Security Challenges of Blockchain-Based Supply Chain Systems

Shereen Ismail, and Hassan Reza - SEECS

UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

Introduction

Supply chain systems are susceptible to dangerous types of cyber-attacks and unauthorized activities.

US supply chain attacks rose by 42% in the first quarter of 2021, impacting up to seven million people.

Blockchain has an ideal architecture to secure supply chain systems that require ensuring distributed transactions between participants and decentralizing computation and management in a trustless environment.

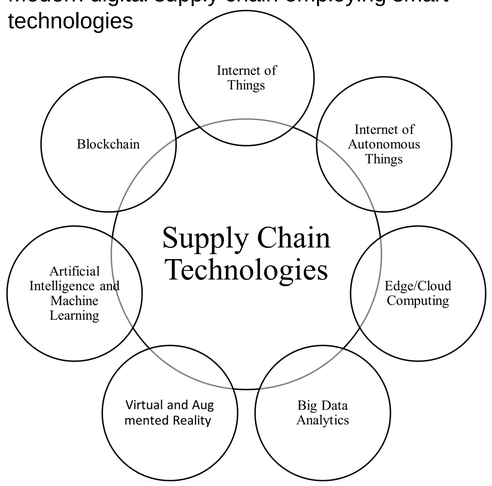
Several security challenges of blockchain-based supply chain systems need to be addressed at different layers.

Objective

Highlighting the main security challenges of blockchain-based supply chain systems according to its three architectural layers: supply chain, blockchain, and IoT.

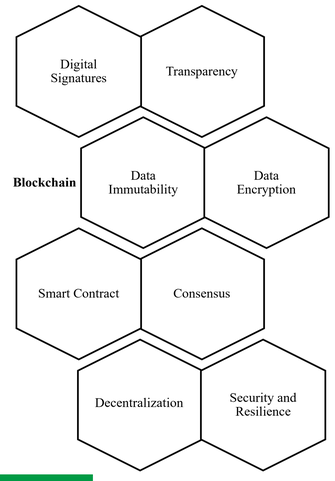
Traditional Vs. Modern Supply Chain Systems

- Traditional linear supply chain systems such as centralized data repository for record keeping
- Modern digital supply chain employing smart technologies



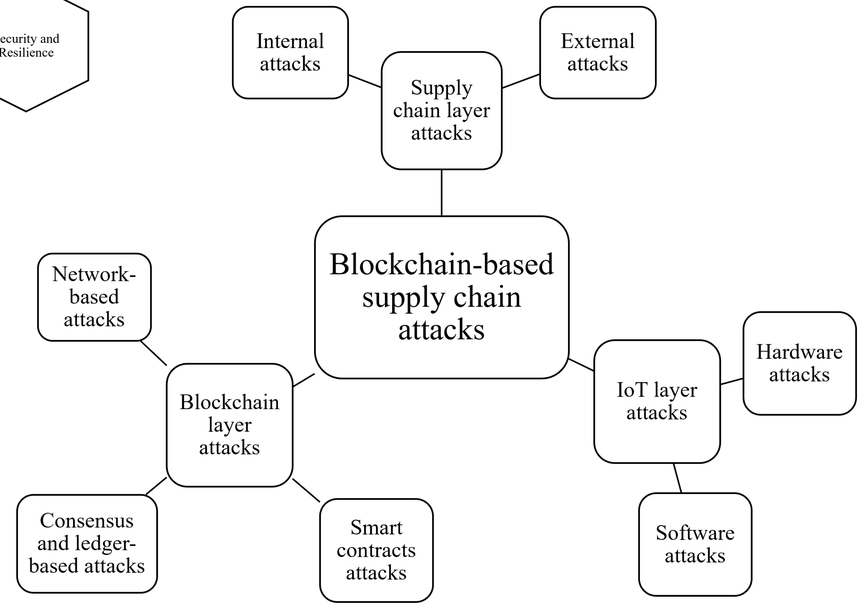
Blockchain Features

- Distributed Ledger Technology (DLT)
- Supports transparency and traceability in supply chain
- A prevention and detection measure to resolve supply chain security risks

