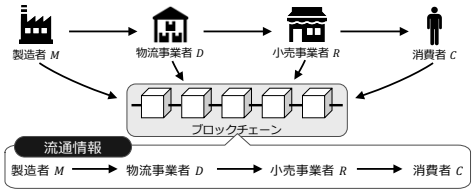
ブロックチェーンを利用したサプライチェーンにおけるデータプライバシー保護と追跡性の両立が可能なプロトコルの提案と動作実験

大阪大学 基礎工学部 情報科学科 村田研究室
上杉 太氣央

研究の背景

- **サプライチェーンマネジメントへの注目**
  - 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
    - 問題発生時に製品の所在特定に要する時間の増大
- **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**
  - ブロックチェーンを共有データベースとして利用
  - 流通情報を統合管理することで、追跡性を担保



ブロックチェーンを利用したサプライチェーン管理手法[4]

- **スマートコントラクトにより流通情報の管理を実現**
  - 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
  - 主な実行処理
    1. 発送処理: 実行者が所有者であることをアドレスで確認後、受領者を指定
    2. 受領処理: 実行者が指定された受領者であることをアドレスで確認後、所有者を変更

- **プライバシーの課題**
  - 所有者として記録されているブロックチェーンアドレスが公開される
    - 企業間の取引関係、二次流通市場における個人間取引の取引情報の特定が可能

ブロックチェーンアドレスを隠蔽することで、流通情報のプライバシーを担保する必要がある

[4] 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.

プライバシーと追跡性の関係

- **プライバシーを保護すると、追跡性の担保が困難**
  - プライバシー保護のために単純にブロックチェーンアドレスを隠蔽すると、以下の点が困難
    - 不正な流通経路の排除
      - 製品を受領しようとする者が、所有者が指定した受領者であることの確認ができない
    - 製品の所在特定
      - 誰を経由して流通したのか特定できない

ブロックチェーンアドレスを公開せずに、真正な事業者間で流通できていることを保証する仕組みが必要

  - 真正な事業者:
    - 製品の所有者は、受領者を指定して製品を発送する者
    - 製品の受領者は、所有者が指定した受領者である者
      - 受領者は製品を受領後、所有者になる

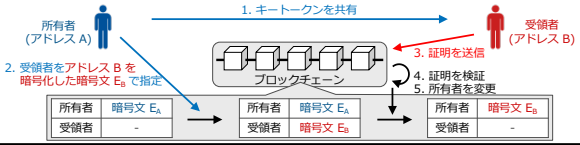
研究目的

研究目的
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、
流通情報のプライバシーを保護しつつも、真正な事業者間での
製品の流通を可能にする手法を提案

要求	要件	実現方法
プライバシー保護	• 流通情報であるブロックチェーンアドレスの隠蔽方法	• 流通情報を隠蔽するために、楕円曲線暗号を利用して流通情報を暗号化
追跡性の担保	• 真正な事業者間での流通を保証するための、真正な事業者であることの証明方法	• 真正な事業者であることを証明するために、ゼロ知識証明を利用
	• 問題の発生時には被害の拡散防止のための、製品を追跡する方法	• 製造者による製品の追跡を行うために、製造者が流通情報を秘密鍵で復号

提案手法を利用した製品流通の概要

- **真正な事業者 (キートークンを持つ者) の間で製品を流通**
  1. 所有者は受領者に、製品を受領するためのキートークンを共有
- **流通情報を暗号化により隠蔽**
  2. 所有者は、受領者のアドレスを暗号化した暗号文で、受領者を指定
- **真正な事業者であることを証明**
  3. 受領者は、手順 1. のキートークンを持っていることをゼロ知識証明し、その証明情報をブロックチェーンに送信
- **ゼロ知識証明を使用して、ブロックチェーン上でキートークンを認証**
  4. 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
  5. 正しい証明と検証されると、ブロックチェーンに記録されている所有者を手順 2. の暗号文に変更

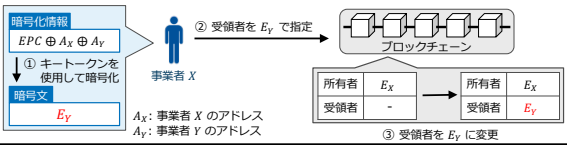


流通情報の隠蔽方法

6

- **製品の所有者を暗号文で記録することで、流通情報を隠蔽**
  - 楕円曲線暗号の暗号文を使用
  - 暗号化には以下を使用
    - キートークン
    - 製造者の公開鍵
      - 製造者が流通情報を特定するため
  - 暗号化する情報
    - EPC、所有者のアドレス、受領者のアドレスの排他的論理和
      - EPC (Electric Product Code): 製品を一意に識別するためのコード情報

