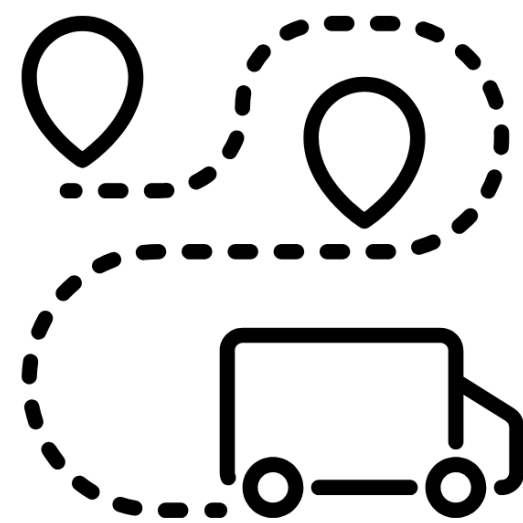


MoveChain

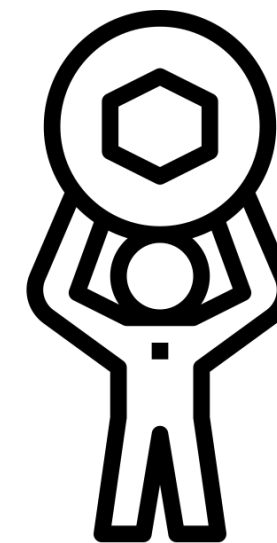
Secure, certified and trusted library for supply chain ownership

Simone Giuffrida, Azmat Ullah, Shahid Salim, Matteo Vaccargiu

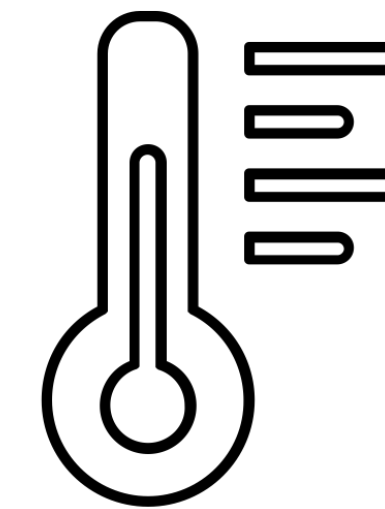
Idea



Secure, certified and
trusted supply chain
management



Control the access and manage
the ownership of a product in a
supply chain

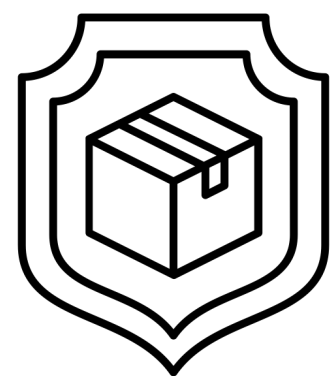


Control the environmental
conditions through IoT
devices

Motivation



Recent supply-chain interference, such as explosive devices built into pagers and remotely triggered (<https://t.ly/AKjnA>)

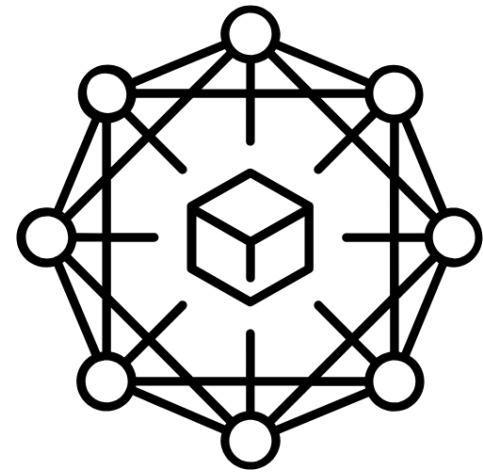


Real-time IoT monitoring of GPS, temperature, and humidity throughout the supply chain detects tampering and allows for early interventions to prevent damage



