Blockchain Enabled E-Transaction Security Services Using ECDSA

Prithiv Sivakumar[1], Navaneetha Krishnan Sreethar [1], Nithin Raj R [1]*

[1,2,3] Student – Sri Krishna College of Technology

E-Mail: [1]19tucs150@skct.edu.in, [2]19tucs135@skct.edu.in, [3]19tucs137@skct.edu.in

Abstract

With the changes over time, the current social security system is facing challenges in meeting people's needs for transparency, security, and distributed services. Blockchain technology has been identified as a possible solution to these challenges due to its ability to provide a transparent, tamper-proof, and traceable system that operates through consensus and trust. The proposed solution of a blockchain-based consortium with ECDSA is a promising approach to establishing and improving social security information. This solution addresses the issues of centralization and single control that are seen in the present social security system. The multi-party data sharing and trust mechanism provided by the blockchain consortium enables the blockchain integration between storage systems and IPFS, which facilitates the security of approval documents, photos, and videos related to the accessibility and traceability handling of social security services. By applying this solution to three important social insurance services - applying for social insurance, applying for social benefits, and social benefits online - the blockchain-based consortium can improve the accessibility, security, and traceability of social security services. This approach represents a significant step forward in creating a more efficient and effective social security system that meets people's needs for transparency, security, and distributed services.

Keywords: Blockchain Technology, E- Transactions, Digital Signature Algorithms

1. INTRODUCTION

In A blockchain is defined as a list of records that are called blocks which are linked together using a cryptography function. The cryptographic hash of the previous block serves as a unique identifier that ensures the integrity of the blockchain. The transaction data contained in each block generally represent a Merkle tree[1]. Blockchains use cryptography and a consensus mechanism to ensure that the data stored in each block cannot be tampered with or altered without the agreement of the majority of the nodes in the network. This makes blockchains a secure and reliable way to store and transfer information and has led to their use in a large number of applications, from cryptocurrencies like Bitcoin to supply chain management, voting systems, and more. By creating a decentralized system where no single entity has control over the data, blockchains offer a way to build trust and transparency in a variety of industries[2]. Blockchains are secure by design and provides a distributed computing system with high Byzantine fault tolerance. Transactions are grouped into blocks, which are hashed, and then encoded into a Merkle tree. Every singl block contains an encoded hash of the previous block, linking them together to form a chain that confirms the integrity of all previous blocks. To ensure the integrity of the data, each block is digitally signed. Although forks are possible when blocks are produced concurrently, the consensus mechanism in the blockchain protocol resolves these forks to maintain the accuracy and reliability of the ledger. Overall, blockchains offer a secure and reliable way to store and transfer information in a decentralized manner[3]. Blockchains use a scoring algorithm to select the most valid version of the history, based on a secure hash-based record. Orphan blocks are those which are not selected for inclusion in the blockchain. As a result, peers in the network may contain a varied number of versions of the history at any given time[4]. When a peer obtains a high-scoring version of the blockchain, they update their database and transmit the update to their peers. The block time represents the time it takes to generate a new block in the chain, which can occur as fast as every five seconds. Once a block is completed, the included data becomes verifiable[5].In cryptocurrency, the block time determines the speed of transactions, with shorter block times leading to faster transactions. Ethereum has a block time of 14-15 seconds, while Bitcoin's block time is around 10 minutes. By using a peer-to-peer network to store data, blockchain eliminates the risks associated with centralized data storage[6]. Blockchains rely on decentralized networks that use two methods which are message-passing and distributed networking. However, a risk of centralization, known as a "51% attack," has a possibility to occur when a single entity controls over 50% of the network and is able to exploit the blockchain record, allowing for double-spending. Unlike centralized networks, peer-to-peer networks doesn’t contain vulnerabilities which hackers can exploit, and there is no single point of failure. Blockchain utilizes a cryptography called public key cryptography, where a public key represents an address stored in the blockchain, and valuable tokens are registered as belonging to that address when sent over the network[7].A private key acts as a password that allows access to features and assets stored on a blockchain. Data stored on a blockchain is typically viewed as immutable, preventing any bad actors from accessing it and applications can be added to the network without a need for approval or trust from others. This makes the blockchain a transport layer for various applications[8].

2. LITERATURE REVIEW

Bitcoin uses the network called Peer to Peer with the help of cryptography algorithms for establishing a digital currency system which is distributed. Most of the bitcoin transactions are stored in the block chain and these transactions are visible to everyone. To remove this problem they [9] introduced a coin mixing scheme which enables the users to mix their bitcoins without the help of a third party system. The concept used above is known as the Ring signature with ECDSA. The ECDSA signatures are a 32 byte secret keys in which the block chain transactions are based. These keys can be stoles and to prevent the theft of the keys the concept of java token security can be implemented. Taking into an account of two use cases CCSC which is the first and the second one is inserting the cloud in CCSC java tag which is connected to RACS server. These two use cases are mainly used to enhance the remote use of ECDSA and security [10]. FPGA (Field Programmable Gate Array) is combined with the concept ECDSA which is used for cryptocurrency transactions in block chain. By the above combination of FPGA and ECDSA allows to make the calculations easy and quick [11]. most of the supply chain threats include false documents, duplicate certificates and modified software's. Introducing a block chain based identity management system to mitigate the supply chain threats. The ECDSA in addition to PRF (pseudo random function is used to prevent the problems [12]. To accommodate the block chain systems along with IoT which requires a procedure which can provide higher form of security. The BFT (Byzantine Fault Tolerance) is a consensus mechanism that achieves Durability with no assumptions about the network. Designing a Asynchronous Byzantine Fault Tolerance with ECDSA signatures [13].

Losing a private key causes a unacceptable loss. The traditional portfolio management system stores the portfolio is a unique location which cannot lead to failures [14]. In order to secure the block chain wallets the article provide a unique plan which is contingent on a threshold elliptic curve DSA with no trust center [15]. The ECDSA uses a reverse mechanism during signing and the verification process it reduces the regulation of digital signs.The low uncertainty ECDSA results in random error threats. Considering the above problem a proven safer ECDSA is designed. The concept which is implemented uses double parameters in signing procedure can avoid the random threat on Bitcoins exchange [16].

ECDSA verification tool rely o specified modular arithmetic syllabus. Proposing a ECDSA affirmation tool which can be used for faster sign affirmation. Optimized ECDSA affirmation engine for the Hyper ledger Fabric by migrating different processes to a pre-compute block clarifying disclosure key ECDSA signature verify [17]. Proposing the most effective and large scale affirmation process along with ECDSA based checking. The use of protocols in Hyper ledger fabric and Cryptocurrencies has been evaluated as favourable and also efficient. When bulk affirmations produces incorrect results, by using a pooling method to enhance the planning of incorrect signatures [18]. The huge scale group affirmation with group testing technology rely on ECDSA. When batch affirmation results in incorrect result make use of the group testing ideology to enhance the process of recognizing the incorrect signatures. The extensive imitation results establish that their rules overcomes and more secure then ECDSA [19]. Establishing a threshold ECDSA signing procedure which gives fast signing and also key distribution. It provides a solution for a longstanding problem. It provides the door to a practical use of the Threshold ECDSA signatures[20]. Such type of applications are building the secure crypto wallets where the private key sharing is distributed across a large number of devices and therefore difficult to b stolen [21]. Cryptocurrency invested currencies are strongly protected by sharing keys between the financial organizations and banks the person who has the currency and a third party fiduciary with some votes per person [22]. The new Dynamic Threshold ECDSA sign algorithm can be combined with the transaction systems of block chain which are available all around the world. It implements the values in exchange, adds a protocol for users to combine and withdraw against collusion threats. This system architecture is build it on top of fundamental crytographic sessions which includes ECDSA and also the distributed key generation, distributed computing [23]. Testing the outputs which maintains rules is more effective compared to threshold ECDSA sign protocols.

The methodical attacks to corrupt digital signs of sending data [24]. An enhanced SPA which is against of ECDSA is provided with the energy performance model. A threat case is presented and ECDSA private key can be recruited by the help of established attack process with a trail. The countermeasures for equal energy consuming at atom level are introduced by introducing null protocols in period doubles, additional protocols to the external devices of the block chain [25]

The first achieved protocol based on the elliptic curve is the ECDSA. The security of the protocol depends on the efficiency of discrete algorithm on elliptic curve (ECDLP). This protocol applies due to low it low cost and shorter key values [26]. Analyzing ECDSA disadvantage in block chain , improving its signs with twodifferent keys. By using the two different keys it reduces the loss of key when the other messages are known. This protocol can provide security of ECDSA [27]. Test results and implementation pf ECC and ECDSA is based on the Java tag. The 163 bit Elliptic curve encryption provides the same higher forms of security which is equal to as the RSA 1024 bit key protocol [28]. On accounting the outcomes o the 163 bit elliptic curve encryption the whole process is 5 times faster than the 1024 bit RSA algorithm. Elliptic curve encryption is suitable for use on encrypting and decryption devices which includes smart cards and wireless devices which has limited computes and less energy consumption [29]. Technically implementing a temporary key (public) for all signatures and establishing a new protocol to generate a unique sign for ECDSA. These signs can be authenticated with the temporary public key [30]. Initializing the ECDSA multiple sign process with the group class whereby designing a exchange mechanism to ensure that the malicious parties during the sign phase and it helps in reducing unwanted consumption. These multiple sign can be used within the block chain to reduce the cost of transaction [31]. The world wide used ECDSA algorithm is applied to block chain and Internet Of Things. Performing a comparison between the EdECDSA and ECDSA , the EdECDSA is more powerful and secured than the ECDSA which can be implemented in various fields of the block chain [32]. Focusing on the efficient and re configurable ECDSA protocol hardware implementation which can used with transaction verification in the applications which are related to block chain. Even though the ECDSA is expensive algorithm it provides the most secured algorithm which is in use for cryptocurrency transactions [33]. The established protocol supports the N-bit elliptic curve encryption operations in groups generating, verifying signs on fields for any of those elliptic curves [34]. The final form of this above discussed literature survey provides a new material framework for multiplication and inverse sessions to be applied to ECDSA related group operations[35].

3. PROPOSED SYSTEM :

The proposed system is a Highly secure social security scheme using blockchain technology with ECDSA or Elliptic Curve Digital Signature Algorithm. To achieve a collaboration between many departments in the government sector, the proposed solution from this project is based on this blockchain technology to overcome many obstacles and set-backs like false claims and low efficiency. This can be able to empower social security services, guarantee information security with a credible system and promote information sharing between departments. Every transaction is recorded in multiple nodes with one single node containing a single completed transaction. Thus, every single node is able to participate in monitoring the legitimacy and validity of different transactions. Blockchain network works in a peer-to-peer network architecture where every node has the same power and functions and start P2P communications to prevent an individual receiving special power to censor or wipe transaction data and occupy the resources. This concept of the authentication process being decentralized means that every single node will check the validity of the transaction in progress and will only allow it to be completed once all the nodes approve that single transaction. In 1997, smart contracts were first introduced by Nick Szabo. A smart contract is defined as a code created in a decentralized network that is able to be executed automatically and also stored, published, managed and controlled by each separate node of the network. There are 3 separate elements in a smart contract. They are: Autonomy- contract is able to function automatically once it is started without any help, Self- Sufficiency-smart contracts in the blockchain are self-sufficient to collect data.

4. MODULES OF THE PROJECT

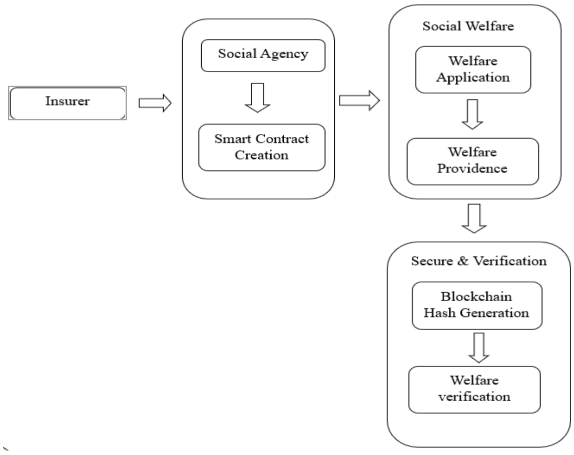
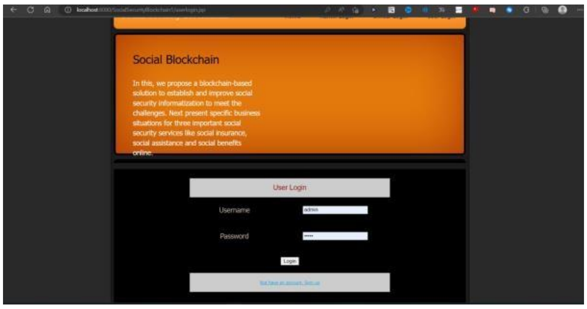


Figure 1. System Flow Diagram

1. Insurer Module

The insurer is the user who can receive the social benefit amount or the insurance amount. Insurers can be elderly, disabled or lower-class families. The insurance company can apply to this application and can apply for the plan or the amount of social assistance and can know the status of whether it is approved or not. The blockchain will be used to secure user transactions, i.e. execute the program and benefit from social support.



In this, we propose a blockchain-based solution to establish and improve social security informatization to meet the challenges. Next present specific business situations for three important social security services like social insurance, social assistance and social benefits online.

Username admin

Password *****

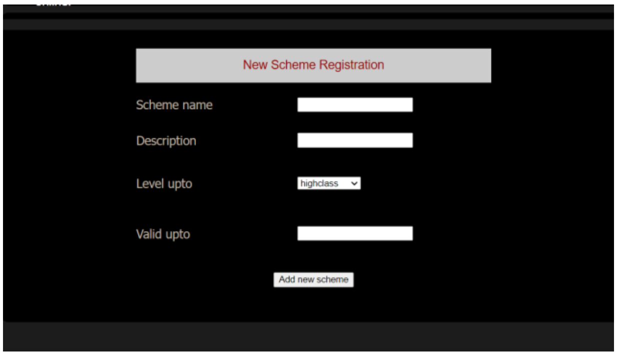
Figure 2. Insurer module

2. Social Agency Module

The social agency is the user who pays the amount of the program, insurance or social allowance. The social agency can be the government, a company or an established businessman. The above candidates can register in this application and approve the applicable user requirements. The blockchain will be used to secure user transactions.

3. Smart Contract Creation

Smart contracts are a collection of code and data residing on the Ethereum blockchain within one address. However, these contracts are not under the user control but are created on the network and can run on a specific schedule. The user is then able to perform transactions with the help of the smart contracts with the specific functions defined on that same contract. They are able to define rules similar to a normal contract and execute the rules through code automatically.



New Scheme Registration

Scheme name

Description

Level upto: highclass

Valid upto

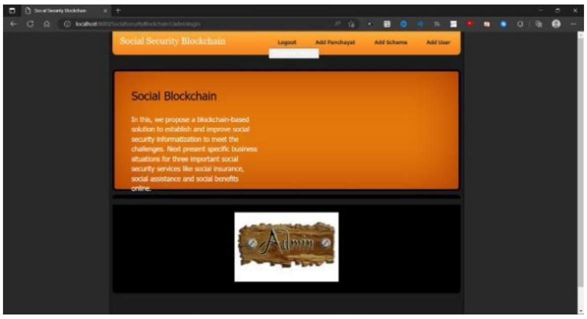
Figure 3. Smart Contract Creation

4. Social Welfare Application

The Social Assistance Application is a financial aid program for socially disadvantaged individuals or families. Often fully or partially funded by the government, social protection programs are designed to cover the cost of food, housing, healthcare, childcare, and more. Most applications for social assistance include a list of eligibility criteria for those who wish to receive financial assistance.

5. Social welfare Providence

Providence staff are professionals who take care of patients and the patient's families. Their knowledge and skills enable the staff to become mentors, promoters, counsellors, organisers and more. People helping the patients can use a combination of resources to secure a safe stay, discharge and recovery in hospitals.



Social Blockchain

In this, we propose a blockchain-based solution to establish and improve social security informatization to meet the challenges. Next present specific business situations for three important social security services like social insurance, social assistance and social benefits online.

Figure 4. Social Welfare Providence

6. Blockchain Hash Generation

Blockchain hash generation collects user inputs as alphabets, numerical digits and media files of varied length and is able to convert it to a fixed length. This length can be different when used by the hash function. It produces an output which is called a hash from a one-way function.

7. Welfare Verification Module

Social welfare is a government support service that is provided to people who needs the welfare for basic necessities including food and shelter. Social security can be similar to welfare which refers to insurance programs giving support to people who may have contributed before unlike assistance programs which is able to provide on the basis of human needs.

5. CONCLUSION

Social Security services are enabled by smart contracts. Hyperledger fabric's contract are ran in virtual machines compared to Ethereum which runs in gas when executing the contracts as virtual machines does not need gas. This proposed solution is able to help users to apply for social services and provide minimum living guarantee. It also stores all the records on the blockchain network and privacy, trust and security are created by the many features of the blockchain network.

