Improved Resilience of Local Energy Markets using Blockchain Technology and Self-Sovereign Identity

Umit Cali [1], Marthe Dynge [2], Md Sadek Ferdous [1], and Ugur Halden [1]

[1]Affiliation not available
[2]Norwegian University of Science and Technology

October 30, 2023

Abstract

The Digital Green Transition of the energy industry is accelerating as decarbonization and digitalization of the power market and system are gaining momentum. Unlocking the full and real potential of local energy markets is among the opportunities to be demystified in the coming years, with blockchain technology being a prominent enabler. Important subcomponents such as functional and fair local energy pricing mechanisms and management algorithms will be required for next-generation digital local energy trading and management platforms. Even though rapid digitalization of the energy sector offers considerable advantages, it also increases the cyber-physical risk levels of energy systems in general. The proposed framework of this paper accommodates considerable undiscovered aspects of democratization of the energy systems and future digital shared economy conventions. Nevertheless, privacy concerns must be addressed in tandem with the cyber-physical security of local energy markets and their ecosystem. This work proposes a joint privacy and cyber-physical security framework designed for local energy markets to improve cyber-physical resilience. All related parts, such as blockchain technology and self-sovereign identity, are used in an organized way to create a possible solution.

Improved Resilience of Local Energy Markets using Blockchain Technology and Self-Sovereign Identity

1[st] Umit Cali
Department of Electric Power Engineering
Norwegian University of Science and Technology
Trondheim, Norway
umit.cali@ntnu.no

2[nd] Marthe Fogstad Dynge
Department of Electric Power Engineering
Norwegian University of Science and Technology
Trondheim, Norway
marthe.f.dynge@ntnu.no

3[rd] Md Sadek Ferdous
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
sadek.ferdous@bracu.ac.bd

4[th] Ugur Halden
Department of Electric Power Engineering
Norwegian University of Science and Technology
Trondheim, Norway
ugur.halden@ntnu.no

***Abstract*—The Digital Green Transition of the energy industry is accelerating as decarbonization and digitalization of the power market and system are gaining momentum. Unlocking the full and real potential of local energy markets is among the opportunities to be demystified in the coming years, with blockchain technology being a prominent enabler. Important subcomponents such as functional and fair local energy pricing mechanisms and management algorithms will be required for next-generation digital local energy trading and management platforms. Even though rapid digitalization of the energy sector offers considerable advantages, it also increases the cyber-physical risk levels of energy systems in general. The proposed framework of this paper accommodates considerable undiscovered aspects of democratization of the energy systems and future digital shared economy conventions. Nevertheless, privacy concerns must be addressed in tandem with the cyber-physical security of local energy markets and their ecosystem. This work proposes a joint privacy and cyber-physical security framework designed for local energy markets to improve cyber-physical resilience. All related parts, such as blockchain technology and self-sovereign identity, are used in an organized way to create a possible solution.**

***Index Terms*—Local energy markets, Blockchain Technology, Privacy, Cybersecurity, Resilience, Self-sovereign identity**

I. Introduction

Over the past decades, the global energy system has undergone a vast transition, due to both technological and political influences. These can generally be described through the "5 D's" [1], starting with the *deregulation* occurring at the end of the last century when electricity markets were introduced. New entities were allowed into the liberalized system, and the following economical and technological development of Decentralized Energy Resources (DERs) have led the traditionally centralized power system towards a more *decentralized* structure. Simultaneously, the global commitment to mitigate climate change *decarbonization* of the energy sector has been a broad political target. In recent years, new opportunities have arisen with the maturity of *digitalization* tools, such as Information and Communication Technologies (ICT) and Internet-of-Things (IoT) devices and Distributed Ledger Technology (DLT), including blockchain. As a result of all these structural changes, a new transition is emerging; *democratization*. As formerly passive consumers transition to prosumerism, by producing their own energy and actively controlling their energy behavior, the possibility of implementing new, prosumer-centric energy management strategies emerges. With the challenges emerging in managing increasingly decentralized and variable energy production, local energy communities have been emphasized as a promising solution. In addition, transactive energy platforms can be established within or between these communities, thus forming local energy markets, where prosumers and consumers can trade locally generated energy among each other. As production is moved closer to consumption, the energy effectiveness is increased along with a decreased carbon footprint, thus being advantageous both in economical and environmental aspects [2]. Furthermore, such a structured organization of distributed flexibility assets opens up new opportunities for grid operators in terms of grid planning and operation [3].

A critical aspect of the implementation of local energy markets is how the identities of different entities are managed. Traditionally, Identity Management Systems (IMS) are used to manage identities. Unfortunately, traditional IMS are mostly provider-centric with users having limited control over their identity data. This has serious privacy implications [4]. To limit these privacy issues, the notion of Self-Sovereign Identity (SSI) has been introduced [5] and has attracted significant attention in the industry and academia.

With the digitalization of the energy domain, the cyber-physical security of energy systems has become a major concern. In fact, this domain is experiencing a growing number of cyber attacks and cyber terrorism [6] with severe economic consequences [7]. Local energy markets, the focus of this research paper, will undoubtedly face similar or novel cyber-physical attacks involving confidentiality, integrity, and resilience. Therefore, it is important to consider different cyber-physical security aspects while designing a local energy market.

In this research paper, we propose a novel SSI and DLT-based framework for a local energy market that aims to address different cyber-physical security and privacy issues. The main contributions of this work are:

- Proposition of a joint framework using DLT and SSI for local energy market practices.
- Developing a focus on the privacy and cyber-physical security aspects of local energy markets using the features provided by SSI.
- Investigating the potential impact of the proposed framework in terms of cyber-physical resilience of local energy markets.

Structure. In Section II we provide a brief overview of local energy markets and their pricing mechanisms. The concept of SSI is presented in Section III. Section IV discusses the proposed architecture and its different aspects while Section V analyzes different cyber-physical security issues and the legislative and privacy aspects with respect to the proposed framework. Finally, we conclude in Section VI.

II. Local Energy Markets

To properly manage the unpredictable nature of DERs and end-user energy behavior, while also ensuring the privacy of market participants, sophisticated management algorithms must be deployed upon the establishment of local energy markets. In recent years, many methodologies have been presented in the literature, generally assuming either a centralized or decentralized approach [2]. The advantages of using a centralized approach are enhanced cooperation between the market participants, and thus a higher possibility of coordinating support of grid operation and community resilience [8]. However, a decentralized approach often provides a higher degree of scalability and transparency, as well as a lower requirement of communicated information [9]. Thus, a higher level of privacy preservation may also be easier to achieve.

A. Pricing Mechanisms

A key aspect for local markets to be commonly accepted is the development of a pricing mechanism for locally traded commodities that is perceived as fair by all participants. For stable market conditions, a common assumption is that the local trading price should remain within the boundaries of the grid buying and selling price. In other words, the consumers would not be willing to participate in the local market if the local price is higher than the price they otherwise could get in the outer market, and prosumers would not sell their surplus at a lower price than what they could get elsewhere. However, many strategies for pricing and bidding between these boundaries have been proposed in the literature, all considering different properties such as product differentiation, heterogeneous participant preferences, and willingness to pay. The price-setting algorithms can generally be sorted into four categories; rule-based, auction-based, optimization-based, and game theoretic algorithms. Some are also combinations of these approaches. The following literature review is sorted into these categories in Table I.

Ref.	Rule-based	Auction	Optimization	Game Theory
[10]	✓			
[11]	✓			
[12]		✓		
[13]		✓		
[14]			✓	
[15]			✓	
[16]				✓
[17]				✓

TABLE I: Sorting of referenced literature based on pricing mechanism.

In most rule-based approaches, the local prices are determined after the actual trade has taken place. This is typically done using the ratio between supply and demand in the local market [10], or similar methods such as bill-sharing or mid-market rates [11]. Auction-based pricing relies on active bidding from the market participants but can be an efficient approach to ensure privacy preservation while ensuring benefits for both sellers and buyers [12]. However, many bidding strategies can be sensitive to market conditions and may lead to fluctuating local trading prices [13]. Another way to obtain local prices is to settle the local market through distributed optimization and obtain the prices from the Lagrangian multipliers [15]. Some argue that this method ensures privacy among market participants while also being able to capture individual preferences and benefits [14]. Lastly, price-setting games like the Stackelberg game [16], [17], where the prices are obtained from Nash equilibrium solutions, are popular ways of modeling competition, while still maximizing social welfare.

III. Self-Sovereign Identity

SSI is an emerging Identity Management System, where the main idea is to allow users the ownership and control of their identity data. Thus, only they can act as an administrator, eliminating the need for any Trusted Third Parties (TTPs) [18], [5], [19].

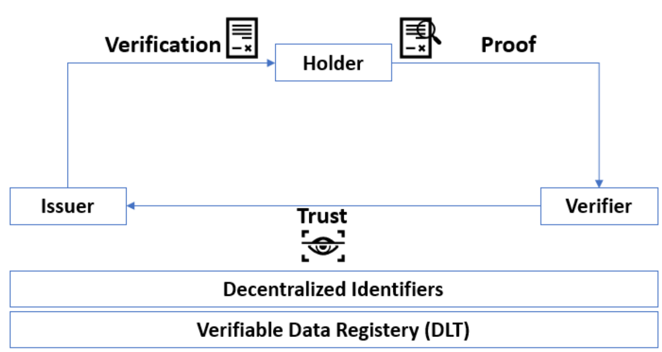

Fig. 1: Entities within the SSI framework.

As can be seen from Figure 1, SSI has several entities as Issuer, Holder, and Verifier, which is similar to other IMS. As the name suggests, an issuer (which can be a government, academic or other institution) issues credentials (known as Verifiable Credentials (VCs)) for a user, where the issued credentials consist of cryptographically signed claims regarding the user [5]. The holder denotes the user who is storing the credentials in a digital wallet. The verifier is the one who requests identity information or various other credentials from the holder, which receives this information within the format of Verifiable Presentations (VPs) [20] together with proof of their correctness. Using the Public Key (PK) of the issuer, the verifier can check the proof of correctness for the credentials sent from the holder.

Another important part within SSI is the Decentralized Identifiers (DIDs) [21], which are identifiers generated by a machine or user that are connected to the PK of the entity for verification purposes and help to uniquely identify them.

This type of verification mechanism can only work if the DIDs of entities, such as issuer can be stored in an immutable and tamper-proof way, which can be enabled by any DLT.

IV. Proposed Framework/Methodology

This section explains the proposed framework for integrating local energy transactions within a multi-DLT platform. Figure 2 shows a high-level architecture that includes the key components of the system.

1): The local energy community comprises the components of the physical layer of the system, such as DERs, storage assets, and the infrastructure of the power grid. Information regarding each of the prosumer's and consumer's net energy demands are provided through smart meter measurements. Each of the community agents will need to use the SSI Agent software to verify the user's identity before interacting with the ledger platform. Through verifiable credentials, the SSI agent also allows the user to control what data is shared with the platform and not. Presumably, the agents would interact with this software through mobile or web apps.

2): The underlying assumption of a functional local energy market is that there are necessary policies and regulations in place. This would further affect how the market is operated; e.g., how the prices are set and communicated back to the market participants. Relevant information issued to the local market trading platform at this point could also include subsidy arrangements, such as feed-in-tariffs, as it would generally influence, for example, the lower limit of local energy prices. Such energy policymakers would use SSI components to verify their identities and to interact with the system.

3): Furthermore, information from the outside power market must be provided to the local energy trading platform. This would naturally include day-ahead electricity spot prices, due to the general assumption that the local energy price should always be lower than the price consumers can get outside the market. Local energy markets could also provide services to the grid operator, and thus information regarding the power market or grid conditions could be issued here.

4): To interact with the local energy trading platform (discussed later) and the Multi-DLT Platform (discussed later), the components mentioned above would need to use the respective DLT Gateway.

5): The Local Energy Pricing and Management Engine is a smart contract-supported service. This component performs the necessary operations for clearing the market based on the information issued by other components through the DLT Gateway. Any of the aforementioned pricing and management mechanisms could be implemented in the engine. This module can be considered a core part of the main functionalities that link the cyber and physical components of the entire system.

6): The Multi-DLT platform consists of three interconnected layers. The transactions and management decisions assigned by the local energy pricing and management engine are facilitated by the DLT platform that supports smart contracts. All SSI agents use the SSI platform to facilitate the SSI functionality. The smart-contract DLT platform is responsible for hosting the Local Energy Pricing and Management Platform through its smart-contract environment. Middleware is used to communicate between the SSI platform and the smart-contract platform. Each entity submits the required information via VCs. The middleware verifies these credentials (after communicating with the SSI Platform) and upon verification, the submitted information is then fed to the smart-contract platform for further processing.

