IoT-Based Decentralized Energy Systems

Marta Biegańska

Institute of Quality Science, Poznań University of Economics and Business, Al. Niepodległości 10, 61-875 Poznań, Poland; marta.bieganska@ue.poznan.pl

Abstract: In traditional energy production at large-scale, conventional methods are being used, including fossil fuels. This in turn leads to greenhouse gas emissions (e.g., carbon dioxide or CO₂) that cause environmental concerns, but also those traditional methods rely on traditional distribution systems, which are burdened with high transmission losses. This paper focuses on a new concept in the energy sector that undergoes transformation from a traditional centralized system to a decentralized one. In reaching sustainability goals, such as net-zero emissions, the energy sector is incorporating renewable energy sources into the energy system. This requires transformation that combines big conventional energy producers with multiple small- and large-scale energy producers (rooftop photovoltaic panels, wind farms and solar plants) in one system. This enormous transformation is a difficult task, but with recent advancements in information and communication technologies, digitalization, the Industry 4.0 paradigm and Internet of Things technology, it is feasible to achieve. This paper provides a review based on keyword bibliometric analysis, and although it cannot be considered exhaustive or conclusive, it provides a picture of the current international research.

Keywords: blockchain; Internet of Things (IoT); fog computing; smart grid (SG); Internet of Energy (IoE); electric vehicles (EV); renewable energy sources (RES); decentralized energy

1. Introduction

The world’s growing population and growing number of electric devices have led to an increase in electricity consumption [1]. Moreover, modern society and economics depend on electricity. Technology innovations that are used in our everyday life are electricity-driven [2]. There is an urgent need to balance the supply–demand of electricity [3,4], especially in the view of sustainability and energy security. The energy sector, which is facing the global trend toward a net-zero emission target, needs to modify energy production behaviors. However, this is not an easy task, and to achieve this, the use of renewable energy sources (RESs) and new power sources are required [3]. Traditional power plants, however, which provide stable electricity supply via the grid, bring inevitable environmental effects [5]. The energy sector is forced to move, nowadays, due to different environmental regulations, towards clean energy. The growing interest in RESs incorporated into an energy distribution system can help in securing the energy supply especially in areas with high electricity demand (e.g., smart cities, smart factories, smart hospitals and smart transport). In addition, RESs compared to traditional fossil fuel energy sources have lower carbon emissions (there are different carbon allowances that undergo trading) [6].

Renewable energy technologies, which are constantly developing and improving, have shifted the role of traditional consumers to prosumers [7]. For example, someone having photovoltaic panels (PVs) can sell their excess energy to the grid provider or other prosumers such as their neighbors [2]. As RESs are cheaper and faster to build than coal or gas generators, there is an increasing number of privately owned generators that join the energy market and are a foundation for a distributed energy system [8]. To sum up, distributed generation is the production of electricity from different small sources [5]. Those
small-scale RESs led to the emergence of the idea of a microgrid (MG). On the other hand, there are also large-scale plants such as wind farms or solar parks [9]. In traditional energy production at large-scale, conventional methods are being used, including fossil fuels. This in turn leads to greenhouse gas emissions (e.g., carbon dioxide or CO$_2$) that cause environmental concerns, but also those traditional methods rely on traditional distribution systems, which are burdened with high transmission losses [7,10].

With more and more things (sensors and actuators) connected to the internet, a new paradigm of the Internet of Things (IoT) has emerged. It is a network of interconnected things and their elements that are able to exchange data with one another over the internet. These include various home appliances, smartphones, smart bands, smartwatches, weather stations and many more, to give an example. IoT is at the forefront of emerging technologies due to the ubiquitous use of sensor-embedded devices [3,11]. IoT enables real-time sensing, actuating, communication and processing in many cases without human intervention. Due to its multiple possibilities, it has been utilized so far in peer-to-peer (P2P) networks, smart homes, smart hospitals, vehicle-to-vehicle (V2V) communication, wearables and smart energy grids [2,11,12]. In present times, the real-time monitoring of an electrical network such as smart grid (SG) is required and can be achieved by means of IoT as it allows for grid automation [3,13].

The energy sector, which is undergoing a transformation from a centralized to a decentralized system, will be the biggest consumer of IoT edge devices, with 1.17 billion in 2019 and 1.37 billion devices in 2020 (26% Greater China, 12% Western Europe and 8% North America) [14]. According to [13], the growth of the smart home market is expected to reach USD 53.45 billion by 2022. The energy sector is integrating operational and information technologies in order to reach the growing demand for energy and legal requirements (a zero emissions target) [15]. Due to the COVID-19 pandemic, the global energy demand has decreased by 6% in 2020 compared to 2019 [16]. However, it will increase up to 30% by 2040 compared to 2017 [17]. Moreover, in 2019, the global renewable capacity reached 2537 GW. It is estimated that in 2050 the global energy demand will be 8% lower than today but will be provided to 2 billion more people [16]. In addition, in 2020 in Finland, the share of RESs has increased to almost 40% [18]. This requires significant investment in order to achieve those sustainability goals. It is estimated that the European Union alone, to transform to a sustainable and reliable energy system, needs to invest a minimum of 200 billion euro and the United States USD 2 trillion by 2030 [9]. Guaranteeing stable energy distribution, especially during peak hours with an increasing number of electricity-driven devices, creates a great challenge for the energy sector. Obtaining this is crucial, as power outages in the US market cost USD 150 billion annually, with equipment failures being responsible for around one third of them [11].

The paper provides a review based on keyword bibliometric analysis and although it cannot be considered exhaustive or conclusive it provides a picture of the current international research. The rest of the paper is formed as follows: Section 2 describes the implementation of the Internet of Things in the energy sector providing opportunities and the limitations it brings. Section 3 contains bibliometric analysis methodology and obtained data analysis. Section 3 takes up the idea of a smart energy grid system. In Section 5, the concept of a smart grid (SG) is presented. Section 6 focuses on smart grid (SG) challenges. In addition, Sections 7 and 8 present the Internet of Energy (IoE) concept and the implementation of blockchain (BC) technology in decentralized energy sector.

2. Internet of Things in the Energy Sector

The Internet of Things (IoT) delivers many novel solutions that can be implemented in the energy sector. IoT is based on smart technologies such as sensors, actuators and intelligent systems that can be integrated and enable digitalization industries (including the energy sector), providing a novel paradigm in business operations. The processing of enormous amount of sensor-generated data are supported by development of information systems such as cloud computing technologies that provide decentralized sharing and
access to information from different geographical locations. The enormous amount of data generated from IoT allows efficient analysis and supports decision making and a quick response to system failures [19–21]. It plays a significant role not only in a digitalized and connected society, but also in industry, healthcare, transportation, etc., and the economy as a whole [22].

It can support the transformation from a conventional energy grid to a modernized smart grid (SG) system. As IoT enables a two-way communication of sensors and devices, it can improve the operation and control in a traditional grid [3,11,13]. IoT, by providing the structure and protocols required for sensing, communication and processing, paves the way for smart energy system with efficient grid automation and control. When sensors and smart metering are implemented in a power grid it becomes a smart grid (SG) with the ability to overcome most electricity industry challenges, such as power generation and distribution. In addition, IoT in a smart grid (SG) allows for the real-time monitoring of power flow and can support decision making in relation to power sources and demand. This in turn can help in balancing supply–demand and elevating energy efficiency. Furthermore, IoT on the end-user side can support the real-time monitoring of energy consumption and help to regulate power uses more effectively. This can be achieved through smart home technology enabling remote (web or mobile application) control of IoT connected devices. This allows for a better control and regulation of smart systems in homes and buildings, thereby helping in energy waste reduction [3,23,24].

The biggest challenges of a conventional power grid system are reliability and power quality that can be overcome with the implementation of IoT. The transformation from a conventional grid to a smart grid (SG) system can be achieved with the utilization of advanced metering infrastructure (AMI), together with smart metering technologies (SM) [5,25–29]. AMI can gather information from the grid such as energy consumption, voltage, current readings, etc., [30]. The huge amount of data being generated can be efficiently transmitted and processed with IoT technologies and support quick response and decision making for effective energy management. The key benefits of IoT in smart grid (SG) systems include:

- Scalability,
- Heterogeneity,
- Energy efficiency,
- Dynamic nature,
- The detection of cyber-attacks [3].

IoT provides the technology to gather and transfer data from the energy grid in real-time and an infrastructure to efficiently process that huge amount of data through edge computing. IoT computing architecture has been described in previous work [31].

3. Research Method

The paper is based on a literature review method considering PRISMA guidelines. This approach allowed for the identification of different studies related to the one undertaken. It is necessary to mention it cannot be considered exhaustive or conclusive; however, it provides a picture of the current international research. This research focused on the relationship between blockchains, IoT, smart grids (SGs) and energy. As keyword searches are most common in identifying the relevant literature, the author used common Boolean operator AND [32]. The following search scheme was adopted in two major databases:

- Scopus database (TITLE-ABS-KEY ( blockchain ) AND TITLE-ABS-KEY ( iot ) AND TITLE-ABS-KEY ( smart AND grid ) AND TITLE-ABS-KEY ( energy ) ) AND ( LIMIT-TO ( PUBSTAGE , “final” ) ) AND ( LIMIT-TO ( LANGUAGE , “English” ) );
- Web of Science Blockchain and IoT and Smart Grids and Energy (All fields).

The research was conducted at the turn of August and September 2022. No temporal restriction was chosen. The search was limited to the publication stage and English language. When the research criteria were met, an initial sample of 230 papers (127 in Scopus...
and 103 in Web of Science) was identified. In the next step, duplicates were excluded as well as papers not connected to the scope of the paper. The sample was further limited to publication with full-text access resulting in 75 publications as the main sample.

The metadata of the papers were exported in comma-separated value (CSV) and .txt formats, which provided necessary information on the papers (title, authors’ name, authors’ affiliations, abstract, keywords and references).

**Data Analysis**

Figure 1 shows the publishing trend of publications meeting the selection criteria. There were no publications dating earlier than 2016 (Scopus) and 2017 (Web of Science). Recent years show an increase in the number of publications. As there were no publications found that met the keyword search criteria before 2016, this is considered a recent subject. Although there are many publications with the selected keywords and their different combinations, there are relatively few works covering all of them.

![Figure 1. Publishing trend of the sample. Keywords: blockchain, IoT, smart grids and energy.](image1)

Figure 2 presents the types of publications retrieved from the databases search. As can be noted, almost half of the published papers are conference papers and over one third are articles.

![Figure 2. Publications by type. Keywords: blockchain, IoT, smart grids and energy.](image2)
The obtained bibliometric data were used for further analysis as it allows for macro-
level assessment in the field area [32]. VOSviewer software was used [32–34] to calculate
and graphically present the matrix of keyword co-occurrence. It calculates the frequency of
two keywords appearing together in one paper and, as a result, a symmetrical co-occurrence
matrix based on the word co-occurrence is obtained. Moreover, “the higher frequency of
co-occurrence between keywords, the closer research theme is” [34]. In Table 1, keyword
clusters based on the VOSviewer co-occurrence analysis are presented.

Table 1. Clusters from bibliometric analysis.

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Cluster Color</th>
<th>Number of Keywords</th>
<th>Cluster Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Red</td>
<td>10</td>
<td>artificial intelligence blockchain cybersecurity electric power transmission networks information management internet of things internet of things (iot) iot smart grid smart power grids</td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td>7</td>
<td>energy efficiency energy trading energy utilization intelligent buildings peer to peer networks power markets smart city</td>
</tr>
<tr>
<td>3</td>
<td>Blue</td>
<td>6</td>
<td>block-chain distributed ledger energy renewable energies renewable energy resources smart contract</td>
</tr>
<tr>
<td>4</td>
<td>Yellow</td>
<td>5</td>
<td>data privacy energy resources network security smart contracts</td>
</tr>
</tbody>
</table>

The next step was to make a map of the analyzed co-occurrence matrix to better
visualize the relationships between the keywords form the bibliometric analysis, as shown
in Figure 3. The color nodes represent keywords, wherein the larger the size of a node,
the higher the frequency of a keyword [34]. Nodes are connected using lines showing the
connections between keywords. Moreover, the thicker the lines between words, the closer
their relationship. It was observed that of the 913 recurring terms, only 28 occurred at least
eight times. With the highest frequency of occurrence are such keywords as blockchain,
internet of things, smart grid and internet of thing (iot).
4. Smart Energy Grid System

Smart grid (SG) is described as technology-assisted efficient electric grid information that increases its performance through smart energy management. Smart grid (SG) also uses RESs (e.g., solar power, wind energy, geothermal energy, hydro energy, tidal energy and biomass energy) and interacts with energy prosumers and consumers. This energy exchange between prosumers and consumers helps to balance supply–demand of energy and is an emerging vehicle-to-grid technology (V2G) [1,2,5,6,15,23,35–38]. Smart grids (SGs) are therefore decentralized energy systems [39,40]. They are different from conventional grids as they provide a self-managing feature, thereby leading to a more reliable grid [41,42]. The term smart grid (SG) was first used in 2003 by Michael T. Burr [5]. An IF 2000 undersea connection located under the English Channel generates 2000 MW high-voltage direct current (HVDC) and connects the national energy networks of France and the UK [5]. Despite their advantages, they have some shortcomings such as “faults in power generation panels, dust accumulation on electricity-generating panels, conductors galloping and icing”. These are associated with renewable energy source that are used in smart grids (SGs) to meet the growing demand for electricity [13,16,43].

It is expected that the global smart meter market will reach USD 10.4 billion in 2022, and it is estimated that compound annual growth rate (CAGR) will be 12% in the period from 2020 to 2027 [13].

Based on IoT computing architecture an IoT-based smart grid (SG) typically consists of three layers:
- Data collection,
- Data communication,
- Data processing [3,12,44].

However, there are works in which other layers are added in order to group different services [12,44,45]. As shown in Figure 4, the data collection layer consists of numerous sensors and actuators collecting different data (e.g., temperature, moisture, noise, energy consumption, water consumption and location) and transporting them to the data communication layer (e.g., switches and routers) [23,46]. At the top of this architecture is the data processing layer (e.g., big data analytics, artificial intelligence and cloud computing) [40].
It is expected that the global smart meter market will reach USD 10.4 billion in 2022, and it is estimated that compound annual growth rate (CAGR) will be 12% in the period from 2020 to 2027 [13].

Based on IoT computing architecture an IoT-based smart grid (SG) typically consists of three layers:

- **Data collection**
- **Data communication**
- **Data processing** [3,12,44].

However, there are works in which other layers are added in order to group different services [12,44,45]. As shown in Figure 4, the data collection layer consists of numerous sensors and actuators collecting different data (e.g., temperature, moisture, noise, energy consumption, water consumption and location) and transporting them to the data communication layer (e.g., switches and routers) [23,46]. At the top of this architecture is the data processing layer (e.g., big data analytics, artificial intelligence and cloud computing) [40].

Figure 4. IoT architecture for smart grid.

Sensors are small elements embedded in a device that are responsible for measuring or detecting a change in a condition, such as temperature, light, movement, pressure, magnetism, humidity, particulate matter, etc., and then generating an electronic signal [13,24]. They can be connected in a network able to transmit data to remote locations by means of wireless sensor networks (WSNs) [3,24]. These networks use a message queuing telemetry transport (MQTT) protocol [47]. This protocol is a machine-to-machine (M2M) publish/subscribe messaging protocol for sensor and actuator solutions. Raspberry Pi gateway uses this protocol for communication with the cloud [48]. Another publish/subscribe messaging protocol used in smart grid systems is an open platform communications unified architecture (OPC-UA) developed by the OPC foundation [49,50]. An actuator is an element that can convert the electronic signal into an act, e.g., motion (in automatic doors and automatic lights). Signals produced by sensors can also be transmitted over the network for gathering and processing. These actuators in order to create motion can be categorized, based on the energy source, as pneumatic, hydraulic, thermal and electric ones [3,24].

The data communication layer is responsible for transmitting sensor raw information to a remote utility for further processing and is comprised of gateway devices. This network can be either a local area network (LAN) or a wide area network (WAN). Local area network communicates between sensors/actuators and a local gateway, whereas a WAN transmits data from LAN to the desired location for processing.

### 4.1. Local Area Network (LAN)

As LAN operates within a local network, it requires specific communication technology. Most common are Bluetooth, Wi-Fi, NFC, UPnP, ZigBee or Ethernet. Bluetooth is a short-range technology that can transmit data between devices over air interface. The 5.2 version has improved features, among others, power efficiency—low-energy (LE) Bluetooth. Wireless Fidelity (Wi-Fi) operates over radio waves and “uses the frequency of 2.4 GHz Ultra High Frequency and 5 GHz Super High Frequency ISM radio band in the domain of 0–250 m at data transmission rate of 54 Mbps”. Universal Plug and Play (UPnP) enables the control of small smart home devices or appliances but is not suitable for commercial surroundings. ZigBee is a power efficient, short-range wireless networking technology with the ability to create a wireless personal area network (WPAN) [3,24]. “Ethernet is a group of wired network technologies used in LAN” and wide area net-
work (WAN). Ethernet is applied in industrial applications (e.g., supervisory and fieldbus networks) [50,51].

4.2. Wide Area Network (WAN)

Wide area network operates over a wider area than LAN and, thus, requires different communication technology. Narrow-band Internet of Things (NB-IoT) uses a subset of long-term evolution (LTE) standard for wireless broadband communication [52]. Another technology is Sigfox—a narrow or ultra-narrow band technology that covers 3–10 km and 30–50 km in urban and rural areas, respectively. A technology with long wireless range is long-range (LoRa) that for IoT purposes uses a low-power wide area networking (LPWAN) protocol in LoRa-WAN. The LoRa-Wan protocol, in combination with LoRa devices, empowers IoT applications [3,24].

4.3. IoT Computing in Smart Grid (SG) Systems

In the processing layer, the closest to the end device are edge and fog computing. In edge computing, an edge device based on locally processed data can make the decision. Fog computing is suitable for resource constraint WSN, as it provides proximity and location awareness, but also hierarchical organization [26]. It acts without extra time required for further analysis in the cloud, as sensor collected data are sent to the fog for processing rather than to cloud servers. On the other hand, cloud computing is an on-demand availability of, e.g., servers, storage, virtualization and applications. It provides on-demand network access to distributed computing resources. The cloud offers multiple users access to data centers located in different geographical locations over the internet. In IoT cloud is used for the aggregation and processing of data coming from sensors and actuators, finally presenting the outcome of analysis to the end user. To achieve this outcome, a massive amount of data are gathered from various sensors and actuators. Approximately, 1 million smart meters in a smart grid (SG) can generate 2920 Tb data with a sampling rate of 4 per hour [26]. The data needs to be efficiently analyzed, but also stored and transferred in a secure manner. Big data analytics (BDA) with machine learning (ML) and artificial intelligence (AI) can analyze and present that sort of data [3,15,53]. Owing to the implementation of those technologies in smart grids (SGs), grid engineers are provided with a tool for more effective energy production management, which leads to outages reduction and allows for less peak-time power control [13].

4.4. SCADA System for Energy Grids

The supervisory control and data acquisition (SCADA) systems are vital in energy systems. SCADA collects data from the energy grid (sensors, cameras and IoT devices); it also supervises automatic procedures in order to control and regulate system parameters. The general SCADA structure consists of sensors and actuators that are controlled and communicated through remote terminal units (RTUs). Human actions, e.g., supervision, can be implemented in the system through human machine interfaces (HMIs) [54]. The SCADA system due to IoT implementation has become even more efficient and complex [54]. The SCADA interface allows system operators to (based on processed data) make decisions and adjust grid parameters. Through IoT real-time monitoring SCADA can quickly detect and communicate faults protecting power lines from potential damage [3,5,13,45]. The SCADA architecture consists of three layers, namely: thing layer, edge layer and cloud layer. Within the thing layer terminal, devices (e.g., sensors, actuators and IoT devices) are interconnected based on efficient communication technologies, such as Wi-Fi, Bluetooth, LTE, NFC or ZigBee. The edge layer is a combination of network devices such as gateways, switches, routers or access points. The SCADA servers in this layer shorten the distance between terminal devices and database, thus, reducing response time. The third layer—the cloud layer—consists of cloud SCADA servers where data are aggregated, analyzed and stored [45].
4.5. Standardization

Data collection from different architecture layers depend on the devices utilized in that layer. As there are many kinds of sensors manufactured by many different entities, in order to make the connection between devices possible, world-wide organizations create standards and protocols. The International Organization for Standardization (ISO) created standards regarding radio-frequency identification (RFID), such as ISO 18047, ISO 15459, ISO 18000 and ISO 11784. In wireless sensor networks (WSN) ISO/IEC 29182, the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standards are made. There are also other standards for short-range communication (e.g., Wi-Fi, Bluetooth and UPnP) [3]. Microgrids, however, have different standards such as ISO/IEC 62264 or IEEE 1547 [55].

5. Smart Grid Concept

In a smart grid (SG), all operations and mechanisms are controlled and managed by an algorithm, in other words, it is a typical cyber-physical system. The smart grid (SG) architecture is like the IoT computing architecture in Figure 1. However, there are differences, as shown in Figure 5.

![Figure 5. Energy trading architecture in the smart grid.](image)

In a smart grid (SG), power is generated by conventional power plants, large-scale and small-scale RESs, which is then sent to the transmission lines and through distribution lines reaches consumers (individual, commercial and industrial). The entire electricity channel is embedded with sensors interconnected over the internet for real-time data acquisition, processing and for effective energy management as well as reliable and secure power supplies [26,56,57].

Among renewable energy sources is solar energy that can be converted into energy by photovoltaic (PV) panels. A photovoltaic panel is simply an installation of photovoltaic cells placed in a framework called modules. Connected in a series of parallel modules, they create a panel. Thereafter, a number of connected panels make an array. Those solar cells absorb sunlight, and a PV module transforms it directly into direct current (DC) energy [58]. Cells are made of hundreds of different photovoltaic materials, such as polycrystalline silicon or thin-film technology, but their morphologies and efficiencies differ [58,59]. One of the PV materials is solution-processed bulk-heterojunction organic solar cells (OSCs). The morphology of those cells is the main aspect for achieving ultimate photovoltaic performance [60]. These cells use solution-processable organic semiconductors with tunable optoelectronic properties. Utilizing organic solar cells (OSCs), in contrast to crystalline inorganic photovoltaics (PVs), can lead to building-integrated photovoltaics (BIPVs) with see-through power windows [61]. With the application of
morphology optimization strategies, it has been reported that OSCs have acquired over 18% power conversion efficiencies (PCEs). Compared to traditional single-junction solar modules with a power efficiency of around 10.7% and tandem solar cells 11.55%, OSCs provide better efficiencies [59]. To obtain best single-junction OSC efficiency, their power conversion efficiency (PCE) must be enhanced. This can be achieved by constructing ternary blends. The research conducted by [60] showed that cutting-edge efficiencies were achieved for co-solvent-processed ternary OSCs using an amorphous polymer acceptor (BN-T: poly[3,9-didodecyl-4,4,10,10-tetraphenyl-4,10-dihydrothieno[3′,2′,3,4]r]-azaborolo[1,5-α]thieno [3′,2′,3,4]r]-azaborolo[1,5-d]thiophene-4,10-diium-4,10-diide-co-2,5-thiophene]). The authors in [61] developed a high-performance see-through power window using semi-transparent organic solar cells (ST-OSCs) showing energy generation and saving functions. The authors used near-infrared (NIR) ternary photoactive blends and introduced a third NIR component into the host binary blend. Furthermore, the calculations of annual carbon dioxide (CO₂) emissions reduction in China and worldwide were made, amounting to 0.13 and 0.67 billion metric tons, respectively. This, in turn, equals to around an 89 kg carbon emission reduction per capita. In another work by [62], a double-skin ventilated transparent photovoltaic window showed reduced energy consumption of air conditioning and good power generation.

This is an economically viable solution for already existing power grids that improves efficiency, connectivity and digitalization [25]. This is only a step forward in today’s power systems, because applying IoT technology paves the way for further development in the power sector.

6. Challenges of Smart Grids

As smart grid (SG) systems are based on IoT technology, they are prone to its vulnerabilities. IoT devices, in general, have limited power; many of them are battery powered, which leads to battery development to extend their life [3]. In [26], some examples of smart grid (SG) challenges are described, such as the real-time control of the monitoring of grid operations, scalable and distributed smart grid (SG) architecture, reliable power supply, security and privacy preserving and effective RES and V2G integration. Every internet-enabled system encounters cyber-attacks, and mitigation plans are necessary, especially in smart energy grids. Additionally, due to the number of sensors, there is increased traffic for transmitting and processing acquired data to the cloud, which becomes a bottleneck due to bandwidth limitations. Moreover, SCADA-regulated smart energy systems are more exposed to security threats [3,12,14,43,45]. Some examples of cyber-attacks are described in [3,13], such as data manipulation, false data injection, energy theft through hacking the energy meters or tampering their operating system. Furthermore, phishing or man-in-the-middle, spoofing, Sybil, eavesdropping or side channel attacks can occur in a smart grid (SG) [1,6,12,14,23,43]. Additionally, the complexity of the interconnected devices in a smart grid (SG) can cause risks, as a loophole in one device can affect the entire system [11]. Stuxnet or Duqu attacks can vandalize industrial control systems, they are hazardous, but they bring with them little chance of spreading [5,63]. In 2016, the Dyn cyber-attack infected and hijacked innumerable IoT devices [11]. The cyber-attacks can disrupt the power grid even of a country. Therefore, to achieve a stable and reliable smart grid (SG), cyber detection and protection measures are becoming crucial [16].

Cyber-Threat Counter Measures

The Defense Advanced Research Projects Agency (DARPA) base the Internet of Things (IoT) security shield, which can impact security beyond the internet itself, on four principles: authentication, confidentiality, integrity and availability [11,43]. Among measures taken to counter cyber-attacks in IoT-based smart grids (SGs) worth mentioning are:

- Limited physical access to the IoT devices,
- Physical access to the devices monitored,
- Avoiding direct connecting IoT devices to the Internet,
• Proxy-based access system implementation,
• Secure remote access mechanism,
• Side-channel protection,
• Firmware protection,
• Secure operating system,
• Network security protocol-supported mechanism,
• Periodical security testing,
• Implementation of crypto mechanism [3].

In addition, the implementation of physically unclonable function (PUF) as the root-of-trust hardware helps smart grid (SG) systems in protecting devices, data and services protection [14]. Another solution is an intrusion detection system (IDS) inspired by recurrent neural networks and based on a deep learning approach [1,5].

7. Internet of Energy (IoE) Concept

Traditional centralized energy sector, with its low efficiency and reliability issues, has been tackled with the introduction of IoT resulting in the concept of the Internet of Energy (IoE). The term Energy Internet (also named Internet of Energy) was first introduced in 2011 by Jeremy Rifkin in his book “The third industrial revolution” [38,64]. Smart grid (SG) systems create a modern power network called IoE [25,57,65–67]. It is developing rapidly and has developed in smart cities creating urban Energy Internet. On a large-scale, global Energy Internet can also be distinguished [68]. In the IoE, large-scale RESs are the main energy supply; therefore, it requires a reliable network to support energy collection, storage and distribution. Additionally, micro-scale energy producers need to be linked to balance energy supply and demand [8,69]. IoT applications in the energy sector create a specific field IoE. For example, in smart commercial buildings it enables improved control and energy consumption optimization [9,70,71].

It can be noted that the Internet of Energy is a prosumer-centric concept [72]. The Internet of Energy (IoE) is expected to consist of five pillars, namely:

• The shift from traditional to renewable energy sources (RESs) as main energy production sources,
• The transformation of building into smart buildings by means of the Internet of Things (IoT) with the ability to sell excess energy to the grid,
• The deployment of storage technologies for better flexibility and efficient energy distribution within the grid,
• The transformation from a centralized system to a decentralized one based on the existing infrastructure,
• The electrification of the transport system in order to become independent from liquid fuels (e.g., oil and gasoline).

As mentioned in [62], several application modes of the Internet of Energy (IoE) have been formed, such as “park-level energy internet, park-level agricultural energy internet, fishery energy internet, commercial energy internet, rail transit energy internet and social energy internet”.

In 2008 the German federal ministry for economic affairs launched a pilot project to build E-Energy. Other countries followed Germany in order to tackle the digitalization in the power sector. The architecture of Internet of Energy (IoE) is similar to that of IoT. It also consists of three layers: the physical layer with smart devices and other terminal devices, such as micro grids, electric vehicles (EVs), RES technologies; the data layer (including routers, Big Data and Blockchains); and finally, the operation layer, with its trade platforms, user interfaces and service-oriented energy platform [73,74].

The Internet of Energy (IoE) is boosting the rapid development of clean and renewable energy, thereby contributing to the achievement of the net-zero emission goal as well as sustainable development goals. The United Nations’ seventh sustainable development goal aims at affordable and clean energy. Among goal targets that are mentioned, for example,
are the substantially increased share of renewable energy sources (RESs) in global energy production and doubling the global pace of energy efficiency growth by 2030.

8. Blockchain in IoE

Although IoT provides various solutions for smart grid (SG) management and the Internet of Energy as a peer-to-peer network, it also brings vulnerabilities. These are mainly security issues, which can undermine the system’s reliability. Continuous growth in the number of prosumers in the grid make them an important part in energy trading. All energy trading parties are involved in trading (producers, prosumers and consumers), which requires reliable and secure transactions in a more and more decentralized system. A promising technology that is able to counter the P2P security risks is a distributer ledger technology (DLT) [3,19,75–79].

One of most recognizable DLT technologies is a blockchain (BC), which can tackle smart transactions [80]. Others include Tangle, Hashgraph, Sidechain, Ethereum or Hyperledger [25]. A blockchain allows for the storage and data processing of transactions over the internet without the involvement of third parties (e.g., banks) [81]. It was first described by Satoshi Nakamoto in 2008 and introduced as a trading platform for Bitcoin [11,18,27,82–86]. The global revenue for enterprise applications of BCs in 2016 accounted for around USD 2.5 billion and is expected to reach USD 19.9 billion in 2025 (CAGR 26.2%) [85].

BC transaction records are stored in blocks that make up the data information, hash functions and hash of the previous blocks. Hash is simply a mathematical calculation required for a blockchain calculation, thus, fulfilling security requirements. Hash allows for block identification and the details it contains and is always unique. It also helps in blocks’ traceability, making all BC transactions visible to its participants. Hashing enables encryption of data in a block [6,14,63]. Each block has a block id, timestamp, cryptographic hash of a previous block, as well as a digital signature. A new block (new transaction) is added to the one before, creating a chain of interconnected blocks. The records stored in blocks cannot be altered, as any change in a block requires a change in all subsequent blocks. This mechanism is a great security advantage of a blockchain [13,40,43,87,88]. Blockchain transactions are based on smart contracts between peers who verify the transaction without third parties’ interference. Every network participant can verify the transaction by accessing their ledger [7,89]. BC network participants are called miners [11,88]. Figure 6 shows the main types of BC.

There are two main types of BC, public and private [18]. In a public blockchain, anyone can join the BC and create new blocks. In this type of blockchain, the PoW consensus protocol is being used. In other words, everyone can take part in the consensus process as long as they were checked as a node. This type of blockchain is mainly used in cryptocurrencies. In a private (or enterprise, consortium) type, the owner of a blockchain restricts the access. Only a few users are allowed to verify and add to the BC; they are managing the consensus process for the entire network [14,43,87,90,91]. On the other hand, in a private/permissioned blockchain, control and management are required to a certain level. The reliability of nodes is ensured when meeting certain conditions ruled by the network initiator. Only the nodes accepted by the network initiator are added as participants [82]. This type of blockchain offers a higher degree of privacy, confidentiality and security, which is key in densely deployed Internet of Energy (IoE) networks [14].

Hashing (e.g., SHA256 algorithm) in a blockchain improves the BC security; however, this is not enough to counter cyber-attacks [81]. Either in a public or a private BC, there must be a consensus network. In order to achieve a consensus, different approaches are used [11,92]. Those consensus algorithms can be applied to the transaction at any time before adding to the chain. There are four consensus algorithms:

- Proof of Work (PoW),
- Proof of Stake (PoS),
- Proof of Authority (PoA),
- Practical Byzantine Fault Tolerance (PBFT) [1,87,91,93,94].
will enable market platform decentralization [95]. Blockchains can resolve limitations as IoE networks are very dense for a cost-effective deployment of BC-based IoE networks, a result of globalization, sustainability goals (such as net-zero emissions) and energy needs to be solved by miners in order to have the block accepted. This consensus protocol is usually used in public permission-less frameworks [11,87,91].

The Proof of Stake algorithm is based on a deterministic choosing of a different block’s producer. The miners take transaction fees in such a way so they can build a loyal node (high-stake node) [11,87].

The Proof of Authority algorithm allows the trusted users (approved accounts) to offer new transactions; this makes verifying much faster [87,91].

Practical Byzantine Fault Tolerance algorithm is based on the amount of fault tolerance [11,87,91].

When choosing the right consensus protocol, it is essential for BC developers to know exactly how they work and what the differences, opportunities and limitations for their easier implementation are [6].

Among blockchain advantages worth mentioning are anonymity, the transparency of transactions, decentralization and reliability, which are essential in the energy sector. As a result of globalization, sustainability goals (such as net-zero emissions) and energy security, due to various geopolitical crises in the energy sector, is moving towards a decentralized system with a deregulated market structure. Decentralized blockchain technology supported by IoT is, thus, opening new possibilities to that transformation [6]. As IoE networks are very dense for a cost-effective deployment of BC-based IoE networks, a layered architecture has been implemented similar to that in a smart grid (SG). This solution provides “maximum versatility for potential expansions and developers can substitute or install any new module without disrupting the rest of the infrastructure” [14].

A blockchain can support the transaction records storage process of any action in the smart grid (SG) by means of blocks in a blockchain. It has been shown that an IoT-based blockchain is essential for securing online monitoring. Therefore, an IoT-based blockchain can help to identify data loss or interruption in the network [13]. Blockchain-based systems provide security through cryptography, decentralization by means of consensus mechanism and transparency due to a distributed ledger system, which together with smart contracts will enable market platform decentralization [95]. Blockchains can resolve limitations in transactive energy systems (TES). Thanks to their ability to protect customer data, blockchains can streamline a multi-party settlement on a local level (Home Area Networks
(HANs) or Neighbor Area Networks (NANs)), customize complex contracts on a mass scale and direct offers on different devices. This brings new possibilities in the energy sector because they can allow electricity consumers and producers (prosumers) at the edge of the network for mass bidirectional transactions [28].

As with almost every new technology, standardization is an important factor. Asif [14] lists several standards concerning DLT/blockchain, such as IEEE P2418 series or ISO 307. Furthermore, the author mentions the Enterprise Ethereum Alliance (EEA) working on transparency, harmonization and interoperability on the global market. The International Telecommunication Union’s Standardization Sector (ITU-T) has developed a focus group responsible for the recognition and review of distributed ledger applications and services, but also for creating best practices and recommendations. The World Wide Web Consortium (W3C) on the other hand is working on ISO 20022-based message format standards and creates guidelines for storage use in both public and private blockchains. A reference architecture for IoT can be found in ISO/IEC 30141; it includes the ISO/IEC 27400:2022 Cybersecurity—IoT security and privacy—guidelines provide guidelines on risks, principles and controls for the security and privacy of Internet of Things (IoT) solutions. The selected standards are presented in Table 2.

Table 2. Selected International Organization for Standardization blockchain standards.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Document Status</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/CD TR 6039</td>
<td>Under development</td>
<td>Blockchain and distributed ledger technologies—identifiers of subjects and objects for the design of blockchain systems.</td>
</tr>
<tr>
<td>ISO 22739:2020</td>
<td>Published</td>
<td>Provides fundamental terminology for blockchain and distributed ledger technologies.</td>
</tr>
<tr>
<td>ISO/TR 23244:2020</td>
<td>Published</td>
<td>Provides an overview of privacy and personally identifiable information (PII) protection as applied to blockchain and distributed ledger technologies (DLT) systems</td>
</tr>
<tr>
<td>ISO/TR 23249:2022</td>
<td>Published</td>
<td>Provides an overview of existing DLT systems for identity management, i.e., the mechanisms by which one or more entities can create, receive, modify and revoke a set of identity attributes.</td>
</tr>
<tr>
<td>ISO 23257:2022</td>
<td>Published</td>
<td>Specifies a reference architecture for distributed ledger technology (DLT) systems including blockchain systems. The reference architecture addresses concepts, cross-cutting aspects, architectural considerations, and architecture views, including functional components, roles, activities, and their relationships for blockchain and DLT.</td>
</tr>
<tr>
<td>ISO/TR 23258:2021</td>
<td>Published</td>
<td>Specifies a taxonomy and an ontology for blockchain and distributed ledger technologies (DLT). The taxonomy includes a taxonomy of concepts, a taxonomy of DLT systems and a taxonomy of application domains, purposes and economic activity sections for use cases. The ontology includes classes and attributes as well as relations between concepts.</td>
</tr>
<tr>
<td>ISO/TS 23455:2019</td>
<td>Published</td>
<td>Provides an overview of smart contracts in BC/DLT systems; describing what smart contracts are and how they work. It also discusses the methods of interaction between multiple smart contracts. This document focuses on the technical aspects of smart contracts. Smart contracts for legally binding use and applications will only be briefly mentioned in this document.</td>
</tr>
<tr>
<td>ISO/TR 23576:2020</td>
<td>Published</td>
<td>Discusses the threats, risks, and controls related to systems and asset information.</td>
</tr>
<tr>
<td>ISO/TR 23635:2022</td>
<td>Published</td>
<td>Provides guiding principles and a framework for the governance of DLT systems.</td>
</tr>
<tr>
<td>ISO/CD TR 23644</td>
<td>Under development</td>
<td>Blockchain and distributed ledger technologies—an overview of trust anchors for DLT-based identity management (TADIM).</td>
</tr>
<tr>
<td>ISO/CD TR 24374</td>
<td>Under development</td>
<td>Information technology—security techniques—DLT and blockchain for financial services.</td>
</tr>
</tbody>
</table>

Source: Based on ISO ICS Code 35.030 (https://www.iso.org/ics/35.030/x/ (accessed on 15 October 2022)).

In the US, a company called Exergy was the first that applied blockchain to a transaction grid, the Brooklyn Microgrid, in 2016. There are also businesses such as Grid+, LO3 energy or Power Ledger that offer new metering and billing BC solutions [96]. Electron is a United Kingdom company applying BC technology to the energy sector [2]. Another startup is the Power Ledger in Australia [35]. The TRANSAX platform for forward-trading energy exchange was described in [97]. Whereas, in [98], a secure blockchain-enabled dynamic monitoring and decision system was proposed for a minimal-information ex-
change framework. ZipZap is a novel tokenization blockchain for local energy exchanges described in [99]. In addition, ref. [100] proposed a blockchain-based system model for smart meter network communication, which uses elliptic curve cryptography (ECC) and digital signature over a home area network (HAN). Whereas [101] investigated smart grid (SG) and energy transactions in a P2P network in a local community in the UK.

9. Conclusions

The increased integration of renewable energy sources, storage systems, electric vehicles, distributed generation and microgrids in smart grids (SGs) make traditional centralized power management no longer attractive. The reasons for this are the system’s disadvantages, such as the cost, security issues, control of a complex network, energy trading and energy management [6].

IoT combined with blockchain technology has the potential to increase transparency and trust between different stakeholders, as it offers both privacy and confidentiality. It can also enhance data security thorough encryption, cryptography and consensus protocols. Moreover, this combination in the new decentralized energy system can minimize transaction costs, support processes automation and facilitate the active participation of small consumers and prosumers in the smart grid (SG) [87,94]. Blockchain is an emerging technology that can use enterprise data with the use of secure transactions between parties. Blockchain-enabled systems are a new trend rising fast in the area of engineering [1].

The transformation currently taking place in decentralization in the energy sector favors customers and is, thus, more consumer-centric and changing the attitude towards customer satisfaction.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

Alphabetical list of abbreviations used within the paper:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AMI</td>
<td>Advanced Metering Infrastructure</td>
</tr>
<tr>
<td>BC</td>
<td>Blockchain</td>
</tr>
<tr>
<td>BDA</td>
<td>Big Data Analytics</td>
</tr>
<tr>
<td>BIPV</td>
<td>Building-Integrated Photovoltaics</td>
</tr>
<tr>
<td>CAGR</td>
<td>Compound Annual Growth Rate</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defense Advanced Research Projects Agency</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>DLT</td>
<td>Distributed ledger</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>EEA</td>
<td>Enterprise Ethereum Alliance</td>
</tr>
<tr>
<td>EV</td>
<td>Electric Vehicle</td>
</tr>
<tr>
<td>HAN</td>
<td>Home Area Network</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interfaces</td>
</tr>
<tr>
<td>HVDC</td>
<td>High-Voltage Direct Current</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection system</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IoE</td>
<td>Internet of Energy</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITU-T</td>
<td>The International Telecommunication Union’s Standardization Sector</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LE</td>
<td>Low Energy</td>
</tr>
<tr>
<td>LoRa</td>
<td>Long Range</td>
</tr>
<tr>
<td>LPWAN</td>
<td>Low-Power Wide Area Network</td>
</tr>
</tbody>
</table>
References


47. Gonzalez, I.; Calderón, A.J.; Folgado, F.J. IoT real time system for monitoring lithium-ion battery long-term operation in microgrids. *J. Energy Storage* **2022**, *51*, 104596. [CrossRef]