Demonstrated the combination of IPFS storage system and blockchain technology to accommodate secured access to data related to transactions in social security services and reducing the necessity for paper documents to receive approvals and solved problems like difficulty in verification of staff and repeated clerk submissions.

This proposed system and its implementation and other elements have been introduced and studied in this article for business processing, to provide a convenient and safety for the public and staff and at the same time, the private data characteristics and channel isolation have been used to make sure the security and efficiency of private user data and public services.

References

[1] Liu, Y., Liu, X., Tang, C., Wang, J., & Zhang, L. (2018). Unlinkable coin mixing scheme for transaction privacy enhancement of bitcoin. IEEE Access, 6, 23261-23270.

[2] Urien, P. (2018, February). Towards secure elements for trusted transactions in the blockchain and blockchain IoT (biot) platforms. invited paper. In 2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ) (pp. 1-5). IEEE.

[3] Tachibana, S., Araki, S., Kajihara, S., Azuchi, S., Nakajo, Y., & Shoda, H. (2019, May). FPGA implementation of ECDSA for Blockchain. In 2019 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW) (pp. 1-2). IEEE.

[4] Sani, A. S., Yuan, D., Meng, K., & Dong, Z. Y. (2020, August). Index: A Blockchain-based Identity Management System for Supply Chain Attacks Mitigation in Smart Grids. In 2020 IEEE Power & Energy Society General Meeting (PESGM) (pp. 1-5). IEEE.

[5] Knudsen, H., Li, J., Notland, J. S., Haro, P. H., & Ræder, T. B. (2021, December). High-performance asynchronous byzantine fault tolerance consensus protocol. In 2021 IEEE International Conference on Blockchain (Blockchain) (pp. 476- 483). IEEE.

[6] Jian, Z., Ran, Q., & Liyan, S. (2021, January). Securing blockchain wallets

efficiently based on threshold ECDSA scheme without a trusted center. In 2021 Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS) (pp. 47-51). IEEE.

[7] Liu, S. G., Chen, W. Q., & Liu, J. L. (2021). An efficient double parameter elliptic curve digital signature algorithm for blockchain. IEEE Access, 9, 77058-77066.

[8] Agrawal, R., Yang, J., & Javaid, H. (2022, July). Efficient FPGA-based ECDSA Verification Engine for Permissioned Blockchains. In 2022 IEEE 33rd International Conference on Application-specific Systems, Architectures and Processors (ASAP) (pp. 148-155). IEEE.

[9] Xiong, H., Jin, C., Alazab, M., Yeh, K. H., Wang, H., Gadekallu, T. R., ... & Su, C. (2021). On the design of blockchain-based ECDSA with fault- tolerant batch verification protocol for blockchain-enabled IoMT. IEEE journal of biomedical and health informatics, 26(5), 1977-1986.

[10] Nyame, G., Qin, Z., Obour Agyekum, K. O. B., & Sifah, E. B. (2020). An ECDSA approach to access control in knowledge management systems using blockchain. Information, 11(2), 111.

[11] Lindell, Y., & Nof, A. (2018, October). Fast secure multiparty ECDSA with practical distributed key generation and applications to cryptocurrency custody. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1837-1854).

[12] Wang, H., Ma, W., Deng, F., Zheng, H., & Wu, Q. (2021). Dynamic threshold ECDSA signature and application to asset custody in the blockchain. Journal of Information Security and Applications, 61, 102805.

[13] Wunan, W., Hao, C., & Jun, C. (2019, July). The attack case of ECDSA on the lockchain is based on improved simple power analysis. In International Conference on Artificial Intelligence and Security (pp. 120- 132). Springer, Cham.

[14] Hussein, N. T., & Kashmar, A. H. (2020, November). An Improvement of ECDSA Weak Randomness in Blockchain. In IOP Conference Series: Materials Science and Engineering (Vol. 928, No. 3, p. 032022). IOP Publishing.

[15] Han, J. H., Kim, Y. J., Jun, S. I., Chung, K. I., & Seo, C. H. (2002, July). Implementation of ECC/ECDSA cryptography algorithms based on Java card. In Proceedings 22nd International Conference on Distributed Computing Systems Workshops (pp. 272-276). IEEE.

[16] Pan, S., Chan, K. Y., Cui, H., & Yuen, T. H. (2022). Multi-signatures for ECDSA and Its Applications in Blockchain. In Australasian Conference on Information Security and Privacy (pp. 265-285). Springer, Cham.

