Privacy-Preserving Techniques in Blockchain-Based Food Supply Chain

CSE 3000: Research Project, 1st of July 2021

RQ: "How are privacy-preserving techniques present in the blockchain-based food supply chain?"

Authors
Nicola-Paul Stepanov
Zekeriya Erkin
Tianyu Li

Affiliations
Cyber Security Group
Department of Intelligent Systems
Delft University of Technology

01

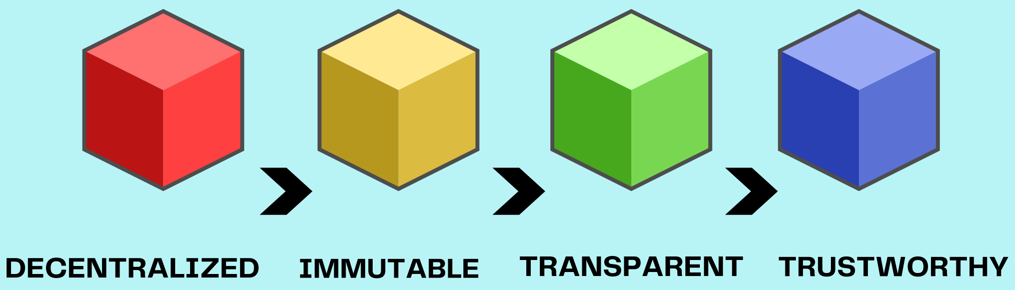
Introduction

Supply Chain is:

- network of all operations, individuals, organizations, information, resources
- from raw materials to end-users

Has some flaws: counterfeit, theft, smuggling, piracy, compromises and attacks

Blockchain is:



Blockchain applied to Supply Chain:

- traceability (fighting foodborne disease)
- product labelling (to ensure integrity)
- real-time tracking
- stoppage of counterfeits
- elimination of middlemen (through smart contracts)

However,

- naturally, not pre-equipped with privacy preservation technology
- lack of central authority, transactions reveal confidential details
- absence of specific ownership laws

This leads to **privacy-preserving techniques**

02

Methods

Systematic literature review, comparison of existing papers to come up with data about:

- How is Blockchain used in the Supply Chain
- Privacy issues and preservation methods
- Most relevant food supply chain cryptocurrencies and their use cases
- The effect of privacy regulations and smart contracts on supply chain privacy

Frequently used databases: Google Scholar, IEEE Xplore Digital Library, Science Direct, Springer and ACM Digital Library

03

Contribution

1. **PRIVACY PRESERVATION METHODS OVERVIEW**

A) Transaction related privacy preservation

- **Identity data preservation** (Mixing Services, Ring Signatures, Zero-Knowledge Proofs, Non-Interactive Zero-Knowledge Proofs)
- **Transaction data preservation** (Mixing Services, Differential Privacy, Homomorphic Hiding)

B) Smart contract related privacy preservation (Hawk)

2. **PRIVACY PRESERVATION PROPOSAL**

Combination of different existing methods:

- **Parallel subsection storage model**
- **Differential privacy**
- **Generation of smart contracts similar to Hawk**
- **Privacy by design**
- **Self-sovereign identification**
- **"Right to be forgotten"**

3. **MOST RELEVANT FOOD SUPPLY CHAIN CRYPTOCURRENCIES OVERVIEW**

Three main pillars: **Ethereum, Hyperledger Fabric, VeChain**

- Waltonchain (WTC)
- Ambrosus (AMB)
- OriginTrail (TRAC)
- Te-Food (TONE)
- Devery.io (EVE)

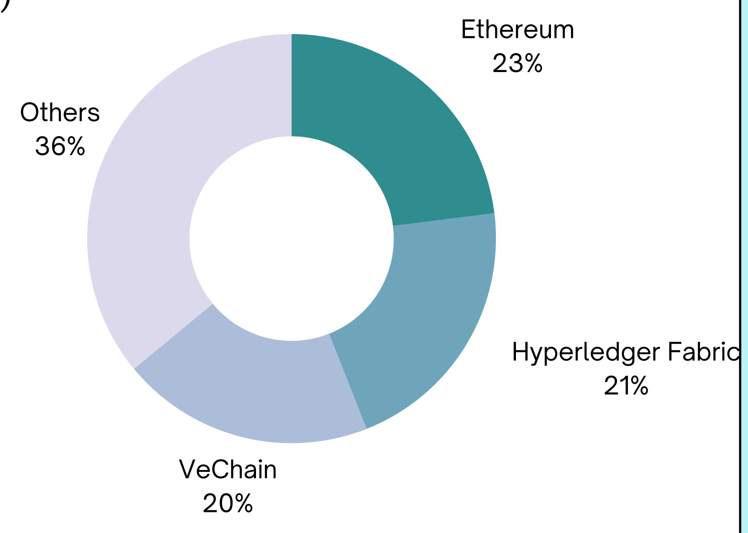


Fig 1) The dominance of the 3 main Blockchain platforms as of 2020 [1]

4. **USE CASES OF BLOCKCHAIN PLATFORMS IN THE FOOD SUPPLY CHAIN SECTOR**

- **Overview** of 22 most relevant projects found
- Categorised into: **project name, technologies it relies on, use case description, focus, optional comments**

04

Conclusion

Central objective: how is privacy maintained in the food supply chain

- Detailed overview of subsisting privacy procedures, coupled with current supply chain applications
- Most important initiatives of supply chain cryptocurrencies and alternative blockchain platforms
- Most representative use cases in the industry of food supply chain
- Blockchain: infrastructure with great potential to revolutionize supply chain
- With advantages, there come challenges: privacy is one of them
- Smart contract privacy techniques, GDPR, transaction and identity-related privacy methods among others are extremely relevant
- No magic formula for privacy: research bring a proposal combining different methods
- Further development needs to be done in this field to maximize the potential of blockchain while preserving privacy in the best possible way

05

References

[1] N. Vadgama and P. Tasca. "An Analysis of Blockchain Adoption in Supply Chains between 2010 and 2020." Frontiers in Blockchain, 4:8, 2021.

Contact

Nicola-Paul Stepanov (4849736)
e-mail: N.P.Stepanov@tudelft.nl