A Trust Framework for Peer-to-Peer Energy Markets

Boitumelo Leotlela[12][0009-0008-5863-9356] Lehlogonolo Ledwaba[2][0000-0002-7292-2835] Marijke Coetzee[1][0000-0002-9157-3079]

[1] North-West University, Potchefstroom 2531, South Africa
[2]Council of Scientific and Industrial Research, Meiring Naude Rd, Pretoria, 0184, South Africa
{tleotlela, lledwaba4}@csir.co.za, Marijke.coetzee@nwu.ac.za

Abstract. Peer-to-peer energy markets rely on trust to enable secure participation; however existing trust models often address only isolated trust concerns. This fragmented approach leaves significant gaps in ensuring holistic trust across the peer-to-peer energy market and exposes participants to threats in the market. To address this, the paper proposes a trust framework grounded in the Trust over IP (ToIP) model, which integrates technical mechanisms and governance policies to sustain trust in decentralised environments. Using the STRIDE threat model, key threats in the peer-to-peer energy market are identified, while also analysing how existing research mitigates these risks. The corresponding trust and security mechanisms are then mapped to the ToIP architecture, offering a comprehensive approach to trust establishment, that unifies social-behavioural and security dimensions of trust. By leveraging ToIP as a formal foundation for trust establishment in this work, the proposed framework provides a holistic approach to building and maintaining trust in the market, thereby fostering greater user confidence and encouraging broader market participation.

Keywords: peer-to-peer energy market, trust, threat model, trust over IP.

1 Introduction

The global energy sector continues to grapple with the persistent challenge of the energy trilemma, which entails balancing the competing demands of energy security, environmental sustainability, and affordability [1]. To address this challenge, peer-to-peer energy markets are seen as an innovative and promising solution [2]. Localised energy markets are facilitated when participants generate energy from renewable energy sources and trade energy directly with each other, without the need for a central authority.

These markets face a significant obstacle, namely a lack of trust. As participants have no prior relationship with each other, and no central authority exists to ensure fair play, doubts arise over whether participants will honour obligations, respect privacy, and avoid exploiting vulnerabilities for personal gain.

Blockchain technology is a foundational trust-enabling technology due to its inherent characteristics, including transparent and immutable ledgers, smart contracts that automate transactions, and consensus mechanisms [2]. However, blockchain on its own does not guarantee the trustworthiness of peers in the market. Prior work has addressed trust in peer-to-peer energy markets in isolation, such as obligation fulfilment [3], fair

transactions [4], or the security and privacy of data [5, 6]. Only a few attempts have approached trust establishment holistically [7, 8]. However, they do not consider critical dimensions such as privacy and fair energy transactions.

This gap highlights the need for a trust framework specifically designed for peer-to-peer energy markets. Such a trust framework can integrate multiple trust dimensions into a unified view that supports reliable and secure trading, while also encouraging broader participation. Next, Section 2 discusses the architecture of the peer-to-peer energy market, as well as trust and reputation considerations. A threat model for the peer-to-peer energy market is presented in Section 3. Section 4 provides a summary of related work, illustrating how market threats are currently addressed. Section 5 provides recommendations for defining a holistic trust framework for the peer-to-peer energy market. The paper concludes in Section 6.

2 Trust, reputation and peer-to-peer energy markets

Trust is defined [9] as 'the reliance upon the behaviour of a person to achieve a desired but uncertain objective in a risky situation'. In the peer-to-peer energy market, buyers and sellers expect their trading counterparts to behave in a trustworthy manner. The presence of risk and uncertainty exists as a buyer could act maliciously in pursuit of their own interests and benefits. The seller, therefore, needs to decide to trust and transact with the buyer even though no trusted third party exists [10]. If the buyer were unreliable, the seller would be vulnerable to being cheated. These uncertainties and threats undermine the willingness of peers to trade in the peer-to-peer energy market.

