Received 10 March 2025; revised 8 April 2025; accepted 22 May 2025. Date of publication 2 June 2025; date of current version 27 June 2025.

*Digital Object Identifier 10.1109/OJCOMS.2025.3575463*

# Blockchain-Based Model for Secure and Fair Data Provision in Crowdsourced Drone Services

**JUNAID AKRAM [1,2], AWAIS AKRAM [3], VANDANA SHARMA [4] (Senior Member, IEEE), ALI ANAISSI [2], RUTVIJ H. JHAVERI [5] (Senior Member, IEEE), AND PRIYANKA VERMA [6] (Senior Member, IEEE)**

***(Special Issue on Industrial Communication Networks (ICNets) for Industry 5.0)***

[1]Engineering and Technology Department, UNSW College, Kensington, NSW 2033, Australia
[2]School of Computer Science, The University of Sydney, Camperdown, NSW 2008, Australia
[3]School of Computing, Korea Advanced Institute of Science and Technology, Daejeon 34141, South Korea
[4]Computer Science Department, Christ University, Bengaluru 560029, India
[5]Department of Computer Science and Engineering, School of Technology, Pandit Deendayal Energy University, Gandhinagar 382009, India
[6]School of Computer Science, University of Galway, Galway, H91 TK33 Ireland

CORRESPONDING AUTHORS: P. VERMA AND R. H. JHAVERI (e-mail: priyanka.verma@universityofgalway.ie; rutvij.jhaveri@sot.pdpu.ac.in)

**ABSTRACT** Current centralized systems for crowdsourced drone services face problems in maintaining data integrity, fairness in data exchanges, and efficient resource allocation. These issues are critical in applications such as bushfire management, where accurate and timely data are essential. In response, we propose a blockchain-based model that creates a decentralized marketplace for secure data provisioning. In this system, drone operators send real-time environmental data to bushfire management authorities, and the data are recorded on a blockchain to ensure traceability. The model includes a time commitment-based mutually verifiable fairness mechanism to prevent dishonest behavior and to ensure that both data providers and consumers follow the agreed terms. Two new consensus mechanisms, Proof-of-Data Integrity (PoDI) and Proof-of-Service (PoSv), are introduced to confirm data authenticity and service quality. Additionally, a dynamic trust model that combines direct and indirect trust metrics is implemented to further support system reliability. Ethereum smart contracts are used to automate secure payment processing and to enforce transaction rules. This approach addresses the shortcomings of current systems and provides a clear framework for secure and fair data management in emergency response scenarios.

**INDEX TERMS** Crowdsourced drone services, verifiable credentials, access control, interoperability, bushfire management.

## I. INTRODUCTION

THE ADVENT of consumer-grade drones has significantly transformed sectors such as environmental management and emergency services. In particular, drones have shown immense potential in bushfire management, enabling local residents in fire-prone areas to actively contribute to detection and management efforts [1], [2], [3]. By collecting real-time, comprehensive data, drones substantially enhance traditional bushfire management systems, improving situational awareness and accelerating response times [4], [5], [6], [7]. However, the widespread deployment of crowdsourced drone services introduces challenges, especially in ensuring the data integrity and fairness of collected information. Traditional centralized data management systems are inadequate for dynamic and distributed drone operations due to vulnerabilities such as single points of failure, data breaches, and high operational costs [8], [9], [10]. These centralized systems often result in poor quality data and a lack of trust between data providers and consumers, which can impede timely emergency response. Establishing fairness and trust in decentralized networks for data transactions between drone operators (data providers) and bushfire management authorities (data consumers) is complex and necessitates robust solutions.

Bushfire management relies on the timely and accurate relay of data [11], [12], [13]. However, conventional centralized systems hinder effective responses by introducing synchronization delays, susceptibility to breaches, and inconsistent data quality [14], [15], [16]. These issues impair decision-making and obstruct rapid intervention during

critical emergencies. The need for a robust mechanism to ensure data integrity is therefore imperative [17], [18], [19]. Our approach employs a decentralized framework leveraging blockchain technology to verify and record data transactions in real time. This design eliminates the dependence on a central authority, thereby minimizing errors and ensuring that every transaction is both verifiable and immutable. By resolving the inherent limitations of traditional systems, our framework supports swift responses and establishes reliable communication between drone operators and emergency management agencies. This solution offers a precise and secure method for maintaining data accuracy and fairness, ultimately enhancing coordination and improving outcomes in high-risk scenarios. Furthermore, this approach represents a significant improvement over conventional methods and demonstrates clear potential for practical deployment.

A critical component of our framework is the time commitment-based mutually verifiable fairness mechanism, which prevents cheating attacks and ensures adherence to agreed-upon terms [20], [21]. Our approach addresses the question, "How can blockchain technology be used to secure data integrity and ensure fairness in crowdsourced drone data provisioning?" The novelty of our method lies in the integration of two custom consensus mechanisms, Proof of Data Integrity (PoDI) and Proof of Service (PoSv), which provide improved data accuracy and service validation compared to existing methods. Additionally, our framework incorporates a dynamic trust model that combines token deposits with direct and indirect trust measures to align economic incentives with reliable data exchange.

Our system's architecture leverages blockchain technology to ensure accountability in data transactions, reducing operational costs and enhancing resilience against attacks [22], [23]. The immutable nature of blockchain records ensures permanent and tamper-proof data transactions, preserving data integrity [9]. The performance of the proposed model is rigorously evaluated using key metrics such as data integrity, service latency, and transaction fairness. Simulation results indicate significant enhancements in data security and reduced service latency compared to traditional models. The system's scalability is validated through extensive proof-of-concept implementations, demonstrating its applicability to large-scale data collection scenarios in real-world bushfire management.

Furthermore, our framework is versatile and can be applied to other domains such as environmental monitoring, disaster response, urban surveillance, and smart city infrastructures. This broad applicability enhances decision-making processes across diverse applications by providing secure, transparent, and equitable data provisioning. Additionally, the integration of Ethereum smart contracts enhances the trustworthiness and security of the data exchange process, establishing an immutable log of operations essential for dispute resolution and ensuring a fair and transparent exchange of data. This approach addresses operational complexities and incentivizes drone operators to share accurate data, creating a symbiotic relationship between data providers and consumers. Our paper contributes to the discourse on secure and ethical data sharing in drone technology applications, offering a practical solution to the challenges in harnessing crowdsourced drone services for societal and environmental betterment. The key contributions of our work include:

- Propose a novel blockchain-based model for fair data provisioning in crowdsourced drone services, enhancing the reliability, efficiency, and data integrity of data collection in bushfire management.
- Establish a decentralized marketplace using blockchain technology to ensure transparent and immutable data exchanges between drone operators and bushfire management authorities.
- Implement a time commitment-based mutually verifiable fairness mechanism to prevent cheating attacks and ensure adherence to agreed-upon terms, fostering a trustworthy data exchange environment.
- Demonstrate enhanced data security and reduced service latency through innovative consensus mechanisms and extensive proof-of-concept validation, proving the model's applicability to large-scale data collection scenarios.

The paper is organized as follows: Section II reviews existing work on blockchain frameworks for data integrity and fairness in drone services. Section III details the system architecture, including decentralized components, smart contracts, fairness mechanisms, and countermeasures against double-spending. Section IV provides an analysis and discussion of the model's security and efficiency, while Section V concludes with key findings and future research directions.

## II. RELATED WORK

Recent advancements in blockchain technology have significantly impacted the domain of drone services, particularly in ensuring data integrity, security, and fairness in decentralized environments. Various studies have explored innovative frameworks to address these challenges. The Distributed Drone Reputation Management (DDRM) framework leverages the Ethereum blockchain to create a transparent and verifiable review mechanism, enhancing the reliability and efficiency of drone operations by implementing a dual-token system [1]. Similarly, the Decentralized PKI Framework introduces D2XChain, a blockchain-based Public Key Infrastructure (PKI) designed to eliminate the vulnerabilities of centralized trust models, thereby improving the security and reliability of drone communications in spatial crowdsourcing scenarios [8]. Privacy-preserving techniques have also been integrated into drone services, combining blockchain with local differential privacy to ensure fair and secure data exchanges in bushfire management applications [24]. Additionally, the Digital Twin-Driven Trust Management framework, TMIoDT, integrates digital twin technology with blockchain to enhance trust management in IoDT, specifically for bushfire monitoring [25].

