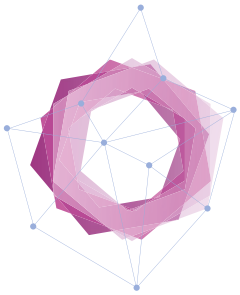
dena
German Energy Agency



Future Energy
Lab

REPORT – EXECUTIVE SUMMARY

Digital Machine Identities as a Building Block for an Automated Energy System

Development of an Identity Registry Based on the Blockchain Technology (Pilot: Blockchain Machine Identity Ledger)

Legal information

Publisher:
Deutsche Energy-Agentur GmbH (dena)
German Energy Agency
Chauseestrasse 128a
10115 Berlin, Germany

Tel.: +49 (0)30 66 777-0
Fax: +49 (0)30 66 777-699

E-Mail: futureenergylab@dena.de

Internet:
www.dena.de
future-energy-lab.de

Authors (all dena):
Sara Mamel, Project Leader
Linda Babilon
Philipp Richard
Moritz Schlösser
Fabian Seiter

Scientific experts:
Matthias Babel, Fraunhofer FIT
Johannes Sedlmeir, Fraunhofer FIT
Prof. Dr. Jens Strüker, Fraunhofer FIT
Christian Wiethe, Fraunhofer FIT
Dr. Marius Buchmann, Jacobs University Bremen
Richard Hänsel, EY Law
Dr. Ing. Sven Rosinger, OFFIS

Conception & design:
die wegmeister GmbH

Last updated:
June 2022

Please cite this publication as follows:
Deutsche Energie-Agentur (Publisher) (dena, 2022) "Digital Machine Identities as a Building Block for an Automated Energy System. Development of an Identity Registry Based on the Blockchain Technology (Pilot: Blockchain Machine Identity Ledger) - Executive Summary"

Federal Ministry
for Economic Affairs
and Climate Action

This publication is issued on behalf of the Federal Ministry for Economic Affairs and Climate Action. The German Energy Agency (dena) assists the Federal Government in various projects to implement the energy and climate targets in the context of the energy transition.

Table of contents

1.	**Digitalisation of the energy industry – opportunities and challenges**	**6**
2.	**The digital gap in the energy industry – from blockchain, SSI and machine identities**	**8**
3.	**Project structure and pilot concept**	**11**
3.1	The partner group	11
3.2	The project objectives	12
3.3	The synergy potential of digital identities and blockchain technology	13
3.4	The three options for plant connection	15
4.	**Summary and recommendations for action**	**16**
4.1	Technical evaluation	16
4.2	Economic evaluation	17
4.3	Regulatory evaluation	18
4.4	Outlook	18
5.	**List of abbreviations**	**19**
6.	**List of figures**	**20**
7.	**List of references**	**21**

Preface

The current decade is decisive for the energy transition: for Germany to achieve its national climate targets - a 65 per cent reduction in greenhouse gases by 2030 compared to 1990 - an enormous effort is required.

It stands to reason that a successful energy transition must also be a digital energy transition. Otherwise, the simultaneous control of a large number of distributed energy resources, together with the integration of countless prosumers into the energy system and, finally, the realisation of a genuine, near real-time energy economy are inconceivable.

Using the Smart-Meter-Gateway (central communication unit of the German energy system [1]) and blockchain technology, the German Energy Agency (dena) initiated the pilot project "Blockchain Machine Identity Ledger" (BMIL) that aimed to fill an important gap toward implementing a near real-time energy economy: namely, the lack of digital identities for energy plants. Like their analogue counterparts, digital identities allow for the unique identification of a person or machine — the difference is that they can be verified and deployed automatically. Equipping every plant in the energy system with a digital identity is an important milestone, without which a scalable, secure and protected digitalization of the overall system is not possible.

However, the project demonstrates that a digital energy transition involves more than just the establishment of sufficient digital metering infrastructure: It is about coordinating and controlling many decentralized plants and market stakeholders of the future. It is about how to provide and access system services automatically; how electricity, heating, transport and industrial sectors will be effectively and efficiently coupled with one another; and finally it is about how a sufficient level of data security and data protection will be ensured. In short, like with any new approach, the issue of data governance (i.e.: the framework for a fair and at the same time competitive data exchange) as well as the need to look at the entire digital value chain — from data collection and transmission infrastructure to data analysis — becomes paramount. Moreover, these issues need to be addressed now, simultaneously rather than subsequently, to ensure that digitalization does not become another bottleneck on the path to a sustainable transformation of the energy system.

dena's Future Energy Lab determined its task as picking up on the potential of digital technologies for the integrated energy transition, identifying corresponding deficits in implementation, developing solutions together with stakeholders from the energy and digital industries, and testing these solutions in practice. In this context, cross-industry exchange plays an important role. After all, many of the challenges facing the energy sector — particularly in the area of digitalization — are being discussed elsewhere, too. The topic of digital identities plays a major role in civil society, for example in the issuance of digital ID cards, as well as in various other industries, such as the

1 Further information: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html

financial sector; the latter has long been concerned with decentralized network architectures, such as blockchain technology, which is often associated with verification around digital identities. Therefore, this project deliberately sought cross-sector contact and exchange.

This report is the result of a collaboration with 22 project partners to whom we would like to express our gratitude for their outstanding cooperation and indispensable contributions. Over more than two years and drawing from across Germany (and despite the Covid-19 pandemic) the involved stakeholders contributed their invaluable insights via multiple video calls, many emails, and the odd socially-distanced physical meeting to make this decentrally organized project – implemented across Germany – a great success. Special thanks also goes to the German Federal Ministry for Economic Affairs and Climate Protection (BMWK), which made the project possible and provided support.

At dena we are convinced that the energy transition will only work as a digital energy transition. The results of this pilot project will contribute to the success of the energy transition and are the starting points for further steps — which dena is already pursuing via a follow-up project. This is also an invitation to you, dear readers: Time is rushing ahead but we can only master these future challenges together. We hope you enjoy reading this report, that it inspires you, and that it can be used to fuel further developments in our industry. We invite you to continue the discussion and join us in taking the next steps toward a sustainable, digital energy transition.

Andreas Kuhlmann
Chief Executive of the
Deutsche Energie-Agentur (dena) –
German Energy Agency

Philipp Richard
Head of Division, Digital Technologies and
Start-Up Ecosystem of the Deutsche the
Energie-Agentur (dena) – German Energy Agency

1. Digitalisation of the energy industry – opportunities and challenges

Digitalisation has been a central topic in politics, business and society for several years. Not a day passes without digitalisation projects being launched, new technologies being introduced or ground breaking digital business fields being developed. The importance of digitalisation has received an additional boost, not least because of the coronavirus pandemic. At the same time, fundamental deficits requiring solutions were once again revealed in the energy sector and beyond.

The **dena project 'Blockchain Machine Identity Ledger' (BMIL)** has addressed this deficit in terms of digitalisation: the lack of standardised and thus scalable, secure **digital identities in the energy sector** that are compliant with data protection policies and are easily accessible for all relevant entities. This report contains a summary of these results. These types of digital identities offer enormous efficiency advantages for the significant coordination requirements of the energy system of the future, which lays the foundation for partially or fully automatic secure communication.

