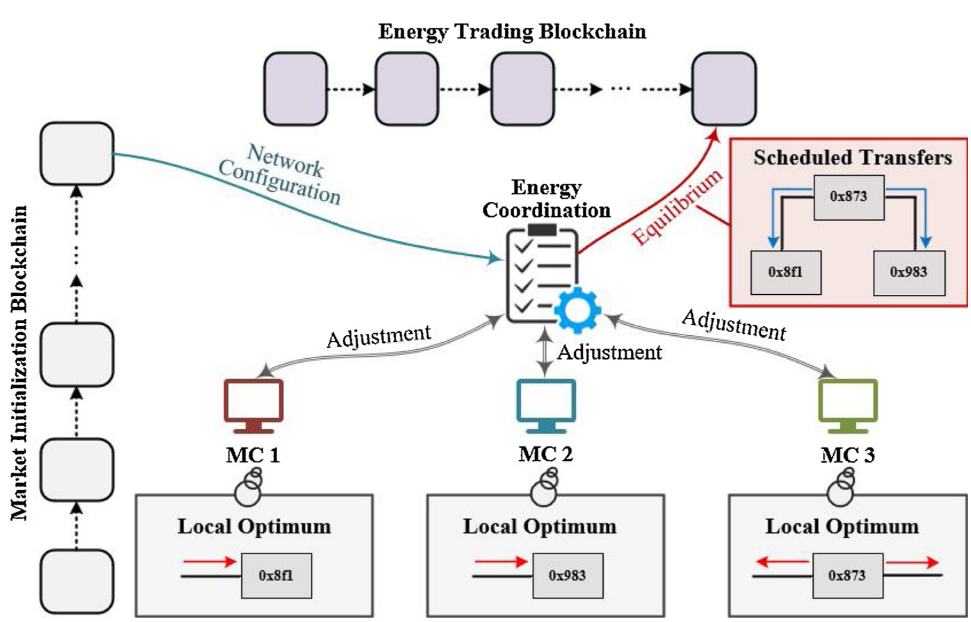

Fig. 14. Blockchain for the market clearing process.

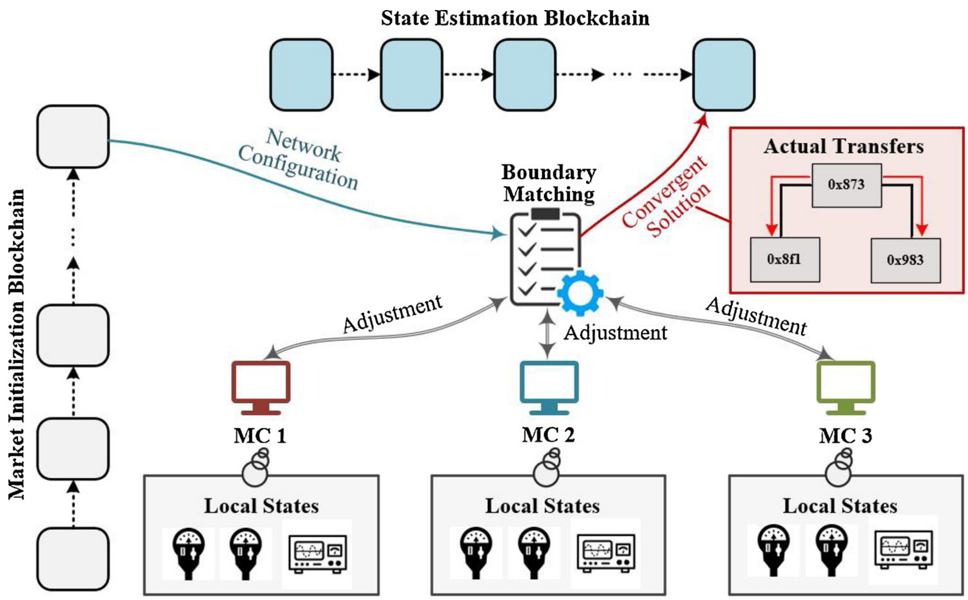

Fig. 15. Blockchain for the state estimation process.

on-site measurements and boundary operating states (i.e., voltage magnitudes and phase angles) provided by its neighbors to calculate the local state estimation at each iteration. Smart contracts with an access to the network configuration, which is recorded on the market initialization block, adjust boundary operating states shared by two neighboring participants so that their boundary operating states are matched in a finite number of iterations. Upon convergence, local estimates will be integrated seamlessly to form a complete operating state associated with tie lines connecting individual participants. Accordingly, steady-state energy transfers across the power network can be extracted from converged estimated states which will be stored on the state estimation blockchain. Fig. 15 illustrates the blockchain for the state estimation process, when the three microgrids interact via smart contracts to reach a consensus on actual energy transfers, as their boundary operating states are matched.

