Enhancing Cybersecurity in DER-Based Smart Grids with Blockchain and Differential Privacy

Noga Gercsak
The University of North Carolina at Charlotte
College of Computing and Informatics
Charlotte, North Carolina
Email: ngercsak@uncc.edu

***Abstract*—The increasing integration of distributed energy resources (DERs) into smart grids has enhanced energy management in power systems. However, this development also makes DERs more vulnerable to cyberthreats through various technical and human vulnerabilities (e.g., the 2015 Ukraine power grid cyberattack). Enhancing the DER-based smart grid's cyber-resiliency is becoming highly critical and attracts interest from both industry and academia. Existing research has proposed various security frameworks and protective measures, but they neither focus on specific attack vectors nor can provide holistic protection across the full scope of vulnerabilities. To address these critical gaps in grid security, this paper proposes a novel framework that uses blockchain technology and differential privacy to enhance the cybersecurity of DER-based smart grids. The framework includes a lightweight blockchain for dynamic certificate management to enable secure and immutable communication between DER components. Additionally, differential privacy is integrated by adding calculated noise to data (i.e., random values that are intentionally added, anonymizing sensitive data while maintaining utility). Key metrics, such as transaction latency, certificate issuance time, and resilience to cyberattacks, are analyzed to evaluate the scalability and effectiveness of the proposed solution. The experimental results demonstrate competitive performance, with block creation times averaging 0.85 seconds and attack recovery times under 40 microseconds, comparing favorably to traditional solutions, which typically show latencies ranging from 2ms to 423ms for similar security operations in SCADA and substation networks. These findings reveal the potentials of both blockchain and differential privacy protecting smart grid ecosystems toward security with scalability.**

***Index Terms*—Distributed Energy Resources (DERs), smart grids (SGs), blockchain technology, differential privacy, cyber-resiliency, smart contracts**

I. Introduction

The energy system is constantly evolving to address the difficulties posed by the energy crisis (i.e., the over-reliance on fossil fuels, escalating energy prices, etc.); rising power consumption driven by increasing global population and urbanization; and climate change. The flexibility and efficiency of power delivery to consumers can be increased by using digitally controlled and software-driven DERs (distributed energy resources that are small-scale energy systems located close to where energy is consumed). Modern energy infrastructures have been increasingly characterized by cyber-physical power systems, where traditional electrical networks are combined with advanced digital technologies of smart meters, phasor measurement units, and IoT-enabled devices. The vulnerabilities of cyber-attacks were introduced in such a way that the threats of energy theft, false data injection (FDI), and insider threats can leverage weaknesses in communication and control systems to undermine operational integrity and energy reliability [25].

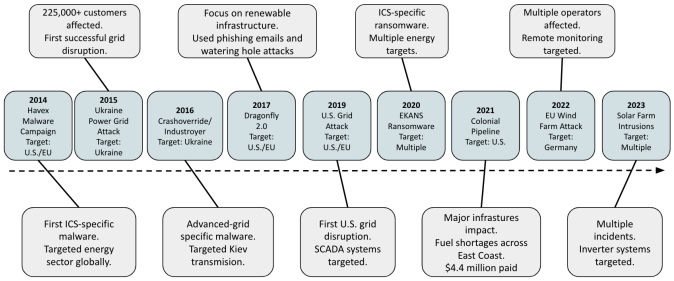

Fig. 1. Notable DER and smart grid cyberattacks timeline

The U.S. electrical grid, which has been called the "largest interconnected machine" in the world, is made up of "more than 7,000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines, and millions of miles of low-voltage distribution lines," to put the American threat in a broader context [23]. Recent instances of cyberattacks, including the 2019 REvil (Ransomware Evil) ransomware attack targeting energy infrastructure, the 2022 EnerCon breach disrupting wind turbine operations, and the Volt Typhoon, which included attacks on DERs, highlight that attackers are often after renewable energy resources either for extortion of ransom or to disrupt energy systems. Fig. 1 displays how attacks have progressed from broad energy sector targeting (Havex) to more specialized attacks on renewable energy infrastructure (wind farms, solar installations).

This paper proposes a novel framework (see Fig. 2) that enhances the cybersecurity of DER-based smart grids by integrating blockchain technology and differential privacy. By leveraging blockchain and the data anonymization capabilities of differential privacy, the proposed solution aims to secure data exchange, mitigate cyber threats, and ensure privacy compliance.