The central prerequisite for secure and fast communication is the continuous verification and checking of the identities and rights of entities (natural and legal persons), but also of plants (machines) that these entities have. The background is that identity and transaction data that are linked to the secure proof of identity can also always be assigned via this secure proof of identity, meaning **digital chains of trust** are built up reliably and quickly. In a heavily decentralised and integrated energy system, the required volume and speed for these processes can only be achieved with digital support, as otherwise the effort for timely and economic implementation would be too great.

The BMIL project was specifically about digital identities for energy plants, whereas the relevance of the topic extends far beyond the energy sector. There are not only numerous parallels to other sectors in the discussion of digital identities, but also points of contact to fundamental questions of digitalisation, such as governance structures (centralised versus decentralised network architectures), data economy, and data protection and security. For this reason, it is important not to consider digital identities in isolation, but in the overall context of digitalisation and the energy transition.

Why is digitalisation important at all?

The use of digital technologies always has a significant impact in terms of speed and efficiency of processes when large amounts of data have to be recorded, transmitted, collected, analysed and/or evaluated. In the energy sector, this need has always existed and it continues to increase. This is due to growing system complexity, primarily caused by the expansion of volatile and decentrally distributed energy resources as well as the emergence of new, controllable and cross-sectoral consumers (heat pumps, electric mobility, for example). A large number of plants participate in the energy system and in turn are causing an increase in **automation demand**. This development towards a more decentralised energy system offers new opportunities for individuals or communities at the local level to participate in the energy transition and to emerge, for example, as energy producers, as aggregators or, in the future, with flexible offerings and other business activities. Among other things, this can have a positive impact on the competitive situation in the energy market, progress in the expansion of renewable energies and the acceptance of the energy transition. [2]

Digitalisation also offers the possibility to exploit the additional degrees of freedom necessary for an integrated energy transition by linking different sectors and balancing volatile generation and load across sectors in terms of time and location. Digitalisation thus acts both as a **driver and as an enabler of the energy transition**. The decisive advantage lies in the ability to process information effectively and efficiently with the help of digital technologies, even in large-scale systems. Today, people often still communicate directly with each other to control processes in the energy system; however, much of this is to be fully automated and take place in near real-time in the future, for instance the change of supplier process, which in Germany still takes up to 15 days in Germany. This reduces the amount of work and therefore also the costs. In this manner, digitalisation facilitates not only the technical, but also the economic implementation of the energy transition.

2 See dena (2022): Energy communities: Accelerating factors in the decentralised energy transition. https://future-energy-lab.de/fileadmin/dena/Publikationen/PDFs/2022/dena-ANALYSE_Energy_Communities_Beschleuniger_der_dezentralen_Energiewende.pdf

What are the challenges as the digital energy transition advances?

The widespread use of digital technologies across value creation stages is facilitated by the standardisation of software interfaces and data formats. A lack of standardisation can be both a barrier to digitalisation and a bottleneck for the transformation of the energy system. Standards usually arise when many providers in the market benefit from uniform standards, there is a monopoly or near-monopoly provider that enforces its standard, or a certain standard is imposed by regulatory law. However, it is important to bear in mind that standards also have certain disadvantages. For example, the process to transition from one standard to the next is usually slow, and it is possible that undesirable path dependencies arise sometimes and that there is a delay in applying newer technologies. In the energy industry, however, it is particularly important that digital applications can draw on reliable data with appropriate quality criteria, as parts of the energy industry form part of critical infrastructure. However, sufficient data quality for digital applications or for automation that relies on artificial intelligence has not always been available in the energy industry to date. This is where standards can ensure uniformity and therefore also efficiency and security, if they do not yet exist. One challenge is to find the right degree of standardisation to provide a reliable framework for investment without limiting innovation.

The potential of digitalisation for the energy system can only be exploited if the necessary data is actually available. This is an issue involving technology (existing metering infrastructure, etc.) and economics (existing economic incentives) that is influenced by the regulatory framework. There is a need for competitive and fair governance – essentially a **data economy** [3] with a suitable regulatory framework within which entities are either given economic incentives to share data of public interest or regulations are introduced that oblige them to share this data. At the same time, it must be respected that companies also have an understandable interest in keeping particularly attractive information for themselves, for example, in order to secure their own market positions and to ensure sustainable economic activity. For this reason, it is also crucial, especially in an unbundled energy system, to know the conditions that must be in place so that information does not have to be shared in a competitive environment without countervalue or consent.

A functioning **data governance** or data economy for the energy system of the future therefore initially also needs clear rules regarding the ownership rights of data that are to be designed in such a way that they facilitate the energy transition rather than hinder it, without neglecting the justifiably high expectations of data protection and data security. With regard to digital identities, it makes a clear difference whether they are self-managed or not and whether they are stored centrally or decentrally.

Data security is of paramount importance in the energy sector. The consequences can be devastating if data that provides the basis for automatic energy trading is manipulated or compromised, for example. Energy quantities that are properly sold and scheduled in a virtual system, for example, contribute to balancing groups being balanced on paper, reinforcing the impression that the system is in balance. However, if the data set assigned to an energy plant is falsified, for example, at a certain quarter of an hour, and the amount of energy does not in fact exist at all, this creates a skewed position that throws the physical system out of balance. This example also shows how important digital identities are in providing a reliable anchor for data sets based on them because the aim is to promote data security.

Data protection is also becoming an increasingly relevant topic in the context of the energy transition. On the one hand, it is because there are significantly more electronic devices that collect and share data, which again in their entirety allow conclusions to be drawn regarding personal information. On the other hand, it is due to the fact that data is increasingly acquiring value and accordingly represents an economic asset. At this point, it is important to emphasise that there are secure and effective methods to protect digital data.

In the context of this general classification of the challenges in the digital energy transition, this report delves deeper into the topics of digital identities as well as digital identity ledgers and gives an overview of the pilot project and what has been achieved. Sections 2 and 3 provide a description of the existing gap in the energy sector and the pilot concept to close it, respectively. The most important results and recommendations for next steps are presented in section 4.

This document represents a summary of the motivation and history of the project as well as its key findings. The original German report goes into more depth on the various aspects and contains a more detailed technical, economic and regulatory assessment of the three different connection options. Moreover, the application possibilities of automated device connection and digital identity management are described and analysed.

3 See dena (2022): The data economy in the energy industry.

2. The digital gap in the energy industry – from blockchain, SSI and machine identities

From idea to pilot project

The importance of end-to-end digitalisation for decarbonisation in the energy industry is largely undisputed today. In particular, the lack of digital person and machine identities is increasingly perceived as one of the biggest barriers to digitalisation in the energy system. The pilot project 'Blockchain Machine Identity Ledger' addresses this digital gap and now that is has been successful completed, it is time to reflect on the path already travelled as well as the path ahead.

