Blockchain Technologies for Smart Energy Systems

Fundamentals, Challenges, and Solutions

©ISTOCKPHOTO.COM/NICO EL NINO

NAVEED UL HASSAN, CHAU YUEN, and DUSIT NIYATO

In this article, we discuss the integration of the blockchain into smart energy systems. We present various blockchain technology solutions, review important blockchain platforms, and describe several blockchain-based smart energy projects in different domains. The majority of blockchain platforms with embedded combination of blockchain technology solutions are computing- and resource-intensive and, hence, are not entirely suitable for smart energy applications. We consider the requirements of smart energy systems and accordingly identify appropriate blockchain technology solutions for smart energy applications. Our analysis can help in the development of flexible blockchain platforms for smart energy systems.

Digital Object Identifier 10.1109/MIE.2019.2940335
Date of current version: 23 December 2019

The Potential for Blockchain Applications

The continuous expansion of smart energy systems for industrial, commercial, and domestic applications presents several new challenges and opportunities [1], [2]. Smart infrastructure (SI), renewable energy sources (RESs), and electric vehicles (EVs) are becoming widespread [3], [4]; energy and carbon trading possibilities are increasing [5]–[7]; and energy management (EM) through demand-response management (DRM) programs is becoming more common

1932-4529/19©2019IEEE

[8], [9]. To take full advantage of various opportunities, it is necessary to understand the requirements of smart energy systems and focus on technologies that might fulfill them.

In recent years, there has been an increased interest in the blockchain and its integration into various application domains. The blockchain is, essentially, a digitally distributed ledger that is maintained and updated by a decentralized network [also called a *peer-to-peer* (*P2P*) *network*] operating according to well-defined protocols [10], [11]. A convergence of several technologies related to network, data, consensus, identity, and automation management is essential for the successful creation and implementation of a blockchain [12]–[16]. In addition, there are also multiple technology solutions in each category. A blockchain has several unique features, such as decentralization, creation of a trustless network (in which nodes can resolve conflicts without a centralized authority), tamperproof data storage, fault tolerance, and auditability. However, the choice of technology solutions has a significant impact on the resulting blockchain features and performance.

The use of the blockchain in smart energy systems is a topic of tremendous research interest because further development of these systems could potentially benefit from the integration of new and innovative technologies. Due to its unique features, the blockchain can facilitate numerous smart energy applications. For example, Figures 1 and 2 depict the blockchain concept and its potential role in two emerging smart energy applications. In Figure 1, blockchain technology is being used to facilitate P2P energy trading (ET). In this application, energy prosumers can trade surplus energy with their neighbors. However, with the introduction of a blockchain, intermediaries and brokers can be eliminated because data recorded on the blockchain are verified by a distributed network of nodes. Automation can be achieved through computer programs called *smart contracts*, which are stored on the blockchain and define the contractual obligations as well as the transfer of assets between peers.

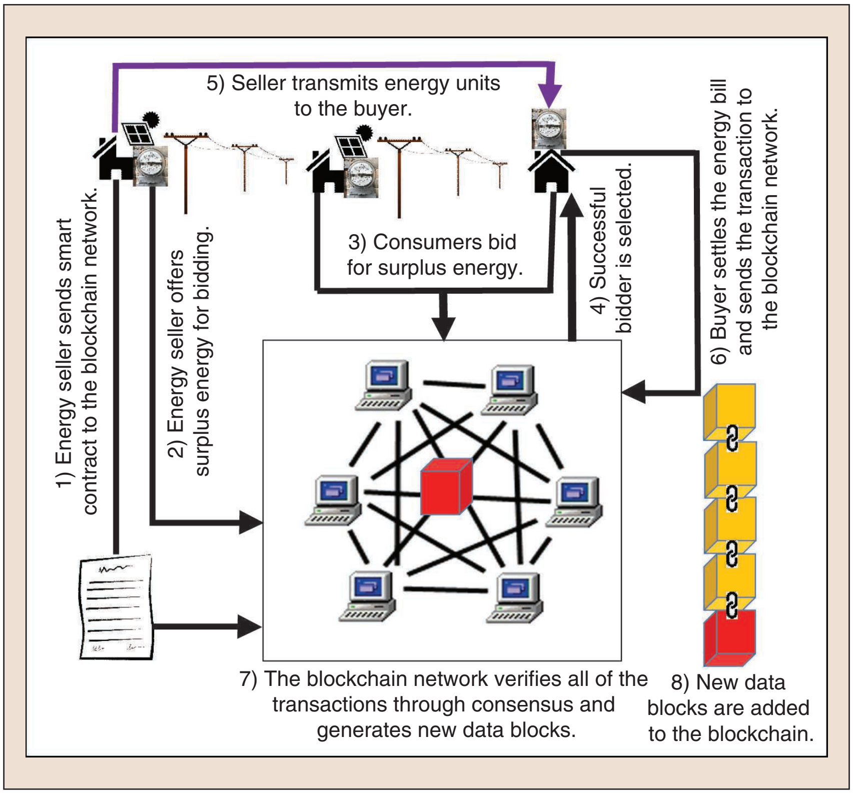
5) Seller transmits energy units to the buyer.
1) Energy seller sends smart contract to the blockchain network.
2) Energy seller offers surplus energy for bidding.
3) Consumers bid for surplus energy.
4) Successful bidder is selected.
6) Buyer settles the energy bill and sends the transaction to the blockchain network.
7) The blockchain network verifies all of the transactions through consensus and generates new data blocks.
8) New data blocks are added to the blockchain.

FIGURE 1 – The P2P ET with the help of the blockchain.

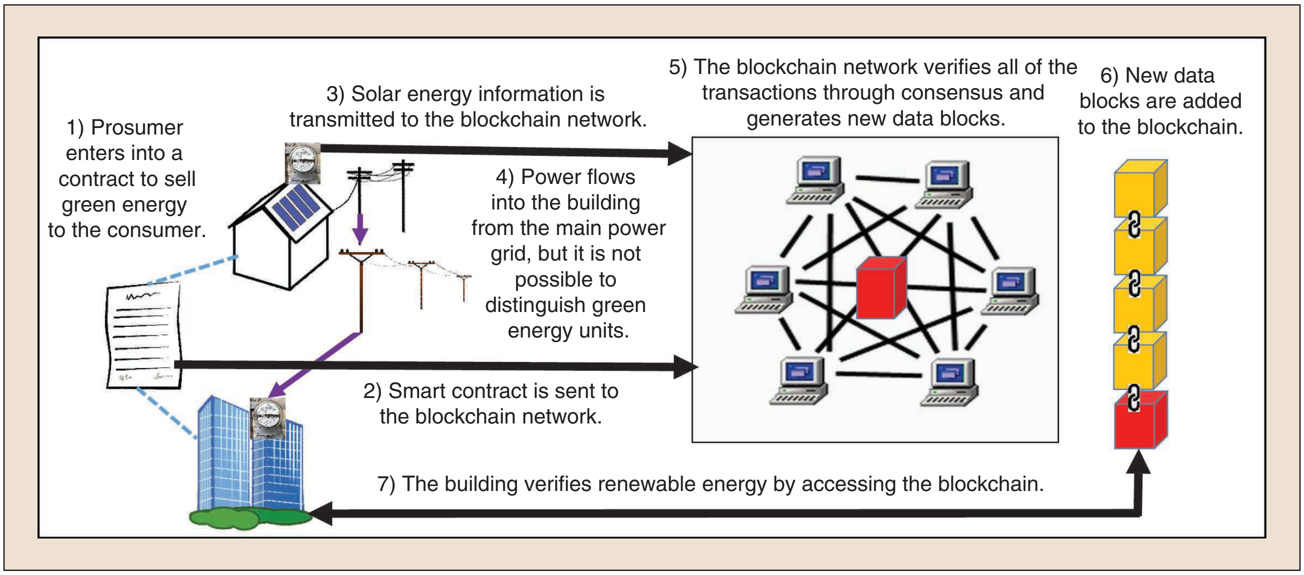
1) Prosumer enters into a contract to sell green energy to the consumer.
3) Solar energy information is transmitted to the blockchain network.
5) The blockchain network verifies all of the transactions through consensus and generates new data blocks.
6) New data blocks are added to the blockchain.
4) Power flows into the building from the main power grid, but it is not possible to distinguish green energy units.
2) Smart contract is sent to the blockchain network.
7) The building verifies renewable energy by accessing the blockchain.

