

# Privacy preserving ZK-STARK based blockchain for agriculture food supply chain

Madhuri Sadashiv Arade, Nitin N. Pise

Department of Computer Engineering and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India

## Article Info

### Article history:

Received Apr 24, 2024

Revised Sep 11, 2024

Accepted Sep 30, 2024

### Keywords:

Blockchain

Food supply chain

Privacy preservation

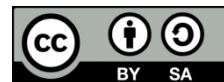
Zero knowledge proof

ZK-STARK

## ABSTRACT

The blockchain-based applications such as food supply chain (FSC), healthcare are becoming increasingly popular due to their decentralized nature, distributed structure, and the ability to track products. Still, there are concerns regarding the privacy of transacted data, including personal identities, as all transactions are recorded on a ledger accessible to participating nodes. Existing technologies of privacy preservation are vulnerable to quantum attacks, which will pose a significant threat to blockchain applications in the future. To address this, a proposed model uses modified zero-knowledge scalable transparent argument of knowledge (ZK-STARK) in the blockchain FSC by utilizing three different polynomial interpolation methods. Performance measurements indicate that the fast fourier transform (FFT) outperforms the others. Unlike ZK-SNARK, ZK-STARK does not require a trusted setup, makes scalable and transparent. By defending against quantum attacks, this model enhances the security of the blockchain system. The blockchain-based FSC is implemented using hyperledger composer, with all entities completing transactions privately through ZK-STARK and smart contracts. But, ZK-STARK may add performance overhead into the blockchain FSC. Future work will aim to reduce the performance overhead of ZK-STARK, decide which operations should be off-chain or on-chain, and compare the performance of this new model to the existing system.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Madhuri Sadashiv Arade

Department of Computer Engineering and Technology

Dr. Vishwanath Karad MIT World Peace University

Pune, Maharashtra, India

Email: arademadhuri15@gmail.com

## 1. INTRODUCTION

Nakamoto [1] introduced bitcoin, a form of cryptocurrency designed for decentralized transactions, eliminating the need for third-party interference. This was made possible through a ledger of records maintained by all participating nodes, and the verification of transactions was achieved through a consensus algorithm known as proof of work. As cryptocurrencies gained popularity, the blockchain technology experienced a significant surge. Blockchain refers to a chain of blocks shown in Figure 1, that are interconnected through pointer addresses. Each time a new block is validated by the consensus algorithm, it is added to the transaction history. Blockchain applications have gained popularity due to their distributed, transparent, and traceable nature of data storage across multiple nodes. Each participating node has access to the data and can ensure the integrity of data transactions. Initially, Bitcoin [1] was primarily used for financial transactions, but the blockchain technology has now been widely adopted for various real-life applications such as hospital management, supply chain management and financial systems.



Figure 1. Blockchain illustration

This research paper considers an agricultural-based food supply chain (FSC) system as a use case to provide traceability while prioritizing privacy. Commercial projects have been implemented to trace food items in the supply chain. For instance, IBM implemented a blockchain solution [2] for Walmart to trace fruit items like mangoes. IBM used hyperledger fabric, a permission based blockchain to implement it. This implementation significantly reduced the time required to trace the journey of a mango from 7 days to just 2.2 seconds.

The blockchain based agriculture FSC must guarantee the authenticity and quality of the food product for the consumer. The consumer can efficiently ascertain the traceability of the food’s origin through the use of blockchain technology. The following entities are involved in this blockchain system as shown in Figure 2.

- a) Farmer/food producer: this is the initial entity involved in the blockchain. They produce food products and register personal information along with details such as quantity, originality, and quality of the products to the blockchain application. The ownership of the products is transferred to the next entity, the food processor, through a smart contract, and a new block is added to the transaction.
- b) Food processor: the food processor is the second entity participating in the blockchain. They process the food items and make them ready for delivery. Once the ownership of the products is transferred to the distributor, a new block is added to the transaction.
- c) Distributor: the distributor is responsible for distributing the food items to retailers. The process of transferring ownership from the distributor to the retailer is repeated, and a new block is added to the transaction.
- d) Retailer: the retailer purchases the items from the distributor and transfers them to the customers.
- e) Consumer: the consumer is the final entity in this process. They can trace the originality of the food items through the transaction details recorded in the blockchain.

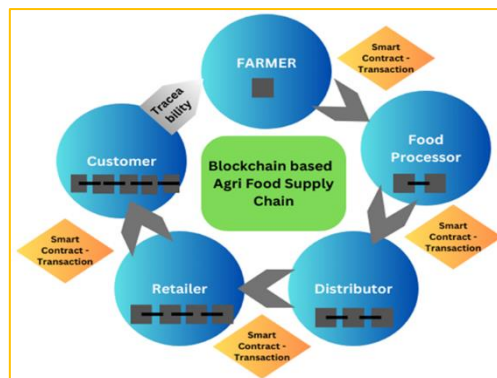


Figure 2. Blockchain based agri-FSC management system

Currently, blockchain applications in the FSC, as well as other domains, offer traceability and a certain level of privacy through the use of permissioned blockchain platforms like hyperledger fabric. Some researchers have employed cryptographic algorithms to enhance data privacy during transactions. Recently, the use of zero-knowledge proof (ZKP) algorithms [3], [4], particularly ZK-SNARK, has been explored to implement privacy in blockchain applications. These cryptographic algorithms, including ZK-SNARK, provide data security. However, a limitation is that they are susceptible to quantum attacks. In the coming years, quantum computers with their immense computing power could potentially compromise blockchain applications with ease, posing a significant threat. Therefore, the motivation behind this research is to develop defences against quantum attacks [5] while ensuring efficient data privacy in blockchain applications.