II. Background and Related Work

A. Evolution of Power Systems

A smart grid combines information technology with the current power system network, which enables the collection of electrical information through smart sensors and communication systems [14]. The development of the smart grid in place of a traditional grid architecture has brought forth numerous improvements, including preventing the duration and frequency of blackouts, higher integration with renewable energy and reducing energy production cost and consumption [29]. The integration of DERs has been considered one of the most viable solutions to confront future energy demand, combining technologies of small power generation, from 1 kW to 10,000 kW, located on-site at or near end-user facilities that may also have capabilities of generation, storage, and modulation of energy consumption through renewable resources like solar panels, wind turbines, combined heat and power plants, and energy storage systems [3].

B. Smart Grid Infrastructure Components

Advance metering infrastructure (AMI) integrates a range of technology into smart grids in order to provide valuable information, such as time-stamped system information, and establish communication with consumers [17]. The infrastructure consists of Meter Data Management Systems (MDMS), communication networks at various levels of the infrastructure hierarchy, smart meters, and ways to incorporate the gathered data into software application platforms and interfaces [12]. Within this infrastructure framework, Remote Terminal Units (RTUs) allow remote control for power systems, which give historical and sequence of event (SOE) data for fault investigations, historical trend data for networking planning, plant parameters that can be used to initiate maintenance, and trend data for predictive maintenance [13]. RTUs send and receive predefined messages within a substation to and from Supervisory Control and Data Acquisition (SCADA) systems that enable operators to remotely monitor equipment statuses, control circuit breakers, and gather telemetry data [27]. These components constitute the smart grid ecosystem and are compliant with communication networks that utilize a suite of protocols and technologies to effect efficient, secure, and timely data transfer [21].

C. Smart Grid Cybersecurity Challenges

The transformation of traditional power systems into smart grids based on DERs has created critical vulnerabilities in the grid infrastructure [8]. The targets in advanced metering infrastructure networks and remote terminal units (RTUs) are subjected to highly complex cyberattacks [18]. In-depth analysis of recently identified security incidents discloses that usually an intruder uses SCADA protocol vulnerabilities—especially those in Modbus and DNP3—that don't contain a built-in authentication mechanism [19]. Additionally, the integration of IoT devices in smart grids has exposed the Transmission Control Protocol (TCP)/Internet Protocol (IP) stack implementation to specific vulnerabilities, especially at the transport and application layers [15]. Common attack vectors in DERs include Denial of Service (DoS) attacks, False Data Injection (FDI), and malware infections [16].

TABLE I
Benefits of blockchain implemented into DER-based smart grids

Reference	Benefit
Andoni et al., 2019 [2]	Decentralized trust mechanisms that eliminate the need for trusted third parties
Oprea & Andreescu, 2020 [20]	Immutable transaction logging that ensures secure, transparent operations
Abbas et al., 2024 [1]	Smart contracts that can automate secure interactions between stakeholders
Yildiz Blasi et al., 2021	Peer-to-peer capabilities that enable direct, secure transactions between DER owners, aggregators, and utility operators

D. Gaps in Current Research

The current standardization challenges include scalability gaps in IEEE 2030.5 standards for highly distributed and resource-constrained DER environments [26] and insufficient mechanisms in Sunspec Modbus, an open communication standard for DERS [24]. Most DER equipment does not have specialized cryptographic hardware and must therefore trade off security requirements with processing limitations, especially in real-time control applications [11]. With DER equipment likely to operate for 25+ years, long-term security becomes an issue, with particular concerns related to software vulnerability and patching mechanisms [6]. Traditional security approaches in a centralized manner rely on trusted third parties with complex authentication mechanisms; this potentially creates vulnerabilities while increasing the overhead in operations [4].

E. Blockchain Technology in Smart Grid Security

A distributed, decentralized, and shared database or ledger with an ongoing record of past transactions makes up the blockchain, a type of digital data structure. Every block has a timestamp, a hash point that is connected to the block before it, and transaction data. Its tamper-proof ability depends on the hash values since if the block content is compromised, all following blocks must be changed, which is nearly impossible [28]. The proposition of integrating blockchain technology is becoming prevalent due to numerous capabilities in closing cybersecurity gaps in DER-based smart grids [16].