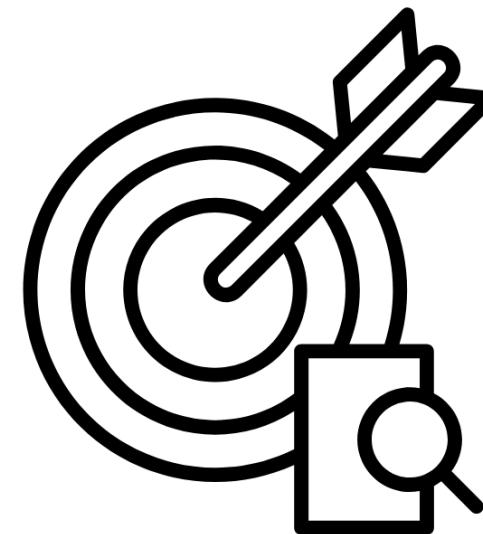
Securing supply chains enhances global health by ensuring safe distribution and building trust in the efficacy and safety of products

Technology and goals



Blockchain: IOTA for secure, scalable transactions.

Language: Move for smart contract functionality.



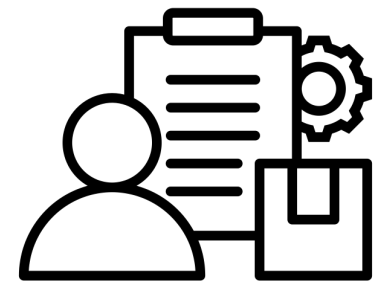
Enhance traceability and transparency in supply chains.

Reduce operational costs with IOTA's fee-less transactions.

Increase supply chain efficiency through automated smart contracts.

Improve security and integrity with immutable record-keeping.

Technical aspects - 1



We use Move's capability for resource-oriented programming to manage state transitions (Owned to Shared) seamlessly and securely.

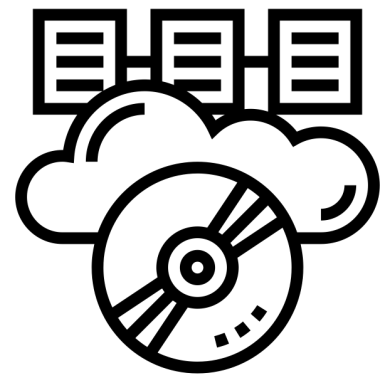


Move's typing and access control features ensure that only authorized users (producers, distributors, buyers) can perform specific actions, enhancing security and integrity.

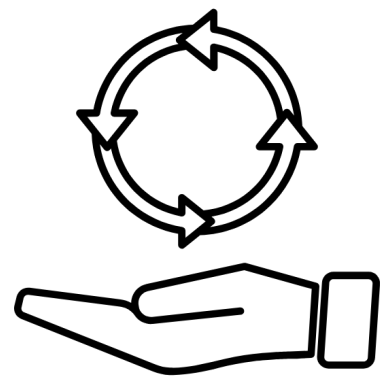


The code is structured into logical modules (creation, assignment, update, confirmation of products), making it maintainable and scalable.

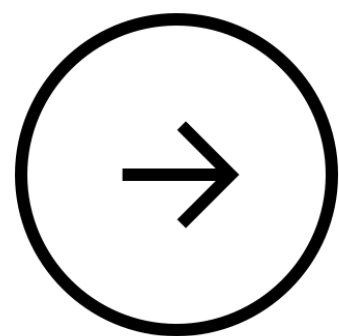
Technical aspects - 2



Store product details and transaction history in the blockchain, preventing tampering and enhancing traceability.