Braga, et al. [10] defined reputation as 'the perception an agent has of another agent, which is used to choose a cooperation partner' based on their previous interactions. Reputation reduces uncertainties in the market by providing buyers and sellers insight into the behaviour of other market participants. By having access to another participant's reputation rating, a seller can choose the best buyer, thereby reducing uncertainties and risks. Reputation in decentralised systems has its own vulnerabilities, such as sybil and collusion attacks [10].

2.1 Trust requirements for the peer-to-peer energy market

For trust to be effectively established in the peer-to-peer energy market, trust requirements [11] must be met. These include authentication, which ensures that only legitimate devices and peers engage in market activities; integrity (immutability) and transparency, which maintain the integrity of records and allow peers to verify actions independently; and privacy and confidentiality, which protect sensitive trading and consumption data. Accountability is required to trace actions and enforce responsibility, while fair trading ensures that transactions reflect terms that were agreed upon.

Reputation management and behaviour tracking enables peers to assess the trustworthiness of others based on their past behaviour and implement incentive/penalty schemes to guarantee Honest peer-behaviour. Reliable consensus guarantees that only reliable participants trade in the market and validate transactions. Together, these requirements form the foundation upon which trust is distributed across the market architecture.

2.2 Trust in the peer-to-peer energy market architecture

Trust in the peer-to-peer energy market should be established and reinforced across all layers of the architecture. The architecture of the peer-to-peer energy market can be structured into six interrelated layers. The architecture is briefly described next, starting with the lowest layer where energy is transferred.

Table 1. Trust in the peer-to-peer energy market

Architecture Layer	Mechanisms (Trust & Security)
Business/ Governance Layer	• Rules for trust and reputation management (market/role-based) [3, 6-8] • Market rules [3, 4, 7, 8, 12, 13, 15] • Policies for smart contract-based dispute resolution and penalty/incentive schemes [3, 4, 8, 12, 14, 15] • Privacy and data protection policies [13]
Application Layer	• Cryptography/encryption (PKI, homomorphic encryption) [5-8, 14] • Trust and reputation monitoring and evaluation [3, 4, 7, 13, 15] • Automated dispute handling and enforcing meeting commitments [8] • Authentication of peer accounts [8]
Market (Blockchain) Layer	• Smart contracts for trading, settlement, and penalties [3, 4, 7, 8, 12, 13, 15] • Reputation-based blockchain consensus [3-8, 12-14] • Identity, registration and privacy mechanisms at the blockchain level [7, 8, 15]
Network Layer	• Secure communication protocols (TLS) between authenticated devices [8, 14] • Anonymity-preserving routing [6] • Session-based authentication [7]
Device/Perception Layer	• Device authentication & access control [7, 8] • Encryption and privacy primitives on devices [5, 15] • Tamper-proof smart meters [7, 15] • Certificate authorities and pseudonymous identities [6, 7]
Grid/Infrastructure Layer	• Secure infrastructure and load balancing and grid stability mechanisms to ensure reliable energy supply (Grid Service Charges based on behaviour) [15]

The *Grid Infrastructure Layer* comprises renewable energy sources and microgrid infrastructure, such as transformers and power connections. The components in this layer are responsible for generating and transferring electricity between participants. The *Perception/Device Layer* consists of IoT devices, including sensor appliances in households and smart meters that monitor energy generation, consumption, and grid conditions. These devices bridge physical energy flows with the digital market platform, linking each smart meter to its corresponding market account to facilitate the automated collection of energy trading data. The Network Layer enables secure, reliable, and efficient data transmission from the devices to higher layers.

The *Market Layer* is where energy trading is orchestrated and managed via pricing, bidding, allocation, and settlement. Blockchain enables decentralised cooperation without relying on central oversight. The *Application Layer* provides user-facing interfaces and services in the market. Interfaces support access to the market platforms through authenticated identities and accounts. Peers trade with each other using reputation scores to make informed decisions, therefore encouraging honesty and

fairness in transactions. Finally, the *Business/Governance Layer* defines overarching policies and compliance rules of the market. By enforcing trading and market rules, this layer ensures accountability, fair trading, and incentive structures for trustworthy behaviour, ensuring that market operations adhere to regulations and security standards, which form a foundation for reliable and secure energy trading in the peer-to-peer energy market.