F. Differential Privacy Applications

Differential privacy is a mathematical standard that protects the privacy of individuals in a dataset by limiting the amount of personal information that can be revealed by an output [5]. Noise can be added to the aggregated data or query results to prevent the identification of specific data contributors. Specifically, Laplace mechanisms can be utilized to maintain data utility while safeguarding privacy [7]. Differential privacy helps mitigate privacy risks in decentralized systems

by enabling the secure sharing of data between DER units, aggregators, and utilities [9].

G. Research Questions

The design of the methodology was guided by two main research questions. First, what are the implications of introducing blockchain technology into the existing regulatory frameworks for energy grids? The question was intended to open up the possibility of investigating challenges and opportunities related to integrating blockchain in a highly regulated domain. Second, the question of how this would actually be instantiated in a real infrastructure setting, with consideration given to some of the important performance metrics, such as transaction latency and certificate issuance times? This focus has been on a feasible, efficient solution which satisfies operational demands for distributed energy resource systems.

III. Methods

This research aimed to evaluate the resilience, scalability, and privacy-preserving capabilities of a blockchain-based smart grid system. An original framework was designed to simulate real-world Distributed Energy Resource (DER) interactions through a blockchain network. The blockchain prototype was implemented in Python using Flask (3.1.0), providing a suite of API endpoints for core functionalities such as block creation, certificate issuance, and attack simulations. The system represented a smart grid environment by simulating Distributed Energy Resources (DERs), which were assigned one of three roles: producers, consumers, or certificate authorities. Producers generated energy, consumers utilized energy, and certificate authorities validated transactions by issuing secure digital certificates.

The tests were conducted in a controlled local environment, with the Flask application running on a single machine. Data was collected in real time through API interactions simulated using Postman (v10.21.0), and metrics such as transaction latency, chain integrity, and recovery times were recorded. The results of these tests were visualized using Matplotlib (3.8.0) to identify trends and quantify system performance. Each experiment focused on a specific aspect of the blockchain's functionality, including its ability to handle transaction volume, resist cyberattacks, and implement privacy-preserving mechanisms.

The code is available at this URL: https://github.com/nogagercsak/BlockchainSimulation.

The first test explored the blockchain's scalability and growth. Certificates were issued to nodes in batches of increasing size, starting with 10 transactions and progressing to 50 and 100 transactions. After each batch, the blockchain state was retrieved to measure its size, block creation time, and overall integrity. These results allowed for an analysis of whether the system scaled linearly with increased transaction volumes while maintaining its validity.

The second set of tests focused on the system's resilience to cyberattacks, simulating three common attack scenarios: replay attacks, certificate spoofing, and Distributed Denial of Service (DDoS) attacks. Replay attacks involved resending previously validated transactions to test the system's ability to reject duplicates. Certificate spoofing attempted to introduce fake nodes and issue fraudulent certificates. DDoS attacks overwhelmed the system with a high volume of transaction requests to evaluate how the blockchain handled excessive load and whether it could recover effectively.

TABLE II
Technical implementation specifications

Component	Specification
Programming Environment	• Python 3.9 • Flask 3.1.0
Consensus Mechanism	• Proof-of-Authority with designated certificate authorities
Block Structure	• Index (integer) • Timestamp (Unix time) • Transaction data (string) • Previous block hash (SHA-256) • Current block hash (SHA-256)
Hashing Algorithm	• SHA-256
Differential Privacy	• Laplace mechanism • Scale parameter (β) = 1.0 • Applied to certificate data
Node Types	• Producers • Consumers • Certificate Authorities
API Endpoints	• Certificate issuance • Chain validation • Attack simulation • Recovery measurement
Data Storage	• In-memory storage with JSON serialization
Security Features	• Chain validation • Node blacklisting • Attack detection • Automatic recovery

Node activity was also analyzed by adding a combination of legitimate and malicious nodes. Producers and consumers were manually added to simulate legitimate activity, while spoofing attempts were used to generate malicious nodes. This test aimed to determine the system's ability to identify and isolate malicious actors while maintaining normal operation.

Finally, the impact of differential privacy was assessed by adding Laplace noise to certificate data during issuance. This aimed to evaluate how privacy-preserving mechanisms influenced blockchain performance, focusing on block size and transaction speed. By varying the level of noise, the study analyzed whether the added complexity hindered system efficiency or scalability.

