RESEARCH

Asset Logging in the Energy Sector: A Scalable Blockchain-based Data Platform

Alexander Djamali[1*], Patrick Dossow[1], Michael Hinterstocker[1], Benjamin Schellinger[2,3,4], Johannes Sedlmeir[2,3,4], Fabiane Völter[2,3,4] and Lukas Willburger[2,3,5]

[*]Correspondence: adjamali@ffe.de
[1]FfE, Am Blütenanger 71, 80995 München, GER
Full list of author information is available at the end of the article

Abstract

Due to a steeply growing number of energy assets, the increasingly decentralized and segmented energy sector fuels the potential for new digital use cases. In this paper, we focus our attention on the application field of asset logging, which addresses the collection, documentation, and usage of relevant asset data for direct or later verification. We identified a number of promising use cases that so far have not been implemented; supposedly due to the lack of a suitable technical infrastructure. Besides a high degree of complexity associated with various stakeholders and the diversity of assets involved, the main challenge we found in asset logging use cases is to guarantee the tamper-resistance and integrity of the stored data while meeting scalability, addressing cost requirements, and protecting sensitive data. Against this backdrop, we present a blockchain-based platform and argue that it can meet all identified requirements. Our proposed technical solution hierarchically aggregates data in Merkle trees and leverages Merkle proofs for the efficient and privacy-preserving verification of data integrity thereby ensuring scalability even for highly frequent data logging. By connecting all stakeholders and assets involved on the platform through bilateral and authenticated communication channels and adding a blockchain as a shared foundation of trust, we implement a wide range of asset logging use cases in a cost-effective manner, and provide the basis for leveraging platform effects in future use cases that build on verifiable data. Along with the technical aspects of our solution, we discuss the challenges of its practical implementation in the energy sector and the next steps for testing through a regulatory sandbox approach.

Keywords: Asset Management; Distributed Ledger; Energy Assets; Merkle Proofs; Privacy; Self-sovereign Identities

Introduction

In light of the ongoing energy transition, the energy sector is subject to significant changes, which are expected to further accelerate in the future. The ever-larger number of decentralized energy assets, most notably wind turbines and photovoltaic systems, but also stationary batteries and battery electric vehicles, increases the complexity of the energy system at a challenging pace. As of today, some owners and operators of energy assets struggle with these changes while others are keen to seize emerging opportunities.

A major field of development and change in the energy sector is the acquisition and usage of digital data for the documentation and verification of the state and operation of assets [1]. For one thing, digitalization in general is a necessity to monitor and evaluate a large number of often decentralized assets and ensure the proper functioning of the complex energy system [2]. This is particularly important for assets of systemic relevance and assets that are newly integrated into already digitalized processes. In addition, reliable digital asset data can enable use cases that were previously unfeasible or impractical. In this regard, complex processes with high demand regarding up-to-date data availability and temporal resolution can be newly implemented through the appropriate provision and handling of high quality data [3].

To achieve actual progress, we focus our research on a field of applications beyond the mere digitization of asset data. Through systematic dialogues and focus groups with experts of partner companies from the energy sector, we identified that most relevant use cases are characterized by a small yet challenging set of common requirements. These use cases, to which we refer to as "asset logging" use cases, generally demand tamper-resistance and verifiability along the entire chain of data usage and traceability of the chronological sequence of collected data, while maintaining data privacy and sovereignty required by the data's respective owner. In turn, these specifications led to our research on device-specific machine identities and a decentralized, blockchain-based platform [4]. In this paper, we aim to create a strong understanding of the requirements, challenges and potentials of the group of asset logging use cases. We present our novel digital platform architecture that we designed and implemented to realize the identified use cases and showcase how it meets the identified requirements. A discussion of prevailing issues and challenges for the intended practical implementation of selected use cases in a sandbox approach completes our contribution.

Use Case Assessment in the Energy Sector

In the energy sector, the transition to digitalization and new digital business approaches tends to be a relatively slow process [5]. As for asset logging, we found that even though the documentation and verification of assets is a necessity for many applications[6], there is still a lack of clear standards and a strong dependency on different degrees of digitalization [1], which opens up room for improvements. At the same time, an increasing overlap and interaction of different roles creates the need as well as the opportunity for new use cases in the field. One example of such new stakeholders in the energy system is the "prosumer", who has emerged as a hybrid of the two conventional roles of electricity producer and electricity consumer as a result of the increasing electricity production by traditional end consumer through their own photovoltaic systems [7, 8].

Basics and Preliminary Investigation

Definition of Asset Logging

To ensure a shared understanding, a clear definition of asset logging as a field of application is essential. According to our definition, asset logging comprises scenarios, in which data from registered assets is logged and stored for later or ongoing verification of certain propositions or processes. Thus, asset logging use cases generally consist of three primary steps: data collection, tamper-resistant data storage, and verification whether certain conditions, which were agreed upon ex-ante, are met on the basis of collected data.

Warranty management represents an exemplary use case. In order to assess in hindsight whether warranty conditions are met, the operation of relevant assets is continuously monitored. Asset data documenting its operation is periodically collected and stored in a tamper-resistant way. If a warrantee raises a warranty claim, the tamper-resistant data serves for assessment whether the asset has been operated according to conditions defined in the warranty agreement. If this is the case, the warranty claim is valid. As the data is only shared in the case of a warranty claim, business secrets of the warrantee are preserved. Due to tamper-resistant data storage, the warrantor can be certain that only genuinely valid warranty cases are confirmed, while the warrantee is assured that all warranty cases can be provably claimed on the basis of verifiable data.

Initial Research

Previous research has already identified asset logging as one of the most promising fields of application for a digital, potentially blockchain-based platform [9]. Inspired by this research, we conducted a close, systematic exchange via bilateral workshops with focus groups of interested, relevant partner companies from the energy sector. In these interactions, we recognized that various stakeholders with different roles in the energy sector are owning or operating a variety of often decentralized energy assets. On the one hand, we identified that existing challenges associated with a lack of digitalization in this field of application can be remedied by a fully automated platform solution. On the other hand, we determined that we can ensure tamper-resistance and data integrity in these cases through the usage of blockchain technology. Furthermore, use cases could be implemented that could previously not or only with difficulty be realized, as the handling of large numbers of both different assets and different stakeholders could be enabled through a platform with automated documentation and verification.

Potential Assessment

Building on our insights of the preceding project, we now took a more detailed and methodical look at the application field of asset logging, its relevant and suited use cases and requirements to realize such use cases. For a start, we identified the potential of asset logging use cases by estimating the number of eligible assets in Germany. For the numbers of today, we gathered status quo data, whereas for our estimation of 2030, we used political targets and projections. In line with [10], we found renewable generation plants as well as electricity consumption and storage units to be the most relevant groups of assets in this regard.

