Blockchain-Enabled Agricultural Contract Fulfillment Mechanism

Xiaolong Liang, Mengzhen Kang, Juanjuan Li, and Rui Qin

***Abstract*—Contract farming is a vital organizational model for mitigating systemic risks in agricultural supply chains, yet it is persistently hindered by severe trust deficits and prohibitive legal enforcement costs. Traditional centralized credit evaluation systems often fail to encompass dispersed smallholder farmers, leaving their historical compliance locked as illiquid, implicit social capital. To address these structural vulnerabilities, this paper proposes a novel blockchain-enabled agricultural contract fulfillment mechanism grounded in decentralized identity (DID) and verifiable credentials. Rather than treating reputation as a direct transactional currency, we design a bidirectional anchoring architecture where on-chain reputation acts as a cryptographic trust anchor to validate the authenticity of verifiable credentials (VCs). These VCs transparently prove a farmer's actual production capacity and off-chain agricultural records. Through the autonomous execution of smart contracts, this endogenous governance system links these authenticated capacity credentials directly to agricultural transactions. Successful fulfillment naturally yields a reputation premium, whereas opportunistic default, or the issuance of falsified credentials, triggers the immediate, systemic destruction of the responsible parties' credit capital. A multi-agent transaction simulation validates the proposed framework, demonstrating its efficacy in filtering market risks based on verifiable capacity and overcoming the cold-start dilemma for new rural entrants.**

***Index Terms*—Blockchain, contract farming, decentralized identity (DID), verifiable credentials, credit tokenization**

I. Introduction

AGRICULTURAL systems are inherently complex cyber-physical-social systems characterized by long production cycles, biological uncertainties, and high information asymmetry [1–4]. As agricultural supply chains expand across regions, the lack of end-to-end visibility often leads to a profound disconnect between growers, storage facilities, logistics providers, and buyers [5–7]. To mitigate these systemic risks and stabilize supply and demand, contract farming has emerged as a primary organizational model. By locking in prices and production quantities in advance, it theoretically hedges market risks [8–13].

However, in practice, existing contract farming frequently suffers from fundamental conflicts of interest and a severe trust deficit between agribusinesses and dispersed smallholder farmers [14–16]. The legal enforcement costs for breach of contract are prohibitively high, leading farmers to easily engage in opportunistic behavior driven by short-term self-interest. Furthermore, traditional centralized credit evaluation systems are ill-equipped to address this structural failure [17, 18]. Centralized institutions struggle with massive data collection and verification costs in rural areas, effectively leaving the majority of smallholders in a credit blind spot. Consequently, a farmer's historical compliance remains locked as abstract, implicit social capital [19, 20]. Without liquidity or dynamic quantification, this social credit fails to serve as a tangible constraint against future defaults, resulting in resource misallocation and price fluctuations across the supply chain [21, 22]. In traditional contract models, whether classical fixed-price agreements [23], relational contracts sustained by repeated interaction [24], or incentive-based designs with performance bonds [25], enforcement ultimately depends on costly judicial intervention or fragile interpersonal trust. These mechanisms scale poorly in dispersed rural settings where legal infrastructure is weak and farmer populations are large and heterogeneous.

To overcome these centralized bottlenecks and transform implicit social trust into tangible constraints, blockchain technology and decentralized autonomous organizations (DAOs) offer a paradigm shift for agricultural governance [26–29]. By deploying an immutable distributed ledger and smart contracts, stakeholders can ensure that complex agreements are automatically executed without relying on expensive intermediaries, drastically reducing legal enforcement costs. Furthermore, DAOs provide a robust organizational framework to integrate dispersed rural entities. They utilize tokenized incentive mechanisms to naturally align the economic interests of diverse stakeholders, from smallholder farmers to large agribusinesses. Within this framework, cooperative trust is algorithmically guaranteed, shifting the paradigm toward decentralized, self-enforcing collaboration.

While blockchain and DAOs provide the infrastructural foundation, existing blockchain-based agricultural solutions remain limited in scope. Prior traceability systems [30–32] focus on recording supply-chain events but do not address the pre-contractual trust deficit or enforce fulfillment incentives. Integrated market platforms [33] digitize procurement workflows yet still rely on centralized credit scoring, which

Manuscript received: 26 February 2026; revised: 7 March 2026; accepted: 18 March 2026. *(Corresponding author: Juanjuan Li.)*

Citation: X. Liang, M. Kang, J. Li, and R. Qin, Blockchain-enabled agricultural contract fulfillment mechanism, *Int. J. Intell. Control Syst.*, 2026, 31(1), 92–99.

Xiaolong Liang, Mengzhen Kang, Juanjuan Li, and Rui Qin are with State Key Laboratory of Multimodal Artificial Intelligence Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China (e-mail: xiaolong.liang@ia.ac.cn; mengzhen.kang@ia.ac.cn; juanjuan.li@ia.ac.cn; rui.qin@ia.ac.cn).

Digital Object Identifier 10.62678/IJICS202603.10319

excludes smallholders lacking formal financial histories. Blockchain-enabled supply-chain models [22, 34] improve transparency but treat reputation as a static attribute rather than a dynamic, stakeable asset with real economic consequences.

