The Next Stage of Green Electricity Labeling: Using Zero-Knowledge Proofs for Blockchain-based Certificates of Origin and Use

JOHANNES SEDLMEIR, FIM Research Center, University of Bayreuth, Germany
FABIANE VÖLTER, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Germany
JENS STRÜKER, Fraunhofer Blockchain Lab, University of Bayreuth, Germany

The labeling of electricity is considered an important mechanism to differentiate renewable power generation and, thus, to incentivize the expansion of green energy. However, today's systems for documenting and trading green energy certificates suffer from multiple challenges. These could be addressed by a digital solution that holistically collects and processes production and consumption data. Blockchain-based architectures have repeatedly been suggested for this purpose since they can provide transparency and can likely be accepted by a broad group of stakeholders. Yet, there are significant scalability and privacy issues of a blockchain-based approach for storing and processing fine-grained production and consumption data. In this paper, we propose and discuss a potential solution that levers succinct cryptographic zero-knowledge proofs to balance the required level of transparency and privacy while at the same time providing a high degree of scalability.

CCS Concepts: • **Security and privacy** → *Privacy protections*; • **Computer systems organization** → *Peer-to-peer architectures*; • **Information systems** → *Enterprise applications*; • **Applied computing** → *Consumer products*;

Additional Key Words and Phrases: climate change, distributed ledger, green energy, guarantee of origin, renewable energy, sustainability

ACKNOWLEDGMENTS

This work is funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) based on a resolution of the German Bundestag (funding code: 03E16026A). We thank Matthias Babel, Alexander Bogensperger, Dennis Jelito, Timon Rückel, Benjamin Schellinger, Nils Urbach, Andreas Zeiselmair, Till Zwede, and our research partner Stiftung Umweltenergierecht for their valuable support.

1 INTRODUCTION

To meet the Paris climate targets and ultimately achieve a 100 % renewable energy system, many researchers consider the electrification of the heating and traffic sector as mandatory [Hansen et al. 2019]. Moreover, a consensus prevails that so-called green or renewable hydrogen that is produced with green electricity will be required for industrial process heat in the future, irrespective of its extent [van Renssen 2020]. In general, owing to the increasing need for sector coupling and electrification, overall electricity consumption is elevating [Fridgen et al. 2020]. However, it is controversial where the necessary additional renewable energy will come from and, thus, how to close the so-called green electricity gap [Bloomberg New Energy Finance 2018]. As covering 100 % of future electricity use with renewable energy seems to be out of reach for a decade at least [Diesendorf and Elliston 2018], differentiating between the degree of "green" is vital for both renewable energy producers and consuming enterprises striving for CO_2 reductions [Comello et al. 2021]. Besides the ecological aspect, this is mainly due to the necessity of verifiable reporting [Financial Times 2021; Sullivan and Gouldson 2012] since shareholders increasingly expect enterprises to disclose the amount of CO_2 emitted through their operations [Heffron 2021]. Furthermore, there is increasing regulation that requires verifiable reporting; for instance, the planned extension of emission trading systems to the traffic and building sector in the European Union will require the holistic documentation of emissions [Reuters 2021]. Businesses are thus increasingly demanding verifiably green products [Whelan and Kronthal-Sacco 2019]. Moreover, they have strong incentives to differentiate from competitors through a lower carbon footprint in order to fulfill their customers' desire for carbon-neutral products [Palacios-Argüello et al. 2020]. The latter also reflects in the increasing demand of green energy tariffs by residential consumers [Herbes and Ramme 2014].

The special physical properties of electricity pose a challenge for a consistent labeling required for verifiable reporting. The tracking or even modification of electricity flows through the grid to ensure that a specific consumer receives "physically" green energy is complex and hardly practical or even impossible at scale. Rather, a common method is to approach the challenge from an economic perspective by somehow "offsetting" the energy consumed, i.e., decoupling the physical flow of electrical energy from its commercialization: Energy producers using renewable energy facilities may claim "certificates of origin" for every unit of renewably produced energy. Stakeholders can then trade these certificates separately from the physical energy. Upon consumption by a consumer relying on a renewable energy tariff, certificates are cancelled out [Morthorst 2003]. The act of cancellation hence indirectly corresponds to a "proof of use". Such systems exist in Europe, where they are called guarantees of origin (GOs), the U.S., and Asian countries [Hamburger 2019]. Nevertheless, existing certificate-based solutions for labeling electricity suffer from significant challenges. For example, they often do not accurately represent carbon emissions and lack transparency and verifiability for end-consumers. This results in susceptibility to fraud and low consumer trust [de Chalendar and Benson 2019; Hamburger 2019].

Several studies have highlighted the suitability of blockchains for the documentation and trading of GOs in order to overcome the existing challenges: Rather than centralized systems, they provide a high degree of transparency by design and have the capability to unite stakeholders on a single, neutral platform [e.g. Albrecht et al. 2018; Castellanos et al. 2017; Knirsch et al. 2020; Richard et al. 2019]. Yet, the replicated data storage and processing of a blockchain represent a

Authors' addresses: Johannes Sedlmeir, johannes.sedlmeir@fim-rc.de, FIM Research Center, University of Bayreuth, Wittelsbacherring 10, Bayreuth, Germany, 95444; Fabiane Völter, fabiane.voelter@fit.fraunhofer.de, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Wittelsbacherring 10, Bayreuth, Germany, 95444; Jens Strüker, jens.strueker@uni-bayreuth.de, Fraunhofer Blockchain Lab, University of Bayreuth, Wittelsbacherring 10, Bayreuth, Germany, 95447.

hurdle regarding privacy and scalability requirements in general [Munilla Garrido et al. 2021; Zhang et al. 2019] and specifically for a sophisticated labeling system that involves millions of generators' and consumers' personal or business-sensitive information [Alt and Wende 2020]. On the other hand, we observe that innovative solutions in decentralized finance have started to address privacy and scalability issues through succinct cryptographic zero-knowledge proofs (ZKPs). In this paper, we hence propose a design how to address challenges of electricity labeling with blockchain technology and ZKPs. We propose and evaluate an architecture for a verifiable, scalable, and privacy-oriented electricity labeling system that can help promote the use of renewable energy. Thus, we also aim to contribute to research on "green IS" demanded by Watson et al. [2010] and Goebel et al. [2014].

The remainder of this paper is structured as follows. We first briefly introduce the concepts of blockchain technology and ZKPs as the technology stack for our architecture in section 2. Next, we review challenges of labeling in general and GOs in particular and summarize related work in section 3. After that, we present the design of our proposed labeling solution in section 4. We then explore some characteristics of our approach in more detail in section 5 and discuss associated challenges and opportunities. We conclude by pointing out avenues for future research in section 6.

2 TECHNICAL BUILDING BLOCKS

2.1 Blockchain Technology

Blockchains are generally defined as a particular type of electronic ledger where data is replicated across multiple servers ("nodes") in a peer-to-peer network. This physically and organizationally decentralized yet logically centralized data management is achieved through an append-only structure in which selected nodes batch and order transactions into blocks that reference the corresponding previous block through a hash-pointer [Butijn et al. 2020]. Changing a single bit in any transaction, or their order, would render the chain of hash-pointers in an inconsistent manner. Accordingly, tamper sensitivity and the subsequent ease to detect fraud are among the distinct properties of a blockchain. The eligibility to append a block and the decision-making about which transactions to include and in which order is decided decentrally through a so-called consensus mechanism [Xiao et al. 2020]. Provided a specific threshold of the network (in some consensus-related metric) is honest, there are firm guarantees regarding retrospective immutability, non-censorship, and the correct execution of transactions. In general, consensus mechanisms combine cryptographic tools such as one-way functions, verifiable pseudo-random functions, and digital signatures and are heterogeneous in terms of security assumptions, latency, finality, and energy consumption [Kannengießer et al. 2020; Sedlmeir et al. 2020; Xiao et al. 2020]. Besides public, permissionless blockchains where anyone can participate, there are also permissioned blockchains where participation is limited, e.g., to a consortium from industry or the public sector [Amend et al. 2021; Wüst and Gervais 2018].

So-called smart contracts extend the functionality of blockchains beyond their initial purpose in applications, namely simple payments in cryptocurrencies like Bitcoin, to the execution of Turing-complete programming logic. Smart contracts are scripts that are redundantly executed and hence cross-checked by all nodes to make sure that the result is correct [Buterin 2013]. Consequently, blockchain technology facilitates general-purpose digital platforms while avoiding dependencies on one or a few distinct entities' availability or honesty [Alt 2020]. This avoidance of a single point of failure from an integrity and availability perspective makes blockchains highly attractive for critical infrastructures and the digital collaboration of mutually distrusting organizations [Fridgen et al. 2019]. Consequently, blockchains have, among others, been suggested in the energy sector for decentralized storage and control in power grids, peer-to-peer energy trading in smart grids, imbalance settlement, electric vehicle charging, e-roaming, carbon emission and green certificate trading, and fine-grained investments through tokenization [Albrecht et al. 2018; Andoni et al. 2019; Bao et al. 2020; Gorenflo et al. 2019; Wang et al. 2021].

Nonetheless, blockchain adoption faces many challenges. The deliberate redundancy of blockchain transaction storage and operation leads to scalability challenges as every node needs to process all other nodes' transactions [Gudgeon et al. 2020; Sedlmeir et al. 2021a; Zhou et al. 2020]. Moreover, the open availability of the same data to all blockchain nodes leads to a degree of information exposure that can be problematic [Kannengießer et al. 2020; Platt et al. 2021; Zhang et al. 2019]. Examples are conflicts with confidential corporate information and anti-trust regulation, as well as data protection regulation that inhibits the storage of sensitive customer data [Schellinger et al. 2022; Tatar et al. 2020]. The immutability and in particular lack of deletion capabilities on blockchains further exacerbate issues with data protection regulation [Rieger et al. 2019]. Consequently, first innovative solutions to scalability and privacy-related issues of blockchains have appeared, many of which are based on cryptographic techniques and specifically ZKPs.

2.2 Zero-Knowledge Proofs

The notion of ZKPs was first introduced by Goldwasser et al. [1989]. ZKPs are a special form of interactive protocols between a so-called "prover" and a "verifier" in which the prover wants to convince the verifier about a specific statement. ZKPs have the additional property that the prover learns *nothing* beyond the truth of this statement. Depending on the precise definition of what constitutes "knowledge" and consequently "learn", there are many nuances like perfect, statistical, and computational zero-knowledge. ZKPs can be "succinct", i.e., the proof size and the computational complexity of proof verification are at least exponentially smaller than the complexity of the original computation.

However, besides a few special applications such as anonymous credentials [Camenisch and Lysyanskaya 2001] that allow for the selective disclosure of attributes in a digital certificate without revealing the value of the signature, practical implementations or even applications of ZKPs remained rare until recently. This was probably owing to the high computational complexity of proof generation and the lack of convenient programming languages or libraries to implement ZKPs. A period of rapid improvements starting from Groth et al. [2006] led to the first implementations of practical and general purpose ZKP libraries, e.g., in Pinocchio [Parno et al. 2013]. In recent

years, different flavors have emerged, such as succinct hybrid arguments of knowledge (SNARKs) [Gennaro et al. 2013] and scalable transparent arguments of knowledge (STARKs) [Ben-Sasson et al. 2019] that differ in cryptographic security assumptions and setup. They all have in common that they allow to create succinct proofs for the correct execution of computations without the need to reveal inputs or intermediate steps. Often, hashes, Merkle proofs, or signature checks for the inputs are a part of the program to force provers to commit to using variables that are unknown to most parties but fixed or that have specific required properties. Domain-specific languages such as Bellman and snarkjs allow to compile rather general programs into arithmetic circuits, and libraries such as libsnark and circom translate these circuits into proving and verification programs. As generic tools for creating and verifying ZKPs have matured and improved in ease of use, performance, and scope over the last years, ZKPs have appeared in blockchain applications for the verification of off-chain computations' (that would previously have been executed in a replicated way in a smart contracts) integrity without revealing sensitive data, starting with the privacy-oriented cryptocurrency Zcash [Sasson et al. 2014; Schellinger et al. 2022]. Regarding the applicability in the energy sector, Wang et al. [2021] propose ZKPs for privacy-perserving energy storing.

One important application associated with blockchains that heavily inspired our architecture are *zk-rollups*. A so-called operator or aggregator, who may be a single service provider or a consortium, collects users' signed cryptocurrency transactions and maintains an associated book of accounts. This book of accounts is either stored on-chain, with domain-specific optimizations regarding storage and computation, or off-chain (in this case, the zk-rollup is sometimes called "Validium"). In case the book keeping occurs entirely off-chain, only the book of accounts' Merkle root is stored on-chain. Any change of the state of this hash that represents the book of accounts' state needs to be legitimized by the aggregator through a ZKP that the owner of the respective account authorized the transaction with their signature – a so-called "validity proof" [Buterin 2021]. Consequently, the operator does not need to be trusted regarding the correctness of the book keeping, because the validity of each modification is redundantly verified by all nodes [Gluchowski 2019]. By "compressing" many transactions into a single update of the book of accounts and a corresponding succinct ZKP (or sometimes just a succinct non-interactive proof that is not necessarily zero-knowledge) that proves the legitimacy of the update, zk-rollups such as Aztec, Hermez, Loopring, StarkDex, and zk-Sync that run as applications on the public Ethereum blockchain already allow for a significant boost in throughput compared to the base layer today [Schaffner 2021].

3 RELATED WORK

3.1 Guarantees of Origin

GOs were introduced in 2001 in the European Union to inform end consumers about the share of green energy in their consumed electricity mix [European Union 2009]. This, in turn, aims to incentivize households and companies to make decisions that minimize their carbon emissions when choosing an electricity supplier or tariff, and, therefore, to advance investments in renewable energy generation [Hamburger 2019; Morthorst 2003]. In practice, however, the design of existing GO systems is coming with a handful of downsides. First, they are often designed as national electronic registries in which GOs are traded for each generated MWh independently of their generation place and time [Will et al. 2017]. Utilities can buy GOs to label non-renewably produced electricity and sell it as green on their consumers' bills [Bogensperger and Zeiselmair 2020]; a practise that is often criticized as "greenwashing" [Johns 2021; Will et al. 2017]. For example, under the German register of guarantees of origin (GOR), GOs can stem from an arbitrary place and be "consumed" within one year. This disentanglement of GOs with the physical reality can reduce consumers' trust [Hamburger 2019], resulting in indifference [Bogensperger and Zeiselmair 2020; Hanimann et al. 2015; Jansen and Seebach 2009; Jochem et al. 2015] and a low willingness to pay premiums for green energy tariffs [Jansen 2017]. Second, low resolutions in time discourage time-specific consumption according to the current supply of green energy and do not accurately reflect the carbon emissions caused by the power grid [de Chalendar and Benson 2019]. Consequently, they fail in their goal to incentivize required investments, for example, storage facilities [Bogensperger and Zeiselmair 2020]. Third, the current practices cause considerable intransparencies regarding the feed-in of green energy and can lead to a gap between a country's disclosed energy mix and its actual consumption [Kaenzig et al. 2013]. Fourth, the lack of a transparent process and the fragmentation of documentation also open the potential for fraud, such as the double-counting of green energy through not properly removing or invalidating certificates upon usage [Correctiv 2021; Hamburger 2019]. Thus, a certificate of use is not bound to a certificate of origin, which hinders consumers from verifying that the electricity they consumed was green. Consequently, there is a strong need for an end-to-end and internationally harmonized digital process [Bogensperger and Zeiselmair 2020; Hamburger 2019]. Finally, the Paris climate agreement has led to many commitments to decarbonization goals by enterprises. In addition to the electrification of transportation and industrial heat, more and more manufacturers are interested in actively managing production processes according to the "greenness" of electricity in the grid. While stakeholders like transmission system operators (TSOs) could provide the carbon emissions associated with the current electricity mix as a service, they also have to cope with the results on the grid level that more short-time purchases have on consumption habits [Strüker et al. 2021].

The lack of a "global" perspective, insufficient harmonization between countries [Hamburger 2019], and the low degree of transparency [Knirsch et al. 2020] are considered primary causes of consumers' lack of ability to verify whether suppliers actually bought a sufficient number of GOs for the sum of their sales. Further, the increasing cross-border trade of energy and the demand for international carbon certificates require a system for digitally verifiable and interoperable GOs. Article 15(9) of the Renewable Energy Directive already expects member states to "recognise GOs issued by other Member States" [European Union 2018, p. 119]; however, to date, varying legal and regulatory frameworks, as well as different progress of the digital transformation in the electricity sector across Europe pose a challenge for cross-border trading [Jackson et al. 2018]. Cross-border labeling requires the synchronization of registries among involved countries and trust in the correctness of data.

