

# Blockchain-Based Courier Tracking Services Using Smart Contracts

Deepti Ram Gangurde<sup>1</sup>, Arun Mishra<sup>2</sup>, Shantanu Singh<sup>3</sup>

Department of Computer Science and Engineering, DIAT, Pune<sup>1,2</sup>  
SAG Lab, DRDO, Delhi<sup>3</sup>

**Abstract-** This research proposes a decentralized courier tracking system using blockchain technology and smart contracts, aimed at enhancing transparency, trust, and security in logistics. The solution is implemented on the Volta blockchain and integrates MetaMask[3] to facilitate secure interactions between participants without relying on centralized intermediaries. The system automates shipment updates, maintains immutable tracking records, and protects sensitive data through cryptographic mechanisms. The implementation demonstrates improved traceability, operational efficiency, and stakeholder accountability. Performance evaluation indicates significant enhancements in security, cost-effectiveness, and scalability when compared to conventional courier tracking methods. The proposed system offers a robust alternative for modern supply chain management[6].

**Index Terms-** Privacy, Security, Data Sharing, QR Scan, Courier Tracking Services, Blockchain, Volta Token, MetaMask.

## I. INTRODUCTION

Courier Tracking Services (CTS) play a vital role in the logistics and supply chain domain by providing digital records of goods movement, including location updates, handling events, and delivery statuses. These services not only enhance the visibility and accountability of goods in transit but also help optimize logistics operations[1]. CTS allows customers and courier service providers to access real-time shipment information, resulting in improved service quality, cost reduction, and operational transparency. The increasing demand for digitization in logistics has highlighted the need for systems that can securely store, track, and share courier information across multiple stakeholders[1].

Despite the advantages, traditional CTS models face several limitations. These include centralized control, vulnerability to data tampering, and restricted interoperability among courier agents. Data often resides in isolated silos, making it difficult for stakeholders to share information seamlessly. In such systems, data integrity and trustworthiness are significant concerns, especially in cross-border and multi-vendor delivery environments.

Blockchain technology[3] has emerged as a transformative solution to these challenges. As a decentralized and tamper-resistant ledger, blockchain enables immutable record-keeping and transparent data sharing across distributed networks. Smart contracts, which are self-executing code blocks deployed on the blockchain, can automate logistics workflows, eliminate paperwork, and ensure rule-based

compliance. The use of smart contracts further reduces administrative overhead and delays in supply chain activities.

In this paper, a decentralized courier tracking solution is presented, implemented on the Volta blockchain with integration of MetaMask for secure user interaction. The system uses smart contracts written in Solidity and is deployed using Truffle.js and Web3.js, enabling real-time and verifiable tracking updates. MetaMask provides a user-friendly interface for secure authentication and transaction management within the blockchain ecosystem.

The study aims to bridge the gap between existing centralized courier tracking systems and the growing need for transparency, security, and automation. It highlights how blockchain can significantly improve traceability, efficiency, and stakeholder trust in logistics.

Supply-Chain-DApp is a blockchain-based decentralized application that transforms traditional supply chain management. By leveraging blockchain technology, it ensures the secure and transparent transfer of products from manufacturers to customers, particularly through online e-commerce platforms[6].

Solidity-written Volta token blockchain network is used to compile, transfer, and deploy smart contracts using Truffle.js power the system. The front end is built with Web3.js, enabling seamless communication between the smart contract and the Volta token. Transactions across the supply chain are facilitated through integration with the MetaMask wallet, ensuring secure and efficient operations[3].

This innovative approach not only eliminates inefficiencies but also fosters trust and accountability among all stakeholders in the supply chain, making it a game-changing solution for modern commerce.

The aim of Supply-Chain-DApp is to revolutionize supply chain management by using blockchain technology and smart contracts to create a transparent, efficient, and secure system. The project seeks to:

- **Enhance Transparency:** Establish a trustworthy and unchangeable logs of transactions across the supply chain, encouraging responsibility from all parties involved.
- **Increase Efficiency:** Streamline processes by reducing paperwork and administrative overhead, enabling faster and more reliable operations.
- **Ensure Security:** Use blockchain's decentralized and cryptographic features to safeguard transactions and protect sensitive supply chain data.
- **Enable Seamless Integration:** Provide a robust interface for e-commerce platforms to securely connect manufacturers, intermediaries, and customers.
- **Promote Decentralization:** Utilize decentralized smart contracts to automate and govern transactions without relying on centralized authorities[1].

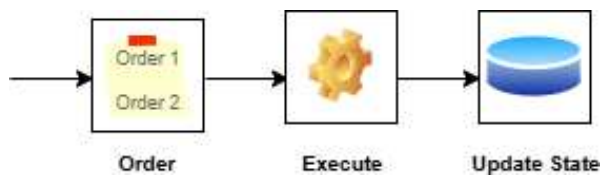


Figure 1: Framework of Order-execute [11]

## II. LITERATURE REVIEW

### 1. Blockchain Technology Using Metamask Blockchain Technology

The evolution of blockchain technology has brought substantial improvements in supply chain transparency, traceability, and security. Originally introduced for financial applications, blockchain has now found extensive use in various domains including logistics and authentication systems. Gupta et al. [1] analyzed how supply chain management can benefit from digital transformations, highlighting opportunities for performance optimization through better tracking systems. The current research builds upon such findings by integrating blockchain to further address visibility and integrity issues in courier tracking.

Buterin [9] introduced Ethereum as a generalized blockchain platform capable of executing smart contracts, allowing decentralized logic implementation without third-party control. These contracts, when integrated into logistics systems, can automate shipment processes and eliminate

fraud. Studies by Omar et al. [6] demonstrated how Ethereum-based smart contracts facilitate secure inventory sharing across different stakeholders. Their findings confirm that permissioned or public blockchains can enforce transaction rules and prevent unauthorized updates, making them suitable for supply chain applications.

MetaMask has emerged as a widely used browser-based wallet that simplifies blockchain interactions. Jogu et al. [3] utilized MetaMask for blockchain-based authentication and demonstrated its compatibility with Ethereum smart contracts. Their results show how decentralized verification mechanisms reduce dependency on traditional identity management systems. In addition, Belotti and Livraga [8] explored blockchain-driven authentication using QR code scanning and MetaMask integration. Their study validated the usability and performance of blockchain-based systems in verifying user identities securely.

Further contributions from Rezaeibagha and Yi [11] and Zhang et al. [10] emphasized secure data access using dynamic policies on distributed ledgers. These works collectively outline the importance of using cryptographic protections, consensus mechanisms, and smart contract-based automation to enhance courier tracking systems. The present study extends this direction by implementing a working prototype of a blockchain-powered courier tracking system integrated with MetaMask and Volta blockchain, filling a critical gap in achieving trust and automation across supply chain stakeholders.

### 2. Metamask Using Volta Faucet with AI Driven Blockchain-Driven Transparency

- Provide an immutable and decentralized ledger to ensure transparency across the supply chain lifecycle.
- Enable stakeholders to track product movement from raw materials to finished goods delivered to customers.

#### Smart Contract Automation

- Use Solidity-based smart contracts to automate critical supply chain operations, reducing the reliance on manual intervention.
- Manage agreements between stakeholders, ensuring seamless and secure execution of supply chain tasks.

#### Secure Transactions

- Leverage the Volta token blockchain network in the MetaMask wallet to handle transactions securely.
- Protect sensitive supply chain data using blockchain's cryptographic features, ensuring data integrity. [8].

**Integration with E-Commerce**

- Facilitate the integration of supply chain management with e-commerce platforms for efficient product delivery.
- Streamline the process of connecting manufacturers, intermediaries, and customers through decentralized protocols.

**Developer-Focused Tools and Setup**

- Support multiple supply chain participants, including raw material suppliers, manufacturers, retailers, and consumers, enabling them to interact in a unified, secure, and decentralized system.

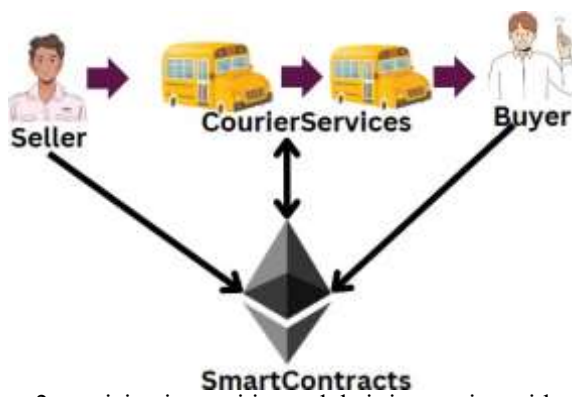


Figure 2: participating entities and their interaction with smart contracts

Allow users to manage roles and responsibilities using MetaMask accounts and the Volta token.

**Scalability and Flexibility**

- Build a scalable solution adaptable to various supply chain configurations, ensuring relevance across industries.
- Provide room for further enhancement and integration of additional features to meet future demands[2].

These nodes in a Blockchain based network execute of three roles, as illustrated in Fig. 2.

- **Seller:** The seller has the item to be packaged for transfer to the interested buyer. The Sellers are represented by the nodes. They help with the implementation transactions for ordering, and submit transaction requests for operation.
- **Buyer:** The buyer wants to update the decentralized ledger, validate the seller, and spend Ether to purchase the item.
- **Courier Service:** The components that make up the order placement process. Depending on the buyer’s and seller’s geolocation, a number of couriers are available to deliver the item from the seller to the buyer. The transporter initiates the subsequent contract in the chain.

**3. Exploring the Use of Metamask Wallet for Blockchain-based Authentication using QR scanning.**

This study’s objective is to detect the used of metamask wallet for blockchain-based certification using the QR code. A prototype -authentication system has been developed and evaluated, which includes meta -masked wallet and Ethereum blockchain smart contracts with QR code scanning. Research follows a qualitative function and collects data through monitoring and evaluation of the authentication system’s operation.[8]

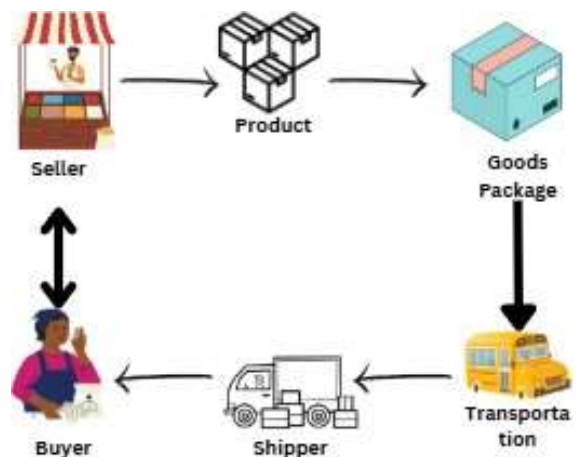


Figure 3: Traditional way of Courier Tracking services

**Data Gathering and Evaluation Procedure:** Data for this study will be collected using a variety of techniques. monitoring and assessment of the Metamask wallet To ascertain the system performance in terms of speed, safety, usefulness [7].To gather data, research and user interviews with authentication system users will also be performed. Questions concern- ing customer happiness, safety, and the technology itself will be part of the search. To get their thoughts on the effectiveness and potential of the system, developers and specialists in the blockchain industry will be interviewed.

**Summary of the Experimental Configuration:** Many prototype authentication system implementations utilizing the Ethereum blockchain’s smart contracts and metamask portfo- lio.The system will include a web application that enables users to log in with their Meta- mask wallets..Smart contracts will be used by the system to authenticate users and provide application access.[8] The above Fig.3 illustrates the Six main stages of the The traditional way of CTS for the transaction flow:

The authentication system’s usability, safety, and performance will all be assessed.Performance metrics that can be measured include response time and the quantity of attempts at successful and unsuccessful authentication.. Security metrics,

including data integrity and encryption level, will also be assessed. Research and interviews will be used to measure usability parameters including user satisfaction and ease of usage.

Use Metamask wallet to restore Safe Customer History Through QR scanning : In addition to certification, Metamask Wallet and QR code scan can be securely utilized to reconstruct the customer history of Blockchain. In this implementation, users scan a unique QR code related to their transaction items, stored on a decentralized account book. When scanning, Metamask Wallet Verification User's identity through smart contracts, and provides access to purchase history, service records, or other relevant data. This method ensures data integrity, increases safety, and ends the traditional database-based requirement for identity confirmation. The efficiency of the system is evaluated based on performance, safety, and user satisfaction calculations, which ensures a spontaneous and reliable customer experience.

