# Security Features in Blockchain-Based Certification for Food Supply Chain Transparency

Emon Monsur

February 14, 2025

## 1 Project Overview

Consumer demands for transparency, sustainability, and ethical sourcing are rising in the food sector today. However the current certification processes are centralised, opaque, and vulnerable to manipulation. Consumers frequently find it difficult to verify ethical claims or understand how eco-scores are even determined. And production costs increase with ethical sourcing, and the lack of transparency prevents consumers from understanding why prices differ, limiting their ability to make informed purchasing decisions.

This project creates a blockchain-based system that certifies food products based on ethical factors. Our system awards certificates based on ethical supply chain practices, unlike the conventional food supply sector. Our approach would use blockchain's immutability and transparency to provide consumers with ethical products that have trustworthy, unchangeable certificates. Consumers can make well-informed decisions based on verified supply chain practices, while retailers can use these certificates to promote sustainable products.

## 2 Focused Analysis - Security Features

This report will focus on the **security features** of blockchain. Security is crucial in the food supply chain, where a blockchain is used to track products from farm to table as it helps ensure data integrity, prevents cyber attacks, and protects supply chain transparency.

**What is a blockchain and what security features needs it have?**

A ***blockchain*** is a distributed, decentralized ledger that records transactions between multiple nodes in a secure, transparent, and tamper-resistant manner. It enables trustless interactions by eliminating the need for a central authority, ensuring that all transactions are unchangeable and cryptographically secure.

Block chains come in different types, including public, private, and consortium blockchains [1]. Our project would entail using a public blockchain to implement certificates, chosen to ensure consumer trust, and the ability to verify data in real-time. Consumers would like to know how scores are calculated, what factors contribute, and whether data has been manipulated, which could be known through a public blockchain.

**What security features do blockchains have?**

Blockchains have built-in security mechanisms that make them resilient in supply chain management, including [2]:

- **Blockchain structure:** Each block in the chain references the previous block's hash, making tampering difficult. The structural design guarantees that all modifications must be agreed upon by the majority of the network, eliminating the possibility of unauthorized changes.
- **Cryptographic hashing:** Each transmission is secured using functions such as SHA-256, which generates a fixed-length unique representation of the data. Any modification to the data will result in a completely different hash. This means even the smallest change to a transparency score would be detected.
- **Immutable and tamper resistant:** Once recorded transactions cannot be modified or deleted.
- **Decentralization:** Unlike traditional databases controlled by a central database, blockchain data is distributed across multiple nodes in the network. This prevents single-point attacks.
- **Consensus Mechanisms:** Protocols like Proof of Work (PoW) or Proof of Stake (PoS) ensure transactions are validated before they are recorded.

**Comparison of Security Features in Traditional vs. Blockchain-Based Food Certificates**

| Security Feature | Traditional Certification | Blockchain-Based Certification |
|---|---|---|
| Data Integrity | Prone to tampering | Immutable records using hashing |
| Transparency | Limited visibility, centralized control | Decentralized and publicly verifiable |
| Authentication | Manual verification process prone to error | Multi-signature with private keys |
| Repeal & Update Certs | Complex and slow | Automated via smart contracts |

Table 1: A comparison of key security attributes between traditional certification and blockchain-based certification, highlighting improvements in data integrity, transparency, authentication.

## 2.1 Consensus Mechanism Security

Decentralized networks often face issues of distrust, particularly as they grow larger. To maintain reliability and security, these systems use consensus, meaning the nodes in the network agree on the validity of the transactions. This ensures that only valid transactions are recorded and makes it extremely difficult for attackers to change past records, preventing them causing issues like fake certificates or duplicate scoring for the same product. Here is the two main consensus mechanisms:

**Proof of Work (PoW):** In PoW, miners compete to solve complex mathematical puzzles to validate records and add new blocks to the blockchain containing supply chain certificates. The first miner to solve the puzzle adds the block and receives a reward. PoW provides strong protection against attacks, because altering the blockchain would require massive computing power, making it extremely costly and impractical. However, while PoW might be highly secure, it requires significant energy and results in slower transaction times.

**Proof of Stake (PoS):** PoS selects validators based on the number of tokens they have and are willing to stake as collateral. Validators confirm supply chain records, issue scores and add new blocks, done without solving complex puzzles. PoS maintains security by penalizing dishonest behaviour - validators who approve fraudulent transactions risk losing their staked tokens. This system discourages manipulation because attackers would face financial losses. PoS consumes less energy than PoW but introduces risks such as the ”nothing at stake” problem, where validators may support multiple chains to maximize rewards.

For our project, PoS is the better choice because it is faster, more energy efficient, and cost-effective compared to PoW. Additionally, PoS enhances security by making manipulation of transparency scores risky as dishonest validators could lose their staked tokens. .

## 2.2 Security Risks and How to Minimize Them

Although blockchains offer strong security, they are still vulnerable to specific risks that could compromise the transparency score system. Here are three of the most common security risks that blockchain systems face [3]:

- **51-Percent Attack:** If an attacker compromises the majority of nodes, transparency scores could be manipulated. This could lead to fake certifications, damaging the systems trustworthiness. To mitigate this, implementing strong consensus mechanisms and ensuring a widely distributed network of nodes is essential.
- **Double Spending:** Attackers can exploit a technological flaw to spend double the user's digital currency by transferring money from the end user's wallet to the attacker's wallet, even if the user's wallet does not have enough funds to do so. Retailers could exploit this flaw to reuse one certification for multiple products. Cryptographic validation techniques, along with data backups can help prevent this.
- **Eclipse Attack:** Here attackers isolate a single node from the network and manipulate its decisions. Due to bandwidth constraints, nodes can only connect up-to a specific number of nodes and an attacker will bombard the user with a large number of IP addresses that the attacker controls to exploit this. If a retailers node is compromised, the attacker could feed outdated or manipulated transparency scores. To prevent this, strict policy on inbound connections could be implemented, blocking inbound nodes and only connecting to outbound connections with specific nodes in the network that are trusted.

## 2.3 Smart Contract Security

Smart contracts are a specific protocol used to carry out the terms of an agreement. They are simply containers of code that encapsulate and replicate the terms of real-world contracts. They replace third persons between contracting parties. They allow transactions between untrusted parties without the necessary for direct contact between the parties, reliance on third parties, and intermediary costs [4]. They would be essential for automating the issuance, updating, and verifications of transparency scores or certificates. They will ensure scores are calculated based on verified supply chain data and are automatically updates if new certifications are added. Additionally they will handle disputes such as invalidate certificates if fraudulent activity is detected.

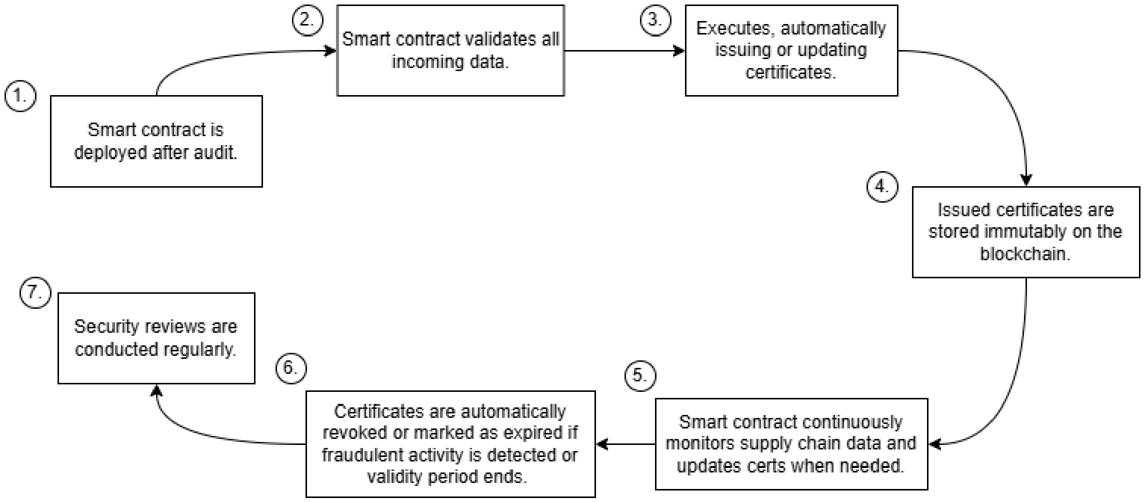
1.
Smart contract is deployed after audit.
2.
Smart contract validates all incoming data.
3.
Executes, automatically issuing or updating certificates.
4.
Issued certificates are stored immutably on the blockchain.
5.
Smart contract continuously monitors supply chain data and updates certs when needed.
6.
Certificates are automatically revoked or marked as expired if fraudulent activity is detected or validity period ends.
7.
Security reviews are conducted regularly.

Figure 1: Smart contract lifecycle for blockchain.

Smart Contract Vulnerabilities and Mitigation Strategies:

- **Reentrancy Attacks:** An attacker repeatedly calls a vulnerable contract before previous ones are able to execute, leading to issuing of multiple certificates for the same product. To mitigate, use the checks-effects-interactions pattern to prevent reentrancy, which defines how code should be organised to minimize undesirable side effects and execution behaviours.
- **Integer Overflows/Underflows:** Here attackers manipulate numeric values beyond set limits, causing incorrect calculations. To mitigate, use *SafeMath* [5] by OpenZeppelin library to avoid integer overflows.
- **Gas Limit Attacks:** If a smart contract's execution exceeds the block's gas limit (the maximum amount of computational effort required to process an operation), the transaction fails. This will cause the score issuance or certification update to fail. To mitigate these, one may optimize smart contract logic such as using efficient loops and splitting complex operations into smaller transactions to minimize gas consumption.

## 3 Conclusion

For blockchain-based technology used to implement the certificates in our project, effective security measures are crucial. By integrating cryptographic security, smart contracts, and consensus mechanisms, we are able to minimise attacks and fraud, prevent score manipulation, and even safeguard supply chain integrity. Through proper security implementation, this system can revolutionise how ethical considerations influence pricing in food industry, benefiting producers, consumers, and retailers.

## References

[1] Y. Zhao, S. Lv, W. Long, Y. Fan, J. Yuan, H. Jiang, and F. Zhou, "Malicious webshell family dataset for webshell multi-classification research," *Visual Informatics*, vol. 8, no. 1, pp. 47–55, 2024.

[2] I. Homoliak, S. Venugopalan, Q. Hum, and P. Szalachowski, "A security reference architecture for blockchains," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 390–397, IEEE, 2019.

[3] M. Iqbal and R. Matulevičius, "Blockchain-based application security risks: A systematic literature review," in *Advanced Information Systems Engineering Workshops: CAiSE 2019 International Workshops, Rome, Italy, June 3-7, 2019, Proceedings 31*, pp. 176–188, Springer, 2019.

[4] H. Taherdoost, "Smart contracts in blockchain technology: A critical review," *Information*, vol. 14, no. 2, 2023.

[5] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y. Alexandrov, "Smartcheck: Static analysis of ethereum smart contracts," in *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pp. 9–16, 2018.