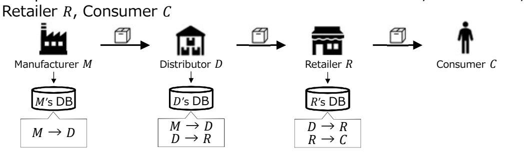
Design and Evaluation of a Privacy-preserving Supply Chain System Based on Public Permissionless Blockchain

Takio Uesugi, Yoshinobu Shijo, Masayuki Murata

Graduate School of Information Science and Technology,
Osaka University, Japan

Background

- **Supply chain is the sequence of processes from production to consumption**
  - The product is distributed in the order of Manufacturer M, Distributor D, Retailer R, Consumer C

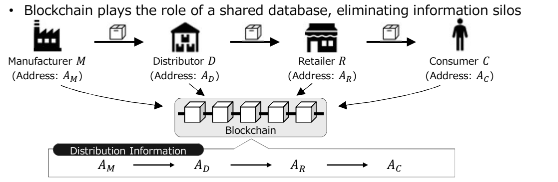


- **Supply chain traceability can no longer be secured**
  - The distribution of counterfeit products is on the rise
  - Problems spread due to delays in tracking when they arise

Supply chain systems using a blockchain have been proposed to secure the traceability.

Supply Chain System using Blockchain[4,5,15]

- **Distribution information is unitarily managed among multiple parties on blockchain**
  - Blockchain verifies and updates information based on a common logic
    - Blockchain prevents unauthorized information from being recorded
    - Blockchain plays the role of a shared database, eliminating information silos

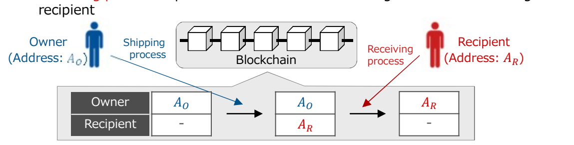


- **Public Permissionless blockchain is desirable**
  - For future scalability, it is desired that anyone can freely update and browse the distribution information on the system

[4] H. M. Kim, et al.,, "Toward an ontology-driven blockchain design for supply-chain provenance," Intel ligent Systems in Accounting, Finance and Management, vol. 25, pp. 18–27, Mar. 2018.
[5] H. Huang, et al., "Food supply chain traceability scheme based on blockchain and EPC technology," in Proceedings of Smart Blockchain, pp. 32–42, Nov. 2019.
[15] "Baseline Protocol." https://docs.baseline-protocol.org/. [Online; accessed 18-September-2020].

Supply Chain System based on Public Blockchain[3]

- **Managing distribution using smart contract**
  - Smart contract: customizable common logic
  - Two main processes
    - Shipping process: Specify the recipient by his/her address after confirming the executor is owner
    - Receiving process: Update the owner after confirming the executor is designated recipient

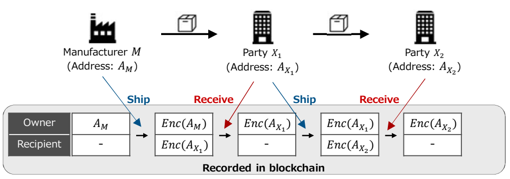


- **Privacy issues**
  - The ownership information about businesses or individuals is made public
    - Competitors can establish distribution relationships at little cost
    - Anyone can know the individual owner of the product

[3] K. Toyoda, P. Takis Mathiopoulos, I. Sasase, and T. Ohtsuki, "A Novel Blockchain- Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," IEEE Access, vol. 5, pp. 17465–17477, 2017.

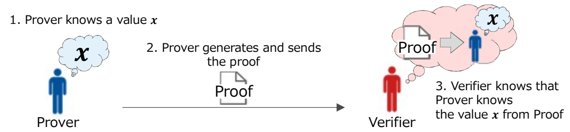
Research Purpose and Approach

- **Research purpose**
  - Propose a method that can secure the traceability of product distribution and preserve the privacy of distribution information in a public permissionless blockchain-based supply chain system
- **Approach**
  - Privacy preservation
    - Encrypt distribution information, or **blockchain addresses** with a manufacturer's public key
    - Prove to be a genuine party based on a zero-knowledge proof
  - Traceability
    - Track products by decrypting the encrypted distribution information



Zero-knowledge proof (ZKP)[19]

- **Proving information or knowledge without sharing it**
  - A prover can prove to a verifier that they know a value x, without conveying any information apart from the fact that they know the value x



- **Using key-pair to prove and verify**
  - A proving–verification key pair is generated in trusted setup
  - Prover generates a proof with the proving key
  - Verifier verifies the proof with the verification key

[19] A. M. Pinto, "An introduction to the use of zk-snarks in blockchains," in Proceedings of Mathematical Research for Blockchain Economy, pp. 233–249, Feb. 2020.