FIGURE 2 – The distributed green EM with the help of the blockchain.

There are several research articles, projects, and ongoing trials that aim to leverage unique blockchain features to advance the digitalization of smart energy systems.

Another application of the blockchain is shown in Figure 2 for the verification of green energy. Once energy is added to the grid, it becomes difficult to distinguish the green energy from traditional energy. However, a consumer can verify the renewable energy generated by the prosumer through the use of blockchain technology. These examples demonstrate the overall concept of blockchain technology and its use in smart energy systems. However, the exact blockchain technology solutions (network, data, consensus, and so on) that must converge to fulfill the requirements of these applications are not obvious.

There are several research articles, projects, and ongoing trials that aim to leverage unique blockchain features to advance the digitalization of smart energy systems. A review of blockchain technology in the energy sector can be found in [17]–[19]. In [17], Andoni et al. provide a comprehensive review and classification of 140 blockchain-based projects in the energy sector. In [18], Ahl et al. explore the potential challenges of blockchain-based P2P microgrids and discuss a framework that incorporates technological, economic, social, environment, and institutional dimensions; the article suggests the inclusion of economic, social, and environmental dimensions to bridge the gap between technology and institutions.

In [19], Musleh et al. review blockchain-based smart grid projects and discuss frameworks for further blockchain integration in smart grids. According to these frameworks, the creation of a cyber layer designed for blockchain applications, aggregation of computing resources in microgrids, and smart grid protection and security issues can be leveraged to achieve better integration of the blockchain in smart grids. Blockchain integration efforts in the Internet of Things (IoT) are also discussed in [20] and [21]. None of these articles identify the exact choice of blockchain technology solutions for different smart energy systems and applications.

Blockchain technology is relatively new, and, although it holds tremendous potential, solutions and implementation platforms are still developing. The choice of blockchain technology solutions that can fulfill the requirements of various smart energy applications (such as those in Figures 1 and 2) is not entirely obvious. In this article, we provide a review of blockchain building blocks, followed by the identification of the most suitable blockchain technologies according to the requirements of various smart energy systems. For example, blockchain-network-management techniques can be classified into public, consortium, and private categories. Similarly, data-management techniques can be classified as on-chain (all data are stored on a blockchain) and off-chain (only data hashes are stored on a blockchain) types.

Different combinations of these options result in blockchain implementation platforms with varying features and performance. We review important existing blockchain platforms and a few representative blockchain-based smart energy projects in four domains: SI, ET, green initiatives (GI), and EM. Through this review, we show that existing blockchain platforms are not entirely suitable for smart energy systems. Therefore, to achieve appropriate integration of blockchain technology solutions for smart energy applications, we first consider 16 requirements that represent the needs of a broad selection of smart energy applications. We analyze the suitability of different blockchain technologies for fulfilling them and determine appropriate blockchain building blocks for various smart energy applications. To summarize, our major contributions are as follows.

- We present a review of blockchain fundamentals and discuss various blockchain building blocks, which include network-, data-, consensus-, identity-, and automation-management techniques.
- We review existing blockchain platforms and classify representative blockchain-based smart energy projects into SI, ET, GI, and EM domains. We show that a large number of projects use blockchain building blocks that are computing and resource intensive and, hence, less efficient in terms of data and identity management.
- We list 16 requirements for smart energy systems and organize them into four categories: decentralization and trust, data management, security, and scalability. Based on these, we determine blockchain building blocks that are suitable for smart energy systems and applications.
- We further customize blockchain technology solutions for multiple energy applications within each domain (i.e., SI, ET, GI, and EM).
- We also identify open research areas related to blockchain technology that are necessary to fulfill the future needs of smart energy systems.

The Blockchain

In this section, we present the blockchain and various blockchain-building technologies for network, data, consensus, identity, and automation management. The key points of this section are also summarized in Table 1.

Blockchain Fundamentals

A blockchain is a decentralized, digitally distributed ledger. A set of transactions, which may indicate the transfer or exchange of monetary value or digital assets, such as information, services, or goods, is produced and collected by a distributed network of computing nodes (a P2P network). A time-stamped data block (containing these transactions) is created through a decentralized consensus mechanism among the nodes according to predefined protocols. The newly created block also contains reference to the block that came before it (parent block) in the form of a cryptographic hash, thus establishing a link between the blocks. The new block is added in front of its parent block, and a chainlike structure of blocks is obtained; hence, we get the term *blockchain* (as shown in Figures 1 and 2).

Once a blockchain grows to a sufficient size, transactions recorded on it become practically immutable and resistant to change. Moreover, with a blockchain, a "trustless" network of nodes is also created. In a trustless network, nontrusting nodes can interact with each other without a centralized entity or an intermediary, and conflicts are automatically resolved with the help of protocols.

Blockchain Technology Solutions

Blockchain creation and maintenance requires network, data, consensus, identity, and automation management. In this section, we present various blockchain technology options in each category and discuss their advantages and disadvantages.

Network Management

Blockchain network management can be classified into three categories [12].

- *Public (N1)*: A pubic blockchain network is truly decentralized and permissionless. Any node can join or leave the network. The nodes have full permission to maintain a complete copy of the blockchain (referred to as *public blockchain*). All of the nodes can issue transactions, and they can participate in the block creation process according to publicly defined protocols and algorithms.
- *Consortium (N2)*: A consortium blockchain network is a permissioned network. The ability of a node to join the network or access the blockchain is controlled by a group of organizations, which assign permissions to nodes across their organizations to join the network and read or modify the associated consortium blockchain. In some situations, nodes outside the consortium may also be allowed to access and read the consortium blockchain contents to achieve greater transparency. However, such nodes are not allowed to modify the blockchain state.
- *Private (N3)*: A private blockchain network is another type of permissioned

TABLE 1 – THE BLOCKCHAIN TECHNOLOGY SOLUTIONS IN DIFFERENT CATEGORIES WITH THEIR ADVANTAGES AND DISADVANTAGES.

