**Blockchain-based decentralized supply chain system with secure**

**Information sharing**

1. Supply Chain Management (SCM):

- Essential for production efficiency and cost reduction.

- Involves various stages like raw material collection, production, transportation, and sales.

- SCM system includes stakeholders such as suppliers, producers, retailers, and users.

2. Challenges in Traditional SCM:

- Information dissymmetry due to stakeholders' geographical dispersion.

- Weak supervision leading to collusion and tampering attacks.

- Dependence on semi-trusted certificate authorities (CAs) in cloud-based SCM systems.

3. Blockchain in SCM:

- Blockchain technology for secure and transparent SCM.

- Previous schemes vulnerable to collusion attacks through the introduction of CAs.

- Proposed decentralized supply chain system leveraging blockchain without fully trusted CAs.

4. Proposed System Features:

- Blockchain-based smart contract for secure registration, authentication, and fair payment.

- Validation mechanisms: one-way validation and transaction-based validation.

- Cryptography for secure transmission and validation of product provenance records.

5. Contributions:

- Introduction of a blockchain-based decentralized supply chain system.

- Construction of validation mechanisms for product provenance record.

- Secure interactive protocols for registration, authentication, and fair payment.

- Scheme resistant to collusion and tampering attacks.

6. Preliminaries:

- Notations used in the proposed scheme.

- Bilinear maps for cryptographic operations.

- Overview of blockchain technology, including structure and transaction representation.

- Smart contracts for automated execution of secure protocols.

7. System Model:

- Involves stakeholders: Supplier, Producer, Retailer, User, Cloud Server, and Blockchain.

- Roles of suppliers, producers, retailers, and users in the supply chain.

- Blockchain as a secure and decentralized management system.

8. Threat Model:

- External adversaries attempting to impersonate valid users.

- Internal adversaries colluding with the cloud server to tamper with product data.

9. Security Goals:

- Privacy-preserving measures against tampering, forgery, and impersonation attacks.

- Record auditability ensuring users can verify product provenance records without revealing original content.

10. System Architecture:

- Integration of smart contracts for secure data management.

- Use of cryptography to integrate product provenance records into blockchain transactions.

11. Security Analysis:

- Demonstration of the scheme's resistance to collusion and tampering attacks.

- Evaluation of the proposed scheme's security measures.

12. Performance Evaluation:

- Assessment of scheme efficiency and feasibility with reasonable computation overhead.

13. Conclusion:

- Summary of proposed scheme features and contributions.

- Reflection on the security, feasibility, and efficiency of the decentralized supply chain system.

14. Future Work:

- Potential enhancements or extensions for future research in blockchain-based SCM.