The GALTrust framework combines generative adversarial networks (GANs) and type-2 fuzzy logic to manage trust within IoDT, overcoming limitations of traditional machine learning methods in detecting malicious nodes [26]. The DroneSSL framework leverages self-supervised multimodal anomaly detection to enhance data collection and analysis in hazardous environments like bushfires [27].

Further, blockchain-based frameworks have been extensively studied in other IoT contexts. FairShare for Industrial IoT (IIoT) ensures fair, accountable, and secure data exchanges through smart contracts and proxy re-encryption [20]. A secure and fair IoT data trading system with bilateral authorization emphasizes the use of smart contracts to guarantee non-repudiation and fairness in data trading [28]. A fair and privacy-preserving data trading scheme incorporates attribute-based credentials, encryption, and zero-knowledge proofs [29]. A blockchain-based labeled training dataset supply system addresses transparency and fairness issues in crowdsourcing [30]. Studies like BC-IoDT [31] and a blockchain-based IoT data marketplace [32] further illustrate the transformative potential of blockchain and advanced cryptographic techniques in revolutionizing data management across various domains. Collectively, these studies underscore the transformative potential of blockchain and advanced cryptographic techniques in revolutionizing data management across various domains, laying a strong foundation for our proposed model.

## III. METHODOLOGY

The proposed blockchain-based model for fair data provisioning in crowdsourced drone services is designed to address challenges of data integrity, fairness, and efficient resource allocation in bushfire management. Our methodology introduces a novel integration of customized consensus mechanisms with a mutually verifiable fairness protocol that systematically aligns economic incentives with data accuracy and resource optimization. This innovative approach is embedded within a decentralized blockchain framework and further reinforced by the automated enforcement capabilities of Ethereum smart contracts. This section provides a comprehensive description of the system architecture, consensus mechanisms, mutual verifiable fairness mechanism, and the integration of Ethereum smart contracts.

### A. SYSTEM MODEL

The architecture of the proposed decentralized system is schematically represented in Figure 1, illustrating the integration of key components designed to optimize data provision in emergency scenarios, specifically for bushfire management. This model is not limited to bushfire scenarios but is applicable to a broad range of real-time data monitoring applications, enhancing its general applicability across various fields.

- *Drone Operators (Data Providers):* Equipped with sensor-laden drones, these operators collect essential environmental data. For consistency, the terms "drone operators" and "data providers" are used interchangeably throughout this study. Each drone, functioning autonomously, gathers critical metrics such as temperature, humidity, and real-time imagery, crucial for monitoring dynamic and hazardous environments.
- *Bushfire Management Authorities (Data Consumers):* Entities responsible for emergency response utilize the data for strategic planning and effective response coordination. The system's flexibility allows adaptation to different data consumer types, broadening the scope beyond bushfire management to include other forms of environmental monitoring.
- *Decentralized Marketplace:* At the core of the system is a blockchain-based platform facilitating secure and transparent data transactions between providers and consumers. This marketplace supports a scalable model for data trading, enhancing the system's utility across varied operational scales.
- *Blockchain Network:* Serving as the infrastructure backbone, the blockchain provides a secure, decentralized ledger that chronologically and immutably records all transactions, thereby ensuring data integrity and non-repudiation.
- *Smart Contracts:* Implemented on the Ethereum platform, these contracts autonomously execute transaction protocols, ensuring compliance with predefined terms and conditions, thus minimizing the reliance on trust between parties.

Data acquisition begins with drone operators deploying drones into designated areas prone to bushfires. The drones perform on-site data processing to enhance data quality by filtering out irrelevant information, ensuring that only pertinent data is transmitted to the marketplace. This preprocessing step is crucial for maintaining high data integrity and reducing the computational load on the system.

The blockchain secures all data transactions, ensuring transparency and immutability. Each transaction is recorded on the blockchain, providing an incontrovertible log of all data exchanges. The network employs a dual-consensus mechanism to validate transactions and enforce system integrity:

- *Proof-of-Data Integrity (PoDI):* This mechanism certifies the authenticity of data by validating cryptographic hashes of the data entries against corresponding hashes stored on the blockchain, ensuring that data remains unaltered post-submission.
- *Proof-of-Service (PoSv):* It confirms that the data collection service was executed as stipulated by validating the metadata against the expected service parameters, thus ensuring compliance with service terms.

An integral aspect of this model is the mutual verifiable fairness mechanism anchored on time commitments, which enhances trust and accountability by ensuring adherence to agreed terms:

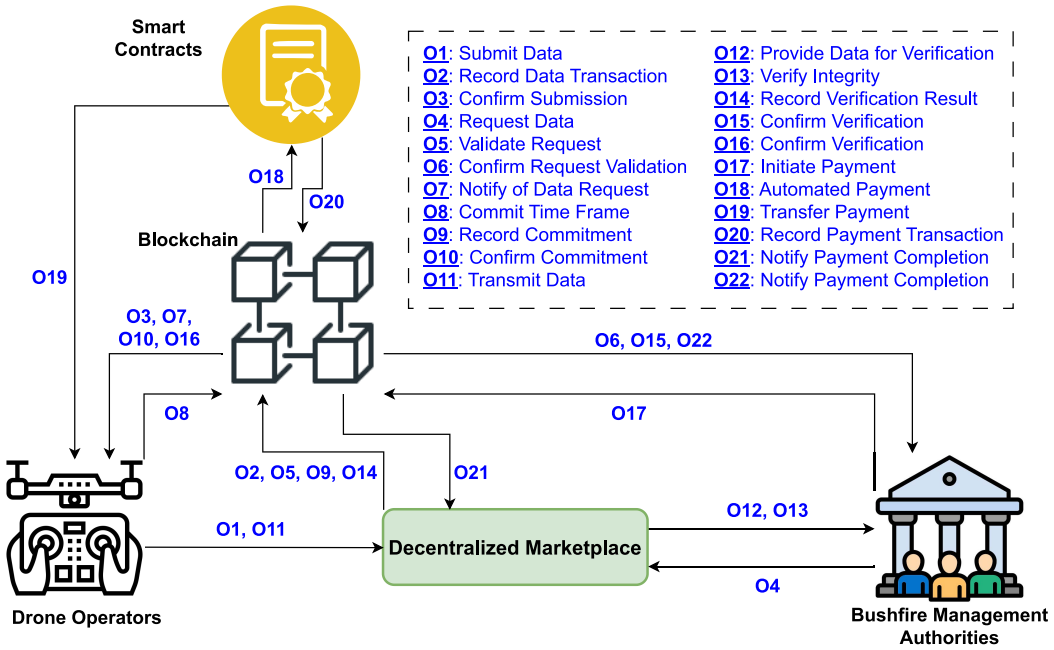


**FIGURE 1.** Illustrative depiction of the proposed system architecture, highlighting component interactions and data flow pathways.

- *Time Commitment and Verification:* Data providers commit to a specific timeframe for data availability, within which consumers verify the data's relevance and integrity. This mechanism ensures that data transactions are executed within agreed temporal bounds.
- *Dispute Resolution Mechanism:* Leveraging immutable transaction logs stored on the blockchain, the system provides a robust framework for resolving disputes, underpinned by evidence embedded within the transaction records.

Ethereum-based smart contracts facilitate automated enforcement of transaction terms, including:

- *Automated Payments:* These contracts ensure timely compensation for drone operators once their data is verified, thus promoting a reliable and continuous data supply.
- *Immutable Records and Dispute Resolution:* They maintain a permanent and unalterable record of all transactions, providing a reliable foundation for resolving disputes based on transparent and verifiable data logs.

This system model not only addresses the specific needs of bushfire management but also offers a robust framework adaptable to various real-time data-intensive applications, ensuring scalability, security, and operational efficiency.

### B. SYSTEM INITIALIZATION

The initialization phase of the proposed decentralized system meticulously incorporates state-of-the-art cryptographic algorithms to ensure robust security and privacy, paramount in environments susceptible to adversarial attacks. This phase is critical as it establishes the foundation for secure and trustworthy interactions throughout the system.