CATEGORY	SOLUTIONS	DESCRIPTION	ADVANTAGES	DISADVANTAGES
Blockchain network management	Public (N1)	Any node can join or leave the network.	Complete decentralization with no single point of failure	Vulnerable to Sybil attacks, high latency, and less scalable
	Consortium (N2)	The network is controlled by a group of organizations.	More suitable for regulated industries	Network management issues when organizations leave or join
	Private (N3)	The network is controlled by a single organization.	More scalable, more private, and less expensive to maintain	Permission management could become a single point of failure, more centralized
Data management	On-chain (D1)	All of the validated transactions are stored on the blockchain.	Greater transparency, auditability, and data availability	Huge storage burden, less scalable, not suitable for resource-constrained nodes
	Off-chain (D2)	Only the hashes of important data are stored on the blockchain.	Smaller storage requirements, suitable for resource-constrained nodes	Conventional databases required to host off-chain data
Consensus management	PoW (C1)	Nodes compete to solve an appropriate hashing puzzle.	Suitable for public networks (prevents Sybil attacks)	Wastes tremendous amount of resources, high latency, less scalable
	PoS (C2)	Nodes are picked according to their economic stake.	Suitable for public networks (prevents Sybil attacks), relatively more scalable	Prone to nothing-at-stake attack, less democratic
	Voting based (C3)	Voting schemes are based on the BFT algorithm and its variants.	More suitable for consortium and private blockchain networks, low latency	Networking and scalability issues (cannot scale beyond a few hundred nodes)
	Authority based (C4)	Trusted nodes create a new block in a round-robin fashion.	Highly scalable, eliminates message exchange, more energy efficient	Requires trusted nodes in the network
Identity management	Self-sovereign identity (S1)	Each node owns and controls its identity without disclosure of personal data.	Guarantees more privacy	Requires a pool of identity providers
	Decentralized trusted identity (S2)	Central server and personal data disclosures are required.	Establishes more trust in the network	More centralized and less private
Automation management	Deterministic smart contracts (T1)	Information from any external party is not required.	Provides greater automation and eliminates human intervention	Execution necessitates sequential processing
	Nondeterministic smart contracts (T2)	This solution depends on information from an external party.	Provides more flexibility and functionality	Nondeterministic nature, requires external party availability

BFT: Byzantine fault tolerant; PoS: proof of stake; PoW: proof of work.

network. It is controlled by a single organization, which allows only a limited number of nodes within the organization to join the network and read or modify the state of the private blockchain.

Data Management

A blockchain records transactions and stores data. There are two broad techniques for blockchain data management [13].

- *On-chain (D1)*: In on-chain data management, all of the transactions are stored on a blockchain. The size of the blockchain continuously grows, and storage requirements keep on increasing. This method is not suitable for resource-constrained nodes.
- *Off-chain (D2)*: In off-chain data management, only the hash values of data transactions are stored in the blockchain, while raw transaction data are stored using traditional techniques. With this method, the amount of storage needed at network nodes is significantly reduced. However, there are additional requirements, such as the synchronization of the database with the blockchain and availability of a server for hosting raw data.

Consensus Management

The choice of node/nodes entrusted to create a new block depends on the consensus algorithm adopted by the blockchain network. Consensus algorithms allow all of the nodes in the network to agree to the same worldview of the state of the blockchain. There are different types of consensus algorithms [14], [21].

- *Proof of work (C1)*: In a proof-of-work (PoW) algorithm, nodes compete to solve an appropriate hashing puzzle that requires expensive computing resources. The block created by the node that is the first to solve the given puzzle is accepted by the network. This method is useful in permissionless networks to avoid Sybil attacks, in which a single node may vote multiple times with different identities to influence the vote outcome. However, PoW is energy intensive and wastes a tremendous amount of resources.
- *Proof of stake (C2)*: In a proof-of-stake (PoS) algorithm, nodes are selected to create new blocks in a pseudorandom fashion. The probability of a node being selected is proportional to its economic stake in the network. This algorithm is also suitable for a permissionless blockchain and punishes misbehaving nodes by confiscating their stake in the network. However, this method is prone to nothing-at-stake attacks.
- *Voting based (C3)*: In permissioned blockchain networks where only known nodes can join the network, consensus among validating nodes on the contents of a new block can be achieved through voting mechanisms. Voting schemes are based on Byzantine-fault-tolerant (BFT) algorithms and its variants, such as Tendermint and Federated BFT. With this method, multiple rounds of voting might be required to reach consensus, and there is also a significant networking overhead, which has a negative impact on network scalability.
- *Authority based (C4)*: A proof-of-authority (PoAu) algorithm can also be used in certain blockchain networks. In this mechanism, authorized (trusted) nodes in the network create a new block in a round-robin fashion. The PoAu method eliminates message exchange among nodes for consensus building and is more resource efficient. However, the inclusion of trusted nodes reduces the trustless nature of the resulting blockchain network.

Identity Management

A blockchain network relies on public key cryptography. Each node has a pair of public/private keys to sign and verify transactions. There are different ways to manage the identity and entitlements of blockchain nodes [15].

- *Self-sovereign identity (S1)*: In this method, every node owns and controls its identity without relying on an external authority for attestation or verification of node credentials. There is no central server, and personal data are not necessary for identity creation. Nodes can perform identity-proofing by gathering attributes from an ecosystem of identity providers. Each node is allowed to create multiple keys as required to keep its identity private. Nodes can also selectively disclose their attributes to maintain privacy. Sovrin and uPort are examples of self-sovereign identity-management systems.
- *Decentralized trusted identity (S2)*: This method requires a central server to perform identity-proofing of nodes. In the initial stage, a node must provide identity proof (personal information) to the central server. After this bootstrap phase, node identity is recorded in the blockchain for later validation. Verified nodes can then create further keys as needed. ShoCard and BitID are examples of a decentralized trusted-identity management system.

Automation Management

Automation management on a blockchain is carried out with the help of smart contracts, which may define contractual obligations, custody or transfer of digital assets, and rights and privileges of nodes. Smart contracts provide greater automation and replicate actions that are generally performed by trusted third parties or intermediaries. Turing-complete programming languages that can support arbitrary logic and computations are generally needed to develop smart contracts. We can broadly classify smart contracts into two types [16].

- *Deterministic smart contracts (T1)*: A deterministic smart contract does not require any information from an external party. All information necessary to execute a smart contract can be obtained from the data already stored on the blockchain.
- *Nondeterministic smart contracts (T2)*: A nondeterministic smart contract depends on information (called *oracles* or *data feeds*) from an external party; for example, it may need external weather information for execution. It provides greater flexibility at the expense of greater vulnerability to external attacks.

There are many blockchain technology solutions. The combination of blockchain building blocks also results in different tradeoffs and varying blockchain features. In addition, the requirements of smart energy applications are also diverse. However, before identifying the best possible blockchain technology solutions for various smart energy applications, we first provide a brief review of existing blockchain platforms and efforts to integrate them into smart energy systems.

Review of Blockchain Integration Into Smart Energy Systems

In this section, we review some blockchain integration efforts in smart energy systems. We do not intend to provide a complete survey; a comprehensive review and classification of 140 blockchain-based projects in the energy sector is available in [17]. Here, we present some selected platforms and projects in each smart energy domain to demonstrate that most of these efforts do not use blockchain technologies customized for energy applications. This review will further help us identify the most suitable blockchain technology solutions according to the requirements of smart energy systems. The contributions of this section are summarized in Table 2 and Figure 3.

Review of Blockchain Platforms Used in Smart Energy Systems

Blockchain platforms combine network-, data-, consensus-, identity-, and automation-management technologies for the creation of blockchain-based projects. Blockchain integration in smart energy applications is being carried out by using either open source or proprietary blockchain platforms. Popular open source platforms include Ethereum, HyperLedger, Tendermint, and Energy Web Foundation (EWF). Proprietary platforms are developed to suit the requirements of specific applications, and, sometimes, these platforms also develop proprietary management protocols and algorithms. The majority of open source and proprietary platforms are nonmodular [22].