To bridge this gap, this study proposes a blockchain-enabled agricultural contract fulfillment mechanism based on decentralized identity (DID) and credit tokenization. The concept of self-sovereign identity and verifiable credentials (VCs) has gained significant traction in recent years [35–37], yet their application to agricultural contract enforcement remains largely unexplored [38]. Unlike the aforementioned approaches, our framework introduces three key differentiators: (1) it decouples verifiable production capacity from abstract credit scores through VCs; (2) it employs a bidirectional anchoring architecture where on-chain reputation strictly authenticates off-chain capacity proofs rather than serving as a direct transactional currency; and (3) it enforces joint liability on credential issuers, creating a multilateral penalty structure absent from existing solutions. By drastically increasing the long-term opportunity cost of default, the mechanism ensures that contract adherence becomes a self-enforcing Nash equilibrium without intensive judicial intervention.

The main contributions are as follows:

(1) A DID-based data certification architecture for agriculture was proposed to bootstrap rural digital identities by using on-chain reputation to authenticate off-chain capacity proofs, resolving the cold-start problem.

(2) A dynamic credit assetization mechanism with bidirectional anchoring between physical fulfillment and reputation updates was designed, enforcing strict joint liability on nodes that issue falsified credentials.

(3) A multi-agent simulation was conducted to validate the framework's ability to filter market risks by verifiable capacity and sustain long-term cooperative equilibrium.

The remainder of this paper is organized as follows. Section II details the architecture of the blockchain-enabled fulfillment model. Section III formalizes the technical implementation of the credit assetization mechanism. Section IV presents the multi-agent simulation and analyzes the results. Finally, Section V concludes the study and outlines future research directions.

II. Blockchain-Enabled Fulfillment Model for Contract Farming

This research proposes a distributed performance framework leveraging blockchain technology to address the inherent issues of contract incompleteness and prohibitive enforcement costs in traditional contract farming. The architecture is grounded in the conceptual paradigms of credit value assetization and the internalization of default externalities. In contrast to conventional governance models that necessitate third-party judicial intervention, the proposed mechanism utilizes the programmability and autonomous execution of smart contracts to establish an endogenous governance system centered on reputation capital.

The operationalization is structured into three core components: the decentralized data module, the distributed certification network, and the application module. First, the decentralized data module focuses on the collection of long-tail data by utilizing decentralized incentive mechanisms to overcome the information silos and high acquisition costs prevalent in traditional supply chains. Second, the distributed certification network establishes a robust framework for verification and value transformation; it utilizes cryptographic primitives to convert heterogeneous verification data into verifiable credentials, effectively minting them into liquid reputation assets through quantitative modeling. Finally, the application module integrates these credit assets into practical agricultural business scenarios. This model redefines the payoff matrix so that performance becomes the Nash equilibrium strategy for farmers, achieving autonomous contract execution through the maximization of long-term credit value. To implement the above logic, this model adopts a bottom-up four-layer technical architecture, as shown in Fig. 1.

A. Decentralized Data Module

Serving as the foundational infrastructure, this module builds the data cornerstone of on-chain credit by aggregating heterogeneous multi-source long-tail data. In the anonymous trusted system of Web3, native digital identities often face a cold start dilemma, lacking historical behavioral data to support initial credit. However, traditional Web2 platforms possess vast yet fragmented behavioral data that accurately reflect farmers' production status. To bridge the gap between the off-chain reality and the Web3 digital ecosystem, this module implements an off-chain data assetization mechanism. This process transforms historical behavioral records into verifiable credit capital, effectively bootstrapping the decentralized identity system. Specifically, this module constructs a trusted channel from off-chain data to on-chain identity through cryptographic signature mechanisms. Distributed certification nodes use private keys to sign off-chain records, transforming them into trust anchors. These data fingerprints

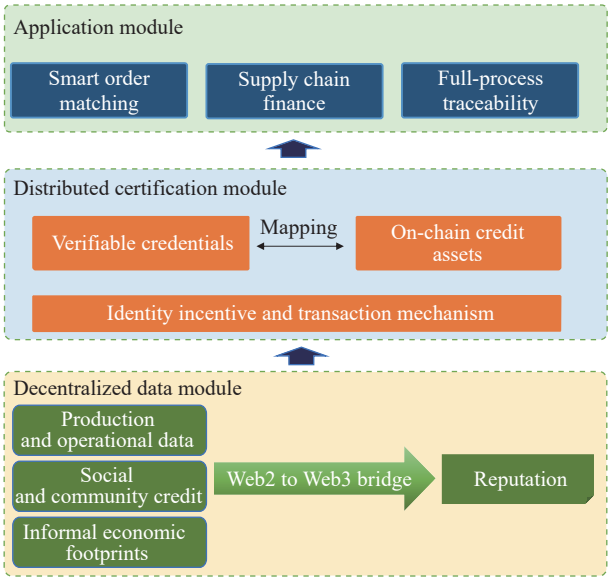

Fig. 1 Model architecture.

are logically associated with the farmer's DID through smart contracts. This mechanism empowers users with data disclosure initiative: farmers can selectively disclose specific fields to meet the trust needs of different business scenarios while protecting data privacy.

B. Distributed Certification Network

The distributed certification network serves as the key hub for trust transfer and the transformation of social credit into economic assets. The network is composed of individuals or institutions acting as certification nodes to distribute verifiable credentials. This behavior represents a credit guarantee by the node for the credential content, backed by a joint liability mechanism: if a credential is falsified, the issuing node's reputation suffers severe penalties.