We use Move's capabilities to interact with dynamic objects such as managing product details and sensor data, showcasing flexibility in handling complex data structures



You can have detailed information about the code from the comments inside the file *movechain.move* and in the *README.md* file in the GitHub Repository

[iota/movechain at movechain · temp-dlt-school-24-org/iota \(github.com\)](https://github.com/temp-dlt-school-24-org/iota-movechain)

Product in MoveChain Library

```
/// Structure representing the product in the supply chain
public struct Product has key, store {
    id: UID,                // Unique product identifier
    owner: address,         // Current owner's address
    state: u8,              // Product state (STATE_OWNED or STATE_SHARED)
    producer: address,      // Producer's address
    distributor: address,   // Distributor's address (optional)
    buyer: address,         // Buyer's address (optional)
    sensor_data: u64,       // Recorded temperature
    min_sensor_data: u64,
    max_sensor_data: u64,
}
```

Deploy and testing - 1

Create a new product object with sensor data limit between 10 and 40:

```
iota client ptb --move-call 0x31266a683d242d2969ce31fb1ffe8d75b2c3c38fe02a93896d2e87e1dd28af22::  
SupplyChain::create_product 40 10 --gas-budget 50000000
```

Assign a buyer for the product object:

```
iota client ptb --move-call 0x31266a683d242d2969ce31fb1ffe8d75b2c3c38fe02a93896d2e87e1dd28af22::  
SupplyChain::assign_buyer "@0xc2a6666f7e42eb6e50ce48d7b40845ad260828c4a29d30bb9515d5aa43bb393d"  
"@0x96a7b331be70eeebf4f225675afd1b148aabe719ffcbe97cdd023adf1e40e2ac" --gas-budget 50000000
```

Assign a distributor for the product object:

```
iota client ptb --move-call 0x31266a683d242d2969ce31fb1ffe8d75b2c3c38fe02a93896d2e87e1dd28af22::  
SupplyChain::assign_distributor "@0xc2a6666f7e42eb6e50ce48d7b40845ad260828c4a29d30bb9515d5aa43bb393d"  
"@0x96a7b331be70eeebf4f225675afd1b148aabe719ffcbe97cdd023adf1e40e2ac" --gas-budget 50000000
```

Change the product object from owned to shared:

```
iota client ptb --move-call 0x31266a683d242d2969ce31fb1ffe8d75b2c3c38fe02a93896d2e87e1dd28af22::  
SupplyChain::change_to_shared "@0xc2a6666f7e42eb6e50ce48d7b40845ad260828c4a29d30bb9515d5aa43bb393d"  
--gas-budget 50000000  
Transaction Digest: 3v8pVW1QHR3VeELQXNYsv9niK9pMHYKeM6dPv5XasxDq
```

The function *confirm_delivery(product)* can be called by the buyer to confirm that the product is delivered correctly after checking the environmental sensor data

Deploy and testing - 2

Update sensor data at 50:

```
iota client ptb -move-call 0x31266a683d242d2969ce31fb1ffe8d75b2c3c38fe02a93896d2e87e1dd28af22::  
SupplyChain::update_sensor_data "@0xc2a6666f7e42eb6e50ce48d7b40845ad260828c4a29d30bb9515d5aa43bb393d"  
50 --gas-budget 5000000
```

id

1 {

2 "id": "0xc2a6666f7e42eb6e50ce48d7b40845ad260828c4a29d30bb9515d5aa43bb393d"

3 }

owner

0x25abb42ab4d3b57f82363d73a2f435e066700435abb2a56a3430c3cbd6aa90de

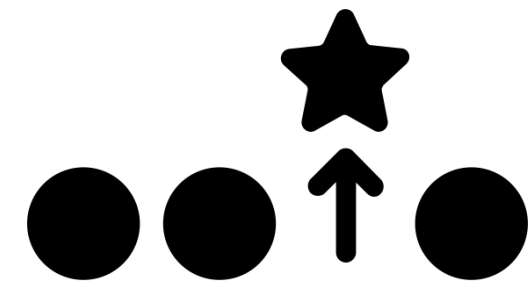
max_sensor_data

product_validity

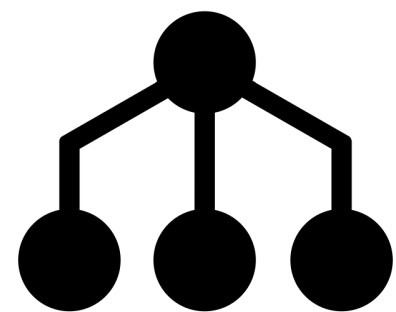
false

As 50 is outside of the range 10-40 the product validity is updated to *false*, so the buyer can check this value when he receives the product to verify the integrity of the object