5.4. Blockchain operations in the ex-post phase

After state estimation results become available, financial settlements are made automatically via smart contracts. A participant's payment or revenue in terms of cryptocurrency (e.g., Bitcoin or Ether) is determined based on its energy transfer reflected in state estimation results. In an ideal case, all participants will trade energy as scheduled and payments/revenues are presented as the product of the scheduled power and the corresponding locational marginal price (as recorded on the energy trading blockchain), which are the same as their expected financial gains. However, transfer amounts could deviate from the commitments considering a variety of uncertainties (e.g., generation or load variations) affecting transactive system operations, when market participants would pay additional fees for compensating the balancing quantity. In this case, the difference is balanced by either a power exchange with the utility network or a power adjustment at the slack-bus microgrid, charged at a penalty price equal to the highest locational marginal price recorded in the energy trading process at the current round of transactive energy management. The DSO's net positive financial gain is invested on the distribution power grid expansion or shared among market participants in proportion to their reputation scores. When the energy transfer difference is outside a pre-defined threshold, the participant will be penalized by reducing its reputation score. If there is a dispute in the financial settlement, DSO will intervene by scrutinizing the recorded track of transactive energy system operations.

The results of financial settlement as well as the changes in participants' reputation scores are recorded in the market settlement blockchain. Noticeably, recorded payments and revenues are associated with pseudonymous identities to preserve the privacy of market participants' financial assets that would be used for inferring actual identities and pertinent trading behaviors. On the contrary, reputation scores are recorded by linking them to their actual identities to fend off malicious market participants while facilitating the selection of miners in charge of blockchain extensions. Market participants are also allowed to poll their current balance encrypted by their public keys and perform decryption by using their private keys. Fig. 16 illustrates the blockchain for the market settlement process, where the three microgrids are notified about financial gains and reputation scores of all participants as well as their own balance after the financial settlement.

6. Cyber-physical security of blockchain-based transactive energy management

Transacting microgrids enclose a host of communication and control devices that are normally manufactured by different vendors, giving rise to various unexpected cybersecurity vulnerabilities (Li et al., 2017b). The malicious exploitation of these cybersecurity vulnerabilities may result in a malfunctioning transactive energy system, and even widespread outages in the power distribution system. Possible cyberattacks include tampering with operation data in metering devices, maliciously altering the pricing and quantity of energy bids and offers, and remotely manipulating field devices. Although the application of common blockchain technologies lays the foundation for distributed and cyber-secure data storage and management, additional cybersecurity enhancement measures are to be identified to realize the merits of the decentralized transactive energy management framework while achieving the defence-in-depth goal against increasingly sophisticated cyberattacks.

6.1. Security-oriented smart contracts

Smart contracts are powerful tools against potential exploitations of cybersecurity vulnerabilities in the transactive energy system. Especially, networked microgrids could rely on smart contracts for maintaining and updating the firmware and software involved in their operations that will overcome cybersecurity vulnerabilities in a credible and automatic manner. In fact, networked microgrid share a similar set

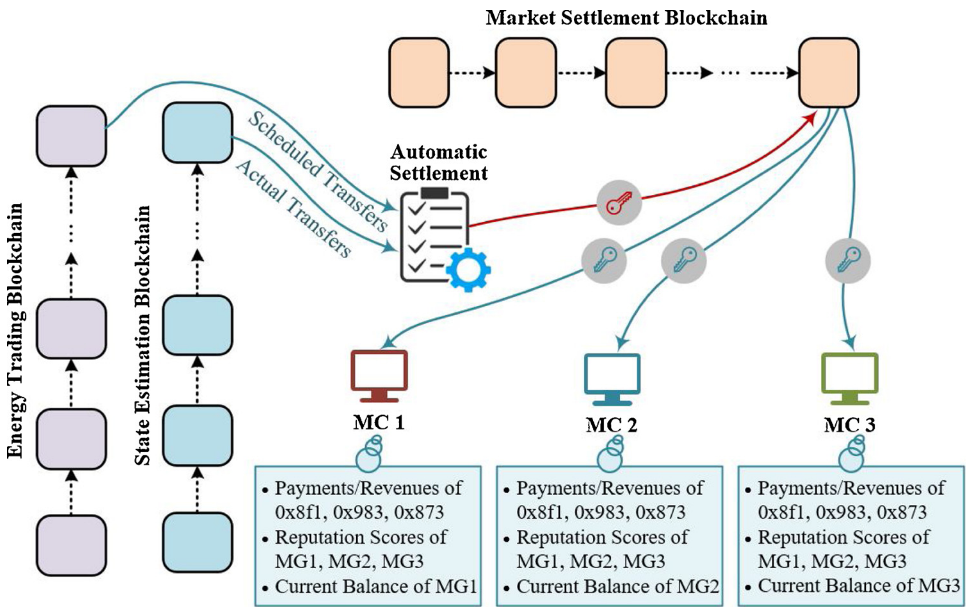

Fig. 16. Blockchain in the market settlement process.

of field devices (e.g., smart meters, smart inverters (Ghiani and Fabrizio, 2015)) and thus a dedicated database can be configured on a blockchain (e.g., market initialization blockchain) for keeping track of properties (e.g., vendor, model, version) and solutions (e.g., updates, patches) for potential cybersecurity vulnerabilities. Once a cybersecurity vulnerability is discovered in a microgrid and stored on blockchain, other microgrids exposed to the same vulnerability will be notified by the related smart contracts to seek a remedial solution. Once a proper vulnerability solution is determined, the smart contracts will store it on blockchain for ensuring its integrity and trigger all the pertinent microgrids to implement the solution. If a vulnerable microgrid fails to implement the solution, the smart contracts will mark the microgrid as a potential cyberattack target, lower its reputation score by a penalty, and potentially exclude it from the transactive energy system. Hence, all the discovered vulnerabilities can be assessed and patched promptly and faithfully with the help of smart contracts.

Additionally, smart contracts can be employed to alleviate the risk of zero-day cybersecurity vulnerabilities (i.e., existing ones that were previously unknown). Currently, the programming language for smart contracts (e.g., Solidity (Solidity 0.4.25 documentation, 2019)) lacks the built-in capability to support advanced arithmetic operations (even floating-point calculation) so that a high-performance external solver is considered to solve computationally expensive mathematical problems (e.g., DSCOPF, DSE). However, such computations without blockchain will fail to ensure the auditability and immutability of the solution process, especially in cyberattacks (e.g., denial-of-service) on the solvers. Accordingly, smart contracts are considered to monitor the solution process and validate the solutions before recording them on blockchains (e.g., energy trading blockchain, state estimation blockchain).

The formulation of each complicated mathematical problem solved for the transactive energy management is required to be recorded on the pertinent blockchain, when the related smart contracts request the invoked solvers to submit candidate solutions periodically during the solution process. Then, the smart contracts verify the feasibility of each submitted solution by checking if it satisfies all equations contained in the mathematical problem and choose the best one among the validated candidate solutions for further decision-making. Eventually, the smart contracts implemented in such computationally-inexpensive tasks make full use of external solvers that would potentially be subject to zero-day cyberattacks while retaining the trustworthiness of blockchain technologies.

6.2. Cyber-physical security evaluation testbed

Theoretically, the proposed transactive energy management framework facilitates the decentralized optimization of energy and financial flows in a scalable and secure manner. However, a testbed simulation is needed to check the validity of the framework, especially its cyber-physical security, before any practical implementations. Fig. 17 shows the proposed setup for evaluating the blockchain cyber-physical security for the transactive energy management, where three Ethernet-connected computers deployed with the proposed modular simulation platform represent three autonomous microgrids posed for energy trading. In the modular platform, the simulations of the power distribution system, the control and communication system, and the