The core logic of this module involves mapping these VCs to on-chain credit assets. The system dynamically calculates a reputation score based on the quantity and quality of VCs held by a DID. This asset serves as an entry ticket for participating in contract farming. The smart contract monitors transaction status in real-time: performance behavior increases the value of credit assets, while default behavior triggers the automatic destruction of corresponding assets. By linking short-term default gains with the long-term loss of credit capital, the module constructs a robust self-enforcement constraint.

To defend against Sybil attacks and large-scale collusion, the mechanism incorporates three complementary safeguards. First, a reputation-gated issuance threshold requires that only nodes with $R \geqslant R_{\text{cert}}$ (e.g., 600) may issue VCs, making it economically prohibitive for an attacker to bootstrap multiple fake identities to the required reputation level. Second, the joint liability penalty ensures that any node endorsing a fraudulent credential suffers a severe reputation slash ($\Delta R_{\text{certifier}} = -150$), which propagates transitively: if a colluding ring is exposed, all endorsing nodes in the chain are penalized, rapidly destroying the accumulated credit capital of the entire ring. Third, a graph-based anomaly detection module monitors the certification topology for suspicious patterns, such as a single node issuing an abnormally high volume of VCs within a short period, or closed endorsement loops among low-reputation entities, and flags these for on-chain arbitration review. Together, these layers ensure that the cost of mounting a coordinated Sybil or collusion attack far exceeds any potential short-term gain.

C. Application Module

The business application module serves as the operational interface where abstract on-chain credit assets are translated into tangible economic utility across the agricultural ecosystem. Rather than functioning as a siloed technical suite, this layer facilitates the monetization of reputation capital by providing a verifiable foundation for diverse industrial scenarios.

For instance, procurement platforms can leverage these verified capacity credentials to facilitate precise matching. Rather than simply highlighting high-credit scores, marketplaces rely on the reputation system to cryptographically guarantee the authenticity of a farmer's production capacity, thereby effectively reducing information asymmetry and transaction friction. Furthermore, the framework allows financial institutions to recognize on-chain reputation as a viable form of digital collateral. This paradigm shift facilitates the issuance of unsecured, low-interest loans by mitigating the information asymmetry and high risk-assessment costs typically associated with smallholder financing. Finally, the integration of these trust credentials into external supply chain systems grants consumers comprehensive end-to-end transparency. The immutability of the underlying VCs guarantees that the entire lifecycle of agricultural products, from planting to harvest, is grounded in verifiable and tamper-proof production data.

III. Credit Assetization Mechanism for Agricultural Scenarios

This section focuses on the underlying technical implementation supporting the proposed model. Addressing the need for agricultural credit data to possess both asset attributes and semantic interoperability, this study constructs a bidirectional anchoring architecture termed on-chain asset + off-chain semantics. As illustrated in the system architecture, the mechanism involves three core participants: the identity issuer I, the credential holder/farmer U, and the verifier V, shown in Fig. 2.

A. Semantic Gateway and Decentralized Identity

Inspired by the Ethereum Name Service (ENS) architecture, the model introduces a decentralized identity resolution framework to provide a unique smart contract entry point for each individual participant. Within this framework, the identity registry and resolver contract SC_{Reg} is designed to resolve the identity impersonation issue in a decentralized environment. It maintains a global mapping from human-readable identifiers to specific smart contract addresses. Building upon this identity routing mechanism, the identity issuance contract SC_{Iss} serves as the core on-chain carrier for credit assets. It maintains the mapping relationship of the verifiable credentials, logically denoted as $\mathcal{M}: \text{TokenID} \rightarrow (\text{URI}, \text{ContentHash})$, where URI stands for uniform resource identifier.

The semantic gateway serves as the critical cryptographic bridge between the immutable ledger and the heterogeneous physical world. Its mechanism is defined by the following core functions. First, to avoid the prohibitive costs of on-chain storage, the raw semantic details of agricultural behavior are transformed into resource description framework (RDF) triples and stored within the gateway. For every stored dataset D, the gateway ensures that its unique URI is paired with a cryptographic digest $H = \text{Hash}(D)$, which is subsequently anchored in the SC_{Iss} contract.

The gateway acts as a query engine that resolves human-readable requests into structured RDF graphs. When a verifier provides a URI, the gateway does not merely return a file, but provides a verifiable proof of the semantic relationship (sub-ject-predicate-object) that constitutes the farmer's credentials.

The gateway enforces a "trust-but-verify" protocol. While it manages the off-chain data, the integrity is guaranteed by the blockchain. Upon retrieval, the gateway provides both

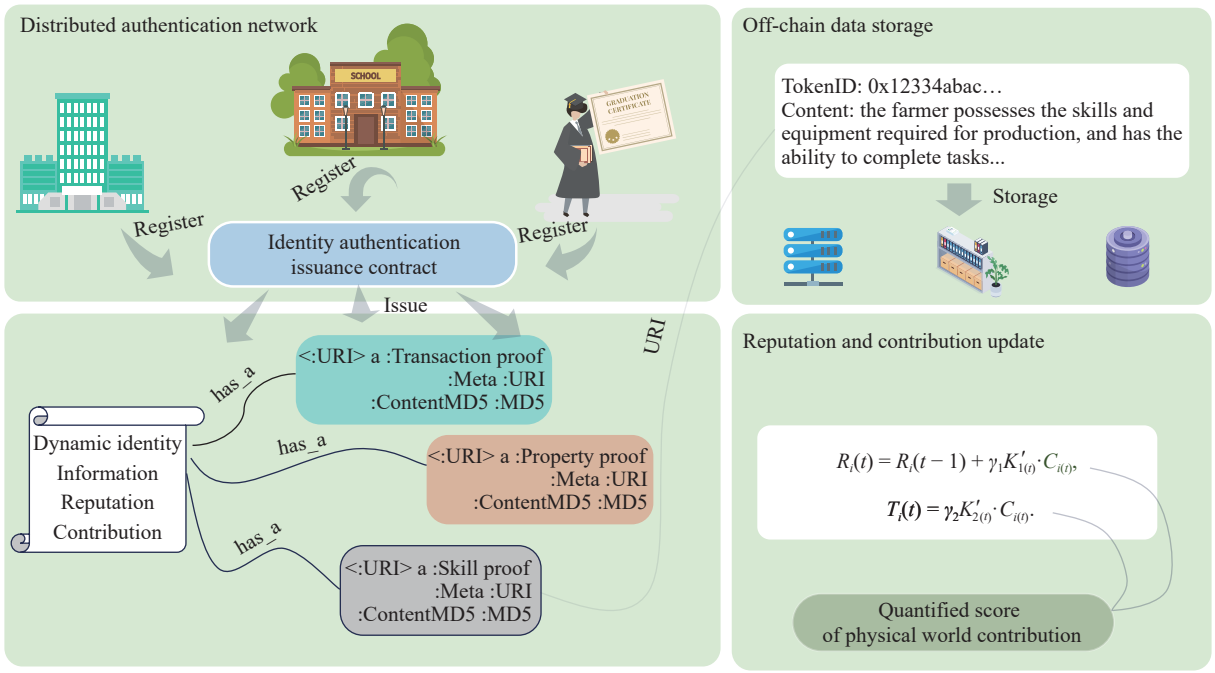

Fig. 2 Credit assetization mechanism.

the raw RDF data and the issuer's signature. The verifier can then independently compute the hash of the retrieved triples and compare it with the on-chain ContentHash to ensure that the gateway has not tampered with the behavioral records.

B. Credential Issuance

The process of transforming offline agricultural attributes into on-chain credit assets begins with the issuer I.

The issuer generates machine-readable RDF data D_{rdf} representing the semantic content off-chain. This is formalized as a set of triples.

$$D_{\text{rdf}} = \{(s,p,o) \mid s = \text{TokenID},\ p \in P,\ o \in O\} \tag{1}$$

where P is the set of predicates and O is the set of object values.

To ensure data integrity, the issuer signs the data using their private key Sk_I and calculates a hash digest h.

$$h = \text{Hash}(D_{\text{rdf}}) \tag{2}$$

$$\sigma = \text{Sign}(\text{Sk}_I, h) \tag{3}$$

The raw D_{rdf} and signature σ are pushed to the semantic gateway.

The issuer calls the identity issuance contract to mint the credential, writing the verification metadata into the blockchain state $\mathcal{S}$.

$$\mathcal{S}' = \mathcal{S} \cup \{(\text{TokenID}, \text{URI}, h, \sigma)\} \tag{4}$$

This minted verifiable credential is then issued to the farmer U, acting as a liquid representation of their reputation.

C. Bidirectional Verification Flow and Reputation Update

A critical prerequisite for triggering smart-contract state transitions is the accurate capture of physical-world events—specifically, whether crops have been delivered and whe-ther their quality matches the contracted specifications. The proposed mechanism could address this through a decentralized oracle layer composed of three complementary channels.

(1) Internet of Things (IoT) sensor feeds: Automated readings from on-site devices (e.g., weight scales at delivery points, soil-moisture sensors, and global positioning system-tagged harvest timestamps) are cryptographically signed at the device level and relayed to the semantic gateway. Each reading is hashed and anchored on-chain, providing tamper-evident physical evidence.

(2) Distributed certification nodes as human oracles: The same reputation-staked certification nodes that issue VCs also serve as human oracles during the delivery phase. Multiple independent nodes inspect the delivered goods and submit attestations. A threshold consensus (e.g., $\geqslant 2$ out of 3 inspectors must agree) is required before the smart contract accepts a delivery confirmation. Because each attestation is tied to the inspector's staked reputation, dishonest reporting triggers the same joint-liability penalty ($\Delta R_{\text{certifier}} = -150$) described in Section II.

(3) Cross-validation: The smart contract cross-checks IoT sensor data against human attestations. A delivery is confirmed only when both channels agree within a configurable tolerance. Discrepancies automatically escalate to the on-chain arbitration module, freezing the transaction until resolution.

This multi-source oracle design ensures that no single point of failure, whether a compromised sensor or a dishonest inspector, can unilaterally trigger or block a contract state transition.

When a farmer U presents his credit credential to a verifier V for business collaboration (e.g., applying for a loan), the system executes a rigorous bidirectional verification flow.

