Evaluating Trust Models for the IoT-enabled Peer-to-Peer Energy Market

[1,2]Boitumelo Leotlela
School of Computer Science and Information Systems
North-West University
Potchefstroom, South Africa
0009-0008-5863-9356

[2]Lehlogonolo P.I Ledwaba
Next-Gen Enterprises and Institutions
[2]Council for Scientific and Industrial Research
Pretoria, South Africa
0000-0002-7292-2835

[1]Marijke Coetzee
School of Computer Science and Information Systems
[1]North-West University
Potchefstroom, South Africa
0000-0002-9157-3079

***Abstract*—The decentralised nature of peer-to-peer (P2P) energy markets creates an environment where trust is difficult to establish. Supported by Internet of Things (IoT) devices, trust and security challenges arise, due to the absence of central oversight and the risk of uncooperative participant behaviour. A comparative analysis of existing trust management models and schemes is conducted in this study comparing how they are designed to encourage cooperation and ensure reliable interactions in decentralized energy markets. Emphasis is placed on how these models integrate security mechanisms to build trust and on their computational efficiency for IoT-constrained environments. The analysis highlights the trade-offs between trust management and IoT device performance, identifying limitations in scalability and latency as participation scales. Results indicate that while several models effectively build trust and promote cooperation, many impose significant resource demands, underscoring the need for balance between trust assurance and operational efficiency. This work provides a comprehensive evaluation of trust mechanisms in transactive energy systems and offers insights into their practical viability in resource-constrained, decentralized environments.**

Keywords—Energy trading, IoT, Trust-model, P2P

I. Introduction

South Africa faces persistent energy shortages, load shedding, and grid reliability issues due to ageing infrastructure, supply constraints, and a reliance on centralised power generation. Peer-to-peer energy markets offer a promising solution that allows consumers to directly trade surplus electricity without intermediaries, promoting energy autonomy, cost efficiency, and sustainability [1]. However, this decentralised approach also challenges trust and cooperation, as it lacks a central authority to enforce rules and guarantee fair transactions. The Internet of Things (IoT) is crucial in enabling these markets by facilitating real-time monitoring and communication [2]. However, IoT devices are resource-constrained and cannot handle computationally heavy processes like complex cryptographic algorithms [3] alongside other market-related operations, making it difficult to deploy strong trust and security mechanisms without overloading devices [4]. Furthermore, the decentralised architecture increases risks such as fraud and not fulfilling their obligations by defaulting on agreements, emphasising the need for robust yet efficient trust solutions. Blockchain has emerged as a promising trust technology offering transparency, immutability, and automation through smart contracts [5, 6]. Yet, models using Proof-of-Work (PoW) are computationally intensive and unsuitable for IoT environments [6]. To enable reliable and secure peer-to-peer energy trading, trust models need to be lightweight while ensuring participants' cooperation and market security. Cooperation in this work refers to participants engaging reliably and honestly in the market, and following market rules, where cooperation hinges on mutual trust [6]. Obligation fulfilment, in this context, refers to participants consistently executing their responsibilities [5]. Ensuring both cooperation and obligation fulfilment is critical to maintaining a functional peer-to-peer energy market that participants will be comfortable to participate in. This research explores how existing trust management models and schemes in peer-to-peer energy markets, hereafter referred to as trust models, foster trust and cooperation. Models are compared across these dimensions to identify those best suited for decentralised peer-to-peer energy trading. Specifically, the study aims to achieve this by examining:

1. How is cooperation achieved in peer-to-peer and decentralised energy markets?
2. How can obligation fulfilment be enforced without a central authority?
3. How do the models affect IoT performance?

This paper will be divided into several sections. Section II discusses the role of IoT devices in the peer-to-peer energy markets along with a background on trust and cooperation. In Section III, the trust models in peer-to-peer energy markets are explored and further analysed in Section IV concerning the establishment of cooperative trust in the market, and their coverage of trust requirements of the peer-to-peer energy markets. A comparative analysis is performed on the trust models in Section V, where the projected performance of the models is presented. The paper concludes by summarising the results and proposing future work.

II. Background

IoT devices are essential for the efficient operation of peer-to-peer energy markets. They collect real-time data, monitor energy consumption and generation, and automate transactions. For instance, smart meters provide accurate data for trading decisions, while Energy Management Systems

This work was supported in part by the Council of Scientific and Industrial Research and the Department of Science and Innovation within the ambit of the Foundational Digital Capabilities Research (FDCR) programme [Project KR5ETRT].

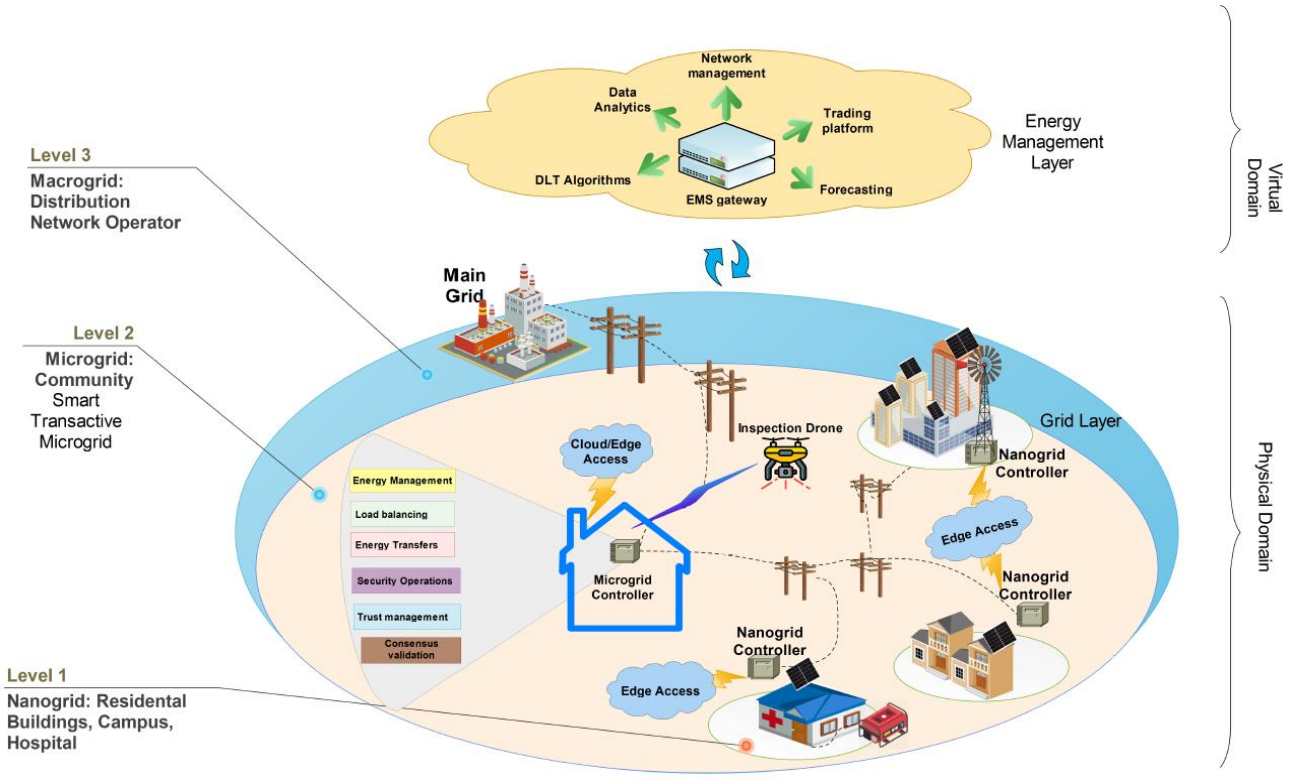

Figure 1: Peer-to-peer energy market facilitated by IoT in a smart transactive microgrid

(EMS) use this data to balance energy supply and demand. An example of an IoT-enabled Peer-to-peer energy market is presented below.

As is depicted in Fig 1. IoT devices are one of the key enablers in the automation of energy trades in the peer-to-peer energy market of a smart transactive microgrid. The use of IoT helps reduce human intervention and improving efficiency [2, 7]. Key IoT devices in peer-to-peer energy markets include microgrid controllers, energy generation systems, automated inspection platforms and connected smart appliances. These devices work together to manage energy flows, optimise energy usage, and ensure grid stability. Connected sensors across the grid help detect anomalies and maintain operational efficiency [2]. The flow of information and transactions in peer-to-peer energy markets is facilitated by IoT devices though cloud and edge communications. Microgrid controllers measure energy data, which is used by the EMS hosted by the Microgrid Controller, for real-time decision making. The EMS triggers smart contracts on the blockchain in the virtual layer to execute energy trades and record them on the blockchain for transparency. Afterwards, IoT devices manage energy distribution, ensuring grid balance and efficiency [2].

Utilising IoT devices in the transactive energy market poses a variety of challenges, particularly in performance and security. According to [8], challenges include, but are not limited to:

- Resource constraints: Limits the ability of devices to run complex cryptographic algorithms required by blockchain networks.
- Scalability: IoT networks may be strained as market participants increase, resulting in latency during transaction execution and data transmission.
- Security and availability: IoT devices are vulnerable to cyberattacks [2] and physical tampering, which could undermine the system's integrity and availability.

Microgrid controllers perform several mission critical operations in smart transactive microgrids and their energy market that must remain consistently available to guarantee the seamless functioning of peer-to-peer energy trading. Key operations include real-time energy monitoring, load balancing to ensure equitable distribution of energy, and grid management to maintain an equilibrium of supply and demand. These controllers also support automated energy trading and market clearing through smart contracts. Micro-controller nodes might participate in blockchain consensus for validating and adding transactions to blocks. Furthermore, each of the controllers have security operations running on them, ensuring data and transaction integrity in the market [2]. Therefore, it is essential for trust management operations in these markets to be lightweight and scalable to not compromise the availability of the essential operations of the underlying IoT infrastructure [8].

A. Trust and Cooperation in Peer-to-Peer Energy Markets

Despite the benefits of peer-to-peer energy markets, one of the key challenges in peer-to-peer energy markets is trust. Trust refers to the belief or confidence that participants will act according to expected behaviours, rules, and agreements [8] within the market. Trust ensures that participants can rely

on others to fulfil their obligations, such as providing energy and making payments without the oversight of a central authority, mitigating the risk of exploitation [4]. Trust is a prerequisite for effective cooperation as it would be difficult to ensure cooperation amongst participants among participants who do not trust each other [6]. In the absence of a central authority, cooperation is essential since the success of the energy market relies on participants fulfilling their roles in the market [6, 9]. However, for cooperation to exist, trust should already be established ensuring that market participants are comfortable with trading with strangers in the market [8, 9]. For trust to be established, there need to be certain requirements relating to trust that need to be addressed [6]. In previous work [10], the following key requirements were identified for building and ensuring trust in the peer-to-peer energy market:

- Security: Data must be protected, and financial transactions secured.
- Privacy: Participants' personal and transactional data need to be confidential to ensure compliance with data protection regulations.
- Transparency: Real-time data and pricing structures are transparent.
- Fairness: Equal market access and regulations to prevent unfair practices are crucial.
- Consensus: Peers in the market should agree that a transaction is legitimate and meets market rules before it is recorded on the blockchain.
- Accountability: Ensuring that peers conduct transactions in a reliable and trustworthy manner by meeting their contractual obligations
- Reputation: Participant ratings and reviews to help maintain the reliability of peers in the market.

While all the identified trust requirements are vital for the smooth operation of peer-to-peer energy markets, the long-term sustainability of trust and therefore cooperation, relies on effective trust management [11]. In decentralised environments, where traditional oversight is absent, trust is not simply assumed; it must be actively monitored and maintained. This is where trust management systems play a crucial role, ensuring that participants are held accountable for their actions and that trust is built and reinforced over time.

B. *Key IoT performance metrics in the peer-to-peer energy market*

In peer-to-peer energy markets, real-time data exchange, system reliability, and transactional trust are critical for efficient operation. IoT devices play a significant role in facilitating decentralised communication amongst market participants, forming the technological backbone of energy trading platforms. Trust management models must not adversely affect the essential operations of the underlying IoT devices in the peer-to-peer energy markets so to maintain continuous availability. It is therefore essential to evaluate key performance metrics of the models within an IoT context to ensure that they do not introduce computing overhead nor do they compromise the security and availability of the energy market and other operations while facilitating informed trading decisions.

When evaluating trust management models for the peer-to-peer energy market the following performance metrics were identified as critical when assessing trust models in IoT-based peer-to-peer energy markets [12, 13]:

- Latency: Time taken to process transactions and communication, including trust evaluation and blockchain validation and confirmation time.
- Resource consumption: Relates to energy efficiency and refers to the computational resources or memory used during operations.
- Security: Ensures trust and that sensitive data is protected while ensuring the system is reliable in the face of adversarial attacks.
- Scalability: Refers to the ability of the system to accommodate more devices without degrading performance. system growth without performance.
- Availability: Measures the system's capability to provide continuous access despite attacks or malicious behaviour.

Evaluating how trust models influence the performance of IoT infrastructure in respect to these metrics is vital to ensure that the IoT infrastructure can support dynamic, real-time energy trading while maintaining reliability, transparency, and user confidence [6,12, 13].

III. Trust Models in Decentralised and Peer-to-Peer Energy Markets

Trust management systems establish, maintain, and evaluate trust between nodes by collecting and analysing trust values and reputations [8]. Trust management systems help participants identify reliable trading partners in peer-to-peer energy markets where there is no central authority. This section explores trust models to identify how cooperative trust and obligation fulfilment are addressed. Six trust models were chosen from a Google Scholar search based on the following keywords:

{Trust model, P2P, Energy market, Energy trading, IoT, performance}

The study employed the protocol by Kitchenham *et al.,* [14] for systematic literature reviews in software. The protocol outlines a method for manual searches using a carefully constructed search string and selecting candidate studies based on predefined inclusion and exclusion criteria. The models were selected based on their relevance to enforcing trust in decentralised and peer-to-peer energy markets, especially those enabled by IoT devices such as smart meters and microgrid controllers.

A key elimination criterion was the evaluation of performance, either through evaluating trust score computation or the impact the model had on the performance of the underlying IoT network. This was a critical criterion that ensured that the selected models were not only theoretically sound, but also practically viable for the market. As a result, only models that evaluated the effectiveness or impact of trust establishment in the decentralised markets were included.

The final set of models was analysed based how they promoted cooperative behaviour, the trust mechanisms they used, how they ensured participants fulfilled their trade obligations, and the penalties imposed for not cooperating.

A. MicroTrust: Lightweight Trust Management for IoT Micro-grids

Ali *et al.,* [15] proposed MicroTrust, a behaviour-scoring trust management framework developed for peer-to-peer energy sharing systems, particularly suited for resource-constrained environments where blockchain was considered too demanding. It replaced decentralised mechanisms with a centralised Control Centre (CC) that computed trust scores using six behaviour-derived parameters: experience, reputation, honesty, availability, compatibility, and competence. Cooperation was established through continuous monitoring and adaptive trust thresholds, allowing only high-trust nodes to engage in energy trading. Obligation fulfilment was supported by a vulnerability detection algorithm that identified dishonest behaviour before it could impact system stability. Although the authors did not assess the model's impact on IoT performance, its lightweight design and lack of blockchain integration implied high suitability for constrained IoT environments. Nonetheless, it minimally addressed privacy and lacked cryptographic accountability or distributed consensus.

B. RETINA: Distributed and Secure Trust Management Using Hyperledger Fabric

Bolgouras *et al.,* [16] proposed RETINA (Reputation Enabled Trust Infrastructure for Networked Applications). RETINA was developed to overcome the limitations of centralised trust systems by integrating Public Key Infrastructure (PKI), Web of Trust (WoT), and Hyperledger Fabric, a permissioned blockchain. It established cooperation among energy nodes through mutual certificate endorsements, which were immutably recorded on the blockchain, enabling decentralised reputation-building. Obligation fulfilment was enforced using smart contracts that automated transactions based on trust level, energy type, and geographic proximity. RETINA maintained two separate ledgers—one for trust and one for transactions—enhancing modularity and transparency. Peer validation ensured accountability, while encrypted identities contributed to privacy protection. Although the authors did not evaluate the model's impact on IoT performance, its reliance on blockchain, smart contracts, and encryption suggested higher resource consumption and less suitability for highly constrained IoT environments compared to lighter models like MicroTrust.

C. Decentralized Transaction System (DTS): Ethereum-Based Secure Energy Trading

The Decentralized Transaction System (DTS) proposed in the work by Khan *et al.,* [17] presented a fully decentralised framework built on the Ethereum blockchain to facilitate peer-to-peer energy trading. Cooperation was established through trust evaluations from direct ratings from participants and their historical interactions, this allowed for trustworthy participants to participate in blockchain consensus and energy trading. The system used smart contracts for critical functions such as user registration, bidding, pricing, and auction settlement. Obligation fulfilment was enforced through a token-based commitment scheme, where users staked tokens that were forfeited upon contract breach, ensuring transactional integrity. Furthermore, an access control system was proposed to ensure that only authorised smart meters were interacting in the market thus enhancing the system's security posture. DTS comprehensively addressed trust requirements—including security, privacy, consensus, and accountability—through decentralised and cryptographically secure mechanisms. The model was simulated in a blockchain test network allowing for the evaluation of transaction times and scalability performance metrics, which serve as an indicator of the performance of the model. However, its reliance on blockchain, access control policies, ratings from participants and computationally intensive smart contracts might make it less suitable for resource-constrained IoT devices without additional support from capable edge infrastructure.

D. Cross-Layer Trust-Based Consensus Protocol for P2P Energy Trading

The Cross-Layer Trust-Based Consensus Protocol proposed by Chowdhury *et al.,* [18] introduced a trust mechanism for peer-to-peer energy trading by integrating human experience and system behaviour across blockchain's meta, application, and consensus layers. Cooperation was fostered through a fuzzy logic-based trust evaluation, where trust scores were derived from behavioural metrics such as transaction volume, feedback, and uptime. These scores influenced validator selection and determined participation eligibility. Obligation fulfilment was enforced through a hybrid Proof-of-Stake and Proof-of-Burn mechanism using a digital token called the trust coin. Misbehaviour led to score reduction and exclusion from validator roles, ensuring compliance and accountability. The use of blockchain infrastructure implicitly addressed trust requirements such as consensus, cooperation, transparency, and security. Although the system was not built for constrained IoT devices, it demonstrated improved CPU and memory performance over traditional consensus mechanisms in simulations. It was optimised for deployment in infrastructure rich environments with smart gateways and edge computing support, rather than minimal IoT nodes.

E. MarketTrust: blockchain-based trust evaluation model for IoT-based smart marketplaces

The MarketTrust model [19], developed for Social Internet of Things (SIoT)-based smart marketplaces, aimed to manage trust in environments characterised by frequent, human-centric interactions. It established cooperation through a multi-dimensional trust evaluation framework that assessed familiarity which was based on availability and success rates, personal interactions, and public perception from community feedback. Smart contracts were used to update trust scores dynamically, and these scores were made publicly accessible to ensure transparency. Although it did not use staking, a mechanism in Proof-of-Stake where validators are required to lock a certain amount of cryptocurrency as collateral to participate in block validation [16], for obligation enforcement, the model relied on reputation dynamics and the visibility of trust scores to encourage participants to fulfil their trade obligations and thus be candidates for future trades. Implemented on a semi-private Ethereum blockchain using Proof-of-Authority (PoA) consensus, the model emphasised lightweight operation and social adaptability. Privacy was supported through anonymised Ethereum identities, while blockchain immutability ensured transactional integrity. Performance evaluations showed that MarketTrust achieved low latency and high trust accuracy, making it suitable for smartphone deployment, embedded devices, and smart home gateways, with minimal impact on IoT performance.

Table 1: Comparison of trust models' cooperative trust establishment mechanisms

Research Question Concepts	MicroTrust [15]	RETINA [16]	DTS [17]	Cross-Layer Protocol [18]	MarketTrust [19]	TRaaS [20]
Cooperation Establishment	Central control; Trust score filtering	PKI; WoT; Certificate endorsements	Reputation model; User Ratings Token staking; Dynamic pricing	Fuzzy logic; Human feedback	Public perception; Historical interaction	Smart contracts; Probability model (Laplace's Law)
Trust Mechanisms	Direct/indirect observation; Qualitative metrics	Blockchain; PKI; WoT; Remote attestation	Blockchain; Commitment tokens; Key pairs	Blockchain; Fuzzy logic; Trust coins; Trust scores	Blockchain; Public opinion; Interaction history	Blockchain; Laplace's Law; Objective feedback; Reputation scores
Obligation Fulfilment	Trust threshold; Behavioural monitoring	Smart contracts; Trust-based triggers	Smart contracts; Token forfeiture; Trust scores	Smart contracts; Dynamic score updates	Smart contracts; Reputation visibility	Smart contracts; Segment-specific reputation tracking
Cooperative Penalties	Temporary bans (7–14 days);	Certificate revocation; Network removal	Token loss; Reputation drops; Blacklisting	Trust score reduction; Validator exclusion	Trust score decay; Marketplace exclusion	Reputation reduction; Transaction trust impact

F. Towards Trust and Reputation as a Service in a Blockchain-based Decentralized Marketplace (TraaS)

Olariu *et al.,* [20] proposed Trust and Reputation as a Service in a Blockchain-based Decentralized Marketplace. Their model (TRaaS) was a probabilistic, blockchain-based trust framework aimed at reducing uncertainty in decentralised peer-to-peer markets. The model established cooperation through objective, context-specific trust scores calculated by smart contracts based on transaction outcomes, replacing subjective buyer feedback. Obligation fulfilment was enforced via smart contracts that verified whether parties met contractual terms, enabling fair and consistent trust scoring. The model used Laplace's Law and Bayesian updates for dynamic trust computation, with discounting mechanisms to prioritise recent behaviour. Though not explicitly evaluated for IoT performance, the model's lightweight, arithmetic-based computations and reliance on smart contracts suggest it would be suitable for resource-constrained IoT environments.

These six trust models show trust is critical in decentralised and peer-to-peer energy markets and how it is established using various trust mechanisms. Furthermore, penalties are enforced in some works to ensure obligation fulfilment, thus ensuring the cooperation of participants in the market even without prior relationships.

IV. Comparing Trust Models In Decentralised And Peer-To-Peer Energy Markets

A comparative analysis was done on the six models discussed in Section III based on the research questions 1 and 2 introduced earlier in this work. The research questions aim to understand cooperation establishment, trust mechanisms, obligation fulfilment, and cooperative penalties. These concepts are used to compare the trust models in Section IV-A. In Section IV-B, the models are then ranked according to their coverage of trust requirements discussed in Section II-B. obligation fulfilment, and cooperative penalties. These concepts are used to compare the trust models in Section IV-A. In Section IV-B, the models are then ranked according to their coverage of trust requirements discussed in Section II-B.

A. Comparison based on cooperation establishment and obligation fulfilment

In peer-to-peer energy trading systems, cooperation among participants is essential and is inherently linked to the trust mechanisms embedded within each model. Table I identifies how cooperative trust is fostered in the peer-to-peer energy market by identifying the mechanisms and methods used for cooperation establishment, establishing trust, enforcing obligation fulfilment and penalising non-cooperative behaviour.

Based on Table I, the selected trust models assumed that cooperation emerges when participants can rely on one another to fulfil obligations, which requires a baseline of trust. This trust is typically derived from historical behaviour, computed reputations, or system-level assurances such as cryptographic mechanisms and blockchain technology or automated enforcement via smart contracts.

The six trust models under comparison differ in how they establish cooperation. A key distinction lies in whether the model adopts a centralised or decentralised approach. MicroTrust is the only model that uses a centralised trust evaluation mechanism. It bases cooperation on qualitative observations and trust scores managed by a central authority. While this approach enables fast trust assessment, it introduces limitations that could adversely affect the security and hence availability of the system. In contrast, the remaining five models employ decentralised mechanisms—relying on blockchain technology to provide immutable transaction histories and support distributed trust evaluation.

The decentralised trust models vary further based on how they foster trust. RETINA and DTS emphasise cryptographic trust, incorporating mechanisms such as Public Key Infrastructure (PKI), remote attestation, and blockchain to ensure security and identity validation. These methods enhance the robustness of cooperation by providing system-

Table I2: Comparison of how trust models address trust requirements

Trust Requirements	*MicroTrust [15]*	*RETINA [16]*	*DTS [17]*	*Cross-Layer Protocol [18]*	*MarketTrust [19]*	*TRaaS [20]*
Security	Behavioural scoring; Centralised control	PKI; Remote attestation	Ethereum smart contracts; access control system	Trust coins; Hybrid Proof of Stake & Proof of Burn	Blockchain; Proof-of-Authority	Smart contracts; Reputation verification
Privacy	Not given	Permissioned blockchain	Access control; Cryptography	Not given	Not given	Not given
Transparency	Not given	Dual blockchain ledgers	Public smart contract transactions; Blockchain	Public trust scores; Blockchain	Public trust scores; Blockchain	Blockchain-based reputation tracking
Fairness	Not given	Dynamic pricing mechanism	Uniform pricing; Token commitment	Fuzzy logic; stake/burn validator selection	Not given	Objective feedback; Segment-specific reputation; Discounting schemes
Consensus	Not given	Proof-of-Authority	Prosumer-centric consensus: trust score & energy-based validator selection	Proof-of-Stake; Proof-of-Burn	Proof-of-Authority	Blockchain-backed trust records. No specific consensus mechanism
Accountability	Not given	Remote attestation; Certificate revocation; Blockchain	Token forfeiture; Access control; Blockchain	Trust score-based validator exclusion; Blockchain	Public trust metrics; Network exclusion; Blockchain	Segment-based scoring; Transaction history; Blockchain
Reputation	Experience; honesty & competence	Web of Trust; Shared ledgers	Token-based scores;	Human ratings; Historical scores; Fuzzy logic	Public opinion; Interaction history	Laplace's Law; Segment-specific scoring

level guarantees and verifiable proof of behaviour, while DTS also incorporates social trust through participant ratings and tracking historical behaviour. MarketTrust and TRaaS place greater emphasis on social trust. They use reputation systems informed by public opinion, familiarity, and probabilistic assessments to gauge trustworthiness. The Cross-Layer Protocol represents a hybrid approach that combines blockchain with human feedback and fuzzy logic to compute trust scores, offering a nuanced model that blends social and technical trust formation.

Smart contracts play a pivotal role in most decentralised models. By automating the execution of terms agreed upon by trading parties, smart contracts facilitate cooperation and enforce accountability. Their presence ensures that once cooperation is established, the rules governing transactions are executed without the need for manual intervention, reducing the likelihood of disputes and enhancing transparency.

Obligation fulfilment, the assurance that parties will honour agreed-upon transactions, is addressed differently across the models. Reputation systems are a common feature, with trust scores adjusting based on participant behaviour. In MicroTrust, obligation fulfilment is monitored by tracking trust scores and enforcing temporary bans for misconduct. DTS and RETINA implement stricter enforcement by leveraging smart contracts, commitment tokens, and cryptographic verification. Penalties in these systems include forfeiture of tokens, certificate revocation, and blacklisting for repeated breaches. The Cross-Layer Protocol integrates a multi-layered enforcement mechanism by reducing trust scores and excluding validator nodes from the consensus process in response to misbehaviour. MarketTrust also enforces trust through social feedback, applying penalties such as reduced trust scores and temporary exclusion from the marketplace. While TRaaS lacks explicitly defined penalties, its probabilistic trust model inherently discourages misconduct by lowering the reputation of unreliable participants, thereby reducing their ability to engage in future transactions.

Across the models, a pattern emerges; the trust models aim to facilitate cooperation and ensure that obligations are fulfilled using different strategies. Centralised approaches favour simplicity while decentralised models offer stronger trust assurances through technical and social mechanisms. All the models enforce similar penalties for non-cooperative behaviour. Participants who have low trust or reputation scores because they do not follow market rules nor conduct themselves honestly during transactions are excluded from participating in the market.

B. Comparison based on trust requirement coverage

This section discusses how the trust models address trust requirements as summarised in Table II. The models are further ranked based on their trust requirement coverage.

Error! Reference source not found. compares how six t rust models address eight key trust requirements in peer-to-peer energy markets. The analysis shows a clear trend toward comprehensive trust enforcement through blockchain and smart contracts, with varying degrees of decentralisation.

Among the evaluated models, RETINA and DTS rank first, each addressing the eight trust requirements. Both models leveraged blockchain technologies and integrated cryptographic mechanisms and access control policies, bolstering the security and reliability of the system. RETINA, for example, used a permissioned blockchain and public key infrastructure, while DTS leveraged Ethereum smart contracts and access control policies. These models balance trust assurance with robust security and privacy features, although they might involve higher computational overhead.

The TraaS model ranks closely behind, addressing nearly all trust requirements. Blockchain's inherent properties were

used in this model for security, consensus and accountability. Smart contracts were used for objective feedback, trust assessment, segment-specific reputation and discounting schemes to support fairness.

The TraaS model rank closely behind, addressing nearly all trust requirements. Blockchain's inherent properties were used in this model for security, consensus and accountability. Smart contracts were used for objective feedback, trust assessment, segment-specific reputation and discounting schemes to support fairness. However, it lacked explicit privacy-preserving mechanisms. Similarly, the Cross-Layer Protocol effectively supports security consensus, accountability and fairness using blockchain and selection of validators based on trust scores derived from participant behaviour in the market, respectively, but it does not address privacy. Both models are adaptable and socially aware, making them suitable for dynamic environments like the peer-to-peer energy market.

MarketTrust ranks in the middle, addressing key requirements such as security, accountability, and reputation through blockchain-based mechanisms and public trust metrics. It uses Proof-of-Authority for consensus and integrates objective feedback systems. However, it lacks explicit privacy and fairness provisions, which limits its comprehensiveness relative to the top-tier models, RETINA and DTS.

MicroTrust is the least comprehensive model addressing only three of the eight trust requirements. It uses a behavioural scoring approach with centralised control, promoting cooperation of participants, but lacking the relevant mechanisms to enhance security and address the other key trust requirements for peer-to-peer energy markets it does not address. While it may be lightweight and efficient, its limited trust requirement coverage makes it less robust in trust-sensitive decentralised energy markets.

The comparison highlights a general movement toward using blockchain and smart contracts as foundational tools for trust enforcement in decentralised energy systems. Models that integrate cryptographic and decentralised mechanisms tend to offer more comprehensive trust coverage. Lightweight models like MicroTrust may be more efficient in terms of computational overhead since it does not implement complex security mechanisms, but it falls short in addressing the full spectrum of trust requirements.

V. Comparing IoT Performance in Trust Models

A comparative analysis was done on the six models discussed in Section III based on the research question 3 introduced in the Introduction of the paper. The research questions aimed to understand cooperation establishment, trust mechanisms, obligation fulfilment, and cooperative penalties.

In this section, the selected trust models are compared and ranked again based on their predicted IoT performance since some models were not evaluated in an IoT context. Since the models were not implemented and validated as part of this work, their evaluation was based on a synthesis of the original performance metrics reported in the source studies. For the trust management models that were not explicitly evaluated based on how they influence IoT performance based on their algorithmic and technical mechanisms, such as blockchain and its consensus mechanisms, cryptographic mechanisms and trust computation logic. The models are further ranked later in the section, this ranking is guided by the performance rankings outlined in Section II, including latency, resource usage, scalability, availability and security, allowing for a consistent literature-based estimation of each of the model's suitability for the IoT-based peer-to-peer energy markets.

A. Performance of Trust Models

MicroTrust prioritised fast and accurate trust evaluation using criteria like reputation, competence, and honesty. It achieved convergence within ~55s (55000ms) for honest nodes and ~69s (69000 ms) for dishonest ones, with an accuracy of over 90%. This indicates shorter times for identifying honest behaviour and longer convergence times for dishonest behaviour as more interaction history would be required, resulting in instabilities for trust score calculations. The model's lightweight design, that does not rely on blockchain, ensures low resource consumption, and may contribute to moderate latency. However, the presence of malicious nodes can influence the responsiveness and stability of trust evaluation during the period of convergence. Moreover, the reliance on a central control centre and lack of cryptographic mechanisms expose it to single points of failure and limited scalability.

Conversely, RETINA was tested in a smart grid testbed with 500 smart meters, integrated PKI, WoT, and blockchain to establish trust securely. It demonstrated a low computation time (19.2 ms) and communication overhead (192 bits) which encompassed trust and market operations, reflecting low latency and resource demands. Despite strong resilience and scalability, its use of PKI, remote attestation and blockchain could increase resource demands, reducing suitability for constrained IoT devices.

In contrast to MicroTrust and RETINA, DTS was deployed on the Ethereum Goerli testnet, used smart contracts and simplified access control for secure energy trading. It showed moderate latency (~1000 ms for 20 users) and linear scalability. While the model showed improved efficiency and privacy using cryptographic methods, Ethereum's transaction throughput limit of 14 transactions per second (TPS) and smart contract overhead could have posed scalability and latency challenges for IoT deployment. Furthermore, the direct user ratings required for trust score calculation could introduce longer transaction times as the system would have to wait for feedback from users. Additionally, the evaluation of latency in this work did not consider the time taken to compute and evaluate trust in the smart contracts.

The Cross-Layer Protocol, evaluated with SimBlock across 250–8000 nodes, achieved up to 45% lower latency and reduced memory usage compared to PoW and PoS. Its hybrid PoS–PoB design offers high scalability but does not evaluate the influence of trust evaluation on the performance of IoT and its consensus mechanisms could be more compute intensive than PoA since more nodes could be required to participate in the consensus, resulting in longer transaction times. This limits its applicability for resource-constrained IoT devices. Similarly to DTS, trust computation was not considered when evaluating latency.

MarketTrust, designed for Social IoT marketplaces, employed PoA and social feedback mechanisms. It achieved 48% lower latency and 21.99% improved trust accuracy over benchmarks, with minimal resource use—ideal for constrained IoT environments. However, it did evaluate how trust computation could influence the overall performance.

Lastly, TRaaS utilised smart contracts and Laplace's Law for probabilistic trust scoring. While it was not experimentally tested for IoT related performance, the model's efficiency in evaluating trust was assessed through blockchain and smart

contract simulations, showing its efficiency in measuring the reliability of participants. Furthermore, its arithmetic-based approach suggests low computational overhead and good Sybil attack resistance, as shown by the convergence of the predicted trust scores over 50 to 150 iterations of the experiment. Its seemingly lightweight, and efficient design makes it a promising candidate for constrained environments.

B. Comparison based on IoT performance metrics

Error! Reference source not found. compares the six t rust models from Section III based on performance metrics relevant to IoT such as latency, resource use, availability, scalability and security, and whether the models considered the time taken for trust evaluation when assessing latency or computation time. The models that were evaluated are evaluated based on the results of their prior evaluations, while those were not evaluated were evaluated based on their projected performance considering the mechanisms they implemented to establish cooperative trust and trust

Table III: Comparison of trust models in peer-to-peer energy market based on performance metrics

	Latency	Resource Use	Availability	Scalability	Security	Trust evaluation latency
MicroTrust [15]	Low	Low	Low	Low	Low	Evaluated
RETINA [16]	Low	High	High	High	High	Evaluated
DTS [17]	Moderate	High	High	Moderate	High	Not Evaluated
Cross Layer Protocol [18]	Low	High	High	High	High	Not Evaluated
MarketTrust [19]	Low	Moderate	High	High	High	Not Evaluated
TraaS [20]	Moderate	Moderate	High	High	High	Not Evaluated

requirement coverage.

The results from **Error! Reference source not found.** s how that Cross-Layer Protocol, and MarketTrust are the most IoT optimised models, excelling across the IoT performance metrics. MarketTrust ranks first overall, offering a strong balance between moderate computational demand and trust requirement support by leveraging PoA consensus and social trust metrics. Cross-Layer Protocol runs second, providing high scalability (up to 8000 nodes) and low latency, but at the cost of increasing resource use due to its hybrid consensus mechanisms.

MicroTrust ranks third, characterised by low latency and minimal resource consumption, however, its centralised trust evaluation introduces scalability and availability limitations.

Its lack of cryptographic and security mechanisms reduces its security robustness.

In contrast to MicroTrust, RETINA delivers strong security and availability. However, RETINA incurs high resource demands due to its reliance on PKI, remote attestation, and blockchain technologies.

TRaaS and DTS are the least IoT optimised models based on their projected performance. TRaaS ranks fifth due to its moderate resource use and latency, while DTS ranks sixth due to its reliance on cryptographic mechanisms and blockchain, possibly making it less suitable for constrained IoT environments.

Lastly, only MicroTrust and RETINA considered the cost of trust evaluation in relation to system latency.

C. Trade-offs between trust coverage and IoT performance

A distinct trade-off emerges when comparing trust requirement coverage with IoT performance. Models such as DTS and RETINA offer comprehensive trust coverage, incorporating strong cryptographic security, blockchain-based integrity, and decentralised access control. However, these capabilities come at the cost of increased computational demands, limiting the viability of their deployment in constrained environments.

Conversely, models like MicroTrust and MarketTrust prioritise IoT performance by minimising computational overhead and achieving low latency and computational overhead. MicroTrust achieved fast trust evaluation within 55-59 seconds with low resource consumption by avoiding complex cryptographic operations. However, it sacrifices decentralisation, scalability, and robust security, making it vulnerable to single points of failure and thus less viable for decentralised peer-to-peer energy markets.

MarketTrust, relying on PoA consensus and social feedback rather than heavy cryptography, delivers improved trust accuracy and computational delay, making it highly suitable for constrained IoT environments. Nevertheless, MarketTrust does not fully enforce all trust dimensions and lacks formal evaluation of trust computation time. achieves a balanced but not complete enforcement of all trust dimensions.

Cross-Layer Protocol represents a hybrid case; offering broad trust coverage and exceptional scalability with lower latency than traditional consensus mechanisms like PoW. However, its hybrid consensus mechanism could incur high resource consumption, making it less suitable for resource constrained environments. This positions Cross-Layer Protocol as a model with strong trust support and scalability, but one that may require optimisation to reduce energy and computational demands for constrained IoT devices. Furthermore, it does not explicitly evaluate how long it takes to evaluate trust.

Similarly, TRaaS addresses multiple trust dimensions through smart contract-driven trust updates and probabilistic scoring, offering moderate IoT performance. However, it lacks explicit privacy-preserving mechanisms and does not evaluate the time taken to predict the trustworthiness of participants. This model could be further improved to better align trust coverage with the demands of secure and efficient IoT deployments.

Considering the need for effective trust establishment that does not compromise the performance of the entire IoT infrastructure, RETINA would be the most appropriate model for trust establishment in the peer-to-peer energy market, as it has full trust requirement coverage, and good system performance based on the identified performance metrics.

From **Error! Reference source not found.** it is evident t hat achieving comprehensive trust enforcement typically incurs higher resource costs, while performance-optimised models like Micro-Trust may compromise on decentralisation, privacy, or trust robustness.

D. Gap Analysis

This evaluation highlights several critical gaps. Although models like MarketTrust and Cross-Layer protocol show improvement in latency compared to other models and consensus algorithms respectively, there is no unified benchmark for evaluating trust management models in the peer-to-peer energy market. This makes comparative analysis between these models challenging.

Additionally, some of the trust management models discussed do not consider the time taken to evaluate trust in its performance assessments [17 – 20]. Models such as DTS and Cross-Layer Protocol were tested in blockchain simulation environments, with measurements on time elapsed and CPU usage, which are valuable performance indicators related to blockchain consensus and transaction processing that influence latency. However, blockchain environments and simulations do not fully replicate the constraints of real IoT networks. Although the blockchain metrics give an idea of IoT feasibility, they may not account for IoT related bottlenecks, necessitating for additional experimental validation on IoT environments.

Furthermore, TraaS was only evaluated based on how accurately trust scores were predicted across several market segments, and not necessarily performance of the underlying IoT infrastructure, highlighting the need for further experimentation in an IoT environment to determine whether it would be a good fit for constrained IoT environments. Given its extensive trust feature coverage but lower IoT efficiency, DTS is a strong candidate for optimisation for better IoT performance. It is a prime candidate for optimisation to reduce computational overhead of its cryptographic security mechanisms and blockchain operations, possibly through more efficient alternatives.

Cross-layer protocol though it is highly efficient, it would benefit from improvements such as encryption mechanisms to ensure privacy in the market, therefore addressing all the trust requirements for peer-to-peer energy markets.

Lastly, TRaaS demonstrates a possibly lightweight and less complex design with promising Sybil attack resistance but lacks empirical performance evaluation. Moreover, TraaS seems to be less efficient than the Cross-Layer Protocol in terms of IoT performance; as such, it would be the best candidate for improvements that strengthen its privacy. Furthermore, the performance of TraaS was not validated in a constrained IoT environment like that of the peer-to-peer energy market in the smart transactive microgrid, therefore this model is the best candidate for improvements based on full trust requirement coverage, and validation in a IoT environment.

The gap emphasises the need for more unified performance metrics for trust management, the necessity to evaluate the time taken to evaluate trust to account for latency in the IoT network of the market [17 – 20] and to validate the practical efficiency of the trust models [18 – 20] under resource-constrained IoT devices for the peer-to-peer energy market, fostering trust using lightweight trust models. Models like TRaaS and DTS are particularly strong candidates for optimisation to achieve lightweight trust models.

VI. Conclusion And Future Work

This study evaluated six trust models based on how they enforce cooperative trust in decentralised peer-to-peer energy markets their effectiveness in trust establishment and impact on IoT performance. Performance was used as exclusion criterion to ensure that only studies that implemented trust mechanisms that did not introduce computation overhead were excluded. By prioritising trust effectiveness and performance, the study ensured that the models that were selected aligned with the constraints of the resource-constrained IoT infrastructure of the peer-to-peer energy market. This approach narrowed down the number of the number of studies to those that would be most likely to ensure effective trust and optimal performance, allowing future work to focus on enhancing models that already demonstrate efficient and scalable trust management in peer-to-peer energy markets.

Based on the selected models, cooperation was enforced using various mechanisms including trust and reputation scores, smart contracts, human feedback, ratings and perceptions. Blockchain technology was the primary mechanism used to establish trust and facilitate cooperation, with its smart contracts widely used to ensure that participants fulfil their obligations.

Majority of the works used trust scores and reputation to encourage participants to fulfil their obligation. A high score represented reliable trading partners, and hence better trading opportunities and roles in the market. Lower scores were associated with unreliable behaviour which was punished through penalties.

Penalties were enforced for non-cooperation across all models, and this ranged from temporary exclusion from the market to trust score decay.

From the comparative analysis of the coverage of trust requirements and projected IoT performance, it was evident that there are trade-offs regarding trust enforcement and IoT performance, such as in RETINA and DTS. MarketTrust and Cross Layer Protocol demonstrated strong IoT efficiency due to their less complex security and trust mechanisms.

In contrast, DTS and RETINA, with their complex mechanisms, were the only models that met all trust requirements, but DTS had the lowest projected IoT suitability. However, RETINA was a more likely candidate for trust establishment due to its full trust requirement coverage and good IoT performance with low latency, moderate resource usage, and high security, scalability and availability.

Furthermore, the analysis revealed that there are no unified metrics to evaluate trust management frameworks in terms of their efficiency and performance.

Additionally, some of the models [17] – [19] were not tested in IoT environments like that of the smart transactive microgrid, presenting a gap in optimal IoT performance of trust models of decentralised and peer-to-peer energy markets, suggesting the need for further optimisation and more rigorous validation methods for deployment ready trust management models. Furthermore, majority of the models [16] – [19] did not consider the time elapsed to calculate and evaluate trust in their respective environments, thus not accurately indicating the latency of their implementation. This could result in the development of trust management models that take too long to evaluate trust and thus undermine the requirement of real-time transactions in the market. As such, future work should prioritise enhancing comprehensive models like DTS and TraaS, for constrained IoT environments. From the analysis, TraaS was the best candidate for enhancement given its limitations relating performance testing for constrained IoT environments. Moreover, an evaluation of trust models in the peer-to-peer energy market in IoT environments, that also accounts for the time taken for trust evaluation, is essential to ensure that the implementation of the trust model does not adversely affect the performance and reliability of the peer-to-peer energy market.

References

[1] Z. Zeng, M. Dong, W. Miao, M. Zhang, and H. Tang, “A data-driven approach for blockchain-based smart grid system,” IEEE Access, vol. 9, pp. 70 061–70 070, 2021.

[2] F. Condon, P. Franco, J. M. Mart´ınez, A. M. Eltamaly, Y.-C. Kim, and M. A. Ahmed, “Energyauction: Iot-blockchain architecture for

local peer-to-peer energy trading in a microgrid," Sustainability, vol. 15, no. 17, 2023.

[3] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, S. khan, and M. K. Khan, "Trust and reputation for internet of things: Fundamentals, taxonomy, and open research challenges," Journal of Network and Computer Applications, vol. 145, p. 102409, 2019.

[4] Q.-u.-A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, "Blockchain-based decentralized trust management in iot: systems, requirements and challenges," Complex & Intelligent Systems, vol. 9, no. 6, pp. 6155–6176, 2023.

[5] D. Mitrea, T. Cioara, and I. Anghel, "Privacy-preserving computation for peer-to-peer energy trading on a public blockchain," Sensors, vol. 23, no. 10, p. 4640, 2023.

[6] R.-V. Tkachuk, D. Ilie, R. Robert, V. Kebande, and K. Tutschku, "Towards efficient privacy and trust in decentralized blockchain-based peer-to-peer renewable energy marketplace," Sustainable Energy, Grids and Networks, vol. 35, p. 101146, 2023.

[7] M. S. Al-Rakhami and M. Al-Mashari, "A blockchain-based trust model for the internet of things supply chain management," Sensors, vol. 21, no. 5, 2021.

[8] O. Okporokpo, F. Olajide, N. Ajienka, and X. Ma, "Trust-based approaches towards enhancing iot security: A systematic literature review," arXiv preprint arXiv:2311.11705, 2023.

[9] C. Marche and M. Nitti, "Can we trust trust management systems?" IoT, vol. 3, no. 2, pp. 262–272, 2022.

[10] "Trust requirements and mechanisms in peer-to-peer energy markets," 2024, paper presented at the Information Security South Africa (ISSA) Conference, Boardwalk International Convention Centre, Gqeberha, South Africa, December 2–3, 2024.

[11] A. J. Mathew, "Can security be decentralised?"

[12] D. K. M. Moulla, E. Mnkandla, and A. Abran, "Systematic literature review of iot metrics," Applied Computer Science, vol. 19, no. 1, 2023

[13] K. Patel, C. Mistry, R. Gupta, S. Tanwar, and N. Kumar, "A systematic review on performance evaluation metric selection method for iot-based applications," Microprocessors and Microsystems, vol. 101, p. 104894, 2023.

[14] W. Ali, I. U. Din, A. Almogren, M. Zareei, and R. Roshan-Biswal, "Microtrust: Empowering microgrids with smart peer-to-peer energy sharing through trust management in iot," IEEE Access, 2024.

[15] Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J. & Linkman, S.: Systematic literature reviews in software engineering – A systematic literature review. In-formation and Software Technology 51, 17-15, 2009.

[16] V. Bolgouras, T. Ioannidis, I. Politis, A. Zarras, and C. Xenakis, "Retina: Distributed and secure trust management for smart grid applications and energy trading," Sustainable Energy, Grids and Networks, vol. 38, p. 101274, 2024.

[17] 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. 47 236–47 257, 2023.

[18] M. J. M. Chowdhury, M. Usman, M. S. Ferdous, N. Chowdhury, A. I. Harun, U. S. Jannat, and K. Biswas, "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. 14 779–14 789, 2021.

[19] R. Latif, B. M. Yakubu, and T. Saba, "Markettrust: blockchain-based trust evaluation model for siot-based smart marketplaces," Scientific Reports, vol. 13, no. 1, p. 11571, 2023.

[20] S. Olariu, R. Mukkamala, and M. Aljohani, "Towards trust and reputation as a service in a blockchain-based decentralized marketplace," arXiv preprint arXiv:2403.04779, 2024.