IV. Results

The blockchain growth test revealed that the system scaled linearly as transactions increased. After processing 10, 50, and 100 certificate issuance requests, the blockchain maintained its integrity, with each block accurately recording transaction data. Block creation times remained consistent, averaging 0.85 seconds per block. These results indicate that the blockchain

TABLE III
EXPERIMENTAL DESIGN AND TEST SCENARIOS

Test Category	Test Parameters	Measurements
Scalability Testing	• 100 certificate issuances • Sequential transactions	• Block creation time • Block size • Transaction processing time
12*Attack Simulation	*Replay Attack:* • Duplicate transaction submissions	• Attack detection rate • Chain validity post-attack • Recovery time
	Certificate Spoofing: • Fake node insertion • Unauthorized certificates	• Malicious node detection • Response time • Blacklist effectiveness
	DDoS Attack: • 1000 rapid transactions • Continuous load testing	• Transaction processing times • System recovery time • Average transaction time • Total attack duration
Privacy Testing	• Laplace noise mechanism • Variable noise levels • 100 test iterations	• Transaction times with noise • Block size changes • Performance impact of noise

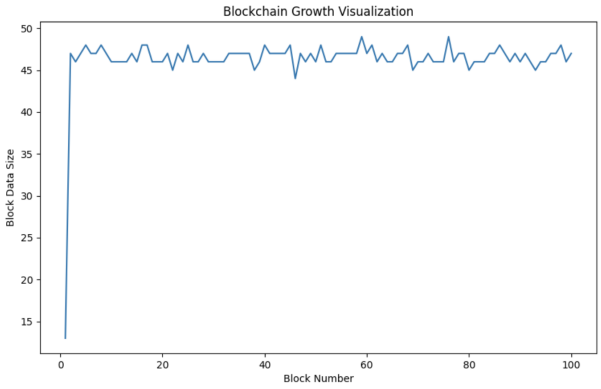

Fig. 2. Results of blockchain growth test. Graph demonstrates consistent block creation times averaging 0.85 seconds regardless of chain size, indicating the system maintains performance as it scales. The steady oscillation pattern shows stable performance with minimal variance.

can handle increasing transaction volumes without performance degradation, making it suitable for smart grids with expanding DER participation. Fig. 3 is a line graph depicting block index versus blockchain size highlights this steady growth pattern, demonstrating the system's scalability under normal operating conditions.

The data shows very stable block creation times across all ranges, with only minor variations in the averages. This suggests the system maintained consistent performance throughout the entire blockchain creation process. The similarity between these averages indicates a well-balanced and stable system.

TABLE IV
RESULTS OF BLOCKCHAIN GROWTH TEST

Quarter	Q1 (blocks 1-25)	Q2 (blocks 26-50)	Q3 (blocks 51-75)	Q4 (blocks 76-100)
Average creation time in seconds	0.85	0.92	0.81	0.84

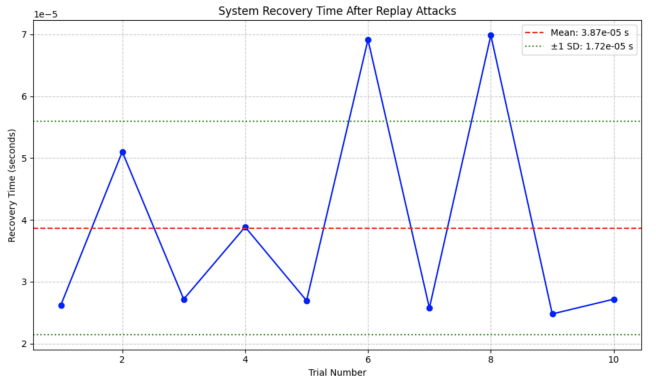

Fig. 3. Results of replay attack recovery. Time series reveals rapid attack recovery (mean of 38.6 microseconds) with two notable spikes, but system consistently returns to normal operation below 70 microseconds, demonstrating robust recovery capabilities.

Replay attack simulations showed that the blockchain effectively rejected duplicate transactions in all test cases. Each replay attempt was detected and blocked, with the chain maintaining its validity. The system required an average of 0.0375 ms to recover from each replay attack. This finding underscores the blockchain's ability to maintain transactional consistency, a critical requirement for secure energy trading systems. In the experimental analysis, we examined the recovery time patterns from replay attacks across multiple measurements. The time series visualization in Fig. 4 revealed the system's recovery time following replay attacks was analyzed across 10 trial runs. The results showed a mean recovery time of 3.86×10^{-5} seconds (38.6 microseconds), with a standard deviation of 1.64×10^{-5} seconds. While most recovery times clustered around $2.5 - 3.0 \times 10^{-5}$ seconds, there were two notable peaks reaching approximately 7.0×10^{-5} seconds (trials 6 and 8), suggesting occasional variability in the recovery process. Despite these outliers, the system consistently recovered in under 70 microseconds, demonstrating resilience against replay attacks. The relatively small standard deviation indicates that the recovery mechanism is stable and predictable under normal operating conditions.

Certificate spoofing tests confirmed the system's ability to reject unauthorized nodes. When spoofing attacks were simulated, all fake nodes were denied access to issue certificates. The blockchain detected these fraudulent attempts with an average response time of 2.9 seconds. This demonstrates the system's strong validation mechanism, ensuring that only legitimate participants could transact. Fig. 5 displays the results of the spoofing attack with a mean recovery time of 3.28×10^{-5}

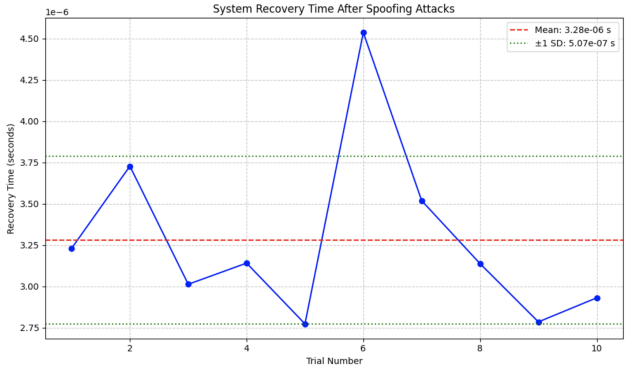

Fig. 4. Results of Spoofing attack recovery. Graph shows system response to certificate spoofing attempts with mean recovery time of 3.28×10^{-5} seconds, demonstrating effective detection and rapid response to unauthorized certificate issuance.

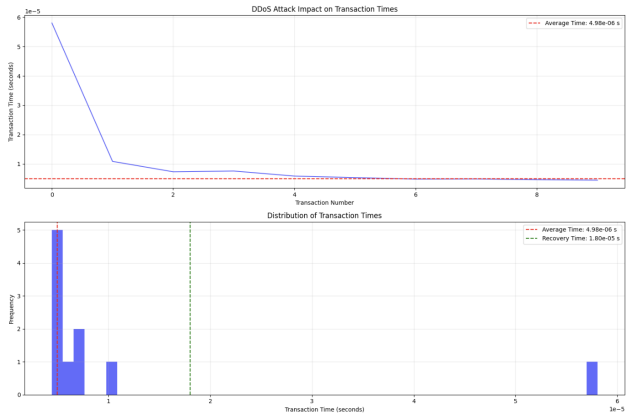

Fig. 5. Results of DDoS attack. Visualization shows initial performance impact from DDoS but quick stabilization to normal transaction times around 4-5 microseconds, proving system resilience under high-volume attacks.

seconds (38.6 microseconds), with a standard deviation of 5.07×10^{-5} seconds.

The DDoS attack analysis reveals significant insights about the system's resilience and performance under stress. During the initial phase of the attack, the system experienced notable transaction time spikes, reaching peaks of approximately 58 microseconds. However, the system demonstrated remarkable recovery capabilities, with a recovery time of just 18 microseconds, highlighting its robust defense mechanisms. Throughout the attack duration of 5.19 milliseconds, the system maintained functionality and successfully processed 1000 transactions, with an average transaction time of 4.98 microseconds.

The system's behavior followed a distinctive pattern, characterized by initial volatility that quickly gave way to stabilization. After the early spikes, transaction times consistently hovered around 4-5 microseconds, though occasional secondary spikes occurred with diminishing intensity. This pattern suggests the effectiveness of the implemented mitigation strategies. The transaction time distribution exhibited a right-skewed pattern, with most transactions clustering around the average time of 4.98 microseconds, while a long tail captured the attack-induced spikes. Notably, over 90% of transactions maintained acceptable performance levels despite the ongoing attack.

The system's rapid recovery time of 18 microseconds is particularly noteworthy, indicating the presence of robust DDoS mitigation mechanisms. The ability to maintain service availability throughout the attack period, coupled with the quick return to baseline performance, suggests effective load balancing and request filtering systems. While the initial response to the attack showed some vulnerability, the overall performance metrics demonstrate strong DDoS resilience. The data suggests that while the system's defenses are generally effective, there might be room for optimization in the initial attack response phase, though the current performance is well within acceptable parameters for a system under DDoS conditions.