System Model

- **Precondition**
  - Target only the distribution of finished products
  - Track products with Electronic Product Codes (EPCs)
    - EPCs are written into RFID or QR code tags attached to the products
  - Use a public permissionless blockchain with turing-complete smart contract functionality
  - Supposed to be linked real-world entities and their blockchain addresses
- **Privacy Model**

Entity	Behabior allowed
Everyone	Browse manufacturer
Only Manufacturer	Browse ownership history

6

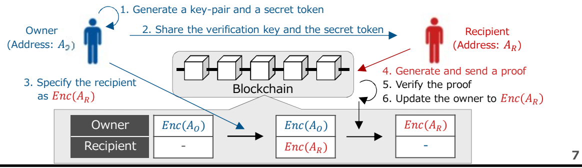
Overview of the proposed method

ship

- **Distribute a product among genuine parties**
  1. The owner generates a key-pair for ZKP and a secret token
  2. The owner shares the verification key and the secret token with the recipient
- **Conceal the distribution information via encryption**
  3. The owner specifies the recipient as the recipient's encrypted address $Enc(A_R)$

receive

- **Prove to be the genuine party**
  4. The recipient generates a proof that shows he/she has the secret token via ZKP and sends the proof to the blockchain
- **Confirm to be the genuine party by verifying the proof**
  5. The blockchain verifies the proof received is valid
  6. The blockchain updates the owner as the recipient's encrypted address $Enc(A_R)$



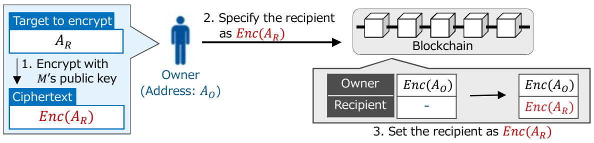
7

Conceal the Distribution Information

- **Record the encrypted address as the distribution information**
  - Encrypt the blockchain address via EC-ElGamal encryption
    - $Enc(A_R) = (kG, T + kQ)$
      - G: The elliptic curve generator
      - k: **The secret token**
      - Q: **The manufacturer's public key**
      - T: Recipient's blockchain address

Practically, T is $A_O \oplus A_R$ for security reasons

Shipping process of the distribution from owner(A_O) to recipient(A_R)

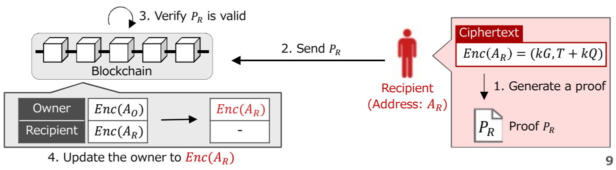


8

Prove to be the genuine party

- **The recipient prove that he/she can calculate the encrypted address by using ZKP**
  - The person who can calculate the encrypted address is considered as a genuine party
    - Only genuine parties hold the secret token
    - Calculating the encrypted address requires the secret token
- **No one knows recipient's blockchain address thanks to ZKP**

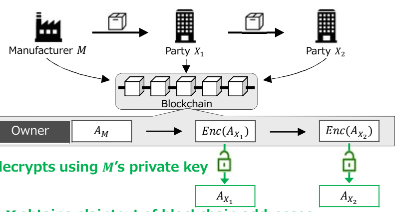
Receiving process of the distribution from owner(A_O) to recipient(A_R)



9

Product Tracking

- **Manufacturer tracks its product by decrypting the distribution information with its private key**
  - The distribution information is encrypted with the manufacturer's public key
- **Example:**
  The product is distributed in the order of manufacturer M, parties X_1, X_2

