Received October 16, 2020, accepted November 5, 2020, date of publication November 9, 2020, date of current version November 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3036994

Blockchain as Key Enabling Technology for Future Electric Energy Exchange: A Vision

ALVISE BAGGIO, (Member, IEEE), AND FRANCESCO GRIMACCIA, (Senior Member, IEEE)
Department of Energy, Politecnico di Milano, 20133 Milan, Italy

Corresponding author: Alvise Baggio (alvise.baggio@mail.polimi.it)

This work was supported by ABB Solar Smart Power Laboratories.

ABSTRACT Our energy scenario is nowadays shaped by progressive electrification of energy final use. In this context, electricity networks are seeing a growing multitude of distributed assets entering from the edges of the grid and acquiring new ICT capabilities that were limited before to a restricted number of major players. Particularly, assets like Photovoltaic Inverter (PvI), Electric Vehicle (EV) chargers, wind turbines controllers, programmable loads, storage systems, and other Distributed Energy Resources (DER) are now able to *communicate* through different technologies and make *conscious choices* under human-decisions or even independently. This is leading to a decentralization of the system's view by increasing single actor independence. Notwithstanding, a problem arises when current centrally-managed electricity networks struggle to coordinate massive amounts of new figures and adapt to this new decentralized paradigm. Therefore, a decentralized coordination-and-control framework will ensure better integration of DERs and new figures as prosumers, while allowing higher exploitation of their potential compared to centrally managed systems. This article seeks in Blockchains the enabling technology for designing and supporting such a grid infrastructure. It develops a first framework to address this need by envisioning a grid-system based on the direct participation of nowadays-used embedded-energy-devices within a decentralized platform hosting specific coordination procedures. The platform was developed in an experimental research campaign performed at ABB Laboratories basing on embedded-devices currently designed as control-connectivity boards for *smart-inverters*. Therefore this article introduces the background theory and reasons behind this proposed system. The intent here is not to give all the specific details of the implementation, but introduce the supporting reason, high-level design, and required characteristic of the Blockchain-based platform for coordinating grid operations. Blockchain technology is seen here as the appropriate technology to enable the realization of a multi-actor energy-management system and enable distributed coordination in power grids.

INDEX TERMS Blockchain, distributed ledger technology, distributed energy resources, embedded software, smart inverters, digital energy.

I. INTRODUCTION

Nowadays's energy infrastructure is probably the most complex engineering machine ever built. It is made of millions of strongly heterogeneous devices and players electrically interconnected and seamlessly transacting. The roles of centralized operators and regulators are now mainly to secure the correct distribution of energy from production to distribution. Nevertheless, the situation is actively changing. The actors' number in the grid is increasing abruptly, and their roles are overlapping [1]. Consumers become able to produce energy through technology like photovoltaic cells or small wind turbines. Parallelly new loads profiles, like electric vehicles or batteries, could represent vital strategic assets for managing the grid [2]. However, system coordination is nowadays mainly centrally managed, and lower-levels are virtually invisible from a control perspective. Centralized control naturally finds it difficult to scale to a large number of scattered actors generating high-frequency transactions [3]. Therefore, Distributed Energy Resources are cut-off from the possibility of participating in electric infrastructure directly, while actors like prosumers are disincentivized of cooperating more tightly with the grid due to low financial returns. This is not only negative for them, but it prevents the

The associate editor coordinating the review of this manuscript and approving it for publication was Junjie Hu.

entire system from employing their potential [4], for example, through the provision of ancillary services like reserves [5]. A system able to better scale to the distributed nature of the actual electric grid will be capable of better integrating DER, offer new economic advantages, foster "green" electricity production, and ensure a more resilient infrastructure. Additionally, the transaction cost embedded with a centralized management method, even if applied to an innovative coordination method, is one of the causes at the root of inefficient economic outcomes [6] and impeding the transition to more efficient framework [5]. Therefore, this research, driven by this idea, seeks in Distributed Ledger Technologies (DLT), and in particular, Blockchain, the enabling tool to build a platform that, on top of the current electric grid, unlocks innovative models of grid scheduling and coordination. In particular this article introduces the concept by describing the main idea, aiming at mapping the technology requirements to the power grid characteristics. This analysis is strengthened by an electric grid that, under current digitalization [7], sees the presence of an increasing number of communication-capable embedded devices [8] such as inverters or Electric Vehicle (EV) chargers, able to exchange information and send data [9] hence able to open innovative way of operating the electric system.

Fundamentally, the authors conceive a novel platform able to support future electric grid coordination activities by allowing new grid-tied actors to participate directly in grid's operations, offering/buying energy products and services independently based on their preferences. This article is structured as follows: the following section describes Blockchain fundamentals starting from the technology's basic concepts towards network nodes characteristics and smart contracts definition; Section III then relates those concepts to the energy sector and the power grid envisioned applications. It finishes with a description of current works and literature that similarly to this one see the possibility of implementing Blockchain-based energy exchange system for coordination of production and consumption. Section IV proposes a multi-layer model based on current and evolving digitalization of the energy sector to segment how the platform's system is divided. It then discusses Blockchain implementation and related advantages, and it describes the proposed framework for comprehending the platform design. Based on this some of the principal and required characteristics, relevant for the power grid application, are discussed. Moreover, details and structure of the implementation are introduced and described, even if they will be deeply discussed in subsequent works specifically devoted to technical characteristics and performances. Finally the authors draw main conclusion in section V, underlying possible short terms evolution, potential implementations and future R&D open fields.

II. BLOCKCHAIN TECHNOLOGY FEATURES

This section is dedicated to introducing the technology and concept of Blockchains potential. The intention is not to provide a complete theoretical background on a topic with its roots in many different areas of computer science discipline. Differently, the intent is to provide the reader with the basic necessary information before discussing the rest of the paper. Additionally, the authors want to share a vision on the nature and characteristics of this technology.

A. BLOCKCHAIN AS A DISTRIBUTED COMPUTER SYSTEM

Blockchains are part of the macro-area of Distributed Computer System (DCS). DCSs are a collection of hardware-software components connected through a communication network and integrated with different levels of interdependence and logic [10]. These distributed systems could be defined as the sum of physical-virtual nodes connected and communicating through a shared physical medium and sharing software logic for coordination purposes. Accordingly, a shared memory multiprocessor, i.e., a computer system, does not wholly differ from a DCS; the main differences could be found under two aspects, namely a quantitative and qualitative one. Brightly, the quantitative differentiation stems from a more extensive area sparseness and, consequently, a less performing communication interfacing, bringing problems like latency, delays, and messages losing, eventually leading to a-synchronicity [11]. Nonetheless, the fundamental differentiation is the qualitative one - in a distributed system, the subsystems, have different priorities, specialization, and more substantial independence, still, once interconnected through a shared network, they coordinate in order to share resources consistently and present a single vision of the system [10]. Differently, a single computer system satisfies its own needs already as a single independent unit. Hence, the complexity embedded in DCS derives from this characteristic of coordination of differentiated nodes' needs while caring for the whole system's state. Parallelisms seems standing between DCS and the nascent distributed digital electric grid.

A Blockchain network in its whole is a DCS - a series of different machines working as a single unit. Indeed, in its core features, **i**) it is a network of replicated state machine nodes, **ii**) interconnected through a communication infrastructure, **iii**) maintaining and updating consistently yet independently the system's state **iv**) affected by transaction sent by other network's nodes. These nodes are identified thanks to their unique identity; therefore, they are distinguished as independent entities. The goal of the system is to maintain and update the system's state represented by a storage organized as a series of chained block: "the Block-Chain" [12]. The motivating reason behind this particular structure is supported by the easiness in verifying its consistency [12], immediately detect malicious tampering [13], possibly ensure higher throughput [14] and, in some implementations, give a simple metric for selecting most updated states[1] [12]. The advantage is that this collective and consistent coordination is achieved without third party intermediation but independently by participating nodes.

[1] Longest chain principle.

The blocks data structure gives the name to the technology itself. Nevertheless, Blockchain is used interchangeably to address the specific storage system and the more general network of nodes exploiting it. More precisely, Blockchain is part of a family of technology called Distributed Ledger Technology (DLT) where the main essential difference is the underlying used data structure, and therefore how the network is organized in exploiting it. Example of DLT not being Blockchain are Tangles[2] [15] that will not be deepened further.

Instead of a monolithic solution, distributed systems could be seen as made of different layers [10]. The different components organization and structure are characteristic of different solutions, as in Tangles and Blockchains' case, where the storage system is organized differently. Clearly, the decomposition could take different levels of detail, but for this work and DLT applications, four primary levels are essential. This levels are the essential components embedded in each network's node to enable it to join and participate in the Blockchain system itself for a specific application. The layered framework is derived from [16] but extended and detailed as follows:

- *Networking*
  It is the component tasked of propagating information and messages between nodes [10]. It is based on specified infrastructures and protocols. It actively contributes in making the distributed system works, starting from its very own nature of an interconnected network of nodes. Within the Blockchain environment, the Internet protocol always provide the main networking component [17].
- *Identity*
  This layer distinguishes unequivocally each participating identity [18]. This does not necessarily mean that there is a direct connection with physical identity, but that, at least, the different nodes are uniquely recognized. Over this, there could be a connection with the physical world. Hence, the solution could then be entirely anonymous, pseudonymous, or require certification. These last characteristics are the base for defining two different types of Blockchain implementations, i.e., permissionless or permissioned [17].
- *Consensus*
  For a distributed system to be useful, it must be consistent (each participating nodes must see a single equal state throughout the network) - this layer is the one tasked of this purpose. The consensus layer is tasked with making the nodes agree on a single ordered-series of consistent updates [19]. Such a consistent series of events ensures that the network appears the same to the external multiple user interacting with it [20]. In general, Blockchains' consensus mechanisms ensure that the network's nodes receive a single and equal set of transactions to be later verified in their correctness and compliance to rules. Indeed, consensus mechanisms are not used to verify the transactions modifying the network state, but they only ensure that the network's nodes receive the same ordered set of update transactions [21] to be later checked.
- *Application*
  Built on top of the consensus layer, the application layer makes the network usable in a specific circumstance. This layer is the most apparent to the external user. Indeed, it represents the business logic of the network built on top of the other components that are more transparent. Looking at the system as a whole, and using the Finite State Machine (FSM) model described by Schneider, Liskov, Alford, et al. [22], the application layer is the state transition function that determines how input-transactions affect the current state and generate outputs. The network is physically made of replicated FSMs that, through communication, receives the same set of update-transactions thanks to a consensus mechanism. Then the application layer applies a series of rules recorded as scripts to verify the compliance of the received transaction, check their applicability in the actual system state, and eventually update the state.
- *Storage*
  Ultimately network's nodes interact with a system state through the logic embedded in the application layer. The state is a vital feature of the distributed system [22]. Nodes apply the previously mentioned state transition function using incoming transactions as input; these affect the current state of the system and generate an updated version of it. Hence, the current state itself is where inputs take action. Such a state is recorded in the form of storage and organized using different strategies within different DCS.

This segmentation helps to understand that the different components could be located only on some predetermined nodes, for example, consensus could be reached and communicated only by a subset of node offering it as a service to the network [14]. In contrast, other nodes may only be used to host business logic and the underlying affected storage that is updated thanks to received transactions. Only the networking and identity layer have to be part of one node's essential functionalities to participate in the network. Indeed the most basic participation scheme is the one of a node sending signed transactions in order to interact with the system' state. This imply that this node do not necessary participate in the system's maintenance but it exploits the other network's nodes for processing its transactions. Necessarily, especially for allowing mas adoption, the DCS internal structure should be transparent and not oblige all users to maintain complex *infrastructural-nodes*. Eventually, the network, even if composed by multiple maintainers, should mimic the behavior of a single co-located machine [10] no matter which *infrastructural-nodes* is queried or used. It is clear that in such a way by exploiting an external service for sending

[2]This particular technology uses directed acyclic graph (DAC) as underlying data structure for transactions recording, rather than single chain of blocks (IOTA is an exemplifying implementation).

transaction or querying information trust is shifted upon the service provider. Nevertheless the advantage is that there is no a single provider but a multitude of equally sostituible provider therefore decreasing the reliance on a single centralized actor.

All the components are built in order to ensure consistency, equality, and verifiability of transactions throughout a network of physically separated nodes. The network-layer allows communication, the identity-layer permits accountability of actions and distinguishes nodes, the consensus-layer ensures that the same set of transactions is consistently applied in an equal-sequential-order on all nodes, the application-layer allows verifying those transactions and updates the state under a single logic shared throughout the network, and eventually, the storage represents the state itself that is the main object of the entire system interactions. DLTs allows us to represent and interact in a decentralized yet consistent way with a state shared over a multi-nodes system as it was withheld in a single machine. This method potentially permits to process transactions within a trustless multi-party network avoiding the need for centralized third-party intermediation.

B. BLOCKCHAIN FUNDAMENTALS

As anticipated, the block-chain is only the chained series of blocks used to store transactions and, ultimately, data [12]. All the components of consensus, cryptography, communication, and coded logic are the structure surrounding it and handling its evolution; nevertheless, when we talk about Blockchains, we mainly talk of the artifact and the network in its entirety.

One of the reasons behind the usage of blocks is not a casual one: grouping transactions, instead of care for single messages is a well-known technique to improves the throughput of the consensus protocol [14], lightening the work-load processed by the algorithm. Rather than repeating it for every single transaction, consensus is reached on a group of them. This is because it is the object of the consensus, rather than its dimension, that requires times for ensuring agreement. Nevertheless, block's dimension in terms of grouped transactions is again a compromise that requires trade-offs. If it is true that batching more transactions improves consensus throughput up to a certain limit, the more transactions are processed, the more effort is required to the application layer in applying successive state transition functions and validating the inputs.

The fundamental blocks structure is the one showed in Figure 1.

A block is mainly made of three macro elements, a header, a blob of data, and some metadata. The "history" of the Blockchain starts with block B_0 that represents the state S_0 of the state machine framework used to model it [22]. This is hardcoded in all the nodes of the Blockchain network to ensure that, starting from it, a consistent state could be generated. At time t and state S_0, network's nodes start sending transactions Tx_i, to be embedded in block B_1, for updating the current state, asking to modify, for example, assets related to their identity. This identity is a unique address related to the node public key. Public key are cryptographic artifacts used to uniquely identify digital entities and for perform secure operation within digital application. Indeed to certify the correspondence address-identity, a secure mathematical relation is inserted in the message. This is a digital signature that could be generated only thanks to a component secured by the node and kept secret, i.e., its private key. Receivers nodes could verify this signature using the visible public key of the incoming transaction, hence checking the sender identity's veracity. Such a usage of public/private key is known as asymmetric cryptography.

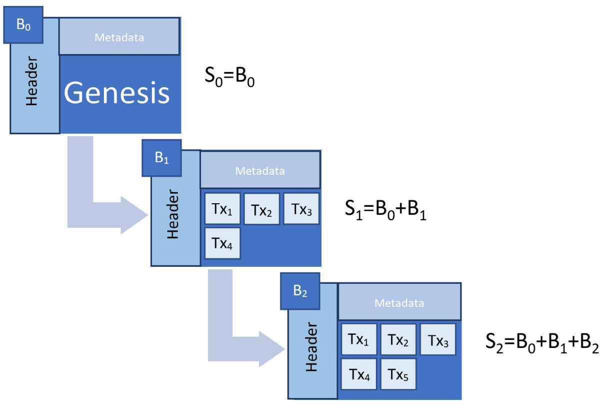

FIGURE 1. Basic Blockchain data structure.

The messages/transactions are usually broadcast to multiple nodes in different manners. Then network's maintainers collect a series of messages and firstly apply to each of them a checking function $c_i = c_i(Tx_i^t, S, Tx_{y \neq i})$. This ensures the validity of the transaction on its own, in the current state of the system, and against other transaction collected by the validator on the same block. Exemplifying it with a Bitcoin-Blockchain metaphor (digital token exchange): the signature correctness, if the sender possess enough money for the transaction issued, and if it did not send other transactions for exchanging the same token.[3]

Multiple transactions are then inserted in a single blob of ordered data under specific mechanisms (the block). A digital summary of the block's information is calculated and inserted in a header of it. This digital summary is called a hash and is calculated using a pseudorandom function called hash function, which property is to generate a unique fingerprint of the data that pass through it. The header also contains a block index, i.e., its number in the chain and the hash of the previous block,[4] in this case, B_0. In this way, the immutable chaining is obtained; indeed, if only a bit in the previous block is changed, its hash is consequently modified, causing a recursive effect on all subsequent blocks. Moreover, it is immediate to detect chain versions containing different blocks. This makes easy to detect inconsistency with

[3] Avoiding double-spending within the same batch of transactions.

[4] In the case of B_0, there is not any previous block; it is therefore an hardcoded value.

the rest of the chains detained by the network's nodes. The header could also contain other elements used for the specific Blockchain implementation and that have specific features, such as timestamps, or nonces in the case of the Bitcoin-like consensus methods. When block B_1 is generated, a series of metadata could be added, such as the creator signature. Then the whole block is broadcasted to the entire network of maintainers under the specific rule of consensus and accepted only if the other nodes verify that c_i for each transaction results true[5] or if a selected set of nodes previously certified this condition [14]. This procedure brings to the consistent replication of B_1 to the entire network. The iteration begins again starting from block B_1. Now the state does not coincides with B_1 but rather, $S_1 = B_0 + B_1$. Once B_2 will be accepted $S_2 = B_0 + B_1 + B_2$. Essentially, the state evolves as a discrete series of steps defined by accepted blocks. As a general rule:

$$S_n = \sum_{j=1}^{n} B_j \tag{1}$$

As it can be noticed, the application layer only comes in action for the checking function, but it does not modify anything permanently. Indeed, as explained before, the application layer is only an overlying structure on top of the logically separated consensus layer. The transactions on the blocks are completely transparent to the Blockchain itself, they gain meanings only in front of the application layer's business logic, i.e., what are called *smart contracts*.[6] Therefore, the application layer, considering the current system's state, performs its action over it. Hence, for each transaction, the update is defined by $S_n = STF(Tx_i; S_{n-1})$, i.e., a state transition function using as input the transaction and the current state. From a higher point of view, the state is modified concurrently by all the transactions inside a block:

$$\begin{aligned} S_n &= STF\left(\sum_{B_n} Tx_i \;\; ; \;\; S_{n-1}\right) \\ &= STF\left(\sum_{B_n} Tx_i \;\; ; \;\; \sum_{j=1}^{n-1} B_j\right) \end{aligned} \tag{2}$$

The persistent state representation results permanently modified every time a transaction is successfully added to the ledger. A transaction essentially acts as a database transaction modifying, updating, or creating values within the particular storage system.

C. PERMISSIONLESS AND PERMISSIONED BLOCKCHAINS

One of the fundamental differences characterizing this technology is how identities are treated inside the distributed system. As anticipated there are currently and traditionally two main implementation within the Blockchain and DLT environment **i**) pseudonymous based (permissionless), **ii**) authorized and recognition based (permissioned). This strongly impacts all the platform, since in the first case, differently from the second one, everyone is free to join and participate directly not only by sending transactions but also by maintaining the system status. Differently, in case ii), the nodes must gain an identity to participate in the network, making the protocol less open. Moreover, since identities are recognized, there is the possibility of entitling them of specialized roles, prominence, or attributes over all the Blockchain resources and components. For example, some nodes could be entitled to hold the distributed ledger and update it under received transactions. Therefore the governance of the system is also eventually affected. Table 1 provides a representation of the derived categories of Blockchain.

TABLE 1. Permissionless and Permissioned Blockchains Comparison.

	Permissionless	Permissioned
Identity	Pseudonymous	Certified
Participation	Freely open	Authorized
Governance	Completely unanimous	Restricted / Divided

By implementing an infrastructure for certifying and authorizing nodes in joining the network, a permissioned implementation open the possibility of using external regulating governance (e.g. Regulatory Authority for Energy) and recognize tasks within the system more finely. Permissioned models present an element of centralization that, nevertheless, could be used for making the platform more efficient [13], still allowing high levels of freedom to nodes' activities by smartly design the roles subdivision. It is clear that the identity layer gains a crucial role in a permissioned implementation, and its feature could be exploited within the consensus and the application layer.

As a corollary of the aforementioned possible implementations, an essential consideration regarding consensus should be made. Indeed if we employ a one-vote-one-node consensus principle[7] in a permissionless Blockchain, the result could be deleterious. Indeed, since here identities are pseudonymous and not related to any physical single-identity, a user could employ multiples nodes and freely join the network with all of them. Therefore, a malicious user could flood the network with its node and ultimately gain the majority over the consensus, simply outvoting the honest nodes with a "dirty trick" technically called a Sybil attack [23, p. 251]. Hence, for relating voting power more strongly to single physical identity, scarce resources, as computing power, could be used to limit accumulable dominance within the network. Even if in this case the risk is power concentration with resource concentration [24].

Nevertheless, such bonding with scarce physical resources, or resources of other nature, as economic value kept inside the Blockchain status, could be seen as a limitation. Therefore,

[5] Some implementation rather than atomically discarding the whole block if a single transaction do not result correct have mechanism to delete only the effects of the specific transaction.

[6] This essentially are rules and logic recorded as computer programs that process incoming transactions.

[7] A framework in which each node cast a vote for deciding which transactions will be used for update the system and consensus is reached thanks to a majority metrics.

permissioned application could be used to enable safe one-vote-one-node mechanism by restricting consensus between a set of recognized entities avoiding the possibility of Sybil attack since the joining process is restricted to authorization. Moreover, it must be remembered that Blockchain is a layered infrastructure. Therefore, roles division could be smartly applied to allocate critical tasks to more centralized minority without strongly impacting the decentralization and fairness of the system, but ensuring more efficient services.

D. CONSENSUS MECHANISM

Given this discussion of identities, it will be straightforward to speak about consensus. This concerns the problem of coordinating a series of distributed processes in converging to a single decision regarding the system state and its update. Formally, the problem can be modeled in the following way, as reported in [25]. Given a set of distributed processes, consensus is reached if the following conditions are satisfied: **i**) *Agreement* - All non-faulty processes must agree on the same value. **ii**) *Validity* - If all the non-faulty processes have the same initial value (as a genesis block $S_0 = B_0$ or the previous version of the Blockchain S_{n-1}), then the agreed-upon value (Sn) by all the non-faulty processes must be that same value. **iii**) *Termination* - Each non-faulty process must eventually decide on a value.

The above conditions are trivial to satisfy in a fault-free system working synchronously [25]. Nevertheless, the consensus layer is designed to allow a series of distributed nodes to agree on the system's state in a failure-prone (crashes), Byzantine (malicious nodes),[8] asynchronous networks of distributed concurrent processes. In these conditions, consensus is less trivial to guarantee. Therefore, in general to overpass complexity, problem relaxation is applied.

Indeed, if in [26] consensus impossibility is proven with a fully deterministic algorithm within a completely asynchronous system, solutions are feasible under two main conditions [26]: **i**) use a partially synchronous network model; **ii**) use a non-deterministic (probabilistic) guarantee model.

In general, consensus algorithms make use of one of these two approaches. The first is used in what are known as *Classical consensus algorithms* that are based on voting. The second is instead one of the most significant innovations brought by Blockchain technology, and by its mysterious inventor Satoshi Nakamoto, hence, this new algorithms group is known as *Nakamoto Consensus*.

As explained in the previous section, a vote-based consensus mechanism cannot be implemented in a permissionless system due to Sybil attacks. Therefore, consensus is reached in a deterministic way by a group of recognized and certified participating nodes. They reach an agreement on the order, number, and which transactions to add to the next block. This agreement is reached thanks to message passing between known identity that then converge to a single solution. Digital signatures are therefore used for ensuring provenience and accountability of messages. In this way, starting from a consistent, equal state (B_0), the network is updated by a sequential order of equal transactions agreed upon by consensus participating nodes. Due to its nature, these mechanisms do not suffer from high computational-resources needs, but it general suffer from scalability issues regarding consensus participating nodes. Indeed, being the solution built upon message passing, as the consensus participating nodes increase, the number of message increase proportionally reaching a limit due to high delays and performances. The advantage of these methods is that the chain of blocks proceeds in a sequential order of equal-for-all blocks since at each step (sequence of accepted blocks) a single consistent update is generated.

In the case of *Nakamoto Consensus*, instead, we do not have voting entities. A block proposer is elected thanks to the solution of a computation puzzle or in a probabilistic relation to some resources put as stakes. It then proposes a single update eventually spread throughout all the network thanks to communication. Receivers then easily verify the veracity of the solution that entitles the proposer to generate a block. The objective of such method is to tide digital entities to scarce resources like computational power[9] or value in the form of a deposit. In this way, it is possible to avoid a system where a malicious entity could outvote the network by inexpensively owning multiple digital entities. The computational-intensive problem solution for proposing a block is the method introduced in Bitcoin and known as Proof of Work (PoW). Here the logic stands on the fact that it is difficult for a malicious actor to accumulate a computational power in terms of hardware and energy consumption higher than the rest of the network. The higher the difficulty of the problem, the higher the security against attacks [12] (a single entity is less likely to be able to compete with the majority of the network). Nevertheless, in this way also the time spent on solving it and the energy consumed increase. Bitcoin PoW, therefore, is a highly secure mechanism as demonstrated throughout these years, but first, it is characterized by long block confirmation time (around 10 min) that could not be suited for a high-frequency transaction system as a platform for managing energy-exchanges between grid-tied devices. Indeed, given a fixed block dimension, state-update proposal-transaction accumulate, waiting to be confirmed. Secondly, energy consumption is a matter of weakness, especially within an energy-related application, and in the case of Bitcoin, PoW, a single transaction requires 431KWh [17] that is quite high. Hence, decreasing computation difficulty could be a solution that nevertheless sacrifices security. Another issue is that centralization is motivated by the possibility of owning cheaper hardware or living in a country with inexpensive electricity. Therefore, other mechanisms for election was introduced. These types of consensus mechanisms rely

[8]Consensus algorithm could be Crash Fault Tolerant (CFT) or Byzantine Fault Tolerant (BFT) depending on the nature of the network and its needs a detailed description is out of the scope of this article.

[9]To solve the mathematical puzzle.

on the internal economy of the platform itself. In PoW, the opportunity cost, for the probability of proposing a block is external to the platform. Indeed nodes invest in electricity and hardware for solving the puzzle. Differently, in Proof of Stake (PoS) consensus, the likeliness of proposing is internal to the platform itself and is measured in a stake quantity owned by the node. These algorithms promise to solve the time and energy issue; nevertheless, the problem here is the necessity of deploying a Blockchain system that must rely on a form of internal value represented by a cryptocurrency that could be something not of interest for the application.

Given the specific election mechanism of *Nakamoto Consensus* algorithms and its non-deterministic nature, and considering network sparsity and distribution, network's partitions could happen when two different nodes entitle to become proposers in a relatively equal moment. A fork is thus generated, i.e., two network portions having different transactions log versions. Nevertheless, the specific Blockchain protocol is designed to resolve such issue within the next generated blocks and thus realigning all the network to a single version. Such a situation could be a problem when the specific application require that in all moment all the maintaining network nodes must be constantly aligned to a single version without risks of partial desynchronization. A negative outcome example is the case in which for the same bidding zone two different ancillary services schedules will be generated dispatching different plants.

Hence, the choice regarding the consensus mechanism is relevant for the application of this technology, indeed it affects the characteristic of the implementation both qualitatively and quantitatively, eventually influencing the system behaviour and design. It is therefore necessary to analyze its attributes and how positively exploit them.

E. NETWORKS NODES AND SMART CONTRACTS

Within a Blockchain network, each node is potentially allowed (in a permissioned implementation under specific access conditions) to embed the fundamentals functionalities for constituting an integral part of the system. These are maintaining the ledger (storage and data-structure), verifying and processing transactions, participating in the consensus mechanism, and updating the state. If all participating nodes embed these functionalities, the network will be a set of completely independent entities safely interacting in a trustless environment. All of them will contribute to sustain the network making it highly secure and decentralized. Indeed, in this case all have capabilities to self-verify and individually check the veracity of the interactions by actively participating in the distributed system protocol without the need to exploit other nodes. Nevertheless, not all nodes are obliged to participate in maintaining the network infrastructure and form the system infrastructural backbone. Some could avoid maintaining the ledger, holding the application layer for modifying it, and participating in the consensus mechanism for block generation, but still be allowed to send transactions. Indeed, ''lighter'' nodes solely participate by interfacing with the core network by sending transactions to be processed and querying relevant information. Such simpler nodes rely on the communication with the main nodes constituting and maintaining the core infrastructural network. Brightly, in this way, trust is shifted upon these infrastructural nodes that perform the main Blockchain functions. Therefore, the differentiation from a fully centralized and individually controlled server stands in the thoughtful design and distribution, over a significant number of non-singularly owned nodes, of core protocol-tasks. Indeed, as an example, a Bitcoin Blockchain network formed solely by lightweight nodes or even simple wallets (nodes with none or limited infrastructural capabilities)[10] will not work, and even one with a non-sufficient number of full nodes will perish under non-security and easiness of performing malicious attack [27]; nonetheless, the usage of lightweight nodes will allow certain users not to carry computational intensive tasks or occupy memory and storage while still interacting by sending and querying transactions information [12]. In this discussion we will distinguish between *transactive-nodes* and *infrastructural-nodes*.

A fully-decentralized solution will require all participating entities controlling a full *infrastructural-node*, i.e., a node maintaining the fundamental functionalities for the system to work. In this way, all participating nodes will represent a fundamental verification point for consistency and veracity of interactions. Nevertheless, different reasons motivate some participants to exploit a secure backbone infrastructure without taking part in maintaining the system, as long as they can freely exploit autonomously of this system. Examples could be scarce available resources or the absence of interest in taking part in it. *Non-infrastructural-nodes*, therefore, take part by sending update transactions and querying the state's information by communicating with listening maintainers, we call these *transactive-nodes*.[11] Admittedly, in this way, trust is shifted upon maintainers that acquire central importance. Nevertheless, two main points have to be kept in mind. First, network decentralization can still be ensured by an infrastructure not controlled by a single central body, but by a series of multiple unbounded *infrastructural-node*. Trust is therefore gained by distributing it over multiple maintainers. Second, the system is built to process transactions in a non-discriminatory way. As long as a meaningful network of *infrastructural-nodes* processes them, transactions represent the principal privilege of updating the state and interacting with it. This is even more marked in a permissioned implementation, where *transactive-nodes* are entitled to this privilege under certification and granting-access. Moreover, nothing impedes that a *transactive-nodes* also hold *infrastructural-nodes* capabilities.

[10]In this article wallets, i.e., artifacts able only to send and sign transactions, even if non participating in the infrastructure directly, are also considered nodes of the network.

[11]In this text a *transactive-node* is basically an independent client sending transactions to the network for processing them and concurrently update the state; its main characteristic is to posses a unique identity for interacting with the network.

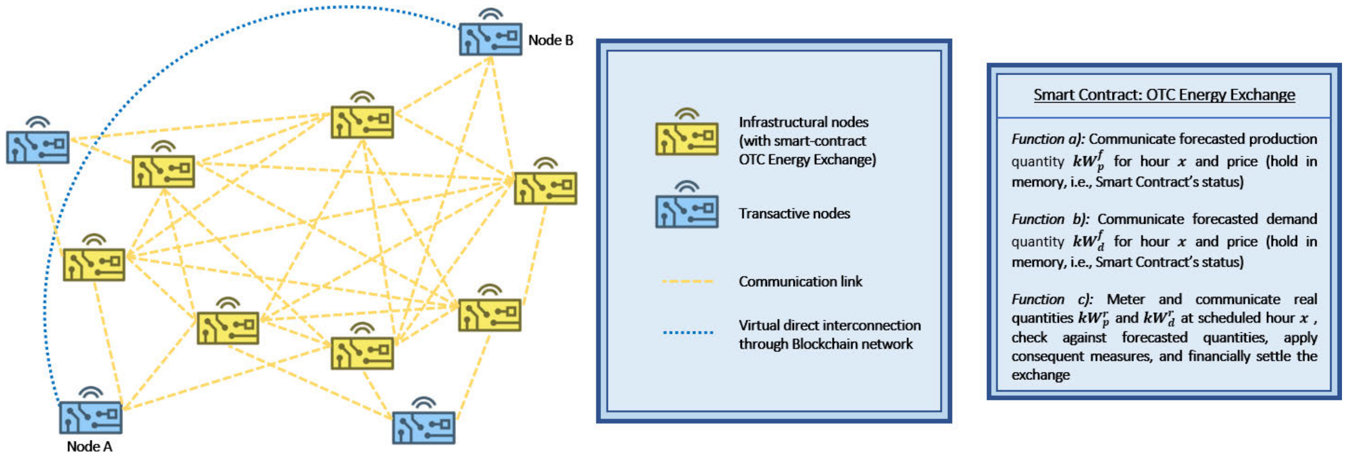

FIGURE 2. Exemplifying a simple Blockchain network and the usage of a smart contract. In this basic scheme, the Blockchain network is formed by a group of central *infrastructural nodes* supporting the system and holding a simple smart contract. Here, OTC (Over The Counter) Smart Contract represent a simplified version of a possible smart contract for managing direct contractual energy exchange between an energy producer (Node A could be a PV, CHP power plant, or a nuclear plant) and a consumer (Node B could be a heat pump, house, or a factory). Some nodes of the network (like Node A and Node B) are not interested in supporting system functionalities but want to partake by transacting; these join as *transactive-nodes*. Even if not embedding infrastructural tasks, A and B can still directly transact by communicating data with the multiply available *infrastructural nodes*. Node A reaches Function a) of the smart contract communicating foretasted production for hour x for a specific price. The smart contract holds within its status this information. Node B reach function b) to purchase its foretasted demand in kW for hour x within a specific price window. The smart contract could be designed to allow buying or selling the exact same quantity for the exact same price already present within the stored state, or more complex schemes could be implemented for allowing adjustment and finer financial settlement. At hour x Node A and Node B meter real production and consumption and communicate these data through Function c). This function is designed for monitoring the real energy exchange against foretasted quantities and consequently proceed with the financial settlement (using Blockchain native currencies or a representation of real fiat currencies) and possibly activate corrective measures in case of deviation between scheduled and real exchange. This example was intended to represent a possible heterogeneous Blockchain network and the usage of a data-driven smart contract to allow direct interaction between participating nodes while exploiting the system state.

What Blockchain brings as an advantage, a feature of great importance, is the capabilities of interacting independently within a system built for processing node communications and coordination. This is related to the accountability provided to each single node (both *transactive-nodes* and *infrastructural-nodes*) by Blockchain applications implementing a secure public key infrastructure in support of a digital coordination system based on coded programs.

Hence, the possibility is to create a platform to allow direct interaction of *transactive-nodes* supported by a meaningful core network of *infrastructural-nodes*. The core platform create a secure distributed machine to process transactions sent by any participating nodes (both *transactive-nodes* and *infrastructural-nodes*). At an aggregated level, the Blockchain network represents the machine processing transactions by constituting a system for formalizing and securing relationships within a multi-node distributed system. In this view, the application layer will represent the coded logic for processing the incoming transactions and automatically manage the relationship under predetermined contractual clauses [21]. This metaphor born with the concept of smart contract introduced by Szabo [28]. In its view, a smart contract is a programmed contractual clause for directly and autonomously secure interactions between parties using computer processes and the infrastructure built around them. Smart contracts could be seen as script procedure for database management system [21] therefore applied to manage, in a standardized way, the action to take under specific input coming from node request and sent data. What constitutes an advantage is the possibility to perform programmed and self-enforced procedures under received inputs in an identical deterministic way, within a distributed system of multiple separated nodes. In this way, digital entities can efficiently interact directly with the fictitious intermediation of pre-determined digital agents written in the form of code, i.e., smart contracts, rather than inefficiently with a single physical third-party. Figure 2 shows an exemplification of a possible implementation.

The efficiency is guaranteed by the standardization of the coded interactions, the autonomous self-enforcing, and the automation of processes under pre-determined logic. All this stands upon a logical, complete, and correct implementation of the necessary procedure in the form of scripts. Therefore, within the Blockchain ecosystem, smart contracts represent the scripts within the infrastructure's application layer, which manage input-driven procedures for processing transactions under specified logic. As a result, the state is consistently modified and updated while meaningful output are generated.

Therefore, the foreseen potential of Blockchain's application to the electric grid is the possibility of building a smart-contract machine for processing energy products and services exchanged between the electric grid's actors. The Blockchain system will allow direct interactions between actors. The deployed application layer, composed by smart contracts, will, therefore, formalize and process them under the specific business logic written for optimizing and managing the grid interactions. The reasons sustaining this idea are therefore analyzed in the following sections.

III. THE ENERGY SECTOR CONTEXT AND POWER GRID APPLICATION

The global energy paradigm is a dynamic reality. Since the industrial revolution, our society is continually reshaping the structure of the central pillar of our progress: *Energy*. Nowadays, we are continuing to follow this dynamic evolution under the pressure of new forces that are driving it. These drivers represent, from one side, important and deep changes affecting the complexity of the electricity spinneret in the name of goals and new paradigms, and on the other side, potential answers on how to cope with these changes. Such drivers, extending the one presented in [29], are: Decarbonization, Distribution, Decentralization, and Digitalization.

Decarbonization is the quest for a sustainable future with its importance for our society now taken for granted [30]. The objective is to reduce harmful emissions from the main activities of our society in which energy production and consumption represent the main contributor [1]. Therefore, this idea strongly influenced the energy sector, especially with the policies meant for increasing the penetration of Renewable Energy Sources (RES) and their subsequent strong increase [1]. From a technical perspective, new generation technologies like solar or wind pose challenges on how to integrate their particular production profiles and nature, requiring to adapt the design of electricity markets and networks [31] for a more dynamic, flexible and adaptive electric grid. A possible answer could come from the integration of low-scale distributed resources [32].

As discussed above, the *Distribution* of resources and assets is indeed a leading dynamic within the context of electric grids [32]. DER are increasing their prominence in the overall energy production [1] while smaller actors are making their way in the electricity spinneret as potential active agents rather than passive. The reality of DERs has brought new agents to the grid edges, especially in the dimension of generation [32], e.g., solar electricity, wind energy, and microgeneration, and in the dimension of flexibility with assets like storage or electric vehicles [33]. If exploited correctly, these distributed energy technologies have the potential to unlock cost reductions [34], beneficially participate in ancillary services [35], and eventually help in meeting the decarbonization goals by integrating renewable energy resources [36]. The problem is that with the current centralized coordination framework and with complex markets' implementation choices, these powerful resources risk not being able to be fully exploited due to the difficulty of scaling the system to a large number of active actors [3] and transfer economic benefits. Indeed, the actual system misses in integrating small active actors - their size impedes them from participating in the market, making it also economically non-convenient due to high latency and high frictional costs caused by numerous intermediated steps [4]. Transaction costs caused by the actual management design and incurred by low scale players are one of the causes cannibalizing benefits of innovative markets schemes [6]. Therefore, the traditional centralized management approach is not efficient in scaling to a large number of distributed agents operating at high frequency, in a non-coordinated manner, and potentially generating an enormous amount of transactions [3].

Moreover, the regulation still impede it, and, even after the introduction of new concepts as Virtual Power Plant or Smart Grid services, we still are fundamentally related to centralization: **i**) markets are non-localized, **ii**) data are managed centrally [4], **iii**) system optimization is handled by singular entity [36], **iv**) transactions at small agent level are aggregated losing specific valuable insight. **v**) single prosumer profitability is not addressed, therefore, decreasing specific economic advantages

As a negative outcome of such centralization, central coordinators mostly detain market power, allowing them to perform grid management techniques for the sake of the incorrect rent-seeking practices. This problem is, therefore, rooted in the existence of a central obliged passage point. It is then clear that the system shifts away from efficient market solutions, towards profit-maximizing outcomes, with the inevitable generation of Deadweight Loss (DWL).

In summary, the transition towards a truly distributed system is impeded by actual electrical network management techniques leaving DER and new small agents as almost invisible assets to utilities, parallelly losing their full exploitation potential.

Therefore, in order to avoid these problems, decentralization of market mechanisms could successfully better integrate renewable generators while exploiting the potential of DERs [37]. This will be reached by a better segmentation of the active actors present in the grid, such as prosumers, leaving them the possibility to participate in energy exchange processes directly. The extension of direct participation to smaller grid actors, if correctly coupled with more granular space and time resolution, could potentially help to better price energy within the specific zones and therefore sustain more efficient economic dispatch [38].

