A Blockchain-based Privacy-friendly Renewable Energy Community

Stephan Cejka[1], Franz Zeilinger[1], Argjenta Veseli[2], Marie-Theres Holzleitner[2] and Mark Stefan[3]
[1]*Siemens AG Österreich, Vienna, Austria*
[2]*Energieinstitut an der Johannes Kepler Universität Linz, Linz, Austria*
[3]*AIT Austrian Institute of Technology GmbH, Vienna, Austria*

Keywords: Energy Community, Privacy, Blockchain, Clean Energy Package, Energy Transition, Energy Efficiency.

Abstract: The European Union's Clean Energy Package introduces two kinds of energy communities, namely the Renewable Energy Community (REC) in the Renewable Energy Directive of 2018 and the Citizen Energy Community (CEC) in the Electricity Directive of 2019. They aim for local improvements of energy efficiency, increasing integration of renewable energy sources, and a reduction of greenhouse gas emissions, to be achieved by jointly producing, temporarily storing, sharing, consuming, and selling locally generated energy. Households and individuals shall thus be enabled to take an active part in the energy transition. When utilizing blockchain technology for the implementation of such energy communities, as proposed in current research projects, a focus must be laid on the technology-inherent area of conflict with privacy issues, especially since data on households' energy consumption count as personal data.

1 INTRODUCTION

Among the biggest challenges of our time is the climate change caused by enormous man-made emissions of greenhouse gas. The global temperature level has risen significantly in the last few decades and the rise is expected to continue if no or not-sufficient countermeasures are taken (IPCC, 2014). To limit the continuing temperature rise to globally stipulated values in the 2016 Paris agreement (UNFCCC, 2016), the European Union aims to reduce greenhouse gas emissions by at least 40 % by 2030 (European Commission, 2019a). It addressed the energy sector, being one of the biggest sources of emissions (IPCC, 2014), by issuing the 'Clean Energy for all Europeans Package' in 2018/2019 (European Commission, 2019c; European Commission, 2019b). This shall also aim to reach further key targets for 2030, which are a share of at least 32 % of renewable energy and an improvement of at least 32.5 % in energy efficiency (European Commission, 2019a).

As suggested countermeasures on the local level, the Clean Energy Package introduces two kinds of energy communities to merge the energy production as well as the consumption of individuals and enterprises. While awaiting concrete transpositions of the Clean Energy Package's directives into national law of the European Union's member states, some research projects are already dealing with possible implementations; for example, by using blockchain technology as proposed in this paper.

We will first introduce the Clean Energy Package with special focus on energy communities (Section 2). Afterwards, we will go into detail about blockchain technology, including its known issues with privacy and energy efficiency (Section 3). The main contribution of this paper will be to combine the two aspects, by describing a possible implementation of a privacy-friendly blockchain-based renewable energy community (Section 4).

2 CLEAN ENERGY PACKAGE

The latest development in European Union's energy law is its 'Clean Energy for all Europeans Package', first proposed in 2016, and finally adopted by the European Parliament, partly in the end of 2018 and partly in Summer 2019. One of its main goals is to bring EU and its member states on track for the revised climate targets for 2030 (European Commission, 2019c; European Commission, 2019a; European Commission, 2019b). The package itself, consists of four directive and four regulation acts:

- Energy Performance of Buildings Directive (EU) 2018/844,

Cejka, S., Zeilinger, F., Veseli, A., Holzleitner, M. and Stefan, M.
A Blockchain-based Privacy-friendly Renewable Energy Community.
DOI: 10.5220/0009391300950103
In *Proceedings of the 9th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2020)*, pages 95-103
ISBN: 978-989-758-418-3

- **Renewable Energy Directive (EU) 2018/2001**,
- Energy Efficiency Directive (EU) 2018/2002,
- Governance of the Energy Union and Climate Action Regulation (EU) 2018/1999,
- Electricity Regulation (EU) 2019/943,
- **Electricity Directive (EU) 2019/944**,
- Regulation on Risk-Preparedness in the Electricity Sector (EU) 2019/941,
- Regulation on the European Union Agency for the Cooperation of Energy Regulators (EU) 2019/942.

The two acts of main interest for the scope of this paper are printed in bold; the revised Renewable Energy Directive (RED II) introducing 'Renewable Energy Communities (RECs)' and the revised Electricity Directive (ED II) introducing 'Citizen Energy Community (CECs)' as a second type of energy communities.

2.1 Evolution to Energy Communities

Those energy communities are a third step in an evolution shown in Figure 1, starting with households optimizing their own energy consumption and proceeding by applying those procedures to apartment buildings next. They are termed 'renewables self-consumer' and 'jointly acting renewables self-consumers' in the definitions of RED II:

Renewables Self-consumer: 'a final customer [...] who generates renewable electricity for its own consumption, and who may store or sell self-generated renewable electricity activity'.

Jointly Acting Renewables Self-consumers: 'a group of at least two jointly acting renewables self-consumers [...] who are located in the same building or multi-apartment block'.

According to RED II, those parties shall be able to 'generate, consume, store, and sell electricity without facing disproportionate burdens' and '[c]itizens living in apartments [...] should be able to benefit [...] to the same extent as households in single family homes'.

Main parts of the two energy communities' definitions are similar while some differences between them exist though. Their legal definitions in RED II and ED II can be summarized as follows:

Renewable Energy Community:

- a legal entity, based on open and voluntary participation, and autonomous,
- controlled by its shareholders or members, which are natural persons, small or medium enterprises, or local authorities,

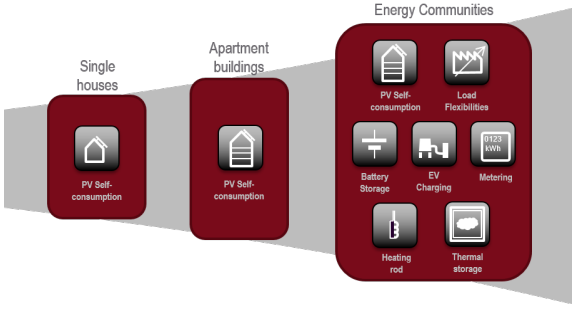

Figure 1: Evolution to energy communities.

- shareholders or members are located in the proximity of renewable energy projects owned and developed by that legal entity,
- its primary purpose is to provide environmental, economic or social community benefits rather than financial profits.

Citizen Energy Community:

- a legal entity, based on open and voluntary participation,
- controlled by shareholders or members that are natural persons, small enterprises, or local authorities; but open for participation of other entities,
- its primary purpose is to provide environmental, economic or social community benefits rather than financial profits,
- it may engage in generation, including from renewable sources, distribution, supply, consumption, aggregation, energy storage, energy efficiency services or charging services for electric vehicles or provide other energy services.

The often appearing term 'local energy community' was contained in the European Commission's draft of the ED II, but was abandoned in favor of the term CEC. However, despite the CEC not having a proximity aspect, in our opinion this technical term is properly suited as an umbrella term for RECs and CECs. Speaking of RECs' proximity aspect, this is one of the main difference between those communities. While an REC's participant needs to be located in close proximity to the community's renewable energy projects, CEC's participants may be widely spread – optionally also over member states' borders. CEC's legal definition includes a number of activities they are able to perform, while REC's definition does not explicitly contain such an enumeration.

However, this paper does not intend to give an in-depth analysis of RECs' and CECs' commonalities and differences (cf. (Cejka, 2020)). The intention is

to describe a possible – and already realized – implementation of an REC; thus, the remainder of this paper will focus on this type of energy communities.

2.2 Renewable Energy Communities

RECs aim for the participation of individuals to improve the local acceptance of renewable energy, local investment, and improved participation of citizens in the energy transition. To that end, the REC shall become a non-discriminating position among the other (larger) competing players on the energy market. In result, the REC shall be enabled to

- produce, consume, store and sell renewable energy,
- share produced renewable energy within the community,
- and access energy markets in a non-discriminatory manner.

Its participants have to incorporate an autonomous legal entity, effectively controlled by them. They have to be located in the REC's proximity, which requires a clarification in the national implementations by either applying technically or geographically defined boundaries. Furthermore, participation is open and voluntary, and shall also be open to indigent participants. In contrast to CECs, RECs are not limited to electricity, but could operate on all kinds of renewable energy (e.g., heating, cooling). Still, there are some open questions remaining, not only for the legal process; for instance, a desired minimum or maximum size of a community, a specification about the desired mix of producers and consumers within a community, the desired 'environmental, economic, or social community benefits' for the community itself, its participants, and the general public, etc.

2.3 National Implementations

National implementations of the directives are due partly at the end of 2020 (e.g., the ED II), partly at the end of June 2021 (e.g., the RED II). Some open issues have been identified to remain open for the national adoption (cf. (Cejka, 2020)). *Frieden et al.* provided a technical report on the current state of the implementations of collective self-consumption and energy communities into national law in June 2019 (Frieden et al., 2019). Accordingly, of 15 investigated Europen Union member states, 7 already have legal frameworks for collective self-consumption, only 3 for energy communities. However, legislative processes for national implementations have been started in some member states. Especially once approaching the implementation deadlines, significant changes to the report's described state need to be considered.

3 BLOCKCHAIN

The use of blockchain technology is increasingly discussed and introduced in many areas (Casino et al., 2019), including the energy sector (Andoni et al., 2019; Alladi et al., 2019; Ahl et al., 2020). Proleptic to national legal adoptions of RECs, research projects are engaging with REC implementations using blockchain technology. As already done by many authors, this paper will skip an introduction into blockchain technology. In this regard, we want to especially point to (Joint Research Centre, 2019; Finck, 2019a) introducing and covering various aspects of blockchain technology. However, privacy issues with blockchain technology are well-known and necessarily need to be taken care of in these projects. Though using blockchain technology seems to be incompatible with privacy law at first sight, there are options to stay compatible. As many authors previously engaged with privacy issues in blockchain technology (e.g., (Finck, 2019a)), this paper will only focus on a few picked aspects of special interest within the use case.

3.1 Privacy Aspects

The General Data Protection Regulation (GDPR) is the main European Union's privacy act. As in the form of a regulation act, it is directly applicable in all 27 member states. It is applicable only for 'personal data' of a data subject, i.e., 'any information relating to an identified or identifiable natural person'. In fact, households' energy consumption data are personal data, as they could reveal much of personal habits when recorded in high frequencies, for example, by Smart Meters (Tang et al., 2015; Greveler et al., 2012). Due to their increasing roll-out around the globe, many authors have previously been engaged with their privacy issues (Cejka et al., 2019; Martinez et al., 2019). For energy communities, a high frequency read-out of energy production and consumption will be necessary; participants will thus be required to be equipped with a Smart Meter.

3.1.1 Identification of the Data Subject

A person is identifiable if it can be unmistakably identified with any available means, including the combination with additional available information in order

to establish a concrete reference to a person. According to the GDPR, all means 'reasonably likely to be used' to identify the respective natural person directly or indirectly are included in this context, taking objective factors such as cost and time involved as well as available technical means into account. Data that is not traceable to any individual is 'anonymous data' and thus not subject to privacy law. It should be noted that pseudonymized data also falls under the term of personal data and that the GDPR remains applicable. Encrypting data is also only a form of pseudonymization that does not remove the reference to an individual.

The application at hand requires to keep the assignment of individuals with their energy production and consumption data, as well as the involved parties in their energy trades. It is expected, that – at least for the time being – the number of participants in RECs will be limited. Therefore, the assignment to a specific subscriber is easily possible even when using pseudonyms. Furthermore, for energy communities most probably a private and permissioned blockchain is used rather than a public and permissionless blockchain; i.e., only authorized entities have access to the blockchain and those entities need to be authorized to execute transactions rather than permitting anyone. Thus, by design an authority is required, that is responsible for adding participants to and removing them from the blockchain, as well as to define proper roles for them. This authority necessarily needs to maintain an exact mapping between individuals and their blockchain pseudonyms' representation.

3.1.2 The Controller

According to the GDPR, the 'controller' 'determines the purposes and means of the processing of personal data'. Its main duty is to take appropriate technical and organisational measures to ensure adequate protection for privacy risks. Furthermore, it is required to ensure that only personal data is processed whose processing is required for the particular purpose. However, in blockchain applications, it is not a priori clear who serves as this controller. Eligible characters are the application's programmer, the application's initiator, every participant executing a transaction, the miner, or the node operator (EU Blockchain Observatory and Forum, 2018). Depending on the use case either none, one, or more of the mentioned options can serve as the controller. In result, the question on who is in charge can only be answered for a concrete use case, but not for blockchain applications per se. If all nodes are considered as controllers, they are nevertheless no 'joint controllers' according to the GDPR, as they do not 'jointly determine the purposes and means of processing' (Finck, 2019a).

3.1.3 Rights of the Data Subject

The GDPR stipulates various rights of the data subject, which the controller is responsible to fulfill. Among them are the 'right to rectification' and the 'right to erasure', which are of special interest in blockchain applications due to their technology-intrinsic immutability of persisted data. Later modifications or even deletions of data on the blockchain are thus not possible. This immutability aspect is one of the biggest advantages of the blockchain from a technical point of view, but critical from the data protection perspective. Thus, special technical and organisational measures need to be taken to ensure suitable fulfillment of those rights.

Principles. In this context, some principles of the GDPR need to be mentioned: Pursuant to the principle of **storage limitation**, personal data may only be kept for as long as necessary in regard of the purposes they were collected for. This requires in particular that the storage period for personal data is limited to the absolutely necessary minimum. Close-by, pursuant to the principle of **data minimization**, only the minimum required personal data for the specific use case shall be collected.

Access and Information. The data subject has the right to know whether and to what extent its personal data is processed by whom and for which purposes. This right of information is the central right in order to claim further rights, for example, the right to rectification, erasure etc.

Amendment. The GDPR requires all personal data to be accurate and up-to-date. Thus, every reasonable step with regard to the specific technology must be taken to correct wrong data. However, modifications of old data on the blockchain are not possible. Thus, it may be sufficient to add the new corrected data as a supplementary statement (Finck, 2019a), though still keeping the old outdated data on the blockchain.

Erasure. If a person no longer wishes their data to be processed and there is no legitimate reason to retain it, its personal data must be deleted by the controller. Furthermore, the controller is obliged to take 'appropriate measures' to inform other controllers and processors of the data subject's request. However, as the GDPR contains no clear definition of erasure, it can be argued that the requirements are not placed

too high. It is arguable to be sufficient if the particular personal data becomes unrecognisable for the processor, i.e., to become illegible or to be no longer available. Furthermore, a supplementary statement disallowing its further processing may be reasonable.

There are proposals for introducing mutability into the blockchain (Politou et al., 2019; Ateniese et al., 2017); however, we disapprove to discard main blockchain principles such as its immutability aspect. Thus, access should be blocked – in an appropriate technical way – without the need to destroy individual data records or change the blockchain's principles.

3.1.4 Data Protection Impact Assessment

GDPR contains the fundamental ideas of 'privacy by design and by default' to ensure a correct handling of personal data in every use case ab initio. Thus, the immutability of persisted data on the blockchain can be considered early in the design of the use cases. The GDPR requires to carry out a 'data protection impact assessment' (DPIA) prior to the data processing if it 'is likely to result in a high risk to the rights and freedoms of natural persons', in particular when using new technologies. The *Article 29 Data Protection Working Party* has issued additional guidelines for criteria in which a high risk can be assumed, which include (Article 29 Data Protection Working Party, 2017):

- data processing on large scale (concerning the number of concerned data subjects, the volume of data processed, the duration or permanence of the data processing activity, the geographical extent of the processing activity),
- innovative use or applying new technological solutions,
- when processing prevents data subjects from exercising a right.

In our opinion, especially the listed criteria are applicable to solutions utilizing blockchain technology as a 'new technology'. According to the GDPR, a DPIA needs to contain at least:

- a description of the envisaged processing operations and their purposes,
- an assessment of the necessity and proportionality of the processing operations,
- an assessment of the risks to the rights and freedoms of data subjects, and
- the measures envisaged to address the risks.

The DPIA needs to be carried out by the controller. However, in our opinion this should be the duty of the initiator of the blockchain application, as this corresponds best to the fundamental 'privacy by design' idea.

3.1.5 Smart Contracts

When using 'smart contracts', a program code triggers an action once an event matches a corresponding contract content without further human intervention. Participants determine desired parameters, for example, at which price how much electricity shall be purchased or sold. As soon as matching declarations of intent of two contracting parties are recognized, the contract is automatically concluded ('matching'), executed on-chain and cannot be rolled-back.

The RED II contains a definition for 'peer-to-peer trading', which – in our opinion – sounds a lot like considering smart contracts for trading (renewable) energy between self-consumers and within energy communities. It is defined as 'the sale of renewable energy between market participants by means of a contract with pre-determined conditions governing the automated execution and settlement of the transaction'. Listed among the DPIA criteria of the *Article 29 Data Protection Working Party* report is also the 'automated-decision making with legal or similar significant effect' (Article 29 Data Protection Working Party, 2017). Furthermore, the *Article 29 Data Protection Working Party* issued an own report on automated individual decision-making (Article 29 Data Protection Working Party, 2018). Only recently, *Finck* dealt with privacy-related questions of smart contracts, that can be subsumed under GDPR's regulation on 'automated individual decision-making' (Finck, 2019b). According to GDPR, the data subject has the right 'not to be subject to a decision based solely on automated processing' producing legal or similarly significant effects. This does not apply, if the decision

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorised by law, which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

It needs to be noted, that smart contracts are not necessarily concluded between the data subject and the controller only. However, there are opinions that define the publisher of a smart contract, or anyone executing this contract (i.e., in essence, every node) as a controller (EU Blockchain Observatory and Forum, 2018). Furthermore, smart contracts are neither smart

in sense of AI nor contracts in the legal sense (Finck, 2019b). In essence, they are `if/then` relations only, computer code that may nevertheless produce legal effects.

Numerous regulations, for example, of civil law, data protection law, consumer protection law, tax law, e-commerce law etc., have to be taken into account within the framework of smart contracts, which cannot, however, be elaborated further in this study.

3.2 Energy Efficiency

Energy communities aim to improve local energy efficiency, yet blockchains are in fact not known for providing an energy efficient operation (de Vries, 2018; Vranken, 2017). It is estimated that the cumulative energy consumption of blockchains already exceeds the energy consumption of medium-sized countries. This is due to the enormous use of energy for the 'proof-of-work' consensus protocol, implemented, for example, in the probably best known blockchain – the Bitcoin blockchain (Joint Research Centre, 2019). According to *University of Cambridge*, the energy consumption of this blockchain alone currently already exceeds those of countries such as Finland, Belgium, or Austria (University of Cambridge, 2020). For energy community applications, however, we do not require a big blown public blockchain. We thus use the 'proof-of-authority' consensus protocol, utilizing a subset of blockchain nodes, trusted to generate new blocks on the chain on behalf of all nodes.

4 A PRIVACY-FRIENDLY BLOCKCHAIN-BASED ENERGY COMMUNITY

The result of the privacy considerations is to avoid persisting personal data on a blockchain whenever possible. To mitigate data protection issues, the use of a combined system with a classic distributed database is often proposed (Zyskind et al., 2015; EU Blockchain Observatory and Forum, 2018). Thus, personal data are saved off-chain; pointers to those data records and their hash values are saved on the blockchain. Modifications are possible in the data base while keeping the pointer on the blockchain intact. They can be identified by comparing the persisted initial hash value on the blockchain with the current one. Deletions in the data base will result in the pointer pointing to an empty cell. In this regard, we do not count hash values as personal data anymore as proper hash functions do not allow to deduce back to the original personal data value. However, this opinion is not yet clarified as some sources do see hash values as pseudonymized data only which would not suspend the applicability of the GDPR (Finck, 2019a; Article 29 Data Protection Working Party, 2014).

If it cannot be avoided to save personal data on the chain itself, additional technical and organisational measures, for example, pseudonymization, anonymization, encryption, must be taken. In that case, accurate handling of encryption keys need to be guaranteed, including the proper dismissal of those keys on a deletion request.

4.1 Architecture

The described solution uses a different approach by only temporarily storing personal energy consumption data. This architecture (Figure 2) intends to meet the requirements for operating an REC as well as of data protection. The central element is a permissioned blockchain, which limits the number of participants. New participants must be added by a central authority, such as the community's operator or administrator ('community representative').

The proof-of-authority process is used as a consensus algorithm for the formation of new blocks, in which only certain assigned participants (so-called 'sealers') write encrypted transactions into the blockchain. In addition to these sealers, there can also be 'full nodes' that also store a full local image of the blockchain ('Node DB'), but do not necessarily have to be a community participant[1]. The nodes' task is to enable the operation and updating of the blockchain for the community. It is assumed that in addition to the actual operator, other parties are accepted by the participants to also operate a node (e.g., the energy regulator or other legal authorities). In the proposed approach, the distribution system operator (DSO) also operates a node in order to be able to process grid capacity releases via the blockchain. Nodes can be added or removed dynamically; in the proof-of-authority process sealers generate blocks in a defined sequence; in case of the particular sealer failing, the block is formed by the next sealer.

The infrastructure server is operated and maintained by the infrastructure manager of the community, which may also be the DSO. The task of this server is the distribution of the information necessary for the operation of the blockchain, the active smart contracts, the configuration of the participants and of

[1]Sealers and full nodes are summarized in Figure 2 and below as 'nodes'.

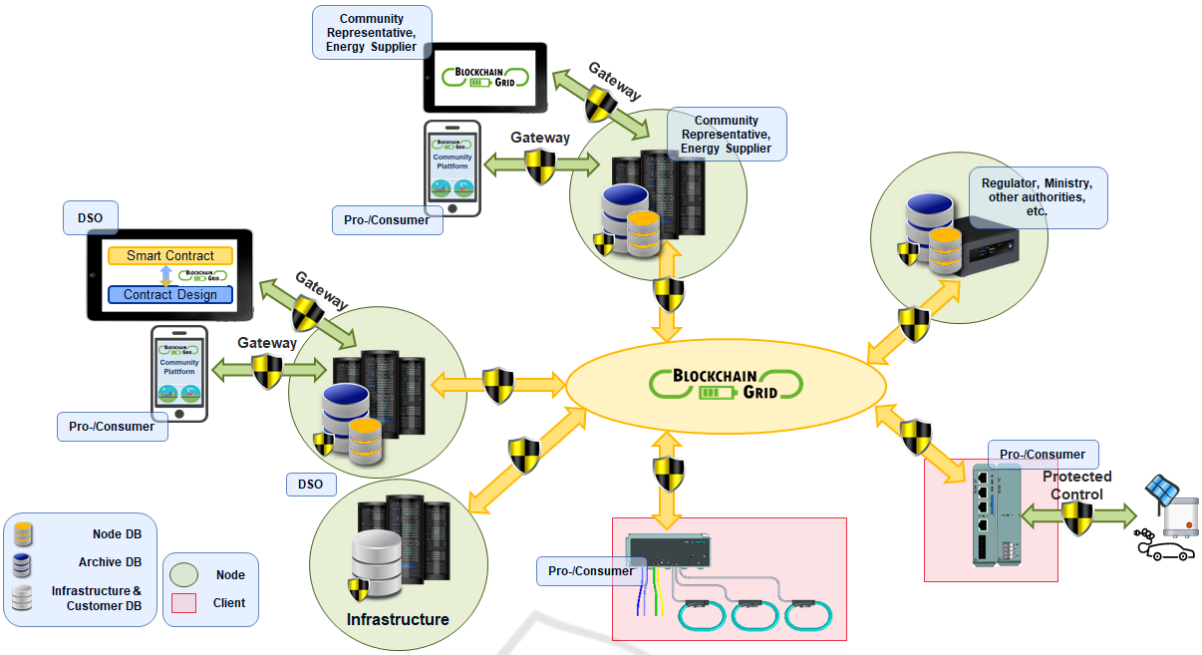

Figure 2: Structure of the privacy friendly blockchain implementation of an energy community.

the nodes. In addition, roles are assigned to the individual participants to determine access rights to data within the blockchain. An assignment of real customer data to the pseudonym in the blockchain is only possible for the infrastructure manager as administrator. This is necessary in order to be able to transmit billing-relevant information to the operator. Data is stored in encrypted form, thus it can be read out by authorized persons only. Along with that all data is exchanged via encrypted connections to ensure maximum data security.

In contrast, end customers as well as local producers are connected to the blockchain as so-called clients only. Customers equipped with their own photovoltaic installation are termed 'prosumers' in combination. Their connection is made exclusively via measuring devices and other sensors or actuators. These hardware elements determine the energy or power flows of the participants into or from the distribution grid. They write these measurements as encrypted data into the blockchain, using appropriate data processing and the communication infrastructure. Clients do not store a complete image of the blockchain, only as far as they require data for the execution of transactions. If data from the blockchain must be passed on to other devices (e.g., to control a charging station for electric vehicles), this is also done via a secure connection ('Protected Control').

By utilizing blockchain technology, stored information (e.g., invoices) can be made available to the participants in a traceable and transparent manner at all times. This creates a high level of acceptance of the technology and trust among the participants. Access to data of the participants is possible in accordance with defined access rights via a web servers or 'Gateway' operated by the individual nodes. Examples of such data are measurements, sales or purchases in or from the community or the storage use of a central battery storage system. The implemented gateways also offer the option of accepting customer settings and forwarding them to the smart contracts (e.g., whether the participant favors to save his surpluses in the battery system for its own later use or if the surplus should rather be distributed within the community).

Peer-to-peer trading within the energy community and the use of the battery system are fully automated by executing smart contracts in the blockchain. Taking the access rights into account, additional tools (e.g., 'Smart Contract / Contract Design') can be connected via a 'Gateway'. Authorized agents can observe and analyze energy flows and thereby draw conclusions for an improvement in the community's operation.

4.2 Implementation in Relation to Data Protection

Due to the previously mentioned technical implementation and the management of the energy community

by the DSO, it is identified as the responsible entity for data protection ('controller') in the proposed system. While this remains questionable regarding smart contracts, the stipulation of the DSO as infrastructure operator does not rule out that there may be other entities responsible for a specific application.

Based on the use cases listed, the following data can be derived, which the REC participants store in pseudonymized form in the blockchain:

- actual energy values in high time resolution,
- amount of energy sold to other energy community participants,
- purchased amount of energy from other energy community participants,
- amount of energy stored in the central storage system,
- amount of energy retrieved from the central storage system.

In addition to the amount of energy, information about the energy price is stored in order to enable billing and to make this data transparent and available to every participant. Unlike the aforementioned energy data, which can be assigned to the respective community participant, price data does not belong to the category of personal data and is therefore not covered by data protection laws.

Subsequently, in accordance with the data minimization principle, the purpose for which personal data is collected or processed needs to be determined:

- execution of the smart contracts (e.g., for handling peer-to-peer trading of energy, for the usage of central storage system, for the allocation of network resources or for the release of network capacities),
- billing of local energy trading within the energy community,
- enabling the traceability of storage usage (e.g., as proof for potential lessors of a battery system and their users),
- provision of billing-relevant information and data for the user (e.g., for control of the running system, motivation of the participants, basis for decisions regarding participant behavior)

Regarding the storage limitation principle, data is only stored on the blockchain for the duration of an accounting period (e.g., one month). At the end of the billing period, the start of a new blockchain is initiated by the infrastructure server ('Infrastructure' in Figure 2). The old blockchain is then archived in a database ('Archive DB') and its hash value is stored as an initial transaction in the new blockchain to keep a proper link to it. Since reading out energy data is required for the operation of the energy community far more often than it is legally defined for households, a clear consent to participate is required which could also be revoked at any time (Cejka et al., 2019). Participants can leave the energy community in this way as legally defined to be always possible in the RED II. Considering this step that may include a request to erasure of personal data according to the GDPR, the data of the former participant will not be available in the next blockchain. Prior to the next blockchain round, processing of his personal data must be restricted.

It may be legally required to keep archived blockchains saved for up to some years according to civil and tax law regulations. If individual blockchains were deleted from the archive, energy trading can no longer be fully retraced. Thus, only the billing information would be available, but not how it was determined.

5 CONCLUSION

As part of the 'Clean Energy for all Europeans Package', energy communities – beside other plans in the package – shall allow individuals to take an active part in the energy transition. Contained in the European Union's revised Renewable Energy Directive of 2018 and the Electricity Directive of 2019, the described implementation of an energy community anticipates their adoption into national law. As those national transpositions are due 2020/2021, this area is expected to be in significant motion within near future.

Although using blockchain technology, which is known for raising privacy questions, we have shown a privacy-friendly implementation that allows to enforce the 'right to rectification' and the 'right to erasure' in a feasible way. It has been rolled-out in a small municipality in Styria, Austria, where the implementation is currently field-tested with real customers. Results of this field test will be part of a subsequent publication. While in the related projects only the type of 'renewable energy communities' was examined, this implementation would also be utilizable in a 'citizen energy community'. As this type of energy communities is not restricted to a defined proximity, a high number of participants may be involved that may be spread widely.

ACKNOWLEDGMENTS

The presented work is conducted in the projects *SonnWende+* (FFG 2808377) and *Blockchain Grid* (FFG 3089755), funded by the Austrian Climate and Energy Fund (KLIEN) and the Austrian Research Promotion Agency (FFG).

REFERENCES

Ahl, A., Yarime, M., Goto, M., Chopra, S. S., Kumar, N. M., Tanaka, K., and Sagawa, D. (2020). Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan. *Renewable and Sustainable Energy Reviews*, 117:109488.

Alladi, T., Chamola, V., Rodrigues, J. J. P. C., and Kozlov, S. A. (2019). Blockchain in Smart Grids: A Review on Different Use Cases. *Sensors*, 19(22):4862.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., and Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, 100:143–174.

Article 29 Data Protection Working Party (2014). Opinion 05/2014 on Anonymisation Techniques.

Article 29 Data Protection Working Party (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

Article 29 Data Protection Working Party (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

Ateniese, G., Magri, B., Venturi, D., and Andrade, E. (2017). Redactable blockchain – or – rewriting history in bitcoin and friends. In *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, pages 111–126.

Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36:55 – 81.

Cejka, S. (2020). Energiegemeinschaften im Clean Energy Package der EU. *ecolex – Fachzeitschrift für Wirtschaftsrecht*. in german, to appear.

Cejka, S., Knorr, F., and Kintzler, F. (2019). Privacy issues in Smart Buildings by examples in Smart Metering. In *25th International Conference on Electricity Distribution (CIRED)*.

de Vries, A. (2018). Bitcoin's Growing Energy Problem. *Joule*, 2(5):801 – 805.

EU Blockchain Observatory and Forum (2018). Blockchain and the GDPR.

European Commission (2019a). 2030 climate & energy framework. https://ec.europa.eu/clima/policies/strategies/2030_en (accessed on 17.02.2020).

European Commission (2019b). *Clean Energy for All Europeans*. Publications Office of the European Union, Luxembourg.

European Commission (2019c). Clean energy for all Europeans package. https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/clean-energy-all-europeans (accessed on 17.02.2020).

Finck, M. (2019a). *Blockchain regulation and governance in Europe*. Cambridge University Press.

Finck, M. (2019b). Smart contracts as a form of solely automated processing under the GDPR. *International Data Privacy Law*, 9(2):78–94.

Frieden, D., Tuerk, A., Roberts, J., d'Herbemont, S., and Gubina, A. (2019). Collective self-consumption and energy communities: Overview of emerging regulatory approaches in Europe. Technical report. https://www.compile-project.eu/wp-content/uploads/COMPILE_Collective_self-consumption_EU_review_june_2019_FINAL-1.pdf (accessed on 17.02.2020).

Greveler, U., Justus, B., and Loehr, D. (2012). Multimedia content identification through smart meter power usage profiles. In *Computers, Privacy and Data Protection (CPDP)*.

IPCC (2014). Climate Change 2014: Mitigation of Climate Change. Contribution of Working Group III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change.

Joint Research Centre (2019). *Blockchain now and tommorow*. Publications Office of the European Union.

Martinez, J., Ruiz, A., Puelles, J., Arechalde, I., and Miadzvetskaya, Y. (2019). Smart Grid Challenges through the lens of the European General Data Protection Regulation. In *28th International Conference on Information Systems Development (ISD2019)*.

Politou, E., Casino, F., Alepis, E., and Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, pages 1–1.

Tang, G., Wu, K., Lei, J., and Xiao, W. (2015). The meter tells you are at home! Non-intrusive occupancy detection via load curve data. In *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 897–902.

UNFCCC (2016). The Paris Agreement. https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement (accessed on 17.02.2020).

University of Cambridge (2020). Cambridge bitcoin electricity consumption index. https://www.cbeci.org/ (accessed on 17.02.2020).

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, 28:1 – 9. Sustainability governance.

Zyskind, G., Nathan, O., and Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops*, pages 180–184.