Supply Chain System using Blockchain

- 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

Supply Chain System based on Public Blockchain

- 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 designated recipient
    - 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

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)

- 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 $x$

1. Prover knows a value $x$
2. Prover generates and sends the proof $\text{Proof}(x)$ to Verifier
3. Verifier knows that Prover knows the value $x$ from Proof

- 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
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
<table>
<thead>
<tr>
<th>Entity</th>
<th>Behavior allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>Browse manufacturer</td>
</tr>
<tr>
<td>Only Manufacturer</td>
<td>Browse ownership history</td>
</tr>
</tbody>
</table>

Conceal the Distribution Information

- Record the encrypted address as the distribution information
  - Encrypt the blockchain address via EC-ElGamal encryption
    - \( \text{Enc}(A) = (kG, T + kQ) \)
    - \( G \): The elliptic curve generator
    - \( k \): The secret token
    - \( T \): The manufacturer’s public key
    - \( Q \): Recipient’s blockchain address
  - Practically, \( k \) is \( m \oplus n \) for security reasons

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, parties \( X_1, X_2 \)

Overview of the proposed method

- 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
  1. The owner specifies the recipient as the recipient’s encrypted address \( \text{Enc}(A) \)
- Prove to be the genuine party
  1. The recipient generates a proof that shows he/she has the secret token via ZKP and sends the proof to the blockchain
  2. Confirm to be the genuine party by verifying the proof
    1. The blockchain verifies the proof received is valid
    2. The blockchain updates the owner as the recipient’s encrypted address \( \text{Enc}(A) \)

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 \( X_1 \) receives Product \( P \) from Party \( M \)
  2. Manufacturer \( M \) tracks the distribution of Product \( P \)
- Environment for implementation
  - Blockchain: Ethereum
  - Language: Solidity (version 0.6.2)
  - JavaScript Virtual Machine: Remix
  - Zk-SNARKS: Zokrates

Conceal the Distribution Information Diagram

Prove to be the genuine party Diagram

Product Tracking Diagram

Demonstration Diagram
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 $2.2 \times 10^6$ 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 $2.2 \times 10^6$ 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**

<table>
<thead>
<tr>
<th>System Architecture</th>
<th>Information Handled</th>
<th>Permissioned</th>
<th>Public Permissionless</th>
<th>Concept Only</th>
</tr>
</thead>
</table>