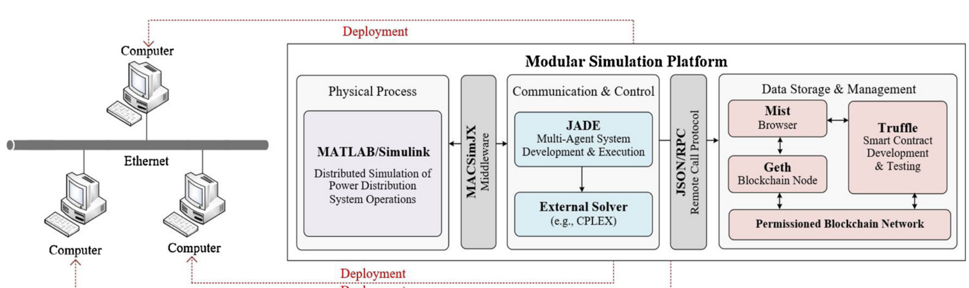

Fig. 17. Simulation setup for cyber-physical security evaluation.

blockchain for the database are performed and synchronized in a cost-effective manner.

As market participants involved in the transactive energy system possess distinct motivations and functionalities, their interactions can be automated based on a multi-agent system (MAS). Essentially, each market participant is identical to a specific agent with inherent intelligence that automatically adapts its trading behavior to dynamic market conditions. In MAS, various types of agents are engaged in behavioral interactions, communications, and run-time collaborative decision making for achieving a pre-specified common goal. The Java Agent Development Framework (JADE) (Bellifemine et al., 2000) provides a cost-effective platform for designing and deploying MAS and enables the co-simulation with MATLAB/Simulink (MATLAB, 2016) via a middleware called MACSimJX (Robinson et al., 2010). Accordingly, the distributed, high-fidelity simulation of power distribution system operations can be carried out in MATLAB/Simulink for investigating physical implications of potential cyberattacks on the MAS-based communication and control system dedicated for transactive energy management. Commercial solvers such as CPLEX could also be externally invoked by JADE for strengthening the decision-making functionality of each agent deployed in MAS.

MAS is integrated with the blockchain network for data management and storage through JSON/RPC (JSON-RPC 2.0 Specification, 2019). Note that JSON is a lightweight data-interchange format for facilitating agents' interactions with the blockchain. Four permissioned Ethereum blockchains are configured with enhanced interoperability, when smart contracts are developed and tested in a common development environment called Truffle. Truffle offers unique advantages for deploying smart contracts and high-level abstractions for interacting with deployed smart contracts (Truffle Suite - Your Ethereum Swiss Army Knife, 2019). Truffle provides a customizable blockchain emulator called Ganache (previously called TestRPC) which boosts the efficiency of developing and testing smart contracts as it allows the interaction of the blockchain without utilizing the overhead of running an actual Ethereum node.

Each agent is a member of the blockchain network after it is configured with a Go-based Ethereum node (Geth) for communicating with its peers (Go Ethereum, 2019). Meanwhile, the dynamic performance of the blockchain network can be easily observed in Mist (Mist. Browse and use Ðapps on the Ethereum network, 2019) which is a sophisticated browser supporting the wallet function for making automatic payments along with a detailed view on the running of deployed smart contracts. Accordingly, any suspicious behavior on the blockchain could be easily detected from monitoring results on the browser.

7. Conclusions

Power distribution systems have been undergoing significant changes driven by a collection of dynamic forces for power grid modernization. Modern power distribution systems will signify an ideal platform for adopting innovative and flexible solutions that contribute to the smart grid mandates. The widespread implementation of networked microgrids plays a critical role in shaping the landscape of power distribution systems while challenging the feasibility of conventional utility-based regulation paradigms.

Transactive energy, as the cross-section of technological, political and economic innovations, opens up the door to a new type of autonomous electricity retail markets together with new business and operation models of power generation, delivery, and consumption. Through active participation in the decentralized transactive energy management process, networked microgrids collectively provide additional opportunities for improving the operational performance of power distribution systems. As networked microgrids are intrinsically cyber-physical systems that may unintentionally expose cybersecurity vulnerabilities to potential disruptive agents, blockchain provides a transformative solution to address the cybersecurity and mutual-trust concerns through the application of cryptography and the execution of smart contracts. Accordingly, networked microgrids interact in an automatic, credible and auditable manner for maintaining a greater degree of efficiency, reliability, resilience, and sustainability in electricity services offered to local communities.