The farmer provides the identity contract address and data

URI. The verifier first queries the registry contract SC_{Reg} to confirm the contract owner's legitimacy, then reads the on-chain ContentHash(h) from the issuance contract. The verifier accesses the semantic gateway via the provided URI to retrieve the raw RDF data D_{rdf}. The verifier computes the hash of the retrieved data locally. The credential is only accepted if two conditions are met:

(1) Integrity: Hash(D_{rdf}) ≡ ContentHash.

(2) Authenticity: Sign(Sk_I, h) is cryptographically valid against the issuer's public key.

Upon successful verification and completion of the agricultural task, the system quantifies the physical contribution into a score $C_i(t)$. This triggers a state transition in the smart contract to dynamically update the farmer's reputation value $R_i(t)$.

$$R_i(t) = R_i(t-1) + \alpha \cdot w(t) \cdot C_i(t) \tag{5}$$

where $R_i(t-1)$ is the accumulated reputation from the previous period, $\alpha \in (0,1]$ is a global baseline weight that controls the overall sensitivity of reputation growth, $w(t)$ is a time-varying adjustment factor that accounts for contextual conditions (e.g., seasonal difficulty or contract scale), and $C_i(t) \in [-1,1]$ is the normalized contribution score derived from the oracle layer: $C_i(t) > 0$ for successful fulfillment and $C_i(t) < 0$ for verified default. In the case study (Section IV), the discrete settlement parameters $\Delta R = 50$ (fulfillment) and $\Delta R = -300$ (default) correspond to specific instantiations of $\alpha \cdot w(t) \cdot C_i(t)$ under the scenario's fixed contract scale. This continuous formulation generalizes the discrete penalties and ensures that verified physical behavior is deterministically mapped into evolving digital credit.

IV. Case Study

To verify the effectiveness of the proposed dynamic updating mechanism and to observe how it reshapes the payoff matrix, we selected a representative agricultural contract farming scenario. This case study highlights the complete lifecycle of a smart contract: mutual verification, price negotiation, execution, and multilateral reputation settlement.

A. Scenario Setup and Initial Parameters

Without loss of generality, we construct a decentralized ecosystem consisting of heterogeneous farmers U and agribusiness merchants V. To confirm mutual capacity for contract fulfillment, both parties must rigorously verify the qualifications held by their counterpart. This is achieved by mutually exchanging and validating verifiable credentials. In this scenario, a strict distributed trust filter is applied: an agent will only acknowledge and accept credentials that are issued or endorsed by an entity possessing a premium reputation score of $R_{cert} \geqslant 600$.

The initial reputation scores at $t = 0$ are initialized as follows:

- **Farmers:** U_1 ($R = 750$, premium veteran), U_2 ($R = 450$, standard performer), U_3 ($R = 0$, new entrant A), U_4 ($R = 0$, new entrant B), and U_5 ($R = 200$, high-risk farmer, history of inconsistent deliveries).
- **Merchants:** V_1 ($R = 800$, premium buyer, pays promptly), V_2 ($R = 450$, standard buyer), and V_3 ($R = 200$, risky buyer, history of delayed payments).

The smart contract governs the reputation settlement. A successful mutual fulfillment yields $\Delta R = 50$ for both the farmer and the merchant. A malicious default triggers a slash penalty $\Delta R = -300$. Crucially, if a verifiable credential issued by a third party is later proven to contain falsified or inaccurate information during arbitration, the certifier suffers a severe penalty for fraudulent endorsement $\Delta R_{certifier} = -150$.

B. Dynamic Evolution of the Scenario

Phase 1 ($t = 1$): Mutual verification and price negotiation. Prior to the planting season, participants initiate matchmaking on the decentralized platform. Unlike traditional centralized systems, trust establishment here is strictly bidirectional.

- **Capacity matching via trusted qualifications:** Merchant V_1 broadcasts a procurement order for a specific crop yield, requiring the farmer to possess sufficient land and farming facilities. Farmer U_1 responds by presenting VCs proving ownership of 50 ha of land. To verify this, V_1 does not blindly trust claims of U_1; instead, V_1 queries the smart contract to check the issuer of these VCs. Discovering that the VCs were minted by a recognized agricultural registry node possessing a premium reputation ($R_{issuer} \geqslant 600$), V_1 trusts the authenticity of the qualifications. Concurrently, U_1 verifies VCs of V_1 regarding payment capacity. Finding that financial VCs of V_1 are endorsed by a premium institutional node ($R_{issuer} \geqslant 600$), U_1 also confirms the qualification of V_1. With mutual capacity cryptographically proven, the contract is successfully established.
- **Reverse filtering of untrusted claims:** Merchant V_3 attempts to purchase crops from farmer U_2, presenting a VC claiming sufficient payment capacity. However, upon querying the blockchain, U_2 discovers that the issuer of credential of V_3 only holds a reputation score of 200 (indicating it is either self-issued by the risky V_3 or endorsed by an untrusted node). Because the issuer's reputation falls drastically below the 600 certification threshold, U_2 deems the financial qualification of V_3 unverified and highly risky. U_2 exercises reverse filtering and rejects the order. Subsequently, U_2 negotiates with merchant V_2. Since V_2 presents capital VCs authenticated by a trusted node ($R_{issuer} \geqslant 600$), U_2 verifies their validity and signs a standard contract matching the capacity of U_2.
- **Capacity endorsement for cold-start:** Farmer U_3 possesses the actual physical capacity (adequate land and planting experience) to fulfill an order for V_1, but holds no VCs from high-reputation issuers. To resolve this, U_3 submits off-chain physical proofs to the premium veteran U_1 ($R_{U1} = 750$). After conducting rigorous off-chain due diligence on actual fields of U_3, U_1 acts as an issuer and mints an endorsed VC validating the capacity of U_3. When U_3 presents this VC, V_1 checks the credential's cryptographic signature. Since the issuer of this VC (U_1) possesses a premium reputation ($750 \geqslant 600$), V_1 accepts the VC as authentic. Mutual trust is logically established, allowing the new entrant U_3 to successfully secure the transaction.

Phase 2 ($t = 2$): Verification audit and multilateral reputation settlement. During the harvest season, the ecosystem undergoes a rigorous verification audit triggered by contract deliveries.

U_1 successfully delivers the crops to V_1 as specified in their high-value contract. Concurrently, V_1 executes the payment instantaneously via the smart contract. The system protocol verifies the transaction's completion and triggers a bilateral reputation reward: U_1 and V_1 both receive $\Delta R = 50$. Similarly, U_2 and V_2 fulfill their standard contract, both earning $\Delta R = 50$.

However, a critical failure occurs in the contract between farmer U_3 and merchant V_1. During the delivery inspection, V_1 discovers that the actual quality and volume of the crops do not match the capacity VCs previously issued by U_1. V_1 triggers the decentralized arbitration function. The investigation reveals that U_3 intentionally falsified their production data (e.g., land productivity and facility status), and U_1, acting as the certifier, failed to perform rigorous off-chain due diligence before minting the VC.

The smart contract executes a multilateral settlement based on the proven misrepresentation. Specifically, U_3 is heavily penalized for fraudulent behavior and contract default, resulting in an updated reputation score of $R_{U3}(2) = 0 - 300 = -300$. Meanwhile, U_1 is penalized for issuing an untruthful certification based on the proven inaccuracy of the endorsed VC content, which updates their reputation score to $R_{U1}(2) = 750 + 50 - 150 = 650$. Finally, V_1 receives automated financial compensation from the contract's staked margin, resulting in an updated reputation score of $R_{V1}(2) = 800 + 50 = 850$.

Phase 3 ($t = 3$): System rebalancing. In the subsequent cycle, the market is rebalanced. U_3 is mathematically blacklisted ($R = -300$). U_1 becomes strictly cautious about issuing future VCs due to the painful joint liability. Observing the severe consequences, the remaining new entrant, U_4, rationally chooses to build initial credit ($\Delta R = 50$) through reliable micro-tasks rather than risking opportunistic behaviors.

C. Execution Results and Analysis

Table 1 and Fig. 3 summarize the reputation dynamics, demonstrating how bilateral verification and settlement reshape the ecosystem.

The deductive walkthrough clearly illustrates that trust in this mechanism is fully bilateral. Farmers are not merely passive receivers; they actively filter out risky merchants prior to negotiation. Furthermore, the multilateral settlement at $t = 2$ proves that the system simultaneously rewards mutual compliance and mathematically punishes malicious acts. The joint liability enforcement on U_1 demonstrates a robust defense against collusion, ensuring that adherence to the negotiated contract remains the only sustainable strategy for both farmers and merchants.

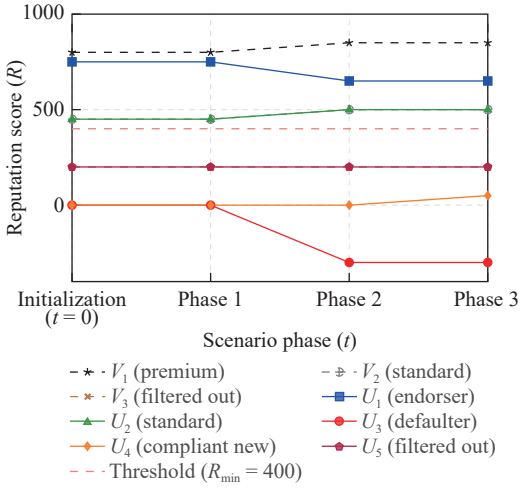

Fig. 3 Dynamic trajectory of all ecosystem agents. Merchants are represented by dashed lines, while farmers are represented by solid lines. The chart visually captures system growth (U_2, V_1, and V_2), severe penalization (U_1 and U_3), gradual cold-start (U_4), and the stagnation of high-risk agents filtered out by the mechanism (U_5 and V_3).

V. Conclusions

This paper presents a novel blockchain-enabled agricultural contract fulfillment mechanism designed to mitigate the long-standing trust deficit and high enforcement costs inherent in smallholder contract farming. By introducing a decentralized identity architecture and a quantifiable credit assetization model, we successfully transition traditional, implicit social reputation into transparent, liquid on-chain credentials.

The multi-agent simulation demonstrated that mapping verifiable physical behavior to a dynamic credit index effectively filters market risks. The smart-contract-driven feedback loops ensure that contract fulfillment becomes a self-enforcing Nash

Table 1 Dynamic reputation score updates across scenario phases.

Role	Agent	$t = 0$ (initialization)	$t = 1$ (verify/negotiate)	$t = 2$ (settle)	$t = 3$ (next cycle)
Farmers	U_1 (premium/endorser)	750	750	650	650
	U_2 (standard)	450	450	500	500
	U_3 (defaulter)	0	0	−300	−300
	U_4 (compliant new)	0	0	0	50
	U_5 (high-risk/filtered)	200	200	200	200
Merchants	V_1 (premium)	800	800	850	850
	V_2 (standard)	450	450	500	500
	V_3 (risky/filtered)	200	200	200	200

equilibrium, heavily penalizing opportunistic defaults through the instant destruction of digital reputation capital. Furthermore, new entrants can leverage the off-chain semantic gateways to overcome initial capital and trust barriers. Future research will focus on scaling the off-chain semantic gateways to handle more complex agricultural IoT data and optimizing privacy-preserving zero-knowledge proofs (ZKPs) during the distributed certification phase.

ACKNOWLEDGMENT

This work was supported by the Science and Technology Development Fund, Macao SAR, China (Nos. 0093/2023/RIA2 and 0157/2024/RIA2).

REFERENCES

[1] A. C. S. Bogado, N. Estrada-Carmona, D. Beillouin, C. Chéron-Bessou, B. Rapidel, and S. K. Jones, Farming for the future: Understanding factors enabling the adoption of diversified farming systems, *Glob. Food Secur.*, 2024, 43, 100820.

[2] M. Gemtou, G. Isakhanyan, and S. Fountas, Advancing climate-smart agriculture: Integrating technology, behavioural insights and policy for a sustainable future, *Smart Agric. Technol.*, 2025, 11, 100861.

[3] J. Gao, Z. Cui, H. Li, and R. Jia, Optimization and coordination of the fresh agricultural product supply chain considering the freshness-keeping effort and information sharing, *Mathematics*, 2023, 11(8), 1922.

[4] V. Singh, S. Agrawal, and S. Kumar, Is effective coordination the key to sustainable performance? A probe into integrated e-agri supply chains in India, *Int. J. Prod. Perform. Manage.*, 2025, 74(5), 1766–1795.

[5] L. Wiseman, J. Sanderson, A. Zhang, and E. Jakku, Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming, *NJAS: Wageningen J. Life Sci.*, 2019, 90&91, 100301.

[6] H. Wang, Y. Wang, and M. S. Delgado, The transition to modern agriculture: Contract farming in developing economies, *Am. J. Agric. Econ.*, 2014, 96(5), 1257–1271.

[7] A. Ruml and M. Qaim, Smallholder farmers' dissatisfaction with contract schemes in spite of economic benefits: Issues of mistrust and lack of transparency, *J. Dev. Stud.*, 2021, 57(7), 1106–1119.

[8] E. M. Meemken and M. F. Bellemare, Smallholder farmers and contract farming in developing countries, *Proc. Natl. Acad. Sci. USA*, 2020, 117(1), 259–264.

[9] M. F. Bellemare and J. R. Bloem, Does contract farming improve welfare? A review, *World Dev.*, 2018, 112, 259–271.

[10] B. Grosh, Contract farming in Africa: An application of the new institutional economics, *J. Afr. Econ.*, 1994, 3(2), 231–261.

[11] C. Eaton and A. W. Shepherd, Contract farming: Partnerships for growth, in *FAO Agricultural Services Bulletin*. Rome, Italy: Food and Agriculture Organization of the United Nations, 2001.

[12] N. Key and D. Runsten, Contract farming, smallholders, and rural development in Latin America: The organization of agroprocessing firms and the scale of outgrower production, *World Dev.*, 1999, 27(2), 381–401.

[13] P. Simmons, P. Winters, and I. Patrick, An analysis of contract farming in East Java, Bali, and Lombok, Indonesia, *Agric. Econ.*, 2005, 33(s3), 513–525.

[14] M. Khapayi, P. Van Niekerk, and C. P. Retief, Challenges of contract farming among small-scale commercial vegetable farmers in Eastern Cape South Africa, *J. Agric. Ext.*, 2018, 22(3), 195–206.

[15] S. Kunte, M. Wollni, and C. Keser, Making it personal: Breach and private ordering in a contract farming experiment, *Eur. Rev. Agric. Econ.*, 2027, 44(1), 121–148.

[16] H. L. Carmichael, Self-enforcing contracts, shirking, and life cycle incentives, *J. Econ. Perspect.*, 1989, 3(4), 65–83.

[17] A. M. Kabungo and G. P. Jenkins, Contract farming risks: A quantitative assessment, *South Afr. J. Econ. Manage. Sci.*, 2016, 19(1), 35–52.

[18] H. Lu, J. H. Trienekens, S. W. F. Omta, and S. Feng, Influence of Guanxi, trust and farmer-specific factors on participation in emerging vegetable markets in China, *NJAS-Wageningen J. Life Sci.*, 2008, 56(1&2), 21–38.

[19] M. Kumarathunga, R. N. Calheiros, and A. Ginige, Smart agricultural futures market: Blockchain technology as a trust enabler between smallholder farmers and buyers, *Sustainability*, 2022, 14(5), 2916.

[20] U. Gurusamy, S. Vijayarajan, P. K. Gunasekaran, and M. Anantharaman, Impact of blockchain technology in agriculture supply chain a comprehensive review of applications, challenges, and future directions, *J. Sustain. Compet. Intell.*, 2025, 15, e0519.

[21] S. Paul, J. I. Joy, S. Sarker, A. A. H. Shakib, S. Ahmed, and A. K. Das, An unorthodox way of farming without intermediaries through blockchain, in *Proc. 2019 International Conference on Sustainable Technologies for Industry*, Dhaka, Bangladesh, 2019.

[22] M. M. Queiroz, R. Telles, and S. H. Bonilla, Blockchain and supply chain management integration: A systematic review of the literature, *Supply Chain Manage.: Int. J.*, 2020, 25(2), 241–254.

[23] I. R. Macneil, Contracts: Adjustment of long-term economic relations under classical and neoclassical, *Northwestern Univ. Law Rev.*, 1978, 72, 854–905.

[24] S. G. Lazzarini, G. J. Miller, and T. R. Zenger, Order with some law: Complementarity versus substitution of formal and informal arrangements, *J. Law, Econ. Organ.*, 2004, 20(2), 261–298.

[25] B. Klein, Contracts and incentives: The role of contract terms in assuring performance, in *Contract Economics*. Oxford, UK: Blackwell, 1992, 149–180.

[26] J. Li, J. Li, X. Wang, R. Qin, Y. Yuan, and F.-Y. Wang, Multi-blockchain based data trading markets with novel pricing mechanisms, *IEEE/CAA J. Autom. Sin.*, 2023, 10(12), 2222–2232.

[27] Y. Yuan and F.-Y. Wang, Blockchain and cryptocurrencies: Model, techniques, and applications, *IEEE Trans. Syst., Man, Cybern.: Syst.*, 2018, 48(9), 1421–1428.

[28] F.-Y. Wang, Parallel philosophy and intelligent science: From Leibniz's Monad to blockchain's DAO, *Pattern Recognit. Artif. Intell.*, 2020, 33(12), 1055–1065.

[29] Y. Wang, M. Kang, Y. Liu, J. Li, K. Xue, X. Wang, J. Du, Y. Tian, Q. Li, and F.-Y. Wang, Can digital intelligence and cyber-physical-social systems achieve global food security and sustainability?, *IEEE/CAA J. Autom. Sin.*, 2023, 10(11), 2070–2080.

[30] J. Lin, Z. Shen, A. Zhang, and Y. Chai, Blockchain and IoT based food traceability for smart agriculture, in *Proc. 3rd International Conference on Crowd Science and Engineering*, Singapore, Singapore, 2018.

[31] F. Tian, A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things, in *Proc. 2017 International Conference on Service Systems and Service Management*, Dalian, China, 2017.

[32] G. Baralla, S. Pinna, and G. Corrias, Ensure traceability in European food supply chain by using a blockchain system, in *Proc. IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain*, Montreal, Canada, 2019.

[33] C.-H. Liao, H.-E. Lin, and S.-M. Yuan, Blockchain-enabled integrated market platform for contract production, *IEEE Access*, 2020, 8, 211007–211027.

[34] S. S. Kamble, A. Gunasekaran, and R. Sharma, Modeling the

blockchain enabled traceability in agriculture supply chain, *Int. J. Inf. Manage.*, 2020, 52, 101967.

[35] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, A survey on essential components of a self-sovereign identity, *Comput. Sci. Rev.*, 2018, 30, 80–86.

[36] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, Digital identities and verifiable credentials, *Bus. Inf. Syst. Eng.*, 2021, 63(5), 603–613.

[37] O. Amraouy, M. Benbrahim, and M. N. Kabbaj, A blockchain- and self-sovereign identity-based collaborative framework for secure and verifiable cross-organizational data sharing in smart irrigation, *Smart Agric. Technol.*, 2025, 12, 101654.

[38] N. R. Puthenveettil and P. K. Sappati, A review of smart contract adoption in agriculture and food industry, *Comput. Electron. Agric.*, 2024, 223, 109061.

Xiaolong Liang received the BS and MS degrees in computer science and technology from Shandong University, Jinan, Shandong, China, in 2011 and 2016, respectively, and the PhD degree in intelligent science and systems from Macau University of Science and Technology, Macau, China, in 2024. He is currently an assistant professor at State Key Laboratory of Multimodal Artificial Intelligence Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. His research interests include blockchain intelligence, DAO, true autonomous organization, intelligent transportation systems, and parallel governance.

Mengzhen Kang received the PhD degree in pattern recognition and intelligent systems from Institution of Automation, Chinese Academy of Sciences, China, in 2003. She is currently an associate professor at State Key Laboratory of Multimodal Artificial Intelligence Systems, Institute of Automation, Chinese Academy of Sciences, China. Her research interests include parallel agriculture and computational plants.

Juanjuan Li received the MS degree in economics from Renmin University of China, Beijing, China, in 2010, and the PhD degree in control science and engineering from Beijing Institute of Technology, Beijing, China, in 2021. She is currently an associate professor at State Key Laboratory of Multimodal Artificial Intelligence Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. Her research interests include blockchain intelligence, Web3, and decision intelligence.

Rui Qin received the PhD degree in computer application technology from University of Chinese Academy of Sciences, Beijing, China, in 2016. She is currently an associate professor at State Key Laboratory of Multimodal Artificial Intelligence Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. Her research interests include blockchain, DAO, and parallel management.