- *Cryptographic Algorithms for Anonymity and Integrity:* The system utilizes the SHA-256 hashing algorithm for its proven collision resistance and security, ensuring data integrity and consistency. Additionally, the Boneh–Boyen short signature scheme is employed for its efficiency in generating and verifying signatures. This scheme is particularly suited for environments where bandwidth and storage space are at a premium, providing strong security guarantees while maintaining minimal signature size.
- *Registration and Certificate Issuance:* All participants, including drone operators and entities within the decentralized marketplace, are required to register with a trusted certificate authority (CA). During registration, the CA conducts a rigorous authentication process to verify the identity of each participant. Upon successful authentication, the CA issues digital certificates, which serve as immutable and non-repudiable identifiers for the participants within the blockchain network. These certificates encapsulate the registered information, binding it cryptographically to ensure that any alterations to the participant's information can be detected and traced.
- *Wallet Address Assignment:* Post-registration, each drone operator is assigned a unique wallet address by the certificate authority. These addresses facilitate the secure and anonymous transfer of digital assets and data within the blockchain network, enabling participants to engage in transactions while preserving their privacy.
- *Hybrid Encryption Technique:* To enhance security against information tampering and unauthorized access, the system adopts a hybrid encryption approach, *AES-128+RSA*. This method combines the rapid encryption

capabilities of AES-128 with the robust key management properties of RSA. AES-128 encrypts the bulk of the data at high speeds with strong security, while RSA encrypts the AES key itself, providing an additional layer of security known as key encapsulation. This dual-layer encryption mechanism significantly mitigates risks associated with single encryption methods, particularly in scenarios vulnerable to advanced persistent threats.

This initialization strategy not only secures the system against a range of cyber threats but also ensures that all transactions and communications within the network are conducted with verifiable authenticity and confidentiality. The robust cryptographic framework supports a scalable and secure infrastructure for real-time data exchanges, critical for systems requiring high integrity and availability. Through this meticulous approach, the system provides a secure environment that upholds the principles of confidentiality, integrity, and availability, crucial for the reliable operation of decentralized networks in dynamic and potentially hostile operational landscapes.

### C. REQUEST AND RESPONSE OF DATA PROTOCOL

This subsection delineates the systematic procedure for data requests and responses within our decentralized data exchange framework, focusing on ensuring transactional integrity, preventing malicious activities, and optimizing response strategies through blockchain technology.

#### 1) DATA REQUEST PROTOCOL

The initiation of the data exchange process occurs when a consumer, such as a bushfire management authority, transmits a data request to the decentralized marketplace. This request explicitly specifies the geographical coordinates and the type of data required, ensuring that only pertinent information is solicited, thus optimizing network resources and response times.

- *Commitment Token:* To mitigate the risk of malicious participation, the request includes a commitment token—a cryptographic deposit—held in escrow by the blockchain network. This token acts as a security deposit that is forfeited in the event of fraudulent activities by the requester, thereby economically disincentivizing deceitful actions and enhancing the overall trustworthiness of the network.
- *Data Encryption and Transmission:* The data request is encrypted using the latest public key of the marketplace, ensuring confidentiality and data integrity during transit. This encryption prevents unauthorized access and ensures that only the intended recipients within the marketplace can decrypt and process the request.
- *Blockchain Verification:* Upon receipt, the marketplace conducts a preliminary verification of the data request's authenticity and completeness by broadcasting it to the blockchain network. This step leverages the distributed nature of the blockchain to achieve consensus on the validity of the request before processing it further.

#### 2) DATA RESPONSE MECHANISM

Following the validation of the data request, drone operators equipped with the requested data capabilities are notified. The response mechanism is designed to ensure timely and secure delivery of data to the consumer.

- *Commitment Token by Drone Operators:* Drone operators interested in fulfilling the request must deposit a commitment token onto the blockchain similar to the consumer's initial deposit. This token is a safeguard that binds the operator to complete the transaction faithfully, under the threat of losing the deposit if the data provided is found to be fraudulent or the service is not rendered as agreed.
- *Encrypted Data Transmission:* Responding drone operators encrypt their data submissions using the marketplace's current public key. This step ensures that sensitive data remains secure and only accessible to authorized parties within the marketplace.
- *Marketplace Data Handling:* The marketplace acts as a mediator, decrypting and conducting a secondary verification of the received data against the original request parameters. Validated data is then securely transmitted to the consumer.
- *Provider Selection Protocol:* If multiple drone operators respond to a request, the marketplace employs a first-come-first-served protocol, selecting the first operator that meets the request criteria and completes the required token deposit. This protocol is designed to incentivize quick and efficient responses from drone operators.

### D. FAIRNESS MECHANISMS IN DATA PROVISIONING

The proposed model systematically enforces fairness in data provisioning through a robust framework built on timed commitments and economic incentives. This approach, adapted from recent advancements in blockchain research [33], ensures equitable treatment of both data providers and consumers by leveraging blockchain technology to manage transactions and dispute resolutions effectively.

- *Commitment Tokens and Economic Incentives:* Both data providers and consumers are required to deposit commitment tokens prior to engaging in any data transactions. These tokens serve as a financial guarantee to enforce strict compliance with the pre-established transaction terms. They are acquired via a predefined issuance mechanism during system registration or as rewards for active participation, with allocations determined by factors such as prior reputation, expected participation levels, and verified identity metrics. The tokens are distributed using a transparent smart contract algorithm that ensures equitable allocation and records all token-related events on the blockchain. Upon the initiation of a transaction, the tokens are securely held in escrow through a multi-signature wallet mechanism, which requires mutual confirmation by the involved

parties. In the event of non-compliance, such as failure to deliver the promised data or to complete the agreed payment, the tokens are subject to forfeiture. The forfeited tokens are then reallocated as compensation to the aggrieved party, according to a predefined penalty rate and slashing parameters. Furthermore, additional parameters such as a minimum deposit threshold, token lock-up period, and dispute resolution window are established to govern the commitment tokens, thereby ensuring that the economic incentives and disincentives are rigorously enforced.

- *Transaction Process and Proof of Payment:* Upon receipt of data, the consumer is obligated to transfer the agreed payment to the provider. Simultaneously, a proof of payment must be sent to the marketplace to confirm the transaction. The provider, upon receiving payment, issues a data exchange bill to the consumer, which details the volume of data transferred and the precise timing of the transaction, ensuring transparency and verifiability.
- *Blockchain Validation and Consensus Protocols:* The decentralized marketplace, along with designated blockchain validators, oversees every data transaction. These validators execute consensus protocols to ensure the integrity and authenticity of each transaction. This decentralized validation mechanism enhances the security and fairness of the data exchange process.
- *Dispute Resolution Mechanism:* In the event of a dispute, the blockchain framework facilitates an equitable resolution process: - *Consumer Complaints*: If a consumer files a complaint regarding non-receipt of data, the provider is required to present the data exchange bill as evidence. Failure to provide this bill is considered indicative of provider fraud. - *Provider Complaints*: Conversely, if a provider raises a complaint concerning non-payment, the consumer must furnish proof of payment. Absence of such proof signifies consumer deception.
- *Reputation System and Enforcement:* The outcomes of these disputes affect the reputation scores of the participants. Negative ratings result from proven dishonesty, decreasing the participant's reputation within the network. Conversely, adherence to protocol and positive transaction outcomes contribute to positive ratings. A user whose reputation falls below a critical threshold is automatically banned and removed from the system, thereby maintaining the integrity and trustworthiness of the marketplace.

This enhanced fairness mechanism not only mitigates the risks associated with asymmetric information and potential fraud but also instills a higher degree of trust among participants by providing a transparent, secure, and responsive framework for managing disputes and enforcing transaction terms. The integration of advanced cryptographic techniques and blockchain-based consensus ensures that all parties engage in data transactions with assured fairness and accountability, thereby fostering a reliable and efficient marketplace for data exchange.

### E. DOUBLE SPENDING ATTACK

This subsection rigorously defines the probabilistic models underpinning the assessment of double spending attacks within the blockchain network. These models quantify the dynamics of blockchain progression under adversarial conditions using three key parameters: the Potential Progress Function ($P$), the Catch-up Function ($C$), and the Double Spending Probability ($DS$).

- *Progress Function* ($P$): Represents the expected branch length an attacker could potentially achieve. It quantifies the adversary's capability to progress within the blockchain, factoring in their computational power and the rate at which they can mine fraudulent blocks.
- *Catch-up Function* ($C$): Measures the likelihood that an attacker, starting from a given disadvantage, can surpass the blockchain length established by honest nodes. This function is vital for assessing the security resilience against an attacker catching up or overtaking the honest chain.
- *Double Spending Probability* ($DS$): Synthesizes the outputs of $C$ and $P$ to evaluate the overall risk of a successful double spending attack. This metric incorporates the attacker's computational resources, required blockchain confirmations, and any temporal advantage they may hold.

**Mathematical Formulation:**

- $C(q, z)$: Probability that the attacker's blockchain surpasses the honest blockchain given an initial disadvantage of $z$ blocks.
- $P(q, m, n, t)$: Probability that within a timeframe $\tau$, the honest network mines $m$ blocks while the adversary mines $n$ blocks, leveraging a computational advantage $q$ and time $t$.
- $DS(q, K, n, t)$: Calculates the likelihood of a double spending attack succeeding, given the adversary's hash power $q$, and the number of confirmations $K$ required for a transaction.

Using the probabilistic framework described in [34], the Potential Progress Function $P$ is articulated as:

$$P(q, m, n, t) = \sum_{z=0}^{n} a(q, t, n) P_R(q, m, n - z) \tag{1}$$

where

$$a(q, t, n) = \begin{cases} 1 & \text{if } t = 0 \text{ and } n = 0 \\ 0 & \text{if } t \leq 0 \\ \frac{(qt)^n}{n!} e^{-qt} & \text{otherwise} \end{cases} \tag{2}$$

The function $a(q, t, n)$ models the likelihood of mining $n$ blocks within $t$ seconds given the adversary's hash power $q$.

$$P_R(q, m, n) = \begin{cases} 1 & \text{if } m = 0 \text{ and } n = 0 \\ \binom{m+n-1}{n} q^n (1 - q)^m & \text{otherwise} \end{cases} \tag{3}$$

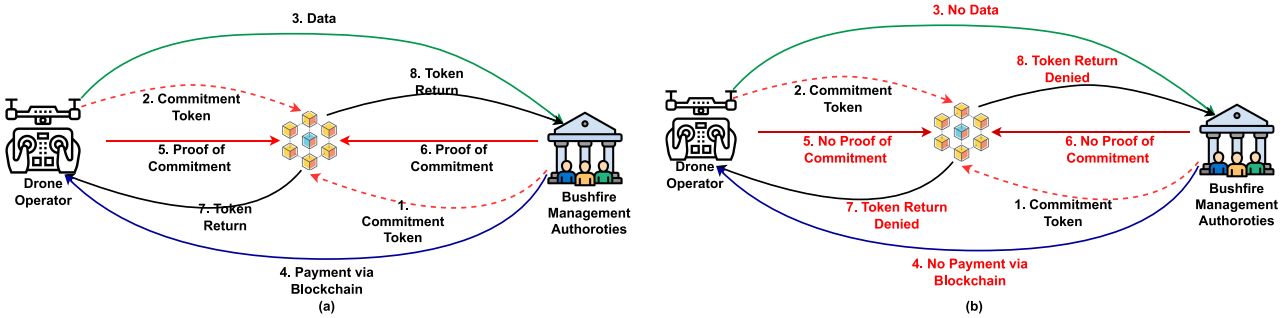


**FIGURE 2.** Illustrative scenarios of data provisioning free from malicious actions and affected by malicious actions, demonstrating the robustness of the fairness mechanism.

The function $P_R(q, m, n)$ assesses the probability that an attacker successfully mines $n$ blocks before the honest nodes mine $m$ blocks.

The integrated probability of a successful double spending attack, $DS$, is then expressed as:

$$\mathrm{DS}(q, K, n, t) = 1 - \sum_{z=0}^{K-n} P(q, K, z, t)(1 - C(q, K - n - z)) \tag{4}$$

$$C(q, z) = \begin{cases} \frac{q}{p}(z+1) & \text{if } q < 0.5 \text{ and } z > 0 \\ 1 & \text{otherwise} \end{cases} \tag{5}$$

where $p = 1-q$ is the probability of the honest nodes finding the next block.

This formulation provides a comprehensive quantitative framework for evaluating the security measures necessary to mitigate the risks posed by potential double spending attacks within blockchain networks.

### F. CONSENSUS MECHANISMS

Consensus mechanisms are integral to ensuring the reliability, integrity, and fairness of blockchain systems. Traditional consensus protocols such as Proof of Work (PoW) [35] are highly resource-intensive, leading to excessive energy consumption and computational costs. Proof of Stake (PoS) [36] was introduced as an alternative to address these inefficiencies; however, PoSv retains certain limitations, including reliance on significant computational resources and potential centralization risks.

To overcome these challenges, we propose two novel consensus mechanisms: Proof of Data Integrity (PoDI) and Proof of Service (PoSv). These mechanisms are designed to achieve efficient validator selection while minimizing gas consumption and reducing the overall computational burden. Both protocols integrate reputation-based systems to ensure that validators with higher integrity and consistent service are prioritized, addressing concerns of fairness and trustworthiness in decentralized networks.

#### 1) PROOF OF DATA INTEGRITY (PODI)

The PoDI protocol ensures that data shared by drone operators is accurate, tamper-proof, and reliable. This is achieved by requiring drone operators to generate cryptographic hashes of their data, which are stored immutably on the blockchain. Validators are selected based on their historical data integrity and reputation, ensuring that only trusted participants contribute to the validation process. In addition, the PoDI mechanism continuously verifies data integrity by recalculating the cryptographic hash of each data submission upon every transaction and comparing it with the corresponding hash stored on the blockchain. Any discrepancy triggers an immediate alert, thus preventing acceptance of tampered or corrupted data. The protocol also employs redundant hash computations and cross-validation among multiple validators to reinforce the reliability of the data verification process.

Let $J = \{1, 2, 3, \ldots, n\}$ represent the set of drone operators in the system. The integrity and service patterns are denoted as $D = \{D_1, D_2, \ldots, D_n\}$ and $S = \{S_1, S_2, \ldots, S_n\}$, respectively. The reputation score for each operator is represented by $R$, a dynamic value updated based on past performance.

The data integrity function $\mathrm{PV}_{di}$ for each drone operator is defined as:

$$\mathrm{PV}_{di} = R \log\left(\frac{1}{\exp^{(S_i - D_i)}}\right) \tag{6}$$

Here:

- $D_i$: Represents the integrity of the data submitted by the drone operator.
- $S_i$: Indicates the validation of the service provided by the drone operator.
- $R$: The reputation score, reflecting historical performance and trustworthiness.

The likelihood of a drone operator being selected as a validator is then given by:

$$\mathrm{Ch}_{win_{di}} = \frac{\mathrm{PV}_{di}}{\sum_{k \in J} \mathrm{PV}_{dk}} \tag{7}$$

#### 2) PROOF OF SERVICE (POSV)

The PoSv mechanism focuses on validating the geospatial and temporal metadata of the data collected by drone operators to ensure it adheres to the expected parameters. This protocol evaluates the consistency and responsiveness

of service delivery, particularly during peak operational hours when efficient validation is critical. Specifically, the PoSv mechanism mandates that each data submission include precise time-stamped and location-tagged metadata. Validators then perform rigorous consistency checks by comparing this metadata against predefined service parameters and, when available, external trusted data sources. Statistical analysis and spatial correlation techniques are employed to assess the accuracy and reliability of the reported metadata, thereby confirming that the service delivered meets the requisite operational standards.

The service function $\mathrm{PV}_{si}$ for each drone operator is defined as:

$$\mathrm{PV}_{si} = R(D_i - \theta \times S_i) \tag{8}$$

The parameter $\theta$, referred to as the winning factor, is calculated to dynamically adjust for peak and off-peak hours:

$$\theta = 1 - \frac{(\rho - \rho_{off})}{\rho} \tag{9}$$

where:

- $\rho$: Service validation rate during peak hours.
- $\rho_{off}$: Service validation rate during off-peak hours.

The likelihood of a drone operator being chosen as a validator is expressed as:

$$\mathrm{Ch}_{win_{si}} = \frac{\mathrm{PV}_{si}}{\sum_{k \in J} \mathrm{PV}_{sk}} \tag{10}$$

#### 3) INTEGRATION AND BENEFITS OF PODI AND POSV

The integration of PoDI and PoSv addresses critical challenges in decentralized validation:

- *Efficiency:* By prioritizing operators with higher data integrity and service reliability, the mechanisms reduce the need for redundant validations, thereby optimizing computational resource usage.
- *Scalability:* The reputation-based selection process enhances scalability by minimizing unnecessary validations and focusing on high-value contributors.
- *Fairness:* Dynamic adjustments for peak and off-peak periods ensure equitable participation among operators with varying resource capabilities.
- *Security:* The cryptographic hashing employed in PoDI, combined with the rigorous geospatial and temporal validation processes in PoSv, mitigates risks associated with data tampering, fraudulent reporting, and inconsistent service delivery.

These novel consensus mechanisms represent a significant advancement in blockchain-based systems, providing a robust framework for achieving trust, efficiency, and security in decentralized data provisioning networks.

### G. TRUST MODEL

The trust model implemented in this decentralized data provisioning framework is designed to guarantee the reliability and integrity of all participating entities. This model adeptly integrates both direct and indirect trust assessments, each playing a pivotal role in establishing comprehensive trustworthiness across the network. Furthermore, our framework incorporates advanced trust computation algorithms that iteratively update trust scores based on Bayesian inference and exponential decay, ensuring that recent interactions are weighted more heavily in the decision-making process.

#### 1) DIRECT AND INDIRECT TRUST

- *Direct Trust:* Generated through firsthand interactions between entities within the data provisioning system. Each drone operator (data provider) and bushfire management authority (data consumer) accumulates a trust score reflecting their historical performance in transactions. This direct trust metric is calculated based on the outcomes of their engagements, where positive experiences increase trust scores and negative experiences decrease them.
- *Indirect Trust:* Composed of trust ratings aggregated from third-party feedback within the network. This form of trust is derived from the collective endorsements or criticisms provided by other participants regarding an entity's reliability and ethical conduct in previous transactions.

The decentralization of trust management enables unbiased collection and processing of these ratings, ensuring transparency and fairness in trust assessments. The integration of direct and indirect trust methodologies leverages the strengths of both approaches, providing a robust measure of trustworthiness that captures a wide spectrum of interactions.

#### 2) TOKEN DEPOSIT SYSTEM

To enhance the effectiveness of the trust model, a token deposit system is introduced. This system acts as a financial assurance, where users deposit tokens that may be forfeited in cases of dishonest or fraudulent activities. The presence of a financial stake adds a layer of security and incentivizes adherence to network rules, significantly enhancing trustworthiness.

$$R = \mathrm{Tr}_{r,w} = \beta(\alpha R_d + (1-\alpha)R_i) + \gamma d \tag{11}$$

$$R_d = \frac{P_r + 1}{P_r + N_r + 2} \tag{12}$$

$$R_i = \frac{\sum_{k=1}^{K} W_i(k) \times R_d(k)}{\sum_{k=1}^{K} W_i(k)} \tag{13}$$

Here, $R_d$ denotes the direct trust computed from personal transaction history, where $P_r$ and $N_r$ are the counts of positive and negative interactions, respectively. $R_i$ represents the indirect trust, calculated as a weighted average of trust scores from other network participants. The weight function $W_i(k)$ is defined as $e^{-\omega(P_r+N_r)}$, emphasizing recent interactions more significantly than older ones.

#### 3) TRUST SCORE UPDATE MECHANISM

The overall trust value $\mathrm{Tr}_{r,w}$ for user $w$ by user $r$ includes:

- $\alpha$ and $(1-\alpha)$: Coefficients balancing the influence of direct versus indirect trust.
- $\beta$ and $\gamma$: Parameters adjusting the sensitivity of the trust score to the token deposit and the combined trust from direct and indirect sources.
- $d$: Represents the token deposit's influence on the trust score, reinforcing the financial commitment to network integrity.

The normalization condition $\beta + \alpha + \gamma = 1$ ensures that the contributions of direct trust, indirect trust, and token deposits are proportionately balanced to sum to unity. The trust score update algorithm employs an iterative process where new transaction data is incorporated in real time, and trust scores are recalculated using a weighted average of previous scores and the latest performance metrics. This updated trust information is then integrated into decision-making processes, influencing validator selection in consensus mechanisms and triggering punitive actions if trust scores fall below predetermined thresholds.

This comprehensive trust model significantly contributes to the security and efficiency of the decentralized system by rigorously evaluating and incentivizing the integrity and reliability of all participants.

## IV. ANALYSIS AND DISCUSSION

In this section, we analyze the proposed blockchain-based model for fair data provisioning in crowdsourced drone services. Simulations were conducted using Python on a system with 16 GB RAM and an Intel Core i7-10750H CPU @ 2.60GHz running Windows 10. Metrics such as proof of value, computational cost, and double spending attack probability were used to assess the model's efficiency and security. The model's robustness was evaluated against double spending attacks using Python 3, and a prototype was developed on an Ethereum framework with Solidity smart contracts, tested with tools like Truffle and Ganache, and managed via Web3.py. Cryptographic operations leveraged PyCryptodome for AES and RSA algorithms, ensuring data integrity and secure communications.

### A. FORMAL SECURITY ANALYSIS

To ensure the robustness and reliability of the proposed blockchain-based model for fair data provisioning in crowdsourced drone services, we conducted a formal security analysis using Alloy Analyzer [37]. This formal analysis is critical as it provides rigorous, mathematically grounded assurance that the system satisfies its intended security properties under adversarial conditions, thereby reducing reliance on empirical testing alone.

Firstly, we examined the property of *Data Integrity*. This property ensures that all data submitted by drone operators remains unchanged during transmission and storage. Formally, for any data $D$ submitted by a drone operator, if $D$ is accepted by the blockchain, then $D$ must remain unchanged. This is expressed as:

$$\begin{aligned} &\forall D \in \text{Data}, \text{submit}(D) \Rightarrow \text{verify}(D) \wedge \text{store}(D) \\ &\Rightarrow D = D_{\text{original}} \end{aligned} \tag{14}$$

Specifically, this property relies on the collision resistance of the employed cryptographic hash functions and the immutability of the blockchain, ensuring that any modification of the data results in a detectable hash mismatch.

Secondly, we verified the *Proof of Value (PoV)* property. This property ensures that the PoV of drone operators accurately reflects their reputation and contribution to the network. For any drone operator $O$ with reputation $R$ and PoV, the calculated PoV should increase with higher reputation and valid data submissions. This is formalized as:

$$\begin{aligned} &\forall O \in \text{Operators}, \\ &\forall R \in \text{Reputation}, \\ &\forall \text{Data}_{\text{valid}} \in \text{Data}, (\text{submit}(O, \text{Data}_{\text{valid}}) \\ &\Rightarrow \text{increase}(\text{PoV}(O))) \wedge (\text{PoV}(O) \propto R) \end{aligned} \tag{15}$$

This property is essential for aligning operator rewards with their historical performance, thereby fostering trust and deterring manipulative behavior through a quantitatively robust incentive mechanism.

Thirdly, we assessed the property of *Fairness in Data Provisioning*. This property ensures that data consumers receive data in a fair and unbiased manner. Formally, for any data request Req made by a consumer, the allocation of data should be fair and unbiased, expressed as:

$$\begin{aligned} &\forall \text{Req} \in \text{Requests}, \\ &\forall \text{Consumer}_i, \text{Consumer}_j \in \text{Consumers}, \\ &\big(\text{request}(\text{Consumer}_i, \text{Req}) \wedge \text{request}(\text{Consumer}_j, \text{Req})\big) \\ &\Rightarrow \text{allocate\_fair}(\text{Req}) \end{aligned} \tag{16}$$

The formal specification of this property models the allocation algorithm and verifies that the mechanism distributes data equitably among consumers regardless of extraneous factors, thus preventing any form of preferential treatment.

The property of *Double Spending Attack Resistance* was also analyzed. This property ensures that the system resists double spending attacks effectively. For any transaction $T$ and any adversary $A$, the probability of a successful double spending attack should be negligible, as shown by:

$$\begin{aligned} &\forall T \in \text{Transactions}, \\ &\forall A \in \text{Adversaries}, \\ &\text{attempt\_double\_spend}(A, T) \Rightarrow \text{prob}(\text{success}) \approx 0 \end{aligned} \tag{17}$$

This property is verified through formal probabilistic models that simulate adversarial behavior, thereby ensuring that the likelihood of a successful double spending attack remains statistically insignificant under realistic network conditions.

Additionally, we verified the property of *Consensus Validity*. This property ensures that only valid transactions

are included in the blockchain. Formally, for any transaction $T$ included in the blockchain, $T$ must be valid as per the consensus rules, expressed as:

$$\forall T \in \text{Transactions}, \ \text{included}(T, \text{blockchain}) \Rightarrow \text{valid}(T) \tag{18}$$

The formal analysis confirms that any deviation from consensus rules is automatically rejected by the system, thus maintaining the overall integrity of the blockchain ledger.

Furthermore, we examined the property of *Incentive Compatibility*. This property ensures that the incentive mechanism makes honest behavior more rewarding than dishonest behavior. For any drone operator $O$, the reward $R$ for honest data submission should be higher than any potential gain from dishonest actions, formalized as:

$$\forall O \in \text{Operators}, \ \text{honest}(O) \Rightarrow R_{\text{honest}} > R_{\text{dishonest}} \tag{19}$$

This property is critical for ensuring that rational participants are naturally incentivized to maintain honest behavior. The formal model quantitatively compares the rewards and penalties, demonstrating that the economic structure of the system inherently discourages fraudulent actions.

The *Non-Repudiation* property was also verified. This property ensures that once a data transaction is recorded, neither the drone operator nor the data consumer can deny the transaction. For any transaction $T$ recorded in the blockchain, both parties $P$ cannot repudiate the transaction, expressed as:

$$\begin{aligned} &\forall T \in \text{Transactions}, \\ &\forall P \in \{\text{Operator}, \text{Consumer}\}, \\ &\text{recorded}(T, \text{blockchain}) \Rightarrow \neg\text{repudiate}(P, T) \end{aligned} \tag{20}$$

The formal verification of non-repudiation leverages digital signatures and the immutable ledger to ensure that all transactions are permanently linked to the involved parties, thereby establishing clear accountability.

Finally, we verified the property of *Privacy Preservation*. This property ensures that the identities of drone operators and data consumers remain confidential unless explicitly revealed. For any participant $P$, their identity $ID$ should remain private, expressed as:

$$\forall P \in \text{Participants}, \ \text{identity}(P) = ID \Rightarrow \text{private}(ID) \tag{21}$$

The formal analysis of privacy preservation incorporates robust anonymization and encryption techniques, ensuring that sensitive identity information is securely protected, even in the presence of colluding adversaries.

These properties were rigorously tested and validated using the Alloy Analyzer [37], ensuring that the proposed model meets the required standards of security, fairness, and efficiency. The significance of this formal analysis lies in its ability to provide a comprehensive, mathematically verifiable assurance that the system's security mechanisms function as intended, thereby establishing a strong foundation for deploying the model in real-world, adversarial environments.

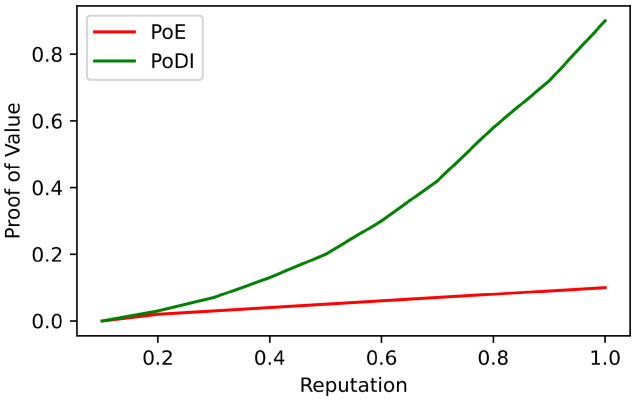


**FIGURE 3.** Comparison of PoDI with PoE.

### B. PERFORMANCE ANALYSIS

To quantitatively assess the efficiency and effectiveness of the proposed Proof-of-Data Integrity (PoDI) mechanism, we conduct a comparative performance analysis against the existing Proof-of-Energy (PoE) mechanism, as detailed in [38]. The performance metrics focus on the Proof of Value (PoV), which is a crucial indicator of the system's ability to incentivize and validate accurate data submissions from drone operators. In this study, we extend our evaluation by incorporating additional parameters including latency, throughput, and computational complexity. Detailed benchmarking experiments were conducted under controlled conditions to compare the PoDI mechanism with PoE, thereby ensuring that our evaluation encompasses both quantitative improvements and practical feasibility for real-world deployments. The analysis rigorously accounts for variations in operator reputation, transaction volumes, and network conditions.

Figure 3 illustrates the performance of PoDI relative to PoE across varying levels of operator reputation. At a reputation level of 0.5, the PoDI mechanism achieves a PoV of 0.2, which is markedly higher than the 0.05 PoV observed for the PoE mechanism. This substantial improvement demonstrates the enhanced capability of PoDI to foster reliable and trustworthy data submissions by drone operators. The refined validation processes in PoDI incorporate rigorous cryptographic verification and an advanced reputation-based scoring system, effectively correlating data integrity with operator reputation to significantly enhance overall system reliability.

In addition to PoV, computational efficiency is another critical metric for evaluating the feasibility of blockchain mechanisms, particularly in contexts where resource constraints are prevalent. Figure 4 presents a detailed comparative analysis of computational costs for the proposed model versus two existing benchmarks, Benchmark 1 [34] and Benchmark 2 [33]. The proposed model demonstrates the lowest computational cost, consuming only 34 computational units, compared to 36 and 37 units for Benchmark 1 and Benchmark 2, respectively. This reduction in computational

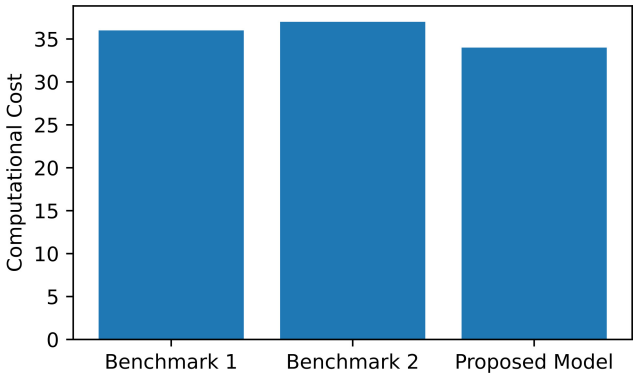


FIGURE 4. Overall comparison of models based on computational cost.

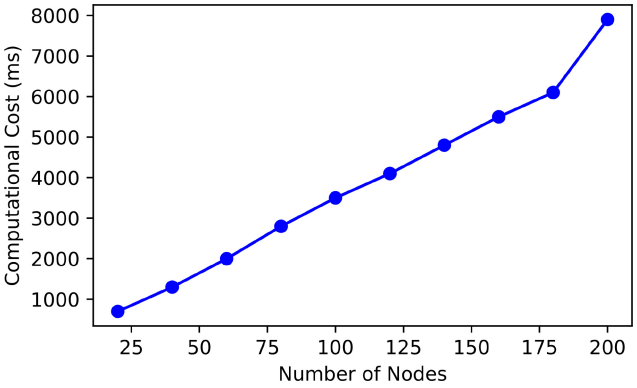


FIGURE 5. Effect of node count on computing costs.

cost is primarily due to the optimized algorithms within the PoDI mechanism, which streamline the data verification process by eliminating redundant computations while maintaining robust security. The decreased computational overhead directly contributes to enhanced scalability and lower operational costs, making the proposed model well-suited for large-scale applications.

Overall, the performance analysis underscores the superiority of the PoDI-based model in both incentivizing high-quality data submissions and minimizing computational overhead. The efficiency improvements not only reduce operational costs but also enable the system to process larger datasets and more complex transactions with reduced resource expenditure. Additionally, evaluations of system throughput and latency under varying network conditions confirm that the proposed model maintains high performance even under heavy transaction loads. The empirical results, derived from rigorous simulations and experimental benchmarks, substantiate the claim that the proposed enhancements significantly improve upon existing blockchain mechanisms, indicating a strong potential for adoption in practical, real-world applications.

### C. IMPACT OF NODE COUNT ON COMPUTATIONAL COST

In assessing the scalability and efficiency of the proposed blockchain model for data provisioning, we analyze the relationship between computational cost and the number of network nodes. Understanding this relationship is critical for determining the model's ability to accommodate network expansion without significantly compromising performance. Figure 5 delineates the computational costs associated with varying node counts within our data provisioning model. It reveals that although computational cost inherently increases with the number of nodes, the growth rate exhibits a sub-linear trend. For instance, at a node count of 200, the computational cost is quantified at 7900 ms, showcasing the model's scalability and efficiency in managing larger networks.

The proposed model leverages an optimized Proof-of-Data Integrity (PoDI) mechanism, which is significantly less computationally intensive than traditional Proof-of-Work (PoW) systems. This optimization in the consensus process substantially reduces the computational load across the network, mitigating the increase in costs typically associated with higher node counts. The model employs advanced communication protocols designed to minimize overhead by ensuring that only necessary data is transmitted across the network. This approach reduces bandwidth usage and alleviates potential delays, contributing to lower computational costs even as the network scales. The system incorporates strategic load balancing to distribute processing tasks evenly among nodes, particularly during peak operational periods. This distribution helps maintain system performance and prevents any single node from becoming a bottleneck, thus supporting a stable and responsive network environment.

The data illustrated in Figure 5 serves as empirical evidence supporting the theoretical benefits of the proposed blockchain architecture. The curve's gentle slope, as node numbers increase, affirms the system's capability to scale effectively. This attribute is essential for applications that may require dynamic scaling based on operational demands or growth scenarios. The performance analysis clearly demonstrates that the proposed model not only supports scalability in terms of node count but also does so with only marginal increases in computational costs. This capability is crucial for blockchain applications destined for operation in diverse and potentially large-scale network environments, highlighting the model's suitability for widespread adoption in industries that demand robust, scalable blockchain solutions.

### D. DOUBLE SPENDING ATTACK ANALYSIS

Understanding the dynamics of double spending attacks within blockchain networks is critical for designing systems that are robust against such vulnerabilities. In our analysis, we adopt a comprehensive quantitative framework to model the probability of double spending attacks by incorporating key network parameters such as computational power (denoted by $q$), block advantage, and the number of transaction confirmations. This rigorous approach enables

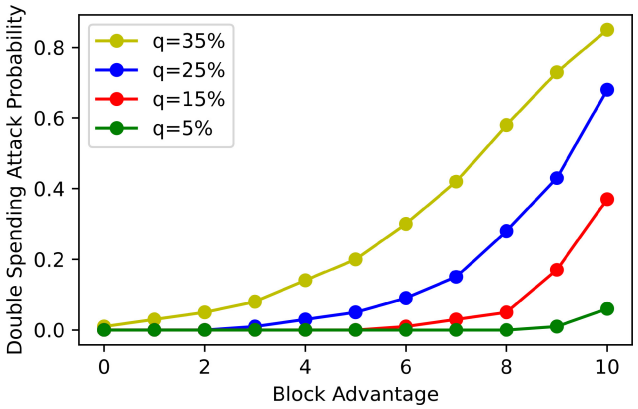


**FIGURE 6.** Double spending attack probability versus block advantage.

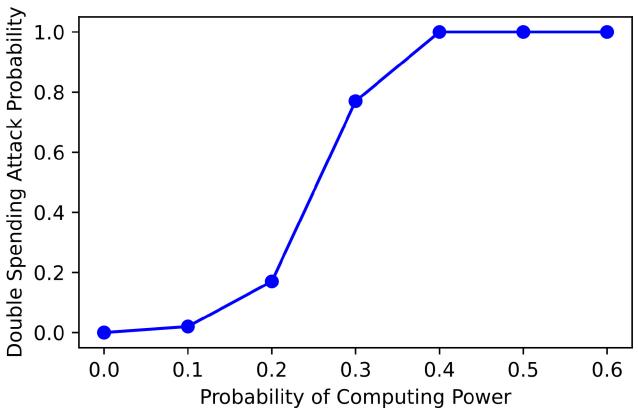


**FIGURE 7.** Attack likelihood of double spending versus computational power.

a deeper insight into the adversarial conditions that can compromise blockchain security.

This analysis presents a detailed exploration of how varying network parameters affect the probability of a successful double spending attack. We model the attacker's ability to extend a fraudulent chain in competition with the honest network using probabilistic methods that account for the stochastic nature of block generation and mining competition. This model explicitly quantifies the relationship between the attacker's computational resources and the resultant risk of a successful attack.

Figure 6 provides a quantitative assessment of the relationship between block advantage and attack probability. Block advantage is defined as the number of blocks by which the honest network is ahead of the attacker's fraudulent chain. Our experimental results indicate that a higher block advantage substantially reduces the probability of a successful double spending attack; however, this protective effect is significantly modulated by the attacker's computational power. For example, at a computational power of 35%, the attack probability increases to approximately 0.85 when the block advantage is 10 blocks, while lower computational powers yield markedly lower probabilities. This observation emphasizes the critical importance of maintaining a robust block advantage as a deterrent to adversarial activities.

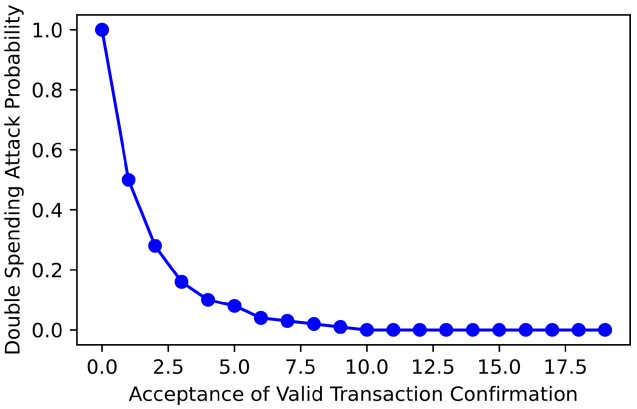


**FIGURE 8.** Comparative analysis of double spending attack probability and valid transaction confirmation likelihood.

The curve in Figure 7 charts the escalation in attack probability as a function of computational power. Our analysis reveals an exponential increase in the risk of double spending as the attacker's computational power increases. Specifically, when the computational power is 30% ($q = 0.3$), the likelihood of a successful double spending attack is approximately 0.77; this probability reaches unity (1.0) as $q$ approaches 0.4. This exponential trend underscores the severe security risks posed by adversaries with substantial computational resources and highlights the need for adaptive security measures that scale with the evolving computational capabilities of potential attackers.

Figure 8 investigates the effect of transaction confirmations on the probability of a double spending attack. In this context, each confirmation represents an additional block appended to the blockchain after a transaction is recorded, thereby increasing the computational work required for an attacker to reverse the transaction. Our findings demonstrate that with five confirmations, the probability of a successful attack drops to approximately 0.08, and with ten confirmations, the probability becomes virtually negligible. This analysis quantitatively confirms that multiple transaction confirmations serve as an effective defense mechanism by exponentially increasing the difficulty of reversing confirmed transactions.

In summary, these detailed analyses provide critical insights into the parameters that influence the security of blockchain systems against double spending attacks. By rigorously quantifying the effects of computational power, block advantage, and transaction confirmations, our study offers a comprehensive understanding of the adversarial landscape. This knowledge is essential for the design and implementation of enhanced security protocols that ensure the overall robustness, reliability, and trustworthiness of blockchain networks in practical, real-world applications.

## V. CONCLUSION

This paper introduced a blockchain-based framework designed to address the challenges of data integrity, fairness, and efficiency in crowdsourced drone services for

emergency management, specifically bushfire response. The proposed model replaces vulnerable centralized systems with a decentralized blockchain marketplace, ensuring secure, transparent, and tamper-proof data transactions. Key contributions include novel consensus mechanisms, namely Proof-of-Data Integrity (PoDI) and Proof-of-Service (PoSv), which significantly enhance data authenticity and operational reliability. A dynamic trust model integrating both direct and indirect trust metrics, along with automated Ethereum smart contracts, further improves the fairness and accountability of the system. Through rigorous formal security analysis and experimental evaluation, the results demonstrate considerable improvements over existing approaches in terms of security, computational efficiency, scalability, and fairness. Despite these advancements, our study acknowledges potential limitations, such as increased computational overhead in densely populated networks or scenarios requiring extremely rapid transaction processing. Nonetheless, the overall findings confirm the model's effectiveness for reliable and secure data provisioning.

Future research will focus on further optimizing the proposed consensus mechanisms to minimize computational overhead and improve scalability in diverse network environments. Additionally, real-world pilot studies in various emergency management contexts, such as urban disaster response or large-scale environmental monitoring, will be conducted to validate and refine system performance. Finally, enhancing the trust model to include adaptive algorithms capable of responding dynamically to changes in participant behavior and network conditions represents another promising direction, ensuring sustained reliability and fairness in long-term deployments.

## REFERENCES


[1] J. Akram and A. Anaissi, "DDRM: Distributed drone reputation management for trust and reliability in crowdsourced drone services," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, 2024, pp. 921–931.

[2] J. Akram and A. Anaissi, "A blockchain-enhanced framework for privacy and data integrity in Crowdsourced drone services," in *Proc. 22nd Int. Conf. Service-Oriented Comput.*, 2024, pp. 1–8.

[3] H. S. Munawar, Z. Gharineiat, and S. I. Khan, "A framework for burnt area mapping and evacuation problem using aerial imagery analysis," *Fire*, vol. 5, no. 4, p. 122, 2022.

[4] S. Malik, S. Ansari, H. Rizvi, D. Kim, and R. Hasnain, "Intelligent target coverage in wireless sensor networks with adaptive sensors," in *Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Fall)*, 2020, pp. 1–5.

[5] S. Sidana and D. Kumar, "Leveraging blockchain-as-a-certificate authority for authentication in 6G-enabled spatial crowdsourcing drone services," in *Proc. IEEE 100th Veh. Technol. Conf. (VTC-Fall)*, 2024, pp. 1–5.

[6] J. Akram, M. Aamir, R. Raut, A. Anaissi, R. H. Jhaveri, and A. Akram, "AI-generated content-as-a-service in IoMT-based smart homes: Personalizing patient care with human digital twins," *IEEE Trans. Consum. Electron.*, early access, Jun. 3, 2024, doi: 10.1109/TCE.2024.3409173.

[7] Y. Wu, Y. Ji, S. Lee, and A. Braytee, "Simplified swarm learning framework for robust and scalable diagnostic services in cancer histopathology," in *Proc. Comput. Sci.*, 2025, pp. 1–12.

[8] J. Akram and A. Anaissi, "Decentralized PKI framework for data integrity in spatial crowdsourcing drone services," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, 2024, pp. 643–653.

[9] J. Akram, A. Anaissi, A. Akram, R. S. Rathore, and R. H. Jhaveri, "Adversarial label-flipping attack and defense for anomaly detection in spatial crowdsourcing UAV services," *IEEE Trans. Consum. Electron.*, early access, Aug. 23, 2024, doi: 10.1109/TCE.2024.3448541.

[10] A. Akram, J. Akram, A. Alabdultif, A. Anaissi, and R. H. Jhaveri, "Secure and interoperable IoMT-based smart homes," *IEEE Consum. Electron. Mag.*, early access, Jan. 27, 2025, doi: 10.1109/MCE.2025.3534442.

[11] M. Shahmohammad, M. M. Salamattalab, W. Sohn, M. Kouhizadeh, and N. Aghamohmmadi, "Opportunities and obstacles of blockchain use in pursuit of sustainable development goal 11: A systematic scoping review," *Sustain. Cities Soc.*, vol. 112, Oct. 2024, Art. no. 105620.

[12] J. Akram, W. Hussain, R. H. Jhaveri, R. S. Rathore, and A. Anaissi, "Dynamic GNN-based multimodal anomaly detection for spatial crowdsourcing drone services," *Digit. Commun. Netw.*, to be published.

[13] Z. Zhang et al., "Enhancing trusted synchronization in open production logistics: A platform framework integrating blockchain and digital twin under social manufacturing," *Adv. Eng. Inform.*, vol. 61, Aug. 2024, Art. no. 102404.

[14] A. S. Ahanger, F. S. Masoodi, A. Khanam, and W. Ashraf, "Managing and securing information storage in the Internet of Things," in *Internet of Things Vulnerabilities and Recovery Strategies*. Boca Raton, FL, USA: Auerbach Publications, 2024, pp. 102–151.

[15] J. Poorvi, A. Kalita, and M. Gurusamy, "Reliable and efficient data collection in UAV based IoT networks," *IEEE Commun. Surveys Tuts.*, early access, Mar. 11, 2025, doi: 10.1109/COMST.2025.3550274.

[16] P. Narsimhulu, R. Sahay, and P. Chithaluru, "Optimal transportation system based on adaptive federated learning techniques for healthcare IoV (HIoV)," *Unmanned Aircr. Syst.*, vol. 2024, pp. 563–608, Dec. 2024.

[17] S. Javaid, R. A. Khalil, N. Saeed, B. He, and M.-S. Alouini, "Leveraging large language models for integrated satellite-aerial-terrestrial networks: Recent advances and future directions," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 399–432, 2025.

[18] V. Pathak, K. Singh, T. Khan, M. Shariq, S. A. Chaudhry, and A. K. Das, "A secure and lightweight trust evaluation model for enhancing decision-making in resource-constrained industrial WSNs," *Sci. Rep.*, vol. 14, no. 1, 2024, Art. no. 28162.

[19] B. S. Bari, D. Puthal, and K. Yelamarthi, "Datasets in vehicular communication systems: A review of current trends and future prospects," *SN Comput. Sci.*, vol. 6, no. 3, pp. 1–25, 2025.

[20] J. Sengupta, S. Ruj, and S. Das Bit, "FairShare: Blockchain enabled fair, accountable and secure data sharing for industrial IoT," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 3, pp. 2929–2941, Sep. 2023.

[21] Y. Djenouri and P. Ingle, "Capability-based multi-tenant access management in crowdsourced drone services," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2025, pp. 1–6.

[22] J. Akram, M. Umair, R. H. Jhaveri, M. N. Riaz, and H. Chi, "Chained-drones: Blockchain-based privacy-preserving framework for secure and intelligent service provisioning in Internet of Drone things," *Comput. Elect. Eng.*, vol. 110, Sep. 2023, Art. no. 108772.

[23] S. I. Khan, F. Ullah, and B. J. Choi, "Drone-as-a-service (DaaS) for COVID-19 self-testing kits delivery in smart healthcare setups: A technological perspective," *ICT Exp.*, vol. 9, no. 4, pp. 748–753, Aug. 2023.

[24] J. Akram and A. Anaissi, "Privacy-first crowdsourcing: Blockchain and local differential privacy in crowdsourced drone services," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, 2024, pp. 1412–1414.

[25] R. S. Rathore, R. H. Jhaveri, and A. Akram, "Digital twin-driven trust management in open RAN-based spatial crowdsourcing drone services," *IEEE Trans. Green Commun. Netw.*, vol. 8, no. 2, pp. 841–855, Sep. 2024.

[26] R. S. Rathore, R. H. Jhaveri, and A. Akram, "GALTrust: Generative adverserial learning-based framework for trust management in spatial crowdsourcing drone services," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 2285–2296, Aug. 2024.

[27] J. Akram, A. Anaissi, W. Othman, A. Alabdulatif, and A. Akram, "DroneSSL: Self-supervised multimodal anomaly detection in Internet of Drone Things," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 4287–4298, Feb. 2024.

[28] Y. Park, M. H. Jeon, and S. U. Shin, "Blockchain-based secure and fair IoT data trading system with bilateral authorization," *Comput., Mater. Continua*, vol. 76, no. 2, p. 1871, 2023.

[29] L. Xue, J. Ni, D. Liu, X. Lin, and X. Shen, "Blockchain-based fair and fine-grained data trading with privacy preservation," *IEEE Trans. Comput.*, vol. 72, no. 9, pp. 2440–2453, Sep. 2023.

[30] H. Xu, Z. He, and D. Lan, "Revolutionizing machine learning: Blockchain-based crowdsourcing for transparent and fair labeled datasets supply," *Future Gener. Comput. Syst.*, vol. 161, pp. 106–118, Dec. 2024.

[31] M. Alazab and H. Chi, "BC-IoDT: Blockchain-based framework for authentication in Internet of Drone things," in *Proc. 5th Int. ACM Mobicom Workshop Drone Assist. Wireless Commun. 5G Beyond*, 2022, pp. 115–120.

[32] M. Sober, G. Scaffino, S. Schulte, and S. S. Kanhere, "A blockchain-based IoT data marketplace," *Clust. Comput.*, vol. 26, no. 6, pp. 3523–3545, 2023.

[33] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6564–6574, Oct. 2020.

[34] C. Pinzón and C. Rocha, "Double-spend attack models with time advantange for bitcoin," *Electron. Notes Theor. Comput. Sci.*, vol. 329, pp. 79–103, 2016.

[35] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3620–3631, Jun. 2019.

[36] M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain-based mechanisms for local energy trading in smart grids," in *Proc. IEEE 16th Int. Conf. Smart Cities Improving Qual. Life Using ICT IoT AI (HONET-ICT)*, 2019, pp. 110–114.

[37] D. Jackson, "Alloy: A language and tool for exploring software designs," *Commun. ACM*, vol. 62, no. 9, pp. 66–76, 2019.

[38] A. S. Yahaya, N. Javaid, M. U. Javed, A. Almogren, and A. Radwan, "Blockchain-based secure energy trading with mutual verifiable fairness in a smart community," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 7412–7422, Nov. 2022.