*energies*

MDPI

*Systematic Review*

# A Review of Cybersecurity Concerns for Transactive Energy Markets

**Daniel Sousa-Dias [1], Daniel Amyot [1,*], Ashkan Rahimi-Kian [1,2] and John Mylopoulos [1]**

[1] School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada; dsous064@uottawa.ca (D.S.-D.); arkian@iemsgroup.ca (A.R.-K.); jm@cs.toronto.edu (J.M.)
[2] IEMS Group Ltd., Kitchener, ON N2G 1H6, Canada
* Correspondence: damyot@uottawa.ca; Tel.: +1-613-562-5800 (ext. 6947)

**Abstract:** Advances in energy generation and distribution technology have created the need for new power management paradigms. Transactive energy markets are integrated software and hardware systems that enable optimized energy management and direct trading between prosumers. This literature review covers unresolved security and privacy vulnerabilities in the proposed implementations of such markets. We first performed a coarse search for such implementations. We then combed the resulting literature for references to privacy concerns, security vulnerabilities, and attacks that their system was either vulnerable to or sought to address. We did so with a particular focus on threats that were not mitigated by the use of blockchain technology, a commonly employed solution. Based on evidence from 28 peer-reviewed papers, we synthesized 14 categories of concerns and their proposed solutions. We found that there are some concerns that have been widely addressed, such as protecting trading history when using a public blockchain. Conversely, there were serious threats that are not sufficiently being considered. While a lack of real-world deployment has limited information about which attacks are most likely or feasible, there are clear areas of priority that we recommend to address going forward, including market attacks, false data injection attacks, single points of failure, energy usage data leakage, and privacy.

**Keywords:** blockchain; literature review; power grid; security; smart contract; transactive energy

check for updates

**Citation:** Sousa-Dias, D.; Amyot, D.; Rahimi-Kian, A.; Mylopoulos, J. A Review of Cybersecurity Concerns for Transactive Energy Markets. *Energies* **2023**, *16*, 4838. https://doi.org/10.3390/en16134838

Academic Editors: Mateus Mendes and Inácio Fonseca

Received: 24 May 2023
Revised: 12 June 2023
Accepted: 16 June 2023
Published: 21 June 2023

**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

Transactive energy (TE) grids, where anyone connected can produce or consume energy, is a burgeoning paradigm in the field of electrical power distribution [1,2]. The past two decades have seen significant advancements in energy distribution, generation, and storage technology, including home batteries, electric vehicles, and renewable energy sources. This has led to the rise of *prosumers* that are capable of producing, storing and selling, but also consuming energy. While this is a positive development, as it can have benefits for efficiency while showing an increased demand for clean energy, TE also creates some logistical difficulties. As an increasing number of consumers transition to becoming prosumers, the inefficiencies of centralized energy markets are compounded. Additionally, new risks of local voltage instability are introduced.

As a result, TE market platforms are being researched as a potential solution to these effects. The new platforms promise to enable more the localized trading of energy, better optimization of power flow, and altogether improved economic performance.

In parallel, developments in distributed computing have been spurred by the release of Bitcoin and the explosive growth in cryptocurrency that followed. The formation of Ethereum and the subsequent advancement of smart contracts as a computing platform have enabled novel applications of distributed ledger technology such as blockchain, including transactive energy [3].

Researchers have discovered ways to use smart contracts to create the distributed versions of many of the necessary mechanisms in the power grid, including demand

response, optimal power flow, state estimation, and auction clearing [4,5]. These distributed solutions have many significant benefits, including reducing single point of failure concerns and eliminating the need for trusted third parties in many cases [6].

The above security concerns and many others that arise when developing a TE market model can be addressed by implementing a solution using distributed ledger technology. For this reason, many of the models that are currently being discussed include blockchain as a platform pro forma [7,8]. However, despite the perception of blockchains as implicitly secure due to their extensive use of encryption and redundancy, the systems that are built upon them must also be carefully considered to ensure reliability, security, trust, and privacy.

This literature review targets cybersecurity threats associated with transactive energy applications that are built on distributed ledger technology. The review then asks: what privacy or data security concerns exist in a transactive energy context that are not implicitly addressed by the use of a blockchain?

There are existing reviews that overlap with ours. For example, there are surveys of the use of smart contracts in energy systems [7]. There are also reviews of security threats to legacy power grids [9,10]. However, as stated above, this survey focuses on cybersecurity threats associated with transactive energy applications built on distributed ledger technology. To our knowledge, there is no literature review that covers this exact juncture of research—perhaps in part due to the novelty of the field itself. This literature review provides researchers with an indication of gaps in the existing TE security literature, and thus areas that should be further explored. For practitioners, this review provides a comprehensive summary of existing solutions that should be considered for their architectures, as well as areas with security risks that should be addressed before deployment.

Note that, as the focus of this literature review is on cybersecurity concerns, the purely physical components of grid infrastructures (power lines, transmission towers, utility poles, transformers, etc.) fall outside the scope of this study. The interested reader is invited to consult the work of Mar et al. [9] and Ardeshiri et al. [10] for a coverage of TE security concerns related to physical components. Note also that although several solutions addressing the surveyed cybersecurity concerns are also mentioned in this paper, it is beyond the scope of this literature review to evaluate the effectiveness of these solutions. Some of the surveyed papers further provide their own self-reported analyses and evaluations.

The rest of this paper is structured as follows. Section 2 presents the background and the motivation for this work. Section 3 explains the research questions that guided the data collection and analysis for this review, whereas Section 4 presents the review methodology. Section 5 presents our study's answer to RQ1, as well as threats discovered in the literature. Section 6 includes our response to RQ2 as well as the solutions proposed in the literature, while Section 7 presents our answer to RQ3, as well as the remaining threats that are yet to be satisfactorily addressed by existing research. Section 8 discusses the limitations and threats to the validity of our review. Finally, in Section 9, we conclude the study with a reflection on the results and suggestions for further research.

## 2. Background and Motivation

In this section, we describe some of the foundational concepts relevant to the study of TE markets and their associated cybersecurity properties. We will also seek to explain the relevance of each of these topics as they relate to TE.

### 2.1. Prosumer

A portmanteau of "producer" and "consumer" [8], the term prosumer refers to a member of the electrical grid that would traditionally have been a consumer (i.e., not a generation plant) but who also has the capability to produce or store electricity. This can be through renewable energy sources (RES), such as solar panels or wind turbines, or storage cells such as electric vehicles (EVs) or battery energy storage systems (BESS).

In some cases, the term prosumer is used to refer to any (non-plant) member of the transactive energy market, i.e., households with or without power storage/production capabilities or, more simply, both prosumers and consumers. This can cause some confusion and should be noted by the reader. We will use prosumer to refer broadly to market participants, as in Section 5.11.

### *2.2. Transactive Energy*

Transactive energy refers to a broad array of economic and control techniques related to electrical distribution, storage, trading, and generation [6,11]. Transactive energy markets (TEM) are software and hardware systems that support these economic and control techniques. TE makes use of increased information flow in electricity markets, facilitated by an advanced metering infrastructure (AMI) and smart meters (SMs) [12].

TE can improve many of the existing functions of the power grid, including the demand response (DR), optimal power flow (OPF), and billing [6,13]. Additionally, it presents opportunities to ease the adoption and integration of new technologies, such as distributed energy resources (DERs), battery energy storage systems (BESSs), and electric vehicles (EVs) [6,12,14]. Finally, TE may enable a new functionality within the power grid, for instance, energy trading between prosumers and supporting consumer energy preferences [11,12].

TE also addresses some concerns within the traditional power grid implicitly. Since it is typically implemented in a decentralized fashion, it naturally improves data privacy, as well as addressing concerns over single point of failure with existing grid infrastructure and reducing the dependence on trusted third parties (TTP) [15].

Energy trading between prosumers is the most substantial paradigm shift promised by TE, and also where it gets the "transactive" in its name from. As DERs and renewable energy sources become more common among consumer households [14], traditional power distribution and billing paradigms present problems with scalability, communication overhead, and single point of failure concerns [16].

Enabling prosumers to trade between each other presents many benefits [6,12]:

- Lower electrical transmission distances;
- Improved market conditions;
- More accurate, transparent, and fair billing;
- Increased stability;
- Greater efficiency (less loss of electricity, more efficient auctions).

The nature of electricity markets, especially regarding their high throughput and essentialness, means that TE applications must satisfy several requirements. These include data security, privacy, scalability, transaction speed, and low energy footprint [11].

It is apparent why TE and TEMs are being researched so thoroughly, as they are expected to confer many benefits to power grid operations, costs, and efficiency. However, their use does generate new security concerns that may not have existed in traditional grids or that may be exacerbated by these new paradigms.

For example, Kirli et al. [7] pointed out that the integration of DERs and RESs can increase the risk of operational failure due to system imbalance or local voltage excursion. The use of AMI and smart metering equipment captures much more data from consumers, resulting in greater privacy risks and thus a greater need to protect such data [11].

Since TEMs are typically implemented as distributed applications, many of the proposed schemes and, indeed, surveys of those schemes take the use of blockchain or distributed ledger technology (DLT) for granted. As discussed, this review examines the security concerns that arise in the presence of such applications.

### *2.3. Blockchain*

Blockchains, or DLTs, are peer-to-peer applications for distributed data storage and computation [5]. This technology is widely considered as a potential foundation for implementing transactive energy frameworks and other smart grid applications, due to its

inherent ability to strongly assure integrity and non-repudiation for the data it manages on its distributed ledger [7,17].

Some of the benefits of employing blockchain technology in these contexts include addressing some security concerns that exist within current legacy energy markets, as well as some that are created or exacerbated by a peer-to-peer or smart energy market.

An example of the former is that blockchain technology is recognized as solving the single point of failure issue that currently exists in the power grid.

Tampering with energy transactions is made vastly more difficult due to blockchain's high degree of redundancy, as noted by Lombardi et al. [12]. Blockchain can also be used to improve privacy. Laszka et al. [13] proposed PETra, an implementation built on DLT that is meant to provide privacy and, where possible, anonymity within necessary TE operations such as communication, bidding, offering, and trading.

There are reasons beyond just security that researchers have proposed the use of DLT. For example, Münsing et al. [5] suggested that the distributed and trustless nature of the blockchain could be used to address and mitigate the effects of monopolistic incentives, lack of cooperation from established utilities, and regulatory shortcomings with regard to peer-to-peer energy trading. DLT has also been touted as having the potential to reduce the costs associated with TE by reducing or removing the need for trusted third parties, as noted by Mylrea and Gourisetti [6]. This could in turn increase the feasibility of DER integration, ultimately leading to a more resilient power grid [18]. Roaming electric vehicles (EVs) present unique challenges for grid integration. Shuaib et al. [16] propose that DLT could be integral to supporting the integration of dynamic EVs into the electrical grid.

Blockchain technology is also necessary for enabling the use of smart contracts, another kind of software that underpins many TE implementations [6]. These DLT smart contracts differ from smart legal contracts, a related but ultimately distinct software engineering challenge. The fact that smart contracts are built on top of DLT means that they inherit its security properties meaning, among other things, that they are immutable [7].

As noted, blockchains or DLT are distributed peer-to-peer applications that are most commonly used for data storage.

The prototypical example of a blockchain is the Bitcoin network. Bitcoin is a DLT application as well as its associated cryptocurrency [19]. In these implementations, the cryptocurrency is used both to facilitate transacting between the members of the network, as well as to incentivize the process of network validation, commonly known as "mining". Every node in the network retains a full copy of the entire blockchain, comprising all of the transactions of cryptocurrency between blockchain addresses. Each new block is cryptographically linked to all of the past blocks via a hash function. This ensures that any attempt to edit the transaction history of the chain is easily detectable, lending the blockchain its non-repudiation.

The process of mining a block involves solving a difficult cryptographic puzzle that must be computed via brute force. This is known as "proof of work" consensus (POW). The complexity of this problem scales with the size of the network. This is meant to ensure that no individual can have undue influence over the network, although this claim is regarded by some to be flawed. However, the common understanding is that, in order to gain control over the ability to validate blocks, an attacker would have to compromise at least 51% of the network, leading to the term 51% *attack* [16].

This is the traditional paradigm for DLT. Since its popularization, alternative strategies were proposed to optimize network flow, increase transaction speed, improve safety, and decrease energy expenditure.

These strategies necessarily come with trade-offs. Private or permissioned blockchains, for example, have a much better performance but are more susceptible to majority attacks, as noted by Münsing et al. [5]. These networks' integrity and availability become only as good as those in traditional decentralized applications.

Finally, we note that blockchain/DLT does not unilaterally solve security. Indeed, this fact provides the motivation for our review.