The Act on the Digitalisation of the Energy Transition (Gesetz zur Digitalisierung der Energiewende, or GDEW) came into force in 2016. This act regulates the equipment and operation of intelligent metering systems (smart meters). Since the year 2017, the Market Master Data Ledger Ordinance (Marktstammdatenregisterverordnung, or MaStRV) has also been in force. It establishes that a central electronic ledger of verifiable energy industry master data that registers all electricity generation plants (this includes small systems on balconies), gas generation plants and electricity storage facilities that are directly or indirectly connected to an electricity or gas grid is to be set up. The Market Master Data Ledger (in short in German, MaStR) therefore pursues its aim of merging previously separate registries and ledgers for identity data: the power plant list, the machine ledger and the photovoltaic reporting portal.

The idea arose to connect the planned communication module of intelligent metering systems – the Smart-Meter-Gateway (SMGW) – to the new plant ledger digitally, both conceptually and technically, from this initial situation. In this context, the increasing willingness to try out innovative new technologies reinforced the existing optimism and impetus. Specifically, a **blockchain** is to be used for the digital management of an advanced plant ledger instead of a conventional database to permit semi-automated registration, management and use of market master data in a system that is as open as possible. In particular, the **connection of an SMGW to the machine ledger via the built-in crypto chip** promised the secure authentication of installations that can be verified electronically at any time. The SMGW was intended to become a participating computer (node) in a blockchain. The advantages were obvious. This would considerably simplify and accelerate some of the verification tasks assigned to distribution system operators under the MaStRV and would also ensure higher data quality in terms of a uniform and consistent database. Specifically, the identities and rights of persons and systems could be verified digitally in real time in a cost-effective and secure manner to enable highly dynamic chains of trust between a PV plant, a SMGW and the MaStR: The rapid switching of plants between self-consumption, the provision of system services and participation in trading markets could technically be implemented. Digital person and machine identities have accordingly been defined as a key linchpin in the emerging real-time energy economy. Overall, from spring 2018 onwards, the insight spread to address the lack of end-to-end digitalisation by building digital chains of trust. At the same time, exchanges on this issue were initiated with relevant ministries.

Initially, however, the stakeholder study by the Deutsche Energie-Agentur (dena) – the German Energy Agency – entitled 'Blockchain in the integrated energy industry', started at the end of April 2018. It quickly became apparent that a number of industry partners had similar views and ideas. As a result, the 'Registration of plants in the Market Master Data Ledger (MaStR)' was defined in a series of workshops and other venues. This resulted in a process that provides for a blockchain for the digital management of a ledger, enables the semi-automated registration and management of market master data and provides for the selective provision of market master data. The technical, economic and regulatory feasibility was examined and the review was generally positive. [4]

Following the 'Blockchain in the integrated energy industry' study, further coordination and discussions with the Federal Ministry for Economic Affairs and Climate Protection finally led to the award of the feasibility study 'Blockchain-based capture and control of energy systems using the smart meter gateway: feasibility study and pilot concept' in May 2019. [5] dena eventually started the project 'Blockchain-based Device ID Registry for the Energy Industry' in mid-2019, together with researchers and more than a dozen companies, to develop a concrete pilot concept, which then led to the implementation project 'Blockchain Machine Identity Ledger' as part of dena's Future Energy Lab in 2020.

Authors: Matthias Babel, Johannes Sedlmeir, Jens Strüker, Christian Wiethe (Fraunhofer FIT)

4 Strüker, Jens et al. (2019): Technical and economic report as part of the multi-stakeholder study 'Blockchain in der integrierten Energiewende' (Blockchain in the integrated energy transition) by the Deutsche Energie-Agentur (German Energy Agency), p. 86–155, https://www.dena.de/newsroom/publikationsdetailansicht/pub/blockchain-in-der-integrierten-energiewende/

5 https://www.bmwi.de/Redaktion/DE/Downloads/Studien/blockchain-smart-meter-gateway-kurzfassung.html

From blockchain to SSI

In recent years, the understanding of the role of blockchain in managing corporate, person and machine identities in particular has developed decisively across the various projects and individual steps. For example, the concept of **self-sovereign identities (SSI) for the management of person and machine identities** became increasingly important. [6] Two aspects in particular proved to be critical if we consider the first intuitive ideas regarding the role of blockchains in the application scenario.

First, there are significant scalability challenges with an **SMGW as a participating computer (node) in a blockchain**. After all, the computing power, the necessary storage space and the (so far extremely low) bandwidth impose significant limitations on the performance of this type of blockchain due to the inherent redundancy of blockchains (replicated information processing).

First, there are significant challenges with an SMGW as a participating computer (node) in a blockchain. Unlike centralized networks, operations such as the execution of financial transactions and smart contracts or the storage of data are executed redundantly by multiple instances rather than just one. For this purpose, the necessary information must be forwarded to all system nodes and they must store the current state of the network. As a blockchain node, the SMGW would therefore also have to download, process and store the information of all other blockchain actors, but – for good reasons – it is not designed for these processes of highly scaled data processing. Due to the inherent redundancy (replicated information processing) of blockchains as described above, the computing power, necessary storage space and (so far extremely low) bandwidth provided for SMGWs impose significant limitations on the performance of such a blockchain. Solutions continue to be promising [7], but currently the challenges are not yet in line with the benefits. Decentralisation is not an end in itself, but a means to achieve a high level of resilience and availability, as well as to create a more decentralised, automated rights management on a common IT infrastructure that all entities in the energy sector can (more easily) agree on. Both goals can already be achieved via a moderate degree of decentralisation, for example, through nodes at the essential institutions in the energy sector. For all other entities, a client application (interface on an edge-device to a central computer) on the relevant systems that can connect to a blockchain node of another trusted institution for read and write access – with regard to the operation to be performed – should be sufficient.

In addition to the SMGW as a node, it also became increasingly apparent that the immediate storage of master and transaction data on the blockchain was a particular challenge to deploy a blockchain. [8] This is because two of the core properties of blockchain technology are the immutability and transparency of the data stored on it. This means that plant master data written to the blockchain can no longer be deleted later. Furthermore, all network participants can view this data, unless the data are stored in encrypted form. This approach quickly becomes incompatible with the General Data Protection Regulation (GDPR) as small-scale systems in particular are usually closely linked to their owner. This is the case, on the one hand, because the right to erasure specified there can no longer be granted. The owner actually loses control over the master data for their plant due to the replicated data storage. On the other hand, encrypted data on the blockchain are problematic in terms of data protection laws precisely because they cannot be changed. There is no guarantee that encryption methods currently considered secure will continue to exist in the future. An illustrative example is asymmetric encryption, the security of which is compromised by quantum computers. Blockchain protocols could be protected by adapting the encryption procedures for new transactions, but this path is blocked for past transactions. In addition, data made unrecognisable to outsiders, as can be achieved through encryption or hash functions, can also constitute sensitive data, either directly or through the associated metadata. Thus, their trace on the blockchain in turn results in information requiring protection. This situation is similar to the pseudonymisation of an account on the Bitcoin blockchain. On the other hand, the usability of encrypted data on a blockchain is largely useless for use in smart contracts, for example. [9]

Another challenge resulting from the redundant storage of data is the limited scalability that blockchain solutions usually entail due to the replicated processing of information. Although there are currently various methods to address this, such as roll-ups or sharding, it is still one of the most significant limitations that blockchain technology has to face and has only limited possibilities even for pure data storage with the purpose of availability without complex calculations.