The primary contribution of this research paper is the application of a modified ZK-STARK privacy-preserving algorithm to the blockchain-based FSC. The key steps are as follows:

- i) Converting information that needs privacy preservation into mathematical expressions.
- ii) Modifying ZK-STARK with three different polynomial interpolations (lagrange polynomial interpolation, barycentric lagrange interpolation, and fast fourier transform (FFT)) for algebraic transformation.
- iii) Testing and comparing the performance of these three polynomial interpolations within the ZK-STARK algorithm.
- iv) Implementing the blockchain FSC using hyperledger composer.

This paper is organized as follows: section 2 presents the related work, serving as a literature review of previous studies. In section 3 introduces the proposed novel ZK-STARK algorithm. In section 4 discusses the experiments and results. The final section offers the conclusion.

## 2. RELATED WORK

To date, most of the work in this area has used various cryptographic techniques, such as proxy re-encryption, ring signatures, homomorphic encryption, secure multiparty computation, and zero-knowledge proofs (specifically ZK-SNARK). The Figure 3 enlist these techniques in brief. Here is a brief explanation of each technique:

- Zero-knowledge proofs [4] allow a user to prove that they know required information without accessing the actual information. This protects the privacy of users who participate in blockchain transactions by allowing them to prove their identity or ownership of certain assets without revealing any details about the information. There are three criteria that a ZKP must satisfy: i) completeness: if the statement is true, an honest verifier will be convinced of its truth by the prover; ii) soundness: if the statement is false, the prover cannot prove or convince the verifier of its truth; and iii) zero knowledge: if the statement is true, the verifier will not gain any information other than the fact it self. In a practical example within the context of blockchain supply chains, let's consider a transaction where a participant farmer conducts a transaction with a food processor. In this scenario, the farmer can prove to the food processor that the transaction data contains correct information regarding the quality and originality of the food item, without revealing any other information, such as the farmer's personal identity. Gong *at al.* [4] presented a paper on comparative analysis of ZKP algorithms as ZK-SNARK, ZK-STARK, MPC based algorithm and BulletProof in different aspects as given in the Table 1.
- Proxy re-encryption [6] allows a user to encrypt data so that only another user can decrypt it. This technique protects the privacy of data transactions by allowing users to share their encrypted data with others without revealing the plaintext content.
- Ring signatures [7] allow a user to sign a message without revealing their identity. This can be used to protect the privacy of users who participate in blockchain transactions.
- Homomorphic encryption [8] performs computations on encrypted data without its decryption. This protects the privacy of data transactions without revealing the plaintext content.
- Secure multiparty computation [9] includes different parties with their own input and performs function on encrypted data with hiding inputs.

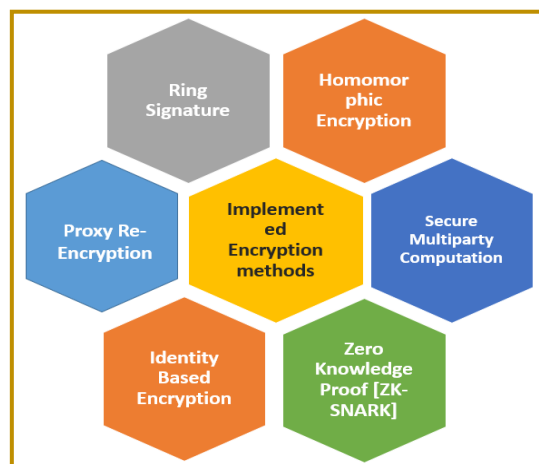


Figure 3. Existing encryption techniques in blockchain

Table 1. Comparison analysis of different ZKP

| ZKP algorithms | Trusted setup | Proof length and complexity  | Application  | Quantum threat                                    |
|----------------|---------------|--|--|---|
| ZK-SNARK       | Yes           | Short proof length, less storage, linear complexity  | Applicable to blockchain, zcash, Filecoin, Loopring DEX 3.0.                                 | Vulnerable to quantum attacks                     |
| ZK-STARK       | No            | Very fast prover time and verification time, large scale computation performs better than ZK-SNARK | Starkware company developing applications, development phase                                 | Provides security against post quantum            |
| MPC BASED      | No            | Large proof – not scalable, high verification cost,  | PICNIC –effective signature scheme provides post quantum security, unsuitable for blockchain | Picnic, a postquantum digital signature algorithm |
| Bulletproof    | No            | Proof size smaller, proof size grows logarithmically   | Low and medium complexity transactions applications- private blockchain                      | Vulnerable to quantum attacks                     |

Boo *et al.* [10] proposed a model that developed a lightweight version of the ZKP protocol suitable for blockchain transactions. The authors aimed to address the system overhead caused by storing data on internet of things (IoT) devices. They introduced a light version of ZKP, specifically ZK-SNARK, which minimized the computational burden by implementing a minimal Merkle tree and integrating ZKP with off-chain payment channels. In their implementation, Raspberry Pi devices served as the IoT devices, while the Ganache-cli Ethereum platform was used to create a private blockchain system. The results of their study indicated that utilizing the lightweight ZKP approach improved efficiency and showed promising potential for real-world implementation.

In a research paper, Mouris and Tsoutsos [11] developed and executed the Zlich framework, a ZKP system, using the Zerojava language with a cross-compiler. Unlike other models, this framework does not rely on a trusted setup for ZKP. Instead, it utilizes traditional instruction sequences rather than arithmetic circuits. The Zlich framework is characterized by its transparency, universality, and resilience against post-quantum threats, achieved by incorporating the ZK-STARK protocol. Li *et al.* [12] designed shellproof an efficient ZKP by modifying the Bulletproof inner product argument by using compression technique. This research Shellproof reduced proof size and computation cost by half of bulletproof proof size as well computation cost.

Gaba *et al.* [13] specifically focus on the healthcare sector and propose a method for maintaining data privacy through authentication key management based on ZKP. Their work demonstrates that the proposed method is both secure and robust against various attacks, such as man-in-the-middle (MITM) attacks and replay attacks. Furthermore, it offers data integrity, confidentiality, and protection against cyber-attacks.

Konkin and Zapechnikov [14] sheds light on the topic of privacy in transactions, specifically addressing identity privacy and transaction privacy. In their research, they utilized a non-interactive zero knowledge proof (NIZK) protocol within a corporate blockchain framework called Masterchain, which is built on the Ethereum platform. However, this article does not provide any specific results.

Guan *et al.* [15] designed BlockMaze for account model blockchain (Ethereum) using ZK-SNARK for secure transactions. This research used Libsnark and go-Ethereum for implementation. Yang and Li [16] proposed a protocol BZDIMS for keeping identity private using ZKP system in blockchain by implementing challenge response model. Zheng *et al.* [17] used non-interactive ZK-SNARK and homomorphic encryption to preserve privacy of the patient information and insurance company while transacting with blockchain. Ma *et al.* [18] designed a privacy preserving account model in supply chain using homomorphic encryption and novel NIZK for encryption of balance and transaction amount. This novel NIZK algorithm proves better in terms of small proof size, minimum computation cost than ZK-SNARK, ZK-STARK and bulletproof. Junejo *et al.* [19] used ZK-SNARK to preserve privacy in their system.

Sharma *et al.* [20] developed novel authentication system for healthcare insurance scheme using ZK-SNARK and proxy encryption (hybrid symmetric- asymmetric encryption) for access control. E-card shared with customer used to generate ZKP. Data stored using IPFS. Results shown it performs better than AWS S3. Bhadra *et al.* [21] developed a novel blockchain FSC overcoming the limitations of payment system, governance. In blockchain supply chain, their own payment system implemented. The government policies are included for farmer, those income less than some criteria. The implemented platform is Ethereum and tested by hyperledger caliper.

### 3. PROPOSED METHOD

#### 3.1. ZK-STARK algorithm

ZK-STARK is a zero-knowledge scalable transparent argument of knowledge. It is one type of ZKP introduced in Santis *et al.* [22], Berentsen *et al.* [23], Ben-Sasson *et al.* [24]. Steps are written as following for ZK-STARK.

- 1) Defining statement to be proved by prover.
- 2) Convert the statement into algebraic problem I working with polynomials and transformation.
- 3) Verifying polynomials is of low degree or not by using FRI (fast reed-solomon interactive oracle proofs of proximity) protocol.
- 4) If it is a low degree, then the initial statement is true.

ZK-STARK is efficient, scalable and transparent as it is not using any trusted setup and is secure. As without revealing other information, the prover can prove the data integrity.

#### 3.2. ZK-STARK algorithm in blockchain food supply chain

The objective of our proposed work is to utilize ZK-STARK for blockchain in FSC to ensure the privacy of sensitive information, including personal identity and the quality of food products, while keeping the food processing techniques confidential. As shown in the Figure 4, all participating entities are proving their transaction details to the next entity. So, in every transaction while transferring ownership, the ZK-STARK protocol will be included, it executes and prove the proof. Our case study focuses on the production of jaggery from sugarcane crops. During the conversion process of sugarcane to jaggery, which involves various food processing techniques, it is crucial to maintain the confidentiality of these methods. The customer should only have access to information regarding the originality and quality of the jaggery, without being exposed to the specific food processing secrets.