Advantages of using Move and IOTA



Unlike Solidity, Move's resource-oriented programming prevents asset duplication and enhances security by treating digital assets as exclusive, non-copyable resources, significantly reducing bugs and vulnerabilities, such as reentrancy

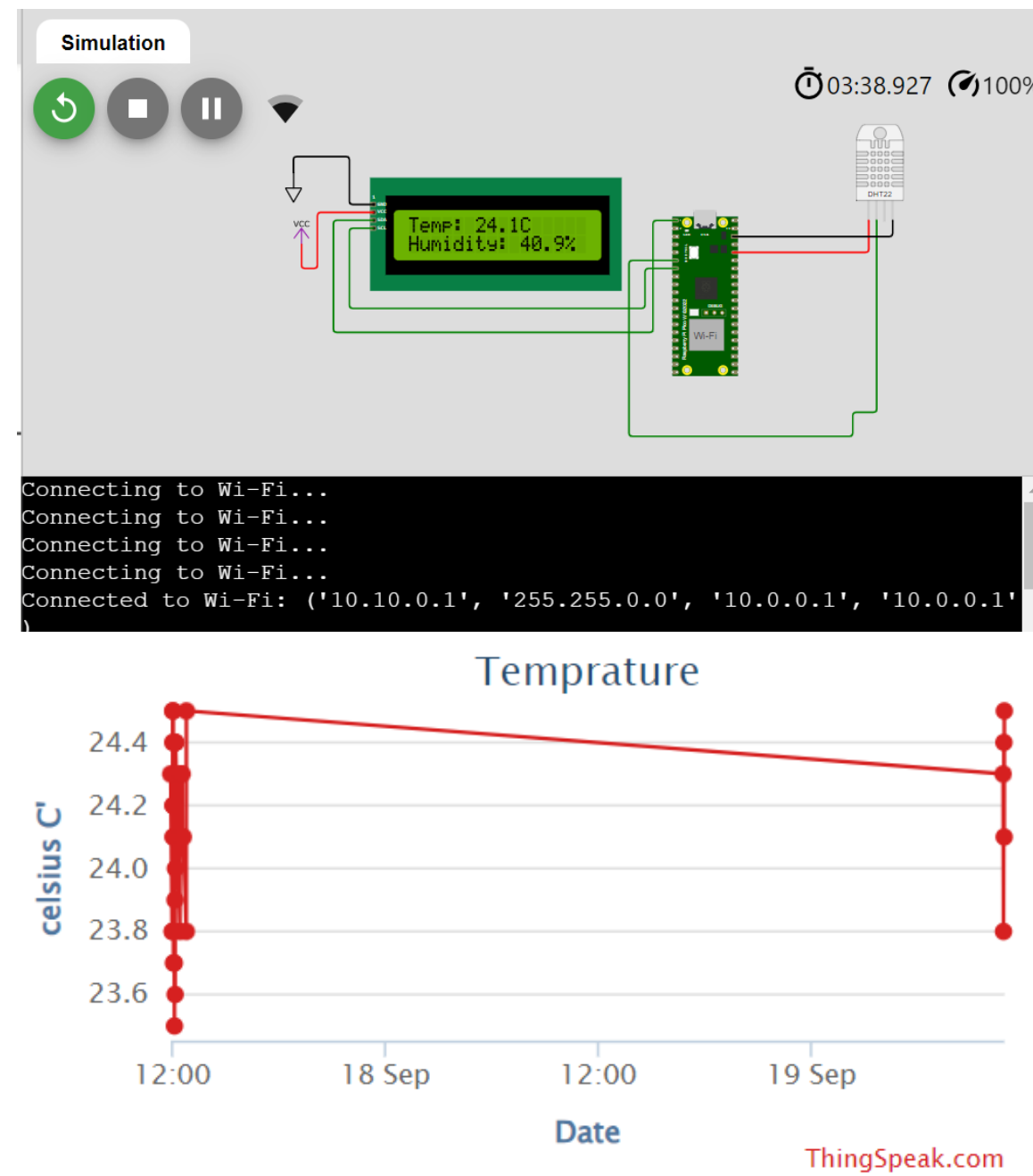


Employing a combination of owned and shared objects in Move optimizes memory usage and enhances accessibility of product information, whereas in Solidity, similar functionality would require complex and manually enforced state management



IOTA's low-fee structure enables cost-effective management of high-frequency events and transactions in supply chains, unlike Ethereum, where fluctuating gas fees can significantly increase operational costs