SSI-based machine identities for consistent end-to-end digitalisation

The SSI concept promises to address the challenges described above and, in doing so, recalls a paradigm that uses a subset of cryptographic procedures and has been known for more than 30 years and has also been successfully applied in practice. These enjoy an increased level of attention today due to the emergence of blockchains, among other things. This paradigm involves digital certificates based on digital signatures and generally asymmetric encryption, which are built on a public key infrastructure (PKI). This approach has been successfully used for decades on secure websites (https), in many security-conscious companies as well as in critical infrastructures. Digital

6 See also Sedlmeir et al. (2021): Digital identities and verifiable credentials, Business & Information Systems Engineering 63, pp. 603–613

7 See blockchain protocols such as Mina: https://minaprotocol.com;

8 See overview in Bogensperger et al. (2021): Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft (What future does blockchain technology have in the energy industry), discussion paper, https://stiftung-umweltenergierecht.de/wp-content/uploads/2021/07/InDEED_Diskussionspapier-Blockchain-Energiewirtschaft_2021-07-22.pdf

9 For further information, see also Sedlmeir et al. (2022): The transparency challenge of blockchain in organizations, Electronic Markets, https://doi.org/10.1007/s12525-022-00536-0

certificates have not yet been regularly opened for cross-domain applications. [10] This is now precisely the innovation that the addition of blockchains promises: a collaborative approach in which a PKI is jointly operated by many entities.

A certificate-based approach allows the bilateral exchange of verifiable information and in turn an even more decentralised architecture than would be the case with data processing via blockchain nodes. The bilateral presentation of certificates enables the data-protection compliant verification of claimed characteristics and attributes of a plant or of rights of its owners. In turn, the local storage of certificates enables the selective provision of data and thus the minimisation of exchanged data to what is absolutely necessary, which is desirable especially with regard to the increase in small plants for the informational self-determination of end users, but also with regard to the protection of company confidentiality. The uniform momentum regarding blockchain-supported, certificate-based digital identities for people and companies in politics (projects at the Federal Chancellery) and business (showcase projects such as ID-Ideal and IDunion) as well as for machines also promises a consolidation of the standards and components to be developed in the medium term, thus benefiting efficiency and security. [11] SSI components are therefore also being discussed in GAIA-X and other projects. [12]

In an SSI-based approach, attributes of plants in the energy sector can be evidenced by what are known as verifiable claims, which are based on certificates issued once by authorities, until they are revoked in the context of implementation in BMIL. One such authority, especially for existing installations, could be the existing MaStR, which does not keep its data on a fully publicly accessible system. Such authorities can generally be verified via certificate chains. For example, the Bundesnetzagentur (Federal Network Agency) could appoint trusted certifiers (market authorities) who in turn certify certifiers for plants (physical asset authorities). These in turn can then issue verifiable claims for the plants via digital signature (certificates). These chains of trust can be checked to ensure that they are correct and up-to-date at any time via schemes and revocation registries on a public blockchain. Therefore, it is also conceivable that entries in the MaStR can be made directly by the wallet of the plant on the basis of verifiable claims. In addition, real-time confirmation of claims without certificates is also generally possible bilaterally from authorities.

A public blockchain (but also databases managed by the authorities with broad read rights) could be used at this point for the registration of public identities of authorities and certificate schemes as well as for the provision of revocation registries for the certificates mentioned (both for plant certificates and authority certificates). Revocation registries allow a certificate to be declared invalid. It is also possible for different blockchains or conventional databases to be used side by side here in the future. Interoperability is ultimately only a question of standardisation since it is primarily a matter of read access; no bridges are required between the blockchains. However, whenever plants are operating in multiple markets on different blockchains in the long term, the option of bridges between blockchains may become necessary to prevent double spends, for example, in the form of double marketing of generation output, by registering on multiple blockchains. It should be emphasised that bridges between blockchains are needed for use cases, but less so in terms of a blockchain that manages public identities of certifiers or revocation registries, that is, unless identity verification also needs to take place in the context of a smart contract. But this is unlikely to be useful due to the sensitivity of data.

The exchange of information between distribution and transmission system operators is still far from end-to-end digitalisation without media discontinuity nowadays. The same applies to congestion management or market communication. Millions of PV plants and thousands of heat pumps, home storage units and CHPs have not yet been digitally integrated into the energy system. Accordingly, switching generation plants and storage facilities from self-consumption to the provision of system services or participation in electricity trading continues to mean error-prone and time-consuming processes on paper. The BMIL project promises to make a decisive contribution to the further digitalisation of energy industry processes with a developed, decentralised plant ledger.

The goal should be to draft a digital target image of the integrated energy industry and then to pursue it consistently. This is because today, it is not only communication-capable electricity and heat meters and the plant ledger that are separate both conceptually and digitally. The proof of origin registry is also by definition disconnected from the plant ledger. A vision that can guide the transformation would help. Here the implementation and testing of the BMIL will already be able to provide valuable design information.

10 See also Schellinger et al. (2022): Mythbusting Self-sovereign Identity (SSI) - Diskussionspapier zu selbstbestimmten digitalen Identitäten (Mythbusting Self-sovereign Identity (SSI) – discussion paper on self-determined digital identities), https://www.fim-rc.de/wp-content/uploads/2022/06/Whitepaper_SSI_Mythbusting_German_version_compressed.pdf

11 See also Sedlmeir et al. (2021): Digital identities and verifiable credentials, Business & Information Systems Engineering 63, pp. 603–613

12 See GAIA-X: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html; Id-Ideal: https://id-ideal.de/ and IDunion: https://idunion.org/

3. Project structure and pilot concept

dena brought together a total of 22 companies, organisations and startups from the energy and digital industries as well as the scientific community in the Blockchain Machine Identity Ledger pilot project to jointly build an essential building block for the digital infrastructure of the future energy system. As with all pilot projects in the Future Energy Lab, the basic approach was to ensure a high degree of openness among the partners involved, which would in turn enable the connectivity for innovations that build on this.

Given below is an explanation of the project structure including problem definition, objective and basic assumptions.

3.1 The partner group

The partner consortium united established companies with considerable experience and young startups. Special importance was attached to equal collaboration that ignores size differences. dena was responsible for project management and control.

A team of experienced scientists was also involved in the project in the technical (OFFIS), economic (Jacobs University) and regulatory (EY Law) evaluations. In parallel, further scientific support (Fraunhofer FIT) ensured that the operational course of the project dovetailed well with the scientific evaluation by publishing a total of four progress reports on the pilot phase, which lasted approximately two years.

The group of commissioned partner companies consisted of companies with a stronger focus on blockchain (and blockchain infrastructure) and digital identities (Energy Web, KILT, OLI Systems, Parity, Riddle&Code, Spherity, T-Systems, YOUKI) as well as organisations from the energy industry and plant connectivity, including certified smart meter manufacturers (PPC, Theben), gateway administrators and companies from the metering point operation sector (GWAdriga, meterpan, Voltaris) and energy supply (VSE).