Ethereum

Ethereum is a generic open source blockchain-development platform governed by Ethereum developers, and it is widely used for developing blockchain applications for smart energy systems [23]. This platform was developed for public (N1) blockchain management. However, the open source code of Ethereum can be easily modified to maintain consortium (N2) and private (N3) networks. Ethereum supports on-chain data management (D1). A PoW (C1) consensus algorithm is currently used, but there are plans to switch to PoS (C2). The platform can support self-sovereign (S1) and decentralized trusted (S2) identity-management techniques as well as Turing-complete programming languages (Solidity and Serpent), which can be used to create deterministic (T1) and nondeterministic (T2) smart contracts.

HyperLedger

HyperLedger is an open source blockchain-development platform supported by the Linux Foundation [24]. This platform can be used to set up consortium (N2) and private (N3) networks. It supports on-chain data management (D1) and voting-based consensus (C3) algorithms as well as self-sovereign (S1) and decentralized trusted (S2) identity-management techniques. Turing-complete programming languages, such as Java, Go, Solidity, Fabric, and Rust, allow the writing of deterministic smart contracts (T1). However, support for nondeterministic smart contracts (T2) through oracles is not yet available.

Tendermint

Tendermint is another application-oriented framework that can be used to set up a public, consortium, or private

TABLE 2 – A REVIEW OF THE BLOCKCHAIN PLATFORMS USED IN SMART ENERGY SYSTEMS.

	BLOCKCHAIN TECHNOLOGY SOLUTIONS													
PLATFORM	NETWORK			DATA		CONSENSUS				IDENTITY		AUTOMATION		PROJECTS
	N1	N2	N3	D1	D2	C1	C2	C3	C4	S1	S2	T1	T2	
Ethereum	✓	✓	✓	✓	×	✓	✓	×	×	✓	✓	✓	✓	Bankymoon TheSunExchange Brooklyn Microgrid NRGCoin
HyperLedger	×	✓	✓	✓	×	×	×	✓	×	✓	✓	✓	×	Car eWallet Tennet & Sonnen SunChain
Tendermint	✓	✓	✓	✓	×	×	×	✓	x	✓	✓	✓	×	GridChain EnerChain Brooklyn Microgrid
EWF	×	✓	✓	✓	×	×	×	×	✓	✓	✓	✓	✓	Slock.it GridSingularity Share&Charge
Proprietary	–	–	–	–	–	–	–	–	–	–	–	–	–	Nasdaq Linq Solar Bankers PROSUME

Here, ✓ is used if the platform supports a certain technology solution, × indicates that it does not support the solution, and – means that information is unavailable or diverse.

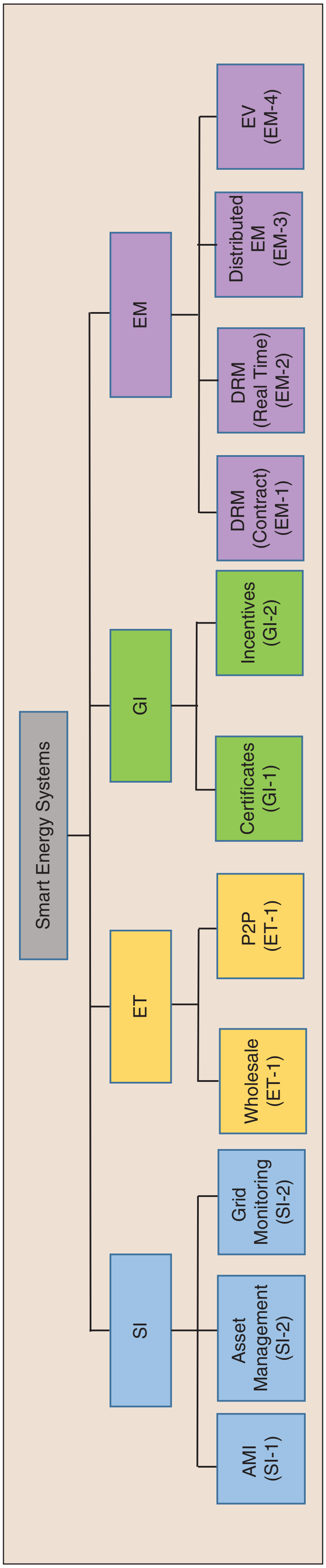

FIGURE 3 – The smart energy system domains and applications. AMI: automated metering infrastructure.

network of P2P nodes (N1, N2, N3) [25]. This platform supports on-chain data management (D1) and voting-based (C3) consensus algorithms as well as self-sovereign (S1) and decentralized trusted (S2) identity-management techniques. It supports various Turing-complete programming languages that currently allow the writing of deterministic smart contracts (T1).

EWF

The EWF blockchain platform is supported by more than 70 companies, and its aim is to integrate and accelerate blockchain technology in smart energy systems [26]. The EWF platform is Ethereum compliant, but it is more customized for smart energy applications. It can be used to set up consortium (N2) and private (N3) networks, and it supports on chain-data management (D1), the PoAu (C4) consensus algorithm, and self-sovereign (S1) as well as decentralized trusted (S2) identity-management techniques. Deterministic (T1) and nondeterministic (T2) smart contracts can be developed in Turing-complete C and C++ programming languages. Tobalaba, which is the test version of this platform, is already available for developers.

Proprietary Platforms

Several proprietary blockchain platforms also exist for smart energy applications. For example, Solar Bankers is developing a proprietary consensus algorithm called *Obelisk*, which runs on their Skychain blockchain [27]. The idea is based on developing a trusted consortium of nodes that generate and validate data blocks. Similarly, PROSUME is also developing a proprietary blockchain-based platform to support a multitude of smart energy applications [28]. In Table 2, we provide a summary of blockchain technology solutions supported by these platforms.

Review of Blockchain-Based Smart Energy Projects

We review blockchain-based smart energy projects in the four smart energy domains: SI, ET, GI, and EM. These domains are broad and cover several interesting and useful applications. The list of domains and considered applications in each domain are presented in Figure 3. A short notation for each application is also introduced for further use in the article. For example, SI-1 notation is used for an automated metering infrastructure (AMI) application. The scenario in Figure 1 represents an ET-2 application, whereas that in Figure 2 represents an EM-3 application. Due to space limitations, we discuss only a few representative projects in each domain. Further details of these projects can be found in [17], [20], [29], [30], and the references therein.

Blockchain Projects in the SI Domain

- *Bankymoon*: This project is related to an AMI (SI-1 application). Smart meters compute and communicate energy consumption of an industrial or residential building at regular intervals for billing automation and reduction of electricity theft incidents [31], [32]. However, in the Bankymoon project, blockchain-enabled smart meters are being developed to further automate financial transactions. These meters can be loaded with cryptocurrencies, and payments can be settled in real time through smart contracts. This project is being developed using the Ethereum platform.
- *TheSunExchange*: This endeavor involves asset management (SI-2 application). The high initial costs of RES technologies could become a barrier to taking communities off-grid. However, this issue may be resolved by creating shared assets in smart energy systems, such as by purchasing solar photovoltaics (PVs) through crowd-funding [33]. TheSunExchange project allows users to purchase solar panels and lease them to earn passive income. Blockchain integration enables transparent management of assets and the administration of the solar energy produced by these assets. Therefore, this project can be also be classified as an example an EM-3 application, which is related to distributed EM.
- *GridChain (PONTON)*: This venture addresses power grid monitoring

(SI-3 application). In power grids, IoT sensors in the transmission and distribution systems facilitate monitoring of grid parameters to automate fault diagnosis and to maintain power-balance for grid stability [34]. Blockchain integration can further help in achieving transparency and fixing liability. In this context, the objective of GridChain project developed by PONTON is to enable real time power balance and congestion management by providing coordination between various grid entities. This project can also be classified as an example of real time DRM application (EM-2).