Mylrea and Gourisetti [6] pointed out that blockchain does not provide 100% security or prevention of attacks. Rather, it only improves security via authentication, encryption, and strong assurances for the integrity of the data. At the same time, it still leaves airgaps; for example, access to behind-the-meter systems [6]. Kirli et al. [7] pointed out that the immutability of smart contracts is a double-edged sword, and can leave the system vulnerable to re-entrancy attacks if proper checks and balances are not in place. As another example, Shuaib et al. [16] noted that the supposed anonymity supported by the use of blockchain can be defeated under some circumstances, thereby introducing significant privacy concerns.

These examples provide an illustration of the kind of security gaps we hope to explore in this review. It is suspected that some TE research has a reduced focus on system security due to the assumptions made about the guarantees associated with DLT. While DLT is a good foundation on which to facilitate TE, it is clearly not an encompassing security solution, and this review provides evidence of that as well as suggestions on how to improve research going forward.

### 2.4. Smart Contracts

Smart contracts (SCs) were introduced by Szabo in the mid-1990s [20]. His vision for the technology was that of an automated legal contract, a computational system that would enable the execution of typical legal functions—such as sales—without human intervention. This would be performed while respecting conditions such as payment terms, liens, and confidentiality.

The modern understanding of a smart contract is slightly different. While Szabo did refer to digital cash protocols in their original description, "smart contracts" as implemented by Bitcoin strayed somewhat from their original smart "legal contract" definition. Smart contracts are best understood now as automated scripts that run on a distributed computing environment, enabled by DLT. This kind of smart contract was first introduced using Bitcoin's Script, which allowed a basic scripting functionality via a stack-based programming language. This language enabled more complex transactions that could have built-in requirements for the recipient, such as requiring a set of private keys in order to retrieve the funds [21].

Ethereum and other platforms have since extended the idea with Turing-complete scripting languages, such as Solidity, which enable much more complex smart contracts to be implemented. Many of the platforms studied for this survey make use of such scripting languages, as they enable the complex functionality required to implement the various grid operations in a distributed manner that would simply not be possible with something such as Bitcoin Script.

SCs are recognized by much of the research on distributed TE implementations as a necessary component of establishing TE on DLT. Münsing et al. [5] recognized SCs as a "key technology" for enabling distributed optimization at all scales of operation—optimization and scalability both being key requirements of a TE application. SCs facilitate the exchange of energy between prosumers [6]. They also removed the need for trusted third parties [18]. Finally, they are considered capable of providing a certain layer of guarantee with regard to money and energy transfer [16].

SCs also have benefits beyond just facilitating distributed TE implementations. They are seen as making energy auctions fairer by making the rules and their execution visible to all parties [6,12]. Moreover, they enable additional security measures, such as the security enhancement layer described by Lombardi et al. [12].

However, there are some risks associated with the use of SCs. Chandra et al. [11] pointed out that privacy protection in TEMs has not been thoroughly studied. It is also noted that protecting the privacy of prosumers can have negative impacts on the safety of the market [17], a tension that will be seen as a running theme in this review. Finally, their immutability is another double-edged sword; meaning that they cannot be maliciously modified but neither can they be patched if a bug or vulnerability is discovered [7].

## 3. Research Questions

This review aimed to answer three research questions:

RQ1. What are the security concerns that exist in blockchain-based transactive energy systems?

- This question will enable us to determine the (cyber-)security landscape in the transactive energy system marketplace.

RQ2. What security solutions currently exist in this space and which of the concerns discovered do they address?

- This will allow us to determine the current techniques that are currently being used to address security in this space. This, in turn, will enable us to find gaps in current security research which could potentially give rise to new techniques, as well as the efficacy of current techniques that may have room for improvement.

RQ3. What are the remaining security concerns that require attention?

- This question is particularly significant for researchers, as it can inform future research directions in the space of TEM security. By examining the threats found in RQ1 and the proposed solutions found in RQ2, we can identify threats for which solutions must be further investigated—either because no solutions have been proposed or because the ones that have been proposed expose significant limitations.

## 4. Methodology

This literature review uses a methodology inspired by Okoli [22], which involves an automated search on reliable and curated databases. The selection of relevant papers is based on repeatable exclusion criteria.

In addition, as suggested by Mourão et al. [23], the automated search results are supplemented by a snowballing phase on the selected papers (based on their references) to find additional relevant papers, satisfying the same criteria.

### *4.1. Source Database*

We limited our search to the Scopus database (https://www.elsevier.com/solutions/scopus/why-choose-scopus, accessed on 12 June 2023), as it provides a comprehensive overview of the publications relevant to our topic, combined with an expressive and reliable search engine. Among its 80 million records, Scopus indexes all peer-reviewed journal and conference papers from IEEE, ACM, Elsevier, Springer-Nature, SAGE, Wiley, MDPI, Taylor & Francis, and many others. As this database is partially curated, the risk of including predatory publications is minimal (unlike with the use of Google Scholar).

### *4.2. Search Query*

The following search query was used on Scopus:

```
TITLE-ABS-KEY (
( blockchain  OR  Ethereum  OR Hyperledger OR ‘‘smart contract’’ )
AND
( security OR attack )
AND (‘‘transactive energy’’ OR DER OR ‘‘distributed energy resource’’ )
AND  ( LIMIT-TO ( LANGUAGE ,  ‘‘English’’ ) )
)
AND  ( EXCLUDE ( DOCTYPE ,  ‘‘cr’’ ) )
```

As a first concept, we included the terms “blockchain” and “Ethereum” as synonymously indicating that the paper in question makes use of blockchain or smart contract technology. We also added “Hyperledger”, a popular technology that supports permissioned blockchain development and that would likely be mentioned in a relevant paper. Finally, we included the possibility of a “smart contract” in case the paper mentions smart

contracts alone rather than the technology they are based upon. Note that Scopus also matches the plural forms of such terms.

As a second concept, we included the term "security" (which also covers the term cybersecurity) to ensure that the results returned present or review security solutions in particular. We include "attack" as an alternative in case a paper mentions a particular cyberattack—which is actually preferable to just mentioning security in general.

Finally, as a third concept, we included the term "transactive energy" to ensure that this research is related to the field of transactive energy markets (including the full "TEM" term served to limit the search results beyond what was useful). We additionally included "DER" and "distributed energy resource" as synonyms, since these technologies are fundamental to transactive energy markets and are sometimes mentioned in lieu of the full TEM term.

We limited the search to papers written in English since this is the primary language spoken by the authors. Conference reviews (i.e., introduction to proceedings written by editors and conference organizers) were also automatically excluded.

This query, which focuses on the intersection between the three concepts, returned, in March 2023, 78 unique papers before exclusion.

### *4.3. Exclusion Criteria*

Many of the returned results only mention security in passing or as a general benefit of their solution (i.e., "our solution promotes privacy, security, etc."). Others only talk of the security benefits of blockchain technology in general, or of specific concerns that are mitigated by the use of blockchain (i.e., the solution provides cryptographic security or consensus guarantees). Papers in either of these categories, or any other paper which does not discuss specific security concerns or cyberattacks, are excluded as irrelevant to the review.

### *4.4. Selected Papers*

The application of the exclusion criteria led to 56 out of the initial 78 papers to be excluded. The backward snowballing phase, based on the older papers cited by the 22 papers selected from the databases, resulted in the addition of 6 papers, for a total of 28 selected papers, as listed in Table 1. These papers are used in the next section to answer our three research questions.

**Table 1.** List of selected papers, with their year and authors.

| Year | Title | Authors |
|---|---|---|
| 2023 | Privacy protected product differentiation through smart contracts based on bilateral negotiations in peer-to-peer transactive energy markets | Chandra et al. [11] |
| 2023 | Blockchain and machine learning for future smart grids: a review | Mololoth et al. [24] |
| 2022 | Smart contracts in energy systems: A systematic review of fundamental approaches and implementations | Kirli et al. [7] |
| 2022 | Operational concerns and solutions in smart electricity distribution systems | Jayachandran et al. [8] |
| 2022 | Impact of blockchain technology on smart grids | Khan and Masood [17] |
| 2022 | Survey on blockchain for smart grid management, control, and operation | Aklilu and Ding [25] |
| 2021 | Security and privacy smart contract architecture for energy trading based on blockchains | Nazari et al. [26] |
| 2021 | Secure data access control with fair accountability in smart grid data sharing: An edge blockchain approach | Yang et al. [27] |
| 2021 | A multilayered semi-permissioned blockchain based platform for peer to peer energy trading | Zaman and He [28] |
| 2021 | A secure distributed ledger for transactive energy: The Electron Volt Exchange (EVE) blockchain | Saha et al. [4] |
| 2021 | Safe and private forward-trading platform for transactive microgrids | Eisele et al. [29] |

**Table 1.** *Cont.*

| Year | Title | Authors |
|---|---|---|
| 2021 | Blockchain for Future Smart Grid: A Comprehensive Survey | Mollah et al. [30] |
| 2021 | A blockchain-supported framework for charging management of electric vehicles | Dorokhova et al. [31] |
| 2020 | Cyber-attacks and mitigation in blockchain based transactive energy systems | Barreto et al. [32] |
| 2020 | An enhanced blockchain-based data management scheme for microgrids | Mbarek et al. [33] |
| 2019 | Blockchain for decentralized transactive energy management system in networked microgrids | Li et al. [3] |
| 2019 | Cyber-physical simulation platform for security assessment of transactive energy systems | Zhang et al. [34] |
| 2019 | Research on the application of blockchain in the energy power industry in China | Song et al. [35] |
| 2019 | Towards a semantic modelling for threat analysis of IoT applications: A case study on transactive energy | Fadhel et al. [36] |
| 2019 | A decentralised bilateral energy trading system for peer-to-peer electricity markets | Khorasany et al. [15] |
| 2019 | Secure blockchain-enabled DyMonDS design | Lauer et al. [14] |
| 2019 | Using blockchains to secure distributed energy exchange | Shuaib et al. [16] |
| 2018 | A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids | Lombardi et al. [12] |
| 2018 | Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid | Wei et al. [37] |
| 2017 | Blockchain: A path to grid modernization and cyber resiliency | Mylrea and Gourisetti [18] |
| 2017 | Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security | Mylrea and Gourisetti [6] |
| 2017 | Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers | Laszka et al. [13] |
| 2017 | Blockchains for decentralized optimization of energy resources in microgrid networks | Münsing et al. [5] |

## 5. RQ1 Results: Threats

This section answers RQ1 on the security concerns and threats about blockchain-based transactive energy systems discovered in the literature. Figure 1 summarizes the threats by their respective position in the TE infrastructure (application, network, or meter layer).

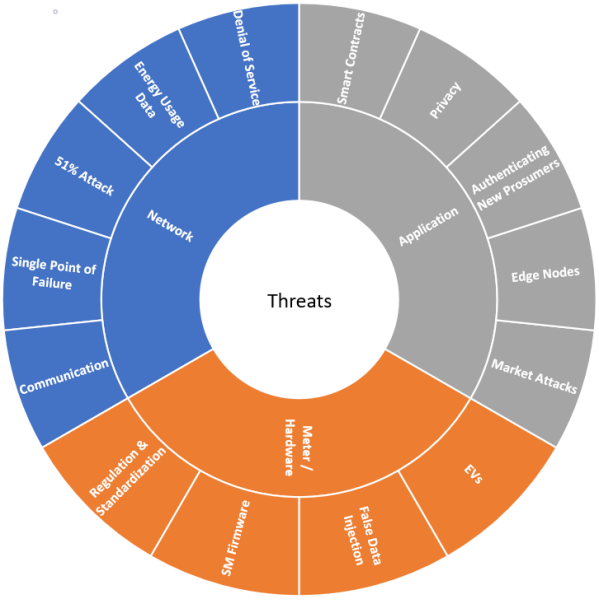


**Figure 1.** Simple taxonomy of the threats discovered. There are three overarching categories; the application layer, the network layer, and the hardware layer (including the smart meter itself). Each threat is relevant to at least one of these categories.

Table 2 presents a short summary of the threats discovered in the literature, as well as their security properties and sources. Please note from Table 2 that some threats are discussed by many papers, and that some papers discuss many different threats.

**Table 2.** Summary of security threats found in the literature and their respective sources.

| Name | Security Property | Found In |
|---|---|---|
| False data injection (FDI) | Validity | [1,4,8,32,33,38,39] |
| Denial of service (DoS) | Availability | [3,7,24,28,32,34,37] |
| Energy usage data | Confidentiality | [12,13,26,29,33] |
| 51% attack | Availability, Integrity | [7,16,24,28] |
| Privacy | Confidentiality | [4,5,7,11,13,15,26,27,29] |
| Market attacks | Integrity | [3,4,6,7,12,13,18,26,28,33,34,36] |
| Single point of failure (SPOF) | Availability | [4,7,11,14,27–29,33] |
| Edge nodes | Confidentiality, Integrity | [8,27,29,34] |
| Regulation and Standardization | Integrity, Availability | [3,5–8,12,14,17,18,35,36] |
| Smart meter firmware | Availability | [3,12,14,26,36] |
| Authenticating new prosumers | Authentication | [3,8,28,29] |
| Smart contracts | Integrity, Availability, Confidentiality | [7,16,17,31,35] |
| Electric vehicles | Confidentiality, Authentication | [4,8,16,17,30,32,40] |
| Communication | Confidentiality, Integrity | [13,29,33,41,42] |

### *5.1. False Data Injection*

A prominent cybersecurity issue is false data injection. From the perspective of data security principles, the blockchain handles data integrity and non-repudiation to an extremely high degree of confidence, so those are of limited concern. False data injection attacks, however, concern data validity. While blockchain software ensures that data entered into the chain are not changed, it cannot guarantee that the data entered are correct in the first place [4].