Trust formation: The formation of trust across the layers is now discussed from an operational perspective. Trust begins at the *Governance Layer*, where market rules and policies set expectations for fair participation, accountability, secure and private communication, authentication, and dispute resolution across all layers. At the *Application Layer*, participants buy and sell energy in accordance with established governance rules. The *Market Layer* operationalises trust through smart contracts that enforce obligations, apply penalties, and ensure compliance via consensus mechanisms, eliminating the need for intermediaries. When a transaction is initiated, blockchain provides trust in the market layer by validating payments through consensus mechanism and recording transactions on immutable and transparent ledgers. Trust is further reinforced in the *Network and Device Layers*, where authentication, secure communication, and privacy-preserving mechanisms protect data flows and device outputs. At the *Grid Infrastructure Layer*, reliable grid operations and legitimate grid components ensure that energy is delivered to the relevant buyer, thus completing the trust loop.

Table 1 lists each layer and the trust and security mechanisms that support it.
This integrated view illustrates how trust requirements and mechanisms combine to establish trust throughout the market's architecture, ensuring trustworthy and secure energy trading. However, several threats may compromise market operations and, consequently, user participation, and are discussed in the next section.

3 Threat model of the peer-to-peer energy market architecture

When security threats undermine the availability, integrity, and confidentiality of systems and data, trust across all layers of the market architecture is eroded. Microsoft's STRIDE [16] threat modelling framework can systematically categorise and map threats to determine their impact on trust in the peer-to-peer energy market.

The STRIDE-based threat model presented in Table 2 summarises the threats and how the threats erode trust and specific layers of the peer-to-peer energy market. The threat model illustrates that threats in one layer of the market architecture can propagate into others, amplifying the impact of the risks. Notably, high-risk threats directly undermine the fairness, immutability, and integrity of transactions, as well as the reliability of consensus, market availability, and the overall system reliability.

Medium-risk threats, although less disruptive in the short term, can still erode accountability, privacy, confidentiality, and eventually user confidence over time. The following section discusses how threats in the peer-to-peer energy market are currently addressed.

Table 2. Threats in the peer-to-peer energy market

STRIDE Category	Threat / Attack	Trust Erosion	Affected Layer	Risk Level
Spoofing	Impersonation of smart meters or user accounts [8]	Loss of legitimacy, manipulated readings, reduced trust in peers	Device & Application Layer	**High**
Tampering	Physical sabotage of grid infrastructure or meters [7]	Compromised data integrity, unfair outcomes, reduced confidence in grid reliability	Grid & Device Layer	**High**
	Double-spending attacks [7, 8]	Same energy sold multiple times, undermines fairness and loss of transaction integrity	Market & Application Layer	**High**
Repudiation	Defaulting on obligations [3]	Peers deny actions, undermines accountability and governance	Governance & Market Layer	**Medium**
Information Disclosure	Eavesdropping/interception of communications [5]	Privacy violations, reduced confidence in secure communication	Network Layer	**Medium**
	Linking attacks via transparent ledgers [4]	Re-identification, loss of privacy, reduced user confidence	Market & Application Layer	**Medium**
Denial of Service (DoS)	Physical sabotage disrupting energy supply [8, 13]	Energy unavailability, reduced trust in reliability of the grid	Grid & Device Layer	**High**
	Flooding attacks on market platforms or consensus nodes [8]	Market inaccessibility, peers perceive instability and unreliability	Network & Market Layer	**High**
Elevation of Privilege	Sybil attacks manipulating consensus & reputation [7]	Loss of fairness, corrupted validation and market integrity	Market & Ap-plication Layer	**High**
	Malicious operator or privileged insider manipulates rules and reputation [5]	Erosion of institutional trust; perception of biased or unfair market rules, corrupted reputation	Governance & Application Layer	**Medium**