事業者 X から事業者 Y への流通 (発送処理)



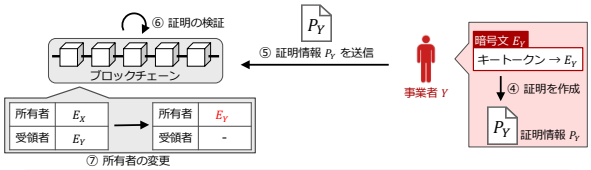
A_X: 事業者 X のアドレス
A_Y: 事業者 Y のアドレス

真正な受領者であることの証明方法

7

- **キートークンを持っていることを証明するために、受領者として記録されている暗号文を計算できることをゼロ知識証明**
  - 暗号文の計算には、共有したキートークンが必要
  - ゼロ知識証明であるため、暗号化前の情報の推測は不可能
    - 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

事業者 X から事業者 Y への流通 (受領処理)



発送者・受領者のアドレス、キートークンの値を公開することなく、自身が真正な受領者であることを証明できる

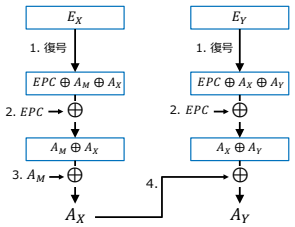
製造者による製品の追跡方法

8

- **製造者は、自身の秘密鍵で流通情報を復号することで製品を追跡**
  - 流通情報は、製造者の公開鍵で暗号化された暗号文

追跡例: 製造者 M、事業者 X、事業者 Y の順で流通したときの流通情報 (E_X, E_Y) から流通経路を特定

1. 製造者は、自身の秘密鍵を用いて、所有者履歴 E_X, E_Y を復号
2. 手順 1. で得られた数値と EPC の排他的論理和を計算
3. E_X から得られた数値と自身のアドレス A_M の排他的論理和から、事業者 X のアドレス A_X を取得
4. E_Y から得られた数値と事業者 X のアドレス A_X の排他的論理和から、事業者 Y のアドレス A_Y を取得

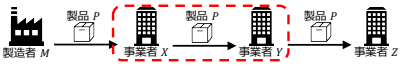


動作実験

9

[17] Remix - Ethereum IDE, https://remix.ethereum.org
[18] ZoKrates, https://github.com/Zokrates/ZoKrates

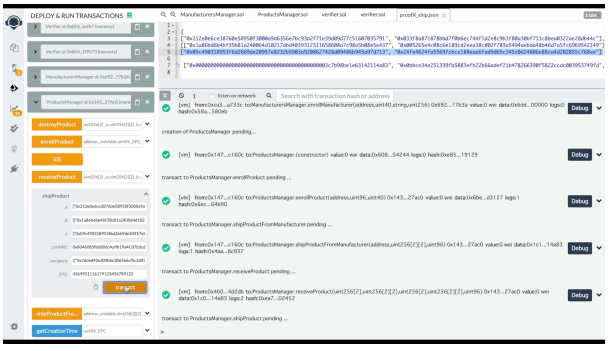
- **動作実験シナリオ**
  - 真正な事業者間の流通に関する検証シナリオ
    - 製品の製造者から複数の事業者を経由して、製品を流通できることを確認



  - 流通情報のプライバシー保護に関する検証シナリオ
    - 自身が関与した流通の情報以外は取得できないことを確認
  - 製品の追跡に関する検証シナリオ
    - 製造者は、自身が製造した製品の流通経路を特定できることを確認
- **動作実験環境**
  - ブロックチェーン
    - 統合開発環境 Remix[17] が提供する Ethereum ローカルネットワーク環境を利用
  - ゼロ知識証明の証明情報生成
    - 非対話型ゼロ知識証明 zk-SNARKs を利用できるツール ZoKrates[18] を使用
  - 楕円曲線暗号に使用する楕円曲線
    - $168700x^2 + y^2 = 1 + 168696x^2y^2$
      $(mod\ 21888242871839275222246405745257275088548364400416034343698204186575808495617)$

動作実験結果

10



まとめと今後の課題

11

- **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、真正な事業者間で流通可能な方法を提案
    - 所有者情報を暗号化することで、流通情報を隠蔽し、プライバシーを保護
    - 発送者・受領者間で共有した秘密の値を知っていることをゼロ知識証明することで、真正な事業者であることを確認
  - シナリオに基づいて実動作を確認
- **今後の課題**
  - 提案手法を利用した流通において、ブロックチェーンで必要となる手数料を用いた定量的な評価
    - スマートコントラクトの実行には、処理負荷に準じた手数料が要求される
  - 発送者・受領者とスマートコントラクトの実行者を分ける仕組みの検討
    - 使用したブロックチェーンプラットフォーム Ethereum は、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