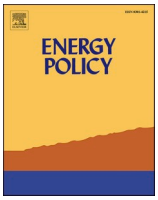
Energy Policy 164 (2022) 112901

Contents lists available at ScienceDirect

Energy Policy

journal homepage: www.elsevier.com/locate/enpol



Systemic risks in electricity systems: A perspective on the potential of digital technologies

Marc-Fabian Körner [a,b,*], Johannes Sedlmeir [a,b], Martin Weibelzahl [b], Gilbert Fridgen [c], Moreen Heine [d], Christoph Neumann [e]

[a] University of Bayreuth, FIM Research Center, Germany
[b] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Germany
[c] University of Luxembourg, Interdisciplinary Centre for Security, Reliability and Trust, Luxembourg
[d] University of Lübeck, E-Government and Open Data Ecosystems, Institute for Multimedia and Interactive Systems, Germany
[e] TenneT TSO GmbH, Germany

ARTICLE INFO

Keywords:
Blockchain
Energy informatics
Privacy-enhancing technologies
Renewable energy sources
Self-sovereign identities
Systemic risks

ABSTRACT

In the last decades, several developments have transformed electricity systems in Europe towards liberalized and decentralized systems that are coupled inter-sectorally and inter-regionally. These developments have yielded various significant benefits, such as increased efficiency and robustness. However, we argue that they have also caused new interdependencies and complexity with a corresponding increase in associated systemic risks, e.g., local failures may spread faster and more extensively throughout the system. In this paper, we illustrate how systemic risks may arise in European electricity systems by discussing three exemplary developments. We also discuss the decisive role of the digital transformation that, on the one hand, speeds up the transition of electricity systems and challenges electricity systems' stability through rapid change, but on the other hand may also provide solutions to tackle systemic risks. We argue that, especially in a strongly interconnected world, policymakers must implement a global perspective on these critical and increasingly complex systems, requiring adequate cooperation with respect to data. Using an exemplary case from Germany, we finally illustrate how an intensified data exchange may help to address systemic risks. In this context, we draw a perspective on the potential of emerging digital technologies, like self-sovereign identities, blockchains, and privacy-enhancing technologies.

1. Introduction

Electricity systems are inherently exposed to risks and potential blackouts (Atputharajah and Saha, 2009). Corresponding damages to the overall system and society can be considerable and long-lasting: In June 2019, almost 50 million people did not have access to electricity due to a massive power outage in all of Uruguay, in most of Argentina, and some parts of Paraguay. Another example relates to heat-storms and misleading "practices in the day-ahead energy market" (Caiso, 2020) that led to significant outages in California, USA, in August 2020. Misaligned incentive mechanisms in the electricity market design were also one of the reasons why there was almost a blackout in Germany in June 2019: As a consequence of short selling and the improper operation of several German balancing groups, the German transmission system operators (TSOs) not only had to fully activate the retained balancing power reserves, but also take additional measures, including requesting emergency reserves from foreign TSOs (50 Hertz et al., 2019).

In the context of blackouts within electricity systems, systemic risks refer to the threat of a collapse of a substantial part of the whole system that may lead to the breakdown of the entire system – as opposed to a collapse of a single component that does not lead to a system breakdown (Ilin and Varga, 2015). Typically, a systemic risk is characterized by only revealing itself after it has occurred. Individual players may not be aware of the hidden risks and may, therefore, in the worst case even contribute to a further increase in these risks. The realization of systemic risks in form of blackouts requires initial events or triggers. Such triggers can be various and include, e.g., external shocks, geopolitical events, political crises, human failures, technical failures, natural disasters, and terrorist or cyberattacks (Pierret, 2013; Wijnia and Herder, 2004). It is expected that in the next decades, especially the number of natural

* Corresponding author. University of Bayreuth, FIM Research Center, Germany.
E-mail address: marc.koerner@fim-rc.de (M.-F. Körner).

https://doi.org/10.1016/j.enpol.2022.112901
Received 13 June 2021; Received in revised form 25 February 2022; Accepted 4 March 2022
Available online 25 March 2022

catastrophes and cyberattacks will increase, making the occurrence of such initial trigger events more likely than before (Xie et al., 2010).

In addition to the increasing occurrence of possible triggers, various international developments have led to a change in systemic risks: Within the past decades, electricity systems have shifted from traditional and unidirectional electricity supply chains towards multidirectional and multinational electricity supply networks. In the European Union (EU), this shift results in particular from (1) electricity market liberalizations, (2) transformations towards decentralized systems based on renewable energy sources (RES), and (3) increased complexity through grown sector coupling and inter-regional coupling. Clearly, these fundamental transformations of the electricity system towards liberalized, coupled, and highly decentralized systems have caused various benefits worldwide (Percebois, 2008), including reduced prices for consumers and increased system efficiency. Additionally, such systems are often argued to be more resilient due to their larger system sizes and the increased number and diversity of backup facilities. The new interconnection between different sectors, markets, networks, and regions has particularly been fostered by significant advances in digitalization, which acts as some kind of catalyst. However, the described developments represent a two-sided sword: the grown system complexity and interconnection may also entail a hidden rise of new systemic risks with the danger of an even faster and further-reaching, cascading spread of local failures (Berizzi, 2004).

We note that there are already academic references and also several policy-driven initiatives, e.g., from the EU or the European association for the cooperation of TSOs for electricity (ENTSO-E), cf., the introduction of regional security coordination service providers in the EU, that consider a purposeful electricity-data exchange (Andersson et al., 2005; Dagle, 2004; Pourbeik et al., 2006) to address systemic risks. In line with and contributing to these initiatives, our article presents and illustrates how emerging digital technologies such as blockchains, decentralized identity management for electricity system infrastructure components, and privacy-enhancing computation techniques like secure multi-party computation may promote such purposeful data exchange in electricity systems: They can foster cooperation in terms of electricity data supply, sharing, and exchange among national and international stakeholders including, e.g., system operators, electricity generators, consumers, aggregators, energy retailers, utilities, and equipment manufacturers. Moreover, we illustrate how these digital technologies may help to foster collaboration and trust and increase security on a more decentralized basis without the need for a single, trusted authority or new intermediaries with high trust and availability requirements, while at the same time enabling the permanent monitoring of the current state of the entire system as well as better forecasts, e.g., of future critical system situations or general resource adequacy. Above all, only such "global" information about the entire system can help to uncover hidden systemic risks that could otherwise grow unnoticed and take countermeasures by, for instance, modifying economic incentive structures or extending monitoring and automatic control activities.

Our article is organized as follows: In Section 2, we briefly describe our analytical approach in the method section. In Section 3, we reflect systemic risks and sketch relevant developments that may contribute to a change in systemic risks in European electricity systems. Based on this, we highlight the potential of secure and trustworthy digital technologies for improved data exchange in Section 4. The latter may promote the necessary cooperation between and coordination among the involved national and international parties. Finally, Section 5 concludes the paper and summarizes the main implications for policy.

2. Method

To analyze the positive and the negative implications of past developments on (1) systemic risks, (2) the importance of data exchange for risk mitigation, and (3) suitable technologies for facilitating the requirements of such data exchange, we conducted nine semi-structured interviews with experts in the field of systemic risks, resilience, and data exchange in electricity systems. We chose to conduct interviews based on studied academic literature as there is an absence of appropriate data within the domain of our research. Table 1 features an overview of the experts. Overall, we interviewed experts from six different companies and research institutes. We selected the experts both through scientific exchange and through our extensive personal and professional network. Owing to the focus of our research on the intersection between systemic risks in electricity systems and information systems with specific characteristics, such as a high degree of reliability or the protection of sensitive data when sharing information, we set an interview focus depending on the respective interviewees' area of expertise. For example, in our interviews with practitioners from TSOs, we mainly discussed how data exchange can help to detect systemic risks and what the functional requirements are from an electricity-system perspective. In the interviews with experts from the technical domain, we then aimed to shed additional light on which information systems tools can actually provide these capabilities. Accordingly, some of the interviews only took 30 min, whereas others lasted up to 1 h. We believe that through setting a focus on the interviewees' expertise, we captured the relevant statements to evaluate the arguments we pulled from our review of literature on recent developments and systemic risks in electricity systems.

To ensure the comparability of the statements of the respective experts, we conducted semi-structured interviews, as is standard practice in qualitative research (Schultze and Avital, 2011). In this way, we could collect relevant statements and strengthen the arguments that we pulled from our review of literature on recent developments and systemic risks in electricity systems. Correspondingly, we asked the experts where they see changes in systemic risks in electricity systems and what their root causes are. Moreover, we asked the experts whether, and if so, about how future data exchange between numerous market parties can be designed to mitigate systemic risks. Finally, we asked the experts – particularly those from TSOs – what guidance and decisions they would recommend to policymakers to encourage such data exchange. Overall, we found a broad agreement of the experts on our findings from reviewing academic literature. All of them acknowledged both the positive and negative implications of the three core developments for systemic risks as well as the expected benefits of improved data exchange. Nonetheless, owing to their different professional background, some experts emphasized specific aspects that we explicitly want to present in our work. Therefore, throughout the paper, we highlight such statements explicitly. Not mentioning an expert when pointing out an important message in our paper does not mean that the remaining experts argued against this statement, but rather that they did not put an explicit focus on this topic during the interview.