4 Related Work

Considering the threats that erode trust in the market, this reviews how current trust frameworks and models target threats and trust enforcement across the architectural layers of the market. The studies are among the ten most frequently cited works identified through a systemic literature review using the PRISMA methodology. Early work focused on securing information exchange and coordination through cryptographic primitives and fault-tolerant algorithms. Ping, et al. [5] proposed to protect against untrusted coordinators and information disclosure using a Byzantine-fault-tolerant algorithm and Shamir's secret-sharing encryption of bids/offers. Similarly, [6, 14, 15] incorporated privacy-preserving cryptography, reputation-enhanced consensus, and economic incentives to enforce fairness, transparency, and accountability, primarily targeting governance, application, and blockchain layers.

A second stream of research emphasises reputation and trust-based consensus mechanisms to regulate participant behaviour. Chowdhury, et al. [13] and Khan, et al. [12] use trust scores, fuzzy logic, and penalties to encourage honest participation, reducing the impact of selfish mining, Sybil attacks, repudiation and malicious trading. The system proposed in [3] builds on these ideas by implementing reputation-based delegated consensus, filtering low-reputation participants, and ensuring fairness and reliability. These works effectively govern participant behaviour and enforce fairness, but do not extend trust mechanisms to the device layer, leaving underlying infrastructure vulnerabilities unaddressed.

More recent contributions adopt broader frameworks that integrate technical, behavioural, and economic safeguards. The work proposed by Khan, et al. [7] combined prosumer-centric consensus, smart contracts, cryptographic protection, and attribute-based access control for tamper-resistant smart meters, securing governance, application, blockchain, and device layers. Similarly, Yahaya, et al. [4] leveraged timed commitments, hybrid encryption, and energy-based reputation mechanisms to ensure fairness, accountability, and privacy across all layers in their implementation. These approaches integrate technical, behavioural, economic, and privacy-preserving mechanisms, demonstrating robust, multi-layered trust enforcement.

Samy, et al. [8] proposed the most holistic model by embedding trust mechanisms into governance, application, blockchain, and device layers simultaneously. At the governance level, collusion, denial-of-service, and price manipulation were mitigated through market rules, allocation limits, and reputation scores. Application-level threats were countered with Hyperledger Fabric channels, private data collections, encryption, digital signatures, and TLS. Blockchain-layer attacks, such as 51% and appending attacks, were addressed through permissioned blockchain consensus and identity management. At the device layer, smart meter identities were validated and data encrypted to prevent malicious injection. Compared to other studies, the studies in [4, 7, 8] addressed the broadest range of trust concerns across all layers, highlighting the importance of integrating governance, technical, privacy, and device-level protections to foster confidence in peer-to-peer energy markets. Despite these advances, many studies [3, 5, 6, 12-15] still address trust in a fragmented manner. This fragmentation underscores the gap between theoretical frameworks and the need for robust, end-to-end trust architectures in peer-to-peer energy markets.

5 A trust framework for peer-to-peer energy markets

A trust framework for peer-to-peer energy markets should be multi-layered, holistic, and socio-technical, since trust is not only about cryptography and blockchain but also governance, market fairness, participant behaviour, and device reliability. van der Peet, et al. [17] define a trust framework as “legally enforceable set of specifications, rules and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements” [17].

Foundational trust frameworks in peer-to-peer network literature include PeerTrust [18] and EigenTrust [19]. However, these frameworks focus on trust evaluation and monitoring peer behaviour, neglecting a holistic approach.

In this regard, the Trust over IP (ToIP) framework [20] aims to bridge technical assurance and human governance into a universal framework for digital trust. Its architecture, modelled on TCP/IP's layers, ensures that trust can be established, verified, and governed at Internet scale through a dual-stack, four-layer system centred on verifiable identifiers. ToIP combines cryptographic assurance at the machine/technology level with a ToIP technology stack and human accountability at the governance, business, legal, and social levels using a ToIP governance stack. For this reason, this framework is selected as a foundation to define a trust framework for peer-to-peer energy markets as it directly addresses the core challenges of decentralisation, trust, and governance.

The Trust over IP (ToIP) framework is a reference model and architectural framework designed to guide the establishment of digital trust through a combination of technical verifiability and human accountability [20]. The ToIP architecture is often depicted as a four-layer hourglass that is inspired by the TCP/IP stack, with each layer serving specific trust functions. At the same time, governance overlays each layer [20]:

- Layer 1 – Trust Support Layer (Utilities): Provides the foundational cryptographic trust primitives, such as decentralised identifiers (DIDs), ledgers, or other cryptographic utilities that anchor digital identity. Utility governance frameworks define who operates the network and under what rules.
- Layer 2 – Trust Spanning (DID Communication) Layer: Enables secure, private, authenticated peer-to-peer communication between agents using DID communication protocols for issuing credentials and providing proofs for the credentials. Governance frameworks define interoperability and security standards for agents and networks.
- Layer 3 – Trust Task (Verified Credentials) Layer: Supports the issuance, holding, and verification of verifiable credentials. Credential governance frameworks define schemas, authorised issuers, and rules for verification to ensure claims are trustworthy.
- Layer 4 – Trust Application (Application Ecosystem) Layer: Provides application-level ecosystems where entities interact based on shared credentials, governed trust frameworks, and mutually recognised rules of engagement. Ecosystem governance frameworks define roles, responsibilities, and accountability within a specific business domain, such as a peer-to-peer energy market.

5.1 ToIP mapped to the peer-to-peer energy market

This research aims to view the peer-to-peer energy market through the ToIP lens as the initial conceptualisation of a trust framework. Peer-to-peer energy markets face three main trust problems. Firstly, technical trust is necessary to ensure data integrity, secure communication, and protection against tampering or fraud [4]. Secondly, behavioural trust ensures that market participants act honestly and do not repudiate or manipulate trades [3]. Finally, institutional trust involves establishing rules, accountability, and governance without relying on a central authority [13].

The ToIP dual stack (technology and governance) mirrors these needs by combining cryptographic assurance with human accountability [20], making it a natural fit.

Table 3. illustrates how ToIP can be applied as a trust framework for the peer-to peer energy market.

Table 3. ToIP layers mapped to the architecture layers of the peer-to-peer energy market.

Technical	Governance
Layer 4: Defines market rules, trust and reputation management, security, and all policies	
• Application-facing trading mechanisms (prioritisation by reputation) [3]. · Smart contracts for trading logic, allocation, dispute handling, penalties [4, 14]. • Fair energy trading mechanisms [3, 4] • Reputation monitoring [13].	• Market rules– pricing fairness, dispute resolution, transaction settlement, and validator selection for blockchain consensus [3, 13] . • Policies implications – privacy frameworks, data protection, access control, authentication, and accountability [5, 7]. • External regulatory alignment – adapting P2P energy trading to national energy laws, consumer protection, grid stability [15].
Layer 3: Issues and verifies digital credentials	
• Device and user identity validation (CA validation of smart meters) [7]. • Reputation as a form of verifiable credential (trust and reputation models to prove trustworthiness) [3]. • Role-based evaluation (buyer, seller, validator reputation as credentials) [8].	• Authentication/identity validation policies [7] • Reputation management – trust scores, smart meter-based behaviour tracking to select reliable nodes [13]. • Incentives and penalties – demurrage fees, rewards for auditing, penalties for malicious behaviour [14].
Layer 2: Ensures secure peer-to-peer communication	
• Secure communication protocols (Fabric channels, encrypted off-chain communication) [4, 5]. • Secure anonymity-preserving message routing [6]. • Session-based authentication to mitigate possibility of linking identity to trading behaviour [7].	• Interoperability policies – who can trade across communities or jurisdictions [12]. • Specify Cryptographic standards to preserve confidentiality [4, 5]. • Communication access and credential policies – rules stipulating that only users with authenticated credentials can interact or trade in the market [6, 7]. • Anonymity and privacy policies [6, 7] to define how anonymity can be preserved during routing or market interactions.
Layer 1: Provides unique, tamper-proof digital identities for participants and devices	
• Pseudonymous identities (in place of decentralised identities) [7] • Blockchain-based immutable ledgers secured through consensus mechanisms	• Certificate Authorities (CAs): Initialisation of keys and registration for pseudonymous identities [6, 7]. • Standards for device/meter certification – ensuring regulatory compliance at the infrastructure level [7, 8, 15]. • Grid stability rules for registered infrastructure [17] • Permissioned lists for which participants/devices can be part of the blockchain network [8].

The foundation of the first three layers provides technical and governance measures to ensure that participant devices are linked to identities in the market, communication is secure, and that identities and participant behaviour are verifiable. These layers help mitigate risks of identity spoofing, tampering, and eavesdropping. This security foundation, in combination with the application ecosystem at Layer 4 and related governance policies for behavioural and market-specific policies, enables the implementation of social trust mechanisms that provide assurances of fair transactions, accountability, honest trading, reliable consensus, and trust/reputation management.

This ensures that threats stemming from malicious participant behaviour is mitigated through market related social trust mechanisms and governance rules.

The ToIP framework stands out by integrating security, governance, and market-oriented trust concepts across all layers, unlike existing approaches that typically address only isolated trust concerns. By covering both technical and governance dimensions, it ensures that trust is reinforced throughout the peer-to-peer energy market architecture. Mechanisms such as consensus, reputation, incentives, and external policy alignment embed trust into operations while supporting decentralization and regulatory compliance. This layered approach establishes a formal foundation for transparency, accountability, and broad participation in decentralised energy trading, while also highlighting gaps overlooked by current frameworks.

By viewing trust establishment in the peer-to-peer energy market through the ToIP inspired trust framework, a comprehensive and holistic approach to trust establishment and management can be achieved. The impact of governance across all layers is made explicit, which is generally not visible in current works.

6 Conclusion

By mapping the layers of the peer-to-peer energy market architecture to those of the ToIP framework, this paper underscores the value of formal foundations for trust frameworks. Additionally, the study demonstrated how the ToIP view can facilitate trust establishment and management in the peer-to-peer energy market. The combination of security foundations, human accountability, and governance of the ToIP framework forms the foundation for a trust framework that guarantees secure transactions and credentials. The integration of social trust mechanisms ensures reliable and fair energy trading.

Future work will focus on utilising this ToIP-inspired trust framework to evaluate existing peer-to-peer energy market trust models. Such an evaluation can identify where current trust models lack technical or governance in a lightweight and efficient manner. In doing so, the framework can serve as a foundation for designing a secure and trust aware decentralised energy market, ensuring energy security and availability.

References

1. World Energy Council, "World Energy Trilemma 2024: Evolving with Resilience and Justice," World Energy Council, 15, 2024. [Online]. Available: https://www.worldenergy.org/publications/entry/world-energy-trilemma-report-2024
2. Y. Zhou, J. Wu, C. Long, and W. Ming, "State-of-the-Art Analysis and Perspectives for Peer-toPeer Energy Trading," Engineering, vol. 6, no. 7, pp. 739-753, 2020/07/01/ 2020, doi: https://doi.org/10.1016/j.eng.2020.06.002.
3. T. Wang, J. Guo, S. Ai, and J. Cao, "RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration," Appl. Energy, vol. 295, p. 117056, 2021, doi: https://doi.org/10.1016/j.apenergy.2021.117056.
4. A. S. Yahaya, N. Javaid, M. U. Javed, A. Almogren, and A. Radwan, "Blockchain-Based Secure Energy Trading With Mutual Verifiable Fairness in a Smart Community," IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 7412-7422, 2022, doi: 10.1109/TII.2022.3141867.