Blockchain Projects in the ET Domain

- *EnerChain (PONTON)*: This project deals with a wholesale-energy-trading ET-1 application. The integration of the blockchain into energy-trading applications achieves greater transparency and automation. The EnerChain was also developed by PONTON to enable wholesale ET in European regional power markets. It aims to offer wholesale-energy-trading solutions in different time frames, including day ahead, monthly, quarterly, and yearly.
- *Brooklyn Microgrid*: This concept is related to a P2P energy-trading ET-2 application, which is shown in Figure 1. In smart energy systems, prosumers can engage in decentralized ET activities where they can directly trade energy with other prosumers or consumers [35], [36]. The Brooklyn Microgrid is an example of the real-world development of a blockchain-based P2P energy-trading solution. In this project, prosumers can directly sell their surplus energy to their neighbors (without needing any brokers or intermediaries), energy transactions are recorded on the blockchain, and payments are settled automatically through smart contracts.

Blockchain Projects in the GI Domain

- *Nasdaq Linq*: This venture involves the management and trading of green certificates and carbon credits (GI-1 application). To encourage RES uptake, several countries and states issue green certificates and carbon credits [7], which can also be traded. However, with greater integration of RESs in power grids, the management of these certificates is becoming challenging. In this context, Nasdaq Linq aims to bring efficiency, quick verification, and elimination of paper records for green-certificate management through the integration of the blockchain. This project is being developed using a proprietary platform.
- *NRGcoin*: This endeavor concerns the management of incentives for green behavior (GI-2 application). In this project, NRGcoins are given as a reward to incentivize local production and consumption of green energy. It should be noted that 1 NRGcoin is equivalent to 1 kWh of energy. The use of virtual currency in this project creates additional value around its blockchain. However, unlike Bitcoin, these coins are not mined but are issued by the blockchain developers. The smart contract framework of NRGcoin is based on the Ethereum platform.

Blockchain Projects in the EM Domain

DRM is an important concept in smart energy grids; however, blockchain-based projects for EM-1 and EM-2 applications are relatively rare.

- *Key2Energy*: This project is related to distributed EM (EM-3 application). The blockchain is used for EM in multi-apartment buildings. The objective is to maximize the profit of each structure by selling PV energy and minimizing the energy cost of shared facilities in the building. Platform details of Key2Energy are not available.
- *Car eWallet*: The number of EVs with batteries is increasing. Due to mobility, the management of EVs and their energy consumption becomes quite challenging [37]. Car eWallet is related to EVs (EM-4 application), and it provides a blockchain-based solution for car sharing, car rental, and EV charging. It also allows automatic processing of payments.

In Table 2, the blockchain platforms used for these projects are also identified. It should be noted that several blockchain platforms (except EWF) were not developed exclusively for smart energy applications. Therefore, the embedded technology options in these platforms are also not entirely suitable for these applications. For example, a large number of projects use Ethereum, which embeds a computing-intensive PoW algorithm. Similarly, several platforms lack the ability to support off-chain data management and nondeterministic smart contract management.

In addition, most of the blockchain-based smart energy projects are still in the development or trial phases, and real-world implementations are rare. In this context, to guide further research and development in this field, there is a need to identify appropriate blockchain technology solutions according to the requirements of smart energy systems. In the next section, we discuss these and, accordingly, identify the appropriate choice of blockchain technology solutions for various applications.

Choosing Appropriate Blockchain Technologies

In this section, we present suitable blockchain technology solutions according to the requirements of smart energy systems; then, we describe the customization of these solutions for various applications. We summarize the key contributions of this section in Tables 3 and 4.

Requirements of Smart Energy Systems

We first discuss a total of 16 requirements (R1–R16) in four categories that are applicable to the broad selection of smart energy applications listed in Figure 3 and the scenarios depicted in Figures 1 and 2.

Decentralization and Trust Requirements

- *Decentralization (R1)*: Due to the inclusion of RESs and mobile loads (EVs), the architecture of smart energy systems is becoming decentralized. Efficient implementation

TABLE 3 – THE SUITABILITY OF BLOCKCHAIN TECHNOLOGY SOLUTIONS IN FULFILLING SMART ENERGY SYSTEM REQUIREMENTS.

		BLOCKCHAIN TECHNOLOGY SOLUTIONS												
		NETWORK			DATA		CONSENSUS				IDENTITY		AUTOMATION	
CATEGORY	REQUIREMENT	N1	N2	N3	D1	D2	C1	C2	C3	C4	S1	S2	T1	T2
Decentralization and trust	Decentralization (R1)	✓	✓	✓	–	–	✓	✓	✓	✓	✓	×	–	–
	Conflict resolution mechanism (R2)	×	✓	✓	–	–	✓	✓	✓	✓	×	✓	✓	✓
	Intermediaries (R3)	–	–	–	–	–	–	–	–	–	–	–	✓	✓
	Nonrepudiability (R4)	–	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data management	Tamperproof record keeping (R5)	–	–	–	✓	×	✓	✓	✓	×	–	–	–	–
	Data correction and erasure (R6)	×	✓	✓	–	–	×	×	×	✓	–	–	–	–
	Data backup (R7)	✓	✓	✓	✓	✓	–	–	–	–	–	–	–	–
	Privacy protection (R8)	×	✓	✓	×	✓	×	×	×	✓	✓	×	–	–
Security	Authentication (R9)	×	✓	✓	–	–	–	–	–	–	✓	✓	–	–
	Authorization (R10)	×	✓	✓	–	–	–	–	–	✓	✓	✓	✓	✓
	Data integrity (R11)	–	–	–	–	–	–	–	–	–	✓	✓	✓	×
	Auditability (R12)	–	–	–	✓	✓	–	–	–	–	✓	✓	✓	✓
Scalability	Throughput (R13)	–	–	–	×	✓	×	✓	×	✓	–	–	×	×
	Latency (R14)	–	–	–	✓	×	×	✓	×	✓	–	–	–	–
	Process automation (R15)	✓	✓	✓	–	–	✓	✓	✓	✓	✓	✓	✓	✓
	Cost (R16)	×	✓	✓	×	✓	×	✓	✓	✓	✓	×	✓	✓

Here, ✓ is used if blockchain technology is suitable, × indicates that it is not suitable, and – means that it is unconcerned.

TABLE 4 – BLOCKCHAIN CUSTOMIZATION FOR VARIOUS SMART ENERGY APPLICATIONS.

