IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 September 2022, accepted 2 October 2022, date of publication 5 October 2022, date of current version 12 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3212148

SURVEY

A Taxonomy and Lessons Learned From Blockchain Adoption Within the Internet of Energy Paradigm

RAIFA AKKAOUI[1,2], ALEXANDRU STEFANOV[1], (Member, IEEE), PETER PALENSKY[1], (Senior Member, IEEE), AND DICK H. J. EPEMA[2]

[1]Department of Electrical Sustainable Energy, Delft University of Technology, 2628 CD Delft, The Netherlands
[2]Department of Software Technology, Delft University of Technology, 2628 CD Delft, The Netherlands

Corresponding author: Raifa Akkaoui (r.akkaoui@tudelft.nl)

ABSTRACT The concept of the internet of energy (IoE) emerged as an innovative paradigm to encompass all the complex and intertwined notions relevant to the transition of current smart grids towards more decarbonization, digitalization and decentralization. With a focus on the two last aspects, the amount of intelligent devices being connected in a scattered way to the existing power grid is ever-growing. Nevertheless, guaranteeing a cyber-secure and resilient control of these IoE components as well as a seamless and reliable delivery of electricity services, such as renewable energy exchange, electric vehicles charging, demand response, and so forth; might be the bottleneck of current power systems that are largely still functioning following a centralized approach. Thus, the future power grid would gradually incorporate a growing number of distributed-based control schemes to deal with this challenge. And many believe that blockchain could be a key-enabler in this transition, due to its consistent characteristics with multiple requirements of future power systems. In this paper, we provide an extensive state-of-the-art of blockchain-based additions to the IoE. Where, we first introduce various concepts related to blockchain and discuss the rationale behind its adoption in the context of IoE. Then, differently from the existing body of literature surveys, we do not only provide a taxonomy and evaluate a wide range of recent research outputs that integrated blockchain within modern power systems. But we also draw some valuable lessons learned for each studied category and discuss the intersection of blockchain with various emerging paradigms that have the potential of radically impacting the smart grid. In addition, we present some real-world industrial initiatives and ongoing projects built on top of blockchain, dedicated for offering diverse electricity services with a case study of a pilot project on energy trading in Amsterdam. Finally, we discuss the remaining challenges and worthwhile opportunities of deploying blockchain in this particular area, with a focus on the aspect of operational cyber-security.

INDEX TERMS Blockchain, cryptocurrency, electric vehicles, energy trading, internet of energy, privacy, security, smart contract, smart grid.

I. INTRODUCTION

The global consumption of energy is anticipated to nearly double by 2050 according to a report published by the U.S. Energy Information Administration [1]. The findings indicate that this increase is particularly noticeable within certain regions in Asia, where the fast-paced economic growth is the major drive behind this increased energy demand. Furthermore, the electricity consumption is not only expected to increase within the industrial sector, but also within the residential and transportation sectors due to the enhancement of living standards with an increased demand for smart appliances and electric vehicles (EVs). This massive growth of energy demand would highly encumber the existing

The associate editor coordinating the review of this manuscript and approving it for publication was Mahdi Pourakbari Kasmaei.

electricity infrastructures, which are not only weak and outdated but already oversaturated. Not to mention that the overload generated from this increased demand would seriously congest the grid's network and deteriorate the quality of the energy transferred. In fact, the current power grid is suffering from a lack of visibility at the edge as a result of inadequate or even absent automatic monitoring, troubleshooting and fault diagnostic mechanisms. In addition, the underlying network of the grid is highly inflexible, making the integration of emerging distributed energy resources (DERs) based on renewable and green sources anything but a seamless task; which eventually negatively impacts our shared vision to transition to a clean and decarbonized grid in order to tackle the no longer deniable climate crisis.

On the one hand, the smart grid (SG) paradigm originated as a response to the challenges of the traditional power systems discussed above. As it can be inferred from its name, the SG is basically an ingenious electricity infrastructure that is intended to guarantee reliability, efficiency, flexibility and sustainability by the incorporation of information and communication technologies (ICTs) [2]. The paradigm enables a bi-directional flow of both energy and data within the grid. Meaning that energy can be delivered to customers from the utilities' generators and/or injected back to the grid by prosumers. Whereas the bi-directional flow of data signifies that both utilities and consumers/prosumers are able to collect real-time energy data and control dynamically the power flow. This bi-directional concept allows for acquiring an in-depth monitoring and understanding of the electricity usage patterns and predicting forthcoming actions in order to achieve more efficiency, real-time response and grid stability with lower costs. However, as appealing as the SG seems to be, the paradigm might not solve the challenge of efficiently deploying DERs management systems (DERMS) at a massive scale, while still meeting the level of scalability and cyber-security required to ensure a reliable and efficient electricity delivery and usage [3], [4].

Therefore, in an attempt to guarantee these fundamental requirements, the internet of energy (IoE) paradigm was instigated by the amalgamation of the SG concept with various cutting-edge technologies [5], [6], [7]. The IoE concept relies on the massive integration of internet of things (IoT) enabled devices, advanced monitoring and optimization algorithms, artificial intelligence (AI) techniques, and fog/edge-based components. The major goal of this creative and novel paradigm is to guarantee a sustainable and reliable power connection no matter when or where. By enabling a close and timely interaction among all entities and components of the grid, an autonomous decision-making, a wide range of bi-directional exchange mechanisms for electricity and data, a seamless access to massive DERs, a smooth adaptation to either centralized and/or distributed power resources, a sustainable and reliable energy demand management, and finally a flexible energy trading that still maximizes the overall social welfare.

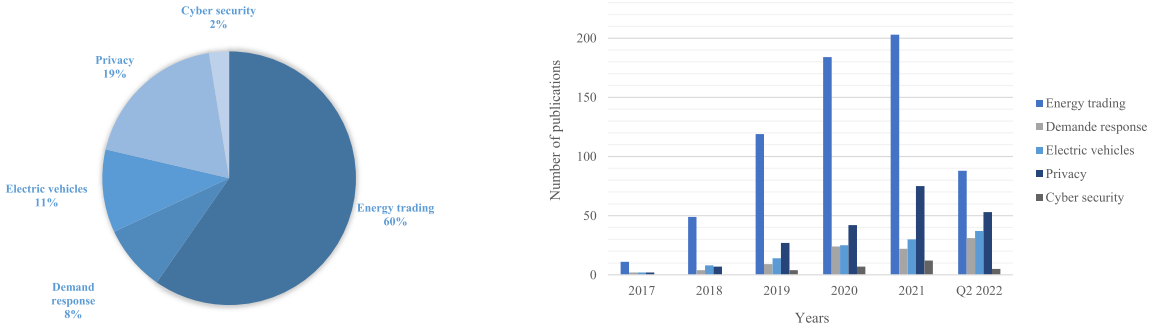
Yet, as the surface area of connected devices within the grid is growing, coordinating this enormous number of distributed components, and incorporating them adequately within the still centralized grid seems to be a major concern. Hence, a shift towards a semi-distributed grid seems inevitable to guarantee a dynamic integration of all these new elements. Nevertheless, managing a distributed grid, with a variety of complex devices, that is still relying on a vulnerable and traditional network and/or protocols designed to exchange raw data with no requirements of encryption or strong authentication seems to be a nightmarish scenario from a cyber-security perspective [8], [9], [10].

On the other hand, blockchain has been recently building momentum at a fast pace as an opportunistic technology for distributed systems. Blockchain is defined as a decentralized ledger managed by a peer-to-peer (P2P) network of nodes, with no centralized or trusted third party (TTP). Thus, mitigating a single point of failure and ensuring trustless autonomy. The participants within the network are in charge of creating, maintaining and storing the immutable chain of blocks following a pre-defined set of rules, namely the consensus mechanism. Which guarantees the reliability, accuracy and fault-tolerance of the ledger's replica among all nodes. The concept of blockchain is based on redundancy and decentralization, hence its resilience to system failures and cyber-attacks such as distributed denial of service (DDoS) attacks and false data injection attacks (FDIAs) faced within centralized systems. Even though blockchain was first built as the foundation of a P2P cryptocurrency market. It soon caught the attention of a vast number of researchers, institutions, companies, start-ups and even governments that saw in it a plausible solution to a wide range of problems. Among them enhancing the cyber-security of the shaking power grid by reinforcing it with the needed level of resilience and perhaps smoothing its transition to fulfilling the three Ds vision (i.e., digitalization, distribution and decarbonization).

A. BIBLIOMETRIC ANALYSIS

In order to first give the readers a synopsis of the existing literature's trend relevant to the adoption of blockchain within power systems, we carried out a bibliometric analysis. Where typical search engines and digital libraries were utilized (i.e., ScienceDirect and IEEE Xplore) for browsing and identifying the most relevant and recent research outputs starting from 2017 to the second quarter of 2022 (Q2 2022).

The used text search (TS) queries were limited to the title, abstract and/or index terms for precision and are the following: *TS1*=((''Index Terms'': ''blockchain'') AND (''Index Terms'': ''smart grid'' OR ''power system'' OR ''energy'') AND ((''Index Terms'' OR ''Abstract'' OR ''Title''): ''trading'' OR ''exchange'' OR ''auction'')); *TS2*=((''Index Terms'': ''blockchain'') AND (''Index Terms'': ''smart grid'' OR ''power system'') AND ((''Index Terms'' OR ''Abstract'' OR ''Title''): ''demand response'' OR ''demand side management'')); *TS3*=((''Index Terms'': ''blockchain'') AND (''Abstract'': ''smart grid'' OR ''power



(a) Publications on blockchain-based applications in the electric power sector between 2017 and Q2 2022 by categories.

(b) Evolving trend of published resources on blockchain applications in the IoE between 2017 and Q2 2022.

FIGURE 1. Blockchain-based applications and trends in the IoE.

system'') AND (''Abstract'': ''electric vehicle'' OR ''smart transportation'')); *TS4*=((''Index Terms'': ''blockchain'') AND (''Abstract'': ''smart grid'' OR ''power system'') AND (''Index Terms'': ''privacy'' OR ''anonymity'')) and *TS5*=((''Index Terms'': ''blockchain'') AND (''Abstract'': ''smart grid'' OR ''power system'') AND ((''Index terms'' OR ''Abstract''): ''security'' OR ''resilience'') AND (''Index terms'': ''access control'' OR ''intrusion detection'' OR ''anomaly'')). Out of these queries we were able to extract a total number of 1096 articles, of which 44 selected journal papers were extensively analysed and categorized into five inclusive areas (i.e., energy markets, demand response management, EVs charging, privacy and cyber-security) based on their research contributions.

Fig. 1a shows the total number of publications starting 2017 to Q2 2022, classified in terms of research targeting either the usage of blockchain for energy trading, publications addressing the demand side management within power systems, others centred around EVs, some concerned with the privacy issue, then solutions focusing on the cyber-security aspect of the grid by proposing blockchain-based prevention and mitigation mechanisms that protect the grid from cyber-attacks. As it can be inferred from the graph in Fig. 1a, it's easy to tell that the major focus up to this moment has been on energy exchange and trading, which is quite expected as blockchain is first and foremost a P2P cryptocurrency market. However, from Fig. 1b, depicting the evolution of the publications' trend throughout these past five years, we can see that the other use cases are starting to pick up momentum. Specifically, the privacy concern, as blockchain itself is still evolving as a technology offering more flexibility and new possibilities to better harness its features and address its own challenges. Yet, the focus on cyber-security is still modest, but it's worth acknowledging that collecting large scale data for research and bringing those findings to publications can take quite a while.

B. RELATED SURVEYS AND OUR CONTRIBUTIONS

Although the integration of blockchain with the SG paradigm is still at its infancy, the technology has already drawn enormous attention from the research community. During these past few years, a plethora of research outputs have been produced that aimed at addressing the challenges of the existing power systems. Up to now, a variety of literature surveys were carried out to examine these research outputs from various perspectives and application needs. For instance, some surveys attempted to overview blockchain application for P2P energy exchange [11], [12], [13], [14], [15]. Whereas the authors in [16], [17] focused on blockchain use cases within microgrids. Similarly, the authors in [18] also explored the adoption of blockchain within P2P microgrids and discussed the practical implications of this shift on institutions and academia.

Meanwhile, Whang et al. [19] explored the impact of blockchain on the energy sector by focusing on a visual bibliometric analysis and real-world applications. Then, a survey on blockchain-based projects/platforms for the electric power sector was carried out in [20]. Furthermore, Jogunola et al. focused on providing an extensive review regarding the potential of combining blockchain consensus algorithms with deep reinforcement learning in transactive energy systems [21]. Nour et al. [22] discussed the potential of adopting blockchain in the energy sector with a focus on pilots and industrial projects. In addition, a number of recent surveys have been presented to overview blockchain-based applications with smart grids [23], [24], [25], [26].

Nevertheless, the aforementioned surveys are either focusing on a specific use case such as energy trading or fail to offer a deep insight into the rationale behind the adoption of blockchain in the IoE as well as the realistic expectations and challenges that would occur from this integration. In Table. 1, we provide an extensive comparison between extant surveys in the literature and our proposed work in terms of various characteristics. Such as whether they cover a wide scope of applications, if they are up-to-date, if they go beyond blockchain to explore the potential of the integration of other emerging paradigms in SGs, and so forth.

In a nutshell, it is of tremendous criticality to determine exactly the recent state-of-the-art of blockchain applications within the IoE paradigm, as the intersection of these realms

TABLE 1. Summary and comparison of important surveys on blockchain-based applications in the IoE.

Ref.	Wide Scope	Up-to-date	Enabling Technologies	Case Study	Cyber Security Potential	Lessons Learned	Technical Challenges	Research Directions	Remarks
[11]	L	L	N/A	N/A	N/A	L	L	L	Focuses on reviewing the deployment and potential of blockchain for decentralized transactive energy.
[12]	L	L	N/A	N/A	N/A	L	L	L	Studies and categorizes the existing P2P blockchain-based energy trading schemes.
[15]	L	M	L	N/A	L	M	M	M	Reviews and examines several energy trading schemes used in the smart grid with a discussion on blockchain's potential.
[18]	L	L	N/A	N/A	N/A	M	M	M	Proposes an analytical framework for P2P microgrids, based on a literature review as well as expert interviews, that incorporates technological, economic, social, environmental and institutional dimensions.
[19]	L	M	N/A	N/A	N/A	L	L	L	Combines a bibliometric and visual analysis to explore what blockchain means to the energy sector with some real-world applications.
[20]	L	L	N/A	N/A	M	M	M	M	Discusses the integration of blockchain into smart energy systems with a review of several important platforms.
[21]	L	M	L	N/A	N/A	M	M	M	Explores the principles, potentials, and current research efforts in regard to the integration of AI into energy trading consensus mechanisms.
[22]	H	H	N/A	N/A	M	M	H	H	Provides a review of potential applications of blockchain in various electricity domains with some industrial-based applications.
[23]	M	M	N/A	N/A	L	L	L	L	Discusses the potential and applications of blockchain and its consensus algorithms within the IoE with some future insights.
[24]	M	M	N/A	N/A	M	M	L	L	Categorizes the applications of blockchain in smart grids, then introduces the current progress and future directions.
[25]	L	M	N/A	N/A	N/A	L	L	L	Studies the transition of electricity systems to energy internet with a focus on blockchain as an enabling technology.
[26]	H	H	N/A	N/A	M	M	M	M	Reviews the state-of-the-art approaches focusing on the integration of blockchain with smart grids.
Our survey	H	H	H	H	H	H	H	H	We provide a holistic review of the existing solutions both in the literature and industry that integrate blockchain and IoE with some valuable lessons learned. In addition, we discuss the intersection of blockchain and IoE with other emerging paradigms. We also examine a real-life case study and discuss the remaining challenges as well as future perspectives.

L : Low Coverage M : Medium Coverage H : High coverage N/A : Not Applicable

is evolving rapidly. In order to assess the remaining opportunities that are worth investigating as well as challenges and pull-backs that could also be the focus of future research work. Thus, the major goals of our survey paper are to first examine comprehensively and critically a variety of literature blockchain-based applications in future SGs that we categorized into five main areas. Second, to give an overview of the IoE-based industrial initiatives and projects that leveraged blockchain as an underlying infrastructure. Third, to pinpoint the research gaps in the existing literature. And last, to investigate the still unresolved challenges as well as future research directions. To summarize, the major contributions of this survey paper are the following:

- We provide a brief yet concise introduction to blockchain including the history of the technology, how it evolved and its major pillars (i.e., P2P networks, consensus algorithms, cryptography and hash primitives), we also discuss the different layers of the blockchain stack, their components as well as the different ways a blockchain-based system can be configured (i.e., permissioning and/or off-chain approaches).
- We then discuss the rationale behind the adoption of blockchain in future electrical power systems which is twofold: (i) the push from conventional, fossil-fuel based and centralized power systems to distributed SGs with a massive integration of DERs; and (ii) the pull from the decentralized, fault-tolerant nature of blockchain as well as its strong cryptographic tools and cyber-security features.
- We present an exhaustive and up-to-date literature review of the existing blockchain-based solutions and approaches that were designed in the recent years focusing on the IoE, including the mechanisms utilized, their implication and limitations. We also classified these research outputs into five inclusive areas (i.e., energy trading, demand side management, EVs, privacy and cyber-security).
- We explore the intersection of blockchain with other emerging technologies and paradigms while discussing the implication and aftermath of this amalgamation on future IoE-based SGs.
- We highlight some industrial projects and platforms that have been developed recently as a response to the

growing interest in blockchain application for electrical power systems. Where we focused on innovative green cryptocurrencies dedicated to incentivizing the use of renewable and clean energy resources, as well as various projects focusing on a wide range of applications such as energy exchange, demand side management, load balancing and carbon compliance units or green certificates.
- We present a case study of a P2P energy trading pilot project that was launched in Amsterdam and discuss the major technical as well as regulatory challenges faced during the project.
- Finally, we draw some lessons learned as well as a realistic perspective with regard to the remaining challenges both in terms of blockchain itself and the energy sector, we also discuss the potential opportunities that are still yet to be taken and translated into concrete solutions.

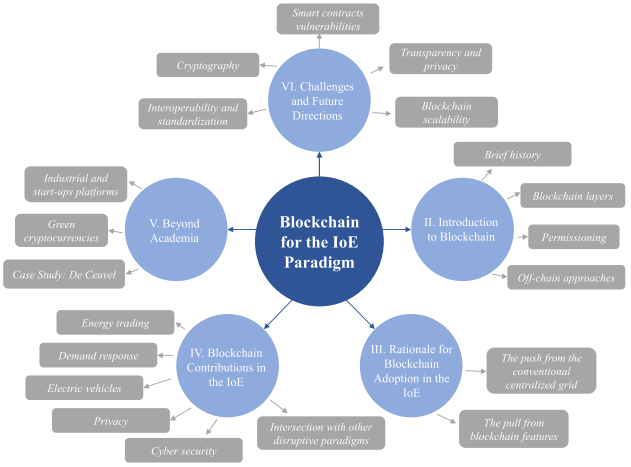


FIGURE 2. Paper organization overview.

C. PAPER ORGANIZATION

The remainder of this paper is organized as follows. In Section II we provide some background notions relevant to blockchain. Section III discusses the evolution that current power systems are witnessing and their shift towards distributed, reliable and secure systems assisted with blockchain technology, where we answer why blockchain precisely. Then, in Section IV we categorize and provide an in-depth evaluation of the major contributions of blockchain in the IoE, in the addition to the intersection of the technology with other paradigms. Section V is dedicated for some industrial blockchain-based initiatives and projects within electrical power systems around the whole globe, with a case study. In Section VI we provide a rational perspective of the challenges remaining with the integration of blockchain within SGs and discuss some worthwhile opportunities. Finally, we conclude this paper in Section VII. In addition, for the reader's convenience we have included a list of abbreviations utilized throughout this paper in Table. 2, whereas Fig. 2 represents an overview of the structure of the whole paper.