5. J. Ping, Z. Yan, and S. Chen, "A Privacy-Preserving Blockchain-Based Method to Optimize Energy Trading," IEEE Transactions on Smart Grid, vol. 14, no. 2, pp. 1148-1157, 2023, doi: 10.1109/TSG.2022.3198165.
6. O. Samuel and N. Javaid, "GarliChain: A privacy preserving system for smart grid consumers using blockchain," Int. J. Energy Res., vol. 46, no. 15, pp. 21643-21659, 2022, doi: 10.1002/er.7040.
7. M. H. D. Khan, J. Imtiaz, and M. N. U. Islam, "A Blockchain Based Secure Decentralized Transaction System for Energy Trading in Microgrids," IEEE Access, vol. 11, pp. 47236-47257, 2023, doi: 10.1109/ACCESS.2023.3275752.
8. A. Samy, H. Yu, H. Zhang, and G. Zhang, "SPETS: Secure and Privacy-Preserving Energy Trading System in Microgrid," Sensors, vol. 21, no. 23, p. 8121, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/23/8121.
9. A. J. I. Jones, "On the concept of trust," Decision Support Systems, vol. 33, no. 3, pp. 225-232, 2002/07/01/ 2002, doi: https://doi.org/10.1016/S0167-9236(02)00013-1.
10. D. D. S. Braga, M. Niemann, B. Hellingrath, and F. B. D. L. Neto, "Survey on Computational Trust and Reputation Models," ACM Comput. Surv., vol. 51, no. 5, p. Article 101, 2018, doi: 10.1145/3236008.
11. B. Leotlela, L. Ledwaba, and M. Coetzee, "Trust requirements and mechanisms in peer-to-peer energy markets," presented at the Information Security South Africa (ISSA) Conference, Boardwalk International Convention Centre, Gqeberha, 2025, preprint.
12. M. H. D. Khan, A. Haider, J. Imtiaz, and M. N. U. Islam, "A Multi-Layered Trust Enhancing Consensus Mechanism for Decentralized Energy Trading," 2024, pp. 1-8, doi: 10.1109/ICECE61222.2024.10505266.
13. M. J. M. Chowdhury et al., "A Cross-Layer Trust-Based Consensus Protocol for Peer-to-Peer Energy Trading Using Fuzzy Logic," IEEE Internet of Things Journal, vol. 9, no. 16, pp. 1477914789, 2022, doi: 10.1109/JIOT.2021.3063710.
14. S. Omaji and N. Javaid, "A Secure Blockchain-based Demurrage Mechanism for Energy Trading in Smart Communities," Int. J. Energy Res., 2020, doi: 10.1002/er.5424.
15. M. Khorasany, A. Dorri, R. Razzaghi, and R. Jurdak, "Lightweight blockchain framework for location-aware peer-to-peer energy trading," International Journal of Electrical Power & Energy Systems, vol. 127, p. 106610, 2021, doi: 10.1016/j.ijepes.2020.106610.
16. Microsoft Learn. "Microsoft Threat Modeling Tool threats." Microsoft. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats (accessed 11 September, 2025).
17. L. van der Peet, N. Bharosa, S. Dijkhuis, and M. Janssen, "Understanding Trust Frameworks: Goals and Components Identified Through a Case Study," in Electronic Participation, Cham, M. R. Johannessen et al., Eds., 2024// 2024: Springer Nature Switzerland, pp. 223-238.
18. X. Li and L. Ling, "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843-857, 2004, doi: 10.1109/TKDE.2004.1318566.
19. S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," presented at the Proceedings of the 12th international conference on World Wide Web, Budapest, Hungary, 2003. [Online]. Available: https://doi.org/10.1145/775152.775242.
20. Trust Over IP Foundation, "Introduction to Trust Over IP Version 2.0," 2021. [Online]. Available: https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf