frontiers | Frontiers in Blockchain

TYPE Original Research
PUBLISHED 13 January 2025
DOI 10.3389/fbloc.2024.1481339

Blockchain oracles for decentralized agricultural insurance using trusted IoT data

Manoj T[1], Krishnamoorthi Makkithaya[1]*, Narendra V. G.[1]* and Vijaya Murari T[2]

[1]Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India, [2]Department of Computer Science and Engineering, NMAM Institute of Technology (NMAMIT), Nitte (Deemed to Be University), Udupi, Karnataka, India

OPEN ACCESS

EDITED BY
Paolo Bottoni,
Sapienza University of Rome, Italy

REVIEWED BY
Remo Pareschi,
University of Molise, Italy
Paolo Buono,
University of Bari Aldo Moro, Italy

*CORRESPONDENCE
Krishnamoorthi Makkithaya,
✉ k.moorthi@manipal
Narendra V. G.,
✉ narendra.vg@manipal.edu

RECEIVED 15 August 2024
ACCEPTED 09 December 2024
PUBLISHED 13 January 2025

CITATION
T Manoj, Makkithaya K, V. G. Narendra and T Vijaya Murari (2025) Blockchain oracles for decentralized agricultural insurance using trusted IoT data.
Front. Blockchain 7:1481339.
doi: 10.3389/fbloc.2024.1481339

Agricultural insurance is one of the formal and reliable risk management instruments to cope with agrarian risks. Presently, agricultural insurance products rely heavily on centralized systems that lack transparency and traceability, leading to suboptimal risk assessment and delays in payouts. To address these concerns the fintech industry has started to embrace a popular decentralized technology called blockchain. However, blockchain operates as a deterministic and synchronized state system, which means it cannot directly access real-world data for decentralized applications. A mechanism called oracle is required for the trusted access of agricultural risk factor data to smart contracts from external sources such as Internet of Things (IoT) devices, web services and databases. Hence, the present study proposes a blockchain-based AgriInsureDON framework with a privacy-preserving decentralized oracle for risk factor data access from trusted IoT devices for agricultural insurance. Initially, a method for computing the direct reputation score of IoT devices based on behavioral and data reputation is illustrated. Next, a privacy preserved decentralized oracle mechanism is designed and implemented using a masked secret sharing and secure aggregation scheme. Later, we demonstrate the working of weather-indexed insurance contracts based on decentralized oracle. Finally, a performance analysis of smart contract transactions w.r.t average latency, throughput, average CPU utilization and total memory usage is conducted on Ganache and Sepolia test networks. The evaluation results of privacy-protected decentralized oracle and an indexed insurance contract within AgriInsureDON framework confirms that transactions are efficient and scalable to meet the requirements of expedited claim settlement.

KEYWORDS

agricultural insurance, blockchain, Ethereum, IoT, oracles, smart contracts

1 Introduction

Agriculture plays the predominant role in satisfying the food security and sustainable development of the economy. In the past few decades, the increased occurrences of climate change have adversely impacted agricultural production, reversing the progress made in eradicating poverty and hunger (Van Wassenaer et al., 2021). Most of the risks having the detrimental effects on agriculture emerge from the climate disasters like floods, droughts, cyclones, forest fires, earthquakes or from wild animals' damage, insect or pest infestation, soil conditions, etc. The risks arising from a variety of sources cause significant income losses, sometimes resulting in loss of life among farmers in developing countries (International Institute for Environment and Development, 2023). The high-impact risks caused by the natural calamities will have long-term ramifications whereas low-impact risks due to weather fluctuations, crop diseases or soil conditions, exhibit short-term effects on the crop production (Lyubchich et al., 2019). In 2022, the total economic losses caused by natural disasters worldwide amount upto USD 224 billion (Centre for Research on the Epidemiology of Disasters, 2022). The participation of all stakeholders in the agri-value chain is essential to effectively tackle the challenges posed by rising agricultural risks. This can be achieved by adopting a range of techniques at the farm level, from informal practices to formal financial instruments such as agricultural insurance. However, despite sustained efforts by governments to publicize formal agricultural insurance, it has not gained widespread adoption among resource-constrained farmers in less developed countries (Rajeev and Nagendran, 2023). This can be primarily attributed to two main reasons. Firstly, from the farmers' perspective, a lack of transparency, high premium costs, delays in payout and low financial literacy contribute to a low adoption rate. Secondly, insurers face challenges in developing high-quality and low-premium insurance products due to a lack of trustworthy risk data and issues of information asymmetry.

Agricultural insurances vary depending upon how the risk assessment is conducted and payout is initiated. The traditional indemnity-based insurance covers the exact losses incurred by farmers. Nevertheless, indemnity-based schemes pose financial challenges for insurers due to issues of asymmetric information and high transaction costs (Just et al., 1999). As alternative, index-based insurance products have emerged, offering protection to farmers against specific risk events, with payouts determined based on predefined indices such as crop yield or weather variables. The index-based insurances can be categorized into yield-indexed and weather-indexed schemes based on type of index generalization (Greatrex et al., 2015). Crop insurers adopt different approaches to collect, store, process and disseminate the weather attributes, crop yield parameters and soil data required for risk assessment in index-based insurance. For yield-indexed insurance, to estimate average crop yield most of the countries still practice and conduct Crop Cutting Experiments (CCEs). Even though CCEs helps to validate the crop yield and assists policy planning, it is manual and labour intensive process with a high chance of human errors and data falsification (Kosmowski et al., 2021). The combination of digital technologies like remote sensing, field-based crop imaging with statistical methods can provide the unbiased crop yield assessment and thereby design better yield indexed insurance schemes (Aggarwal et al., 2016). Since weather-indexed insurance does not necessitate crop yield estimation at farm level, losses can be assessed by integrating *in situ* field measurements with remotely sensed data for climatic events. Recently, with increased adoption of precision agricultural practices combined with Internet of Things (IoT) has simplified the automated monitoring and collection of field data (plant-soil-atmosphere) that can be used for assessment in weather-indexed insurance (Chamara et al., 2022).

Presently, most of the agricultural digital platforms created with the synergy of IoT devices and cloud storage are highly centralized. This centralization makes them vulnerable to a single point of failure and results in fragmented data silos leading to information asymmetry (Dey and Shekhawat, 2021). Furthermore, the recognition of stakeholders' involvement in agricultural insurance within a centralized architecture results in a lack of transparency, integrity, and data provenance. This also gives rise to numerous security and privacy concerns. Blockchain technology helps to address the issues of centralized systems by combining the cryptographic solutions with decentralized systems. It enhances transparency within a distributed stakeholder environment, such as agricultural insurance framework, by creating an immutable record of transactions in a distributed ledger without any intermediary. However, blockchain operates as an isolated and deterministic state system, where smart contracts are unable to independently access real-world data like weather, soil, and crop management data from off-chain resources (Beniiche, 2020). An oracle serves as the interface connecting external data sources, including IoT devices, web services, external databases, and decentralized storage systems, to on-chain smart contracts. Oracles play a crucial role in authenticating, verifying, and validating the trustworthiness of the data before relaying it to smart contracts. This study proposes an AgriInsureDON framework for decentralized agricultural insurance with privacy-preserved decentralized oracle using trusted risk factor data from IoT devices. The framework utilizes reputation scores to ensure the reliability of the data sources. The collected data is then fed into blockchain-based agricultural insurance smart contracts for risk assessment. The major contributions of this research work are given as follows:

1. We describe the method for direct reputation score computation of IoT edge devices based on their behavioral and data reputation.
2. We design and implement the direct reputation score-based decentralized oracle utilizing masked secret sharing and secure aggregation scheme.
3. We develop and demonstrate the working of weather-indexed agriculture insurance smart contracts for risk assessment using decentralized oracle.
4. We conduct a detailed performance analysis of deployed smart contracts w.r.t average latency, throughput, average CPU utilization and total memory usage.

The remainder of the article is organized into following sections: Section 2 elaborates on the background for the research study, with a subsection dedicated to preliminaries followed by a subsection on related work conducted in the field. Section 3 provides a comprehensive overview of the AgriInsureDON framework and provides a detailed description of methods employed for direct reputation score of IoT edge devices and privacy-preserved decentralized oracle for secure access of risk factor data. Section 4 elucidates required experimental setup. Section 5 presents implementation details, results along with performance and security analysis of implemented schemes. Section 6 concludes the research study by offering future scope of work.

2 Background

2.1 Preliminaries

2.1.1 Blockchain oracles

Blockchain is a distributed ledger technology that has gained significant momentum in various domains, driven by the successful transaction of the cryptocurrency Bitcoin and the addition of programming capabilities. It forms a decentralized and distributed network that records the timestamped transaction data into blocks and appends it to immutable ledger based on the consensus of participating peers Ismail and Materwala (2019). The features of blockchain such as transparency, immutability, traceability, and disintermediation, establish it as a foundational platform for decentralized finance applications Kar and Navin (2021). Smart contracts are the set of self-executing instructions defined within the application layer of a blockchain. They serve as mutually agreed digital contracts between transacting entities, eliminating the need for trusted third parties. These contracts are triggered automatically when predetermined conditions are met, enabling the seamless digital transfer of assets. However, the application of smart contracts to real-world scenarios often involves accessing data from external sources and results be sent to the outside world. For example, consider a smart contract deployed for crop insurance between a Farmer and Insurer that requests real-time rainfall value from off-chain weather resources and triggers the payout based on the loss incurred. A blockchain operates in an isolated and self-contained environment that requires all its participating nodes in a synchronized state for a transaction to be successful. As a result the states of real-world data is not directly accessible by smart contracts (CSIRO Data61 Group, 2021). This can be effectively addressed by an entity or service called oracle that validates and fetches data off the blockchain and relays it to smart contracts for use.

The design and implementation of blockchain oracles can be realized through a variety of approaches. From a high-level perspective, an oracle can be defined as either a pure off-chain entity or a combination of off-chain and on-chain components. The design considerations for oracles encompass their intended purpose, functionalities, and desired features (Al-Breiki et al., 2020). Oracles have the capability to retrieve data from diverse sources such as hardware devices, software systems, or even human input. The trust model for oracles can adopt a centralized approach, wherein a single node undertakes the validation of external data, or a decentralized approach, wherein a group of nodes collaboratively assesses the validity of off-chain data. The data flow within oracles can be categorized as inbound when external data is inputted into smart contracts and outbound when data is transmitted from smart contracts to off-chain systems. Depending on the specific application domain requirements, the design of oracles can incorporate various query/response mechanisms, such as publish-subscribe, request-response, immediate-read, or push-pull communication patterns. The utilization of decentralized oracles in comparison to their centralized counterparts offers enhanced trust in input data, mitigating risks associated with single points of failure and improving overall availability (Zhao et al., 2022). Taking into account the primary concerns of data source authenticity, data validity, and integrity, decentralized oracles can be classified into aggregation-based, stacking-based, voting-based and reputation-based approaches (Pasdar et al., 2023). The aggregation-based approaches involve utilizing aggregation functions such as mean, median, or mode to obtain responses from data providers in response to oracle queries. In the stacking-based approach, trust in data is ensured by oracle nodes stacking a specific amount of digital assets, enabling penalties or rewards based on the outcome. The voting-based approach employs oracle nodes as voters or certifiers to ensure consistency in the received responses from data providers. Reputation-based oracles rely on authentication proofs and reputation scores for data providers to verify the integrity of retrieved data.

2.1.2 Trust in IoT devices

Trust is a multidimensional concept that finds application in diverse contexts and has been extensively investigated across various domains such as social science, philosophy, psychology, economics, and communication networks. It can be perceived as a subjective belief concerning the expected behavior of an entity, as observed by an individual or a group. Standardizing and quantifying the notion of trust within the IoT environment poses a complex challenge (Sicari et al., 2015). While cryptographic techniques can address the security and privacy concerns of IoT devices, trust must additionally encompass the implementation of security solutions in accordance with the ethical norms of the IoT ecosystem, enabling the analysis of device behavior over time (Sharma et al., 2016). Behavioral trust exhibits characteristic properties including asymmetricity, dynamicity, non-transitivity, subjectivity, and context-dependence. To comprehensively capture the range of activities performed, trust management in IoT encompasses several stages like information collection, computation, propagation and updation. In quantifying trust for IoT devices, it is crucial to gather information pertaining to their behavior, including attributes such as credibility, reliability, responsiveness, and susceptibility. Subsequently, trust can be derived by leveraging components such as reputation, experience, or knowledge. Trust information can be collected either through direct observations or indirectly from third parties. The trust computation stage involves selecting appropriate computational models to evaluate IoT devices. Mathematical models commonly employed for trust score calculation includes fuzzy logic, statistical analysis, probabilistic methods, entropy calculation, graph theory, and machine learning approaches (Aaqib et al., 2023). Typically, trust scores are propagated within the network using either centralized or distributed approaches. Finally, the trust score assigned to IoT devices can be periodically updated at regular intervals or triggered by specific events as determined by the trustor.

2.1.3 Secure data aggregation in decentralized oracle

In a decentralized oracle network, each autonomous oracle node collects data from IoT devices. However, the aggregation and transmission of data from these oracle nodes to smart contracts does not guarantee the data privacy for each individual oracle node. While a decentralized oracle network incorporates multiple nodes to collectively achieve a common goal, it is required to assume that all participating nodes are mutually distrusting and share the data without revealing the individual contributions. For example, consider a scenario where multiple nodes $n_1,n_2,n_3 \ldots n_i$ owning the data $d_1,d_2,d_3 \ldots d_i$

computes some common aggregation function $(y_1, y_2, y_3 \ldots y_i) = f(d_1, d_2, d_3 \ldots d_i)$ where each node n_i learns only y_i without acquiring the knowledge of other individual data inputs. This mechanism of privacy-preserved computation on data inputs was first introduced in 2003 as Secure Aggregation (SA) in Wireless Sensor Networks (WSNs) (Hu and Evans, 2003). As the popularity of IoT started to surge, an increasing number of SA solutions have emerged to facilitate privacy-preserving computations. A SA protocol typically consists of three consecutive stages: Setup (generation of required cryptographic primitives), Protection (Securing the input data) and Aggregation (Aggregation of inputs to retrieve the result). Based on the underlying cryptographic primitives adopted the SA protocols can be classified into encryption-based SA and MultiParty-Computation (MPC)-based SA (Mansouri et al., 2023). An encryption-based secure aggregation (SA) scheme employs cryptographic keys to secure user inputs, achieved through techniques such as masking, functional encryption, and homomorphic encryption. In contrast, an MPC-based SA scheme does not rely on cryptographic keys to secure user inputs. Instead, the input data is divided into multiple shares and distributed to servers for the reconstruction of the original data. In a combined approach of encryption-based and MPC-based secure aggregation (SA), two primary tasks are performed. Firstly, each node generates a public-private key pair and creates private masks to encrypt the input data. Secondly, the masked input data is divided into 'n' shares and transmitted to the server for the purpose of aggregation.

2.2 Related work

Agricultural insurance has been proved as one of the reliable and key risk management tool for coping with multiple weather-based risks. But the penetration of insurance schemes in developing countries is relatively low that can be attributed to a complex interplay of social, economic, educational, and demographic factors (Biswal and Bahinipati, 2022). These challenges are further compounded by the inadequate adoption of technology (Xiong et al., 2020). The multiple studies in the literature have focused to suitably integrate new age Information and Communication Technologies (ICTs) to enhance processes involved in agriculture insurance value chain. To efficiently administer crop insurance schemes for smallholder farmers while minimizing costs, the adoption of big data approaches has been identified as an appropriate solution (Soyka et al., 2016). The implementation of the IoT and its seamless integration with other data-driven technologies present substantial opportunities for the insurance industry (Manral, 2015). The features of IoT technology enable it to deploy a network of sensors for real-time monitoring and gathering of data measurements in an edge or cloud storage (Elijah et al., 2018). These measurements can be subsequently utilized for computing losses in indexed-based insurance. An IoT-based agricultural field monitoring system was proposed (Das et al., 2018; Hatture and Yankati, 2021) for efficient crop loss estimation. Nevertheless, the proposed solutions that combine big data, IoT and cloud storage exhibit centralization, limited transparency, fragmented databases, security and privacy concerns. To address these concerns, researchers in academia and industry started to explore possibility of decentralized insurance ecosystem with blockchain. The Blockchain Insurance Industry Initiative (B3I) founded in 2016 played a significant role in examining benefits and drawbacks of distributed ledger technology on all stakeholders in value chain. The advancements in scripting capability using smart contracts in blockchain led to many studies proposing decentralized insurance for transport, healthcare, travel and shipping industries (Vo et al., 2017; He et al., 2018; Jia-lan et al., 2019). Motivated by the developments, Food and Agriculture Organization (FAO) derived key insights regarding promises and limitations of blockchain in agriculture (Food and Agriculture Organization, 2019). These insights underpinned the need for decentralized peer-to-peer agricultural insurance for facilitating immediate payouts to producers impacted by weather incidents.

The decentralized framework for flexible deployment and execution of index-based insurance smart contracts was proposed in the research studies conducted by (Jouini and Sethom, 2023; Luo et al., 2022). An exploratory study was conducted by (Amponsah et al., 2021) to analyze the prospective threats and opportunities of integrating blockchain in insurance industry. Kshetri through his study presented the status of blockchain-based crop insurance programmes in developing countries like Sri Lanka, Kenya and Cambodia (Kshetri, 2021). A discussion on role of blockchain in offering transparency, immutability and secure access of agricultural data into smart contract based insurance is identified in the literature (Sajja et al., 2023; Huang and Zhang, 2022). Schwarze and Sushchenko (2022), conducted a detailed study on merits of distributed ledger technologies and smart contracts for yield-indexed and weather-indexed insurance in European agriculture. An earth observation data-driven BEACON project was initiated by (Lekakis et al., 2020) to efficiently synergize weather intelligence with blockchain for agriculture insurance products. Jha et al. (2021), proposed a decentralized crop insurance framework to modernize insurance workflow for Indian farmers. The notable tasks within workflow such as farmer registration, premium payment, claim assessment and payout disbursement are implemented and tested on simulated Ethereum blockchain. Similar kind of empirical studies were conducted (Patel and Shrimali, 2023; Dayana and Kalpana, 2023) to realize a disintermediated, traceable and automated payout system for agricultural insurance using blockchain. Bai et al. (2022), proposed a mechanism to combine IoT data with calamity-indexed insurance, implementing smart contracts for automatic claim settlement on the Hyperledger Fabric blockchain. In his study (Johnson, 2022), formulated a proof-of-concept blockchain system designed to enable mass reinsuring of bush fire parametric insurance within the Australian continent. However, aforementioned studies focus either on describing a framework for decentralized agricultural insurance or exploit inherent characteristics of blockchain for implementation of insurance workflow. These studies did not address pressing issue of retrieving trusted risk factor data (oracle problem) for claim assessment in insurance contracts. To overcome these issues, Nguyen et al. (2019), devised a blockchain-enabled drought insurance contracts connected with oracles for relaying real-time weather information from off-chain resources. Decentralized Financial (DeFi) organizations including Etherisc (Mussenbrock et al., 2018) and Arbol (Jha et al., 2018) have developed their decentralized insurance platforms relying on decentralized oracle named Chainlink for trusted risk factor data access. Similarly,

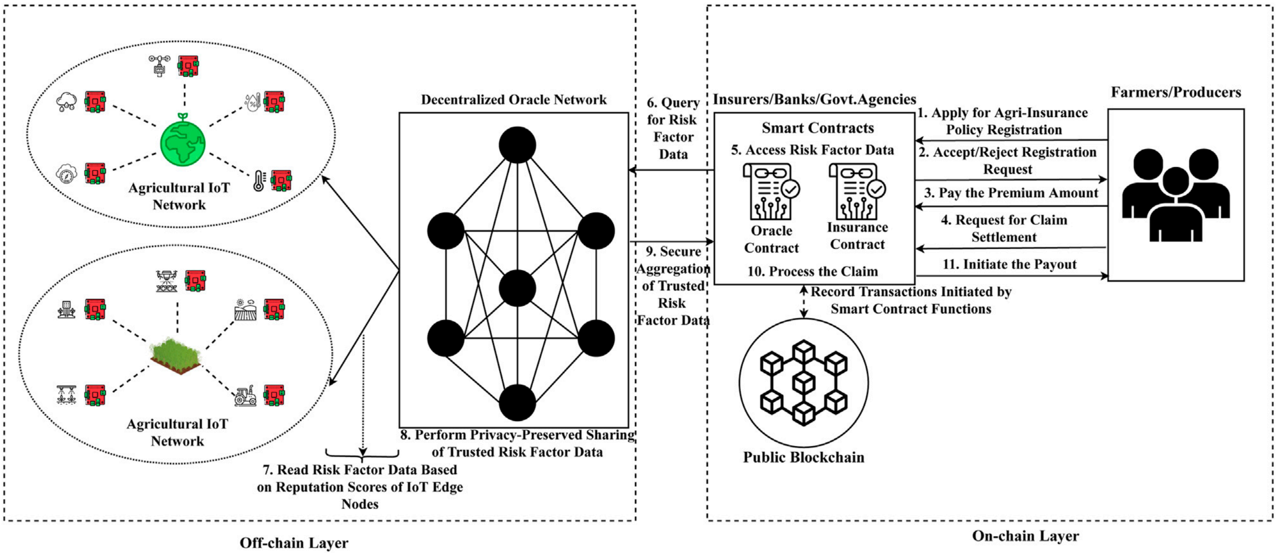

Agricultural IoT Network
Agricultural IoT Network
Decentralized Oracle Network
6. Query for Risk Factor Data
9. Secure Aggregation of Trusted Risk Factor Data
8. Perform Privacy-Preserved Sharing of Trusted Risk Factor Data
7. Read Risk Factor Data Based on Reputation Scores of IoT Edge Nodes
Off-chain Layer
Insurers/Banks/Govt.Agencies
Smart Contracts
5. Access Risk Factor Data
Oracle Contract
Insurance Contract
10. Process the Claim
Record Transactions Initiated by Smart Contract Functions
Public Blockchain
Farmers/Producers
1. Apply for Agri-Insurance Policy Registration
2. Accept/Reject Registration Request
3. Pay the Premium Amount
4. Request for Claim Settlement
11. Initiate the Payout
On-chain Layer

FIGURE 1
An overview of AgriInsureDON framework.

research work by (Iyer et al., 2021) designed the decentralized crop insurance for expedited loss assessment and immediate payout utilizing Chainlink oracle network.

3 Methods

3.1 AgriInsureDON framework

This section provides an overview of the AgriInsureDON framework for a blockchain-based agricultural insurance system featuring a privacy-preserving decentralized oracle that utilizes reliable IoT risk factor data as depicted in Figure 1. At a high level, the framework consists of two interconnected layers: the on-chain and off-chain layers. These layers collaborate to carry out critical tasks in the insurance workflow, such as policy registration, underwriting, premium payment, risk assessment, claim settlement, and payout initiation. The on-chain layer is built on the blockchain infrastructure. The insuring agency deploys smart contracts, known as “InsuranceContract” and “OracleContract,” on the blockchain to facilitate the aforementioned tasks in the insurance workflow. A farmer or producer seeking insurance coverage against agricultural risks initiates interactions with the “InsuranceContract” for tasks like policy registration, underwriting, and premium payment. In the event of a risk occurrence, the farmer or producer requests claim settlement via the “InsuranceContract” to the “OracleContract.” For risk assessment and claim settlement, the “OracleContract” queries the off-chain layer module, a decentralized oracle network, for specific risk factors data such as rainfall, temperature, and humidity. The independent nodes within the decentralized oracle network retrieve the requested risk factor data from IoT edge nodes based on reputation scores. Subsequently, the oracle nodes collaborate to share masked risk factor data, which is securely aggregated by the “OracleContract” for risk assessment. Based on the results, the “InsuranceContract” triggers the payout to the farmer or producer based on index-based indemnity. A conceptual diagram illustrating the implementation of the AgriInsureDON framework is shown in Figure 2. It consists of a front-end layer featuring a Decentralized Application (DApp) dashboard for IoT data monitoring, agricultural insurance policy management, and risk assessment, as well as a back-end layer comprising smart contracts, blockchain, decentralized oracles, and IoT devices. Remote Procedure Call (RPC) mechanisms are used to establish the connection between the front-end and back-end layers.

3.2 Reputation score based decentralized oracle with masked secret sharing and secure aggregation

This section illustrates the method used for direct reputation score computation for IoT edge devices and the working of privacy-preserved decentralized oracle using masked secret sharing and secure aggregation.

3.2.1 Direct reputation score for IoT edge devices

The direct reputation score for IoT edge devices is computed based on their behavioral reputation and data reputation. The present study assumes IoT devices are the edge devices that sense and store weather, soil, and crop management data locally. The method to compute direct reputation scores for IoT edge devices is replicated in this study based on the BD-Trust framework Sharma et al. (2022) as it suits the current problem setting. The direct reputation score calculation for IoT Edge Device (IED) by the Decentralized Oracle Node (DON) passes through three stages: collecting information for trust attributes, score computation, and score updation. Trust attributes like Transmission Status, Response Time, Vulnerability Score, and Data Value are considered to model the behavioral and data reputation effectively. Using a binary

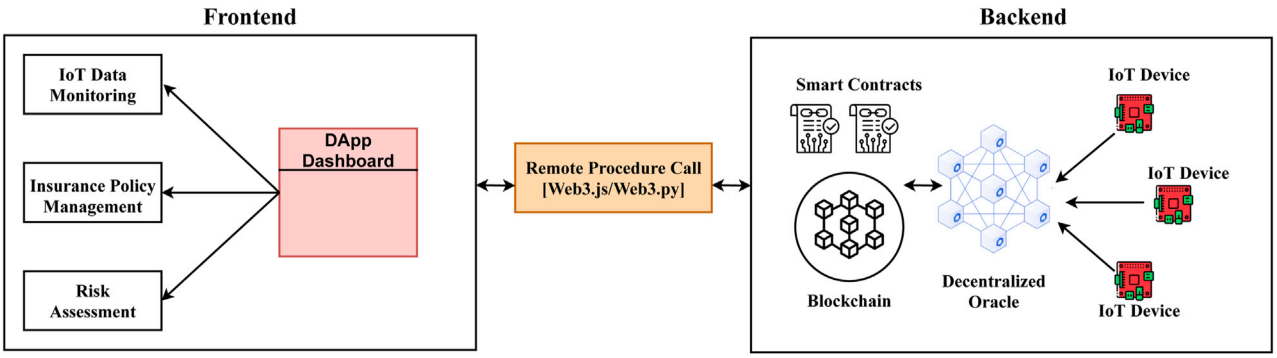


FIGURE 2
A conceptual diagram for AgriInsureDON framework implementation.

TABLE 1 Vulnerability score for IoT devices.

Vulnerability level	Criteria					Score
	Authentication	Confidentiality	Integrity	Availability	Privacy	
V1	Low	Low	Low	Low	Medium	0.2
V2	Low	Low	Low	High	Medium	0.4
V3	Low	Low	High	High	High	0.6
V4	High	Low	High	High	High	0.8

attribute, the *Transmission Status* determines whether a specific transmission *'j'* is successful or unsuccessful. *Response Time* is the time taken to complete a particular transmission *'j'* characterized by a continuous-valued attribute. *Vulnerability Score* measures the vulnerability level of the IoT devices with a static attribute depending upon exposure to security and privacy threats detailed in Table 1. *Data Value* is requested risk factor data in a transmission *'j'* represented by a continuous-valued attribute. For reputation score computation, initially, Behavioral Reputation (BR^f_{mn}) for the functionality *'f'* offered by the nth IED (IED_n) is determined by an independent mth DON (DON_m). This determination utilizes trust parameters such as Completion Rate (CR), Tolerance Level (TL), and Security Credibility (SCR) derived from corresponding trust attributes, namely *Transmission Status*, *Response Time*, and *Vulnerability Score*, respectively. In addition, while computing Behavioral Reputation, care has been taken to obtain the rate at which IEDs misbehave by propagating negative behavior (SCR) along with positive ones (CR, TL) Feng et al. (2015). Subsequently, Data Reputation (DR^f_{mn}) for functionality *'f'* is computed based on the reliability (consistency) of data values transmitted between IED_n and DON_m. Finally, the direct reputation score is obtained by combining both the BR^f_{mn} and DR^f_{mn} using the weighting parameter. The reputation score is updated periodically by the DON_m based on number of transmissions observed between it and IED_n in a particular computation period. Furthermore, a decaying factor (δ) propagates the previously computed reputation with the recent ones. The detailed steps for computation of direct reputation score based on behavioral and data reputation scores are illustrated in Algorithm 1.

3.2.2 Privacy-preserved decentralized oracle using masked secret sharing and secure aggregation

The privacy-preserved sharing of risk factor data by decentralized oracle nodes using masked secret sharing and subsequent secure aggregation by oracle contract is detailed in Figure 3. The key steps involved in the procedure are: (i) Setup the cryptographic parameters, (ii) Read the risk factor data based on reputation score, (iii) Generate secret masks and compute shares, (iv) Propagate masked risk factor data using oracle network (v) Secure aggregation of risk factor data. In the context of the AgriInsureDON framework, the initial step involves the mutual authentication of all participating oracle nodes with the aggregating oracle contract using a public key infrastructure. The oracle node within the network sets up its cryptographic parameters by generating required public-private key pairs. These public keys are broadcasted to other nodes to derive shared private keys on the agreement. Suppose the reputation score of IoT Edge Device (IED) computed by an independent oracle node using Algorithm 1, exceeds a predetermined threshold value. In that case, it acquires risk factor data from the corresponding device. Now, if two-thirds of the nodes within the decentralized oracle possess risk factor data, generating secret masks and shares is initiated to obscure the risk factor data. The masked secret shares are propagated throughout the oracle network. Upon receiving these masked shares, the oracle contract proceeds to unmask the shares through a summation process and reconstructs the original risk factor data for the claim assessment. Algorithm 2 elicits the privacy-preserved risk factor data sharing and its secure aggregation procedure.

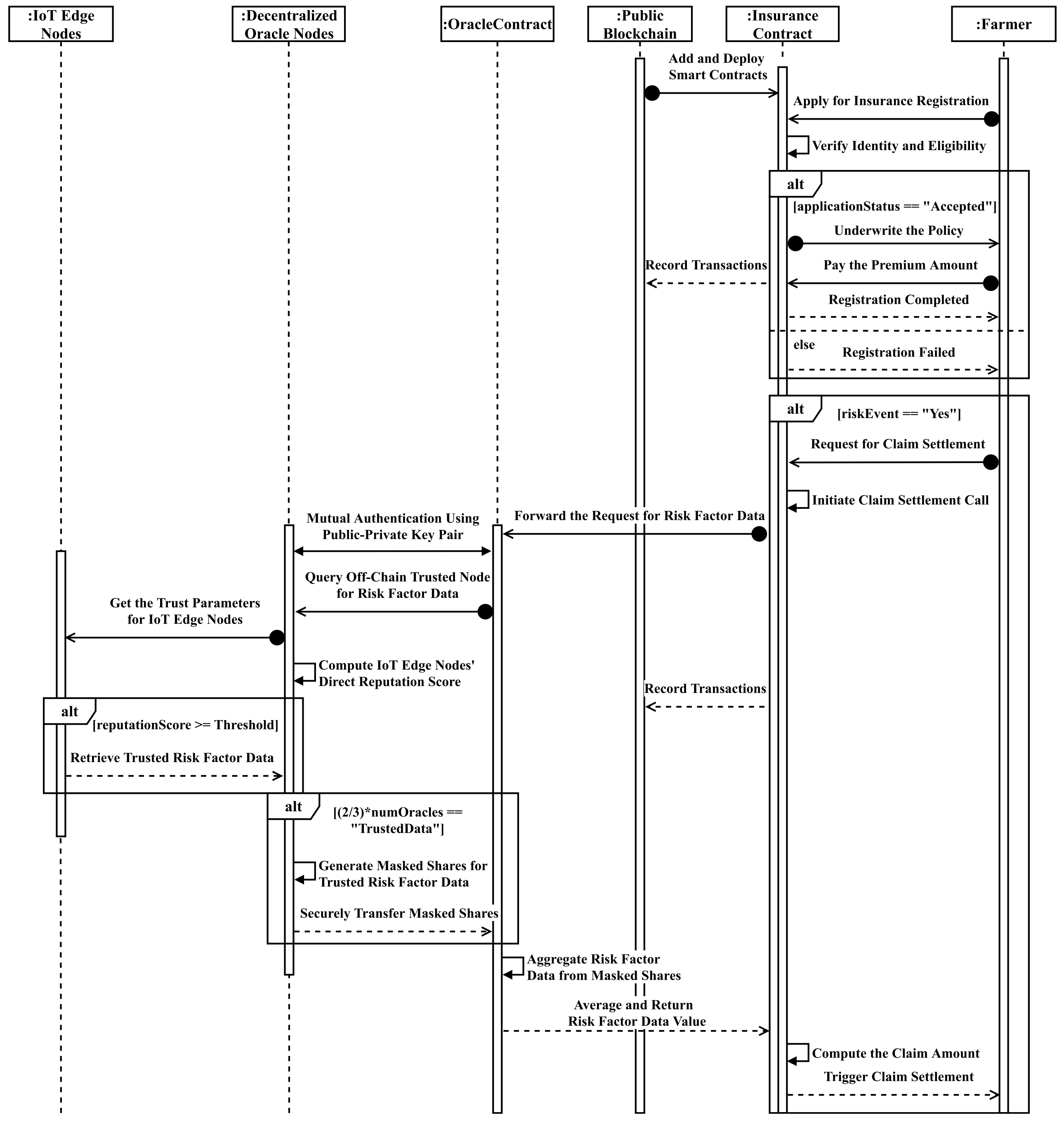

:IoT Edge Nodes
:Decentralized Oracle Nodes
:OracleContract
:Public Blockchain
:Insurance Contract
:Farmer
Add and Deploy Smart Contracts
Apply for Insurance Registration
Verify Identity and Eligibility
alt
[applicationStatus == "Accepted"]
Underwrite the Policy
Record Transactions
Pay the Premium Amount
Registration Completed
else
Registration Failed
alt
[riskEvent == "Yes"]
Request for Claim Settlement
Initiate Claim Settlement Call
Mutual Authentication Using Public-Private Key Pair
Forward the Request for Risk Factor Data
Query Off-Chain Trusted Node for Risk Factor Data
Get the Trust Parameters for IoT Edge Nodes
Compute IoT Edge Nodes' Direct Reputation Score
Record Transactions
alt
[reputationScore >= Threshold]
Retrieve Trusted Risk Factor Data
alt
[(2/3)*numOracles == "TrustedData"]
Generate Masked Shares for Trusted Risk Factor Data
Securely Transfer Masked Shares
Aggregate Risk Factor Data from Masked Shares
Average and Return Risk Factor Data Value
Compute the Claim Amount
Trigger Claim Settlement

FIGURE 3
A detailed sequence diagram for agricultural insurance workflow in AgriInsureDON framework.

4 Experimental setup

This section describes the experimental setup and implementation details necessary to achieve a privacy-preserved decentralized oracle for blockchain-based agricultural insurance smart contracts within the AgriInsureDON framework. A workstation and a laptop running on the Ubuntu 22.04 operating system are utilized to implement a decentralized oracle and develop the required smart contracts for agricultural insurance. The decentralized network is emulated on the workstation with multiple oracle nodes, which retrieve trusted risk factor data based on reputation score from IoT devices. The agricultural insurance contracts are designed and deployed on both a simulated (Ganache) and a test (Sepolia) Ethereum public blockchain network operating on the Proof of Stake (PoS) consensus. Python is used to code the scripts required for the decentralized oracle, while Solidity is employed to program the smart contracts. A Python-based Brownie environment is utilized to test and deploy smart contract functions, and a framework known as Hyperledger Caliper is used to conduct a performance evaluation of the smart contracts. The performance metrics such as average latency ($T_{AvgLatency}$), transaction throughput ($T_{Throughput}$), average CPU(T_{AvgCPU}), and total memory usage ($T_{TotalMemory}$) are considered to determine the scalability of the developed decentralized oracle mechanism. $T_{Throughput}$ measures the rate at which the system commits valid transactions to the blockchain in a given time interval, represented as Transactions Per Second (TPS). $T_{AvgLatency}$ is the time interval between the transaction being sent, and confirmation received for the same.

```
Input  : Trust attributes for computation of behavioral and data reputation
Output : Direct reputation score for IoT Edge Device
Initialize and capture the trust attributes such as Transmission Status(TS), Response Time(RT),
  Vulnerability Score(VS), Data Value(DV) for the interactions between Decentralized Oracle Node
  'm'($DON_m$) and IoT Edge Device 'n' ($IED_n$).
The Behavioral Reputation($BR^f_{mn}$) is calculated by $DON_m$ at time period 't'
foreach functionality f in $IED_n$ do
    a. Determine the Completion Rate(CR) which is the fraction of successful transmissions to total
      transmissions initiated between $IED_n$ and $DON_m$.
          $CR^f_{mn}(t) = \frac{NST_{mn}}{NST_{mn}+NFT_{mn}}$
    where $NST_{mn}$ - Number of successful transactions, $NFT_{mn}$ - Number of failed transactions.
    b. Assess the Tolerance Level(TL) of $IED_n$ by accounting the delay in transmission using RT.
          $TL^f_{mn}(t) = \frac{\sum_{j=1}^{NST_{mn}}(1-P_j)}{NST_{mn}}$
    where $P_j$ is a penalty factor for a particular transmission which is obtained using
          $P_j = \begin{cases} 0, & \text{if } RT_j \leq RT_{\text{Threshold}} \\ \frac{|RT_j - RT_{\text{Threshold}}|}{RT_{\max} - RT_{\text{Threshold}}}, & \text{otherwise} \end{cases}$
    c. Evaluate the Security Credibility(SCR) which determines the vulnerability of $IED_n$ during the
      interactions in the system
          $SCR_n = (1 - VS_n)$
    where $VS_n$ is inferred on the basis of vulnerability criteria given in Table 1.
    d. Compute the behavioural reputation for a functionality 'f' at time period 't' using following
      equation:
          $BR^f_{mn} = (\frac{\log_2(NT_{mn}+1)}{1+\log_2(NT_{mn}+1)}) * CR^f_{mn} * TL^f_{mn} + (\frac{1}{\log_2(NT_{mn}+1)}) * SCR_n$
    where $NT_{mn}$ is the total number of transmissions observed between 'm' and'n'.
The Data Reputation($DR^f_{mn}$) is calculated by $DON_m$ at a given time 't' based on reliability of DV.
      $DR^f_{mn} = DV_{Rel} * \frac{NRT_{mn}}{NST_{mn}}$
where $NRT_{mn}$ is number of consistent data value transmissions out of successful transactions and
  $DV_{Rel} = (1 - (\frac{DV_{StdDev}}{DV_{StdDev}+1})$
The direct reputation score for functionality 'f' is obtained by combining $BR^f_{mn}(t)$ and $DR^f_{mn}(t)$
      $ReputationScore^f_{mn}(t) = \epsilon * BR^t_{mn} + (1 - \epsilon) * DR^f_{mn}(t)$
where $\epsilon$ is the weighting parameter ranging between 0 to 1 used to balance the impact of behavior
  and data reputation.
The direct reputation score is updated by using decay factor $\delta$
$UpdatedReputation^f_{mn}(t) = \delta * ReputationScore^f_{mn}(t) + (1-\delta) * UpdatedReputation^f_{mn}(t - \triangle t)$
where $\delta = [1 - \frac{ReputationScore^f_{mn}(t) - UpdatedReputation^f_{mn}(t-\triangle t)}{NT_{mn}}]$
```

Algorithm 1. Direct Reputation Score Computation for IoT Edge Devices by Decentralized Oracle Nodes.

TABLE 2 Details of software tools used in experiments.

Software	Description
Ethereum Ganache	A simulated public blockchain network
Sepolia Testnet	An Ethereum based real-time test network
Brownie	A python-based blockchain development platform Software
Solidity	Programming language for coding smart contracts
Hyperledger Caliper	A framework for measuring performance of blockchain transactions

```
Input  :List of 'N' authenticated Decentralized Oracle Nodes(DONs)
        DOL=don$_1$,don$_2$,don$_3$......don$_N$
Output :Aggregated Risk Factor Data($RF_{AggData}$)
Generate a public-private key pairs $< don^{i}_{PK}, don^{i}_{SK} >$ for i=1,2.....N
Each $don_i$ broadcasts its public key to all other nodes via the coordinator.
foreach $don_i$ forming a pair with another oracle node $don_j$ do
    Derive a shared private key $< don^{i,j}_{SK}, don^{j,i}_{SK} >$ using a Diffie-Hellman algorithm.
foreach oracle node i=1,2,.....N in DOL do
    if $ReputationScore_{IED} \geq Threshold$ then
        Read the risk factor data(RFData) into the $don_i$
                    $don_i = RFData_i$
    else
        return "Reject risk factor data"
if $\frac{2}{3} * |DOL| ==$ "RFData" then
    Generate the secret masks S$^{i,j}$ and S$^{j,i}$ using shared private key as a seed value to pseudo-random
      number generator(PRNG)
        $S^{i,j} = PRNG(don^{i,j}_{SK})$      $-S^{j,i} = PRNG(don^{j,i}_{SK})$
    Assign a threshold 't' out of 'N' oracle nodes for secure aggregation.
    Generate the masked shares by combining risk factor data from pair $don_{i,j}$ with secret masks
        $y^{i,Mask} = RFData_i + S^{i,j}$      $y^{j,Mask} = RFData_j - S^{j,i}$
    Encrypt and send the masked shares to the oracle contract.
else
    return "Requested risk factor data not available"
foreach masked shares($y^{i}_{Mask}$,$y^{j}_{Mask}$) received by oracle contract do
    Decrypt the masked shares and aggregate the RFData by cancelling out mask values
        $RF_{AggData} = y^{i}_{mask} + y^{j}_{mask}$
        $RF_{AggData} = RFData_i + S^{i,j} + RFData_j - S^{j,i}$
        $RF_{AggData} = RFData_i + RFData_j$
```

Algorithm 2. Privacy-Preserved Sharing and Secure Aggregation of Risk Factor Data.

Table 2 illustrates the blockchain frameworks, tools, and programming languages used to implement the agricultural insurance workflow. In the present study, a weather-indexed insurance workflow is considered to demonstrate the working of objectives stated in the AgriInsureDON framework. In particular, the "temperature" is an index that triggers the payout. The smart contracts named "IndexedInsurance.sol" and "DecentralizedOracle.sol" are developed with necessary functions to accomplish the tasks within the insurance workflow. To enhance understanding of the implementation details, the code is made publicly available to all users on GitHub[1].

5 Implementation, results and analysis

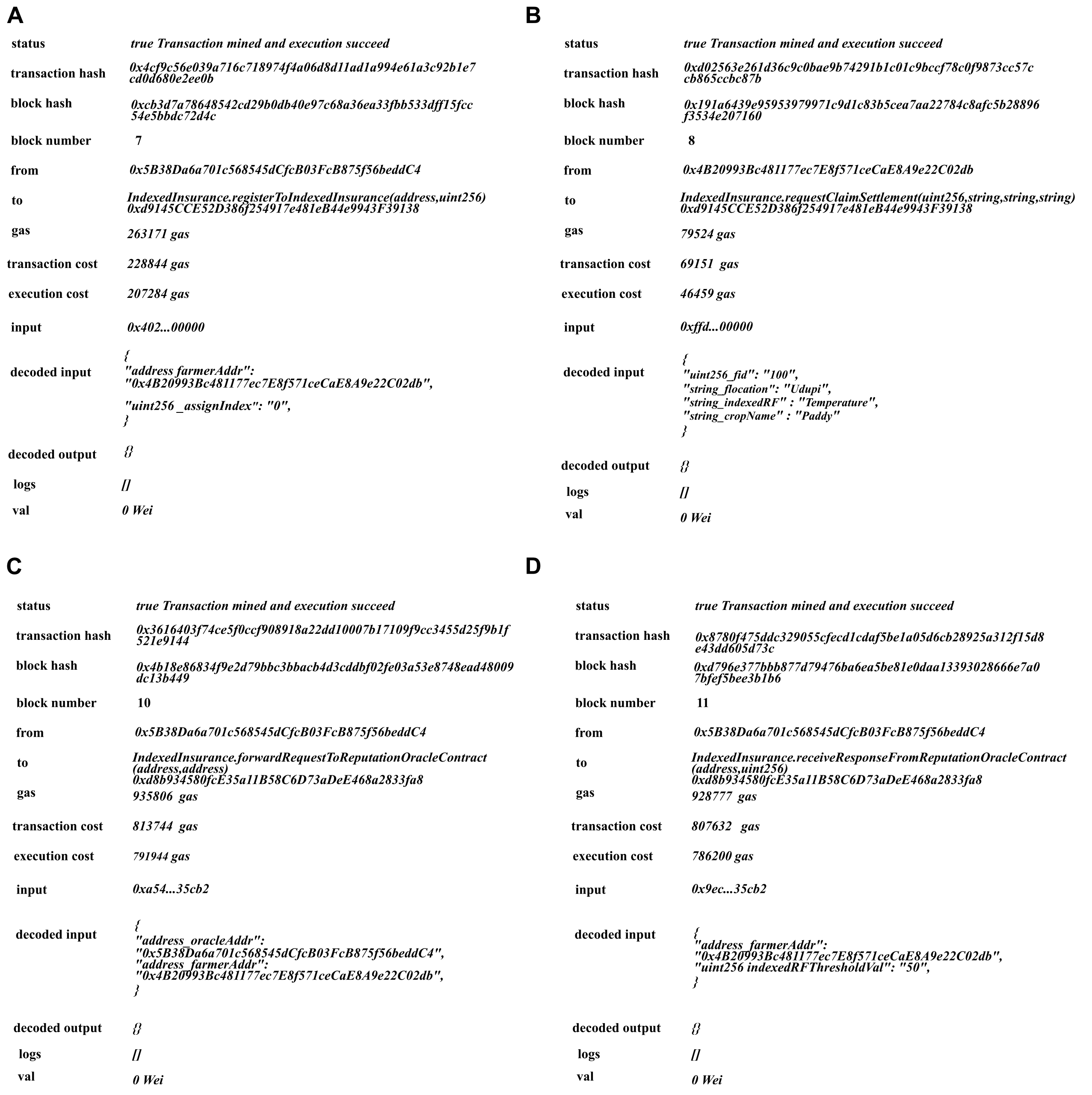
5.1 Smart contract transactions in indexed agricultural insurance

The insurance workflow in the experiments implement specific tasks such as verifying and registering the farmer, underwriting the policy, registering to indexed insurance, requesting claim settlement, forwarding and receiving response from the decentralized oracle, triggering the payout as functions in smart contracts. These tasks implemented within "IndexedInsurance.sol" and "DecentralizedOracle.sol" for

[1] https://github.com/ManojTaleka/AgriInsureDON.git

TABLE 3 Gas consumption details of smart contract functions in agricultural insurance workflow.

Transaction name	Gas consumed	Transaction name	Gas consumed
underwritePolicy ()	188093	forwardRequestToOracleContract ()	935806
registerToIndexedInsurance ()	263171	receiveResponseFromOracleContract ()	928777
requestClaimSettlement ()	79524		



```
status              true Transaction mined and execution succeed
transaction hash    0x4cf9c56e039a716c718974f4a06d8d11ad1a994e61a3c92b1e7
                    cd0d680e2ee0b
block hash          0xcb3d7a78648542cd29b0db40e97c68a36ea33fbb533dff15fcc
                    54e5bbdc72d4c
block number         7
from                0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                  IndexedInsurance.registerToIndexedInsurance(address,uint256)
                    0xd9145CCE52D386f254917e481eB44e9943F39138
gas                 263171 gas
transaction cost    228844 gas
execution cost      207284 gas
input               0x402...00000
decoded input       {
                    "address farmerAddr":
                    "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db",

                    "uint256 _assignIndex": "0",
                    }
decoded output      {}
logs                []
val                 0 Wei
```

```
status              true Transaction mined and execution succeed
transaction hash    0xd02563e261d36c9c0bae9b74291b1c01c9bccf78c0f9873cc57c
                    cb865ccbc87b
block hash          0x191a6439e95953979971c9d1c83b5cea7aa22784c8afc5b28896
                    f3534e207160
block number         8
from                0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
to                  IndexedInsurance.requestClaimSettlement(uint256,string,string,string)
                    0xd9145CCE52D386f254917e481eB44e9943F39138
gas                 79524 gas
transaction cost    69151  gas
execution cost      46459 gas
input               0xffd...00000
decoded input       {
                    "uint256_fid": "100",
                    "string_flocation": "Udupi",
                    "string_indexedRF" : "Temperature",
                    "string_cropName" : "Paddy"
                    }
decoded output      {}
logs                []
val                 0 Wei
```

```
status              true Transaction mined and execution succeed
transaction hash    0x3616403f74ce5f0ccf908918a22dd10007b17109f9cc3455d25f9b1f
                    521e9144
block hash          0x4b18e86834f9e2d79bbc3bbacb4d3cddbf02fe03a53e8748ead48009
                    dc13b449
block number         10
from                0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                  IndexedInsurance.forwardRequestToReputationOracleContract
                    (address,address)
                    0xd8b934580fcE35a11B58C6D73aDeE468a2833fa8
gas                 935806  gas
transaction cost    813744  gas
execution cost      791944 gas
input               0xa54...35cb2
decoded input       {
                    "address_oracleAddr":
                    "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
                    "address_farmerAddr":
                    "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db",
                    }
decoded output      {}
logs                []
val                 0 Wei
```

```
status              true Transaction mined and execution succeed
transaction hash    0x8780f475ddc329055cfecd1cdaf5be1a05d6cb28925a312f15d8
                    e43dd605d73c
block hash          0xd796e377bbb877d79476ba6ea5be81e0daa13393028666e7a0
                    7bfef5bee3b1b6
block number         11
from                0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                  IndexedInsurance.receiveResponseFromReputationOracleContract
                    (address,uint256)
                    0xd8b934580fcE35a11B58C6D73aDeE468a2833fa8
gas                 928777  gas
transaction cost    807632   gas
execution cost      786200 gas
input               0x9ec...35cb2
decoded input       {
                    "address_farmerAddr":
                    "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db",
                    "uint256 indexedRFThresholdVal": "50",
                    }
decoded output      {}
logs                []
val                 0 Wei
```

FIGURE 4
Results for smart contract transactions in indexed agricultural insurance. **(A)** Register farmer to indexed insurance transaction **(B)** request claim settlement transaction **(C)** forward request to oracle contract transaction **(D)** receive response from oracle contract transaction.

agricultural insurance conducts the blockchain transactions. The computational effort required by functions in terms of gas consumed for performing a transaction in blockchain network is shown in Table 3. The results obtained while performing these key transactions for weather indexed insurance is shown in Figure 4.

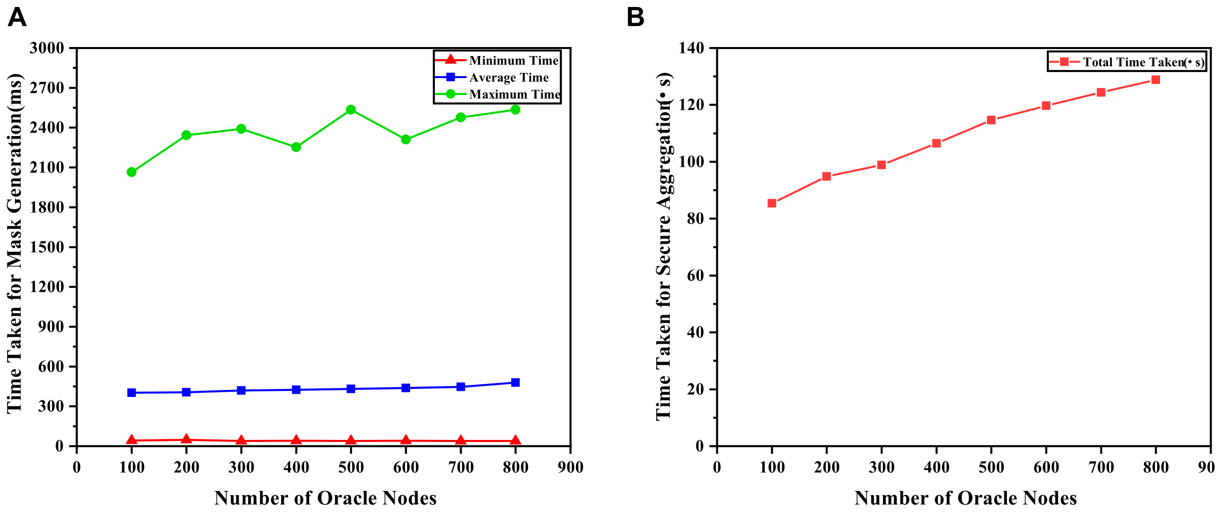


FIGURE 5
Mask generation and secure aggregation time for masked secret sharing in indexed insurance workflow. **(A)** Time taken for mask generation **(B)** time taken for secure aggregation.

5.2 Performance analysis of masked secret sharing and secure data aggregation scheme

Masked secret sharing scheme does not depend upon the trusted third party for the key distribution and to derive a shared secret key required for masking. It involves only modular addition for masking and unmasking operations for the decentralized oracle. However, the significant overhead is incurred by oracle nodes in terms of communication and computation costs during the setup phase of the masks and securing the risk factor data. The computing and communication cost for ‘n’ oracle nodes, each with input risk factor data of size |RFData| is O (n+ |RFData|). The computation time required for mask generation is determined by performing the experiments by varying the number of oracle nodes from 100 to 800. Figure 5A shows the minimum, average, and maximum time required for mask generation. For the experiments conducted with the 100 to 800 oracle nodes, the average time taken for mask generation varies in the range of 400 ms–470 ms. Similarly, the analysis of total time taken for secure aggregation of masked risk factor data ranges between 85 μs to 130 μs as depicted in Figure 5B. The solution employs the threshold ‘t’ out of ‘n’ oracle nodes method for secure aggregation to overcome the problem of all masked risk factor data being available at aggregation time.

5.3 Latency, throughput and resource consumption analysis

The performance analysis of blockchain transactions initiated by smart contract functions within the indexed insurance workflow is conducted on two target environments: the Ethereum simulation platform (Ganache) and the Ethereum Testnet (Sepolia). The key smart contract functions considered for evaluation include *underwritePolicy()*, *registerToIndexedInsurance()*, *requestClaimSettlement()*, *forwardRequestToOracleContract()* and *receiveResponseFromOracleContract()*. The scalability of transactions invoked by these functions is assessed through metrics such as $T_{AvgLatency}$, $T_{Throughput}$, T_{AvgCPU}, and $T_{TotalMemory}$. Benchmarking is conducted using the Hyperledger Caliper tool, organizing transactions into multiple rounds. The analysis is performed on the Ganache and Sepolia blockchain networks, varying the number of transactions from 100 to 800 at a fixed rate with a transaction send rate of 50. The results for the Ganache network are depicted in Figures 6A–D, while the results for the Sepolia test network are illustrated in Figures 7A–D. In the Ganache network, a locally simulated blockchain, it is observed to achieve lower $T_{AvgLatency}$ and higher $T_{Throughput}$ compared to the Sepolia network for most of the transactions. Additionally, the local blockchain consistently demonstrates a decrease in average CPU utilization and a linear increment in memory usage with an increase in the number of transactions as depicted in Figures 6C, D. For transactions within the Sepolia testnet shows high variability in T_{AvgCPU} with no consistent pattern. However, a steady increment is observed for $T_{TotalMemory}$, as shown in Figures 7C, D.

As this study focuses on the implementation of a decentralized oracle for indexed insurance contracts, the emphasis lies in analyzing the performance of *forwardRequestToOracleContract()* and *receiveResponseFromOracleContract()* transactions within the Ganache and Sepolia test network. For Ganache and Sepolia test networks, transactions involving *forwardRequestToOracleContract()* exhibit higher $T_{AvgLatency}$. In contrast, those with *receiveResponseOracleContract()* display lower $T_{AvgLatency}$ compared to all other transactions, as illustrated in Figures 6A, 7A. This results in lower $T_{Throughput}$ for *forwardRequestToOracleContract()* and higher $T_{Throughput}$ for *receiveResponseFromOracleContract()*, as shown in Figures 6B, 7B. The increased delay and decreased throughput in transactions involving *forwardRequestToOracleContract()* can be attributed to the need to request data from multiple oracle nodes for the risk factor data while ensuring the reliability of the reputation score. Furthermore, the *underwritePolicy()*, *registerToIndexedInsurance()*, *requestClaimSettlement()* transactions show $T_{AvgLatency}$ and

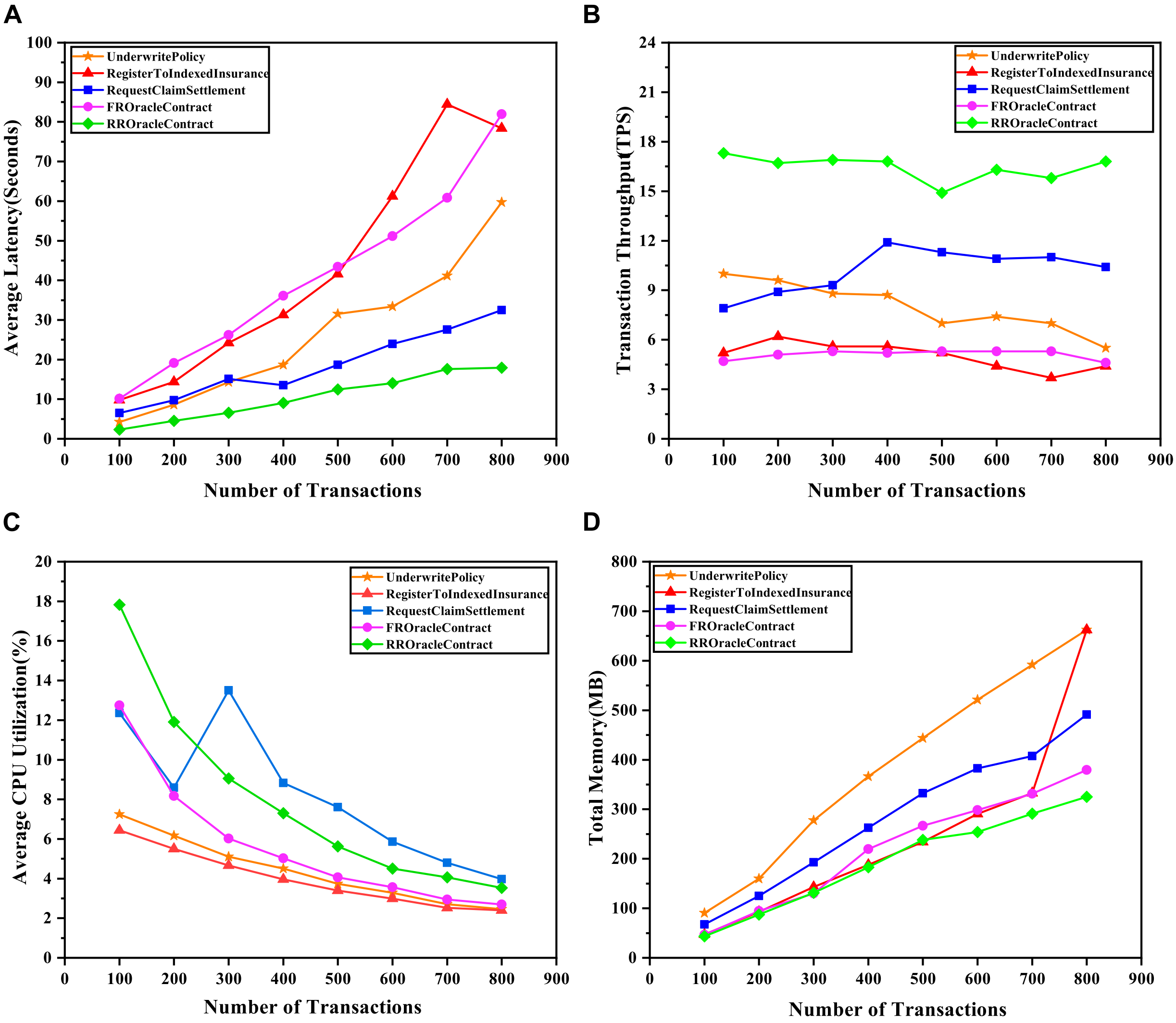


FIGURE 6
Average Latency, Throughput, Average CPU Utilization and Total Memory Usage for Smart Contract Transactions using Ganache Network. **(A)** Average Latency **(B)** Throughput **(C)** Average CPU Utilization **(D)** Total Memory Usage.

$T_{Throughput}$ that fall between the latency and throughput of forwarding request and receiving response transactions. The experimental observations indicate that the Sepolia test network displays variations in all performance metrics due to network communication delays and transaction loads lacking the consistency observed in the Ganache network.

5.4 Comparison of blockchain with IOTA tangle

IOTA Tangle is a promising alternative Distributed Ledger Technology (DLT) designed specifically for data-intensive IoT applications. It offers a flexible architecture by arranging transactions in a Directed Acyclic Graph (DAG) known as Tangle. Its unique features, such as feeless transactions and a highly scalable architecture, make it well-suited for the collection and relay of high-frequency IoT data to decentralized agricultural insurance (Pullo et al., 2024). However, despite its impressive capabilities in handling real-time IoT data, IOTA's smart contract ecosystem is still in the early stages of development, and it lacks a mature oracle framework. These limitations pose challenges for its adoption in agricultural insurance applications, particularly for risk assessment. Furthermore, blockchain excels in providing superior security for transaction data due to the integration of well-established cryptographic protocols. Table 4 presents a comparison of the tradeoffs between blockchain and IOTA Tangle based on key features.

5.5 Security and privacy analysis

Three components, namely data source, oracle nodes, and oracle mechanisms, play a crucial role in ensuring the security and privacy of blockchain oracle. The desired trust factors required for these three components include authenticity, correctness, integrity, validity, availability, and privacy of data (Sadawi et al., 2022;

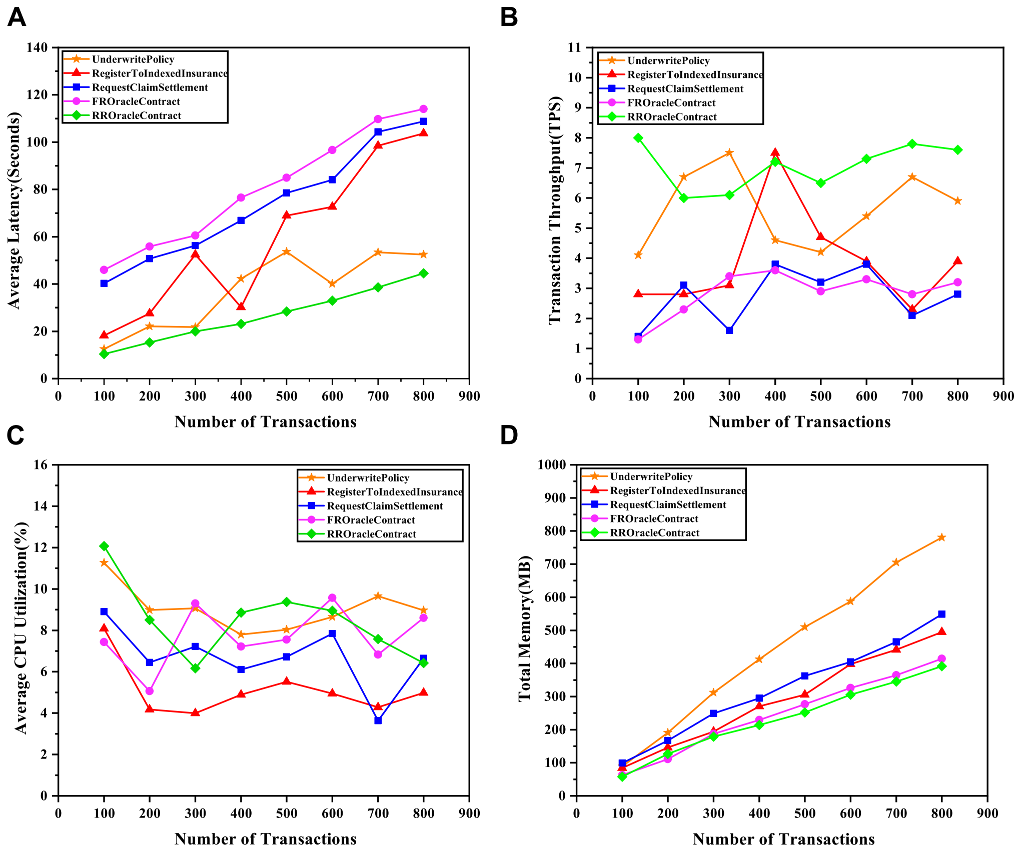


FIGURE 7
Average Latency, Throughput, Average CPU Utilization, and Total Memory Usage for Smart Contract Transactions using Sepolia Network. **(A)** Average Latency **(B)** Throughput **(C)** Average CPU Utilization **(D)** Total Memory Usage.

TABLE 4 Tradeoffs between blockchain and IOTA tangle in key features.

Feature	Blockchain	IOTA tangle
Architecture	Hashed chain of blocks	Directed Acyclic Graph (DAG)
Consensus Protocol	Proof of Stake (Ethereum)	Lightweight validators
Transaction Costs	Transaction fees charged in relation to the native cryptocurrency	Transactions without fee
Scalability	Limited, can be addressed by layer 2 solutions	Scalable with diverse networks
Smart Contract Integration	Mature ecosystem	Emerging ecosystem
Oracle Maturity	Well-established	Early stage development
Security	High due to mature cryptographic protocols	Sufficient, not tested for large scale deployment
Privacy	Advanced privacy mechanisms (Zero knowledge proofs, differential privacy) can be integrated	Evolving privacy mechanisms

Pasdar et al., 2023). In the AgriInsureDON framework, the direct reputation score computed for the IoT data sources encompasses behavioral and data reputation. Behavioral reputation considers the security credibility of IoT data nodes, which accounts for vulnerabilities associated with authentication, confidentiality, integrity, availability, and privacy, while data reputation validates the risk factor data based on its reliability. The trustworthiness of IoT data sources can be further enhanced by computing an indirect reputation score, which accounts for the global reputation of a device as experienced by other devices in the network. To facilitate the assessment of the global reputation score, the computed direct reputation scores are processed and stored in the coordinator oracle node.

Each oracle node collects risk factor data from the corresponding IoT data node and performs privacy-preserved masked secret sharing without revealing the actual input values

TABLE 5 Comparison of AgriInsureDON framework features with existing studies.

	Features				
	Insurance type	Blockchain platform	Data trust	Oracle	Data privacy
Nguyen et al. (2019)	Weather Indexed- Drought	NEO	✗	Centralized Oracle	✗
Jha et al. (2021)	Weather Indexed	Ethereum	✗	✗	✗
Iyer et al. (2021)	Weather Indexed- Rainfall	Ethereum	✗	Decentralized Oracle	✗
Omar et al. (2023)	Weather Indexed	Ethereum	✗	✗	✗
AgriInsureDON (Our Solution)	Weather Indexed	Ethereum	Direct Reputation Score	Decentralized Oracle	Masked Secret Sharing

to other honest-but-curious oracle nodes. Data privacy in oracle nodes can be leveraged by adopting a differential privacy mechanism. Differential privacy ensures that only aggregated risk data is provided, without revealing individual values, thereby minimizing the risk of privacy breaches. This mechanism guarantees that even if multiple queries are made on the risk data, the results will not enable adversaries to infer the presence or absence of data from any individual oracle node. Furthermore, the decentralized oracle mechanism adopted in the framework mitigates the risk of a single point of failure and is readily interoperable with existing IoT standards. To ensure seamless communication between diverse IoT devices, protocols such as Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), and Lightweight Machine to Machine (LwM2M) can be adopted, thereby improving the framework's adaptability. The qualitative comparison of the AgriInsureDON framework with the existing studies is presented in the Table 5.

6 Conclusion

A trusted, transparent, and disintermediated agricultural insurance platform is essential for overcoming information asymmetry and providing high-quality insurance schemes, leading to expedited claim settlement for agricultural risks. This study proposes and implements the blockchain-based AgriInsureDON framework, which incorporates a privacy-preserved decentralized oracle for secure access of trusted risk factor data from IoT devices for agricultural insurance. Initially, a method for computing direct reputation score of IoT edge devices based on behavioral reputation and data reputation is described and a detailed algorithm is presented. Then a masked secret sharing scheme based privacy-preserved decentralized oracle mechanism is designed and implemented for secure access of risk factor data into insurance contracts. Later, the working of indexed agricultural insurance smart contracts is demonstrated with help of decentralized oracle for risk assessment. A detailed analysis of masked secret sharing and secure aggregation of risk factor data is presented. Finally, performance evaluations of smart contract transactions is conducted w.r.t average latency, throughput, average CPU utilization and total memory usage in simulated and test Ethereum networks. The performance metric values for indexed insurance transactions evidence the fact that proposed solution is suitable for real-time deployment. Thus, the AgriInsureDON framework can be extended to other type of insurance applications that need to access the external data with decentralized oracle. As a future work, we want to incorporate the indirect trust for behavioral trust of IoT devices along with real-time monitoring capabilities and user-friendly dashboard interface. Furthermore, we are interested in exploring the other privacy-preserving mechanisms and make the decentralized oracle more trusted with participation of more number of nodes.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

MT: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Software, Validation, Writing–original draft, Writing–review and editing. KM: Conceptualization, Formal Analysis, Investigation, Methodology, Resources, Supervision, Validation, Visualization, Writing–original draft, Writing–review and editing. NV: Conceptualization, Investigation, Methodology, Project administration, Supervision, Validation, Writing–original draft, Writing–review and editing. VT: Conceptualization, Formal Analysis, Supervision, Validation, Writing–review and editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. This research work was supported, and the publication cost was covered by Manipal Academy of Higher Education, Manipal.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Aaqib, M., Ali, A., Chen, L., and Nibouche, O. (2023). Iot trust and reputation: a survey and taxonomy. *J. Cloud Comput.* 12, 42. doi:10.1186/s13677-023-00416-8

Aggarwal, P., Chand, R., Bhutani, A., Kumar, V., Goel, S., Rao, K., et al. (2016). Report of the task force on enhancing technology use in agriculture insurance. Tech. rep.

Al-Breiki, H., Rehman, M. H. U., Salah, K., and Svetinovic, D. (2020). Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE Access* 8, 85675–85685. doi:10.1109/ACCESS.2020.2992698

Amponsah, A. A., Adekoya, A. F., and Weyori, B. A. (2021). Blockchain in insurance: exploratory analysis of prospects and threats. *Int. J. Adv. Comput. Sci. Appl.* 12, 445–466. doi:10.14569/IJACSA.2021.0120153

Bai, P., Kumar, S., and Kumar, K. (2022). "Use of blockchain enabled iot in insurance: a case study of calamity based crop insurance," in 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), 1135–1141.

Beniiche, A. (2020). A study of blockchain oracles. *ArXiv abs/2004.07140*. doi:10.48550/arXiv.2004.07140

Biswal, D., and Bahinipati, C. S. (2022). Why are farmers not insuring crops against risks in India? a review. *Prog. Disaster Sci.* 15, 100241. doi:10.1016/j.pdisas.2022.100241

Centre for Research on the Epidemiology of Disasters (2022). Disasters in numbers. Available at: https://www.cred.be/sites/default/files/CredCrunch70.pdf (Accessed July 03, 2024).

Chamara, N., Islam, M., Bai, G., Shi, Y., and Ge, Y. (2022). Ag-iot for crop and environment monitoring: past, present, and future. *Agric. Syst.* 203, 103497. doi:10.1016/j.agsy.2022.103497

CSIRO Data61 Group (2021). Blockchain patterns-oracle. Available at: https://research.csiro.au/blockchainpatterns/general-patterns/interacting-with-the-external-world/oracle/ (Accessed July 03, 2024).

Das, R. K., Panda, M., and Dash, S. S. (2018). Smart agriculture system in India using internet of things. *Adv. Intelligent Syst. Comput.* 758, 247–255. doi:10.1007/978-981-13-0514-6_25

Dayana, D., and Kalpana, G. (2023). A secured blockchain based approach for decentralized agri-insurance for food crops supply chain. *J. Theor. Appl. Inf. Technol.* 101, 3547–3556.

Dey, K., and Shekhawat, U. (2021). Blockchain for sustainable e-agriculture: literature review, architecture for data management, and implications. *J. Clean. Prod.* 316, 128254. doi:10.1016/j.jclepro.2021.128254

Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., and Hindia, M. N. (2018). An overview of internet of things (iot) and data analytics in agriculture: benefits and challenges. *IEEE Internet Things J.* 5, 3758–3773. doi:10.1109/JIOT.2018.2844296

Feng, R., Han, X., Liu, Q., and Yu, N. (2015). A credible bayesian-based trust management scheme for wireless sensor networks. *Int. J. Distributed Sens. Netw.* 11, 678926. doi:10.1155/2015/678926

Food and Agriculture Organization (2019). E-agriculture in action: blockchain for argiculture opportunities and challenges. *Tech. Rep.*

Greatrex, H., Hansen, J., Garvin, S., Diro, R., Le Guen, M., Blakeley, S., et al. (2015). Scaling up index insurance for smallholder farmers: recent evidence and insights. CCAFS Report

Hatture, S. M., and Yankati, P. V. (2021). Iot-based smart farming application for sustainable agriculture. *Adv. Intelligent Syst. Comput.* 1270, 573–583. doi:10.1007/978-981-15-8289-9_56

He, X., Alqahtani, S., and Gamble, R. (2018). "Toward privacy-assured health insurance claims," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (Halifax, Canada: SmartData), 1634–1641.

Hu, L., and Evans, D. (2003). Secure aggregation for wireless networks. *2003 Symposium Appl. Internet Work. 2003*, 384–391. doi:10.1109/SAINTW.2003.1210191

Huang, Y., and Zhang, H. (2022). "Blockchain innovation in the agriculture aspect," in 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), 579–583. doi:10.1109/ipec54454.2022.9777458

International Institute for Environment and Development (2023). Climate change driving increase in farmer suicides in India. Available at: https://www.iied.org/climate-change-driving-increase-farmer-suicides-india (Accessed July 03, 2024).

Ismail, L., and Materwala, H. (2019). A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions. *Symmetry* 11, 1198. doi:10.3390/sym11101198

Iyer, V., Shah, K., Rane, S., and Shankarmani, R. (2021). *Decentralised peer-to-peer crop insurance*. Hong Kong, Virtual Event: Association for Computing Machinery, Inc, 3–12.

Jha, N., Prashar, D., Khalaf, O. I., Alotaibi, Y., Alsufyani, A., and Alghamdi, S. (2021). Blockchain based crop insurance: a decentralized insurance system for modernization of indian farmers. *Sustain. Switz.* 13, 8921. doi:10.3390/su13168921

Jha, S., Andre, B., and Jha, O. (2018). Arbol: smart contract weather risk protection for agriculture. Available at: https://www.semanticscholar.org/paper/ARBOL:-Smart-Contract-Weather-Risk-Protection-for-Jha-Andre/255c9377a89aa27c0b36d50b80628b6df4bb334d (Accessed July 04, 2024).

Jia-lan, L., Xiao-yu, W., Wan-jun, Y., Zi-chen, W., Huai-lin, Z., and Nai-meng, C. (2019). Research and design of travel insurance system based on blockchain. *2019 Int. Conf. Intelligent Inf. Biomed. Sci. (ICIIBMS)*, 121–124. doi:10.1109/ICIIBMS46890.2019.8991444

Johnson, O. (2022). Decentralized reinsurance: funding blockchain-based parametric bushfire insurance. *2022 IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, 1–3. doi:10.1109/ICBC54727.2022.9805502

Jouini, O., and Sethom, K. (2023). Agribiot: a blockchain-based iot architecture for crop insurance. *Lect. Notes Netw. Syst. 655 LNNS*, 340–350. doi:10.1007/978-3-031-28694-0_32

Just, R. E., Calvin, L., and Quiggin, J. (1999). Adverse selection in crop insurance: actuarial and asymmetric information incentives. *Am. J. Agric. Econ.* 81, 834–849. doi:10.2307/1244328

Kar, A. K., and Navin, L. (2021). Diffusion of blockchain in insurance industry: an analysis through the review of academic and trade literature. *Telematics Inf.* 58, 101532. doi:10.1016/j.tele.2020.101532

Kosmowski, F., Chamberlin, J., Ayalew, H., Sida, T., Abay, K., and Craufurd, P. (2021). How accurate are yield estimates from crop cuts? evidence from smallholder maize farms in Ethiopia. *Food Policy* 102, 102122. doi:10.1016/j.foodpol.2021.102122

Kshetri, N. (2021). Blockchain-based smart contracts to provide crop insurance for smallholder farmers in developing countries. *IT Prof.* 23, 58–61. doi:10.1109/MITP.2021.3123416

Lekakis, E., Kotsopoulos, S., Mygdakos, G., Dimitrakos, A., Tsioutsia, I.-M., and Simeonidou, P. (2020). Redefining agricultural insurance services using earth observation data. the case of beacon project. *IFIP Adv. Inf. Commun. Technol. 554 IFIP*, 90–101. doi:10.1007/978-3-030-39815-6_9

Luo, Q., Liao, R., Li, J., Ye, X., and Chen, S. (2022). Blockchain enabled credibility applications: extant issues, frameworks and cases. *IEEE Access* 10, 45759–45771. doi:10.1109/ACCESS.2022.3150306

Lyubchich, V., Newlands, N. K., Ghahari, A., Mahdi, T., and Gel, Y. R. (2019). Insurance risk assessment in the face of climate change: integrating data science and statistics. *Wiley Interdiscip. Rev. Comput. Stat.* 11, e1462. doi:10.1002/wics.1462

Manral, J. (2015). Iot enabled insurance ecosystem-possibilities challenges and risks. *arXiv Prepr. arXiv:1510.03146*. doi:10.48550/arXiv.1510.03146

Mansouri, M., Önen, M., Jaballah, W. B., and Conti, M. (2023). Sok: secure aggregation based on cryptographic schemes for federated learning. *Proc. Priv. Enhancing Technol.* 2023, 140–157. doi:10.56553/popets-2023-0009

Mussenbrock, C., Karpischek, S., and Khasanshyn, R. (2018). Etherisc decentralized insurance. Available at: https://etherisc.com/ (Accessed July 04, 2024).

Nguyen, T., Das, A., and Tran, L. (2019). Neo smart contract for drought-based insurance. *2019 IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, 1–4. doi:10.1109/CCECE.2019.8861573

Omar, I. A., Jayaraman, R., Salah, K., Hasan, H. R., Antony, J., and Omar, M. (2023). Blockchain-based approach for crop index insurance in agricultural supply chain. *IEEE Access* 11, 118660–118675. doi:10.1109/ACCESS.2023.3327286

Pasdar, A., Lee, Y. C., and Dong, Z. (2023). Connect api with blockchain: a survey on blockchain oracle implementation. *ACM Comput. Surv.* 55, 1–39. doi:10.1145/3567582

Patel, H., and Shrimali, B. (2023). Agrionblock: secured data harvesting for agriculture sector using blockchain technology. *ICT Express* 9, 150–159. doi:10.1016/j.icte.2021.07.003

Pullo, S., Pareschi, R., Piantadosi, V., Salzano, F., and Carlini, R. (2024). Integrating iota's tangle with the internet of things for sustainable agriculture: a proof-of-concept study on rice cultivation. *Informatics* 11, 3. doi:10.3390/informatics11010003

Rajeev, M., and Nagendran, P. (2023). Protecting land and livelihood under climate risks: what hinders crop insurance adoption? *Land Use Policy* 131, 106711. doi:10.1016/j.landusepol.2023.106711

Sadawi, A. A., Hassan, M. S., and Ndiaye, M. (2022). On the integration of blockchain with iot and the role of oracle in the combined system: the full picture. *IEEE Access* 10, 92532–92558. doi:10.1109/ACCESS.2022.3199007

Sajja, G. S., Rane, K. P., Phasinam, K., Kassanuk, T., Okoronkwo, E., and Prabhu, P. (2023). *Towards applicability of blockchain in agriculture sector* 80. Elsevier Ltd, 3705–3708.

Schwarze, R., and Sushchenko, O. (2022). Climate insurance for agriculture in europe: on the merits of smart contracts and distributed ledger technologies. *J. Risk Financial Manag.* 15, 211. doi:10.3390/jrfm15050211

Sharma, A., Pilli, E. S., and Mazumdar, A. P. (2022). Bd-trust: behavioural and data trust management scheme for internet of things. *J. Ambient Intell. Humaniz. Comput.* 14, 16195–16207. doi:10.1007/s12652-022-03841-w

Sharma, A., Pilli, E. S., Mazumdar, A. P., and Govil, M. C. (2016). A framework to manage trust in internet of things. *2016 Int. Conf. Emerg. Trends Commun. Technol. (ETCT)*, 1–5. doi:10.1109/ETCT.2016.7882970

Sicari, S., Rizzardi, A., Grieco, L., and Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: the road ahead. *Comput. Netw.* 76, 146–164. doi:10.1016/j.comnet.2014.11.008

Soyka, D. M., Liang, F.-Y., Patankar, M. N., and Van, S. (2016). "Big data approaches to crop insurance in Asia,". Rüschlikon, Switzerland: Swiss Re Centre for Global Dialogue. Tech. rep.

Van Wassenaer, L., van Hilten, M., Van Ingen, E., and Van Asseldonk, M. (2021). *Applying blockchain for climate action in agriculture: state of play and outlook*. Rome, Italy: Food and Agriculture Organization.

Vo, H. T., Mehedy, L., Mohania, M., and Abebe, E. (2017). "Blockchain-based data management and analytics for micro-insurance applications," in Proceedings of the 2017 ACM on Conference on Information and Knowledge Management (Singapore: Association for Computing Machinery), 2539–2542.

Xiong, H., Dalhaus, T., Wang, P., and Huang, J. (2020). Blockchain technology for agriculture: applications and rationale. *Front. Blockchain 3* 3, 7. doi:10.3389/fbloc.2020.00007

Zhao, Y., Kang, X., Li, T., Chu, C.-K., and Wang, H. (2022). Toward trustworthy defi oracles: past, present, and future. *IEEE Access* 10, 60914–60928. doi:10.1109/ACCESS.2022.3179374