DOMAIN	APPLICATION	BLOCKCHAIN TECHNOLOGY OPTIONS	REMARKS
SI	AMI (SI-1)	(N2, N3), (D2), (C2, C4), (S2), (T1)	Blockchain integration is more suitable in new smart meter rollout programs.
	Asset management (SI-2)	(N2, N3), (D2), (C2, C4), (S1, S2), (T1)	Blockchain integration is more suitable to track-shared or crowd-funded RES assets.
	Grid monitoring (SI-3)	(N2, N3), (D2), (C4), (S2), (T1)	Latency requirements are a few milliseconds; even PoAu (C4) might not be able to fulfill these.
ET	Wholesale (ET-1)	(N1, N2), (D2), (C1, C2, C3, C4), (S1, S2), (T1, T2)	Blockchain integration can eliminate existing brokers, but initial implementation costs could be high.
	P2P (ET-2)	(N2), (D2), (C2,C3), (S1, S2), (T1, T2)	The high potential for blockchain integration is due to the localized nature and lack of P2P trading platforms.
GI	Certificates (GI-1)	(N1, N2), (D2), (C1, C2, C3, C4), (S1, S2), (T1)	Blockchain integration can eliminate existing brokers, but initial implementation costs could be high.
	Incentives (GI-2)	(N2, N3), (D2), (C3, C4), (S2), (T1)	N3 can be established if all users belong to the same utility company.
EM	DRM (contract) (EM-1)	(N2, N3), (D2), (C2, C4), (S2), (T1)	C2 is to be avoided if the stake of a node is low, and S2 is listed due to KYC requirements.
	DRM (real time) (EM-2)	(N2, N3), (D2), (C4), (S2), (T1)	Latency requirements are a few milliseconds; even PoAu (C4) might not be able to fulfill these.
	Distributed EM (EM-3)	(N2), (D2), (C2,C4), (S1, S2), (T1, T2)	T2 can be used if external weather information is needed.
	EV (EM-4)	(N2), (D2), (C2, C3, C4), (S1, S2), (T1, T2)	C2 or C3 can be used if they reduce costs. There is a high potential for blockchain integration.

of various applications in different domains necessitates decentralized networking and control.

- *Conflict-resolution mechanism (R2)*: Smart energy domains involve interactions between multiple nontrusting nodes; therefore, some mechanisms (entities or technologies) are needed to mediate between nodes to resolve conflicts.
- *Intermediaries (R3)*: In several smart energy applications, intermediaries are required to support the activities of the principal players. The role of the intermediary arises due to the operational and technological limitations of the principal players. For example, financial transactions between consumers and generators are mostly settled through banks. Similarly, brokers or energy-trading platforms are necessary to match the buying and selling requirements of generators and consumers.
- *Nonrepudiability (R4)*: Nonrepudiability refers to the availability of irrefutable proof of who performed a certain action even if the nodes are not cooperating. In smart energy domains, nonrepudiability is needed to establish liability.

Data-Management Requirements

- *Tamperproof record keeping (R5)*: Recording, trading, and transporting electricity, assets, and other resources is necessary in various smart energy systems. In some situations, electricity flow occurs almost immediately, whereas financial settlements, for example, are carried out later. Therefore, it becomes important to store data in a tamperproof manner.
- *Data correction and erasure (R6)*: In the event of malfunction, hacking, or tampering of sensors or equipment, wrong data could get recorded. If such events are detected or reported, data correction or data erasure becomes essential. With increased automation, all of the smart energy domains need a certain ability to correct and erase such erroneous data.
- *Data backup (R7)*: Data loss can create inconvenience, disruption, and financial loss. Similarly, data storage and retrieval from a single database also requires permanent availability of the data hosting node. Thus, a single point of failure is created in centralized systems. Data collected in various smart energy system domains are often critical and, therefore, necessitate adequate backup to ensure smooth operations.
- *Privacy protection (R8)*: In various smart energy systems, there is a high requirement to keep data and node identity private. For example, smart meter data reveals private information about the habits, schedule, and behavior of users.

Security Requirements

- *Authentication (R9)*: Authentication is concerned with determining the identity of a node in the system to block unauthorized access. A node can be authenticated through its unique credentials in the system (e.g., public key, address, name). Smart energy systems often involve critical data and infrastructure. Therefore, authentication is always required in all of the smart energy domains.
- *Authorization (R10)*: Authorization deals with managing the access and privileges of various nodes in the network. In smart energy systems, nodes have varying roles and, therefore, need different authorization in individual applications. In addition, there is also a role for regulatory bodies and government agencies. Therefore, appropriate authorization and the ability to detect any violations of privileges and rights is necessary in such systems.
- *Data integrity (R11)*: Data integrity refers to the detection of unauthorized changes in data. A decentralized architecture requires that a large number of critical messages be exchanged between various nodes, and data integrity violations can result in safety problems or harmful attacks on the critical infrastructure.
- *Auditability (R12)*: Auditability is concerned with the ability to reconstruct a complete history of a certain event or action from historical records. In smart energy systems, auditability is needed to fix liability in the case of malfunctions or conflicts, safeguard commercial and financial interests, or fulfill regulatory requirements.

Scalability Requirements

- *Throughput (R13)*: In smart energy systems, a single node often produces a small amount of data. However, a large number of nodes are involved in building meaningful applications. If the data requirements of a single node are considered as a single transaction, then a large number of transactions happen every second. Therefore, smart energy systems need high data throughout.
- *Latency (R14)*: Smart energy applications require low latency to ensure smooth monitoring, control, and operation of appliances, equipment, and processes. The latency of some critical applications, such as that needed for grid stabilization, is only a few milliseconds.
- *Process automation (R15)*: Smart energy systems are built on the promise of making RES integration, energy transportation, and ET more efficient. This can be achieved through increased process automation, resulting in a reduction in human intervention and simplification of legacy procedures.
- *Cost (R16)*: Smart energy systems integrate novel technologies and new equipment (smart meters, sensors, and so on), which helps reduce various operating costs. However, high upfront expenses due to equipment replacement or technology upgrades is a major barrier to the adoption of various concepts. In this context, all of the smart energy domains can benefit from cost reductions.

Based on these requirements, we can determine the suitability of blockchain technology solutions for various smart energy systems and applications. The suitability analysis is presented in Table 3. It was carried out by matching the features, advantages, and disadvantages of the various blockchain technology solutions discussed in the "Blockchain" section with smart energy system needs. Based on this analysis, the consortium (N2) and private (N3) network-management methods emerge as more suitable options for such systems. Off-chain data management (D2) can fulfill more conditions than on-chain data management techniques. Similarly, authority-based consensus management (C4) is the best consensus algorithm for smart energy systems, and self-sovereign identity management (S1) and deterministic smart contracts (T1) can fulfill more requirements. This analysis enables quick identification of appropriate blockchain technology solutions for smart energy systems. However, various smart energy applications, such as P2P ET and distributed green EM (as shown in Figures 1 and 2), also have slightly different needs. Hence, there is a need to further customize blockchain technology solutions for various smart energy applications.

Customization of Blockchain Technology Solutions

The requirements of smart energy applications differ from each other, necessitating further customization of blockchain technology solutions. For example, some applications need low latency, some necessitate high privacy protection, and so on, [38], [39]. In this section, we further identify appropriate blockchain technology solutions for the various smart energy applications shown in Figure 3; this discussion is summarized in Table 4.

SI Domain

The AMI SI-1 application has relatively relaxed latency and throughput requirements. For this application, consortium (N2) and private (N3) network-management techniques can be used. Private network management is preferred if data are directly handled by the utility. Since smart meters are resource-constrained nodes, the off-chain data-management (D2) technique is more suitable. For consensus management, the PoS (C2) and PoAu (C4) algorithms are better options. This application needs high privacy protection; however, due to the regulatory and registration requirements of smart meters with a utility company, self-sovereign (S1) identity management cannot be used. Instead, decentralized trusted (S2) identity management is a more desirable option.

Moreover, the necessary automation, if needed, can be managed with the help of deterministic smart contracts (T1). The asset management SI-2 application has relatively low privacy and throughput requirements. For this application, the choices of network-, data-, consensus-, and automation-management are the same as for SI-1. For managing shared RESs, PoS (C2) is a more fitting option. However, when there are low latency needs, the PoAu (C4) algorithm is preferable. For identity management, self-sovereign (S1) and decentralized trusted (S2) identity management are suitable. However, if know-your-customer (KYC) requirements are not applicable, then the self-sovereign (S1) technique can also be used. A grid-monitoring application has extremely stringent latency needs (on the order of a few milliseconds). For this application, network-, data-, identity-, and automation-management options are the same as those identified for the SI-1 application. However, due to extremely low latency requirements, only PoAu (C4) is an ideal consensus management solution for this application, and even this algorithm can fail to achieve the necessary performance.

ET Domain

The wholesale-energy-trading application has relatively low privacy requirements; therefore, public and consortium network-management techniques (N1, N2) are most appropriate. N1 should be used if a trading platform is being developed across multiple regional markets. For a more localized P2P-energy-trading (ET-2) application, only the consortium network-management technique (N2) is suitable. For both applications, the off-chain data-management (D2) technique is ideal. For consensus, all of the options are acceptable for ET-1. For ET-2, PoW (C1) should be avoided because it is more resource intensive. The PoAu (C4) algorithm should also be avoided for the ET-2 application because it requires trusted nodes in the network and dilutes the trustless feature of the blockchain. Both of the identity management schemes may be used for ET-1 and ET-2. Similarly, for both applications, the choice between deterministic and nondeterministic smart contracts (T1, T2) can be made based on the availability of information inside or outside the network for the execution of smart contracts. With this information, the necessary ingredients to build the best blockchain for the P2P-energy-trading scenario depicted in Figure 1 can be easily identified.

GI Domain

The privacy requirements of green-certificate (GI-1) applications are less stringent. Suitable blockchain technology solutions for this application are the same as those identified for the ET-1 application. Regarding behavior incentives, for a GI-2 application with less stringent latency and throughput requirements, the choices of network, data, identity, and automation management is the same as those identified for the SI-1 application. However, for consensus, the voting-based (C3) technique can be used if there are a limited number of nodes in the network, and PoAu (C4) methods can also be adopted to conserve resources.

EM Domain

For the contract-based DRM (EM-1) application, viable technology options are the same as those identified for the SI-1 application. However, for a real-time DRM EM-2 application, due to extremely low latency requirements, only the PoAu (C4) algorithm is a good choice; all other options remain the same as those determined for EM-1. For the distributed-energy-management (EM-3) application, suitable technology options for network, data, identity, and automation management are the same as those chosen for the ET-2 application. However, for this application, due to relatively low latency requirements, the PoS (C2) and PoAu (C4) techniques are more appropriate for consensus management. Finally, optimum technology options for the EV (EM-4) application are the same as those chosen for the ET-2 application, except that, for EM-4, we can also use the PoAu (C4) algorithm to conserve resources.

Blockchain Technology Gaps for Smart Energy Systems

Blockchain is still evolving, and there are several technology gaps that could limit its adaptation in smart energy systems. Here, we discuss some of them.

Network Management

Management of a blockchain network requires appropriate protocols and algorithms. These protocols are necessary for forwarding transaction, disseminating data, discovering nodes, maintaining a list of misbehaving nodes, and limiting the number of peer connections. The performance of these protocols has a direct impact on the latency, throughput, and speed of transaction processing. In this context, there is a need to develop delay-aware, security-aware, privacy-aware, and scalable network-management protocols for blockchain integration into smart energy systems. Moreover, the protocols must also provide flexible parameters to achieve various tradeoffs according to the latency and throughput requirements of smart energy applications.

Data Management

The implementation of off-chain data management, which is generally needed for resource-constrained nodes in smart energy systems, is more challenging as it requires the synchronization and availability of conventional databases. In this context, determination of the optimal amount of data that should be kept on-chain and off-chain for various applications is important. Storage of off-chain data in a tamperproof manner is also difficult. Furthermore, data models and database schema can vary across different organizations or applications. Novel techniques for handling multiple types of data models, database schema, and query processing on the blockchain are also necessary.

Consensus Management

The PoAu algorithm is the fastest consensus-management algorithm. However, the latency and throughput requirements of some applications are extremely stringent (measured in milliseconds), and even PoAu may fail to fulfill these. There is a clear need for further improvements in the consensus-management techniques for smart energy applications; for example, the use of implicit consensus (proposed in [40]) may be explored.

Identity Management

In several smart energy applications, due to KYC requirements enforced by regulators, a decentralized trusted identity scheme must be used. This has fewer advantages compared to a more private self-sovereign identity-management scheme. Recovering compromised identities can also become a challenge in some smart energy systems, particularly for nodes with private or critical data.

Automation Management

The security of smart contracts is critical, because if a smart contract is not well written and secure, it may be hacked or invoked under different circumstances that may not represent the actual intention of the original programmer. Nondeterministic smart contract management presents an even bigger security challenge. Smart energy applications involving critical data and industrial infrastructure necessitate appropriate programs and templates for the development of secure and well-written smart contracts. Smart contract execution often require sequential processing, which can slow down transaction verifications. Therefore, the development of appropriate sharing techniques for parallel processing is necessary to match the high performance demands of various applications.

Lack of Suitable Implementation Platforms

Many popular blockchain platforms are nonmodular, and they do not embed the appropriate technology solutions for smart energy systems. For example, the platforms lack support for off-chain data management and nondeterministic smart contracts, which are generally required for resource-constrained nodes. Therefore, the development of open source and modular blockchain platforms with appropriate embedded technologies to support multiple smart energy applications is critically needed.

Conclusion

Blockchain technology is novel but complicated, and its integration into any domain requires the convergence of appropriate building blocks to achieve the desired objectives. Existing blockchain integration efforts in smart energy systems mostly use open source blockchain platforms with embedded functionalities. These platforms are not entirely designed for energy applications, and the development of blockchain-based energy projects through these platforms may not provide the expected blockchain integration benefits.

In this article, we adopted a systematic approach through which we first collected the requirements of smart energy systems. After detailing the needs for each smart energy domain, we determined the most suitable blockchain building blocks for the respective smart energy systems. Accordingly, we identified blockchain technologies that meet these conditions. We further customized blockchain technologies for various smart energy applications in the SI, ET, GI and EM domains.

The analysis in this article can help in the design of flexible blockchain platforms customized for smart energy systems and assist with reaping the most benefit out of blockchain integration into smart energy systems. Significant new research in blockchain technologies is still needed to meet the diverse and often stringent latency, privacy, and security requirements of smart energy applications. Moreover, modular blockchain platforms, in which embedded technology options can be changed on demand, would also be necessary to support and accelerate blockchain integration in a wide variety of smart energy applications.

Acknowledgment

This work was supported in part by the Lahore University of Management Sciences Faculty Initiative Fund Pakistan and, in part, the Natural Science Foundation of China and Jiangsu Province under grants 61750110529, 61850410535, and BK20161147.

Biographies

Naveed Ul Hassan (naveed.hassan@lums.edu.pk) earned his B.E. degree in avionics from the College of Aeronautical Engineering, Risalpur, Pakistan, in 2002 and his M.S. and Ph.D. degrees in telecommunications from Ecole Superieure d'Electricite, Gif-sur-Yvette, France, in 2006 and 2010, respectively. He is currently an associate professor in the Electrical Engineering Department, Lahore University of Management Sciences, Pakistan. He is also an associate editor of *IET Smart Grid*. His research interests include wireless communication, smart energy systems, blockchain technology, and indoor positioning systems. He is a Senior Member of the IEEE.

Chau Yuen (yuenchau@sutd.edu.sg) earned his B.Eng. and Ph.D. degrees in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2000 and 2004, respectively. He is currently an associate professor with the Singapore University of Technology and Design. He was a recipient of the IEEE Asia–Pacific Outstanding Young Researcher Award in 2012. He is an editor of *IEEE Transactions on Communications* and *IEEE Transactions on Vehicular Technology*. His current research interests include wireless communications beyond 5G, smart grid, smart building, industry Internet of Things, and urban mobility. He is a Senior Member of the IEEE.

Dusit Niyato (dniyato@ntu.edu.sg) earned his B.Eng. degree in computer engineering from King Mongkuts Institute of Technology Ladkrabang, Thailand, in 1999 and his Ph.D. degree in electrical and computer engineering from the University of Manitoba, Canada, in 2008. He is currently a professor in the School of Computer Science and Engineering at Nanyang Technological University, Singapore. His research interests include energy harvesting for wireless communication, the Internet of Things, and sensor networks. He is a Fellow of the IEEE.

References

[1] M. Liserre, T. Sauter, and J. Y. Hung, "Future energy systems: Integrating renewable energy sources into the smart power grid through industrial electronics," *IEEE Ind. Electron. Mag.*, vol. 4, no. 1, pp. 18–37, 2010.

[2] H. Farhangi, "A road map to integration: Perspectives on smart grid development," *IEEE Power Energy Mag.*, vol. 12, no. 3, pp. 52–66, 2014.

[3] T. Strasser, P. Siano, and Y. Ding, "Methods and systems for a smart energy city," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1363–1367, 2018.

[4] O. Hafez and K. Bhattacharya, "Integrating EV charging stations as smart loads for demand response provisions in distribution systems," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1096–1106, 2018.

[5] T. Sousa, T. Soares, P. Pinson, F. Moret, T. Baroche, and E. Sorin, "Peer-to-peer and community-based markets: A comprehensive review," *Renewable Sustain. Energy Rev.*, vol. 104, pp. 367–378, Apr. 2019.

[6] W. Tushar, C. Yuen, H. Mohsenian-Rad, T. Saha, H. V. Poor, and K. L. Wood, "Transforming energy networks via peer to peer energy trading: Potential of game theoretic approaches," *IEEE Signal Process. Mag.*, vol. 35, no. 4, pp. 90–111, 2018.

[7] M. Hustveit, J. S. Frogner, and S.-E. Fleten, "Tradable green certificates for renewable support: The role of expectations and uncertainty," *Energy*, vol. 141, pp. 1717–1727, Dec. 2017.

[8] H. T. Haider, O. H. See, and W. Elmenreich, "A review of residential demand response of smart grid," *Renewable Sustain. Energy Rev.*, vol. 59, pp. 166–178, June 2016.

[9] K. Ma, Y. Yu, B. Yang, and J. Yang, "Demand-side energy management considering price oscillations for residential building heating and ventilation systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 8, pp. 4742–4752, 2019.

[10] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surv. Tuts.*, vol. 18, no. 3, pp. 2084–2123, 2016.

[11] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton Univ. Press, 2016.

[12] M. Vukolić, "Rethinking permissioned blockchains," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, 2017, pp. 3–7.

[13] X. Xu et al., "A taxonomy of blockchain-based systems for architecture design," in *Proc. IEEE Int. Conf. Software Architecture (ICSA)*, 2017, pp. 243–252.

[14] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, 2018.

[15] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[16] M. Alharby and A. van Moorsel, Blockchain-based smart contracts: A systematic mapping study. 2017. [Online]. Available: https://arXiv: 1710.06372

[17] M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.

[18] A. Ahl, M. Yarime, K. Tanaka, and D. Sagawa, "Review of blockchain-based distributed energy: Implications for institutional development," *Renewable Sustain. Energy Rev.*, vol. 107, pp. 200–211, June 2019.

[19] A. S. Musleh, G. Yao, and S. Muyeen, "Blockchain applications in smart grid-review and frameworks," *IEEE Access*, vol. 7, pp. 86,746–86,757, June 2019.

[20] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[21] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2018.

[22] M. Belotti, N. Bozic, G. Pujolle, and S. Secci "A vademecum on blockchain technologies: When, which and how," Sorbonne University, Paris, July 9, 2019. [Online]. Available: https://hal.sorbonne-universite.fr/hal-01870617

[23] V. Buterin. 2019. "An introductory paper to Ethereum," GitHub, Inc., San Francisco, White Paper, June 17, 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[24] "An introduction to Hyperledger," Hyperledger White Paper Working Group, San Francisco, CA, White Paper, July 2018. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf

[25] "Tendermint documentation," Tendermint Inc. Accessed on: Mar. 19, 2019. [Online]. Available: https://media.readthedocs.org/pdf/tendermint/v0.21.0/tendermint.pdf

[26] "The energy web chain: Accelerating the energy transition with an open-source, decentralized blockchain platform," Energy Web Foundation, Zug, Switzerland. Accessed on: Mar. 19, 2019. [Online]. Available: https://energyweb.org/wp-content/uploads/2018/10/EWF-Paper-TheEnergyWebChain-v1-201810-FINAL.pdf

[27] "Solar Bankers: Initial coin offering whitepaper," Solar Bankers, Prague, Czech Republic, White Paper. [Online]. Available: https://solarbankers.com/wp-content/uploads/2017/10/SB-White-Paper_version2.pdf

[28] PROSUME, "PROSUME: Decentralizing power," Prosume Energy Foundation, Milano, Italy, White Paper, 2017. [Online]. Available: https://prosume.io/wp-content/uploads/2017/09/white-paper_v2-2017.pdf

[29] J. Wu and N. Tran, "Application of blockchain technology in sustainable energy systems: An overview," *Sustainability*, vol. 10, no. 9, p. 3067, 2018.

[30] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *Proc. IECON 2017-43rd Annu. Conf. IEEE Industrial Electronics Society*, pp. 6153–6158.

[31] D. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 425–436, 2015.

[32] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable Sustain. Energy Rev.*, vol. 57, pp. 302–318, May 2016.

[33] P. T. Lam and A. O. Law, "Crowdfunding for renewable and sustainable energy projects: An exploratory case study approach," *Renewable Sustain. Energy Rev.*, vol. 60, pp. 11–20, July 2016.

[34] A. Zidan et al., "Fault detection, isolation, and service restoration in distribution systems: State-of-the-art and future trends," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2170–2185, 2017.

[35] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, 2017.

[36] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, 2017.

[37] F. A. Silva, "Modern electric, hybrid electric, and fuel cell vehicles, (book news)," *IEEE Ind. Electron. Mag.*, vol. 12, no. 4, pp. 46–48, 2018.

[38] V. C. Gungor et al., "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, 2013.

[39] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 2012.

[40] Z. Ren, K. Cong, J. Pouwelse, and Z. Erkin, Implicit consensus: Blockchain with unbounded throughput. 2017. [Online]. Available: arXiv: 1705.11046