Table 1
Overview of the experts that we interviewed.

Expert	Area of Expertise/Professional Field of Activity	Years of Experience
#1	Team lead system operations and data flows, TSO	>5
#2	Project lead energy data, TSO	>25
#3	Freelancer involved in several European initiatives for data exchange & management between TSOs	>10
#4	Researcher on electricity systems, Research institute	>5
#5	Researcher on electricity systems, University	>4
#6	Researcher on decentralized digital technologies, Research institute	>3
#7	Researcher on privacy-enhancing technologies and electricity systems, Car manufacturer	>2
#8	Researcher on decentralized digital technologies and digital identities in the energy sector, Research institute	>2
#9	Team lead system operations and data exchange, TSO	>10

3. Systemic risks in electricity systems

Systemic risks have traditionally been analyzed in finance (Acemoglu et al., 2015; Acharya et al., 2017; Angelini et al., 1996; Billio et al., 2012; Haldane and May 2011; Kaufman and Scott, 2003). Research defines a systemic risk as the risk of a collapse of a substantial part of a system that induces cascading effects in most or all parts of the system, which results in the breakdown of the whole system (Berizzi, 2004; Kaufman and Scott, 2003). This is in contrast to the risk that a single component collapses without leading to a system breakdown. We note that there is literature that considers systemic risks in various systems, among others also in whole energy supply systems (Lucas et al., 2018; Renn et al., 2020). Research with a particular focus on systemic risks in energy systems often takes a finance- or economics-related perspective: for instance, Kerste et al. (2015) pose the question of (financial) regulation, Lautier and Raynaud (2012) analyze derivative energy markets, and Reboredo (2015) and Du et al. (2019) reflect on the specific role of oil for whole energy systems. In addition, for instance, Berizzi (2004) and Ezzeldin and El-Dakhakhni (2019) analyze systemic risks in electricity networks from a broader perspective, focusing on specific events and in the electricity network of a single country. Furthermore, there is a whole research stream in engineering science dealing with issues of blackouts and resilience from a technical perspective (Lee et al., 2019; Meng et al., 2017; Saleh et al., 2015).

In our study of related work, we found a lack of research that specifically analyzes current technical, regulatory, and market developments in electricity systems from a system perspective and that draws a holistic view of their impact on systemic risk. Neither did we find literature that points out the challenges or corresponding solutions to tackle these issues. With this paper, we aim to close this gap by combining insights from the field of electricity systems and the field of information systems to draw on the perspective of digital technologies for managing systemic risks in electricity systems. Here, we also note that there is research from the information systems discipline that reflects digital technologies to tackle systemic risks, for instance, in complex networks outside the area of electricity grids (Fridgen et al., 2019; Gozman et al., 2020; Lorig et al., 2019). It is also noteworthy that there are first policy-driven initiatives, e.g., from the EU or ENTSO-E with respect to a purposeful electricity data exchange to increase resilience.

Taking a system-wide perspective is important to reflect and mitigate the impact of potential triggers of systemic risks and to design solutions that make the system more resistant against cascades of failures. Based on literature, ongoing discussions among practitioners, and the expert interviews that we conducted, in the following we present developments in European electricity systems that may already have contributed or will contribute to a change in systemic risks. In line with clusters obtained from the topics discussed in the expert interviews, we group these developments into three categories, cf. Sections 3.1, 3.2, and 3.3.

3.1. The electricity market liberalization and the unbundling of traditional electricity supply chains

Starting in the 90s of the last century, energy sectors have transformed from vertically integrated monopolies to liberalized systems with lots of different and independent market players. Given the corresponding unbundling, electricity markets have come into being, with only the transmission and distribution level remaining highly regulated in European countries (Grimm et al., 2016a, 2016b; Weibelzahl, 2017). Typically, the electricity system is now operated in a rather decentralized way by many stakeholders on different levels of the electricity supply chain. For example, there are more than 1000 public utilities acting as distribution system operators in Germany alone, whereas most of them also run their own generation assets and backup facilities. Moreover, long-run system expansions are the outcomes of complex and iterative public decision, planning, and approval procedures involving various authorities (Buijs et al., 2011). Independent market parties, e.g., generation firms, industrial companies, traders, or balance responsible parties, compete on different electricity markets, including day-ahead, intraday, and balancing markets. These firms operate their own electricity generation facilities with the help of modern information and communication technologies in the short run and determine their capacity investments based on expected market profits in the long run (Grimm et al., 2016a).

Following market liberalization and corresponding market design decisions, the dispatch of power plants is, therefore, now governed by market-price signals and no more by an integrated, public company. This development clearly led to considerable improvements in terms of efficiency and robustness through diversity, specifically when entities were “too big to fail” (Expert 1). Nonetheless, besides these benefits, Experts 2, 4, 5, and 9 stated that a fragmented market with numerous different market players may also increase systemic risks. Individual stakeholders’ profit orientation, together with the lack of a holistic perspective of private firms on overall system stability, poses the question of how to align the individual behavior of the various players such that economic incentives represent system stability needs. Especially in the case of multiple interacting and typically imperfect markets, a high complexity arises where individual firms may not necessarily be aware of the underlying and possibly growing systemic risks, which they may also contribute to. Expert 9 also mentioned that in the current environment, with a large number of potentially responsible market parties, it is difficult to find the right contacts within an acceptable timeframe to reconcile corresponding activities to ensure system stability.

One example for misalignment in terms of complex and incomplete market design is the following incident: incorrect forecasts for photovoltaic feed-in on December 14, 2018 triggered rapidly increasing prices on the German intraday market. In a well-designed market, this should have led to a decreasing electricity demand such that balancing power could handle the remaining system imbalance. However, a mis-designed market mechanism has led to a situation where the maximum balancing electricity price at this time was lower than the intraday price. Therefore, it was more profitable for individual market participants to use standard power reserves instead of trading on the intraday market; see Preiβ (2019). Ultimately, many large consumers in Germany had to be taken off the grid to prevent a blackout as both the secondary and the minute control power were crucially exhausted.

Several experts also emphasized in our interviews that liberalization and unbundling per se need not necessarily contribute to an overall increased systemic risk but that the current pace of this development does not allow necessary adjustments in terms of data exchange and market design in the appropriate timeframe. This indeed leads to an increase in systemic risks, which can be mitigated by, among other things, better data exchange between individual companies, some of which are in competition with each other. According to Experts 2, 5, 6, 7, and 9, it is particularly important to consider the protection of competition-relevant data and to pay attention to consumers’ privacy when designing improved data exchange.

3.2. The transformation towards a decentralized energy system based on RES

Within the energy transition, the share of RES grows steadily in many European countries (Trancik, 2014). In contrast to the past, where a few conventional power plants centrally supplied consumers, nowadays a major share of electricity is generated by many smaller plants that are highly spatially distributed (Nguyen, 2007). These small-scale plants are also run by small businesses or even households that act as prosumers, i.e., their role switches between consumers and producers of electricity (Fridgen et al., 2021; Parag and Sovacool, 2016). This development further increases the number of players and corresponding complexities described in Section 3.1.

Moreover, RES generation is exposed to uncertain daily and seasonal

weather patterns. With the increase in RES generation, electricity systems are therefore also experiencing a growth in the demand for system flexibility, e.g., in terms of demand response, that is, the short-term adaption of load profiles, following market price signals (Hanny et al., 2022; Heffron et al., 2022; Palensky and Dietrich, 2011; Papaefthymiou et al., 2018). In this context, flexibility is a crucial prerequisite for inter-temporally balancing demand and supply on the system level (Heffron et al., 2021). The corresponding new market players that can supply flexibility on existing markets include flexible consumers or standalone storage facility operators (Haupt et al., 2020; Körner et al., 2019). Ultimately, these developments yield an even more fine-grained, multi-party market environment with additional complexities, dependencies, and interconnections (Schott et al., 2019). In the near future, this complexity and the number of involved market parties will further increase with the integration of millions of households and small assets that are currently 'behind the meter' (Strüker et al., 2021). According to Experts 2, 3, 4, and 9, this will make it necessary to develop processes and standards for the exchange of generation, grid, and market data between consumers and distribution system operators (DSOs) on the one hand, and between TSOs and DSOs on the other hand.

