Review

Blockchain, Data Protection and P2P Energy Trading: A Review on Legal and Economic Challenges

Alessandra Chiarini [1] and Lorenzo Compagnucci [2,*]

[1] European Banking Federation, B-1000 Brussels, Belgium
[2] Department of Law, University of Macerata, 62100 Macerata, Italy
* Correspondence: lorenzo.compagnucci@unimc.it

Abstract: Blockchain technology (BCT) enables the automated execution of smart contracts in peer-to-peer (P2P) energy trading. BCT-based P2P platforms allow the sharing, exchange and trade of energy among consumers or prosumers as peers, fostering the decarbonization, decentralization and digitalization of the energy industry. On the other hand, BCT-based P2P energy trading relies on the collection, storage and processing of a large amount of user data, posing interdisciplinary challenges, including user anonymity, privacy, the governance of BCT systems and the role of energy market players. First, this paper seeks to review the state of the art of European data protection law and regulations by focusing on BCT compliance with the General Data Protection Regulation (GDPR) of 2018. Second, it explores both the potentials and the challenges of BCT-based P2P energy trading from a legal–economic perspective. To do so, the paper adopts an interdisciplinary approach which intertwines both law and economics, by reviewing the recent literature on BCT and P2P energy trading. Findings have revealed that the deployment of BCT-based P2P energy trading is still in its pilot stage because of technology immaturity, data protection uncertainty, incomplete disintermediation and the lack of both user awareness and collaboration among market players. Drawing on the review, the paper also proposes a selection of solutions to foster the implementation of BCT-based P2P energy trading.

Keywords: blockchain; data protection; energy community; P2P energy trading; prosumer; transaction cost

1. Introduction

The Member States (MSs) of the European Union (EU) are committed to fostering a sustainable and decarbonized energy system. The EU aims at reducing greenhouse gas emissions by at least 55% by 2030, compared to 1990 [1]. Within this framework, buildings account for 43% of final energy consumption [2]. In particular, in 2020, households accounted for 27.0% of energy consumption in the EU. This consumption was primarily covered by natural gas (31.7%) and electricity produced from renewable energy sources (RESs) (e.g., hydro, wind and solar photovoltaic) (24.8%), followed by renewables such as solid biofuels, biogas and thermal energy (20.3%) [3]. The main use of energy was for heating households (62.8%) [3]. It means that energy consumption in households is a serious challenge for achieving the environmental goals set by the EU [2].

On the other hand, over the last decade, the energy industry has witnessed a rapid digitalization thanks to the introduction of innovative smart devices, which perform tasks and collect and process a large amount of data autonomously [4], improving energy efficiency [2]. Furthermore, the diffusion of the Internet of Things (IoT), big data, artificial intelligence (AI) and blockchain technology (BCT) has started to exert a disruptive impact on both the business environment [5] and society [6,7], leading energy suppliers, distributors, institutions and consumers to rethink the traditional vertical structure of the energy value chain [8]. From the policy perspective, several governments are promoting the development of RESs and distributed energy resources (DERs) [9], which include both

energy storage technology and generation units such as batteries, solar panels and wind turbines [10]. To do so, national and regional policy makers have adopted tax subsidies, direct incentives, long-term agreements with firms and local authorities [9], as well as mixed financing schemes to fund locally based projects [11]. Indeed, RESs and DERs can contribute to a long-term energy pathway for the transition to a cleaner and more sustainable energy system for both households and firms [12], while supporting the decentralization of energy trading [13].

Within this framework, blockchain technology (BCT) has recently gained increasing attention from both academics and professionals [14], leading to several real-world implementations in the energy industry [15]. Indeed, BCT permits the automated execution of smart contracts in peer-to-peer (P2P) energy trading [16], which is based on the collection, storage and processing of a large amount of user data [17]. BCT-based P2P energy trading establishes a horizontal platform for sharing, transferring, exchanging and trading electricity. It allows prosumers to sell their surplus electricity directly to local consumers without the need for a retailer, enabling mutually beneficial transactions [14]. It means that BCT-based P2P energy trading can foster the transition from a centralized energy market, to a decentralized market of RESs, dominated by energy communities (EC) [18].

As BCT-based platforms for P2P energy trading process a large amount of prosumers data, they have posed unprecedented challenges for data protection. Indeed, several issues concern user anonymity, privacy [19], the governance of BCT systems [16] and the role of energy market players [20–24]. It implies that BCT represents an interdisciplinary research field which involves technical, legal and economic aspects [25]. With regards to the European framework, the General Data Protection Regulation (GDPR) came into force in 2018, before the diffusion of BCT-based P2P energy trading platforms. On the one hand, BCT provides a decentralized system without third-party intervention [26] and makes information publicly available, ensuring the integrity and immutability of data [27]. On the other hand, these key features of BCT seem to clash with some GDPR provisions, including the principle of accountability (Article 5 GDPR), the right to rectification (Article 16 GDPR) and the right to erasure ('right to be forgotten') (Article 17 GDPR) [28]. Although there are several case studies on BCT [29], and ongoing trials to implement BCT-based P2P platforms [30], P2P energy trading is still facing major challenges in achieving large-scale deployment due to both data protection issues [31–34] and obstacles to cooperation among market players [35].

Thus, this paper seeks, first, to review the state of the art of European data protection law and regulations by focusing on BCT compliance with the GDPR. Second, it explores both the potentials and the challenges of BCT-based P2P energy trading from a legal–economic perspective. The paper adopts an interdisciplinary approach which intertwines both law and economics. The analysis is performed through the lens of a legal research methodology which uses both hard and soft law sources. This investigation of the GDPR is supported by European case law and by a selection of recommendations made by national and European institutions, including the European Data Protection Board (EDPB), national data protection authorities and the European Blockchain Observatory and Forum of the European Commission (hereinafter, the EU Observatory). For the economic aspects, the investigation draws on the recent literature on BCT and P2P energy trading. Figure 1 shows the flowchart diagram of the research process.

This paper is organized as follows. Section 2 focuses on the relationship between GDPR and BCT. This section reviews the main subjects, principles, rights and obligations enshrined in the GDPR and the challenges that rise from GDPR application to BCT. Section 3 sheds light on both the potentials and the challenges of BCT-based P2P energy trading platforms, by leveraging a legal–economic perspective. Section 4 summarizes the main findings.
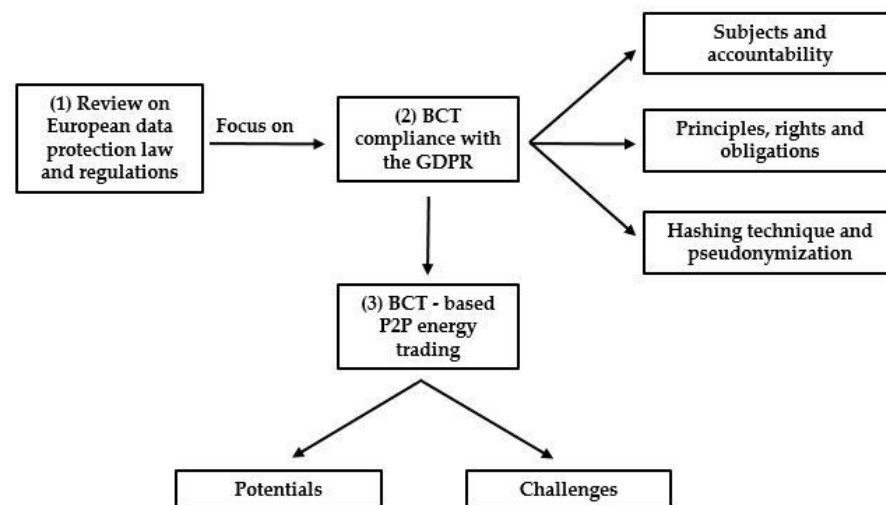
Figure 1. Flowchart diagram of the research process. Source: Authors' elaboration.

2. The European Data Protection Law and BCT

The General Data Protection Regulation (hereinafter, the GDPR or Regulation) was adopted in 2016 and became binding in 2018 in the European Union (EU). The GDPR draws on Directive 95/46/EC (General Data Protection) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. From a general standpoint, the Regulation addresses the challenges posed by the digital economy regarding the protection of personal data. To do this, the GDPR focuses both on the obligations of data controllers and processors, and on the rights of data subjects.