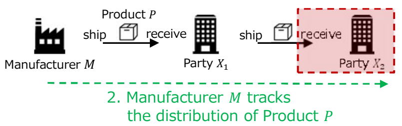


10

Demonstration

- **Distribution scenario**
  - Manufacturer M manufactures a product P
  - Product P is distributed in the order of M, X_1, X_2
- **Demonstration**

1. Party X_2 receives Product P from Party X_1



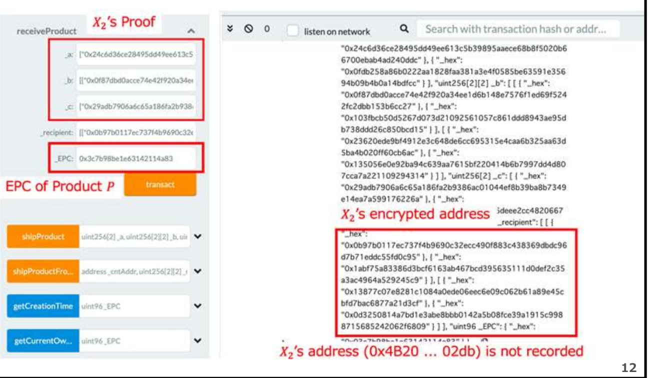
Party	Blockchain address
M	0x5B38 ... ddC4
X_1	0xAb84 ... 5cb2
X_2	0x4B20 ... 02db

- **Environment for implementation**
  - Blockchain: Ethereum[16]
  - Language: Solidity[21] (version 0.6.2)
  - JavaScript Virtual Machine: Remix[22]
  - Zk-SNARKs toolbox: ZoKrates[23]

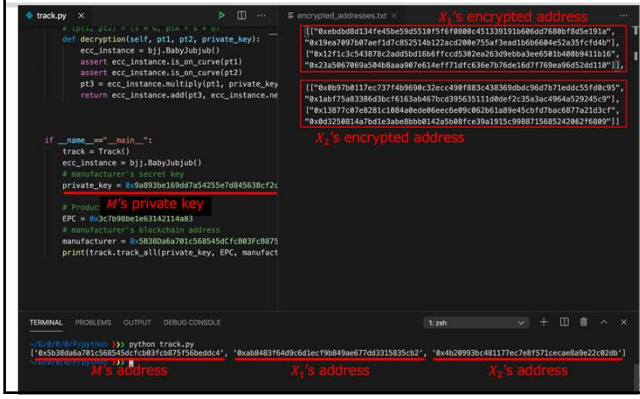
[16] V. Buterin, "Ethereum Whitepaper." https://ethereum.org/en/whitepaper/, 2013.
[21] "Solidity." https://solidity.readthedocs.io/
[22] "Remix - Ethereum IDE." https://remix.ethereum.org
[23] "ZoKrates." https://github.com/Zokrates/ZoKrates

11

Demo 1: Receiving a product

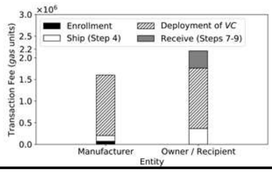


Demo 2: Product Tracking



Cost Evaluation

- **Evaluation Method**
  - Measure the transaction fees required for the distribution
- **The transaction fees per party are at most 2.2×10^6 *gas* units**
  - This is equivalent to 84.41 USD (September 9, 2020)
  - The transaction fees may be regarded as a kind of warranty
    - The proposed method can be applied to high-priced products such as automobiles and large home appliances
    - These are subject to recall if the products have a problem or defect



Summary and Future work

- **Summary**
  - We proposed a method for using a public permissionless blockchain to track product distribution while preserving privacy in a supply chain.
  - We preserved the privacy of distribution information via encryption and zero-knowledge proof.
  - We implemented the proposed method and verified that the fee per person involved in the distribution was at most 2.2×10^6 *gas* units.
- **Future work**
  - Preserve privacy at the protocol level
    - The proposed method only preserves privacy in the smart contract
  - Reduce the transaction fees
    - The proposed method can only be applied to high-priced products because the transaction fees are a bit high
  - Extend the proposed method so that it can deal with product assembly and disassembly
    - The proposed method can only be applied to finished products

(Appendix) Related Work

- **Only our method can realize both of traceability and privacy preservation in supply chain system based on public permissionless blockchain**