RETINA: Distributed and Secure Trust Management for Smart Grid Applications and Energy Trading

Vaios Bolgouras[a], Thodoris Ioannidis[c], Ilias Politis[b,c], Apostolis Zarras[a], Christos Xenakis[a]

[a] *Secure Systems Laboratory, University of Piraeus, Greece*
[b] *Industrial Systems Institute, Research Centre "ATHENA", Greece*
[c] *InQbit Innovations SRL, Romania*

Abstract

The rapid adoption of smart grids demands robust security and efficiency measures due to their critical role in delivering electricity and their potential for customer-oriented benefits. This article presents an innovative framework, named `RETINA`, which provides a resilient and secure energy trading mechanism within smart grid systems. `RETINA` tackles the inherent security and infrastructure challenges in smart grids by establishing a trust-based security layer and facilitating energy transactions through blockchain technology. Our proposed solution integrates *Public Key Infrastructure* (PKI) and the *Web of Trust* (WoT) concepts, promoting decentralized communication channels and robust key management. We further introduce a smart contract-based energy trading mechanism that factors trust, distance, and energy type (green or non-green) in the cost calculation. The utility and robustness of `RETINA` have been validated in a virtualized testbed environment with 500 nodes, demonstrating superior performance in terms of scalability and resilience compared to the existing WoT scheme. Furthermore, `RETINA` successfully enables a secure and efficient energy trading scheme, promoting the use of renewable energy sources and promptly recovering from market manipulation attacks. Future enhancements will include applying it to a realistic smart grid deployment and integrating additional functionalities. This groundbreaking solution can potentially revolutionize the smart grid ecosystem, addressing its current limitations and propelling the industry toward a future of advanced and secure energy exchange.

Keywords: Smart grids, Trust Management, Blockchain, Security, Energy Trading

1. Introduction

Smart grids, which intelligently integrate digital communication and control technologies into the traditional electricity delivery system, have emerged as a pivotal focus for enhancing electricity distribution efficiency and environmental sustainability. Recent advancements, such as client-oriented metering mobile apps and provider-oriented data aggregation software, have contributed to this trend [1]. These advancements offer environmental benefits and financial advantages to consumers, prosumers (those who both produce and consume electricity), and energy providers by reducing operational expenses—*Operational Expenditure* (OPEX) [2]. As critical national infrastructures [3], smart grids require continuous operation and integrity protection, making it crucial to implement state-of-the-art security measures.

Robust security measures are essential for smart grids due to their criticality. Establishing a strong security foundation for financial transactions and secure operation of smart applications supporting grid functionalities is mandatory [4]. As smart grids rely on distributed computing, such as smart meters, information exchange over power lines or wireless channels is susceptible to security threats. Security operators propose solutions utilizing advanced technologies to prevent and mitigate these threats. However, smart grids face technical infrastructure security and network architecture challenges that must be addressed to fully realize their potential and enable energy exchange among prosumers.

First, using certificate authorities—*Central Authorities* (CA)—and nodes in smart grid networks can create single points of failure [5], compromising system safety and functionality. If the CA fails, communication among smart grid nodes may be delayed or suspended, significantly impacting performance and reliability. Second, while decentralized solutions based on blockchain technology are gaining popularity for their potential to enhance security and transparency in smart grid systems, they can also be resource-intensive and contradict smart grid principles. The maintenance of such solutions can consume significant electricity [6]. Third, there are concerns about the operational cost of energy trading solutions built on the Ethereum network, which currently incurs high transaction fees. This inhibits providers' and customers' adoption of such solutions, reducing their financial benefits. Lastly, scalability is critical for widespread energy trading adoption among prosumers

in smart grids. Existing energy trading solutions primarily focus on small-scale electricity networks, such as microgrids [7]. Scaling up poses significant challenges due to increased complexity and resource requirements.

One widely adopted solution for establishing trust between grid components is the *Web of Trust* (WoT) [8]. In smart grids, WoT operates through cryptographic authentication and authorization. Each grid entity is assigned a digital identity, typically in the form of a digital certificate or *Public Key Infrastructure* (PKI) mechanism, to verify the authenticity and integrity of exchanged data. WoT employs digital signatures to ensure that only trusted entities participate in communication, protecting data during transit.

In addition to the security challenges posed by the distributed nature of smart grids, energy trading among grid participants has also sprouted along the smart grids. With the smart grid's ability to perform simple computational processes on smart meters, which are essentially IoT devices, the role of energy prosumers has evolved, facilitating the ability to trade energy between two parties over the grid [9]. Energy exchange infrastructures can emerge based on this concept, which is pivotal in enabling modern electric grids to reach their full potential. By aiming for eco-friendly solutions and financial benefits for users, energy trading adds value to consumers compared to legacy grids. Additionally, energy trading complements other solutions, such as pumped storage hydro-power infrastructures [10], that aim to minimize battery usage for storage purposes by instantly distributing and consuming electricity to areas in need. Reduced use of batteries and easy access to green sources of electricity helps decrease the environmental footprint. Moreover, consumers have a variety of available sources offering energy, allowing them to choose the most cost-effective one.

By embracing energy trading, the potential occurrence of blackouts resulting from catastrophic failures in power plants can be notably mitigated. Unlike traditional energy trading models, which may lack the agility and adaptability to promptly redistribute electricity in response to unforeseen disruptions, a blockchain-based energy trading platform, such as RETINA, enables a more resilient and responsive energy distribution system. The decentralized and peer-to-peer nature of RETINA allows for real-time adjustments, minimizing the impact of unexpected events on the power grid. This is in contrast to conventional centralized systems, where the rerouting of electricity in the event of a power plant failure might encounter delays or inefficiencies.

The motivation behind this article stems from the imperative need for

robust security measures in smart grids, acknowledging their criticality in supporting grid functionalities. The inherent challenges in smart grid security, such as the vulnerability associated with CAs creating potential single points of failure, resource-intensive decentralized solutions conflicting with smart grid principles, high operational costs in existing energy trading solutions, and scalability issues, underscore the demand for an innovative approach. `RETINA` addresses these challenges by combining the WoT for trust establishment, addressing its shortcomings through robust security protocols, effective key management, and collaboration among stakeholders. Additionally, `RETINA` recognizes the evolving role of energy prosumers in smart grids, facilitating energy trading among participants. The platform leverages the smart grid's computational capabilities, particularly in smart meters, to enable efficient, eco-friendly energy trading, adding significant value to consumers by reducing environmental impact and offering cost-effective energy choices. The proposition of `RETINA` emerges as a comprehensive solution to enhance security, scalability, and energy awareness in smart grids, aligning with the evolving landscape of energy exchange among prosumers.

This article introduces a framework that establishes the basis for a secure and resilient energy trading mechanism, enabling the secure and efficient operation of smart applications within smart grids. Energy exchange necessitates a robust underlying architecture that adheres to essential standards to facilitate the seamless and secure execution of associated actions. Without those standards, untrusted entities can appear, posing a risk of dishonest trading and potentially leading to market price manipulation and disruption of smart grid operations. In smart grid ecosystems, the concepts of supply and demand play crucial roles. Demand represents the requirement for additional electricity, while supply refers to the surplus electricity that can be provided to the grid. These two concepts are intertwined in a way that they complement each other, offering an opportunity to fulfill the needs of a smart grid without solely relying on the traditional provider. Blockchain technology facilitates this, leveraging a dedicated smart contract and functionalities that empower participants to place *"buy"* or *"sell"* orders. Blockchain enables transparent and secure energy transactions within the smart grid ecosystem.

`RETINA`'s peer-to-peer (P2P) blockchain-based energy trading system signifies a transformative shift in the energy market, contrasting with conventional supply models. While traditional approaches involve centralized contracts with energy providers, RETINA introduces a decentralized platform. Direct prosumer transactions streamline procurement, eliminating complex

agreements. This system adapts in real-time to supply and demand, optimizing energy distribution. Incentives for prosumers enhance collaboration, contributing to a more robust energy market and additional revenue streams. RETINA's elimination of intermediaries and use of Hyperledger Fabric ensures feeless and efficient transactions, reducing operational costs. Aligned with sustainability goals, the platform encourages eco-friendly practices, making it an attractive prospect for energy providers seeking a greener and more efficient energy landscape.

By integrating trust and energy awareness, `RETINA` enhances current smart grid implementations. One of the key features of `RETINA` is its ability to ensure business continuity even with mitigation failures and realized risks, allowing participating nodes to continue their operations securely. Scalability is another vital aspect addressed in the design of `RETINA`, recognizing the dynamic and evolving nature of smart grids [11]. With this in mind, `RETINA` is designed to be a swift and secure solution that facilitates secure bidirectional communication among smart grid participants.

`RETINA` facilitates autonomous and decentralized communication channels within the smart grid ecosystem. These communications can utilize existing internet infrastructure, and the connectivity may be provided by the Distribution System Operator (DSO) or other relevant entities responsible for smart meters' management in certain countries. While the DSO often oversees connectivity, the platform operates independently, offering a decentralized framework for secure and efficient communication among smart grid participants. To fortify the security infrastructure of `RETINA`'s energy trading mechanism, we employ an innovative hybrid paradigm that amalgamates the PKI and WoT concepts. This novel amalgamation is further reinforced by integrating Hyperledger Fabric, an advanced blockchain framework that facilitates feeless and expeditious transactions. Utilizing Hyperledger Fabric, as a decentralized and distributed ledger technology, maintains trust among network participants while concurrently diminishing the susceptibility to malicious activities. The energy trading mechanism within `RETINA` orchestrates prosumers' involvement in a distinctive bartering process, strategically incentivizing the consumption of energy derived from renewable sources. This represents a scientific novelty, aligning with the platform's overarching objective of seamlessly integrating security, scalability, and energy awareness. The holistic integration of these elements advances the functionality and efficiency of smart grids, thereby fostering a paradigm shift towards adopting renewable energy sources within the ecosystem.

In summary, this article makes the following main contributions:

- It introduces RETINA, a novel hybrid approach combining PKI and WoT architectures on Hyperledger Fabric, enhancing trust through endorsements, attestation, and the security features of blockchain.
- It overcomes challenges related to resource-friendly trust management and enables fee-less transactions by incorporating a permissioned ledger, providing an efficient solution for energy trading processes.
- It integrates key exchange, trust management, and energy trading, enabling decentralized participation in green energy production and consumption through smart contracts and a continuous trust mechanism among smart grid entities.
- The outcomes of RETINA are quantified and validated using a virtualized experimental testbed, demonstrating its superiority over existing trust management solutions for smart grids.

The remainder of this article is organized as follows. In Section 2, the background information required by the reader to know is provided. Section 3 provides a detailed description of the proposed solution's architecture and functions. In Section 4, a performance evaluation of the proposed framework is conducted, comparing its computation and delay efficiency to state-of-the-art solutions from the literature. Section 5 focuses on the energy trading aspect of the proposed solution, highlighting the applicability of RETINA. The security risks of RETINA and their impact are discussed in Section 6. Section 7 critically appraises the proposed framework, discussing the advantages of the hybrid trust establishment scheme. Section 8 presents a literature review related to RETINA, focusing on infrastructure security and current energy exchange schemes. The article's major innovations are also summarized in this section. Finally, Section 9 concludes the article.

2. Background

In this section the necessary foundational knowledge required to comprehend the key concepts and technologies associated with RETINA are presented.

2.1. Energy Trading

Energy trading among prosumers is a dynamic process that operates on the principles of supply and demand, where these entities, which generate and consume electricity, actively buy and sell electricity based on their specific production and consumption patterns. In this market, prosumers can optimize their energy usage and potentially reap financial benefits by participating as either buyers or sellers, depending on their current energy requirements.

To initiate the energy trading process, prosumers place orders specifying their desired quantity of energy to be bought or sold. These orders reflect their needs and preferences, considering factors such as their electricity generation capacity, consumption patterns, and any surplus or deficit in their energy supply. Through a transparent and efficient marketplace, these orders are matched with corresponding offers from other prosumers, facilitating the exchange of electricity between parties. By actively participating in energy trading, prosumers can effectively manage their energy resources and optimize their overall energy consumption. For instance, a prosumer with excess energy generation beyond their own consumption needs can sell the surplus to another prosumer requiring additional electricity. Conversely, a prosumer with higher energy consumption demands than their own generation capacity can purchase the needed energy from a willing seller. This mutual exchange of electricity enables prosumers to balance their energy needs, enhance grid stability, and contribute to the overall efficiency and sustainability of the energy system.

Energy trading among prosumers provides a decentralized and market-driven approach to electricity exchange, allowing participants to leverage their individual generation and consumption capabilities. By actively buying and selling electricity, prosumers play an integral role in shaping the energy landscape, fostering renewable energy adoption, and fostering a more efficient and sustainable energy ecosystem.

2.2. Public Key Infrastructure

PKI is a fundamental mechanism for creating and signing certificates. PKI serves as a trusted framework that facilitates secure communication and authentication within a smart grid. Each smart meter is equipped with unique cryptographic keys and digital certificates. These certificates serve as a form of identity verification and endorsement for the smart meters. When smart meters interact with each other, they can present their certificates as

a means of mutual authentication. By verifying the digital signatures of the certificates using the public keys stored on the blockchain, the smart meters can confirm the identity and trustworthiness of their counterparts.

Using PKI in this context enables a robust and secure endorsement process for smart meters. It ensures that only authorized and trusted devices are involved in energy trading transactions. By relying on the cryptographic capabilities of PKI, the integrity and confidentiality of communication between smart meters are protected, safeguarding against unauthorized access, tampering, or impersonation.

2.3. Web of Trust

The utilization of PKI enables the establishment of a Web of Trust, which facilitates the system's operation without the need for a central authority. PKI serves as a foundational framework for creating and managing trust relationships among the smart meters in a decentralized manner. Through PKI, a WoT is formed among the smart meters, where each smart meter can verify the certificates of other smart meters based on the trustworthiness of the signing authorities. By building and maintaining a network of trusted relationships, smart meters can operate autonomously and securely without relying on a central authority for every transaction or communication.

In this WoT, smart meters can validate the digital signatures of certificates using the public keys stored in their local trust repositories. This process allows them to verify the authenticity of the certificates and the identities of other participating smart meters. The decentralized nature of the WoT enables smart meters to establish and manage trust relationships among themselves. As smart meters interact and engage in energy trading, they can evaluate their counterparts' trustworthiness based on the signing authorities' reputation and the history of successful interactions. By leveraging PKI to create a WoT, the energy trading system achieves a resilient and secure operation without relying on a central authority. This decentralized trust model ensures that only trusted smart meters are involved in transactions, mitigating the risks of malicious activity and unauthorized access.

2.4. Blockchain and Distributed Ledgers

Blockchain technology, specifically the Hyperledger Fabric platform, establishes two immutable and transparent ledgers that record the endorsed certificates. Each smart meter's signed certificate, representing the endorsement of its identity and trustworthiness, is stored in one of those distributed

ledgers. The blockchain ensures the integrity and tamper-resistance of the endorsements, as any modification or tampering attempts would be immediately detectable through consensus mechanisms and cryptographic hashes. The second ledger, utilized for trading orders, facilitates energy exchange among prosumers. It is a decentralized platform where participants can place orders to buy or sell electricity based on their production and consumption needs. By leveraging blockchain and distributed ledgers, three key benefits are provided. First, the immutability of the blockchain ensures the integrity of the stored certificates and trade orders, and prevents unauthorized modifications, enhancing the overall security of the system. Second, the distributed nature of the ledger eliminates the reliance on a centralized authority, enabling decentralized and autonomous energy trading. Third, the transparency of the ledger allows participants to verify the validity of certificates and track the transactions' history, promoting trust and accountability.

The separation of the two ledgers in `RETINA` ensures a clear distinction between the storage of certificates (endorsements) and the trading orders. This design choice allows for efficient management and retrieval of endorsements while providing a dedicated platform for energy trading operations. The certificates ledger serves as a foundation for establishing trust among smart meters, while the trading orders ledger enables the secure and transparent exchange of electricity among prosumers.

3. Architecture

The architecture of the proposed framework follows a "bottom-up" approach, beginning with analyzing the smart grid architecture and the role of blockchain. The goal is to establish trust among the network elements and create a secure and decentralized environment. To achieve this, a hybrid approach that combines the concepts of PKI and WoT is employed, augmented with blockchain. The PKI infrastructure is leveraged to incorporate certificates, which attest to the trustworthiness of individual network nodes. However, instead of relying solely on certificates issued by a centralized certificate authority, the proposed architecture promotes the creation of a glsWoT among all network nodes. This means the entire network endorses and recognizes certificates rather than a single authority. This distributed approach ensures the network's resilience if certificate authorities (empowered nodes) become unavailable. In addition, blockchain technology is crucial in enhancing the security of the smart grid architecture. It provides an im-

mutable and transparent ledger to store the certificates securely. By logging the certificates on the blockchain, their integrity and authenticity can be verified by any participant in a tamper-resistant manner.

The capabilities of `RETINA` are further extended by incorporating an energy trading mechanism. This mechanism is built on the secure and trusted environment established through the WoT, reflected in the ledger entries. Like the trust establishment process, blockchain ensures the immutability and transparency of energy production and consumption activities. These activities are logged on the blockchain, enabling accurate and verifiable customer billing. By integrating the secure and trusted environment of `RETINA` with the energy trading mechanism supported by blockchain, the proposed framework provides a robust and transparent infrastructure for smart grid operations. It leverages the inherent characteristics of blockchain, such as immutability and transparency, to enhance the security and reliability of the smart grid architecture, ultimately benefiting both consumers and energy providers.

3.1. RETINA Smart Grid and Blockchain Architecture

The proposed smart grid infrastructure, as illustrated in Figure 1, consists of three main components: (*i*) energy provider, (*ii*) empowered nodes, and (*iii*) prosumers' smart meters. The energy provider includes various entities such as energy plants, administration systems, and billing systems. They play a pivotal role in managing and providing energy to the grid. The empowered nodes are strategically positioned in the network to ensure its robustness and mitigate the risk of a single point of failure. Each empowered node defines a neighborhood representing a distinct administrative area within the smart grid. By compartmentalizing the network, administrative responsibilities and resources are distributed among multiple empowered nodes, enhancing the resilience and security of the overall system. Finally, the prosumers' smart meters are key elements in the smart grid infrastructure. They enable measuring and monitoring energy consumption and production at the individual prosumer level. These smart meters interact with the empowered nodes and participate in the secure communication channels established within the framework.

`RETINA` is depicted as an overlay framework on top of the energy grid in Figure 1. It utilizes blockchain to provide a secure infrastructure to establish communication channels and gateways. These channels facilitate inter-neighborhood connections, enabling access to a larger market with multiple

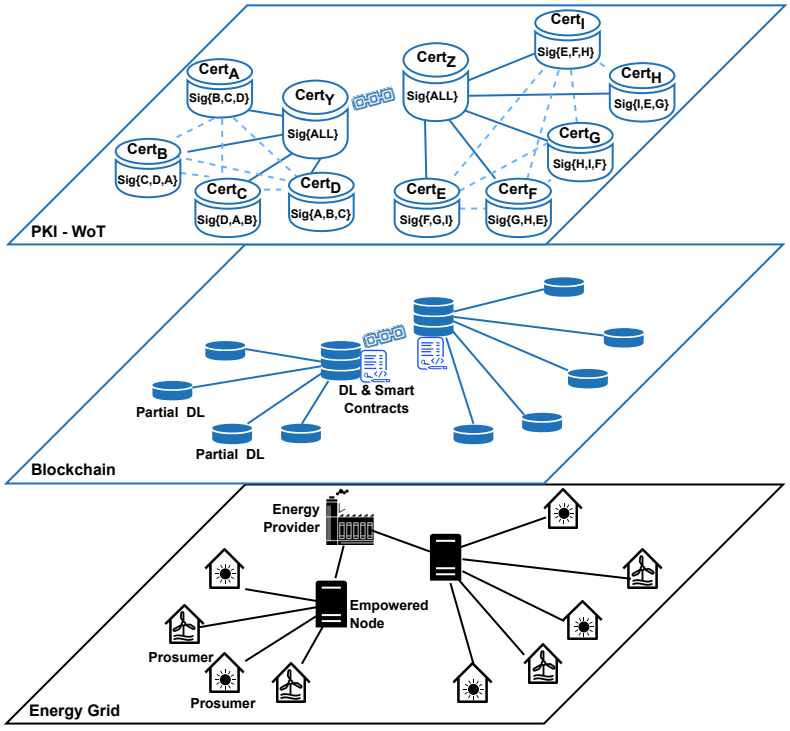

Figure 1: RETINA as an overlay framework, where network participants possess their own certificates, signed by nodes that endorse them

electricity buying and selling offers. By leveraging the blockchain, RETINA ensures the integrity and transparency of the communication infrastructure. Further, the PKI concept is employed on top of the blockchain to facilitate the issuance and management of personal certificates for each smart meter. These certificates serve as a means to establish trust and accumulate endorsements from other participants in the grid. This process creates a WoT, where data exchange can occur securely with trusted entities. One of the advantages of this infrastructure is its resilience in the face of empowered node failures. Even if an empowered node becomes unavailable, the grid can continue its operations due to the trust relationships established among the network participants. These relationships are reflected in the *Distributed Ledger* (DL), ensuring the continuity and reliability of the smart grid.

As shown in Figure 2, each smart meter in the smart grid system pos-

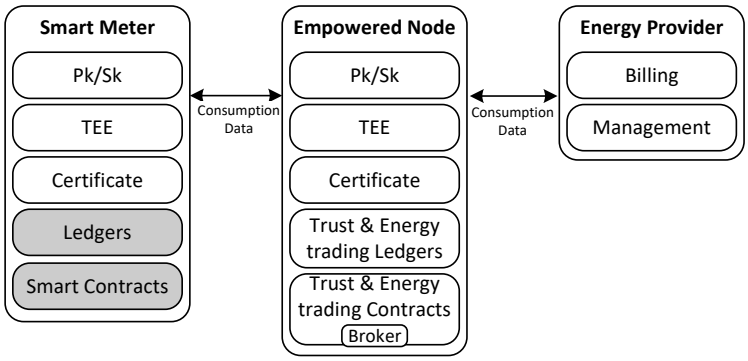

Figure 2: Resources and operations within the RETINA network components

sesses a Secret/Public (S_k/P_k) key pair, along with its associated certificate. To ensure the security of cryptographic operations and protect the secret key, a secure *Trusted Execution Environment* (TEE) is utilized within each smart meter. Additionally, each smart meter maintains a partial copy of the trust management ledger. This ledger contains relevant information about the trust relationships and endorsements among the network participants. A partial copy of the ledger enables smart meters to assume the corresponding duties and responsibilities in case an empowered node becomes compromised or unavailable. This feature enhances the resilience and continuity of the system. In essence, the empowered nodes play a paramount role in the blockchain infrastructure. They host the ledgers and smart contracts necessary for the operation of the smart grid system. They are also responsible for resource-intensive operations such as consensus, transaction processing, and executing smart contracts. The system achieves higher scalability and resilience by distributing these tasks among multiple empowered nodes. Finally, the energy provider, depicted in the diagram, receives information from the empowered nodes for billing and management purposes. It utilizes the data collected from the smart meters and processed by the empowered nodes to calculate and manage energy consumption, billing, and other administrative tasks within the smart grid system.

The blockchain's vital characteristics ensure robust security, accountability, and non-repudiation. Moreover, its immutability guarantees the creation of indisputable records. The operational functionalities of the em-

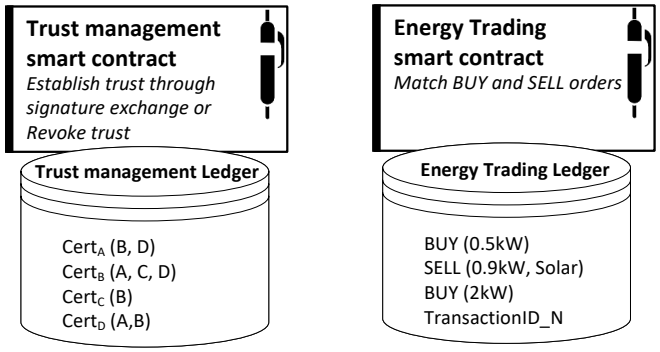

Figure 3: RETINA smart contracts and Ledgers residing on the empowered nodes

powered nodes encompass the execution of smart contracts and the maintenance of up-to-date ledgers. As a decentralized node certificate storage platform, the blockchain facilitates energy exchange, where two smart contracts are deployed, and corresponding ledgers are formed, as depicted in Figure 3. While P2P energy trading introduces a novel and potentially more dynamic approach, the ease of the process for prosumers compared to traditional contracts offered by energy suppliers depends on various factors. In the traditional model, energy suppliers provide contracts specifying prices for excess energy or compensation for consumption at different times. The choice between P2P trading and traditional contracts involves transaction simplicity, contractual complexities, and prosumers' desired level of autonomy. The comparison can be further nuanced based on specific market dynamics, regulatory frameworks, and individual preferences within the smart grid ecosystem. To establish a secure foundation for the smart grid, the ledger is consistently updated whenever a new trust relationship is established or an existing one is revoked. Figure 3 presents a snapshot of the Trust Ledger, illustrating the bidirectional trust relationship between smart meter A and smart meters B and D. The smart contract securely maintains this trust relationship, which automates and safeguards energy transactions for the energy trading mechanism of RETINA, encompassing "buy" and "sell" orders. The outcomes of completed transactions are accurately recorded on the ledger, ensuring transparency and accountability.

Selecting a consensus algorithm for a blockchain infrastructure is critical, as it significantly impacts system performance and financial implications. In

this scheme, the empowered nodes have chosen the *Proof-of-Authority* (PoA) consensus algorithm [12] to achieve consensus and record information on the ledgers. PoA is advantageous due to its minimal computational resource requirements, resulting in low energy consumption during operation. The PoA consensus mechanism relies on a limited number of validators to approve transactions for ledger entry. This enables frequent updates to the blockchain, reduces the time between block creation, and facilitates the processing of numerous transactions within short timeframes. The scalability of PoA is particularly beneficial for smart grids, where the network size may vary and potentially increase substantially. In `RETINA`, the verification of blocks and transactions is carried out by the empowered nodes, who assume the responsibility of maintaining the blockchain infrastructure.

3.2. Key Management and Authentication

The security of the `RETINA` platform rests on two fundamental pillars: (*i*) key management operations and (*ii*) authentication of network entities. These pillars exclude untrusted entities from all network communications and energy trading operations, effectively mitigating the risk of fraudulent activities. The following functionalities are instrumental in realizing this secure scheme.

3.2.1. New Smart Meter Joining the Smart Grid

The process followed by a new node to join the network is illustrated in Figure 4. In order for a new node to join a smart grid that incorporates the `RETINA` authentication scheme, it must acquire a signature from at least one empowered node with a valid certificate that is already part of the network, as shown in Listing 1. When a node intends to join the network for the first time, it generates a key pair consisting of a *Public key* (P_k), a *Secret key* (S_k), and a corresponding self-signed certificate. Subsequently, the new node initiates a request to join the network. A remote attestation procedure is then conducted by the empowered node responsible for the respective neighborhood. This attestation verifies that the candidate node is utilizing provider-approved software and has not been tampered with or subjected to unauthorized alterations. If the remote attestation yields a positive result, the empowered node acting as an introducer signs the certificate of the new node. This signed certificate is logged in the DL along with the corresponding identification number of the new node, denoted as ID_n (where $n \in [1, N]$, and N represents the network size). In Listing 1, the certificate

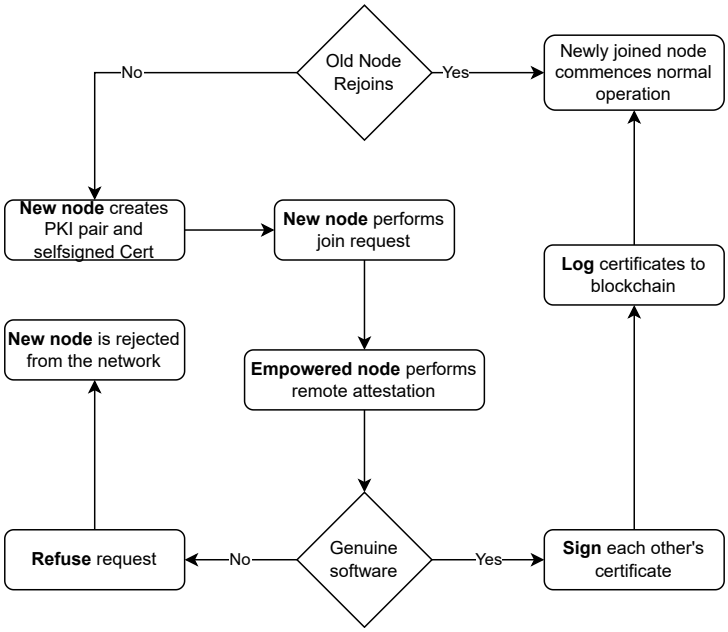

Figure 4: Node join operation

format is depicted. The *Public key* (P_k) is publicly available for all-access, followed by its owner's address (Node A). The first signature accumulated originates from the self-signing step, which precedes the endorsement from an empowered node. Lastly, a signature from Node B follows, establishing a trust relationship between Nodes A and B.

```
Pk 2048R/678455A3 2022-02-07 [expires: 2023-06-07]
uid Node A <nodea@retina.org>
sig 962789D1 2023-02-07 Node A <nodea@retina.org>
sig F4V7287Z 2023-02-07 Empowered <emp@retina.org>
sig A55CDCC1 2023-02-07 Node B <nodeb@retina.org>
```

Listing 1: Format of the certificate

The new node engages in certificate signature exchanges with the nodes residing in the 2^x network positions, where $0 \leq x \leq N/4$, as depicted in Figure 5 for Nodes A and J. This approach is not employed arbitrarily but is inspired by the demonstrated effectiveness of *Distributed Hash Table* (DHT) routing algorithms in establishing communication channels among nodes that are not necessarily directly connected [13, 14]. This eliminates the need for a new node to exchange and store signatures from all other network nodes. In

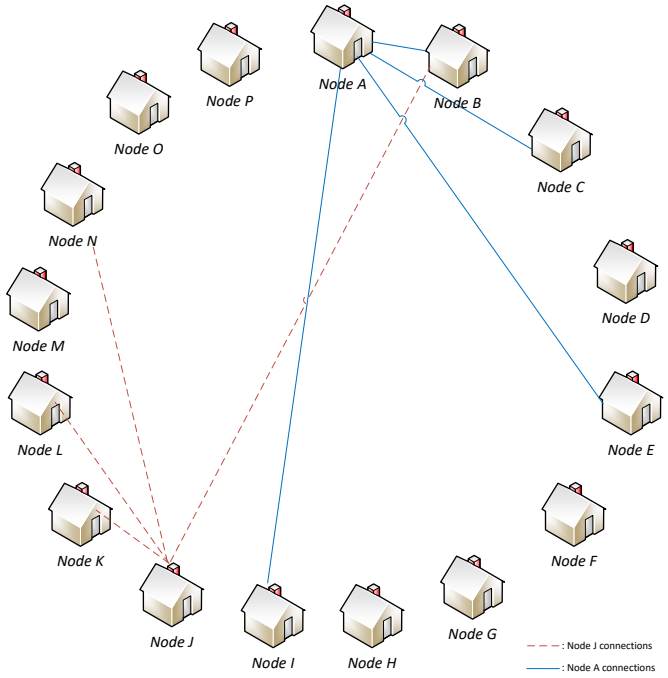

Figure 5: A random snapshot of the process of exchanging signatures, depicting the connections that Nodes A and J make with the nodes that reside on the 2^N network positions

contrast, in a traditional WoT network, each node must exchange signatures with all other participants. The utilization of DHT-based routing algorithms simplifies the process and reduces the signature exchange requirements for new nodes, allowing them to establish trust relationships with a subset of nodes within the network.

The newly signed certificates are stored locally on the smart meter and the empowered node. To avoid unnecessary storage, simple network nodes maintain only the portion of the ledger corresponding to the endorsements they have given and received. In contrast, empowered nodes possess the complete version of the ledger, including the entire network's trust relationships. Partial ledgers maintained by simple nodes are not actively used during normal operations but are stored and updated. This storage approach ensures that simple nodes do not need to store and manage the entire ledger, reducing their storage requirements. However, they retain the information related

to their endorsements and received certificates, enabling them to validate trust relationships when required. If all empowered nodes in a neighborhood are compromised, simple nodes have the potential to assume the elevated responsibilities and role of an empowered node. This ensures the continuity of network operations and the preservation of trust within the neighborhood, even in the face of compromised empowered nodes.

In addition to new nodes, previous network participants who may have gone offline have the potential to rejoin the smart grid, as depicted in Figure 4. In such cases, if the certificate previously used by the participant is still valid and has not been revoked or expired, no further action is required. The participant can use its existing ID_n and the corresponding certificate already stored on the DL. However, if the old certificate is no longer valid, the participant must repeat the aforementioned process of joining the network. A comprehensive procedure is implemented to ensure the seamless reintegration of participants who have left the smart grid network and to enable participants with expired or revoked certificates to regain access. This procedure involves the generation of a new key pair, obtaining a signature from an authorized node, undergoing remote attestation, and acquiring a newly signed certificate that is recorded on the DL. By following this process, the smart grid guarantees that participants with valid previous certificates can easily rejoin the network while ensuring that those with expired or revoked certificates must go through the necessary steps to regain network access.

3.2.2. Establishing Trust Relationships

In a smart grid ecosystem, devices inherently execute applications that require communication among the network's participants. To ensure the smooth execution of these applications, a reliable trust system is necessary. This is achieved by leveraging the initial signature(s) acquired by a new node from the empowered nodes that introduced it to the network. As smart applications are utilized, communication is attempted with other nodes, resulting in an exchange of certificate signing among the network's entities. As mentioned earlier, every new node joining the network, as well as nodes rejoining the smart grid, possesses a certificate signed by one or more empowered nodes. Using this certificate, additional signatures are acquired from common nodes residing in the 2^x positions (as indicated by the last signature in Listing 1). A smart contract is employed to facilitate this process. For instance, if Node A has been introduced to the network by Empowered Node S, the smart contract will utilize Node A's certificate endorsement by

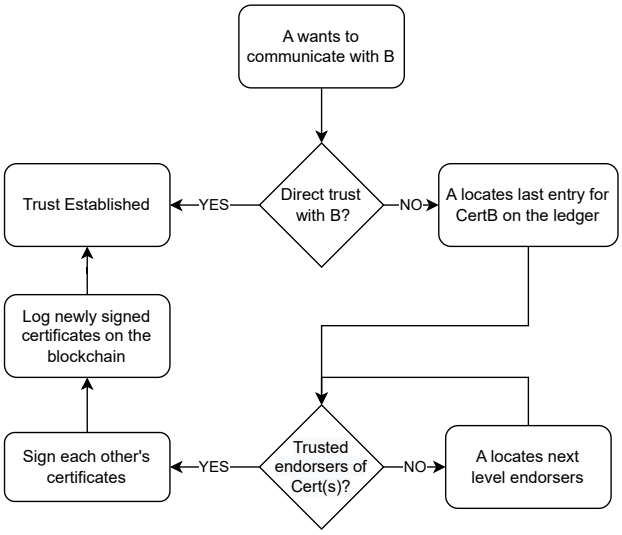

Figure 6: Trust establishment

Node S to introduce itself to other nodes that Node S has also introduced. This introduction lets the nodes exchange signatures by signing each other's certificates. Normal communication within the smart grid, driven by the operational requirements of smart applications, relies on the trust established through these mechanisms. The trust serves as a foundation for establishing the desired relationships among network participants, allowing for effective and secure communication.

In scenarios where specific empowered nodes (i.e., introducers) are unavailable, and there is no direct trust path between two nodes (i.e., they have not previously signed each other's certificates), the smart contract initiates a process of indirect trust establishment. To provide a clearer understanding of the procedure followed by the smart contract in establishing trust relationships, Figure 6 is provided. The following example illustrates the actions taken when Node A aims to establish a trust relationship and communicate with Node B:

Step 1. Node A first checks its own certificate to see if it has an existing endorsement from Node B. If such an endorsement exists, the process is completed, and Node A can establish a trust relationship with Node B.

Step 2. If Node A does not find an endorsement from Node B in its own certificate, a *Certificate Lookup* procedure is initiated. This procedure aims

to find the certificate of Node B, denoted as $Cert_B$.

Step 3. Node A examines the trustworthiness of the endorsers of $Cert_B$. If any of the endorsers of $Cert_B$ are trusted by Node A, such as Node C, this information is communicated to Node B. Both Node A and Node B then sign each other's certificates, log the new trust relationship on the Trust ledger, and conclude the procedure. In this case, only one intermediate entity, Node C, establishes the trust relationship between Node A and Node B.

Step 4. If no trusted endorsers of Node B are found in Step 3, the Certificate Lookup procedure continues by exploring the signatures collected by the certificates of endorsers of Node B. For example, unlike Step 3, Node A does not initially trust Node C. However, while searching for a trusted entity in the signatures of the nodes' certificates that have endorsed Node B, Node A discovers that Node D has signed the certificate of Node C. This finding establishes a trust path to Node B through Node D. Therefore, the formed chain of trust, in this case, would be $A \Rightarrow D \Rightarrow C \Rightarrow B$.

In scenarios where Node D initially lacks trust from Node A, Node A can actively search for trusted endorsers of Node D and expand the trust path accordingly. This iterative process continues until a trusted entity is discovered or until a predefined maximum chain length is reached. It is important to note that the performance of the trust establishment procedure, including delays and success probability, can be influenced by the chosen maximum chain length within the `RETINA` system.

The maximum chain length determines the number of intermediate entities or endorsers that can be explored in the search for a trusted path between nodes. A longer chain length increases the likelihood of finding a trusted path as more intermediate entities are considered. However, it also introduces additional delays in the trust establishment process, as each step necessitates further verification and validation of the endorsers. Conversely, a shorter chain length reduces delays but may limit the probability of finding a trusted path in certain scenarios.

Determining the optimal maximum chain length requires balancing the desired success rate of trust establishment and the acceptable process delay. This decision should consider the specific requirements and constraints of the smart grid ecosystem, including network size, the trustworthiness of entities, and performance considerations. Evaluating and optimizing the maximum chain length in `RETINA` is crucial to achieving efficient trust establishment while meeting the security requirements of the smart grid network.

3.2.3. Certificate Lookup

The Trust DL employed in the RETINA blockchain implementation is distributed across all network participants. Each participant stores their established trust relationships locally, while the empowered nodes maintain a complete copy of the Trust DL. The primary purpose of the Trust DL is to facilitate the certificate lookup procedure, which occurs on the empowered nodes when a direct trust relationship is not present but is desired. To perform the certificate lookup procedure, the empowered nodes utilize the process outlined in Section 3.2.2. This process identifies the nodes that should be considered when finding a trust path between two unrelated nodes. As previously explained, trust paths can be established indirectly through multiple intermediate nodes. This, combined with the fact that the Trust DL is processed locally on the empowered nodes, offers two main advantages:

- RETINA's swiftness is not limited by network constraints that may be presented due to bandwidth limitations or increased overhead because of heavy traffic.
- The network load will not be burdened with extra traffic due to the certificate lookup operation, which will be executed locally.

Figure 7 represents a visual depiction of an instance found in every node's locally stored Trust DL. This simplified representation illustrates an already-formed WoT among seven nodes. Each node's certificate contains multiple accumulated signatures, establishing new trust relationships. In this instance, Node A has exchanged signatures with Nodes B, C, and F, as indicated by the signatures in their respective certificates. Likewise, Nodes B and C have established trust paths with other nodes. Node B has trust paths with Nodes A, D, E, and Node C has trust paths with nodes A, E, F, and G. This visualization of the trust relationships showcases the interconnected nature of the trust paths. It highlights how trust can be established indirectly through the involvement of intermediate nodes. The Trust DL stored on each node enables the identification and utilization of these trust paths to facilitate secure interactions and transactions within the blockchain network. Overall, this graphical representation demonstrates the practical application and effectiveness of the Trust DL in enabling trust establishment and verification between nodes in the RETINA blockchain implementation.

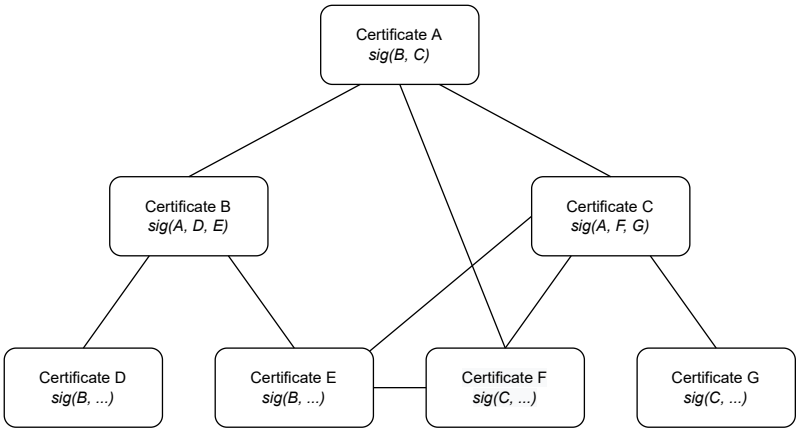

Figure 7: Snapshot of the Trust Paths that have been formed among seven network participants

To better understand the *Lookup Procedure*, an example based on Figure 7 is presented. In this scenario, Node A needs to contact Node E. The following actions will be performed:

Step 1. The initial search focuses on the signatures that $Cert_A$ has accumulated in order to determine whether the target Node E has already signed it or not.

Step 2. In this scenario, Nodes A and E have not exchanged signatures yet, so a search for trust with one intermediate node commences by examining the endorsers of Node's E certificate.

Step 3. The inquiry of Step 2 returns a positive result, as Node B, which is trusted by Node A, is an endorser of $Cert_E$. At this point, the lookup procedure is concluded successfully, and the process of establishing a trust relationship by exchanging signatures, as described in the previous section, commences.

Following the same train of thought, if the target node was at the next level in terms of depth, the procedure's execution would be extended, and an additional intermediate would be included in the formed trust path. Due to the nature of the network's ring-like structure, similar to the one found in DHT networks, an iterative-recursive hybrid approach [15] was utilized in terms of search routing, benefiting the overall performance of the system as showcased in Section 4 below.

3.2.4. Certificate Revocation

Node certificates may be revoked for two main reasons:

1. A node may voluntarily leave the network and choose to revoke its certificate.

2. A node might be considered untrustworthy or potentially malicious.

To ensure the integrity of the network, all participating entities undergo periodic remote attestation conducted by empowered nodes. As Panos et al. [16] described, this attestation process involves generating a hash value from each reviewed node's TEE. This hash value is derived from predetermined software components and parameters that should remain unchanged. If most nodes conducting the remote attestation procedure conclude that a particular node's software has been tampered with and could potentially engage in malicious actions, its corresponding certificate is revoked. For instance, in Figure 7, if $Cert_B$ is revoked, the associated signatures in $Cert_A$, $Cert_D$, and $Cert_E$ would be removed. This revocation process also applies to empowered nodes to safeguard the smart grid against malicious actors. Irrespective of whether the revoked certificate belongs to an empowered or a common node, the network's operations remain unaffected due to the existing WoT, which interconnects all smart grid nodes directly or indirectly. In the aforementioned example, the revocation of $Cert_B$ as an intermediate certificate between Nodes A and E can be compensated by Nodes C and F. Furthermore, the revoked certificate will not be utilized in any future attempts by other nodes to establish trust relationships among themselves.

Once a certificate revocation occurs, the trust relationships the revoked node establishes become unavailable if the node later rejoins the network. In such cases, the procedure for a new smart meter joining the grid must be repeated only after addressing the compromised software that initially led to the node's exclusion from smart grid operations. This entails issuing a new pair of keys and the associated certificate. Conversely, nodes that abruptly depart from the smart grid due to connection issues or technical problems do not need to repeat the join process since their certificate remains valid.

The certificate revocation process is inherently sensitive due to potential abuse, which could lead to denial of service. To mitigate this risk, the remote attestation performed by empowered nodes to network participants is securely protected and inaccessible to users or third parties. This safeguarding is achieved by utilizing TEE technology, which masks and shields these

operations from malicious actors. The calculation of attestation hashes from the attestee and the verification process conducted by the attesters occur within this protected environment, rendering them immune to tampering by any entity. Additionally, cryptographic processes related to certificate signing and energy trading rely on TEE utilization to mitigate various risks associated with fraudulent activities.

4. Performance Evaluation

The proposed framework has undergone rigorous testing and validation across various scenarios, comparing it to state-of-the-art solutions in terms of communication and computational costs during trust establishment. A comparison against WoT implementations confirms that RETINA significantly improves the time required to establish trust in scalable smart grid environments and demonstrates superior responsiveness when empowered nodes are lacking. To demonstrate the practicality of RETINA in real-world scenarios, performance evaluation has been extended to validate an energy trading scheme that utilizes RETINA to establish trusted nodes as energy traders. This scheme ensures security guarantees in cases of trust revocation or unauthorized access by malicious traders. The evaluation of the RETINA-based energy trading scheme focuses on examining energy trading price fluctuations resulting from tampering by malicious nodes. These simulations demonstrate the framework's reliability, efficiency, and security in trust establishment and energy trading scenarios, providing compelling evidence of its applicability and effectiveness in real-world deployment.

4.1. RETINA Configuration

The simulation of `RETINA` was deployed on a physical machine running *Ubuntu 18.04 LTS*, equipped with an *Intel i7 6700HQ* processor and 32 gigabytes of RAM. The implementation was implemented in Java, utilizing smart contracts for *Key Management* and *Energy Trading* functionalities as the main components. To facilitate the blockchain deployment of `RETINA`, the Hyperledger Fabric framework was employed with the assistance of the *Hyperledger fabric-gateway-java* dependency. Up to 500 nodes were simulated to assess the network's performance and responsiveness in various real-life scenarios. Each node was assigned corresponding certificates and wallets for these simulations and evaluations. The certificates adhere to the PGP standard and employ the `SHA-1` hash function, which generates block hashes.

Table 1: Comparison in terms of average communication cost and average computation time between RETINA and other similar solutions

Frameworks	**Computation Time (ms)**	**Communication Cost (bits)**
FeneChain [17]	2000	540.67
SURVIVOR [18]	117.35	448
BEST [19]	35	961
Secure ET in DRM [20]	33	968
EnergyChain [21]	33	576
RETINA	19.2	192

4.2. Evaluation of Computation Time and Communication Cost

As depicted in Table 1, RETINA's evaluation centers around its comparison to related works, specifically regarding two key factors: (*i*) computation time required for signature exchange between two nodes, and (*ii*) communication costs associated with the data transferred during the mutual endorsement process between network nodes. These evaluation criteria aim to assess the performance and efficiency of RETINA to similar approaches in the field.

In assessing *Computation Time* (CT), multiple factors have been carefully analyzed to determine the average CT involved in the process of trust establishment among smart grid nodes. To quantify this, we precisely gauged the time required for executing a range of blockchain-related operations integral to building trust. Both hardware and software variables arising from the *Virtual Machine* (VM) architecture critically influence the overall computation time. On the hardware front, elements such as CPU processing power, available RAM, disk access speeds, and the capabilities of *Network Interface Cards* (NICs) on host machines directly affect the simulation's efficiency. On the software side, parameters like the operational efficiency of the blockchain software, its compatibility with the VM environment, the operating system's resource management protocols, and the choice of virtual machine monitor (hypervisor) can significantly impact the allocation of computational resources like CPU and memory across VMs, consequently affecting the simulation speed. While these parameters are not directly quantified during the simulations, their influence on the measured computation time is captured as variances from the average values across multiple simulation runs. Furthermore, for the sake of simplicity and without compromising the general applicability of our findings, we assume that the communication channels between nodes in the smart grid are error-free. Operations that

directly influence computation time are identified as follows:

VerifyCertificate: Use the certificate's *Public key* (Pk) to decrypt and verify its validity. For `RETINA`, the average time to decrypt and validate the certificate was $2.7ms$.

SignCertificate: Use own *Secret key* (Sk) to sign a certificate. In `RETINA`, the time required to sign the certificate was calculated at $2.7ms$ on average.

Addition: Making a new entry on the DL (`addToDL`). On average, the time required for this process in `RETINA` is measured at $1ms$.

One-way hash function (SHA-1): Hashing the information pertaining to a new block (`hashData`). The SHA-1 operation required in `RETINA` an average of $2.7ms$.

Append: Collecting data into a single string, giving it a proper form to introduce it to the blockchain (`addNonce`). The append operation in `RETINA` has been timed at $0.5ms$ on average.

$$CT_{total} = \sum_{n=2}^{N} (VerifyCertificate_n + SignCertificate_n + addNonce_n + hashData_n + addToDL_n) \tag{1}$$

where, n is the number of nodes active during the simulation. Since the endorsement process for establishing a trust relationship is executed mutually from both ends, the entire process is performed twice, once for each node involved. Therefore, we calculate the total Computation Time as CT_{total} by doubling the computed value of CT. This accounts for the bidirectional nature of the endorsement process, ensuring a comprehensive evaluation of the computational efficiency of `RETINA` in establishing trust between network nodes.

Regarding the *Communication Cost* (CC), higher values could impact the efficiency of data exchange among nodes, potentially leading to delays or increased resource consumption. This may hinder the real-time responsiveness crucial for smart grid operations, affecting energy trading, demand response, and system reliability. On the contrary, a lower communication cost enhances the responsiveness and overall performance of the smart grid. It promotes faster information dissemination, enabling quicker decision-making and more seamless collaboration among grid components. The CC in the

Algorithm 1 Computation Time & Communication Cost calculation

1: //Computation Time calculation
2: N =2
3: **for** $i = 1toN$ **do**
4: $\quad CT_{total} = VerifyCertificate_n + SignCertificate_n + addNonce_n + hashData_n + addToDL_n$
5: **end for**
6: //Communication Cost calculation
7: $H_b = Identity + PreviousBlockHash + Transactions$
8: $H_{out} = H_b + nonce + padding$
9: $CC_{PoA} = Identity + SHA - 1Digest(H_{out})$

case of RETINA is evaluated based on the number of bits transferred while establishing a trust relationship between two nodes. In this context, we consider the specific components (i.e., SHA-1 Input and Digest Size) involved in the process:

SHA-1 Input and Digest Size: The total input size for the SHA-1 algorithm is 416 bits, and after digesting, the final output size is 160 bits.

- ***Block Header Size:*** The number of bits processed at the block header, denoted as Hb, is calculated as $H_b = 320bits$.
  Specifically: $H_b = 32bits \quad (Identity)$
  $+ 256bits \quad (previous\ block\ hash)$
  $+ 32bits \quad (transactions)$

- ***Hash Output:*** Utilizing the SHA-1 hash function, the output size of the hash, denoted as H_{out}, has the value of $H_{out} = 416bits$ calculated as $H_{out} = 320bits \quad (H_b)$
  $+ 32bits \quad (nonce)$
  $+ 64bits \quad (padding)$

Based on these calculations, the total cost of the PoA consensus algorithm is determined as:

$$CC_{PoA} = Identity + SHA\text{-}1_Digest \tag{2}$$
$$CC_{PoA} = 32bits + 160bits = 192bits$$

It is important to note that CC_{PoA} is borne solely by the Empowered nodes due to the nature of the PoA consensus algorithm implemented in RETINA.

Algorithm 1 provides an addition point of view, showcasing how RETINA's CT and CC are calculated. Studying Table 1, RETINA exhibits improved average CT and CC compared to the other frameworks due to its efficient design and utilization of advanced techniques. In particular, RETINA integrates a series of finely-tuned optimizations that substantially enhance its CT. Through meticulous engineering of certificate verification and digital signing processes, the cryptographic operations are executed in a minimized time frame. Additionally, the framework excels in proficiently managing data-related tasks, such as data addition, hashing, and appending, further driving down the overall computation time. As a result of these optimizations, RETINA boasts an exceptional average CT of 19.2ms, notably surpassing competing frameworks, including FeneChain, SURVIVOR, BEST, Secure ET in DRM, and EnergyChain.

In the context of CC_{PoA}, RETINA stands out for its exceptional efficiency, achieved through a carefully engineered, streamlined approach. By innovatively adopting the *Proof-of-Authority* (PoA) consensus algorithm, RETINA significantly minimizes communication overhead, reducing it to 192 bits. This represents a substantial improvement over the overhead costs commonly associated with alternative frameworks. Key optimizations include a streamlined block header size, fine-tuned hash output parameters, and the judicious selection of input and digest sizes tailored explicitly for the SHA-1 algorithm. Collectively, these refinements contribute to RETINA's dramatic reduction in communication cost. This efficiency gain becomes particularly salient when contrasted with other established solutions, such as FeneChain, SURVIVOR, BEST, Secure ET in DRM, and EnergyChain, which exhibit higher communication overheads ranging from 448 to 968 bits.

4.3. RETINA's Performance Against Web of Trust

An infrastructure based on the WoT was implemented, drawing from the descriptions outlined in the OpenPGP standard [22] and the corresponding official guide [23]), as a decentralized trust model. This implementation enables a comparative performance analysis between RETINA and WoT, highlighting the distinct advantages of each solution. Specifically, we examine the decentralized performance of RETINA's algorithm in contrast to a traditional WoT network, focusing on the time required for (*i*) introducing a new node to the network and (*ii*) establishing communication between two network participants. Notably, previous literature has conducted network experiments in similar scenarios involving network sizes ranging from 100 to 500

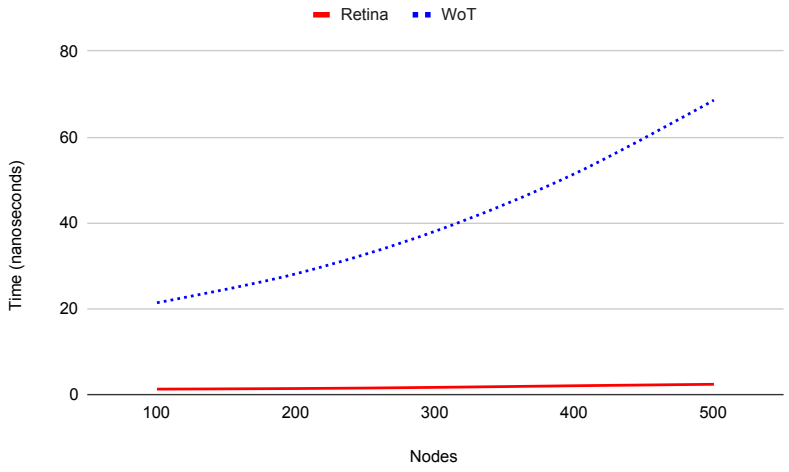

Figure 8: Comparison in terms of time required for a node to establish a new trust relationship with a random node under RETINA and WoT schemes, for different network sizes

nodes [24, 25, 26]. To ensure comparability with these studies, the following performance evaluation encompasses network sizes of $100, 200, 300, 400$, and 500 nodes.

As illustrated in Figure 8, RETINA exhibits a marked performance advantage over traditional WoT networks, particularly in the context of new network node initialization. The data reveals that the time required for a node to join the network in the RETINA framework ranges from a rapid $1.2ms$ to $2.7ms$. In contrast, the initialization times in a WoT network are considerably longer, ranging from $21.4ms$ to $144.7ms$. This striking difference in performance is attributable to the unique mechanisms each system employs for node integration. Specifically, in the RETINA environment, a new node must perform signature exchanges solely with the nodes occupying the 2^x positions. On the other hand, in a WoT network, the new node is compelled to introduce itself to all existing nodes through a more laborious flooding procedure, inevitably leading to higher initialization times.

While RETINA shows superior performance during the introduction phase of new nodes, there is a trade-off regarding trust establishment, as illustrated in Figure 9. In a WoT network, a node needs to query its database to locate the endorsement for another node, whereas, in RETINA, this may not always be necessary. If the endorsement is not locally stored on a node, a search is

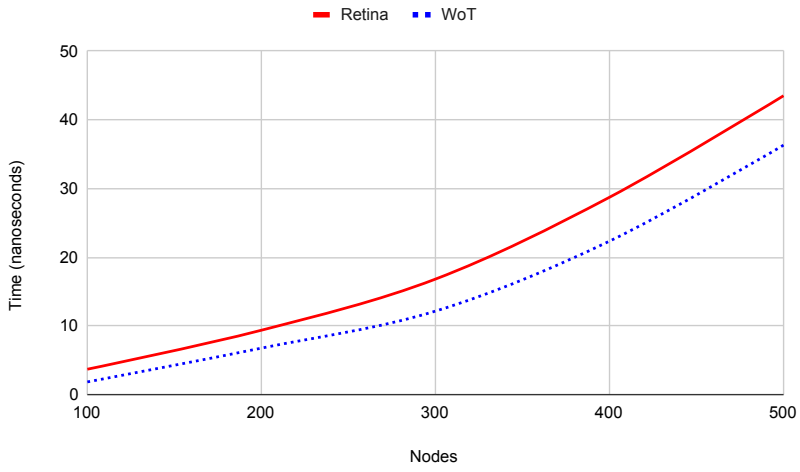

Figure 9: Comparison in terms of time required for a new node to join the network and establish trust among the first tier nodes under RETINA and WoT schemes, for different network sizes

initiated using trust relationships established by other trusted nodes.

In Figure 10 the increasing average number of hops required to be performed in order to establish a new trust relationship as the network grows can be observed. Due to RETINA's recursive/iterative hybrid search method, the time delay for establishing a trust relationship remains relatively low, albeit higher compared to that of a WoT node, but still within a reasonable range. It is important to note that this metric applies explicitly to a decentralized RETINA scenario where the empowered node is unavailable. In alternative scenarios, where the empowered node is present, RETINA's performance closely aligns with that of a CA-centered network, resembling the WoT approach. This resemblance occurs because, in both cases, the search involves a single database.

5. Energy Trading Mechanism

To demonstrate the advantages and practicality of the proposed framework, an energy trading mechanism for smart grids has been integrated into RETINA. This mechanism enables all participating entities, chiefly prosumers, to buy or sell generated energy within the smart grid ecosystem. By establishing this exchange platform among these entities, increased consumption

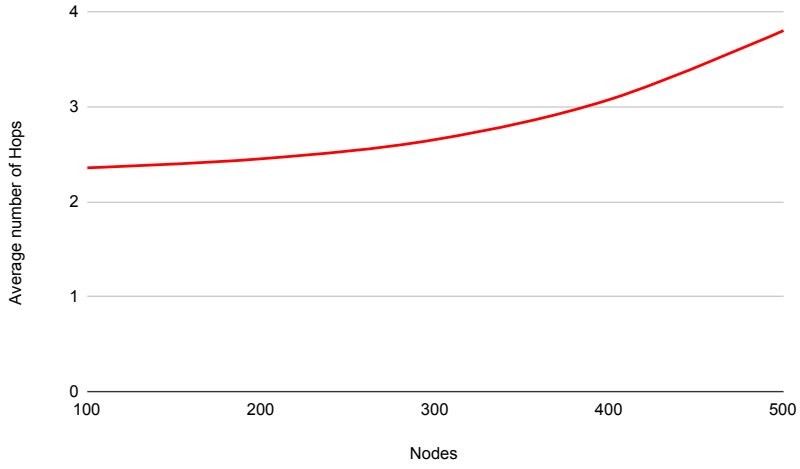

Figure 10: Average number of Hops required to be performed by a node to establish a new trust relationship with a random node under `RETINA`, for different network sizes

of green energy is facilitated. This is made possible by the availability of diverse energy sources and the seamless accessibility granted by the trading mechanism. As a result, the integration of `RETINA` facilitates a more sustainable and environmentally friendly utilization of energy resources within the smart grid infrastructure.

Within `RETINA`, every network node possesses a wallet that contains the quantity of produced energy and a corresponding balance. The energy trading mechanism implemented in `RETINA` leverages the trust relationships formed during the earlier stages of the nodes' life cycle. All entities involved in the exchange processes are considered trusted, indicating that their certificates have received one or more signatures from valid endorsers. This reliance on established trust ensures the integrity and reliability of energy transactions within the network, fostering a secure and efficient energy trading environment.

The "buy" and "sell" orders within the energy trading mechanism are posted on the blockchain and signed by the entities issuing them. This approach ensures that the orders are openly accessible to all participants in the network, allowing for easy verification of their authenticity. These orders possess specific characteristics, including:

- ***kW:*** The amount of energy to trade.

- ***Production method (*** CO_2 ***footprint):*** It states whether the power in kW referred to in an order has been produced using renewable energy sources or not.

- ***Location:*** It refers to the smart grid location, in terms of neighborhood, of the order originator.

Defining the $\frac{Price}{kW}$ in the energy trading mechanism is not deterministic and considers the aforementioned characteristics, which can vary between nodes. This architecture is flexible and can accommodate various pricing models. For the presented energy trading scheme, a theoretical pricing model has been chosen, incorporating the listed criteria through the utilization of two weights:

$$\alpha = \begin{cases} 0.2 & \text{corresponds to a higher proportion of green energy being offered} \\ 0.5 & \text{corresponds to a lower proportion of green energy being offered} \end{cases}$$

$$b = \begin{cases} 0.2 & \text{account for the lower distance between the trading nodes} \\ 0.5 & \text{account for the larger distance between the trading nodes} \end{cases}$$

It should be noted that the specific values of these weights are merely indicative and can be adjusted according to the policies of the energy provider. Thus, the theoretical price assigned to the energy trading contract between two nodes in the grid can be calculated using the following formula, where `StartingPrice` represents the base price per kW.

$$Price = (1 + a + b) \times StartingPrice \tag{3}$$

During periods of high load on the grid's infrastructure, prices within the energy trading mechanism may favor participants who exchange energy with nearby counterparts within the same neighborhood. This approach helps minimize the utilization of network resources, and it can be achieved by setting a minimum value for the location proximity weight (b), thereby reducing the corresponding energy cost accordingly. To illustrate this concept, the following example highlights how the cost of *1kW* of energy can vary based on its specific traits. It is important to note that additional factors, such as the scarcity of electric power during peak hours, can also be considered in the price calculation, adhering to the fundamental principles of supply and demand.

Consider the example of *1kW* of energy (with a base price of €$1/kW$) produced from renewable energy sources (where $a = 0.2$) originating from a node located in a different neighborhood (with $b = 0.5$). The indicative price of the energy transaction can be calculated using Equation 3, resulting in an energy transaction of $Price =$ €1.7 per KW. In the case of *1kW* of energy (with a base price of €$1/kW$) generated from renewable energy sources (with $a = 0.2$) originating from the same neighborhood (with $b = 0.2$). Using the same calculation as in Equation 3, the price for this transaction, accounting for the impact of distance, would be $Price =$ €1.4 per KW.

In the energy trading mechanism, the nodes automatically place orders based on the status of their energy reserves. A broker, represented by an algorithm running on the smart meters, considers multiple variables to determine whether placing either "sell" or "buy" orders is necessary. These variables include the current rates of electricity production and consumption and the availability of battery reserves. By analyzing this data, the broker creates a projection regarding the potential need or surplus of electricity. Moreover, the broker considers behavioral patterns observed in the past, such as increased electricity demand at noon. Based on these considerations, the broker places the corresponding orders on the ledger.

The energy trading smart contract then takes control, matching "buy" and "sell" orders that complement each other. The smart contract ensures that the conditions of each order are met before executing the transaction. Additionally, it should be noted that the broker can also receive manual input from the user. This enables the fulfilling of specific needs that may arise and cannot be anticipated solely by the broker's algorithm. Once a transaction is completed, the result is recorded on the ledger, including the updated values of the remaining energy and balance of the node involved in the transaction. This logging process ensures transparency and accountability within the energy trading system.

The trading process is comprehensively outlined in Algorithm 2, encompassing a series of steps that ensure efficient electricity exchange. Initially, each node determines whether it needs to buy or sell electricity. If a node possesses an excess amount of electricity, it diligently searches for the most favorable "buy" offer available at that particular moment. Once the search concludes, the "sell" order is meticulously examined to ascertain if it meets any predetermined minimum requirements established by the seller. Subsequently, upon finding a "buy" order that satisfies these prerequisites, the transaction is promptly executed. However, if no "buy" order meets the

Algorithm 2 Trading smart contract

```
1: if EnergyReserves = HIGH then
2:     Action ← SELL;
3: else if EnergyReserves = LOW then
4:     Action ← BUY;
5: end if
6: if Action = SELL then
7:     for everyBuyorder do
8:         GetStartingPrice;
9:         Price = StartingPrice + StartingPrice × b;
10:        Save OrderID if price is the highest so far;
11:    end for
12:    Sell to highest offer;          ▷ Provided that minimum expectations set beforehand are met
13:    if no Buy orders then
14:        Create Sell order
15:    end if
16: else if Action = BUY then
17:    for everySellorder do
18:        GetStartingPrice;                                          ▷ a has been factored in
19:        Price = StartingPrice + StartingPrice × b;
20:        Save OrderID if price is the lowest so far;    ▷ may skip orders concerning non-green energy
21:    end for
22:    Buy lowest offer;               ▷ Provided that minimum expectations set beforehand are met
23:    if no Sell orders then
24:        Create Buy order
25:    end if
26: end if
```

seller's specified requirements, a corresponding "sell" order is generated with the expectation of being matched by an equally qualified "buy" order. The same procedure is reversed when a node intends to purchase electricity. In this scenario, the node strives to identify a matching "sell" order and, if unsuccessful, creates a "buy" order accordingly.

5.1. Performance Evaluation of the Trading Mechanism

The experimental setup for the subsequent evaluation remains consistent with the description provided in Section 4. Leveraging the pre-established trust relationships, a series of simulations were conducted to showcase the intended functionality of the `RETINA` energy trading system, enabling nodes to achieve independence from traditional providers. These experiments highlight that price fluctuations align with participants' inclination to buy or sell electricity, following the fundamental principle of supply and demand. To facilitate this demonstration, a simulation environment was created, encompassing a predetermined number of neighborhoods, participating nodes, and their corresponding attributes: (i) individual electricity reserves, (ii) electricity reserve thresholds, which, when crossed the participant seeks to either buy

Table 2: Energy trading network configurations

	Network Configuration 1	**Network Configuration 2**
Neighborhoods	10	3
Nodes per Neighborhood	30	100
Market Cycles	30	30

or sell electricity and (*iii*) electricity consumption and production rate.

In addition, randomness was incorporated into the individual electricity reserves, consumption, and production rates to attain more realistic outcomes. This stochastic component was introduced to better simulate inherent variability and uncertainties in real-world scenarios. By including this randomness, the experimental setup aimed to capture the dynamic nature of electricity trading and accurately reflect participating nodes' diverse characteristics and behaviors.

Three distinct scenarios have been explored, each based on the initial intentions of the participating nodes. These scenarios encompass:

- ***Scenario 1:*** 75% Buyers, 25% Sellers
- ***Scenario 2:*** 50% Buyers, 50% Sellers
- ***Scenario 3:*** 25% Buyers, 75% Sellers

For each experimental scenario, two unique network configurations were utilized, designated as *Network Configuration 1* and *Network Configuration 2*. The term *"Market Cycles"* was coined to encapsulate a specified time interval during which individual network nodes partake in electricity generation, consumption, and the corresponding financial transactions based on their energy reserves. A comprehensive summary of the network configurations employed in the simulation is presented in Table 2. In *Network Configuration 1*, the geographical area under study was subdivided into ten distinct neighborhoods, each comprising ten nodes. In contrast, *Network Configuration 2* retained the same aggregate number of nodes but reconfigured their distribution across a reduced number of neighborhoods. The objective of comparing electricity price dynamics in these configurations was to validate the system's flexibility and seamless inter-neighborhood connectivity. Additionally, it was posited that the energy provider would offer incentives to stimulate the uptake of green energy. This led to the establishment of specific

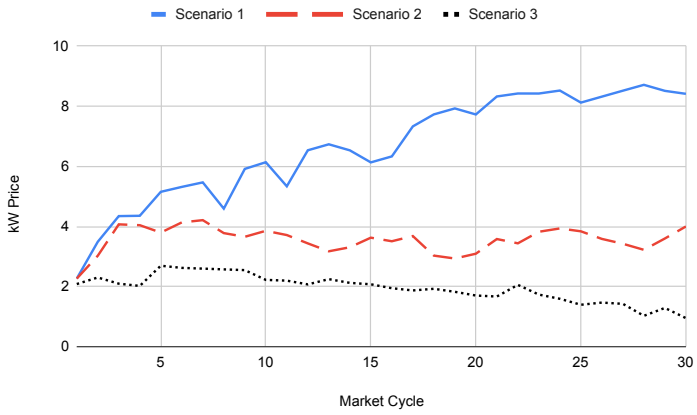

Figure 11: kW price chart – Network configuration 1

weight values, based on Equation 3, for two key factors: `(i) a = 0.2` and (*ii*) `b = 0.5`.

In both *Network Configuration 1* (Figure 11) and *Network Configuration 2* (Figure 12), observed price fluctuations conform to fundamental supply and demand principles. Specifically, a surplus of buyers relative to sellers results in an uptick in price, whereas the converse scenario triggers a price decline. Incorporating stochastic elements into the simulation yields a price graph that authentically mirrors the electricity requirements of the network. In *Network Configuration 1*, where a higher concentration of buyers coexists with numerous smaller neighborhoods, the likelihood of encountering two buyers from disparate neighborhoods escalates. This dynamic is further influenced by the weight factor `b = 0.5`, ultimately driving the energy price higher compared to what is observed in *Network Configuration 2*.

5.1.1. RETINA's Robustness Against Market Manipulation

Further experiments were conducted to evaluate the resilience of `RETINA` against market manipulation attacks, the results of which can be observed in Figures 13 and 14. Specifically, these experiments simulated cases where a coordinated attack from a malicious actor exploited a zero-day vulnerability in 20% of the network's smart meters (60 out of 300)—an acceptable average according to other works [27, 28], to artificially drop the electricity price. The details of the attach mechanism and the mitigation actions are described in Section 6.4. It can be observed in both Network Configurations that the

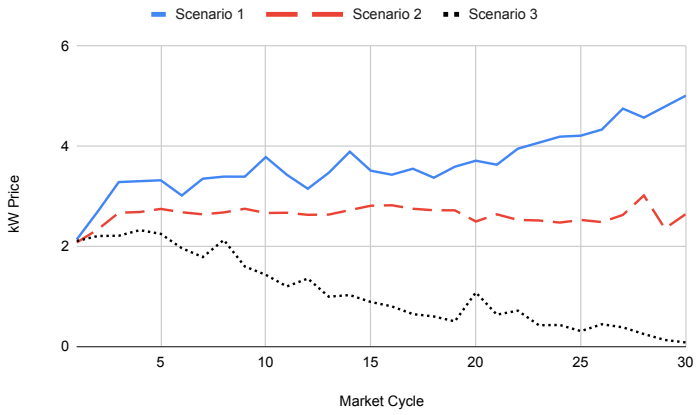

Figure 12: kW price chart – Network configuration 2

impact of the attack was more evident in Scenario 1, when the buyers far exceeded the sellers. The size and number of the neighborhoods do not affect the impact of the attack, as shown in both Figures 13 and 14.

The robust security protocols deployed by `RETINA` during trust establishment, notably including remote attestation, demonstrated efficacy in the timely detection and identification of malicious smart meters within the network. Upon such detection, `RETINA` promptly initiated recovery mechanisms, effectively mitigating any attempted price manipulation. These recovery processes were autonomously executed within the `RETINA` system, obviating the need for external assistance or intervention. These experimental outcomes underscore `RETINA`'s proficiency in neutralizing market manipulation attacks, thereby preserving the integrity and stability of the energy trading market, even when confronted with advanced zero-day vulnerabilities.

6. Security Analysis

The subsequent security analysis primarily identifies potential attack scenarios that may arise due to the innovative characteristics inherent in the described architecture. The aim is to assess the system's vulnerability to security threats and devise appropriate mitigation measures. By comprehensively examining the security landscape, it becomes possible to enhance the robustness and resilience of the architecture, ensuring the protection of critical resources and maintaining the integrity of the overall system.

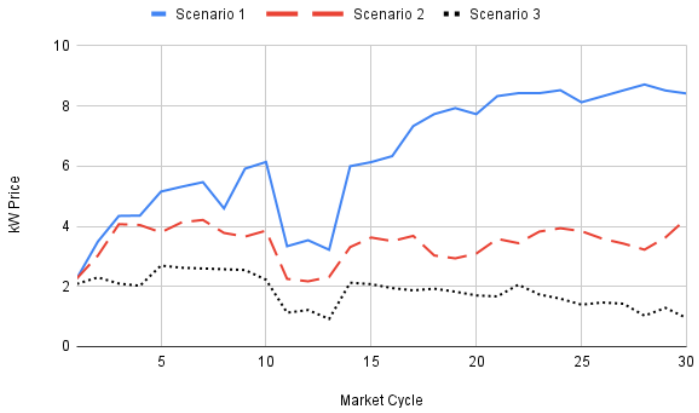

Figure 13: kW price chart – Market manipulation attempt in Network configuration 1

6.1. DoS Attacks

The functionality of `RETINA` heavily relies on the empowered nodes, particularly regarding blockchain operations. While the network operates in a distributed manner without a single point of failure, a coordinated attack targeting these specific nodes could potentially disrupt the entire network. However, robust mitigation measures have been implemented, including establishing trust relationships among entities independent of empowered nodes. In the event of such an attack, the most trusted node(s) within the affected neighborhood would assume an elevated role, temporarily replacing the compromised empowered node. This ensures the continuity of network operations and growth, as demonstrated in the performance evaluation, even in a worst-case scenario. The system's resilience safeguards against potential disruptions and underscores the effectiveness of the implemented mechanisms in addressing security concerns.

6.2. Energy Trading Privacy

The privacy of information stored on the ledgers is an inherent characteristic of the permissioned blockchain employed by `RETINA`. This ensures that entities not participating in the network cannot access the associated data. However, it is essential to acknowledge the possibility of a node being compromised and maliciously exploited to leak information outside the smart grid ecosystem. If such a scenario occurs, indicating a failure of the remote attestation procedure, measures are in place to anonymize the stored

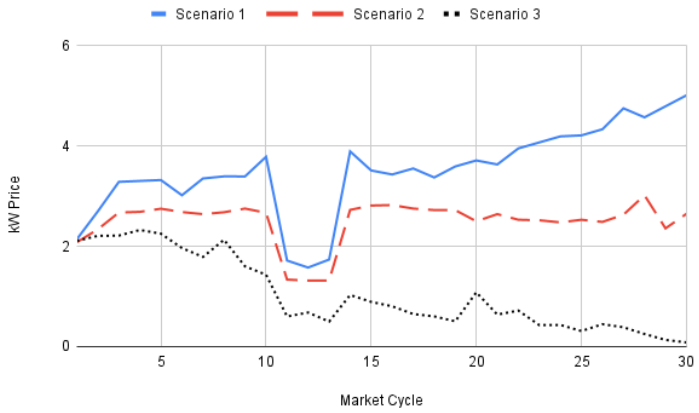

Figure 14: kW price chart – Market manipulation attempt in Network configuration 2

information using the Pk/Sk pairs possessed by each node through the utilization of TEE. This ensures that external parties cannot obtain readable and usable information unless they are part of the network. Specifically, while the provider can match a node ID to a specific smart meter or empowered node, readable and usable information remains inaccessible to external entities, preserving the data's privacy.

6.3. Attack of the Clones

Like the well-known 51% attack and the Byzantine problem, the proof of authority consensus mechanism can be vulnerable [29] if there is an insufficient number of nodes available to validate transactions relative to the network's size. However, this vulnerability can be effectively mitigated by ensuring an adequate number of empowered nodes within the network. Additionally, including seemingly ordinary nodes that are prepared to assume authoritative responsibilities in the event of a security incident or compromise of an empowered node further strengthens the system's resilience. By maintaining a sufficient number of empowered nodes and establishing contingency plans with backup nodes, the potential risks associated with the proof of authority consensus mechanism can be effectively addressed, bolstering the overall security and stability of the network.

6.4. Energy Trading Manipulation

The electricity offered within the energy trading mechanism can be regarded as a tradable commodity, accompanied by various associated risks.

One such risk involves the potential for exploiting price differentials by purchasing inexpensive electricity during the night and selling it at a higher price during the day. However, several factors contribute to the unlikelihood of such an attack materializing:

Continuous Production of New kW: Prosumers continuously generating new electricity mitigates the probability of experiencing a shortage on the grid. This ongoing production ensures a relatively stable supply, reducing the feasibility of manipulating prices through artificial scarcity.

Price Adaptation: In response to an increase in demand, whether during the day or night, the pricing mechanism within the energy trading system adapts accordingly. This dynamic adjustment helps balance supply and demand, limiting opportunities for price manipulation.

Optimized Broker Behavior: The system's broker component is designed to learn from the behavior of the energy trading mechanism, enabling it to make informed decisions. By monitoring patterns and identifying nodes that frequently require external assistance for electricity, the broker can anticipate future needs and ensure fulfillment during periods of lower electricity prices.

By considering these factors, the energy trading mechanism mitigates the risks associated with opportunistic trading strategies and promotes a fair and efficient marketplace for electricity exchange.

7. Critical Appraisal

In summary, `RETINA` presents a solution that addresses the challenges outlined in Section 1, offering smart grids the means to overcome these obstacles and unlock their full potential by incorporating an energy trading mechanism. This achievement is made possible by strategically integrating several established and proven technologies and concepts, including blockchain, PKI, and the WoT. By combining these elements, `RETINA` establishes a robust foundation that synergistically complements one another, providing a comprehensive solution for the smart grid domain. However, as shown in Section 4, `RETINA` confronts a limitation in the expeditious establishment of new trust relationships, demonstrating a comparative lack of celerity when contrasted with conventional and WoT-based smart grids.

Nevertheless, by implementing `RETINA`, a notable advancement towards achieving autonomy and independence from centralized solutions within smart

grid ecosystems is realized. While a central authority, represented by the provider, establishes policies and configures the network initially, once normal operations commence, smart grids exhibit self-sovereign characteristics and can autonomously perform fundamental functions. RETINA's blockchain infrastructure addresses the limitations often encountered in related literature that employs similar DL concepts. This innovative solution minimizes operational costs and optimizes utilizing computational resources available within smart meters, leading to enhanced efficiency and improved resource management. The integration of RETINA thus marks a significant milestone in progressing towards fully autonomous smart grid ecosystems.

The scalability is a critical aspect supporting the claim of RETINA's ability to enable fully decentralized smart grid ecosystems. The experiments demonstrate that RETINA-based smart grids can maintain their functionality in a decentralized manner, even with networks comprising at most 500 nodes. Given the nature of smart grids, which involve executing multiple applications such as the energy trading mechanism, constant and frequent communication among nodes is inevitable. Consequently, communication packets are transmitted within short intervals, resulting in an incremental "incubation" time for the network. This inherent characteristic ensures that RETINA can effectively handle the increasing communication demands as the network expands, facilitating the seamless operation of various applications within the smart grid ecosystem. The scalability of RETINA further strengthens its viability and potential for large-scale deployment in real-world smart grid scenarios.

Direct access to collectively produced green energy from smart grid participants holds significant importance for prosumers, liberating them from the limitations of their infrastructures and the provider's capacity to supply electricity. With the implementation of the energy trading mechanism, participants gain access to a vast green energy market, enabling them to buy and sell electricity directly. This arrangement offers substantial financial benefits for all involved parties while contributing to environmental sustainability. By facilitating direct transactions within the smart grid ecosystem, RETINA empowers prosumers to actively participate in the green energy market, fostering a more efficient and environmentally conscious energy consumption landscape.

8. Related Work

The existing body of research on smart grid security is vast, with numerous works exploring various aspects such as user and device authentication, data privacy and confidentiality, and secure communication channels. To provide a comprehensive understanding of the innovations proposed in this article, the related work is discussed in two distinct categories: (*i*) security solutions for smart grids and (*ii*) security solutions specifically designed for energy trading mechanisms. By examining the related work in these categories, this article aims to highlight the novel contributions of the proposed framework in addressing the security challenges of both smart grids and energy trading mechanisms. The discussion of previous research provides valuable insights into the existing state of the art, enabling a clear understanding of the advancements and innovations offered by the proposed solution.

8.1. Smart Grid Security

The following works focus on blockchain technology's authentication and privacy aspects in the context of IoT and smart grids, which are vital for successfully implementing endeavors such as an energy trading mechanism. Yakubov et al. [30] propose an authentication solution that combines an x.509 certificates ecosystem with blockchain technology, covering processes like issuance, validation, and revocation of certificates. However, a drawback of this approach is that if the certificate authority loses access to the blockchain and is excluded from the network, a new certificate authority smart contract must be created, completely restructuring the network's certificates. In contrast, `RETINA` handles the exclusion of central nodes differently, allowing operations to continue based on endorsements among network nodes.

Wang et al. [31] present an anonymous authentication and key management scheme for smart grids utilizing edge computing and blockchain technology. Experimental results demonstrate its efficiency and speed. However, a single point of failure is observed in their solution, where if an edge server goes offline, the corresponding nodes' connection to the blockchain network is disrupted. This issue is not present in `RETINA`, as nodes are independently connected to the blockchain.

Zhang et al. [32] design a decentralized access-control manager that utilizes the *Practical Byzantine Fault Tolerance* (PBFT) consensus algorithm for participant authentication. The network's security relies on the assumption that malicious nodes will not reach a threshold defined by the PBFT's

security requirements, which limits scalability. In contrast, RETINA employs remote attestation based on TEE to exclude malicious nodes from the network rather than tolerating them.

Finally, Bolgouras et al. [33] combine the PKI and WoT concepts into a hybrid solution tailored for microgrids. While innovative and efficient in search speed, this solution falls short compared to RETINA regarding nodes joining and leaving operations. In their approach, when a node goes offline or rejoins the network, a reconstruction of successor nodes where certificates are stored is required, whereas, in RETINA, certificates remain on the DL without any alterations.

By leveraging blockchain technology in RETINA, network security is enhanced through the blockchain's transparency, immutability, and accountability properties. RETINA improves detection of malicious actions by auditing the DL entries and renders a DHT obsolete for information logging purposes.

8.2. Energy Trading

Park et al. [34] and Bosco et al. [35] propose energy trading schemes using the Ethereum blockchain infrastructure. However, the high transaction fees associated with the Ethereum network reduce the financial benefits for potential adopters. In [36] and [37] the authors partially tackle this issue by utilizing IPFS technology along with Ethereum-based smart contracts in order to provide a more secure P2P trading scheme, compared to more traditional solutions. In contrast, RETINA is built on the Hyperledger platform, utilizing a PoA consensus algorithm, which enables transactions without fees.

Aitzhan et al. [38] present a decentralized energy trading system using blockchain technology. The authors emphasize the requirement for multiple signatures to execute a transaction. A transaction must be signed by a predetermined number of participating entities in their scheme before being submitted to the blockchain. In RETINA, entities form trust bonds and do not need to sign numerous transactions constantly.

Regarding payments in energy trading, Aitzhan et al. [38] utilize the Bitcoin system, which relies on the power-hungry *Proof-of-Work* (PoW) consensus algorithm. This protocol is not suitable for resource-constrained IoT devices like smart meters. Similarly, Li et al. [39] suggest an ecosystem where prosumers can trade electricity using the blockchain-based medium of exchange, NRGcoin, which also employs PoW. Although the consensus al-

gorithm is executed on aggregators with enhanced processing power, it still contradicts the principle of energy efficiency.

Gai et al. [40] introduce a solution to ensure consumer-privacy regarding trading habits and patterns on the blockchain. However, this solution relies on a centralized exchange rather than a peer-to-peer bartering process, making it susceptible to a single point of failure risk. All trading activities pass through the Token Bank responsible for the transactions.

In contrast, `RETINA` addresses these challenges by utilizing a decentralized architecture, low-cost transactions, and a PoA consensus algorithm, ensuring energy efficiency, scalability, and resilience against a single point of failure.

9. Conclusion

Smart grids are experiencing rapid global adoption, but there is still considerable room for performance, security, and efficacy improvement. In this context, `RETINA` emerges as a groundbreaking solution that addresses modern smart grids' diverse needs and requirements. By integrating the PKI/WoT architectures with blockchain technology, `RETINA` establishes a resilient infrastructure immune to CA-oriented threats, operating in a decentralized and distributed manner.

The scalability and resilience of `RETINA` were extensively validated through simulations on a virtualized testbed environment of 500 nodes. The results demonstrate that `RETINA` outperforms the Web of Trust scheme, significantly reducing the time required for new nodes to establish trust relationships. Furthermore, even in compromised sections within the grid, `RETINA` ensures uninterrupted network operations, showcasing its robustness. Additionally, this article presents a novel energy trading scheme based on smart contracts, leveraging the established trust between network nodes and adapting electricity prices based on factors such as distance to prosumers and the chosen production method. This secure energy trading mechanism plays a crucial role in unlocking the full potential of renewable energy sources while proving its resilience to market manipulation attacks.

With its comprehensive capabilities, `RETINA` has the potential to set the course for smart grids, providing a solid foundation for implementing intelligent programs with diverse functionalities. As an ongoing research initiative, future work will apply the trust management scheme to a realistic testbed involving an actual use case implementation. Furthermore, `RETINA` will be

enhanced with additional applications beyond energy trading, further cementing its position as a pioneering solution.

Expanding RETINA beyond energy trading presents numerous opportunities for additional applications in the smart grid ecosystem. One potential application is the integration of advanced demand response mechanisms. RETINA could facilitate more dynamic and responsive demand-side management, allowing consumers to actively adjust their energy consumption patterns based on real-time grid conditions and pricing. Another avenue is the incorporation of grid management functionalities, such as fault detection and localization. RETINA's decentralized architecture could enhance the resilience and reliability of the grid by enabling distributed fault detection algorithms, improving the system's ability to promptly identify and respond to disruptions. Furthermore, the platform could support the implementation of decentralized electric vehicle (EV) charging systems, optimizing charging schedules based on grid conditions and individual user preferences. These additional applications showcase the versatility of RETINA in addressing various challenges and advancing the capabilities of smart grid technologies.

In summary, `RETINA` signifies a notable advancement within blockchain-based frameworks for smart grid applications, particularly in energy trading. By addressing current limitations in this specific domain, RETINA contributes significantly to the evolution of smart grid technologies. The platform offers a comprehensive solution tailored to enhance the security, scalability, and energy-awareness aspects of energy trading within smart grids.

Acknowledgements

This research has been partially funded from the European Union's research and innovation programmes under grant agreements No. 824015 (INCOGNITO), No. 101020416 (ERATOSTHENES), and No. 101070214 (TRUSTEE).

References

[1] Farmanbar, M.; Parham, K.; Arild, Ø.; Rong, C. A widespread review of smart grids towards smart cities. *Energies* **2019**, *12*, 4484.

[2] Strielkowski, W.; Streimikiene, D.; Fomina, A.; Semenova, E. Internet of energy (IoE) and high-renewables electricity system market design. *Energies* **2019**, *12*, 4790.

[3] Gunduz, M. Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Computer networks* **2020**, *169*, 107094.

[4] Tkachenko, V.; Kwilinski, A.; Korystin, O.; Svyrydiuk, N.; Tkachenko, I. Assessment of information technologies influence on financial security of economy. *Journal of Security & Sustainability Issues* **2019**, *8*.

[5] Al-Hinai, A.; Alhelou, H. H. A multi-agent system for distribution network restoration in future smart grids. *Energy Reports* **2021**, *7*, 8083–8090.

[6] Lin, X.; Wu, J.; Mumtaz, S.; Garg, S.; Li, J.; Guizani, M. Blockchain-based on-demand computing resource trading in IoV-assisted smart city. *IEEE Transactions on Emerging Topics in Computing* **2020**, *9*, 1373–1385.

[7] Fotis, G.; Dikeakos, C.; Zafeiropoulos, E.; Pappas, S.; Vita, V. Scalability and replicability for smart grid innovation projects and the improvement of renewable energy sources exploitation: the FLEXI-TRANSTORE case. *Energies* **2022**, *15*, 4519.

[8] Golbeck, J. Weaving a Web of Trust. *Science* **2008**, *321*, 1640–1641.

[9] Sirojan, T.; Lu, S.; Phung, B.; Ambikairajah, E. Embedded edge computing for real-time smart meter data analytics. 2019 International Conference on Smart Energy Systems and Technologies (SEST). 2019; pp 1–5.

[10] Abdelshafy, A. M.; Jurasz, J.; Hassan, H.; Mohamed, A. M. Optimized energy management strategy for grid connected double storage (pumped storage-battery) system powered by renewable energy resources. *Energy* **2020**, *192*, 116615.

[11] Venayagamoorthy, G. K. Dynamic, stochastic, computational, and scalable technologies for smart grids. *IEEE Computational Intelligence Magazine* **2011**, *6*, 22–35.

[12] De Angelis, S.; Aniello, L.; Baldoni, R.; Lombardi, F.; Margheri, A.; Sassone, V. PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. **2018**,

[13] Maymounkov, P.; Mazieres, D. Kademlia: A peer-to-peer information system based on the xor metric. International Workshop on Peer-to-Peer Systems. 2002; pp 53–65.

[14] Stoica, I.; Morris, R.; Karger, D.; Kaashoek, M. F.; Balakrishnan, H. Chord: A scalable peer-to-peer lookup service for internet applications. *ACM SIGCOMM computer communication review* **2001**, *31*, 149–160.

[15] Kunzmann, G. Recursive or iterative routing? Hybrid! KiVS Kurzbeiträge und Workshop. 2005; pp 189–192.

[16] Panos, C.; Xenakis, C.; Kotzias, P.; Stavrakakis, I. A specification-based intrusion detection engine for infrastructure-less networks. *Computer Communications* **2014**, *54*, 67–83.

[17] Li, M.; Hu, D.; Lal, C.; Conti, M.; Zhang, Z. Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things. *IEEE Transactions on Industrial Informatics* **2020**, *16*, 6564–6574.

[18] Jindal, A.; Aujla, G. S.; Kumar, N. SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. *Computer Networks* **2019**, *153*, 36–48.

[19] Chaudhary, R.; Jindal, A.; Aujla, G. S.; Aggarwal, S.; Kumar, N.; Choo, K.-K. R. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Computers & Security* **2019**, *85*, 288–299.

[20] Kumari, A.; Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. When blockchain meets smart grid: Secure energy trading in demand response management. *IEEE Network* **2020**, *34*, 299–305.

[21] Aggarwal, S.; Chaudhary, R.; Aujla, G. S.; Jindal, A.; Dua, A.; Kumar, N. Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem. Proceedings of the 1st ACM MobiHoc workshop on networking and cybersecurity for smart cities. 2018; pp 1–6.

[22] Callas, J.; Donnerhacke, L.; Finney, H.; Shaw, D.; Thayer, R. RFC 4880: OpenPGP message format. 2007.

[23] Zimmermann, P. R. *The official PGP user's guide*; MIT press, 1995.

[24] Zhang, D.-g.; Gao, J.-x.; Liu, X.-h.; Zhang, T.; Zhao, D.-x. Novel approach of distributed & adaptive trust metrics for MANET. *Wireless Networks* **2019**, *25*, 3587–3603.

[25] Yang, H.; Yuan, J.; Yao, H.; Yao, Q.; Yu, A.; Zhang, J. Blockchain-based hierarchical trust networking for JointCloud. *IEEE Internet of Things Journal* **2019**, *7*, 1667–1677.

[26] Selvaraj, P.; Srinivasan, V. B. Capture Based Trust Dependence framework for authorized node identification in mobile agent systems. *Measurement: Sensors* **2022**, *24*, 100471.

[27] Halgamuge, M. N. Estimation of the success probability of a malicious attacker on blockchain-based edge network. *Computer Networks* **2022**, *219*, 109402.

[28] Ganesan, A.; Kombaiya, A. K. Predicting Malicious Node Behavior in Wireless Network Using DSR Protocol and Network Metrics. *International journal of computer communication and informatics* **2022**, *4*, 1–10.

[29] Ekparinya, P.; Gramoli, V.; Jourjon, G. The attack of the clones against proof-of-authority. *arXiv preprint arXiv:1902.10244* **2019**,

[30] Yakubov, A.; Shbair, W.; Wallbom, A.; Sanda, D.; others A blockchain-based PKI management framework. The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018. 2018.

[31] Wang, J.; Wu, L.; Choo, K.-K. R.; He, D. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. *IEEE Transactions on Industrial Informatics* **2019**, *16*, 1984–1992.

[32] Zhang, H.; Wang, J.; Ding, Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy* **2019**, *180*, 955–967.

[33] Bolgouras, V.; Ntantogian, C.; Panaousis, E.; Xenakis, C. Distributed key management in microgrids. *IEEE Transactions on Industrial Informatics* **2019**, *16*, 2125–2133.

[34] Park, C. H.; Barlongo, I. M.; Kim, Y. A market place solution for energy transaction on ethereum blockchain. 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). 2019; pp 1–5.

[35] Bosco, F.; Croce, V.; Raveduto, G. Blockchain technology for financial services facilitation in RES investments. 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI). 2018; pp 1–5.

[36] Kumari, A.; Shukla, A.; Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. ET-DeaL: A P2P Smart Contract-based Secure Energy Trading Scheme for Smart Grid Systems. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2020; pp 1051–1056.

[37] Kumari, A.; Chintukumar Sukharamwala, U.; Tanwar, S.; Raboaca, M. S.; Alqahtani, F.; Tolba, A.; Sharma, R.; Aschilean, I.; Mihaltan, T. C. Blockchain-Based Peer-to-Peer Transactive Energy Management Scheme for Smart Grid System. *Sensors* **2022**, *22*.

[38] Aitzhan, N. Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing* **2016**, *15*, 840–852.

[39] Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE transactions on industrial informatics* **2017**, *14*, 3690–3700.

[40] Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Transactions on Industrial Informatics* **2019**, *15*, 3548–3558.