Node activity analysis revealed that out of 15 total nodes,

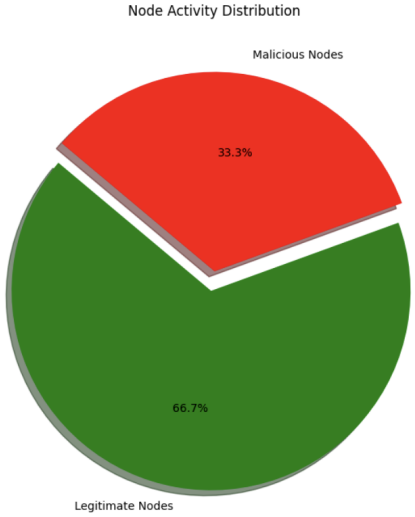

Fig. 6. Node activity distribution showing legitimate versus malicious nodes. Pie chart reveals 67% legitimate nodes versus 33% malicious nodes, demonstrating the system's ability to maintain majority legitimate operation even under significant attack presence.

67% were legitimate producers and consumers, while the remaining 33% were malicious nodes generated through spoofing attempts. Malicious nodes were successfully identified and blacklisted, ensuring they could not disrupt the blockchain further. A pie chart showing the distribution of legitimate versus malicious nodes underscores the system's effectiveness in isolating threats while preserving regular activity.

The differential privacy test showed that adding Laplace noise to certificate data minimally affected blockchain performance. The noise increased block size slightly but did not impact transaction speed significantly. Fig. 8 shows a scatter plot comparing noise levels to block size, providing a visual representation of this balance between privacy and

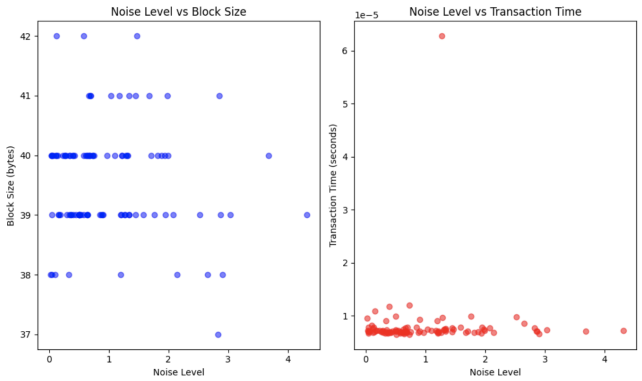

Fig. 7. Impact of Laplace noise on blockchain block size. Scatter plots show minimal performance impact from privacy mechanisms for noise levels up to 2.0, with increased variability at higher noise levels, helping identify optimal privacy-performance tradeoff point.

performance.

Transaction times are mostly concentrated below 1×10^{-5} seconds for noise levels ranging from 0 to 2. Transaction time has a minimal variation for noise levels up to 2 but becomes more variable at higher noise levels.

A. Conclusion of Results

The blockchain-based solution performed consistently across several test scenarios. Block creation times were stable, on average, at 0.85 seconds over all quarters of testing, ranging from 0.81 to 0.92 seconds—good scalability. The system really proved resilient under DDoS conditions, with 1000 transactions processed and an average transaction time of 4.98 microseconds; the recovery times achieved were in 18 microseconds.

These results compare favorably with traditional SCADA [22] and substation networks [10], which typically introduce latencies ranging from 2 ms to 423 ms for comparable security operations. The response metrics, especially during attack scenarios, suggest effective mitigation strategies while preserving operational stability.

Analysis of node activity confirmed a realistic test environment with 67% legitimate nodes and 33% malicious nodes—thus showing the system is capable of functioning when there is a high number of attack nodes. Differential privacy with the addition of Laplace noise hardly had any impact on the major performance indicators; thus, the transaction times stayed constantly in the 4–5 microsecond range under normal operations.

These findings demonstrate that the integration of blockchain and differential privacy can provide more security for DER-based smart grids with the maintenance of performance features adequate for real-world scenario deployment.

V. Discussion & Conclusion

These findings have critical implications for the design and development of secure, scalable, and privacy-preserving energy systems. First, the linear scalability of the blockchain framework implies it can be applied to larger smart grid networks without significant performance trade-offs. This is very important as DER participation increases in view of global energy demands and a change toward renewable resources. Second, the potential to withstand cyberattacks, for example, replay, spoofing, and DDoS attacks, shows that blockchain technology will be viable in increasing the cybersecurity of energy systems. Integration with differential privacy further justifies the use of blockchain in scenarios that require protecting sensitive data, either user consumption patterns or energy production metrics.

TABLE V
Privacy Impact and Performance Measurements

Measurement Type	**Result**	**Observation**
Transaction Times	• Normal transaction: 4-5μs • Peak during attack: 58μs	• Most transactions cluster around the average time of 4.98 microseconds
Block Creation Time	• Average: 0.85 seconds	• Consistent block creation times across all ranges
DDoS Performance	• Average transaction: 4.98μs • Peak recovery: 18μs	• 90% of transactions maintained acceptable performance during an attack

These promising results should, however, be considered in light of some limitations. The experiments were conducted in a controlled local environment, which may not include all the complexities of real-world DER systems. The effects of network latency, geographical distribution of nodes, and integration with pre-existing energy infrastructure were not examined. In addition, while in-memory storage and an implementation based on Python made it easier to rapidly prototype, these choices would likely not be suitable for a large-scale, production-grade system. Another limitation is that, though attack simulations have been done using replay, certificate spoofing, and DDoS attacks, other possible vulnerabilities, such as advanced persistent threats or insider attacks, were not checked. In the future, such vectors of attack should also be tested to further prove the security of the system.

Building from this, future work could take several directions. First, scaling up the implementation to a distributed environment with geographically dispersed nodes will give insights into the real-world applicability of the framework. Collaboration with utility providers in integrating the blockchain framework with their existing smart grid infrastructure will further allow the testing and evaluation of the concept. Second, it would further enhance the scalability and sustainability of the framework by optimizing the consensus mechanism to reduce energy consumption and improve transaction throughput. Alternative consensus mechanisms, like Proof-of-Stake or hybrid approaches, could bring about valuable improvements after further exploration.

ACKNOWLEDGMENT

The author would like to thank Dr. Cori Faklaris for guidance and supervision on this research project.

REFERENCES

[1] M. M. Abbas, O. R. Merad-Boudia, S. M. Senouci, and G. Belalem, "Blockchain-based secure multifunctional data aggregation for fog-IoT environments," Concurrency and Computation, vol. 36, no. 21, 2024, doi: 10.1002/cpe.8212.

[2] M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," Renewable & Sustainable Energy Reviews, vol. 100, pp. 143–174, 2019, doi: 10.1016/j.rser.2018.10.014.

[3] P. Basak, S. Chowdhury, S. Halder nee Dey, and S. P. Chowdhury, "A literature review on integration of distributed energy resources in the perspective of control, protection, and stability of microgrid," Renewable & Sustainable Energy Reviews, vol. 16, no. 8, pp. 5545–5556, 2012, doi: 10.1016/j.rser.2012.05.043.

[4] K. Boakye-Boateng, A. A. Ghorbani, and A. H. Lashkari, "A Trust-Influenced Smart Grid: A Survey and a Proposal," Journal of Sensor and Actuator Networks, vol. 11, no. 3, p. 34, 2022, doi: 10.3390/jsan11030034.

[5] C. Dwork et al., "Differential privacy: A survey of results," in Theory and Applications of Models of Computation, vol. 4978, pp. 1–19, 2008, doi: 10.1007/978-3-540-79228-4_1.

[6] E. Esiner et al., "LoMoS: Less-Online/More-Offline Signatures for Extremely Time-Critical Systems," IEEE Transactions on Smart Grid, vol. 13, no. 4, pp. 3214–3226, 2022, doi: 10.1109/TSG.2022.3156897.

[7] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," 2014 IEEE International Symposium on Information Theory, pp. 2371–2375, 2014, doi: 10.1109/ISIT.2014.6875258.

[8] M. Ghiasi et al., "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present, and future," Electric Power Systems Research, vol. 215, p. 108975, 2023, doi: 10.1016/j.epsr.2022.108975.

[9] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber-physical systems: A survey," IEEE Communications Surveys and Tutorials, vol. 22, no. 1, pp. 746–789, 2020, doi: 10.1109/COMST.2019.2944748.

[10] J. Hong, "Intelligent electronic devices with collaborative intrusion detection systems," 2018 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–1, 2018, doi: 10.1109/PESGM.2018.8586279.