3.2 Existing solution approaches

To overcome these issues, all involved stakeholders could agree on a centralized platform (for example provided through a European institution) that is responsible for the aggregation and verification of GO-related data. However, it is often difficult to agree on a central trusted party within federal ecosystems, and the reliance on a single institution bears the risk of manipulation, aggregation of market power, or being compromised by an attack. For these reasons, among others, levering blockchain technology to provide a neutral platform has often been suggested [e.g. Albrecht et al. 2018; Castellanos et al. 2017; Knirsch et al. 2020; Richard et al. 2019; Velazquez Abad and Dodds 2020]. For example, Castellanos et al. [2017] simulate blockchain-based green certificate trading and, thus, focus on a market-based solution. However, the authors do not discuss scalability and neglect privacy and data sovereignty issues related to blockchain-based marketplaces such as the de-anonymization of users [Béres et al. 2020]. Diniz et al. [2021] present a blockchain-based architecture to facilitate reporting processes. The authors address the high complexity involved in reporting processes and aim to improve information flows, yet they do not discuss scalability requirements. To mitigate the sensitive information exposed on the blockchain, they propose to record certificate information only in encrypted form. However, trading patterns recorded on blockchains can allow for de-anonymization [Liu et al. 2021]; and by encrypting generation- and consumption-related information, the desired transparency of accounting is compromised. Knirsch et al. [2020] highlight the importance of verifiability for end-consumers and suggest a decentralized and permissionless system for the trading and verification of GOs. To prevent the necessity of trust in a central player, the authors suggest not to rely on distribution system operators (DSOs) or TSOs as natural intermediaries to issue green certificates. Producers and consumers can then trade GOs directly on a blockchain. The authors suggest to conduct audits of generation as well as consumption units to detect sources of wrong information. However, consumers have to rely on producers for cancelling certificates upon consumption. Furthermore, while providing mechanisms for the transparent verification of GOs, the authors neglect privacy-related aspects: Their approach only provides pseudonyms for customers, which has already proven to be insufficient to conceal identities in the long-term in cryptocurrencies [Biryukov et al. 2014]. Furthermore, the authors aim to ensure scalability by solely storing the hash reference of transactions. This approach is unlikely sufficient for an internationally-scalable solution: Considering the 195 Mio. private households in Europe, for example, would require about 2,260 transactions being processed per second on average in case households update their consumption solely on a daily basis. A daily update still does not provide high timely granularity; and yet, public permissionless blockchain systems such as the Ethereum blockchain are limited to only about 15 tx/s [Schäffer et al. 2019]. In addition, transaction fees have increased significantly over the last years, representing an additional burden for generators as well as consumers. In comparison to Knirsch et al. [2020], Karakashev et al. [2020] focus on protecting producers' and consumers' sensitive information. The authors explicitly focus on delivering a privacy-preserving solution by making use of ring signatures and stealth addresses. However, their approach does not ensure global verifiability as total production and consumption cannot be transparently retraced.

Thus, while previous authors have argued for the benefits of blockchain-based solution approaches for trading GOs, they have not yet sufficiently focused on aligning privacy, data sovereignty, and scalability requirements. Consequently, to the best of our knowledge, to date no proposed approach balances out transparency and verifiability with privacy and data sovereignty for all stakeholders and at the same time achieves the scalability that is necessary for an international GO system that operates close to real-time.

3.3 Requirements of Labeling Systems

Our analysis of the challenges of existing approaches to electricity labeling (see also table 1 in the supplements for a summary) allowed us to derive a set of requirements that energy labeling systems need to fulfill to overcome. First, labeling systems need to prevent the double-counting of green energy and allow for verification across borders. In turn, this aspect requires end-to-end verifiability starting from the very source of data generation. Furthermore, a platform for GOs needs to be open, support the harmonization of existing solutions, and may not discriminate against the participation of stakeholders bound to different legislations, data processing paradigms, or other parameters. At the same time, no personally identifiable information or otherwise sensitive data, such as utilities' and electricity producers' business secrets, may be accessible to third parties that have no legitimate need to see it. Also, the platform needs to scale in terms of a high resolution in time and space to allow for fine-grained GOs that reflect the regional and temporal specificities of electricity generation and consumption, even with the expected increase in the number of generation assets to be sustainable in the long run. Lastly, labeling procedures need to be automated end-to-end and should involve as little manual interaction as possible. These requirements can be summarized as *verifiability*, *privacy*, *openness* and *scalablity*.

4 PROPOSED ARCHITECTURE

We propose an alternative architecture to electricity labeling that addresses the requirements outlined in section 3.3. First, in line with the literature presented, we suggest using blockchain technology as an underlying neutral and non-proprietary infrastructure to facilitate a decentralized electricity labeling system. This building block allows for transparency and enables stakeholders to verify transactions independently. Second, to strike a balance between verifiability and privacy, our solution levers ZKPs. Last, to meet the requirement of scalability, we further make use of the succinctness of ZKPs. Thus, we design an interoperable, scalable system that prevents fraudulent or incorrect accounting by design while maintaining the required information privacy for all participants. We will illustrate our approach using an example of n generators, one utility, and m consumers. We also start with only two labels (green and grey electricity) and postpone the discussion of how to implement additional discrete labels and spatial origin to future work.

Prerequisites. As a foundational layer in our process, electricity generators and consumers need to establish an authenticated communication channel to reliably send their generation and consumption data

to their electricity utility.[1] To do so, in line with Knirsch et al. [2020], we propose relying on a conventional public key infrastructure (PKI) or newer developments like self-sovereign identity (SSI) [Sedlmeir et al. 2021b] for providing a secure bilateral communication layer and certificate-based proofs of the authenticity of sensor data. In specific, generators can digitally sign the produced quantities of electricity at its source to make the data trustworthy. As such, the proposed solution relies on data logging modules integrating crypto-chips and digital certificates that are currently being rolled out in many countries in the same way as previous propositions including Knirsch et al. [2020] and Karakashev et al. [2020] discussed. However, this is not an indispensable prerequisite for our approach: End users can check whether their data is referenced truthfully by the system by readily comparing their meter reading with the information in their (verifiable) electricity bill, and audits on the side of generators can be conducted. Nonetheless, cryptographically verifiable generation and consumption data is beneficial for a system so that correctness checks can happen by default rather than through costly or tedious manual effort. Moreover, using digital certificates, assets can prove their generation attributes automatically on request, which makes new generation facilities' onboarding easier. For example, assets can prove that they have been attested the attribute of "renewable wind energy" by their certified manufacturer or another entity such as DSOs or TSOs that are considered trustworthy regarding this claim. Consumers' devices also periodically digitally sign their consumption data with the private key in their digital meter or data logging device and communicate it to the utility.

Bootstrapping a utility. In the beginning, a utility, which acts as the operator or aggregator that creates proofs of correct accounting (and, thus, proofs of origin and use) in our design, creates a large Merkle tree [Merkle 1987]. Initially, all leaves contain an agreed-upon, public value (e.g., 0). The number of leaves should be significantly larger than the maximum number of accounts that the utility expects to manage at any time. For example, for a utility that usually holds a million user accounts, we would suggest a depth of 22 and, thus, $N = 2^{22} \approx 4.2$ million leaves, which corresponds to the maximum number of accounts that can be managed. As such, the proposed architecture is of fixed size: all involved stakeholders must agree beforehand how many consumers and generators can at maximum be reflected in the process. While dynamically extending the Merkle tree during operation is technically feasible, it would significantly complicate the designed system, so we will not consider this in this work. The Merkle tree is locally stored by the utility and serves as a record for accumulated generation and consumption data. Any leaf in the Merkle tree represents either a consumer or a generator and contains the aggregated consumption or generation since their onboarding. The left half of the Merkle tree will contain generators; the right half will contain consumers.

Onboarding process and data collection. Now, a consumer can be onboarded by the utility as follows: The consumer's digital meter establishes a bilateral, end-to-end encrypted communication channel with the utility and sends a request of being onboarded, together with a presentation of a digital certificate that proves that the metering device is certified. The presentation includes the metering device's public key for signing consumption data and the (signed) current meter reading ("balance"). Consecutively, the utility replaces one empty leaf in the right half of the Merkle tree by the sensor's public key (which is essentially a pseudonym for the consumer), the current meter reading, the timestamp of account creation, and an array initialized with zeros that represents the amount of green and grey energy that the consumer has received during the contract period so far (see also Figure 2 in the supplementary material). Similarly, generation units can be onboarded. If there has been a consumer or utility request to de-register, for instance, because they want to switch their energy provider, accounts have to be "offboarded". This involves overwriting the previously described account details in the corresponding leaf of the Merkle tree with the initial publicly known value (e.g., 0) so that the leaf is prepared to be re-used in a later onboarding process. Based on consumption and generation data, the utility can locally update the leaves periodically (in discrete steps, which we call "epochs" that may be, e.g., 15 minutes), incorporating new data communicated by generation or consumption units' sensors during the respective epoch. In specific, the utility's locally stored Merkle tree serves as a running record for accumulated labelled generation and consumption data. To do so, utilities need to maintain local data registries for recording all account balances and accumulate this generation and consumption data. The symmetry in treatment of generators and consumers also allows for a rather flexible change of roles, which is necessary for so-called prosumers to efficiently participate in the system.

Proving local integrity. So far, the described architecture essentially corresponds to how a utility would handle their book keeping today while the data is managed in an unusual data structure of a Merkle tree. In any stage of the process, the Merkle tree that includes transaction data is kept entirely off-chain. The Merkle tree and differences of subsequent states of the Merkle tree represent fine-granular and, thus, highly sensitive consumption and generation data that must not be distributed to other stakeholders. For example, fine-grained consumption data can be used to derive information on a consumer's habits or location [Hinterstocker et al. 2017]. In a first step, the utility can increase transparency and give consumers and auditors some control on what it is doing by updating the Merkle root of its off-chain accounting data periodically on a blockchain. Every consumer and generator can then verify that the data from their metering device has been included truthfully by requesting their historic account states from the utility, together with Merkle proofs [Djamali et al. 2021] and a transaction receipt from the blockchain for the transaction including the associated Merkle root. Using a blockchain client, an end-user can check whether this transaction exists and – using the Merkle proof – verify that their own data has been included correctly in the corresponding Merkle tree. The analogous construction holds for a generation unit that sends its generation data to the utility.

Proving global integrity. This combination of the on-chain Merkle root and the Merkle proof is not yet sufficient for a certificate of origin or use: While the blockchain transaction receipt and Merkle proof allow for *local* integrity checks from the side of consumers and generators already, so far, there is no way to check whether the

[1] We acknowledge that different deregulated and regulated electricity schemes around the world involve a heterogenous denomination of system actors. Accordingly, we simplify the electricity value chain by considering a utility as the intermediary party between generators and consumers.

generation and consumption data for green and grey electricity match *globally* at any time and, thus, whether or not certificates have been double-used. As only the utility has access to all generation and consumption data and, thus, a global overview of total generation and consumption, an additional mechanism is necessary to exclude manipulations on the utility's behalf. Against this backdrop, we propose relying on ZKPs. Specifically, the utility must prove the legitimacy of *any* (batched) update of the Merkle tree that they perform on the blockchain, i.e., once per epoch. This involves that proofs for three different types of operation need to be given:

(1) Proving the correctness of the on- and offboarding procedures.
(2) Confirming that account balances have been updated according to the signed consumers' and generators' sensor data.
(3) The total sum of generation and consumption match for each label.

Requirement (3) represents the core requirement for globally correct accounting under the condition that the local accounting is correct. Accordingly, the utility aims to prove that the total amount of energy sold to consumers is not larger than the total generation for each label and epoch. To facilitate labeling and prevent the "greenwashing" of energy, this process involves not only proving the matching of the total sum of generation and consumption but also the matching of energy types: The sum of green consumption when updating the Merkle tree may never exceed the sum of green production. At the same time, the sum of grey consumption may also never exceed the sum of grey production.

As outlined in section 2.2, ZKPs can be used to convince another party of the correctness of some mathematical statement without providing any further information. Applying this to the underlying context, the utility aims to prove the legitimacy of the Merkle tree updates to all involved stakeholders. As such, the utility seeks to prove the correctness of every update of the Merkle root that happens on-chain. To generate the ZKPs, exemplified with SNARKs, all stakeholders initially must agree on a proving and verification key generated from public code representing all conditions that the proof must satisfy by a key generation algorithm. This involves a so-called trusted setup that can be conducted as multi-party computation, so that the presence of one honest party ensures the correctness of ZKPs checked with the verification key [Bowe et al. 2018]. To calculate the ZKP, the utility uses public inputs (previous and suggested updated Merkle root), a private input or "witness" (the whole Merkle tree and the signed updates from the consumers and generators that authorize their on-/offboarding or include their updated balances), and the generated proving key. On this basis, the utility executes a proving algorithm that uses the proving key to generate a proof attesting that the utility knows a correct witness to the proposed update. Thus, the utility can prove that it updated the Merkle root correctly according to pre-defined conditions by revealing publicly only the previous and updated Merkle root and the ZKPs that contains no more information than the correctness of the updating procedure according to the conditions set in the public algorithm from which the proving and verification key were computed. In particular, the ZKP demonstrates that the updated Merkle root was computed from a Merkle tree representing leaves with the property that the cumulative increase in consumption balances for each label does not exceed the corresponding cumulative increase in generation balances.

To make this proof of global integrity accessible and, thus, verifiable to all relevant stakeholders, the utility sends the generated ZKP and the updated Merkle root to a smart contract, which can verify the ZKP with the help of the verification key and the previous Merkle root. If the ZKP is considered valid by the majority of blockchain nodes (in the metric corresponding to the consensus mechanism), the Merkle root is updated in the smart contract accordingly. This approach allows any stakeholder to verify that the global accounting has been conducted correctly. Consequently, the combination of local proofs of integrity using Merkle proofs with ZKPs attest the correct global accounting and in particular prevent double usage.

To summarize, in our proposed architecture, utilities receive all meter readings from generators and consumers, which resonates with familiar responsibilities regarding data availability and protection in today's power systems. Consumers and generators still need to trust utilities regarding *data privacy* as of today when they communicate their generation and consumption data for billing purposes. The fundamental change in introducing the ZKP-based labeling is that consumers and auditors need to trust the utility solely with data privacy but not with the *integrity* of the accounting. We illustrate the overall architecture of our proposed solution in figure 1.

5 DISCUSSION

Technological Readiness. The proposed architecture relies on building blocks that are already in productive use in decentralized finance, for example, in the form of zk-rollups [Schäffer et al. 2019]. In parallel to the underlying use case, payments require a certain level of trust in the operator regarding the protection of users' privacy, but the need for trust in the operator's accounting needs to be avoided for acceptance reasons. To achieve the former, current payment solutions like StarkWare [2021] also rely on off-chain accounting and batching of transactions to achieve scalability requirements. What's more, the energy sector has less rigid requirements regarding data availability than the use cases of existing zk-rollup implementations. This is mainly related to on-chain data availability. It is likely not essential to recover an account if the utility crashes or loses data in the case of electricity: re-starting the process through onboarding all entities will likely be sufficient as this use cases focuses on ensuring that in each epoch no more green energy was consumed than generated. By contrast, in the case of digital assets, losing the state of the book of accounts is problematic because users cannot reconstruct the respective part of the Merkle tree to claim their locked funds. Thus, we expect that the proposed solution suits the underlying use case very well. Moreover, as we argued in section 4, the responsibilities for data collection and evaluation in our design reflect the status quo in the energy sector well.

On the other hand, there are some requirements of our use case which exceed those of existing use cases. First, we need very high throughput for close-to-real-time accounting, because every single consumer will need a transaction every 15 minutes or so. Additionally, it may be more difficult to parallelize the processing of transactions as there will not always be a pair of transactions that guarantees constant supply, as in the case of payments. However, we expect

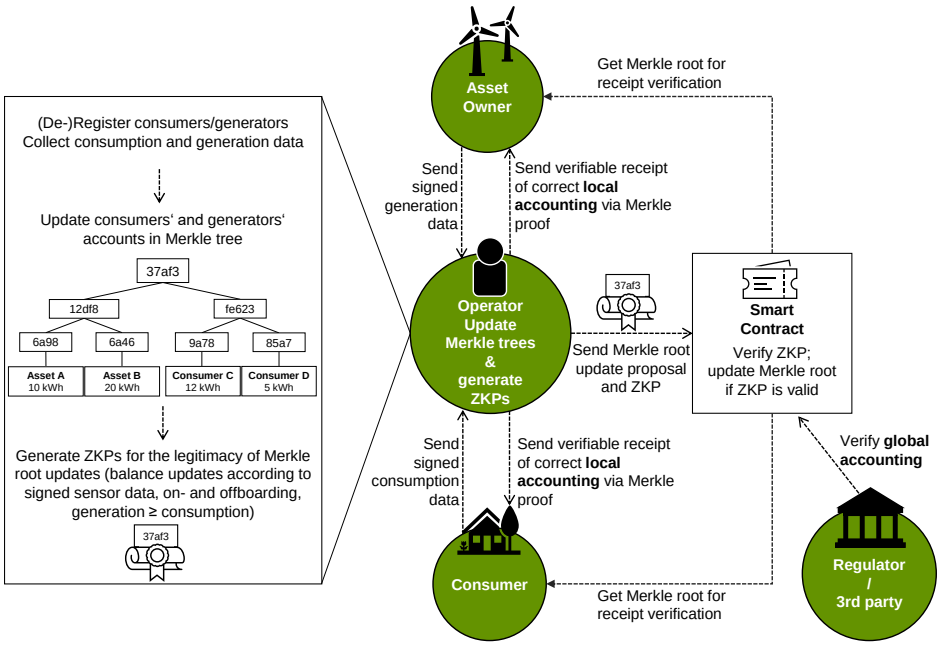

Fig. 1. Overall architecture of our labeling platform.

that partial updates should be feasible by building clusters of generating and consuming units when the number of accounts is large. Besides, questions of error handling, e.g., in the case of delayed communication of sensor data, need to be addressed.

Complexity & Costs. The proving and verification complexity of ZKPs have decreased significantly over the last years due to many theoretical advances and performance optimizations. For example, when using Poseidon as a hashing mechanism [Grassi et al. 2021], verifying the computation of a single hash contributes around 300 constraints; a metric for the complexity of proof generation. Thus, proving that an update from a previous to a new Merkle root is legitimate when every single account is updated involves re-computing both Merkle roots from the leaves, which corresponds to $2 \cdot 2N$ hashes for the trees that we illustrate here. Checking that the accumulated consumption of green energy in an epoch is lower than the accumulated generation (and potentially the correct range of the transactions' timestamp) only adds a small number of additional constraints. From ongoing projects on the public Ethereum blockchain and our own first tests with the circom, snarkjs and rapidsnark libraries, we know that an operator (i.e., the utility) with dedicated hardware can prove approximately $2^{27} \approx 128$ million constraints in two minutes with a 64-core server [Hermez Network 2021]. Without any optimizations, this would allow the management of around 100,000 accounts and updates of each of them every two minutes. Looking at the fast developments in the last years, including the appearance of new solutions such as STARKs, which do not involve a trusted setup, and the utilization of graphics processing units (GPUs), we expect that proofs for Merkle trees involving millions of accounts can be created in reasonable time with common enterprise hardware and, thus, at low costs in the near future.

Regarding costs, the verification of a Groth16-SNARK currently costs around 200,000 gas on the public Ethereum blockchain, plus around 9,400 gas per public input [Eberhardt 2021]. In our architecture, the only inputs for the ZKP are the root hashes of the utility's previous and updated Merkle tree, so the gas costs stay below 250,000 gas, which is $\frac{1}{60}$ of the current public Ethereum block capacity. For comparison, a simple payment on Ethereum consumes 21,000 gas, while more complex transactions in decentralized finance are on the order or 100,000 gas. Yet, the costs of verifying a SNARK to a utility would still be considerable today: around 50 USD using gas prices from October 2021, which would amount to almost 2 million USD per utility and year. With a block time of around 13 seconds, if a utility has their SNARK verified by a smart contract every 15 minutes, this occupies around 0.02 % of the total Ethereum capacity. Given a potentially large number of utilities, this still seems impractical. Initially, we thus recommend to move to a permissioned blockchain that is operated by several organizations in the energy sector; this does not involve gas costs and allows for a significantly larger number of SNARKs to be verified per time period as higher hardware requirements allow for better performance [Sedlmeir et al. 2021a]. Moreover, since the ZKP in our architecture only has two public inputs, aggregated verification techniques through recursion [Bowe et al. 2020] or batching [Gailly et al. 2021] can be used to significantly further reduce the ZKP verification effort: In each epoch, utilities can send their SNARK to an untrusted aggregator that creates a ZKP that attests the correctness of many utilities' SNARKs and that is exponentially less costly to verify than the whole of individual SNARKs (public inputs, however, contribute linearly). This approach

further enhances the scalability in system with many utilities and indicates practicability also with a permissionless blockchain in the future.

Double-spend Prevention for Generators. Our architecture design makes sure that the double-usage of green electricity certificates is not possible, as consumers can verify whether their own consumption data is reflected in the on-chain Merkle root and whether the utility does the global accounting correctly. Signed smart meter data further increases authenticity guarantees. However, so far, our design is still vulnerable to generation units that fraudulently register at different utilities and subsequently submit their sensor data attesting the generation of a certain amount of green energy to multiple utilities. Thus, mechanisms to prevent the double-commercialization of generated labeled electricity are needed. A promising approach beyond spot-checks by auditors or regulators that could integrate well with the proposed blockchain-based approach could involve a token that a generation unit receives on its installation by the local grid operator. Generating units could then transfer their "registration token" to a specific utility. The utility then needs to additionally prove in their ZKP that they only included generation data from units that had transferred their registration token to this utility. Future research could compare this and alternative approaches regarding their complexity and the level of authenticity that they can provide.

Trading. Considering the trading only on the level of utilities and energy producers already significantly reduces the complexity of electricity trading and, thus, makes it easier to detect the double-usage of GOs both for centralized and decentralized trading platforms. For a decentralized platform on a permissioned blockchain – an approach that several papers like GECKO have suggested [Knirsch et al. 2017] – GOs would be traded as tokens. This is possible in combination with our approach, where utilities not only publish the Merkle root of their generation and consumption database but additionally the difference between consumption and generation for each label. Since this data is already highly aggregated over many generators and consumers, it exhibits significantly less privacy and scalability issues than consumers' and generators' individual data. Nonetheless, this information may still not be appropriate for publishing on a blockchain because net balances for each label and epoch can be sensitive business data and may even be problematic regarding antitrust regulation. Consequently, it may be important to add a ZKP-based level of privacy and scalability also on this level, where the aggregate consumption and generation or their difference can be referenced as public information or private inputs to further ZKPs. In the latter case, this could directly integrate with constructions as suggested by Karakashev et al. [2020], which -– as we argued in section 3.2 – may be problematic to introduce on the level of small producers because it is very difficult to find compromised sensors that fraudulently generate GOs in an anonymized system, but which may be suitable to apply to the business-to-business (B2B) trading layer. Essentially, the cryptographically verifiable aggregation below the utility layer in our approach aims to mitigate the privacy and scalability challenge for GOs on a decentralized infrastructure without a significant tradeoff in risk mitigation. We believe that our architecture can be used as a scalable, privacy-oriented, decentralized and, thus, neutral base layer for aggregate GO trading and documentation on a B2B layer.

6 CONCLUSION AND OUTLOOK

In this paper, we identified the requirements of *verifiability*, *privacy*, *openness* and *scalability* for the documentation of GOs and proposed a technical architecture that builds on blockchain technology and ZKPs to solve these challenges. We provide transparency and verifiability by design by storing Merkle roots and verifying ZKPs on-chain with no access restrictions for stakeholders. Since on-chain data does not reveal any information itself but only the adherence to ex-ante-defined data processing rules, we protect all involved stakeholders' privacy and data sovereignty by design, too. Lastly, succinct ZKPs allow for a future increase in the number of production facilities and a high time-resolution of their production and end consumers' consumption despite blockchains' limited performance. Future research can consider introducing additional labels to further distinguish between renewable sources of energy to reflect consumer preferences beyond carbon emissions. This may not only include discrete labels but also continuous labels, for example, to facilitate regional GOs. In addition, researchers can analyze to which extent our proposal is applicable also to related areas that require transparency and that need to prevent double-counting by design while ensuring scalability and the privacy of the involved stakeholders. In particular, we suggest the trading of carbon emissions as a promising area in which the combination of blockchains, ZKPs, and potentially PKI- and certificate-based digital identities for assets and similar ideas will be useful. Moreover, future research could address the trading of labelled energy tokens to allow utilities to purchase additional green energy to satisfy consumer demand.

Our research is bound to several limitations. While we have already fully designed our labeling platform's roles and information flows and started with the implementation, we still lack a practical evaluation of the architecture in a field test. This also includes an encompassing security model and analysis. For example, assets' digital identity certificates could be used for access management if a zero-trust paradigm in terms of security is chosen [Buck et al. 2021]. Furthermore, collecting experiences regarding users' trust in a blockchain- and ZKP-based labeling mechanism also is essential: Winther and Ericson [2013] already demonstrated that Norwegian consumers mistrust GOs not only owing to unreliable methodology but also because physical electricity is untraceable. Further research could thus also analyze whether the well-known "trust machine" blockchain will help convince consumers of the integrity guarantees and tamper-resistance of the proposed solution [Völter et al. 2021].

In sum, the lack of verifiable GOs with a high temporal and spatial granularity represents a critical barrier to popularizing green energy products and is required for an efficient computation of carbon footprints and associated certificates. We believe that the proposed architecture provides a transparent, accurate, scalable, and privacy-preserving alternative to current GO practises and existing blockchain-based architectures that have been proposed. Further, we conclude that a base layer of digital identities for organizations, natural persons, and things, combined with new and potentially decentralized platforms for the verifiable exchange of data and privacy-enhancing cryptographic solutions, may be a promising approach to address many of the challenges both in and beyond the energy sector.

