IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 May 2022, accepted 30 August 2022, date of publication 8 September 2022, date of current version 26 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3205121

RESEARCH ARTICLE

A Coexistence Analysis of Blockchain, SCADA Systems, and OpenADR for Energy Services Provision

ALESSANDRO AUGELLO, PIERLUIGI GALLO, ELEONORA RIVA SANSEVERINO, GIUSEPPE SCIUMÈ, AND MARCO TORNATORE

Department of Engineering, University of Palermo, 90128 Palermo, Italy

Corresponding author: Giuseppe Sciumè (giuseppe.sciume01@unipa.it)

This work was supported by the Research Project BloRin–Blockchain for decentralized management of renewables, Piano Operativo Fondo Europeo Sviluppo Regionale [Operational Program European Regional Development Fund (PO FESR)] Sicilia 2014/2020–Action 1.1.5-identification code: SI_1_23074, Codice Unico Progetto [Unique project code (CUP)], under Grant G79J18000680007.

ABSTRACT The advent of blockchain technology allows the raise of new business models for the electricity market, opening the way also to end-users and letting them offer regulation services to the power grid. Thanks to the characteristic of being distributed, the blockchain technology could be a solution to balancing problems caused by the penetration of renewable sources, implementing a platform for Demand-Response programs delivery. Demand-Response allows consumers to respond to market signals by increasing or reducing their energy consumption, contributing to greater flexibility and stability of the grid and to a more efficient use of infrastructures and energy resources. Currently, Demand-Response is carried out by controlling aggregates of loads, storage or generating units managed by centralized Supervisory Control and Data Acquisition systems such as SCADA. Regulatory changes and the increasing penetration of renewable sources distributed over the territory are turning the whole electricity system into a smart-grid. More recently and with reference to the end-users participation in regulation services, smartness is achieved through the so-called Internet of Things, which can be considered the modern equivalent of SCADA, but with the possibility of to being applied to distributed and diversified assets. For this reason, great efforts have been made to study the interoperability and coexistence between Internet of Things and blockchain, two emerging paradigms that are gaining popularity in the energy world. Limited or no contribution can instead be found in the literature on the integration of SCADA systems and blockchain. Indeed, in order to ensure an easier and faster widespread application of blockchain in the context of power systems, it is interesting to study its possible coexistence with legacy and more established industrial technologies such as OpenADR or SCADA. In Europe, the prevailing technology is the latter one. For this reason, in this paper, the coexistence of blockchain technology with SCADA systems is discussed. In particular, both Hyperledger Fabric blockchain and SCADA systems are considered together to assess the feasibility of aggregation of energy resources for Demand-Response, as well as the relevant measured data. The analysis is carried out by first presenting the two different paradigms: the centralized data acquisition in trusted environments and analysis via OpenADR and SCADA, and the global, distributed and secured ones with the blockchain. Then an architecture for the integration of SCADA and blockchain technology is proposed and the related challenges within the frame of a project for innovative technologies DR programs implementation are outlined.

INDEX TERMS Blockchain, communication protocol, distributed energy services, industrial applications, OpenADR, SCADA, smart grids.

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

I. INTRODUCTION

With the advent of the Internet of Things (IoT) and various edge devices, the power grid, such as other systems, has

gone through a significant transformation. Meanwhile, a new paradigm, called the Smart-Grid (SG), has emerged combining Information and Communication Technology (ICT) with conventional power generation, transmission, and distribution. The SGs are power networks capable of monitoring and controlling the bidirectional energy flows in real time, providing all stakeholders in the electricity supply chain a global view over both the energy flows and the infrastructure that carries them. A SG can predict power demands and suitably adapt them to non dispatchable generation and, through appropriate management and control systems, a SG can address several problems of conventional networks such as reducing energy consumption, reducing risks of short circuits, etc… [1]. In SGs, through Demand-Response (DR) techniques, it is possible to regulate the power flows in the hours in which the grid is mostly overloaded. By integrating recent technologies such as blockchain, machine learning and big data analytic with SGs, it is possible to predict customers' electricity demand and efficiently automate for example DR services [2].

Real-time monitoring and control play an important role in the management and operation of SGs. With the rapid increase of the number of *Prosumers* (users who are not just energy consumers but also producers), many functions of the SGs, including regulation and energy production, are distributed. Therefore, SGs management problems can no longer be efficiently addressed under a centralized environment, but they rather need decentralized approaches and architectures. In addition, variations in energy production, whether in excess or deficit, can threaten the security of energy supply, overload existing networks and result in service interruptions. Such variations are mostly due to the unpredictable nature of the renewable energy sources (RES). By integrating different heterogeneous technologies for data collection and processing, SGs can mitigate the effects of RES on the grid operation security by controlling dispatchable energy resources. In power systems, local monitoring and control have been traditionally performed via SCADA (supervisory control and data acquisition) systems, while the last decade has been characterized by a transition towards the Internet of Things (IoT) paradigm, which allows various equipment and devices to be connected in a distributed way over the Internet to data analytics systems. IoT technology covers all the tools, systems, sensors, both hardware and software for supporting the deployment of applications and IoT devices. By means of IoT technology, common objects in a house can be made smart thus enabling the implementation of smart homes. In the definition of IoT technologies also security tools are included thus preventing internet-based attacks.

As end-users have become central actors in power systems, IoT has also become a technology to consider and suitably integrate in SGs management. Such as in other applications, also in SGs, IoT includes the use of wireless devices such as sensors, radio modules, gateways and routers. Figure 1 shows an example of IoT devices integration in the power system that also makes use of SG technology. These devices provide

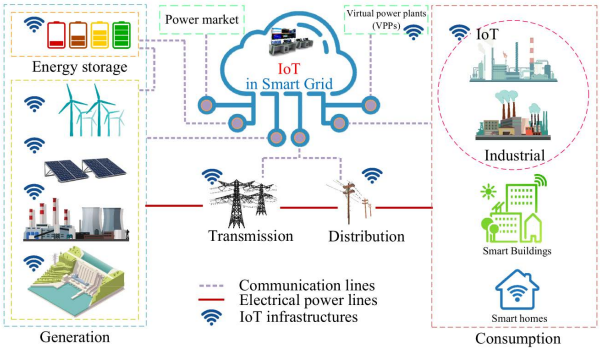

FIGURE 1. IoT integration in power systems [3].

greater connectivity of power system components allowing different stakeholders to make better decisions about power use, storage or generation, and enabling power system operators to more quickly restore service after a fault. In addition, progress in technology has made wireless technology cheap and easy to use in SG applications. The use of IoT in SGs allows the power system to be constantly monitored in more details than it was previously possible and to interact with the system components.

The use of IoT devices in SGs enables, for example, better prediction and response to load fluctuations or to promptly act on substations in order to automatically manage power flows in the event of a fault. With SG technology, energy can be automatically redirected as soon as a fault occurs, while minimizing the effects on users. IoT sensors can also report equipment conditions and help with predictive maintenance. The use of IoT devices in SGs would also support the tracing, monitoring and management of distributed small power generation by making the power system more robust. Smart meters can help in efficient billing service implementation and in data collection for demand forecasting. On the other hand, the limited processing resources of IoT devices, such as smart meters, hinder the adoption of conventional security measures such as asymmetric encryption mechanisms. In addition, the inherent characteristics of IoT lead to a number of challenges, such as decentralization, poor interoperability, privacy and security vulnerabilities. New information technologies such as blockchain enable the IoT challenges to be effectively addressed. In this context, the Paper [4] analyzes these challenges and proposes an architecture in which blockchain plays as a middleware between IoT and industrial applications, offering a set of services to support various industrial applications by overcoming the inherent problems of IoT devices. Whereas, the paper in [5] presents a comprehensive survey of existing blockchain protocols for IoT, provides an overview of the application domains of blockchain technologies in IoT, and classifies the threat models considered by blockchain protocols in IoT networks into five main categories: identity-based attacks, manipulation-based attacks, cryptanalytic attacks, reputation-based attacks, and service-based attacks. In [6], the authors examine blockchain-based security and privacy

systems for seventeen types of IoT applications and various consensus algorithms in terms of latency, throughput, computational cost, etc. Finally, they classify security analysis techniques in order to stable the main steps to be followed to build and evaluate blockchain-based security and privacy systems. Other works, on the other hand, address the topic of security of Smart Contracts (SCs), which are widely used in blockchain applications, in IoT. For example, [7] and [8] discuss the opportunities and challenges, while [9] explore the vulnerabilities and attacks in smart contracts, which can affect the stability of the IoT ecosystem and presents the main solutions to address these security issues.

The huge amount of data generated by various interconnections of IoT devices in a SG makes it more difficult to establish proper rules and policies for access control. This trend towards distributed and decentralized models is confirmed by the recent regulation about energy districts, energy communities, and virtual aggregates of different energy resources. The switch from centralized to distributed generation and control opens the door to cybersecurity threats and requires new trust models. The distributed model exposes the electrical system to novel attacks, which aim, primarily, at compromising the availability of data and, secondarily, their integrity and confidentiality. For example, various types of *Denial of Service* attacks can disrupt the network functionality, with disastrous consequences such as blackouts, *False Data Injection* attacks can compromise smart meter data, while *Man-in-the-Middle* attacks can compromise data privacy. Novel trust models where prosumers are peers that do not trust each other, call for the use of emerging technologies. However, such technologies pose a lot of questions about their feasibility to handle many industrial applications. In particular, energy services trading and tracing appear quite suitable for blockchain applications [10], [11], [12], [13]. However in these cases, security is critical since energy assets are of great interest for governments and industrial compounds, while energy consumption are sensitive data. For this reason, SG technology, although relying for communication on several protocols, reviews attentively the security issue [14].

A. MOTIVATION AND CHALLENGES IN THE IMPLEMENTATION OF DISTRIBUTED ENERGY SERVICES

This paper is motivated by the recent advancements in distributed systems in the energy sector, which contrasts with the lack of innovation in data acquisition and control mechanisms, where SCADA has dominated for several decades. SCADA is still widely used despite a modern approach proposing to switch to the Internet of Things (IIoT, Industrial IoT for energy production). The IoT revolution appears like an evolution where this new paradigm enhances SCADA instead of substituting it. The research question is thus whether a wide adoption of the blockchain in the energy sector would require completing the switch from SCADA to IoT. This paper tries to answer this question, analysing the interoperability and coexistence between blockchain, IoT and legacy SCADA systems to answer this question. Using the blockchain disruptive technology on top of a well-consolidated one (as SCADA) appears to be an evolutionary approach that benefits the IoT transition and the diffusion of protocols such as OpenADR.

In this paper, a DR and aggregation system based on SCADA client-server architecture is considered for integration with a blockchain system implementing DR management and aggregation functions. The blockchain architecture presented here does not involve the need for a third party market actor called *aggregator* [15] between the grid operator requiring the service and the end users providing the service by modulating the demand. We propose to use the blockchain as a tool for aggregating data and implementing policies set by different actors, thus truly disintermediating the business model. However, in many cases, the aggregator is a market actor defined by the law. In this case, we propose it keeps administrative and verification roles, while transferring the technical aggregation actions to the blockchain. In the current scenario across Europe, the aggregator intermediates between the end-users and the Transmission System Operator (TSO) and, therefore, it is useful to analyse communication messages flowing through the links ''TSO/aggregator'' and ''aggregator/end-users''. The two links are constrained by the time in which the load modulation must be carried out, the first link is more tightly constrained also in terms of privacy and thus underlying TLC technology.

The main goal of this paper is to assess the interoperability of the client-server systems typically used for DR programs and the blockchain technology. The analysis further checks if their peculiar heterogeneous features can coexist, in terms of reliability, throughput, timing, and security, within a unified architecture. In addition, the system architecture proposed in this paper solves the challenges of current DR platforms.:

- enables the secure aggregation of small users;
- increases transparency in the remuneration of DR events;
- improves information asymmetry;
- ensures data security;

At the same time, the proposed approach overcomes the listed challenges of blockchain platforms for DR, as:

- it is compliant with the General Data Protection Regulation through the use of an authorized blockchain platform;
- it is scalable and enables end-user participation in real-time markets due to the lighter consensus algorithms of the permissioned blockchain;
- it is easily integrated with existing IoT devices.

The paper is organized as follows. In Section II, the most common protocol to exchange information and signals in DR contexts is described. Section III explains the Italian model for DR, with a focus on the Italian grid code and Terna's (the Italian Transmission System Operator) technical specifications. Then, in Section IV there is a description of the SCADA system; section V introduces the operation and features of the blockchain technology. After that, Section VI focuses on the integration of blockchain in SGs and the experimental

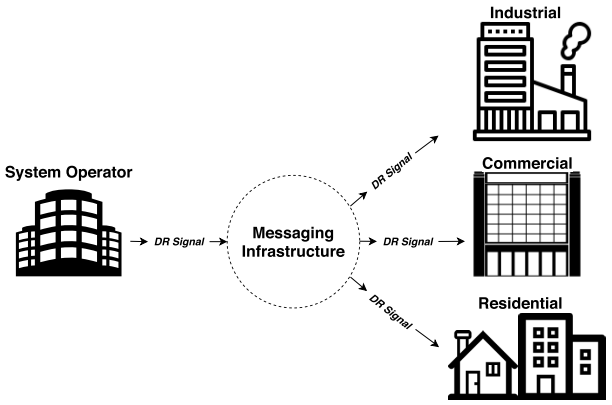

FIGURE 2. General DR messaging architecture.

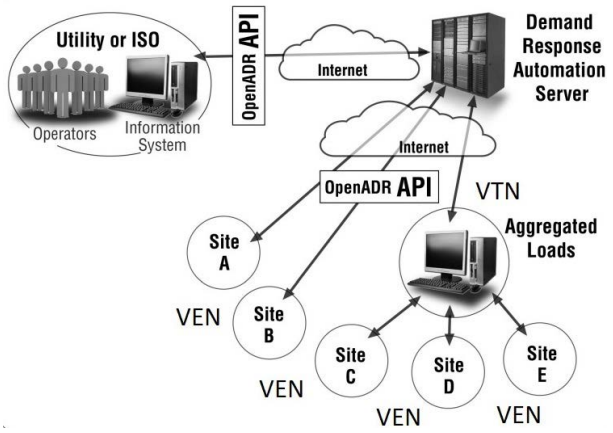

FIGURE 3. General openADR communication architecture.

setup of BloRin project, where the technical specifications described in section III are implemented.

II. OPEN AUTOMATIC DR

DR is an important tool that helps to maintain the correct operation of the electrical system due to RES penetration, as it allows to adapt the energy demand to the supply in a short time. During peak periods and in response to market signals, prosumers can modulate production and consumption for obtaining financial incentives. In any case, the participation of prosumers in DR programs requires that their facilities are connected.

IoT technologies support distributed generation, such as residential photovoltaic panels and electrical storage systems, allowing users to implement more efficient actions and, when possible, supporting the solution of balancing problems in distribution and transmission networks. Traditionally, DR systems use a classical client–server service architecture, where a server keeps the links with industrial, commercial or residential customers for collecting measurements and issuing control signals. Figure 2 shows a general architecture, where the System Operator through a client-server messaging infrastructure is able to exchange information and DR signals with the customers.

The most applied protocol to exchange information and signals in DR contexts is the Open Automatic DR, OpenADR [16]. It is a text-based open access client-server protocol that extends HTTP and uses Public key cryptography for security, based on IEC 62746-10-1 technical specification. The IEC 62746-10-1 [17], developed by the OpenADR Alliance in 2018, specifies a minimum data model and services for DR event, pricing, and distributed energy resource communications for managing customer energy resources, including load, generation, and storage, via signals provided by network and/or market operators. These resources can be identified and managed as individual resources with specific capabilities or as virtual resources with an aggregate set of capabilities. OpenADR works well both in push and pull. A pull client connects to the server and requests data; a push client connects to the server and waits for data that are sent by the server. Also, the OpenADR protocol is open, anyone can implement it, and uses Extensible Messaging and Presence Protocol (XMPP) as a transport protocol. OpenADR supports many services and allows the implementation of several applications, such as peer-to-peer sessions, user lists, group messaging, notification, encryption and authentication. The fundamental feature of XMPP is the ''transport'': the possibility, through appropriate gateways on the Internet, to interconnect different services. With XMPP on the client it is not necessary to have software for each type of service, but it is enough that gateways exist for that service. This feature makes the XMPP protocol ideal for push and fast DR applications, while pull is also possible. OpenADR supports continuous transmission of DR signals to customers, giving them constant visibility of wholesale prices and helps to better balance supply and demand. The advantages are to facilitate a timely and predictable response for the system operator, while allowing the customer's choices. OpenADR creates a common language, the ADR 2.0 protocol, to communicate a DR event over an IP-based network, such as the Internet. Many energy providers, in several states of USA, parts of Europe, China, Japan, Australia, and Korea support OpenADR and allow system operators to call DR events. OpenADR works by having pre-programmed Application Programming Interfaces (API) that provide two-way communications between the service provider (Utility/Independent System Operator (ISO)/Aggregator) and customers (Sites) through a logical interface of the Demand Response Automation Server (DRAS), see Fig. 3.

Service providers initiate a DR event through the Demand Response Automation Server (DRAS). The DRAS is responsible for communicating specific details about the event, such as duration, start time and price signals to the end-user devices. The DR signal communication is always carried out through two main actors, the VTN (Virtual Top Node) and the VEN (Virtual End Node). A VTN controls many VENs and is responsible for transmitting event specifications, such as price, and programming signals. The VENs may utilize HTTP or XMPP, while both of the protocols are mandatory

for a VTN. Hence, the OpenADR standard event communication process is a push-pull action between the VTN and the VENs. Aggregators, or balancing service providers that sell their modulated loads in the wholesale market, can be either the top node or an end node, depending on whether they also own facilities or are just a third-party company providing the service. The customers are the VENs that provide the demand reduction/increase to the aggregators. Examples of messages conveyed via OpenADR from VTN to VEN include:

- PRICE_ABSOLUTE: the price per kilowatt-hour.
- PRICE_RELATIVE: a change in the price per kilowatt-hour.
- PRICE_MULTIPLE: a multiple of a basic rate per kilowatt-hour.
- LOAD_AMOUNT: a fixed amount of load to shift.
- LOAD_PERCENTAGE: the percentage of load to shift.

A VEN can be integrated into the hardware of the on-site energy management system, or as a separate hardware device to pass signals directly to the end devices or building control system. The OpenADR protocol allows to obtain high speed in response from customers, enabling the possibility of participating in ancillary services such as frequency regulation. It also allows to choose the devices on which to act according to the signals received. But, the client-ssystem architecture, although efficient, suffers from the weaknesses of centralized systems, such as low scalability, the presence of a trusted third party (the aggregator) and the presence of centralized element (the DRAS or the VTN). In fact, the failure of a VTN leads to the failure of the connected VENs and consequently the non-participation of users in the DR event.

In Italy, DR is managed through SCADA systems, with a client-server architecture as for OpenADR, but with a different protocol for information exchange. This model is described in the next section.

III. ITALIAN MODEL FOR DR

Today in Italy, DR programs engaging all categories of end-users are still in a pilot phase. They are expected to allow residential, commercial and industrial users to help with electricity regulation by participating in the Dispatching Services Market (MSD). With Resolution 300/2017/R/EEL of the ARERA (the Italian energy Authority), and under a pilot experimentation, Terna opened the MSD for the first time to virtual aggregations of small power plants with non-programmable production, loads and storage systems (UVAMs). Currently, UVAMs represent the benchmark form of aggregation in Italy. UVAMs allow users to provide flexibility by modulating consumption or production through DR programs. Managed by Balancing Service Providers (BSPs), UVAMs offer capacity to the MSD and are remunerated on the basis of the variation of the exchanged energy derived on the MSD (€/MWh) plus a fixed amount (in €/MW/year) that is proportional to the offered capacity and awarded by auction.

According to the UVAM MSD Regulation by Terna [18], UVAMs can provide the following dispatching services:

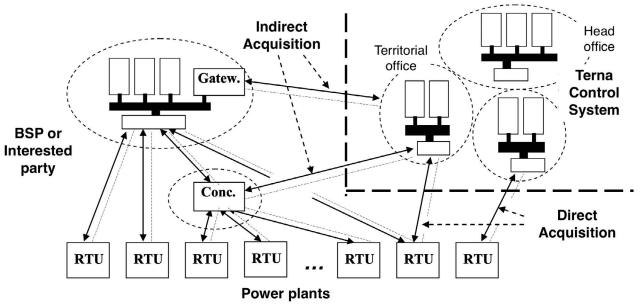

FIGURE 4. Connection models to Terna's control center.

1) resolution of congestion, increasing and/or decreasing;
2) rotating tertiary reserve, increasing and/or decreasing;
3) tertiary replacement reserve, increasing and/or decreasing;
4) balancing, increasing and/or decreasing;

UVAMs provide the services indicated above if they are able to modulate loads with the following features:

- within **15 minutes** of receipt of Terna's dispatching order for the services referred to in points 1), 2), 4);
- within **120 minutes** from the receipt of Terna's dispatching order for the services referred to in point 3);

and support such modulation for a period at least equal to:

- 120 minutes for the services referred to in letters 1), 2), 4);
- 480 minutes for the services referred to in letter 3);

In addition, the BSP interfacing with Terna systems must be able to send every 4 seconds the voltage, the frequency and the total power input/output at the input/output points included in the UVAM [19]. Annex A13 of the Grid Code, which establishes the criteria for connection to the Terna control system, also states that data exchange must be performed using the file transfer mode provided by the IEC 60870-5-104 protocol and through a private communication network between the BSP and the TSO's access point, with an approximate latency of 50msec Round Trip Time (RTT) with a minimum payload of 300 bytes [20]. The same annex then establishes the connection modes allowed with the Terna control system, which are:

- Direct acquisition: where the data exchange takes place through direct connections between the Remote Terminal Units (RTUs) and the Terna control system.
- Indirect acquisition: where the BSP or other interested party concentrates the information relating to several plants at a single collecting point and sends it to Terna through Concentrators or Gateways.

The following figure 4 shows these possible connection models.

IV. SCADA SYSTEMS

SCADA systems are commonly used for monitoring and controlling automatic power transmission and distribution procedures. They mainly consist of:

1) a Master Terminal Unit (MTU);
2) a human-machine interface (HMI);

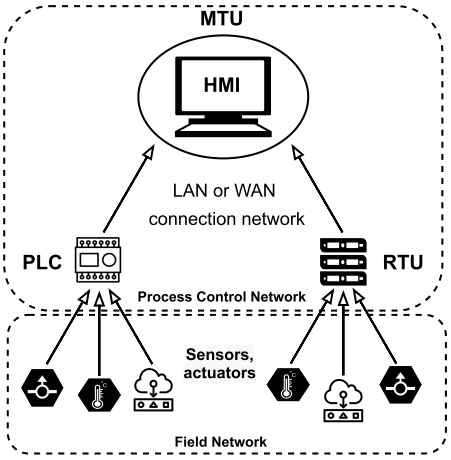

FIGURE 5. General SCADA architecture.

3) logic controllers;
4) communication interfaces;
5) sensors.

The MTU is a server that communicates with the logic controllers, which in turn monitors the field environment by detecting and preventing possible anomalies and fault states. Examples of logic controllers are Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). Communication interfaces enable the exchange of data between MTUs and logic controllers, while the HMI, installed in the MTU, is used by the system operator to transmit and receive data from the controllers, while the sensors send data to the logic controllers. Figure 5 shows a simple SCADA architecture.

These components allow to perform supervision/control and data acquisition for the management of industrial processes. These two activities are performed through two separate networks, the *field network* that consists of physical components such as sensors, actuators, etc…and the *process control network* that enables the connection through TCP/IP protocol between the various components of the SCADA system (database, RTUs, human-machine interfaces, etc…). In both cases, the physical layer for communication can be implemented through twisted pairs, optical fiber, radio, etc…TCP/IP specifies how data is exchanged over the Internet by providing end-to-end communications. It specifies how data is to be divided into packets, addressed, transmitted, routed and received at its destination. TCP/IP requires minimal central management and is designed to make networks secure with the ability to automatically recover if any device on the network fails. TCP defines how applications can create communication channels through a network and also manages how a message is assembled into smaller packets before they are then transmitted over the Internet and reassembled in the correct order at the destination address. IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network controls this IP address to determine where to forward the message. There are many communication standards used for the SCADA systems operation, but the one used by Terna for the management and operation of DR services is based on the IEC 60870-5-104 standard. In the field of electrical engineering and power plant automation, the international standard IEC 60870 defines supervisory and remote control systems for production, transport and distribution networks and other geographically distributed service networks. This standard allows interoperability between devices from different manufacturers and is divided into six parts that define general information, operating conditions, electrical interfaces, performance requirements and standard transmission protocols.

Section 5 of IEC 60870 (IEC 60870-5) [21] provides a communication profile for sending basic messages for remote control between two systems using directly connected circuits. The IEC 60870-5-10x protocols define which messages and values should be sent spontaneously from a logic controller to a control server after any change. After establishing the connection, the server sends a request to the controller in order to obtain the status of the variables. The controller checks these states and sends data only if changes have occurred. The IEC 60870-5-104 standard (also called IEC-104) derives from the better known IEC-101, both having the same level of application, therefore the same reference data structure. The difference between the two protocols is that IEC 104 uses the TCP/IP standard that gives more flexibility and better performance but from which it unfortunately inherits several vulnerabilities. While the IEC-101 uses serial communication, so suitable only for basic remote control tasks. In addition to the weaknesses of TCP/IP, a major security problem of IEC-104 is that application level data is transmitted without encryption mechanisms, so it is possible to perform traffic analysis and launch *Man-in-the-Middle* [22] attacks. In addition, many commands in this protocol, such as *reset*, *query* or *read*, do not implement essential security mechanisms such as authentication and access control. This vulnerability is crucial, as a cyber attacker can access the control of PLCs and possibly the overall operation of an automated substation, thus generating disastrous consequences. The use of SCADA systems and the IEC-104 standard for DR management allows for a high speed of response from customers and lets them choose which devices to act on based on the signals received. The high speed of response also allows ancillary services such as secondary frequency regulation to be supported. This service can only be achieved through real-time signaling because it requires a fast response, often two to four seconds. On the other hand, the SCADA architecture, although efficient, suffers from the weaknesses of classic client-server systems, such as low scalability or the presence of centralized elements. In fact, the failure of an MTU leads to the failure of the connected RTUs and consequently to the non-participation of users in the DR event. These and other problems can be overcome through the use of distributed technologies such as blockchain. In the following sections, the blockchain technology and its use for DR is addressed.

V. BLOCKCHAIN AS TECHNOLOGY FOR SGs

In the concept of SGs, data from sensors are very important for application decision making and therefore need to be securely protected. Currently, the SCADA system provides a centralized data collection and storage mechanism that is vulnerable to cyber attacks. Moreover, in a centralized approach, the availability and reliability of the system can be compromised due to errors or attacks to a single node [23]. However, the decentralized SG system with a large number of components and connections may improve redundancy, resiliency, security, privacy, and trust [24]. Blockchain is a promising alternative to conventional centralized systems to improve security, privacy, and trust while helping the migration to a more decentralized and resilient system. In blockchain, a failure of one node would not cause damage to the whole network as, by means of the consensus mechanism, transactions have to be validated by the other nodes in the network. The main features of this technology [25] such as decentralization, register immutability, transparency, transaction traceability, and security based on cryptographic techniques, promise to realize many applications in energy systems. In [26] for example, a Blockchain-based distributed information collection and storage mechanism has been designed to securely manage sensor data. Smart grid performance depends not only on the advancement of power equipment, but also on monitoring, analysis, optimization and control technologies that can involve all participants. Blockchain provides monitor, control and manage complex power systems in a decentralized way, providing new opportunities for building decentralized systems. In the blockchain, no central authority is required for trust; instead, multiple entities in the network can interact with each other to create, maintain, and store a distributed ledger. Each entity can verify that the order of the chain and the data has not been tampered with. This structure makes any system redundant and resilient to failures and cyber attacks, solving many of the problems existing in centralized systems. The blockchain is also promoting secure, privacy-preserving and reliable smart grid developments towards decentralization. The work in [10] outlines the potential of blockchain and notable use cases in energy applications, such as energy trading, microgrids and power grids, etc. A survey on the potential benefits of blockchain for the smart energy system is presented in [27], where some projects and related blockchain platforms are showcased. A more recent survey [28], aims to analyze the applicability of blockchain technology in future SGs, which would facilitate a seamless decentralization process. In addition, the work elaborates on blockchain-based applications of future SG operations and the role of blockchain in each scenario.

In the SG system, blockchain also offers new opportunities to monitor, measure and control, although it is necessary to choose appropriate platforms and consensus protocols that are not resource-intensive. There are many studies aimed at testing blockchain in the context of SG, in [29] a new efficient consensus mechanism (PoRCH) for private blockchain suitable to be implemented in SCADA systems is introduced. The paper proposes a new consensus mechanism and presents a simplified demo by including a customized mining node selection procedure for a data acquisition system in a private blockchain where no incentives or penalties are required for validators. The performance evaluation shows that the entire process requires very low computational capacity while preserving data security, privacy, and trust. A security architecture integrating blockchain and Software-Defined Network (SDN) technologies is tested in [30]. The proposed security architecture consists of: (a) an intrusion detection system, to defend against hacked commands, which target the industrial control process, and (b) a Blockchain-based integrity control system (BICS), which can prevent the attack on routing, which would compromise the OpenFlow rules of SDN-enabled industrial IoT systems. The results demonstrate the effectiveness and efficiency of this security solution. Although the blockchain introduced in SGs adds significant advantages, it also has drawbacks that can be solved with the integration of other technologies by reinforcing future SGs.

As already introduced, SGs are power networks that can monitor, analyze and control power flows and energy demand according to market and user needs, using two-way power and information flows. For a stable and cost-effective operation of the grid, consumption and production should be balanced, but as is well known this does not always happen and can cause failures or increases in the price of energy. One of the most cheap solutions to operate the power grid addressing this problem is the implementation of DR programs, scheduling user loads as a result of requests from grid operators in exchange for a reward. The increase of number of consumers and especially small and locally distributed producers leads to the need for a decentralized, secure and open power grid that allows for reliable and fast transactions. Using the blockchain, DR programs can be executed directly between the grid operator and the users, unlike the current scenario where the aggregator mediates between the user and the grid operator. The blockchain allows the grid operator to send the load reduction/increase request directly to the users distributed over the network, who will respond accordingly. The transaction is not a direct exchange of energy between two parties, but a request to provide a service, where users will then be paid if they respond appropriately. Today, one of the main problems in DR service provision is the lack of transparency between the different parties involved, but through the blockchain it is possible to manage this problem. In addition, blockchain allows small prosumers to participate in capacity and balancing markets by aggregating them into virtual load units that can be managed as needed. Several works approaching DR service using blockchain can be found in the literature. The authors in [31] propose a blockchain platform for storing information about the energy use and generation of active/passive users of a microgrid thanks to SCs executed on the Ethereum blockchain that evaluate the flexibility of each prosumer, the associated remuneration or penalty, and the rules for the energy balance in the considered microgrid. In [32], a blockchain platform for managing the

aggregate load of a SG through DR events is described. Miner nodes, which are responsible for transaction authentication, are selected based on their energy consumption and computing power. The proposed scheme is light in terms of communication and computation costs, and the obtained results demonstrate the efficiency of the platform for secure demand response management in the SG. The work in [33] shows a secure energy and data exchange system in order to provide DR service among the users of a SG. The data is generated by smart meters and stored and processed through a blockchain-based energy trading system. The results show shorter execution times compared to traditional centralized architecture for DR while ensuring privacy, transparency and security. In [34] the authors applied blockchain technology for securely tracking DR, focusing on validation, data integrity and origin, and sharing of data among stakeholders on an permissioned network. The feasibility and performance were evaluated on an experimental SG. Results showed transaction execution times of less than 1s and high scalability, enabling real-world deployment of this technology for DR. In this context, the BloRin research project [35] aims to create a blockchain-based platform for renewable energy deployment and energy service management. Unlike the aforementioned platforms, BloRin aims at an integration of current systems used for load aggregation into a unified architecture where blockchain technology enables overcoming the problems of centralized systems. This platform will help the creation and deployment of solar Smart Communities and will be able to aggregate small and medium/large prosumers to provide DR services. In the next section, the BloRin platform for DR event execution and user aggregation is presented with the aim of showing the strengths as compared to the aforementioned centralized systems and time compatibility.

VI. BLOCKCHAIN BASED DR PLATFORM AND AGGREGATION

The advent of blockchain in the energy sector is well compatible with the trend of decentralized generation through the widespread deployment of PV systems, other distributed generators, and IoT devices in generation systems. Due to the high penetration of renewables in the power network, grid operators are currently dealing with several issues, such as the need for new ancillary services from distributed units, the supervision and coordination of said processes, and the aggregation of local resources for participation in capacity and balancing markets to respond to power fluctuations due to the high penetration of renewables. The use of blockchain technology allows the aggregation of end-users without the need for third parties, as for example currently occurs in Italy with UVAM, enabling the implementation of new methods for the management of these issues. Using blockchain, DR programs can be executed directly between the network operator and users, involving small prosumers in capacity and balancing markets by aggregating them into virtual load units that can be managed as needed.

We suggest to use the blockchain technology for managing aggregation: because of the traceability feature supported by the blockchain, users can register their willingness to participate to DR programs on the blockchain, this permits to asynchronously aggregate participants to DR events giving visibility of their willingness. The registrations of requests can be written in blocks that are immutable and ordered in time. However, the utility of aggregation refers to the energy data detected by the smart meters that communicate with the ICT infrastructure. This data, taken individually, has certainly an intrinsic value, but speaking for example of energy transactions, it is clear that the participation in ancillary services for the network or the self-production of energy of a single user, is subject to the importance that this action takes within the electrical system. We can therefore say that thanks to blockchain technology the individual user data can be recorded by the infrastructure and can be aggregated with other similar data in a vertical logic that will create a flexible power offer of adequate size, making comparable the network's side demand and consumers' side offer. Therefore, the blockchain aggregation is twofold: on one hand it aggregates the prosumers' willingness to participate to programs, on the other hand it aggregates and validates metering data provided by smart meters and EMSs in the smart grids.

A. THE BloRin BLOCKCHAIN PLATFORM

The BloRin project aims to develop a system able to aggregate end-users for the distributed provision of Demand-Response (DR) and Vehicle-to-Grid (V2G) services with the aim of contributing to the management of demand volatility and especially the production from renewables. In fact, through DR programs it is possible to address these issues by increasing the flexibility of the power system while keeping costs relatively low and facilitating the integration of renewable energy without the need for power grid expansion. The BloRin network includes the islands of Lampedusa and Favignana and the power grid of the University of Palermo. Lampedusa and Favignana will allow to evaluate the effectiveness of blockchain for DR and V2G management in small isolated networks, while the university's network will be used for preliminary tests. The currently deployed network includes 7 blockchain nodes running on the physical nodes hosted by the project partners, as shown in figure 6.

The component that interfaces the measurement and control units to the blockchain is the SNOCU, an independent proprietary device produced by Regalgrid [36] that allows to connect pure generation or storage resources to the platform that enables different energy services. Instead, for the management of consumption profiles of households is used an Energy Management System (EMS, developed at the University of Palermo) able to interact both with the blockchain and with smart plugs connected to shiftable loads. The BloRin platform is *permissioned*, which means that users enroll in the platform through a trusted provider. As a result, transaction validation and network security do not need "proof of work" algorithms to ensure trust between users, while avoiding unknown identities from accessing the platform. Among other innovations, this project offers several

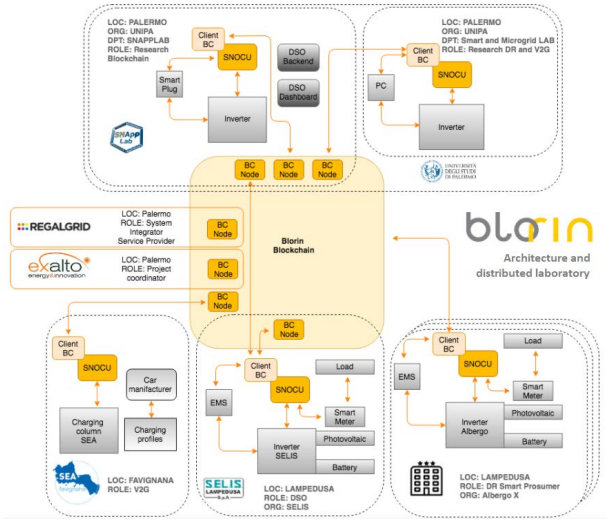

FIGURE 6. BloRin network architecture.

mechanisms and tools that can be combined allowing easy integration with existing technologies. The blockchain used is Hyperledger Fabric, a *permissioned* platform that allows participants to access and manage their transactions through purpose-developed SCs, which can also be used to validate data [37]. Thanks to its modular, configurable, and versatile architecture, Hyperledger Fabric enables the development of applications across multiple use cases. Being a *permissioned* network, participants are not anonymous. For this reason, the network can only function with a governance model built in such a way that trust is guaranteed between participants previously authorized by the trusted provider. The members of a Hyperledger Fabric network are registered through a Membership Service Provider (MSP), this does not allow unknown identities to participate and therefore there is no need to use computationally expensive consensus protocols such as PoW to validate transactions and secure the network [38]). As a result, there are no transaction costs associated with mining transactions as with *permissioless* blockchains. The elementary network consists of five components:

1) a Peer;
2) a SC;
3) a ledger copy;
4) an App client;
5) ad Ordere.

The Peer is the main element that maintains a copy of the ledger and hosts and executes the SC to write and read data from the ledger. Members of the blockchain can choose to own a peer or interact with other members' peers. The interaction with peers is performed thanks to the App client, external to the blockchain network and owned by each member. The App client is needed both to communicate with peers and interact with the ledger and to display results following a query or ''transaction proposal''. Each time a user sends a transaction proposal to the network, this is processed by the SC of the peer that received it. If the response to the proposal is consistent with the logic implemented by the SC, the new transaction is sent to all peers participating in the network who verify its authenticity through their copy of the SC. The App client of the user who submitted the transaction proposal compares the proposal responses of all peers to determine if they are the same. If the majority is the same, it proceeds to the next step by sending the transaction to the Orderer who is the component responsible for the consensus process. The transaction message will contain the transaction data and the signatures of the peers. The Orderer does not need to inspect the entire contents of a transaction to perform its operation, it simply receives the transactions, sorts them chronologically and creates the transaction blocks. This creates a method for rejecting erroneous transactions that have been sent to the network by mistake (or maliciously). The consensus mechanisms implemented by the Orderer do not require a native cryptocurrency to incentivize costly mining or power the execution of SCs. Avoiding the use of a cryptocurrency to operate the platform reduces the risk of attacks and, in the absence of mining operations, power consumption is also greatly reduced. The absence of cryptographic mining operations allows the platform to be deployed at the same operational cost as any other distributed system. The combination of these features makes Fabric a very high-performance platform in terms of transaction processing and transaction confirmation latency, and ensures privacy among users and confidentiality of transactions. The execution time of the SC depends on the function being called. For BloRin applications, with a network consisting of 5 nodes (1 in Favignana, 1 in Lampedusa and 3 at the University of Palermo) times between 0.13 s (for a query) and 15 s (baseline computation) have been estimated, resulting in a new block generation between 30 and 60 s. While regarding memory consumption, it was estimated that the size in bytes of a transaction ranges from 5 kB to 13 kB, so a block composed of 10 transactions has a size slightly higher than 130 kB.

Fabric is also the first platform to support SCs written in generic programming languages such as Java, Go and Node.js, rather than specific programming languages such as Ethereum's Solidity. They function as a trusted distributed application that acquires its security/trust from the blockchain and consensus mechanism. In a Hyperledger Fabric network, the SC, that is installed on each node, represents the fundamental element of the network, because it is the component that implements the logic of any transaction and verifies the integrity of each transaction sent by the network users before joining a new blockchain. The BloRin platform aims to address the challenges arising from the increasing uncertainty in energy balancing due to the growing contribution of renewable sources and the increasing penetration of electric mobility. The platform is proposed as a useful tool for the evolution of the electricity market in a direction that involves more and more end-users on the regional, national and international scenario.

B. THE BloRin BLOCKCHAIN FOR DEMAND-RESPONSE

On the island of Lampedusa, the BloRin platform will be used for the implementation of the DR service by aggregating in virtual units simple consumers or prosumers living in the

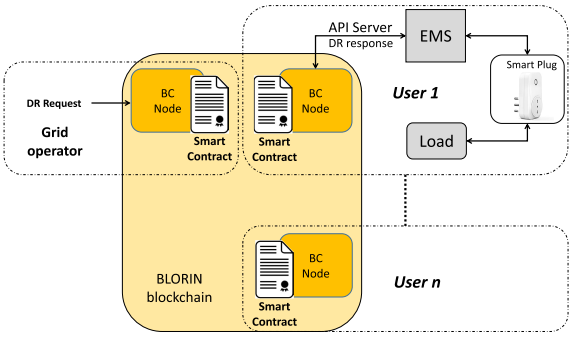

FIGURE 7. Load control and monitoring via BloRin blockchain platform.

island. In general, the control and monitoring of flexible loads is implemented and recorded through the BloRin platform. The platform interfaces with the household and their loads through an Infrastructure consisting of an EMS connected to smart plugs and an internet connection. While for users with PV production system with and without storage, the platform interfaces with users through SNOCUs for system and storage management and eventually through EMS and smart plugs for load management. The EMS is the system that allows the monitoring and control of the loads of the passive domestic user; it is installed directly in the user's home in a special switchboard and consists of a data processing controller, a smart meter and a protection switch. The controller works as a personal computer, inside which a blockchain client is implemented; in fact, it allows communication with the BloRin platform, receives from the blockchain the DR requests and provides it with the power data used for the calculation of the Baseline and the quantification of the service provided by the user (push and pull client), see figure 7.

The EMS itself is connected with the various smart plugs installed in the residence, which are equipped with a communication and control system capable of receiving on or off signals and sending their status to the device. This approach also makes the intervention on the user's electrical system non-invasive, since, to make the system operational, it is sufficient to install the switchboard in which the EMS is present and connect the smart plugs to the classic sockets of the house.

The implementation of the DR event logic is performed through a purpose-developed SC, which also establishes the roles of the various actors on the BloRin network. In this case, the actors involved will be the DSO and the users who decide to join the service by providing their flexible loads or production/ storage systems. The figure 8 describes the flowchart for the execution of a DR event.

The meters record the load or production profiles of the users which through the EMS or SNOCU are sent to the blockchain. The DSO notifies the DR event on the blockchain with the purpose of increasing the efficiency of the power plant or mitigating any expected problems in a given hour due to production from renewables while users. The SC evaluates the baseline of users participating in the service and distributes the DSO request. Through the EMS/SNOCU, users will be able to automatically respond to the request by turning off some loads or managing generation/storage

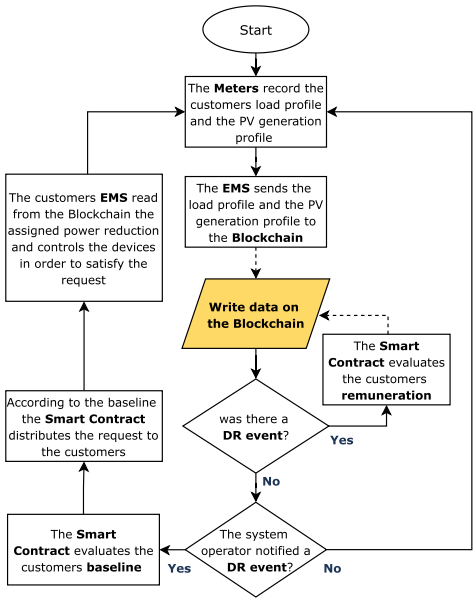

FIGURE 8. BloRin DR flowchart.

during the hours when the DR event is expected. From this moment, it is the EMS/SNOCU that takes control, as only these devices know the status of the various household loads or the production system, and consequently decide which of them can turn on, turn off or modulate in order to meet the request received from the Blockchain. Through the smart meter, the user's consumption/production data is sent to the blockchain at regular intervals; this is necessary to certify, and therefore consequently remunerate, the load modulation service put in place by the user. In fact, the methodology used to establish whether the user has satisfied the DR request consists in comparing the user's Baseline with the load profile measured on the day in which the DR event occurs.

Unlike the traditional system where the execution of the DR event is started by the grid operator and reported to the end-users through the aggregator, with the BloRin platform the grid operator interacts directly with the end-users. It is the blockchain that acts as an intermediary and aggregator with the capabilities, through the SC, to share the request, verify the response of users and remunerate them according to the provided contribution, in a totally transparent and trusted way.

In the next section, a unified architecture is proposed that integrates the client-server systems seen for DR with the BloRin blockchain network, with the aim of demonstrating their possible coexistence by overcoming the issues that afflict centralized systems.

VII. UNIFIED ARCHITECTURE FOR DR SERVICE PROVISION

The blockchain technology allows the aggregation of users in a transparent way and without the need for a trusted entity as BSP or an aggregator, thus generating a loads aggregation able to provide flexibility to the power network. To find an intyegration between SCADA systems and blockchain, it is needed to clarify that while the blockchain acts at the level of application, the SCADA protocols includes several ISO/OSI

layers. Therefore for the integration it is sufficient to pass from the blockchain application layer the data to the transport layer. Data will use the format typical of SCADA protocols, but the way in which they are trasnferred to other nodes is not Master-slave, but rather P2P. The blockchain works as a distributed DRAS where the DR logic is run trasparently by smart contracts. To check the technical feasibility of the provided architecture, it remains to check whether the Hyperledger Fabric blockchain platform can accomplish all the requirements imposed by Terna's grid code for load aggregation. Before going into these details, it is necessary to identify the similar points and differences between a simple traditional SCADA system for DR and an integrated SCADA-blockchain system.

In general a SCADA system consists of two separate networks, the field network that includes the sensors connected to the various RTUs and the process control network that includes the connection of RTUs to MTUs (see Fig. 5). Generally in the field network the devices (sensors, actuators, etc…) communicate with the RTUs through radio or optical fiber, while in the process control network, RTUs and MTUs communicate through an intranet with TCP/IP protocol. The same arrangement is also found in the OpenADR architecture and in a blockchain network with two separate networks. In the case of OpenADR, the Internet connects the VTN to the VENs and a virtual private network (VPN) connects the VTN to the DRAS. In the case of the blockchain, similarly, the Internet connects household loads or energy systems to the EMS and the Virtual Private Network connects the EMS to the blockchain nodes.

The network connecting the DRAS with VTNs can be considered the analogue of the process control network of SCADA systems, since it is this part that implements the energy services logic, implements the control logic and manages and processes the data obtained from the VENs. The same consideration can be made between Blockchain nodes and EMSs. The difference with the process control network of SCADA and OpenADR systems is that the architecture is distributed and trust on data integrity is achieved through the consensus mechanism. Similarly, the VENs are connected to the VTN and the end-devices of the blockchain architecture are connected to the EMS through a network that can be considered as a field network. The figure 9 shows the comparison among the three systems.

An important difference is how messages are propagated over the network. In the centralized client-server SCADA architecture or OpenADR, the service provider initiates a DR event by communicating with an MTU (DRAS in OpenADR) through specific APIs. After that, the signal is transmitted to all RTUs connected to that MTU. Thus, the event communication process is a push-pull action between the MTU and the RTUs. In these systems, the signal transmission logic allows for high response rates, but suffers from the inherent problems of centralized systems, such as the need for a trusted third party, one single point of failure, low scalability, high hardware cost and possibility of congestion on the network.

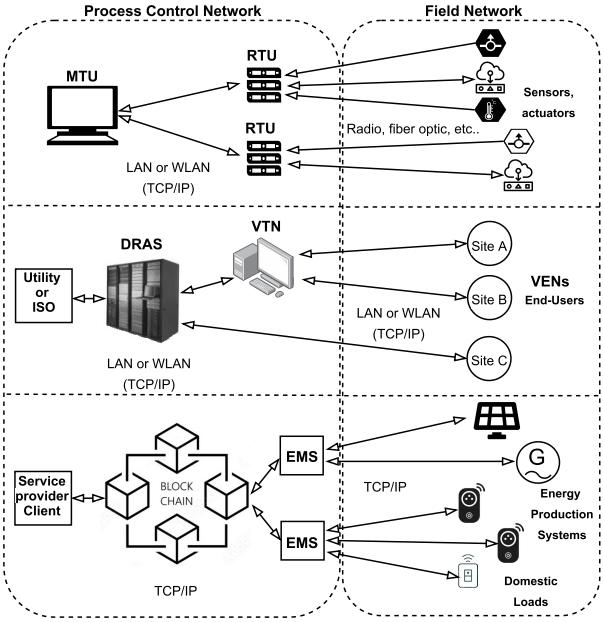

FIGURE 9. SCADA, OpenADR and blockchain architecture comparison.

While using a blockchain network, when the service provider sends a DR request, the latter goes through consensus mechanisms before becoming part of the network and being used by EMS to command loads. In this case, it is not the MTU/DRAS that processes the request distribution logic, but the SC running on the blockchain. Messages dissemination can be schematized with the following next steps:

1) The service provider sends the DR request, through its client, to the blockchain.
2) The SC processes the request and distributes it among the various users participating in the network.
3) Through the consensus mechanism both the DR event communicated by the service provider and the distribution of the request are recorded on the blockchain.
4) EMSs receive the request assigned to them and process load management logic to satisfy it.
5) The users' response is recorded by the meters and sent by the EMSs to the blockchain.
6) The SC evaluates the contribution provided by each user who participated in the event.
7) Through the consensus mechanism the results of the event are recorded on the blockchain.

The messages dissemination process is more complex than in client-server systems because of the greater number of network elements involved and the consensus mechanism needed to ensure trust on the exchanged data. But the use of *permissioned* blockchain, such as Hyperledger Fabric, allows for fast consensus on data by employing low computational power.

In addition, the use of blockchain enables decentralized business and technical models. By distributing the computational load among several nodes, each hardware resource is under less stress, allowing each node to be more efficient. The system can continue to work even if one of the nodes fails, and by operating across a number of different machines,

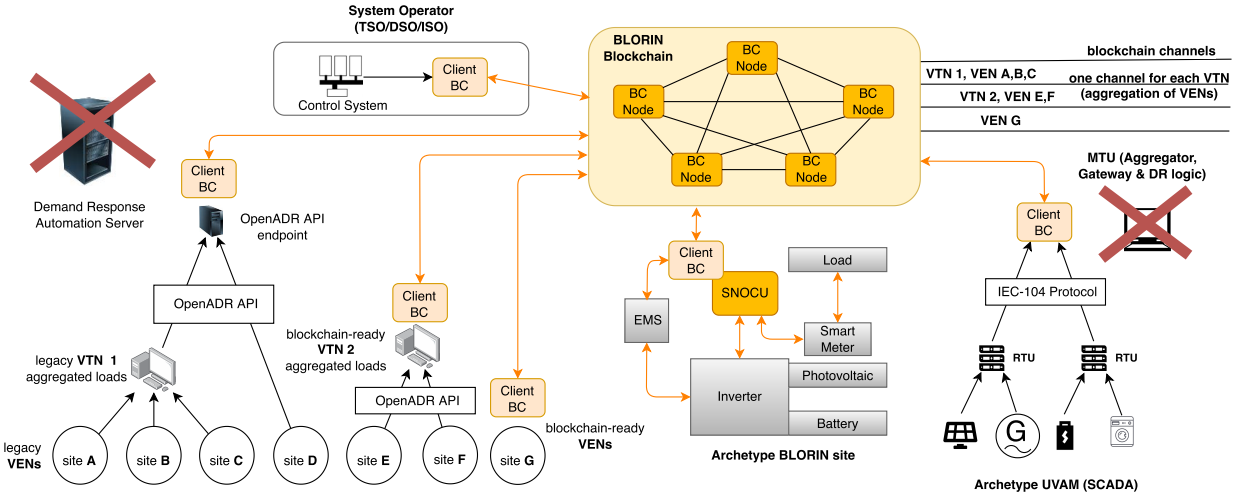

FIGURE 10. Joint use of blockchain, OpenADR and SCADA in the BloRin blockchain network.

it is inherently scalable. In this case, the blockchain acts as a DRAS in OpenADR and as a concentrator of distributed energy resources in the indirect connection model envisioned by Terna for UVAM where RTUs are comparable by EMSs which communicate with IoT devices such as smart plugs or directly with small energy production systems.

Figure 10 shows the unified architecture integrating the OpenADR and the UVAM models based on SCADA with the BloRin blockchain network.

Several architectural components take different roles in this integrated ecosystem. From left to right, the figure shows three different archetypal blocks; all can interoperate with each other. On the left, there is the integration between blockchain and OpenADR; in the middle, the self-explaining BloRin blockchain-native approach; on the right, it reports the integration with SCADA. The OpenADR integration can work with three possible options: at the level of DRAS, VTN or VEN. The leftmost part of the figure reports the integration at the DRAS level, which is substituted by a blockchain client and an endpoint for OpenADR API. One or more smart contracts provide the traditional functionalities of the DRAS, as they are able to elaborate the DR logic and interact with both VTNs and VENs. The API endpoint for OpenADR is integrated with a blockchain client that directly writes transactions. All the elements in the OpenADR tree below each client trust each other as they belong to the same administrative unit. This trust consideration holds in all three cases: when the client is at the DRAS level (left three), at the VTN level (central three) or the VEN level (the single node on the right). The integration with SCADA requests a blockchain client that works as an MTU aggregation gateway that uses the IEC-104 protocol to monitor and enforce control commands to RTUs.

The proposed model provides a system capable of interacting with the technologies currently used for DR and eliminate the elements of centralization, allowing to overcome the problems of such systems, but ensuring at the same time security, traceability, data certification and privacy. In fact, by using separate communication channels, data related to an aggregate of users is only accessible to the users of that aggregate and the system operator.

TABLE 1. UVAM and BloRin platform requirements comparison.

	UVAM	BloRin
Data exchange protocol	IEC-104	Configurable
Communication network	Private	Private
Network latency	max 50 msec RTT	50 msec RTT
Minimum payload	300 bytes	300 bytes
Connection mode	Direct, indirect	Indirect
Electrical parameters acquisition time	4 s	from 1s to 15 min

As already said, currently in the world, DR is performed by aggregating different users in virtual units managed by an aggregator through client-server systems, which are connected to the control system of the grid operator according to specific rules. In Italy, DR is managed by Terna, which establishes the rules and methods of connection to its control centers. The table 1 shows on one side the requirements that a UVAM must meet to be connected to Terna's management and control center and on the other side that these requirements are also met by the BloRin platform.

Regarding the IEC 60870-5-104 protocol imposed by Terna for data exchange, the blockchain can become compliant by integrating the support of this protocol into the clients.

Experimental tests conducted on the BloRin platform show that the execution times of the main functions of the SC (2.3 seconds to 12 seconds for a write operation and 0.065 seconds in a read operation) are compliant with the times required by Terna (4 seconds for the acquisition of electrical parameters and 15 minutes of notice for a DR request). The timing of the proposed blockchain platform are compatible with the needs of balancing services on the MSD. Even better when the DR signal is handled by an EMS for automatizing user's response.

VIII. CONCLUSION

DR service is an important resource for addressing problems on the power grid due to RES penetration. Demand and production peaks management as well as the load shifting reduce

occurrences and consequences of congestion on the grid. They also contribute to the reduction of GHG emissions and stabilize energy prices. Such positive effects can be obtained by a joint application of IoT and blockchain for a decentralized application of sensing, decision making and control within smart grids. However, in many cases, legacy SCADA systems are deployed instead of IoT platforms, which led us towards an interoperability analysis between blockchain and SCADA. This study encourages to open the door to distributed systems for data handling also for those industrial platforms that are still based on SCADA, thus improving their scalability and transparency, with limited investments in new hardware. The use of blockchain technology for managing, tracking, and certifying DR services enables the creation of a distributed system where even residential customers, who account for an average of one-third of a country's consumption, can communicate with the system operator. The blockchain opportunistically aggregates their flexibility, in a secure, scalable, transparent, and traceable manner. This paper presented the possible coexistence of blockchain and SCADA and, through the results obtained from the BloRin experimental tests, verifies that specific blockchain platforms meet the requirements imposed by system operators and encourages to revamp SCADA-based infrastructures.

ACKNOWLEDGMENT

The authors wish to thank the SNAPP and the SMG Laboratories at the Department of Engineering, University of Palermo.

REFERENCES

[1] A. Alirezazadeh, M. Rashidinejad, A. Abdollahi, P. Afzali, and A. Bakhshai, "A new flexible model for generation scheduling in a smart grid," *Energy*, vol. 191, Jan. 2020, Art. no. 116438. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360544219321334

[2] S. M. S. Siddiquee, B. Howard, D. T. J. O'Sullivan, and K. Bruton, "Demand response in smart grid—A systematic mapping study," in *Proc. 2nd Int. Conf. Smart Power Internet Energy Syst. (SPIES)*, 2020, pp. 327–332.

[3] H. Shahinzadeh, J. Moradi, G. B. Gharehpetian, H. Nafisi, and M. Abedi, "IoT architecture for smart grids," in *Proc. Int. Conf. Protection Autom. Power Syst. (IPAPS)*, Jan. 2019, pp. 22–30.

[4] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[5] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[6] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17236–17260, Dec. 2021.

[7] G. Schmitt, A. Mladenow, C. Strauss, and M. Schaffhauser-Linzatti, "Smart contracts and Internet of Things: A qualitative content analysis using the technology-organization-environment framework to identify key-determinants," *Proc. Comput. Sci.*, vol. 160, pp. 189–196, Jan. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919316758

[8] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X19316280

[9] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K.-K.-R. Choo, "Security challenges and opportunities for smart contracts in Internet of Things: A survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12004–12020, Aug. 2021.

[10] 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. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1364032118307184

[11] J. Golosova, A. Romanovs, and N. Kunicina, "Review of the blockchain technology in the energy sector," in *Proc. IEEE 7th IEEE Workshop Adv. Inf., Electron. Electr. Eng. (AIEEE)*, Nov. 2019, pp. 1–7.

[12] Y. Baashar, G. Alkawsi, A. A. Alkahtani, W. Hashim, R. A. Razali, and S. K. Tiong, "Toward blockchain technology in the energy environment," *Sustainability*, vol. 13, no. 16, p. 9008, Aug. 2021. [Online]. Available: https://www.mdpi.com/2071-1050/13/16/9008

[13] H. Li, F. Xiao, L. Yin, and F. Wu, "Application of blockchain technology in energy trading: A review," *Frontiers Energy Res.*, vol. 9, p. 130, Apr. 2021. [Online]. Available: https://www.frontiersin.org/article/10.3389/fenrg.2021.671133

[14] M. Kuzlu, M. Pipattanasompom, and S. Rahman, "A comprehensive review of smart grid related standards and protocols," in *Proc. 5th Int. Istanbul Smart Grid Cities Congr. Fair (ICSG)*, Apr. 2017, pp. 12–16.

[15] K. Ponds, A. Arefi, A. Sayigh, and G. Ledwich, "Aggregator of demand response for renewable integration and customer engagement: Strengths, weaknesses, opportunities, and threats," *Energies*, vol. 11, no. 9, p. 2391, Sep. 2018. [Online]. Available: https://www.mdpi.com/1996-1073/11/9/2391

[16] A. Yassine, "Implementation challenges of automatic demand response for households in smart grids," in *Proc. 3rd Int. Conf. Renew. Energies Developing Countries (REDEC)*, Jul. 2016, pp. 1–6, doi: 10.1109/REDEC.2016.7577546.

[17] K. Zīle and R. Strazdiņa, "Blockchain use cases and their feasibility," *Appl. Comput. Syst.*, vol. 23, no. 1, pp. 12–20, May 2018.

[18] Terna. (2020). *Regolamento Recante le Modalitá Per la Creazione, Qualificazione e Gestione di Unità Viegoltuali Abilitate Miste (UVAM) al Mercato dei Servizi di Dispacciamento*. Accessed: Nov. 16, 2020. [Online]. Available: https://download.terna.it/terna/Regolamento-UVAM-MSD-8d803bd91884d36.pd%f

[19] Terna. (2020). *Requisiti Tecnici Minimi Delle Apparecchiature Per la Rilevazione e Comunicazione Delle Misure e Per la Gestione Degli Ordini di Bilanciamento*. Accessed: Nov. 16, 2020. [Online]. Available: https://download.terna.it/terna/Allegato-202-8d803be56f0fd2d.pdf

[20] Terna. (2017). *Criteri di Connessione al Sistgema di Controllo Terna*. Accessed: Dec. 12, 2020. [Online]. Available: https://download.terna.it/terna/0000/0995/38.PDF

[21] G. Clarke, D. Reynders, and E. Wright, *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*. London, U.K.: Newnes, 2004.

[22] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, and E. Panaousis, "Attacking IEC-60870–5–104 SCADA systems," in *Proc. IEEE World Congr. Services (SERVICES)*, Jul. 2019, pp. 41–46.

[23] D. Zhaoyang, L. Fengji, and G. Liang, "Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems," *J. Mod. Power Syst. Clean Energy*, vol. 6, no. 5, pp. 958–967, 2018.

[24] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2886–2927, 3rd Quart., 2019.

[25] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Mar. 2009. [Online]. Available: https://www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System

[26] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.

[27] N. Ul Hassan, C. Yuen, and D. Niyato, "Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions," *IEEE Ind. Electron. Mag.*, vol. 13, no. 4, pp. 106–118, Dec. 2019.

[28] C. Yapa, C. de Alwis, M. Liyanage, and J. Ekanayake, "Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research," *Energy Rep.*, vol. 7, pp. 6530–6564, Nov. 2021.

[29] M. T. Hossain, S. Badsha, and H. Shen, "PoRCH: A novel consensus mechanism for blockchain-enabled future SCADA systems in smart grids and industry 4.0," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Sep. 2020, pp. 1–7.

[30] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, p. 3119, Jul. 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/14/3119

[31] 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.
[32] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "GUARDIAN: Blockchain-based secure demand response management in smart grid system," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 613–624, Jul. 2020.
[33] A. Kumari, R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "When blockchain meets smart grid: Secure energy trading in demand response management," *IEEE Netw.*, vol. 34, no. 5, pp. 299–305, Sep. 2020.
[34] A. Lucas, D. Geneiatakis, Y. Soupionis, I. Nai-Fovino, and E. Kotsakis, "Blockchain technology applied to energy demand response service tracking and data sharing," *Energies*, vol. 14, no. 7, p. 1881, Mar. 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/7/1881
[35] BloRin Consortium. *BloRin*. Accessed: Aug. 29, 2021. [Online]. Available: https://www.blorin.energy/
[36] Regalgrid Europe Srl. *Regalgrid*. Accessed: May 16, 2022. [Online]. Available: https://www.regalgrid.com/en/
[37] E. Androulaki, C. Cachin, C. Ferris, C. Murthy, B. Nguyen, S. Muralidharan, M. Sethi, and C. Stathakopoulou, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 30th EuroSys Conf.*, Apr. 2018, pp. 1–15.
[38] M. Sadek Ferdous, M. Jabed Morshed Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," 2020, *arXiv:2001.07091*.

ALESSANDRO AUGELLO received the bachelor's degree in cybernetics engineering (L8), mechatronics curriculum and the master's degree in electronic engineering (LM29), mechatronics curriculum from the University of Palermo, in 2018 and 2020, respectively. He has been an Grant Holder at the University of Palermo, since December 2020. His research interests include the creation of a platform that allows the management of energy exchanges between different users, using Blockchain technology for the management of energy flows without intermediaries in a traceable, transparent, secure, and intermediary-free way by exploiting automation from the development of smart contracts.

PIERLUIGI GALLO received the graduate degree (Hons.) in electronic engineering in July 2002 and the Ph.D. degree in 2015. He worked at Electronic Research Centre in Sicily (CRES) until 2009. His work there was dedicated to QoS in IP core routers, IPv6 network mobility and wireless networks. Since he joined the University of Palermo, he has given courses of application services over the internet and signal theory. He has been an Assistant Professor with the University of Palermo, since November 2010. His research interests include wireless networks at the MAC layer, 802.11 extensions, localization based on the time of arrival and cross-layer solutions, blockchain technologies and their applications in smart grids, real estate, tracing foods and processes, and e-commerce. He has contributed to several national and European research projects: ITEA- POLLENS (from 2001 to 2003) on a middleware platform for a programmable router; IST ANEMONE (from 2006 to 2008) about IPv6 mobility; IST PANLAB II on the infrastructure implementation for federating testbeds; ICT FLAVIA (from 2010 to 2013) on flexible architecture for virtualizable future wireless internet access, CREW (from 2013 to 2014) on cognitive radio experimentation and software-defined networks. He coordinates the research unit on the "Smart health 2.0" national project, which is focused on e-health and cloud computing applications. He contributed to the WiSHFUL EU project on radio and network control of wireless software and hardware platforms as work package leader. He is the coordinator of more than two ERASMUS projects and with the Posts and Telecommunications Institute of Technology in Hanoi.

ELEONORA RIVA SANSEVERINO received the master's degree in electrical engineering from the University of Palermo, Italy, in 1995, and the Ph.D. degree in electrical engineering, in 2000. She has been an Associate Professor of electrical power systems with the University of Palermo, since 2002, where she is currently a Full Professor, since November 2019. She is a scientific coordinator of various research projects with research organizations and companies. She is also responsible of various research and teaching cooperation agreements with foreign institutions and private companies. These include European institutions Aalborg University (DK), Chalmers University (SE) and extra-European institutions like Electric Power University and the Institute of Energy Science both in Hanoi, Vietnam. She authored more than 250 articles on international journals, edited books and book chapters and conference proceedings. She is the coordinator of the Ph.D. degree in 'Energy' with the University of Palermo. She is the Editor in Chief of the *UNIPA Springer Series*.

GIUSEPPE SCIUMÈ received the bachelor's degree in energy engineering, the master's degree in electrical engineering, and the Ph.D. degree in energy and information technology from the University of Palermo, Italy, in 2014, 2017, and 2021, respectively. Since 2021, he has been a Postdoctoral Researcher with the University of Palermo. His research interests include the use of the Blockchain technology for power systems and the development of systems based on this technology to enable peer-to-peer energy exchange among the final users of the power network or energy services provision without intermediaries in a fast, transparent, traceable and secure way, and the provision of a distributed demand-response service.

MARCO TORNATORE received the bachelor's degree in telecommunications engineering (DM509) and the master's degree in telecommunications engineering (LM27) from the University of Palermo, in 2016 and 2019, respectively. He has been an Grant Holder with the University of Palermo, since July 2020. His research interests include the creation of a platform that allows the management of energy exchanges between different users, using Blockchain technology for the management of energy flows without intermediaries in a traceable, transparent, secure and intermediary-free way by exploiting automation from the development of smart contracts.

Open Access funding provided by 'Università degli Studi di Palermo' within the CRUI CARE Agreement