

Blockchain-Supply Chain Security Solution

Project submitted for the partial fulfillment of the requirements for the
course

<CSE 315L: Network Security Lab>

Offered by the

Department Computer Science and Engineering

School of Engineering and Sciences

Submitted by

- | | |
|------------------|-----------------|
| 1) Arun | - AP21110011317 |
| 2) Aravind Kumar | - AP21110011605 |
| 3) Nithish | - AP21110011607 |



SRM University-AP

Neerukonda, Mangalagiri, Guntur

Andhra Pradesh – 522 240

[March, 2024]

Content

Page No

Introduction.....	1
Background.....	2
Challenges in Supply Chain Security.....	3
Proposed Work.....	5
Potential Solutions.....	8
Supply chain Algorithm.....	11
Output of SmartContract.....	17
Conclusion.....	17
References.....	18

1. Introduction

Supply chains are the backbone of global Ecommerce, facilitating the movement of goods and services from suppliers to consumers. However, in today's interconnected world, supply chains face a myriad of challenges that threaten their efficiency, security, and integrity. Issues such as counterfeit products, opaque processes, data breaches, and trust deficits among stakeholders have become increasingly prevalent, necessitating innovative solutions to safeguard supply chain operations.

Blockchain technology has emerged as a promising solution to address these challenges by offering transparency, immutability, and traceability throughout the supply chain. By leveraging blockchain, organizations can enhance security, establish trust, and streamline operations, thereby creating a more resilient and efficient supply chain ecosystem.

This report delves into the application of blockchain technology in enhancing supply chain security. It examines the challenges faced by modern supply chains, explores the relevance of blockchain in mitigating these challenges, and presents potential solutions leveraging blockchain technology. Through an in-depth analysis supported by illustrative figures and case studies, this report aims to provide valuable

insights into the transformative potential of blockchain in fortifying supply chain operations and ensuring the integrity of global trade.

2. Background

Supply chains are complex networks of interconnected entities involved in the production, distribution, and delivery of goods and services. However, this complexity also makes them vulnerable to a range of security threats, including counterfeiting, theft, and data breaches. These threats can have serious consequences for businesses, consumers, and the economy as a whole.

Counterfeiting is a significant issue across various industries, including pharmaceuticals, electronics, and luxury goods. Counterfeit products not only undermine brand reputation and consumer trust but also pose health and safety risks. Moreover, counterfeiters often exploit vulnerabilities in supply chains to introduce fake products into the market, bypassing regulatory controls and quality assurance processes.

Theft is another prevalent security threat in supply chains, with goods being stolen during transportation, storage, or handling. Cargo theft, for example, is a widespread problem that results in significant financial losses for businesses and disrupts the flow of goods.

The 2018 E. coli outbreak linked to contaminated romaine lettuce serves as a poignant example of the consequences of supply chain failures. The outbreak resulted in numerous illnesses and deaths, highlighting the need for improved traceability and accountability in

food supply chains. and underscored the importance of implementing robust traceability systems to ensure food safety.

3. Challenges in Supply Chain Security:

Supply chains operate within a complex landscape fraught with security challenges that undermine their integrity and resilience. Among these challenges are the pervasive threats of counterfeit products infiltrating the market, theft incidents occurring during transportation, and the looming specter of data breaches compromising sensitive information. Counterfeit goods pose a considerable risk across industries, exploiting vulnerabilities in supply chains to introduce fraudulent products, endangering both consumer safety and brand reputation. Concurrently, theft incidents during transportation disrupt the flow of goods, leading to financial losses and logistical complications. Moreover, the digitization of supply chain operations has amplified the risk of data breaches, with breaches compromising the confidentiality and integrity of critical information, leading to legal liabilities and reputational harm.

One of the fundamental obstacles to addressing these security challenges is the inherent lack of visibility and transparency within supply chain operations. The intricate networks and numerous stakeholders involved in supply chains create complexities that obscure the movement of goods and hinder efforts to verify product authenticity. Without comprehensive visibility and transparency, stakeholders struggle to detect and mitigate security threats effectively,

leaving supply chains vulnerable to exploitation and disruption. This lack of transparency also erodes trust among stakeholders, impeding collaboration and exacerbating security risks.

To confront these challenges, supply chains must adopt a multifaceted approach that integrates technology, collaboration, and risk management strategies. Embracing innovative solutions such as blockchain technology can enhance transparency and traceability, enabling stakeholders to track the journey of goods and verify their authenticity. Collaboration among supply chain partners is also paramount, as it fosters information sharing and enables coordinated efforts to address security threats collectively. Additionally, robust risk management practices, including regular assessments and contingency planning, are essential for identifying vulnerabilities and implementing proactive measures to mitigate security risks effectively. By adopting a holistic approach to supply chain security, organizations can fortify their operations, protect against security threats, and uphold the integrity of global commerce.

4. Proposed Approach:

1. Define Requirements:

- Identify the specific security challenges faced by the supply chain industry, such as counterfeit products, theft, and data breaches.

- Determine the key features and functionalities required to address these challenges, such as transparent traceability, automated transactions, and secure data sharing.

2. Design Smart Contracts:

- Utilize Solidity to design and implement smart contracts that encapsulate the logic and rules governing supply chain transactions.

- Define data structures and functions to enable transparent traceability of products, automate transactions using smart contracts, and facilitate decentralized data sharing among supply chain stakeholders.

3. Develop Smart Contracts:

- Use Hardhat as the development environment to write, compile, and test the smart contracts locally.

- Write Solidity code to implement the defined smart contract functionalities, ensuring robustness, efficiency, and security.
- Conduct comprehensive testing to verify the correctness and reliability of the smart contracts, including unit tests, integration tests, and scenario-based tests.

4. Integrate Meta-mask:

- Integrate Meta-mask into the supply chain solution to provide a user-friendly interface for interacting with the Ethereum blockchain.
- Enable users to securely manage their Ethereum accounts, sign transactions, and interact with the smart contracts directly from their web browsers using Meta-mask.

5. Deploy on Ethereum:

- Deploy the developed smart contracts onto the Ethereum blockchain using Hardhat.
- Configure deployment parameters, such as gas limits and transaction fees, to optimize deployment efficiency and cost-effectiveness.

- Verify the deployed smart contracts on Ethereum blockchain explorers, ensuring transparency and integrity of the deployed code.

6. Test and Iterate:

- Conduct thorough testing of the deployed solution to validate its functionality, security, and performance.

- Gather feedback from stakeholders and end-users to identify any issues or areas for improvement.

- Iterate on the solution based on feedback and testing results, making necessary adjustments and enhancements to enhance its effectiveness and usability.

7. Document and Deploy:

- Document the project approach, design decisions, and implementation details to provide comprehensive documentation for future reference and knowledge sharing.

- Deploy the finalized supply chain solution to production, ensuring seamless integration with existing supply chain processes and systems.

- Provide training and support to stakeholders and end-users to ensure successful adoption and utilization of the deployed solution.

5. Possible Solutions

1. Transparent Traceability: Blockchain technology can be leveraged to create an immutable record of product movement throughout the supply chain, enabling transparent traceability from manufacturer to consumer. Each transaction and transfer of ownership is recorded on the blockchain, providing stakeholders with real-time visibility into the entire supply chain process. Through transparent traceability, organizations can quickly identify the source of any security threats, such as counterfeit products or unauthorized diversions, and take prompt action to mitigate risks. Additionally, consumers can verify the authenticity and origin of products, fostering trust and confidence in the supply chain ecosystem.

2. Smart Contracts: Smart contracts, self-executing contracts with predefined terms and conditions encoded into code, offer a powerful solution for automating and enforcing agreements between supply chain stakeholders. By implementing smart contracts on a blockchain platform, organizations can automate various aspects of supply chain transactions, including payments, shipments, and compliance checks. Smart contracts ensure that transactions are executed according to agreed-upon terms, reducing the risk of disputes, delays, and errors. Moreover, smart contracts enable transparent and auditable transactions, enhancing accountability and trust among supply chain partners.

3. Decentralized Data Sharing: Blockchain-based platforms can facilitate secure and decentralized data sharing among supply chain partners, enhancing data integrity and privacy. By storing data on a distributed ledger, blockchain ensures that information remains tamper-proof and resistant to unauthorized access or manipulation. Supply chain stakeholders can securely share sensitive information, such as inventory levels, production data, and compliance records, without compromising data privacy or confidentiality. Decentralized data sharing fosters collaboration and transparency within the supply chain ecosystem, enabling stakeholders to make informed decisions and mitigate security risks effectively.

These solutions harness the transformative potential of blockchain technology to enhance supply chain security, transparency, and efficiency. Detailed explanations and figures will be provided to elucidate the implementation of these solutions and their benefits, showcasing how blockchain can revolutionize supply chain management and safeguard the integrity of global commerce.

6. Supplychain Algorithim

1. Defined a Solidity contract named SupplyChain.
2. Declared an enumeration named SupplyChainStatus with values: Manufacturing, Distribution, Retail.
3. Declared a struct named Product to represent a product in the supply chain.

4. Defined a mapping named products to store products with their IDs as keys.

5. Declared a public uint256 variable named productId to keep track of product IDs.

6. Defined events:

- ProductManufactured: Log when a product is manufactured.
- ProductDistributed: Log when a product is distributed.
- ProductSold: Log when a product is sold.
- ProductCertified: Log when a product is certified.

7. Implemented the constructor:

- Initialized productId to 0.

8. Implemented the manufactureProduct function:

- Accept parameters: _name (string), _quantity (uint256), _price (uint256).
- Increment productId.
- Created a new Product struct with provided parameters and default values.
- Store the product in the products mapping.
- Emit a ProductManufactured event.

9. Implemented the distributeProduct function:

- Accept parameters: _id (uint256), _distributor (address).
- Verify that the product is in the manufacturing stage and the caller is the manufacturer.
- Update the distributor and product status.

- Emit a ProductDistributed event.

10. Implemented the sellProduct function:

- Accept parameters: _id (uint256), _retailer (address).
- Verify that the product is in the distribution stage and the caller is the distributor.
- Update the retailer and product status.
- Emit a ProductSold event.

11. Implemented the certifyProduct function:

- Accept parameters: _id (uint256), _isCertified (bool).
- Verify that the product is in the retail stage and the caller is the retailer.
- Update the certification status of the product.
- Emit a ProductCertified event.

12. Implemented the getProductDetails function:

- Accept parameter: _id (uint256).
- Retrieve the product details from the products mapping based on the provided ID.
- Return the product details as a tuple.

```

I.   | Product |
II.  +-----+
III. | id      |
IV.  | name     |
V.   | quantity |
VI.  | manufacturer|
VII. | distributor|
VIII.| retailer   |
IX.  | status    |

```

X. | price |
XI. | certified |
XII. +-----+

id: A unique identifier for each product.

name: The name of the product.

quantity: The quantity of the product.

manufacturer: The address of the manufacturer.

distributor: The address of the distributor.

retailer: The address of the retailer.

status: The current stage of the product in the supply chain.

price: The price of the product.

certified: A flag indicating whether the product is certified.

7. Output of SmartContract

1. deployed the smartcontract in remix.ethereum-IDE

```

[vm] from: 0x583...eddC4 to: SupplyChain.(constructor) value: 0 wei data: 0x608...90033 logs: 0 hash: 0xb76...602b5

status                                0x1 Transaction mined and execution succeed

transaction hash                       0xb76d99c2b88af7182c707cdfd36641bf117a43cc65d94cd1226552ec599602b5

block hash                            0x29d8b913322f7eecd8934fbd689359d0ea82af826d288c7506dca56045d77dbf

block number                           176

contract address                      0x90D41ECd6e1701CE34523ed98423c1eFb0805a8D

from                                  0x58380a6a701c568545dCfcB03Fc8875f56beddC4

to                                    SupplyChain.(constructor)

gas                                    1789653 gas

transaction cost                       1556220 gas

execution cost                         1396462 gas

input                                  0x608...90033

decoded input                          {}

```

2. Supplychain.manufactureProduct transmission Started

```

transact to SupplyChain.manufactureProduct pending ...

[vm] from: 0x583...eddC4 to: SupplyChain.manufactureProduct(string,uint256,uint256) 0x90D...05a8D value: 0 wei data: 0xf35...00000 logs: 1
hash: 0x6c8...571bd

status                                0x1 Transaction mined and execution succeed

transaction hash                       0x6c81a771ccc53136759137dc2d301720aa299a7e25776f538a694376212571bd

block hash                            0x389db3cf8968bbd1a83b7b8d20032c0bbc16b38ea2f52e3197be95add2d674e

block number                           177

from                                  0x58380a6a701c568545dCfcB03Fc8875f56beddC4

to                                    SupplyChain.manufactureProduct(string,uint256,uint256) 0x90D41ECd6e1701CE34523ed98423c1eFb0805a8D

gas                                    224117 gas

transaction cost                       194884 gas

execution cost                         173084 gas

input                                  0xf35...00000

decoded input                          {
    "string_name": "milk",
    "uint256_quantity": "1",
    "uint256_price": "23"
}

```

```

input                                0x90d41ec06e1701ce34523ed98423c1efb0805a80
decoded input                        {
                                     "string_name": "milk",
                                     "uint256_quantity": "1",
                                     "uint256_price": "23"
                                   }
decoded output                       {}
logs                                 [
                                     {
                                       "from": "0x90D41ECd6e1701CE34523ed98423c1efB0805a80",
                                       "topic": "0x21a383d6747d32728419dfb020ea9b6e90878eaf973f75828cc9352ac904d22c",
                                       "event": "ProductManufactured",
                                       "args": {
                                         "0": "1",
                                         "1": "milk",
                                         "2": "1",
                                         "3": "0x58380a6a701c568545dCfcB03FcB875f56beddC4",
                                         "4": "23",
                                         "5": "1715067383",
                                         "id": "1",
                                         "name": "milk",
                                         "quantity": "1",
                                         "manufacturer": "0x58380a6a701c568545dCfcB03FcB875f56beddC4",
                                         "price": "23",
                                         "timestamp": "1715067383"
                                       }
                                     }
                                   ]
transact to SupplyChain.distributeProduct pending ...

```

3.supplyChain.DistributeProduct

```

[vm] from: 0x583...eddC4 to: SupplyChain.distributeProduct(uint256,address) 0x90D...05a8D value: 0 wei data: 0xd6c...35cb2 logs: 1
hash: 0x18a...a04de

status                                0x1 Transaction mined and execution succeed
transaction hash                      0x18a716c7dc4c23266309701fdc0f3a50e3ac907b6731e56b9ba6dd6335a04de
block hash                           0x789e19d3050e3e1109776c6cbf096a711be982eb74af56fae049b82d4a450a80
block number                         178
from                                  0x58380a6a701c568545dCfcB03FcB875f56beddC4
to                                    SupplyChain.distributeProduct(uint256,address) 0x90D41ECd6e1701CE34523ed98423c1efB0805a8D
gas                                   107807 gas
transaction cost                      93745 gas
execution cost                       72173 gas
input                                0xd6c...35cb2
decoded input                        {
                                     "uint256_id": "1",
                                     "address_distributor": "0xAb8483F64d9C6d1EcF9b849Ae677d03315835cb2"
                                   }
decoded output                       {}
logs                                 [
                                     {
                                       "from": "0x90D41ECd6e1701CE34523ed98423c1efB0805a80",
                                       "topic": "0x35835fb24fe4b2370145ed5524e86ddb17d89264edad8254f6e9bcd196234b1a",

```


4. SupplyChain.sellProduct

```
✓ [vm] from: 0xAb8...35cb2 to: SupplyChain.sellProduct(uint256,address) 0x9DD...05aB0 value: 0 wei data: 0x0b5...c02db logs: 1 hash: 0xafb...5db72

status                                0x1 Transaction mined and execution succeed
transaction hash                       0xafb6c965b5411ee3552578af92f79f9c4133d4ea364360b5f86e1f9e0fd5db72
block hash                            0x70076e037cc62ee892110ffab51cb0da519d716af98d16ccfe48972fbfe7d50e
block number                          179
from                                   0xAb8483F64d9C6d1EcF9b849Ae677d03315835cb2
to                                     SupplyChain.sellProduct(uint256,address) 0x9DD41ECd6e1701CE34523ed98423c1eFb0805aB0
gas                                    65830 gas
transaction cost                       57243 gas
execution cost                         35671 gas
input                                  0x0b5...c02db
decoded input                          {
  "uint256 _id": "1",
  "address _retailer": "0x4820993Bc481177ec7E8f571ceCaE8A9e22C02db"
}
decoded output                         {}
```

```
logs
[
  {
    "from": "0x9DD41ECd6e1701CE34523ed98423c1eFb0805aB0",
    "topic": "0x1996dfdf9a942c2ec8fc8b5da7010c303a8b65bc587a754469c06cdc0d09236f",
    "event": "ProductSold",
    "args": {
      "0": "1",
      "1": "0x4820993Bc481177ec7E8f571ceCaE8A9e22C02db",
      "2": "23",
      "3": "1715067503",
      "id": "1",
      "retailer": "0x4820993Bc481177ec7E8f571ceCaE8A9e22C02db",
      "price": "23",
      "timestamp": "1715067503"
    }
  }
]

call to SupplyChain.getProductDetails
```

5. Supplychain.getProductDetails

```
CALL [call] from: 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2 to: SupplyChain.getProductDetails(uint256) data: 0x681...00001

from      0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2  ⓘ

to      SupplyChain.getProductDetails(uint256) 0x90D41ECd6e1701CE34523ed98423c1eFb0805a8D ⓘ

execution cost      26931 gas (Cost only applies when called by a contract) ⓘ

input      0x681...00001 ⓘ

decoded input      {
    "uint256 _id": "1"
} ⓘ

decoded output      {
    "0": "string: milk",
    "1": "uint256: 1",
    "2": "address: 0x5B380a6a701c568545dCfc803Fc8875f56beddC4",
    "3": "address: 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
    "4": "address: 0x4B209938c481177ec7E8f571ceCaE8A9e22C02db",
    "5": "uint8: 2",
    "6": "uint256: 23",
    "7": "uint256: 1715067383",
    "8": "uint256: 1715067435",
    "9": "uint256: 1715067503",
    "10": "bool: false"
} ⓘ

logs      [] ⓘ ⓘ

transact to SupplyChain.certifyProduct pending ...
```

6. SupplyChain.certifyProduct

[vm] from: 0x4B2...C02db to: SupplyChain.certifyProduct(uint256,bool) 0x9DD...05aBD value: 0 wei data: 0x4a6...00001 logs: 1 hash: 0x310...418ac	
status	0x1 Transaction mined and execution succeed
transaction hash	0x310a876b7adc95b113cd9aaef5a2a1f6357b77f1b9d8e96c75a8b5cd413418ac
block hash	0x0f2376670e8a9315e05c888c157224d977cd5e7a33211aabc1f0920bd13c63e8
block number	181
from	0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
to	SupplyChain.certifyProduct(uint256,bool) 0x9DD41fCd6e1701CE34523ed98423c1eFb0805aBD
gas	55613 gas
transaction cost	48359 gas
execution cost	27015 gas
input	0x4a6...00001
decoded input	{ "uint256_id": "1", "bool_isCertified": true }

7. SupplyChain.ProductId

CALL [call] from: 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db to: SupplyChain.productId() data: 0xc5c...e3911	
from	0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
to	SupplyChain.productId() 0x9DD41fCd6e1701CE34523ed98423c1eFb0805aBD
execution cost	2447 gas (Cost only applies when called by a contract)
input	0xc5c...e3911
decoded input	{}
decoded output	{ "0": "uint256: 1" }
logs	[]
call to SupplyChain.products	

7. Supplychain.Products

```
CALL [call] from: 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db to: SupplyChain.products(uint256) data: 0x7ac...00001

from          0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db  ⓘ

to            SupplyChain.products(uint256) 0x9DD41ECd6e1701CE34523ed98423c1eFb0805aBD ⓘ

execution cost 26453 gas (Cost only applies when called by a contract) ⓘ

input          0x7ac...00001 ⓘ

decoded input  {
                "uint256 ": "1"
              } ⓘ

decoded output {
                "0": "uint256: id 1",
                "1": "string: name milk",
                "2": "uint256: quantity 1",
                "3": "address: manufacturer 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
                "4": "address: distributor 0xAb8483F64d9C6d1EcF9b849Ae677d03315835cb2",
                "5": "address: retailer 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db",
                "6": "uint8: status 2",
                "7": "uint256: price 23",
                "8": "uint256: manufacturingTimestamp 1715067383",
                "9": "uint256: distributionTimestamp 1715067435",
                "10": "uint256: retailTimestamp 1715067503",
                "11": "bool: isCertified true"
              } ⓘ

logs          [] ⓘ ⓘ
```

8. Conclusion

In conclusion, blockchain technology offers significant potential to enhance supply chain security through transparent traceability, smart contracts, and decentralized data sharing. However, addressing implementation challenges is crucial for realizing its full benefits. Collaboration and innovation are key to driving successful blockchain adoption in supply chains.

9. Reference

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

2. Shen, L., & Chang, Y. (2019). "Blockchain technology and supply chain financing: A review of research and future research directions." *International Journal of Operations & Production Management*, 39(1), 70-87.

3. Tapscott, D., & Tapscott, A. (2016). "Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world."

4. Lu, X., & Xu, X. (2020). A blockchain-based quality and safety traceability system for supply chain management. *Journal of Intelligent Manufacturing*, 31(1), 159-169.