Figure 1 displays the resulting list and numbers of potential assets in the energy sector. As of today, already more than three million assets are potentially of relevance for use cases in the field of asset logging, where photovoltaic systems and heat pumps account for the largest numbers of assets. Within the next decade, we estimate that the number of relevant assets is likely to multiply, resulting in over 17 million potentially applicable assets for 2030. With more than half of the potential assets, battery electric vehicles are anticipated to be by far the most relevant group of assets for 2030, while photovoltaic systems continue to play a major role with a share of more than 20 %. As the number of assets potentially suitable for

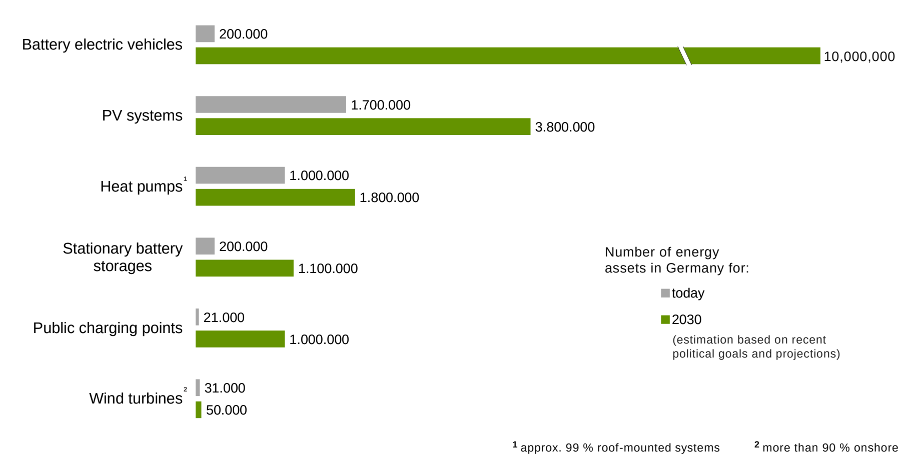

Figure 1 Estimation of the number of units in different fields that are relevant for asset logging, based on national policy goals, such as [11] for battery electric vehicles, and own calculations derived from simulations of the future energy system [12].

logging solutions will most likely grow significantly in the future, we expect asset logging to increasingly gain relevance. For further investigations of the real potential and motivation of the energy sector to implement such use cases and to test our technical solutions developed in this context, we must identify, discuss and rank potentially relevant use cases.

Use Case Analysis

In our current research, we set out to methodologically develop and select relevant use cases in the field of asset logging. For this purpose, we implemented a three-step process to identify, prioritize and select use cases, which should potentially be tested later in a sandbox approach. Our use case process allowed us to combine practical input from our partner companies of the energy sector and scientific expertise of the interdisciplinary project team in the fields of energy economics, computer science, and legal science.

Identification

To start with the identification and development of potentially relevant use cases, we conducted a total of eleven bilateral workshops with more than 70 expert participants from various business areas of the energy sector. Apart from public utility companies, partners from large energy providers, full-service providers, as well as from component manufacturers and both distribution network operators and transmission system operators were represented. In a first phase of the workshops, a total of 90 separate high-level discussions were hold on 32 different use cases, 16 of which we assign to the field of asset logging. In a second phase, most of the workshop time was devoted to in-depth interviews concerning the specific benefits and pitfalls of the use cases considered to be most relevant for each group of experts.

Resulting from these focused examinations, we identified twelve asset logging use cases to be of high relevance for both commercial application and scientific research in the fields of energy economics, computer science, and legal science. These use cases are characterized by high business potential, where an economic added value in the form of cost savings or additionally generated revenues through automation is frequently complemented by an added value in tamper resistance and privacy of the data. Additionally, it is precisely these high expectations on tamper-resistant processing and transfer of data for verification in combination with the prevailing demands for data privacy and data sovereignty that make the cases highly interesting from a scientific point of view. Finally, we clustered the identified twelve asset logging use cases based on their data requirements and created a comprehensive definition for each relevant use case, including user story, added value, required data, descriptions of the roles involved, and various representations of the process flow. An overview of the asset logging use cases as well as exemplary parts of the use case definitions are published in [10].

Prioritization

The second methodological step consists of combining several use case rankings that were developed after the workshops. We created a first ranking of the use cases based on the insights of the workshop series, taking the gained assessment over stakeholder benefits, technical requirements, customer potential and legal obstacles as perceived by the partner companies into account. Here, the frequency as well as the depth of detail and recognized relevance were converted into a numerical rating.

A second ranking was compiled by incorporating the view of all participating research institutes. To do so, all research partners provided an expert assessment of the use cases from a legal, technical and energy economics perspective. Again, we converted these assessments into a single numerical rating. Combining these two rankings, a conclusive ranking was created which thus reflects both the practice-oriented view of the partner companies and the research perspective of scientific experts. On the basis of this ranking, we concluded that eight of the previously identified asset logging use cases have a fundamentally high relevance across all perspectives.

Selection

In a third and final step, we selected those use cases best suited for actual implementation under real conditions. To be selected, a use case must meet two conditions: First, it must have both a high business potential and a high added value from a research perspective. This condition is represented by a high ranking in the conclusive ranking resulting from the prioritization step. Second, efforts arising from an initial implementation must be manageable, which implies easy access to asset data and voluntary participation of stakeholders. From the pool of identified asset logging use cases, four use cases meet these conditions [10]:

1) Service and maintenance models, where contractual agreements are verified through the tamper-resistant documentation of maintenance data
2) Warranty management, where a warranty claim is verified through the tamper-resistant documentation of asset data
3) Operation contracting, where the operation of an asset is outsourced and thus documented in a tamper-resistant manner to prevent conflicts between operator and owner

4) Regulatory requirements, where tamper-resistant asset data is transmitted for regulatory requirements such as verification or proof of provision.

These four use cases share similar data and infrastructure requirements, such that implementing one use case makes implementing the other use cases easier due to emerging synergies.

Requirements for Asset Logging in the Energy Sector

In the course of the use case process, we found that a shared set of requirements must be met for all relevant asset logging use cases. The requirements we identified can be classified in two groups. In group one, requirements for data measurement and collection are defined. The second group specifies requirements for the actual technical solution i. e. the platform architecture. Here, we outline the necessities for the storage, processing and further use of collected data on the platform.

Data Measurement and Collection Requirements

To ensure data integrity in asset logging, the entire chain of data processing must be tamper-resistant, which includes the step of data collection. Hence, tamper-resistant data collection must be technically possible, which means that manipulation of data during or immediately after measurement must be prevented on all accounts [3]. At the same time, the data must be clearly attributable to its origin, i. e. the corresponding asset, where the chronological sequence of the measurement must be transparent [3]. We refer to this set of requirements as traceability. In addition, the asset owner or operator must permit the tamper-resistant collection of asset data. In this regard, most asset owners demand data privacy and data sovereignty, especially since the data might contain sensitive business secrets.

In the case of warranty management, for instance, the following types of data must be collected: maintenance and operation schedule, maintenance and availability reports, and operational data. These different types of data are measured and collected by different means at different intervals, e. g., maintenance reports are compiled at the discrete time of reporting, whereas operational data is continuously collected by sensors in a fixed temporal resolution. Regardless of these differences, all data must be collected in a tamper-resistant, traceable manner and their further use must be permitted by the asset owner.