On the grid level, the described decentralization of RES generation leads to a growing demand for additional transmission capacity, i.e., spatial flexibility, to carry electricity over larger distances (Neuhoff et al., 2013). Existing electricity networks were typically not designed for systems with a high penetration of decentralized RES (Krewitt and Nitsch, 2003), which led to optimizations that make the grid dependent on the functioning of power electronics devices (Experts 1 and 9) (van der Welle et al., 2015). Multiple injections and withdrawals of electric power also increase complexity and lead to a large number of bidirectional electricity flows that challenge system operation. Here, Experts 1, 2, and 4 emphasized that the main challenge for system operation is the speed at which these changes are under their way. Therefore, ensuring system stability, frequency, and voltage control as well as congestion management become increasingly important but also highly complex and challenging tasks for grid operators and policymakers. While the number of active and decentralized market parties will increase in the future, it is necessary to define standards in terms of communication and data exchange between market parties to give a holistic overview of the system's current state and to mitigate a cascading collapse in electricity networks. When it comes to households, Experts 5 and 8 mentioned that privacy-oriented data exchange may be of particular relevance.

3.3. Increased sector and inter-regional coupling

All experts mentioned that sector coupling as well as the inter-regional coupling of national electricity networks are at first hand commendable trends that provide many benefits. Moreover, some measures against this coupling like the ability for "island mode" have already been taken, as stated by Experts 1 and 3. However, all experts consent that these trends, on the other side, increase system complexity considerably. The following paragraphs describe the two trends and illustrate how they may increase the threat of cascading failures in the sense of systemic risks.

Being an enabler of core processes in almost all sectors, e.g., in manufacturing industries, in public facilities such as administrative buildings or hospitals, in communication, and in the transportation sector, which is targeted to rely largely on e-mobility in the future, a stable electricity supply system is a crucial backbone for a country's economy (Heffron et al., 2020). The well-functioning of many sectors depends to a large extent on their access to a reliable electricity system, which yields complex dependencies. Sector coupling implies the electrification of energy-consuming sectors (Brown et al., 2018; Fridgen et al., 2020a). One purpose of sector coupling is to provide more flexibility with respect to both electricity generation and electricity demand: In times of low electricity generation, electricity-demanding sectors may contribute to system stability by consuming less electricity or even feeding in electricity by re-converting stored energy with power-to-X technologies. In contrast, in times of high electricity generation, electricity-demanding sectors may contribute to system stability by consuming more electricity, possibly serving as a power-to-X technology that enables the storage of surplus electricity (Fridgen et al., 2016; Lund and Kempton, 2008). However, this also results in a significantly more complex electricity network, where failures in one sector may propagate to others, as they are directly connected. An illustrative example may be the case of e-mobility that couples the sectors of electricity and mobility through both physical and business connections. While digital-enabled concepts like smart charging hold unique potentials for grid stability, one may also reflect these connections as a possibility to convey shocks from one sector to the other. Hence, one may also consider a trigger in e-mobility as a trigger for systemic risks in electricity systems.

Concerning the inter-regional coupling, a growing number of international cooperation initiatives aim at increased electricity trading between countries, with a prime example being Europe; see, e.g., Gnansounou and Dong (2004). In particular, corresponding initiatives try to foster competition and facilitate a more stable and reliable system with, for instance, smoothing effects and a higher number of backup generation capacities (Schipper and van der Vleuten, 2008). For instance, the Pan-European market with around 40 different TSOs that act in a highly inter-connected electricity system clearly demonstrates the new system size. Regarding congestion management and stable system operation, an increased interconnectedness of national electricity systems is typically associated with significant growth in the number of loop and transit flows (Hutcheon and Bialek, 2013). Loop flows, both within and between countries, must be constantly monitored and controlled through the exchange of grid-related data and corresponding forecasts in order to avoid the overloading of individual transmission lines, which may then propagate through the coupled system (Baldick and Kahn, 1997). Our interviews endorse that it is crucial for system stability to share respective information among all the players that feed in or withdraw electricity from the coupled system to appropriately calculate these flows.

To give a current example of a systemic risk under inter-regional coupling, a malfunction of a Croatian transformer station almost pushed the European electricity system to its limits on August 01, 2021: To stabilize the grid frequency, some countries had to be temporarily disconnected from the European interconnected system. Additionally, disconnectable loads in France and Italy, electricity imports from northern Europe, and a controlled ramp-up resp. ramp-down of conventional generation plants contributed to solving the critical situation. Due to the disconnection of some countries, up to 6300 MW of electric power were missing in the north-western part of the European system. Again, this example suggests that it is necessary to establish standards for communication and data exchange between sectors and market parties and between national TSOs that had no direct connection before to enable purposeful network operation in an increasingly complex system.

3.4. Arising systemic risks in modern electricity systems

The previous sections illustrate that European electricity systems are currently undergoing far-reaching structural changes. Against this background, we consider the three developments in electricity systems outlined above as relevant for business and policy. For example, transforming the traditional supply chain involves splitting and, where necessary, reassembling businesses, as well as re-forming and implementing data and information flows between businesses that are now in a new relationship to each other, e.g., in economic competition. Also, the increasing share of decentralized RES, sector coupling, and inter-regional coupling of national electricity systems may change profit opportunities and incentives. Accordingly, all of these developments require an adjustment of market design, which must account for these changes and which may affect underlying systemic risks (Fridgen et al.,

2020b).

In addition to intended changes in business and regulation, the increasing digital transformation plays a decisive role in the context of systemic risks: Digitalization speeds up the developments that structurally transform electricity systems, but it may also provide solutions to tackle arising risks (see Section 4). In this light, electricity systems themselves become increasingly dependent on electricity, as control mechanisms and systems heavily rely on digital services that require electricity to run and communicate (Buldyrev et al., 2010). The blackout that spread from Switzerland to Italy in 2003 only grew to such an extent because a series of cascading effects caused the shut-down of electronic control systems of the electricity network themselves as they did no longer have power to run properly. Accordingly, backup generators must be provided for TSOs' critical control system units (Expert 1).

At the same time, the developments described above require an adjustment of information flows, i.e., an adequate cooperation and data exchange, to mitigate systemic risks and to avoid taking away the global perspective from established approaches of managing systemic risks. The situation in Germany in June 2019 represents a real-world example of a systemic risk due to insufficient data exchange or analyses among market parties as well as market and system operators: As mentioned above, there were significant shortfalls in the balance of the German electricity system of more than 6000 MW on June 06, 2019, of almost 10,000 MW on June 12, 2019, and of more than 6000 MW on June 25, 2019 resp. June 26, 2019 (50 Hertz et al., 2019). On these days, the German TSOs, among other measures, had to fully activate their control reserves and request emergency reserves from foreign countries to prevent a black-out. In their report (50 Hertz et al., 2019), the German TSOs found that – in addition to uncertainties in the feed-in forecast on June 06, 2019 and June 12, 2019 – the balancing group managers reacted to high intraday prices with short-term, within-day schedule changes on all three days, while the market incentive for balancing group obligation was low owing to the corresponding pricing procedure. The German TSOs conclude that to a considerable extent, improper short selling by balancing group managers led to the strong imbalance in the electricity system. We argue that it will help system operators to monitor and analyze information about the planned schedule changes from the balancing group managers proactively in quasi real-time to prevent such events in the future.

In particular, the experts agreed that a fundamental precondition for successful risk and crisis management and for effectively preventing and managing such events is the availability of reliable and up-to-date data on the infrastructure, local production and demand, contractual delivery agreements, corresponding forecasts on expected network congestion, as well as general generation adequacy. In times of the electricity system transformation with an increasing number of decentralized RES plants, growing system complexity, and highly fluctuating generation, the available data is typically outdated very fast. In consequence, there is the question how to collect, update, exchange, and synchronize the required data appropriately as mentioned by Experts 1, 2, 3, and 9. For example, in the EU there are first regulations to publish transportation-, generation-, and consumption-related data and to inform the public, for instance, the ENTSO-E Transparency Platform for the pan-European market (Hirth et al., 2018). Additionally, also first EU-regulations for data sharing with respect to network operation have emerged, e.g., the System Operation Guidelines (European Union, 2017). However, these regulations may not be sufficient for a necessary global systemic risk analysis, since stakeholders may not always be willing to provide information that helps to detect risks. The relevant data is often competition-relevant or personal, making cooperation challenging in practice. To enable such a data exchange nonetheless, Expert 9 emphasized the need for appropriate economic incentive structures for market parties to share their data with others, and Expert 7 suggested to consider privacy-enhancing digital technologies.

Hence, the following Section 4 sketches digital solutions on how to exchange competition-relevant information among market parties to mitigate systemic risks. We aim to provide a perspective on possible ways to promote the cooperation concerning relevant electricity system data provision and exchange by (1) increasing current efforts, e.g., in the EU, and (2) setting up new solutions on a green field.

4. On the potential of digital technologies for data exchange

The above section highlights the need for an adequate information exchange to regain a global view on the state of the electricity system as well as to allow for corresponding system analyses and forecasts. As a managing director for data availability at a European TSO, Expert 9 emphasized that "the only way to solve the issues and bring more dynamics and opportunities is to unlock data, making sure it is available at the right place and the right time." In this context, especially recent advances in digital technologies may foster the necessary provision, synchronization, and sharing of system-relevant data on a trustworthy and secure basis. In the following, we will therefore describe potential approaches for data exchange in line with insights we gained from the interviewed experts to mitigate systemic risks.

4.1. Centralized and decentralized architectures for information exchange

In Europe, stakeholders such as TSOs and DSOs are currently investigating the opportunities for increased information exchange based on a centralized platform. In a corresponding report, Jenssen et al. (2017) highlight the challenges of the energy transition and the resulting necessity for improved coordination and cooperation among TSOs and DSOs in Europe, in particular across national borders. In this context, a common data exchange platform may be an essential tool for improving coordination and market functionality across borders and thus to exchange data that is necessary to investigate and uncover systemic risks (all experts). Table 2 lists some specific types of data that such a joint platform can provide for improving the identification of systemic risks and reconciling countermeasures. Experts 2, 3, 4, and 5 specifically emphasized that these are, among others, market data like contractual agreements, auction results or prices coming from stock exchanges, weather forecasts and maintenance schedules for predicting the future generation and consumption, and data on the current supply and demand of flexibility from aggregators, utilities, or balance responsible parties. Moreover, Experts 1, 3, 4, and 5 explicitly mentioned that real-time data concerning the status of the grid provided by TSOs, DSOs, and responsible agencies is necessary for system operation.

Concrete measures and metrics for a corresponding risk assessment and analysis can, for instance, be found in Jenssen et al. (2017). In Europe, the model of jointly creating trusted institutions has already succeeded in many areas as, for instance, the establishment of the European Central Bank illustrates in the financial sector. However, owing to neutrality and reliability considerations – as mentioned by Experts 4,

Table 2
Selection of relevant data for systemic risk management.

Group	Owner/Provider	Examples
Generation	Utilities/suppliers, prosumers	Schedule, maintenance, irregularities
Consumption	Utilities/suppliers, prosumers, industry	Current and expected demand
Market	Stock exchanges	Contractual agreements, auction results and current or forecasted prices, volatility, anomalies
Flexibility	Aggregators, utilities, balance responsible parties	Current flexibility reserves
Weather	Forecasting services, measuring devices	Local cloudiness, wind strength, air temperature, expected thunderstorms
Grid	TSO, DSO, responsible agencies	Real-time frequency, electricity line temperature, planned maintenance and expansions, known outages

6, 7, 8, and 9 – and to the sensitivity of the information involved – as mentioned by Experts 3, 4, 8, and 9 –, some cases may require a more decentralized approach. This indicates that despite the undisputed advantages of a centralized solution in terms of simplicity and efficiency, there are good reasons that prevent the relevant stakeholders from agreeing on a platform operated by a single, trusted institution. As one of the main reasons for the hesitation to exchange relevant data, the involved players may have too little confidence in this institution that would collect enormous amounts of data and control the access to it, or they may fear that their data could be used against them. This may also hold for public entities like system operators, where foreign countries or terrorists may misuse data. Even if all participants of a coupled network were to agree that a central authority would generally result in a win-win situation for the involved participants by being able to coordinate and monitor their systems as well as hidden risk agglomerations, this authority would be given a central market role and in consequence potential market power. Such a potential monopoly would always involve risk for countries and corresponding aversion or a need for very strict regulation that can slow down needed activities. As electricity is of high strategic relevance from a political and economic perspective, national governments may hesitate to accept an authority from another country to monitor or even control considerable components of their national system. Moreover, if the availability of a centralized service is essential for the functioning of a critical infrastructure, this also raises security concerns: Using a centralized platform is "paradox", because it could become a systemic risk in its own (Expert 6).

Modern digital technologies can provide the necessary tools to facilitate the exchange of data and even collaboration between multiple parties also in a more decentralized way. In the following, we will elaborate on how decentralized identity management based on public key infrastructures and digital certificates – also known as self-sovereign identity (SSI) – and blockchain or, more generally, distributed ledger technology, combined with privacy-enhancing computation, can improve current risk management by addressing some of the described challenges. Blockchain technology in specific is frequently mentioned in the context of trust; yet discussing trust in all details is beyond the scope of our paper. Investigating to which extent trust – as a notion of encapsulated interest (Cook et al., 2005) – is already present between TSOs and other system operators that follow similar goals and aim for long-term relationships when considering electricity system stability and the mitigation of systemic risks may be a promising avenue for future research. For example, Experts 2 and 9 pointed out that personal bilateral communication through phone calls and general confidence in other system operators' competencies already facilitate a certain degree of trust. Nonetheless, in the future, it may become more relevant to split the two core reasons for coordinated action: (1) an individual perspective through economic incentives and (2) trust-related actions from the perspective of encapsulated interest. Fig. 1 summarizes the technologies on the communication, storage, and data processing layer that we will briefly introduce and compare in this section. The alternatives on the data storage and processing layer may well be combined depending on the reliability and confidentiality requirements of specific types of information or operations.

Leveraging decentralized technologies for managing digital identities of the electricity system's components can already help to address several challenges on the communication layer: According to the IT security company esatus AG, "the massive increase of infrastructure digitalization also harbors a growing risk of incidents with equally devastating consequences: hacking threats, compromise in data confidentiality and/or integrity and availability" (esatus AG, 2021). Consequently, every component of the electricity system whose functionality considerably contributes to the stability of the overall system should be secured individually, cf., zero-trust architectures (Buck et al., 2021), and the more important the component, the higher security is needed, cf. risk-based authentication. It is essential that the digital access to these components is only possible through authentication with a high level of assurance, and that no single failure or compromise of a component can lead to a cascade of security incidents that ultimately can cause a local or even a large-scale blackout. Experts 3, 7, and 9 mentioned that a decentralized management of the digital identities of units and stakeholders in the electricity system, based on a Public Key Infrastructure (PKI) that is already used in several domains and certification could help here (TenneT, 2021), particularly as the automated verifiability of identities and their data in real time (Expert 8) and corresponding

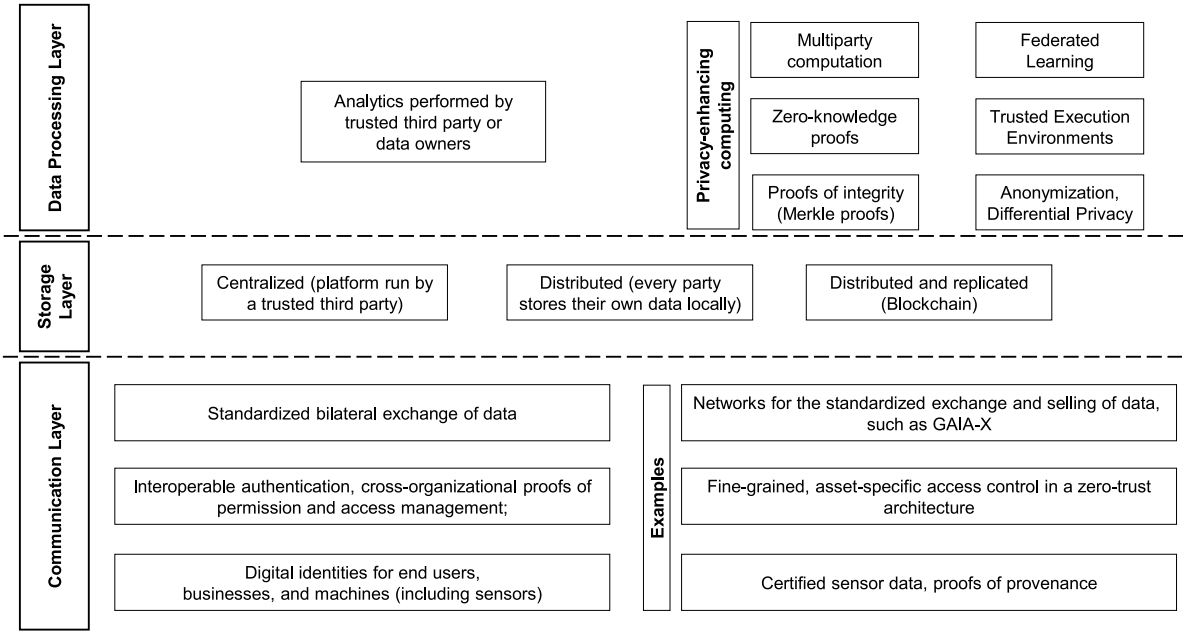


Fig. 1. Overview of digital technologies that can be used for the communication, storage, and privacy-oriented processing of data to detect systemic risks in electricity systems.

accountability (Expert 9) is required also for information from "behind the meter" (Expert 3). Expert 9 even noted that "if you cannot verify identity, then you can as well throw away the data". Emerging ecosystems for digital identities for humans, institutions, and things often use blockchains instead of certificate authorities for anchoring their public keys, which aims to increase tamper-resistance and availability and provides an alternative in cases where stakeholders have difficulties in agreeing on one or few certificate authorities (Sedlmeir et al., 2021a).

Using such a common, decentralized PKI and corresponding governance frameworks can also be leveraged to foster the bilateral exchange of data between entities in the electricity system: With digital certificates, parties' eligibility of data access can be decided based on roles and permissions that can be verified across organizations. One notable approach here are the dataspaces that are currently being discussed for playing a major role in the European cloud initiative GAIA-X (German Federal Ministry for Economic Affairs and Energy, 2021; Otto et al., 2019). By providing standardized components and policies through which data can be exchanged between different stakeholders via "dataspace connectors", they can foster the bilateral and authenticated exchange of data, coordinating the processing on distributed data sources with no or low degree of replication. Consequently, these dataspace connectors are also being considered for the exchange of information between stakeholders in electricity systems, as highlighted by Expert 2. Nevertheless, while the bilateral exchange of data is an important ingredient for better collaboration between stakeholders with respect to addressing systemic risks, there is also a need for computations (for instance, total expected consumption or generation) on data that are collected from many sources. Moreover, for multi-stakeholder processes in which there is also a high need for public auditability of which data is being exchanged, data storage and processing require additional coordination.

As previously described, centralized data collection and storage is highly efficient, but not a viable option for every scenario. For cases that need broad market transparency or the redundant storage and operation of data, blockchain technology may be a useful building block. A blockchain (or more generally, a distributed ledger) can provide all the capabilities of a centralized IT platform, such as authenticated transactions, tamper-resistance, and the enforcement of business logic, with high availability and integrity guarantees and, in particular, without the need for a distinguished entity that operates the platform, thus removing extra influences that a centralized operator could impose on the system (Experts 6 and 9). A blockchain achieves consensus between the participants by ensuring an append-only structure that prevents ex-post modifications (Butijn et al., 2020). Consensus can also be achieved for the execution of code: Smart contracts are scripts that are redundantly executed by every DLT node and may be useful to trigger events or even enforce specific and foreseeable measures in critical electricity grid situations. A built-in PKI implements authorization. There are permissioned and permissionless blockchains – in the former case, only entitled users can participate, i.e., read and write on the blockchain, whereas in the latter case, any node of the network can participate. Various types in-between exist. Against this background, blockchains could take on the role of a central authority, which would be necessary to uncover and deal with systemic risks that may be hidden from an individual perspective (Fridgen et al., 2019). Utilizing blockchain-based solutions is already being discussed and tested in the financial sector for optimizing supervision processes and faster detection of systemic risks (Gozman et al., 2020). Yet, Expert 7 noted that for some of these properties, replication alone can already be sufficient.

4.2. The need for privacy-enhancing technologies

The key challenges of blockchain arise from its main strength, namely the high degree of availability and transparency through the replicated and synchronized storage of data and execution of code (Kannengießer et al., 2020). This means that every participant in the blockchain system sees identical data and performs the same computations. While there are blockchains that permit private data and partially private smart contracts, e.g., Hyperledger Fabric and Quorum, this also implies that the data which these smart contracts can work with, or the degree of redundancy that was initially desired, will decrease. Hence, it appears that the higher the degree of privacy that is required for a blockchain transaction, the lower the number of participants that can access the data, and consequently, that can ensure availability and verify computations on it. Consequently, insensitive data can be directly stored on a blockchain and benefit from the additional utility that its transparency and availability provide. For sensitive data, however, additional privacy-enhancing techniques need to be used. The integrity of data can still be proved to participants using a hash value that has been stored on-chain instead of the original data. Convincing a larger number of nodes that a computation has been executed correctly, or that private input data from several participants has been aggregated in the right way, however, seems difficult without disclosing the data. Experts 4, 6, 7, 8, and 9 noted that the sharing of sensitive information about end users' master data, contracts, and real-time consumption is already often problematic when data is shared only bilaterally, and when storing the data on a blockchain, this challenge is exacerbated. While in some cases, obtaining consent or anonymizing data through removing highly personal information and adding noise through differential privacy techniques is feasible as stated by Experts 3, 4, 6, 7, and 9, re-identification and sophisticated analyses as well as regulatory aspects like the GDPR's "right to be forgotten" pose specific challenges for processing information on a blockchain (Schellinger et al., 2022). Expert 4 also suggested to use federated learning that is often combined with differential privacy or blockchains (Rückel et al., 2022).

More complex privacy-enhancing cryptographic techniques like fully homomorphic encryption, trusted execution environments, and zero-knowledge proofs (ZKP) may also help to address these challenges (Expert 8) (Birch, 2021) and provide utility and public auditability without exposing confidential information (Zhang et al., 2019): They can help overcome the so-called copy-problem, where providing data to other parties automatically implies that these parties can copy, store, and even distribute it (Garrido et al., 2021). For example, ZKPs allow a single party to compute on their data locally and only display the result of the computation, including a proof of the computation's correctness that can be verified by all other parties at low computational effort. ZKPs have become a highly valuable tool in blockchain applications and particularly in decentralized finance for providing privacy, i.e., the private data does not need to be shared, and for scalability, i.e., the verification of the proof grows significantly less than the complexity of the original computation (Ben Sasson et al., 2014; Ben-Sasson et al., 2018; Buterin, 2021). So far, their main application can be found in cryptocurrencies and in particular Decentralized Finance on Ethereum, but they are increasingly researched also for use cases in the energy sector, such as electricity labeling (Sedlmeir et al., 2021b). In the context of electricity systems, ZKPs may, for example, be used to demonstrate that the forecasted and realized consumption of a party coincide up to a certain threshold, without the party revealing the forecasted and consumption data in non-obfuscated form (Expert 6). Provided a sophisticated digital identity for units and devices, as currently explored in a pilot in Germany (Future Energy Lab, 2021), a ZKP can even demonstrate that the data to which the computation refers has been signed by a certified sensor. If no cryptographic root of trust is available, at least one can prove that the computation was conducted on data that has been publicly committed to earlier via a hash value on a blockchain.

Generating a ZKP requires that the entity that generates the proof can access all the data that is required for the computation for which correctness must be verified (Buterin, 2014). If this is not possible, e.g., because a computation requires the confidential input of several parties, once a PKI, and hence, authenticated end-to-end encrypted communication channels between parties and a platform for displaying public data is established, this provides a natural infrastructure for multi-party

computation (MPC). MPC is a special kind of computation performed by an ensemble of parties in which cryptography is used to ensure that every participant only knows his/her own input but can still be convinced that the joint computation that uses the inputs from all the other participants in the system was performed correctly. In fact, first MPC protocols that are coordinated through a blockchain to add transparency and integrity guarantees to the joint and private computation have been implemented recently for decentralized exchanges on a cryptocurrency (Li et al., 2021). Experts 3 and 7 noted the advantages of MPC and that its use has also been explored by TSOs among other options like trusted execution environments and federated learning, even though, currently for many practical purposes it is still complex to use, specifically when the degree of digitalization is still low.

To illustrate the concept behind MPC in a very related, though simplified example, consider the case where several (in this example, three, however, generalization to more than three is straightforward) market parties have private information on some system-relevant capacities or, e.g., production schedules, at some point of time. We denote the three involved parties by A, B, and C. The associated capacities of the three parties are a, b, and c. Each party does not want to give its information to any of the other parties because they regard this information as competition-relevant information (cf. Section 3.4). We assume that the three parties want to evaluate the aggregated capacities of a coupled electricity system to detect possible under-capacities that may cause some risks. In this example, the three parties can proceed as follows[1]: Party A first generates a random number r in a sufficiently large range and gives $r+a$ to party B. In turn, party B adds its own number b and passes the result to party C, which then adds c and arrives at $r+a+b+c$. This subtotal is subsequently forwarded to party A, which is the only party, which knows r. Party A can then subtract r from the last subtotal and gets the desired result $a+b+c$. Finally, A communicates this sum to the other parties. Note that this protocol makes sure that no single party can draw any conclusions about the others' individual and private inputs. Consequently, none of the three parties gets any additional information apart from the final sum $a+b+c$ unless they conspire with another party. Also, no central authority is needed to perform the protocol. Even though the example is quite simple, it gives an illustrative way of describing the main idea behind MPC. In its standard version, "curious-but-honest" participants are assumed. More advanced problems often employ further mechanisms such as permuting the roles of A, B, and C to detect potential misbehavior by checking whether the result is the same for each permutation, or ZKPs to enforce each party's correct behavior.

Using MPC may also avoid that the increased transparency offers new possibilities for attacking the system if underlying information falls into the "wrong" hands and is misused by, e.g., (cyber) terrorists. Ultimately, such concepts can ensure that system-relevant information can be constructed for crisis management. MPC has already been suggested for other areas in which collaboration or coordination is necessary, e.g., in an environment exhibiting some degree of mutual distrust, such as the detection of bottlenecks and monopolies in supply chain networks (Kerschbaum et al., 2011). Without any doubt, real-world applications of MPC will be much more advanced and will require further research. However, also for rather complex questions, such as the detection of systemic risks in supply chains, a specific solution based on MPC has been proposed by Zare-Garizy et al. (2018), illustrating that also complex MPC protocols are already viable. Also for determining collision paths of satellites jointly by military opponents, the viability of MPC could already be demonstrated (Kamm and Willemson, 2015). In the context of the critical electricity system situation in Germany in 2018 and 2019, MPC may have provided an opportunity for balancing group managers to contribute their competition-relevant information about planned schedule changes confidentially into a system-comprising computation of generation shortages or grid congestion. Other areas where MPC could prove useful is the joint computation of some overall measure for resistance/impedance of grid infrastructure, or the aggregated capacity of balancing power.

[1] This example was inspired by Schneier (1996).

5. Conclusion and policy implications

While electricity systems are traditionally exposed to systemic risks, different developments on the national and global stage have led to significant growth in system complexity. Amongst others, these developments comprise (1) electricity market liberalizations, (2) the transformation towards decentralized RES, and (3) increased sector and inter-regional coupling. Especially, new digital technologies have speeded up business processes and, thus, boosted the opportunity for, e.g., sector-coupling. Ultimately, all of the three described developments have contributed to a beneficial shift from traditional electricity supply chain structures towards interacting electricity supply networks. In this paper, we argue that these developments represent a two-sided sword: Owing to growing system complexity and interconnection, there may be hidden systemic risks that are associated with a faster spread of local failure. Individual players are typically not aware of the hidden risks, which is why, in the worst case, they may even contribute to increase these risks. Therefore, responsible policymakers must take these risks seriously and search for effective actions.

In line with the interviews that we conducted within this paper, we call for further collaboration and coordination with respect to relevant data collection, provision, and exchange to be able to construct a "global picture" of the current state of the system. The current endeavors in committees, such as ENTSO-E, is without any doubt a highly valuable first step, and such efforts need to be intensified and expanded if systemic risks are to be adequately addressed. The experts we interviewed especially emphasize that policymakers must now urgently provide impetus so that standards can be defined and implemented. In this context, developing and implementing appropriate economic incentive structures for market parties to exchange data with others is clearly among the issues to be addressed by policymakers as soon as possible.

We also argue that the simplest solution to obtain the required comprehensive information would be a centralized IT system. However, such a system might be challenging to implement due to economic and political reasons, such as the threat of the new platform being a systemic risk on its own, leading to a data monopoly, or the exchange of sensitive information about a critical infrastructure with other countries. Digital technologies such as self-sovereign identities and blockchain offer the opportunity to exchange data and even to enforce the business logic in decentralized architectures and should be combined with privacy-enhancing technologies like ZKPs and MPC to improve collaboration among the involved market parties without raising data privacy issues and to additionally contribute to security that ensures a more integrated management and control of systemic risks. Ultimately, this may support the secure integration of more RES and, thus, jointly tackle climate change.

For a better understanding of underlying risks and their interdependencies, there is a need for additional research. In the light of ongoing sector-coupling, future research may consider "entire" energy systems, of which electricity systems will become an increasingly important part. In particular, to validate our conclusions, we call on future research to investigate data exchange in light of systemic risks more quantitatively using, for instance, simulation studies. Furthermore, we argue that due to the global nature of systemic risks, collaboration of the involved parties to gain a holistic information on the system state is necessary to help researchers and institutions localize systemic risks and identify concrete countermeasures. In the case of the EU, looking at the European GAIA-X initiative in which the capabilities for exchanging data bilaterally between organizations are being created, and the European Blockchain Service Infrastructure that targets at facilitating multiple blockchains on which member states can cooperate,

first attempts for setting up an infrastructure that might also help to tackle systemic risks in electricity systems are already being made. Combining these decentralized technologies with privacy-enhancing computing to prove or aggregate necessary information involving multiple stakeholders might be a promising direction for the electricity system and requires further research at the interface of decentralized identity management, distributed ledger technologies, cryptography, and systemic risk mitigation in electricity systems.

Disclaimer

The views expressed in the paper are those of the authors and do not necessarily reflect the view of the TenneT TSO GmbH.

CRediT authorship contribution statement

Marc-Fabian Körner: Conceptualization, Writing – original draft, Project administration. **Johannes Sedlmeir:** Writing – original draft, Investigation. **Martin Weibelzahl:** Conceptualization, Writing – original draft. **Gilbert Fridgen:** Conceptualization, Supervision. **Moreen Heine:** Conceptualization, Supervision. **Christoph Neumann:** Writing – original draft, Project administration, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We gratefully thank the nine experts that shared their insights with us to make this manuscript possible. We gratefully acknowledge the financial support of the Kopernikus-Project “SynErgie” by the Federal Ministry of Education and Research of Germany (BMBF) and the project supervision by the project management organization Projektträger Jülich (PtJ). This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, grant reference “P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen” (PEARL).

References

50 Hertz, Amperion, TenneT, Transet, B.W., 2019. Untersuchung von Systembilanzungleichgewichten in Deutschland im Juni 2019. German TSOs. https://www.regelleistung.net/ext/download/STUDIE_JUNI2019. (Accessed 25 February 2022).

Acemoglu, D., Ozdaglar, A., Tahbaz-Salehi, A., 2015. Systemic risk and stability in financial networks. Am. Econ. Rev. 105, 564–608. https://doi.org/10.1257/aer.20130456.

Acharya, V.V., Pedersen, L.H., Philippon, T., Richardson, M., 2017. Measuring systemic risk. Rev. Financ. Stud. 30, 2–47. https://doi.org/10.1093/rfs/hhw088.

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., Vittal, V., 2005. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. IEEE Trans. Power Syst. 20, 1922–1928. https://doi.org/10.1109/TPWRS.2005.857942.

Angelini, P., Maresca, G., Russo, D., 1996. Systemic risk in the netting system. J. Bank. Finance 20, 853–868. https://doi.org/10.1016/0378-4266(95)00029-1.

Atputharajah, A., Saha, T.K., 2009. Power system blackouts - literature review. IEEE 2009 Int. Conf. Industr. Inform. Syst. (ICIIS) 460–465. https://doi.org/10.1109/ICIINFS.2009.5429818.

Baldick, R., Kahn, E., 1997. Contract paths, phase-shifters, and efficient electricity trade. IEEE Trans. Power Syst. 12, 749–755. https://doi.org/10.1109/59.589670.

Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., 2014. Zerocash: decentralized anonymous payments from bitcoin. In: IEEE Symposium on Security and Privacy (SP), 459–474. https://doi.org/10.1109/SP.2014.36, 2014.

Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M., 2018. Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptol. ePrint Arch.

Berizzi, A., 2004. The Italian 2003 blackout. In: IEEE Power Engineering Society General Meeting, 2004. IEEE, Denver, CO, USA, pp. 1673–1679.

Billio, M., Getmansky, M., Lo, A.W., Pelizzon, L., 2012. Econometric measures of connectedness and systemic risk in the finance and insurance sectors. J. Financ. Econ. 104, 535–559. https://doi.org/10.1016/j.jfineco.2011.12.010.

Birch, D.G., 2021. Most blockchain pitches I hear make no sense, yet I’m sure that blockchain will transform business. Forbes. https://www.forbes.com/sites/davidbirch/2021/01/17/most-blockchain-pitches-i-hear-make-no-sense-yet-im-sure-that-blockchain-will-transform-business. (Accessed 25 February 2022).

Brown, T., Schlachtberger, D., Kies, A., Schramm, S., Greiner, M., 2018. Synergies of sector coupling and transmission reinforcement in a cost-optimised, highly renewable European energy system. Energy 160, 720–739. https://doi.org/10.1016/j.energy.2018.06.222.

Buck, C., Olenberger, C., Schweizer, A., Völter, F., Eymann, T., 2021. Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust. Comput. Secur. 110, 102436. https://doi.org/10.1016/j.cose.2021.102436.

Buijs, P., Bekaert, D., Cole, S., van Hertem, D., Belmans, R., 2011. Transmission investment problems in Europe: going beyond standard solutions. Energy Pol. 39, 1794–1801. https://doi.org/10.1016/j.enpol.2011.01.012.

Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S., 2010. Catastrophic cascade of failures in interdependent networks. Nature 464, 1025–1028. https://doi.org/10.1038/nature08932.

Buterin, V., 2014. Secret Sharing DAOs: the Other Crypto 2.0. https://blog.ethereum.org/2014/12/26/secret-sharing-daos-crypto-2-0/. (Accessed 25 February 2022).

Buterin, V., 2021. An Incomplete Guide to Rollups. https://vitalik.ca/general/2021/01/05/rollup.html. (Accessed 25 February 2022).

Butijn, B.-J., Tamburri, D.A., van Heuvel, W.-J. den, 2020. Blockchains: a systematic multivocal literature review. ACM Comput. Surv. 53, 1–37. https://doi.org/10.1145/3369052.

Caiso, C.I.S.O., 2020. Preliminary Root Cause Analysis - Mid-August 2020 Heat Storm. http://www.caiso.com/Documents/Preliminary-Root-Cause-Analysis-Rotating-Outages-August-2020.pdf. (Accessed 25 February 2022).

Cook, K.S., Hardin, R., Levi, M., 2005. Cooperation without Trust? Russell Sage Foundation.

Dagle, J.E., 2004. Data management issues associated with the August 14, 2003 blackout investigation. In: IEEE Power Engineering Society General Meeting, 2004. IEEE, Denver, CO, USA, pp. 1680–1684.

Du, R., Dong, G., Tian, L., Wang, Y., Zhao, L., Zhang, X., Vilela, A.L., Stanley, H.E., 2019. Identifying the peak point of systemic risk in international crude oil importing trade. Energy 176, 281–291. https://doi.org/10.1016/j.energy.2019.03.127.

esatus AG, 2021. Protecting Critical Data Infrastructuress. https://esatus.com/schutz-von-kritischen-infrastrukturen/?lang=en, 25 February 2022.

European Union, 2017. Commission Regulation (EU) 2017/1485 of 2 August 2017: Establishing a guideline on electricity transmission system operation.

Ezzeldin, M., El-Dakhakhni, W.E., 2019. Robustness of Ontario power network under systemic risks. Sustain. Resilient Infrastruct. 69, 1–20. https://doi.org/10.1080/23789689.2019.1666340.

Fridgen, G., Häfner, L., König, C., Sachs, T., 2016. Providing utility to utilities: the value of information systems enabled flexibility in electricity consumption. JAIS 17, 537–563. https://doi.org/10.17705/1jais.00434.

Fridgen, G., Körner, M.-F., Sedlmeir, J., Weibelzahl, M., 2019. (How) can blockchain contribute to the management of systemic risks in global supply networks? Systemic risks in global networks: Proceedings of the first workshop on systemic risks in global networks, co-located with 14. Internationale Tagung Wirtschaftsinformatik 89–96.

Fridgen, G., Keller, R., Körner, M.-F., Schöpf, M., 2020a. A holistic view on sector coupling. Energy Pol. 147, 111913. https://doi.org/10.1016/j.enpol.2020.111913.

Fridgen, G., Michaelis, A., Rinck, M., Schöpf, M., Weibelzahl, M., 2020b. The search for the perfect match: aligning power-trading products to the energy transition. Energy Pol. 144, 111523. https://doi.org/10.1016/j.enpol.2020.111523.

Fridgen, G., Körner, M.-F., Walters, S., Weibelzahl, M., 2021. Not all doom and gloom: How energy-intensive and temporally flexible data center applications may actually promote renewable energy sources. Bus Inf. Syst. Eng. 63, 243–256. https://doi.org/10.1007/s12599-021-00686-z.

Future Energy Lab, 2021. Machine ID Ledger. https://future-energy-lab.de/piloten/machine-id-ledger/. (Accessed 25 February 2022).

Garrido, G.M., Sedlmeir, J., Uludağ, Ö., Alaoui, I.S., Luckow, A., Matthes, F., 2021. Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: a systematic literature review. arXiv. http://arxiv.org/pdf/2107.11905v1.

German Federal Ministry for Economic Affairs and Energy, 2021. GAIA-X: a federated data infrastrcture for Europe. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html. (Accessed 25 February 2022).

Gnansounou, E., Dong, J., 2004. Opportunity for inter-regional integration of electricity markets: the case of Shandong and Shanghai in East China. Energy Pol. 32, 1737–1751. https://doi.org/10.1016/S0301-4215(03)00164-2.

Gozman, D., Liebenau, J., Aste, T., 2020. A case study of using blockchain technology in regulatory technology. MISQE 19, 19–37. https://doi.org/10.17705/2msqe.00023.

Grimm, V., Martin, A., Schmidt, M., Weibelzahl, M., Zöttl, G., 2016a. Transmission and generation investment in electricity markets: the effects of market splitting and network fee regimes. Eur. J. Oper. Res. 254, 493–509. https://doi.org/10.1016/j.ejor.2016.03.044.

Grimm, V., Martin, A., Weibelzahl, M., Zöttl, G., 2016b. On the long run effects of market splitting: why more price zones might decrease welfare. Energy Pol. 94, 453–467. https://doi.org/10.1016/j.enpol.2015.11.010.

Haldane, A.G., May, R.M., 2011. Systemic risk in banking ecosystems. Nature 469, 351–355. https://doi.org/10.1038/nature09659.

Hanny, L., Körner, M.-F., Leinauer, C., Michaelis, A., Strüker, J., Weibelzahl, M., Weissflog, J., 2022. How to trade electricity flexibility using artificial intelligence: an integrated algorithmic framework. In: Proceedings of the 55th Hawaii International Conference on System Sciences.

Haupt, L., Körner, M.-F., Schöpf, M., Schott, P., Fridgen, G., 2020. Strukturierte Analyse von Nachfrageflexibilität im Stromsystem und Ableitung eines generischen Geschäftsmodells für (stromintensive) Unternehmen. Z. Energiewirtschaft 44, 141–160. https://doi.org/10.1007/s12398-020-00279-5.

Heffron, R., Körner, M.-F., Wagner, J., Weibelzahl, M., Fridgen, G., 2020. Industrial demand-side flexibility: a key element of a just energy transition and industrial development. Appl. Energy 269, 115026. https://doi.org/10.1016/j.apenergy.2020.115026.

Heffron, R.J., Körner, M.-F., Schöpf, M., Wagner, J., Weibelzahl, M., 2021. The role of flexibility in the light of the COVID-19 pandemic and beyond: contributing to a sustainable and resilient energy future in Europe. Renew. Sustain. Energy Rev. 140, 110743. https://doi.org/10.1016/j.rser.2021.110743.

Heffron, R.J., Körner, M.-F., Sumarno, T., Wagner, J., Weibelzahl, M., Fridgen, G., 2022. How different electricity pricing systems affect the energy trilemma: assessing Indonesia's electricity market transition. Energy Econ. 107, 105663. https://doi.org/10.1016/j.eneco.2021.105663.

Hirth, L., Mühlenpfordt, J., Bulkeley, M., 2018. The ENTSO-E Transparency Platform – a review of Europe's most ambitious electricity data platform. Appl. Energy 225, 1054–1067. https://doi.org/10.1016/j.apenergy.2018.04.048.

Hutcheon, N., Bialek, J.W., 2013. Updated and validated power flow model of the main continental European transmission network. In: IEEE Grenoble PowerTech, Grenoble, France. 2013. IEEE, pp. 1–5.

Ilin, T., Varga, L., 2015. The uncertainty of systemic risk. Risk Manag 17, 240–275. https://doi.org/10.1057/rm.2015.15.

Jenssen, A., Borsche, T., Wolst, J., 2017. Data exchange in electric power systems: European state of play and perspectives. ENTSO-E. https://eepublicdownloads.entsoe.eu/clean-documents/news/THEMA_Report_2017-03_web.pdf. (Accessed 25 February 2022).

Kamm, L., Willemson, J., 2015. Secure floating point arithmetic and private satellite collision analysis. Int. J. Inf. Secur. 14, 531–548. https://doi.org/10.1007/s10207-014-0271-8.

Kannengießer, N., Lins, S., Dehling, T., Sunyaev, A., 2020. Trade-offs between distributed ledger technology characteristics. ACM Comput. Surv. 53, 1–37. https://doi.org/10.1145/3379463.

Kaufman, G.G., Scott, K.E., 2003. What is systemic risk, and do bank regulators retard or contribute to it? Indepen. Rev. 7, 371–391.

Kerschbaum, F., Schroepfer, A., Zilli, A., Pibernik, R., Catrina, O., Hoogh, S. de, Schoenmakers, B., Cimato, S., Damiani, E., 2011. Secure collaborative supply-chain management. Computer 44, 38–43. https://doi.org/10.1109/MC.2011.224.

Kerste, M., Gerritsen, M., Weda, J., Tieben, B., 2015. Systemic risk in the energy sector—is there need for financial regulation? Energy Pol. 78, 22–30. https://doi.org/10.1016/j.enpol.2014.12.018.

Körner, M.-F., Bauer, D., Keller, R., Rösch, M., Schlereth, A., Simon, P., Bauernhansl, T., Fridgen, G., Reinhart, G., 2019. Extending the automation pyramid for industrial demand response. Procedia CIRP 81, 998–1003. https://doi.org/10.1016/j.procir.2019.03.241.

Krewitt, W., Nitsch, J., 2003. The potential for electricity generation from on-shore wind energy under the constraints of nature conservation: a case study for two regions in Germany. Renew. Energy 28, 1645–1655. https://doi.org/10.1016/S0960-1481(03)00008-9.

Lautier, D., Raynaud, F., 2012. Systemic risk in energy derivative markets: a graph-theory analysis. Energy J. 33 https://doi.org/10.5547/01956574.33.3.8.

Lee, H., Byeon, G.-S., Jeon, J.-H., Hussain, A., Kim, H.-M., Rousis, A.O., Strbac, G., 2019. An energy management system with optimum reserve power procurement function for microgrid resilience improvement. IEEE Access 7, 42577–42585. https://doi.org/10.1109/ACCESS.2019.2907120.

Li, Y., Bellemare, S., Quintyne-Collins, M., Miller, A., 2021. HoneyBadgerSwap: Making MPC as a Sidechain. https://medium.com/initc3org/honeybadgerswap-making-mpc-as-a-sidechain-364bebdb10a5. (Accessed 25 February 2022).

Lorig, F., Timm, I.J., Mertens, P., 2019. Control of systemic risks in global networks–a grand challenge to information systems research. Proceedings Wirtschaftsinformatik.

Lucas, K., Renn, O., Jaeger, C., 2018. Systemic risks: theory and mathematical modeling. Adv. Theory Simul. 1, 1800051. https://doi.org/10.1002/adts.201800051.

Lund, H., Kempton, W., 2008. Integration of renewable energy into the transport and electricity sectors through V2G. Energy Pol. 36, 3578–3587. https://doi.org/10.1016/j.enpol.2008.06.007.

Meng, L., Shafiee, Q., Ferrari Trecate, G., Karimi, H., Fulwani, D., Lu, X., Guerrero, J.M., 2017. Review on control of DC microgrids. IEEE J. Emerg. Sel. Topics Power Electron 1. https://doi.org/10.1109/JESTPE.2017.2690219.

Neuhoff, K., Bach, S., Diekmann, J., Beznoska, M., El-Laboudy, T., 2013. Distributional effects of energy transition: impacts of renewable electricity support in Germany. EEEP 2. https://doi.org/10.5547/2160-5890.2.1.3.

Nguyen, K.Q., 2007. Alternatives to grid extension for rural electrification: decentralized renewable energy technologies in Vietnam. Energy Pol. 35, 2579–2589. https://doi.org/10.1016/j.enpol.2006.10.004.

Otto, B., Steinbuß, S., Teuscher, A., Lohmann, S., 2019. Reference architecture model, Version 3.0. https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/IDS-Reference-Architecture-Model.pdf. (Accessed 25 February 2022).

Palensky, P., Dietrich, D., 2011. Demand side management: demand response, intelligent energy systems, and smart loads. IEEE Trans. Ind. Inf. 7, 381–388. https://doi.org/10.1109/TII.2011.2158841.

Papaefthymiou, G., Haesen, E., Sach, T., 2018. Power system flexibility tracker: indicators to track flexibility progress towards high-RES systems. Renew. Energy 127, 1026–1035. https://doi.org/10.1016/j.renene.2018.04.094.

Parag, Y., Sovacool, B.K., 2016. Electricity market design for the prosumer era. Nat. Energy 1. https://doi.org/10.1038/nenergy.2016.32.

Percebois, J., 2008. Electricity liberalization in the European Union: balancing benefits and risks. EJ 29. https://doi.org/10.5547/ISSN0195-6574-EJ-Vol29-No1-1.

Pierret, D., 2013. The systemic risk of energy markets. SSRN J. https://doi.org/10.2139/ssrn.2245811.

Pourbeik, P., Kundur, P.S., Taylor, C.W., 2006. The anatomy of a power grid blackout - root causes and dynamics of recent major blackouts. IEEE Power Energy Mag. 4, 22–29. https://doi.org/10.1109/MPAE.2006.1687814.

Preiß, S., 2019. Steigender Anteil Erneuerbarer führt zu erhöhtem Flexibilitätsbedarf im Stromnetz. EUWID Neue Energie.

Reboredo, J.C., 2015. Is there dependence and systemic risk between oil and renewable energy stock prices? Energy Econ. 48, 32–45. https://doi.org/10.1016/j.eneco.2014.12.009.

Renn, O., Laubichler, M., Lucas, K., Kröger, W., Schanze, J., Scholz, R.W., Schweizer, P.-J., 2020. Systemic risks from different perspectives. Risk Analysis: An Official Publication of the Society for Risk Analysis.

Rückel, T., Sedlmeir, J., Hofmann, P., 2022. Fairness, integrity, and privacy in a scalable blockchain-based federated learning system. Comput. Network. 202, 108621. https://doi.org/10.1016/j.comnet.2021.108621.

Saleh, M.S., Althaibani, A., Esa, Y., Mhandi, Y., Mohamed, A.A., 2015. Impact of clustering microgrids on their stability and resilience during blackouts. In: International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). IEEE, Offenburg, Germany, pp. 195–200.

Schellinger, B., Urbach, N., Völter, F., Sedlmeir, J., 2022. Yes, I do: marrying blockchain applications with GDPR. Proc. 55th Hawaii Int. Conferen. Syst. Sci. 4631–4640.

Schipper, F., van der Vleuten, E., 2008. Trans-European network development and governance in historical perspective. Network Industries Quarterly 10.

Schneier, B., 1996. Applied Cryptography. In: Protocols, Algorithmos, and Source Code in C, second ed. J. Wiley, New York, p. 758.

Schott, P., Sedlmeir, J., Strobel, N., Weber, T., Fridgen, G., Abele, E., 2019. A generic data model for describing flexibility in power markets. Energies 12, 1893. https://doi.org/10.3390/en12101893.

Schultze, U., Avital, M., 2011. Designing interviews to generate rich data for information systems research. Inf. Organ. 21, 1–16.

Sedlmeir, J., Smethurst, R., Rieger, A., Fridgen, G., 2021a. Digital identities and verifiable credentials. Bus Inf. Syst. Eng. 63, 603–613. https://doi.org/10.1007/s12599-021-00722-y.

Sedlmeir, J., Völter, F., Strüker, J., 2021b. The next stage of green electricity labeling. SIGENERGY Energy Inform. Rev. 1, 20–31. https://doi.org/10.1145/3508467.3508470.

Strüker, J., Weibelzahl, M., Körner, M.-F., Kießling, A., Franke-Sluijk, A., Hermann, M., 2021. Decarbonisation through Digitalisation: Proposals for Transforming the Energy Sector. University of Bayreuth. https://doi.org/10.15495/EPub_UBT_00005762.

TenneT, 2021. PKI certificates. https://www.tennet.eu/electricity-market/dutch-market/pki-certificates/. (Accessed 25 February 2022).

Trancik, J.E., 2014. Renewable energy: back the renewables boom. Nature 507, 300–302. https://doi.org/10.1038/507300a.

Weibelzahl, M., 2017. Nodal, zonal, or uniform electricity pricing: how to deal with network congestion. Front. Energy 11, 210–232. https://doi.org/10.1007/s11708-017-0460-z.

van der Welle, A.J., Haffner, R., Slot, T., Dijk, H., 2015. Options for future European electricity system operation. European Commission: Directorate-Gen. Energy Inter. Energy Market. https://ec.europa.eu/energy/sites/ener/files/documents/15-3071%20DNV%20GL%20report%20Options%20for%20future%20System%20Operation.pdf. (Accessed 25 February 2022).

Wijnia, Y.C., Herder, P.M., 2004. Modeling interdependencies in electricity infrastructure risk. In: 1st Annual CZAEE International Conference "Critical Infrastructure in the Energy Sector: Vulnerabilities and Protection".

Xie, L., Mo, Y., Sinopoli, B., 2010. False data injection attacks in electricity markets. In: 1st IEEE International Conference on Smart Grid Communications. SmartGridComm, Gaithersburg, MD, USA, pp. 226–231.

Zare-Garizy, T., Fridgen, G., Wederhake, L., 2018. A privacy preserving approach to collaborative systemic risk identification: the use-case of supply chain networks. Secur. Commun. Network. 1–18. https://doi.org/10.1155/2018/3858592, 2018.

Zhang, R., Xue, R., Liu, L., 2019. Security and privacy on blockchain. ACM Comput. Surv. 52, 1–34. https://doi.org/10.1145/3316481.