TABLE 2. List of Acronyms.

Abbreviation	Expanded name
AI	Artificial Intelligence
APIs	Application Programming Interfaces
BFT	Byzantine Fault Tolerance
CIDS	Collaborative Intrusion Detection System
DAG	Directed Acyclic Graph
DApps	Decentralized Applications
DDoS	Distributed Denial of Service
DERs	Distributed Energy Resources
DERMS	DERs Management Systems
DPoS	Delegated Proof of Stake
DT	Digital Twin
EMS	Energy Management Systems
EVs	Electric Vehicles
EVM	Ethereum Virtual Machine
FDIA	False Data Injection Attack
ICTs	Information and Communication Technologies
IEDs	Intelligent Electrical Devices
IoE	Internet of Energy
IoT	Internet of Things
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PoA	Proof of Authority
PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof of Work
PV	Photovoltaic
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SG	Smart Grid
SHA	Secure Hash Algorithm
SP	Service Provider
TPS	Transaction per Second
TTP	Trusted Third Party
UIs	User Interfaces
UTXO	Unspent Transaction Output
V2G	Vehicle-to-Grid
VPPs	Virtual Power Plants

II. BLOCKCHAIN PRELIMINARIES

The aim of this section is to lay down the important background notions relevant to blockchain which is threefold: first a brief history of blockchain, second a description of its abstract layers, last its different modes of configuration.

A. A QUICK DIVE INTO THE HISTORY OF BLOCKCHAIN

Blockchain made its first public debut as a revolutionary technology when Satoshi Nakamoto published the notorious white-paper *"Bitcoin: A peer to peer electronic cash system"* back in 2008, which provided a detailed description of an utterly P2P version of a digital monetary system, namely Bitcoin [27]. The technology was seen as ground-breaking because it offered a concrete solution to the problem of digital trust. Blockchain is defined as an open, dispatched and transparent ledger with the capacity of providing verifiable and permanent records of each transaction between all the different parties.

In brief, the technology is built on top of a P2P network, where peers are collectively abiding by a consensus mechanism for inter-node exchange and acceptance of new

blocks. Once a block is chained to the distributed ledger (i.e., blockchain) its transactional data cannot be subject to any modification retroactively, without changing all the subsequent blocks of the replicated chain, which necessitates having control over the majority of the blockchain's computational resources. Furthermore, rather than being owned by a centralized server or authority, the blockchain ledger is dispatched across all peers' part of the distributed network, which ensures that an identical copy of the ledger is saved among the different nodes to be seen, verified, and/or audited by any node anytime and anywhere.

Five years after the release of the first functional blockchain (i.e., Bitcoin), Vitalik Buterin (the co-founder of Ethereum) started being frustrated with bitcoin's programming limitations and began pushing towards more of a malleable blockchain. However, met with a pull-back from the Bitcoin community, he set forth to construct the second public blockchain, namely Ethereum, known as blockchain 2.0 [28]. In a nutshell, the proposed platform (i.e., Ethereum) is a programmable blockchain, which does not only enable the exact same functionalities of Bitcoin, such as smooth, pseudo-anonymous and international financial transactions. But is also capable of running decentralized applications known as DApps based on smart contracts within the Ethereum virtual machine (EVM). During the middle of 2014, the platform received some online funding, which then led to its release in 2015.

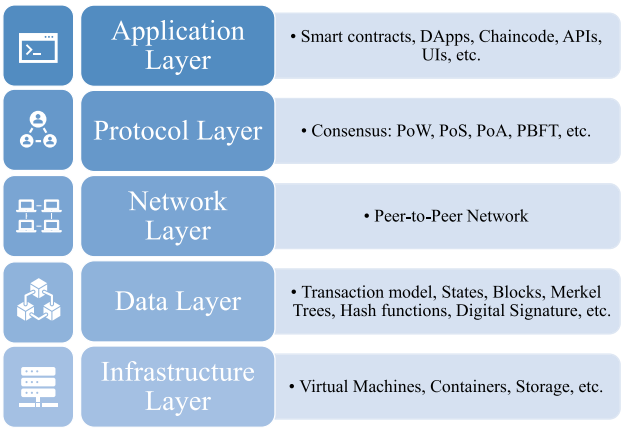


FIGURE 3. Blockchain stack model.

Blockchain, the technology that was once used to only exchange Bitcoin, has evolved over the past decade into one of today's greatest pioneering paradigms, with more and more emerging platforms such as the Hyperledger projects under the Linux foundation (e.g., Fabric, Besu, Burrow, etc.), Corda, Parity, Ripple, Tendermint, IOTA, etc. The technology has proven its high potential to impact every industry, from finance to manufacturing and supply-chains to critical infrastructures such as the electrical power grid, which is the main focus of this survey paper.

B. TOP-DOWN DIVE INTO BLOCKCHAIN LAYERS

The blockchain's stack, which is depicted in Fig. 3, can be mainly divided into five components: application layer, protocol layer, network layer, data layer and infrastructure layer. In what follows, we discuss each of these abstract layers in further detail.

1) APPLICATION LAYER

Being at the top of the technology's stack, the application layer is comprised of instances that are primarily utilized by end-users in order to interact with the blockchain network. These include smart contracts, DApps (in case of Ethereum), or chaincode (for the Hyperledger Fabric) as well as scripts, application programming interfaces (APIs) and user interfaces (UIs). Precisely, the blockchain network acts as the back-end system for these applications, where they establish a connection with it using APIs. Then, each transaction initiated would be executed following the predefined rules and conditions within the smart contract/chaincode, which guarantees the deterministic feature of blockchain.

Within a blockchain-based system, smart contracts are defined as self-autonomous executing digital programs, which contain a set of conditions and terms of agreements. The concept was first defined by the developer Szabo in [29]. It is intended to facilitate and enforce the execution of any given agreement in a decentralized manner among different entities, in opposition to a traditional contract in which a TTP is needed. In the case of the Ethereum blockchain, these smart contracts are designated to run within a particular virtual machine (i.e., EVM), whereas in the case of the Hyperledger Fabric, chaincodes are supposed to run within containers (i.e., Docker).

2) PROTOCOL LAYER

The process by which all nodes agree on whether a transaction gets to be added to the shared ledger or a block to be orphaned is what we refer to as a consensus protocol, which is the very core principle of every blockchain platform. Consensus mechanisms are utilized to ensure that the whole system is not governed by any central entity, but rather a majority of peers jointly working together to reach a logical agreement, even with the possibility of having faulty nodes or even malicious ones within the network. For efficiency, we have decided to discuss only the widely adopted ones in this subsection. However, we refer the reader to the following surveys that provide an in-depth discussion of several consensus approaches that currently exist in the literature [30], [31]. Whereas the authors in [32] also review the existing body of consensus algorithms in the literature, but with a particular focus on the ones applied in SGs.

Proof-of-Work (PoW): With no single doubt, PoW has been the de facto consensus protocol since the beginning of blockchain, precisely with Bitcoin. The algorithm requires solving a hard-mathematical puzzle (subject to frequent changes in terms of complexity to keep the network secure)

that the mining nodes are competing for. When a peer solves the puzzle (i.e., verifies the transactions and calculates the block's nonce) the mined block (i.e., the block to which the solution of the puzzle or nonce is attached) is then broadcasted within the blockchain network to be validated by the rest of the nodes to make sure that it is not fraudulent. Once the consensus regarding the legitimacy of the block among the peers is reached, the validated block will be chained to the previously mined blocks and the miner will get the incentives for his computational work (i.e., finding the nonce).

It is important to note that in order for the nodes to reach an agreement, the majority of peers needs to be in consensus. Hence, it is less likely for a fraudulent block to be validated unless a node (or a mining pool) is in control of at least 51% of the mining resources. Finally, it is worth mentioning that PoW can hardly be considered as a green consensus mechanism and this is due to the enormous resources it requires in terms of computation to achieve mining. In fact, based on a study conducted by the Cambridge Centre for Alternative Finance [33], Bitcoin currently consumes around 79 Terawatt Hours per year, which is nearly equivalent to twice the annual energy consumption of New Zealand.

Proof-of-Stake (PoS): Quite the opposite from PoW, PoS does not rely on a mining approach in which a node has to invest some computational power to solve a puzzle. Rather, the node allowed to create the next block is decided following a random approach. Well, an ''almost'' random approach to be more accurate, as the selection is based on the amount of stake a node has, so the more stakes a node has (basically the wealthier the node is) the more likely the peer will get chosen to mine/create the new following block in the chain. The original version of the protocol doesn't include the notion of rewards, in opposition to its extensions which does include it as well as the notion of punishment of miners following their performance. The primary downside of the PoS mechanism is that the selection procedure is based on how much wealthy is an account, which might eventually lead to a centralized network controlled by a set of unique accounts who own the majority of stakes, leading to an unjust dispersion or none at all (i.e., no decentralization). Meanwhile, in a recent attempt to address the carbon footprint of mining Ether (i.e., Ethereum's cryptocurrency) the platform is currently working on shifting its consensus protocol from Ethash (a variation of PoW) to PoS.

Delegated Proof-of-Stake (DPoS): Derived from the previous consensus we discussed, DPoS is based on the concept of having peers within the blockchain network vote and elect a delegated node (referred to as a witness) that would be in charge of validating the new block. The procedure of voting on delegates is done by pooling tokens into a staking pool associated with a certain delegate. The number of witnesses that other peers can choose from is limited, roughly scaling from 20 to 100 depending on the implementation of the protocol, in order to guarantee that a witness that was chosen to validate a block during a given epoch is not the same during the next one. Meanwhile, the peers that voted for a successful delegate also receive a reward based on the share of their stake. DPoS offers a more democratic approach to the procedure of selecting a validator, as it allows a wide range of peers to take part of the voting mechanism. In addition, as the number of delegates is limited during each round this ensures a quick finality in terms of blocks' creation. The protocol was first implemented on BitShares back in 2015 and is being used by various blockchain platforms such as Cardano.

Proof-of-Authority (PoA): Building one's reputation can take years of work, but ruining it can be done in a matter of minutes. That's basically the core idea behind the PoA consensus algorithm. The mechanism does not require any mining, but it rather uses sealing, a process by which a validated sealer (or voter) can approve a block. The algorithm was invented by Gavin Wood (the co-founder of Ethereum and Parity). In PoA, sealers are not incentivized using coins but rather in terms of reputation. By attaching a reputation to each validator, they are driven to act in a non-malicious way to uphold the position they have gained. Furthermore, PoA only allows sealers to approve blocks in a non-consecutive turn to avoid having a centralized network in terms of validation. In addition, the consensus can tolerate up to half the nodes being compromised.

Proof-of-Elapsed-Time (PoET): The consensus offers a solution of the computational problem of randomly selecting a leader in a fair manner and was developed in early 2016 by Intel Corporation. Following PoET, each peer in the P2P network should generate and wait for a random chosen period of time. While the node with the shortest time, meaning the one that first finishes the chosen sleeping time, gets to validate the next block. The consensus enables running applications within a trusted execution environment, guaranteeing that the random selection of the waiting time as well as its completion are genuinely met. PoET is currently utilized within the Hyperledger Sawtooth distributed ledger sponsored by Intel.

Practical Byzantine Fault Tolerance (PBFT): Like PoA, a miner following the PBFT consensus protocol doesn't need to invest any resources to create a block, but instead relies on a Byzantine fault tolerance (BFT) mechanism. The procedure starts with the selection of a leader, to which all peers within the network agree. Then, the chosen leader is responsible for the creation of the new block to validate the transactions and disperse the block to all the remaining peers. A transaction can be committed to the blockchain only and only if two thirds of the peers vote on its legitimacy. Furthermore, to guarantee that the solution won't fall into a centralized approach each leader is subject to frequent changes. Although PBFT has proven its practicality in terms of scalability compared to its competitors, the mechanism suffers from some network overhead issues [34]. Furthermore, it can only tolerate up to one third of the peers being compromised.

3) NETWORK LAYER

This layer defines the network topology of all blockchain systems and is basically a P2P network that has the responsibility of coordinating the communication between the

different nodes. The network layer manages the transactions, how blocks are propagated and the procedure of discovery among peers. Specifically, this layer guarantees that all peers are able to discover one another, to communicate, broadcast transactions/blocks and synchronize their own copy of the ledger as well as state of the whole chain of data to ensure the validity and reliability of the blockchain network. In a nutshell, P2P networks are based on a distributed architecture where every node participating in the network shares his own resources (e.g., computing, storage, links, etc.) with other nodes of the network. In addition, the aforementioned shared resources can be leveraged for the provision of different services (e.g., file sharing and storage, parallel computing, anonymized routing for traffic, etc.) accessible to all participants without the need of a centralized entity to manage them.

Blockchain itself, as mentioned previously, is based on a P2P network topology to guarantee a decentralized and fault-tolerant system. Furthermore, nodes within a blockchain network can be either node members (also referred to as light nodes) or mining/voter nodes (also referred to as full nodes). The node members are consumers of the services provided by the blockchain, and they only keep block headers for the sake of verification rather than the full chain. Whereas the mining/voter nodes are peers who are not only consumers, but they also validate and verify the new transactions based on a predefined and agreed upon consensus protocol. The overall functionality of these miners/voters is to maintain a valid copy of the shared ledger, broadcast the newly generated transactions and group them into blocks to be validated then chained by enforcing the consensus rules.

4) DATA LAYER

The data layer is based on a variety of concepts that jointly constitute the building blocks of a blockchain system. These concepts are transaction-models, data-structure, Merkel trees, hash functions and digital signatures. The widely used transaction models within blockchain systems are unspent transaction output (UTXO) and account-based models. In the first one, a transaction represents a transfer of the UTXO ownership to the recipient. Whereas the second has more efficiency as it is based on atomic updates of the state of accounts, where a transaction can be initiated from a user account to either another user account, or a smart contract account by triggering its execution.

Within the blockchain ledger, transactions as well as the smart contract states are contained inside the blocks, which are jointly linked to form the whole chain. This is achieved by using the hashed content of the preceding block as the value of a section within the header of the recent block. Both Ethereum and Hyperledger Fabric follow a double-layer structure for data to arrange the content of each block. The states are saved within a key-value database, such as LevelDB for Ethereum or CouchDB in the case of Hyperledger Fabric and are indexed using the Patricia-Merkle tree or Bucket-Merkle tree in the case of Ethereum and Hyperledger Fabric respectively.

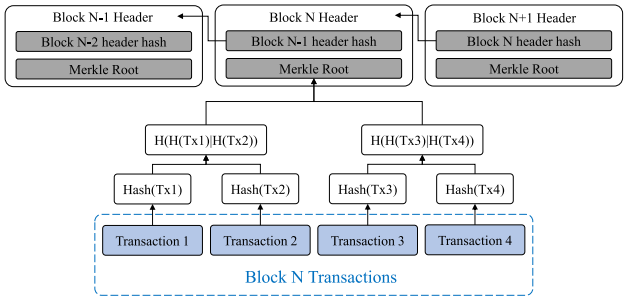


FIGURE 4. Blockchain Merkle tree representation.

Furthermore, blockchain is also heavily relying on hash functions defined as one-way mathematical functions that have a string, with no length restrictions as an input and give a string output of a well-defined size, which is referred to as the hash value, checksum, or electronic fingerprint. These functions are characterized by merely three distinguishing features: collision free (i.e., finding two different inputs with the same output is hardly possible), hiding (i.e., it is implausible to figure out the input of any hash hence the one-way) and puzzle friendly (i.e., finding the hash of any data is not computationally expensive). The hash function used in blockchain is the secure hash algorithm (SHA), precisely the SHA-256 version (or the Keccak-256 for Ethereum).

Meanwhile, in order to build a blockchain data structure a hash pointer is needed, which is a hash pointing out to the referenced data. Basically, each blockchain header contains the hash of the previous block that was chained to verify the non-repudiation of data inside blocks. This concept, depicted in Fig. 4, constitutes an important part of blockchains' data-structure, along with Merkle trees that are themselves binary trees of hash pointers.

In addition, among the building components of blockchain's data layer is the digital signature. The technique is based on a pair of public/private cryptographic keys (i.e., P_k and S_k), which ensures the wholeness, non-repudiation and authenticity of a transaction as well as its origin and it also allows others to verify it. Precisely, the digital signature leverages the asymmetric cryptography, as each user has two keys combined, the S_k is supposed to be kept safe, and the P_k is to be known by anyone to verify a signature, or could be used for the encryption of some private data that need to be sent to a specific user and only his S_k would be able to decipher it.

Back to blockchain, the technology leverages precisely the elliptic curve digital signature algorithm for its digital signatures. The procedure is based on the following steps: generate, sign and check. First the cryptographic pair of keys, S_k and P_k, are created using the proper tools for that depending on the platform. The user is supposed to keep the S_k while the P_k is shared over the P2P blockchain network. Then, upon the creation of a transaction, it should be signed with the S_k and the output of the method is added to the transaction as a digital signature to prove the origin and integrity of the transaction, meaning that its content has not been tempered

with. Finally, every node in the blockchain network can check the validity of a transaction using the P_k of the sender and the digital signature attached to it.

5) INFRASTRUCTURE LAYER

Finally, the infrastructure layer is composed of all the necessary tools needed for the execution of the contracts or low-level machine codes (i.e., bytecodes) within the dedicated runtime environment configured on each peer of the blockchain network. For instance, the Ethereum platform has its unique virtual machine (i.e., EVM), which allows for the processing of each transaction in the network. The EVM is a Turing complete virtual machine (in brief, a Turing machine is a machine capable of simulating any computer algorithm) based on a stack architecture in which each item is of a 256-bit size with a maximum stack size of 1024-bit. As for its memory, the storage is based on a volatile word-addressed byte array. The EVM also disposes of a non-volatile memory which is responsible for storing the Ethereum states.

Meanwhile, the storage of the smart contracts code is managed separately within a virtual read-only memory with restricted access control. In addition, smart contracts in Ethereum are written in Solidity and compiled utilizing Solidity compiler into bytecode, which is an assembly language formed of multi-opcodes (where an opcode is responsible for performing a given task on the blockchain). Meanwhile, Hyperledger fabric uses Docker containers to run its chaincode, which can be written either in GoLang, node.js, or Java. It is worth noting that the environment dedicated for the execution of the smart contracts or transactions should have a high efficiency, where the results must also be of a deterministic nature to prevent having uncertain or inconsistent states among all peers. As this discrepancy would result in wasted computational resources and lower the overall system's performance.

C. DIFFERENT MODES OF CONFIGURATION

In this subsection, we highlight the different manners in which a blockchain system can be configured based on its level of permissioning, and how it can process transactions outside the main-chain.

1) LEVELS OF PERMISSIONING

Starting with blockchain's permissioning, this can be broadly categorized into three main degrees: public, private, or consortium. Within a public blockchain, such as Bitcoin or Ethereum mainnet, joining or taking part of the blockchain network main activities is allowed for anyone. This includes reading, writing, or auditing the public chain, which basically sustains the network's self-governance. Public blockchains operate following incentive models that motivate additional peers to join the network and maintain its agility. This type of blockchains is extremely valuable in a sense of being fully decentralized and not relying on a TTP or/and a central authority to provide their functionalities. However, they still come with their own drawbacks as they necessitate high energy consumption to carry on the mining tasks sustaining the chain, in addition to their limited privacy.

Meanwhile, a private blockchain is totally at the opposite end of the permissioning spectrum compared to a public one. Participants are extremely limited and can only join the network upon a strict verified selection procedure, which is authenticated by the owner or operator of the blockchain (e.g., a company). The degree to which the peers are allowed to participate in the blockchain activities (e.g., sending transactions, mining, executing the consensus algorithm, maintaining the ledger, etc.) is also highly restricted, while the operator has the full right to manage the network. In this sense, a private blockchain is not fully decentralized but can be seen as rather a distributed and secure database operated using cryptographic mechanisms.

