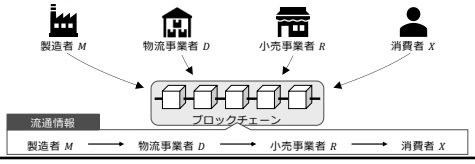
Protection of Confidential Information in Supply Chain System Based on Public Permissionless Blockchain

大阪大学 大学院情報科学研究科 村田研究室
上杉太氣央

情報ネットワーク学専攻修士論文発表会
2022年2月10日

研究背景

- **サプライチェーンの巨大化・グローバル化に伴う追跡性の低下**
  - 偽造品の流通拡大
    - 流通の正しさが保証されていない
  - 製品に問題・欠陥が発生した際の被害拡大
    - 製品製造者による迅速な追跡が実現されていない
- **ブロックチェーンを利用したサプライチェーン管理方法の登場**
  - 流通情報をブロックチェーンで一元管理することで、追跡性を担保
  - パブリックパーミッションレスブロックチェーンを使用
    - 新規事業者の参入、二次流通市場における個人間取引を実現可能



ブロックチェーンを利用したサプライチェーンシステム[3]

[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, Jun. 2017.

- **スマートコントラクトで製品の所有者情報の履歴を管理**
  - スマートコントラクト: ブロックチェーン上でプログラムを実行可能な仕組み
  - 所有者情報: ブロックチェーンアドレス (プログラム実行者の識別子)
  - 主な実行処理
    - 発送処理: 実行者をブロックチェーンアドレスで確認後、受領者を指定
    - 受領処理: 実行者が受領者であることをブロックチェーンアドレスで確認後、所有者を更新

- **既存手法の課題**
  - 機密情報の公開
    - 所有者情報を表すブロックチェーンアドレスが公開されてしまう
      - 企業間の取引関係、二次流通市場における個人間取引の特定が可能
  - 複数製品の流通が不可能
    - 実世界では、複数製品がダンボールやコンテナに集約される操作が存在

研究目的とアプローチ

研究目的

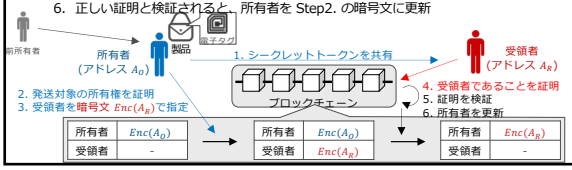
- パブリックパーミッションレスブロックチェーンを利用したサプライチェーンシステムにおいて、機密情報を保護しつつ、正規の所有者・受領者間での流通を可能にする手法を提案
- 複数製品の流通の実現
- 製造者による製品追跡の実現

アプローチ

- ゼロ知識証明を利用した所有権証明
  - 機密情報を保護しつつ、正規の所有者・受領者であることを確認
- 属性ベース暗号を利用した機密情報の保護
  - 流通単位に関わらず、流通情報を隠蔽

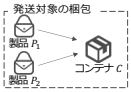
提案手法を利用した製品流通の手順

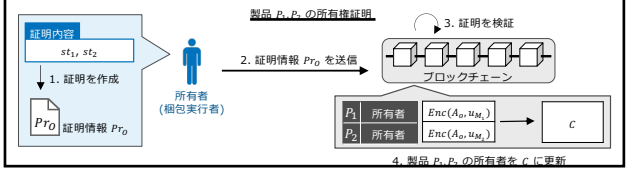
- **正規の事業者間での製品流通**
  1. 所有者は受領者に、シークレットトークンを共有
- **発送対象の製品の所有権証明**
  2. 前の所有者と共有したシークレットトークンを持っていることをゼロ知識証明に基づき証明
- **流通情報の隠蔽**
  3. 所有者は、受領者のブロックチェーンアドレスを暗号化した暗号文で、受領者を指定
- **正規の受領者であることの証明**
  4. 受領者は、Step1. のシークレットトークンを持っていることをゼロ知識証明に基づき証明
- **ブロックチェーン上で所有権を認証**
  5. ブロックチェーンは、証明検証用のスマートコントラクトで、受信した証明を検証
  6. 正しい証明と検証されると、所有者を Step2. の暗号文に更新



Step2: 発送対象の所有権証明

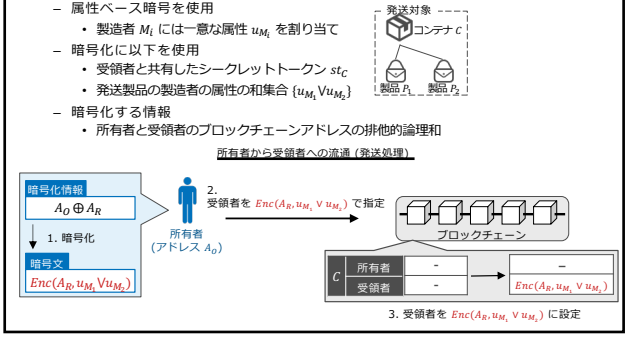
- **シークレットトークンから、製品の所有権証明を作成**
  - 前の所有者と共有したシークレットトークンを使用
- **複数製品は、発送単位に集約**
  - 製品とコンテナの包含関係を記録し、梱包を表現
- **ゼロ知識証明を利用するため、所有権の隠蔽が可能**
  - ゼロ知識証明: 情報を知っていることを、その情報を開示せずに、証明する手法
  - シークレットトークンが隠蔽され、他者が所有権を証明することを防止





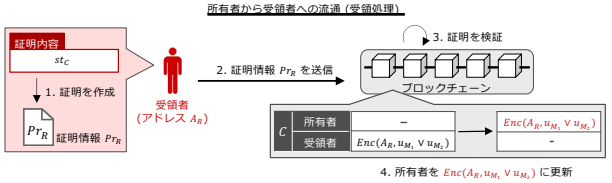
Step3: 流通情報の隠蔽方法

- **製品所有者を暗号文で記録することで、流通情報を隠蔽**
  - 属性ベース暗号を使用
    - 製造者 M_i には一意な属性 u_{M_i} を割り当て
  - 暗号化に以下を使用
    - 受領者と共有したシークレットトークン st_C
    - 発送製品の製造者の属性の和集合 $\{u_{M_1} \vee u_{M_2}\}$
  - 暗号化する情報
    - 所有者と受領者のブロックチェーンアドレスの排他的論理和



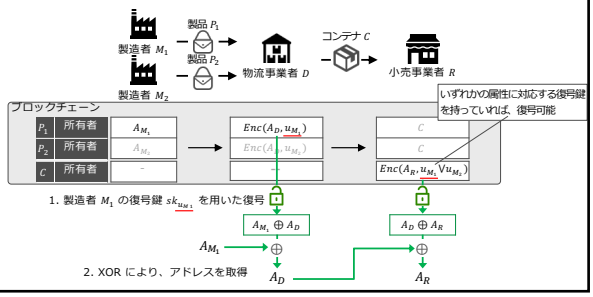
Step4-6: 受領者であることの証明方法

- **シークレットトークンを使い、所有権を証明**
  - 所有者と共有したシークレットトークンを使用
- **証明を検証後、所有者を更新**
  - 受領者に指定されていた暗号文で、所有者を更新



製品の追跡方法

- **製造者は、流通情報を復号することで製品を追跡**
  - 流通情報は、製品製造者の属性が指定された暗号文
  - 製造者は自身の製品であれば、流通情報を復号することが可能



シナリオ評価

[18] OpenABE, https://github.com/Fraunhofer-AISEC/OpenABE
[19] ZoKrates, https://github.com/Zokrates/ZoKrates
[20] Ganache, https://github.com/trufflesuite/ganache-ui

- **評価環境**

項目	説明
ブロックチェーン	Ganache[20] が提供する Ethereum ローカルネットワーク，Binance Smart Chain テストネットワーク
ゼロ知識証明	非対話型ゼロ知識証明 zk-SNARKs を利用できるツール ZoKrates[19]
属性ベース暗号	属性ベース暗号 (CP-ABE) を利用できるライブラリ OpenABE[18]

- **評価シナリオ**

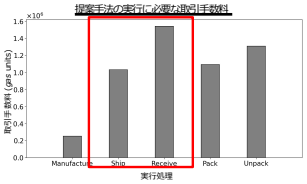
- **評価項目**
  - 正規の事業者間の流通が可能であることを確認
  - 製品の製造者確認が可能であることを確認
  - 流通情報の機密情報が保護されることを確認
  - 製品が製造者によって追跡できることを確認
  - 偽造品が登録できないことを確認

正しく動作することを確認した

コスト評価

設計した手法が、現実的に利用可能であることを確認する

- **一回の流通 (発送・受領) の取引手数料は 2.6×10^6 *gas* units**
  - 法定通貨換算の金額では最安 4.5 USD
    - 所有者情報の保護を行わない場合、0.4 USD (2.2×10^5 *gas* units)



  - コストは増加するものの、機密情報を保護可能
    - 偽造品が問題となるような高単価商品に適用可能
  - 問題・欠陥が発生した製品の交換・修理代金としての利用

まとめと今後の課題

- **まとめ**
  - ブロックチェーンを利用したサプライチェーンにおいて、流通情報を隠蔽しつつも、様々な流通単位での流通可能な方法を提案
    - 属性ベース暗号を利用した暗号化により、流通情報を隠蔽し、機密情報保護を実現
    - ゼロ知識証明を利用した所有権証明により、機密情報を保護しつつも、正規の所有者・受領者であることを確認
    - 製品製造者による流通の追跡を実現
    - 正規の製造者のみが流通を開始できることを保証
      - 消費者は製品の製造者を確認可能
    - 複数製品の集約、およびその逆操作である分解を実現
  - シナリオに基づいて実動作を確認、その際の取引手数料を計測
    - 一回の流通に必要な取引手数料は、2.6×10^6 *gas* units であることを確認
- **今後の課題**
  - プロトコルレベルでの機密情報の保護
    - ブロックチェーンは、スマートコントラクト実行者のアドレスを公開
    - 現在の提案手法では、発送者・受領者が自らスマートコントラクトを実行する実装であり、発送者・受領者のアドレスが、実行者のアドレスとして公開されてしまう