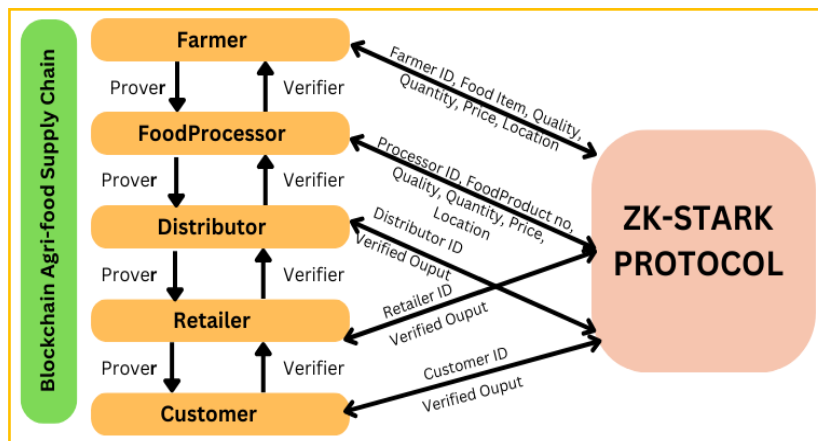


Figure 4. ZK-STARK for blockchain agriculture FSC

The steps involved for transferring information using ZK-STARK from one entity to another are as follow. We assume that jaggery has been produced by a food processor and it is now transferring to the next entity distributor. We have to keep secret data as food processing technique. Algorithm 1 shows the working of the algorithm.

#### Algorithm 1. Using ZK-STARK for preserving privacy

Entities involved - Food processor (FD), distributor (D)

Input - Jaggery item serial number, food processing technique, food safety result, location, quantity, price

Steps -

1. Two inputs, Jaggery serial number and food safety result, will be provided to the ZK-STARK protocol.
2. These inputs will generate a polynomial representation of the data.
3. The prover will output a polynomial that demonstrates a specific property of the food item, it is safe and of desired quality.
4. The verifier will use the FRI protocol to check if the polynomial created by the prover possesses the desired property, provided it is of low degree.
5. If the polynomial is of low degree, it indicates that the prover's statement is

true, confirming that the jaggery item is of the desired quality and origin.  
 6. By proving the claimed quality of the food item without revealing other data, the privacy of the transaction between the food processor and distributor is preserved.  
 Output - Verified proof

The ZK-STARK algorithm uses lagrange polynomial interpolation [25] by default. For this research, we experimented with different interpolations such as barycentric lagrange interpolation [26] and FFT [27], and compared their performance against the lagrange polynomial interpolation.

First, we will formulate our organic jaggery usecase into the mathematical expression (J). We use I=4, where I means ingredients (I<sub>1</sub>, I<sub>2</sub> are organic ingredients and I<sub>3</sub>, I<sub>4</sub> are inorganic ingredients).

$$\begin{aligned}
 J &= [I_1, I_2, I_3, I_4] \\
 J_{true} &= [1, 1, 0, 0]
 \end{aligned}
 \tag{1}$$

In (1) satisfies the statement (I<sub>1</sub>, I<sub>2</sub> are organic ingredients value set to 1, I<sub>3</sub>, I<sub>4</sub> are non-organic ingredients represented by 0).

$$J_{false} = [1, 1, 2, 2]
 \tag{2}$$

In (2) does not satisfy the statement (as I<sub>3</sub>, I<sub>4</sub> are set to other than 0, indicating presence of non-organic ingredients).

The prover and verifier must agree on the conditions for following statement is true.

$$J_i^2 - J_i = 0, \text{ where } i = 0, 1, \dots, I - 1
 \tag{3}$$

We used three different polynomial interpolations langrange polynomial interpolation, barycentric lagrange interpolation, FFT to convert (3) into polynomial expression given in Table 2. This polynomial interpolation includes three steps: i) creating polynomial interpolation equations, ii) finding constraint polynomial, and iii) forming composition polynomial.

The composition polynomial will create Merkle tree proof which will be used for low degree testing. As given in Table 3, we can use the constraint to trace the polynomial contains 1 or 0 if the statement is true.  $J_i^2 - J_i$  where,  $i = 0; 1; \dots; I - 1$  and define this expression as the constraint polynomial  $c(x)$  with (4).

$$c(x) = f(x)^2 - f(x) = 0
 \tag{4}$$

Table 2. Polynomial interpolations with formulas and  $f(x)$  values

| Sr. no | Polynomial interpolation equation  | Polynomial equation formula  | $f(x)$                                     |
|--------|------------------------------------|--|--|
| 1      | Lagrange interpolation             | $p(x) = \sum_{i=0}^3 y_i \cdot li(x)$ Where<br>$P(x)$ :- Lagrange interpolation polynomial,<br>$y_i$ :- y-coordinates<br>$li(x)$ :- Lagrange basis polynomials.  | $f(x) = -60x^3 - 68x - 128$                |
| 2      | Barycentric lagrange interpolation | $p(x) = \frac{\sum_{j=0}^n \frac{w_j}{x - x_j} f_j}{\sum_{j=0}^n \frac{w_j}{x - x_j}}$ Where<br>$P(x)$ :- Barycentric interpolation polynomial,<br>$w_i$ :- Weight at each point, $f_j$ :- Data Factor | $f(x) = 2x^3 - 771x^2 + 12561x + 13758208$ |
| 3      | FFT                                | $X_k = \sum_{m=0}^{n-1} x_m e^{-i2\pi km/n}$ For $k = 0, 1, \dots, n - 1$ , Here, $Y_k$ are the values of the polynomial at the n-th roots of unity  | $f(x) = -x^2 + 18x + 19983$                |

Table 3. Constraint polynomials  $C(x) = f(x)^2 - f(x)$

| Sr. No | Constraint polynomial $c(x)$       | $C(x) = f(x)^2 - f(x)$                             |
|--------|------------------------------------|--|
| 1      | Lagrange interpolation             | $C(x) = 2x^6 - 64x^4 - 2x^2 + 64$                  |
| 2      | Barycentric lagrange interpolation | $C(x) = 4x^6 - 128x^4 - 122x^3 - 4x^2 - 104x - 98$ |
| 3      | FFT                                | $C(x) = x^4 - 36x^3 - 63x^2 + 27x - 80$            |

The prover transforms  $c(x)$  using the properties of roots of polynomials to get another composition polynomial  $p(x)$  given in Table 4. The upper bound of the degree on  $p(x)$  as per (5), i.e.,

$$\text{Deg}(p) = I - 2 = 2. \text{ as } I = 4$$

$$p(x) = \frac{c(x)}{u(x)} = \frac{f(x)^2 - f(x)}{x^{N-1}} \quad \forall x \in F \text{ and } x \notin \{g^0, g^1, \dots, g^{N-1}\} \quad (5)$$

After calculating  $p(x)$  and  $f(x)$ , calculated merkle tree root proof MT\_f for  $f(x)$  and MT\_p for  $P(x)$ ,  $x = [1,2,3,4,5,6,7,8]$  for sending to verifier. It uses SHA-256 hash function. Prover sends Merkle root of MT\_f and MT\_p to verifier.

Table 4. Composition polynomials  $P(x)$

| Sr. No | Composition polynomial             | $P(x)$              |
|--------|------------------------------------|---------------------|
| 1      | Lagrange interpolation             | $P(x) = 2x^2 - 64$  |
| 2      | Barycentric lagrange interpolation | $P(x) = 4x^2 - 128$ |
| 3      | FFT                                | $P(x) = 1$          |

The third step is to test for low degree using FRI protocol (fast reed-solomon interactive oracle proofs of proximity). The verifier can verify after querying some steps ends up with constant by proving the polynomial is of low degree  $d$  (for our example  $d=2$ ). If this number of steps does not exceed a certain number, then there is high probability that, polynomial is of low degree. If polynomial is low degree then data received to the verifier is correct. In this experiment, since the data was provided according to equation 1, the low-degree test of the polynomial was successful, confirming that the received data is accurate.

## 4. EXPERIMENTS AND RESULT

### 4.1. Experimental setup

For this research, we implemented the modified ZK-STARK algorithm using Python programming. We installed the Ubuntu 22.04 app on Windows 11 via the Windows Subsystem for Linux (WSL) feature on a laptop with 8 GB RAM and a Core i5 processor. The laptop served as a server, while participants accessed the system through the WebAPI tool via browsers.

We installed Hyperledger Composer [28] and Hyperledger Fabric, opting for the Hyperledger Fabric platform due to its permission-based nature. Hyperledger Composer is a WebAPI framework used for developing blockchain projects, with a backend architecture based on Hyperledger Fabric. Before installing Hyperledger Fabric and Hyperledger Composer, several prerequisites were required, including Ubuntu, node.js, npm, docker desktop, git, curl, and Python with specific versions. Once the prerequisites and Composer were successfully installed, we started it by accessing the WebAPI on the browser using the URL-<http://localhost:8080>.

### 4.2. Results

We implemented three different polynomial interpolations for the ZK-STARK algorithm using python: lagrange polynomial interpolation, barycentric lagrange interpolation, and FFT. The performance of these interpolations was measured using different parameters as given in Table 5, proof generation time (seconds), proof verification time (seconds), proof size (KB), and throughput (operations per second). The graph for Figure 5 is based on the values presented in Table 5. Based on the performance results in Table 5, the FFT provides better throughput compared to the other two interpolation methods in ZK-STARK. Additionally, the proof verification time for FFT is significantly shorter than that for lagrange and barycentric lagrange interpolation methods.

We implemented the FSC using hyperledger composer, involving participants like farmers, food processors, distributors, retailers, and customers. The asset starts with the farmer and transfers through the chain via transaction logic, ending with the customer. All transactions are recorded and visible to participants, each with a unique ID for logging in and performing transactions. The ZK-STARK algorithm, implemented separately using Python on Google Colab, verifies the quality claimed by the prover using inputs like product number and quality. The Figure 6 depicts some executions of this supply chain process in Hyperledger Composer, where Figure 6(a) displays (a) business network farmer with product and (b) business network shows commodity asset.