The proposed blockchain-based framework for decentralized transactive energy management is expected to pave the way to the optimization of energy and financial flows in the transition toward active distribution networks. Accordingly, networked microgrids leverage sophisticated information and operation technologies to tap the full potential of DERs which empower customers in a more proactive, secure, and environmentally-friendly manner. Given the tightly-coupled operation of critical energy carriers (e.g., electricity, natural gas, heat, water), networked microgrids are evolving toward a network of energy hubs that integrate the production, consumption and storage of multiple energy forms in local communities. The proposed framework would also establish the foundation for enforcing trustworthy interactions between electricity and other energy sectors in order to achieve the maximum social welfare for energy delivery.

References

Aitzhan, N.Z., Svetinovic, D., 2016. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secur. Comput.

Androulaki, E., et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference. pp. 30.

Basden, J., Cottrell, M., 2017. How utilities are using blockchain to modernize the grid. Harv. Bus. Rev.

Bellifemine, F., Poggi, A., Rimassa, G., 2000. Developing multi-agent systems with JADE. Intelligent Agents VII Agent Theories Architectures and Languages. Springer, pp. 89–103.

Bhargavan, K., et al., 2016. Formal verification of smart contracts: short paper. Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. pp. 91–96.

Callegati, F., Cerroni, W., Ramilli, M., 2009. Man-in-the-Middle attack to the HTTPS protocol. IEEE Secur. Priv. 7 (1), 78–81.

Che, L., Shahidehpour, M., Alabdulwahab, A., Al-Turki, Yusuf, 2015. Hierarchical coordination of a community microgrid with AC and DC microgrids. IEEE Trans. Smart Grid 6 (6), 3042–3051.

Christakou, K., Paolone, M., Abur, A., 2017. Voltage control in active distribution networks under uncertainty in the system model: a robust optimization approach. IEEE Trans. Smart Grid.

Christidis, K., Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303.

Darghouth, N.R., Barbose, G., Wiser, R., 2011. The impact of rate design and net metering on the bill savings from distributed PV for residential customers in California. Energy Policy 39 (9), 5243–5253.

Distributed Generation Buy-All, Sell-All Program, 2019. Distributed Generation Buy-All, Sell-All Program. [Online]. Available:. . [Accessed: 01-May-2018]. https://www.energy.gov/savings/distributed-generation-buy-all-sell-all-program.

Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P., 2017. Blockchain for IoT security and privacy: the case study of a smart home. Pervasive Computing and Communications Workshops (PerCom Workshops) 618–623.

Farzin, H., Fotuhi-Firuzabad, M., Moeini, M., 2016. Enhancing power system resilience through hierarchical outage management in multi-microgrids. IEEE Trans. Smart Grid 7 (6), 2869–2879.

Feng, C., Li, Z., Shahidehpour, M., Wen, F., Liu, W., Wang, X., 2018. Decentralized short-term voltage control in active power distribution systems. IEEE Trans. Smart Grid 9 (5), 4566–4576.

Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S., 2016. On the security and performance of proof of work blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 3–16.

Ghiani, E., Fabrizio, P., 2015. Smart inverter operation in distribution networks with high penetration of photovoltaic systems. J. Mod. Power Syst. Clean Energy 3 (4), 504–511.

Gilbert, H., Handschuh, H., 2003. Security analysis of SHA-256 and sisters. International Workshop on Selected Areas in Cryptography. pp. 175–193.

Go Ethereum, 2019. Go Ethereum. [Online]. Available: https://geth.ethereum.org/. [Accessed: 01-May-2018].

Grid Singularity, 2019. Grid Singularity. [Online]. Available:. http://gridsingularity.com/.

Hahn, A., Singh, R., Liu, C.C., Chen, S., 2017. Smart contract-based campus demonstration of decentralized transactive energy auctions. 2017 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. ISGT 2017.

Hyperledger Fabric - Hyperledger, 2019. Hyperledger Fabric - Hyperledger. [Online]. Available:. . [Accessed: 01-May-2018]. https://www.hyperledger.org/projects/fabric.

Jin, D., Li, Z., Hannon, C., Chen, C., Wang, J., Shahidehpour, M., Lee, C.W., 2017. Toward

a cyber resilient and secure microgrid using software-defined networking. IEEE Trans. Smart Grid 8 (5), 2494–2504.
JSON-RPC 2.0 Specification, 2019. JSON-RPC 2.0 Specification. [Online]. Available:. . [Accessed: 01-May-2018]. http://www.jsonrpc.org/specification.
Khodayar, M.E., Manshadi, S.D., Vafamehr, A., 2016. The short-term operation of microgrids in a transactive energy architecture. Electr. J. 29 (10), 41–48.
Koutsoukis, N.C., Siagkas, Di.O., Georgilakis, P.S., Hatziargyriou, N.D., 2017. Online reconfiguration of active distribution networks for maximum integration of distributed generation. IEEE Trans. Autom. Sci. Eng. 14 (2), 437–448.
Li, H., Lu, R., Zhou, L., Yang, B., Shen, X., 2014. An efficient merkle-tree-based authentication scheme for smart grid. IEEE Syst. J. 8 (2), 655–663.
Li, Z., Shahidehpour, M., Alabdulwahab, A., Abusorrah, A., 2016. Bilevel model for analyzing coordinated cyber-physical attacks on power systems. IEEE Trans. Smart Grid 7 (5), 2260–2272.
Li, Z., Shahidehpour, M., Aminifar, F., Alabdulwahab, A., Al-Turki, Y., 2017a. Networked microgrids for enhancing the power system resilience. Proc. IEEE 105 (7), 1289–1310.
Li, Z., Shahidehpour, M., Aminifar, F., 2017b. Cybersecurity in distributed power systems," Proc. IEEE 105 (7), 1367–1388.
Li, Z., Shahidehpour, M., Abdulwhab, A., Abusorrah, A., 2018. Analyzing locally coordinated cyber-physical attacks for undetectable line outages. IEEE Trans. Smart Grid 9 (1), 35–47.
Liu, Y., Fan, R., Vladimir, T., 2016. Power system restoration: a literature review from 2006 to 2016. J. Mod. Power Syst. Clean Energy 4 (3), 332–341.
Liu, Y., et al., 2017. Distributed robust energy management of a multi-microgrid system in the real-time energy market. IEEE Trans. Sustain. Energy 3029 (c), 1–11.
LO3 Energy: The Future of Energy, Blockchain, Transactive Grids, Microgrids, Energy Trading, 2019. LO3 Energy: The Future of Energy, Blockchain, Transactive Grids, Microgrids, Energy Trading. [Online]. Available:. . [Accessed: 01-May-2018]. https://lo3energy.com/.
Ma, S., Chen, B., Wang, Z., 2018. Resilience enhancement strategy for distribution systems under extreme weather events. IEEE Trans. Smart Grid 9 (2), 1442–1451.
MATLAB, 2016. MATLAB Version R2016a. The MathWorks Inc., Natick, Massachusetts.
Minot, A., Lu, Y.M., Li, N., 2015. A distributed gauss-newton method for power system state estimation. IEEE Trans. Power Syst. 31 (5), 3804–3815.
Mist. Browse and use Ðapps on the Ethereum network, 2019. Mist. Browse and Use Ðapps on the Ethereum Network. [Online]. Available: https://github.com/ethereum/mist. [Accessed: 01-May-2018].
Moore, D., Shannon, C., Brown, D.J., Voelker, G.M., Savage, S., 2006. Inferring internet denial-of-service activity. ACM Trans. Comput. Syst. 24 (2), 115–139.
Nakamoto, S., 2008. Bitcoin: a Peer-to-peer Electronic Cash System.
NRGcoin, Smart Contract for green energy, 2019. NRGcoin, Smart Contract for Green Energy. [Online]. Available: https://www.nrgcoin.org/. [Accessed: 01-May-2018].
Papadimitriou, C.H., 2003. Computational Complexity. John Wiley and Sons Ltd.
Power Ledger & Clean Energy Blockchain Network Partner With Northwestern University For First Commercial Deployment In United States, 2019. Power Ledger & Clean Energy Blockchain Network Partner With Northwestern University For First Commercial Deployment In United States. [Online]. Available: https://medium.com/power-ledger/power-ledger-clean-energy-blockchain-network-partner-with-northwestern-university-for-first-7daca76914b6. [Accessed: 01-May-2018].
PowerLedger Token Generation Event, 2019. PowerLedger Token Generation Event. [Online]. Available:. . [Accessed: 01-May-2018]. https://powerledger.io/.
Rahimi, F.A., Ipakchi, A., 2012. Transactive energy techniques: closing the gap between wholesale and retail markets. Electr. J. 25 (8), 29–35.
Robinson, C.R., Mendham, P., Clarke, T., 2010. MACSimJX: A Tool for Enabling Agent Modelling With Simulink Using JADE.
Shahidehpour, M., Li, Z., Bahramirad, S., Li, Z., Tian, W., 2017. Networked microgrids: exploring the possibilities of the IIT-Bronzeville grid. IEEE Power Energy Mag. 15 (4), 63–71.
SolarCoin, 2019. SolarCoin. [Online]. Available:. . [Accessed: 01-May-2018]. https://solarcoin.org/en/node/6.
Solidity 0.4.25 documentation, 2019. Solidity 0.4.25 Documentation. [Online]. Available:. . [Accessed: 01-May-2018]. http://solidity.readthedocs.io/en/latest/.
Swan, M., 2015. Blockchain: blueprint for a new economy. O'Reilly Media, Inc.
Tai, X., Lin, Z., Fu, M., Sun, Y., 2013. A New distributed State estimation technique for power networks. 2013 American Control Conference (ACC). pp. 3338–3343.
The Energy Web Blockchain, 2019. The Energy Web Blockchain. [Online]. Available:. . [Accessed: 01-May-2018]. https://energyweb.org/blockchain/.
Truffle Suite - Your Ethereum Swiss Army Knife, 2019. Truffle Suite - Your Ethereum Swiss Army Knife. [Online]. Available:. . [Accessed: 01-May-2018]. http://truffleframework.com/.
Underwood, S., 2016. Blockchain beyond bitcoin. Commun. ACM 59 (11), 15–17.
Wang, H., Huang, J., 2016. Incentivizing energy trading for interconnected microgrids. IEEE Trans. Smart Grid 3053 (c), 1–11.
Wood, G., 2014. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 151, 1–32.
Yuan, W., Wang, J., Qiu, F., Kang, C., Zeng, B., 2016. Robust optimization based resilient distribution network planning against natural disasters. IEEE Trans. Smart Grid 7 (6), 2817–2826.
Zizzo, G., Riva Sanseverino, E., Ippolito, M.G., Di Silvestre, M.L., Gallo, P., 2018. A technical approach to P2P energy transactions in Microgrids. IEEE Trans. Ind. Informatics 3203 (c).

Zhiyi Li received the B.S. degree from Xi'an Jiaotong University, Xi'an, China, in 2011 and the M.S. degree from Zhejiang University, China, in 2014. He is currently pursuing the Ph.D. degree in the Electrical and Computer Engineering Department, Illinois Institute of Technology. His research interests include large-scale system optimization and cyber-physical security in smart grids.

Shay Bahramirad serves as ComEd's Vice President of Engineering and Smart Grid. She holds executive responsibility for the company's vision of the grid of the future, system reliability, engineering, and planning, as well as the development of frameworks for smart grid roadmaps and investment strategies. In her role as IEEE/PES Vice President of New Initiatives and Outreach, Bahramirad oversees the organization's engagement with utilities and policy makers across the globe, and develops the next generation of standards and frameworks, including Smart Cities.

Aleksi Paaso serves as Director of Distribution Planning & Smart Grid at ComEd. In his current role, Paaso is responsible for ComEd's distribution planning activities, distributed energy resource interconnection, as well as Smart Grid technology strategy and project execution. He is a senior member of the IEEE and Technical Co-Chair for the 2020 IEEE PES Transmission & Distribution Conference and Exposition.

Mingyu Yan received the B.S. degree from the College of Electrical Engineering, Zhejiang University, Hangzhou, China, in 2016 and his M.S. degree from Huazhong University of Science and Technology, Wuhan, China in 2018. He is a PhD student at the Robert W. Galvin Center for Electricity Innovation at Illinois Institute of technology. His research interests include power system operation and planning, multiple energy system integration, and power system reliability.

Mohammad Shahidehpour received the Honorary Doctorate degree from the Polytechnic University of Bucharest, Bucharest, Romania. He is a University Distinguished Professor and Bodine Chair Professor of Electrical and Computer Engineering and serves as Director of the Robert W. Galvin Center for Electricity Innovation at Illinois Institute of Technology. He is a member of the US National Academy of Engineering, Fellow of the American Association for the Advancement of Science (AAAS), Fellow of IEEE, and Fellow of the National Academy of Inventors (NAI).