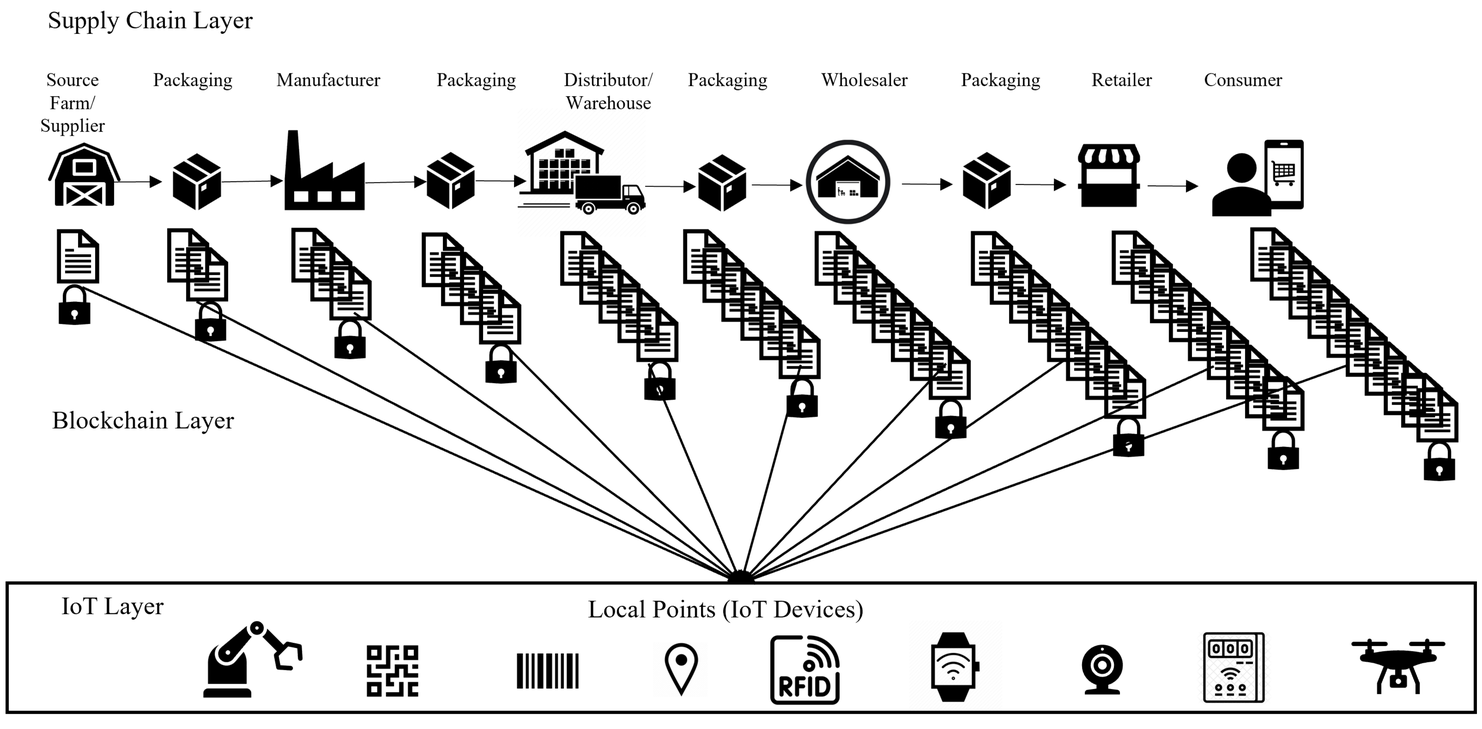


Security Challenges

- Supply chain layer attacks
  - Internal (internal infrastructure)
  - External (external infrastructure)
- Blockchain layer attacks
  - Network-based attacks: Eclipse and Sybil attacks
  - Consensus and ledger-based attacks: Compromise the hashing power-based consensus process
  - Smart contracts attacks: Modify the smart contract's code or execution and exploit the vulnerabilities, faults, or bugs in the contract or its execution engine
- IoT layer attacks
  - Hardware and Software attacks: due to weak security measures, inefficient transmission standards and protocols, limited resources, etc.



Layered Architecture of Blockchain-based Supply Chain Systems



Conclusion and Future Work

- Blockchain protects supply chain systems against cyber-attacks and unauthorized activities due to its key security features.
- Considering other cybersecurity countermeasures: machine learning detection methods, performing periodic network vulnerability scanning, and providing proper cybersecurity guides.
- Open issues besides security in blockchain-based supply chain systems are storage consumption, unbalanced workload, and latency.