[17] Guruprakash, J., & Koppu, S. (2022). An Empirical Study to Demonstrate that EdDSA can be used as a Performance Improvement Alternative to ECDSA in Blockchain and IoT, 46(2).

[18] Devika, K. N., & Bhakthavatchalu, R. (2021). Efficient hardware prototype of ECDSA modules for blockchain applications. TELKOMNIKA (Telecommunication Computing Electronics and Control), 19(5), 1636-1647.

[19] Aumasson, J. P., Hamelink, A., & Shlomovits, O. (2020). A survey of ECDSA

threshold signing. Cryptology ePrint Archive.

[20] Shlomovits, O., & Seres, I. A. (2019). Sharelock: mixing for cryptocurrencies from multiparty ecdsa.

[21] Narbayeva, S., Bakibayev, T., Abeshev, K., Makarova, I., Shubenkova, K., & Pashkevich, A. (2020). Blockchain technology on the way of autonomous vehicle development. transportation research Procedia, 44, 168-175.

[22] Yi, X., & Lam, K. Y. (2019, July). A new blind ECDSA scheme for bitcoin transaction anonymity. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (pp. 613- 620).

[23] Umran, S. M., Lu, S., Abduljabbar, Z. A., Zhu, J., & Wu, J. (2021). Secure data of industrial internet of things in a cement factory based on Blockchain technology. Applied Sciences, 11(14), 6376.

[24] Taleb, N. (2019). Prospective applications of blockchain and bitcoin cryptocurrency technology. TEM Journal, 8(1), 48-55.

[25] Lin, C., He, D., Huang, X., Kumar, N., & Choo, K. K. R. (2020). BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 22(12), 7408-7420.

[26] X. Xu, M. J. Rothrock, A. Mohan, G. D. Kumar, and A. Mishra, ''Using farm management practices to predict Campylobacter prevalence in pastured poultry farms,'' Poultry Sci., vol. 100, no. 6, Jun. 2021, Art. no. 101122.

[27] H. Hasnah, R. Hariance, and M. Hendri, ''Analysis of the implementation of Indonesian sustainable palm oil-ISPO certification at farmer level in west Pasaman regency,'' IOP Conf. Ser., Earth Environ. Sci., vol. 741, no. 1, May 2021, Art. no. 012072.

[28] W. Cai, L. Yu, R. Wang, N. Liu, and E. Deng, ''Research on application system development method based on blockchain,'' J. Softw., vol. 28, no. 6, pp. 1474–1487, 2017.

[29] M. Chen, M. A. G. von Keyserlingk, S. Magliocco, and D. M. Weary, ''Employee management and animal care: A comparative ethnography of two large-scale dairy farms in China,'' Animals, vol. 11, no. 5, p. 2357, Apr. 2021.

[30] L. Montoro-Dasi, A. Villagra, S. Vega, and C. Marin, ''Influence of farm management on the dynamics of Salmonella enterica serovar infantis shedding and antibiotic resistance during the growing period of broiler chickens,'' Vet. Rec., vol. 188, no. 10, p. e302, Apr. 2021.

[31] L. Wu, X. Liu, H. Yang, and X. Ma, ''How agricultural management practicesaffect nitrogen transportation and redistribution under the dryingrewetting process of loessial sloping lands?'' Agricult., Ecosyst. Environ., vol. 315, Aug. 2021, Art. no. 107440.

[32] E. Androulaki, ''Hyperledger fabric: A distributed operating system for permissioned blockchains,'' in Proc. 13th EuroSys Conf., Apr. 2018, pp. 1–15.

[33] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, ''Blockchain architectures for physical internet: A vision, features, requirements, and

applications,'' IEEE Netw., vol. 35, no. 2, pp. 174– 181, Mar. 2021.

[34] S. Li, T. Qin, and G. Min, ''Blockchain-based digital forensics investigation framework in the Internet of Things and social systems,'' IEEE Trans. Computat. Social Syst., vol. 6, no. 6, pp. 1433– 1441, Dec. 2019, doi: 10.1109/TCSS.2019.2927431.

[35] J. A. T. Casallas, J. M. Cueva- Lovelle, and J. I. Rodríguez Molano, ''Smart contracts with blockchain in the public sector,'' Int. J. Interact. Multimedia Artif. Intell., vol. 6, no. 3, p. 63, 2020.