V. Cyber-Physical Security, Legislative and Privacy Aspects

Massive digitalization of modern power systems increases the potential cyber security risks due to the larger number of surfaces for cyber attacks. Therefore it is essential to increase the number of precautional methods to prevent, mitigate or minimize such new cyber-attack risks accordingly. End-user Advanced Metering Infrastructure (AMI) is becoming a mainstream part of the distribution network and collects massive amounts of data from multiple sources in real-time. To reduce the power grid's reliability, an attacker could try to attack either the data sources themselves or during the data transfer from the source to the intended destination. Thus, the data across the system should be recorded in a tamper-proof and immutable way, while also preserving the privacy of the end-users.

Using DLT as an underlying technological enabler for SSI allows participants to create a single source for their identity that everyone within the ecosystem can trust. Furthermore, the encrypted communication channel facilitated by SSI along with the usage of VCs to submit crucial information ensure the confidentiality and non-repudiation of the data. Additionally, with either interactive or non-interactive Zero Knowledge Proof (ZKP) protocols [22], the verification of user attributes can be done in a privacy-friendly manner.

The smart-contract DLT platform would require that every single interaction is digitally signed, which ensures the provenance of data. Since these transactions are verified by each node on the DLT platform and recorded across all, making

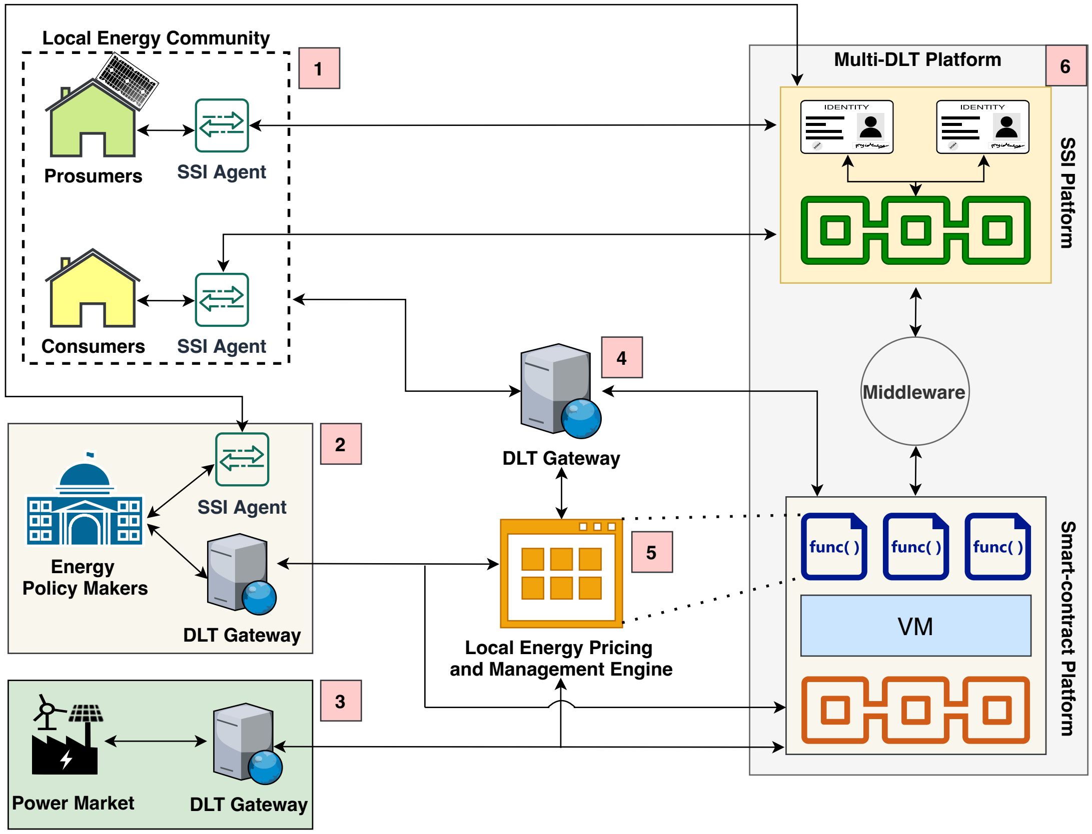

Fig. 2: High-level Architecture for the proposed framework.

malicious changes to any data submitted without the overall node becoming aware of it and rejecting them very difficult, if not impossible [23]. Furthermore, due to the decentralized and distributed nature of any DLT platform, designing a local energy market that utilizes a smart contract supporting the DLT platform will add a certain degree of resiliency.

Furthermore, local energy markets provide opportunities for new players like prosumers to participate in the power market. Information collection and processing related to interactive trading processes among end-users and other market entities can trigger new privacy discussions. Moreover, the proposed or similar SSI-based solutions give participating entities control over their identity data and how they interact with each other. Thus, only they can decide on which information to share with whom and can achieve more privacy than currently existing IMS. This approach is also beneficial for commercial organizations as they do not need to manage and store highly sensitive Personally Identifiable Information (PII) and take rigorous measures to comply with complex data protection regulations such as General Data Protection Regulation (GDPR). In addition to the pure cyber security framework, it is possible to extend the framework to cyber-physical security territories. IoT devices such as smart meters must be protected using additional security methods that can be associated with physical communication protocols. It is evident that various wireless communication protocols consist of embedded encryption algorithms that can provide additional protection to the system [24].

VI. Conclusions and Outlook

Decarbonization and decentralization of power systems with large penetration of renewable energy generations distributed over the electrical grid have been some of the main drivers of the current power markets and systems. Considerable amounts of distributed and renewable energy resources, primarily solar power, have been integrated into the grid-edge side of the power systems where consumers and prosumers are located. Local energy markets are among the most promising emerging domains of modern power systems and markets. These new markets also offer new options for various market participants, including new actors such as prosumers and aggregators. The interconnections and interrelations between power markets and local market participants are becoming more sophisticated and require new solutions to reduce complexity and address new threats to security and privacy. In addition, other new-generation digitalization technologies (e.g. blockchain) offer a wide spectrum of potential solutions related to complexity and interoperability. Blockchain technology can also provide a certain degree of cyber-physical security as discussed in previous sections. Such new solutions include the local energy trading and management platform that also consist of various vital features such as pricing mechanisms. Since solutions are data-driven and may require the share of private data such as prosumer power generation and consumption time series, privacy concerns also need to be considered. This will require the use of new models of IMS as older models are often privacy invasive. This work proposed a joint blockchain technology and SSI framework to provide a considerable solution to all these concerns. It is also essential to quantify the potential cyber-physical risks of use cases by developing new experimental or real industrial setups in the future. The technological solutions are quite mature in comparison to the legislative and juristic frameworks. These should still be developed by policy makers by considering early-stage studies like this work or more advanced studies to make better and conscious decisions to propose the next-generation legislative framework.

References

[1] U. Cali, M. Kuzlu, M. Pipattanasomporn, J. Kempf, and L. Bai, *Digitalization of Power Markets and Systems Using Energy Informatics*, 2021.

[2] S. Bjarghov, M. Loschenbrand, A. U. Ibn Saif, R. Alonso Pedrero, C. Pfeiffer, S. K. Khadem, M. Rabelhofer, F. Revheim, and H. Farahmand, "Developments and Challenges in Local Electricity Markets: A Comprehensive Review," *IEEE Access*, vol. 9, pp. 58 910–58 943, 2021.

[3] W. Tushar, C. Yuen, T. K. Saha, T. Morstyn, A. C. Chapman, M. J. E. Alam, S. Hanif, and H. V. Poor, "Peer-to-peer energy systems for connected communities: A review of recent advances and emerging challenges," *Applied Energy*, vol. 282, p. 116131, 1 2021.

[4] M. S. Ferdous, "User-controlled identity management systems using mobile devices," 2015.

[5] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103 059–103 079, 2019.

[6] S. K. Venkatachary, J. Prasad, and R. Samikannu, "Cybersecurity and cyber terrorism-in energy sector–a review," *Journal of Cyber Security Technology*, vol. 2, no. 3-4, pp. 111–130, 2018.

[7] ——, "Economic impacts of cyber security in energy sector– a review," *International Journal of Energy Economics and Policy*, vol. 7, no. 5, p. 250, 2017.

[8] K. Zhang, S. Troitzsch, S. Hanif, and T. Hamacher, "Coordinated Market Design for Peer-to-Peer Energy Trade and Ancillary Services in Distribution Grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 4, pp. 2929–2941, 2020.

[9] M. F. Zia, M. Benbouzid, E. Elbouchikhi, S. M. Muyeen, K. Techato, and J. M. Guerrero, "Microgrid transactive energy: Review, architectures, distributed ledger technologies, and market analysis," *IEEE Access*, vol. 8, pp. 19 410–19 432, 2020.

[10] U. Cali and O. Cakir, "Energy Policy Instruments for Distributed Ledger Technology Empowered Peer-to-Peer Local Energy Markets," *IEEE Access*, vol. 7, pp. 82 888–82 900, 2019.

[11] M. Grzanic, J. M. Morales, S. Pineda, and T. Capuder, "Electricity Cost-Sharing in Energy Communities under Dynamic Pricing and Uncertainty," *IEEE Access*, vol. 9, pp. 30 225–30 241, 2021.

[12] L. Wang, J. Liu, R. Yuan, J. Wu, D. Zhang, Y. Zhang, and M. Li, "Adaptive bidding strategy for real-time energy management in multi-energy market enhanced by blockchain," *Applied Energy*, vol. 279, no. C, 12 2020. [Online]. Available: https://ideas.repec.org/a/eee/appene/v279y2020ics0306261920313398.html

[13] J. Lin, M. Pipattanasomporn, and S. Rahman, "Comparative analysis of auction mechanisms and bidding strategies for P2P solar transactive energy markets," *Applied Energy*, vol. 255, no. August, p. 113687, 2019. [Online]. Available: https://doi.org/10.1016/j.apenergy.2019.113687

[14] T. Morstyn and M. D. McCulloch, "Multiclass Energy Management for Peer-to-Peer Energy Trading Driven by Prosumer Preferences," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 4005–4014, 2019.

[15] M. H. Ullah, A. Alseyat, and J. D. Park, "Distributed Dynamic Pricing in Peer-to-Peer Transactive Energy Systems in Smart Grid," *IEEE Power and Energy Society General Meeting*, vol. 2020-Augus, pp. 1–5, 2020.

[16] E. Fernandez, M. J. Hossain, K. Mahmud, M. S. H. Nizami, and M. Kashif, "A Bi-level optimization-based community energy management system for optimal energy sharing and trading among peers," *Journal of Cleaner Production*, vol. 279, p. 123254, 1 2021.

[17] Y. Jiang, K. Zhou, X. Lu, and S. Yang, "Electricity trading pricing among prosumers with game theory-based model in energy blockchain environment," *Applied Energy*, vol. 271, p. 115239, 8 2020.

[18] C. Allen. The Path to Self-Sovereign Identity - Life With Alacrity. Accessed: 2022-04-27. [Online]. Available: http://www.lifewithalacrity.com/previous/2016/04/the-path-to-self-sovereign-identity.html

[19] J. Strüker, N. Urbach, T. Guggenberger, J. Lautenschlager, N. Ruhland, V. Schlatt, J. Sedlmeir, J.-C. Stoetzer, and F. Völter, "Mixed Self-Sovereign Identity Foundations, Applications, and Potentials of Portable Digital Identities Self-Sovereign Identity Foundations, Applications, and Potentials of Portable Digital Identities," Fraunhofer FIT, Tech. Rep., 2021. [Online]. Available: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/FraunhoferFIT_SSI_Whitepaper_EN.pdf

[20] Verifiable Credentials Data Model 1.0. Accessed: 2022-04-27. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[21] Decentralized Identifiers (DIDs) v1.0. Accessed: 2022-04-27. [Online]. Available: https://www.w3.org/TR/did-core/

[22] C. Lin, D. He, H. Zhang, L. Shao, and X. Huang, "Privacy-Enhancing Decentralized Anonymous Credential in Smart Grids," *Computer Standards & Interfaces*, vol. 75, p. 103505, 4 2021.

[23] V. Dehalwar, M. L. Kolhe, S. Deoli, and M. K. Jhariya, "Blockchain-based trust management and authentication of devices in smart grid," *Cleaner Engineering and Technology*, vol. 8, p. 100481, 6 2022.

[24] M. P. Manuel and K. Daimi, "Implementing cryptography in LoRa based communication devices for unmanned ground vehicle applications," *SN Applied Sciences*, vol. 3, no. 4, pp. 1–14, 2021.