The Regulation is based on two main rationales. First, the GDPR aims to reinforce the free movement of personal data within the EU. Indeed, the previous Directive of 1995 proved anachronistic in the face of recent technological developments [36]. Second, the GDPR confirms that the right to data protection is a fundamental right, which was, originally, recognized by the Charter of Fundamental Rights of the European Union (CFREU). The Charter was declared in 2000 and came into force in December 2009, along with the Treaty of Lisbon. According to Article 8 of the CFREU, "1. Everyone has the right to the protection of personal data concerning him or her. 2 Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority." Drawing on this provision, the Regulation has ensured a higher level of rights protection for an "identified or identifiable natural person" (Article 4, GDPR), while seeking to standardize the EU data protection legal framework [37]. The GDPR has widened the material scope of European data protection law. Indeed, the "[. . .] Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." Furthermore, the GDPR "[. . .] applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union." In addition, the GDPR "[. . .] applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.".

In light of this set of provisions, the literature has stated that the Regulation also applies to BCT-based platforms when the latter have an establishment within the EU or

when the BCT platform processes the personal data of subjects located in the EU [38]. On the other hand, it is worth noting some tensions between the Regulation and BCT. In particular, the GDPR was originally based on the following assumption: data in the digital economy is in the hands of identifiable actors. Nevertheless, BCT relies on anonymization. Moreover, when the GDPR came into force in 2018, it did not take into account the most recent applications of BCT [39] which is increasingly becoming an interdisciplinary research field [25]. Some key features of BCT—disintermediation and decentralization—might clash with the enforcement of the GDPR [28] as described in the following sections. However, ensuring BCT compliance with the GDPR is also important because it might accelerate the creation of an EU digital market [39].

2.1. Subjects and Accountability

The GDPR identifies the main subjects involved in data protection: the controller and the processor. Article 4(7)(8) of the GDPR states that the controller is "[. . .] the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data [. . .]", while the processor is "[. . .] a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller [. . .]". Then, according to Article 5(2) of the GDPR "2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Accountability is a common principle for organizations in several disciplines. The GDPR integrates accountability as a principle which requires that organizations put in place appropriate technical and organizational measures and are able to demonstrate what they did, and its effectiveness, when requested. Accountability is one of the most important data protection principles set by the GDPR along with lawfulness, fairness and transparency, as well as: purpose limitation; data minimization; accuracy; storage limitation; integrity; and confidentiality [40].

According to Article 5(1) of the GDPR: "1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; [. . .] ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; [. . .] ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

In further detail, the controller has the responsibility of "[. . .] taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons [. . .]" in order to "[. . .] implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. [. . .]" (Article 24(1), GDPR). Furthermore, "[. . .] where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with the obligations under this Regulation [. . .]" (Article 26(1), GDPR). On the other hand, "[. . .] where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of

this Regulation and ensure the protection of the rights of the data subject [...]" (Article 28(1), GDPR).

From the theoretical point of view, the roles of both the controller and the processor seem to be clearly separated, and these subjects appear easily identifiable. Nevertheless, in practice, this division is difficult to discern, especially in the case of public BCT-based platforms. On one side, in private, permissioned BCT, it is easy to identify the controller because the BCT is more centralized, thus closer to the logic of the Regulation. The controller is the subject responsible for defining both the purposes and the means of data processing. On the contrary, the decentralized nature of public BCT can make it difficult to identify the controller or the joint controllers, and as such to allocate accountability. Since Google Spain and Google, the European Court of Justice (ECJ) has stressed the importance "[...] to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects [...]" [41] (p. 10). Then, in Wirtschaftsakademie Schleswig-Holstein, the ECJ has stated that it is "[...] clear from the case-law of the Court that the concept of 'controller' must be given a broad definition, so as ensure effective and complete protection of data subjects [...]" [42] (p. 9). More recently, in Fashion ID, the ECJ has recalled that "[...] for there to be joint control and joint responsibility, it is not required that each of the controllers must have access to (all of) the personal data concerned [...]" [43] (p. 13). Indeed, "[...] the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. [...] those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case [...]" [43] (p. 18).

To address these issues, the literature has suggested some solutions. With respect to protocol developers, a stream of knowledge has argued that these subjects can be qualified as data controllers [38]. On the other hand, the EU Observatory has stated that holding protocol developers accountable is purposeless since these subjects only design the open-source BCT, without determining the purposes and the means of data processing [39]. Other scholars have stressed that the subjects running the BCT protocol—the computers storing a copy of a blockchain, thus validating a new block—can be qualified as joint-controllers according to Article 26 of the GDPR. However, the nodes of the chain do not determine the purpose and the means of data processing under Article 26 of the GDPR. Validating nodes only take part in the network to contribute to its stability or to access data [44].

Qualifying network users is also unclear. When network users process data for business purposes, they can be considered data controllers. On the contrary, when network users submit personal data to the BCT ledger for their own personal use, they might fall under the personal or household activity exemption as the GDPR "*[...] does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities [...]*" (Recital 18, GDPR). It is worth noting that the qualification of network users has not been filed in any court by the European Data Protection Board (EDPB), which is an independent European body that ensures the application of the Regulation and promotes cooperation between national data protection authorities. However, the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés, hereinafter CNIL) has examined the role of network users and has suggested some insights. The CNIL has stated that network users, through written permissions, can agree upon being regarded as data controllers before submitting data for validation. The CNIL has also argued that network users can be considered as controllers under the Regulation in two cases: first, when the user is a natural person processing personal data for business purposes; and second, when the user is a legal person writing personal data on BCT [45]. According to the European Parliament, when a natural person submits a transaction and the processing involves data of their own

and of other subjects, then on-chain data are available to unlimited people. As a result, the household exemption does not apply [46].

2.2. Principles, Rights and Obligations

Two cornerstones of the Regulation are the right to rectification (Article 16, GDPR) and the right to erasure ('right to be forgotten') (Article 17, GDPR) [45]. According to Article 16 of the GDPR, "[. . .] the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement [. . .]". Then, Article 17(1) states that: "[. . .] the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies [. . .]".

There is a tension between immutability, which is a key feature of BCT, and both the right to rectification and the right to erasure. Indeed, in BCT-based platforms, new information can only be added through new blocks, not by modifying data unilaterally. While BCT ensures data integrity and fosters trust across the network, the controller might find it difficult to comply with the obligation to rectify personal data when data are stored on-chain. However, some technical solutions might prove helpful in removing data from the chain. In particular, the CNIL has suggested registering data by using the hashing technique, encryption or digital signatures to encrypt data [45]. As stated by Xu et al. [47], BCT involves a timestamp mechanism to generate an ID for each transaction. The user can query the relevant transaction data according to the ID. When the new block is verified, the current block is added to the main block. Each block uses a hash of an algorithm to identify its uniqueness. Moreover, when personal data are stored off-chain, they can be linked back to the ledger by a hash and other identifiable information [45]. Thus, the use of a key management protocol enables the deletion of the link between off-chain and on-chain data [48].

Another way to address data immutability in BCT-based platforms is to establish, in advance, a consensus mechanism which enables block deletion from the chain [49]. Although it is not clear whether using a key management protocol corresponds to the exercise of the right to erasure [50], the CNIL has advised registering personal data directly on the blockchain using encryption. By drawing on the privacy by design principle, "[. . .] the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization [. . .]" (Article 25(1), GDPR). Thus, non-protected personal data will be recorded outside the BCT. The latter will only indicate that data are stored in a separate database. As a result, it is possible to protect the subject's data against data alteration, integrity compromises or unauthorized access [44].

Regarding the right to be forgotten, since the processing of personal data for BCT follows the performance of a contract to which the data subject is party under Article 6(1)(b) of the GDPR, an erasure request can only occur when personal data are no longer necessary in relation to the purpose for which the data were collected. Thus, the blockchain retains personal data for its duration until the last server on which the blockchain is stored is physically destroyed. With respect to this latter point, the principle of storage limitation (Article 5(1), GDPR) fixes a temporary limit for data processing. Indeed, once the processing operations are successfully completed, data concerned must be either deleted or made anonymous. The controller is obliged to inform the data subject about the storage period (Articles 13(2)(a), GDPR and Article 14(2)(a), GDPR). It follows that the storage period should be decided before the beginning of the processing.

BCT challenges two further key principles of European data law: purpose limitation and data minimization. According to Article 5(1)(b) and (c) of the GDPR: "1. Personal data shall be: [. . .] (b) collected for specified, explicit and legitimate purposes and not

further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization') [. . .]".