Finally, between the two extreme ends we find the permissioned blockchains or also referred to as consortium. This type enables a mash-up between public and private blockchains as it supports a wide range to customized features, such as granting access to anyone but only with an adequate identity verification as well as a set of permissions based on roles that can be allocated to the peers, that enable the performance of specific tasks (e.g., create, validate or read blocks) within the blockchain network. This type of blockchains has attracted the attention of many businesses for a wide range of applications during the past years, and this is due to their flexibility in terms of configuration but also their decentralization as they are not fully owned or controlled by a single authority.

2) OFF-CHAIN APPROACHES

Even though the original idea behind blockchain was that everything should be processed on-chain and recorded on the immutable shared ledger. The scalability issue from such approach has pushed towards off-chain solutions to alleviate the burden of having each transaction processed by the main chain, and eventually to increase the overall throughput of blockchain-based systems. Off-chain solutions can be divided into either off-chain transaction protocols or approaches dedicated for off-chain storage. For the first type, there is a wide range of off-chain transaction protocols that are built on-top of an existing blockchain network (e.g., Bitcoin or Ethereum), referred to as layer two solutions, that offer the benefit of cheap and rapid transactions. For instance, the Lightning network enables peers to transfer bitcoin off-chain instantaneously, without any transactional fees. Whereas the Liquid network is a side-chain protocol that allows rapid settlement than Bitcoin, in addition to the feature of enabling confidential transactions where the amount transferred within the transaction is unknown.

Moving on to the second type, due to the transparent nature of blockchain-based systems, storing critical data on-chain might raise some privacy concerns. In this regard, some solutions have been dedicated to address this by leveraging off-chain storage, in a sense that the actual data would be stored somewhere safe, with only the metadata with a hash

pointer or a cryptographic proof being recorded on-chain within the immutable ledger for audit and non-repudiation. In addition, storing large files within the blockchain ledger would only add-up to its exponential rise, which would be cumbersome in the long run. This is due to the duplicated nature of blockchain, where each node is supposed to keep a replica of the whole chain.

Summary and Main Takeaways

Blockchain was first fully conceptualized back in 2008 in the form of the bitcoin network. Soon after, myriads of other platforms were developed that allowed the technology to go beyond the concept of solely transacting cryptocurrencies, by integrating smart contracts for intelligent computations. The technology owes its ingenuity to the clever rearrangement of existing concepts such as digital signatures, hash functions, Merkle trees, P2P networks and distributed systems. Blockchain relies on its consensus mechanisms that can be broadly classified under proof-based or voting-based algorithms, which guarantee the correctness of the shared ledger. Last, a blockchain-based system can be set as public, private, or consortium. Whereas its computation and storage could be fully on-chain or partially, using off-chain techniques to scale the overall system.

III. RATIONALE FOR BLOCKCHAIN ADOPTION IN IoE

In this section, we discuss the rationale behind adopting blockchain for IoE-based systems, which is twofold. First, we investigate the push from the traditional centralized, fossil fuel-based power grids to more digitalized, decarbonized and decentralized systems. Second, we weigh in the pull from the distributed nature of blockchain technology and its attractive security properties, that are well aligned with the requirements needed for the next smart grid paradigm.

A. THE PUSH FROM CENTRALIZED POWER GRIDS TO DERs

Since the late 19^{th} century, electrical grids all over the globe had three main features in common. First, central power plants running on fossil fuels (e.g., coal or natural gas) were the backbone of their energy generation. Second, managing these power systems in terms of scheduling the production within the generators and delivering the electricity to end-users was carried out in a unidirectional and centralized manner by either utilities or regional authorities. Which left consumers with no control or whatsoever over their power usage, whereas utilities had to ensure a reliable generation of electricity to meet the fluctuating consumers' demand. Third, grid utilities had a constrained visibility over real-time consumption data, or the state of the grid's components deployed over the edge of the distribution system.

As hard as it is to accept, these three aspects are still the reality of some if not most power grids all over the globe, nevertheless, we have started to witness some changes during these past decades. First and foremost, the proliferation of DERs (e.g., roof-top solar panels, micro-turbines and others) is threatening the dynasty of centralized fossil fuel-based plants, which is becoming a necessity more than ever now as we're experiencing more catastrophic and disastrous effects of climate change. Consequently, this growth in terms of distributed green resources is making the second feature of traditional power systems (i.e., centralized management) a complicated task in terms of operation. In the past, utilities relied solely on adjustable power generators to sustain the electricity supply. However, a growing amount of this power is being generated now from solar or wind based DERs relying on a fluctuating supply following the weather.

Furthermore, customers are rapidly taking control over their own electricity consumption and/or production by massively deploying DERs locally. In the form of roof-top solar panels with IoT-based devices enabling a smart and optimized management of their energy consumption. For instance, commercial customers can utilize their local batteries as well as energy optimization algorithms to adjust their demand in order to reduce their bills. Whereas residential customers can monitor their smart electric appliances such as thermostat, air conditioner or even charging EVs to optimize their electricity usage. Eventually, these new capacities are supposed to enable the power grid to efficiently balance supply and demand. Yet, and for the time being, empowering electricity end-users is only stressing the traditional centralized model for managing power grids. For instance, utilities in California would be required to make some hefty improvements to the distribution grid in order to meet the rising power supply and demand in some area resulting from the increasing enthusiasm towards EVs [35].

Last but not least, the current power grid is experiencing a large-scale wave of digitalization that would enable the creation of massive volumes of operational information, that could be eventually leveraged for big data analytics and forecasting. In fact, nearly 47 billion U.S. dollars were used globally during 2016 as investment in digital infrastructures and software for the electricity grid, by integrating new sensor devices at both the transmission and distribution levels (i.e., EVs charging stations as well as upgrading the old ICTs components) [36].

As a consequence of this ever-growing and profound shift within power systems, operators are acquiring at a slow pace the ability of real-time monitoring the electrical grid operations, scaling form supply/demand imbalance, forecasting energy trends, to customers electricity usage profiles. Although these advancements remain embryonic as power grids still function widely the way they did in the past century, these transitions will eventually get more evident with time. However, merely crucial actions taken by utilities are able to steer the revolution of power systems to guarantee more reliability and efficiency as well as cheap and clean energy. Where prosumers can feed back their surplus of energy back to the grid to meet the energy demand, and EVs can be seen

as mobile batteries that could also direct their electricity to the grid.

Hence, utilities, customers and stakeholders should be all working jointly to exploit the massive bi-directional flow of real-time data in order to guarantee a seamless operational and secure grid. Simultaneously, as the electric power sector is undergoing this profound transformation, blockchain came to light as a compelling technology dedicated to ease the complexity of managing distributed trustless systems in the digital realm. The conjunction of these two trends rationalizes the rise of blockchain-based contributions and initiatives within the electric power sector. Yet, it's worth mentioning that this is beyond a mere coincidence or a hype, as the technology offers various features arguably seen as fit to enable the grid's transition to a fully distributed as well as secure system, which we will discuss in the next subsection.

B. THE PULL FROM BLOCKCHAIN's DESIRABLE FEATURES

Every critical infrastructure is required to be built in a way that ensures security, privacy and trust. Hence, the future SG is no exception to this rule. Precisely, this cyber-physical system is required to guarantee that access to critical data or resources is only performed upon correct authentication, to rely on strong cryptographic primitives, to prevent tempering with data, to enable a reliable auditing and logging of all performed actions/operations, to be fault-tolerant with no single point of failure, to provide seamless troubleshooting and monitoring of all components, to protect private data from being divulged and finally to be fully transparent, with inherent trust and democracy between all participants.

Bitcoin (i.e., the pioneer implementation of blockchain) was seen as revolutionary not in terms of its novelty but more because of its practicality as it offered the first concrete solution that established trust within a distributed system by proposing PoW (i.e., the consensus mechanism of Bitcoin). Nonetheless, all blockchains don't rely solely on their consensus algorithms but they are also leveraging other mechanisms that build intrinsic security and trust (which are needed within SGs to achieve the goals mentioned in the first paragraph of this subsection). Including hash functions that ensure the reliability and integrity of the whole chain, digital signatures for non-repudiation, cryptography for confidentiality, timestamps to prevent replay attacks and incentive mechanisms to guarantee the sustainability of the system, as well as other techniques we have already detailed in Section II. In addition, although blockchain was first designed to serve as a P2P digital cash system, which still counts for the vast majority of its applications (i.e., cryptocurrencies) to this moment. It is worth stressing that there is no necessity in developing a crypto-token to build a blockchain-based distributed system that still makes use of all remaining security features of the technology.

As we have discussed in the previous subsection, the way that the SG is designed relies heavily on a centralized model in which entities or participants depend on a central authority, platform or intermediary to make use of various ancillary services or operational technology systems e.g., supervisory control and data acquisition (SCADA), energy management systems (EMS), etc. Although, it is worth acknowledging that for the time being these approaches are still able to deliver fairly what they have promised, this might no longer be the case with the rising challenges and complexity that the SG is facing. Specifically, the proliferation of DERs, EVs and prosumers at a large scale would expand the landscape of security threats and complexity of the cyber-physical grid.

Consequently, the topology of current power systems is expected to take a drastic shift from being fully centralized to incorporating various distributed aspects by enabling automated and wider P2P interactions as well as increased flexibility and visibility between the grid's entities at the edge. Similarly, this decentralization is also witnessed at the market level of the grid which is slowly experiencing with P2P energy exchange models among prosumers. While the SG is progressively evolving towards a degree of distribution, the application of blockchain seems to be an intuitive yet justified choice that would enable a seamless transition of the SG due to the technology's characteristics, detailed below, that overlap with the IoE paradigm's requirements.

1) DECENTRALIZATION

Blockchain is basically a P2P network as mentioned previously, meaning that it is a set of distributed peers jointly interconnected and able to maintain the shared ledger using the predefined consensus algorithm. Thus, a blockchain-based system is able to perform its tasks without the need of intervention from a central-authority. In addition, this topology is aligned with the structure of DERs, or broadly speaking, the edge components of the electricity grid, which are lacking the security and proper visibility needed as well as automated control.

2) AUDIT AND TRANSPARENCY

As the whole blockchain ledger is stored within all nodes part of the P2P network, this inherently guarantees a high level of transparency of the system, thus all peers are capable of verifying the reliability of any transaction within the chained record that is immutable (only if no adversary is in control of more than 51% of the blockchain's resources). Eventually, as blockchain is transparent, meaning anything that happens within it can be seen by other peers, this feature guarantees its auditability and that all participants can be held accountable for their previous actions logged in the ledger, thus being unable to deny them. Which could enable tracing back the root of cyber-attacks.

3) BUILT-IN-TRUST

The concept of blockchain shifted the notion of trust in people or institutions to trust in technologies. In other words, the way blockchain is constructed enables it to work without relying on trusted intermediaries or centralized entities as trust is built-in within its components (i.e., consensus protocols, cryptography, P2P networks and smart contracts). Thus,

trust within blockchain is not enforced by institutions, but it's already encoded within the way it was designed and conceived.

4) RECORD's IMMUTABILITY

As blockchain leverages cryptographic primitives, hash functions and Merkle trees to structure all transactions within the shared ledger which is in synchronization among all peers. The information within each block can't be subject to change without altering all previous blocks due to the chained nature of the ledger, which requires an adversary to be in control of the majority of the nodes within the blockchain network. Thus, guaranteeing the integrity of the SG's data.

5) SECURED EXECUTION

Blockchain-based systems inherent their cyber-resilience and security from the way the technology is built. As blockchains are distributed systems this ensures their fault-tolerance and guarantees that they don't have a single point of failure that could easily be targeted by an adversary. In addition, in the case of a malicious activity within the network, the root of the disruption can be traced back allowing the implementation of preventive and/or mitigation techniques. Furthermore, the way smart contracts are stored in the blockchain and how their clauses and functions are executed in an independent and automated manner, following the logic of their codes, ensures a secure deployment of DApps with little to no interventions.

Hence, it is clear to see that leveraging these appealing characteristics of blockchain in combination with its rigorous cryptographic techniques is proven to be an advantageous choice to enhance the grid's cyber-security and trust compared to traditional centralized power systems. At the same time, blockchain could offer a seamless transition towards more distribution and resilience within SGs.

Summary and Main Takeaways

For over centuries, power systems relied on fossil fuel plants and functioned largely following a centralized model where energy would flow from generators to the households. However, with the proliferation of renewable DERs in conjunction with the increased digitalization and automation of the grid. The procedure of managing electricity supplies based on conventional controls fails to guarantee the required level of reliability, fault-tolerance and cyber-security. Thus, blockchain was regarded by many as a plausible alternative that could pave the way for a seamless transition of power systems to distributed smart grids powered with the IoE paradigm. While ensuring resilience, transparency, trust, secure automation, auditability and immutability due to the technology's inherent features.

IV. BLOCKCHAIN-BASED IoE APPLICATIONS

In this section, we present an up-to-date state-of-the-art of blockchain contributions in the IoE. Whether they are under the form of energy trading schemes, demand side management systems, solutions focusing on EVs, privacy-aware mechanisms, or approaches dedicated to enhancing the cyber-security of electrical grids. We also take a step further by exploring the intersection of blockchain with other emerging paradigms and assess their impact and potential on future IoE-based SGs. In addition, Fig. 7 represents an illustration of the taxonomy elaborated in this section.

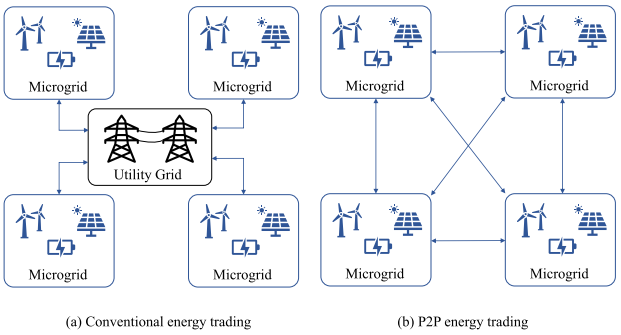


FIGURE 5. The transition from utility-based energy markets to P2P microgrid-based energy trading.

A. P2P ENERGY TRADING

Recently, the amount of distributed energy generated from renewable sources, such as rooftop photovoltaic (PV) power stations, or micro-turbines has increased remarkably [37]. This eventually would lead to a potential shift towards a novel P2P electricity market based on microgrids, illustrated in Fig. 5. In which users can both consume and produce their own energy, thus becoming prosumers capable of trading their oversupply of electricity without much interference from gird's operators. However, as the energy market is expanding beyond its traditional centralized model, dominated by few utilities, this has sparked new concerns such as guaranteeing reliability and auditability within this novel decentralized energy market governed by microgrids and DERs. To address this concern, many researchers harnessed the potential of blockchain in order to ensure a self-governed, transparent, open and decentralized electricity-trading market.

For instance, Guo et al. [38] proposed B-ET, an electricity trading framework built on a consortium blockchain. The framework is composed of two subsystems (i.e., an IoE subsystem and a blockchain subsystem) jointly interconnected. The IoE subsystem is representing a single city comprising SG agents and DERs, where a smart contract is designed to ensure an autonomous trading of energy. Whereas the blockchain subsystem is a P2P network connecting all the SG agents based on a hybrid consensus algorithm that combines both PoW and PoS to mediate the low throughput of the first and the non-randomness of the latter. The authors also modelled the process of trading between the SG agents and the DERs as a Stackelberg game and proved the existence of a unique equilibrium that can be reached with minimal

interactions. Meanwhile, the authors in [39] focused on the risk of market manipulation at the early stage of deployment of P2P energy trading frameworks as well as satisfying the multitude of trading-agents' preferences. In this regard, they also utilized a consortium blockchain as the building infrastructure of their proposed framework, which incorporates four trading schemes (i.e., bilateral contracts, e-commerce, double-auction Vickrey-Clarke-Groves and main-grid trading). The framework allows for diverse trading profiles, maximizes the social welfare, and is immune to shill-bidding and collusion attacks, by designing a novel consensus mechanism (i.e., proof of clearance) that manages the digital ID of all entities part of the framework.

Moreover, the authors in [40] presented DeTrade a two layered energy trading platform (i.e., market layer and blockchain layer). The first layer, called DeMarket, is a distributed parallel auction, with the aim of maximizing the social welfare of the independent prosumers. This layer is enhanced with a new clearing method based on a distributed ant-colony optimization algorithm, that is able to reach a near-optimal auction solution within an acceptable range of iterations. Whereas the second layer is implemented by leveraging a Hyperledger implementation of Ethereum and smart contracts to ensure automated settlements and management of crypto tokens.

Then, Wang et al. [41] presented the design of a blockchain-based architecture with a crowdsourcing model for SGs, incorporating different transactional types of energy-trading, that can be extended to microgrids running on an island mode without any operator control. The framework enables random P2P trading and is based on a two-phase algorithm: day-ahead planning of generation and hour-ahead/real-time balance of the energy's shortages or excesses utilizing incentive mechanisms. Furthermore, the authors in [42] proposed a blockchain-based architecture interconnecting microgrids and SGs following an efficient relaxed-consensus innovation algorithm that they developed. In this proposed P2P market, microgrids (i.e., wind turbines, PVs and storage units) and SGs (i.e., distributed generations and IEEE 24-bus lines) are trading energy by negotiating among each other following their personal benefit.

Furthermore, in the work presented by Li et al. [43], the authors also exploited consortium blockchains for the design of a secure and cooperative P2P energy trading framework. The proposed architecture is composed of energy buyers/sellers and aggregators, where the process of sharing and auditing energy transactions is managed by a set of pre-selected aggregators without trusted third parties. They then designed a loan-based payment mechanism based on an optimum Stackelberg pricing strategy to enable rapid transactions. In [44], the authors proposed a two-module energy trading platform: a blockchain module for energy transactions and a smart contract predictive-module. The first one enables real-time monitoring, seamless control trading, incentive mechanisms and immutable transactional records. Whereas the second one is based on a predictive model that utilizes data mining techniques to draw patterns from previous trends of energy consumption in order to foresee short-term energy usage and meet the SG load-demand. The platform was then tested on real energy data taken from the Jeju province energy department. Besides, Gough et al. [45] presented a novel multilevel transactive energy optimization model that is used to schedule DERs part of VPPs. Where the hierarchical inter and intra energy trading transactions are automated and recorded immutably by introducing a blockchain-enabled smart contract layer atop the proposed optimization model. Furthermore, the authors addressed the lack of consideration of energy legislations or regulation that govern the energy markets within the previous studies by examining the effect of the Portuguese regulations on DERs' usage, as designing a system that aligns to those rules is of important practicality.

Whereas in the work of Luo et al. [46] a multi-agent coalition blockchain-based energy trading architecture was proposed, which considers prosumers as self-ruling heterogeneous individuals. The architecture is based on the decoupling of the upper layer of trading negotiations and lower layer of electricity management, enabling more flexibility. The framework is based on a parallel double-chain system, where the first chain is used to store the negotiation contracts and the second is dedicated for the energy trading. In addition, reputation was also addressed in the work of [47], where the authors designed a blockchain-enabled distributed reputation-based system dedicated for P2P energy trading. Scores within the reputation scheme are calculated based on users' behaviour, whether it's in terms of reaching consensus or buying/selling energy, which are stored within the blockchain ledger for immutability. The reputation mechanism was implemented using smart contracts for automation and distribution, that was then utilized for the design of a

Discussion and Lessons Learned

Undoubtedly, P2P transactive energy has been the prominent application of blockchain in modern smart grids. Which comes without a surprise as the technology is first and foremost a digital distributed monetary system. A plethora of researchers in the literature approached the challenges of this innovative concept from various angles by proposing different solutions. Such as, but not limited to, novel market models, game theoretical models (e.g., Stackelberg game, Vickrey-Clarke-Groves, etc.), new and lightweight consensus mechanisms as well as incentives and rewards schemes. Nonetheless, the existing studies in the literature fail to evaluate the scalability of the P2P trading system at larger scales (e.g., metropolitan areas). In addition, the governance of a fully autonomous energy community (i.e., without the intervention of utilities or grid operators) is far than being a trivial matter, due to legislative, privacy and accountability concerns.

delegated consensus algorithm as well as a k-double auction matchmaking mechanism for P2P trading that favours participants with greater reputations.

B. DEMAND-RESPONSE

The ever-increasing urge of changing power grids from their traditional design to smarter ones has consequently led to the emergence of more advanced grids, namely cyber-physical SGs leveraging complex ICTs. This amalgamation has promoted a seamless sharing of energy-data among all units' part of the SG, thus ensuring efficiency and smart-governance vis-à-vis the demand side management, grid stabilization and maintenance. Nevertheless, integrating complex networking paradigms and technologies with the grid has unlocked a myriad of novel security concerns that could threaten the whole system (e.g., power loss, cascading failures, blackouts, etc.), which could get further complicated and unpredictable by adding DERs to the grid. In an attempt to mitigate these challenges, blockchain was extensively utilized to design secure demand side or demand-response schemes based on this bi-directional flow of data.

For instance, the authors in [48] combined reinforcement learning with blockchain to propose an efficient, stable and secure demand-response management scheme for SGs. Q-learning was utilized to optimize the decision-making process of prices, thus reducing consumption. Whereas Ethereum smart contracts were incorporated to secure the process of sharing energy data, which are stored off-chain using the InterPlanetary File System. Then, the authors in [49] developed a blockchain-enabled energy management framework for virtual power plants (VPPs), where prosumers' smart meters play the role of the blockchain nodes. The framework provides various services including demand-response management and incentivizes users by paying them rewards to calibrate or save their energy for load regulation to ensure the gird's stability. In addition, by using the cooperative mode, users are able to reduce the cost of managing their energy by roughly 11%.

Zhang et al. [50] addressed the challenge of demand-response while managing P2P electricity exchange within a heterogeneous market by proposing two non-cooperative model games where dynamic pricing is implemented for suppliers. The authors build a prototype of the system that utilizes an automated coordinator in the form of a smart contract deployed on the Hyperledger-based blockchain network. To assess the scalability and performance of the system, an on-chain and off-chain handling modes were implemented. The results of the experiments conducted under multiple solar conditions indicate a reduction in terms of net-peak load with a profit increase as well as a low latency due to the off-chain approach leveraged while still maintaining the level of security of the on-chain mode.

Meanwhile, Noor et al. addressed the challenges of the rapid penetration of renewable supply resources into the power infrastructure in [51], by proposing a blockchain-based demand side management framework to balance and enhance the reliability of microgrids supply/demand under restricted conditions. The authors also proposed a game-theoretical model capable of reducing the peak-to-average ratio as well as flattening the load-profile dips. Furthermore, the authors in [52] utilized blockchain for its traceability feature to implement a demand-response certification scheme. Precisely, they developed a chaincode on Hyperledger Fabric that is responsible for logging all demand-response event into the blockchain, calculating users' baseline as well as their contribution to the solicited electricity load-curve adjustments and incentivizing users with utility-tokens. In addition, Tsaousoglou et al. proposed in [53] a blockchain-enabled architecture for demand-response based on a modified version of the Ausubel's clinching auction mechanism with continuous energy items, in which the number of these elements is bound to a reward function. The framework ensures truthfulness, scalability, seamless queries, efficiency and low overhead due to its implementation. Whereas GUARDIAN was proposed in [54], which is also a blockchain-based demand-response framework dedicated for managing different types of power loads (i.e., residential, commercial and industrial). In this framework, the nodes responsible for verifying blocks are chosen based on their consumption as well as processing power, and they are also in charge of the authentication procedure of all transactions within the grid.

Furthermore, the authors in [55] addressed the demand-response problem, by first designing a blockchain-based system that is used to record users' power consumption/production from the smart meters for immutability. Second developing a smart contract to calculate the potential contribution of each user to adapt the power load upon request by the grid operator. Which then rewards users following a parabolic function (i.e., the higher the consumption is matching the request of the operator the more likely the customer would be rewarded).

Moreover, DELTA [56] is a novel blockchain multi-agent based decision-making framework that offers a transition from aggregator-based demand-response management to a distributed energy-cluster based architecture. The introduced energy clusters or virtual nodes act as a gateway to enable a smooth exchange of electricity data from end-users to aggregators using smart contracts in order to deliver demand-response strategies that would guarantee the stability of the whole grid. In addition, the end users in this proposed architecture were enhanced with fog-enabled intelligent devices responsible for the blockchain actions, and the Ethereum-based architecture was also coupled with OpenADR protocol for data-exchange interoperability.

In the work of Danzi et al. [57] an Ethereum-based imbalance settlement framework was proposed, which was divided into two main layers. The first layer is composed of both the system operator and the balance parties responsible for sending the aggregation of the predicted generation/consumption data within the grid to the operator. Whereas the second layer involves the consumers who are linked to the balance parties that oversee offloading the imbalance cost based on the

measured consumption to ensure a flexible demand-response management, which was achieved by the means of a smart contract.

Discussion and Lessons Learned

The digitalization of the SG promoted a seamless and bi-directional flow of real time energy-data among all entities of the grid. Whereas blockchain was harnessed by multiple researchers with the aim of ensuring efficiency and transparency vis-à-vis the demand-response management. For instance, the technology was utilized to implement incentive schemes that help regulating energy flows, thus guaranteeing the stability of the grid. Dynamic pricing was also implemented using smart contracts to reduce the net-peak load as well as help flattening the load-profile dips. Meanwhile, demand-response certificates for prosumers were also implemented by leveraging the traceability feature of blockchain. Nevertheless, the cost of designing, deploying and managing such distributed schemes in the long term has not been addressed so far. Which might be a bottleneck for utilities and grid operators, as blockchain is decentralized, meaning each peer within the system is required to keep an immutable copy of the shared ledger.

C. ELECTRIC VEHICLES CHARGING

While oil-reserves are starting to decline, and the impact of climate change on our planet is drastically intensifying, EVs are at the peak of their innovative period. However, as these eco-friendly vehicles are becoming more and more connected and autonomous, they are also becoming more prone to cyber-attacks, which could have disastrous effects on the whole power grid that constitutes the backbone of all societies. In this regard, blockchain potential at securing various services within these vehicle to grid (V2G) ecosystems, illustrated in Fig. 6, has been extensively studied in the past few years.

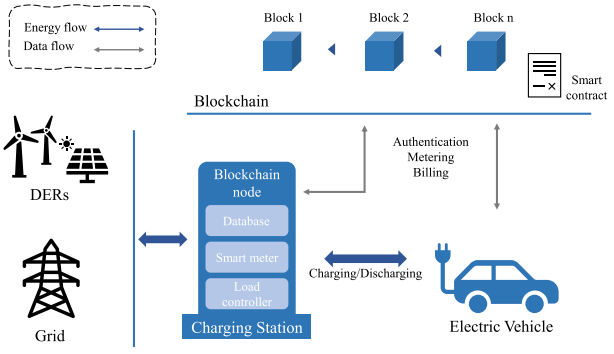


FIGURE 6. Blockchain adoption for EVs charging schemes.

For instance, the authors in [58] presented a blockchain-based architecture dedicated for charging points. They designed a sharing trust environment that ensures storing and querying the charging-data in a secure and efficient way. Precisely, by using smart contracts that manage the fairness of charging prices as well as the security of each transaction within the network. Meanwhile, the authors in [59] proposed a rank-based algorithm to prioritize and differentiate the EVs as well as to ensure a guided-charging procedure based on the drivers' behaviour with no involvement of incentives. They then presented a blockchain-based EV-incentive scheme in order to enhance the ranking based model. Finally, to verify their proposed model, the authors simulated the EV charging system and demonstrated the effectiveness of the incentive mechanism introduced. In Hassija et al. [60] DV2G is presented, which is a lightweight blockchain network based on directed acyclic graphs for managing V2G communication. The blockchain does not require any mining as it's based on a selection algorithm for adding new trading transactions, precisely, the authors utilized a tangle-data structure for a secure as well as scalable recording of transactions. In addition, an optimization game-theoretical model (i.e., a Stackelberg game model) was developed to negotiate the interactions between the vehicles and the grid. The results from the proposed model show a high degree of scalability, while still supporting micro-transactions needed for the V2G scenario studied.

Furthermore, PETCON [61] is an electricity-trading system for plug-in hybrid EVs based on a consortium blockchain that guarantees the level of security and privacy needed for charging EVs. The authors presented a model to locally buy and sell electricity within the smart grid among EVs, by leveraging an incentive mechanism for discharging EVs, the model is capable of achieving a balanced demand and response. The authors also proposed a solution to the problem of pricing vis-à-vis the amount of electricity exchanged among the EVs by proposing a double-auction scheme, which ensures a maximal social welfare. Whereas the authors in [62] also looked at the problem of charging and discharging EVs using hierarchical and local scheduling. Where they proposed a double-layered model in order to optimize the process of electricity-trading among EVs, and to decrease the grid disruption or load variance while still being constrained by the EVs demand and power flow. Meanwhile, blockchain was used to secure the transactions in combination with an access control and key distribution schemes.

Whereas Jindal et al. proposed SURVIVOR [63], an edge software defined networking enabled framework based on blockchain for energy trading within a V2G ecosystem. In the presented edge-as-a-service framework, the trading transactions are handled closer to the EVs by using edge nodes, which decreases the overall latency of the V2G system. Furthermore, some of these edge nodes (referred to as approver nodes) are also in charge of validating transactions after undergoing a utility-based selection process, whereas other edge nodes are assigned the task of solving the blockchain PoW puzzles. However, using PoW in this use case might not be an adequate choice due to its high computation. Meanwhile, Su et al. [64] presented an energy permissioned

blockchain-based secure charging system for EVs, they also proposed a BFT consensus mechanism based on reputation for efficiency. Then following the contract theory, they found the optimal solution to guarantee the energy demand of each individual EV, while at the same time maximizing the utility of the operators. In addition, a new allocation scheme was designed to coordinate the scarce green energy resources for the EVs.

Discussion and Lessons Learned

V2G eco-systems are gradually expanding within the realm of the IoE paradigm. These EVs and their charging points, equipped with IoT devices, paved the way for a remote control and management of these V2G systems. Blockchain was also utilized to guarantee the security of energy services provided within these connected and intelligent charging infrastructures. For instance, smart contracts were used to securely store the charging data and guarantee the fairness of the electricity prices. Dynamic incentives and rewards schemes were proposed by capturing the vehicles' behaviour in terms of charging. Game theoretical models were also designed to study the interaction between the vehicles and the grid in terms of charging and discharging. Nevertheless, the majority of the presented work focuses solely on the fairness of charging and discharging EVs, while eluding the cyber-security control aspect of this ecosystem in terms of access control, authorization and authentication as well as auditability in regard to equipment's software maintenances.

D. PRIVACY AND ANONYMITY

As power systems are becoming more digitalized, and more advanced metering infrastructures as well as EVs are being introduced to the grid. The level of interaction between utility companies and costumers has increased remarkably, allowing a two-way autonomous communication flow using these smart devices. Thus, enabling the collection of a wide range of electricity usage/production data for an enhanced monitoring, control and troubleshooting. However, these massive volumes of data are transferred via the public internet, sparking potential risks of private information leakages (e.g., real identity of users, or their exact geographical locations). In fact, some grid services require the use of the exact location, which necessitates users to divulge their real geo-location, thus allowing an attacker to trail the activity of a specific user.

To address these privacy concerns, the authors in [65] for instance proposed a blockchain-based anonymous proof of location mechanism that proves a participant's location yet protects the real data. The mechanism utilizes certificates of location that are delivered by randomly selected smart meters (referred to as verifiers). They are responsible for verifying the provided credentials by interacting with a certificate authority (in this case the utility company) without divulging the real location of the smart meter sending a request but only his public key and Merkle tree. However, on the one hand, the level of privacy ensured in this scheme is highly dependent on the amount of public keys utilized to generate the blockchain transactions; on the other hand, managing a huge number of keys induces an enormous overhead. Hence, the scheme suffers from the trade-off between privacy and efficiency. Meanwhile, Singh et al. addressed the privacy issue of data aggregation within the SG in [66] by utilizing deep learning and homomorphic encryption as well as blockchain to guarantee an accurate prediction model and offload the computational overhead from constrained smart meters. The framework is able to achieve a high efficiency of 80% compared to traditional schemes.

Then, in [67] the authors proposed a blockchain-based optimized energy market model with restricted access to users' private data. The framework enables parallelized processing and was implemented using the Ethereum platform, where the full participants' data are stored on sub-chains with only the price signals being recorded on the main chain, hence preventing privacy disclosure of consumers' data. Whereas the authors in [68] focused on protecting neighbouring electricity trading systems from data mining linking attacks using blockchain, while still guaranteeing the accuracy and reliability of the trading transactions within the ledger. The proposed framework is composed of a black box module, used for the construction of the smart contact implemented. The module relies on the creation of dummy accounts in order to erase and weaken the actual distribution or trend of the legitimate accounts, thus, ensuring privacy.

Moreover, Aitzhan et al. [69] addressed the privacy concern within decentralized SGs without the need of a TTP. They implemented a blockchain-based private electricity trading framework with a multi-signature scheme and anonymous cyphered message propagation flows to guarantee a certain degree of privacy for users. The system was simulated to prove that the identity of all entities is not revealed, however, the solution is based on the PoW consensus mechanism which would hinder its efficacy in terms of scalability and latency. Then, Yang and Wang proposed an IoT blockchain-based energy management framework dedicated for smart homes with a focus on the transactions' privacy [70]. The framework enables two types of transactional flows (i.e., vertical and horizontal), meaning to either transact with the operator by selling surplus of energy from DERs as well as providing demand-response services, or with other smart home peers for local trading. In addition, the developed smart contract is able to preserve the smart homes' privacy by limiting the data revealed (precisely the optimization procedure of decision-making while trading) to the other participants within the framework. The system was prototyped using Quorum (an altered version of the Ethereum blockchain) and the results obtained prove the efficiency and practicality of the solution with a cost reduction of nearly 25%.

Meanwhile, Guan et al. proposed PP-BCETS [71] a blockchain-based transactive energy model addressing the privacy concern by leveraging ciphertext-policy attribute-based encryption in order to protect sensitive data within the energy trading scheme. Differently than the traditional attribute-based encryption that uses attributes in order to characterize the ciphered data and construct rules into the keys, ciphertext-policy attribute-based encryption uses attributes to characterize users' credentials while the deciphering of the data is determined by a party cyphering data. The solution achieves fine-grained access-control by allowing users to set predefined rules and authorization policies governing the access to their private data. In addition, the scheme is also utilizing filtering to mitigate leakage of sensitive data to other entities.

In [72] the authors proposed a privacy-aware dual blockchain-based scheme dedicated for energy supplies pricing control-centres, where users can send their energy data safely without divulging their identity. The architectural design of the scheme is based on two blockchains: a private one responsible for managing the mapping between real-identities and pseudonyms of all participants, and a shared one with access control restrictions. The scheme is also utilizing the identity-based proxy re-encryption mechanism with a lightweight signature-based authentication scheme to guarantee the protection of private data. Furthermore, Hassan et al. proposed DEAL [73], which is a consortium blockchain-based framework for microgrid electricity auction. The authors utilized the differential privacy technique to guarantee that queries on the energy transactions within the system do not allow revealing private data or linking a transaction to the real identity of a user. Whereas the computational cost and complexity of the system were reduced by leveraging only authorized peers to write on the blockchain ledger.

Discussion and Lessons Learned

The digitalization of the distribution system of the grid in the form of advanced metering infrastructures, EVs and others; has increased remarkably the amount of energy data generated at the edge. These data could be harnessed by utilities and grid companies in order to provide reliable supply and optimized performance. Yet, with big data comes privacy concerns. Researchers tried to tackle this using blockchain in addition to other techniques, as the technology itself might not provide the required privacy due to its inherent transparency feature. For instance, anonymous proof-of-location mechanisms were designed. Homomorphic encryption was utilized to guarantee the privacy of smart meters' aggregated data. Whereas blockchain sharding was also leveraged to provide restricted access to users' private data. However, the trade-offs between ensuring privacy and the utility of the data as well as the performance of the system remain to be tackled.

E. CYBER-SECURITY AND RESILIENCE

The major challenge faced with a real-world deployment of the smart grid 2.0 paradigm mainly resides at guaranteeing the required level of cyber-resilience within this IoE-enabled infrastructure. Specifically, as the SG is becoming more digitalized and connected with IoT-enabled devices (while eluding the need to assess the security risk these devices might bring). The landscape of cyber-attacks that could target power systems is also expanding as the grid is undeniably inheriting the potential vulnerabilities of these new devices. That if exploited strategically and at a larger scale they could disrupt the normal operation of SGs or even cause blackouts. To tackle this, many recent studies have adopted blockchain as the building infrastructure that would not only enable sharing and managing the exchanged data securely and in a tamper-proof manner, but also enable deploying prevention and/or mitigation schemes to protect the grid from cyber-attacks.

For example, in [74], the authors presented DeepCoin which is a blockchain-enabled framework for SGs energy exchange, with a deep learning-based intrusion detection system that deploys the recurrent neural network technique in order to detect cyber-attacks or compromised transactions. The workflow of the framework was divided into five phases (i.e., setup, agreement, block creation, consensus and queering changes), and leverages the PBFT consensus algorithm to achieve a higher throughput. In addition, to guarantee privacy, the block creation phase uses bilinear pairing, short-signatures and hash functions. Furthermore, Chen et al. designed DA-SADA [75], which is a double-blockchain fog-enhanced secure and anonymized data-aggregation framework for SGs. The proposed architecture is comprised of three tiers (i.e., user, fog and service tier), where the whole SG is assumed to be dispatched into sub-areas managing a set of smart meters for measuring users' consumption, that form the user aggregation chain. Then, each sub-area has a fog node responsible for the collection and secure aggregation of the energy data using Paillier encryption and batch signature, these fog nodes form subsequently the fog tier which also deploy the fog aggregation chain. The scheme is proven to be effective against replay attacks, FDIA and eavesdropping. In addition, the simulation results indicate that the probability of launching an attack declines with the increase of the number of smart meters that the attacker has to manipulate, until reaching a relatively negligible value when the number of smart meters exceeds 500.

In addition, Bera et al. presented DBACP-IoTSG [76] a private blockchain-based authorization scheme dedicated for IoT-enable SGs, where data generated from smart meters are transferred to the service providers (SPs) in a secure and tamper proof manner. The blockchain network is comprised of the SPs nodes who are in charge of data aggregation as well as blocks creation and validation following the PBFT consensus

mechanism. The authors then conducted a formal security analysis of the protocol following the random oracle model to prove its resistance against impersonation and replay attacks, man-in-the-middle and ephemeral secret leakage. However, the execution time of the scheme increases exponentially with the increase of the number of peers in the blockchain network and this is due to utilizing the PBFT algorithm for consensus.

In [77], the authors proposed a blockchain-based load sharing scheme for renewable microgrids utilizing a master-slave approach, that enhances the voltage stability and ensures an efficient management of load distribution. The scheme was evaluated against different types of FDIAs, in terms of smart sensors' voltage or current (either an increase or decrease of the load's current). If the measured data from the smart sensors are tempered with by an attacker the hash of the aggregated data within the blockchain ledger would not match the previous hash, thus the measurements are considered unreliable by the master agent and are not taken into account by the microgrid controller. Then, Wang et al. proposed a modified blockchain-based stochastic power management scheme for networked microgrids in [78] by using directed acyclic graphs to tackle the computational and storage complexity within traditional blockchains. The framework is based on three chains (i.e., public, private and transaction blockchain) that are mapped into a directed acyclic graph (DAG) topology. Each microgrid has a private chain with full data relevant to it and only publishes some to the public chain that contains all microgrids' open data, thus in case the data within the private ledger are lost it's possible to be partially recovered.

Meanwhile, to address the security issue of multi-microgrids, the authors in [79] proposed a collaborative intrusion detection system (CIDS) leveraging blockchain without the need of a TTP. The CIDS is based on trigger patters that are detected within each microgrid and then used for the generation of a proposal alert, which is chained to the shared ledger after undergoing a correlation model and being validated following a modified version of the delegated PoS consensus algorithm. The scheme is also enhanced with a reward/penalty mechanism that serves as a motivation for the single-microgrids to take part of the CIDS. Then, Sadu et al. [80] presented the design of a blockchain-based automated and distributed scheme using smart contracts, which guarantees that the fundamental functionalities of a distribution grid automation system are available in the case of a failure of a substation. The process is based on the virtualization and migration of these functionalities from one substation to another via blockchain for security and reliability using smart contracts. The limitation of this approach is that it relies on a heartbeat signal to assess whether a substation failed within the power system in order to start the migration procedure. However, in case of a cyber-attack the hacker can still send those signals to make the other peers believe that the station is still functioning. Thus, the mechanism can be considered as crash tolerant, but not byzantine tolerant.

Moreover, the authors in [81] proposed a blockchain-enabled framework to protect data and enhance the self-defence abilities of SGs against cyber-attacks, precisely FDIA. The framework is built on a set of distributed yet connected smart meters following a geographical pattern that act as private blockchain nodes. Each node (i.e., smart meter) has the public keys of the other peers, its private key, the pre-defined rules of consensus, the chain of blocks and the broadcasted data from the other nodes (basically plaintext and digital signatures). The performance evaluation of the framework shows that the probability to successfully launch an attack decreases with the increase of the required number of nodes (i.e., meters) that the adversary must manipulate. Similarly, the authors in [82] addressed the concern of cyber-attacks within smart metering infrastructures, by proposing a four-tier architecture (i.e., user, edge, fog and cloud layer): the user layer is composed of the smart appliances and/or DERs, the edge layer is the collection of smart meters, the fog layer is represented by the data aggregators, last the cloud layer is the utility data centre. The framework is able to achieve higher efficiency in terms of data storage due to its segmented blockchain-based architecture and is resilient against DDoS attacks (as long as one blockchain peer is available) as well as FDIAs as the measured data could always be compared with other peers to detect tampering or any fraudulent activities. However, the scheme requires deleting the databases of the smart meters or DERs after sending the aggregated data to the cloud centre, due to their constrained storage resources, which violates the immutability feature of blockchains.

Discussion and Lessons Learned

Cyber security and resilience are among the primary concerns of modern SGs, but they are usually overlooked. As the number of IoE devices connected to the grid is ever-growing, so is the landscape of cyber-attacks and vulnerabilities. Meanwhile, although blockchain guarantees a priori a certain degree of security (i.e., integrity and immutability as well as traceability) just by leveraging the technology. Various researchers took a step ahead by implementing various security control schemes based on the technology. Such as collaborative intrusion detection systems. Resistant schemes against FDIA, impersonation, replay and man-in-the-middle attacks. Fault-tolerance and resilience in terms of configuration settings within substations. Nevertheless, blockchain could still offer more than this in the form of distributed role-based access control schemes tailored for SGs, mutual authentication, access control delegation, traceability of grid devices' maintenance and so forth.

F. A STEP AHEAD OF BLOCKCHAIN: EMERGING INNOVATIVE TECHNOLOGIES AND PARADIGMS FOR IoE

The past few years witnessed the rise of various novel technologies and paradigms that were deemed suited to tackle the computational and networking setbacks of smart grids,

as a form of complex cyber-physical systems, and to profoundly transform their design. So far, we have focused on blockchain as one of the many technologies out there, but the spectrum is way wider than to be confined within that. For instance, in the realm of ICT, the next 5G and 6G mobile broad-band systems are expected to unlock communications at extreme high data rates and reliability with reduced latency. Meanwhile, edge and fog computing would allow bringing computation closer to the physical processes, thus achieving lower latency in terms of intensive computational tasks. In addition to providing a smooth integration with cloud-based or blockchain-based systems. Whereas software-defined networking (SDN), through network virtualization, would enable malleable and demand-driven arrangement of communication and computational resources. Furthermore, the remarkable advancement in big data analysis and AI, particularly deep learning, is expected to break the boundaries of what we can achieve, unlock novel control schemes and enable a plethora of innovative and intelligent applications. In what follows, we discuss some of these disruptive technologies, their intersection with blockchain as well as their integration within IoE-based eco-systems.

1) BIG DATA AND ARTIFICIAL INTELLIGENCE

Although the concept of AI has been there for quite some decades now, there is no collective and agreed upon definition of it up to this moment in academia. Among its definitions is the one provided by the founder of the discipline (i.e., John McCarthy) that used the term for the first time in a conference back in 1956. Where he defined AI as the engineering science of conceptualizing and developing intelligent machines. AI relies broadly on three major techniques: machine learning (e.g., support vector machine, decision tree, artificial neural network, etc.), deep learning (e.g., deep neural network, convolutional neural network, long short-term memory, Auto-encoder, etc.) and reinforcement learning (e.g., Markov decision process, Q-learning, deep deterministic policy gradient, etc.). Various surveys in the literature reviewed the applications of AI in smart grids that span from data pre-processing, anomaly detection, load/generation forecasting, stability analysis, to automated control [83], [84], [85]. Meanwhile, blockchain was also enhanced with AI techniques, where for instance the authors in [86] provided the design of a blockchain-based framework that utilized deep learning to protect smart grid network with an anomaly detection module. Whereas Ganesh et al. [87] proposed a hybrid AI and blockchain-based framework for smart grids' protection against FDIA and DDoS attacks. Furthermore, the authors in [88] evaluated the integration of both AI with Blockchain to provide a secure, efficient and decentralized EVs charging infrastructure.

2) INDUSTRY 4.0 AND 5.0

The increasing progress that ICTs have been undergoing paved the way to the fourth industrial revolution, referred to as Industry 4.0, specifically within the energy industry (i.e., SGs) being the focus of this survey. The key vision behind this transformation is building extremely reliable, intelligent as well as flexible cyber-physical infrastructures that would enable real-time interactions and autonomous exchange of massive volumes of data between all entities within the SG. This would facilitate the procedure of monitoring the power system while making decentralized and optimized decisions in terms of load and generation control, fault diagnosis and management, automated scheduling and distribution, etc. Meanwhile, IoT is also strongly coupled with Industry 4.0, particularly SGs, as the paradigm offers various benefits in the form of advanced smart metering, substations automation with intelligent electrical devices (IEDs) and advanced EMS using remote sensors. While guaranteeing state-of-the-art connectivity between machine-to-machine, human-to-machine as well as services. Meanwhile, speculations already started about Industry 5.0, being the next industrial revolution, which is expected to be strongly driven by the remarkable progress the field of AI has witnessed during the recent years. In the work proposed by Faheem et al. [89], the authors presented a comprehensive survey in regard to the role played by information technologies, protocols and standards on SG critical components in the context of Industry 4.0. Furthermore, the authors in [90] evaluated the integration of blockchain with Industry 5.0 focusing on several applications among them the smart grid (specifically DERs and micro-grids) and how the technology can enhance the security of these cyber-physical systems. Besides, Repsol [91], which is a multi-energy provider that utilizes advances technologies to build sustainable energy models. Launched a project that leverages blockchain, AI, and robotic-based procedure automation to ameliorate the security as well as productivity of its Industrial 5.0. plants.

3) 5G, 6G AND BEYOND

The next-generation communication standard, known as 6G, is expected to be the near replacement of 5G in 2030 [92]. The standard is anticipated to significantly improve future power systems, characterized with highly dense chains of thousands even millions of IoE devices such as sensors and remote IEDs, in terms of bandwidth and latency requirements. By means of delivering ultra-high data transfer ratios (i.e., terabits per second), ultra-reduced latency (less than 1ms), extreme reliability and energy efficiency, etc. Thus, utilizing 6G within IoE-based infrastructures would enable high-quality services by improving applications' efficiency and efficacy as well as incorporating AI functionalities. Whereas handover control, being one of the challenges associated with 6G, could be addressed using AI-based solutions to attain the optimized mobility predictions, therefore, ensuring efficiency in terms of connectivity and lower latency. 5G and 6G have been the focus of multiple surveys, such as [93], where the authors evaluated the integration of blockchain, AI and 5G as the backbone for the next generation SG. Whereas Yap et al. [94] focused on 6G and its applications for managing renewable

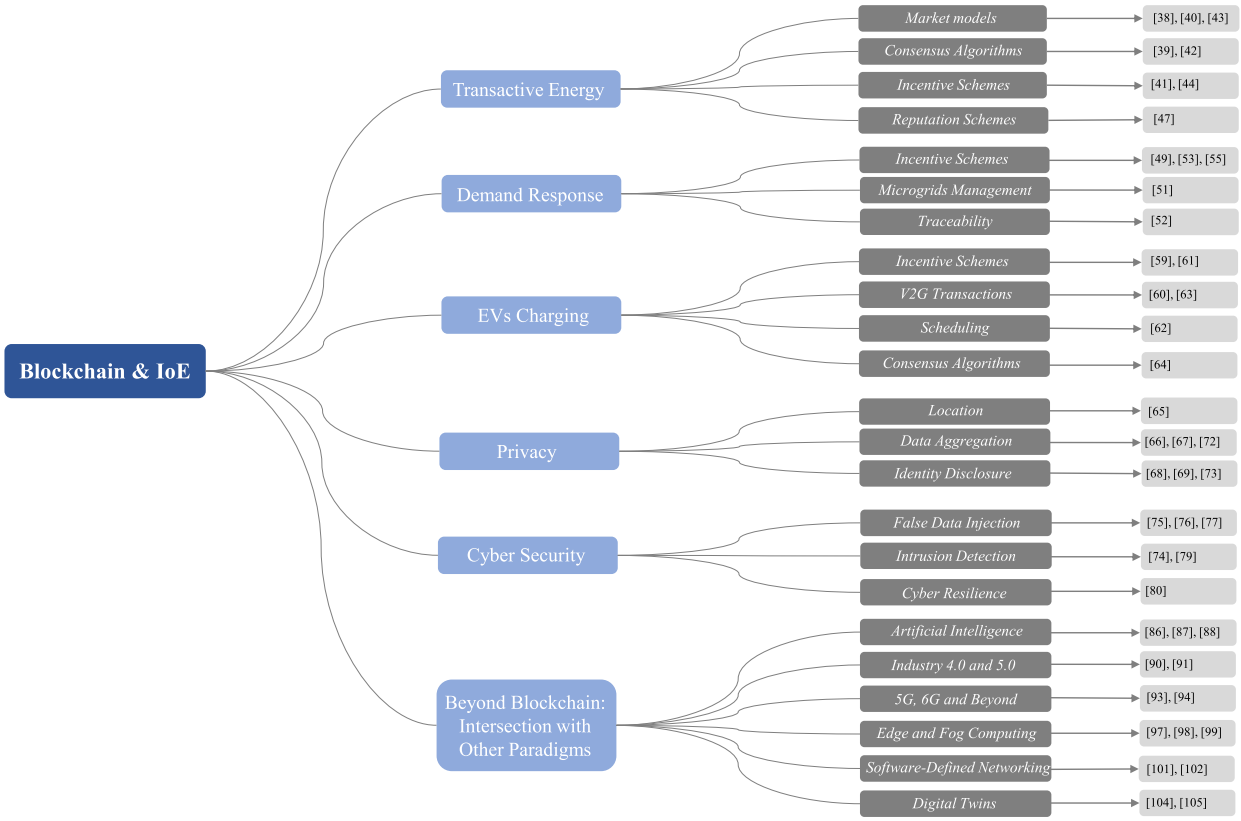


FIGURE 7. Taxonomy of blockchain applications in IoE with other emerging paradigms.

energy resources (e.g. energy trading, EVs networks, batteries, etc.) with some future outlooks including the utility of blockchain in this particular use case.

4) EDGE AND FOG COMPUTING

Cloud computing-based infrastructures have been and are still the dominant solutions utilized to deal with the heavy computational tasks within SGs. The paradigm enables on-demand services and allows gathering data across the whole grid eco-system to be analysed efficiently. However, one of the many issues with cloud computing is its latency, as scaling a cloud-based system relies only on the improvement of the bandwidth and communication links. In addition, as the number of IoT devices within the edge of the smart grid is ever-increasing the amount of generated data would grow astonishingly and centralized computing might fail at processing them, not to mention that it represents a single point of failure.

In an attempt at addressing these concerns, innovative network paradigms emerged such as fog and edge computing. They offer computational resources near the end-users, thus lowering the overall latency of the system. By the means of offloading the computational tasks to edge/fog nodes and thus providing context-aware services that could be deployed within these small-scale edge/fog servers. The integration of edge computing with smart grid infrastructures has been evaluated in the literature [95], [96]. Whereas the integration of the paradigm with blockchain was also investigated. For instance, the authors in [97] leveraged blockchain with contract theory, for a secure and reliable trading of energy within a V2G ecosystem, as well as edge computing to guarantee the scalability of the framework. Meanwhile, Gai et al. designed a blockchain edge computing based traceable energy-governance framework in [98] using the Ethereum platform, which detects malicious energy consumption behaviours within the SG to minimize the risk of cyber-attacks. Whereas Wang et al. [99] proposed an anonymous blockchain-based authentication scheme within a smart grid infrastructure, with the integration of edge computing to tackle the low latency of cloud-based systems.

5) SOFTWARE-DEFINED NETWORKING

SDN is based on the abstraction or separation of various layers (i.e., control and data plane) of a network in order to enhance its agility and flexibility. Where network switches for instance are simply forwarding data, whereas the rules governing these procedures can be configured in a dynamic manner using a centralized controller. It allows improving network control and enabling operators to swiftly respond to changes in terms of logic or business requirements. An SDN-based architecture is usually composed of three main layers, i.e., application, control and infrastructure layer, which all communicate using APIs (e.g. OpenFlow). Besides, communication networks are considered as the fundamental part

of SG infrastructures as they connect a tremendous number of grid devices spanning across wide geographical areas in order to support the grid's SCADA system. Currently, these networks are roughly based on conventional IP networking paradigms and protocols such as multi-protocol label switching in which the network capabilities (e.g., routing) are fixed at the design phase. Nevertheless, the adoption of such approach might be the bottleneck of future SGs as the addition of new services (e.g., V2G, P2P energy trading) and devices (e.g., IoT) would require a re-configuration in terms of routers and switches each time. Thus, disrupting the services that the utilities provide and hindering fast responses to accidents or malicious events.

Consequently, SDN has been regarded by various researchers as a solution to these issues, due to its attractive features such as traffic prioritization, isolation, network slicing, interoperability and resiliency [100]. Furthermore, SDN was also combined with blockchain, for instance, Chaudhary et al. proposed BEST [101], a framework for EVs energy exchange based on blockchain to guarantee the security of the system's requests, while SDN was utilized as the backbone of the network to ensure minimized latency and real-time services. In addition, the authors in [102] designed a blockchain-based mutual authentication scheme within a V2G eco-system to preserve privacy and a smart contract for an efficient demand-response during the bi-directional exchange between EVs and the SG. The authors also utilized SDN for its capabilities to efficiently manage the complex interactions among the components of the V2G system.

6) DIGITAL TWINS

A digital replica of a given physical system is what is known as a digital twin (DT). The concept allows the digital representation of real-world objects or whole systems such as wind or solar farms, smart grids or even smart cities. A DT can be defined as a software-based abstraction of a physical system characterized by high complexity which is linked to an actual real system via communication channel used to exchange data at a continuous rate with the real-world environment. Thus, establishing a vigorous digital mirror based on extensive modelling. Although the concept was first conceptualized back in 2002, when NASA created a mirror of a spacecraft part of the Apollo program and named it a ''twin''. The concept only started catching momentum in the recent few years with the advancement and expansion of the IoT paradigm. By using IoT-based devices, massive volumes of data relevant to real-world physical objects or systems can be fed to their mirrored digital counterparts for evaluation, improvement and adaptation.

A DT can be summarized in three main components, i.e., a physical and virtual system as well as the exchanged data between the two realms. Thus, building a DT is based on accurate models (e.g., physics-based or mathematical models, data driven models or hybrid ones) which are integrated with various data (e.g., sensor and historical data, technical data, maintenance information, etc.). These data are also used to evaluate and adapt the model under various operational states using AI mechanisms and automatic learning approaches. In order to help decision making and prevent complications, faults or anomalies before their occurrence in the real-world system.

Even though the aerospace industry was the cradle of DTs, it soon was harnessed within various domains and a wide spectrum of applications including the energy industry. Where a DT is seen as highly beneficial throughout the whole cycle of a smart grid, from planning to operation as well as maintenance and system scaling. In a survey paper presented by Wang et al. [103], the potential of DTs in energy applications is evaluated where the concept could be used for low carbon cities, smart grids (e.g., architecture models, design of new devices, energy storage systems, analysis of data, resilience and restoration, interdependency of the cyber and physical layers, etc.). Whereas the authors in [104] explored various applications of DTs for micro-grids in terms of design, control and operation, energy forecasting, troubleshooting, policy-making, etc. In addition, they suggested that blockchain could be utilized to ensure the data management for DTs in a secure manner. Furthermore, Lopez et al. [105] conducted a prospective evaluation of future SGs with DTs, where they envisioned that the electricity grid would shift to a fully decentralized an autonomous model using blockchain, guided by intelligent authorization mechanisms.

Discussion and Lessons Learned

It is fair to say that one single technology does not hold the key to all problems of future SGs, but rather the combination of various paradigms in a meticulous and ingenious manner. On the one hand, even though blockchain has the capacity and potential of ameliorating the cyber-security and resilience of IoE-based ecosystems, due to its built-in security features. It still comes with certain limitations that could be addressed using various innovative technologies and paradigms, such as 6G, AI, edge/fog computing, and SDN. On the other hand, blockchain itself can also complement some of these emerging concepts, as for instance, it can be used to protect the integrity and authenticity of DTs' data and deal with the single point of failure of centralized SDN-based controllers. This then constitutes a functionality loop between both realms, where each technology can benefit from the other reciprocally.

V. BEYOND ACADEMIA: BLOCKCHAIN-BASED INDUSTRIAL PROJECTS FOR IoE

The revolutionary technology (i.e., Blockchain) did not only succeed at drawing the attention of researchers within academia, but there is also a myriad of ongoing projects and platforms within the industry that leverage the appealing features of the technology, which we will examine in this

section. In addition to a case study of an energy community pilot project in De Ceuvel, Amsterdam.

A. GREEN CRYPTOCURRENCIES

Blockchain first started as a cryptocurrency system with Bitcoin, thus it only makes sense that its widely adoption within the electric power sector would also follow the same trend. However, the focus here is precisely on tokens (i.e., cryptocurrencies) utilized to incentivise and encourage participants to trade and invest in green energy.

1) SolarCoin

In early 2014, Gogerty and Zitoli launched SolarCoin [106], a blockchain-based green token harvesting the energy of the sun by utilizing a network of PV-nodes all around the globe. The public ledger was first using the PoW consensus but soon switched to the PoS-Time consensus, due to the high computational resources needed in the first. The vision behind this token is based on a tangible source of energy that has been there for roughly four billion years (i.e., the sun) as well as the individuals' will to save this blue planet from the disastrous consequences of climate change. The whole network does not require an existing grid to function or deliver its goals as the PV-peers themselves are energy sources forming a P2P open electricity market.

2) CyClean

This token is intended to promote the consumption of clean energy via a rental platform of electric cars, motorbikes, or other vehicles. CyClean [107] is built on top of the Ethereum platform using smart contracts and is operated in South Korea but would be soon extended to the whole south Asia. The idea is that users can receive CyClean coins after renting clean products based on the distance or amount of time the product has been used in order to motivate individuals to invest in green energy products and eventually reduce our global greenhouse gas emissions.

3) NRGCoin

The cryptocurrency is the outcome of an academia-industry collaboration that started back in 2014 between the Vrije Universiteit Brussel and Enervalis (a software company for energy solutions). NRGcoin [108] facilitates the penetration of green energy sources by rewarding local production/consumption in a low-voltage power system. In addition to creating a secure and open electricity provisioning scheme, it also enables promoting a mutually beneficial ecosystem that fosters seamless interactions among all stakeholders (i.e., consumers, prosumers, operators and utilities). The mechanism is deployed on a set of hardware devices, which play the role of gateways within the residential homes for various measurements that are regularly sent to the smart contract governing the whole process of energy exchange (i.e., energy imported or exported to the power system). Prosumers can inject their generated renewable energy excess to the grid and are rewarded with NRGcoins automatically based on the rules defined within the smart contract, whereas consumers can purchase that energy in exchange of some coins.

4) CHARG COIN

Aimed to promote crowdsourced energy distribution among EVs' charging stations using blockchain, Charg coin [109] is a token built upon the Ethereum platform using smart contracts. The platform is comprised of a set of Charg-nodes (i.e., charging stations) and a Charg-App that allows users to navigate a map of private and public charging stations they could use for their EVs in exchange of some coins. The cryptocurrency attempts to solve the problem of finding a secure charging point no matter when or where, by allowing various entities to join and share their resources.

Discussion and Lessons Learned

The list of existing green-cryptocurrencies is quite exhaustive. Nonetheless, it is worth mentioning that this ever-growing trend of utilizing blockchain-based cryptocurrencies is highly susceptible to include an unwanted burden or congestion within the underlying infrastructure of the SG or to result in siloed and fragmented markets. Thus, the focus should be on alleviating the complexities that would arise from the incorporation of these crypto tokens by developing adequate methods for managing the power demand resulted from mining and avoiding negative pricing or price spikes within this contemporary SG P2P markets.

B. BLOCKCHAIN IoE-BASED INDUSTRIAL PLATFORMS

Beyond its cryptocurrency trading, blockchain was also harnessed to cope with the increasing complexity of the novel SG paradigm. In fact, the technology's potential was able to attract a myriad of start-ups all around the globe. During 2017 alone an amount of over 300 million U.S. dollars was raised by various companies that applied the technology to solve some of the electric power sector challenges [110]. Some of these start-ups were dedicated to smooth the transition towards novel P2P electricity trading markets, some focused on managing the demand-response and supply in a decentralized and auditable way. Whereas others focused on clean energy resources by fostering the use of renewable energy, EVs or any other clean product as well as raising funds to tackle climate change or issuing certificates for carbon-footprints. Some of these start-ups along with their vision and brief technical details are presented in Table. 3.

C. A CASE STUDY OF DE CEUVEL ENERGY COMMUNITY IN AMSTERDAM: JOULIETTE TOKEN

Known as the CleanTeck Playground of Amsterdam, De Ceuvel [111] is among the utmost sustainable and innovative urban projects in the Netherlands, or even in Europe. The former industrial zone was entirely redesigned using a

TABLE 3. Industrial blockchain-based initiatives in the electric power sector.

Project	Year	Description	Platform	Country
Greeneum [118]	2018	The project's vision is to provide a seamless demand-response management and accurate market forecasting by leveraging machine learning and IoT for clean energy resources. Greeneum offers a wide range of services such as electricity trading by utilizing the proof of energy transaction algorithm, decentralized energy management and optimization for utilities and microgrids, green capital for clean projects as well as carbon credits and green certificates for electricity producers.	Ethereum public chain	Israel
Drift [119]	2017	The project is aiming to address the intense disconnection and inflexibility witnessed in the current energy market in terms of renewable energy and funds access, or prosumers and their energy choices. Drift enables electricity producers to rapidly recoup investments and gives full ownership to users over their electricity, by playing the role of a transmission operator fully distributed and leveraging blockchain for an open exchange energy market. The platform also offers various services such as demand-response, grid management, EVs charging and smart metering.	Ethereum private chain	USA
Pylon [120]	2017	The platform enables a seamless, distributed and direct exchange of green energy from producers to consumers with no TTP intervention. Pylon is also based on an incentive mechanism for producing green energy in order to mediate the imbalance within the traditional power market.	Litecoin	Spain
Synergy [121]	2017	The platform is the by-product of the energy market liberalisation across Asia and is dedicated for enhancing energy trading by connecting a large number of local electricity producers/consumers and ensuring certainty of prices as well as transparency and accountability. Synergy is characterized by a modular architecture, allowing it to be easily integrated into existing SG infrastructures.	Ethereum public chain	Singapore
Power Ledger [122]	2016	To address the ever-growing demand of consumers to take control over their own energy needs by the massive integration of local PVs, Power Ledger focuses on providing smooth, low cost/carbon P2P electricity trading using blockchain technology to foster a dynamic, decentralized and autonomous market of renewable energy.	Solana	Australia
RecorDER [123]	2016	The platform is a coordinated architecture that allows national and local grid utilities, suppliers and DERs owners to interact among each other in a unified ecosystem to resolve conflicts of energy exchange, stack in a vertical way as well as share the value of those exchanges and confirm/approve the value of assets all in a single framework.	Ethereum private chain	UK
SunContract [124]	2017	Based on a mobile app, SunContract is a green energy sharing platform where customers (e.g., residential, commercial, or industrial entities) can exchange electricity with no centralized authority, enabling more sustainability and self-sufficiency in terms of energy management. The goal of the platform is to reduce the consumption of fossil fuel-based energy by incentivizing both costumers and producers to shift towards sustainable resources.	Ethereum private chain	Slovenia
DAO IPCI [125]	2016	The initiative is a non-profit, distributed and autonomous blockchain-based ecosystem developed to tackle climate change by proposing a set of mitigation instruments (e.g., carbon compliance units, renewable energy credits, carbon emission allowances, etc). The platform is built using smart contracts to enable a secure, transparent and cost-efficient transfer of the mitigation tokens.	Ethereum public chain	Russia
Omega Grid [126]	2017	The project is intended to provide a dynamic market system for electric utilities as well as their prosumers, with the goal of changing prosumers' DERs from a liability (requiring extensive management) into an asset. Omega Grid offers various services such as demand-response, peak shaving and helps the utilities at determining efficiently the best mixed strategy of balancing loads within a local SG.	Private blockchain	USA
SunChain [127]	2016	The platform offers a set of blockchain-based solutions dedicated for green energy exchange within local communities (e.g., residential/professional, or mixed buildings). SunChain is based on a virtual private blockchain built on top of the physical public grid to enable secure and certified exchange of power as well as virtual storage.	Hyperledger	France

fund of roughly 450 000 euros from a joint start-up grant and a bank loan back in 2012. Since then, the modernized urban neighbourhood, which location and layout are shown in Fig. 8 became a thriving hotspot for industry partners, entrepreneurs as well as researchers from all over the globe to experiment with. The site is composed of 16 upcycled old houseboats that were renovated into office buildings. They are equipped with 150 solar panels in total generating nearly 36 000 kWh per year, with a single connection to the grid. The local community also hosts a greenhouse, a B&B and a sustainable café [112].

1) JOULIETTE PROJECT OVERVIEW

Being a booming hub for innovative and ingenious experiments, De Ceuvel became a vibrant open lab, where novel concepts and disruptive technologies can be tested, to then be scaled into larger implementations. In fact, this has been the case for blockchain technology, with a pilot project that took off starting late 2017. The Jouliette (derived from Joule the energy unit) project [113] involved a partnership between both Alliander (one of the largest distribution system operators in the Netherlands) and Spectral (a smart energy company focusing on developing technological solutions

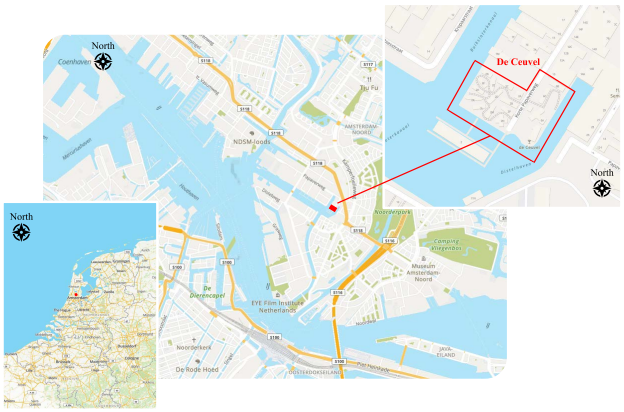


FIGURE 8. Location and layout of Jouliette's site De Ceuvel in Amsterdam.

unlocking the potential of smart grids and accelerating the transition to a 100% clean energy).

The idea behind the pilot is to build and test the applicability and sustainability of a private behind-the-meter locally confined and self-sufficient micro-grid energy community. The platform enables P2P energy trading between occupants of the area within the De Ceuvel eco-system, independently from the national grid operator, using Jouliette tokens. This designed crypto-currency and the whole underlying system are managed using a developed application by Spectral, accessible to only authorized entities and allows participants to:

- Visualize in real-time their local energy consumption/production and CO2 savings.
- Check their wallet's balance and transactions' history.
- Visualize energy forecasts based on machine learning models.
- Modify market exchange rules, energy costs, etc.
- Purchase goods at the café using their tokens.

The project was implemented using the MultiChain [114] blockchain platform, enabling fine-grained access rules and allowing members of the community to perform secure transactions in a distributed and transparent manner. Not only was the token used to buy energy, where for each produced 0.1 kWh of energy one Jouliette is mined. But it was also traded in exchange of other goods and services. For instance, a cup of cappuccino with a price equal to 2.60 Euro is worth 260 Jouliette in De Ceuvel's café. Meanwhile, car sharing is an additional service that was expected to be included in the trading system.

2) PHASE II: BEYOND DE CEUVEL, REGULATORY AND TECHNICAL CHALLENGES

The second phase of the project, that was launched in mid 2018, involved scaling the ecosystem by extending it to the nearby Buiksloterham neighbourhood and focusing on the technical as well as regulatory challenges that might arise from this expansion [115]. Although the parties involved in this project were able to gain several exemptions from grid regulations. They came to the conclusion that scaling a P2P energy trading eco-system would require a cautious navigation of the regulatory landscape by exploiting loopholes and that some cases might simply not be possible given the current market's conditions. Another concern was in terms of taxes as the electricity generated from the PVs and stored within batteries was taxed twice: while charging the battery and also when the electricity is retrieved for supply. Thus, making the plausibility of largely scaling this system in the future quite unclear.

In fact, the regulations in the Netherlands specify that prosumers are not allowed to freely trade their surplus of energy. Rather, they can sell this surplus directly to their energy supplier following a netting scheme. Meaning that the energy injected back to the grid is reduced from the energy consumed from the provider. In case, the prosumers are to generate more electricity than they have consumed (e.g., during summer for instance) they are required to sell it back to the utility (if they don't have batteries where they can store this surplus), and the energy providers could buy it with a lower price.

Furthermore, the idea of the project is that theoretically any person should be allowed to take part of the eco-system, consequently, there will be multiple blockchain writers. However, not all participants are assumed to be known. This might be exceptionally the case at De Ceuvel site, due to the small size of the community emerging from the location of the site, but it's not a technical aspect that could be generalized for all micro-grid systems. Nonetheless, participants should have the capacity to verify if others are adhering to the rules, if the eco-system is to support free trading of tokens and energy. But this could be problematic as the Jouliette token is mined when a given amount of energy has actually been generated by a rooftop PV panel at a certain moment. Unlike verifying the solution of a mathematical puzzle in PoW for example, verifying whether electricity was produced isn't that straightforward.

In this use case and in order to record Jouliettes, the project relied on a special hardware device that was developed by Spectral, which is tamper-proof and does not put any trust on the participants using it to write on the blockchain's ledger. Therefore, Spectral, being the supplier of the software as well as the hardware tools used by the participants to write, could basically be seen as a trusted third party (i.e., representing a single root of trust). Thus, if we are to follow Wüst and Gervais's scheme [116] on whether blockchain is the appropriate solution to adopt. The answers to both questions: ''are writers known?'' and ''are they trusted?'' are affirmative, due to the tamper-proof nature of the software and hardware devices utilized, leading to a conclusion not advocating the use of blockchain in the first place. Meanwhile, if we are to follow Koens and Pool's scheme [117], by considering Spectral as a TTP we end up with a shared database rather than a blockchain.

Discussion and Lessons Learned

Even if blockchain is still the right choice of technology, the accountability aspect within such energy trading frameworks is not that trivial. Suppose for instance a participant within the community tries tampering with the hardware or software components of the system by exploiting a firmware vulnerability or bug within the eco-system, how is he going to be held accountable? Or who would be held accountable? In addition, how are participants going to agree on the market rules?

What if they don't reach consensus in this supposedly open free market? Furthermore, if the system is implemented in a fully decentralized manner, meaning the actual prosumers are the blockchain nodes, how can the privacy of each participant be protected if all their transactions' history is to be seen by anyone part of the system? These raised questions could pave the way to the implementation of novel solutions that would try to tackle these challenges. For instance, layer-2 blockchain approaches such as zero-knowledge proof could be leveraged to avoid disclosing sensitive data related to the prosumers. Governance could be addressed using fair and democratic voting-based schemes. Whereas malicious behaviours might be dealt with using reputation and/or punishment-based mechanisms that would meet the requisites of such eco-systems.

VI. REMAINING CHALLENGES AND FUTURE DIRECTIONS

In this section, we examine the remaining challenges and future perspectives of both blockchain itself as a technology, which is far from being mature and is still evolving, as well as the limitations of its applications within IoE-based scenarios.

A. BLOCKCHAIN LIMITATIONS AND POTENTIAL RESEARCH DIRECTIONS

The technical challenges that blockchain is still facing can be broadly summarized in terms of throughput, consensus protocols, smart contracts flaws, ledger storage, and last but not least, the imminent threat that quantum computers might pose to blockchain's cryptography.

1) TRANSACTIONS PER SECOND RATE

The rate at which a blockchain is capable of processing transactions is usually referred to as the transaction per second (TPS) rate, or simply the throughput of the blockchain-based system. Up to this moment, the TPS rate remains one of the major issues faced while deploying blockchain at a large scale, such as SGs, which are expected to be dealing with an enormous number of transactions and are highly sensitive to latency to ensure a real-time response and monitoring. Although several approaches have been proposed in the literature to tackle this concern, scaling from applying DAG, sharding, sidechain, cross-chain, or off-chain techniques [128], the efficiency of these solutions and whether they provide full decentralization in regard to the blockchain trilemma remain an open issue.

2) CONSENSUS ALGORITHMS

Although there exist various consensus protocols, each of them has its own advantages and drawbacks. For instance, PoW offers high security within a public decentralized blockchain setting but it is extensively expensive in terms of computational resources, thus it has a high carbon footprint and it won't make much sense to leverage it for a SG use case where the paradigm is all about decarbonization. Perhaps it's possible to utilize green energies as a source for mining, but that would still be way far-fetched. Meanwhile, PoS solves the computation issue of PoW, but raises another concern of not being fully decentralized as its based-on wealth and that tends to condense following a centralized pattern. Whereas the BFT-based algorithms are taxed in terms of success rate when the number of nodes exceeds a certain threshold. In other words, they don't scale well as the number of validators within the blockchain increases. Extensive work is still being carried on in order to address these limitations and to provide a more enhanced performance. However, we are far yet to reach the required goal for these consensus mechanisms to be adopted efficiently within power grids. Specifically, the SG is expected to encompass a variety of IoT-based devices which are highly constrained in terms of their computational capabilities, thus, designing edge-based schemes to offload the consensus tasks while ensuring trust still needs to be investigated.

3) SMART CONTRACTS VULNERABILITIES

What ensures the malleability of blockchains is their ability to host smart contracts that enable the execution of various functionalities. However, a smart contract is first and foremost a piece of code, that is written in a development language depending on the blockchain platform in which it is deployed. Besides, it goes without saying that those contracts are susceptible to have some vulnerabilities or flaws that could be exploited to jeopardize the whole blockchain system [129], [130]. For instance, the decentralized autonomous organization, an Ethereum crowdsourcing platform, was the victim of a massive hack in 2016 worth nearly 60 million U.S dollars. The hack exploited a call-back vulnerability of the withdraw function within its smart contract, enabling the attacker to transfer ether. The attack was highly controversial, and it eventually led to the hard forking of Ethereum in order to recover the hacked funds, as a part of the Ethereum community (now known as Ethereum Classic) decided to honour the immutability of the chain. Thus, it is important to keep in mind the security risk these contracts might entail, and design them following some proper security guidelines.

4) LEDGER STORAGE AND REDUNDANCY

It is worth acknowledging that blockchain redundancy is both an advantageous and disadvantageous thing simultaneously. Duplicating the whole ledger among all peers ensures the reliability and accuracy of data stored within the blockchain. If one node goes down or is compromised the rest of the nodes are still intact and this would ensure the normal functioning of the distributed system. However, it is important to also stress the fact that as new transactions and blocks are being added to the immutable chain (i.e., nothing can be deleted, or at least theoretically that's what blockchain stands for) the size of the ledge would keep growing exponentially leading to what is known as the blockchain bloat. Basically, the size of the whole chain would make it hard and cumbersome for new nodes to download the previous record and synchronize with the blockchain, which might also affect the speed at which transactions are processed. Specifically, combining blockchain with IoE-based systems would inevitably yield to this issue, as SGs encompass a wide range of devices, components and entities that are supposed to exchange data frequently and at high speed. Several techniques have been proposed in the literature to address this challenge such as sharding, zero knowledge proofs or ephemeral blockchains, yet these solutions bring their own complexity that need to be solved for them to be implemented efficiently.

5) QUANTUM COMPUTERS AND CRYPTOGRAPHY

The security of blockchains is highly dependent on one-way mathematical functions, used for instance to derive a public key from a private one or the generation of a digital signature, which can be easily checked but nearly unforgeable. Those one-way functions are also used for the validation of the shared ledger, precisely the history of all blocks and transactions, which are structured using hash functions (i.e., Merkle trees or hash pointers). However, it is estimated that within the next decades, quantum computers that exploit superposition of states, might have the capacity to break these functions and cryptographic algorithms. Thus, jeopardizing the major defence mechanism of blockchain systems as well as others of course [131].

B. IoE CHALLENGES AND POTENTIAL RESEARCH DIRECTIONS

The energy sector is known to be highly regulated, thus the prospects of leveraging the potential of blockchain crucially depend on policymakers. It is important for these decision-makers to fully understand the intersection of privacy within blockchain with various regulations and the right to be forgotten. To foster the development of open-source projects and standards that would enable interoperability rather than fragmented platforms. To think of innovative ways that would ensure the sustainability of these blockchain-based solution in terms of incentive mechanisms. Finally, to enhance the cyber-resilience of SGs, which has been neglected so far.

1) INTEROPERABILITY AND STANDARDIZATION

To embrace the full potential and benefit of blockchain, the distributed ledgers underpinning it must be capable of exchanging freely information, however, it is not the case. Blockchain platforms are currently not designed to be interoperable directly, as each ledger has its own way of structuring data and blocks, and they define differently who, how and what data are to be chained following the consensus mechanisms they utilize [132]. For instance, in the case of SGs there is a high risk of inconsistency and ending up with fragmented markets, where each operator or utility would be using its own private blockchain platform to manage consumption or metering data, the demand-response or provide other services which are only functional within a defined environment or framework. Thus, it is tremendously important to set standards that would guarantee the long-term interoperability of blockchain-based frameworks for power systems in terms of devices, protocols used, software, etc. As this would eventually ease the development of the power sector that is becoming tangled with other sectors such as transportation with the high increase of EVs.

2) PRIVACY AND IMMUTABILITY

As we have explained before, the fundamental characteristics of blockchain are transparency and immutability, which do not necessarily align with or guarantee privacy in a direct manner. For instance, personal data are highly regulated in the European Union based on several laws that sometimes require certain information to be anonymized or even deleted to be compliant with individuals' right to be forgotten. However, it is not straightforward to figure out how blockchain can still ensure efficient automation, auditability and transparency while the records are fully anonymous, as blockchain in the way it is built now can only offer pseudo-anonymity. Furthermore, if it's possible to delete data or change it within the shared ledger, this would violate the very core idea of what blockchain is. Thus, it is important to acknowledge that blockchain as it is defined might not be the right solution in certain cases and if stretched way far beyond the boundaries of its defined concept and core values, we might end up with simply a distributed database using cryptography managed in a somehow centralized manner.

3) INCENTIVES AND SUSTAINABILITY

The mechanism that guarantees agreement among all peers of a blockchain network is the consensus protocol, which satisfies the following characteristics: correctness, consistency and traceability. Nevertheless, it is possible that the peers might disagree vis-à-vis the chain to be adopted by deviating from the longest chain. Thus, a consensus algorithm is supposed to be combined with game theoretical incentive

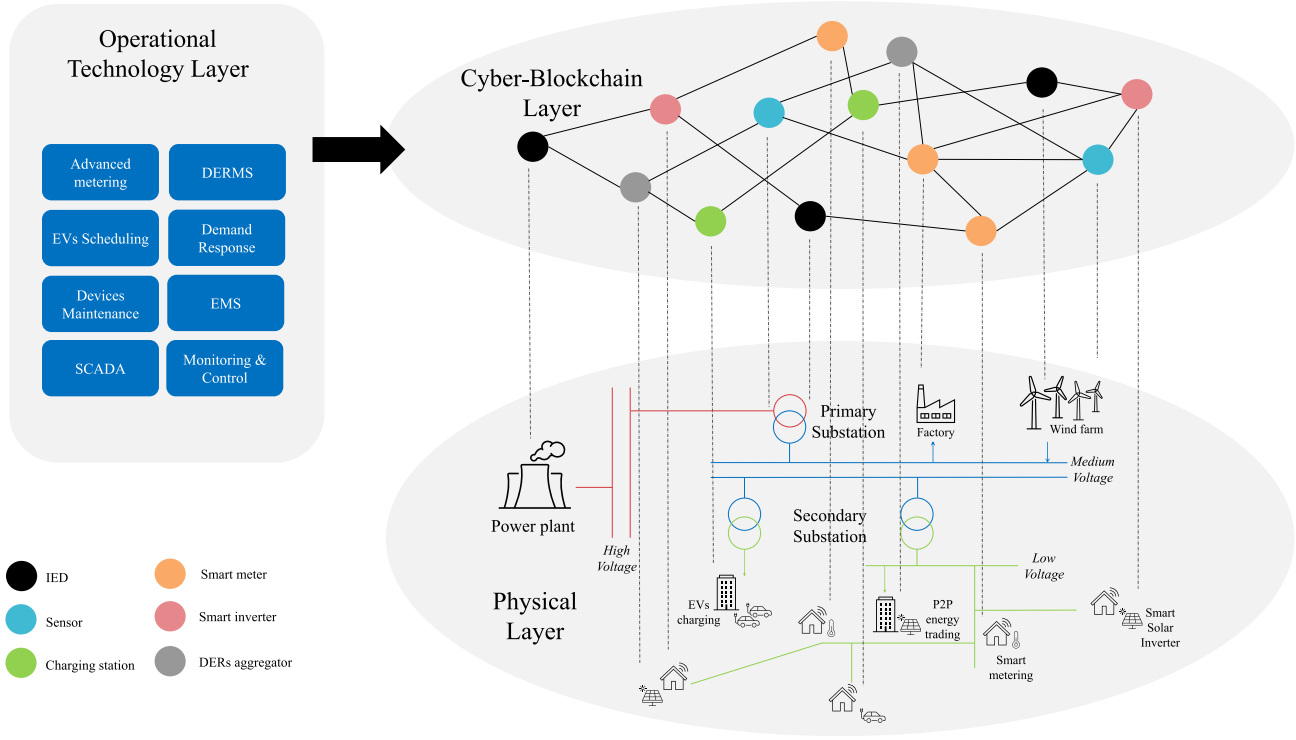


FIGURE 9. Future IoE-enabled cyber-blockchain physical system infrastructure.

mechanisms. Meaning that nodes would be subject to a loss, such as a wasted investment in computational resources to solve a puzzle in the case of PoW, if they don't follow the protocol to guarantee reliability and sustainability. In the case of SGs it is not straightforward how to design incentive mechanism that would incorporate the essence of the energy sector, its ambitions and goals while transcending monetary values or cryptocurrencies. Thus, a major future research direction would be designing, from a game theoretical perspective, efficient and reliable incentive/penalty schemes that would integrate all entities [133]. Scaling from utilities, consumers/producers, sensors, blockchain validators and stakeholders within the blockchain-based IoE framework, while still ensuring continuity, longevity, correctness and reliability within the whole grid.

4) CYBER-RESILIENCE OF SGs

Blockchain was the focus of different literature outputs dedicated to enforcing the cyber-resilience of SGs, which we have discussed previously in Subsection IV-E. Nonetheless, compared to the interest shown towards the market-based applications of the technology in the electric power sector; the number of solutions deeply focusing on the cyber-resilience of SGs is quite modest. Thus, some research topics and ideas can be further investigated, which are highlighted in Fig. 9 that depicts what the future smart grid might look like as a cyber-blockchain physical system. For instance, blockchain can be utilized as a framework to manage in a distributed and auditable way the security updates of IEDs and to protect against potential malicious modifications or reverse engineering attacks. As this could temper with the software/firmware of the IEDs and eventually lead to undesired behaviour or complicate the remote response to an attack (which was the case during the Ukrainian cyber-attack [134]).

In addition, blockchain could be used to isolate or segregate compromised field-sensors or maybe devices susceptible to be exploited using zero-day vulnerabilities by flagging them in a way that attackers would not be able to temper with. Furthermore, the technology could also serve as an immutable ledger that would record and log all activities and control commands within the power transmission or distribution system. As those would serve as a baseline for audit or monitoring. Because how can we tell that something is wrong unless we have a trusted baseline that would tell us what's right?

For instance, the SG would be segregated into different regions monitored by a variety of IoT-blockchain enabled devices. Where each region would be represented by a blockchain shard to increase the throughput of the blockchain system. These shards would contain a set of smart contracts defining the logic and operational functionalities within a segment of the power grid. While also considering the synchronization issue between all shards to ensure a wide visibility and consistency of measurements across regions as well as controls.

Discussion and Lessons Learned

Arguably, the primary challenge associated with blockchain is an inadequacy of understanding how the technology functions. In addition to a general lack of awareness around its technical limitations (e.g., scalability, latency, vulnerabilities, interoperability, etc.) as well as its complex governance (e.g., consensus rules, incentives, penalties, etc.) and finally its intersection with the regulatory frameworks that currently exist (e.g., privacy, free energy markets, etc.). Nonetheless, the technology already proved its potential in various scenarios within the energy sector, where multiple organizations and stakeholders could work jointly on shared areas. Rather than having each organization develop its own blockchain with different standards defeating the purpose of having a distributed ledger in the first place. Consequently, ending up with a roughly less efficient system compared to conventional approaches. Besides, there remain numerous plausible scenarios where blockchain is still yet to be leveraged, particularly in the cyber-security realm, in order to assess whether it is the right choice of technology. After all, the fundamental core of research is all about testing new hypothesis.

VII. CONCLUSION

Although the integration of blockchain as an emerging technology within IoE-based systems is still at its infancy, it already succeeded at drawing the attention of several researchers in a myriad of ways. In this paper, we tried to provide a holistic and exhaustive review of several blockchain-based contributions within the IoE paradigm. First, we started with a brief yet concise introduction to blockchain and its concepts for the unfamiliar readers. We then laid out the rationale behind the adoption of blockchain in the IoE, by first going through the transition towards decentralization that SGs are partially witnessing with the massive integration of DERs, and second explaining how the security and distribution requirements for future SGs are consistent with the characteristics that blockchain offers. Afterwards, we categorized blockchain-based applications in the IoE into five inclusive areas and for each of them we provided a comprehensive up-to-date state-of-the-art. We gave some insights into future paradigms, their intersection with blockchain and implications for future SGs. We also presented some industrial initiatives to show the real-world adoption of blockchain in the electric power sector from different angles, which demonstrates the practicality of the technology, in addition to a case study. Last but not least, we discussed some lessons learned as well as the remaining challenges faced while adopting blockchain for future SGs, and how those could be the focus of novel research outputs. We hope this paper would offer some useful guidance for future research efforts by providing a comprehensive overview in regard to what has been achieved so far and what are the next steps to be taken in this area to fully leverage the potential of blockchain applied to IoE.

REFERENCES

[1] U.S. Energy Information Administration (EIA). *International Energy Outlook 2020*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.eia.gov/outlooks/ieo/

[2] G. Dileep, "A survey on smart grid technologies and applications," *Renew. Energy*, vol. 146, pp. 2589–2625, Feb. 2020, doi: 10.1016/j.renene.2019.08.092.

[3] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 2814–2825, Jul. 2018, doi: 10.1109/TII.2018.2819169.

[4] C. Peng, H. Sun, M. Yang, and Y. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1612–1623, Aug. 2019, doi: 10.1109/TSMC.2018.2884952.

[5] S. Marzal, R. Gonzalez-Medina, R. Salas-Puente, G. Garcera, and E. Figueres, "An embedded Internet of Energy communication platform for the future smart microgrids management," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 7241–7252, Aug. 2019, doi: 10.1109/JIOT.2019.2915389.

[6] K. Mahmud, B. Khan, J. Ravishankar, A. Ahmadi, and P. Siano, "An Internet of Energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview," *Renew. Sustain. Energy Rev.*, vol. 127, Jul. 2020, Art. no. 109840, doi: 10.1016/j.rser.2020.109840.

[7] V. Caballero, D. Vernet, and A. Zaballos, "Social Internet of Energy—A new paradigm for demand side management," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9853–9867, Dec. 2019, doi: 10.1109/JIOT.2019.2932508.

[8] M. D. Smith and M. E. Paté-Cornell, "Cyber risk analysis for a smart grid: How smart is smart enough? A multiarmed bandit approach to cyber security investment," *IEEE Trans. Eng. Manag.*, vol. 65, no. 3, pp. 434–447, Feb. 2018, doi: 10.1109/TEM.2018.2798408.

[9] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094, doi: 10.1016/j.comnet.2019.107094.

[10] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP protocol: Security threats and challenges," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2452–2459, Sep. 2017, doi: 10.1109/TSG.2017.2669647.

[11] P. Siano, G. De Marco, A. Rolan, and V. Loia, "A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets," *IEEE Syst. J.*, vol. 13, no. 3, pp. 3454–3466, Sep. 2019, doi: 10.1109/JSYST.2019.2903172.

[12] N. Wang, X. Zhou, X. Lu, Z. Guan, L. Wu, X. Du, and M. Guizani, "When energy trading meets blockchain in electrical power system: The state of the art," *Appl. Sci.*, vol. 9, no. 8, pp. 3454–3466, Apr. 2019, doi: 10.3390/app9081561.

[13] A. Baggio and F. Grimaccia, "Blockchain as key enabling technology for future electric energy exchange: A vision," *IEEE Access*, vol. 8, pp. 205250–205271, 2020, doi: 10.1109/ACCESS.2020.3036994.

[14] M. Troncia, M. Galici, M. Mureddu, E. Ghiani, and F. Pilo, "Distributed ledger technologies for peer-to-peer local markets in distribution networks," *Energies*, vol. 12, no. 17, p. 3249, Aug. 2019, doi: 10.3390/en12173249.

[15] S. Aggarwal, N. Kumar, S. Tanwar, and M. Alazab, "A survey on energy trading in the smart grid: Taxonomy, research challenges and solutions," *IEEE Access*, vol. 9, pp. 116231–116253, 2021, doi: 10.1109/ACCESS.2021.3104354.

[16] A. Goranovic, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *Proc. 43rd Annu. Conf. IEEE Ind. Electron. Soc.*, Beijing, China, Oct. 2017, pp. 6153–6158, doi: 10.1109/IECON.2017.8217069.

[17] M. F. Zia, M. Benbouzid, E. Elbouchikhi, S. M. Muyeen, K. Techato, and J. M. Guerrero, "Microgrid transactive energy: Review, architectures, distributed ledger technologies, and market analysis," *IEEE Access*, vol. 8, pp. 19410–19432, 2020, doi: 10.1109/ACCESS.2020.2968402.

[18] A. Ahl, M. Yarime, K. Tanaka, and D. Sagawa, "Review of blockchain-based distributed energy: Implications for institutional development," *Renew. Sustain. Energy Rev.*, vol. 107, pp. 200–211, Jun. 2019, doi: 10.1016/j.rser.2019.03.002.
[19] Q. Wang, R. Li, and L. Zhan, "Blockchain technology in the energy sector: From basic research to real world applications," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100362, doi: 10.1016/j.cosrev.2021.100362.
[20] N. U. Hassan, C. Yuen, and D. Niyato, "Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions," *IEEE Ind. Electron. Mag.*, vol. 13, no. 4, pp. 106–118, Dec. 2019, doi: 10.1109/MIE.2019.2940335.
[21] O. Jogunola, B. Adebisi, A. Ikpehai, S. I. Popoola, G. Gui, H. Gacanin, and S. Ci, "Consensus algorithms and deep reinforcement learning in energy market: A review," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4211–4227, Mar. 2021, doi: 10.1109/JIOT.2020.3032162.
[22] M. Nour, J. P. Chaves-Ávila and Á. Sánchez-Miralles, "Review of blockchain potential applications in the electricity sector and challenges for large scale adoption," *IEEE Access*, vol. 10, pp. 47384–47418, 2022, doi: 10.1109/ACCESS.2022.3171227.
[23] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for Internet of Energy management: Review, solutions, and challenges," *Comput. Commun.*, vol. 151, pp. 395–418, Feb. 2020, doi: 10.1016/j.comcom.2020.01.014.
[24] A. Hasankhani, S. M. Hakimi, M. Bisheh-Niasar, M. Shafie-khah, and H. Asadolahi, "Blockchain technology in the future smart grids: A comprehensive review and frameworks," *Int. J. Electr. Power Energy Syst.*, vol. 129, Jul. 2021, Art. no. 106811, doi: 10.1016/j.ijepes.2021.106811.
[25] A. Joseph and P. Balachandra, "Smart grid to energy internet: A systematic review of transitioning electricity systems," *IEEE Access*, vol. 8, pp. 215787–215805, 2020, doi: 10.1109/ACCESS.2020.3041031.
[26] Y. Guo, Z. Wan, and X. Cheng, "When blockchain meets smart grids: A comprehensive survey," *High-Confidence Comput.*, vol. 2, no. 2, Jun. 2022, Art. no. 100059, doi: 10.1016/j.hcc.2022.100059.
[27] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf
[28] V. Buterin. (2013). *A Next Generation Smart Contract and Decentralized Application Platform*. Accessed: Oct. 3, 2022. [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
[29] N. Szabo. (1996). *Smart Contracts: Building Blocks for Digital Markets*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
[30] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, Jan. 2020, doi: 10.1109/COMST.2020.2969706.
[31] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.
[32] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," *IEEE Access*, vol. 8, pp. 54371–54401, 2020, doi: 10.1109/ACCESS.2020.2981415.
[33] *Cambridge Bitcoin Electricity Consumption Index*. Accessed: Oct. 3, 2022. [Online]. Available: https://cbeci.org/
[34] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.* Zurich, Switzerland, pp. 112–125, May 2016, doi: 10.1007/978-3-319-39028-4_9.
[35] B. Abdulkadir, N. Crisostomo, J. Allen, E. Wood, and C. Rames. (2018). *California Plug-in Electric Vehicle Infrastructure Projections: 2017–2025*. California Energy Commission. Accessed: Oct. 3, 2022. [Online]. Available: https://www.nrel.gov/docs/fy18osti/70893.pdf
[36] International Energy Agency. *Digitalization and Energy*. Accessed: Oct. 3, 2022. [Online]. Available: https://iea.blob.core.windows.net/assets/b1e6600c-4e40-4d9c-809d-1d1724c763d5/Digitalizationand Energy3.pdf
[37] International Renewable Energy Agency (IRENA). *Renewable Energy Statistics 2021*. Accessed: Oct. 3, 2022. [Online]. Available: https://irena.org/publications/2021/Aug/Renewable-energy-statistics-2021
[38] J. Guo, X. Ding, and W. Wu, "A blockchain-enabled ecosystem for distributed electricity trading in smart city," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 2040–2050, Feb. 2021, doi: 10.1109/JIOT.2020.3015980.
[39] M. K. Alashery, Z. Yi, D. Shi, X. Lu, C. Xu, Z. Wang, and W. Qiao, "A blockchain-enabled multi-settlement quasi-ideal peer-to-peer trading framework," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 885–896, Jan. 2021, doi: 10.1109/TSG.2020.3022601.
[40] A. Esmat, M. de Vos, Y. Ghiassi-Farrokhfal, P. Palensky, and D. Epema, "A novel decentralized platform for peer-to-peer energy trading market with blockchain technology," *Appl. Energy*, vol. 282, Jan. 2021, Art. no. 116123, doi: 10.1016/j.apenergy.2020.116123.
[41] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn, "Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1612–1623, Aug. 2019, doi: 10.1109/TSMC.2019.2916565.
[42] A. Kavousi-Fard, A. Almutairi, A. Al-Sumaiti, A. Farughian, and S. Alyami, "An effective secured peer-to-peer energy market based on blockchain architecture for the interconnected microgrid and smart grid," *Int. J. Electr. Power Energy Syst.*, vol. 132, Nov. 2021, Art. no. 107171, doi: 10.1016/j.ijepes.2021.107171.
[43] 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, Aug. 2017, doi: 10.1109/TII.2017.2786307.
[44] F. Jamil, N. Iqbal, S. Ahmad, and D. Kim, "Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid," *IEEE Access*, vol. 9, pp. 39193–39217, 2021, doi: 10.1109/ACCESS.2021.3060457.
[45] M. Gough, S. F. Santos, A. Almeida, M. Lotfi, M. S. Javadi, D. Z. Fitiwi, G. J. Osorio, R. Castro, and J. P. S. Catalao, "Blockchain-based transactive energy framework for connected virtual power plants," *IEEE Trans. Ind. Appl.*, vol. 58, no. 1, pp. 986–995, Jan. 2022, doi: 10.1109/TIA.2021.3131537.
[46] F. Luo, Z. Y. Dong, J. Murata, Z. Xu, and G. Liang, "A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4097–4108, Sep. 2018, doi: 10.1109/TPWRS.2018.2876612.
[47] T. Wang, J. Guo, S. Ai, and J. Cao, "RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration," *Appl. Energy*, vol. 295, no. 8, Aug. 2021, Art. no. 117056, doi: 10.1016/j.apenergy.2021.117056.
[48] A. Kumari and S. Tanwar, "A reinforcement-learning-based secure demand response scheme for smart grid system," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2180–2191, Feb. 2022, doi: 10.1109/JIOT.2021.3090305.
[49] Q. Yang, H. Wang, T. Wang, S. Zhang, X. Wu, and H. Wang, "Blockchain-based decentralized energy management platform for residential distributed energy resources in a virtual power plant," *Appl. Energy*, vol. 294, Jul. 2021, Art. no. 117026, doi: 10.1016/j.apenergy.2021.117026.
[50] M. Zhang, F. Eliassen, A. Taherkordi, H.-A. Jacobsen, H.-M. Chung, and Y. Zhang, "Demand–response games for peer-to-peer energy trading with the hyperledger blockchain," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 1, pp. 19–31, Jan. 2022, doi: 10.1109/TSMC.2021.3111135.
[51] S. Noor, W. Yang, M. Guo, K. H. van Dam, and X. Wang, "Energy demand side management within micro-grid networks enhanced by blockchain," *Appl. Energy*, vol. 228, pp. 1385–1398, Aug. 2018, doi: 10.1016/j.apenergy.2018.07.012.
[52] G. Sciume, E. J. Palacios-Garcia, P. Gallo, E. R. Sanseverino, J. C. Vasquez, and J. M. Guerrero, "Demand response service certification and customer baseline evaluation using blockchain technology," *IEEE Access*, vol. 8, pp. 139313–139331, 2020, doi: 10.1109/ACCESS.2020.3012781.
[53] G. Tsaousoglou, K. Steriotis, N. Efthymiopoulos, P. Makris, and E. Varvarigos, "Truthful, practical and privacy-aware demand response in the smart grid via a distributed and optimal mechanism," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3119–3130, Jul. 2020, doi: 10.1109/TSG.2020.2965221.

[54] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "GUARDIAN: Blockchain-based secure demand response management in smart grid system," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 613–624, Jul. 2020, doi: 10.1109/TSC.2019.2962677.

[55] M. L. Di Silvestre, P. Gallo, E. R. Sanseverino, G. Sciumè, and G. Zizzo, "Aggregation and remuneration in demand response with a blockchain-based framework," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4248–4257, Aug. 2020, doi: 10.1109/TIA.2020.2992958.

[56] A. C. Tsolakis, I. Moschos, K. Votis, D. Ioannidis, T. Dimitrios, P. Pandey, S. Katsikas, E. Kotsakis, and R. García-Castro, "A secured and trusted demand response system based on blockchain technologies," in *Proc. Innov. Intell. Syst. Appl.,* Thessaloniki, Greece, Sep. 2018, pp. 1–6, doi: 10.1109/INISTA.2018.8466303.

[57] P. Danzi, S. Hambridge, C. Stefanovic, and P. Popovski, "Blockchain-based and multi-layered electricity imbalance settlement architecture," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2018, pp. 1–7, doi: 10.1109/SmartGridComm.2018.8587577.

[58] Y. He, C. Zhang, B. Wu, Z. Geng, K. Xiao, and H. Li, "A trusted architecture for EV shared charging based on blockchain technology," *High-Confidence Comput.*, vol. 1, no. 2, Dec. 2021, Art. no. 100001, doi: 10.1016/j.hcc.2021.100001.

[59] X. Chen, T. Zhang, W. Ye, Z. Wang, and H. H.-C. Iu, "Blockchain-based electric vehicle incentive system for renewable energy consumption," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 1, pp. 396–400, Jan. 2021, doi: 10.1109/TCSII.2020.2996161.

[60] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5799–5812, Jun. 2020, doi: 10.1109/TVT.2020.2967052.

[61] 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, Dec. 2017, doi: 10.1109/TII.2017.2709784.

[62] Y. Li and B. Hu, "An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2627–2637, May 2020, doi: 10.1109/TSG.2019.2958971.

[63] J. Anish, A. G. Singh, and K. Neeraj, "SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," *Comput. Netw.*, vol. 153, pp. 36–48, Apr. 2019, doi: 10.1016/j.comnet.2019.02.002.

[64] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019, doi: 10.1109/JIOT.2018.2869297.

[65] M. Khorasany, A. Dorri, R. Razzaghi, and R. Jurdak, "Lightweight blockchain framework for location-aware peer-to-peer energy trading," *Int. J. Electr. Power Energy Syst.*, vol. 127, May 2021, Art. no. 106610, doi: 10.1016/j.ijepes.2020.106610.

[66] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107209, doi: 10.1016/j.compeleceng.2021.107209.

[67] B. Wang, S. Zhao, Y. Li, C. Wu, J. Tan, H. Li, and K. Yukita, "Design of a privacy-preserving decentralized energy trading scheme in blockchain network environment," *Int. J. Electr. Power Energy Syst.*, vol. 125, Feb. 2021, Art. no. 106465, doi: 10.1016/j.ijepes.2020.106465.

[68] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019, doi: 10.1109/TII.2019.2893433.

[69] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018, doi: 10.1109/TDSC.2016.2616861.

[70] Q. Yang and H. Wang, "Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11463–11475, Jul. 2021, doi: 10.1109/JIOT.2021.3051323.

[71] Z. Guan, X. Lu, W. Yang, L. Wu, N. Wang, and Z. Zhang, "Achieving efficient and privacy-preserving energy trading based on blockchain and ABE in smart grid," *J. Parallel Distrib. Comput.*, vol. 147, pp. 34–45, Jan. 2021, doi: 10.1016/j.jpdc.2020.08.012.

[72] K. Li, Y. Yang, S. Wang, R. Shi, and J. Li, "A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102189, doi: 10.1016/j.cose.2021.102189.

[73] M. U. Hassan, M. H. Rehmani, and J. Chen, "DEAL: Differentially private auction for blockchain-based microgrids energy trading," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 263–275, Apr. 2020, doi: 10.1109/TSC.2019.2947471.

[74] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2019, doi: 10.1109/TEM.2019.2922936.

[75] S. Chen, L. Yang, C. Zhao, V. Varadarajan, and K. Wang, "Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid," *Engineering*, vol. 8, pp. 159–169, Jan. 2022, doi: 10.1016/j.eng.2020.06.018.

[76] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in IoT-enabled smart-grid system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021, doi: 10.1109/JIOT.2020.3030308.

[77] W. Xu, J. Li, M. Dehghani, and M. Ghasemigarpachi, "Blockchain-based secure energy policy and management of renewable-based smart microgrids," *Sustain. Cities Soc.*, vol. 72, Sep. 2021, Art. no. 103010, doi: 10.1016/j.scs.2021.103010.

[78] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7300–7309, Nov. 2019, doi: 10.1109/TIA.2019.2919820.

[79] B. Hu, C. Zhou, Y. C. Tian, Y. Qin, and X. Junping, "A collaborative intrusion detection approach using blockchain for multimicrogrid systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1720–1730, Aug. 2019, doi: 10.1109/TSMC.2019.2911548.

[80] A. Sadu, A. Jindal, G. Lipari, F. Ponci, and A. Monti, "Resilient design of distribution grid automation system against cyber-physical attacks using blockchain and smart contract," *Blockchain, Res. Appl.*, vol. 2, no. 1, Mar. 2021, Art. no. 100010, doi: 10.1016/j.bcra.2021.100010.

[81] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, Mar. 2018, doi: 10.1109/TSG.2018.2819663.

[82] J. C. Olivares-Rojas, E. Reyes-Archundia, J. A. Gutierrez-Gnecchi, J. Cerda-Jacobo, and J. W. Gonzalez-Murueta, "A novel multitier blockchain architecture to protect data in smart metering systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1271–1284, Nov. 2020, doi: 10.1109/TEM.2019.2950410.

[83] Z. Shi, W. Yao, Z. Li, L. Zeng, Y. Zhao, R. Zhang, Y. Tang, and J. Wen, "Artificial intelligence techniques for stability analysis and control in smart grids: Methodologies, applications, challenges and future directions," *Appl. Energy*, vol. 278, Nov. 2020, Art. no. 115733, doi: 10.1016/j.apenergy.2020.115733.

[84] L. Richter, M. Lehna, S. Marchand, C. Scholz, A. Dreher, S. Klaiber, and S. Lenk, "Artificial intelligence for electricity supply chain automation," *Renew. Sustain. Energy Rev.*, vol. 163, Jul. 2022, Art. no. 112459, doi: 10.1016/j.rser.2022.112459.

[85] M. Massaoudi, H. Abu-Rub, S. S. Refaat, I. Chihi, and F. S. Oueslati, "Deep learning in smart grid technology: A review of recent advancements and future prospects," *IEEE Access*, vol. 9, pp. 54558–54578, 2021, doi: 10.1109/ACCESS.2021.3071269.

[86] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K. R. Choo, "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5110–5118, Aug. 2020, doi: 10.1109/TII.2019.2957140.

[87] S. Ganesh, S. S. Siddharthan, B. R. Rajakumar, S. N. Pari, J. Padmanabhan, and V. Priya, "Hybrid-AI blockchain supported protection framework for smart grids," in *Proc. Sci. Inf. Conf.*, Jul. 2022, pp. 646–659, doi: 10.1007/978-3-031-10467-1_39.

[88] H. ElHusseini, C. Assi, B. Moussa, R. Attallah, and A. Ghrayeb, "Blockchain, AI and smart grids: The three musketeers to a decentralized EV charging infrastructure," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 24–29, Jun. 2020, doi: 10.1109/IOTM.0001.1900081.
[89] M. Faheem, S. B. H. Shah, R. A. Butt, B. Raza, M. Anwar, M. W. Ashraf, M. A. Ngadi, and V. C. Gungor, "Smart grid communication and information technologies in the perspective of industry 4.0: Opportunities and challenges," *Comput. Sci. Rev.*, vol. 30, pp. 1–30, Nov. 2018, doi: 10.1016/j.cosrev.2018.08.001.
[90] A. Verma, P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain for industry 5.0: Vision, opportunities, key enablers, and future directions," *IEEE Access*, vol. 10, pp. 69160–69199, 2022, doi: 10.1109/ACCESS.2022.3186892.
[91] *Repsol—Energy and Innovation Industry 5.0*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.repsol.com/en/energy-and-innovation/technology-lab/industry/index.cshtml
[92] W. Hong, Z. H. Jiang, C. Yu, D. Hou, H. Wang, C. Guo, Y. L. H. Kuai, Y. Yu, Z. Jiang, Z. Chen, J. Chen, Z. Yu, J. Zhai, N. Zhang, L. Tian, F. Wu, G. Yang, Z.-C. Hao, and J. Y. Zhou, "The role of millimeter-wave technologies in 5G/6G wireless communications," *IEEE J. Microw.*, vol. 1, no. 1, pp. 101–122, Jan. 2021, doi: 10.1109/JMW.2020.3035541.
[93] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022, doi: 10.1109/ACCESS.2022.3140595.
[94] K. Y. Yap, H. H. Chin, and J. J. Klemeš, "Future outlook on 6G technology for renewable energy sources (RES)," *Renew. Sustain. Energy Rev.*, vol. 167, Oct. 2022, Art. no. 112722, doi: 10.1016/j.rser.2022.112722.
[95] J. A. S. Aranda, R. dos Santos Costa, V. W. de Vargas, P. R. da Silva Pereira, J. L. V. Barbosa, and M. P. Vianna, "Context-aware edge computing and Internet of Things in smart grids: A systematic mapping study," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107826, doi: 10.1016/j.compeleceng.2022.107826.
[96] J. Li, C. Gu, Y. Xiang, and F. Li, "Edge-cloud computing systems for smart grid: State-of-the-art, architecture, and applications," *J. Mod. Power Syst. Clean Energy*, vol. 10, no. 4, pp. 805–817, 2022, doi: 10.35833/MPCE.2021.000161.
[97] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020, doi: 10.1109/TSMC.2019.2896323.
[98] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019, doi: 10.1109/JIOT.2019.2904303.
[99] J. Wang, L. Wu, K.-K.-R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020, doi: 10.1109/TII.2019.2936278.
[100] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2637–2670, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2908266.
[101] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K. K. R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Comput. Secur.*, vol. 85, pp. 288–299, Aug. 2019, doi: 10.1016/j.cose.2019.05.006.
[102] K. Kaur, G. Kaddoum, and S. Zeadally, "Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5178–5189, Aug. 2021, doi: 10.1109/TITS.2021.3068092.
[103] Y. Wang, X. Kang, and Z. Chen, "A survey of digital twin techniques in smart manufacturing and management of energy applications," *Green Energy Intell. Transp.*, vol. 2022, Jun. 2022, Art. no. 100014, doi: 10.1016/j.geits.2022.100014.
[104] N. Bazmohammadi, A. Madary, J. C. Vasquez, H. B. Mohammadi, B. Khan, Y. Wu, and J. M. Guerrero, "Microgrid digital twins: Concepts, applications, and future trends," *IEEE Access*, vol. 10, pp. 2284–2302, 2022, doi: 10.1109/ACCESS.2021.3138990.
[105] J. Lopez, J. E. Rubio, and C. Alcaraz, "Digital twins for intelligent authorization in the B5G-enabled smart grid," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 48–55, Apr. 2021, doi: 10.1109/MWC.001.2000336.
[106] L. Johnson, A. Isam, N. Gogerty, and J. Zitoli. (2015). *SolarCoin Whitepaper: Connecting the Blockchain to the Sun to Save the Planet*. Accessed: Oct. 3, 2022. [Online]. Available: https://ssrn.com/abstract=2702639
[107] *CyClean Coin Whitepaper*. Accessed: Oct. 3, 2022. [Online]. Available: https://medium.com/cyclean-coin/cycleans-white-paper-what-to-expect-dbf2ad1efac5
[108] M. Mihaylov, I. Razo-Zapata, and A. Nowé, "NRGcoin—A Blockchain-based reward mechanism for both production and consumption of renewable energy," in *Transforming Climate Finance and Green Investment With Blockchains*. Cambridge, MA, USA: Academic, 2018, ch. 9, pp. 111–131, doi:, 10.1016/B978-0-12-814447-3.00009-4.
[109] *Charg Coin Whitepaper*. Accessed: Oct. 3, 2022. [Online]. Available: https://golden.com/wiki/Charg_Coin-VKEPD44
[110] S. Lacey. (2018). *Energy Blockchain Startups Raised $324 Million in the Last Year. Where's the Money Going?*. Greentech Media. Accessed: Oct. 3, 2022. [Online]. Available: https://www.greentechmedia.com/articles/read/energy-blockchain-startups-raised-324-million-since-2017
[111] *De Ceuvel*. Accessed: Oct. 3, 2022. [Online]. Available: https://deceuvel.nl/en/
[112] J. Mens, E. van Bueren, R. Vrijhoef, and E. Heurkens, "A typology of social entrepreneurs in bottom-up urban development," *Cities*, vol. 110, Mar. 2021, Art. no. 103066, doi: 10.1016/j.cities.2020.103066.
[113] *Jouliette Token*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.jouliette.net/
[114] *MultiChain—Enterprise Blockchain Platform*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.multichain.com/
[115] J. Swens and L. Diestelmeier, "Developing a legal framework for energy communities beyond energy law," *Energy Communities*, vol. 2021, pp. 59–71, Jan. 2022, doi: 10.1016/B978-0-323-91135-1.00019-5.
[116] K. Wust and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 45–54, doi: 10.1109/CVCBT.2018.00011.
[117] T. Koens and E. Poll, "What blockchain alternative do you need?" in *Proc. Int. Workshop Cryptocurrencies Blockchain Technol.*, Barcelona, Spain, Sep. 2018, pp. 113–129, doi: 10.1007/978-3-030-00305-0_9.
[118] *Greeneum*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.greeneum.net/
[119] *Drift*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.drifttrader.com/
[120] *Pylon*. Accessed: Oct. 3, 2022. [Online]. Available: https://pylon.network/
[121] *Electrify Synergy*. Accessed: Oct. 3, 2022. [Online]. Available: https://electrify.asia/synergy/
[122] *Power Ledger*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.powerledger.io/platform
[123] *Electron RecorDER*. Accessed: Oct. 3, 2022. [Online]. Available: https://electron.net/projects/project-recorder-uk/
[124] *SunContract*. Accessed: Oct. 3, 2022. [Online]. Available: https://suncontract.org/about-suncontract-blockchain-project/
[125] *Integral Platform for Climate Initiatives*. Accessed: Oct. 3, 2022. [Online]. Available: https://ipci.io/
[126] *Omega Grid*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.omegagrid.com/
[127] *SunChain*. Accessed: Oct. 3, 2022. [Online]. Available: https://www.sunchain.fr/
[128] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020, doi: 10.1109/ACCESS.2020.2967218.
[129] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, vol. 7, pp. 77894–77904, 2019, doi: 10.1109/ACCESS.2019.2921624.
[130] Y. Huang, Y. Bian, R. Li, J. L. Zhao, and P. Shi, "Smart contract security: A software lifecycle perspective," *IEEE Access*, vol. 7, pp. 150184–150202, 2019, doi: 10.1109/ACCESS.2019.2946988.
[131] J. J. Kearney and C. A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks," *Array*, vol. 10, Jul. 2021, Art. no. 100065, doi: 10.1016/j.array.2021.100065.
[132] Y. Pang, "A new consensus protocol for blockchain interoperability architecture," *IEEE Access*, vol. 8, pp. 153719–153730, 2020, doi: 10.1109/ACCESS.2020.3017549.

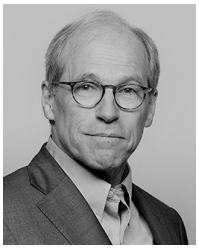
[133] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on blockchain: A game theoretical perspective," *IEEE Access*, vol. 7, pp. 47615–47643, 2019, doi: 10.1109/ACCESS.2019.2909924.

[134] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Protective Relay Eng. (CPRE)*, Apr. 2017, pp. 1–8, doi: 10.1109/CPRE.2017.8090056.

RAIFA AKKAOUI received the M.Eng. degree in information and communication technologies from the National Institute of Posts and Telecommunications, Rabat, Morocco, in 2016, and the Ph.D. degree in information and communication engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2020. Since 2021, she has been a Postdoctoral Researcher at TU Delft, The Netherlands. Her research interests include blockchain, edge computing, the Internet of Things, cyber security, smart grids, and game theory.

ALEXANDRU STEFANOV received the M.Sc. degree from the Politehnica University of Bucharest, Romania, in 2011, and the Ph.D. degree from University College Dublin, Ireland, in 2015. He is currently an Assistant Professor in intelligent electrical power grids at TU Delft, The Netherlands. He is also the Scientific Director of the Control Room with the Future Technology Centre, Department of Electrical Sustainable Energy. His research interests include cyber security for power grids, resilience of cyber-physical systems, and next generation grid operation. He holds the professional title of Chartered Engineer from Engineers Ireland.

PETER PALENSKY (Senior Member, IEEE) received the M.Sc. degree in electrical engineering and the Ph.D. and Habilitation degrees from the Vienna University of Technology, Austria, in 1997, 2001, and 2015, respectively. He co-founded Envidatec, a German startup on energy management and analytics. In 2008, he joined the Lawrence Berkeley National Laboratory, Berkeley, CA, USA, as a Researcher, and the University of Pretoria, South Africa. In 2009, he became appointed as the Head of the Business Unit, Austrian Institute of Technology (AIT) in sustainable building technologies, where he was the first Principal Scientist of Complex Energy Systems. In 2014, he was appointed as a Full Professor in intelligent electric power grids with TU Delft, The Netherlands. He is active in international committees, such as ISO or CEN. His research interests include energy automation networks, smart grids, and modeling intelligent energy systems. He also serves as an IEEE IES AdCom Member-at-Large in various functions for IEEE. He is the past Editor-in-Chief of *IEEE Industrial Electronics Magazine* and an associate editor of several other IEEE publications and regularly organizes IEEE conferences.



DICK H. J. EPEMA was a Full Professor in distributed systems with the Delft University of Technology, The Netherlands. He has authored more than 140 scientific papers and has been on numerous program committees in grids, clouds, and P2P computing. His research interests include the areas of resource management in distributed systems and in blockchain technology. He was an Associate Editor of the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS and the IEEE TRANSACTIONS ON CLOUD COMPUTING. He was the General Co-Chair of EuroPar 2009 and IEEE P2P 2010 and he was the General Chair of HPDC 2012 and CCGrid 2013. He was the Program Committee Co-Chair of HPDC 2013.