A false data injection attack, in general, involves modifying measurements before a system receives them or inserting fake measurements into a system in the place of real measurements. In a transactive energy setting, a false data injection attack may be carried out to observe the response it generates, to maliciously affect market operations by causing bids based on bad data, or to physically damage grid infrastructure [32,33,43].

State estimation is a process in which mathematical modeling is used to infer the power grid's total state based on real-world measurements collected by the supervisory control and data acquisition (SCADA), such as the power injection of buses. This state comprises any number of variables that might assist with modeling or otherwise concern the control center, such as bus voltage angles or magnitudes. Such a control center then makes decisions about grid operations based on the state estimation. It has been shown that an attacker could select values for their attack that thwart current algorithms for detecting bad measurements, ultimately allowing them to undermine the state estimation process [43,44].

False data injection attacks in a traditional power grid would involve physically altering meter readings in some way. Additionally, the attacker would require knowledge of the configuration of the power system they are attempting to compromise [43]. Access to an energy management system controller would also provide an opportunity for such an attack, although it would be much more difficult to obtain than access to a measurement device [45,46].

Smart grids and grids operating TE would also be vulnerable to these kinds of physical attacks, but may also present new vectors for the false data injection attack, an issue that would require further study.

In the electron volt exchange transactive energy model, for example, aggregators are uniquely positioned to inject false readings into the system. In this case, the false data would be injected into the blockchain rather than the grid's control center. Since aggregators combine the measurements of many prosumers, they are then relied upon to accurately report on those measurements [4].

As stated, this attack can have several motivations, such as observing grid response or causing faulty bids. It can also be used to facilitate a denial-of-service attack by causing "algorithm divergence". In these cases, injected data are carefully computed to prevent the state estimation algorithm from converging on a result, thus preventing the process from moving forward by trapping it at a particular iteration [4,43].

### *5.2. Denial of Service*

A denial of service (DoS) attack is a type of cyberattack that involves overwhelming a network with traffic in order to render its services inaccessible. In the context of a transactive energy market, a DoS attack can have several negative consequences. For example, a DoS attack can cause bids to be randomly discarded throughout the market [32].

This kind of attack is problematic because it is simple to implement, requiring minimal knowledge of the grid or network configuration (unlike the false data injection attack). As noted by Barreto et al. [32], even an attacker who cannot necessarily perform a more complex or targeted attack can still launch a DoS attack to great effect.

As noted by Zaman and He [28], the proof of a stake system of consensus that is employed by some blockchains in order to reduce the computational load—a necessity in the context of transactive energy, where there will be many transactions rapidly occurring due to its nature—can also make the system more vulnerable to this kind of attack.

Measures can be employed to detect and mitigate DoS attacks, such as the deep learning model described by Barreto et al. [32], which is trained to detect malicious nodes. The system uses this knowledge to dynamically modulate the cost of network access for offending nodes to make such attacks infeasible.

While DoS attacks are possible in many domains, in part due to their broad definition, advanced metering infrastructure can provide unique opportunities for DoS attack vectors. One of the most commonly referenced DoS attack in this domain is the puppet attack. In this attack, a malicious node receives a route request packet and returns a route with a nonexistent node at its end. This causes the penultimate node to enter the route discovery process when it cannot find a valid route to this nonexistent node. This process eventually results in a domino effect in which the last legitimate node sends route request packets to all of its neighbors, who then do the same, and so on. In this way, the network is flooded with route requests, causing a denial of service [47].

### *5.3. Energy Usage Data*

A commonly referenced concern is that of the potential leakage of energy usage data. These data are of course accessible by prosumers who are providing energy to consumers. Due to the nature of the market and the fact that the system must make predictions about future energy usage patterns, they are privy to a large amount of information about these energy usage patterns of other members of the market.

In Figure 2, we can see the different ways this information might flow in a TE environment.

- $\alpha$—this represents the transmission of energy usage data from a household to a central authority. Although many TE implementations have distributed elements, most still have some operations that must be performed in a centralized manner, necessitating this flow of information.

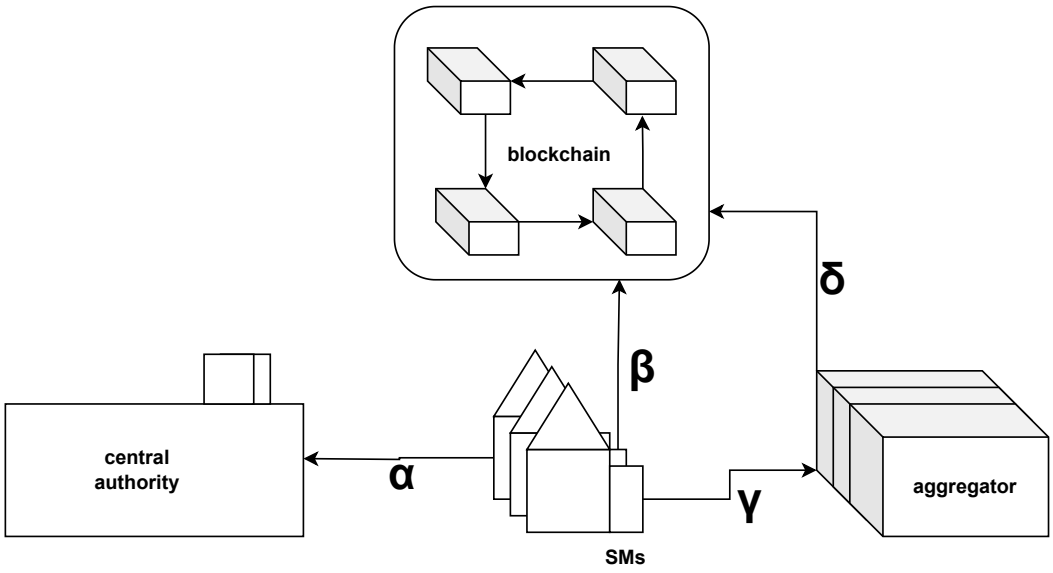


**Figure 2.** This diagram shows the flow of energy usage data in TE environments. Each letter corresponds to a different source of infrastructural risk with regard to the information's distribution.

- $\beta$—this represents data that go straight from the smart meter to the blockchain. This is in some sense the safest path for the data, as it is never owned by a single party who might exploit it; however, there is still the risk of a man-in-the-middle attack on $\beta$.
- $\gamma$—some TE models aggregate energy usage data before disseminating them in order to mitigate malicious analysis. This is a good solution, but introduces the risk of a malicious aggregator.
- $\delta$—sending aggregated data to the blockchain is extremely secure since even a man-in-the-middle attack would glean very little useful information. However, it suffers from the fact that the data have to be aggregated by a trusted party.

A typical TEM model might include any or all of these vectors for energy usage data to flow according to the structure of the architecture. For example, most implementations do not have a distributed solution for state estimation, which means that it would be performed by a central utility, necessitating the inclusion of $\alpha$. However, the electron volt exchange [4] does include such a solution (distributed state verification), thus eliminating this vector.

As noted by Lisovich et al. [48], these data can be used to glean an undesirable amount of information about the households purchasing said power. This can include their appliance profiles, work schedules, and other behavioural data, such as when one is watching television [48,49]. The extent to which this information can be exploited is not known, but even these limited examples are troubling.

The privacy of these data is therefore a commonly referenced concern. It is considered relevant that these data should be obfuscated in some way so that this privacy is not violated by the energy-producing members of the market.

### *5.4. The 51% Attack*

The 51% attack is a scenario in which an attacker gains control of over half of the computing power in a distributed ledger system. In doing so, they would undermine the consensus algorithm that is intended to maintain the integrity of the information [28]. A successful 51% attack would enable the attacker to insert fake transactions into the blockchain, compromising the integrity of the market and auction in a TE setting [16]. While this attack can have outcomes similar to those of a false data injection attack (FDIA), its method of execution relies on an attack on the blockchain network as a whole—something

that is generally taken for granted as secure by designers. This distinguishes the 51% attack from other methods of FDI.

This kind of attack is unlikely in a global blockchain such as Bitcoin or Ethereum [7]. This is due to the fact that these blockchains comprise many millions of nodes which, altogether, consist of enough computational resources that they consume roughly the same amount of power as the entire country of Sweden. This makes it extremely impractical for any singular entity to take over the network, as it is infeasible for one to generate or purchase sufficiently new computing power to take over the network, and a hacker taking over existing nodes would be at a scale that is unprecedented.

However, transactive energy markets would operate at a significantly smaller scale than the blockchains being discussed here. In some implementations, distributed ledgers could operate at a scale as small as a portion of a neighborhood [4,29]. These ledgers would then contribute to a larger ledger that would consist of the local power distribution grid. In both of these cases, the scale of computing resources is such that a 51% attack is much more feasible than in global blockchains.

This is an important note, since this kind of attack is generally ignored by larger DLTs due to its impracticality. Thus, there is a gap in security research on this topic—one that could have negative consequences for these smaller networks that may, in fact, be vulnerable to this kind of attack.

### *5.5. Privacy*

Privacy is an important consideration in all cyber-physical systems, and especially so in the TE setting. TE systems necessarily have considerable information about their users, and even information that is not explicitly personal can be used to violate privacy or worse, as we discussed in Section 5.3. These peer-to-peer (P2P) energy markets in particular are cited as having significant privacy concerns, especially in those employing a public blockchain. Smart contracts also present unique privacy concerns [7].

Many studies and reviews acknowledge an overall insufficient focus on privacy within the TE literature [11,26,29]. As an example, Lombardi et al. [12] explicitly stated that they do not address privacy concerns in their proposal. Chandra et al. [11] noted that only a small subset of TE studies have focused on securing SM data, and further claim that privacy regarding smart contracts in P2P market settings has not been studied at all. Eisele et al. [29] referenced the literature review of Andoni et al. [50], who found that, among 47 DLT TE applications, privacy preservation was a key area that has yet to be addressed.

There are two major areas of concern when it comes to privacy in TEMs, namely market privacy and data privacy, which we will use to organize our discussion here.

#### 5.5.1. Market Privacy

Market privacy involves protecting consumers' identities and market activities within the TE system, typically in the context of the application layer. Solutions in this space involve protocols that enable trading energy while protecting participants' identities.

Indeed, the transaction history can be used to glean a great deal of information about prosumers, and thus most researchers agree that their identity should be obfuscated in some way in the market application [11,29,34].

Some systems can operate with extreme levels of privacy. Bitcoin, for example, provides total anonymity to its users, at the expense of safety mechanisms that might otherwise be desirable in a financial setting, such as legal enforcement, repudiation, and fraud protection. On the other hand, some systems can operate with limited privacy in favor of integrity and trust. In any case, there is a tension between privacy, trust, and safety that cannot be reconciled. Since TE cannot totally sacrifice quality either, it must make its trade-offs with extreme consideration.

This tension means that attempts to address privacy can often have unintended consequences. For example, in the TRANSAX platform [29], prosumers are totally anonymous but can be associated with groups to allow for safety constraints. While this addresses the

grid safety problem, an inability to associate a trading profile with a particular prosumer under any circumstances still harms dispute resolution and other legal considerations. Conversely, attempts to improve safety without consideration can accidentally create privacy risks. Mbarek et al. [33] introduced a solution in which malicious trading activity is sent to endorsing peers. It is clear that the goal is to identify and track malicious behaviour, which is important, but doing so in this manner presents privacy concerns that might reduce consumer trust in the TEM.

As a final example of such a trade-off, Laszka et al. [13] presented the issue of a prosumer trading maliciously and causing grid instability. In order to mitigate this, the DSO must be able to enforce safety restrictions, but this requires access to the prosumer's transaction history, which can be used to estimate their future state.

Another significant issue is that privacy presents a barrier to dispute resolution, as noted by Khan and Masood [17]. They pointed out that most works provide total anonymity on the premise that the market application and associated smart contracts will execute flawlessly, something which should not be relied upon.

#### 5.5.2. Data Privacy

Data privacy primarily concerns data flow in the network, although it can also involve information used by the application layer. This kind of datum is typically less identity-oriented than market privacy data. Solutions in this space are more likely to involve noising, encryption, and aggregation. Impersonal data that might be subject to privacy concerns can include commercial and operational information, user preferences, consumption and production constraints, energy bids, and energy usage data [4,11,28,34,51].

These data must be communicated and stored in ways that prevent unauthorized access [34]. Examples such as personal information are obvious and thus handled by most researchers, but there are less apparent sources of privacy risk that must also be considered. Metering data can also be used maliciously, again, as we discuss in Section 5.3.

Many operations in a TE system require some amount of potentially compromising information to function, exacerbating the problem. Processes such as market clearing require private information such as participants' utility and cost curves and preferences [15]. Shuaib et al. [16] noted the difficulty of performing auction operations, such as negotiating prices, contracts, and payments, while also preserving user privacy. The challenge of negotiating prices in a P2P setting while maintaining privacy is also discussed by Kirli et al. [7] and Son et al. [52]. Implementing safety measures also often requires a significant degree of detail about a prosumer's trading history, consumption and production history, and production and storage capacities. The desire to protect this information presents challenges to implementing safety measures, and vice versa [13,29]. Finally, Li et al. [3] mentioned the necessity of certain operational information, such as production cost coefficients or operating states, as well as the preference to keep this information secret.

Applications such as home energy management (HEM), which operate as extensions of TE systems, can present additional privacy concerns due to the sensitive positioning of the hardware involved and the information collected [7].

### *5.6. Market Attacks*

Market attacks are a broad class of cyberattacks within the TE framework that can be performed either by market participants or by external parties. We differentiate these attacks by their positioning within the TE framework because they are specified this way in the literature, rather than by their technical execution. Unfortunately, details about such technical execution were lacking in the literature, which instead focused on the kinds of outcomes that could potentially be achieved by an adversary, assuming that they had some particular ability within the system (i.e., manipulating bids). The attacks aggregated here have particular relevance to TE markets for one of three reasons:

- The kind of data involved (i.e., energy usage);
- The possible outcomes of an attack (i.e., grid instability);

- How TE structures might affect an adversary's approach (i.e., manipulating a smart meter to falsify consumption metrics).

A term that comes up frequently is *malicious trading*. This refers to the actions of malicious market participants, who might perform a number of adversarial actions within the market [3,7,26], including:

- Falsely reporting consumption/production;
- Not following through on payment/energy production;
- Falsely claiming that energy/payment was not received;
- Posting fake bids/offers.

Market participants are understood to have financial incentives to cheat [4], so creating a robust TE system that is resilient to attacks that prosumers might try to carry out is critical. Any of these effects can also be produced by error rather than malice. The intent does not necessarily change the impact, however, so we will not differentiate between erroneous vs. malicious trades.

Malicious trading is considered a serious threat to TEMs. It is understood that such practices can cause outcomes as serious as physical grid instability [3,13]. Malicious trading can also threaten the integrity of market operations and produce instability in the market application [3,13]. In addition, it can be used to steal energy or money [4]. For example, a consumer might falsely report that no energy was received after a transaction, causing the transaction to fail and preventing their account from being charged (as well as the producer from receiving their compensation). This demonstrates another risk of FDI (Section 5.1) [33].

The problem of fraudulent energy transactions is somewhat novel to the TE paradigm, as observed by Mylrea and Gourisetti [6]. This new framework also introduces other concerns, such as bid manipulation [34]. The generation of fake bids and offers is also discussed in [7].

Attacks can include maliciously alter the pricing and quantity of energy bids and offers. These in particular can cause financial harm, TEM malfunctioning, and even widespread power outages [3]. Li et al. [3] also point out that the amount of power transferred might deviate from the contractual obligation due to various physical uncertainties, another issue that must be accounted for when designing TE.

Adversaries (market participants or otherwise) can also use market information to invade the privacy of participants. These situations can sometimes be intractable, a problem we discuss in Section 5.5. For example, Laszka et al. [13] pointed out that the TE system must have access to a prosumer's transactions for safety, but that this information can be used inappropriately to infer future energy consumption.

### 5.7. Single Point of Failure

Decentralization is an overall operational goal of TE systems, often supported by DLT. As Lauer et al. [14] pointed out, a centralized entity should not be trusted with full control of a transactive grid, since it would represent a single point of failure (SPOF).

SPOF is a universal infrastructural concern, whether in the domains of software, physical, or process architectures. The essential concern is that a system reliant on the presence, reliability, or trustworthiness of a single entity is consequently vulnerable to the failure or compromise of this entity. SPOFs should be avoided both for data security and operation. As noted by Eisele et al. [29], the market should remain available regardless of whether some nodes or the DSO are offline.

Single points of failure are present in the existing power delivery system. Generation is typically handled by a single or few plants, meaning that access to electricity is dependent on the reliable operation of these plants. Traditional attempts to mitigate this dependence might include backup generators or, more recently, battery storage systems.

TE attempts to ameliorate energy accessibility by enabling prosumers to trade directly between each other, meaning that in some cases, energy delivery can still be successfully performed even if central generation is compromised. Distributed TE further enhances

these qualities by enabling the operation of the energy market completely independently of a centralized server.

Distributed TEMs, however, still contain single points of failure. Because TEMs are complex, interconnected systems that contain many software and hardware components, SPOFs still arise within them, even if their primary functionality, such as market clearing, is handled in a decentralized manner [4]. In some cases, these SPOFs are simply an oversight, while in others, there may be technical reasons that a distributed solution has not yet been proposed.

Even if a TE implementation avoids total centralization, it often will have single points of failure within its architecture. For example, Chandra et al. [11] mentioned that cloud-based aggregation creates a SPOF concern at the aggregator, since hackers now have a single target that they can compromise to access all of the data being aggregated. Beyond this, the aggregator is required to be operational for the system to function, an assumption that would be preferable to avoid as the system would be more reliable without it.

Zaman and He [28] referenced an SPOF concern created in the NRGcoin [53] solution, wherein the DSO is required to maintain the private data of all market participants. This, again, represents an SPOF both in terms of operation and data security. They similarly discussed a solution by Mihaylov et al. [54], who attempted to address scalability using a redundant Byzantine fault tolerance consensus mechanism; however, in doing so, this resulted in needing a central authority (i.e., a SPOF). In many cases, attempts to address the scalability and security concerns of public blockchains require some compromise in terms of decentralization, increasing SPOF concerns.

Another subproblem that can create SPOFs is the authentication of new prosumer nodes [28,29]. Having a central authority that performs this task can lead to operational risks as well as service delays. Additionally, it presents trust implications that are undesirable in a distributed application context.

Cryptographic key issuance is another area in which SPOFs can be unwittingly created. As Yang et al. [27] pointed out, many existing schemes that employ asymmetric key distribution require centralized key generation, an undesirable trait in a distributed TE setting.

Finally, Saha et al. [4] observed that most TE blockchain solutions still require centralized computation to achieve market convergence, among other necessary computations.

From these examples, we can see that even highly decentralized, DLT-based systems can suffer from single points of failure within specific processes. With this in mind, it is important that researchers carefully consider each process that their system will be required to perform, and whether the design of that process creates any SPOFs.

### *5.8. Edge Nodes*

Edge nodes, sometimes also referred to as "fog nodes", are auxiliary computing devices that provide additional computer power to client devices on a distributed network application, such as a blockchain.

Edge nodes are often employed in TEM proposals for services such as data aggregation, performing cryptographic functions or other computations that are too intense for IoT devices such as smart meters, or an providing additional communication infrastructure [8,27,34].

The use of edge computing devices presents obvious risks regarding data ownership and access, since sensitive data relating to prosumer behaviour and TE operations may be communicated to compromised or faulty nodes. Yang et al. [27] mentioned these risks, as well as some that are specific to their access control implementation. For one, nodes might collude to reconstruct secret information (such as cryptographic keys) that was intentionally discarded. Another such concern is incorrect calculations returned by faulty or malicious nodes, which may result in bad data. TE operations acting on bad data can affect both market stability, as well as physical grid stability.

### 5.9. Regulation and Standardization

While regulation and standardization are not cybersecurity threat surfaces in the traditional sense, they are referenced frequently enough as general concerns that affect TE cybersecurity overall that it is appropriate to enumerate them here.

#### 5.9.1. Regulation

The lack of clear regulation surrounding the operation of TE markets is frequently cited as a concern in the literature. This kind of regulation falls into two categories: that of Internet of Things (IoT) device standardization and interoperability, and the regulation of the TE market operations. TE market operations include market clearing, trading practices, and reconciliation when there is a trade dispute.

In the work of Münsing et al. [5], regulatory expenses are presented as potentially not worthwhile in a bid to demonstrate why a distributed market, despite possibly introducing market inefficiency, would be preferable to a highly regulated centralized market.

The issue of IoT device regulation and interoperability was introduced by Mylrea and Gourisetti [6]. In fact, the simulation testbed they introduced was explicitly positioned to be capable of exploring this area of concern to ensure the health and adoption of the proposed decentralized TE systems. They also mentioned questions of legality with regard to DLT-based platforms, and while they did not provide suggestions, they draw attention to the problem of regulation and reconciliation in these environments. Fadhel et al. [36] also pointed out that the adoption of decentralized TE solutions is limited by the absence of a clear regulatory body.

Finally, the issue of an underdeveloped legal framework for decentralized energy applications with regard to their safety is referenced by Kirli et al. [7] as well as Khan and Masood [17].

#### 5.9.2. Software Standards

DLT software solutions, and particularly smart contracts, are still relatively new software paradigms. This novelty on its own brings forth concerns that they may not yet be ready for widespread adoption [33].

The recency of the development of these technologies also means that no software standards have been established to date. Song et al. [35] pointed out that the lack of a standardized security architecture for blockchain and smart contracts has led to an exceptional number of vulnerable smart contracts being deployed [55]. These concerns are extremely relevant to DLT-based TE, as the latter will inherit the security posture of the architecture it is built upon, and this posture will be facilitated by standardized security and development practices. Additionally, the standard protocols and software architecture of TE itself have yet to be established, as noted by Jayachandran et al. [8].

#### 5.9.3. Hardware Standards

In addition to inheriting the security posture of the software systems they are built on, TEMs will inherit the security of the hardware they are run on. Of particular concern are IoT devices, which are heavily involved in TE operations, often limited by processing power, and a relatively recent technological development. While we discuss these limitations in more detail elsewhere, the specific concern of a lack of standardization in TE and IoT hardware is mentioned in several studies [56].

Lombardi et al. [12] mentioned the security concerns raised by the lack of security standards for SM hardware. Additionally, however, they note the difficulty raised in designing TE software specifications when the hardware choices are inconsistent and difficult to predict. Li et al. [3] note that the variety of vendors producing communication and control devices, and the lack of security standardization between them, produce unpredictable cybersecurity threats. This concern is also noted by Lauer et al. [14], with an emphasis on the fact that integrating vulnerable technology into a critical service such as the power grid presents additional risks.

### 5.10. Smart Meter Firmware

Smart meters are considered a significant weak point in TEM security stature. In particular, firmware vulnerabilities are often cited as an area of concern. This is a highly relevant threat point for our purposes, since SM firmware security is not inherently improved by a blockchain-based architecture. In fact, data integrity on the blockchain can be harmed by vulnerable smart meters.

Lombardi et al. [12] pointed out that smart meters are often poorly designed, which can lead to firmware bugs and vulnerabilities. These present challenges that have limited their deployment thus far, despite efforts to do so by large utility companies.

Adversaries who control vulnerable smart meters can cause a variety of unwanted effects, including severe outcomes such as a blackout [36].

Due to the positioning within the TE architecture as monitoring devices supporting trading, load balancing, state estimation, and many more critical grid operations, keeping SM firmware up to date with security patches is widely recognized as an area of great importance and research [3,12,14,26,36].

### 5.11. Authenticating New Prosumers

New prosumers in a TEM will need to be authenticated by the network [28]. In most cases, it is expected that they will be registered by a regulatory authority such as the DSO before they can be activated on the market [3,29].

This presents several security concerns. Often, a TTP is required to perform the authentication, which is an inherent risk [26]. In most cases, this reliance also results in a single point of failure. Additionally, requiring market participants to register with a centralized authority presents privacy concerns.

### 5.12. Smart Contracts

Smart contracts are present in most proposed distributed TEM architectures to enable auction trading on DLT, as well as facilitating distributed versions of other critical functionalities in some cases. While smart contracts enable the distribution of many TE applications, addressing the threats of SPOF and TTPs, they also present new security concerns.

Smart contracts are immutable by nature once they are deployed on the blockchain [16]. This is a double-edged sword, as this prevents tampering, but also limits the ability to patch contracts when vulnerabilities are discovered [7]. Such vulnerabilities are a real threat: Nikolić et al. [55] found that 34,200 smart contracts on the Ethereum blockchain contain dangerous code. Smart contracts also face implementation limitations that affect their ability to enable some security functionality Khan and Masood [17].

In addition to vulnerabilities, Kirli et al. [7] noted that there is a risk of smart contracts being misused by malicious actors with profit incentives. These parties can use backdoors in the SC code to perform re-entrancy attacks. Such attacks have already seen effective use in the decentralized finance sector, with a particular variant known as a rug-pull thrifting the users of their crypto assets [7].

Smart contracts can have impacts beyond just financial assets. Song et al. [35] note that vulnerable or malicious SCs could cause auction malfunction resulting in extreme deviations in power trading demand, an effect that threatens security as well as the physical stability of the grid.

### 5.13. Electric Vehicles

Electric vehicles (EVs) present some unique challenges in the TE domain. They form a new attack surface for adversaries, that can use EVs as a vulnerability to affect grid operations, as noted by Barreto et al. [32]. Malicious EV users could also misuse their own vehicle for such purposes [8]. Additionally, the ability for hackers to exploit vehicles with autonomous capabilities can lead to extremely harmful outcomes, ranging from damaging the vehicle to serious injury or even death [40]. The concern is that of connecting to a TE when roaming charging could present a novel attack vector for hackers to target

autonomous EVs. This concern is only going to become more relevant as vehicles continue to adopt autonomous driving features [57].

EVs also suffer from familiar challenges. Mollah et al. [30] noted that EVs are subject to many of the privacy concerns of smart meters, including the leakage of identifying information [4] and energy usage data, as well as some novel concerns such as location data. These concerns can also be exacerbated by the fact that EVs may have to connect to different TE networks depending on where they are charging.

In fact, this leads to probably the most unique concern associated with EVs. Unlike smart meters connected to homes, EVs may wind up charging in a TE network operated by a different DSO. This presents a two-sided challenge: the DSO does not have the required information to authenticate the EV, and sharing personal information with a foreign DSO represents a privacy risk for the EV [16,17].

### *5.14. Communication*

Although it is often not explicitly mentioned, networking protocols and communication devices provide a substantial attack surface for TEM cybersecurity.

Mengelkamp et al. [41] noted that, even a secure smart meter and TE system can be undermined by an insecure communication network. In a similar vein, the authors of TRANSAX, Eisele et al. [29], pointed out that communication privacy is a baseline foundation that must be present in order to provide privacy and anonymity in a distributed application. Finally, Mbarek et al. [33] discussed the particular risk of the operating environment that TE components are deployed in. They note that smart meters and other sensors collect data on the customer premises, an open environment, and communicate via wireless protocols. These factors, as well as the sensitivity of the data in question, make them especially likely cyberattack targets, both in terms of appeal to hackers and vulnerability.

Another consideration is the security of the blockchain itself. While this is often taken for granted, the blockchain's security posture is based on the difficulty of cryptographic operations, as we discussed in Section 2.3. A looming concern is that the development of increasingly powerful quantum computers will render cryptography based on prime factorization—currently the most popular cryptographic technique—virtually insecure [42]. This is a problem for systems built on top of blockchains that employ this kind of cryptography, as the integrity of the system's records will be nullified if difficult hash puzzles can be solved at will.

## 6. RQ2 Results: Solutions

This section answers RQ2 on the security solutions that currently exist in this space, together with the concerns they address.

Table 3 presents a summary of the solutions discovered in the literature organized by the threats they are associated with, and the papers they were found in. Solutions without titles or that appear as components of larger systems are denoted as "various".

### *6.1. False Data Injection*

As noted in the discussion on false data injection attacks in RQ1, power grid state estimation is the process of estimating various state variables about the grid using mathematical models and real-world measurements. However, real-world measurements are unreliable—which may be due to tampering or simple equipment failure. For this reason, methods were developed for detecting bad measurements. These methods presume that good measurements should produce state estimations closer to the actual state, while bad measurements should do the opposite, meaning that there should be detectable inconsistencies between the good and bad measurements [43].

The robust state verification of the electron volt exchange (EVE) is strongly inspired by these methods and assumptions [4]. It approaches the new challenges imposed by decentralization by introducing distributed measurement verification. This method shifts the focus from full state estimation to real power injection within an aggregator region and power

flow between aggregator regions. It does so by solving a regression problem—similar to state estimation, but a continuous function—one time-step after a given market iteration [4].

**Table 3.** Summary of security threats found in the literature, with their respective solutions and sources.

| Threat | Solutions | Found In |
| --- | --- | --- |
| False data injection (FDI) | RSV, ETSE, various | [1,4,33,38,39] |
| Denial of service (DoS) | Smart contracts, various | [3,28] |
| Energy usage data | HE, aggregation, various | [4,11] |
| 51% attack | Various | [28] |
| Privacy | Pseudonymity, anonymity, various | [4,13,15,16,26,28,29] |
| Market attacks | Reputation, access blocking, various | [3,12,26,28,29,58] |
| Single point of failure (SPOF) | Various | [4,27–29] |
| Edge nodes | Incentives, distributed authority, BFT, various | [8,27,29] |
| Regulation and standardization | ETSE | [12] |
| Smart meter firmware | BBPS, various | [3,12,26,36] |
| Authenticating new prosumers | Smart contracts, distributed verification, various | [3,28,29] |
| Smart Contracts | Third-party verification, various | [7,16] |
| Electric vehicles | Various | [4,17,59,60] |
| Communication | Quantum-safe cryptography, quantum key distribution, PETra | [13,42,61] |

Similarly to the older methods for bad measurement detection in state estimation described by Liu et al. [43], the robust state verification of EVE is itself vulnerable to certain attacks. An attacker can cause a circumstance known as algorithm divergence, a type of denial of service attack in which the market operations are unable to iterate since the verification process will become stuck in an infinite loop. Additionally, malicious aggregators may be able to inject false data that are passed along to neighboring aggregators [4].

A novel system for remedial (rather than preventative) action is mentioned by Onumanyi et al. [1]. They describe a scheme based on thyristor-controlled series capacitors that was found to successfully ameliorate the effects of some FDI-based cyberattacks after they occurred.

There are other solutions proposed in articles that did not show up in the primary results. Extended distributed state estimation is another mechanism for attempting to detect false data injection attacks, specifically those that are thought to be tolerable to the usual state estimation algorithms as discussed previously [38]. Introduced by Wang et al. [38], the technique predates EVE's solution by several years. Finally, He et al. [39] use a machine learning-based method to detect FDI attacks by comparing incoming measurements to models of historical data.

### *6.2. Denial of Service*

Smart contracts are positioned by Li et al. [3] as potentially mitigating the effects of DoS attacks on edge devices by monitoring and validating their solution process while it occurs.

Zaman and He [28] explicitly addressed DoS attacks in their proposal by continuously modifying which blockchain nodes are performing prosumer verification, which are also validating each transaction. Additionally, they use different sets of nodes for each of these tasks. Finally, their Q-score mechanism, which we discuss in more detail in Section 6.6, ensures that only well-behaved nodes should induce transactions. A misbehaving node will quickly have its Q-score decreased, preventing it from launching transactions en masse and reducing its ability to perform a DoS attack.

### 6.3. Energy Usage Data

A common solution to protecting energy usage data is aggregation. In some cases, temporally aggregated data are sufficient information to perform a necessary function, such as billing a customer every month. In others, aggregated data from multiple prosumers can be used effectively [4]. Methods of typically aggregating data employ intermediate edge nodes (Section 5.8) as aggregators. These data are often encrypted using a partially homomorphic cryptosystem such as the Paillier cryptosystem, in order to enable the aggregators to aggregate the data without compromising it [11].

Homomorphic encryption (HE) refers to encryption schemes that have a specific property. This property is that cyphertext encrypted by an HE scheme can have some mathematical operations performed on it, and decrypting the result of these operations will provide the same answer as if the operation had been performed on the plain text.

There are a variety of such schemes. RSA, which was not created with this in mind, is consistent under multiplication, making it homomorphic. Fully homomorphic encryption schemes, which support arbitrary operations on cyphertext consistent with plain text, have also been devised. However, these are typically computationally demanding. As such, most real-world solutions, especially those in the IoT space (where computational resources are constrained and time is often a factor), limit their homomorphism to just the necessary operations. For data aggregation, the required operation is usually addition.

### 6.4. The 51% Attack

There has been a lack of consideration for 51% attacks in the TE literature, most likely due to their difficult execution in most real-world blockchain applications. However, Zaman and He [28] noted that their solution presents a hurdle to potential 51% attacks: rather than simply obtaining more computer power to gain control over the network, an attacker would have to take over 51% of the smart meters, which is a much more challenging prospect.

### 6.5. Privacy

Coin mixing is introduced as a privacy solution in the TRANSAX protocol [29]. It addresses the problem that all transactions in the blockchain are publicly available, meaning that prosumers' energy trades could be tracked.

In the traditional public blockchain model, such as Bitcoin, users are anonymous since they are not publicly connected to their account addresses. However, this anonymity is limited: since the transaction is public, if the account address is ever deanonymized, then the users' transactions can be linked to their actual identity [62]. This problem is even more apparent in the transactive energy setting since, in that case, the main account addresses are actually connected to the prosumers' identity.

To address this, TRANSAX allows prosumers to create anonymous accounts from which to perform trades. However, if the transfer of resources into these accounts can be easily tracked, then the additional security they offer is negligible, since attaching them to an identity would be as simple as looking up the transaction that added funds to their account and tracing back the source account.

Thus, TRANSAX employs CoinShuffle, a coin mixing technology. This platform is fully distributed and requires no trusted third party. It allows multiple prosumers to engage in a coin-mixing protocol, allowing them to create several anonymized accounts which cannot be linked back to any individual prosumer. In this way, they are now able to perform trades anonymously.

Other implementations also seek to decouple a prosumer's identity from its trading activity, such as those introduced by Laszka et al. [13], Zaman and He [28], Nazari et al. [26], and Shuaib et al. [16]. While these approaches improve user privacy, they can harm system security and trust by impeding legal enforcement and dispute resolution, as discussed in Section 5.5.

The electron volt exchange [4] addresses bid and constraint privacy, ensuring that energy scheduling is performed without revealing this information. Finally, Khorasany et al. [15] discussed a solution which involves decomposing the market optimization problem. In doing so, the solution limits the information required about the market participants while still accounting for their utility curves and preferences.

### *6.6. Market Attacks*

The fundamental problem of forging energy transactions on the market database is handled by the blockchain [3,12]. However, as we discussed in Section 5.6, many threat vectors remain beyond this basic attack pattern.

Market integrity is also vulnerable to FDI attacks, for which solutions are outlined in Section 6.1. These attacks can facilitate outcomes such as falsely claiming failed energy delivery and falsifying consumption data.

Eisele et al. [29] do not specifically address market attacks, but do bring forward suggestions such as employing reputation mechanisms or requiring security deposits to enable fines for malicious actors. However, it is questionable whether security deposits would be a desirable mechanism for TEM membership, because they could be introducing consumer wariness and/or social inequality.

The ability to detect attacks, and especially to differentiate malicious data from erroneous data, is as important as a system's response to bad data. This is even more true when considering a critical service such as energy delivery; it is essential that punishment is meted out with restraint and accuracy. Methods of detecting and responding to attacks have been extensively researched in the domain of control systems [58]. This research includes the consideration of automatic response mechanisms leading the system to an unsafe state, a concern we reference later in this section. Techniques from this field, such as sequential detection and change detection, could be directly employed or tailored for TEMs by designers to further enhance market security beyond the blockchain.

Reputation mechanisms are systems or protocols designed to keep track of a node/prosumer's behaviour over its lifetime on the network. These systems intend to promote positive and honest behaviour and discourage malicious or dishonest behaviour. They must be carefully designed such that they promote desired behaviours and maintain an accurate estimate of a node's value to the network.

These reputation mechanisms can address many of the discovered security concerns, including general structural threats such as DoS attacks, in addition to market attacks such as price manipulation, fake sale, fake purchase, and others. Most attacks that require repeated malicious interactions with the network can be mitigated to some extent by a reputation mechanism, although it is not recommended as a sole security solution—rather it could work as a deterrent in concert with other cybersecurity techniques.

One such implementation we found was Q-score, a reputation mechanism developed by Zaman and He [28]. It attempts to track the reliability of a node by assigning a numerical value to each node. This score is applied to all parties; including prosumers, consumers, verifying nodes, and validation nodes. Q-score uses a simple mechanism that rewards successful transactions and punishes unsuccessful transactions. In a successful transaction, all parties receive a positive boost to their Q-score. This includes the buyer, the seller, and the verifier and validation peers and leaders. If a transaction is unsuccessful, both the verifier and validation peers receive a negative impact on their Q-score. Depending on the reason for the transaction failure, either the seller or the buyer may receive a negative impact on their Q-Score: if the seller fails to provide energy, they will be punished; alternatively, if the purchaser fails to pay, then they will receive a score punishment.

Access blocking is a blunt approach to addressing misbehaving nodes, proposed explicitly by Nazari et al. [26]. Unlike the more refined reputation mechanisms discussed earlier, access blocking involves simply banning a particular node from the transactive energy network altogether. This unrefined approach has the benefit of being extremely secure but has the potential drawback of unfairness. On the one hand, preventing access

altogether eliminates undesirable behaviour entirely. On the other, it may unreasonably punish mistaken behaviour. With a service as essential as electricity, it is important that social fairness be maintained [8].

### *6.7. Single Point of Failure*

As discussed in Section 5.7, single points of failure can appear in a variety of circumstances within a TEM architecture. As such, there is no single solution, but rather methods of decentralizing different parts of the process.

Zaman and He [28] presented a solution for decentralizing the authentication of new prosumers, which we discuss in more detail in Section 6.11. TRANSAX offers a robust solution for market operations that is tolerant to the disruptions of any critical entities [29]. However, both approaches still require the DSO for prosumer registration. Yang et al. [27] employed a secret sharing scheme to enable distributed key generation, solving the SPOF of centralized key distribution in their application.

The electron volt exchange [4] takes significant strides in the pursuit of comprehensive decentralization, proposing a TE-tailored distributed state estimation algorithm RSV, which we discussed in detail in Section 6.1. Additionally, their solution uses a decentralized price optimization algorithm to fully avoid SPOF in the market clearing process, unlike many similar works.

### *6.8. Edge Nodes*

Edge nodes themselves are a solution to some of the threats presented by IoT device limitations (Section 5.8) by enabling stronger security operations than would otherwise be possible. However, the edge nodes themselves then present potential points of failure.

In the scheme proposed by Yang et al. [27], edge nodes are extensively used to assist with cryptographic computations. As such, it was critical that they address the concerns presented by their involvement. They used a decentralized key generation scheme to distribute authority. They also mentioned that other schemes employ user-performed verification in order to reduce the risk of malicious or erroneous edge nodes.

Jayachandran et al. [8] proposed that standards for IoT blockchain applications should be expanded upon. The lack of software design standards in this space is noted as a threat in Section 5.9.

In TRANSAX [29], prosumers embody edge node responsibility by acting as solvers for market operations. In this scheme, the prosumers are implicitly incentivised to perform this task, since it enables them to create beneficial trades. Eisele et al. [29] do note, however, that this is safe since the overall application will only accept new solutions if they are strictly better than the current solution, creating a mutually beneficial incentive structure.

Another solution that impacts edge nodes is reputation, which we discuss in Section 6.6. These reputation mechanisms can be applied similarly to edge nodes as they are to prosumer nodes in order to mitigate adversarial behaviour by reducing the exposure to bad actors.

Byzantine fault tolerance is a mathematical technique for reducing the impact of incorrect or malicious results when consensus is required. It is extensively used in blockchain implementations to reduce the impact of failure for any given node, making malicious behaviour and collusion much more difficult as it means that bad actors must control much larger portions of the network to have an impact on its consensus mechanisms. It can also be used in validation applications to ensure that data are being reported and calculated accurately. For example, in the scheme of Yang et al. [27], multiple fog nodes may perform the same calculation to prevent a single node from unilaterally affecting a client node's reputation or ability to purchase power.

### *6.9. Regulation and Standardization*

While many papers highlight a lack of standardization and regulation of various processes and components in TEMs, few present solutions to such issues. This is sensible in

some cases as the issue would be beyond our scope, such as IoT hardware standards, and the focus should be on mitigating the effects of vulnerable or inconsistent hardware. One example of such a technique is presented by Lombardi et al. [12] with their Energy Trading and Security Enhancement (ETSE) module, intended to make their solution agnostic to SM hardware. However, the authors did not propose the actual implementation of such a module, noting the significant difficulty of doing so.

In cases where proposals would be more expected, such as architectural standards, we suppose that the field is still in its innovation stage and is not sufficiently mature yet to support the creation of such standards. With regard to regulation, work will need to be coordinated with government bodies and other stakeholders. Such work is out of the scope of our review.

### *6.10. Smart Meter Firmware*

SM firmware security is critically important due to TEM's significant dependence on accurate readings from SMs.

Lombardi et al. [12] introduced a framework that includes a security enhancement layer (SEL), which attempts to mitigate the threat of vulnerable smart meters. Before a transaction is executed, the smart meter on each side of the transaction is checked for known firmware vulnerabilities. If any are found, the transaction is not executed and the SM is temporarily quarantined from the network until a patch becomes available or is installed. This concept of device block-listing is also mentioned by Fadhel et al. [36] as well as by Nazari et al. [26], who reference the SEL study.

Zero-day exploits are of particular concern in such highly sensitive and vital industries as power distribution. The lack of electrical power can cause economic losses or even loss of life under some circumstances (see the 2021 Texas power crisis [63]). As such, keeping relevant software and firmware up to date with the latest patches and bug fixes is of even greater importance than it is in most cybersecurity settings.

To this end, Li et al. [3] proposed a blockchain-based patch system, as shown in Figure 3. Such a system would keep security patches in a public cryptographic ledger, making them universally accessible and unmodifiable. The first benefit ensures that all users will be able to access the patches at all times and removes the single point of failure—there is no reliance on a particular server or supplier to be available for them to download the new binary. The second benefit prevents malicious modifications to patch binaries, hopefully addressing some phishing and Trojan attacks that would otherwise be possible.

There may be drawbacks to such a system, such as the potential for exploitation by adversarial microgrid controllers. These parties would suddenly be in a position to report fake threats or post fake solutions that may be automatically downloaded by other microgrid controllers. These cases demonstrate a need for further security's consideration of DLT-based software or firmware update solutions.

These kinds of systems are still being explored and would likely benefit any transactive energy implementation, although they could also be conceived as separate systems to primarily handle smart meter firmware updates, for example.

### *6.11. Authenticating New Prosumers*

There are three solutions proposed in our selected papers. Li et al. [3] suggested that smart contracts might be used to automate the authentication process, eliminating the SPOF concern (Section 5.7) while maintaining market integrity. Zaman and He [28] proposed a distributed solution in which prosumers already on the market can verify new participants via their SMs. Finally, TRANSAX also has its own protocol for authentication [29].

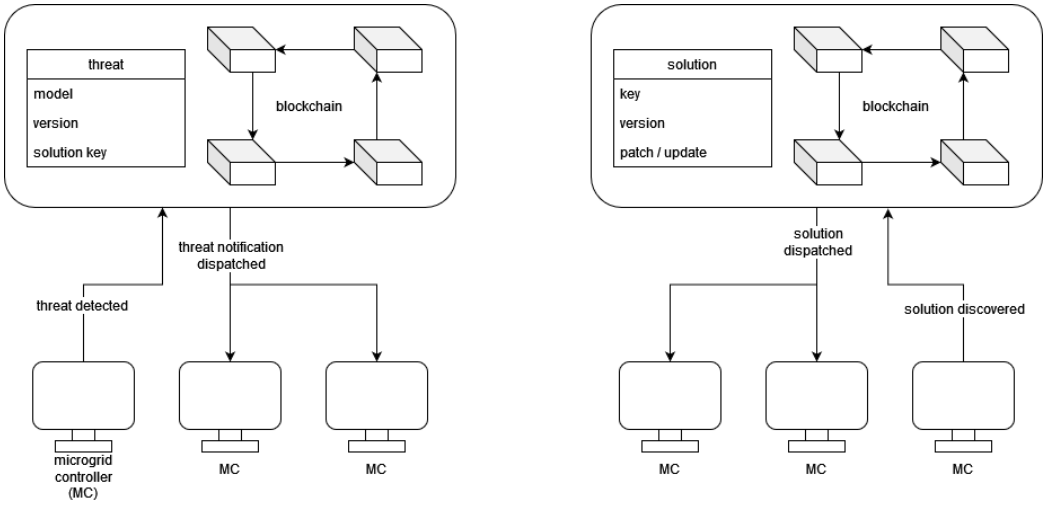


**Figure 3.** The visualization of the DLT-based patch system proposed by Li et al. [3], with the threat detection and notification (**left**) followed by the solution discovery and dispatching (**right**).

### *6.12. Smart Contracts*

The effects of vulnerable smart contracts are somewhat outside of the domain of TEM designers; however, some ideas to address these are brought forward.

Kirli et al. [7] mentioned the possibility of employing third parties to verify smart contracts. They note that this technique is common practice in the decentralized finance industry. Shuaib et al. [16] discussed the lack of standard security architecture. This could be considered the invocation of such standardization as a solution for SC security and fraud prevention, although the authors do not make specific suggestions towards producing such a standard.

### *6.13. Electric Vehicles*

Regarding charging outside of an EV's home network, Khan and Masood [17] referenced a mutual authentication scheme that disguises the EV's information from the supplier of energy, while still maintaining safety requirements.

In terms of privacy, many schemes were proposed to facilitate privacy-preserving energy trading between EVs, some of which are found in [4,17,59,60].

From what we observed, attention has not been given to the particular problem of EVs intentionally disrupting stability. This makes sense since this concern is present in many DERs, and as such, research to prevent load imbalances as a result of malicious behaviour would be device-agnostic.

### *6.14. Communication*

As stated in RQ1, network security is not frequently referenced in TEM proposals. Solutions referenced typically exist outside the TE domain, such as onion routing, garlic routing, or the matrix protocol [29]. Laszka et al. [13] also claimed to provide communication anonymity with their protocol, PETra.

In order to address the threat of quantum computers, efforts have begun to produce the next generation of cryptography which will be impenetrable even to quantum algorithms, with these techniques being generally referred to as *quantum-safe cryptography*. Yin et al. [42] go further by developing a quantum-secure network, laying the foundation for future quantum-safe blockchain technology. This technology will require continued development before it can be integrated into TEMs.

## 7. RQ3 Results: Remaining Security Concerns

This section answers RQ3 on the remaining security concerns that require attention.

### 7.1. False Data Injection

While some solutions exist to address false data injection attacks, such as EVE's robust state verification (Section 6.1), they themselves present certain threats. Due to the risk of algorithm divergence present in state estimation algorithms, it would be interesting to investigate whether there is a way to mitigate this threat or perhaps another method of FDIA detection that avoids this threat entirely.

### 7.2. Denial of Service

While DoS attacks are not extensively considered in the TE literature, we do not consider them a top remaining threat. DoS attacks within the market application, which are the kind that TEM designers should be most concerned with, are well handled by existing concepts such as reputation mechanisms.

DoS attacks on communication infrastructure are beyond the scope of TEM design, but that does not mean that researchers should not attempt to mitigate their effects. However, since solutions addressing SPOF concerns implicitly address DoS concerns, we reason that DoS attacks and their outcomes will be mitigated by the general trend of decentralization within TE, and are thus not a priority in their own right.

### 7.3. Energy Usage Data

While some solutions for energy usage data privacy exist, primarily data aggregation, these are not currently sufficient. The variety of use cases for energy usage data means that aggregation is not always optimal or even possible while maintaining the usefulness of the data. Additionally, the threat received insufficient attention in general in the TE literature, indicating a need for further research.

In traditional energy management models, this information would only be accessible to the system operator, thus presenting significantly less risk [43]. However, in distributed models, this information is often required for market operations and is therefore sent to verifying or aggregating nodes.

The leakage of energy usage data presents very acute, real-world threats to safety and privacy [48,49]. For these reasons, we consider this to be a serious gap in the security posture of current TE models.

### 7.4. The 51% Attack

As we noted in Section 5.4, 51% attacks are rare in global blockchain networks due to the scale of computational resources required to launch such an attack. However, many TEM implementations have sub-blockchains that service very small areas, such as a neighbourhood. This can make the prospect of a 51% attack much more likely, something that we did not see discussed in the literature. We thus consider 51% attacks to be a remaining threat, and of particular concern to TE research. Either research would have to demonstrate that the attack is not a concern despite the small network sizes or solutions should be proposed; however, no such works have been performed to date.

### 7.5. Privacy

As we noted in Section 5.5, there is an insufficient level of privacy consideration in the existing literature. The two main areas of privacy we discuss are market privacy and data privacy.

Solutions that address market privacy currently do so at the expense of traceability, and thus inhibit the dispute resolution and tracking of criminal behaviour. For example, TRANSAX [29] and other proposals present privacy solutions that disconnect a prosumer's identity from their trading history. This prevents attacks that rely on using trading history to predict features about the consumer, as well as discovering the identity of a trading partner. However, these proposed systems do not enable this connection under any circumstances; a desirable attribute for the consumer but one that prevents recourse altogether, even by the DSO.

Data privacy solutions are being proposed, such as those within the electron volt exchange [4] that protect user constraints and bids. However, given the sprawling, complex nature of TEMs, there still remain gaps in data privacy (notably energy usage data, which we discuss in Section 5.3). Furthermore, there is a lack of consensus about which approaches best suit which applications, as data must be obfuscated while remaining useful to the requesting party. Some approaches employ noising techniques, whilst others use algebraic transformation, just to name a few. Some of these techniques will be more appropriate for certain kinds of data than others, and until an optimum is realized, protocols that treat data differently with respect to its operational function will need to continue to be developed.

Privacy is a broad and multifaceted issue. Combined with the fact that TEMs are large, complex systems mean that it is difficult to address privacy holistically. Given the broad scope of the problem, the intricacies in the systems involved, and the lack of coverage of the solutions proposed, we consider privacy to continue to be a threat that requires further research.

### *7.6. Market Attacks*

While reputation mechanisms are a promising method of encouraging good behaviour in the TEM, they do not guarantee it. Furthermore, they are not a proactive solution, something that was largely missing from the literature.

Attack detection needs to be improved. At present, it is impossible to distinguish between malicious and erroneous input, instead relying on repeated behaviour to influence an eventual response. Furthermore, dispute resolution needs to be considered by TEM designers if the effects of malicious behaviour cannot be mitigated. Prosumers will not want to join a market where occasional theft is considered a cost of doing business, and DSOs will not want to subsidize fraud.

Overall, we consider market attacks to be a medium-level priority. Assessing such a broad category introduces some limitations, but the presence of some solutions, such as reputation, mitigate the potentially disastrous effects of unregulated markets (examples of which have been seen in the non-fungible token space [7], an unregulated market with vulnerabilities similar to TE's that we discussed briefly in Section 5.12). However, it would be preferable to have more proactive and reliable solutions going forward.

### *7.7. Single Point of Failure*

As we discussed in Sections 5.7 and 6.7, a single point of failure is a broad threat that can present in different ways. As such, it would not be reasonable to present a single solution that achieved the full coverage of the problem. Rather, we would hope to find that it has been eliminated in all processes involved with TEM operation, from onboarding to market clearing to billing. Since this is not the case, we considered SPOF to remain a high-priority threat, and work should continue to decentralize TEM architectures holistically.

### *7.8. Edge Nodes*

Edge nodes present a variable security threat depending on their positioning within a given architecture.

Edge nodes often perform tasks that require sensitive data. Combined with the fact that they are typically independently operated nodes, they can be seen as a significant security threat. Indeed, edge nodes are only as secure as the systems that use them, and there are many examples in the literature of edge nodes being insecurely deployed in TEM architectures.

However, despite often being employed to augment the TEM computing environment, edge nodes are *not* a mandatory component of a TEM infrastructure. Additionally, existing solutions to edge node concerns, such as distributing authority, reputation mechanisms, and incentives, are fairly comprehensive (Section 6.8). For these reasons, we do not consider edge nodes to be a top security priority for TEM designers, and we hence classify them as a medium-level threat.

Future solutions should decrease reliance on edge nodes when possible, whether through hardware improvements or more efficient algorithms. Where they cannot be avoided, researchers should incorporate them with care, and consider inventing more secure protocols or employing existing mechanisms to mitigate the threat of malicious or error-prone nodes.

### *7.9. Regulation and Standardization*

As we discussed in Section 6.9, much of the solution space to this issue is beyond the scope of technical DLT-based TE research, which we surveyed for this review. However, work can and should be performed in order to mitigate the potential side effects of inconsistent and vulnerable hardware, as well as those of vulnerable smart contracts.

### *7.10. Smart Meter Firmware*

While vulnerable SM firmware presents a significant security risk in a TEM framework, proposed solutions look promising in terms of mitigating the effects of compromised SMs. Research that more directly addresses the problem is beyond the scope of TEM designers. We believe that the techniques present in the proposed solutions, such as device blocklisting [12] or blockchain-based patching [3], provide a promising foundation for addressing this threat. That said, it is a serious threat, and so must be handled comprehensively. Additionally, some existing solutions, such as the blockchain-based patch system (BBPS), presents their own concerns and must be studied further. For these reasons, we consider SM firmware to present a medium-priority threat going forward.

### *7.11. Authenticating New Prosumers*

While a de facto standard protocol for authenticating new prosumers has yet to arise, we do not consider this area of TEM operation a significant security risk. Many papers that raise the concern of authentication focus on availability [26]. The trend is towards the decentralization of this process, which inherently improves the availability. Overall, the presence of several proposed solutions compared to the relatively minor security risk presented by this stage of operations lead us to rank this threat as a low-priority one.

### *7.12. Smart Contracts*

Smart contracts clearly present a significant source of vulnerability in TE systems that employ them. This is mostly due to the fact that popular smart contract implementations themselves are relatively insecure [29], and have caused problems in many of the industries that have attempted to use them [7].

While much of the work to improve SC security posture happens outside the TE domain, in the meantime, TEM researchers should strongly consider this factor. They should seek to employ SCs only where absolutely necessary, and write the chaincode with the utmost consideration when doing so.

### *7.13. Electric Vehicles*

Although EVs present a unique challenge in terms of integration into the energy market, their cybersecurity implications are not as significant. In terms of presenting a novel attack surface within the market, they share this property with other innovations such as RESs, BESSs, and smart meters. For this reason, EVs cannot be singled out as presenting a uniquely concerning safety threat to the stability of the system.

Solutions were not discovered for preventing TE-to-EV hacking; however, this is considered external to the TE domain, and vehicle cybersecurity should be handled by automakers.

The other main concern is user data management when roaming. While this does present some design challenges, the nature of roaming charging also makes these data less threatening than, say, SM energy usage data, which gives adversaries insights into a user's

home. Additionally, this problem has received considerable research attention. For these reasons, we classify EVs as a low-level threat overall.

### *7.14. Communication*

Although we noted in Sections 5.14 and 6.14 that network security has not been a strong consideration for TE researchers to date, we do not consider it a priority remaining issue for TE research. This is due to the fact that network security is already a richly researched field outside of the context of TE; as noted by Eisele et al. [29], communication security research is orthogonal to TE security research. Similarly, cryptography research is a field that supports TE development, rather than being a subset of it. TE resources would be better spent enhancing the security of TE protocols and applications to reduce the impact of potentially insecure communication devices.

## 8. Limitations and Threats to Validity

There are common validity threats in the literature reviews that also apply here [64]. From an internal validity perspective:

- We only use one database and our query was limited to English papers and only a few synonyms per concept. This means that we likely missed relevant papers in our selection. This was partly mitigated by the wide coverage of that database (Scopus) and its constant updates. Further mitigation was provided by relying on a complementary search technique, namely backward snowballing.
- Another decision was to exclude non-peer-reviewed documents, including white papers and patents. This means that the selected papers, and our conclusions, are biased towards academic contributions, at the expense of purely industrial concerns and solutions that might have brought complementary views and information.
- As most of the paper selection and data extraction was performed by one person (the first author), the process might have been subject to various unconscious biases. This was partly mitigated by involving some of the other co-authors for borderline decisions. We also made the raw data extracted from the selected papers available online for documenting, reproducing, and extending our literature review.

From the perspectives of external validity and conclusion validity, there are also important threats and limitations that can be identified:

- The relatively narrow subject of this review, namely cybersecurity concerns that affect TEMs that use blockchains, presents a limitation in terms of available research. TE and blockchains are both relatively new fields. Among papers that fall into this category, many include little to no security analysis. Often, security concerns that were discussed were those that were addressed by including a blockchain, i.e., concerns that were not relevant to our review.
- Perhaps just as impactful is the limited real-world deployment of TE systems. Most of the systems investigated for this review are in the proof-of-concept stage, meaning that they have not been tested in the wild, leading to a paucity of empirical data. It is difficult for researchers to predict which attacks will be most feasible or rewarding for hackers, but this is the analysis which we must rely on until TEMs are broadly implemented. As such, it is likely that some weaknesses have gone unnoticed, leaving gaps in security solutions.

## 9. Conclusions and Future Work

While TE promises to revolutionize power management operations, it introduces cybersecurity threats that need to be managed before it can be widely implemented. DLT is a widely employed solution for maintaining market integrity, but it only solves a subset of the issues brought on by TE paradigms.

By rigorously studying our selection of 28 peer-reviewed contributions to the DLT-based TE literature, we found 14 important cybersecurity concerns that remain beyond the scope of the blockchain. Among those, we identified five that we consider as presenting the

highest risks: market attacks, FDI, SPOF, energy usage data leakage, and privacy. Although other security threats remained, they were either of a lower priority or beyond the scope of purely TE-centric research.

For market attacks, we believe that proactive attack detection and mitigation measures within the TE market/application layer should be researched. Existing literature on network security could likely be mined for techniques that identify malicious nodes and handle them in a more sophisticated manner than with access blocking. It is also possible that new techniques will have to be designed due to the ethical considerations related to power access, which could present an interesting research opportunity.

Considering FDI, existing solutions are themselves vulnerable to additional threats, such as algorithm divergence. Efforts should be made to design FDIA countermeasures that are robust to such attacks.

SPOF is a critical structural threat and should be avoided with great effort, both to protect data as well as the availability of a vital utility. Improving this factor will require researchers to find ways around operations that have traditionally relied on centralized computation or trusted entities. This might include designing new power management protocols that are tailored to the distributed nature of TE, or discovering algorithms to decentralize existing operations (as was performed with OPF [5]), both of which present exciting research opportunities.

Energy usage data are often ignored as a privacy element within the TE literature. However, we found it to be one of the most dangerous potential data leaks and feel that more robust solutions need to be crafted. Data anonymization techniques are insufficient due to the network topology; as such, future research should focus on the methods of obfuscating or encrypting the data while maintaining its usefulness to relevant parties. This could be via improved aggregation techniques, which we discuss in Section 6.3, noising methods that preserve the statistical qualities of the data, or some novel technique that suits the limited computing power and sensitive nature of the domain.

Finally, privacy research is found to be lacking overall in the TE literature. Additionally, many solutions that address privacy ignore the practical outcomes of total anonymity and introduce their own problems with security and trust. Balance must be sought between anonymity and trust in order to establish a legitimate and fair market. Future work should focus on creating systems within TE markets that maximize consumer privacy without sacrificing traceability, an ideal that has not yet been met in our view.

**Author Contributions:** Conceptualization, A.R.-K., D.A., D.S.-D. and J.M.; methodology, D.S.-D. and D.A.; formal analysis, D.S.-D.; investigation, D.S.-D.; data curation, D.S.-D.; writing—original draft preparation, D.S.-D. and D.A.; writing—review and editing, A.R.-K., J.M., D.S.-D. and D.A.; supervision, D.A., J.M. and A.R.-K.; project administration, D.A., J.M. and A.R.-K.; funding acquisition, D.A. and J.M. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the ORF-RE project *CyPreSS: Software Techniques for the Engineering of Cyber-Physical Systems* as well as an NSERC Discovery Grant titled *Engineering Requirements for Socio-Technical Systems*.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The raw data extracted for the selected papers are available online at https://bit.ly/Energies2023-ExtractedData, accessed on 12 June 2023.

**Acknowledgments:** The authors thank Luigi Logrippo for feedback on this work and for providing pointers to useful references. We are also thankful to the anonymous reviewers for their suggestions.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| AMI | Advanced Metering Infrastructure |
| BBPS | Blockchain-Based Patch System |
| BESS | Battery Energy Storage System |
| DER | Distributed Energy Resource |
| DoS | Denial of Service |
| DSO | Distributed System Operator |
| ETSE | Energy Trading and Security Enhancement |
| EV | Electric Vehicle |
| EVE | Electron Volt Exchange |
| FDI | False Data Injection |
| FDIA | False Data Injection Attack |
| HE | Homomorphic Encryption |
| HEM | Home Energy Management |
| MC | Microgrid Controller |
| P2P | Peer-to-Peer |
| RES | Renewable Energy Sources |
| SC | Smart Contract |
| SEL | Security Enhancement Layer |
| SG | Smart Grid |
| SM | Smart Meter |
| SPOF | Single Point of Failure |
| TE | Transactive Energy |
| TEM | Transactive Energy Market |
| TTP | Trusted Third Party |

## References


1. Onumanyi, A.J.; Isaac, S.J.; Kruger, C.P.; Abu-Mahfouz, A.M. Transactive Energy: State-of-the-Art in Control Strategies, Architectures, and Simulators. *IEEE Access* **2021**, *9*, 131552–131573. [CrossRef]
2. Cox, W.; Considine, T. Structured energy: Microgrids and autonomous transactive operation. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6. [CrossRef]
3. Li, Z.; Bahramirad, S.; Paaso, A.; Yan, M.; Shahidehpour, M. Blockchain for decentralized transactive energy management system in networked microgrids. *Electr. J.* **2019**, *32*, 58–72.
4. Saha, S.; Ravi, N.; Hreinsson, K.; Baek, J.; Scaglione, A.; Johnson, N.G. A secure distributed ledger for transactive energy: The Electron Volt Exchange (EVE) blockchain. *Appl. Energy* **2021**, *282*, 116208. [CrossRef]
5. Münsing, E.; Mather, J.; Moura, S. Blockchains for decentralized optimization of energy resources in microgrid networks. In Proceedings of the 2017 IEEE Conference on Control Technology and Applications (CCTA), Maui, HI, USA, 27–30 August 2017; pp. 2164–2171. [CrossRef]
6. Mylrea, M.; Gourisetti, S.N.G. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In Proceedings of the 2017 Resilience Week (RWS), Wilmington, DE, USA, 18–22 September 2017; pp. 18–23. [CrossRef]
7. Kirli, D.; Couraud, B.; Robu, V.; Salgado-Bravo, M.; Norbu, S.; Andoni, M.; Antonopoulos, I.; Negrete-Pincetic, M.; Flynn, D.; Kiprakis, A. Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renew. Sustain. Energy Rev.* **2022**, *158*, 112013. [CrossRef]
8. Jayachandran, M.; Rao, K.P.; Gatla, R.K.; Kalaivani, C.; Kalaiarasy, C.; Logasabarirajan, C. Operational concerns and solutions in smart electricity distribution systems. *Util. Policy* **2022**, *74*, 101329. [CrossRef]
9. Mar, A.; Pereira, P.F.; Martins, J. A Survey on Power Grid Faults and Their Origins: A Contribution to Improving Power Grid Resilience. *Energies* **2019**, *12*, 4667. [CrossRef]
10. Ardeshiri, A.; Lotfi, A.; Behkam, R.; Moradzadeh, A.; Barzkar, A. Introduction and Literature Review of Power System Challenges and Issues. In *Application of Machine Learning and Deep Learning Methods to Power System Problems*; Springer International Publishing: Cham, Switzerland, 2021; pp. 19–43. [CrossRef]
11. Chandra, R.; Kaippilly Radhakrishnan, K.; Panda, S.K. Privacy protected product differentiation through smart contracts based on bilateral negotiations in peer-to-peer transactive energy markets. *Sustain. Energy Grids Netw.* **2023**, *34*, 100997. [CrossRef]
12. Lombardi, F.; Aniello, L.; De Angelis, S.; Margheri, A.; Sassone, V. A Blockchain-based Infrastructure for Reliable and Cost-effective IoT-aided Smart Grids. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018. [CrossRef]

13. Laszka, A.; Dubey, A.; Walker, M.; Schmidt, D. Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers. In Proceedings of the Seventh International Conference on the Internet of Things, Linz, Austria, 22–25 October 2017. [CrossRef]
14. Lauer, M.; Jaddivada, R.; Ilić, M. Secure Blockchain-Enabled DyMonDS Design. In Proceedings of the COINS'19: International Conference on Omni-Layer Intelligent Systems, Crete, Greece, 5–7 May 2019; ACM: New York, NY, USA, 2019; pp. 191–198. [CrossRef]
15. Khorasany, M.; Mishra, Y.; Ledwich, G. A Decentralised Bilateral Energy Trading System for Peer-to-Peer Electricity Markets. *IEEE Trans. Ind. Electron.* **2019**, *67*, 4646–4657. [CrossRef]
16. Shuaib, K.; Abdella, J.; Sallabi, F.; Abdel Hafez, M. Using Blockchains to Secure Distributed Energy Exchange. In Proceedings of the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; pp. 622–627. [CrossRef]
17. Khan, H.; Masood, T. Impact of Blockchain Technology on Smart Grids. *Energies* **2022**, *15*, 7189. [CrossRef]
18. Mylrea, M.; Gourisetti, S.N.G. Blockchain: A path to grid modernization and cyber resiliency. In Proceedings of the 2017 North American Power Symposium (NAPS), Morgantown, WV, USA, 17–19 September 2017; pp. 1–5. [CrossRef]
19. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 12 June 2023).
20. Szabo, N. Smart Contracts. 1994. Available online: https://bit.ly/3B0KLir (accessed on 12 June 2023).
21. Bitcoin Wiki. Script. 2021. Available online: https://en.bitcoin.it/wiki/Script (accessed on 12 June 2023).
22. Okoli, C. A guide to conducting a standalone systematic literature review. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 879–910. [CrossRef]
23. Mourão, E.; Pimentel, J.F.; Murta, L.; Kalinowski, M.; Mendes, E.; Wohlin, C. On the performance of hybrid search strategies for systematic literature reviews in software engineering. *Inf. Softw. Technol.* **2020**, *123*, 106294. [CrossRef]
24. Mololoth, V.K.; Saguna, S.; Åhlund, C. Blockchain and Machine Learning for Future Smart Grids: A Review. *Energies* **2023**, *16*, 528. [CrossRef]
25. Aklilu, Y.T.; Ding, J. Survey on Blockchain for Smart Grid Management, Control, and Operation. *Energies* **2022**, *15*, 193. [CrossRef]
26. Nazari, M.; Khorsandi, S.; Babaki, J. Security and Privacy Smart Contract Architecture for Energy Trading based on Blockchains. In Proceedings of the 2021 29th Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, 18–20 May 2021; pp. 596–600. [CrossRef]
27. Yang, W.; Guan, Z.; Wu, L.; Du, X.; Guizani, M. Secure Data Access Control With Fair Accountability in Smart Grid Data Sharing: An Edge Blockchain Approach. *IEEE Internet Things J.* **2021**, *8*, 8632–8643. [CrossRef]
28. Zaman, I.; He, M. A Multilayered Semi-Permissioned Blockchain Based Platform for Peer to Peer Energy Trading. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), Denver, CO, USA, 7–9 April 2021; pp. 279–285. [CrossRef]
29. Eisele, S.; Eghtesad, T.; Campanelli, K.; Agrawal, P.; Laszka, A.; Dubey, A. Safe and Private Forward-Trading Platform for Transactive Microgrids. *ACM Trans. Cyber-Phys. Syst.* **2021**, *5*, 1–29. [CrossRef]
30. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 18–43. [CrossRef]
31. Dorokhova, M.; Vianin, J.; Alder, J.M.; Ballif, C.; Wyrsch, N.; Wannier, D. A Blockchain-Supported Framework for Charging Management of Electric Vehicles. *Energies* **2021**, *14*, 7144. [CrossRef]
32. Barreto, C.; Eghtesad, T.; Eisele, S.; Laszka, A.; Dubey, A.; Koutsoukos, X. Cyber-Attacks and Mitigation in Blockchain Based Transactive Energy Systems. In Proceedings of the 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS), Denver, CO, USA, 7–9 April 2020; Volume 1, pp. 129–136. [CrossRef]
33. Mbarek, B.; Chren, S.; Rossi, B.; Pitner, T. An Enhanced Blockchain-Based Data Management Scheme for Microgrids. In *Web, Artificial Intelligence and Network Applications. WAINA 2020*; Springer: Cham, Switerland, 2020; pp. 766–775. [CrossRef]
34. Zhang, Y.; Eisele, S.; Dubey, A.; Laszka, A.; Srivastava, A.K. Cyber-physical simulation platform for security assessment of transactive energy systems. In Proceedings of the 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Montreal, QC, Canada, 15 April 2019; pp. 1–6. [CrossRef]
35. Song, W.; Li, Y.; Yang, D. Research on the Application of Blockchain in the Energy Power Industry in China. *J. Phys. Conf. Ser.* **2019**, *1176*, 042079. [CrossRef]
36. Fadhel, N.; Lombardi, F.; Aniello, L.; Margheri, A.; Sassone, V. Towards a semantic modelling for threat analysis of IoT applications: A case study on transactive energy. In Proceedings of the Living in the Internet of Things (IoT 2019), London, UK, 1–2 May 2019; pp. 1–6. [CrossRef]
37. Wei, L.; Rondon, L.P.; Moghadasi, A.; Sarwat, A.I. Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid. In Proceedings of the 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Denver, CO, USA, 16–19 April 2018; pp. 1–9. [CrossRef]
38. Wang, D.; Guan, X.; Liu, T.; Gu, Y.; Shen, C.; Xu, Z. Extended Distributed State Estimation: A Detection Method against Tolerable False Data Injection Attacks in Smart Grids. *Energies* **2014**, *7*, 1517–1538. [CrossRef]
39. He, Y.; Mendis, G.J.; Wei, J. Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2516. [CrossRef]
40. Channon, M.; Marson, J. THE liability for cybersecurity breaches of connected and autonomous vehicles. *Comput. Law Secur. Rev.* **2021**, *43*, 105628. [CrossRef]

41. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
42. Yin, H.L.; Fu, Y.; Li, C.L.; Weng, C.X.; Li, B.H.; Gu, J.; Lu, Y.S.; Huang, S.; Chen, Z.B. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2022**, *10*, nwac228. [CrossRef] [PubMed]
43. Liu, Y.; Ning, P.; Reiter, M.K. False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33. [CrossRef]
44. Vuković, O.; Dán, G. Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1500–1508. [CrossRef]
45. Yapa, C.; de Alwis, C.; Liyanage, M.; Ekanayake, J. Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research. *Energy Rep.* **2021**, *7*, 6530–6564. [CrossRef]
46. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187. [CrossRef]
47. Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Li, J. A denial of service attack in advanced metering infrastructure network. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 1029–1034. [CrossRef]
48. Lisovich, M.A.; Mulligan, D.K.; Wicker, S.B. Inferring Personal Information from Demand-Response Systems. *IEEE Secur. Priv.* **2010**, *8*, 11–20. [CrossRef]
49. McDaniel, P.; McLaughlin, S. Security and Privacy Challenges in the Smart Grid. *IEEE Secur. Priv.* **2009**, *7*, 75–77. [CrossRef]
50. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
51. Siddiqui, F.; Zeadally, S.; Alcaraz, C.; Galvao, S. Smart Grid Privacy: Issues and Solutions. In Proceedings of the 2012 21st International Conference on Computer Communications and Networks (ICCCN), Munich, Germany, 30 July–2 August 2012; pp. 1–5. [CrossRef]
52. Son, Y.B.; Im, J.H.; Kwon, H.Y.; Jeon, S.Y.; Lee, M.K. Privacy-Preserving Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids Using Functional Encryption. *Energies* **2020**, *13*, 1321. [CrossRef]
53. Wang, S.; Taha, A.F.; Wang, J.; Kvaternik, K.; Hahn, A. Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1612–1623. [CrossRef]
54. Mihaylov, M.; Jurado, S.; Avellana, N.; Van Moffaert, K.; de Abril, I.M.; Nowé, A. NRGcoin: Virtual currency for trading of renewable energy in smart grids. In Proceedings of the 11th International Conference on the European Energy Market (EEM14), Krakow, Poland, 28–30 May 2014; pp. 1–6. [CrossRef]
55. Nikolić, I.; Kolluri, A.; Sergey, I.; Saxena, P.; Hobor, A. Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. In Proceedings of the ACSAC'18: 34th Annual Computer Security Applications Conference, San Juan, PR, USA, 3–7 December 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 653–663. [CrossRef]
56. Fernandes, E.; Jung, J.; Prakash, A. Security Analysis of Emerging Smart Home Applications. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 636–654. [CrossRef]
57. Wiseman, Y. Autonomous Vehicles. In *Research Anthology on Cross-Disciplinary Designs and Applications of Automation*; IGI Global: Hershey, PA, USA, 2022; pp. 878–889. [CrossRef]
58. Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Huang, Y.L.; Huang, C.Y.; Sastry, S. Attacks against Process Control Systems: Risk Assessment, Detection, and Response. In Proceedings of the ASIACCS'11: 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; Association for Computing Machinery: New York, NY, USA, 2011; pp. 355–366. [CrossRef]
59. Cantillo-Luna, S.; Moreno-Chuquen, R.; Chamorro, H.R.; Sood, V.K.; Badsha, S.; Konstantinou, C. Blockchain for Distributed Energy Resources Management and Integration. *IEEE Access* **2022**, *10*, 68598–68617. [CrossRef]
60. Saha, S.S.; Gorog, C.; Moser, A.; Scaglione, A.; Johnson, N.G. Integrating Hardware Security into a Blockchain-Based Transactive Energy Platform. In Proceedings of the 2020 52nd North American Power Symposium (NAPS), Tempe, AZ, USA, 11–13 April 2021; pp. 1–6. [CrossRef]
61. Gu, J.; Cao, X.Y.; Fu, Y.; He, Z.W.; Yin, Z.J.; Yin, H.L.; Chen, Z.B. Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci. Bull.* **2022**, *67*, 2167–2175. [CrossRef]
62. Ruffing, T.; Moreno-Sanchez, P.; Kate, A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In Proceedings of the Computer Security—ESORICS 2014, Wroclaw, Poland, 7–11 September 2014; Kutyłowski, M., Vaidya, J., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 345–364. [CrossRef]
63. Flores, N.; McBrien, H.; Do, V.; Kiang, M.; Schlegelmilch, J.; Casey, J. The 2021 Texas Power Crisis: Distribution, duration, and disparities. *J. Expo. Sci. Environ. Epidemiol.* **2022**, *33*, 21–31. [CrossRef] [PubMed]
64. Zhou, X.; Jin, Y.; Zhang, H.; Li, S.; Huang, X. A Map of Threats to Validity of Systematic Literature Reviews in Software Engineering. In Proceedings of the 2016 23rd Asia-Pacific Software Engineering Conference (APSEC), Hamilton, New Zealand, 6–9 December 2016; pp. 153–160. [CrossRef]


**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.