Journal of Ubiquitous Systems & Pervasive Networks
Volume 17, No. 2 (2022) pp. 73-81

Design and Specification of a Privacy-Preserving Registration for Blockchain-Based Energy Markets

Michell Boerger [a*], Philipp Lämmel [a*], Nikolay Tcholtchev [a*], and Manfred Hauswirth [a,b]

[a] *Fraunhofer Institute for Open Communication Systems (FOKUS), Berlin, Germany*
[b] *Technical University of Berlin, Berlin, Germany*

Abstract

The challenges of climate change and the related demand to integrate non-plannable and weather-dependent renewable energy resources pose enormous challenges for the entire energy domain, e.g. in the context of grid control. These challenges reveal the need for new technical solutions and new business models while they indicate the required and inevitable transition to smart grids. Many blockchain-based solutions are being discussed in this context, ranging from peer-to-peer energy trading to grid-serving applications. However, especially in connection with public blockchains, clear security privacy challenges arise since the security and privacy of private data must be guaranteed while traceability must be avoided. Therefore, in this paper, we will specify privacy-protecting registration processes for blockchain-based flexibility markets that enable pseudonymous access to the latter. Furthermore, in collaboration with a governmental regulating institution named DGA, we will show that using an existing X.509-based PKI and RSA-based cryptographic processes, the integrity of all market participants can be guaranteed. This integrity is essential for the security-critical use of operating reserve. In addition, we will evaluate the specified processes in terms of efficiency, scalability, security, and privacy protection.

Keywords: *Blockchain, privacy, security, encryption, distributed ledger, energy market*

1. Introduction

In modern and future-oriented energy systems, renewable and distributed energy resources (DERs) are playing an increasingly important role. For example, statistics show that in 2020, already 46% of the electricity supply in Germany was covered by renewable energies [1]. However, the unreliability of these energy sources in terms of non-plannable and weather-dependent energy production poses significant challenges to the operators of electric grids with respect to grid stability [2]. For this reason, traditional electricity grids must be modernized, and new technological and economic solutions must be developed, which even integrate decentralized energy resources in a grid-serving manner. However, such decentralized next-generation smart grids require fine-grained control and a high level of security, which poses new security and privacy challenges for the operators. In this context, we have developed blockchain-based operating reserve markets as part of a research project related to the German energy sector. The trading semantics of the proposed operating markets were already presented and evaluated in our previous work [3]. Precisely, on these markets, operators of renewable and distributed energy resources can offer the flexibilities of their resources in the energy production and consumption on intraday and day-ahead markets. Then, operators of electric grids can purchase these flexibilities and integrate them as operating reserves in their grid congestion management processes.

After having already described the markets' trading semantics in [3], this paper focuses on presenting, formally specifying, and evaluating the underlying privacy-preserving and integrity-guaranteeing registration processes implemented in the proposed markets. This approach aims to ensure the privacy and security of the trading data stored on a publicly accessible blockchain utilized by the proposed operating reserve markets. Precisely, we will assign pseudonymous identifiers to all market participants, thus

*Corresponding authors. E-mail: {firstname.lastname}@fokus.fraunhofer.de

DOI: 10.5383/JUSPN.17.02.004

guaranteeing pseudonymous access to the markets. As a result, we protect the users' privacy and render it difficult to trace the users' market and trading behavior for malicious identities. Furthermore, since the use of operating reserve for grid management processes is a security-critical area in the energy sector, we also investigate ensuring the integrity of all market participants. For this purpose, we assume a collaboration with a governmental institution named *data and grid authority (DGA)*. In our model of the energy system, the DGA regulates all market participants and establishes an X.509-based public key infrastructure (PKI) [4][5] using asymmetric Rivest-Shamir-Adleman (RSA) keys [6] between all actors. In this paper, we will then show how to exploit this PKI to guarantee the integrity of the market participants.

Although our registration process was designed for the operating markets described in [3], the presented approach can be adapted to other application domains in which blockchain-based applications require a high-level of privacy and integrity of participating users. The essential requirement for adapting our approach to other domains is the existence of a regulating entity similar to the proposed DGA, which is capable of verifying the integrity of actors in the real-world.

1.1. Related Work

Blockchain is a technology that has been discussed in a wide range of domains and uses cases, for example, among others, emergency communication [7], logistics [8], and supply chains [9]. In addition, particularly in the energy domain, the realization of privacy-preserving and blockchain-based energy trading is an active research topic that many authors have already discussed. For example, in [10], [11], and [12] Ciphertext Policy Attribute-Based Encryption was used to achieve privacy protection and access control for sensitive energy trading data. In contrast, in [13] and [14], the authors present functional encryption methods in which privacy protection is achieved by using functional secret keys through which only a predetermined function of the plaintext values can be retrieved from a set of ciphertexts. Another interesting approach is presented by Gai et al. in [15], in which the authors propose a differential-privacy-based approach. Here, noise and dummy data is added to the trading data to solve the problem of privacy leakage. Unterweger et al. [16] are using the Ethereum blockchain [17] to implement a privacy-preserving energy tariff matching protocol, in which they achieve pseudonymity through Ethereum addresses. In contrast, Kvaternik et al. [18] use a middleware called PETra to achieve pseudonymity and protect privacy in a blockchain-based transactive energy system. Two additional solutions are presented by Brenzikofer et al. [19]. Precisely, they propose a UTXO based coin mixing protocol and an off-chain smart contract running in a trusted execution environment to achieve privacy in a peer-to-peer energy market. Guan et al. [20] propose a privacy-preserving aggregation scheme for energy data, in which they divide users into groups. Each group uses a private blockchain to record the energy data. Within these groups, users are assigned multiple pseudonyms to hide their identity and protect their privacy. Aitzhan et al. [21] use multi-signatures and anonymous encrypted messaging streams to achieve privacy and security in blockchain-based energy trading. Last but not least, Jiang et al. [22] propose a privacy-preserving energy trading scheme, in which they leverage elliptic curve cryptography, homomorphic hiding, and non-interactive zero-knowledge proofs to protect data privacy and hide users' identities in a trustworthy manner.

Although some of the presented works provide satisfying approaches to protect privacy in the context of energy trading, none of the approaches was fully applicable in the conducted project involving a number of industrial partners and the belonging specific requirements. Hence, in order to fullfil the needs of the cooperation in this application context, we had to devise the approach presented in this paper.

2. Background

In the following, we will introduce some technologies and concepts relevant for understanding the paper.

2.1. Blockchain

The use of a blockchain allows our system to benefit in terms of security and privacy. In simple terms, a blockchain is a distributed ledger that orders transactions chronologically and cryptographically securely. As the name indicates, it is a chain of blocks that is distributed decentralized in an underlying untrusted peer-to-peer network with a dynamic number of nodes. These blocks contain a list of public and verifiable transactions with traceable origin where the transactions describe the transfer of digital assets. These transactions are combined into a block and linked to the list of previous transactions. This is done by including a hash of the header of the previous block in the current block. Via this mechanism, the blocks are cryptographically securely chained together. In this untrusted peer-to-peer network, a consensus mechanism called *proof-of-work* is used to find agreement among all participants on which transactions will be recorded in a block [23]. In this mechanism, no node needs to trust any other nodes. Furthermore, an attacker requires more than fifty percent of the entire computational resources of the underlying network to tamper with the blockchain, rendering it hard to attack and tamper-proof [24]. Furthermore, users are represented pseudonymously on a blockchain by using cryptographic techniques. For each user, a wallet is created, consisting of an asymmetric key pair. A unique identifier to represent the user and their account is calculated based on the public key. This identifier is often referred to as address and is used for the user's pseudonymous access to the blockchain network. The private key must be kept confidential and is used to digitally sign a transaction created by the user. The concept of a blockchain was first introduced by Satoshi Nakamoto in 2008 when he presented the Bitcoin network [25]. Bitcoin is a digital peer-to-peer currency that runs without a central instance and does not require any trust. Five years later, in 2013, Buterin introduced a general-purpose blockchain called Ethereum [17]. In Ethereum, apart from the transfer of digital assets, any calculation can be represented and recorded as transactions by leveraging the concept of smart contracts.

2.2. PKI, X.509, and RSA

In addition, we use cryptographic processes based on an X.509-based PKI and the RSA public-key cryptosystem in the specified registration process. In simple terms, a public key infrastructure describes how digital certificates and public keys are managed and securely distributed. These digital certificates bind a public

key of corresponding asymmetric key pair to a certain identity or proof that a public key belongs to a specific person [26]. Using these digital certificates, we can identify the originator of a digital signed messages, provide non-repudiation, and guarantee the integrity of a message. In this paper, we will use the X.509 standard to describe the format of digital certificates. It is created by the ITU-T [4] and also known as ISO/ICE 9594-8 [5]. Furthermore, we will use the RSA public-key cryptosystems for the creation of asymmetric key pairs in the mentioned PKI. RSA was introduced in 1977 by Rivest, Shamir, and Adleman is based on the integer factorization problem in which, given two large primes, it is easy to compute the product, but it is very difficult to factor the resulting product [6]. For details about the mathematical modeling of RSA we refer to the work of Katz et al. [26].

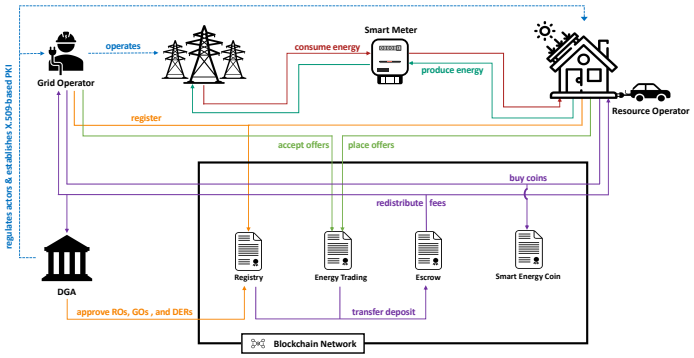

Fig. 1. Architecture of the blockchain-based operating reserve markets which are the basis of this paper.

3. System Overview and Preliminaries

In the context of the mentioned research project related to the German energy system, we developed blockchain-based operating reserve markets. Figure 1 illustrates a simplified version of the proposed operating reserve markets. A detailed specification, implementation, and extensive evaluation of the markets have already been presented in [3]. Therefore, we refer the interested reader to our previous work for more information about the exact market semantics and proposed system. The paper at hand focuses solely on the design and specification of the privacy-preserving registration processes applied in the already presented markets. Therefore, in the following, we will only provide all information about the developed system required to understand the registration processes discussed in this paper.

As depicted in Figure 1, a blockchain network is the main technical component of the system. On this blockchain, multiple smart contracts are deployed, which implement different logical aspects of the system. The most essential smart contract relevant for this paper is the `Registry`, which implements the registration processes described in this paper.

In the illustrated system, two types of market participants exist. The first type of users are the resource operators (ROs), which are the operators of the DERs. The ROs offer the flexibilities in the schedulable energy production and consumption of their DERs on the blockchain-based markets. The second type of users are the grid operators (GOs), which can purchase these offered flexibilities. In our system, the GOs are represented by the transmission system operators (TSOs) and distribution system operators (DSOs), which operate the electric grids and are responsible for their stability. Therefore, they will use the flexibilities offered at our blockchain-based markets as operating reserves for grid control in order to maintain the grid balance.

The electrical grid is a critical infrastructure in any country. In addition, the safety-critical application of operating reserve also requires high security, integrity, and regulation. In order to guarantee these characteristics, we, therefore, introduce a third actor in our system. This actor is represented by the DGA. The DGA is an independent governmental institution that is responsible for regulating the real-world energy system and its actors, thus assuring safety and integrity. In this paper, we make some assumptions about the capabilities of the DGA and the already existing infrastructure between the DGA and actors of the energy system. Based on these assumptions, we will show that we can define privacy-preserving registration processes with guaranteed integrity of all actors and DERs by collaborating with the DGA on the blockchain-based markets.

3.1. Assumptions

First, we assume that the DGA has exclusive access to proprietary data on actors, roles, and resources in the already established energy system. We even assume that in order to participate in the energy system and its manifold applications, actors must first register in the real-world with the DGA (independently of our system). This real-word registration and regulation of the DGA is intended to ensure the integrity and security of the energy system. During this process, all actors are assigned an identifier ID_{user}. Similarly, DERs are assigned an identifier ID_{DER}. These identifiers will then be used in the entire energy system and its various applications. In addition, we further assume that each DER is associated with exactly one smart meter. This assignment is also known to the DGA via the identifier of the smart meter denoted as ID_{SM}.

Furthermore, to also ensure the integrity of the communication between actors in the energy system, we also assume that the DGA deploys a PKI. In this context, the DGA acts as a certificate authority (CA) by issuing digital certificates. In this regard, each actor creates a cryptographic key pair consisting of private and public keys during the real-world registration at the DGA. The DGA then certifies the ownership of the created public key by issuing a digital certificate to the user. Subsequently, this certificate allows users to authenticate themselves to the institution and third parties in a cryptographically secure manner. In the paper, we assume that the PKI is based on the X.509 standard [4][5] and that the RSA cryptosystem [6] is used to create the key pairs.

Finally, we also assume that the DGA provides a registration code n to each actor, which is exclusively provided for the registration at our system. As we will explain later, the users will use it as an additional pseudo-random component in our designed registration process.

4. The Privacy-Preserving Registration Processes

In the following section, based on the assumptions specified above, we will define a blockchain-based registration of users

and DERs in which we can guarantee the integrity of all actors. In this context, the DGA is the trust anchor for the verification and registration in our system. Therefore, we will collaborate with the DGA in the processes described to guarantee the integrity of all market actors. Furthermore, we will also define the registration processes in a privacy-preserving manner. This means that no user has to reveal sensitive information about themselves or their DERs in the openly accessible blockchain. Precisely, we will calculate a unique pseudonym for each user and DER, which will then be used with the blockchain-based markets to represent these identities. The resulting pseudonymous access to the markets protects the users' privacy while also rendering it hard for malicious actors to trace their trading behavior.

4.1. User registration

The user registration process is illustrated in Figure 2. As we can see, it consists of two separate steps. First, the user must provide encrypted registration information on the blockchain-based markets in order to prove their integrity. In the second step, the DGA verifies this information and either guarantees the user's integrity or reject the registration attempt.

In the first step, to store the registration information on the markets, the users must invoke a smart contract function, which triggers a blockchain transaction using their blockchain account. In this function, the user specifies the market role they wish to perform (either GO or RO) and a calculated pseudonymous hash identifier based on their identifier ID_{user} provided by the DGA. Furthermore, they must provide a specific digital signature calculated using their RSA-based private key. Therefore, the smart contract function input triple reg_{user} is defined as:

$$reg_{\text{user}} := (role,\ h(ID_{\text{user}},\ n),\ u) \tag{1}$$

where the ciphertext parameter u is defined as:

$$u := pk_{\text{DGA}}(ID_{\text{user}},\ sk_{\text{user}}(ID_{\text{user}},\ n)) \tag{2}$$

In this context, $pk_*(\cdot)$ defines the ciphertext encrypted with the RSA-based public key pk_*. Accordingly, $sk_*(\cdot)$ defines the ciphertext encrypted using the corresponding secret key sk_*. Furthermore, $h(\cdot)$ represents the SHA-256 hash function [27]. The parameter n is the user's registration code provided by the DGA and is defined as:

$$n := sk_{\text{DGA}}(h(ID_{user})) \tag{3}$$

The parameter $h(ID_{\text{user}},\ n)$ is a pseudonymous identifier representing the user and prevents them from revealing their real-world identity on the public blockchain, thus protecting their privacy. Only the user and the DGA can create this pseudonymous identifier, as only they know the assigned registration code n.[1] The uniqueness characteristic of the pseudonymous identifier has the additional advantage that the system can guarantee that no user can register twice. No other blockchain account can register using the same $h(ID_{\text{user}},\ n)$. If the system detects a duplicated usage of this parameter, the corresponding registration transactions would be reverted. Thereby, we want to highlight that the parameter is only used during the registration process to identify a user in order to prevent double registration. For all subsequent market actions, the system uses the pseudonymous blockchain account address to identify registered users. In this context, we require the registration code n as a pseudo-random component in the calculation of the hash identifier in order to prevent attackers who either already know the user ID or are using brute-force attacks to reveal the user's identity and thus link the blockchain account to real-world users, which would violate their privacy. Therefore, the users have to ensure that the parameter n gets not leaked to third parties. As the definition of the registration code (see Eq. 3) implies, there is no additional effort for the DGA other than to provide the registration code during the real world registration. As we will show below, the DGA does not have to store the registration code because it can verify it at any time using its public key and the parameter ID_{user}. After this first registration step, the data from reg_{user} is now stored and assigned to the user's blockchain account, containing all relevant information to verify the integrity of the applying market participant. However, the user behind the account is not yet successfully registered and must wait for approval from the DGA.

In the second registration step, in order to guarantee the integrity of the user data, the DGA has to verify the stored registration data. When a user has performed a registration transaction, the smart contract emits an event to notify the DGA that a user needs to be verified. Subsequently, the DGA reads the parameters u, $h(ID_{\text{user}},\ n)$, and the stored role from the blockchain to prove the integrity of the user data in a three step verification process:

1) First, the DGA uses its private key sk_{DGA} and the parameter u to identify the real-world user. Specifically, the DGA can extract the identifier ID_{user} and the user's digital signature $sk_{\text{user}}(ID_{\text{user}},\ n)$ by applying the arithmetic of asymmetric cryptography to u:

$$sk_{\text{DGA}}(u) = sk_{\text{DGA}}(pk_{\text{DGA}}(ID_{\text{user}},\ sk_{\text{user}}(ID_{\text{user}},\ n))) \tag{4}$$

$$= (ID_{\text{user}},\ sk_{\text{user}}(ID_{\text{user}},\ n)) \tag{5}$$

Then it checks the validity of the provided signature by using the public key pk_{user} of the user known to it and extracts the signature input data by applying:

$$pk_{\text{user}}(sk_{\text{user}}(ID_{\text{user}},\ n)) = (ID_{\text{user}},\ n) \tag{6}$$

The DGA now verifies that the extracted ID_{user} and the registration code n are valid. For this purpose, it uses its public key pk_{DGA} to decrypt the registration code n in order to extract the encrypted value $h(ID_{\text{user}})$ (see Eq. 3). Then, it uses the parameter ID_{user} just extracted from $sk_{\text{user}}(ID_{\text{user}},\ n)$ and applies the SHA-256 hash to it. Finally, it checks whether the calculated and extracted hash matches to prove the validity of the registration code. Then, it also verifies that the inner and outer ID_{user} parameters extracted from u are identical. If these parameters also match, the DGA assumes that the signature and parameter u are correct and were created by the user ID_{user}.

2) As a next step, the DGA verifies the pseudonym $h(ID_{\text{user}},\ n)$ read from the blockchain. Therefore, it simply recalculates the parameter based on the parameters ID_{user} and n just extracted from the already verified parameter u. Then, it validates whether the calculated hash value and the value read

[1] Since the DGA is the trust anchor for the verification and registration in our system and represented by a governmental institution, we do not see any potential attack vector or privacy-leakage here.

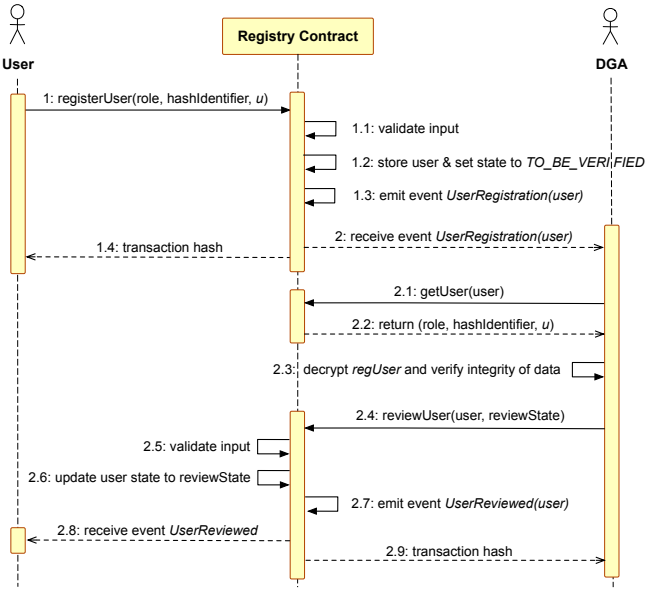

Fig. 2. Sequence diagram visualizing the user registration.

from the blockchain match. If this is the case, it is guaranteed that the user also used the correct pseudonymous identifier.

3) In the third and last verification step, the DGA finally checks whether the user is allowed to operate as the claimed role in the energy system using its proprietary data set. If all three verification steps were successful, it issues a blockchain transaction to unlock the user, which grants them access to the blockchain-based markets. On the contrary case, it blocks the user in the markets with a different kind of transaction.

In the described user registration process, the DGA is the only instance that can decrypt and interpret the parameter u and identify real-world users behind the pseudonymous identifiers $h(ID_{\text{user}},\ n)$. Therefore, it is also the only instance that can link blockchain accounts to real-world users. Through this mechanism, we can guarantee the real-world user's integrity behind the blockchain account used for registration while protecting the user's privacy through pseudonymous access.

4.2. Resource registration

In a similar way, we can define the registration process for DERs. If an RO wants to trade flexibilities of one of its owned DERs on the markets, they must first register them on the markets and the registration has to be verified by the DGA. This verification is needed to confirm that the RO is the actual operator and the DER really exists and can provide operating reserve. As a requirement for this registration process, we impose the apparent condition that the user has previously registered as RO and were successfully verified by the DGA based on the process described above. Afterward, the RO can register a DER on the markets by initiating a blockchain transaction by invoking a smart contract function with the following input:

$$reg_{\text{DER}} := (\text{type},\ h(ID_{\text{DER}},\ n),\ h(ID_{\text{SM}}),\ r) \tag{7}$$

where we define the encrypted ciphertext r as:

$$r\ :=\ pk_{\text{DGA}}(ID_{\text{user}},\ ID_{\text{DER}},\ ID_{\text{SM}},\ sk_{\text{user}}(ID_{\text{user}},\ n)) \tag{8}$$

The tuple reg_{DER} is stored on the blockchain and assigned to the blockchain account address of the transaction inititating and already successfully registered user. The input parameters consist of the $type$ of the DER and the SHA-256 hash of the smart meter identifier ID_{SM} assigned to the DER's, which we notate as $h(ID_{\text{SM}})$. In addition, the RO must provide the input parameters $h(ID_{\text{DER}},\ n)$ and r, which serve two purposes.

The parameter $h(ID_{\text{DER}},\ n)$ is used as a pseudonymous identifier of the DER. For all market activities, users must specify this parameter to identify DERs uniquely. Using this parameter prevents the RO from revealing the real-world identifier of their DER to the blockchain, protecting the privacy of their trading and production data. Additionally, since $h(ID_{\text{DER}},\ n)$ is also unique for each DER and operating RO pair, we can use it to guarantee that no RO can register DERs twice by reverting registration transactions when duplicated $h(ID_{\text{DER}},\ n)$ parameters are detected.

The ciphertext r is used to guarantee the integrity of the DER and is understood as a digital signature. The parameter can only be decrypted and interpreted by the DGA, which makes its involvement necessary. Similar to the user registration process, the DGA receives an event when a DER was registered and needs to be verified. Therefore, the DGA retrieves the parameters contained in reg_{DER} from the blockchain and verifies them in a four-step verification process.

1) In the first step, the DGA uses its private key sk_{DGA} to decrypt r and to extract the contained encrypted parameters by applying:

$$sk_{\text{DGA}}(r) = (ID_{\text{user}},\ ID_{\text{DER}},\ ID_{\text{SM}},\ sk_{\text{user}}(ID_{\text{user}},\ n)) \tag{9}$$

Then, it checks the validity of the provided signature $sk_{\text{user}}(ID_{\text{user}},\ n)$ by using the public key pk_{user} exactly as described in the user registration process. Furthermore, the DGA also checks whether the found user ID_{user} is a registered RO and assigned to the specified resource ID_{DER} based on information from its proprietary database. If all requirements are fulfilled, the DGA assumes that the parameter r is correct.

2) In the next verification step, the integrity of the pseudonymous identifier $h(ID_{\text{DER}},\ n)$ gets verified. For this purpose, the DGA recalculates the parameter based on the parameters ID_{DER} and n just extracted from the verified parameter r. Subsequently, it validates whether the calculated hash value and the value read from the blockchain match. If this is the case, the system can guarantee that the RO also used the correct pseudonymous identifier for their DER.

3) As the third step, the DGA checks whether the smart meter ID_{SM} is allocated to this DER ID_{DER} using its proprietary database. It also checks whether the RO provided the correct smart meter hash by just recalculating it and comparing it with the value read from blockchain.

4) In the last step, the DGA must ensure that a user with multiple identities registers the DER for the correct blockchain account[2]. To do this, the DGA uses the parameters ID_{user} and n extracted from r to calculate the pseudonymous hash identifier $h(ID_{\text{user}},\ n)$ of the RO that is currently trying to register the DER (see Eq. 1). Then it reads from the blockchain the address

[2] For example, grid operators could also operate DERs and therefore be ROs. In this case, they would have to register with two distinguished blockchain accounts for each role on the blockchain-based markets.

of the user with this calculated pseudonymous identifier. Next, the DGA checks whether this address matches the one that issued the transaction for registering the DER. This procedure ensures that the user is using their correct blockchain identity. If all these four verification steps succeeded, the DGA approves the DER by issuing a blockchain transaction that unlocks the DGA. Henceforth, the RO can offer flexibilities for it on the markets using the pseudonymous identifier.

In the two registration processes presented, we can guarantee the integrity of users and DERs in the markets. At the same time, we have enabled pseudonymous access to the markets. This protects the privacy of the users and their trading data. Since only the DGA can link blockchain accounts to real-world users and DERs, malicious actor must break the protection measures of the former to trace market and trading behavior to real world identities. This enables the implementation of free, protected, non-discriminatory, and privacy-preserving markets while guaranteeing the integrity of all participants. A more detailed security and privacy analysis is provided in Section 5..

5. Evaluation

In the context of the mentionend research project, we developed a prototype of the blockchain-based operating reserve markets outlined in Section 3.. A detailed description of the implemenation and evaluation of the developed prototype is discussed in our previous work [3]. To summarize, the system simplified shown in Figure 1 was implemented by utilizing the Ethereum blockchain [17]. All illustrated smart contracts were implemented using Solidity [28]. Furthermore, we created a test environment simulating the X.509-based PKI based on 2048 bit RSA keys required for the registration of users and DERs. Thereby, all X.509 certificates and RSA keys are generated using the node-forge [29] library. In the following, based on the controlled market simulation[3] described in [3], we will evaluate the implemented registration processes with respect to efficiency and scalability. In addition, we will discuss some security and privacy characteristics of the presented system.

5.1. Gas Costs Analysis

As transactions are executed in a decentralized manner, the CPU and memory utilization of an application are not of great importance in the Ethereum ecosystem. Instead, the most relevant metric determining the efficiency of an Ethereum-based application are the gas costs required to execute corresponding transactions. The gas costs are an approximate indicator for the efficiency and resource utilization of the developed smart contract functions [30]. Therefore, in order to be able to evaluate the efficiency of the registration processes, we examined the gas costs of the essential smart contract functions in a controlled market simulation discussed in [3]. Precisely, we have stepwise registered 60 users in the simulated market environment. Thereby we registered a total of 30 ROs and GOs in the system. Furthermore, each of the 30 ROs registered two DERs in the simulation, resulting in a total of 60 DERs. The market simulation and the

Fig. 3. Illustration of measured transaction costs.

measurement of the transaction gas costs were performed using the Ganache blockchain [31], a local running private Ethereum blockchain representing a test environment for this platform.

In the following, we will solely evalute the efficency and scalability of the Registry smart contract, as it implements all registration processes discussed in this paper. As described in Section 4., the double-registration of users and DERs is prevented by using a pseudonymous hash identifier. Therefore, all already stored hash identifiers must be considered during registration, rendering the transactions cost of the correspoding functions dependend on this parameters. For this reason, we have evaluated these functions in relation to the number of users and DERs already registered in the system during the market simulation. This also allows us to make statements about the scalability of these processes.

The results of our measurements are illustrated in Figure 3. By investigating the function `registerUser`, we can infer that the transactions costs for registering a user are almost constant. The function manifests an average gas cost of 908.716 gas $\cdot 10^3$ with a standard deviation of just 2.716 gas $\cdot 10^3$. Similary, the costs for performing a DER registration using the `registerResource` function are relatively stable with an average gas cost of 1388.954 gas $\cdot 10^3$ and a standard deviation of 10.877 gas $\cdot 10^3$. The reason for the almost constant costs is that hash identifiers of both objects are stored in a Solidity mapping. This enables us to verify if the respective hash identifier is already used in a constant time, rendering the complexity of the whole registration process constant. Small variations in the costs of these functions can be explained by the initial initiation of different data instances and helper objects. Assuming a Ethereum mainnet block gas limit of 12487205 gas[4], we can represent a maximum of 13 user registration and up to 9 resource registration transactions in one Ethereum mainnet block.

Furthermore, we can deduce from Figure 3 that the functions `reviewUser` and `reviewResource`, which represent the positive or negative verification of the users or DERs, are also to be regarded as constant. Our measurements show that the average transaction cost for the positive user verification is 131.308

[3] Again, we refer the interested reader to [3] for a detailed description and evaluation of the implemented operating reserve markets and conducted market simulation experiments.

[4] Block gas limit of the Ethereum mainnet on the 08/17/2020 taken from https://ethstats.net/

gas $\cdot 10^3$ with a standard deviation of 0.003 gas $\cdot 10^3$. For a negative verification, the average transaction cost is 131.403 gas $\cdot 10^3$ with the same standard deviation. For DERs, the transaction costs are 152.517 gas $\cdot 10^3$ in the positive case and 152.588 gas $\cdot 10^3$ in the negative case. Both cases have no standard deviation. As a result, we can place a maximum of 95 user and 81 resource review transactions in an Ethereum mainnet block.

In summary, we conclude that the registration processes have been implemented in an efficient and scalable fashion. All discussed functions demonstrate an almost constant complexity and do not depend on the already registered objects of the same kind. We have also shown that in the Ethereum mainnet up to 13 user or 9 resource registration transactions per 15 seconds are possible[5]. Therefore, we consider the possible throughput for the registration processes as sufficient.

5.2. Security and Privacy Analysis

In the following, we will discuss some security and privacy characteristics of the presented system. Thereby, we are assuming an operation of the system using a public Ethereum blockchain.

5.2.1. Integrity

As a result of the registration processes presented in this paper, we can guarantee the integrity of all market participants by utilizing cryptographic procedures and a collaboration with the DGA. Especially in the security-critical domain of deploying operating reserves, this integrity is of crucial importance and contributes to the security of the energy sector. Furthermore, the inherent properties of the utilized blockchain also increase the security and integrity of the system, as all market operations are represented as blockchain transactions. The used Ethereum blockchain automatically ensures the security and integrity of all blockchain transactions. Concretely, all transactions are cryptographically securely signed using the keys of the users' owned and self-managed Ethereum wallet. Therefore, we can also ensure the integrity of the transactions and thus the integrity of the corresponding market operations.

5.2.2. Accountability and Non-Repudiation

Thanks to the verification of all market participants by the DGA and the cryptographically secure signing of all transactions on the blockchain layer, we can also guarantee accountability in our system. On the one hand, the underlying Ethereum blockchain ensures the accountability of Ethereum accounts used for performed blockchain transactions. Second, through the registration processes described in Section 4., we can also prove that verified market participants are in possession of certain Ethereum accounts. Since they must then use this verified Ethereum account to execute all market operations, we can also make concrete market participants accountable for their operations on the blockchain-based markets. As a result, the system also manifests non-repudiation since sellers and buyers cannot repudiate their bids and trading behavior.

[5] For the Ethereum mainnet a block time of about 15 seconds applies[32].

5.2.3. Decentralisation

Our proposed system also benefits from the distributed nature of the underlying Ethereum blockchain and the decentralized execution of transactions. The decentralized data administration and processing of transactions increases the *reliability*, *robustness*, and *fault-tolerance* of our system. Furthermore, the increased decentralization also increases the *availability* of our system. In addition, the proof-of-work consensus mechanism used in the Ethereum blockchain also renders our system and the stored data *tamper-proof* [23].

5.2.4. Trust

By using the public Ethereum blockchain, users can access our markets without trusting any third parties for all trading processes. Nevertheless, we require the market participants to trust the DGA during the registration processes described in this paper. However, we do not consider this to be a problem, as the DGA is a fundamental component in guaranteeing the integrity of all market participants and thus ensuring security in the energy sector. If we assume malicious behavior of the DGA, it is obvious that it could corrupt the registration processes described in Section 4. at any time. For example, the DGA could incorrectly fail to verify the integrity of users or even register fake users and DERs. However, since in our energy system model the DGA is a governmental institution responsible for regulating and controlling the energy sector, we assume a permanent trustworthy and proper behavior of the DGA. Therefore, we do not see a realistic attack vector in this case. Hence, we believe that this required trust is justifiable concerning the required integrity and security of the energy system. Nevertheless, we want to emphasize that it is of paramount importance to protect the security of the DGA and its managed infrastructure in our system.

5.2.5. Privacy Protection, Traceability, and Confidentiality

In this paper, we presented privacy-preserving registration processes in which users and DERs are assigned static and cryptographically secure pseudonyms which enables pseudonymous access to the markets. Precisely, the system assigns a pseudonym to DERs that is used for all trading operations on the blockchain-based markets. In contrast, pseudonyms assigned to the users are only used during the registration processes in order to avoid double-registration attacks. After successful verification, users are identified by their Ethereum account used during the registration process. However, since this also represents a pseudonym, we claim that pseudonymity is still preserved. As a result, the DGA is the only entity in our system that can link the pseudonymous identifiers and blockchain accounts to real-world users and DERs. This is caused by its required responsibilities for guaranteeing the integrity of market participants and DERs during registration. However, as just discussed, since the DGA can be trusted, we still consider the privacy of the users to be protected and conclude that it is difficult for malicious actors to trace the market and trading behavior to real-world identites as it would require to break the protection measures of the DGA. As a result, we conclude that our system ensures appropriate security of personal data against unauthorized or unlawful parties through pseudonymous access to the markets.

However, we would like to mention that pseudonymity is not to be understood as anonymity. In fact, manifold attack vectors exist to deanonymize (static) pseudonyms and violating the traceability [33][34]. For example, studies have shown that it is feasible to use *Transaction Fingerprinting* or *AS-level deployment analysis* attacks to map IP addresses to pseudonymous blockchain accounts and thus deanonymize users [34]. In this case, applications such as Tor [35], which promise anonymity on a network layer, can help to mitigate the risk. A comprehensive survey on privacy-protecting approaches in the context of blockchain can be found in [33].

6. Conclusion

In this paper, we designed and specified privacy-preserving registration processes for blockchain-based operating reserve markets, in which we can guarantee the integrity of all market actors through cryptographic processes. In concrete terms, we enabled pseudonymous access to the markets by collaborating with a governmental institution named *data and grid authority*. Since the energy grid is a critical infrastructure, we assume that this institution regulates the real-world energy sector and establishes an X.509-based PKI between actors. Based on these assumptions, we designed a verification process that makes it possible to guarantee real-world users' and DERs' integrity in our blockchain-based markets, which is relevant for the critical application of operating reserves. Furthermore, we enabled pseudonymous access by creating cryptographic secure pseudonyms for each market actor and DER, thus protecting their privacy in the presented market mechanisms. Hence, we enabled the implementation of free, protected, non-discriminatory, and privacy-preserving blockchain-based operating reserve markets.

In conclusion, we demonstrated the applicability of blockchain-based operating reserve markets that fulfil the fine-grained access control and high security and integrity requirements demanded by decentralized next-generation smart grids. Furthermore, we have shown that access control and integrity verification can be implemented efficiently and scalable by using the Ethereum blockchain. Precisely, all proposed and evaluated registration processes manifest constant transaction gas costs. Although our registration process was designed for the operating markets described in [3], the presented approach can be adapted for other blockchain-based applications where user privacy and integrity are of great importance. Therefore, we recommend investigating the applicability of the presented approach in other domains for future work.

References

[1] Bundesministerium für Wirtschaft und Energie. Erneuerbare Energien. URL https://www.bmwi.de/Redaktion/DE/Dossier/erneuerbare-energien.html.

[2] BMWi. Ein Stromnetz für die Energiewende. URL https://www.bmwi.de/Redaktion/DE/Dossier/netze-und-netzausbau.html.

[3] Michell Boerger, Philipp Lämmel, Nikolay Tcholtchev, and Manfred Hauswirth. Enabling short-term energy flexibility markets through blockchain. *ACM Trans. Internet Technol.*, may 2022. ISSN 1533-5399. . URL https://doi.org/10.1145/3542949. Just Accepted.

[4] ITU-T, . URL https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509.

[5] ISO/IEC 9594-8:2017. URL https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/25/72557.html.

[6] R L Rivest, A Shamir, and L Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. page 15.

[7] Budankailu Kumar Subudhi, Faruk Catal, Nikolay Tcholtchev, Kin Tsun Chiu, Yacine Rebahi, Michell Boerger, and Philipp Lämmel. Performance testing for VoIP emergency services: a case study of the EMYNOS platform and a reflection on potential blockchain utilisation for NG112 emergency communication. *Journal of Ubiquitous Systems and Pervasive Networks*, 12(1):01–08, November 2019. . URL https://doi.org/10.5383/juspn.12.01.001.

[8] Yassine Issaoui, Azeddine Khiat, Ayoub Bahnasse, and Hassan Ouajji. Smart logistics: Blockchain trends and applications. *Journal of Ubiquitous Systems and Pervasive Networks*, 12(2):09–15, March 2020. . URL https://doi.org/10.5383/juspn.12.02.002.

[9] Kamalendu Pal and Ansar-Ul-Haque Yasar. Convergence of internet of things and blockchain technology in managing supply chain. *Journal of Ubiquitous Systems and Pervasive Networks*, 14(2):11–19, January 2021. . URL https://doi.org/10.5383/juspn.14.02.002.

[10] Zhitao Guan, Xin Lu, Wenti Yang, Longfei Wu, Naiyu Wang, and Zijian Zhang. Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid. *Journal of Parallel and Distributed Computing*, 147:34–45, January 2021. ISSN 0743-7315. . URL https://www.sciencedirect.com/science/article/pii/S0743731520303609.

[11] Xin Lu, Zhitao Guan, Xiao Zhou, Longfei Wu, Xiaojiang Du, and Mohsen Guizani. An Efficient and Privacy-Preserving Energy Trading Scheme Based on Blockchain. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, December 2019. . ISSN: 2576-6813.

[12] Wenti Yang, Zhitao Guan, Longfei Wu, Xiaojiang Du, Zefang Lv, and Mohsen Guizani. Autonomous and Privacy-preserving Energy Trading Based on Redactable Blockchain in Smart Grid. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pages 1–6, December 2020. . ISSN: 2576-6813.

[13] Turabek Gaybullaev, Hee-Yong Kwon, Taesic Kim, and Mun-Kyu Lee. Efficient and Privacy-Preserving Energy Trading on Blockchain Using Dual Binary Encoding for Inner Product Encryption. *Sensors*, 21(6):2024, January 2021. . URL https://www.mdpi.com/1424-8220/21/6/2024. Number: 6 Publisher: Multidisciplinary Digital Publishing Institute.

[14] Ye-Byoul Son, Jong-Hyuk Im, Hee-Yong Kwon, Seong-Yun Jeon, and Mun-Kyu Lee. Privacy-Preserving Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids Using Functional Encryption. *Energies*, 13(6):1321, January 2020. . URL https://www.mdpi.com/1996-1073/13/6/1321. Number: 6 Publisher: Multidisciplinary Digital Publishing Institute.

[15] Keke Gai, Yulu Wu, Liehuang Zhu, Meikang Qiu, and Meng Shen. Privacy-Preserving Energy Trading Using

Consortium Blockchain in Smart Grid. *IEEE Transactions on Industrial Informatics*, 15(6):3548–3558, June 2019. ISSN 1941-0050. . Conference Name: IEEE Transactions on Industrial Informatics.

[16] Andreas Unterweger, Fabian Knirsch, Christoph Leixnering, and Dominik Engel. Lessons Learned from Implementing a Privacy-Preserving Smart Contract in Ethereum. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5, February 2018. . ISSN: 2157-4960.

[17] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform, November 2013. URL https://github.com/ethereum/wiki/wiki/White-Paper.

[18] Karla Kvaternik, Aron Laszka, Michael Walker, Douglas Schmidt, Monika Sturm, Martin lehofer, and Abhishek Dubey. Privacy-Preserving Platform for Transactive Energy Systems. *arXiv:1709.09597 [cs]*, January 2018. URL http://arxiv.org/abs/1709.09597. arXiv: 1709.09597.

[19] Alain Brenzikofer and Noa Melchior. Privacy-Preserving P2P Energy Market on the Blockchain. *arXiv:1905.07940 [cs]*, May 2019. URL http://arxiv.org/abs/1905.07940. arXiv: 1905.07940.

[20] Zhitao Guan, Guanlin Si, Xiaosong Zhang, Longfei Wu, Nadra Guizani, Xiaojiang Du, and Yinglong Ma. Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities. *IEEE Communications Magazine*, 56(7):82–88, July 2018. ISSN 1558-1896. . Conference Name: IEEE Communications Magazine.

[21] Nurzhan Zhumabekuly Aitzhan and Davor Svetinovic. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852, September 2018. ISSN 1941-0018. . Conference Name: IEEE Transactions on Dependable and Secure Computing.

[22] Shunrong Jiang, Xiaoyan Zhang, Jinpeng Li, Hao Yue, and Yong Zhou. Secure and Privacy-preserving Energy Trading Scheme based on Blockchain. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pages 1–6, December 2020. . ISSN: 2576-6813.

[23] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain Technology Overview. *arXiv:1906.11078 [cs]*, page NIST IR 8202, October 2018. . URL http://arxiv.org/abs/1906.11078. arXiv: 1906.11078.

[24] F. Tschorsch and B. Scheuermann. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123, 2016. ISSN 1553-877X. .

[25] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. page 9, October 2008. URL https://bitcoin.org/bitcoin.pdf.

[26] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. Chapman & Hall/CRC cryptography and network security. CRC Press, Taylor & Francis Group, Boca Raton London New York, second edition edition, 2015. ISBN 978-1-4665-7026-9. OCLC: 900419026.

[27] Tony Hansen and Donald E. Eastlake 3rd. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). URL https://tools.ietf.org/html/rfc6234#section-4.1.

[28] Solidity — Solidity 0.5.16 documentation, . URL https://docs.soliditylang.org/en/v0.5.16/index.html.

[29] node-forge, . URL https://www.npmjs.com/package/node-forge.

[30] Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. 2014. URL https://ethereum.github.io/yellowpaper/paper.pdf. Edition: d6ff64f - 2019-06-13.

[31] Ganache CLI, November 2020. URL https://github.com/trufflesuite/ganache-cli. original-date: 2016-01-08T17:40:36Z.

[32] M. Bez, G. Fornari, and T. Vardanega. The scalability challenge of ethereum: An initial quantitative analysis. In *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, pages 167–176, April 2019. . ISSN: 2642-6587.

[33] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L. Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, 7:164908–164940, 2019. ISSN 2169-3536. . Conference Name: IEEE Access.

[34] Sumit Soni and Bharat Bhushan. A Comprehensive survey on Blockchain: Working, security analysis, privacy threats and potential applications. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, volume 1, pages 922–926, July 2019. .

[35] The Tor Project | Privacy & Freedom Online, . URL https://torproject.org.