*energies*

MDPI

*Review*

# Cryptographically Anchored Distributed Ledgers for Smart Grid Cybersecurity: An Attribute-Oriented Framework

**Hubert Szczepaniuk [1,*] and Edyta Karolina Szczepaniuk [2]**

[1] Department of Management, Faculty of Economic and Social Sciences, Warsaw University of Life Sciences (WULS-SGGW), Nowoursynowska 166 St., 02-787 Warsaw, Poland
[2] Faculty of Aviation Safety, Polish Air Force University, Dywizjonu 303 Street no. 35, 08-521 Dęblin, Poland; e.szczepaniuk@law.mil.pl
* Correspondence: hubert_szczepaniuk@sggw.edu.pl

## Abstract

This article provides an overview of the applications of cryptographically anchored distributed ledgers in supporting smart grid cybersecurity. The discussion focuses on multilayer cyber–physical architecture, smart grid cybersecurity requirements, information security attributes, distributed ledger mechanisms, and technical limitations. Distributed consensus algorithms and smart contracts are analyzed as conditions under which ledger writing can support smart grid security functions. The literature is then synthesized across identity and authentication, access control and policy enforcement, data integrity and tamper protection, resilient communication, and privacy protection. Based on this, the BC-Sec-SG framework was proposed to structure the requirements, architectural layers, consensus algorithms, ledger mechanisms, and constraints from the perspective of information security attributes. Blockchain technology is considered a complement to existing security mechanisms, not a substitute for them.

**Keywords:** cybersecurity; consensus algorithms; smart contracts; distributed ledger; blockchain; smart grid; information security attributes

## 1. Introduction

Cybersecurity is a key determinant in the development of future smart grids (SGs). The deep integration of power grids with ICT, cyber–physical systems (CPSs), and the IoT significantly expands the cyber threat landscape, including cyberattack vectors targeting critical infrastructure. The literature highlights cyber threats to SGs concerning confidentiality, integrity, and availability, as well as historical incidents involving energy systems (e.g., [1,2]). Control, monitoring, billing services, and energy transmission in SGs are currently largely based on centralized platforms [3]. However, applying a purely centralized security model to a distributed SG architecture has limitations. For example, it is pointed out that ensuring scalability in large-scale SG networks is a significant challenge for centralized architecture [4]. Service centralization offers undeniable benefits regarding resource management. However, it entails the risk of a single point of failure (SPoF) and creates attack vectors for critical targets. Unavailability or compromise of the central point could disable the service or lead to data disclosure.

In this context, a distributed ledger based on cryptographic proofs and consensus algorithms can be considered a complementary component of the security architecture of SGs. Furthermore, smart contracts support the programmatic definition and enforcement

Check for updates

Academic Editor: Edmund Widl

Received: 18 September 2026
Revised: 16 October 2026
Accepted: 20 October 2026
Published: 24 October 2026

**Copyright:** © 2026 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.

of security rules and policies. At the same time, the literature identifies open challenges for smart contracts in energy systems related to security, privacy, and scalability [5].

It should be noted that significant studies already exist in the literature that provide an overview of blockchain applications in the SG environment. In particular, study [6] provides a comprehensive review of this area, covering system architectures, implementation platforms, and applications across different SG domains. An important contribution of the study is the organization of blockchain applications into three areas: field measurement and communications, power generation and transmission, and power distribution and utilization [6]. The security requirements, in turn, were addressed in four aspects: integrity, confidentiality, availability, and accountability/non-repudiation [6]. Another significant study [7] focuses on blockchain architectures and application domains, as well as cybersecurity threats, challenges, and countermeasures. A key contribution of the study is the analysis of blockchain architectures for different SG areas, including electric vehicles, home automation, and energy management systems, together with implementation challenges, cybersecurity threats, common attack models, and corresponding countermeasures [7].

This article presents an overview of blockchain technology applications in supporting SG cybersecurity and assesses how its mechanisms meet information security requirements. The study is based on the general architectural perspective introduced in the holistic framework for smart grid cybersecurity presented in [8]. The previous framework holistically assigned security measures and mechanisms to individual SG layers in relation to information security attributes [8]. Blockchain was one of many possible security measures. In this study, this perspective is adapted to the analysis of blockchain technology. Compared to [8], the framework is expanded by introducing sublayers, considering six information security attributes, and organizing the synthesis by security function. Some of the analyzed attributes, including accountability and non-repudiation, have already been considered in previous studies [6]. In this review, they are incorporated into an analytical framework that links security functions, architectural layers, and blockchain mechanisms, while also taking into account the conditions on which these attributes depend.

The starting point is the layered SG model and the attributes of confidentiality, integrity, and availability, complemented by accountability, non-repudiation, and authenticity. The analyses conducted compared the properties of blockchain architecture and consensus algorithms with SG cybersecurity requirements. Subsequently, the literature was categorized according to security functions: identity management, access control, data integrity protection, communication resilience, and privacy protection. Based on this, the BC-Sec-SG framework was developed to structure the use of blockchain in SG cybersecurity. The framework identifies which distributed ledger mechanisms can support specific information security attributes across the business, application, communication, and power layers.

The main contributions of this article can be summarized as follows:

1. A structured account of SG cybersecurity requirements linking the multi-layer cyber–physical architecture with six information security attributes;
2. An assessment of consensus algorithms and smart contracts as conditions under which a ledger record can support SG cybersecurity, including the associated trust model;
3. A function-oriented synthesis of blockchain applications for SG security, covering identity and authentication, access control and policy enforcement, data integrity and tamper protection, resilient communication, and privacy protection;
4. An analysis of implementation barriers to blockchain in SG environments and of their implications for individual information security attributes;

5. The BC-Sec-SG conceptual framework, which integrates cybersecurity requirements, architectural layers, consensus conditions, ledger mechanisms, and implementation limitations in order to relate blockchain support to information security attributes.

The following sections of this article are organized as follows. Section 2 describes the research methodology adopted in the article. Section 3 analyzes SG cybersecurity requirements, taking into account technical conditions and information security attributes. Section 4 analyzes the technical architecture of blockchain in the context of SG cybersecurity, considering consensus algorithms and smart contracts. Section 5 reviews recent research on securing SGs using blockchain technology. Section 6 analyzes the barriers and limitations associated with implementing blockchain in the SG environment. Section 7 presents the BC-Sec-SG framework. The final section, Conclusions, summarizes the research findings and addresses the research questions posed.

## 2. Materials and Methods

The subject of the research presented in this article is blockchain-supported cybersecurity of SGs. The paper provides a review and analysis of studies thematically related to computer science, security sciences, and management sciences. Computer science provided the foundation for the technical analysis of SG cybersecurity and blockchain technology, encompassing IT system architectures, cyber threats and attacks, network components, and software-related aspects. Security sciences provided the scientific basis for analyzing cybersecurity in the context of information security attributes. Management sciences, in turn, complemented this approach by providing an organizational perspective on the implementation of blockchain technology in SGs.

The main objective of the study was to develop a framework based on a literature review that systematizes the application of blockchain technology to enhance the cybersecurity of SGs, with particular emphasis on information security attributes. On this basis, the BC-Sec-SG framework was proposed, aiming to organize cybersecurity requirements, architectural layers, consensus algorithms, ledger mechanisms, and constraints from the perspective of information security attributes.

In accordance with the adopted research objective, the following research questions (RQs) were formulated:

- RQ1: What cybersecurity requirements arise from the multi-layer architecture of SGs when assessed against an extended set of information security attributes?
- RQ2: How do consensus algorithms and smart contracts determine when a distributed ledger record can support SG cybersecurity?
- RQ3: In which SG security functions—identity and authentication, access control and policy enforcement, data integrity and tamper protection, resilient communication, and privacy protection—can blockchain mechanisms be applied, and what forms of support do they provide?
- RQ4: What technical limitations and barriers constrain blockchain use in SGs, and how do they affect information security attributes?
- RQ5: How can SG cybersecurity requirements, architectural layers, consensus conditions, ledger mechanisms, and implementation limits be combined in a conceptual framework relating blockchain support to information security attributes?

To achieve the adopted research objective and address the formulated RQs, a research method based on the review, analysis, and synthesis of the relevant literature was applied. The literature review was conducted, employing an iterative process for the search and selection of publications. The literature search covered publications from 2020 to 2026 and was conducted using the international bibliographic databases Scopus and Web of Science, supplemented by searches on leading publishing platforms, including MDPI.

This period covers the main set of publications analyzed, while earlier studies were used as fundamental or supplementary sources. The literature search combined three groups of terms: blockchain-related terms ("blockchain" OR "distributed ledger" OR "smart contract"), smart grid-related terms ("smart grid" OR "smart metering" OR "microgrid" OR "AMI"), and security-related terms ("cybersecurity" OR "privacy" OR "integrity" OR "authentication" OR "access control" OR "false data injection"). These groups were combined using the AND operator, with minor adjustments to database-specific search syntax. Due to the iterative nature of the literature search and its focus on the RQs, the combinations of search terms varied across queries, and not all terms were used in every query. The literature selection focused on publications relevant to the formulated research questions RQ1–RQ4. The analysis included 62 publications that directly supported the answers to these questions. Additionally, fundamental and supplementary sources were used to provide context and interpretation of the issues analyzed. Further analysis was organized according to RQ1–RQ4: cybersecurity requirements, conditions under which ledger entry can support security, security features, and technical limitations. The outcome of the conducted review is the BC-Sec-SG framework, which systematizes the application of blockchain in SG cybersecurity (RQ5).

## 3. Smart Grid Cybersecurity Considerations

Cybersecurity is directly related to information security. In the literature, cybersecurity is often analyzed in the context of information security attributes, namely confidentiality, integrity, and availability (e.g., [9–11]). The confidentiality attribute refers to the protection of information from unauthorized access [12]. Availability denotes reliable on-demand access to systems and information while maintaining trust and functionality [13]. In turn, the integrity attribute concerns protecting data against any unauthorized or undesired modification in order to ensure its accuracy and consistency [14]. It should be noted that information security and cybersecurity are not fully synonymous concepts. Cybersecurity falls within the scope of information security [15]. In reality, information can be transmitted, processed, and stored in both digital and analog forms. Therefore, it can be assumed that cybersecurity protects cyberspace from cyberattacks, while information security concerns the protection of information from all digital and physical threats [15]. It should be noted that in a distributed SG environment, various processes are implemented by multiple actors in the cyber domain. Therefore, to enhance the cybersecurity analysis, this article includes additional information security attributes: accountability, non-repudiation, and authenticity. Accountability refers to the ability to account for one's actions, as well as to accept responsibility and transparently disclose results [16]. In turn, non-repudiation is a key security requirement in many applications [17]. Non-repudiation services must ensure that the parties exchanging information over a network cannot deny participation in part or all of that communication [18]. Authenticity, in turn, is achieved when it is possible to verify the association of a resource or a signature with its legitimate owner and with the specific data that it represents [19].

The highlighted information security attributes provide the basis for further analysis of SG cybersecurity and its enhancement through blockchain-based solutions. To achieve this, it is necessary to first examine the technical characteristics of SGs and then analyze the corresponding cybersecurity requirements.

### *3.1. Technical Context*

In computer science, network architecture is often modeled in layers, as exemplified by the seven-layer ISO/OSI model or the four-layer TCP/IP reference model. Since SG architecture is inherently embedded in an information and communication technology

environment, it can likewise be analyzed from a layered perspective. In line with the general concept of a layered approach to SG architecture (e.g., [20–24]), a four-layer SG model was adapted from [8] to further analyze blockchain applications and cybersecurity.

The business layer encompasses business models and the operating rules of the energy market. The application layer is responsible for implementing energy service logic within ICT systems. Specifically, it implements automated data processing, storage, and analysis processes to make decisions related to energy grid management and customer services. Within the application layer, two sublayers are distinguished: the software sublayer and the data sublayer. The software sublayer implements algorithms and business rules that operate on data models prepared at the data sublayer. A key aspect is the implementation of software supporting both energy consumers and energy providers. In turn, the data sublayer integrates data obtained from smart meters, IoT sensors, Advanced Metering Infrastructure (AMI), Phasor Measurement Units (PMUs), and Supervisory Control and Data Acquisition (SCADA) systems. It can also integrate external data from sources such as energy markets, GIS systems, or weather stations. The communication layer comprises three sub-layers: network protocols, network devices, and transmission media. This layer is responsible for exchanging measurement and control data between SG components. The network protocol sublayer defines the rules for formatting, addressing, and securing transmissions. The network devices sublayer encompasses gateways, concentrators, routers, and switches that facilitate data forwarding. The transmission media sublayer refers to the physical or wireless medium through which data are transmitted. The power supply layer, in turn, handles electric power processes. It includes, among other elements, energy generation, transmission, and distribution, as well as distributed components, AMI meters, and control and security systems.

It should be emphasized that Figure 1 was developed specifically to support the analysis of information security attributes and is not intended to replace established reference models. SGAM provides an established reference architecture for SGs, comprising five interoperability layers: Business, Function, Information, Communication, and Component, mapped across domains and zones [25]. NIST SP 1108, in turn, defines a conceptual framework consisting of seven domains: Customer, Markets, Service Provider, Operations, Generation Including DER, Transmission, and Distribution, interconnected through energy and communication flows [26]. Figure 1 considers the level of decomposition required to analyze information security attributes and should therefore not be considered formally equivalent to any of these models.

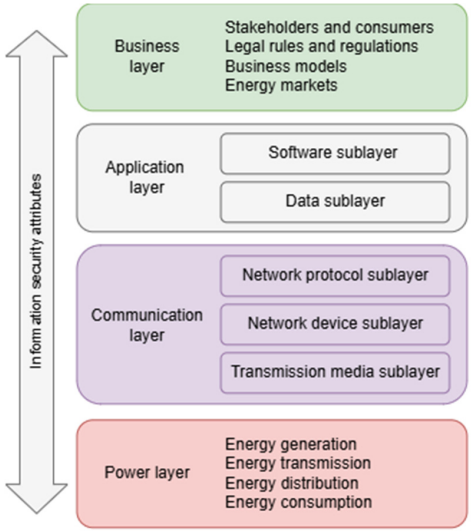



**Figure 1.** Layered SG architecture for cybersecurity analysis. Source: Adapted from [8].

### 3.2. Cybersecurity Requirements

In the next step, cybersecurity requirements related to information security in Smart Grids were defined. The analysis was based on the findings presented in [8], which considered information security requirements in the SG environment. In this study, these requirements were assigned to each of the six analyzed information security attributes. The results of the analysis are presented in Table 1.

**Table 1.** Smart grid cybersecurity requirements organized by information security attribute.

| Information Security Attribute | Smart Grid Cybersecurity Requirements |
| --- | --- |
| Confidentiality | • Data concerning energy ecosystem users, including identification data, AMI metering data, billing information, and profiling data, must not be disclosed to unauthorized entities.<br>• Protection of operational data confidentiality in the control of IoT devices, substations, and load distribution.<br>• Ensuring the confidentiality of transmission between individual components of the SG infrastructure.<br>• Protecting the confidentiality of data at rest, i.e., stored in databases and files. |
| Availability | • Providing authorized users, entities, devices, and systems with access to SG data and services at the required time.<br>• Ensuring the continuity of critical operational technology (OT) systems.<br>• The availability of communication channels used for transmitting operational and measurement data must be maintained. |
| Integrity | • User, control, and measurement data must be protected against unauthorized modification (intentional, unintentional, or accidental) in transit and at rest.<br>• Information systems should be capable of detecting unauthorized data modification, inconsistency, loss, or corruption.<br>• Scripts and configuration files of devices (AMI, RTU, IoT, IED, PLC, etc.) must be subject to integrity control.<br>• Modifications and deletions of data must be recorded in system logs. |
| Accountability | • Actions performed by users, devices, and information systems must be uniquely attributable to specific actors.<br>• The business logic of processes involving users, stakeholders, and SG services must be enforceable and auditable.<br>• The outcome of a process must be attributable to a specific actor.<br>• Actions of users, stakeholders, devices, and SG services must be recorded in audit logs. |
| Non-repudiation | • Evidence must confirm that a user, stakeholder, device, or SG service performed a specific action, including generating, modifying, or transmitting data.<br>• Evidence must confirm the trustworthiness of the time at which the event occurred. |
| Authenticity | • Unambiguous identification and authentication of users, entities, devices, systems, and services.<br>• Ensuring that data generated, transmitted, and stored in a distributed environment originates from a trusted source (a device, service, or entity). |

Source: Based on [8].

Table 1 shows that SG requirements are complex and extend beyond channel protection and power supply continuity. Therefore, it was crucial to define SG cybersecurity requirements with respect to a specific information security attribute. Individual requirements pertain to various architectural layers, services, and resources.

## 4. Blockchain Architecture in Smart Grid Cybersecurity

Blockchain technology exhibits several properties that may support SG cybersecurity. Therefore, the next stage of research focuses on analyzing the blockchain's technical architecture to identify mechanisms that can strengthen information security attributes in the SG environment. Blockchain is credited with a robust set of security mechanisms, which makes it attractive for a wide range of business applications [27]. In general terms, blockchain can be considered a distributed database in which data is replicated across a network of peer nodes, with data consistency maintained through decentralized consensus [28]. Specifically, all peer participants must agree on the state stored in the distributed database and also have the ability to verify state changes within the network [28]. Technically, Nakamoto's model relies on several mechanisms: a chain of digital signatures proving ownership without a trusted third party, blocks of transactions linked by cryptographic hashes, a distributed timestamp proving the order of events, and proof-of-work (PoW) performed by peer-to-peer network nodes [29]. From an SG cybersecurity perspective, it is important that the integrity and ordering of records rely on cryptographic proofs and network consensus rather than on trust in a single operator.

### *4.1. Smart Grid Cybersecurity Perspective*

The analyzed blockchain architecture exhibits several important security properties. Authenticity and non-repudiation can be supported by digital signatures, and data integrity and immutability can be ensured by cryptographic block chaining and consensus mechanisms. A distributed timestamp server can provide temporal ordering, while a peer-to-peer network and consensus mechanisms can increase resistance to compromise. Table 2 presents the potential contribution of these mechanisms to SG cybersecurity and their limitations.

**Table 2.** Potential and limitations of blockchain features for smart grid cybersecurity.

| Blockchain Feature | Potential for Smart Grid Cybersecurity | Limitations |
| --- | --- | --- |
| Distributed ledger structure in a peer-to-peer network | Reduces reliance on a single storage point and mitigates the impact of node failures or compromise. Replication preserves record availability despite partial node loss. | Does not maintain communication channels or control loops during a DoS attack. Node coordination may delay emergency response. |
| Chain of digital signatures | Supports the authenticity and non-repudiation of commands, readings, firmware updates, and transactions, provided the private key remains under the control of an authorized entity. | Compromise of a key or end device may enable a formally valid but false record. A signature does not verify the correctness of the source measurement. |
| Blocks | Makes retrospective modification of approved entries, including telemetry, logs, or balancing records, more difficult. Enables detection of post-approval inconsistencies in the record history. | Does not detect false data injection before submitting a record. High memory and communication overhead with a long history. |
| Distributed timestamp server | Establishes the order of approved records and supports proof that a record existed before a subsequent block. | Ledger order does not provide a trusted physical event time. Replay protection requires additional mechanisms in the communication channel. |

**Table 2.** *Cont.*

| Blockchain Feature | Potential for Smart Grid Cybersecurity | Limitations |
| --- | --- | --- |
| Consensus algorithms | Consensus without a trusted third party; increased resilience to malicious nodes; greater difficulty of falsifying data history; stronger protection against Sybil attacks. | The choice of algorithm strongly affects security and efficiency; an unsuitable choice may introduce new attack vectors and increase latency and cost. |
| Immutability | Protects the integrity of historical measurement records and system events. | Makes it difficult to correct erroneous or harmful records after they have been committed. |
| Transparency | Facilitates audit of actions, anomaly detection, and post-incident analysis. | May expose measurement data and energy consumption patterns, potentially conflicting with privacy and data protection requirements. |
| Absence of a central trust point | Limits the impact of a single-node compromise. One compromised ledger copy cannot alter the approved history. | May complicate the enforcement of security policies and rapid centralized crisis management. |

Source: Own work.

Analysis of blockchain technology's features has demonstrated its potential to enhance smart grid cybersecurity. Significant potential benefits include enhanced data integrity, event traceability, command authenticity, and the elimination of SPoFs. However, implementing these solutions poses significant challenges. The limitations presented in Table 2 also define the conditions under which blockchain can support smart grid cybersecurity. It should be noted that in a permissioned environment, resistance to Sybil attacks depends on effective control of the validator approval process. Compromising this mechanism may weaken or eliminate the resulting protection, but it does not automatically invalidate digital signatures or previously finalized records. On the other hand, public blockchains can pose privacy risks because user interactions are often publicly visible, and related data can be stored indefinitely [28]. The effective use of blockchain in energy infrastructure, therefore, requires a deliberate balancing of security benefits against operational and technical constraints.

### *4.2. Distributed Consensus Algorithms in Smart Grid Cybersecurity*

Blockchain technology inherits the Byzantine generals problem from classical distributed systems, which is traditionally solved by a state machine replication approach [30,31]. In a distributed blockchain system, a consensus algorithm is a set of rules and procedures for selecting a block from among competing proposals. Similar to blockchain, the SG is a complex CPS with an increasing number of distributed nodes, in which maintaining a common, secure state of the overall energy system is essential. Implementing different consensus algorithms in an SG environment can have a direct impact on supporting the information security attributes analyzed in Table 1. Therefore, it is reasonable to evaluate consensus algorithms in terms of their support for SG cybersecurity.

#### 4.2.1. Proof of Work Consensus Algorithms

The general concept of the PoW algorithm is that nodes perform a specific computational work. A miner attempts to solve a cryptographic puzzle in order to propose a newly created block [32]. In the original PoW, a block contains a list of transactions, the hash of the previous block, the Merkle root, a timestamp, a hash, and a nonce [33]. Mining a new block

involves searching for a nonce value such that the block hash starts with a certain number of zeros [29]. The first miner to find a valid nonce announces the block to the network, is recognized as the leader of the current block-creation round, and receives a reward [33]. Because miners propose many distinct blocks, the rate of block generation and transaction confirmation is kept at a low constant level to ensure security [34].

The PoW algorithm played a key role in the widespread adoption of blockchain technology, ensuring the integrity and reliability of decentralized systems [35]. However, it should be pointed out that the PoW algorithm provides strong security guarantees and decentralization, but at the cost of high energy consumption and slower transaction throughput [36]. Moreover, a substantial portion of the network's computational resources does not directly contribute to producing the final ledger state [37]. The literature also indicates that energy expenditure, which is a characteristic of PoW algorithms, is a key indicator for assessing the system's impact on the environment [38]. At the same time, recent studies provide interesting evidence that competitive dynamics in PoW-based cryptocurrency mining have shifted from access to energy resources toward access to semiconductor resources [39]. For SG security, such a dependency could potentially limit the nature of distributed computing work on which the classic PoW assumption is based.

#### 4.2.2. Proof of Stake Consensus Algorithms

One of the leading alternatives to PoW is the Proof-of-Stake (PoS) algorithm, in which network security is based on participants' economic commitment rather than on computational power. In PoS, the right to propose a new block is typically assigned through a pseudorandom selection process among validators who stake their cryptocurrency [40]. Based on [41,42], the algorithm's general operation can be described as follows:

1. Validator selection: in each slot, the system pseudorandomly selects one validator to propose a block, with the probability of selection being proportional to the amount of stake committed by the validator.
2. Block proposal: the selected validator collects transactions, creates a block, and broadcasts it to the network.
3. Attestation: the remaining validators verify the validity of the block and submit attestations, or votes, for the chain head they consider valid.
4. Finalization: A block becomes finalized when the relevant checkpoints receive support from at least two-thirds of the total staked value through the justification and finalization process.

To ensure security and prevent attacks, the PoS algorithm provides a system of rewards and penalties. Honest validators receive rewards for correctly proposing blocks, while protocol violations may result in partial or complete loss of the staked amount [43]. The literature highlights the energy efficiency, cost-effectiveness, and speed of this method, while also pointing out the risk of centralization, as wealthier participants could gain disproportionately large influence [36].

One important extension of the PoS algorithm is Delegated Proof of Stake (DPoS). In this approach, the authority to create blocks and validate transactions is delegated to a limited number of selected delegates. Token holders vote to elect delegates responsible for block validation [44]. DPoS reduces the communication overhead associated with network transmission and confirmation, allowing for high throughput [45].

For SG cybersecurity, low energy consumption and fast block finalization are desirable characteristics of PoS algorithms. Not relying on computational power reduces hardware requirements, facilitating easier integration with resource-constrained devices. Furthermore, DPoS algorithms can improve performance by reducing the number of active validators, thereby increasing throughput. However, both PoS and DPoS carry the risk

of centralization. In PoS algorithms, this risk stems from staking concentration. In DPoS algorithms, consensus is influenced by a relatively small number of delegates. In SGs, such a concentration requires carefully designed permission-control mechanisms.

#### 4.2.3. Proof of Authority Consensus Algorithms

Another consensus mechanism crucial for SG cybersecurity is Proof of Authority (PoA). This model, used primarily in permissioned networks, relies on the identity, trust, reputation, and accountability of authorized validators. In general terms, the algorithm involves selecting a limited number of trusted nodes to validate transactions and create new blocks [46]. Based on [47,48], the algorithm's operation can be described as follows:

1. The network includes a set of authorized validators that are permitted to create new blocks and whose identities and reputations are known;
2. Validators are selected to act as leaders in turn, for example, using a round-robin mechanism;
3. The selected leader collects transactions, creates a block, and signs it;
4. The remaining authorized nodes verify the validity of the block;
5. Once successfully verified, the block is added to the blockchain;
6. The leadership role is then transferred to the next validator according to the rules of the specific protocol.

The PoA algorithm features security based on identity-based trust rather than a computational or economic model [49]. The literature indicates that these algorithms are used in permissioned blockchain networks due to their high throughput, security, and efficiency [50]. Their use in blockchain helps to increase trust and security [51]. This mechanism can be used in applications such as supply chains and retail networks [52]. The literature indicates that in some cases, PoA algorithms may face performance limitations [53].

In the context of cybersecurity, PoA algorithms can effectively support SG requirements. Energy systems are largely permissioned in nature, involving various stakeholders, including prosumers, operators, and distributors. Identity-based and reputation-based validator mechanisms, such as PoA, support rapid network consensus with low resource consumption and deterministic finality. This is particularly important when processing measurement data and control commands in SGs. At the same time, the risk of centralization requires secure management of the authority list.

#### 4.2.4. Byzantine Fault Tolerance-Based Consensus Algorithms

BFT mechanisms are also important for SG cybersecurity, but they address a different aspect of consensus than the previously discussed algorithms. They are derived from classical solutions to the Byzantine Generals Problem. The Practical Byzantine Fault Tolerance (PBFT) [54] protocol was one of the first practical implementations to solve this problem and was applicable to real distributed systems. One of the algorithm's key premises is achieving system correctness through communication and voting mechanisms among nodes, while maintaining resilience against a certain number of malicious nodes [55]. Based on [54], the general steps of the algorithm can be described as follows:

1. The client sends a request to execute an operation to the primary node;
2. The primary broadcasts this request to all remaining backups;
3. The backups execute the request and return a reply to the client;
4. The client accepts the result after receiving $(f + 1)$ matching replies from different backups.

The algorithm's main advantages are security and ensuring rapid deterministic finalization, provided the number of faulty nodes does not exceed one-third [56]. The algorithm

has been adopted by many permissioned blockchain systems [57]. Since the development of PBFT, numerous other approaches have emerged, proposing extensions and optimizations, among other things, to improve system performance [58].

BFT algorithms demonstrate potential in speed, deterministic finality, and the ability to achieve consensus even in the presence of malicious or faulty nodes. In power infrastructures, where multiple components and systems may operate on a permissioned or consortium basis, these algorithms can support the secure and integral exchange of measurement data, control commands, and energy balance information. The advantages of the analyzed algorithms include strong security guarantees and relatively low latency, which are crucial for critical control operations in power grids. However, their scalability may be limited by communication complexity, which can become a significant challenge as the number of participants and devices increases.

Research on consensus mechanisms has led to numerous improvements and extensions of the analyzed algorithms. For example, study [49] analyzed 32 consensus mechanisms, which illustrates the scale of the phenomenon. Recent studies present concepts such as Proof of Energy [59], Proof of Task [60], Proof of Prediction [61], and mechanisms based on dynamic reputation assessment and verifiable random functions [62].

The analysis indicated that consensus algorithms support SG cybersecurity requirements to varying degrees. Requirements concerning integrity, availability, transaction finality time, and computational costs are particularly critical. PoW and PoS mechanisms are important in public networks. Solutions based on a limited number of validators, such as DPoS, PoA, and classic quorum protocols like PBFT, can be beneficial in environments requiring greater control over participants and predictable finality. In the context of SG cybersecurity, permissioned and consortium networks are particularly important because validator privileges can be associated with specific components of the energy infrastructure. However, no consensus mechanism can independently provide complete cybersecurity for the system. No algorithm inherently ensures confidentiality or full availability. The selection of consensus algorithms should take into account the trust model, process timeframes, acceptable latency, scalability requirements, and the degree of authority concentration.

### *4.3. Smart Contracts in Smart Grid Cybersecurity*

Smart contracts are one of the key blockchain functionalities that can support selected information security attributes in SGs. In general, smart contracts are computer programs that run on a distributed blockchain network and can be implemented in various programming languages [63]. A smart contract contains a set of instructions stored and deployed on the blockchain, enabling its decentralized execution [64]. In practice, smart contracts enable the programming of specific rules and functionalities, whose automatic execution and integrity are ensured by distributed ledger mechanisms. This means that the security of smart contracts relies primarily on cryptographic mechanisms and blockchain network consensus, reducing reliance on a trusted third party. Synthesizing [65–69], the typical life cycle of a smart contract in blockchain networks can be described as follows:

1. Contract preparation: programming the smart contract code, including the business logic, functions, rules, and conditions, in a language supported by the given blockchain platform;
2. Compilation: transforming the source code into an executable form understood by the blockchain runtime environment;
3. Deployment: sending to the blockchain network a deployment transaction that contains the compiled contract code; once this transaction has been accepted by the consensus mechanism, the contract receives a unique address and is permanently recorded in the distributed ledger;

4. Execution: users or other contracts invoke the functions of the deployed contract through transactions that contain the contract address, the function identifier, and the arguments;
5. Verification and consensus: network nodes verify the transaction, execute the contract code in the runtime environment, and reach a consensus on the execution result;
6. State update: the result of contract execution, which may include, among other things, a state change, value transfer, or event emission, is permanently recorded in the blockchain;
7. Termination or continued operation: the contract remains active and can be called repeatedly until it blocks or self-destructs, if such a function is implemented.

Smart contract functionality is not available on all blockchains. Their architectural implementation depends primarily on the platform's technical specifics. It is indicated that smart contracts can support automated data management [70]. On the other hand, the immutability and transparency of smart contracts can make potential security vulnerabilities critical, as implemented contracts cannot be modified [71].

The concept of smart contracts as computer programs cryptographically secured by a distributed ledger implies a number of properties that can support SG cybersecurity. The comparison in Table 3 summarizes the key properties of smart contracts in terms of their support for SG cybersecurity.

**Table 3.** Potential and limitations of smart contract properties for smart grid cybersecurity.

| Smart Contract Property | Potential for Smart Grid Cybersecurity | Limitations and Risks |
| --- | --- | --- |
| Automated rule enforcement | Support for the automatic enforcement of security policies, access rules, and operational conditions; reduced manual handling of processes. | Incorrect or vulnerable contract logic is executed automatically and may be difficult to stop or correct after deployment. |
| Code immutability | Protects deployed rules against unauthorized modification. | Security vulnerabilities are difficult to remediate after deployment. |
| Deterministic execution | Ensures repeatable and predictable execution of security rules, facilitating verification and correctness analysis. | The outcome depends on the quality of the input data and the trustworthiness of oracles. |
| Transparency and auditability | Facilitates anomaly detection, operational event tracking, and post-incident analysis through persistent and verifiable records of activities. | High transparency can reveal sensitive consumption patterns, network topology, or participant behavior. |
| Integrity of state and rules | Resistance to the manipulation of records and of control and settlement rules. | Integrity does not protect against errors in the code itself. |
| Reduced reliance on trusted third parties | Lower risk of compromise of a central intermediary. | Dependence on oracles, administrators, or the consensus model may still remain. |
| Programmatic enforcement of security policies | Automatic control of access, privileges, and responses to events. | Effectiveness depends on the quality of the designed rules and integration with the OT/IT layer. |

Source: Based on literature synthesis [5,63,68,72–74].

Table 3 indicates that smart contracts can significantly support SG cybersecurity. In particular, programmable automation and verification mechanisms based on distributed consensus algorithms can enhance the security of energy infrastructure. The potential of smart contracts stems primarily from the ability to embed operating rules directly into the network's transaction layer. This enables consistent enforcement of security policies and increased resistance to selected forms of data and process manipulation. At the same time, it should be noted that smart contracts remain dependent on the quality of implementation, the method of integration with OT/IT systems, and the limitations inherent to the smart contract model itself.

## 5. Blockchain for Smart Grid Security Functions

The review of blockchain applications was organized by security functions critical to SG cybersecurity. For the purposes of the study, five functions were distinguished that appear in the literature and in security engineering as distinct issues: (1) establishing the identity of an entity; (2) determining who is authorized to perform a given operation; (3) protecting records against unauthorized modification; (4) securing communication channels against disruption and impersonation; and (5) ensuring privacy and protecting sensitive data.

### *5.1. Authentication and Identity Management*

The distributed architecture of SGs requires the development of secure authentication and identity management mechanisms. The literature highlights security issues in SGs related to device authentication and data integrity (e.g., [75]).

A consortium-blockchain-based authentication mechanism for distributed electricity trading was proposed in [76]. In particular, the proposed architecture introduces a certificate authority into the blockchain network and controls participants' public and private keys to verify the authorization of parties to energy transactions [76]. From a technical perspective, the solution was implemented on Hyperledger Fabric, with business logic encoded in chaincode [76]. Authentication proceeds in two stages: off-chain (initial identity verification) and on-chain (confirmation and recording on the blockchain) [76]. The analyzed solution has the potential to strengthen SG cybersecurity across access control, authentication, and identity management, while also enhancing the integrity of energy transactions.

A blockchain-based authentication protocol employing efficient cryptographic algorithms was proposed in [75] to establish decentralized trust in SGs. The protocol integrates blockchain with authorization, supporting decentralized registration and verification of privileges and thereby reducing dependence on a central authority and SPoF risk [75]. Recording credentials on the blockchain provides tamper-resistant verification and also supports the immutability of registration data and logs [75]. From a technical perspective, the solution employs, among other mechanisms, cryptographic hash functions, one-time passwords, and session updates based on one-time values [75]. Research results indicate that the solution supports the secure establishment of session keys between smart meters and control centers, while maintaining computational and communication efficiency appropriate to a resource-constrained environment [75].

An authentication and key agreement protocol for smart microgrid environments was proposed in [77]. From the technical architecture side, elliptic-curve cryptography (ECC), hardware, physically unclonable functions (PUFs), and a blockchain with the PBFT consensus algorithm were used, among other elements [77]. The communicating parties perform mutual authentication using ECC and PUF and derive a common session key to protect subsequent data exchange [77]. In turn, blockchain stores the results of registration and

authorization, thus supporting decentralized key management and reducing dependence on a central point of trust [77]. The analyzed solution has the potential to strengthen SG cybersecurity by supporting mutual device authentication, secure session key establishment, and protection against eavesdropping, impersonation attacks, and attacks targeting device identities.

In the literature, blockchain is described as a technology that supports authentication and identity management in SGs. Synthesizing the reviewed literature [75–77], the following aspects appear to be particularly valuable for SG cybersecurity:

- Securing identities and privileges through their permanent recording in a distributed ledger;
- Authentication of energy transaction parties and mutual authentication of devices,
- The ability to link an identity to a hardware device;
- Support for secure session key establishment;
- Mitigation of cyberattacks, including impersonation, replay, and MITM attacks.

### *5.2. Access Control and Policy Enforcement*

The literature emphasizes that classical access control mechanisms may be insufficiently suited to the distributed and dynamic nature of SGs [78]. A dynamic attribute-based access control method based on a hybrid blockchain architecture was proposed in [79] to enhance security and trust in smart home energy systems. Conceptually, the analyzed solution builds on the Attribute-Based Access Control model, smart contracts, and the Know Your Customer (KYC) protocol [79]. On the technical side, hybrid integration of Hyperledger Fabric and Hyperledger Besu, CouchDB, universal JSON, and the SHA-256 algorithm were used, among others [79]. The Fabric platform operates as a private, permissioned blockchain and supports internal operations that require controlled access [79]. Besu enforces decentralized access rules and external interactions through a public blockchain network [79]. The results of the analyzed studies indicate significant potential for decentralized, attribute-based access control with identity components based on certificates and KYC.

A blockchain-based access control model for SGs was presented in [78], incorporating privilege levels and peak-hour attributes. The concept extends the ABAC model by incorporating attributes related to permission levels and peak hours [78]. This allows for the prioritization of critical devices during periods of energy constraints [78]. Blockchain was used to store access rights and policies. Smart contracts, in turn, enabled automated policy enforcement, enhancing tamper resistance in access management [78]. From the technical side, Ganache, Node.js, Web3, and Solidity tools were used to implement the proposed solution [78]. The research results indicate that the proposed method can enhance cybersecurity during peak energy demand by supporting the operation of critical devices.

A data-sharing method for SGs that supports access policy updates and traceability was proposed in [80]. The method uses blockchain and hybrid encryption. In particular, the method refers to the ciphertext policy attribute-based encryption (CP-ABE) mechanism and uses smart contracts to eliminate centralized attribute authentication [80]. The access control policy can be updated while maintaining data confidentiality. The data owner can flexibly modify the access control policy, e.g., in the event of irregularities [80]. The research results indicate that the method provides significant cybersecurity support for data sharing within the power grid.

The literature analysis indicates that traditional access control mechanisms may not be fully suited to the distributed nature of SGs. Approaches that integrate blockchain with established access control models and cryptographic mechanisms offer the potential for automated policy enforcement without a central point of trust, as well as decentralized

storage and management of access rights. Synthesizing the reviewed literature [78–80], the following aspects are particularly relevant to SG cybersecurity:

- Enforcement of access policies using smart contracts;
- Policy updates with privacy protection;
- Contextual access control in a distributed environment;
- Reduced risk of SPoFs;
- The ability to trace unauthorized sharing of privileges.

### 5.3. Data Protection Against Manipulation

The reliability of control and monitoring systems in energy infrastructure depends on the integrity of measurement data and control commands [81]. A hierarchical blockchain-based architecture for auditing measurement integrity in distributed energy resources (DERs) was proposed in [81]. In particular, a lightweight Merkle-tree anchoring scheme was developed that supports data integrity without relying on a single trusted third party. The implementation used, among other components, Geth (an Ethereum protocol implementation), Node.js, the web3.js library, the JSON-RPC API, and Solidity for smart contract programming [81]. The reported results indicate significant potential to support SG cybersecurity in residential low-voltage networks. In particular, the analyzed solution supports the detection of measurement data tampering and the protection of control commands.

Study [82] presented significant findings related to data integrity by proposing a method for detecting false data injection attacks (FDIAs) in microgrids. The overall concept combines signal analysis for extracting relevant features from data, support vector machine (SVM) learning for anomaly detection, and blockchain technology to enhance data integrity and transparency [82]. It is worth noting that the SVM model can leverage blockchain's immutability and distributed ledger capabilities [82]. The research results indicate a significant improvement in cybersecurity in power grids through greater resistance to data manipulation and a reduced risk of making erroneous control decisions based on falsified measurements.

A blockchain-based method supporting data integrity in IoT-enabled renewable and grid energy metering systems was presented in [83]. In particular, the presented method supports the integrity of settlements between prosumers and energy suppliers. The developed framework integrates blockchain and IoT for energy monitoring with an immutable proof of integrity on-chain. On the technical side, the following were used: the Ganache environment for Ethereum, the local InfluxDB database for receiving MQTT messages in JSON format, and Solidity for programming a smart contract with the implementation of SHA-256 cryptographic hashes [83]. Integrity verification involves comparing a recalculated hash from the local InfluxDB database with a hash loaded from the blockchain [83]. Research results indicate significant potential to ensure the integrity of measurement data, protect against tampering, and support the auditability and transparency of energy billing.

A reputation-based blockchain architecture was proposed in [84] to protect smart AMI systems against data tampering and FDIAs. The analyzed concept includes two types of blockchains. The first blockchain ensures the integrity of measurements transmitted from smart meters to concentrators [84]. The second blockchain protects measurements between the concentrator and the control center [84]. It is also worth noting that the proposed architecture introduces a PoR-BFT consensus protocol that integrates reputation-based consensus with PBFT [84]. The system was implemented using the Hyperledger Fabric framework. The research results indicate that the presented architecture significantly protects measurements transmitted from smart meters to the control center and counteracts FDIAs.

The literature analysis indicates that blockchain has significant potential to support data integrity and protect against data manipulation in SGs. It should be noted that a distributed ledger does not prevent a compromised data source, such as a sensor, from generating false measurements, nor does it detect FDIAs before the data are recorded in the ledger. Synthesizing the reviewed studies [81–84], the following aspects are particularly important for data integrity:

- Distributed auditing of measurement records already submitted to the ledger;
- Recording of AMI readings resistant to subsequent changes, separate from the protection of the meter itself;
- Recording and subsequent verification of control commands;
- Support for detection and analysis of FDIAs;
- Verification of data integrity by comparing locally stored data with hashes recorded on the blockchain.

### *5.4. Resilience to Cyberattacks and Secure Communication*

The integration of energy networks into the environment of information systems and computer networks expands the threat horizon to include various cyberattacks. In particular, SGs are vulnerable to attacks that may compromise key information security attributes, including confidentiality, availability, and integrity (e.g., [1,4]). Potential attack types include DoS, DDoS, MITM, FDIA, SQL injection, and malware attacks, among others (e.g., [2,85–89]). In the face of growing threats, a number of studies have emerged on the use of blockchain in SGs to counter cyberattacks.

A blockchain-based communication protocol designed to provide resilient communication in SGs was presented in [90]. The protocol uses, among others, the SHA-256 hash function, the AEAD cryptographic method, and elliptic curve cryptography [90]. Blockchain, combined with the PBFT consensus mechanism, is used to secure and persist data after a communication session is established between a service provider and a smart meter [90]. The reported security analysis indicates that the proposed protocol counteracts, among others, MITM, DoS, privileged insider, impersonation, replay, and anonymity attacks [90].

A blockchain-based protocol supporting data protection and transaction management in SGs through digital signatures and certificates was proposed in [91]. The main components of the proposed solution include smart meters, service providers, a registration authority, and a cloud server [91]. Smart meters and service providers receive security tokens after registering with the registration authority. The protocol employs an elliptic-curve-based digital signature algorithm and PBFT as the consensus mechanism. Service provider data is stored in a private blockchain, ensuring an immutable record of transactions [91]. The reported results indicate that the method provides protection against several types of attacks, including, among others, MITM, session hijacking, replay, impersonation, privileged insider, key escrow, side-channel, and forgery attacks [91].

A blockchain-based method for load frequency control (LFC) in SGs under DoS attacks was proposed in [92]. When a DoS attack targets the communication channel, interruption of control signal exchange can lead to a deterioration of frequency stability [92]. The proposed solution relies on a private blockchain using the PoW algorithm to store copies of control data and enable recovery of valid information during an attack [92]. The blockchain is combined with classical PI control and with an H-infinity controller [92]. The reported results indicate that the proposed blockchain-H-infinity approach outperforms traditional controllers in protecting LFC systems against DoS attacks [92].

Literature analysis indicates that blockchain can support the replay and accountability of communication records. However, it should be noted that it does not maintain a

broken channel and does not replace authentication or session protection. Synthesizing the reviewed literature [90–92], the following blockchain applications are particularly relevant to SG cybersecurity:

- Supporting communication security and accountability by recording authenticated readings, transactions, or control commands;
- Ensuring persistent and tamper-resistant storage of measurement data and transactions on the blockchain;
- Storing approved copies of control data to support record recovery after DoS and DDoS attacks.

### 5.5. Privacy and Protection of Sensitive Data

Privacy and the protection of sensitive data are key challenges in implementing the SG concept. Information transmitted over the network, e.g., regarding energy consumption or the type of devices used, creates the potential for user profiling [12]. Protecting energy consumption profiles while maintaining data usability and network efficiency remains challenging, especially given the limited resources of smart meters [93].

A blockchain-based privacy-preserving data aggregation scheme for SGs was presented in [94]. In particular, the proposed approach enables privacy-preserving aggregation of metering data while maintaining operation in the presence of failures affecting some smart meters or servers [94]. Meter readings are masked with random numbers to prevent disclosure of individual consumption profiles during aggregation [94]. Furthermore, a Shamir threshold secret sharing scheme was used, which supports operation even when some smart meters do not transmit data or some servers are unavailable [94]. In turn, blockchain is used for distributed data storage, reducing the risk of a SPoF or attack [94]. The implementation was carried out using, among others, the Java and Python programming languages, the matplotlib and numpy libraries, and the Flask framework [94]. The blockchain was implemented in the Hyperledger Fabric environment with the Raft consensus mechanism [94]. The results of the reviewed studies indicate that the proposed method can protect the privacy of smart-meter data while preserving correct aggregation even if some meters or servers fail or come under attack.

A method combining user privacy protection with secure authentication for SGs and electric vehicles in a vehicle-to-grid scenario was presented in [95]. The proposed method assumes four entities operating within the blockchain network, i.e., the supervisor, the smart grid, the holder, and the verifier [95]. The study utilized, among other techniques, decentralized identifiers, zero-knowledge proofs (ZKPs), and Pedersen commitments [95]. The study results indicate significant potential for enhancing privacy in SGs. In particular, users can employ anonymous identifiers that cannot be easily linked to their real identities [95].

The study [96] developed a method for secure peer-to-peer energy trading that combines machine learning and blockchain. Among other elements, the study presented a dynamic time-series clustering algorithm for federated zero-knowledge machine learning (ZKML) [96]. In the proposed approach, ML model computations are performed off-chain, and only zero-knowledge proofs attesting to the correctness of the results are submitted to the blockchain, thereby protecting user data [96]. A smart contract was also developed to verify the ZKML proof, confirming the correctness of the model's inference without revealing private input data [96]. The results indicate that the proposed method increases the privacy of P2P trading participants while maintaining the ability to verify operations.

Literature analysis indicates that blockchain, combined with additional cryptographic mechanisms, can play an important role in protecting privacy in SGs. The reviewed studies [94–96] show that blockchain-based approaches can support, in particular:

- Aggregation of measurements without disclosing an individual consumption profile;
- Anonymization of identity while retaining the ability to oversee malicious activity;
- Verifiable inference in energy trading without publishing raw data on the blockchain.

## 6. Barriers and Limitations of Blockchain Implementation in Smart Grids

Despite the cybersecurity applications discussed above, the literature identifies several barriers and limitations associated with implementing blockchain in SG environments. In particular, it is indicated that the challenges related to blockchain technology result, among other things, from transaction throughput, scalability, and energy demand of consensus protocols [97]. Synthesizing the literature on the subject [5,98–104], the following barriers and limitations, among others, can be listed:

1. Scalability: Limited transaction throughput may be related to blockchain technology's scalability problem [101]. Blockchain provides high tamper resistance but is associated with relatively high latency [105]. SGs involve numerous distributed components that generate a large volume of events and data. As the number of SG components increases, blockchain throughput and latency may therefore become insufficient for systems operating under quasi-real-time requirements. The literature also indicates that storing raw data and performing real-time control are not well-suited to on-chain processing [99]. Blockchain solutions for SGs should therefore scale with the increasing number of devices and events while maintaining acceptable latency.
2. Interoperability and compatibility: Individual blockchains deployed in SGs may operate on different consensus models, transaction formats, smart-contract rules, or access policies. On the other hand, SGs integrate multiple heterogeneous systems, such as AMI, SCADA, IT systems, and energy trading platforms. The lack of uniform standards hinders the exchange of data and services between operators, suppliers, users, and the market layer. Blockchain protocols and standards are still emerging, making it difficult to ensure compatibility between blockchain platforms and energy grid systems [106]. Difficulties are also noted in integrating blockchain with legacy systems and in meeting functional requirements in energy systems [102].
3. Demand for computing power: The growing number of IoT devices increases the volume of transactions to be processed and requires a sufficiently efficient computational base [103]. Energy-intensive consensus algorithms may be poorly suited to the critical infrastructure of power grids. Even lighter algorithms may require a compromise between cryptographic security and node resources. It should be noted that some SG end devices have limited hardware resources and may not be able to handle heavy public key cryptography [100]. Security mechanisms should therefore minimize computational overhead without compromising protection and privacy. Possible approaches include greater reliance on symmetric encryption and hash functions while limiting frequent signing and signature verification operations [100]. At the same time, moving computation onto other components introduces new architectural dependencies. Furthermore, smart contracts entail a certain computational cost [5].
4. Data privacy: A distributed ledger is, in its original design, public and replicated across the nodes of the network. However, replicating data such as payment records, energy generation data, and consumption information may lead to the disclosure of sensitive information [104]. Public verifiability and transparency can conflict with privacy, which is one of the fundamental requirements of SGs. In addition, blockchain may be vulnerable, among other things, to key leakage, disclosure of energy-consumption patterns, 51% attacks, and threats associated with selfish node behavior and reputation [103]. At the same time, the literature suggests that privacy does not necessarily constitute a major barrier to blockchain adoption in SGs. It is

noted that, compared with traditional centralized solutions, blockchain may provide users with a higher level of privacy protection and greater control over data [101].

5. Programming barriers: Smart contract programming languages may be limited by the lack of certain programming constructs compared to classical programming languages such as Java, Python, or C++. In particular, constraints on data types and floating-point operations may complicate the implementation of complex calculations used in energy systems, such as power-flow computations [5]. At the same time, in a cybersecurity context, the literature indicates that blockchain could offer developers primitives for building a more secure application than classical solutions [101].

In addition to technical limitations, the literature also identifies legal, social, and economic barriers that may hinder the adoption of blockchain in SGs (e.g., [5,98,102,106]).

The barriers and limitations discussed above do not affect all information security attributes to the same degree. Table 4 analyzes their impact on individual information security attributes and identifies potential measures to mitigate their effects in SG environments.

**Table 4.** Blockchain implementation limitations and their mitigation in smart grids, organized by information security attributes.

| Information Security Attribute | Limitations | Mitigation |
|---|---|---|
| Confidentiality | Ledger transparency, public visibility, and data replication may enable profiling based on metering data and transaction patterns. | Permissioned networks; minimization of the on-chain record; sensitive data as hashes/aggregates or off-chain. |
| Availability | Possibly low throughput as the volume of AMI/IoT events grows; possibly high latency and slow finality; high computational cost on end devices. | Permissioned networks; lower-latency BFT algorithms; off-chain processing; recording only critical events on-chain; shifting consensus operations to gateways and more resource-capable nodes. |
| Integrity | Incorrect or malicious data may become persistent once committed; native contract languages may not directly support the data types required for complex power-system calculations. | Data validation before on-chain recording; smart contract testing and formal verification; off-chain correction mechanisms with audit trails; off-chain numerical computation, with only results and proofs, or hashes, recorded on-chain. |
| Accountability | In public models, actions are linked to cryptographic addresses rather than directly to identifiable SG entities or components; correcting state and determining who is authorized to modify it may be difficult. | Permissioned models with identifiable participants and components; access control policies and off-chain logs linked to on-chain hashes. |
| Non-Repudiation | Probabilistic or delayed finality may reduce the evidentiary value of blockchain records. | Deterministic finality (BFT/permissioned); a timestamp bound to the record; attribution of actors. |
| Authenticity | Limited resources of smart meters and sensors may constrain the use of PKI and frequent digital signature verification. | Lightweight cryptography and authentication at the gateway; certificates in a permissioned model. |

Source: Based on literature synthesis [5,98–104].

The analysis of information security attributes in the context of blockchain limitations in SGs indicates that a distributed ledger alone should not be expected to ensure them. Blockchain implementation in SGs should therefore be designed in combination with

permissioned architectures, off-chain mechanisms, cryptographic techniques, and privacy-preserving solutions.

## 7. Blockchain Framework for Smart Grid Cybersecurity

Based on the conducted analyses, the BC-Sec-SG framework was developed to systematize the application of blockchain in SG cybersecurity. Information security attributes constitute the axis of the assessment. The BC-Sec-SG framework is relevant to the research questions posed. Specifically, it integrates SG cybersecurity requirements and layers (RQ1), consensus algorithms and smart contracts (RQ2), security functions (RQ3), and implementation limitations (RQ4). Figure 2 presents the BC-Sec-SG framework.

Information security attributes remain a key determinant of SG cybersecurity. Blockchain is considered when it addresses SG cybersecurity requirements and is applicable to the business, application, communication, or power layers.

SG cybersecurity requirements, the consensus protocol, and the trust model are positioned above the architectural layers. They do not constitute additional SG layers, but rather a condition from which an entry in the ledger can enhance information security attributes. In line with the analysis of consensus algorithms for energy infrastructure, the framework assumes a permissioned network using PBFT, PoA, or another mechanism providing deterministic or near-deterministic finality. PoW and public PoS were retained as an analytical reference point or as hybrid support.

Each layer summarizes the mechanisms associated with a distributed ledger, omitting network channel primitives that are not derived from blockchain. The right column with information security attributes specifies the extent of support for the attribute, but does not guarantee it. Consensus latency relative to timing requirements, OT device resources, interoperability, compatibility, programming limitations, and legal, social, and economic barriers constitute the limitations of the overall framework.

The proposed BC-Sec-SG framework does not expand the scope of blockchain applications already discussed in the literature, but rather organizes them from a different analytical perspective. Distributed ledger mechanisms are linked to SG cybersecurity requirements, architectural layers, information security attributes, consensus mechanisms, trust assumptions, and appropriate boundary conditions. This framework facilitates the assessment of the conditions under which individual blockchain mechanisms can support specific security functions and the distinction between properties supported at the ledger level and those requiring complementary off-chain processing or conventional security mechanisms. Blockchain technology should therefore be considered a complement, not a replacement, for existing security mechanisms used in SGs.

Table 5 presents two example use cases for the BC-Sec-SG framework. The analyzed use cases include AMI meter reading and device firmware updates. However, these examples do not constitute an experiment or validation of the framework. The purpose is to illustrate how the framework can be used to separate the mechanisms that operate before a record is accepted on the blockchain, the data stored in the ledger, and the limitations.

The scenarios presented in Table 5 illustrate the application of the BC-Sec-SG framework to protect data authenticity and integrity. They correspond to the solution directions discussed in Section 5. For the AMI meter reading, the use case demonstrates how record protection can be separated from the source measurement's accuracy. Recording in the ledger can ensure the durability of the record, confirm its origin, and facilitate detection of subsequent modifications. However, it does not confirm the accuracy of the measurement if the disrupted meter generated an erroneous value before recording it in the ledger. In the firmware update use case, blockchain can support verification of its origin and integrity. The ledger can record the approved firmware hash, version, publisher, and digital signature,

enabling verification. However, it does not guarantee secure installation or correct device operation after the update.

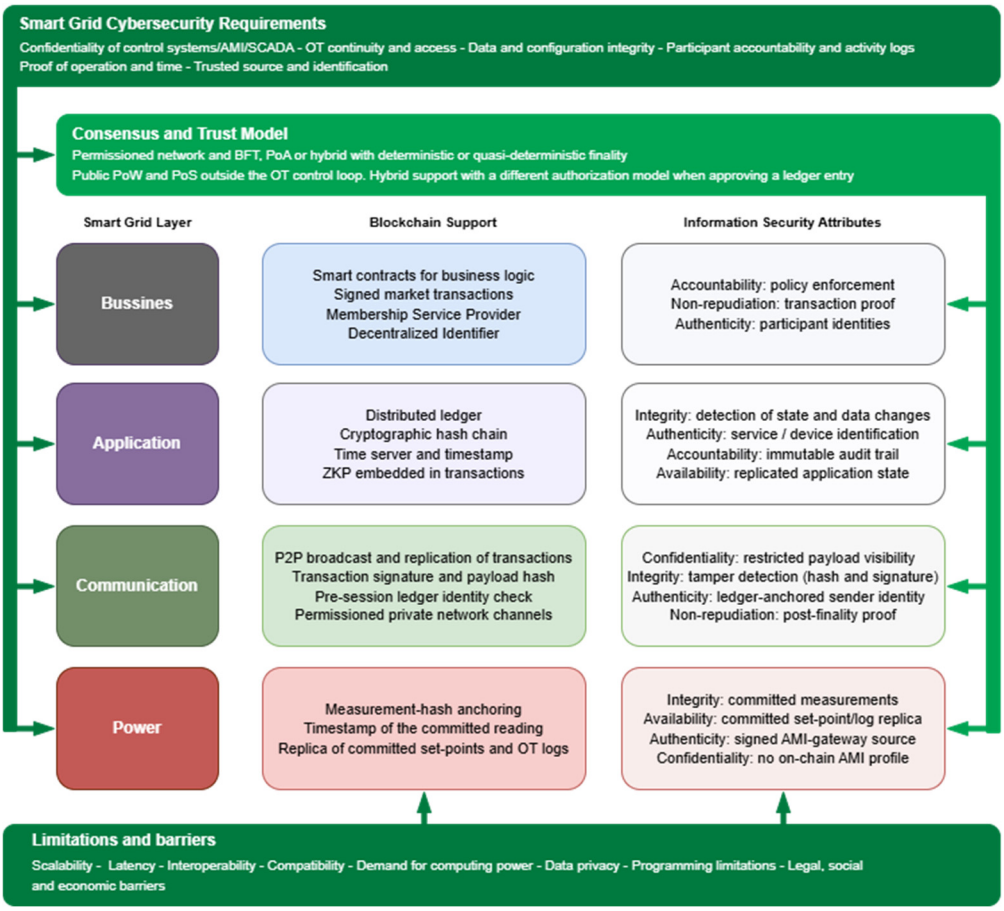



**Figure 2.** The BC-Sec-SG framework for blockchain support of smart grid cybersecurity. Source: Own work.

**Table 5.** Illustrative application of the BC-Sec-SG framework.

| Analysis Aspect | AMI Meter Reading | Device Firmware Update |
|---|---|---|
| Layer | Application—Data; Communication | Application—Software; Communication |
| Security attribute | Record authenticity and integrity | Update authenticity, integrity, and non-repudiation |
| Ledger type and consensus | Permissioned; BFT among billing-organization nodes; the meter does not validate | Permissioned; BFT among utility and vendor nodes; the device does not validate |
| On-ledger record | Reading hash; meter and interval identifiers; signature; verification result | Firmware hash; version, issuer; device identifier; signature |
| Off-ledger security mechanisms | Device signature; certificate-based authentication; key management; replay protection | Issuer signature; device identification; firmware version and hash verification; secure boot |
| Limitations | A signed record may contain an incorrect measurement | Correct recording does not guarantee safe installation or proper operation of the device |

Source: Own work.

## 8. Conclusions

The article presented a review of blockchain applications supporting SG cybersecurity, structured according to an extended set of information security attributes. The analyses conducted showed that distributed ledger mechanisms, including consensus algorithms, smart contracts, hash chains, cryptographic signatures, and timestamps, can support selected information security attributes in individual network layers.

With regard to the first research question (RQ1), SG cybersecurity requirements stem from the cyber–physical and layered architecture of the grid, as well as from the information security attributes of confidentiality, integrity, availability, accountability, non-repudiation, and authenticity. Depending on the network layer, these include, among others, the protection of AMI operational and measurement data, timely access and OT business continuity, detection of unauthorized changes, verifiable evidence of operations and their timing, actor and device attribution, and source traceability.

Regarding the second research question (RQ2), it is important that consensus algorithms in themselves do not guarantee information security attributes. Network consensus determines the point at which data recorded in the distributed ledger is secured and difficult to challenge. The choice of consensus algorithm affects network latency, the type of finality achieved, and the level of trust placed in validators. In an SG environment, permissioned networks and BFT and PoA algorithms may find particular application. Smart contracts, in turn, support accountability, enable the definition of security rules and policies, and enforce their execution. However, the correctness of the code implementing the smart contract logic is crucial.

The third research question (RQ3) concerns the support of SG security functions by blockchain mechanisms. In particular, the literature documents applications in, among others, authentication and identity management, access control and policy enforcement, protection against manipulation and cyberattacks, and support for the privacy of sensitive data. However, it should be noted that distributed ledger mechanisms were, in most cases, components of the analyzed solutions rather than systems based solely on the blockchain. In terms of communication, blockchain does not directly protect the OT channel but supports the security of the signed payload, which is anchored in the distributed ledger. Similarly, in the power layer, it is possible to protect the write history after finalization, but not guarantee the control loop in real-time systems.

Regarding the fourth research question (RQ4), the main barriers and limitations include scalability, latency, interoperability, compatibility with existing systems, computational demands, the trade-off between ledger transparency and privacy, and legal, organizational, and economic challenges.

The answer to the fifth research question (RQ5) synthesizes the conducted analyses. The developed BC-Sec-SG framework integrates SG cybersecurity requirements (RQ1), consensus conditions and smart contracts (RQ2), support for SG security functions (RQ3), and implementation limitations (RQ4). The architectural layers serve as reference points, while information security attributes constitute the assessment criteria. It should be noted that the BC-Sec-SG framework indicates the scope of possible support, not a guarantee of meeting requirements. Blockchain is considered a complement to existing mechanisms where a consensus-based, attributable, and accountable record is required.

Regarding the limitations of this study, it should be noted that the article presents a literature review rather than a systematic literature review. It should also be emphasized that the BC-Sec-SG framework is conceptual in nature and has not been tested in a real SG infrastructure environment. Furthermore, the assessment of individual information security attributes is presented in a technical sense, without analysis or resolution of legal implications.

Future research should include empirical comparisons of selected blockchain mechanisms against the timing and resource requirements of the OT layer, as well as validation of the BC-Sec-SG framework in real-world SG operational scenarios.

**Author Contributions:** Conceptualization, H.S. and E.K.S.; methodology, H.S. and E.K.S.; investigation, H.S. and E.K.S.; resources, H.S. and E.K.S.; writing—original draft preparation, H.S. and E.K.S.; writing—review and editing, H.S. and E.K.S.; visualization, H.S. and E.K.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| ABAC | Attribute-Based Access Control |
| AEAD | Authenticated Encryption with Associated Data |
| AMI | Advanced Metering Infrastructure |
| API | Application Programming Interface |
| BC-Sec-SG | Blockchain Security for Smart Grid (framework) |
| BFT | Byzantine Fault Tolerance |
| CPS | Cyber–Physical System |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| DPoS | Delegated Proof-of-Stake |
| ECC | Elliptic Curve Cryptography |
| FDIA | False Data Injection Attack |
| GIS | Geographic Information System |
| ICT | Information and Communication Technology |
| IED | Intelligent Electronic Device |
| IoT | Internet of Things |
| ISO/OSI | International Organization for Standardization/Open Systems Interconnection |
| JSON | JavaScript Object Notation |
| KYC | Know Your Customer |
| LFC | Load Frequency Control |
| MQTT | Message Queuing Telemetry Transport |
| OT | Operational Technology |
| OT/IT | Operational Technology/Information Technology |
| P2P | Peer-to-Peer |
| PBFT | Practical Byzantine Fault Tolerance |
| PKI | Public Key Infrastructure |
| PLC | Programmable Logic Controller |
| PMU | Phasor Measurement Unit |
| PoA | Proof-of-Authority |
| PoS | Proof-of-Stake |
| PoW | Proof-of-Work |
| PUF | Physically Unclonable Function |
| RQ | Research Question |
| RPC | Remote Procedure Call |
| RTU | Remote Terminal Unit |
| SCADA | Supervisory Control and Data Acquisition |
| SG | Smart Grid |

| | |
|---|---|
| SHA | Secure Hash Algorithm |
| SPoF | Single Point of Failure |
| SQL | Structured Query Language |
| SVM | Support Vector Machine |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| ZKML | Zero-Knowledge Machine Learning |
| ZKP | Zero-Knowledge Proof |

## References


1. Alomari, M.A.; Al-Andoli, M.N.; Ghaleb, M.; Thabit, R.; Alkawsi, G.; Alsayaydeh, J.A.J.; Gaid, A.S.A. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. *Energies* **2025**, *18*, 141. [CrossRef]
2. Bouslimani, M.; Benbouzid-Si Tayeb, F.; Amirat, Y.; Benbouzid, M. Cyber-Physical Security in Smart Grids: A Comprehensive Guide to Key Research Areas, Threats, and Countermeasures. *Appl. Sci.* **2025**, *15*, 12367. [CrossRef]
3. Aklilu, Y.T.; Ding, J. Survey on Blockchain for Smart Grid Management, Control, and Operation. *Energies* **2022**, *15*, 193. [CrossRef]
4. Amanlou, S.; Hasan, M.K.; Asma' Mokhtar, U.; Mahmood Malik, K.; Islam, S.; Khan, S.; Attique Khan, M.; Asghar Khan, M. Cybersecurity Challenges in Smart Grid Systems: Current and Emerging Attacks, Opportunities, and Recommendations. *IEEE Open J. Commun. Soc.* **2025**, *6*, 1965–1997. [CrossRef]
5. 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]
6. Zhuang, P.; Zamir, T.; Liang, H. Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3–19. [CrossRef]
7. Waseem, M.; Adnan Khan, M.; Goudarzi, A.; Fahad, S.; Sajjad, I.A.; Siano, P. Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies* **2023**, *16*, 820. [CrossRef]
8. Szczepaniuk, E.K.; Szczepaniuk, H. Cybersecurity of Smart Grids: Requirements, Threats, and Countermeasures. *Energies* **2025**, *18*, 5017. [CrossRef]
9. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
10. Lin, I.-C.; Kuo, Y.-H.; Chang, C.-C.; Liu, J.-C.; Chang, C.-C. Symmetry in Blockchain-Powered Secure Decentralized Data Storage: Mitigating Risks and Ensuring Confidentiality. *Symmetry* **2024**, *16*, 147. [CrossRef]
11. Saini, A.; Krishan, K.; Gaur, M.S. Analyzing ICS security: A survey of design principles, risks, threats, and mitigation methods. *Comput. Electr. Eng.* **2026**, *132*, 110967. [CrossRef]
12. Nazir, I.; Mushtaq, N.; Amin, W. Smart Grid Systems: Addressing Privacy Threats, Security Vulnerabilities, and Demand–Supply Balance (A Review). *Energies* **2025**, *18*, 5076. [CrossRef]
13. Lallie, H.S.; Thompson, A.; Titis, E.; Stephens, P. Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. *Computers* **2025**, *14*, 49. [CrossRef]
14. Elbez, G.; Keller, H.B.; Bohara, A.; Nahrstedt, K.; Hagenmeyer, V. Detection of DoS Attacks Using ARFIMA Modeling of GOOSE Communication in IEC 61850 Substations. *Energies* **2020**, *13*, 5176. [CrossRef]
15. Taherdoost, H. Cybersecurity vs. Information Security. *Procedia Comput. Sci.* **2022**, *215*, 483–487. [CrossRef]
16. Argento, L.; Buccafurri, F.; Furfaro, A.; Graziano, S.; Guzzo, A.; Lax, G.; Pasqua, F.; Saccà, D. ID-Service: A Blockchain-Based Platform to Support Digital-Identity-Aware Service Accountability. *Appl. Sci.* **2021**, *11*, 165. [CrossRef]
17. Chang, Y.-F.; Tai, W.-L.; Fung, K.-H. Offline User Authentication Ensuring Non-Repudiation and Anonymity. *Sensors* **2022**, *22*, 9673. [CrossRef] [PubMed]
18. Kremer, S.; Markowitch, O.; Zhou, J. An intensive survey of fair non-repudiation protocols. *Comput. Commun.* **2002**, *25*, 1606–1621. [CrossRef]
19. Acheampong, R.; Popovici, D.-M.; Balan, T.; Rekeraho, A.; Ramos, M.S. Enhancing Security and Authenticity in Immersive Environments. *Information* **2025**, *16*, 191. [CrossRef]
20. Wei, T.; Li, H.; Miao, J. Integration and Development Path of Smart Grid Technology: Technology-Driven, Policy Framework and Application Challenges. *Processes* **2025**, *13*, 2428. [CrossRef]
21. Rajendran, G.; Raute, R.; Caruana, C. A Comprehensive Review of Solar PV Integration with Smart-Grids: Challenges, Standards, and Grid Codes. *Energies* **2025**, *18*, 2221. [CrossRef]
22. Shees, A.; Tariq, M.; Sarwat, A.I. Cybersecurity in Smart Grids: Detecting False Data Injection Attacks Utilizing Supervised Machine Learning Techniques. *Energies* **2024**, *17*, 5870. [CrossRef]
23. Kiasari, M.; Aly, H. Agentic Artificial Intelligence for Smart Grids: A Comprehensive Review of Autonomous, Safe, and Explainable Control Frameworks. *Energies* **2026**, *19*, 617. [CrossRef]

24. Matta, C.; Pinna, S.; Ortu, S.; Parodo, F.; Giusto, D.; Anedda, M. A Survey on IoT-Based Smart Electrical Systems: An Analysis of Standards, Security, and Applications. *Energies* **2026**, *19*, 965. [CrossRef]
25. CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture. 2012. Available online: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/reference_architecture_smartgrids.pdf (accessed on 9 October 2026).
26. Gopstein, A.; Nguyen, C.; O'Fallon, C.; Hastings, N.; Wollman, D. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0*; NIST Special Publication 1108r4; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021. [CrossRef]
27. Tanchangya, T.; Sarker, T.; Rahman, J.; Islam, M.S.; Islam, N.; Siddiqi, K.O. Mapping Blockchain Applications in FinTech: A Systematic Review of Eleven Key Domains. *Information* **2025**, *16*, 769. [CrossRef]
28. Ziegler, M.H.; Nowostawski, M.; Katt, B. A Systematic Literature Review of Information Privacy in Blockchain Systems. *J. Cybersecur. Priv.* **2025**, *5*, 65. [CrossRef]
29. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 10 July 2026).
30. Arafat, S.M. A study of blockchain consensus protocols. *Cybersecurity* **2026**, *9*, 120. [CrossRef]
31. Duan, S.; Reiter, M.K.; Zhang, H. BEAT: Asynchronous BFT Made Practical. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), Toronto, ON, Canada, 15–19 October 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 2028–2041. [CrossRef]
32. Merlina, A.; Garrett, T.; Vitenberg, R. On Replacing Cryptopuzzles with Useful Computation in Blockchain Proof-of-Work Protocols. *ACM Comput. Surv.* **2026**, *58*, 358. [CrossRef]
33. Lasla, N.; Al-Sahan, L.; Abdallah, M.; Younis, M. Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. *Comput. Netw.* **2022**, *214*, 109118. [CrossRef]
34. Alhamrani, R.H.; Bamashmoos, F.O.; Khairallah, E.F. Trustworthy Federated Learning with Blockchain-Based Consensus for Mitigating Poisoning Attacks in Healthcare Systems. *Information* **2026**, *17*, 201. [CrossRef]
35. Yonezawa, N. Proof of Team Sprint: A Collaborative Consensus Algorithm for Reducing Energy Consumption in Blockchain Systems. *IET Blockchain* **2026**, *6*, e70034. [CrossRef]
36. El-Kosairy, A.; Aslan, H.; AbdelBaki, N. IRDS4C–CTIB: A Blockchain-Driven Deception Architecture for Ransomware Detection and Intelligence Sharing. *Future Internet* **2026**, *18*, 66. [CrossRef]
37. Cruz-González, V.D.; Benítez-Pérez, H.; Aldeco-Pérez, R. Modeling the Energy Consumption of a Public Blockchain as a Stochastic Process. *Mathematics* **2026**, *14*, 2282. [CrossRef]
38. Amamra, S.-A. A Hybrid Blockchain Solution for Electric Vehicle Energy Trading: Balancing Proof of Work and Proof of Stake. *Energies* **2025**, *18*, 1840. [CrossRef]
39. Tao, G.; Zhou, X.; Wang, C. Beyond Energy: Semiconductor Efficiency as the Structural Driver of Proof-of-Work Resource Consumption and Market Concentration. *Sustainability* **2026**, *18*, 4913. [CrossRef]
40. John, K.; Rivera, T.J.; Saleh, F. Proof-of-Work versus Proof-of-Stake: A Comparative Economic Analysis. *Rev. Financ. Stud.* **2025**, *38*, 1955–2004. [CrossRef]
41. Ethereum. Proof-of-Stake (PoS). Available online: https://ethereum.org/developers/docs/consensus-mechanisms/pos/ (accessed on 10 July 2026).
42. Ethereum. Block Proposal. Available online: https://ethereum.org/developers/docs/consensus-mechanisms/pos/block-proposal/ (accessed on 10 July 2026).
43. Ethereum. Proof-of-Stake Rewards and Penalties. Available online: https://ethereum.org/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/ (accessed on 10 July 2026).
44. Hacıfevzioğlu, A.; Kalkan, K. EDPoS: Energy-Aware Delegated Proof of Stake for resource-constrained devices. *Comput. Netw.* **2026**, *288*, 112608. [CrossRef]
45. Liu, A.; An, Q.; Xie, S.; Yan, Y. SQDPoS: A Secure and Practical Semi-Quantum Blockchain System for the Post-Quantum Era. *Computers* **2026**, *15*, 210. [CrossRef]
46. Shen, Z.; Qu, Q.; Chen, X.-B. Blockchain Consensus Mechanisms: A Comprehensive Review and Performance Analysis Framework. *Electronics* **2025**, *14*, 3567. [CrossRef]
47. Ethereum. Proof-of-Authority (PoA). Available online: https://ethereum.org/developers/docs/consensus-mechanisms/poa/ (accessed on 14 July 2026).
48. Techskill Brew. Proof of Authority or PoA in Blockchain (Part 11—Blockchain Series). *Medium*, 8 February 2022. Available online: https://medium.com/techskill-brew/proof-of-authority-or-poa-in-blockchain-part-11-blockchain-series-be15b3321cba (accessed on 14 July 2026).
49. Švarcmajer, M.; Kohler, M.; Krpić, Z.; Lukić, I. Consensus-Driven Framework for Data-Driven Optimization of Distributed Systems Through Blockchain Consensus Mechanism Selection. *Big Data Cogn. Comput.* **2026**, *10*, 154. [CrossRef]

50. Lu, S.-P.; Lei, C.-L.; Tsai, M.-H. An efficient Proof-of-Authority consensus scheme against cloning attacks. *Comput. Commun.* **2024**, *228*, 107975. [CrossRef]
51. Mohan, G.; Shanmugavel, T.R. ADeepCRF: Real-Time Threat Detection in IoT Network Using Blockchain-Based Advanced Proof of Authority and Adaptive Deep Conditional Random Fields. *Sci. Rep.* **2026**, *16*, 18080. [CrossRef] [PubMed]
52. Wankhede, S.B.; Patel, D. The Proof of Authority Consensus Algorithm for IIoT Security. In *Proceedings of the International Conference on Recent Innovations in Computing (ICRIC 2022)*; Singh, Y., Verma, C., Zoltán, I., Chhabra, J.K., Singh, P.K., Eds.; Springer: Singapore, 2023; Volume 1011, pp. 803–811. [CrossRef]
53. Wu, X.; Chang, J.; Ling, H.; Feng, X. Scaling proof-of-authority protocol to improve performance and security. *Peer-Peer Netw. Appl.* **2022**, *15*, 2633–2649. [CrossRef]
54. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99), New Orleans, LA, USA, 22–25 February 1999*; USENIX: Berkeley, CA, USA, 1999. Available online: https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance (accessed on 22 July 2026).
55. Du, D.; Feng, W.; Huang, M.; Feng, S.; Wang, J. Research on Consensus Algorithm for Intellectual Property Transactions Based on Practical Byzantine Fault Tolerant (PBFT) Algorithm. *Electronics* **2025**, *14*, 1665. [CrossRef]
56. Lin, J.; Zheng, J. DC-PBFT: A Censorship-Resistant PBFT Consensus Algorithm Based on Power Balancing. *Electronics* **2026**, *15*, 1818. [CrossRef]
57. Zhang, G.; Pan, F.; Mao, Y.; Tijanic, S.; Dang'Ana, M.; Motepalli, S.; Zhang, S.; Jacobsen, H.-A. Reaching Consensus in the Byzantine Empire: A Comprehensive Review of BFT Consensus Algorithms. *ACM Comput. Surv.* **2024**, *56*, 134. [CrossRef]
58. Chen, R.; Zhu, R.; Wang, L. NetTopoBFT: Network Topology-Aware Byzantine Fault Tolerance for High-Coverage Consortium Blockchains. *Entropy* **2025**, *27*, 1088. [CrossRef] [PubMed]
59. Shamaseen, A.; Qatawneh, M.; Elshqeirat, B. Smart Grid System Based on Blockchain Technology for Enhancing Trust and Preventing Counterfeiting Issues. *Energies* **2025**, *18*, 3523. [CrossRef]
60. Yu, Y.; Liu, G.-P.; Huang, Y.; Chung, C.Y.; Li, Y.-Z. A Blockchain consensus mechanism for real-time regulation of renewable energy power systems. *Nat. Commun.* **2024**, *15*, 10620. [CrossRef] [PubMed]
61. Sun, H.; Weingärtner, T. A Blockchain-Based Architecture for Energy Trading to Enhance Power Grid Stability. *Electronics* **2025**, *14*, 4629. [CrossRef]
62. Wang, H.; Liu, X.; Chen, J. RVR Blockchain Consensus: A Verifiable, Weighted-Random, Byzantine-Tolerant Framework for Smart Grid Energy Trading. *Computers* **2025**, *14*, 232. [CrossRef]
63. Honari, K.; Rouhani, S.; Falak, N.E.; Liu, Y.; Li, Y.; Liang, H.; Dick, S.; Miller, J. Smart Contract Design in Distributed Energy Systems: A Systematic Review. *Energies* **2023**, *16*, 4797. [CrossRef]
64. Santos, L.; Gomes, A.; Rupino, P. Energy trading using blockchain: Smart contracts functionalities—A Systematic Review. *Energy Strategy Rev.* **2025**, *61*, 101825. [CrossRef]
65. Hu, B.; Zhang, Z.; Liu, J.; Liu, Y.; Yin, J.; Lu, R.; Lin, X. A Comprehensive survey on smart contract construction and execution: Paradigms, tools, and systems. *Patterns* **2021**, *2*, 100179. [CrossRef] [PubMed]
66. Liu, Y.; He, J.; Li, X.; Chen, J.; Liu, X.; Peng, S.; Cao, H.; Wang, Y. An overview of blockchain smart contract execution mechanism. *J. Ind. Inf. Integr.* **2024**, *41*, 100674. [CrossRef]
67. Ethereum. Ethereum Virtual Machine (EVM). Available online: https://ethereum.org/developers/docs/evm/ (accessed on 10 August 2026).
68. Liu, D.; Zhang, J.; Wang, Y.; Shen, H.; Zhang, Z.; Ye, T. Blockchain Smart Contract Security: Threats and Mitigation Strategies in a Lifecycle Perspective. *ACM Comput. Surv.* **2026**, *58*, 104. [CrossRef]
69. Cruz, E.M.; Souza, Y.H.J.; Alcantara, G.S.A.; Peixoto, M.L.M. TRUST: A Lifecycle-oriented system architecture for governed evolution of smart contract applications. *Inf. Softw. Technol.* **2026**, *198*, 108210. [CrossRef]
70. Kurt, K.K.; Timurtaş, M.; Pınar, S.; Ozaydin, F.; Türkeli, S. Smart Contracts, Blockchain, and Health Policies: Past, Present, and Future. *Information* **2025**, *16*, 853. [CrossRef]
71. Kezadri Hamiaz, M.; Driss, M. Ethereum Smart Contracts Under Scrutiny: A Survey of Security Verification Tools, Techniques, and Challenges. *Computers* **2025**, *14*, 226. [CrossRef]
72. Rwegasira, D.S.; Namane, S.; Ben Dhaou, I. A Systematic Review of Blockchain and Multi-Agent System Integration for Secure and Efficient Microgrid Management. *Energies* **2026**, *19*, 1517. [CrossRef]
73. Nasrinasrabadi, M.; Hejazi, M.A.; Chaharmahali, E.; Hussein, M. A comprehensive review of blockchain integration in smart grid with a special focus on internet of things. *Energy Convers. Manag. X* **2025**, *27*, 101196. [CrossRef]
74. Mohanta, B.K.; Awad, A.I.; Elsaka, T.; Kheddar, H.; Baraka, E. Smart-contract-based blockchain-enabled decentralized scheme for improving smart-grid security. *Internet Things* **2025**, *34*, 101811. [CrossRef]
75. Kumar, V.; Yadav, P.; Rana, P.; Kaur, M.; Rawat, R.; Ali, R. AF-SGS: Blockchain-assisted secure authentication framework for smart grid systems. *Int. J. Inf. Technol.* **2026**. [CrossRef]

76. Che, Z.; Wang, Y.; Zhao, J.; Qiang, Y.; Ma, Y.; Liu, J. A Distributed Energy Trading Authentication Mechanism Based on a Consortium Blockchain. *Energies* **2019**, *12*, 2878. [CrossRef]
77. Ponnuru, R.B.; Kumar, S.A.P.; Azab, M.; Palaniswamy, B.; Alavalapati, G.R. Robust authentication and key agreement protocol for smart microgrid environment. *J. Inf. Secur. Appl.* **2025**, *94*, 104202. [CrossRef]
78. Namane, S.; Ben Dhaou, I. Blockchain-based access control model for smart grids using peak hour and privilege level attributes (BACS-HP). *J. Inf. Secur. Appl.* **2026**, *96*, 104261. [CrossRef]
79. Waheed, U.; Khan, S.A.; Masud, M.; Jamshed, H.; Jumani, T.A.; Malik, N.U.R. Blockchain-Based, Dynamic Attribute-Based Access Control for Smart Home Energy Systems. *Energies* **2025**, *18*, 1973. [CrossRef]
80. Yang, X.; Yao, K.; Li, S.; Du, X.; Wang, C. A smart grid data sharing scheme supporting policy update and traceability. *Sci. Rep.* **2025**, *15*, 26343. [CrossRef] [PubMed]
81. Akkaoui, R.; Palensky, P.; Epema, D.H.J.; Ştefanov, A. A Cyber Secure and Scalable Blockchain-Based Framework for Monitoring and Controlling Distributed Energy Resources. *IEEE Access* **2025**, *13*, 138460–138474. [CrossRef]
82. Subramaniam, R.; Sheela, A.J.; Alwabli, A. Enhanced cybersecurity and cyber-attack detection in smart DC micro grids using blockchain technology and SVM technique. *Ain Shams Eng. J.* **2025**, *16*, 103400. [CrossRef]
83. Amoani Lartey, O.; Kwao Dawson, J.; Opoku, R.; Oppong, S.; Twum, F. A proposed blockchain technology approach for securing IoT-enabled renewable and grid metering systems. *Int. J. Sustain. Energy* **2025**, *44*, 2597047. [CrossRef]
84. Aoufi, S.; Derhab, A.; Guerroumi, M.; Laoui, A.A.; Lazib, B. Two-tier reputation-based blockchain architecture against false data injection in smart AMI systems. *Comput. Electr. Eng.* **2025**, *124*, 110317. [CrossRef]
85. Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. *Energies* **2022**, *15*, 6799. [CrossRef]
86. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*, 5894. [CrossRef]
87. Paul, B.; Sarker, A.; Abhi, S.H.; Das, S.K.; Ali, M.F.; Islam, M.M.; Islam, M.R.; Moyeen, S.I.; Badal, M.F.R.; Ahamed, M.H.; et al. Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. *Heliyon* **2024**, *10*, e37980. [CrossRef] [PubMed]
88. Jørgensen, B.N.; Ma, Z.G. Cybersecurity and Resilience of Smart Grids: A Review of Threat Landscape, Incidents, and Emerging Solutions. *Appl. Sci.* **2026**, *16*, 981. [CrossRef]
89. Vigneshwaran, P.; Thuseethan, S.; Shanmugam, B.; Thennadil, S. Cyber attack detection in smart grids: A survey of methods, challenges and future directions. *Comput. Sci. Rev.* **2026**, *60*, 100915. [CrossRef]
90. Alrashdi, I.; Tanveer, M.; Aldossari, S.A.; Alshammeri, M.; Armghan, A. BSCP-SG: Blockchain-enabled secure communication protocols for IoT-driven smart grid systems. *Internet Things* **2025**, *32*, 101626. [CrossRef]
91. Mutlaq, K.A.-A.; Nyangaresi, V.O.; Omar, M.A.; Abduljabbar, Z.A.; Ma, J.; Al Sibahee, M.A.; Aldarwish, A.J.Y.; Ali, A.H. Blockchain assisted signature and certificate based protocol for efficient data protection and transaction management in smart grids. *PLoS ONE* **2025**, *20*, e0318182. [CrossRef] [PubMed]
92. Mohamed, M.V.O.; Abdelaziz, A.Y.; Abo-Elyousr, F.K. Blockchain-based approach for load frequency control of smart grids under denial-of-service attacks. *Comput. Electr. Eng.* **2024**, *116*, 109150. [CrossRef]
93. Bibi, H.; Abolhasan, M.; Lipman, J.; Abdollahi, M.; Ni, W. A comprehensive survey on privacy-preserving technologies for Smart Grids. *Comput. Electr. Eng.* **2025**, *124*, 110371. [CrossRef]
94. Zhou, Y.; Zhao, T.; Jing, Z.; Zhao, Q.; Zhu, Y. A blockchain-based privacy-preserving data aggregation scheme with robustness in smart grids. *J. Supercomput.* **2025**, *81*, 675. [CrossRef]
95. Tang, B.; Yao, S.; Su, L.; Xu, F. SGDID: A Privacy-Enhanced Supervised Distributed Identity Model for Smart Grid and Electric Vehicle Integration. *Symmetry* **2025**, *17*, 253. [CrossRef]
96. Fan, C.; Sohrabbeig, A.; Musilek, P. Zero-knowledge machine learning models for blockchain peer-to-peer energy trading. *Internet Things* **2025**, *32*, 101638. [CrossRef]
97. Sivakumar, E.; Ganesan, G.; Premkumar, R.; Rani, R.H.J.; Srinivasan, K. A systematic review on the current scenarios and future frontiers for securing smart grid systems. *Discov. Comput.* **2026**, *29*, 554. [CrossRef]
98. Andreoulaki, I.; Papapostolou, A.; Marinakis, V. Evaluating the Barriers to Blockchain Adoption in the Energy Sector: A Multicriteria Approach Using the Analytical Hierarchy Process for Group Decision Making. *Energies* **2024**, *17*, 1278. [CrossRef]
99. Wang, C.; Fan, Z.; Yan, A.; Zhang, G.; Lv, Y.; He, Y.; Su, H. Blockchain in the Energy Sector: Applications, Challenges, and Future Directions. *Energies* **2026**, *19*, 2283. [CrossRef]
100. Guo, Y.; Wan, Z.; Cheng, X. When blockchain meets smart grids: A comprehensive survey. *High-Confid. Comput.* **2022**, *2*, 100059. [CrossRef]
101. Zhao, W.; Qi, Q.; Zhou, J.; Luo, X. Blockchain-Based Applications for Smart Grids: An Umbrella Review. *Energies* **2023**, *16*, 6147. [CrossRef]

102. Roth, T.; Utz, M.; Baumgarte, F.; Rieger, A.; Sedlmeir, J.; Strüker, J. Electricity powered by blockchain: A review with a European perspective. *Appl. Energy* **2022**, *325*, 119799. [CrossRef]
103. 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]
104. Karumba, S.; Sethuvenkatraman, S.; Dedeoglu, V.; Jurdak, R.; Kanhere, S.S. Barriers to blockchain-based decentralised energy trading: A systematic review. *Int. J. Sustain. Energy* **2023**, *42*, 41–71. [CrossRef]
105. Feng, B.; Zhang, Y.; Zhang, C.; Zhang, B.; Liu, X.; Feng, S. Tamper-proof strategy of dynamic hash chain for smart grid cloud storage based on reinforcement learning key update mechanism. *Discov. Comput.* **2025**, *28*, 285. [CrossRef]
106. Abrar, I.; Nautiyal, A.; Ghosh, S.; Sheikh, J.A.; Abrar, I. Blockchain-driven decentralization of energy sector: A path towards resilience, efficiency, and equity. *Sustain. Energy Technol. Assess.* **2026**, *86*, 104874. [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.