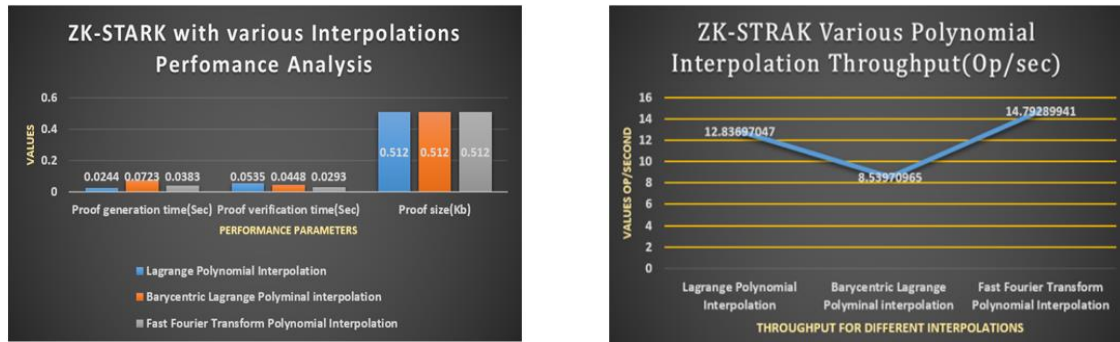
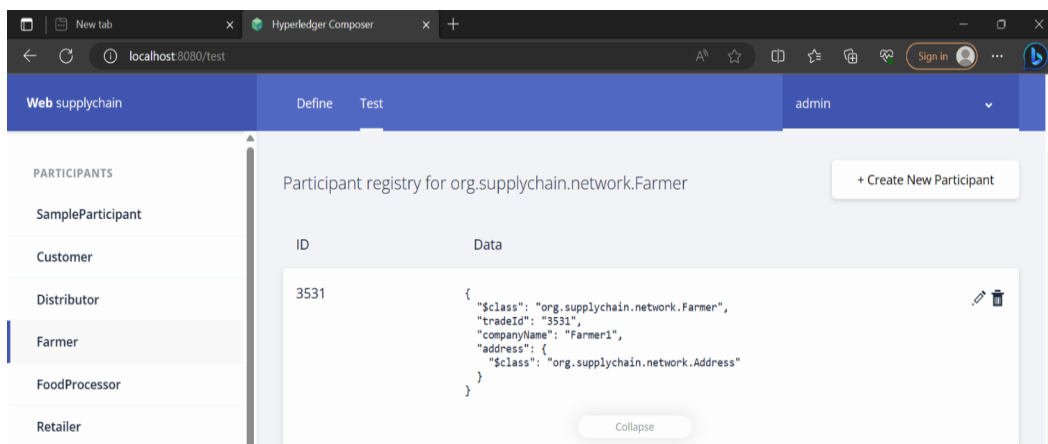


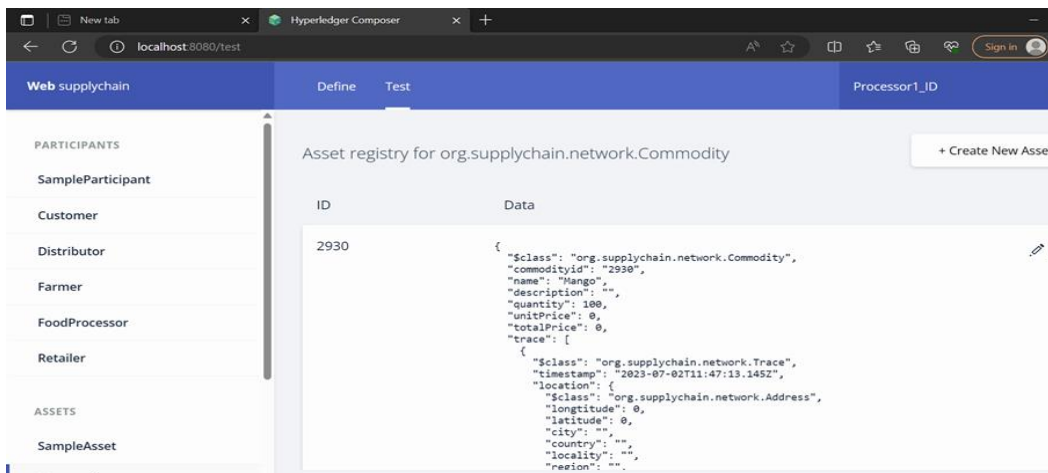
Figure 5. Graph of performance comparisons ZK-STARK with various polynomial interpolation

Table 5. Performance comparison for various polynomial interpolations in ZK-STARK

| Sr. No. | Polynomial interpolation           | Proof generation time (second) | Proof verification time (second) | Proof size (KB) | Throughput (op/second) |
|---------|------------------------------------|--------------------------------|----------------------------------|-----------------|------------------------|
| 1       | Lagrange interpolation             | 0.0244                         | 0.0535                           | 0.512           | 12.8369                |
| 2       | Barycentric lagrange interpolation | 0.0723                         | 0.0448                           | 0.512           | 8.5397                 |
| 3       | FFT                                | 0.0383                         | 0.0293                           | 0.512           | 14.7928                |