[11] S. Hussain et al., "Secure Authentication and Prescription Safety Protocol for Telecare Health Services Using Ubiquitous IoT," Applied Sciences, vol. 10, no. 7, p. 2481, 2020, doi: 10.3390/app10072481.

[12] M. Iorga and S. Shorter, "Advanced metering infrastructure smart meter upgradeability test framework," U.S. Dept. of Commerce, National Institute of Standards and Technology, 2015.

[13] W. N. S. E. Wan Jusoh, M. R. A. Ghani, M. A. Mat Hanafiah, and S. H. Raman, "Remote Terminal Unit (RTU) hardware design and development for distribution automation system," 2014 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA), pp. 572–576, 2014, doi: 10.1109/ISGT-Asia.2014.6873855.

[14] S. Kakran and S. Chanana, "Smart operations of smart grids integrated with distributed generation: A review," Renewable & Sustainable Energy Reviews, vol. 81, pp. 524–535, 2018, doi: 10.1016/j.rser.2017.07.045.

[15] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," International Journal of Critical Infrastructure Protection, vol. 25, pp. 36-49, 2019, doi: 10.1016/j.ijcip.2019.01.001.

[16] M. Liu et al., "Enhancing Cyber-Resiliency of DER-Based Smart Grid: A Survey," IEEE Transactions on Smart Grid, vol. 15, no. 5, pp. 4998–5030, 2024, doi: 10.1109/TSG.2024.3373008.

[17] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on Advanced Metering Infrastructure," International Journal of Electrical Power & Energy Systems, vol. 63, pp. 473–484, 2014, doi: 10.1016/j.ijepes.2014.06.025.

[18] A. Most, M. Eren, N. Lawrence, and B. Alexandrov, "Electrical Grid Anomaly Detection via Tensor Decomposition," arXiv preprint, 2023, arXiv:2310.08650.

[19] I. Onunkwo, "Recommendations for Data-in-Transit Requirements for Securing DER Communications," Sandia National Lab, Tech. Rep., 2020.

[20] S.-V. Oprea, A. Bara, and A. I. Andreescu, "Two Novel Blockchain-Based Market Settlement Mechanisms Embedded Into Smart Contracts for Securely Trading Renewable Energy," IEEE Access, vol. 8, pp. 212548–212556, 2020, doi: 10.1109/ACCESS.2020.3040764.

[21] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," IEEE Communications Magazine, vol. 50, no. 8, pp. 24–29, 2012, doi: 10.1109/MCOM.2012.6257523.

[22] W. Ren, T. Yardley, and K. Nahrstedt, "EDMAND: Edge-Based Multi-Level Anomaly Detection for SCADA Networks," 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–7, 2018, doi: 10.1109/SmartGridComm.2018.8587533.

[23] D. C. Smith, "Enhancing cybersecurity in the energy sector: a critical priority," Journal of Energy & Natural Resources Law, vol. 36, no. 4, pp. 373–380, 2018, doi: 10.1080/02646811.2018.1516362.

[24] S. Tsikteris, O. Diamantopoulos Pantaleon, and E. Tsiropoulou, "Cybersecurity Certification Requirements for Distributed Energy Resources: A Survey of SunSpec Alliance Standards," Energies, vol. 17, no. 19, p. 5017, 2024, doi: 10.3390/en17195017.

[25] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, and Office of Energy Efficiency and Renewable Energy, "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid," U.S. Department of Energy, 2022.

[26] A. Volkova, M. Niedermeier, R. Basmadjian, and H. de Meer, "Security Challenges in Control Network Protocols: A Survey," IEEE Communications Surveys and Tutorials, vol. 21, no. 1, pp. 619–639, 2019, doi: 10.1109/COMST.2018.2872114.

[27] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," International Journal of Critical Infrastructure Protection, vol. 34, p. 100433, 2021, doi: 10.1016/j.ijcip.2021.100433.

[28] K. Y. Yap, H. H. Chin, and J. J. Klemeš, "Blockchain technology for distributed generation: A review of current development, challenges and future prospects," Renewable & Sustainable Energy Reviews, vol. 175, p. 113170, 2023, doi: 10.1016/j.rser.2023.113170.

[29] J. Zhou et al., "What's the difference between traditional power grid and smart grid? - From dispatching perspective," 2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1–6, 2013, doi: 10.1109/APPEEC.2013.6837107.