REFERENCES

Simon Albrecht, Stefan Reichert, Jan Schmid, Jens Strüker, Dirk Neumann, and Gilbert Fridgen. 2018. Dynamics of Blockchain Implementation – A Case Study from the Energy Sector. In *Proceedings of the 51st Hawaii International Conference on System Sciences*. 3527–3536. https://doi.org/10.24251/HICSS.2018.446

Rainer Alt. 2020. Electronic Markets on Blockchain Markets. *Electronic Markets* 30, 2 (2020), 181–188. https://doi.org/10.1007/s12525-020-00428-1

Rainer Alt and Erik Wende. 2020. Blockchain Technology in Energy Markets – An Interview with the European Energy Exchange. *Electronic Markets* 30, 2 (2020), 325–330. https://doi.org/10.1007/s12525-020-00423-6

Julia Amend, Julian Kaiser, Lucas Uhlig, Nils Urbach, and Fabiane Völter. 2021. What Do We Really Need? A Systematic Literature Review of the Requirements for Blockchain-based E-Government Services. In *Wirtschaftsinformatik 2021 Proceedings*. Springer, 398–412. https://doi.org/10.1007/978-3-030-86790-4_27

Merlinda Andoni, Valentin Robu, David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter McCallum, and Andrew Peacock. 2019. Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities. *Renewable and Sustainable Energy Reviews* 100 (2019), 143–174. https://doi.org/10.1016/j.rser.2018.10.014

Santiago Bañales. 2020. The Enabling Impact of Digital Technologies on Distributed Energy Resources Integration. *Journal of Renewable and Sustainable Energy* 12, 4 (2020), 13. https://doi.org/10.1063/5.0009282

J. Bao, D. He, M. Luo, and K. R. Choo. 2020. A Survey of Blockchain Applications in the Energy Sector. *IEEE Systems Journal* 15, 3 (2020), 12. https://doi.org/10.1109/JSYST.2020.2998791

Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. 2019. Scalable Zero Knowledge with no Trusted Setup. In *Annual International Cryptology Conference*. Springer, 701–732. https://doi.org/10.1007/978-3-030-26954-8_23

Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. 2014. Deanonymisation of Clients in Bitcoin P2P Network. In *Proceedings of the SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 15–29. https://doi.org/10.1145/2660267.2660379

Bloomberg New Energy Finance. 2018. New Energy Outlook 2018 – BNEF's Annual Long-Term Economic Analysis of the World's Power Sector out to 2050. https://bnef.turtl.co/story/neo2018

Alexander Bogensperger and Andreas Zeiselmair. 2020. Updating Renewable Energy Certificate Markets via Integration of Smart Meter Data, Improved Time Resolution and Spatial Optimization. In *17th International Conference on the European Energy Market*. IEEE, 5. https://doi.org/10.1109/eem49802.2020.9221947

Sean Bowe, Alessandro Chiesa, Matthew Green, Ian Miers, Pratyush Mishra, and Howard Wu. 2020. ZEXE: Enabling Decentralized Private Computation. In *Symposium on Security and Privacy*. IEEE, 947–964.

Sean Bowe, Ariel Gabizon, and Matthew D Green. 2018. A Multi-party Protocol for Constructing the Public Parameters of the Pinocchio zk-SNARK. In *International Conference on Financial Cryptography and Data Security*. Springer, 64–77. https://doi.org/10.1007/978-3-662-58820-8_5

Christoph Buck, Christian Olenberger, André Schweizer, Fabiane Völter, and Torsten Eymann. 2021. Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-trust. *Computers & Security* 110 (2021), 26. https://doi.org/10.1016/j.cose.2021.102436

Vitalik Buterin. 2013. A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/

Vitalik Buterin. 2021. An Incomplete Guide to Rollups. https://vitalik.ca/general/2021/01/05/rollup.html

Bert-Jan Butijn, Damian A Tamburri, and Willem-Jan van den Heuvel. 2020. Blockchains: A Systematic Multivocal Literature Review. *Comput. Surveys* 53, 3 (2020), 37. https://doi.org/10.1145/3369052

Ferenc Béres, István András Seres, András A. Benczúr, and Mikerah Quintyne-Collins. 2020. Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users. https://arxiv.org/abs/2005.14051

Jan Camenisch and Anna Lysyanskaya. 2001. An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation. In *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 93–118. https://doi.org/10.1007/3-540-44987-6_7

J. Alejandro F. Castellanos, Debora Coll-Mayor, and José Antonio Notholt. 2017. Cryptocurrency as Guarantees of Origin: Simulating a Green Certificate Market with the Ethereum Blockchain. In *International Conference on Smart Energy Grid Engineering*. IEEE, 367–372. https://doi.org/10.1109/SEGE.2017.8052827

Stephen Comello, Julia Reichelstein, and Stefan Reichelstein. 2021. Corporate Carbon Reduction Pledges: An Effective Tool to Mitigate Climate Change? http://dx.doi.org/10.2139/ssrn.3875343

Correctiv. 2021. Grand Theft Europe – A Cross-Border Investigation. https://correctiv.org/top-stories/2019/05/06/grand-theft-europe/

Jacques A de Chalendar and Sally M Benson. 2019. Why 100 % Renewable Energy is Not Enough. *Joule* 3, 6 (2019), 1389–1393. https://doi.org/10.1016/j.joule.2019.05.002

Mark Diesendorf and Ben Elliston. 2018. The Feasibility of 100 % Renewable Electricity Systems: A Response to Critics. *Renewable and Sustainable Energy Reviews* 93 (2018), 318–330. https://doi.org/10.1016/j.rser.2018.05.042

Eduardo H Diniz, João Akio Yamaguchi, Teresa Rachael dos Santos, André Pereira de Carvalho, Andre Salem Alego, and Mateus Carvalho. 2021. Greening Inventories: Blockchain to Improve the GHG Protocol Program in Scope 2. *Journal of Cleaner Production* 291 (2021), 12. https://doi.org/10.1016/j.jclepro.2021.125900

Alexander Djamali, Patrick Dossow, Michael Hinterstocker, Benjamin Schellinger, Johannes Sedlmeir, Fabiane Völter, and Lukas Willburger. 2021. Asset Logging in the Energy Sector: A Scalable Blockchain-based Data Platform. *Energy Informatics* 4, 3 (2021), 20. https://doi.org/10.1186/s42162-021-00183-3

Jacob Eberhardt. 2021. Scalable and Privacy-preserving Off-chain Computations. https://www.depositonce.tu-berlin.de/bitstream/11303/13087/4/eberhardt_jacob.pdf

European Union. 2009. Directive 2009/28/EC on the Promotion of the Use of Energy from Renewable Sources. https://www.buildup.eu/sites/default/files/RES%20Directive%202009-28-EC.pdf

European Union. 2018. Directive (EU) 2018/2001 of the European Parliament and of the Council. *Official Journal of the European Union* L 328, 82 (2018), 128. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L2001&from=EN

Financial Times. 2021. Heavyweight Investors Demand More Disclosure of Environmental Risks. https://www.ft.com/content/7d23ef7f-33ba-4466-b2f1-2a5dfeba1e33

Gilbert Fridgen, Nikolas Guggenberger, Thomas Hoeren, Wolfgang Prinz, Nils Urbach, Johannes Baur, Henning Brockmeyer, Wolfgang Gräther, Elisaweta Rabovskaja, Vincent Schlatt, André Schweizer, Johannes Sedlmeir, and Lars Wederhake. 2019. Opportunities and Challenges of DLT (Blockchain) in Mobility and Logistics. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1105/wi-1105.pdf

Gilbert Fridgen, Robert Keller, Marc-Fabian Körner, and Michael Schöpf. 2020. A Holistic View on Sector Coupling. *Energy Policy* 147 (2020), 8. https://doi.org/10.1016/j.enpol.2020.111913

Nicolas Gailly, Mary Maller, and Anca Nitulescu. 2021. SnarkPack: Practical SNARK Aggregation. https://eprint.iacr.org/2021/529.pdf

Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. 2013. Quadratic Span Programs and Succinct NIZKs without PCPs. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 626–645. https://doi.org/10.1007/978-3-642-38348-9_37

Alex Gluchowski. 2019. Optimistic vs. ZK Rollup: Deep dive. https://medium.com/matter-labs/optimistic-vs-zk-rollup-deep-dive-ea141e71e075

Christoph Goebel, Hans-Arno Jacobsen, Victor del Razo, Christoph Doblander, Jose Rivera, Jens Ilg, Christoph Flath, Hartmut Schmeck, Christof Weinhardt, Daniel Pathmaperuma, Hans-Jürgen Appelrath, Michael Sonnenschein, Sebastian Lehnhoff, Oliver Kramer, Thorsten Staake, Elgar Fleisch, Dirk Neumann, Jens Strüker, Koray Erek, Rüdiger Zarnekow, Holger Ziekow, and Jörg Lässig. 2014. Energy Informatics. *Business & Information Systems Engineering* 6, 1 (2014), 25–31. https://doi.org/10.1007/s12599-013-0304-2

Shafi Goldwasser, Silvio Micali, and Charles Rackoff. 1989. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.* 18, 1 (1989), 186–208. https://doi.org/10.1137/0218012

Christian Gorenflo, Lukasz Golab, and Srinivasan Keshav. 2019. Mitigating Trust Issues in Electric Vehicle Charging Using a Blockchain. In *Proceedings of the 10th International Conference on Future Energy Systems*. ACM, New York, NY, USA, 160–164. https://doi.org/10.1145/3307772.3328283

Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. 2021. Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. In *30th {USENIX} Security Symposium*. {USENIX}, 17. https://www.usenix.org/conference/usenixsecurity21/presentation/grassi

Jens Groth, Rafail Ostrovsky, and Amit Sahai. 2006. Perfect Non-Interactive Zero Knowledge for NP. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 339–358. https://doi.org/10.1007/11761679_21

Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. 2020. SoK: Layer-two Blockchain Protocols. In *International Conference on Financial Cryptography and Data Security*. Springer, 201–226. https://doi.org/10.1007/978-3-030-51280-4_12

Ákos Hamburger. 2019. Is Guarantee of Origin Really an Effective Energy Policy Tool in Europe? A Critical Approach. *Society and Economy* 41, 4 (2019), 487–507. https://doi.org/10.1556/204.2019.41.4.6

Raphael Hanimann, Johan Vinterbäck, and Cecilia Mark-Herbert. 2015. Consumer Behavior in Renewable Electricity: Can Branding in Accordance with Identity Signaling Increase Demand for Renewable Electricity and Strengthen Supplier Brands? *Energy Policy* 78 (2015), 11–21. https://doi.org/10.1016/j.enpol.2014.12.010

Kenneth Hansen, Christian Breyer, and Henrik Lund. 2019. Status and Perspectives on 100% Renewable Energy Systems. *Energy* 175 (2019), 471–480. https://doi.org/10.1016/j.energy.2019.03.092

Raphael J. Heffron. 2021. Energy Multinationals Challenged by the Growth of Human Rights. *Nature Energy* 6 (2021), 849–851. https://doi.org/10.1038/s41560-021-00906-6

Carsten Herbes and Iris Ramme. 2014. Online Marketing of Green Electricity in Germany – A Content Analysis of Providers' Websites. *Energy Policy* 66 (2014), 257–266. https://doi.org/10.1016/j.enpol.2013.10.083

Hermez Network. 2021. Open Sourcing an Ultra-fast ZK Prover: Rapidsnark. https://blog.hermez.io/open-sourcing-ultra-fast-zk-prover-rapidsnark/

Michael Hinterstocker, Paul Schott, and Serafin von Roon. 2017. Disaggregation of Household Load Profiles. In *10. Internationale Energiewirtschaftstagung an der TU Wien*. 11.

Adrian Jackson, Ashley Lloyd, Justin Macinante, and Markus Hüwener. 2018. Networked Carbon Markets: Permissionless Innovation with Distributed Ledgers? In *Transforming Climate Finance and Green Investment with Blockchains*. Academic Press, 255–268.

Jaap C Jansen. 2017. Does the EU Renewable Energy Sector Still Need a Guarantees of Origin Market? https://www.ceps.eu/ceps-publications/does-eu-renewable-energy-sector-still-need-guarantees-origin-market/

Jaap C Jansen and Dominik Seebach. 2009. Requirements of Electricity End-Users on Tracking of Electricity Generation Attributes and Related Policies. https://repository.tno.nl//islandora/object/uuid:f5d30541-a69a-467a-93f8-fcdc21c9f33a

Patrick Jochem, Sonja Babrowski, and Wolf Fichtner. 2015. Assessing CO_2 Emissions of Electric Vehicles in Germany in 2030. *Transportation Research Part A: Policy and Practice* 78 (2015), 68–83. https://doi.org/10.1016/j.tra.2015.05.007

Tim Johns. 2021. Green Energy Tariffs Often 'Misleading'. https://www.bbc.com/news/business-56602674

Josef Kaenzig, Stefanie Lena Heinzle, and Rolf Wüstenhagen. 2013. Whatever the Customer Wants, the Customer Gets? Exploring the Gap between Consumer Preferences and Default Electricity Products in Germany. *Energy Policy* 53 (2013), 311 – 322. https://doi.org/10.1016/j.enpol.2012.10.061

Niclas Kannengießer, Sebastian Lins, Tobias Dehling, and Ali Sunyaev. 2020. Trade-offs between Distributed Ledger Technology Characteristics. *Comput. Surveys* 53, 2 (2020), 37. https://doi.org/10.1145/3379463

Dimcho Karakashev, Sergey Gorbunov, and Srinivasan Keshav. 2020. Making Renewable Energy Certificates Efficient, Trustworthy, and Anonymous. In *International Conference on Communications, Control, and Computing Technologies for Smart Grids*. IEEE, 1–7. https://doi.org/10.1109/SmartGridComm47815.2020.9302967

Fabian Knirsch, Clemens Brunner, Andreas Unterweger, and Dominik Engel. 2020. Decentralized and Permission-less Green Energy Certificates with GECKO. *Energy Informatics* 3, 1 (2020), 1–17. https://doi.org/10.1186/s42162-020-0104-0

Fabian Knirsch, Andreas Unterweger, Günther Eibl, and Dominik Engel. 2017. Privacy-Preserving Smart Grid Tariff Decisions with Blockchain-based Smart Contracts. In *Sustainable Cloud and Energy Services: Principles and Practices*, Wilson Rivera (Ed.). Springer International Publishing, Cham, Switzerland, Chapter 4, 85–116.

Xiao Fan Liu, Huan-Huan Ren, Si-Hao Liu, and Xian-Jian Jiang. 2021. Characterizing Key Agents in the Cryptocurrency Economy through Blockchain Transaction Analysis. *EPJ Data Science* 10, 1 (2021), 13. https://doi.org/10.1140/epjds/s13688-021-00276-9

Ralph C. Merkle. 1987. A Digital Signature Based on a Conventional Encryption Function. In *Conference on the Theory and Application of Cryptographic Techniques*. 369–378. https://doi.org/10.1007/3-540-48184-2_32

P.E. Morthorst. 2003. A Green Certificate Market Combined with a Liberalised Power Market. *Energy Policy* 31, 13 (2003), 1393–1402. https://doi.org/10.1016/S0301-4215(02)00198-2

Gonzalo Munilla Garrido, Johannes Sedlmeir, Ömer Uludağ, Ilias Soto Alaoui, Andre Luckow, and Florian Matthes. 2021. Revealing the Landscape of Privacy-Enhancing Technologies in the Context of Data Markets for the IoT: A Systematic Literature Review. https://arxiv.org/abs/2107.11905

Laura Palacios-Argüello, Natacha Gondran, Imen Nouira, Marie-Agnès Girard, and Jesus Gonzalez-Feliu. 2020. Which is the Relationship between the Product's Environmental Criteria and the Product Demand? Evidence from the French Food Sector. *Journal of Cleaner Production* 244 (2020), 118588. https://doi.org/10.1016/j.jclepro.2019.118588

Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova. 2013. Pinocchio: Nearly practical verifiable computation. In *Symposium on Security and Privacy*. IEEE, 238–252. https://doi.org/10.1109/SP.2013.47

Moritz Platt, Ruwan J. Bandara, Andreea-Elena Drăgnoiu, and Sreelakshmi Krishnamoorthy. 2021. Information Privacy in Decentralized Applications. In *Trust Models for Next-Generation Blockchain Ecosystems*, Muhammad Habib Ur Rehman, Davor Svetinovic, Khaled Salah, and Ernesto Damiani (Eds.). Springer. https://doi.org/10.1007/978-3-030-75107-4_4

Reuters. 2021. EU to Apply CO2 Emissions Trading to Buildings, Transport, European Commission Says. https://www.reuters.com/business/environment/eu-apply-co2-emissions-trading-buildings-transport-european-commission-says-2021-04-22/

Philipp Richard, Sara Mamel, and Lukas Vogel. 2019. Blockchain in the Integrated Energy Transition. https://www.dena.de/fileadmin/user_upload/dena-Studie_Blockchain_Integrierte_Energiewende_EN.pdf

Alexander Rieger, Florian Guggenmos, Jannik Lockl, Gilbert Fridgen, and Nils Urbach. 2019. Building a Blockchain Application that Complies with the EU General Data Protection Regulation. *MIS Quarterly Executive* 18, 4 (2019), 263–279. https://doi.org/10.17705/2msqe.00020

Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *IEEE Symposium on Security and Privacy*. IEEE, 459–474. https://doi.org/10.1109/SP.2014.36

Markus Schäffer, Monika di Angelo, and Gernot Salzer. 2019. Performance and Scalability of Private Ethereum Blockchains. In *Business Process Management: Blockchain and Central and Eastern Europe Forum*. Springer International Publishing, Cham, 103–118. https://doi.org/10.1007/978-3-030-30429-4_8

Tobias Schaffner. 2021. Scaling Public Blockchains. https://wwz.unibas.ch/fileadmin/user_upload/wwz/00_Professuren/Schaer_DLTFintech/Lehre/Tobias_Schaffner_Masterthesis.pdf

Benjamin Schellinger, Fabiane Völter, Nils Urbach, and Johannes Sedlmeir. 2022. Yes, I Do: Marrying Blockchain Applications with GDPR. In *55th Hawaii International Conference on System Sciences*.

Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. 2020. The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering* 62, 6 (2020), 599–608. https://doi.org/10.1007/s12599-020-00656-x

Johannes Sedlmeir, Philipp Ross, André Luckow, Jannik Lockl, Daniel Miehle, and Gilbert Fridgen. 2021a. The DLPS: A Framework for Benchmarking Blockchains. In *Proceedings of the 54th Hawaii International Conference on System Sciences*. 6855–6864. https://doi.org/10.24251/HICSS.2021.822

Johannes Sedlmeir, Reilly Smethurst, Alexander Rieger, and Gilbert Fridgen. 2021b. Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering* 63, 5 (2021), 603–613. https://doi.org/10.1007/s12599-021-00722-y

StarkWare. 2021. How Does StarkDEX Enhance Decentralization. https://www.starkdex.io/

Jens Strüker, Martin Weibelzahl, Marc-Fabian Körner, Axel Kießling, Ariette Franke-Sluijk, and Mike Hermann. 2021. Dekarbonisierung durch Digitalisierung: Thesen zur Transformation der Energiewirtschaft. https://doi.org/10.15495/EPub_UBT_00005596

Rory Sullivan and Andy Gouldson. 2012. Does Voluntary Carbon Reporting Meet Investors' Needs? *Journal of Cleaner Production* 36 (2012), 60–67. https://doi.org/10.1016/j.jclepro.2012.02.020

Unal Tatar, Yasir Gokce, and Brian Nussbaum. 2020. Law versus Technology: Blockchain, GDPR, and Tough Tradeoffs. *Computer Law & Security Review* 38 (2020). https://doi.org/10.1016/j.clsr.2020.105454

Sonja van Renssen. 2020. The Hydrogen Solution? *Nature Climate Change* 10, 9 (2020), 799–801. https://doi.org/10.1038/s41558-020-0891-0

Anthony Velazquez Abad and Paul E. Dodds. 2020. Green Hydrogen Characterisation Initiatives: Definitions, Standards, Guarantees of Origin, and Challenges. *Energy Policy* 138 (2020). https://doi.org/10.1016/j.enpol.2020.111300

Fabiane Völter, Nils Urbach, and Julian Padget. 2021. Trusting the Trust Machine: Evaluating Trust Signals of Blockchain Applications. *International Journal of Information Management* (2021), 12. https://doi.org/10.1016/j.ijinfomgt.2021.102429

Nan Wang, Sid Chi-Kin Chau, and Yue Zhou. 2021. Privacy-Preserving Energy Storage Sharing with Blockchain. In *Proceedings of the Twelfth International Conference on Future Energy Systems*. ACM, 185–198. https://doi.org/10.1145/3447555.3464869

Richard T Watson, Marie-Claude Boudreau, and Adela J Chen. 2010. Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community. *MIS Quarterly* 34, 1 (2010), 23–38. https://doi.org/10.2307/20721413

Tensie Whelan and Randi Kronthal-Sacco. 2019. Research: Actually, Consumers Do Buy Sustainable Products. https://hbr.org/2019/06/research-actually-consumers-do-buy-sustainable-products

Christian Will, Patrick Jochem, and Wolf Fichtner. 2017. Defining a Day-ahead Spot Market for Unbundled Time-specific Renewable Energy Certificates. In *14th International Conference on the European Energy Market*. IEEE, 6. https://doi.org/10.1109/EEM.2017.7981967

Tanja Winther and Torgeir Ericson. 2013. Matching Policy and People? Household Responses to the Promotion of Renewable Electricity. *Energy Efficiency* 6, 2 (2013), 369–385. https://doi.org/10.1007/s12053-012-9170-x

Karl Wüst and Arthur Gervais. 2018. Do You Need a Blockchain?. In *Crypto Valley Conference on Blockchain Technology*. IEEE, 45–54. https://doi.org/10.1109/CVCBT.2018.00011

Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou. 2020. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys Tutorials* 22, 2 (2020), 1432–1465. https://doi.org/10.1109/COMST.2020.2969706

Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and Privacy on Blockchain. *Comput. Surveys* 52, 3 (2019), 34. https://doi.org/10.1145/3316481

Q. Zhou, H. Huang, Z. Zheng, and J. Bian. 2020. Solutions to Scalability of Blockchain: A Survey. *IEEE Access* 8 (2020), 16440–16455. https://doi.org/10.1109/ACCESS.2020.2967218

#	Challenge	Specifics	Sources
1	Temporal/spatial decoupling	Allows to label grey energy as green (“greenwashing”)	[Will et al. 2017], [Johns 2021]
2	Temporal/spatial decoupling	Indifference and minimal user acceptance Low willingness to pay premiums for green electricity tariffs	[Hamburger 2019], [Bogensperger and Zeisel-mair 2020], [Hanimann et al. 2015], [Jansen and Seebach 2009], [Jochem et al. 2015] [Jansen 2017]
3	Temporal/spatial decoupling	Lacks to incentivize consumers for time-specific consumption	[Bogensperger and Zeiselmair 2020]
4	Intransparency of feed-in quota	Gap between disclosed enery mix and acutal consumption, potential for fraud	[Kaenzig et al. 2013], [Correctiv 2021]
5	Non-automated processes	Complexities and high costs for suppliers and regulators	[Bogensperger and Zeiselmair 2020]
6	Limited scalability	Long-term sustainability regarding increase in decentralied energy production facilities not expected	[Bogensperger and Zeiselmair 2020], [Bañales 2020]
7	Verifiability	Difficulties to detect and prevent double-counting	[Hamburger 2019]
8	Lack of cross-border harmonization	(EU) countries’ registries are not synchronized	[Hamburger 2019], [Jackson et al. 2018]

Table 1. Overview of problems of current GOs registries and sources (supplementary material).

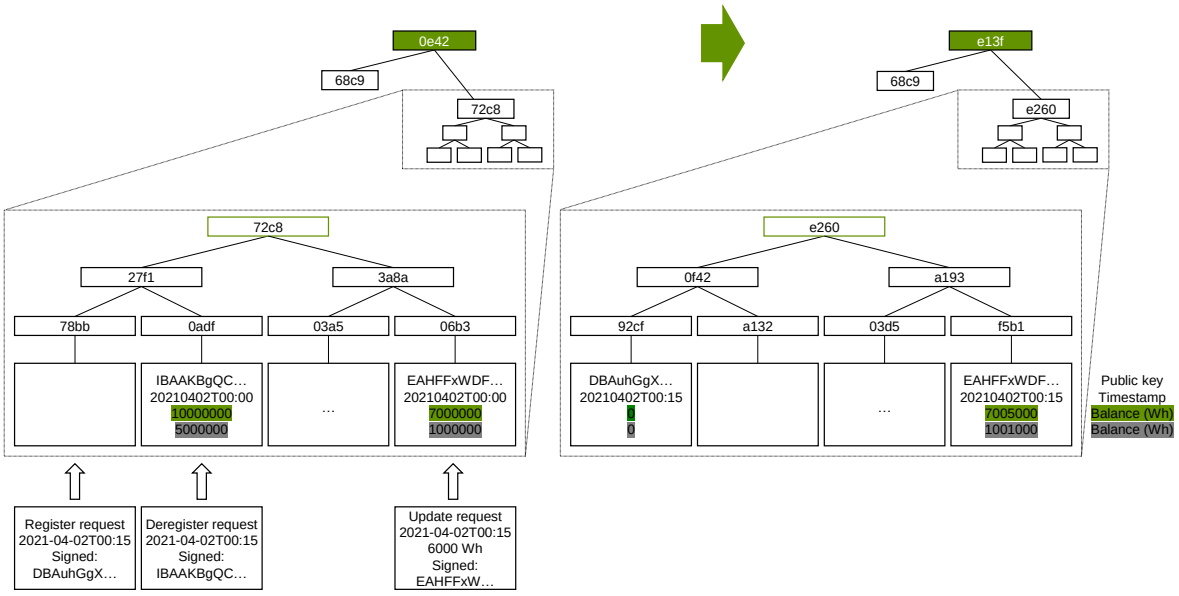

Fig. 2. Account structure of the Merkle tree based accounting.