Future works



Interact with a simulated
data from a server using
an oracle
(ALREADY STARTED)

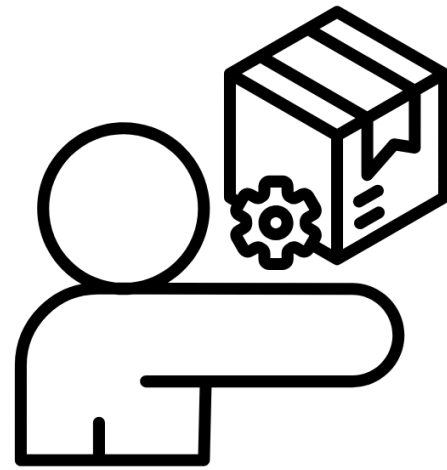


Try to implement a signing
mechanism that allowed us to use
Raspberry Pi to send a transactions
to IOTA

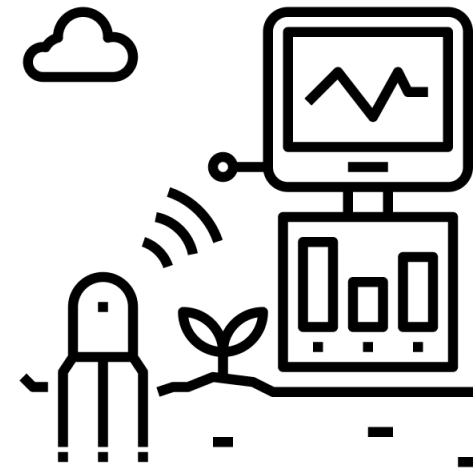


Implement a payment
mechanism in the library

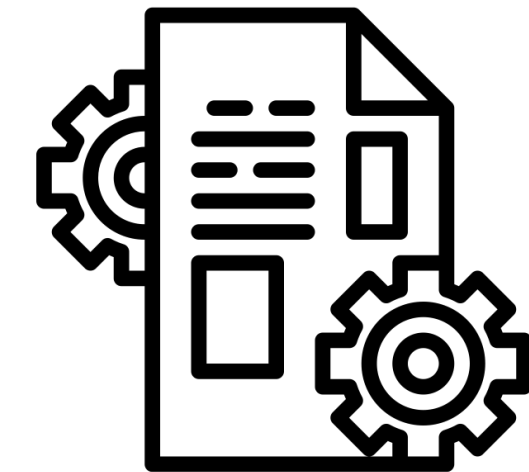
Takeaways



Move and IOTA help to
secure, certified and trusted
product ownership
management in a supply chain



Move and IOTA allowed to
interact with real time data
from sensors



Move Language provides
technical features that help us
to prevent some vulnerabilities
typical in Solidity