(a)



(b)

Figure 6. Snapshot of the hyperledger composer blockchain (a) business network farmer with product and (b) business network shows commodity asset



Based on these results, the future task is to integrate the FFT polynomial interpolation into the ZK-STARK algorithm and the blockchain FSC code, then compare its performance to the current system. By incorporating the ZK-STARK algorithm into the blockchain network may introduce additional computational overhead, potentially impacting system performance. To mitigate these effects, in future our research will explore strategies for optimizing the division of operations between on-chain and off-chain processes. Additionally, we will investigate methods to reduce the size of the cryptographic proofs, thereby enhancing the overall efficiency of the system.

## 5. CONCLUSION

The existing blockchain FSC system provides traceability but faces limitations in maintaining the privacy of personal information. This research proposes using the ZK-STARK algorithm to enhance privacy in blockchain-based agri-FSC. It emphasizes the importance of privacy preservation in blockchain systems and identifies the limitations of current methods. To counter the threat of quantum attacks, we employ the efficient ZK-STARK algorithm. We modified this algorithm using different polynomial interpolation methods and found that the FFT performed the best. Future work involves integrating this FFT-based ZK-STARK algorithm into the blockchain FSC and evaluating its impact. Since adding this algorithm to the blockchain network may increase system overhead, future research will explore which operations should be performed off-chain or on-chain and how to minimize proof size.




## REFERENCES

- [1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, pp. 1–9, 2008, [Online]. Available: <https://git.dhimmel.com/bitcoin-whitepaper/>.
- [2] Hyperledger, "Case study: how walmart brought unprecedented transparency to the food supply chain with hyperledger fabric challenge," *Hyperledger*, p. 7, 2019, [Online]. Available: [https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger\\_CaseStudy\\_Walmart\\_Printable\\_V4.pdf](https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf).
- [3] Y. Zhong, J. Hovanes, and U. Guin, "On-demand device authentication using zero-knowledge proofs for smart systems," in *Proceedings of the ACM Great Lakes Symposium on VLSI, GLSVLSI*, Jun. 2023, pp. 569–574, doi: 10.1145/3583781.3590275.
- [4] Y. Gong, Y. Jin, Y. Li, Z. Liu, and Z. Zhu, "Analysis and comparison of the main zero-knowledge proof scheme," in *Proceedings - 2022 International Conference on Big Data, Information and Computer Network, BDICN 2022*, Jan. 2022, pp. 366–372, doi: 10.1109/BDICN55575.2022.00074.
- [5] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.
- [6] I. Keshta *et al.*, "Blockchain aware proxy re-encryption algorithm-based data sharing scheme," *Physical Communication*, vol. 58, p. 102048, Jun. 2023, doi: 10.1016/j.phycom.2023.102048.
- [7] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A blockchain privacy protection scheme based on ring signature," *IEEE Access*, vol. 8, pp. 76765–76772, 2020, doi: 10.1109/ACCESS.2020.2987831.
- [8] B. Wang, Y. Zhan, and Z. Zhang, "Cryptanalysis of a symmetric fully homomorphic encryption scheme," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1460–1467, Jun. 2018, doi: 10.1109/TIFS.2018.2790916.
- [9] J. Zhou, Y. Feng, Z. Wang, and D. Guo, "Using secure multi-party computation to protect privacy on a permissioned blockchain," *Sensors*, vol. 21, no. 4, pp. 1–17, Feb. 2021, doi: 10.3390/s21041540.
- [10] E. S. Boo, J. Kim, and J. G. Ko, "LiteZKP: lightening zero-knowledge proof-based blockchains for IoT and edge platforms," *IEEE Systems Journal*, vol. 16, no. 1, pp. 112–123, Mar. 2022, doi: 10.1109/JSYST.2020.3048363.
- [11] D. Mouris and N. G. Tsoutsos, "Zilch: a framework for deploying transparent zero-knowledge proofs," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3269–3284, 2021, doi: 10.1109/TIFS.2021.3074869.
- [12] X. Li, C. Xu, and Q. Zhao, "Shellproof: more efficient zero-knowledge proofs for confidential transactions in blockchain," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2020, pp. 1–5, doi: 10.1109/ICBC48266.2020.9169437.
- [13] G. S. Gaba, M. Hedabou, P. Kumar, A. Braeken, M. Liyanage, and M. Alazab, "Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare," *Sustainable Cities and Society*, vol. 80, p. 103766, May 2022, doi: 10.1016/j.scs.2022.103766.
- [14] A. Konkin and S. Zapechnikov, "Privacy methods and zero-knowledge proof for corporate blockchain," *Procedia Computer Science*, vol. 190, pp. 471–478, 2021, doi: 10.1016/j.procs.2021.06.055.
- [15] Z. Guan, Z. Wan, Y. Yang, Y. Zhou, and B. Huang, "BlockMaze: an efficient privacy-preserving account-model blockchain based on ZK-SNARKs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1446–1463, May 2022, doi: 10.1109/TDSC.2020.3025129.
- [16] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Computers and Security*, vol. 99, p. 102050, Dec. 2020, doi: 10.1016/j.cose.2020.102050.
- [17] H. Zheng, L. You, and G. Hu, "A novel insurance claim blockchain scheme based on zero-knowledge proof technology," *Computer Communications*, vol. 195, pp. 207–216, Nov. 2022, doi: 10.1016/j.comcom.2022.08.007.
- [18] S. Ma, Y. Deng, D. He, J. Zhang, and X. Xie, "An efficient NIZK scheme for privacy-preserving transactions over account-model blockchain," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 641–651, Mar. 2021, doi: 10.1109/TDSC.2020.2969418.
- [19] A. Z. Junejo, M. A. Hashmani, A. A. Alabdulatif, M. M. Memon, S. R. Jaffari, and M. N. B. Abdullah, "RZee: cryptographic and statistical model for adversary detection and filtration to preserve blockchain privacy," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 7885–7910, Nov. 2022, doi: 10.1016/j.jksuci.2022.07.007.