Decentralization is therefore seen as a necessary evolution under this light. In full sincerity, such a transformation already strongly impacted the electricity sector with the liberalization processes taking place in many countries. They shift away from the vertical integration paradigm towards the quest for a more economically efficient competitive structure [31]. This ended the hegemony of monopolistic integrated utility and marked the birth of competition foremost at generation level and, in a lesser-way, at the retail level, while restructuring the distribution and transmission segments. Recently in Europe discussion are held to introduce competition also in the area of market operators. Competition successfully became a standard for electricity wholesale market, while retail had different levels of success. Nevertheless, these changes were done almost two decades ago for a system highly centralized and different from today's one. Moreover, while competition at the wholesale level consistently decrease wholesale energy prices, at the retail level benefits was not as effective, and in certain situations final consumers even saw price increases or lower savings [39]. With the current market implementation, small actors, such as prosumers, are obliged to accept lower financial returns by exploiting third-party financial intermediation that distorts beneficial price signals effects. [40] shows how a more direct exposure of consumers/DERs to variable electricity wholesale prices, rather than their intermediation through averaged prices charged by retailers, will be beneficial both for them as well as the grid, even at the cost of higher price-risk levels. Additionally examples like the one of Liu, Yu, Wang, et al. [34] demonstrate how a more direct exposure of prosumers to innovative market schemes is beneficial both for them as well as for increasing usage of renewable PV energy in line with *Decarbonization* goals. The question is in which way can we allow the direct participation of grid participants that is safe both for them as well as for the grid?

The current idea of this research is that this driver, namely *Decentralization*, needs now to increase further the possibility of coordinate the daily operations without relying on central aggregators or a set of intermediaries contributing to distorting beneficial price signals effects [38], [40]. Decentralized market settings will allow markets to secure higher freedom to individual actors, both consumers, and producers, fostering the integration of lower-scale actors and distributed resources by allowing them direct participation. This will allow for new forms of coordination more strongly related to economic incentives. Such an innovative design must, on the other hand, be based on responsive and enabling technologies allowing to decrease the gap between scheduling and real-time dispatching.

These, in conjunction with correct remuneration formulas and market designs, will increase the efficiency of the electric systems by contributing to send more precise price signals thanks to more direct actors' participation,[12] higher spatial resolution, and lower time gaps between scheduling and operations.

Hence, to allow such a responsive system, *Digitalization* of the energy sector is seen as the necessary enabling element. Indeed, *Digitalization*, the fourth driver, is strengthening its position as a powerful ally for a better energy future. First, it is reinforced by a shift towards electrification of the energy demand [1], able to create a better entanglement between digital technology and energy. Second, the investments in smart digital energy assets have demonstrated their power in better managing the complex network of the electricity sector and, with their growth at a rate of more than 20%, have overtaken the investments in other core infrastructures of the energy sector as the gas-fired power generations [7].

This digital evolution is therefore seen as the opportunity to build a distributed architecture for connect and coordinate a multitude of grid-tied smart-actors. Two major digital characteristics are then seen as fundamental: **i**) the increase of computational capabilities within the single distributed energy devices, **ii**) the possibility of communicating and interconnect through different technology allowing sending and receipt of data [41]. .

[12] A compelling case could be the one of easily incentive homeowners to cool down their houses during off-peak period and decrease on-peak usage of electricity avoiding criticalities like the actual California situation where utilities are indeed trying to incentive such a behaviour.

The first is essentially increasing the capabilities of the single devices in responding to input and take actions [42], like in the case of Zero Injection commands for PvI, or smart devices, like HVAC, responding to external input as real-time spot prices. Fundamentally devices increase their independence in controlling the physical flow of electricity they generate or consume. Moreover, forecasting capabilities at the service of DER are enablers of more advanced scheduling and decision-making [43]–[45].

Communication capabilities are the second fundamental piece for allowing decentralized forms of control [8]. Indeed, due to the strong physical interconnections of activity performed by the various actors in the grid, coordination must be reached by communication between them. Hence, if grid-edge devices are allowed to participate in the foreseen coordination protocol actively, they must transmit data about their preferences/choices and real-time activities while possibly receiving information regarding commands or requested services. Communication is therefore seen as a necessary feature for a grid system required to coordinate a multitude of distributed actors [46]. This is undoubtedly a leading transformation [47] as various research and new advancements demonstrate, e.g., the usage of LTE as enabling technology [8].

A. DECENTRALIZED ELECTRIC GRID PLATFORM

Given a base of communication and computing capable energy devices, within a grid made of distributed agents, what this research finds necessary to investigate is a way to enable their coordination through a decentralized coordination protocol allowing to schedule near to real-time operations. It foresees agents' direct participation rather than a centralized system controling their operations directly. The goal is to build a system where principal-agent control is minimized in favour of an environment fostering competition under predefined and carefully designed rules enforced by the virtual-digital coordination platform. This goal is influenced by ideas coming from prominent researches.

Indeed in [5], the authors describe an innovative scheme and procedure where individual actors can make and express choices regarding their physical participation within the electric grid. While describing the algorithm, its characteristics, and impacts, Caramanis, Ntakou, Hogan, et al. [5] did not address the specific underlying platform to be used for sustain the described scheme (since out of their scope). What is argued, nevertheless, is that the platform enabling it, must ensure direct participation of distributed actor and supports their individual decision, while ensuring their certification for participation.

Parallelly, [48] highlight how a single coordination entry point will have difficulty in controlling millions of distributed agents. They suggest that a decentralized, individual, and

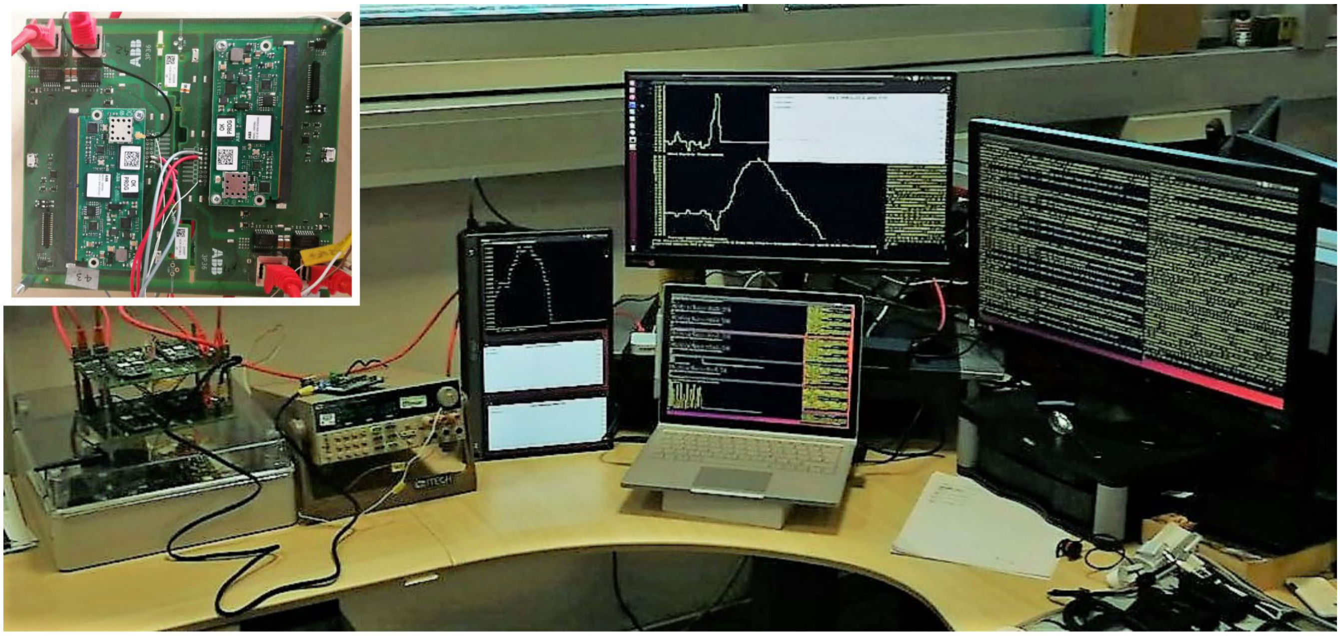

FIGURE 3. Experimental setup for implementing a first-prototypical Blockchain based energy coordination platform for embedded-energy devices.

directly accessible decision-making protocol will be better suited.

Hence, the system should allow direct participation of a greater base of actors, not only limited to big producers, utilities, and market operators. As a benefit, non-intermediated market exposure will potentially decrease transaction costs for participating actors. First, due to disintermediation and avoidance of usage of centralized aggregators, and secondly due to non-transfer of risks [49]. At a higher level it will enable more efficient allocation of resources and the exploitation of new services and products coming from a broader actor base now impeded, not for technological reasons, but due to organizational one, as in the case of ancillary services procurement from DER.

First, this research envisions a way to allow direct transactability of services at a single-actors' level. It entitles actors to be singularly accounted from a physical and financial point of view, by ensuring their direct access as single entities (avoiding intermediation) [50], and by the personal embodiment of their associated risk. It could allow to transit to more efficient market schemes now impeded by today's market implementation's latency, inefficiencies, and embedded costs [5].

Secondly, the system must allow, within its protocol, for identities authentication and consequential relation of their interactions. It must treat and verify them under specific policies, ensuring trust in the system from all parties' point of view, both transactive ones and affected ones. This is also motivated by IEEE standards regarding the need to ensure access control for all connected grid devices [51].

Therefore, automation of process must be ensured under agreed and shared rules, while striving for a decentralized, yet still regulated and supervised, coordination system. Indeed, example exist of implementation where Blockchain are used to enhance performances of system still under central supervision [52]. Automation will help to decrease the time gap between planning and physically dispatching, allowing for more flexible operations and decreasing the risk associated with forecasting eventually bringing to lower cost for backup and ancillary services.

Such infrastructure will represent a rule-based digital system for coordination of energy-exchanges at the grid level. Through enhanced connectivity allowed by nowadays advancements in IoT technology, energy devices, such as generators and loads, will optimize their physical energy-exchange preferences by coordination with a decentralized digital market platform hosting the specific logic and rules for managing these interactions, constituting an environment for allow safe exchange of energy related products.

These characteristics motivated us to seek in Blockchain technology the tool and potential to build an infrastructure based on the aforementioned paradigm. The present research, thanks to a strong collaboration with ABB Solar Smart Power Laboratories, started from the fundamental aspect of such energy-IT infrastructure, namely the layer made by hardware components represented by real control boards of today's ABB inverters, as depicted in Figure 3. These exemplify DER assets present within a grid infrastructure. In doing so, the reason was to enforce the usage of designs and technologies compatible with the current energy management systems to reduce costs and indirectly decrease the one absorbed by final users to exploit it. This is deemed as a fundamental point [51]. On top of this test-bed infrastructure, the research developed the network and the software logics needed to build such a Blockchain-based coordination platform and allow the direct interactions of the physical entities. The test network was composed of a multi-node Blockchain system embodying the IT infrastructure hosting the protocol and the coordination logic. Physical devices use this for schedule production and generation. Since the focus was demonstrating the feasibility of the system and not implementing a specific market design and framework, this did not yet represent a fundamental part of the research while it will in the future looking at specific examples as [5] or [36]. Differently, a minimal market framework was implemented just in its fundamental parts. In summary, the final goal was developing a prototype Blockchain-platform for managing power exchange activities of electronics embedded devices representing grid-connected loads and generators. The Blockchain infrastructure embodied the directly accessible market and control environment.

The reason for exploring Blockchain as an enabling tool is that they can potentially address the required characteristics listed above if appropriately accompanied by other enabling tools.

First, Blockchains are built on the concept of allowing direct transactability of digital assets within a digital platform. Secondly, the protocol itself is built upon creating an authentication, verification, and storage system for allowing trust between multiple heterogeneous participating actors. Third, these technologies allow the creation of autonomous coordination logics in the form of software for forming rules-based systems managing actors' interaction in a decentralized and distributed way. In connection with IoT, this technology could allow us to build a system for direct interactions of devices under the precise set of rules encoded as software within the protocol [21], i.e., smart contracts.

The paper's intention was to introduce the motivation, context, and technological background behind this decision. The intention is to provide a first high-level vision of the idea, provide a framework for comprehend it, and mapping technology's requirements for its application. In a following article the technicality and performances of the developed IT-infrastructure will be detailed. Next, on top of a test-bed infrastructure, coordination processes and market designs, coming from the available academic or industrial literature, will be implemented in order to test its functionalities.

B. PREVIOUS AND CURRENT EXPERIENCES IN DLT-ENERGY CONTEXT

Given this premise, it is therefore necessary to understand how the academic and industrial world has moved within the field of application of Blockchain technology in the energy world. Such a topic has acquired an extreme interest as demonstrated by [4]. They report a comprehensive review of the many cases and the nature of different applications. As they highlight, the technology is still in a nascent phase, with a substantial lack of regulation and low compliance to laws like, for example, General Data Protection Regulation (GDPR) [53]. At the same time, a plethora of implementations makes the topic rather confused. Therefore, there are no standardized and widely accepted solutions for the application of these technologies in the energy sector. This is reflected in the power grid applications, with a substantial lack of clear methodologies and standardization.

Therefore, starting from previous work, we try to formalize the context of this manuscript. In line with [54] and [55], we divided the landscape of the applications of Blockchain technology within the energy sector into two major groups: process-oriented and platform-oriented applications. Process-oriented applications [54] are focused on improving or innovating the actual procedure and business models. They move towards creating new services adjacent to existing ones, offering new kinds of possibilities, or modifying, in part, some business processes. In general they are interested in optimize some aspects of the energy spinneret.

Differently, platform-oriented applications [54] are interested in providing digital instruments to allow interaction between two or more power grid's actors and participants. They could be wide in their scope (a whole grid coordination platform) or more limited (focused on micro-grids). Yet, the objective is to provide a platform to coordinate the grid's actor interactions. Due to our work's focus, the second category is the one we think our research has to be located in.

Regarding process-oriented applications, as noted by [4], these are applied in fields like billing [56] (also within specialized context like EV-charging), metering and data transferring [57], security [18], and in other processes affecting the energy business. An example is the solution given by [58]. Here the authors propose the integration of Blockchain technology in the Energy Management System for providing better functionality to monitoring/recording information about inbound and outbound energy exchanged with the power grid. The purpose is to simply store this information, mainly focusing on the distributed ledger functionalities. They could be seen as the application of blockchain technology to enhance offered services and provide solutions to perform activity in a more efficient way. Their differentiation with platform-oriented application become less marked as the direct participation of users is increased and as the system become a tool to coordinate interactions of independent agents rather than offering a third-party-governed service. In this regard the work of [59] envisages a bidirectional framework for a future electric vehicles participation scheme using a Blockchain based system to prioritize charging operations.

So, of greatest interest to us is the platform-oriented Blockchain-based electricity-exchange literature that has guided our paper and which is in a closer context. One of the most successful implementations towards the direction of energy-DLT platforms is undoubtedly the LO3 Brooklyn microgrid [60]. Here Ethereum-based smart contracts are used to allow user-to-user secure and autonomous transactions. The platform makes use of dedicated smart-meters, recording energy production/use while energy is sold in a localized energy market coordinating transacting entities that are financially accounted for these economic exchanges. Our work, was indeed steered by this design as it was from the one reported in [61]. The peculiarity here is the contextualization within a localized energy markets with the presence of a super-node (a connection to the grid) able to correct all imbalances. Such a characteristic was also part of our first implementation, with the presence of a supervisor and an imbalance solving node. Additionally, as in this article, [61] exploits and suggest a permissioned implementation. This is done to restrict market access and gain higher control over participants, while, as they highlight, possibly make use of more efficient consensus mechanism. Moreover, in line with the methodology of [61], in our research we used real power profiles acquired by data-banks as shown in Figure 7. In [62] the authors implement a particular solution dedicated to a sectorized purpose. A Blockchain-based platform is designed to facilitate energy exchanges between digitally interconnected agents through the usage of market rules encoded as smart contract. Again, it shows the potential of coordination through a directly accessible rule-based platform, thus, avoiding governing intermediaries, and potentially decreasing the cost of transacting [61]. Again, in [63] the authors propose a trading platform for energy exchanges supposing a bi-directional power system. What is peculiar of their work is the usage of digital inverters and their connectivity as gateway devices for supporting the connection to the platform, as also this research does. Of particular interest then is the work of [52]. Here an Ethereum based solution for Distribution System Operator (DSO) commands issued to DER is used to request ancillary services. The DSO still acts as a central master, while smart contracts are used to ease DER's direct participation in providing services. This remarks the possibility of being able to entitle predetermined entities to more powerful controlling and monitoring tasks even within a decentralized system. In line with this, also our implementations makes use of this paradigm. Hence, as pointed out in [64], if the main goal is to develop a secure and disintermediated platform for exchange of goods, electricity seems to be an ideal type of asset to be managed through the Blockchain technology, but noticing that the network operation must remain under an attentive scrutiny of supervisors like operators. [36] and later [65], propose a design using DLT to develop a fully decentralized localized energy market for distributed agents. The virtual agent involved are supposed to directly participate in an environment created to coordinate their interactions. Smart contracts provide the rules for interaction, focusing both on the grid's constraints and actors' optimal decisions. What is extremely interesting of these two articles is the usage of decentralized optimization algorithm. Contrary to relying exclusively on the blockchain platform for market clearing, their solution recognizes a greater level of independence for single participants by allowing a first step of local optimization and only at the end coordination is ensured through the platform.

This research goes in the direction of these platform-related works. It aims to contribute by starting to bring the technology within real hardware devices currently in use in the energy sector. This article deems necessary to first strongly motivate the reason behind this necessities, deliver a conceptual introduction to the technology, and provide the framework that steered the design. These elements are addressed in the next session, and they are built on the concept of Blockchain-based platforms reported in this literature section that actually provide a useful background.

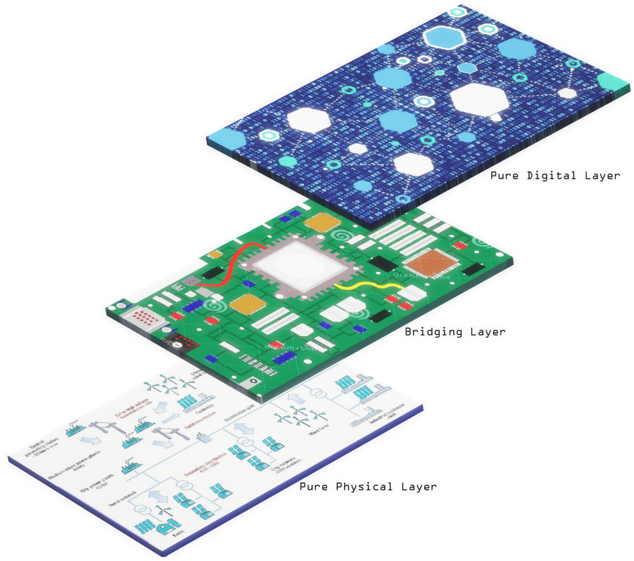

FIGURE 4. 3-layered grid model.

IV. PLATFORM DESIGN AND MULTI-LAYER MODEL

A. GRID's PHYSICAL-VIRTUAL MODEL

To better segment the conceptual framework a simple model was here developed as illustrated in Figure 4. The three-layer cyber-physical model is designed to understand how and in which way the main grid domains are affected. Starting from the bottom, there is the Pure Physical Layer (PPL). This is the physical electric grid made up of loads, generators, and necessary hard infrastructures. It sustains the grid operations physically and permits physical energy interconnection. This layer is recognized with the task of holding everything together and physically bear the energy flows. It must be capable of properly decreasing and addressing fluctuation and imbalance risks, accommodate demand with a properly sufficient supply, and account for necessary reserves. The PPL makes use of: 1) Distribution lines capable of hold the requested energy flows; 2) Wide electricity transport lines able spanning over broad areas and able to exploit geographic heterogeneity of electricity production and demand to contrast imbalances [48]; 3) A correct physical balance between supply assets and demand loads by making use of storage, sinks, proper production infrastructures, and necessary available reserves.

Embedded in this physical layer is the substrate of smart devices capable of control or measure the electrical flows, communicate, and perform computations. This network of nodes takes the name of Bridging Layer (BL). Indeed it transposes the analogical domain of electrical flows in the digital measures one. Nowadays, at DER level, these capabilities are mainly exploited as control end-points or simple sources of information [9], i.e., external controls are issued by operators or users for directly interacting with the underlying physical flows or meter the delivered electricity. Similarly, power plants make use of communication means to transmit information about production and scheduled dispatch. Control is then manually performed under markets' outcomes or ancillary-service requests. Nevertheless, thanks to a distributed multitude of small actors at the distribution level, the unforeseen potential of this hardware layer is the possibility of using it to generate a digital representation of the grid eventually used to coordinate the interaction of the actors with the physical system.

Therefore, the third layer, namely the Pure Digital Layer (PDL), is where, through communication, grid actors coordinate in a virtual domain their actions. Such a layer collects information received by the underlying physical actors to schedule and govern their operations. Coordination is carried out by a series of software logic and algorithms hosted in the layer itself and physically supported by a properly designed IT-infrastructure. The design of this layer could take many different forms. Indeed it could be represented by a fully centralized server collecting information from the various underlying energy devices while controlling them. This is how nowadays market like DAM are organized at transmission level, with a central market operator clearing the schedule for delivery. On the other hand, it could be an architecture allowing direct actors access and leaving to designed mechanisms to manage their coordination subjected to constraints, objective, and optimal choices. Nonetheless, a critical requirements is that the digital platform itself must be built on a secure Crash and Byzantine fault tolerant protocol able to safely register, secure, process, and identify interactions. Within this layer, therefore, the authors foresaw the application of Blockchain to provide this secure, autonomous, and robust digital infrastructure eventually used for coordination of grid-connected energy assets.

B. BLOCKCHAIN IMPLEMENTATION AND ADVANTAGES

As argued before, Blockchain technology seems an extremely valid candidate. Indeed their characteristics, as introduced above, are: **i**) being a distributed system, directly accessible by devices, allowing decentralized coordination, and ensuring fair direct participation [21]. **ii**) securing communication and interaction through recognition and signature mechanism, in a potential adversarial and fault-prone system [12]. **iii**) the ability to safely register and store transactions and communicated information [14]. **iv**) the natural necessity to ensure a single consistent vision of the network status [17]. **v**) automating, through standardized code, the coordination, without requiring the third-party intermediation [21]. **vi**) the possibility to recognize to different nodes different prominence level both from transactive as well as infrastructural role point of view [14].

Parallelly, the technology have to recognize and correlate the digital counterpart of nodes, with their physical identity. This could be reached thanks to the usage of certification processes embedded in the protocol itself. Moreover, the ability to entitle different computational burdens and characteristics to different devices will avoid expenses for new, more costly hardware. Therefore, modularity must be a necessary requirements in parallel to a flexible set of governance policy and settings.

One of the features that must be highlighted about this technology is the potential to ensure the critical necessity of interactions accountability. Indeed it could be possible to envision a purely IP-based infrastructure for coordinating grid operations without the need to use an over-complexity as Blockchain. Nevertheless, a purely IP-based system lacks a robust accountability system [66]. Consequently, the hosting system, i.e., the grid, will lack this vital feature if simply based upon an IP infrastructure. Therefore, the use of Blockchain technology on top of such an infrastructure would ensure accountability. This is possible by exploiting the immutable consistent storage and the uniqueness of entities provided by the identity layer. Indeed, each transaction-capable device is associated with a unique identity and a public-private key pair for performing actions within the digital coordination level. Not considering the unfortunate case of a key being stolen, each entity would be accounted specifically for the actions performed. This, in addition to the immutability of stored information, will impose that each individual will be permanently and consistently related to them. Such an advantage nevertheless, is limited to the digital identity level only. This level is not necessarily directly correlated with a known underlying physical-hardware device (BL). Specific implementation should be provided to address this point. Indeed, such correlation should be provided in order to ensure full accountability not only of an easily-created digital identity but also of the correlated physical asset.

For ensuring a direct relation between the digital identity and the physical one is necessary to certify this connection. A certification infrastructure can be a viable option. For this the advantage of a permissioned implementation comes to help. While pseudonymous could be an excellent choice for a purely digital application like Bitcoin [12], a different choice should be made for an electric grid application. Notably, smart meters already relate to physical identity for direct billing [67], power plants are also uniquely recognized within the actual infrastructure, and all grid-tied devices are uniquely recognized and identified. Therefore the natural choice would be to maintain such recognition also in the virtual-infrastructure. This will allow to uniquely correlate the associated real-identity to the digital one participating in the platform and consequently to possibly activate physical ex-post corrective measures if necessary. A downturn of this implementation will be a more expensive and complex procedure for registering new nodes, but this cost will more than compensate the risk related to accepting, within such a critical system, pseudonymous entities with low attention to access control. Indeed, IEEE standards [51] highlight how access control represents a vital feature for preventing attackers from performing malicious action within the grid's ICT systems [68]. A permissioned Blockchain implementation should, therefore, be better suited for this task.

It has to be stressed that this is not related to performance issues, governance requirements, or privacy constraints but to its advantage of ensuring the security level necessary for an electric grid system in terms of accountability and actions tracking. Especially the entities proposing ledger updates, i.e., transactions, should be uniquely identified and related to their physical counterpart. Grid constraints could be indeed related to the location of the device, its characteristics, and its specific identity.

Certification, therefore, would represent a layer of security against possible issues like preventing attackers from connecting pseudonymous identity to the coordination infrastructure or perform actions at the damage of the grid without being easily identified. Indeed, it will allow us to correlate actions to real entities and take corrective measure more rapidly. A more robust identification layer will provide stronger security mechanisms within the context of an electric grid massively permeated by ICT devices and therefore threatened by cyber-security issues [68]. Authentication schemes, potentially based on certification, and secure encryption mechanism, naturally provided by Blockchain technology, are indeed listed as necessary features against grids' future digital threats [51], [68].

Moreover, attaching certification to performed transaction could relate the node to specific characteristics representing the physical asset. Consequently, it will identify the device's nature and allow more powerful operations at programming level such as Attribute Based Access Control (ABAC) or actions filtration. For example, an asset categorized as a load-only will not be granted the possibility of scheduling production operations.

Therefore, a permissioned Blockchain was deemed more appropriate to develop the first implementation of the envisioned system. In order to be as clear as possible, and by repeating it, the decision is mostly based on the necessity of identifying the physical transactive-actor. Infrastructural role subdivision, governance organization, and performance issues did not represent the main motivating reason. Nevertheless, it will be difficult, but not impossible, to host a grid control system infrastructure in a public Blockchain infrastructure where governing bodies will recognize the same authority to all actors.

First and foremost, the research's objective was to test the technology itself, how to integrate the hardware used, design the software components, and build the IT-infrastructure for sustain the application. Hence, a network topology made of several assets and actors was imagined and used as the underlying PPL. The real board computers used represented the controlling devices composing the BL and forming the test-bed environment for experimenting the system.

This first research did not focus on the organizational and hierarchical structure within the protocol. Indeed it did not address in detail the subdivision of infrastructural roles. This topic will be deepened in successive publications. Instead, the objective was to focus on the core functionalities, capabilities, and requested features of the developed system.

C. PROPOSED PLATFORM DESIGN

The design that represents the basic idea for the envisioned coordination platform is depicted in Figure 5. As it is possible to see, physical devices in the PPL are represented by various types of actors within a grid environment. These are connected loads (houses, commercial building, industry, EV charger, batteries, etc.), generators (power plants, PV plants, wind generators, etc.), prosumer (being both loads and producers as houses with PV systems) and other grid-connected actors. Within this layer, there are also actors such as utilities or grid operators not directly interacting with electric flows but representing prominent roles in the energy spinneret from an operation management point of view.

All these are direct participants and supervisors of the physical exchanges at the electric grid level. They participate as individual self-controlled actors within the exchanges of energy products and services. Participation is allowed by the direct connection of the physical actors with digital devices controlling their operations and communicating with the cyber-coordination system. These are hardware-software smart agent controlling the device and working as gateway-node for the connection to the cyber-digital coordination network.

In the implemented design participants express their choices represented by the willingness to inject or withdraw power. Clearly this could be easily extended to more complex and general choices like bid/offers of coupled energy products and services (real power, reactive power, reserves). This are made under specific preferences and available information (forecasts, needed energy, recharge time, indoor temperature, etc.). Hence, smart-agents are required of forecasting available capacity or needed energy based on information like weather and individual optimal strategies while, using external inputs, as energy prices, make conscious decisions. Examples are smart-thermostats connected to HVAC systems, forecasting systems for PV output coupled with battery systems, programmable EV-chargers, and others. As noted before, these are in line with the current evolution of digital capabilities within the grid system. This does not impede more traditional control procedure where choices are instead taken by human-user through user interface applications. Also non-programmable loads could be entitled of the possibility to participate following specific schemes; for example a home-hub device buying a certain amount of power in advance for risk-hedging reasons and purchasing the rest on real time market, as proposed by [40]. Smart-agents control the operations of the single assets, scheduling and programming them.

Nevertheless, as known, grid-tied loads and generators are not allowed to free-ride or independently inject/withdraw energy from the grid at need as if they stand in a vacuum. This is motivated by the necessity of respecting physical

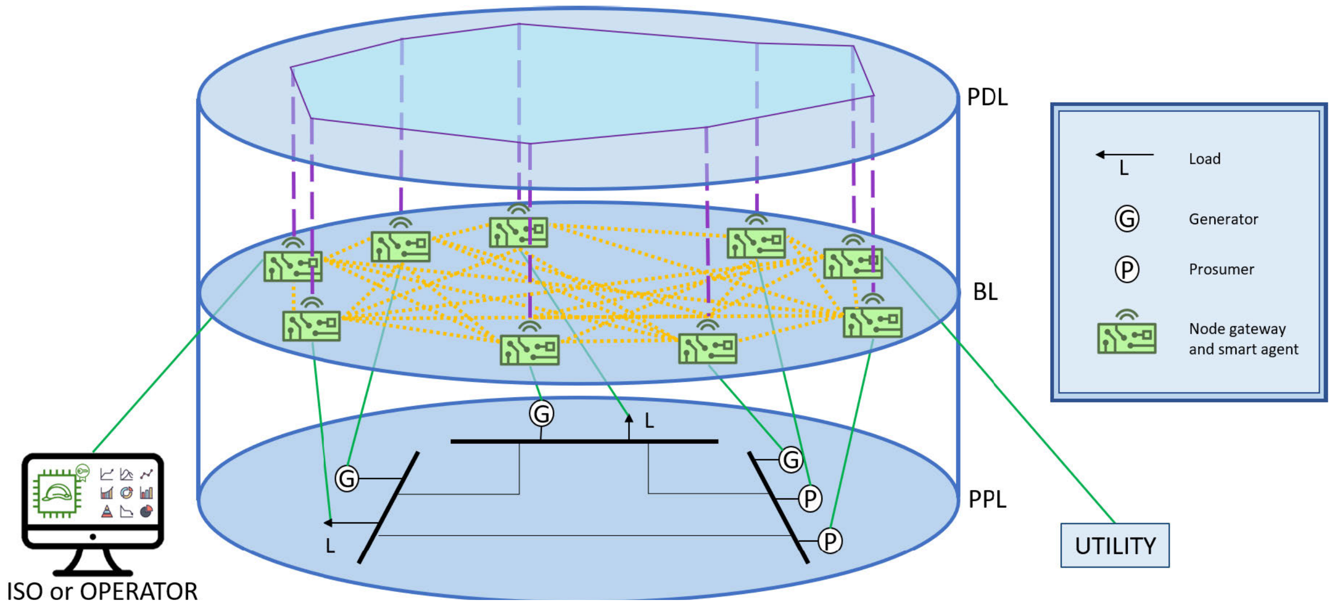

FIGURE 5. Coordination platform architecture.

constraints (first of all load-generation balance) and ensuring optimal economic outcomes. Hence, scheduling is provided by the interaction of the independent smart-agents with the designed platform. Gateway devices are the components entitled of connecting physical assets to the coordination network in this case represented by a Blockchain implementation.

At the same time, non-energy-exchanging actors such as grid operators, utilities, market operators, and others will participate offering and ensuring necessary supervision and management services to the grid or they will impose rules like the impossibility of using a certain interconnection due to maintenance operations. Additionally, a potential advantage for them could be using the Blockchain platform itself for inferring the state of the grid system by using the available information that *transactive-node* send in order to participate. Moreover, increased direct participation at more extended level could ease the actual need to better incentive homeowners to shift consumption behaviour through immediate and flexible price signals.[13]

This highlights the necessity of having a differentiation of roles and prominence between participating entities. Some actors, indeed, would be allowed to perform more critical operations by sending specific transactions to critical smart-contract functions. All the possible actions,i.e., meaningful application's business logic, would indeed be seen as proposed transactions to the network. Hence, given the characteristics of the transacting node, different levels of filtration could be used. These characteristics would be possible thanks to the choice of a permissioned Blockchain implementation able to recognize to each node specific attributes embedded within the identity's certificate. Thus, it is clearer why permissioned features could add a higher level of flexibility for control and monitor operations wile still leaving higher level of independence compared to today's system.

This is not related to the infrastructure. Indeed, allowed actions have to be intended as the state-modifying transactions that specific actors can perform targeting a specific smart contract's function and representing performed or scheduled action in the electric grid. A different discussion in terms of roles is instead related to the Blockchain infrastructural functions, i.e., nodes pertaining to the *infrastructural-nodes* category. On the other hand, *transactive-nodes*, will be solely interested in interacting with the platform by sending transactions about their decisions in order to update the state and possibly receive information or commands. Moreover nothing will impedes that a node would embody both roles as in the Bitcoin Blockchain protocol where full-nodes perform both roles, i.e., sending and singing transaction, while participating in performing the core protocol functions (maintain and updating the ledger, collect incoming transactions, verifying them, participating in the consensus mechanism etc.).

As explained, specific actors could not be interested in holding infrastructural-functions since they are concerned to minimize the used computational resources (like memory, CPU, and storage) to bear lower participation costs. Differently, other actors could be entitled of holding both the functionalities as in the case of grid-operators maintaining the infrastructure while interacting with it for business-related functions. It is clear that in this way governance is more concentrated rather than fully decentralized.Further discussion have to be made in order to understand the best trade-off between ease of implementation and governance decentralization. As argued before, even if not technically impossible, hosting the grid coordination system over a fully

[13]A situation that could be massively beneficial to systems like California's grid where utilities like PG&E are desperately trying to shift of modify electricity consumption behaviour for avoid blackouts during heatwaves [69].

public Blockchain infrastructure could represent a non-secure and non-valid choice for a platform oriented implementation. Moreover, obliging all participating devices to bear intensive power computation processes could be negative, therefore modularity must be an option to subdivide roles.

Anyway, *infrastructural-nodes* represent the physical IT infrastructure for allowing coordination. These are directly connected each other in order to sustain the DCS functions of a distributed set of interconnected processes sharing the state and rules on how modifying it. Transactive actors, on the other hand, have to be connected solely with at least one infrastructural node (different configuration depends on specific implementation, policy, and choices regarding trust distribution[14]) in order to send transactions proposals to the platform that will be processed later. Synchronization of information will be therefore performed at the distributed infrastructure level. Each individual could be seen as an asynchronous process synchronizing with the grid operations thanks to its direct interconnection with the coordination platform represented by the main Blockchain infrastructure.

Here the application layer represents the logic of this synchronization process and the model describing how the grid is affected by nodes' interaction. Specifically, the process' logic will be represented by the deployed smart contracts. This could take different forms under different implementation choices. Here we will give just two exemplifying versions; others are undoubtedly also possible. The intention is to give some possible exemplification of the role of the application layer within the platform.

One possibility could be to have an approach similar to today's Italian electricity markets but with wider participation. Actors will first interact in a real-power exchange market, represented by a first smart contract. They will send bids/offers transactions for purchasing or generating electrical power on a time-frame basis (hour, 15 minutes, or others). These are based on their marginal cost and related to their preferences and local information. On a time-frame basis, the algorithm will define an overall unique price for the grid system similar to today's Italian PUN (Prezzo Unico Nazionale[15]). In the case of line constraints or congestion, smart contracts could be designed to require adjustment or even split markets' zones based on nodes location and physical grid data and recalculate local prices while avoiding lines overloading. Another approach could be entitle grid operators to activate this option by sending special transactions interacting with specific smart-contract functions. It is worth noticing that these actors, in line with previous consideration about certification of identity, are entitled to perform critical operations for keeping the grid safe. Surely this privilege cannot be extended to all participating actors without risking dangerous attacks. Then, other smart contracts, interacting with the first one, could be used to allow reschedule of bid/offer quantities to correct previous session and possible arisen imbalances. Another smart contract could then be used to schedule ancillary services as reserves. Actors, therefore, could decide to smartly allocate their capacity between real-power market or the ancillary one.

An interesting approach is applying the procedure proposed in [5] especially for its focus in integrating DER and providing higher decentralization. Indeed, here segmentation is performed on location represented by the bus to which the actor is connected. In [5], price computation is done at the bus level by a multi-commodities market algorithm allowing to bid/offer energy products and services together (real power, reactive power, reserves). Participants send their bid/offers after computing individual optimal choices, given prices, preferences, and local information. It is worth notice that the connection between busses is given by two-bus connected devices such as transformers or lines. Then, the bus computation procedure receives these inputs from actors and updates prices and imbalances. The iteration continues until satisfying convergence of imbalances. As described in [5], the bus prices-imbalances computation works as a distributed synchronization mechanism for bus-connected actors. Without going into details of the specific framework what Caramanis, Ntakou, Hogan, et al. [5] highlight is the need for a platform sustaining it, where actor directly partake into the exchange. Hence, the possibility is to use the proposed Blockchain framework with bus' smart-contracts reached by bus-connected actors. Therefore, the smart-contracts here will work as the aforementioned distributed synchronization mechanism. Once it receives all devices' choices,[16] it will coordinate the scheduling of resources and demand. Once convergence is reached, it will work as an immutable proof-of-convergence at the bus level for locational price calculation. Smart contract to smart contract communication will represent bus to bus communication to reach global network convergence, hence, as explained in [5], such procedure does not need any centralized supernode but will propagate global convergence information in a fully decentralized method.

These are two different possible implementations of the platform application layer. They did not represent the core focus of the current research since this was first interested in addressing the prototypical platform development. Indeed, the first step was interested in building the IT-infrastructure made of physical board-computers, connecting these nodes, and testing its functionalities. Nevertheless, the application layer logic will be the focus of the next part of the research.

What is important to understand is the function of the cyber-space defined by the digital infrastructure. Once an essential infrastructure is developed, made of *infrastructural* and *transactive-nodes*, it will sustain the logic coordinating the exchanges and scheduling the resources within the physical grid. The specific logic will be designed for ensuring optimal economic conditions and physical grid operations

[14]Connection to more than one infrastructural node will ensure not to receive tampered, non-synchronized information by a single, potentially malicious, node.

[15]National unique electricity price.

[16]To avoid Denial of Service attacks, a minimum time could be used to avoid indefinitely waiting for non-communicating devices.

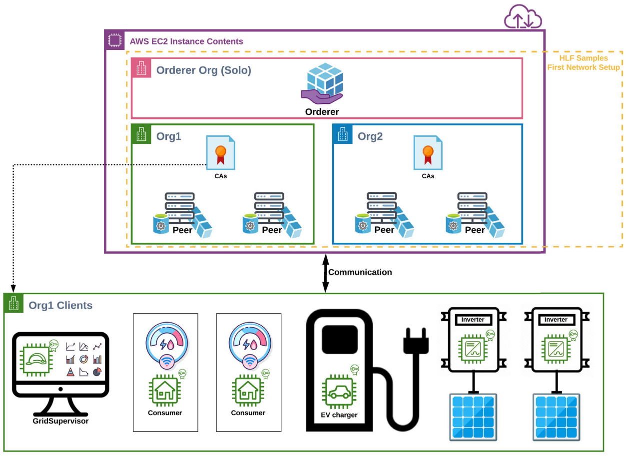

FIGURE 6. Network setup.

management; the platform instead will ensure wide participation, security of the protocol, and safe interactions.

D. PLATFORM IMPLEMENTATION CHARACTERISTICS

Based on the discussed grid physical-virtual model and the proposed platform framework, the research developed the network implementation represented in Figure 6. As mentioned, the primary goal was to test the integrability of Blockchain technology with currently used DER's embedded-controller and, in the future, extend the coordination mechanism and algorithms. We want to stress again that here the intention is not to give the specific details of all the platform's technicalities since this will be the focus of future work. Therefore, neither the technology neither the software architecture are here presented, while a high-level perspective is provided.

As it is possible to see, in this implementation, the nodes are distinguished in 13 different processes. Of these, six, the one in the green box at the bottom, are *transactive-nodes* representing physical grid actors operating at the PPL layer. They represent two consumers (houses), one EV-charger, two PV-panel, and one grid operator (GridSupervisor). Above, in the purple box the *infrastructural-nodes* are presented. As explained, they are the nodes supporting the main Blockchain platform's functionalities, i.e., processing transactions, managing ledger updates, and reach consensus. An AWS EC2 instance (with a Linux Ubuntu OS) was used to host the latter. As already noticed, these are processes/nodes that could be hosted within one single physical hardware, making an entity (the owner) able to both transact and actively support the infrastructure.

The technology used was Hyperledger Fabric (HLF) [70]. Since the beginning, we want to stress that this does not constitute a binding choice; we selected this technology since it satisfied some of the characteristics we deemed relevant and suitable based on the previous considerations. Indeed, HLF gave us the possibility to exploit its modularity, its permissioned implementation through certification authority, the possibility of integrating it with embedded devices, the expressiveness of its smart-contract language, and the flexibility of the policy-based constraints.

Thus, HLF influenced part of the terminology and characteristic of the implemented solution. Nodes, as noticeable, are divided into organizations (Org). This derives from his permission-based characteristic, where certification could be done under different certification authority, thus defining different Org. Once enrolled, nodes acquire the right to perform specific functions (sending transactions, or infrastructural ones). Moreover, the specific structure of the infrastructure layer and the related nodes' role derives from HLF environment. Indeed, in HLF *transactive-node* are classified as clients and, when enrolled (certification acquisition), they are entitled to transact following the specific logic recorded as smart-contract at the infrastructure level. Therefore, all nodes mounted the specific SDK used for implementing HLF's clients. Apart from the GridSupervisor (hosted in a separated x86 Linux OS machine), clients were deployed on the board-computer currently used as connectivity-board of ABB inverters. They are the Linux-embedded processor based on ARMv7 architecture depicted on top in Figure 3. Each of them could schedule its operations independently and communicate them to the hole network through its direct connection with the infrastructure. Additionally, in this implementation, clients communicate their real production/consumption profiles to compare with forward-scheduled one and calculate deviations for implementing corrective actions.

The logical operations organization was recorded in the form of smart-contracts, with which the *transactive-node* was predisposed to interact. This was organized as a simplified single forward market section with a fixed price, and a subsequent series of sections to communicate real-time profiles. Clients send their forward schedules based on forecasts and preferences, and the platform records them. Through this, the overall system expected demand/production is calculated thanks to the interactions of all the physical actors and the aggregation done at the platform level. Eventually, real demand/production profiles were sequentially communicated by participants using the system's specific time-interval (15 minutes), inferring the overall grid's situation. The system, basically, is a DC-based model representing scheduled and real energy flows. The GridSupervisor node was supposed to ensure the balance of the system consuming/selling or producing/acquiring the imbalance between overall demand and production. It has to be stressed that no real flow of electricity was involved. Indeed all production/consumption data was fed to the embedded-devices through some preloaded files representing the forecasted/real profiles. Two examples are provided in Figure 7 for an EV-charger (cli2) and an inverter tied to a PV panel (cli3).

Nevertheless, demand/supply curves were produced using real data coming from ABB's AuroraVision database in the case of photovoltaic systems, and from Open Power System Data in the case of consumers and EV charger. Since the connectivity-boards of ABB inverters are already designed to acquire the underlying production data, the passage for

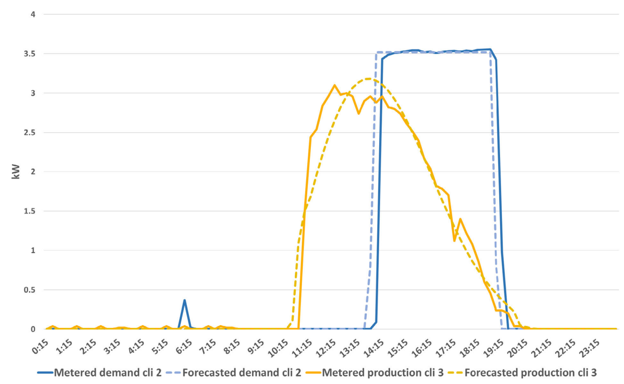

FIGURE 7. Real power profiles examples used in the tests.

using real measures is straightforward. Nevertheless, avoiding using the real underlying flows was essential to speed the testing since it was unnecessary to use additional laboratory precautions or safety measures that would have slowed testing.

Different implementation was tested, and multiple simulations were used to analyze and retrieve different performances under different conditions. We will discuss them in detail in a dedicated article, with the specific software and hardware organization. Nevertheless, the physical implementation of a real platform using real embedded devices was essential to comprehend how to model and design the framework presented above. Moreover, this was important in understanding the principal requirements we deemed critical for bringing such design within a real grid context, as explained below.

E. REQUIRED CHARACTERISTICS

One of the main point to address when conceiving such an infrastructure is a series of required characteristics for integrating Blockchain technology within the electric grid.

Using the layered segmentation introduced at the beginning, and starting from the first component, surely the networking layer should satisfy some vital characteristics.

Indeed as previously discussed, the internet protocol is a fundamental characteristic of all Blockchain implementation [17]. Therefore such networking layer should also be present within the hosting grid-hardware infrastructure. This means that the grid has to adopt IP-enabled and internet-capable devices. This is indeed a major trend within the actual power sector landscape [68]. Different researchers are exploring a wider adaptation of internet communication capabilities through different technologies to allow more flexible operations, such as LTE [8]. Indeed, the devices used in the experimental setup of this research, the one in Figure 3, were provided with connection-capabilities and eventually, the ability to communicate with a cloud server infrastructure.

Nevertheless, it must be highlighted that while TCP/IP is a flexible and powerful option for connecting many different devices, it lacks the capability for addressing time-critical operations [68]. These operations, also given their critical importance, would probably be restrained to a different type of controls capable of addressing real-time conditions. This is even truer if we think that the Blockchain infrastructure itself could risk extending reactions/response times. Therefore real-time critical operations would not probably be managed through the digital Blockchain layer. This instead will represent, as explained, the system to schedule, program and eventually coordinate markets, exchanges, services provision, and power dispatch.

With the respect to internal characteristics, Blockchains, like other digital infrastructure, are garbage-in-garbage-out systems. While the protocol can ensure the consistency and compliance of digital transactions, it cannot verify the "truth" behind inserted data if no other additional mechanism is provided. This problem is even more true if, as in this case, analogical data are measured and transposed as digital information. This issue goes under the name of the Oracle problem. Therefore to avoid the possibility of sending mendacious data, there must be a mechanism to verify the veracity of inserted information. Indeed, if a solution is not provided, nothing will impede for example a prosumer to bid a fraction of its solar-generated power in the market, collect the money at delivery time, but actually use that energy for other activity within its house without injecting the promised one. This problem, also beyond Blockchain grid application like other cyber-physical grid coordination system, is not always attentively addressed even if it is surely a vital and critical aspect. Therefore further research are needed to address such an issue of data-veracity.

An exemplifying solution to this issue is using a dedicated component to perform such actions as Trusted Execution Environments (TEEs) [71], [72]. A different approach is currently being developed by one of the authors. Such a mechanism is now under patent recognition, therefore given the impossibility of sharing specific details, the general idea is to ensure the necessary trust in the transmitted data. A successive article will present such details after patent granting.

Another central issue is the choice of the consensus mechanism. This choice is certainly influenced by the application itself and some characteristics listed above, especially the identity recognition one. Indeed, the usage of a permissioned implementation, recognizing and granting the access to certified identity, allows exploiting mechanisms such as Proof of Authority or Byzantine Fault Tolerance mechanisms [73]. Without discussing which mechanism in specific, surely some main characteristics have to be addressed. First of all, the algorithm should not comprise high energy consumption procedures. Secondly, it should allow for reasonably fast operations. Hence, it should be able to scale to a high number of *transactive-nodes* generating transactions with relative high frequency without risking to compromise the system or loose some transactions due to overloading. Thirdly it should scale to a significant number of consensus nodes to avoid the hegemony of a single institution. Fourthly the infrastructure both in terms of node numbers, and resistance, it should be both Crash and Byzantine fault-tolerant to ensure an adequate level of security as necessary for grid's operations [51].

While networking, identity, consensus, and storage are more concerned to the usage of the Blockchain system itself, the application layer will embed the main business logic and rules recognized to the coordination system. Overall, it will be the platform's component on which to perform transactions for coordinating interactions within the underlying physical system. Therefore the programming language itself should be expressive enough for this task. The approbation of smart contracts should be a multi-party procedure, allowing the approval and agreement of the main regulatory and governance institution, while it should not be limited to a single decisional figure. The method used for running smart contract could be of different types, e.g., running on a virtual machine executing smart contract code, or using Docker containerization for contracts' code; nevertheless, the method itself should be flexible enough to allow a differentiation of trust constraints between the consensus mechanism and the business logic processes, hence platform related issues against smart contract execution layer [14].

At storage level, instead, the necessary feature could be comprised of the capability of substantially record all meaningful information in a representative way, without the need of sacrificing vital information due to constraints of any sort. Additionally, regarding privacy, the possibility of limit ledger maintenance tasks within a specific group of recognized actors could help in keep privacy-related information secure and filter queries without providing sensitive information of participating nodes. Nevertheless, the compliance of GDPR regulations, especially rules like the right to be forgotten, could critically influence and complex Blockchain application [53], especially considering their immutability and transparency features. Therefore, specific mechanisms, like private data collection or private storage between selected nodes, or more complex solutions should protect or shade sensitive information. More research is yet to be done in this field of applicability of Blockchain technology and GDPR compliance [53], especially within the electric grid infrastructure.

Another great challenge is the integration of the necessary technological components with resource-constrained devices currently used within the grid system [68]. The objective is to try not to strongly impact cost or even allow for the use of the currently employed devices without expensive updates. Such features imply modularity of the technology employed and restraining computational intensive tasks to identified nodes, while common devices should participate without the implication to sustain intense computation.

V. CONCLUSION

This manuscript introduced Blockchain technology's main features, which make it crucial for the authors in future employment as fundamental tool for advanced applications in the electric sector. In fact, as deeply discussed, the evolving energy landscape represents a context in need of solutions for a digital energy transition towards the paradigm of distributed systems. Blockchain technology seems to properly comply with such a necessity.

Indeed, the ICT technologies penetration in the power sector will crucially support a general transformation of the old central model with well-defined actors on the offer or demand side. The point is that the simple consumer goods market logic starts to clash with new players (prosumers) and technology (e.g., storage, EVs, HVAC, etc.) asking to be integrated into the strategic complex infrastructure now arising, while consumers might require more direct involvement.

Hence, in this light, the authors analyzed Blockchain characteristics that put the technology in the position to properly support its application in this context. The analysis has to take into account not only network infrastructure and protocols, but also consensus mechanism, participant identity, and technical requirements as key aspects to understand its applicability in the considered domain. IoT and advanced metering devices employed in the energy system will further support the future development of such a visionary application as already proven at a laboratory scale.

Thus the paper aimed to propose a particular Blockchain structure, framework, and design for defining and ground its applicability as a key enabler to foster an energy transition seeing a high penetration of renewables and towards distributed systems paradigm. The intent is to formalize and use such a framework as a base for future work and better structure discussions. The technology proved itself to have the potential to be applied through ad hoc solutions in different power grid parts, but for the authors it seems reasonable to see the first pilots primarily in the wholesale market to properly manage energy transactions.

REFERENCES

[1] *World Energy Outlook 2018*, IEA, Paris, France, 2018.

[2] J.-H. Teng, S.-H. Liao, and C.-K. Wen, "Design of a fully decentralized controlled electric vehicle charger for mitigating charging impact on power grids," *IEEE Trans. Ind. Appl.*, vol. 53, no. 2, pp. 1497–1505, Mar. 2017.

[3] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, early access, May 11, 2020, doi: 10.1109/JIOT.2020.2993601.

[4] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019, doi: 10.1016/j.rser.2018.10.014.

[5] M. Caramanis, E. Ntakou, W. W. Hogan, A. Chakrabortty, and J. Schoene, "Co-optimization of power and reserves in dynamic T&D power markets with nondispatchable renewable generation and distributed energy resources," *Proc. IEEE*, vol. 104, no. 4, pp. 807–836, Apr. 2016.

[6] P. Joskow and J. Tirole, "Retail electricity competition," *RAND J. Econ.*, vol. 37, no. 4, pp. 799–815, 2006. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1756-2171.2006.tb00058.x, doi: 10.1111/j.1756-2171.2006.tb00058.x.

[7] *Digitalization & Energy*, IEA, Paris, France, 2017.

[8] C. Kalalas, L. Thrybom, and J. Alonso-Zarate, "Cellular communications for smart grid neighborhood area networks: A survey," *IEEE Access*, vol. 4, pp. 1469–1493, 2016.

[9] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renew. Sustain. Energy Rev.*, vol. 57, pp. 302–318, May 2016, doi: 10.1016/j.rser.2015.12.114.

[10] J. A. Stankovic, "A perspective on distributed computer systems," *IEEE Trans. Comput.*, vols. C–33, no. 12, pp. 1102–1115, Dec. 1984.

[11] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement. (OSDI)*. New Orleans, LA, USA: USENIX Association, 1999, pp. 173–186.

[12] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[13] J. Chen and S. Micali, "Algorand," 2016, *arXiv:1607.01341*. [Online]. Available: http://arxiv.org/abs/1607.01341

[14] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15.

[15] S. Popov. (2015). *The Tangle*. [Online]. Available: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

[16] Cosmos. (2020). *What is Cosmos?* [Online]. Available: https://cosmos.network/intro

[17] 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, 2nd Quart., 2020. [Online]. Available: https://arxiv.org/pdf/1904.04098.pdf

[18] 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.

[19] L. Lamport, "Time, clocks, and the ordering of events in a distributed system," *Commun. ACM*, vol. 21, no. 7, pp. 558–565, Jul. 1978.

[20] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, White Paper EIP-150 REVISION, 2014, pp. 1–32. [Online]. Available: https://arxiv.org/abs/arXiv:1011.1669v3, doi: 10.1017/CBO9781107415324.004.

[21] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[22] M. W. Alford, J. P. Ansart, G. Hommel, L. Lamport, B. Liskov, G. P. Mullery, and F. B. Schneider, *Distributed Systems: Methods and Tools for Specification. An Advanced Course*. Berlin, Germany: Springer-Verlag, 1985.

[23] J. D. Douceur, "The sybil attack," in *Proc. 1st Int. Workshop Peer-Peer Syst. (IPTPS)*, in Lecture Notes in Computer Science, vol. 2429, Jan. 2002. [Online]. Available: https://www.microsoft.com/en-us/research/publication/the-sybil-attack/

[24] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2013. [Online]. Available: http://arxiv.org/abs/1311.0243

[25] A. D. Kshemkalyani and M. Singhal, "Consensus and agreement algorithms," in *Distributed Computing: Principles, Algorithms, and Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2008, pp. 510–566.

[26] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *J. ACM*, vol. 32, no. 2, pp. 374–382, Apr. 1985.

[27] Bitcoin Wiki. (2018). *Lightweight Node*. [Online]. Available: https://en.bitcoin.it/wiki/Lightweight_node

[28] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, Sep. 1997. [Online]. Available: https://journals.uic.edu/ojs/index.php/fm/article/view/548, doi: 10.5210/fm.v2i9.548.

[29] M. L. Di Silvestre, S. Favuzza, E. Riva Sanseverino, and G. Zizzo, "How decarbonization, digitalization and decentralization are changing key power infrastructures," *Renew. Sustain. Energy Rev.*, vol. 93, pp. 483–498, Oct. 2018, doi: 10.1016/j.rser.2018.05.068.

[30] IPCC. (2018). *Global Warming of 1.5°C*. [Online]. Available: https://www.ipcc.ch/sr15/

[31] R. Jones, B. Haley, G. Kwok, J. Hargreaves, and J. Williams, "Electrification and the future of electricity markets: Transitioning to a low-carbon energy system," *IEEE Power Energy Mag.*, vol. 16, no. 4, pp. 79–89, Jul. 2018.

[32] J. M. Carrasco, L. G. Franquelo, J. T. Bialasiewicz, M. A. M. Prats, J. I. Leon, E. Galvan, R. C. PortilloGuisado, and N. Moreno-Alfonso, "Power-electronic systems for the grid integration of renewable energy sources: A survey," *IEEE Trans. Ind. Electron.*, vol. 53, no. 4, pp. 1002–1016, Jun. 2006.

[33] N. Sujitha and S. Krithiga, "RES based EV battery charging system: A review," *Renew. Sustain. Energy Rev.*, vol. 75, pp. 978–988, Aug. 2017.

[34] N. Liu, X. Yu, C. Wang, C. Li, L. Ma, and J. Lei, "Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3569–3583, Sep. 2017.

[35] S. Xia, S. Bu, C. Wan, X. Lu, K. W. Chan, and B. Zhou, "A fully distributed hierarchical control framework for coordinated operation of DERs in active distribution power networks," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 5184–5197, Nov. 2019.

[36] E. Munsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *Proc. IEEE Conf. Control Technol. Appl. (CCTA)*, Aug. 2017, pp. 2164–2171.

[37] L. Kristov, P. De Martini, and J. D. Taft, "A tale of two visions: Designing a decentralized transactive electric system," *IEEE Power Energy Mag.*, vol. 14, no. 3, pp. 63–69, May 2016.

[38] W. W. Hogan, "Market design practices: Which ones are best? [In my view]," *IEEE Power Energy Mag.*, vol. 17, no. 1, pp. 100–104, Jan. 2019.

[39] S. Benedettini, "The Italian electricity retail market: A critical overview of the recent monitoring report by the national regulatory authority," ISPI, Milan, Italy, 2015. [Online]. Available: https://www.ispionline.it/en/energy-watch/italian-electricity-retail-market-critical-overview-recent-monitoring-report-national-regulatory-authority-12649

[40] S. Borenstein, "Time-varying retail electricity prices: Theory and practice," in *Electricity Deregulation: Choices and Challenges*. Chicago, IL, USA: Univ. of Chicago Press, doi: 10.7208/chicago/9780226308586.003.0009.

[41] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.

[42] I.-M. Moreno-Garcia, A. Moreno-Munoz, F. Domingo-Perez, V. Pallares-Lopez, R.-J. Real-Calvo, and I. Santiago-Chiquero, "Implementation of a smart grid inverter through embedded systems," *Electron. Electr. Eng.*, vol. 19, no. 3, pp. 3–6, Mar. 2013.

[43] G. Li, H. Wang, S. Zhang, J. Xin, and H. Liu, "Recurrent neural networks based photovoltaic power forecasting approach," *Energies*, vol. 12, no. 13, p. 2538, Jul. 2019.

[44] J. Hu, H. Morais, T. Sousa, and M. Lind, "Electric vehicle fleet management in smart grids: A review of services, optimization and control aspects," *Renew. Sustain. Energy Rev.*, vol. 56, pp. 1207–1226, Apr. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032115013970

[45] A. R. Bhatti, Z. Salam, M. J. B. A. Aziz, K. P. Yee, and R. H. Ashique, "Electric vehicles charging using photovoltaic: Status and technological review," *Renew. Sustain. Energy Rev.*, vol. 54, pp. 34–47, Feb. 2016, doi: 10.1016/j.rser.2015.09.091.

[46] J. Taft and P. De Martini, "Scalability, resilience, and complexity management in laminar control of ultra-large scale systems," CISCO, San Jose, CA, USA, Tech. Rep. 715939, 2014. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/connected-grid-network-management-system/scalability_and_resilience_in_laminar_control_networks.pdf

[47] T. Strasser, F. Andren, J. Kathan, C. Cecati, C. Buccella, P. Siano, P. Leitao, G. Zhabelova, V. Vyatkin, P. Vrba, and V. Marik, "A review of architectures and concepts for intelligence in future electric energy systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2424–2438, Apr. 2015.

[48] J. Y. Tsao, E. F. Schubert, R. Fouquet, and M. Lave, "The electrification of energy: Long-term trends and opportunities," *MRS Energy Sustainability*, vol. 5, pp. 1–14, Jun. 2018, doi: 10.1557/mre.2018.6.

[49] D. R. Bohi and K. L. Palmer, "The efficiency of wholesale vs. Retail competition in electricity," *Electr. J.*, vol. 9, no. 8, pp. 12–20, Oct. 1996.

[50] M. Iansiti and K. R. Lakhani. (2017). *The Truth About Blockchain*. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain

[51] *IEEE Guide For Smart Grid Interoperability of Energy Technology and Information Technology Operation With the Electric Power System (Eps), End-Use Applications, and Loads*, IEEE Standard 2030-2011, Sep. 2011, pp. 1–126.

[52] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 2, p. 162, Jan. 2018. [Online]. Available: http://www.mendeley.com/research/blockchain-based-decentralized-management-demand-response-programs-smart-energy-grids

[53] EUBlockchain. (2018). *Blockchain and the GDPR*. [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

[54] J. Mather. (2019). *The Energy Blockchain—Believe the Hype, Just Don't Forget the Physics*. [Online]. Available: https://berc.berkeley.edu/news/energy-blockchain-%E2%80%93-believe-hype-just-don%E2%80%99t-forget-physics

[55] C. Burger, A. Kuhlmann, P. R. Richard, and J. Weinmann, "Blockchain in the energy transition. A survey among decision-makers in the German energy industry," German Energy Agency, Berlin, Germany, 2016, p. 41. [Online]. Available: https://esmt.berlin/sites/main/files/2019-08/dena_esmt_studie_blockchain_english.pdf

[56] S. Jeong, N.-N. Dao, Y. Lee, C. Lee, and S. Cho, "Blockchain based billing system for electric vehicle and charging station," in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2018, pp. 308–310.

[57] A. Baggio, G. Bonet, A. Sharma, and Y. Xie. (2019). *EnerDatX*. [Online]. Available: https://github.com/Guillembonet/EDMP/blob/devel/EnerDatX.pdf

[58] T. Gorski, J. Bednarski, and Z. Chaczko, "Blockchain-based renewable energy exchange management system," in *Proc. 26th Int. Conf. Syst. Eng. (ICSEng)*, Dec. 2018, pp. 1–6.

[59] C. Liu, K. Chai, X. Zhang, E. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[60] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The brooklyn microgrid," *Appl. Energy*, vol. 210, pp. 870–880, Jan. 2018, doi: 10.1016/j.apenergy.2017.06.054.

[61] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, Feb. 2018.

[62] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, vol. 195, pp. 234–246, Jun. 2017.

[63] K. Tanaka, K. Nagakubo, and R. Abe, "Blockchain-based electricity trading with digitalgrid router," in *Proc. IEEE Int. Conf. Consum. Electron.-Taiwan (ICCE-TW)*, Jun. 2017, pp. 201–202.

[64] M. L. Di Silvestre, P. Gallo, J. M. Guerrero, R. Musca, E. R. Sanseverino, G. Sciumè, J. C. Vásquez, and G. Zizzo, "Blockchain for power systems: Current trends and future applications," *Renew. Sustain. Energy Rev.*, vol. 119, Mar. 2020, Art. no. 109585.

[65] J. Coignard, E. Munsing, J. MacDonald, and J. Mather, "Co-simulation framework for blockchain based market designs and grid simulations," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[66] K. Ioannis, G. Raimondo, G. Dimitrios, D. G. Rosanna, K. Georgios, S. Gary, N. Ricardo, and N.-F. Igor, "Blockchain in energy communities," JRC, Eur. Commission, Ispra, Italy, Tech. Rep. JRC110298, 2017. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC110298/del.344003.v09%281%29.pdf, doi: 10.2760/121912.

[67] A. Pitì, G. Verticale, C. Rottondi, A. Capone, and L. L. Schiavo, "The role of smart meters in enabling real-time energy services for households: The Italian case," *Energies*, vol. 10, no. 2, p. 199, Feb. 2017.

[68] M. Emmanuel and R. Rayudu, "Communication technologies for smart grid applications: A survey," *J. Netw. Comput. Appl.*, vol. 74, pp. 133–148, Oct. 2016, doi: 10.1016/j.jnca.2016.08.012.

[69] Business Wire. (2020). *As California Heatwave Extends Into the End of this Week, PG&E Urges Customers to Continue Conserving Energy Through the Afternoon and Evening Hours*. [Online]. Available: https://www.businesswire.com/news/home/20200820005562/en/California-Heatwave-Extends-Week-PGE-Urges-Customers

[70] Hyperledger. (2020). *Hyperledger-Fabricdocs Master Documentation*. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/whatis.html

[71] S. Woo, J. Song, and S. Park, "A distributed oracle using intel SGX for blockchain-based IoT applications," *Sensors*, vol. 20, no. 9, p. 2725, May 2020.

[72] Chainlink. (2018). *Enterprise Smart Contracts: Trusted Computation Framework & Chainlink*. [Online]. Available: https://blog.chain.link/driving-demand-for-enterprise-smart-contracts-using-the-trusted-computation-framework-and-attested-oracles-via-chainlink/

[73] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform," in *Proc. 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.* Piscataway, NJ, USA: Institute Electrical Electronics Engineers, Jul. 2018, pp. 51–58.

ALVISE BAGGIO (Member, IEEE) was born in Padua, Italy, in 1995. He received the B.S. degree in aerospace engineering and the M.S. degree (Hons.) in energy engineering from the Politecnico di Milano. He was a Research-Developer with ABB Solar Smart Energy Laboratories. He is currently an Alumnus of the Milan Polytechnic Honours Programme, one of his university's high-level training courses. Here, he focused on applying innovative ICT to photovoltaic inverters; specifically, he implemented a first prototype of a Blockchain-based coordination platform for energy devices intending to allow more complex forms of energy exchange methodologies. Parallelly, he has taken part in academic and research experiences at an international level. In particular, he completed a period of study at TU Delft. Then, he collaborated at the IT University of Copenhagen for a research and development project in partnership with the JRC's European laboratories aiming to develop IT methodologies for the governance of complex systems. He is also the winner of a fully granted research position at the Department of Electrical Engineering, Politecnico di Milano. His research interests include energy economics, electric power markets, the digitalization of electric grids, and innovative coordination and market schemes.

FRANCESCO GRIMACCIA (Senior Member, IEEE) received the M.S. and Ph.D. *(cum laude)* degrees in electrical engineering from the Politecnico di Milano, Milan, Italy, in 2003 and 2007. In 2018, he was a Full Professor in electrical engineering by the Ministry of Research and Education. He is currently with the Energy Department, Politecnico di Milano. He has been active in different projects in ICT, energy, and aeronautics fields funded by the Seventh Framework Programme of European Commission and SESAR-Joint Undertaking. He has authored more than 130 publications among international journal, book chapters, and conference proceedings. His current research interests include artificial intelligence, wireless sensor networks, sensor technology and hybrid evolutionary optimization techniques, and remote systems and relative digital application in different engineering fields, such as the unmanned systems, monitoring, and control of renewable plants, and other energy systems.

Prof. Grimaccia is a member of the IEEE Computational Intelligence Society and the Vice-President of the AEIT, Milan Section.