On the one hand, these principles state that data collection should be limited to the extent that data are required to fulfil a specific purpose decided in advance. On the other, the principle of data minimization might clash with BCT architecture as distributed ledger technologies (DLT) grow with the addition of new data. Indeed, data are replicated by all the nodes along the network. Thus, it is not clear to what extent the principle of purpose limitation might apply to BCT. Zemler and Westner [51] have emphasized that personal data collection should be kept as minimal as possible, while processing should be carried out within a fixed scope. In addition, the CNIL has stressed that nodes are identified along a blockchain through both a public and a private key: this is the minimum standard required for a blockchain to work. For instance, a public key allows the user to receive cryptocurrency transactions. It is a cryptographic code which is paired to a private key. While anyone can send transactions to the public key, the user needs the private key to unlock them and prove that he/she is the owner of the cryptocurrency received in the transaction. Further minimization is not achievable, and processing should be within a limited scope [45].

2.3. Hashing Technique and Pseudonymization

Personal data are defined as "[. . .] any information relating to an identified or identifiable natural person ('data subject') [. . .]" (Article 4(1), GDPR) and the material scope of the Regulation is to protect "[. . .] the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system [. . .]" (Article 2(1), GDPR).

On the other hand, data processing and storing on BCT rely on the hashing technique, which is the process of transforming any given key or a string of characters into another value [44]. It is unclear whether transaction data linked to natural persons by using the hash function, and stored on the chain, can be qualified as personal data, and thus fall into the scope of the GDPR. This issue was first addressed by the European Parliament which stated that the hash function can be qualified as an operation of user pseudonymization, falling under the Regulation [52]. Pseudonymization is "[. . .] the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [. . .]" (Article 4(5), GPDR).

Nevertheless, pseudonymization is not anonymization. Indeed, Recital 26 of the GDPR states that anonymous information "[. . .] does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable [. . .]". It implies that the Regulation does not apply in the case of successful anonymization. On the contrary, the GDPR applies in the case of pseudonymized data, which remain as personal data, as it is possible to identify the data subject using additional information [53]. Furthermore, the literal interpretation of Article 4(5) of the GDPR reveals that pseudonymization deals with a particular method for processing personal data, not with an outcome of data processing [54], and it is one among several measures of data protection that "[. . .] can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations [. . .]" (Recital 28, GDPR).

To ascertain whether data can be qualified as personal data, Recital 26 of the GDPR might also prove helpful as it states the principle of the reasonable likelihood of identification. The Recital describes a risk-based test to establish a reasonable risk of re-identifying the data subject. When the risk is missing, it means that personal data have been successfully anonymized, thus falling outside the scope of the Regulation. With respect to BCT, several techniques have been suggested to overcome the anonymization threshold, including zero-knowledge proofs and homomorphic encryption [46]. In the case of BCT-based P2P energy trading, the transaction record includes the block producers' identification, payer ID, payee ID and the payment amount. The list of transaction records is encrypted using homomorphic encryption or zero knowledge proof and forms a block [14]. Zero-knowledge proofs enable the BCT to only show that a transaction has occurred, not which key was used or the value (if any) transferred [55]. With regards to homomorphic encryption, it enables the deletion of any relationships between plaintext and the corresponding ciphertext [46]. Homomorphic encryption generates a ciphertext which is indistinguishable from a random number. The only way to determine which plaintext corresponds to a certain ciphertext is to use the proper key to decrypt it [56]. As a result, the prover demonstrates possession of knowledge without revealing any computational information whatsoever [57]. While the implementation of this cryptographical method to distributed ledger technology (DLT) is becoming progressively more commonplace, it is still far from being established as a technological standard that would be implemented in the Bitcoin protocol [58]. Overall, the EU Observatory has stressed that it is up to the European Data Protection Board (EDPB), the courts and the legislators to assess the validity of these techniques and their compliance with the GDPR [39]. Table 1 summarizes the main legal challenges regarding BCT compliance with the GDPR. The table also shows the solutions proposed in the literature.

Table 1. BCT compliance with GDPR: legal challenges and proposed solutions.

Domains	Challenges	Proposed Solutions
Accountability	• Defining the accountability of both the controller and the processor in permissioned BCT and in public BCT-based platforms.	• In permissioned BCT, the controller is the subject responsible for defining both the purposes and the means of data processing. • In public BCT-based platforms, it is necessary to ensure, through a broad definition of the concept of controller, effective and complete protection of data subjects. However, protocol developers and subjects running the BCT protocol should not be considered accountable because they do not determine the purposes and the means of data processing.
	• Defining the accountability of network users.	• Network users, through written permissions, can agree upon being regarded as data controllers before submitting data for validation. • The household exemption does not apply when the user is a natural person processing personal data for business purposes; or, when the user is a legal person writing personal data on BCT.
Right to rectification	• BCT compliance with the right to rectification.	• When personal data are stored off-chain, they can be linked back to the ledger by a hash and other identifiable information. • A consensus mechanism which enables block deletion from the chain should be established in advance.

Table 1. *Cont.*

Domains	Challenges	Proposed Solutions
Right to erasure	• BCT compliance with the right to erasure.	• Since the processing of personal data for BCT follows the performance of a contract to which the data subject is party, an erasure request can only occur when personal data are no longer necessary in relation to the purpose for which it was collected.
Principle of purpose limitation	• BCT compliance with the principle of purpose limitation.	• Data collection should be limited to the extent data are required to fulfil a specific purpose. The latter should be decided in advance.
Principle of data minimization	• BCT compliance with the principle of data minimization.	• Although data collection should be kept as minimal as possible, nodes should be identified along a blockchain through both a public and a private key: this is the minimum standard required for a BCT to work.
Hashing technique and pseudonymization	• Transaction data and their qualification as personal data.	• Implementing a risk-based test to establish a reasonable risk of re-identifying the data subject. Zero-knowledge proofs and homomorphic encryption should be used.

Source: Authors' elaboration.

3. BCT-Based P2P Energy Trading

3.1. The Rise of Energy Communities and P2P Energy Trading

The energy industry has witnessed a massive revolution, from its traditional fossil-based status towards a renewables-centered industry [34]. In this context, the emerging sharing economy has been described as something which promotes more sustainable consumption practices, such as access over ownership [59]. Along with the sharing economy, the increased viability of individual self-consumption is leading to new collective forms of energy self-production and consumption. In the European framework, Article 21 of the Renewable Energy Directive (RED II) (Directive (EU) 2018/2001) states that "[. . .] Member States shall ensure that renewables self-consumers located in the same building, including multi-apartment blocks [. . .] are permitted to arrange sharing of renewable energy that is produced on their site or sites between themselves, without prejudice to the network charges and other relevant charges, fees, levies and taxes applicable to each renewables self-consumer. Member States may differentiate between individual renewables self-consumers and jointly acting renewables self-consumers [. . .]". In particular, "[. . .] renewables self-consumers, individually or through aggregators, are entitled: (a) to generate renewable energy, including for their own consumption, store and sell their excess production of renewable electricity, including through renewables power purchase agreements, electricity suppliers and peer-to-peer trading arrangements [. . .]". Moreover, self-consumers are entitled "(b) to install and operate electricity storage systems combined with installations generating renewable electricity for self-consumption without liability for any double charge, including network charges, for stored electricity remaining within their premises; (c) to maintain their rights and obligations as final consumers; (d) to receive remuneration, including, where applicable, through support schemes, for the self-generated renewable electricity that they feed into the grid, which reflects the market value of that electricity and which may take into account its long-term value to the grid, the environment and society [. . .]".

Drawing on these premises, since 2019 energy communities (ECs) have started spreading in the form of legal entities, especially across Italy and Spain [60]. Ecs are usually set up on a voluntary basis, and they are mainly driven by environmental awareness rather than

commercial goals [61]. From the socio-economic perspective, Ecs are not new because they existed before the energy transition. Since the 1970s, Ecs have been linked to the advocacy of alternative technologies for local, small-scale and collective approaches to sustainable energy generation [62]. However, following the rise of renewable energy sources (RESs) and distributed energy resources (DERs), policy makers, firms and consumers have focused anew on Ecs as they have the potential to become a standard model on the energy markets [63]. In particular, Ecs might be the first step of a more virtuous cycle [64] towards implementing a sharing economy [65]. To do so, one of the most promising ways is to apply BCT to DERs by speeding up decentralization and disintermediation, thus enabling P2P energy trading [31,66] which is "[. . .] the sale of renewable energy among market participants by means of a contract with pre-determined conditions. The contract is governing the automated execution and settlement of the transaction, either directly among market participants or indirectly through a certified third-party market participant, such as an aggregator [. . .]" (Article 2, RED II).

When coupled with BCT, P2P energy trading permits the sharing, transfer, exchange and trade of energy among consumers or prosumers as peers, fostering the decarbonization, decentralization and digitalization of the energy supply chain [67]. The prosumer is someone who both produces and consumes his/her own electricity [68]. P2P trading aims at avoiding the traditional energy utility company [69], while introducing both prosumers and consumers who make use of the BCT functionality for the payment of shared renewable energy [14]. P2P includes all possible interactions between participants in self-consumption schemes (individual, collective and community self-consumption) [70]. Indeed, P2P participants can supply energy to the electrical grid or take energy from the grid depending on their energy use and production balance. Prosumers are incentivized to supply renewable energy through payment for the energy they provide, in the form of a cryptocurrency or a crypto-utility token. Consumers are also incentivized as they can purchase energy from their peers at a competitive tariff using cryptocurrency [14]. Along with consumers and prosumers, intermediaries can be replaced with a distributed network of digital users or validator nodes, known as miners, who work in collaboration to verify transactions and safeguard the integrity of the ledger [71].

Thanks to BCT and smart contracts, energy demand and supply can be balanced in P2P trading while transaction costs—those associated with the exchange of goods and services—are reduced [65,72]. Indeed, BCT consensus mechanisms and smart contracts can change two main features of transaction costs: human specificity and time specificity [73]. Regarding human specificity, the BCT-based P2P model can ensure a more equitable distribution of costs and profits among market participants [74]. In particular, Catalini and Gans [75] have observed that BCT fosters transparency which can significantly reduce the validation costs for trading partners. Furthermore, BCT-based trust among trading partners avoids the need for any centralized authority—e.g., a bank—to finalize transactions. At the same time, BCT has the potential to improve the performance of IoT security because BCT consensus mechanisms and smart contracts do not require trust between nodes. In addition, the distributed network structure of BCT ensures that, even if one node is attacked, the data of the whole network is still reliable and safe. As a result, BCT consensus mechanisms prevent major attacks, and so reduce transaction costs [47]. Sun et al. [76] have also stressed that human-specific resources can be transferred to several partners on-chain rather than exclusively dealing with a centralized authority. With respect to time specificity, both BCT and smart contract automation facilitate data flows and exchange, and so decrease the time required for collecting and digitalizing information [77]. As argued by Xu et al. [47], BCT involves data encryption and timestamps to identify and record each transaction, adding a time dimension to the data. The timestamp method lessens the risk of lost or corrupted data and makes traceability less time-consuming, thus reducing transaction costs. Figure 2 shows how a BCT-based P2P energy trading system works.
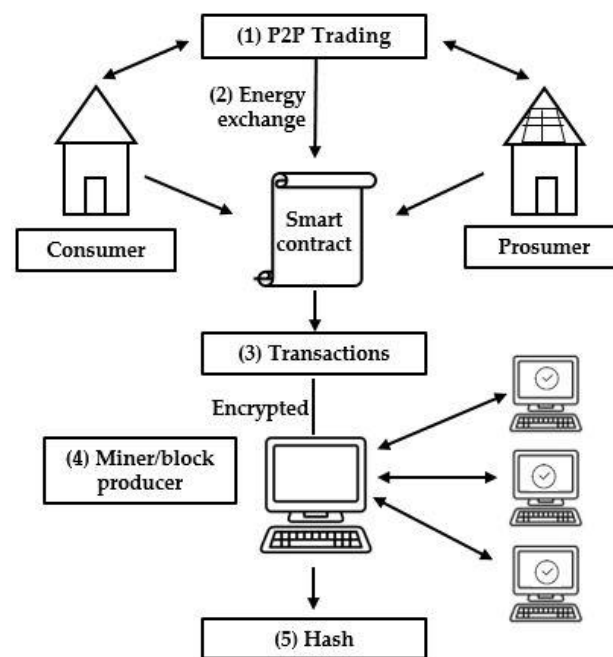
Figure 2. Overview of BCT-based P2P energy trading system. Source: Authors' elaboration.

3.2. Potentials of BCT-Based P2P Energy Trading

BCT-enabled P2P energy trading has several features that could, potentially, contribute to the transformation of the energy industry [78]. First, BCT makes renewable energy sources (RESs) more accessible and also empowers prosumers who can thus make better informed choices, and use, of their distributed energy resources (DERs). Indeed, prosumers are able to track the energy they consume, thus enhancing the flexibility of the whole system even while boosting the use of RESs [79]. Furthermore, the P2P model can be designed to achieve specific targets set by the energy community (EC), such as promoting clean energy or reducing billing [80]. However, several studies have demonstrated that economic incentives are not the main drivers for implementing P2P energy trading [81]. Along with the possibility of supporting local ECs [82], increasing the share of RESs is one of the main reasons for participating in the decentralized energy market at the local level [61,81].

Second, the P2P model increases the overall efficiency of the power system, even addressing power outages [80]. Mollah et al. [83] have observed that P2P trading fosters the balance between energy demand and supply; it also reduces energy losses during distribution. To improve the imbalance of energy production between users, Kwak and Lee [84] have recently designed a BCT-based P2P energy trading platform which includes two main components: a software and a hardware platform. Regarding the software platform, the solution uses Ethereum to permit the transaction to proceed. With respect to the hardware platform, the solution provides a testbed for an energy trading system that includes light emitting diode (LED) sensors, batteries and controllers for both the energy supplier and the consumer. Kumari et al. [85] have also shown that BCT-based P2P trading can improve data flow, thus reducing peak loads.

Third, P2P energy trading enables consumers to create a new energy market as they have access to alternative energy sources [78]. It means that the decentralization of both energy production and distribution could encourage broader social participation. Moreover, the socioeconomic benefits deriving from P2P energy trading could drive increased private investment in RESs [80], as well as encouraging consumers to purchase green energy certificates which ensure they consume only green energy [67].

Fourth, being able to exchange data in a trustworthy manner makes BCT even more attractive for P2P energy trading [86]. Although technologies such as radio frequency identification (RFID) already exist to collect and share information, BCT relies on data encryption and record validation which ensure higher integrity of data [5]. Nevertheless, as the number of prosumers increases, it is crucial to properly manage a growing amount of data streaming from grid operations, surveilling both information security and data loss. To this purpose, BCT-based platforms rely on more efficient and resilient information technology (IT) infrastructures compared to existing systems, ensuring greater transparency [87,88], tamper resistance and security among peers. Furthermore, BCT permits safe storage and ensures the validity of data which is collected through cryptographic techniques that cross-check data sources [89] and is not manipulated by intermediaries [90].

Fifth, smart contracts run on BCT to implement agreements between several parties and to monitor real-time transactions. Prosumers can use smart contracts to agree to trade electricity, defining both the price and the payment method. For instance, parties can agree that the smart contract will automatically perform electricity supply when the price falls below a threshold [89].

Sixth, by drawing on validated data, smart contracts can run on BCT to match energy demand and supply, simultaneously monitoring the consumption and production of energy [91]. Monacchi and Elmenreich [92] have stressed that the energy market usually fails to react to energy demand in real-time due to both the intermittency and the volatility of wind, solar, thermal and other renewable energy technologies [93]. As stated by Joskow [9], the electricity generated by these technologies strongly depends on weather characteristics. It means that electricity is not a homogeneous good in time, because supply and demand vary and electricity storage is costly [93]. Thus, variable renewables are difficult to be controlled or dispatched by system operators based on traditional economic and technical criteria [9]. On the other hand, BCT offers the key to unlock a real-time response through smart contracts by ensuring that excess energy is stored automatically and used whenever the generated output is insufficient. Thus, BCT-based smart contracts directly control energy flow, grid stability [93] and promote interconnectivity among prosumers in a decentralized and fault-tolerant grid [94]. Smart contracts also increase grid flexibility, speed, scalability and security [95].

3.3. Challenges of BCT-Based P2P Energy Trading

The rapid evolution of P2P energy trading has challenged the way utility companies operate [96]. In the past, energy distribution has been made possible across multiple grid levels thanks to the interaction of different actors across interconnected infrastructures. The centralized fossil fuel-based energy market has grown as a vertical structure, based on agreements between few energy providers, retailers and consumers [97]. However, this model is now having to face major issues, such as the loss of energy, long-distance transmission and environmental pollution. Thus, the need to improve energy efficiency and resource allocation has encouraged the recent focus on both renewable energy sources (RESs) and on distributed energy resources (DERs) [83]. Examples of RESs include solar panels and wind turbines, while DERs include both energy storage technology and generation units, namely batteries, photovoltaics and electric vehicles. The diffusion of RESs into the power system has reduced losses as energy is generated close to the place where it is consumed. Moreover, DERs have enabled consumers to control their power, thus reducing gas emissions and saving costs [10]. It means that DERs have made final consumers the active players in the energy market [83]. To do so, BCT-based P2P platforms function as online marketplaces where prosumers trade electricity directly, without the involvement of an intermediary. Prosumers sell electricity in excess to the grid at a 'buy-back rate'. On the contrary, in the traditional vertical model, consumers purchase electricity from utility suppliers at fixed tariffs or time-of-use tariffs [79], and the flow of transactions is mainly unidirectional [98].

However, BCT-based P2P energy trading is still in its developmental stage [99]. Huang et al. [100] have observed that technological readiness is the basis for BCT implementation which is still posing several challenges, namely technology maturity, data security and technical feasibility. Regarding technology maturity, the application of BCT requires important economic investments in infrastructures [101]. Indeed, scalability, interoperability, system performance and calculation time are still the main topics debated by both professionals and academics to ensure the correctness of transactions [14]. Yu et al. [15] have recently developed a new dual-BCT system for P2P energy trading to reduce time-consuming calculations because smart contracts are mainly created for simple calculations and cannot address large interactive computation deriving from complex energy price schemes [102]. The first BCT stores the data of P2P transactions while the second BCT performs the compute-intensive tasks in order to execute P2P energy transactions in a computational efficient manner. As regards to data security, it is crucial to ensure trustworthy BCT-based transactions. It implies that governments and BCT developers should improve user privacy, platform credibility and both on-chain and off-chain data management [103]. Moreover, BCT adoption is still hindered by the cost-effectiveness and feasibility of current BCT-based systems [104].

It is worth noting that BCT continues to lack acceptance among users [80]. The latter are less likely to participate in P2P platforms when BCT runs the operations. This is due to the fact that consumers usually associate BCT with Bitcoin and its price volatility [30]. Thus, building partnership trust is the first step to engage users in a BCT-based P2P model [105]. To do so, local governments and BCT developers should foster information exchange and transparency on BCT-based platforms among citizens and companies [100]. Moreover, goal alignment plays a crucial role in BCT adoption: consumers and firms should be made aware of the importance of taking part in P2P energy trading as a way of exploiting RESs and reducing the environmental footprint of their households and industries in general [105]. Then, governments and BCT developers should promote users' participation in BCT-based P2P energy trading by understanding their needs and expectations [100]. In particular, it is challenging to simulate the decision mechanism in a network with several users since their logics and decisions may clash with the interests of other participants, threatening energy supply and demand [106].

In addition, embedding the P2P model into an existing electricity infrastructure offers a number of issues [107]. Indeed, a P2P trading system cannot be completely detached from the centralized energy infrastructure [108]. On the one hand, an electric power system relies on both the physical system for electricity transmission and the IT system which provides settlement, balancing and billing. On the other, BCT can only automate transactions through smart contracts and record all the transactions in an immutable way. Thus, BCT cannot substitute the whole existing infrastructure. For instance, in the case of trading between two distant peers, the exchange of energy is possible only through power-distribution lines connected to an existing utility company. Moreover, given that RESs are characterized by volatility, prosumers will likely have a stable power source from the centralized energy infrastructure. This means that disintermediation—a key feature of BCT—has not yet been fully implemented in the energy industry [109]. Otherwise, as argued by Javed et al. [106], the energy community (EC) might autonomously address the supply–demand gap by using a diesel generator or local storage.

BCT-based P2P energy trading also implies the management of a large amount of user data, which might raise confidentiality issues [17,72]. Because BCT is designed to ensure the integrity of verifiable transactions, all transaction data on the BCT are visible to the participating nodes [110]. Even when a company uses a private, permissioned BCT, every node participating in the network can capture confidential data. To process such data, the GDPR requires specific precautions such as the prior consent of the data owner. Nevertheless, to the best of our knowledge, there are no standard solutions to protect transaction data while performing prosumer matching on BCT [111,112]. To ensure BCT compliance with the GDPR, consumers and prosumers can use a private Ethereum

BCT [109] that permits anonymity for prosumers, while a retail company can identify prosumers for accounting and billing purposes, through pseudorandom addresses [113]. However, Ethereum is not immune from privacy disclosure. For instance, based on the data stored, unauthorized individuals are able to infer energy consumption habits [114]. On the other hand, Finck [44] has suggested implementing zero-knowledge protocols when designing BCT-based P2P platforms. Developing these protocols, and other encryption techniques, could make BCT more compliant with GDPR provisions because these techniques make it possible to record transactions without showing either which keys were involved or the value transferred [115].

Designing BCT-based P2P platforms poses further data protection challenges with respect to decentralization [10]. Indeed, the emergence of new market actors—e.g., the aggregator—makes it difficult to identify both the data controller or the (joint) controllership, and subsequently to allocate responsibility [66]. This is especially clear when enforcing the GDPR principle of accountability, the right to erasure and the right to rectification [31]. Although these issues are not directly addressed by the Regulation, in June 2022 the EU Observatory published a report entitled "Blockchain Applications in the Energy Sector" which urges the European Commission to collect BCT-based use cases in the energy sector, by adopting an information-sharing approach [116]. The exchange of good practices among practitioners and stakeholders could lead to designing more effective tools, thus improving data protection in BCT-based P2P energy trading.

Table 2 summarizes the main challenges regarding the implementation of BCT-based P2P energy trading platforms. The table also shows the solutions proposed in the literature.

Table 2. BCT-based P2P energy trading platforms: challenges and solutions.

Domains	Challenges	Proposed Solutions
Technological maturity	• Scalability. • Interoperability. • System performance. • Time-consuming calculation.	• Public and private investments, and mixed investment schemes, for infrastructures to foster both scalability and system interoperability. • Dual-BCT system for P2P energy trading to reduce time-consuming calculations and improve system performance.
Disintermediation	• The BCT-based P2P energy trading system cannot be completely detached from the centralized energy infrastructure. • Volatility of RESs.	• BCT-based P2P energy trading systems have to rely on both the physical system for electricity transmission and the IT system which provides settlement, balancing and billing. • To address RES volatility, prosumers should have a stable power source from the centralized energy infrastructure. Otherwise, energy communities should use their own diesel generators or local storage.
Data protection	• BCT compliance with the GDPR. • User privacy uncertainties. • On-chain and off-chain data management.	• Permissioned BCT networks seem closer to GDPR logic due to their more centralized nature. • Implementing zero-knowledge protocols and other encryption techniques, could make BCT more compliant with GDPR provisions. • Enhancing the exchange of good practices among practitioners to design more compliant tools, thus improving data protection.

Table 2. *Cont.*

Domains	Challenges	Proposed Solutions
Social awareness and market players	• Increase BCT-based P2P platform credibility. • Building partnership trust among network users, BCT developers, governments and firms. • Cost-effectiveness of P2P solutions based on RES exploitation.	• Local governments and BCT developers should foster information exchange and transparency about BCT-based platforms, among users and firms. • Making network users aware of the importance of taking part in P2P energy trading as a way of exploiting renewables and reducing the environmental footprint. • Governments and BCT developers should promote users participation by understanding their needs and expectations. • Renewables should be controlled and dispatched by introducing new criteria for both pricing and distribution.

Source: Authors' elaboration.

4. Conclusions

This paper has sought to advance the understanding of various legal and economic challenges that hinder the large-scale deployment of BCT-based P2P energy trading. First, it has reviewed the state of the art of European data protection regulations and the main issues concerning BCT compliance with the General Data Protection Regulation (GDPR). Some key features of BCT—disintermediation, decentralization and immutability—conflict with what are crucial GDPR provisions: the rectification of data stored, the right to be forgotten, the principle of purpose limitation and the principle of data minimization. The French Data Protection Authority (CNIL) has stressed that there is room for harmonization between BCT and the GDPR. In particular, the CNIL has recommended both avoiding any storage of personal data on blockchain and, also, making full use of data obfuscation, encryption and aggregation techniques to anonymize data and collect them off-chain. The EU Observatory too, has emphasized that "[...] Just like there is no GDPR compliant Internet, or GDPR-compliant artificial intelligence algorithm, there is no such thing as a GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications [...]" [39] (p. 4). Although these recommendations are not legally binding, the EU Observatory has strongly encouraged the European Data Protection Board (EDPB), national and European courts to take a clear and shared position to overcome the uncertainties about BCT compliance with European data protection law and regulation. To promote the application of BCT in different industries, a fruitful dialogue among Member States must begin and an updated discipline drawn up.

Second, this paper has explored both the potentials and the challenges of BCT-based P2P energy trading by adopting a legal–economic perspective. While the deployment of BCT-based P2P energy trading is still in its pilot stage, this model is a data-driven innovation able to speed up the decentralization, digitalization and decarbonization of the energy industry, by empowering prosumers. BCT-based P2P places both the producer and the consumer on the same level, as peers, in a decentralized energy market. BCT also changes the transactions concerning energy production and distribution: it avoids any intermediary even while empowering consumers to manage data about supply and consumption. Moreover, BCT unlocks a real-time response to energy demand thanks to the use of smart contracts, and also by balancing energy demand and supply. Thus, BCT has the potential both to reduce transaction costs, and to encourage renewable energy consumption. Overall, P2P energy trading could lead to innovation within the traditional vertical energy value chain by introducing a horizontal platform where consumers or prosumers act as peers and invest in renewable energies.

Nevertheless, BCT-based P2P platforms rely on the collection, storage and elaboration of a large amount of personal data. In particular, data traceability might hamper the

enforcement of data subjects' rights as set out in the GDPR, rights such as the right to erasure and the right to rectification, thus making it difficult to identify the controller(s) and as such to allocate accountability. Although these issues have not been filed with the Court of Justice of the European Union (CJEU), some solutions have been suggested by national data protection authorities and by the EU Observatory. The latter has recently published the study "Blockchain and the General Data Protection Regulation", which has introduced four rule-of-thumb recommendations: (1) assessing the actual need for the blockchain; (2) avoiding storing personal data on a blockchain and making full use of data obfuscation, encryption and aggregation techniques to anonymize data; (3) collecting personal data off-chain, or if the blockchain cannot be avoided, on private, permissioned blockchain networks; and (4) being as clear and transparent as possible with users [39]. These recommendations might prove useful to encourage the adoption of private, permissioned BCT-based P2P platforms and use them in a more secure and effective way. Compared to public BCT, permissioned BCT networks seem closer to GDPR logic due to their more centralized nature. Overall, scholars, practitioners and policy makers have shown a growing need to further explore the intertwined legal–economic features of BCT. This might lead to the spread of standardized BCT-based P2P energy trading among Member States, thus accelerating both the creation of the EU digital market and the transition towards a cleaner and more sustainable energy system.

References

1. Pérez-Montalvo, E.; Zapata-Velásquez, M.-E.; Benítez-Vázquez, L.-M.; Cermeño-González, J.-M.; Alejandro-Miranda, J.; Martínez-Cabero, M.-A.; de la Puente-Gil, A. Model of monthly electricity consumption of healthcare buildings based on climatological variables using PCA and linear regression. *Energy Rep.* **2022**, *8*, 250–258. [CrossRef]
2. Enerdata. Available online: https://d1owejb4br3l12.cloudfront.net/publications/executive-briefing/eu-evolution-households-energy-patterns.pdf (accessed on 2 December 2022).
3. Eurostat. Available online: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220617-1 (accessed on 2 December 2022).
4. Deconinck, G.; Vankrunkelsven, F. Digitalised, decentralised power infrastructures challenge blockchains. *Proc. Inst. Civ. Eng. Smart Infrastruct. Constr.* **2020**, *173*, 29–40. [CrossRef]
5. Shen, B.; Dong, C.; Minner, S. Combating copycats in the supply chain with permissioned blockchain technology. *Prod. Oper. Manag.* **2022**, *31*, 138–154. [CrossRef]
6. Cho, J.; DeStefano, T.; Kim, H.; Kim, I.; Paik, J.H. What's driving the diffusion of next-generation digital technologies? *Technovation* **2022**, *119*, 102477. [CrossRef]
7. Organization for Economic Cooperation and Development (OECD). Available online: https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2020_bb167041-en (accessed on 7 November 2022).
8. Financial Times. Available online: https://www.ft.com/content/7d9874c0-a25d-11e5-8d70-42b68cfae6e4 (accessed on 7 November 2022).
9. Joskow, P.L. Comparing the costs of intermittent and dispatchable electricity generating technologies. *Am. Econ. Rev.* **2011**, *101*, 238–241. [CrossRef]
10. Yahaya, A.S.; Javaid, N.; Alzahrani, F.A.; Rehman, A.; Ullah, I.; Shahid, A.; Shafiq, M. Blockchain based sustainable local energy trading considering home energy management and demurrage mechanism. *Sustainability* **2020**, *12*, 3385. [CrossRef]
11. Cory, K.; Schwabe, P. *Wind Levelized Cost of Energy: A Comparison of Technical and Financing Input Variables*; National Renewable Energy Lab. (NREL): Golden, CO, USA, 2009. [CrossRef]

12. Tushar, W.; Saha, T.K.; Yuen, C.; Smith, D.; Poor, H.V. Peer-to-peer trading in electricity networks: An overview. *IEEE Trans. Smart Grid* **2020**, *4*, 3185–3200. [CrossRef]

13. Abrell, J.; Rausch, S.; Streitberger, C. Buffering volatility: Storage investments and technology-specific renewable energy support. *Energy Econ.* **2019**, *84*, 104463. [CrossRef]

14. Wongthongtham, P.; Marrable, D.; Abu-Salih, B.; Liu, X.; Morrison, G. Blockchain-enabled Peer-to-Peer energy trading. *Comput. Electr. Eng.* **2021**, *94*, 107299. [CrossRef]

15. Yu, T.; Luo, F.; Pu, C.; Zhao, Z.; Ranzi, G. Dual-blockchain-based P2P energy trading system with an improved optimistic rollup mechanism. *IET Smart Grid* **2022**, *5*, 246–259. [CrossRef]

16. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]

17. Wang, D.; Zhao, J.; Wang, Y. A survey on privacy protection of blockchain: The technology and application. *IEEE Access* **2020**, *8*, 108766–108781. [CrossRef]

18. Rossetto, N.; Reif, V. *Digitalization of the Electricity Infrastructure: A Key Enabler for the Decarbonization and Decentralization of the Power Sector*; Florence School of Regulation; [Electricity]; European University Institute: Fiesole, Italy, 2021; Volume 47, Available online: https://cadmus.eui.eu/handle/1814/70736 (accessed on 2 December 2022).

19. Doan, H.T.; Cho, J.; Kim, D. Peer-to-peer energy trading in smart grid through blockchain: A double auction-based game theoretic approach. *IEEE Access* **2021**, *9*, 49206–49218. [CrossRef]

20. Zhou, Y.; Wu, J.; Long, C.; Ming, W. State-of-the-art analysis and perspectives for peer-to-peer energy trading. *Engineering* **2020**, *6*, 739–753. [CrossRef]

21. Mazzola, L.; Denzler, A.; Christen, R. Towards a Peer-to-Peer Energy Market: An Overview. 2020. Available online: http://arxiv.org/abs/2003.07940 (accessed on 7 November 2022).

22. Cali, U.; Cakir, O. Energy policy instruments for distributed ledger technology empowered peer-to-peer local energy markets. *IEEE Access* **2019**, *7*, 82888–82900. [CrossRef]

23. Morstyn, T.; McCulloch, M.D. Peer-to-peer energy trading. In *Analytics for the Sharing Economy: Mathematics, Engineering and Business Perspectives*; Springer: Cham, Switzerland, 2020; pp. 279–300. [CrossRef]

24. Sousa, T.; Soares, T.; Pinson, P.; Moret, F.; Baroche, T.; Sorin, E. Peer-to-peer and community-based markets: A comprehensive review. *Renew. Sustain. Energy Rev.* **2019**, *104*, 367–378. [CrossRef]

25. Compagnucci, L.; Lepore, D.; Spigarelli, F.; Frontoni, E.; Baldi, M.; Di Berardino, L. Uncovering the potential of blockchain in the agri-food supply chain: An interdisciplinary case study. *J. Eng. Technol. Manage.* **2022**, *65*, 101700. [CrossRef]

26. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2020. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 7 November 2022).

27. Zhao, J.L.; Fan, S.; Yan, J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financ. Innov.* **2016**, *2*, 2–7. [CrossRef]

28. Gambino, A.; Bomprezzi, C. Blockchain e protezione dei dati personali. *Il Dirit. Dell'Informazione e Dell'Informatica* **2019**, *35*, 619–646.

29. Islam, I.; Munim, K.M.; Oishwee, S.J.; Islam, A.K.M.N.; Islam, M.N. A critical review of concepts, benefits, and pitfalls of blockchain technology using concept map. *IEEE Access* **2020**, *8*, 68333–68341. [CrossRef]

30. Fell, M.J.; Schneiders, A.; Shipworth, D. Consumer demand for blockchain-enabled Peer-to-Peer electricity trading in the United Kingdom: An online survey experiment. *Energies* **2019**, *12*, 3913. [CrossRef]

31. De Almeida, L.; Cappelli, V.; Klausmann, N.; Van Soest, H. *Peer-to-Peer Trading and Energy Community in the Electricity Market: Analysing the Literature on Law and Regulation and Looking Ahead to Future Challenges*; Florence School of Regulation; [Electricity]; European University Institute: Fiesole, Italy, 2021; Volume 35, Available online: https://cadmus.eui.eu/handle/1814/70457 (accessed on 2 December 2022).

32. van Soest, H. Peer-to-peer electricity trading: A review of the legal context. *Compet. Regul. Netw. Ind.* **2018**, *19*, 180–199. [CrossRef]

33. Yang, Q.; Wang, H. Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain. *IEEE Internet Things J.* **2021**, *8*, 11463–11475. [CrossRef]

34. Siano, P.; de Marco, G.; Rolan, A.; Loia, V. A survey and evaluation of the potentials of distributed ledger technology for Peer-to-Peer transactive energy exchanges in local energy markets. *IEEE Syst. J.* **2019**, *13*, 3454–3466. [CrossRef]

35. Wu, Y.; Wu, Y.; Cimen, H.; Vasquez, J.C.; Guerrero, J.P. P2P energy trading: Blockchain-enabled P2P energy society with multi-scale flexibility services. *Energy Rep.* **2022**, *8*, 3614–3628. [CrossRef]

36. European Commission. Available online: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46 (accessed on 7 November 2022).

37. Ibáñez, L.-D.; Kieron, O.; Simperl, E. On Blockchains and the General Data Protection Regulation. 2018. Available online: https://www.researchgate.net/publication/326913146_On_Blockchains_and_the_General_Data_Protection_Regulation (accessed on 7 November 2022).

38. Daoui, S.; Fleinert-Jensen, T.; Lampiere, M. GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions. *Stanf. J. Blockchain Law Policy* **2019**, *2*, 240.

39. Lyons, T.; Courcelas, L.; Timsit, K. Blockchain and the GDPR. Thematic Report. 2018. Available online: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (accessed on 7 November 2022).

40. European Data Protection Supervisor. Available online: https://edps.europa.eu/data-protection/our-work/subjects/accountability_en (accessed on 7 November 2022).
41. European Court of Justice. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (accessed on 7 November 2022).
42. European Court of Justice. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CC0210 (accessed on 7 November 2022).
43. European Court of Justice. Available online: https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:62017CJ0040 (accessed on 7 November 2022).
44. Fink, M. Blockchains and data protection in the European Union. *Eur. Data Prot. Law Rev.* **2018**, *4*, 17–35. [CrossRef]
45. Commission Nationale de l'Informatique et des Libertés (CNIL). Available online: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf (accessed on 7 November 2022).
46. European Parliament. Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law? 2019. Available online: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (accessed on 7 November 2022).
47. Xu, L.D.; Lu, Y.; Li, L. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet Things* **2021**, *8*, 10452–10473. [CrossRef]
48. Truong, N.B.; Sun, K.; Lee, G.M.; Guo, Y. GDPR-compliant personal data management: A blockchain-based solution. *IEEE Trans. Inf. Secur.* **2020**, *15*, 1746–1761. [CrossRef]
49. Kadena, E.; Holicza, P. Security issues in the blockchain(ed) world. In Proceedings of the IEEE 18th International Symposium on Computational Intelligence and Informatics (CINT), Budapest, Hungary, 21–22 November 2019. [CrossRef]
50. European Parliament. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018IP0373 (accessed on 7 November 2022).
51. Zemler, F.; Westner, M. Blockchain and GDPR: Application scenarios and compliance requirements. In Proceedings of the Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR, USA, 25–29 August 2019. [CrossRef]
52. European Law Institute. Available online: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf (accessed on 7 November 2022).
53. Finck, M.; Pallas, F. They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *Int. Data Priv. Law* **2020**, *10*, 11–36. [CrossRef]
54. Mourby, M.; Mackey, E.; Elliot, M.; Gowans, H.; Wallace, S.; Bell, J.; Smith, H.; Aidinlis, S.; Kaye, J. Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Comput. Law Secur. Rep.* **2018**, *34*, 222–233. [CrossRef]
55. Martini, M.; Weinzierl, Q. Die Blockchain-Technologie und das Recht auf Vergessenwerden. *Neue Z. Für Verwalt.* **2017**, *17*, 1251–1256.
56. Munjal, K.; Bhatia, R. A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex Intell. Syst.* **2022**. [CrossRef] [PubMed]
57. Feige, U.; Fiat, A.; Shamir, A. Zero-knowledge proofs of identity. *J. Cryptol.* **1988**, *1*, 77–94. [CrossRef]
58. Giannopoulou, A. Putting data protection by design on the blockchain. *Eur. Data Prot. Law Rev.* **2021**, *7*, 388–399. [CrossRef]
59. Curtis, S.K.; Lehner, M. Defining the sharing economy for sustainability. *Sustainability* **2019**, *11*, 567. [CrossRef]
60. de Simón-Martín, M.; Bracco, S.; Piazza, G.; Pagnini, L.C.; González-Martínez, A.; Delfino, F. The role of energy communities in the energy framework. In *Levelized Cost of Energy in Sustainable Energy Communities*; Springer: Cham, Switzerland, 2022. [CrossRef]
61. Cuenca, J.J.; Jamil, E.; Hayes, B. State of the art in energy communities and sharing economy concepts in the electricity sector. *IEEE Trans. Ind. Appl.* **2021**, *57*, 5737–5746. [CrossRef]
62. De Almeinda, L.; Klausman, N. Peer-to-Peer, Energy Communities, Legal Definitions and Access to Markets. 2021. Available online: https://fsr.eui.eu/peer-to-peer-energy-communities-legal-definitions-and-access-to-markets/ (accessed on 7 November 2022).
63. Lowitzsch, J.; Hoicka, C.E.; van Tulder, F.J. Renewable energy communities under the 2019 European Clean Energy Package—Governance model for the energy clusters of the future? *Renew. Sustain. Energy Rev.* **2020**, *122*, 109489. [CrossRef]
64. Torabi Moghadam, S.; Di Nicoli, M.V.; Manzo, S.; Lombardi, P. Mainstreaming energy communities in the transition to a low-carbon future: A methodological approach. *Energies* **2020**, *13*, 1597. [CrossRef]
65. Stephant, M.; Hassam-Ouari, K.; Abbes, D.; Labrunie, A.; Robyns, B. A survey on energy management and blockchain for collective self-consumption. In Proceedings of the 7th International Conference on Systems and Control (ICSC 2018), Valencia, Spain, 24–26 October 2018. [CrossRef]
66. World Energy Council. Available online: https://www.worldenergy.org/assets/downloads/Full-White-paper_the-developing-role-of-blockchain.pdf (accessed on 7 November 2022).
67. Esmat, A.; de Vos, M.; Ghiassi-Farrokhfal, Y.; Palensky, P.; Epema, D. A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. *Appl. Energy* **2021**, *282*, 116123. [CrossRef]

68. Thukral, M.K. Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: A review. *Clean Energy* **2021**, *5*, 104–123. [CrossRef]

69. Lei, N.; Masanet, E.; Koomey, J. Best practices for analyzing the direct energy use of blockchain technology systems: Review and policy recommendations. *Energy Policy* **2021**, *156*, 112422. [CrossRef]

70. Council of European Energy Regulators. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A3 2018L2001 (accessed on 7 November 2022).

71. Greenspan, G. Avoiding the Pointless Blockchain Project. Available online: https://www.multichain.com/blog/2015/11/ avoiding-pointless-blockchain-project/ (accessed on 2 December 2022).

72. Baashar, Y.; Alkawsi, G.; Alkahtani, A.A.; Hashim, W.; Razali, R.A.; Tiong, S.K. Toward Blockchain Technology in the Energy Environment. *Sustainability* **2021**, *13*, 9008. [CrossRef]

73. Malone, T.; Yates, J.; Benjamin, R. Electronic markets and electronic hierarchies. *Commun. ACM* **1987**, *30*, 484–497. [CrossRef]

74. Wilkinson, S.; Hojckova, K.; Eon, C.; Morrison, G.M.; Sandén, B. Is peer-to-peer electricity trading empowering users? Evidence on motivations and roles in a prosumer business model trial in Australia. *Energy Res. Soc. Sci.* **2020**, *66*, 101500. [CrossRef]

75. Catalini, C.; Gans, J.S. Some simple economics of the blockchain. *Commun. ACM* **2020**, *63*, 80–90. [CrossRef]

76. Sun, R.; Garimella, A.; Han, W.; Chang, H.; Shaw, M.J. Transformation of the transaction cost and the agency cost in an organization and the applicability of blockchain—A case study of Peer-to-Peer insurance. *Front. Blockchain* **2020**, *3*, 24. [CrossRef]

77. Peters, G.; Panayi, E. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. 2015. Available online: https://ssrn.com/abstract=2692487 (accessed on 2 December 2022). [CrossRef]

78. Abdella, J.; Shuaib, K. Peer to Peer distributed energy trading in smart grids: A survey. *Energies* **2018**, *11*, 1560. [CrossRef]

79. International Renewable Energy Agency (IRENA). Available online: https://irena.org/-/media/Files/IRENA/Agency/ Publication/2020/Jul/IRENA_Peer-to-peer_trading_2020.pd (accessed on 7 November 2022).

80. Junlakarn, S.; Kokchang, P.; Audomvongseree, K. Drivers and challenges of peer-to-peer energy trading development in Thailand. *Energies* **2022**, *15*, 1229. [CrossRef]

81. Scuri, S.; Tasheva, G.; Barros, L.; Nunes, N.J. An HCI perspective on distributed ledger technologies for Peer-to-Peer energy trading. In Proceedings of the 17th IFIP Conference on Human-Computer Interaction (INTERACT), Paphos, Cyprus, 2–6 September 2019. [CrossRef]

82. Brisbois, M.C. Powershifts: A framework for assessing the growing impact of decentralized ownership of energy transitions on political decision-making. *Energy Res. Soc. Sci.* **2018**, *50*, 151–161. [CrossRef]

83. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things* **2021**, *8*, 18–43. [CrossRef]

84. Kwak, S.; Lee, J. Implementation of blockchain based P2P energy trading platform. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Republic of Korea, 13–16 January 2021; pp. 5–7. [CrossRef]

85. Kumari, A.; Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. When blockchain meets smart grid: Secure energy trading in demand response management. *IEEE Netw.* **2020**, *34*, 299–305. [CrossRef]

86. Brilliantova, V.; Thurner, T.W. Blockchain and the future of energy. *Technol. Soc.* **2019**, *57*, 38–45. [CrossRef]

87. Mannaro, K.; Pinna, A.; Marchesi, M. Crypto-trading: Blockchain-oriented energy market. In Proceedings of the 2017 AEIT International Annual Conference, Cagliari, Italy, 20–22 September 2017.

88. Ahl, A.; Yarime, M.; Tanaka, K.; Sagawa, D. Review of blockchain-based distributed energy: Implications for institutional development. *Renew. Sustain. Energy Rev.* **2019**, *107*, 200–211. [CrossRef]

89. Peter, V.; Paredes, J.; Rosado Rivial, M.; Soto Sepúlveda, E.; Hermosilla Astorga, D.A. *Blockchain Meets Energy: Digital Solutions for a Decentralized and Decarbonized Sector*; European University Institute: Fiesole, Italy, 2019; Available online: https://cadmus.eui. eu/handle/1814/63369 (accessed on 2 December 2022)Florence School of Regulation; Energy.

90. Di Silvestre, M.L.; Gallo, P.; Guerrero, J.M.; Musca, R.; Riva Sanseverino, E.; Sciumè, G.; Vásquez, J.; Zizzo, G. Blockchain for power systems: Current trends and future applications. *Renew. Sustain. Energy Rev.* **2020**, *119*, 109585. [CrossRef]

91. Dong, H.; Chengzhenghao, Z.; Jian, P.; Zheng, Y. Smart contract architecture for decentralized energy trading and management based on blockchains. *Energy* **2020**, *199*, 117417. [CrossRef]

92. Monacchi, A.; Elmenreich, W. Assisted energy management in smart microgrids. *J. Ambient Intell. Hum. Comput.* **2016**, *7*, 901–913. [CrossRef]

93. Kounelis, I.; Steri, G.; Giuliani, R.; Geneiatakis, D.; Neisse, R.; Nai Fovino, I. Fostering consumers' energy market through smart contracts. In Proceedings of the International Conference in Energy and Sustainability in Small Developing Economies (ES2DE), Funchal, Portugal, 10–12 July 2017. [CrossRef]

94. Kapassa, E.; Themistocleous, M.; Touloupos, M.; Quintanilla, J.R.; Papadaki, M. Blockchain in smart energy grids: A market analysis. In Proceedings of the 17th European, Mediterranean, and Middle Eastern Conference (EMCIS), Dubai, United Arab Emirates, 25–26 November 2020.

95. Mylrea, M.; Gourisetti, S.N.G. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In Proceedings of the 2017 Resilience Week (RWS), Wilmington, DE, USA, 18–22 September 2017; pp. 18–23. [CrossRef]

96. Nai Fovino, I.; Andreadou, N.; Geneiatakis, D.; Giuliani, R.; Kounelis, I.; Lucas, A.; Marinopoulos, A.; Martin, T.; Poursanidis, I.; Soupionis, I.; et al. *Blockchain in the Energy Sector*; Publications Office of the European Union: Luxembourg, 2021. [CrossRef]

97. Borges, C.E.; Kapassa, E.; Touloupou, M.; Legarda Macón, J.; Casado-Mansilla, D. Blockchain application in P2P energy markets: Social and legal aspects. *Connect. Sci.* **2022**, *34*, 1066–1088. [CrossRef]
98. Vieira, G.; Zhang, J. Peer-to-peer energy trading in a microgrid leveraged by smart contracts. *Renew. Sustain. Energy Rev.* **2021**, *143*, 110900. [CrossRef]
99. Wang, Q.; Su, M. Integrating BCT into the energy sector—From theory of blockchain to research and application of energy blockchain. *Comput. Sci. Rev.* **2020**, *37*, 100275. [CrossRef]
100. Huang, L.; Zhen, L.; Wang, J.; Zhang, X. Blockchain implementation for circular supply chain management: Evaluating critical success factors. *Ind. Market. Manag.* **2022**, *102*, 451–464. [CrossRef]
101. Wang, H.; Chen, K.; Xu, D. A maturity model for blockchain adoption. *Financ. Innov.* **2016**, *2*, 12. [CrossRef]
102. Yang, J.; Paudel, A.; Gooi, H.B.; Nguyen, H.D. A proof-of-stake public blockchain based pricing scheme for peer-to-peer energy trading. *Appl. Energy* **2021**, *298*, 117154. [CrossRef]
103. Esposito, C.; de Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
104. Chod, J.; Trichakis, N.; Tsoukalas, G.; Aspegren, H.; Weber, M. On the financing benefits of supply chain transparency and blockchain adoption. *Manag. Sci.* **2020**, *66*, 4378–4396. [CrossRef]
105. Khaqqi, K.N.; Sikorski, J.J.; Hadinoto, K.; Kraft, M. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Appl. Energy* **2018**, *209*, 8–19. [CrossRef]
106. Javed, H.; Irfan, M.; Shehzad, M.; Abdul Muqeet, H.; Akhter, J.; Dagar, V.; Guerrero, J.M. Recent trends, challenges, and future aspects of p2p energy trading platforms in electrical-based networks considering blockchain technology: A roadmap toward environmental sustainability. *Front. Energy Res.* **2022**, *10*, 810395. [CrossRef]
107. Parag, Y.; Sovacool, B.K. Electricity market design for the prosumer era. *Nat. Energy* **2016**, *1*, 16032. [CrossRef]
108. Espe, E.; Potdar, V.; Chang, E. Prosumer communities and relationships in smart grids: A literature review, evolution and future directions. *Energies* **2018**, *11*, 2528. [CrossRef]
109. Son, Y.-B.; Im, J.-H.; Kwon, H.-Y.; Jeon, S.-Y.; Lee, M.-K. Privacy-preserving Peer-to-Peer energy trading in blockchain-enabled smart grids using functional encryption. *Energies* **2020**, *13*, 1321. [CrossRef]
110. Majeed, U.; Khan, L.U.; Yaqoob, I.; Ahsan Kazmi, S.M.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
111. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
112. German Energy Agency (DENA). Available online: https://www.dena.de/fileadmin/user_upload/dena-Studie_Blockchain_Integrierte_Energiewende_EN.pdf (accessed on 7 November 2022).
113. Rui, Z.; Rui, X.; Ling, L. Security and privacy on blockchain. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]
114. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
115. Lang, M.; Müller, M. Blockchain and smart contracts in the energy industry: A European perspective. In Proceedings of the International Mining and Oil & Gas Law, Development, and Investment, Rio de Janeiro, Brazil, 10–12 April 2019; p. 17B-1. Available online: https://www.twobirds.com/-/media/pdfs/blockchain-and-smart-contracts-in-the-energy-industry--article.pdf (accessed on 7 November 2022).
116. EU Blockchain Observatory & Forum. Available online: https://www.eublockchainforum.eu/sites/default/files/reports/EUBOF-Thematic_Report_Energy_Sector_0.pdf (accessed on 7 November 2022).