- [20] B. Sharma, R. Halder, and J. Singh, "Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption," in *2020 International Conference on COMMUNICATION SYSTEMS & NETWORKS (COMSNETS)*, Jan. 2020, pp. 1–6, doi: 10.1109/COMSNETS48256.2020.9027413.
- [21] O. Bhadra, S. Sahoo, R. Halder, and C. M. Kumar, "AgroBLF: blockchain-based framework for smart agriculture," *Innovations in Systems and Software Engineering*, vol. 20, no. 3, pp. 443–453, Sep. 2024, doi: 10.1007/s11334-022-00468-0.
- [22] A. De Santis and G. Persiano, "Zero-knowledge proofs of knowledge without interaction," in *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*, 1992, vol. 1992-October, pp. 427–436, doi: 10.1109/SFCS.1992.267809.
- [23] A. Berentsen, J. Lenzi, and R. Nyffenegger, "A walk-through of a simple Zk-STARK proof," *SSRN Electronic Journal*, 2022, doi: 10.2139/ssrn.4308637.
- [24] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," *Eprint.Iacr.Org*, no. 693423, pp. 1–83, 2018, [Online]. Available: <https://eprint.iacr.org/2018/046.pdf>.
- [25] A. Mathematics, O. F. Kashpur, and V. V. Khlobystov, "Lagrange interpolation formula," in *encyclopedia of Mathematics*, vol. 2, no. 128, EMS Press, 2018, pp. 61–68.
- [26] J. P. Berrut and L. N. Trefethen, "Barycentric lagrange interpolation," *SIAM Review*, vol. 46, no. 3, pp. 501–517, Jan. 2004, doi: 10.1137/S0036144502417715.
- [27] E. O. Brigham, *The Fast Fourier Transform and its Applications*. New York, 2002.
- [28] "Hyperledger composer installation documentation." <https://hyperledger.github.io/composer/v0.19/installing/installing-index>.

## BIOGRAPHIES OF AUTHORS



**Madhuri Sadashiv Arade**    is currently pursuing a Ph.D. in Computer Engineering at Dr. Vishwanath Karad MIT World Peace University, located in Pune, Maharashtra, India. Her research interests lie in blockchain technology and information security. Notably, she excelled academically during both her Bachelor of Technology (B.Tech) and Master of Technology (M. Tech) programs, earning high rankings within the university. Presently, she serves as an Assistant Professor in the Department of Artificial Intelligence and Data Science at Government College of Engineering Kolhapur, Maharashtra, India, leveraging over 14 years of experience in academia. Additionally, she is a life member of ISTE (Indian Society for Technical Education). She runs her own YouTube channel where she delivered lectures on various subjects such as C#, ASP.NET, Linux, and computer hardware. She can be contacted at email: [arademadhuri15@gmail.com](mailto:arademadhuri15@gmail.com).



**Dr. Nitin N. Pise**    is a highly accomplished academician and researcher, with over 25 years of experience in teaching and 2 years of industrial experience. He received his Ph.D. in Computer Engineering from the College of Engineering Pune (Savitri Bai Phule Pune University) in 2016, after completing his graduation in Computer Engineering in 1994 and obtaining a Master's degree in Computer Science and Engineering in 2004 from Walchand College of Engineering, Sangli. He is currently working as a Professor in the School of Computer Engineering and Technology, Dr. Vishwanath Karad MIT World Peace University, located in Pune, Maharashtra, India. He also supervises Ph.D. candidates. He has published more than 60 papers in national and international conferences and journals, showcasing his research and contribution to the field in artificial intelligence, machine learning, data science and analytics, and blockchain. He can be contacted at email: [nitin.pise@mitwpu.edu.in](mailto:nitin.pise@mitwpu.edu.in).