**Performance Metrics Description:** To evaluate the performance of the solutions, several metrics will be used:

- **Response Time:** A timer that logs the user's login time and the moment the system allows or prohibits access will be used to gauge the response time.
- **Authentication Accuracy:** Authentication accuracy quantifies the quantity of successful and unsuccessful authentication attempts. The number of successful and unsuccessful authentication attempts will be monitored and analyzed in order to determine the system's accuracy rate.
- **Security Level:** Evaluates data integrity and encryption strength. The system's encryption algorithm will be examined. The veracity of the data recorded on the blockchain will be verified in order to assess data integrity.
- **Usability:** Evaluates user pleasure and ease of usage. Users who have used the authentication systems will be surveyed and interviewed in order to assess this measure

### III. BLOCKCHAIN-BASED CTS USING METAMASK

The suggested method for blockchain-based authentication utilizing Metamask Wallet : The suggested method for blockchain-based authentication utilizing Metamask Wallet: This section will give a thorough explanation of the suggested solutions that use the Metamask wallet as a Blockchain-based verification mechanism. The solutions include the use of smart contracts and a metamask wallet in the Blockchain Ethereum to implement a prototype authentication system. The platform will enable users to.

Fig 4 displays the following critical elements for Building a CTS system using Blockchain, smart Contracts and Architectural Design of Metamask:

#### 1. Integration with the Blockchain Network

The proposed solution is part of the blockchain networks work with the use of intelligent contracts. An intelligent contract The parameters of the agreement between the parties are contained in this self-executive contract. Intelligent contracts are perfect for authentication since they run automatically when specific requirements are met. The Ethereum blockchain is connected to the authentication mechanism via the Metamask wallet. When a user logs into the web application, the system asks the Ethereum network to confirm their identity. To authenticate the user and grant access to the application, the system makes use of a smart contract.

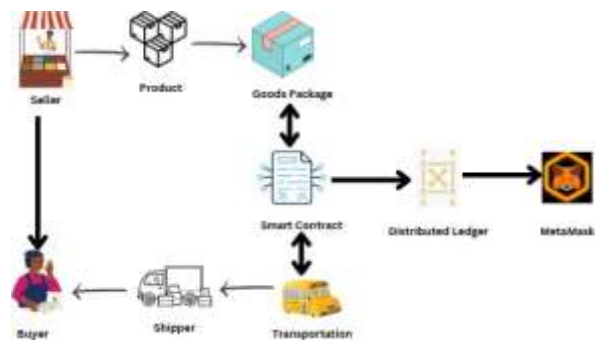


Figure 4: Courier Tracking services Using Blockchain, Smart Contracts and MetaMask

#### 2. Using the Metamask wallet for authentication requires the following steps:

- Using their Metamask wallets, the user logs onto the web application. user is prompted by the system to input their Metamask wallet information.
- The Ethereum network receives a request from the system to start the authentication process after the user logs in. [7].
- The Ethereum network executes the smart contract to verify the user's identity.
- 4. The smart contract verifies the user's public key via the Ethereum blockchain.
- Depending on whether the public key matches the user's Metamask wallet, access is either permitted or denied.
- . [8].

#### 3. Features of the Security

Several security features are offered by the suggested method, which uses the Metamask wallet for authentication:

- **Tamper-proof Smart Contracts:** Smart contracts deployed on the Ethereum blockchain cannot be modified, ensuring a secure authentication process.

- **Metamask Walletsecurity:** It is a secure browser extension that encrypts and stores private keys locally on the user’s device, preventing hacker attacks[8].
- **Data Encryption:** User data is encrypted when logging into the web application, preventing unauthorized access.
- **Blockchain-based Identity Verification:** The use of the Ethereum blockchain ensures a decentralized and immutable authentication mechanism. [?].

Overall, users may log into online apps safely and effectively with the suggested approach that uses the Metamask wallet for authentication. To verify user identity and safeguard user data, the system makes use of intelligent contracts on the Ethereum blockchain network. The metamask wallet ensures that user data is shielded from unwanted access by adding an additional degree of protection to the authentication process.

#### IV. HOW PRIVACY AND SECURITY ARE ATTAINED IN CTS

The integration of MetaMask in a blockchain-based courier tracking system ensures privacy and security through multiple layers of cryptographic protection and decentralized mechanisms.