Finally, other associated companies accompanied the project progress with their additional energy and digital business knowledge and acted as sounding boards for the results achieved (EnBW, E.On, SAP and 50Hertz).

Figure 1: Overview of the project partners involved

3.2 The project objectives

The underlying vision of the project is the automated registration and deregistration of plants in the energy system and ability to participate in changing markets with little complication. This is to be achieved by linking the SMGW infrastructure with digital identities and a blockchain-based plant ledger, as shown in the following figure.

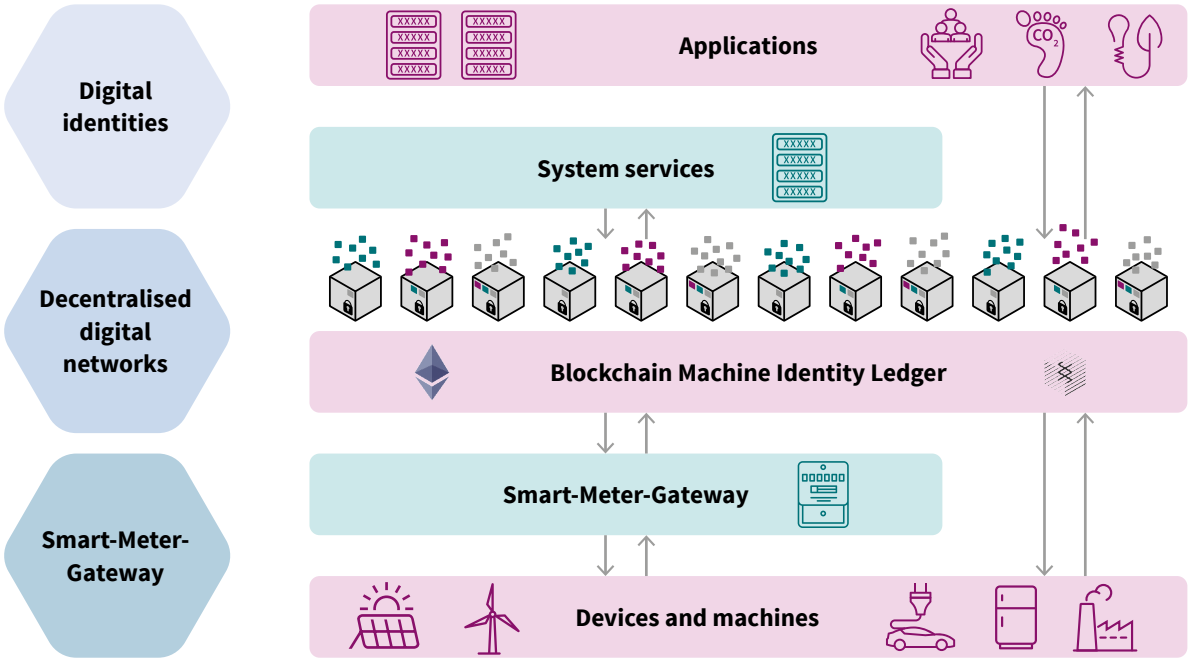


Figure 2: BMIL infrastructure for the energy system of the future

At the heart of the pilot project is a decentralised, blockchain-based identity ledger with which energy systems can be linked via the secure SMGW infrastructure or smart home devices and record their identity there: usable, traceable and tamper-proof for all entities.

This ledger is then used by the plants as a common basis to automatically identify themselves in communication with system-relevant services and a wide range of market applications. The project also follows the approach of only passing on the data that is actually needed for the respective application or system service ('selective disclosure') by linking digital identities with the principle of local data storage and cryptographic procedures.

This basic orientation marked the start of the BMIL project.

This vision led specifically to the following tasks with a focus on demonstrating proof of technical feasibility in the context of the pilot project in the following three sub-areas:

(1) Creating a machine identity
The goal for the machine identity aspect was set to create a digital, self-sovereign and decentralised machine identity.

(2) Transmission and security anchor (SMGW)
The goal for the transmission or communication of the identity and its characteristics was set to use the smart meter gateway infrastructure in normal operation as an additional security anchor.

(3) Entry into the ledger
The third goal was to build a decentralised digital ledger based on blockchain and to test two different blockchains.

In addition, some showcase application examples of the project partners in the areas of proof of origin, flexibility markets, smart CO2 certificates and energy communities are intended to highlight the potential added value of digital identities.

The group of companies involved in the BMIL pilot was also set up with a view to sufficiently reflecting the heterogeneous technological developments in the field of decentralised network technologies (blockchain technology). The highly dynamic developments in the blockchain and identity ecosystems in particular have made it necessary to integrate several different technology providers with different approaches into the project.

The aim of the BMIL pilot project was also to provide an outlook on a possible series implementation in the heterogeneous energy and blockchain ecosystem, which is why two different blockchain environments were part of the pilot project: one ledger is based on the technological environment of the Ethereum blockchain, while the other ledger was built on the Substrate development environment from the Polkadot ecosystem. However, the focus at the beginning was also placed on agreeing on an identity standard that could be used productively by all the protocols and system connection options used, for example, by building bridges between the two blockchain protocols, in order to avoid going beyond the scope of the project.

3.3 The synergy potential of digital identities and blockchain technology

Given below is a detailed description of the construction of digital identities and how this was used advantageously in the project in interaction with blockchain technology. Figure 3 shows an example of how a digital identity is structured in general, for persons or for machines.

As the diagram illustrates, digital identities consist of two components: an ID number, known as the 'identifier', and specific 'characteristics' or 'attributes' assigned to this identifier.

For example, the identifier is an ID card number (unique and unchangeable) for a person, while the attributes contain further information about the person's biography and identity, such as different degrees and certificates, interests, physical characteristics, etc.

In the context of an (energy) asset, the identifier would simply be a number, while the attributes of the plant would comprise, for example, its location, its owner's name, its nominal power and its grid connection point. First and foremost, this is master data, which is usually static – that is, unchangeable – over time.

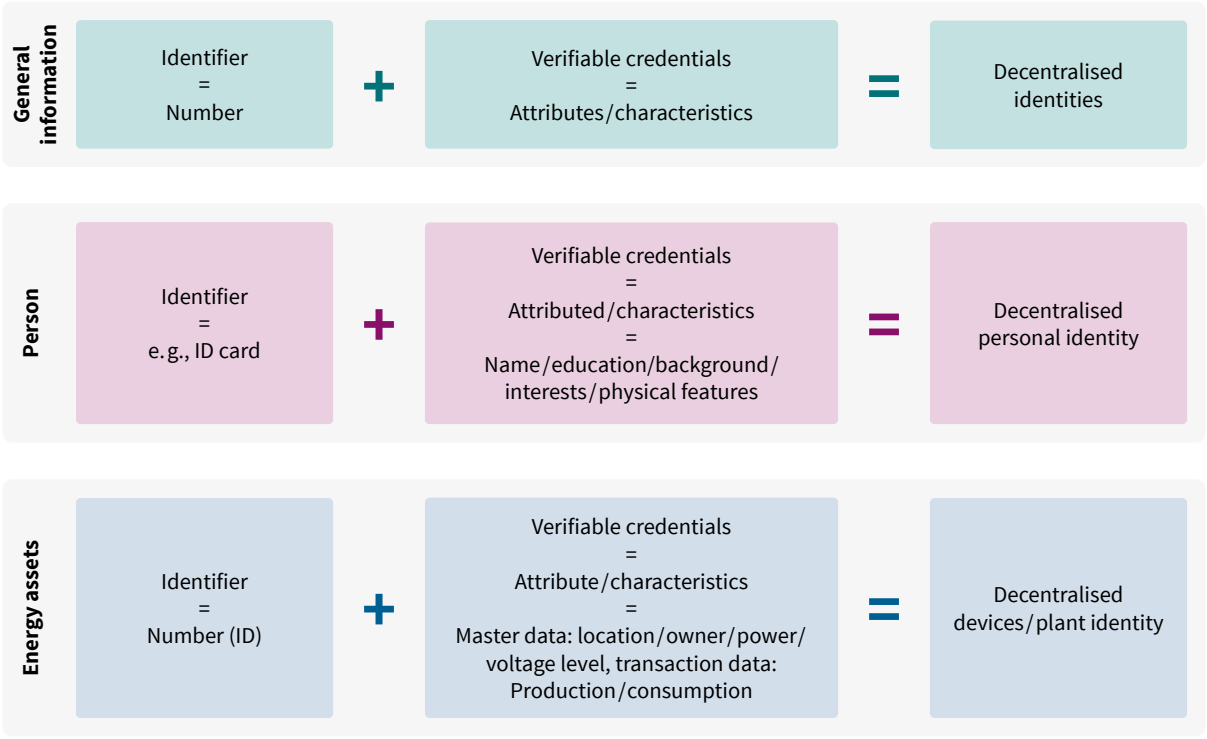


Figure 3: Basics of digital identities

However, it is also conceivable that there are characteristics that are dynamic, that is, ones that change over time, such as the generation output or the consumption at a certain time.

The division of the digital identity into the components identifier and attributes results in an immediate advantage. Both components can be stored separately from each other, unlike, for example, an ID card, which inseparably combines the card number and the attributes in one document.

Figure 4 shows an example of the opposing poles arising in digitalisation across all sectors and how the separation of the identifier from the attributes and the decentralised storage of attributes can help to solve the dilemma. It is possible to meet the requirement for visibility at all times that a plant is registered on the system as the identifier can be stored independently of the attributes if necessary, in a ledger that can be viewed by all parties. The project thus benefits from the best features of blockchain technology in that the identifiers of the plants are stored in a decentralised, transparent and tamper-proof manner. On the other hand, the separation enables decentralised data storage so that the principles of data protection and data economy are supported. Selective data sharing becomes possible, meaning that decentralised data storage also promotes the idea of data sovereignty and facilitates a data economy. In particular, it should be emphasised that although it is possible to deposit identifiers on the blockchain when using a blockchain, this is by no means necessarily required. The identifier (possibly even together with attributes) can be stored on a highly available blockchain if visibility and availability are paramount; if very high data protection requirements exist, it is also possible to refrain from storing identifiers or attributes on the blockchain altogether and only anchor the identity of the issuer of verifiable claims on the blockchain.

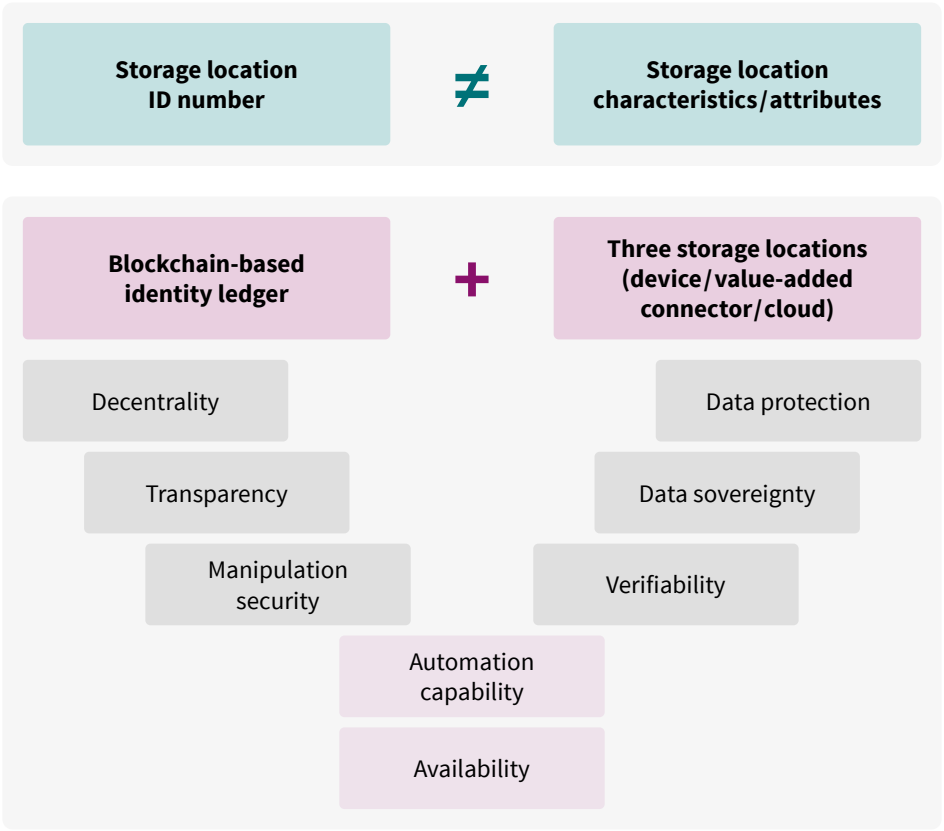


Figure 4: The synergy potential of digital identities and blockchain technology

3.4 The three options for plant connection

There are also different options with regard to the storage of the attributes, as figure 5 illustrates. The project goal was to investigate three different storage locations. The reason for this was that it is not currently clear which option will ultimately prevail in which applications or where there might be different options that exist in parallel.

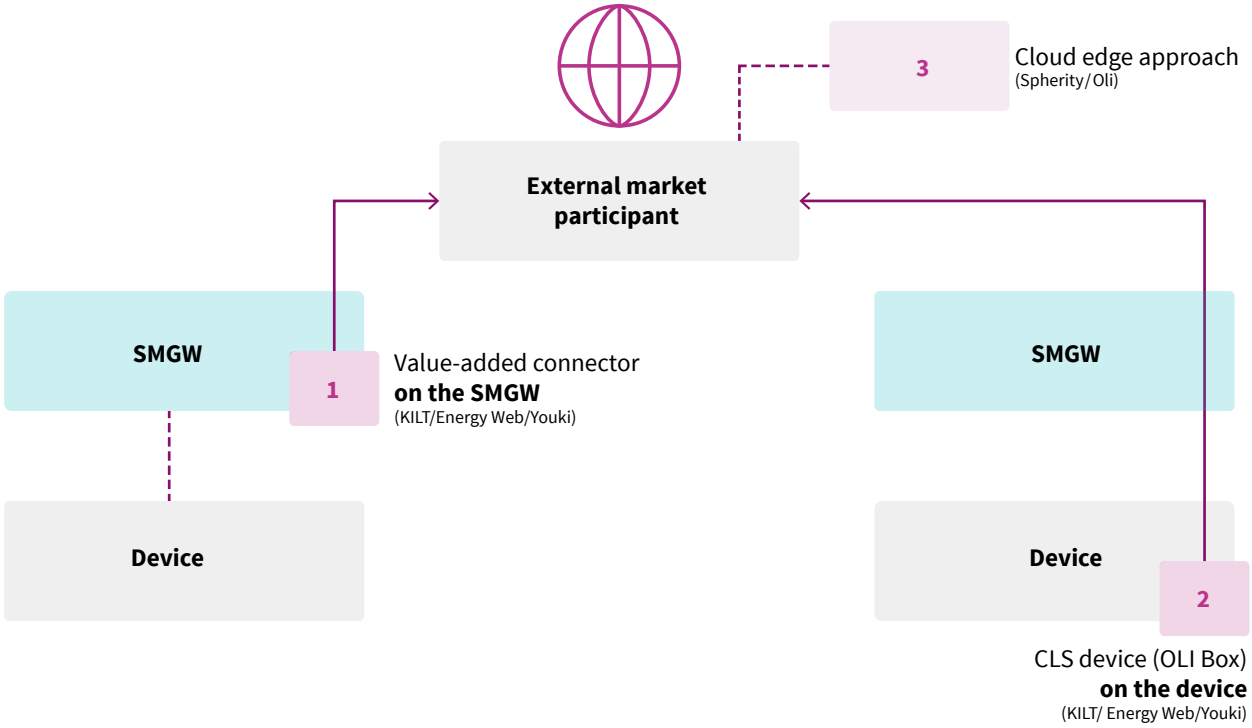


Figure 5: The three connection options in the BMIL

The following three options were examined:

1st option: on the SMGW

In this option, the characteristics of the identity are stored directly at the smart meter gateway on an adapted value-added module from YOUKI.

This option was implemented in the pilot project by the companies Theben (smart meter), YOUKI (value-added module on the SMGW), KILT (blockchain-based identity protocol) and meterpan (MSO).

2nd option: on the device

In this option, the characteristics of the identity are stored directly at the plant on a dedicated CLS (controllable local system) device.

This option was implemented in the pilot project by the companies PPC (smart meter), OLI Systems (CLS device), KILT (blockchain-based identity protocol) and GWAdriga (gateway administrator).

3rd option: on a digital twin in the cloud

In this option, the characteristics of the identity are stored in a cloud.

This option was implemented in the pilot project by the companies Spherity (cloud edge approach), PPC (smart meter), OLI Systems (CLS device), GWAdriga (gateway administrator), VSE (energy supply) and Voltaris (metering point operation).

4. Summary and recommendations for action

Proof of technical feasibility was a critical factor as the BMIL project is a pilot, in other words, it is actually being implemented. Feasibility was successfully demonstrated for all three stated implementation milestones (creating a device identity, transmission and security anchor (SMGW), entry into the ledger). This is an important stage in directing the formulated vision and represents a key building block for the automated energy system that can be attached to specific applications in future.

Essential **framework requirements and standards for the use of digital identities in the energy system** were developed and tested through the BMIL pilot project. The following specific points were achieved:

- ... conclusion of an agreement on identity standards in the partner group.
- ... setup of a digital, self-sovereign and decentralised device identity.
- ... realisation of an anchoring of the identity on the devices (options 1 and 2), and
- ... an anchoring of a digital twin in the cloud (option 3).
- ... successful implementation of a transmission of the digital identity via SMGW infrastructure in normal operation.
- ... establishment of a link with two blockchain-based identity ledgers (Ethereum and Substrate).

Further technical, economic and regulatory key statements can be made and respective recommendations for action, which relate in particular to the thematic strands of SMGW infrastructure, digital identities (SSI) and interoperability, can be derived from the scientific evaluation of the pilot project.

The study has not identified any fundamental barriers to serial implementation of the BMIL infrastructure to date, yet there are still unanswered questions.

4.1 Technical evaluation

- The device registration based on digital identities (SSI) and the self-determined identity system can be implemented within the smart meter PKI in normal operation and using smart metering systems available on the market. However, a large number of technical questions remain unanswered at present time. In particular, it is not clear from a technical point of view which approach should be preferred for the integration of identity creation and, beyond that, the business logic of value-added applications, since the spectrum of value-added applications brings with it very different requirements for the execution platform.

- The scalability of the chosen identity directory on blockchain basis is given with regard to subsequent series implementation. In addition, the coexistence of different device ledgers is possible and therefore no commitment to a specific blockchain technology is necessary (just think: interoperability, bridges), although further standardisation efforts will be needed in the future.

- Technical limitations in terms of available communication channels, computing power of edge devices, bandwidths and latency times do not represent a limitation for digital identity-based device registration and the self-determined identity system, but will come into focus for use cases based on it and must be considered in more detail. An obligation on the part of the metering point operator (MSO) to provide information on the connectivity of each metering point (including availability of the CLS channel) would create certainty and transparency about which use cases are technically possible in each case. The status of a metering point includes information on whether and which SMGW has been installed, as well as a qualification of the accessibility (depending on device bandwidth and communication technology) in stages.

- The lack of standardisation of non-functional characteristics of the CLS channel communication path is a technical issue currently. In future, further factors such as minimum requirements for the CLS channel in terms of availability, transmission bandwidth and latency are to be considered.

- Encapsulating the endpoint of the CLS chain of trust via a certified value-added module or a certified CLS proxy is of common and particularly high importance in all connection options, as it keeps the development effort for future value-added applications low and allows manufacturers and developers to focus on the application logic. It can be deduced from the project that a combination of a potential value-added module (that is, the possibility of self-hosted applications) with the purely pass-through proxy functionality would represent a desirable implementation of the endpoint of the CLS chain of trust. This option would be open to all technologies and would, in particular, offer a corresponding execution platform for all the identity management connection options described. The basic requirement of openness of the CLS channel must therefore be maintained. Standardisation of value-added applications would slow down innovation.

4.2 Economic evaluation

- The transaction costs of establishing identity can potentially be significantly reduced with all three connection options. However, the different connection options can generate different costs and different benefits and added values. This implies that ensuring effective technology competition under consideration of the necessary level of data protection and data security should have high priority in this early phase of developing the different connection options in order to avoid discriminating against any technology option. Potential barriers to technology competition lie in various aspects relevant to competition: possible path dependencies in connection with the smart meter rollout , market entry barriers due to repercussions of competition in the metering point market on the possible connection variants, and repercussions due to different forms of competition in the applications based on the connection options. To develop more concrete options for action to ensure technology competition between the different connection options, the barriers are to be investigated further.

- The interoperability of digital identities is a central prerequisite for raising the potential for reducing the transaction costs in identity establishment. Network effects play an important role here. Standardisation of the SSI components might be necessary in the energy sector to overcome path dependencies and to permit stronger market penetration of the SSI concept in the first place. Therefore, it should be examined in which areas a standardisation of the SSI approach in the energy sector can be promoted without restricting technology competition and to be able at the same time to leverage possible synergies with other sectors.

- The installation costs for the connection options or for the necessary CLS proxy can be reduced by installing SMGWs at the same time. However, the potential trade-off between cost savings in the installation of the devices and the possible restriction of competition (and thus of efficiency gains) must be weighed up. By commissioning a value-added module or a CLS proxy in parallel, market players can avoid a second technician visit and thus higher costs as well as the time delay in rolling out the components that are critical for the connection options.

4.3 Regulatory evaluation

- All connection options comply with the IT security regulatory requirements of the Metering Point Operation Act (Messstellenbetriebsgesetz, or MsbG) and Technical Guideline TR-03109 of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, or BSI) and thus comply with the current legal framework. However, regulatory standards for certain communication channels are lacking. Defining these standards would facilitate forced interoperability, simplify series implementation and ensure legal certainty (see Economic evaluation). The protection of the rights of the persons affected (Articles 15 to 21 of the DSGVO) in all connection options must first be ensured by appropriate options for action (e.g., agreement with the persons affected).

- In all three connection options, both non-personal and personal data are processed. The required lawfulness as well as the limitation on use of the data can predominantly be affirmed in the application of data protection law and the processing of personal data. However, the compliance with the principle of transparency regarding the processing of data must be ensured towards the affected persons for serial implementation of the BMIL.

- A discussion on the concretization of governance structure for digital identities in the energy sector is necessary to establish clarity on responsibilities for stakeholders. There is a great deal of legal uncertainty who is responsible (system operator, party involved in the identification process or the party who entered the data) for the correctness of the data required for the creation of the machine identifier (liability in the event of misinformation). Since the MsbG does not contain any provisions in this regard, recourse to civil law and generally applicable standards is necessary. Therefore, an examination of the individual case is critical and carries a high risk for the parties involved to be held liable for any data violation. Clear regulation on who is responsible for which data in the identity determination or identity process would increase legal certainty for market players and thus drive forward series implementation. Further analysis is to be carried out on a rights and roles concept for the BMIL identity model in the energy industry (rights for organisations and institutions) and, based on this, a further data protection evaluation of the new identity standards carried out.

4.4 Outlook

The BMIL project has shown that it is advantageous to approach the development of solutions in technical, economic, and legal terms in parallel and to collaborate across the different fields at an early stage. This stakeholder process must be continued with established as well as young entities from the digital and energy sectors, all on an equal footing to advance the series implementation of the BMIL infrastructure. With regard to other showcase projects and pilot projects (including ID-Ideal, IDunion, InDEED), options for collaboration and linking of results should also be sought across projects in order to achieve network effects in the future. The discussion held during the course of the project with central players such as the Federal Network Agency (Bundesnetzagentur, or BNetzA) and the BSI should be continued, too.

The goal should be to draft a digital target image of the integrated energy industry and then to pursue it consistently. This is because today, it is not only communication-capable electricity and heat meters and the plant ledger that are separate both conceptually and digitally. The proof of origin registry is also by definition disconnected from the plant ledger. A vision that can guide the transformation would help. Here the implementation and testing of the BMIL will already be able to provide valuable design information.

Closing the digital gap in the energy system promises to significantly increase process efficiency in particular. This is also urgently necessary in view of the significant increase in coordination requirements in a more decentralised energy system. Digitalisation can therefore prove to be a significant accelerating factor in the decarbonisation of the energy industry, and we should seize this opportunity whenever possible.

5. List of abbreviations

BMIL	Blockchain Machine Identity Ledger
BMWK	Federal Ministy for Economic Affairs and Climate Protection (in German: Bundesministerium für Wirtschaft und Klimschutz)
CLS	Controllable local system
EMT	Externer Marktteilnehmer (in English: External Market Participant)
MaStR	Market Master Data Ledger (in German: Markststammdatenregister
MaStRV	Market Master Data Ledger Ordinance (in German: Markststammdatenregisterverordnung)
MsbG	Metering Point Operation Act (in German: Messstellenbetriebsgesetz)
MSO	Metering point operator
PKI	Public key infrastructure
SMGW	Smart-Meter-Gateway
SSI	Self-sovereign identity

6. List of figures

Figure 1: Overview of the project partners involved 11
Figure 2: BMIL infrastructure for the energy system of the future 12
Figure 3: Basics of digital identities 13
Figure 4: The synergy potential of digital identities and blockchain technology 14
Figure 5: The three connection options in the BMIL 15

7. List of references

1 Further information: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html

2 See dena (2022): Energy communities: Accelerating factors in the decentralised energy transition. https://future-energy-lab.de/fileadmin/dena/Publikationen/PDFs/2022/dena-ANALYSE_Energy_Communities_Beschleuniger_der_dezentralen_Energiewende.pdf

3 See dena (2022): The data economy in the energy industry.

4 Strüker, Jens et al. (2019): Technical and economic report as part of the multi-stakeholder study 'Blockchain in der integrierten Energiewende' (Blockchain in the integrated energy transition) by the Deutsche Energie-Agentur (German Energy Agency), p. 86–155, https://www.dena.de/newsroom/publikationsdetailansicht/pub/blockchain-in-der-integrierten-energiewende/

5 https://www.bmwi.de/Redaktion/DE/Downloads/Studien/blockchain-smart-meter-gateway-kurzfassung.html

6 See also Sedlmeir et al. (2021): Digital identities and verifiable credentials, Business & Information Systems Engineering 63, pp. 603–613

7 See blockchain protocols such as Mina: https://minaprotocol.com;

8 See overview in Bogensperger et al. (2021): Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft (What future does blockchain technology have in the energy industry), discussion paper, https://stiftung-umweltenergierecht.de/wp-content/uploads/2021/07/InDEED_Diskussionspapier-Blockchain-Energiewirtschaft_2021-07-22.pdf

9 For further information, see also Sedlmeir et al. (2022): The transparency challenge of blockchain in organizations, Electronic Markets, https://doi.org/10.1007/s12525-022-00536-0

10 See also Schellinger et al. (2022): Mythbusting Self-sovereign Identity (SSI) - Diskussionspapier zu selbstbestimmten digitalen Identitäten (Mythbusting Self-sovereign Identity (SSI) – discussion paper on self-determined digital identities), https://www.fim-rc.de/wp-content/uploads/2022/06/Whitepaper_SSI_Mythbusting_German_version_compressed.pdf

11 See also Sedlmeir et al. (2021): Digital identities and verifiable credentials, Business & Information Systems Engineering 63, pp. 603–613

12 See GAIA-X: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html; Id-Ideal: https://id-ideal.de/ and IDunion: https://idunion.org/

www.dena.de future-energy-lab.de

dena
German Energy Agency