Architecture Requirements

As the collected data must be stored for later use or processing, requirements arise for the technical implementation of a suitable data platform. For asset logging, these architecture requirements are:

1) Ex-post verification of data integrity
2) Protection of business or trade secrets
3) Secure identification of participating stakeholders
4) Scalability of the platform.

As all relevant asset logging use cases involve some kind of data verification process, all data stored on and accessed from the platform must be both traceable and tamper-resistant to ensure data integrity. Similar to the requirements during data collection, a sufficient degree of data privacy is demanded to protect important business or trade secrets without impeding the verification process. Furthermore, all relevant stakeholders, which include public authorities in some cases, must be able to clearly identify themselves when accessing the platform. Finally, the platform must be designed in a way that guarantees scalability, i. e. that it can be easily expanded to additional use cases and participants, and at the same time ensure cost-effectiveness.

Technical Background

To provide a basic understanding of our proposed technical solution for asset logging that meets all requirements, we must first outline the relevant technological concepts of metering infrastructure, relevant aspects of blockchain technology, and Self-Sovereign Identity (SSI) in the following.

Tamper-resistant Metering Infrastructure

To guarantee data integrity along the entire data processing line, tamper resistance is a basic prerequisite right from the data collection stage. For this reason, the metering infrastructure directly at the asset must meet high data security and privacy standards for asset logging use cases. To discuss these requirements for metering, the smart metering infrastructure in Germany is considered as a relevant example, since its technological development is well advanced and comprehensive standards for secure data processing and transmission exist [13]. Other data collecting technology must meet the same criteria as defined in Use Case Assessment in the Energy Sector, for which no industrial standard as with smart meters has been defined yet.

The basic principle of smart metering infrastructure is to provide government-certified infrastructure for tamper resistance, privacy and traceability of the data collection process [13]. In this context, the smart meter provides tamper-resistant and traceable measurements of at least electrical energy, with meter readings at 15-minute-intervals, electricity feed-in (for electricity generating assets), and grid status (current, voltage and phase angle) [14]. These measurements can be forwarded through an encrypted Local Metrological Network (LMN) to the Smart Meter Gateway (SMGW), which can transmit meter data towards authorized stakeholders via an encrypted Wide Area Network (WAN) [15]. The smart meter rollout in the European Union follows respective guidelines [16]. Since implementation of the guideline is in the responsibility of the member states, progress on meters, infrastructure, and rollout differs within the member states of the European Union [17].

Blockchain Technology

A blockchain represents a particular type of distributed data structure that contains information grouped into blocks. Each node participating in the peer-to-peer network redundantly stores the data. Since each block refers to the previous block using a hash pointer, the data blocks are chronologically ordered and concatenated into a chain. Any modifications to data in the chain are detected, making the blockchain a tamper-resistant database [18, 19]. Upon creating a transaction, a user digitally signs their transaction using a private key. Prior to processing transactions, the nodes use the sender's public key to verify the transaction. Thus, a blockchain relies on public-private key cryptography to ensure the legitimacy of transactions.

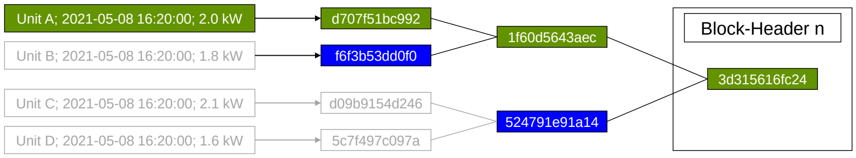
Unit A; 2021-05-08 16:20:00; 2.0 kW
Unit B; 2021-05-08 16:20:00; 1.8 kW
Unit C; 2021-05-08 16:20:00; 2.1 kW
Unit D; 2021-05-08 16:20:00; 1.6 kW
d707f51bc992
f6f3b53dd0f0
d09b9154d246
5c7f497c097a
1f60d5643aec
524791e91a14
Block-Header n
3d315616fc24

Figure 2 Merkle tree and Merkle proof.

When transactions are propagated on the network, nodes must agree on the state of the system, i. e., the integrity of the transactions and the correct order of the blocks. The mechanisms for reaching consensus are manifold and imply different benefits and drawbacks [20, 21, 22, 23]. Using consensus protocols eliminates the need for a central trusted party, which is seen as a core value of the technology [24]. After the network reaches consensus, each node adds this new block to its own copy of the blockchain [18]. Researchers and practitioners generally distinguish between the design parameters access restriction and reading/writing permissions [20]. The former addresses whether transactions are publicly visible or only visible to pre-defined parties. The latter design parameter defines whether participation in consensus and the validation of transactions is permissioned or permissionless.

The hash of a block is derived from the data stored in the block, e. g., transactions, a timestamp, or the difficulty. Transactions and their corresponding metadata are typically saved in a data structure using a Merkle tree. Merkle trees allow to efficiently aggregate arbitrarily transactions or data sets within one hash. Using a binary Merkle tree, data points are repeatedly hashed in pairs to form a final hash. This last represents a cryptographic commitment to all the underlying transactions or "leaves", also referred to as Merkle root. In addition, Merkle trees allow the integrity of a data point to be verified using only a subset of the hashed data points [25]. Against this backdrop, Merkle Proofs (MPs) are generated. MPs allow third parties to verify the integrity of a data point solely on the basis of a subset of hashed data and corresponding Merkle roots. As a result, this enables verification with low computational overhead compared to hashing all data points in a stream. In this case, a verifier would need the hashes of all data points to verify that a particular data point was included in the processing. The depth of a binary Merkle tree (and hence the computational and storage complexity of a MP) scales with $\log_2(N)$, or in a p-ary tree with $\log_p(N)$, where N represents the number of data entry points. In the case where every data point is individually hashed, the leghtn of the hash list scales with N. As pointed out above, verifiers require only a subset of hashes to verify the integrity of a data point when using MPs. This mechanism is illustrated in Figure 2. In order to create a referencing structure along blockchains, each block points towards the Merkle root of the transactions of the previous block.

In addition to storing plain data such as transactions, it is also possible to integrate business logic into the blockchain via the deployment of Smart Contracts (SCs). SCs are computer programs that execute predefined code when certain conditions are met [26, 27]. Generally, external information, i. e. a transaction to a SC, triggers the inherent functions. Thus, with the introduction of the Ethereum blockchain, decentralized applications and digital tokens could be implemented using SCs for the first time and enables the creation of new ecosystems [27]. In sum, researchers and practitioners acknowledge several important characteristics of the technology [18, 19, 21, 28, 29, 30]. First, by using cryptographic hash references, blockchains establish tamper-resistant data records [18]. Second, consensus mechanisms provide a single source of truth [29]. Third, its distributed manner and redundant data storage ensure a relatively high resistance against malicious attacks and crashes [21]. Fourth, MPs facilitate the verification of data integrity [25]. Fifth, SCs allow to implement arbitrary business logic on blockchains [27]. As a result, blockchains are considered as highly trusted, which is beneficial for critical infrastructures such as the energy sector [31, 32], and enable the implementation of other technologies.

Self-Sovereign Identity (SSI)

Our discussions in the bilateral workshops with stakeholders revealed that siloed and outdated data are frequent problems in the energy sector. Furthermore, the commonly used public key infrastructure is always relying on the communication with trusted third parties in order to verify the correctness of existing data [33]. To achieve authenticated and End-to-End (E2E) encrypted bilateral communication channels between certain parties, identities and their attributes remain indispensable – regardless of analog or digital information exchange [34]. Concerning the latter, the verifiability of credentials without physical interaction remains an issue. In addition, digital identities can mostly be duplicated indefinitely. A centralized identity management solution addresses these problems but may not leave the users in control of their own information [35, 36, 37]. Against this backdrop, concepts like SSI provide an architecture to leverage portable identities saved in a decentralized manner [38, 39]. It can best be described with an analogy from the real world: Everyone possesses a wallet which contains multiple plastic cards like a drivers licence or a personal ID card. In the context of SSI, this storage relates to the digital wallet, which can be represented by an app on the owner's smartphone [40]. The physical identification cards themselves only contain the relevant information for a certain context. Drivers licenses may include the name of drivers and the range of vehicles they are allowed to drive, but not their birthplace, as it is not important in a traffic control. The issuing authority, like the federal state, ensures the credibility, tamper-resistance and uniqueness of the document and makes its underlying schema publicly available. Therefore, third parties can verify its integrity without contacting the issuer. SSI provides a similar approach to physical ID cards by using Verifiable Credentials (VCs) [41, 37]. VCs contain identity data about their owner, which are digitally signed by trustworthy authorities using cryptographic techniques [42]. Usually they are stored in a dedicated digital wallet to which only the owner has access. In addition, the rise of agents provide a complementary solution by managing certain VCs without the need for the owner to be permanently available [43, 44]. Either way, credentials are generally not transferred directly to other parties: The owner generates Verifiable Presentations (VPs) of one or more VCs, respectively a subset of their properties, to present tamper-resistant evidence to a verifying party [45, 42]. VCs are not limited to information itself but include possibilities to also provide statements, e.g., whether a person is a resident of a certain city. The underlying cryptographic techniques include amongst others Zero-Knowledge Proofs (ZKPs). ZKPs solely guarantee the validity of a statement and do not disclose any additional information, thereby preserving privacy [46].

With the absence of physical interaction and the need for secure data transmission, SSI assigns unique identifiers, Decentralized Identifiers (DIDs), to all participating parties leading to E2E encrypted message channels. DIDs must hence be created decentrally and should be renewed for every interaction, especially when natural persons are participating, to ensure that correlations are impossible. A standard format developed by the W3C defines three mandatory components of a DID [47]: The first part contains the underlying URI-schema followed by the DID method which specifies the chosen DLT and how operations shall be executed. The third block completes the DID by providing a method-specific identifier. A given DID resolves to a linked DID document consisting of related information like cryptographic details.

However, in order to a achieve a fully integrated system, further infrastructural components are necessary. To verify the integrity of VPs, information about their underlying schema and their issuers is essential. In addition, credentials can be revoked at any given time by the original issuer. Therefore a registry must be established to verify that a VC is valid. Using such a public yet privacy-ensuring registry in combination with the verification of the issuer's digital signature, holders can prove that a VC is not revoked without contacting the issuer. Against this background, the blockchain is considered perfectly suited for an unbiased registry. Due to its decentralized, high available and tamper-resistant nature, blockchain can thus perfectly facilitate the convergence to other technologies such as SSI, releasing synergies created by the combination of both [43, 48].

Platform Architecture for Asset Logging

We propose a decentralized blockchain-based approach for the architecture of our platform. This could impede monopolization and increase stakeholder acceptance through direct participation. Since there are no alternative centralized approaches to the best of our knowledge, a comparison in this regard has yet to be made [9].

Architecture Development

In order to easily verify data integrity, it is reasonable to first write plaintext data to the blockchain. However, storing plaintext data on the blockchain raises privacy concerns and thus may violate data protection requirements. To reconcile data verifiability and privacy, hashes of data are therefore stored on the blockchain. In addition, scalability is critical to save data efficiently on the blockchain. Given these requirements, MPs offer a suitable solution to achieve this goal.

Limitations of Existing Blockchain-based Approaches

On the basis of our derived requirements, we propose an approach building on four essential components: Tamper-resistant data logging through certified components (e. g., sensors), digital signatures as well as the authenticated and E2E encrypted bilateral data exchange via SSI, blockchain technology, and Merkle trees. Overall, our architecture involves interactions of two players. Generally, asset owners take the role of provers while any other stakeholder might represent a verifier. In a typical use case, asset owners or operators aim to prove that their asset data is reliable – i. e., authentic at the time of generation, and unchanged since. Verifiers check ex-post that the data is trustworthy with high reliability. As data is shared in cases of disputes, provers might have conflicts of interest, which may spur manipulations. Against this backdrop, verifiers are interested in tamper-resistant data storage.

A simple and frequently suggested solution to achieve this goal would run blockchain clients on assets to directly push the data that they generated onto a distributed ledger. Due to a blockchain's familiar characteristics of tamper-resistance and practical immutability, this would ensure a high level of trust and availability of data to third parties when they request it later; in fact, verifiers could directly query the relevant data from their own blockchain node or request it from a node that they trust. However, when following this approach, we would encounter two significant problems. On the one hand, data privacy is not guaranteed as any blockchain node would be able to access the data under consideration. This challenge could be solved by hashing the written data and providing plain-text data to third parties off-chain through a bilateral communication channel. Yet, on the other hand, we would encounter large scalability issues. Storing data on public blockchains such as Ethereum is typically highly expensive and only feasible to a very limited amount in the order of a few kilobytes per second[1]. In addition, the performance of permissioned blockchains is also limited to a few hundred up to a few thousand transactions per second [50]. Even if optimizing for upload capacity, a medium-sized Hyperledger Fabric network, which is a popular permissioned blockchain and one of the enterprise blockchains with the highest performance in a larger comparison [50], cannot upload more than 15 MB/s of data even with solid hardware [51]. Taking into account that millions of assets in the energy sector are potentially relevant and a high temporal granularity would require each of them to send a sensor date every few minutes, this exceeds the capacity of permissionless blockchains by orders of magnitude and even the capacity of dedicated permissioned networks. In addition, the redundant storage of these amounts of data are expensive and waste storage resources. Thus, solely registering asset data in plain text or in hashed form on distributed ledgers does not fulfill the requirements set out in Use Case Assessment in the Energy Sector.

Proposed Architecture

Against this backdrop, our architecture builds on hierarchical aggregation of data in the form of Merkle trees. The entire architecture is depicted in Figure 3. Accordingly, we propose that data logging modules of assets make use of their private keys to sign their generated data. We propose so as signatures allow to ensure authenticity of logged data. In specific, a third party can verify whether the provided data actually

[1] On the Ethereum blockchain, a single block typically contains around 50 kB of data, and the average block time is around 13 s. An operation for only storing data in a SC consumes 20,000 gas, which is required for the network's computational work. Thus, the theoretical maximum for a simple storing operation would be 50 transactions per second (or 650 transactions per block). At present, the empirical mean is 15 transactions per second on Ethereum, driven by more complex computations and consequently requiring larger amounts of gas [49].

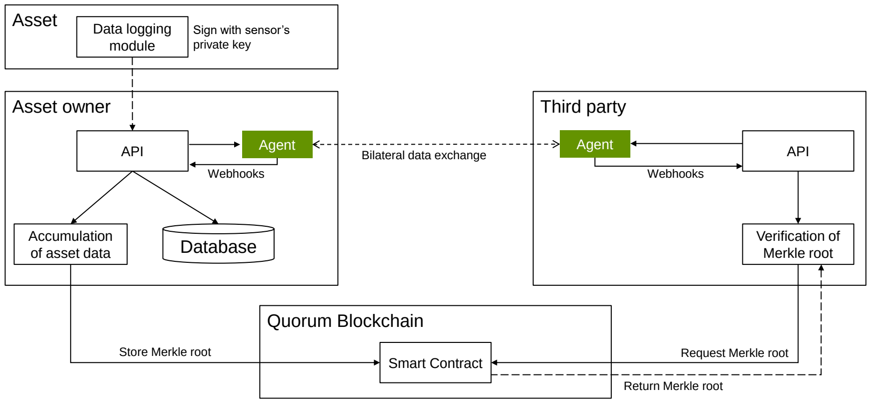

Figure 3 Asset logging architecture.

stems from the asset referred to. In case data remains unsigned, verifiers have no means to ensure whether the data was generated by an asset under contract or any other asset. Thus, no matter which processing mechanisms are applied, digital signatures should always be used to ensure data authenticity.

The entire process of the asset logging's business logic is illustrated in the sequence diagram in Figure 4. After signing the logged data for a certain epoch (e.g., every 15 minutes), assets send the data to their owner (or an aggregation service provider) using a bilateral, E2E-encrypted communication channel. Subsequently to receiving the signed data, owners aggregate the received data into a binary Merkle tree. Consructing a Merkle tree involves the subsequent hashing of signed transaction data. As a result, asset owners generate a Merkle root that consists of the asset's logged data as displayed in Figure 2. Asset owners run a blockchain client that sends the Merkle root to a specific SC address, which in turn includes the Merkle root in a batch, writing a new block to the blockchain. Thus, the Merkle root stored on the blockchain represents a digital fingerprint of the logged asset data for a distinct epoch.

In addition, asset owners locally save the asset's logged data in plain text, the full Merkle tree, including its root and the block number. The block number is included in the SC transaction receipt when the block is stored on the blockchain. Against this backdrop, owners can provide third parties with relevant signed plain text data upon request over a bilateral E2E encrypted communication channel. After receiving the relevant plain-text data, third parties can request a MP to verify that the logged data has not been changed in the meantime. Based on the Merkle tree, asset owners generate a MP on demand (e. g., by a third party) containing the path to the corresponding root of the Merkle tree, which requires only a minimum number of hashes and configuration information. Then, third parties can first verify digital signatures using the public keys from corresponding DID documents. Second, using the MP it can be verified whether the data provided by the asset owner represents a valid input to the corresponding root. Third, verifiers check whether the MP is based on the same Merkle root as saved on the blockchain (see Figure 4). Based on this information, the third party can verify the integrity of the data.

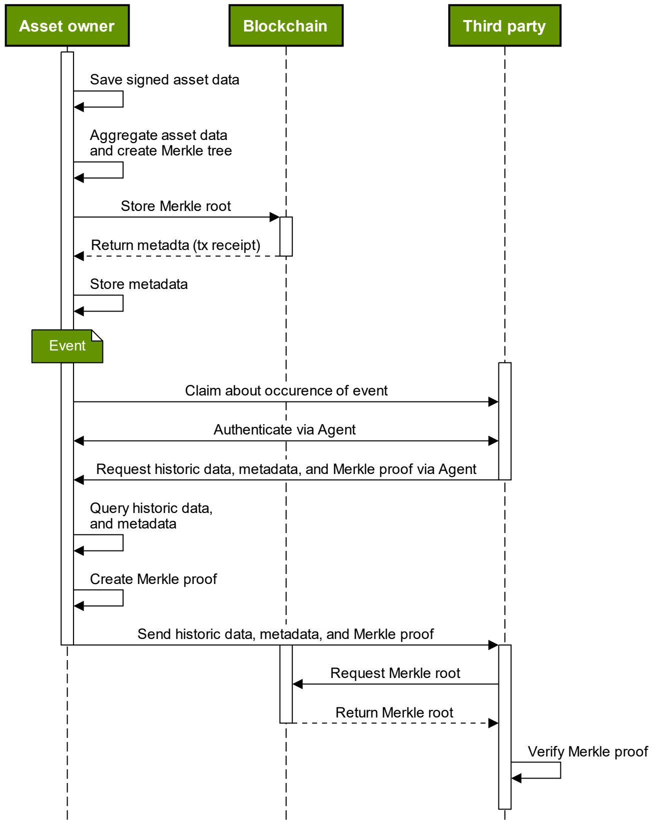

Figure 4 Sequence diagram.

Requirements-based Evaluation

The proposed approach bears three central advantages. First, by compressing large batches of data at once, MPs represent a scalable solution. With an arbitrary amount of data points, the size of Merkle roots remains at fixed size (e.g. 256 bits when relying on SHA256). Thus, no matter how many data points are used as an input, on-chain transaction data remains at a predetermined size. Second, as verifiers require only a subset of encrypted records, verification of the Merkle tree scales (both the computational complexity for the verifier and the amount of communication that is necessary between the prover and the verifier) with $\log_2(N)$. Third, in contrast to unordered batching of data points, MPs enable privacy by default. This is as verifying the integrity of MPs requires only surrounding hashes of the respective data input (see also Figure 2). Thus, no additional data points must be revealed. In contrast, while unstructured batching of data to a single hash also is considered a scalable solution, it requires revealing all other inputs to verify the integrity of the resulting hash. Third, due to high entropy, Merkle roots also do not allow to trace back to the input data (as do single hashes). Hence, resistance to preimage attacks can be considered high [25].

As a result, by storing only Merkle roots on a blockchain that are associated with a large number of sensor values (from multiple sensors or multiple epochs), privacy risk and scalability issues are minimized. Thus, our approach can be considered scalable and privacy-preserving and does not reveal any trade and business secrets or personal data. Notably, the blockchain does not guarantee that the original data, hence the logged data by an asset, has been altered by the owner or the operator in the first place. However, the energy sector provides certified infrastructures, such that we may rely on trusted data logging devices (see Tamper-resistant Metering Infrastructure). Combining a blockchain-based approach, digital signatures at the point of trusted data creation and resource-friendly verification mechanisms allow to verify whether an alteration has taken place. Furthermore, our approach allows for a public, permissionless blockchain as it serves for tamper-resistant storage of Merkle roots only. The transactions themselves do not reveal any information without bilateral exchange of plain-text data from asset owners. We propose an open platform, which any stakeholder can access at any time and is private by design. As a result, our platform is not limited to an underlying use case but can be extended to further use cases and even domains in future.

Challenges for Practical Implementation

The focus of designing our blockchain-based platform for asset logging use cases is not only on its academic contribution but also to be practically implemented and tested. During planning and implementing our field trials, we already encountered various challenges, gained first experiences in trial preparation, and collected feedback on the side of stakeholders such as commercial energy asset operators, energy service providers, or network operators.

Prevailing Challenges and Limitations

Some of the identified challenges can be bypassed or eliminated before long, others pose clear limitations in the field of asset logging.

Digitalization and Infrastructure

To date, data collection and in particular data transfer and processing in Germany's energy sector often remain a manual task [5]. Therefore, the lack of digital infrastructure remains a severe impediment to the implementation of digital use cases such as asset logging. In some instances, asset data is even recorded analogously by employees and digitalized in a subsequent step only. Furthermore, numerous assets are not yet equipped with any measurement devices or sensors, which poses a major obstacle to the implementation of any digital use cases. In this respect, our solution for asset logging use cases can serve as an additional motivation for the involved stakeholders to digitalize, although this digitalization must take place before the platform can be implemented on a large scale.

In particular, the German SMGW rollout, which would provide a convenient way of tamper-resistant, privacy-ensuring data collection, proceeds slowly. Due to currently unresolved legal concerns, it is unclear when SMGWs will be wide-spread operational in Germany [52]. In contrast, similar infrastructure is already available in other countries. Yet, the slow rollout in Germany can be bypassed by using suitable measurement equipment that can communicate in an E2E encrypted way with an SSL-certified server. Such suitable measurement equipment could in some cases also be applied to collect other types of necessary data, which cannot be collected with a SMGW. Other metering solutions must, however, not only guarantee the tamper resistance of the meter, but also that the meter is connected to the correct data generating process.

Regulation

Another potentially limiting factor for swift large-scale implementation represents the mandatory involvement of public authorities or regulators in some of the most promising asset logging use cases, such as the German grid regulator in the case of the verification of balancing services[9]. The digital transformation of regulatory processes and the necessary detailed review of compliance with regulatory guidelines requires a great deal of time and effort and involved authorities must first appreciate the added value of the platform before the use cases can be implemented in practise.

To implement the proposed digital use cases, these authorities must recognize the blockchain-based proof of data integrity in their guidelines and must be able to perform the necessary verification based on the provided data and MPs.

Governance

Furthermore, questions about blockchain governance prevail. This applies to both blockchain used for SSI as well as the blockchain infrastructure used for the storage of Merkle roots. Following [53], stakeholders should agree on the dimensions decision rights, accountability, and incentive structures. For example, the operation of nodes might not be efficient or feasible for small-scale stakeholders. However, asset owners will still need reading and writing access. In contrast, economic benefits caused by a high reliability of underlying data might serve as a sufficient incentive for larger players to operate nodes themselves. Further design choices can be configured in dependence of stakeholders' interests. In general, there are various design choices of how to process Merkle trees and store them on the blockchain. Moreover, also alternative design choices with regards to the creation of Merkle trees need to be considered. For example, larger sizes of data can be commited by recursively creating Merkle trees. Nevertheless, the increase in commitment sizes comes with downsides regarding the efficiency and privacy of verification. Thus, before transforming our prototype to a productive solution, further governance- and design-related questions should be considered. Advantages and drawbacks should be carefully balanced off. In general, computations should be performed solely off-chain while blockchains are used for tamper-resistant documentation purposes only.

User Acceptance

Lastly, for successful adoption of emergent technologies, user acceptance studies are crucial [54]. This is especially so as the underlying context involves various different stakeholder groups. Thus, in order to sucessfully implement the proposed solution, stakeholders will need to be informed about the processing and mechansims of the above-mentioned architecture. For example, workshop series and on-site trainings allow to showcase the inner workings of systems and the adherence to requirements which was previously shown to be particularly important for acceptance [55].

Use Case Field Trials: A Sandbox Approach

To test our platform under realistic conditions despite the existing challenges, most of which are beyond our control, we pursue a regulatory sandbox approach. The term describes trans-disciplinary field trials of innovative solutions without necessarily complying with existing regulations, which becomes possible through the mutual consent of contractual experimentation clauses. Through this approach, we especially circumvent legal restrictions and the issues of data collection in particular, while nonetheless demonstrating the full, unobstructed technical functionality of the platform architecture. Nevertheless, we address the typical regulatory and technical challenges corresponding to the usage of blockchain technology, namely data protection [56] and scalability [50], by design to make sure that the solution is ready to be implemented on large-scale and in production as soon as the external dependencies have been cleared.

Resulting from the series of workshops with our company partners (see Use Case Assessment in the Energy Sector), we found that the motivation of relevant stakeholders involved to actively contribute to the realization of the use case beyond mere participation is essential for a successful field trial. After consulting with our partner companies in bilateral meetings, we decided on two motivated partners and correspondingly on two out of the previously identified four most relevant use cases, which are about to be implemented in the field trials:

- Warranty management – tamper-resistant asset logging for the verification of warranty claims
- Regulatory requirements – tamper-resistant asset logging for the verification of the provision of requested balancing services

For both use cases, we will create a sandbox environment that is as close to real conditions as possible. For data collection, we plan to newly install appropriate sensors and, if no alternative is available, to use synthesized asset data. To operate the actual platform, all assets will be equipped with Raspberry Pis including LTE modules to host respective agents used for certification and communication purposes. On this basis, assets and stakeholders can use certificates to prove their identities. Besides a cloud-hosted Hyperledger Indy network for SSI-based interactions (see Technical Background), we will also need a cloud-based blockchain network for storing the generated Merkle trees. While any network can be used for the latter purpose, we suggest relying on a public, permissionless network to lever the platform's characteristics of openness and availability. At this stage, we are in the process of preparing the field trials, and hope to present further results on the insights, challenges, and opportunities associated with the implementation of our use cases in the near future.

Conclusion and Outlook

Our research in the field of asset logging in the energy sector highlighted that many use cases offer both business relevance and scientific significance. With regards to the identified use cases and associated requirements, we draw the following conclusions: First, the future market potential for asset logging is high due to an already significant, but also expected increase in the number of relevant energy assets. Second, the prospects of cost reduction and improved data protection represent the main drivers for stakeholders involved in the field of asset logging. Third, the applied methodical process of exchange with partner companies allowed us to identify eight asset logging use cases as highly relevant in the energy sector both from a business and a research perspective. Regarding the technical solution for realizing most asset logging use cases, we found that they must enable an ex-post verification of data integrity, while simultaneously protecting relevant business secrets and allowing for scalability. Furthermore, since most use cases require different types of data, a key challenge represents the collection of signed data that is tamper-resistant from the moment it is generated. Last, the lack of digitalization in the energy sector poses a considerable obstacle to swift implementation.

We presented a platform architecture as a suitable technical solution for implementing asset logging use cases. Any asset that can provide signed data can in principle be connected to the platform, which therefore enables the implementation of a range of use cases. The interplay of blockchain, Merkle proofs and E2E-encrypted communication channels guarantees traceability, data integrity and privacy for all participating stakeholders. Finally, the architecture is designed for cost-effective implementation and scaling, i. e. it is extendable to other use cases and stakeholders.

We selected two use cases – namely warranty management and regulatory requirements – to be implemented in a sandbox approach. These field trials are intended to demonstrate the functionality and acceptability of the solution to pave the way for an implementation of asset logging use cases at larger scale in future. This is especially so, if we succeed in demonstrating the added value to relevant stakeholders including public authorities and regulators. This will allow to increase participation in and wide-spread acceptance of our solution. To achieve this objective, complementing the SMGW infrastructure with tamper-resistant data collection processes for other types of data represents the key necessity to be addressed in the near future. Furthermore, our research highlights the importance of the wide-spread roll-out of reliable and certified data measurement infrastructures such as SMGWs. Regarding future research opportunities, we propose a detailed analysis of market potential, feedback effects on the energy system and synergies in terms of use cases and collected data. Furthermore, future research should address how the proposed data infrastructure can be used for the processing of additional business logic. For example, our proposed architecture can build the foundation for processing subsequent warranty conditions. Also, as the proposed infrastructure enables verifiable data integrity, previously proposed use cases for further data processing and disbursement such as suggested in [57] become feasible.

Acronyms

DID Decentralized Identifier. 10, 12

E2E End-to-End. 9, 10, 12, 14, 17

LMN Local Metrological Network. 7

MP Merkle Proof. 8, 9, 10, 12, 13, 15

SC Smart Contract. 8, 9, 11, 12
SMGW Smart Meter Gateway. 7, 14, 15, 17
SSI Self-Sovereign Identity. 7, 9, 10, 11, 15

VC Verifiable Credential. 9, 10
VP Verifiable Presentation. 9, 10

WAN Wide Area Network. 7

ZKP Zero-Knowledge Proof. 10

Acknowledgements
We thank Nicolas Ruhland for his help with implementing the network of aries-cloudagents, as well as Anna Walter and Marvin Ehaus for their help with bringing the implementation to a productive environment. We would also like to thank Nils Urbach and Jens Strüker for their scientific guidance and our research partner Stiftung Umweltenergierecht as well as our partner companies Bayernwerk, BayWa r.e., E-Werk Schweiger, innogy/E.ON, Lechwerke, RheinEnergie, SMA, Stadtwerke Bad Tölz, Stadtwerke Dachau, Thüga, TransnetBW and VWEW for supporting the project.

Funding
The project InDEED is funded by the Federal Ministry for Economic Affairs and Energy (BMWi) based on a resolution of the German Bundestag (funding code: 03E16026A).

Availability of data and materials
There is no additional data and materials.

Author's contributions
Removed for double-blind review.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]FfE, Am Blütenanger 71, 80995 München, GER. [2]Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Wittelsbacherring 10, 95447 Bayreuth, GER. [3]Research Center Finance & Information Management, Universitätsstraße 12, 86159 Augsburg, GER. [4]University of Bayreuth, Universitätsstraße 30, 95447 Bayreuth, GER. [5]University of Augsburg, Universitätsstraße 2, 86159 Augsburg, GER.

References

1. Zeiselmair, A., Hinterstocker, M., Bogensperger, A., von Roon, S.: Asset Logging – Transparent Documentation of Asset Data Using a Decentralized Platform. In: 8th DACH Conference on Energy Informatics, Salzburg (2019)
2. BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.: Digital@EVU 2020: Unternehmen planen höhere Investitionen in Digitalisierung (2020). https://www.bdew.de/service/publikationen/digitalevu-2020-unternehmen-planen-hoehere-investitionen-in-digitalisierung/ Accessed 2021-05-07
3. Albrecht, S., Reichert, S., Schmid, J., Strüker, J., Neumann, D., Fridgen, G.: Dynamics of Blockchain Implementation - A Case Study From The Energy Sector. In: Proceedings of the 51st Hawaii International Conference on System Sciences, pp. 3527–3536 (2018)
4. Carminati, B., Ferrari, E., Rondanini, C.: Blockchain as a Platform for Secure Inter-Organizational Business Processes. 4th International Conference on Collaboration and Internet Computing (2018)
5. Bundesministeriums für Wirtschaft und Energie (BMWi): Digitalisierung der Wirtschaft in Deutschland – Langfassung eines Ergebnispapiers im Projekt "Entwicklung und Messung der Digitalisierung der Wirtschaft am Standort Deutschland". In: Digitalisierungsindex 2020 (2020)
6. Balzer, G., Schorn, C.: Asset Management Für Infrastrukturanlagen – Energie und Wasser, 2nd edn. VDI-Buch. Springer Vieweg, Berlin/Heidelberg (2014)
7. Kotler, P.: The Prosumer Movement. In: Prosumer Revisited, pp. 51–60. Verlag für Sozialwissenschaften, Wiesbaden (2010)
8. Toffler, A.: The Third Wave. William Morrow, New York (1980)
9. Bogensperger, A., Zeiselmair, A., Hinterstocker, M., Dufter, C.: Blockchain – Chances for the Transformation of our Energy System, Report Section: Use Cases, FfE, Munich (2018)
10. Hinterstocker, M., Dossow, P., Djamali, A., Zeiselmair, A., Bogensperger, A., von Roon, S.: Blockchain Technology as an Enabler for Decentralization in the Energy System. In: 10th Solar & Storage Integration Workshop, Darmstadt (2020)
11. Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU): Förderung der Elektromobilität durch die Bundesregierung (2020). https://www.bmu.de/themen/luft-laerm-verkehr/verkehr/elektromobilitaet/foerderung/ Accessed 2021-05-07
12. Fattler, S., Conrad, J., Regett, A., Böing, F.: Dynamic and Intersectoral Evaluation of Measures for a Cost-Efficient Decarbonisation of the Energy System: Final Report of the Project Dynamis, FfE, Munich (2019)
13. Bundesamt für Sicherheit in der Informationstechnik (BSI): Das Smart-Meter-Gateway, Bonn (2018). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf;jsessionid=2B8E6EA51425F1392177F452127901EA.internet081?__blob=publicationFile&v=1 Accessed 2021-05-07
14. Bundesregierung: Gesetz zur Digitalisierung der Energiewende, Berlin (2016). https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetz-zur-digitalisierung-der-energiewende.pdf?__blob=publicationFile&v=4 Accessed 2021-05-07
15. Bundesamt für Sicherheit und Informationstechnik: Technische Richtlinie BSI TR-03109-1 – Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems (2013). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.pdf?__blob=publicationFile&v=1 Accessed 2021-05-07
16. Europäische Union: Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates – über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG (2009). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:de:PDF Accessed 2021-05-07
17. Alaton, C., Tounquet, F.: Benchmarking Smart Metering Deployment in the EU-28 (2020). https://op.europa.eu/o/opportal-service/download-handler?identifier=b397ef73-698f-11ea-b735-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part= Accessed 2021-05-07
18. Beck, R., Czepluch, J.S., Lollike, N., Malone, S.: Blockchain — The Gateway to Trustfree Cryptographic Transactions. In: 24th European Conference on Information Systems (2016)
19. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Business & Information Systems Engineering **59**(3), 183–187 (2017)
20. Wüst, K., Gervais, A.: Do You Need a Blockchain? In: Crypto Valley Conference on Blockchain Technology, pp. 45–54 (2018). IEEE
21. Zhang, R., Xue, R., Liu, L.: Security and Privacy on Blockchain. ACM Computing Surveys **52**(3), 1–34 (2019)
22. Kannengießer, N., Lins, S., Dehling, T., Sunyaev, A.: Trade-offs between Distributed Ledger Technology Characteristics. ACM Computing Surveys **53**(2), 1–37 (2020)
23. Sedlmeir, J., Buhl, H.U., Fridgen, G., Keller, R.: The Energy Consumption of Blockchain Technology: Beyond Myth. Business & Information Systems Engineering **62**(6), 599–608 (2020)
24. Fridgen, G., Radszuwill, S., Urbach, N., Utz, L.: Cross-organizational Workflow Management using Blockchain Technology – Towards Applicability, Auditability, and Automation. In: Proceedings of the 51st Hawaii International Conference on System Sciences, pp. 3507–3517 (2018)
25. Merkle, R.C.: A Digital Signature Based on a Conventional Encryption Function. In: Conference on the Theory and Application of Cryptographic Techniques, pp. 369–378 (1987). Springer

26. Szabo, N.: Formalizing and Securing Relationships on Public Networks. First Monday **2**(9) (1997)
27. Buterin, V., et al.: A Next-Generation Smart Contract and Decentralized Application Platform (2014). https://github.com/ethereum/wiki/wiki/White-Paper Accessed 2021-05-07
28. Butijn, B.-J., Tamburri, D.A., Heuvel, W.-J.v.d.: Blockchains: A Systematic Multivocal Literature Review. ACM Computing Surveys **53**(3), 1–37 (2020)
29. Xiao, Y., Zhang, N., Lou, W., Hou, Y.T.: A Survey of Distributed Consensus Protocols for Blockchain Networks. IEEE Communications Surveys Tutorials **22**(2), 1432–1465 (2020)
30. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., Gervais, A.: SoK: Layer-two Blockchain Protocols. In: International Conference on Financial Cryptography and Data Security, pp. 201–226 (2020). Springer
31. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A.: Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities. Renewable and Sustainable Energy Reviews **100**, 143–174 (2019)
32. Bao, J., He, D., Luo, M., Choo, K.R.: A Survey of Blockchain Applications in the Energy Sector. IEEE Systems Journal (2020)
33. Zhu, X., Badr, Y.: A Survey on BlockchainbBased Identity Management Systems for the Internet of Things. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1568–1573 (2018)
34. Bernal Bernabe, J., Canovas, J.L., Hernandez-Ramos, J.L., Torres Moreno, R., Skarmeta, A.: Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access **7**, 164908–164940 (2019)
35. Der, U., Jähnichen, S., Sürmeli, J.: Self-Sovereign Identity – Opportunities and Challenges for the Digital Revolution (2017). http://arxiv.org/abs/1712.01767 Accessed 2021-05-07
36. Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K., Raymond Choo, K.-K.: Blockchain-based Identity Management Systems: A Review. Journal of Network and Computer Applications **166** (2020)
37. Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C.: A Survey on Essential Components of a Self-sovereign Identity. Computer Science Review **30**, 80–86 (2018)
38. Allen, C.: The Path to Self-sovereign Identity (2016). http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html Accessed 2021-05-07
39. Wang, F., De Filippi, P.: Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain **2**, 28 (2020)
40. Hong, S., Kim, H.: VaultPoint: A Blockchain-based SSI Model that Complies with OAuth 2.0. Electronics **9**(8) (2020)
41. Avellaneda, O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K.H., Maler, E., Reed, D., Sporny, M.: Decentralized Identity: Where Did it Come From and Where is it Going? IEEE Communications Standards Magazine **3**(4), 10–13 (2019)
42. Sporny, M., Longley, D., Chadwick, D.: Verifiable Credentials Data Model 1.0. W3C (2019). https://www.w3.org/TR/vc-data-model/ Accessed 2021-05-07
43. Ferdous, M.S., Chowdhury, F., Alassafi, M.O.: In Search of Self-sovereign Identity Leveraging Blockchain Technology. IEEE Access **7**, 103059–103079 (2019)
44. Nauta, J., Joosten, R.: Self-Sovereign Identity: A Comparison of IRMA and Sovrin (2019). https://www.researchgate.net/profile/Rieks-Joosten/publication/334458262_Self-Sovereign_Identity_A_Comparison_of_IRMA_and_Sovrin/links/5d2c1ea092851cf44085008d/Self-Sovereign-Identity-A-Comparison-of-IRMA-and-Sovrin.pdf Accessed 2021-05-07
45. Preukschat, A., Reed, D.: Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials MEAP. Manning, Shelter Island, NY (2019)
46. Goldwasser, S., Micali, S., Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing **18**(1), 186–208 (1989)
47. Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., Holt, J.: Decentralized Identifiers (DIDs) v1.0. W3C (2020). https://w3c.github.io/did-core/ Accessed 2021-05-07
48. van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., Zarin, N.: Self-sovereign Identity Solutions: The Necessity of Blockchain Technology (2019). http://arxiv.org/abs/1904.12816 Accessed 2021-05-07
49. Etherscan: The Ethereum Blockchain Explorer (2021). https:/etherscan.io/ Accessed 2021-05-07
50. Sedlmeir, J., Ross, P., Luckow, A., Lockl, J., Miehle, D., Fridgen, G.: The DLPS: A Framework for Benchmarking Blockchains. In: Proceedings of the 54th Hawaii International Conference on System Sciences, pp. 6855–6864 (2021)
51. Guggenberger, T., Sedlmeir, J., Fridgen, G., Luckow, A.: An In-Depth Performance Analysis of Hyperledger Fabric (2021). https://arxiv.org/pdf/2102.07731.pdf Accessed 2021-05-07
52. Oberverwaltungsgericht Münster: OVG NRW: Einbaupflicht für vernetzte Stromzähler (Smart Meter Gateway/SMGW) einstweilen gestoppt. In: VG NRW, Beschluss vom 04.03.2021, Az. 21 B 1162/20 (2021)
53. Beck, R., Müller-Bloch, C., King, J.L.: Governance in the Blockchain Economy: A Framework And Research Agenda. Journal of the Association for Information Systems **19**(10) (2018)
54. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 425–478 (2003)
55. Ostern, N.: Do You Trust a Trust-free Transaction? Toward a Trust Framework Model For Blockchain Technology. In: 39th International Conference on Information Systems, pp. 1–17 (2018)
56. Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., Urbach, N.: Building a Blockchain Application that Complies with the EU General Data Protection Regulation. MIS Quarterly Executive **18**(4), 263–279 (2019)
57. Mohanta, B.K., Panda, S.S., Jena, D.: An Overview of Smart Contract and Use Cases in Blockchain Technology. In: 9th International Conference on Computing, Communication and Networking Technologies, pp. 1–4 (2018). IEEE