Here’s how these aspects are achieved:

##### 1. Privacy in Courier Tracking with MetaMask

- **Decentralized Identity Management** MetaMask allows users to interact with the blockchain using pseudonymous wallet addresses, reducing the risk of personally identifiable information (PII) exposure.
- **Users control their private keys,** ensuring that no central authority can access their identity or transaction history. [?].
- **Data Anonymization and Encryption** Since all transactions are recorded on the Volta token blockchain, the use of cryptographic hashing ensures that data cannot be linked directly to a real-world identity. Sensitive supply chain details (such as parcel location and recipient identity) can be encrypted using asymmetric cryptography. [?].
- **Role-Based Access Control** Smart contracts define the roles of manufacturers, intermediaries, and customers, restricting unauthorized access to sensitive courier information. Only relevant stakeholders with the correct MetaMask wallet permissions can retrieve tracking details.

The data flow and interactions inside the network are depicted in Fig. 5.

##### 2. Security Measures in Blockchain-Based Courier Tracking

Immutable Ledger and Tamper-Proof Transactions of the blockchain’s decentralized nature ensures that courier tracking records cannot be altered or deleted, preventing fraud. Every transaction (e.g., package transfer, delivery confirmation) is cryptographically signed using MetaMask, ensuring authenticity.

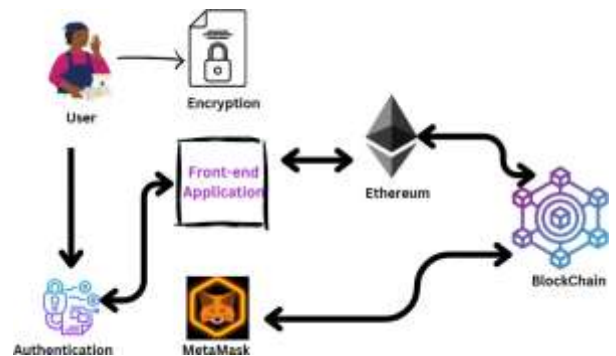


Figure 5: Privacy and Security in CTS

Smart Contracts for Secure Transactions automate courier tracking without relying on centralized third parties, reducing the risk of data breaches. The contracts execute predefined conditions (e.g., package delivery confirmation) to prevent unauthorized modifications.

Secure Wallet-Based Transactions on MetaMask secures all transactions with a seed phrase and private key encryption, making it resistant to phishing and hacking attempts. Two-factor authentication (2FA) or hardware wallet integration can be used to enhance security.

Fraud Prevention and Transparency in Blockchain-based tracking eliminates counterfeit updates in the courier lifecycle, as every stakeholder verifies each stage. The public ledger provides an auditable trail of package movements, preventing malicious activities like fake deliveries.

#### V. METHODOLOGIES

##### 1. Establishing Local Development

The blockchain-based courier tracking system was developed using Visual Studio Code, Node.js, Git, and MetaMask. The application was built on the Volta blockchain test network using Solidity smart contracts, compiled and deployed via the Truffle framework. MetaMask was configured for secure wallet-based interactions and funded through the Volta faucet. The frontend used HTML, CSS, JavaScript, and Web3.js to connect with smart contracts. QR code scanning enabled item-level authentication, and user identities were verified using MetaMask. System performance was evaluated through

metrics like response time and data integrity, confirming its effectiveness for secure and decentralized courier tracking.

### Configuration and Installation

- **VSCODE:** Visual Studio Code is available for download at <https://code.visualstudio.com/>.
- **Node.js:** Get the most recent LTS Node.js version from <https://nodejs.org/>, then use terminal: `node -v` to verify the version after installation.
- **Git:** Go to <https://git-scm.com/downloads> to download the most recent version of Git and make sure `git-version` is the terminal version.
- **MetaMask:** accessible as a browser plugin through the Chrome Web or the Firefox.
- **QR Scanner:** Can be available automatic as the customer update there transactions.

### 2. Connect Meta Musk with Volta Token

- Click the network dropdown in the upper right corner of MetaMask after opening it in your browser.
- After Clicking on add network u will get interface to add network name, rpc , url, chain id put same as shown in the image below and click on Add or Save.
- To copy and paste your address in this URL, click on Account Address:
- Now You Will get the 1 volta on your account and check in MetaMask wallet.

### 3. Use Metamask wallet to restore Safe Customer History Through QR scanning

In addition to certification, Metamask Wallet and QR code scan can be securely utilized to reconstruct the customer history of Blockchain.

In this implementation, users scan a unique QR code related to their transaction items, stored on a decentralized account book. When scanning, Metamask Wallet Verification User's identity through smart contracts, and provides access to purchase history, service records, or other relevant data. This method ensures data integrity, increases safety, and ends the traditional database-based requirement for identity confirmation.

The efficiency of the system is evaluated based on performance, safety, and user satisfaction calculations, which ensures a spontaneous and reliable customer experience.

### 4. Compile & Implement Smart Contract

Use `Ctrl +` to launch VScode and Terminal.

The Clone The project After entering the command, hit Enter:  
Git clone: Set up dependencies: After entering the command, hit Enter: `npm i`

### 5. DApp's File Structure

- **Contracts:** The Solidity Smart contracts for the DApp are located in this folder. Truffle automatically generates the `Migrations.sol` contract, which is used to manage migrations.
- **Migrations:** This package contains the JavaScript migration files required to put the smart contracts on the blockchain network into practice.
- **Test:** This package contains the JavaScript test files required to assess the smart contracts.
- **truffle-config.js:** The `truffle-config.js` file contains the necessary settings, such as the blockchain network to be used.
- **package.json:** This automatically generated file contains the exact version of each dependency used in the project.
- **package-lock.json:** The precise version of every dependency used in the project is contained in this automatically created file.
- **Clients:** This folder contains the client-side code, often HTML, CSS, and JavaScript, that can be organized into a client folder.

### 6. Mnemonic

The mnemonic, which is the seed phrase for the account you want to deploy from, must be entered for the provider. To get started, create a `new.secret` file in the root directory and add your 12-word mnemonic seed phrase. The seed words can be obtained from the Metamask wallet by going to Metamask Settings, selecting Security and Privacy from the menu. A button labeled "reveal seed words" will appear.

### 7. Compile the Smart Contract

In the terminal, use the following command to compile the smart contract: `npm compile`.

### 8. Configuring MetaMask for VoltaToken

- After Compile We Need To Deploy our Smart Contract on Blockchain. In Our Case We are Deploying on sepolia token Which is token blockchain for development, used to test and develop Smart Contracts.
- We need to install HDWallet run this command in npm `install @voltatoken/hdwallet-provider`.
- As you can see we have token which has network id-3000 which identity volta token id.
- `meta migrate-network token` Command Will deploy Smart Contract to volta Blockchain. It will take some time For deployment and u will able find transaction hash, contract address and many more.

### 9. Run DAPP

- Go to the client folder after launching Terminal.
- `cd client` : Install all packages in the `package.json` file.
- `npm i` : Install Web3 in the `package.json` file
- Run this Command : Launch the app

- npm start : By default, port 3000 is used to host the application.

**10. Setup Account for Supply Chain Player.**

- Go to MetaMask, click on the account icon in the top-right corner, select Create Account, name as Raw Material Supplier, and Click "Create".
- Add All participate(Raw Material, Supplier, Manufacture,Retail). by following above Step.
- Get Volta for Each Player from this URL <https://tool.voltachain.net/faucet/>In Order to do Transaction.

**VI. OUTPUTS**

Supply Chain Management Tutorial to MetaMask

Figure 6: Secure Your Supply Chain with Blockchain - Connect MetaMask

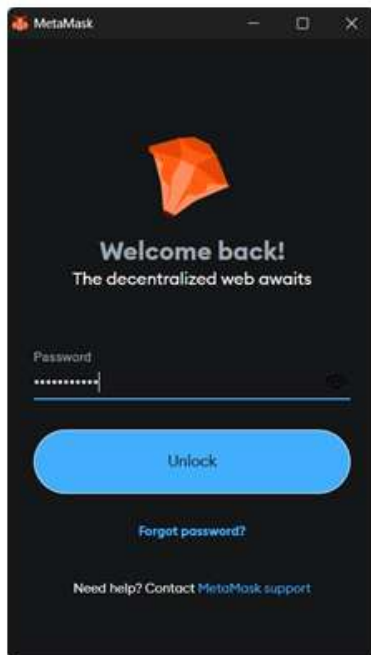


Figure 7: Secure and Decentralized – Log into MetaMask

Supply Chain Management Connected Account: 0x200AC0E4803aE000515344EA119E2100

Products

| ID | Name       | Manufacturer | Current Location |
|----|------------|--------------|------------------|
| 1  | Laptop     | Techno       | Warehouse 1      |
| 2  | Smartphone | MobileX      | Warehouse 2      |
| 3  | Tablet     | TabletPro    | Store 1          |
| 4  | Monitor    | VisualTech   | Store 4          |
| 5  | Headphones | AudioPlus    | Store 2          |
| 6  | Mouse      | ClickMaster  | Warehouse 3      |
| 7  | Keyboard   | KeyPro       | Warehouse 1      |
| 8  | Printer    | PrintPro     | Store 3          |
| 9  | Scanner    | ScanPro      | Store 3          |

Figure 8: Blockchain-Powered Supply Chain: Track Products

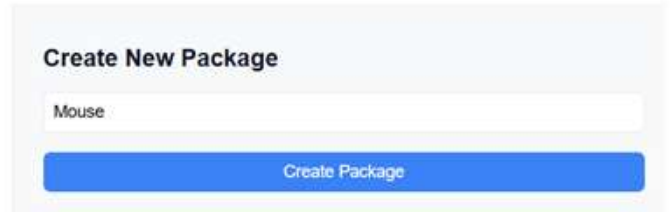


Figure 9: Create New Package with Description

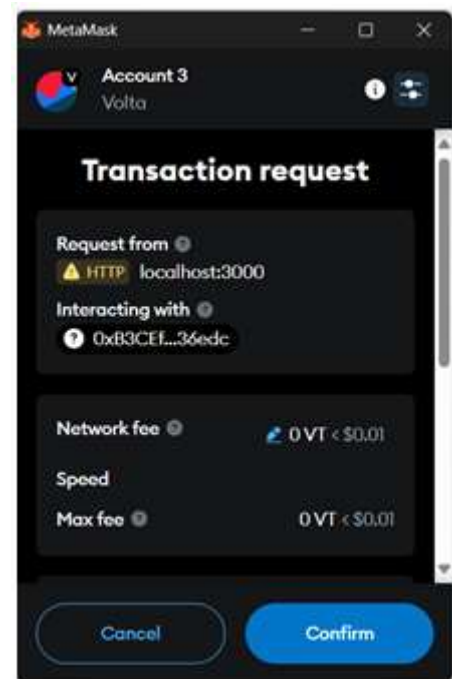


Figure 10: Confirmation for Create New Package

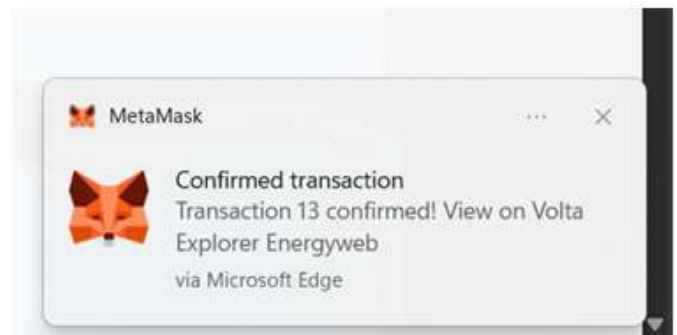


Figure 11: Confirmation from MetaMask

Packages

| ID | Description | Current Handler                   | Stage     | Creator                           | Timestamp            | QR |
|----|-------------|-----------------------------------|-----------|-----------------------------------|----------------------|----|
| 1  | Tablet      | 0x03AC0E4803aE000515344EA119E2100 | Completed | 0x1A15C7E94C08C1784E5F5A02640089  | 8/30/25, 9:16:10 pm  |    |
| 2  | Mouse       | 0x03AC0E4803aE000515344EA119E2100 | Created   | 0x03AC0E4803aE000515344EA119E2100 | 8/30/25, 11:53:10 am |    |

Figure 12: Immutable Records and Transparent Handling



Figure 13: Update our Package Status



Figure 14: Update from Create – Transit



Figure 15: Upload QR for Updating



Figure 16: Uploaded Qr



Figure 17: History Of our Package Status

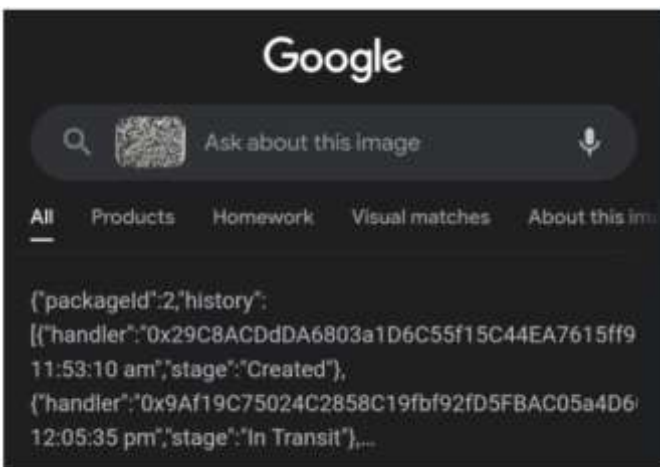


Figure 18: After Scanned the Qr

## V. CONCLUSION AND FUTUREWORK

This study successfully demonstrates the feasibility and effectiveness of a blockchain-based courier tracking system using smart contracts deployed on the Volta blockchain and integrated with the MetaMask wallet. The proposed decentralized approach ensures secure data handling, tamper-proof transaction logging, and transparent courier information sharing among all stakeholders. Through the use of Solidity contracts, QR code authentication, and Web3.js-powered interaction, the system streamlines logistics operations while minimizing dependency on centralized authorities. The integration with MetaMask further enhances user privacy and simplifies access control by enabling cryptographically secure identity verification. System evaluation indicates that the solution achieves improved traceability, high data integrity, and operational efficiency compared to conventional courier tracking platforms. The implementation demonstrates robustness, scalability, and strong alignment with current needs in supply chain security and digital transformation. Furthermore, the use of open-source development tools makes this solution replicable and adaptable for other industrial applications. Future work may focus on extending the platform with computer vision models for object recognition, enabling autonomous tracking of packages via smart devices or drones. Integration with deep learning-based range estimation methods could further enhance the accuracy and responsiveness of real-time delivery status updates. Additional improvements could involve multi-sensor fusion and the deployment of edge computing nodes to enable offline processing and local decision-making in remote areas. Real-time analytics and visualization dashboards could also be incorporated to provide operational insights to logistics providers. The architecture may be adapted to support regulatory compliance and audit logging features required in highly regulated industries such as pharmaceuticals or defense logistics. Overall, this project establishes a novel paradigm for secure, decentralized, and verifiable courier tracking that can contribute significantly to the modernization of global supply chains.

## REFERENCES

- Gupta, C., Kumar, V., & Kumar, K. (2022). A study on the applications of supply chain management. In Proceedings of the SMART 2022 Conference, 737–741. doi:10.1109/SMART55829.2022.10047167.
- Arthi, M., Avrit, M., Evangeline, S. C., Gogineni, J., Bharadwaj, R., & Siran-jeevi, G. P. (2024). Design and implementation of a decentralized voting system using Volta blockchain. Logistics, 1–6. doi:10.1109/Wintechcon61988.2024.1083790

3. Jogu, S. C., Nishitha, A., & Chary, R. V. R. (2021). Blockchain-based authentications using MetaMask wallet as a tool. *Logistics*, 5, 33. doi:10.3390/logistics5020033.
4. Dujak, D., & Sajter, M. (2019). Blockchain's capability in supply chain transparency and security.
5. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, Article 21260.
6. Omar, I. A., Jayaraman, R., Debe, M. S., Hasan, H. R., Salah, K., & Omar, M. (2022). Supply chain inventory sharing using Ethereum blockchain and smart contracts. *IEEE Access*, 10, 2345–2356. doi:10.1109/ACCESS.2021.3139829.
7. MetaMask. (2021). About MetaMask. Retrieved from <https://metamask.io/about.html>.
8. Belotti, F., & Livraga, G. (2020). Blockchain-based authentication in decentralized environments: A comprehensive survey. *Journal of Network and Computer Applications*, 148, 102454.
9. Buterin, V. (2014). Ethereum: A secure decentralized generalized transaction ledger. *Ethereum Project Yellow Paper*, 151(5), 1–32.
10. Zhang, X., Xie, C., & Liu, J. (2019). Blockchain-based authentication: An overview. In *International Conference Proceedings*.
11. Rezaeibagha, F., & Yi, M. (2016). Distributed clinical data sharing via dynamic access-control policy transformation. *International Journal of Medical Informatics*, 89, 25–31.
12. Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with healthcare information technology. In *Proceedings of the International Conference of the IEEE Engineering in Medicine and Biology Society*.
13. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain.