偽物商品流通防止に向けたブロックチェーンを利用した商品所有権管理システム

豊田 健太郎[1]　P. Takis Mathiopoulos[2]　笹瀬 巌[3]　大槻 知明[3]

概要：10 年以上に渡って，RFID (Radio Frequency Identification) はサプライチェーンにおける偽物商品の混入を防止する手法として用いられてきた．しかしながら，RFID タグは簡単に複製できるため，一度公共の場，すなわちポスト・サプライチェーンに晒されるともはや製品の正規性を保証することができない．そこで本研究では，ポスト・サプライチェーンにおいても偽物商品の検知が可能なシステムを提案する．本システムは，商品の所有権管理を透明性の高いブロックチェーン上で行うことで商品の唯一性を保証する．本論文では，そのシステムのプロトタイプをブロックチェーンを用いた分散アプリケーションプラットフォームの `Ethereum` に実装し，そのコストの評価を行う．

キーワード：商品所有権管理システム, ブロックチェーン, Ethereum

A Blockchain-Based Products Ownership Management System for Anti-Counterfeits

Kentaroh Toyoda[1]　P. Takis Mathiopoulos[2]　Iwao Sasase[3]　Tomoaki Ohtsuki[3]

Abstract: RFID (Radio Frequency IDentification) technology has been successfully contributed as anti-counterfeits measures in the supply chain for more than a decade. However, the genuineness of RFID tags is no longer guaranteed in the post supply chain since these tags can be rather easily copied in the public space. To remedy this problem, we propose a system for anti-counterfeits that can be used in the post supply chain. Our idea is to publicly manage the products ownership with blockchain technology. We have implemented a proof-of-concept experimental system employing a blockchain-based decentralized application platform, `Ethereum`, and evaluated its cost performance.

Keywords: POMS (Product Ownership Management System), blockchain, Ethereum

1. はじめに

OECD (Organisation for Economic Co-operation and Development) によると 2007 年の時点で既に，世界における偽物の市場規模は 2,500 億米ドルに及ぶとされている [1]．その当時と比較しても e コマースは格段に発達していることから，偽物商品の流通を抑える手法の提案は喫緊の課題である．そのために，10 年以上もの間，RFID (Radio Frequency IDentification) を用いることで，サプライチェーンにおいて商品毎に入出荷イベントをトラッキングすることで各商品が偽物でないことを保証する仕組みが検討されてきた ([2–5] 等)．RFID サプライチェーンにおいて，製造者は商品毎に識別コードである EPC (Electronic Product Code) を割り当て，RFID タグにそれを書き込む．サプライチェーンの各パーティは RFID タグの付加された商品が到着する度に RFID リーダを用いて EPC を読み取る．さらに，次にそれらの商品を受け取るパーティが正しい経路を通過したことを確認するために，到着した証拠と

[1] 慶應義塾大学大学院
Graduate School of Keio University, Japan
[2] National and Kapodestrian University of Athens, Greece
[3] 慶應義塾大学 理工学部 情報工学科
Department of Information and Computer Science, Keio University, Japan

なるデータを各タグに書き込む．これにより，RFID タグに記述されたデータの整合性に不一致が生じた場合には偽物の可能性があると考えることができる．

しかしながら，一度サプライチェーンの外に商品が小売店まで届き，店頭に並んだ場合，それらの商品の正規性はもはや保たれない．これは RFID リーダは市販されていることから，誰でもタグの情報を読み取ることができるためである．偽物の流通を目的とする攻撃者は，このように読み取った正しいタグの情報を偽物に付加したタグに書き込むことにより，RFID による偽物の判別を行うことを困難にすることが可能である．したがって，ポストサプライチェーンにおいて，RFID タグの情報の正規性が保証されない状況においても偽物と正規の商品を見分けられるシステムの構築が早急に求められている．

そこで本論文では，商品所有権管理システム (POMS: Product Ownership Management System) を提案する．本システムにより，攻撃者が例え正規のタグの情報を複製したとしても，その商品の所有権を主張することを防止し，本物の所有者のみがその商品を所持することを保証する．この目的のために，分散管理型の仮想通貨である `Bitcoin` を考えを用いる [6]．`Bitcoin` ではユーザの所持する取引残高はユーザが自律的に管理する唯一の公開台帳 (ブロックチェーン) に保存される．すなわち `Bitcoin` では残高の所有権証明を行うのに対し，提案システムでは商品の所有権証明を行う．システムが正しく稼動するために，いくつかの要件が存在する．例えば，正規の製造者のみが商品の所有権最初の所有者であり，かつその商品は自社のものでなければならない．これらの要件を考慮に入れ，ポストチェーンにおいても偽物検知が可能なように，ブロックチェーンを用いた商品所有権管理システムを提案する．まず初めにシステム全体に必要な要件をまとめた後に，サプライチェーンにおける各パーティならびに消費者が RFID の付加された商品の所有権の移行および証明を可能とするプロトコルを示す．本システムの利点のひとつとして，消費者は商品の購入前にその商品が正規であるかを確認できる点である．この提案プロトコルに基づき，ブロックチェーンを利用した分散アプリケーションプラットフォームである `Ethereum` 上に PoC (Proof-of-Concept) となるシステムを構築する．特性評価により，提案システムを用いて所有権を移行・管理するのに 1 商品あたりに 1 米ドルで十分であることを示す．

以下，2 章で前提となるシステムモデルと従来の RFID サプライチェーンにおける偽物検知手法の欠点，`Bitcoin` とブロックチェーン，`Ethereum` について紹介する．5 章で提案システムを説明し，6 章において特性評価を示す．最後に 7 章において結論を述べる．

2. 前提

2.1 商品の流れ

図 1 に商品が製造者 (Manufacturer) によって製造され，消費者 (Customer) に渡るまでの流れを示す．RFID サプライチェーンは製造者 (Manufacturers)，配送業者 (Distributors)，小売店 (Retailers) の 3 つのパーティから構成される．製造者は商品を製造，梱包し，配送業者に配送する．配送業者は一旦商品を取り出し，それぞれの小売店に向けて再梱包し，配送する．小売店は商品の在庫を保管し，店頭に並べて販売する．ポストサプライチェーンにおいては，小売店が顧客に商品を販売し，顧客はそれを保持し続けるか，中古品店もしくはインターネットオークションなどで売却する．

さらに製造者は商品毎に識別コードである EPC を割り当て，RFID タグにそれを書き込む．各パーティは EPCglobal C1G2 (Class 1 Generation 2) に準拠した UHF (Ultra High Frequency)RFID リーダを使用し，入出荷時に商品に付加されたタグの読取を行う．これにより，(i) 商品のトラッキングや在庫管理 ([7,8] 等)，(ii) 商品が正規の経路を通過したかを確認 ([2–5,9] 等) を可能とする．

3. 関連研究

3.1 従来研究の問題点

しかしながら，一度小売店に商品が展示されると商品の RFID タグは誰でも RFID リーダを用いて読み取ることができるため，RFID を用いた商品の唯一性は保証されない．従来研究はいずれもタグに記述された内容が安全に管理されていることを前提としているため，ポストサプライチェーン環境においては適用できない．そこで商品毎に所有権を管理することが考えられる．すなわち，商品が製造されてから現在の所有者までの所有権の移行履歴を管理するシステムが必要である．偽物の所有者はその正規の商品の所有権を主張できないため，このようなシステムによって偽物であることを検知することができる．この論理を理解するために，以下の例を考える．中古品店でブランドの商品を購入しようとしている顧客が存在し，その商品には固有の EPC が書き込まれた RFID タグが付加されているが実は偽物である．このとき EPC の正規性のみを確認しただけでは，その商品が偽物であるかを判定することはできない．この顧客は EPC の正規性の確認だけでなく，(i) その商品 (もしくはその EPC) がその製造者であり，(ii) 現在の所有者が中古品店であることを確認する必要がある．これらの要件を満たす最も単純な実現方法としては，製造者が大規模な商品の所有者管理システムを構築し，運営することである．しかしながら，この方法はまずスケーラビリティの問題に直面する．すなわち，どのユーザも所有権

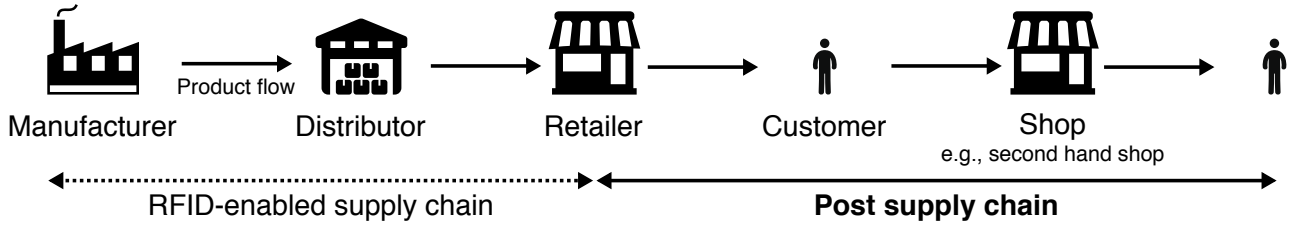

図 1　ポストサプライチェーンまでの商品の流れ.
Fig. 1　Product flow of until the post supply chain.

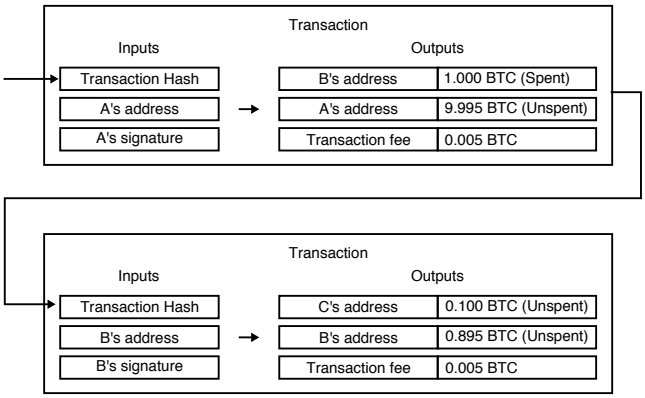

図 2　Bitcoin におけるトランザクションの例.
Fig. 2　An example of a Bitcoin transaction.

を購入した商品の所有権を主張するために，ユーザ登録を行う必要がある．近年では，世界規模で同一商品を販売する必要があるため，世界規模のユーザ管理を行う可能性がある．さらにこの方法はセキュリティの面で懸念がある．より具体的には，製造者が一括して所有者を管理する場合，ユーザ毎にパスワード管理が必要となるだけでなく，システムから情報が流出した場合各商品の所有者が露呈してしまう．近年の RockYou に代表されるパスワード流出問題が後を絶たない [10]．このことから本システムは規模だけでなくセキュリティ対策への投資が必要となるため，現実的でない．

4. ブロックチェーン関連技術

4.1 Bitcoin とブロックチェーン

上記の問題点を回避するために，中央管理ではなく，分散管理による商品所有権管理システムを検討する．そのために，分散管理型の仮想通貨である Bitcoin に着目する．その理由として，Bitcoin ではユーザ認証を必要とせずにユーザの取引履歴を管理しており，この概念を応用すると所有権の管理を行うことができるためである．そのために，ここで Bitcoin の仕組みを簡潔に説明する．Bitcoin は銀行のような中央管理者が存在しない金融システムである．**図 2** に Bitcoin における取引の例を示す．この図の上の Transaction において，ユーザ A が B に対して 1.000 BTC (Bitcoin の通貨単位) だけ送金する例を示しており，下の Transaction ではユーザ B がここで受け取った 1.000BTC

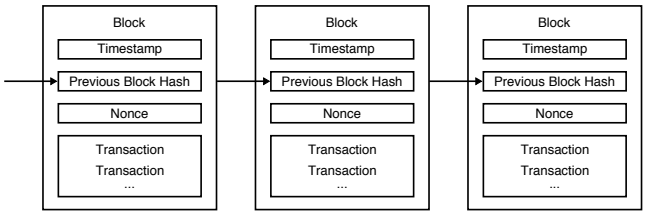

図 3　ブロックチェーンの例.
Fig. 3　An example of a blockchain.

のうち 0.100 BTC をユーザ C に送金する例を示す．ここでトランザクションが Inputs と Outputs の 2 つから構成されている．Inputs は送金者が自身が保有する残高を指定し，Outputs には受領者のアドレスを指定する．さらに Inputs では残高が含まれるトランザクションのハッシュ値で指定し，さらにその残高を使用することの確認としてそのアドレスに対する秘密鍵で生成した署名を付加する．一度使用された残高は Spent となり，それ以降使用することができない．この図の例では，ユーザ B は自身の管理するアドレスに宛てて送金された 1.000 BTC を使用するためにそのアドレスの秘密鍵で署名し，ユーザ C に対して送金を行っている．したがって，あるアドレスに対する秘密鍵さえ知っていればその取引に含まれる未使用の残高を使用できるため，ユーザは任意の個数のアドレスを生成し，使用することができる．これにより一定のプライバシを保つことができる．通常，ウォレットと呼ばれるアプリケーションによって複数のアドレスおよび鍵を管理する．

Bitcoin は分散管理システムであり，P2P ネットワークを通じてユーザによって管理される．そのために，ネットワーク全体で唯一正しいと認める取引履歴を維持・管理する必要がある．このネットワーク全体での合意が形成されないと，悪意のるユーザによって一度使用された取引を無かったこととし，再び別の取引に使用することを許してしまう．この攻撃は二重払いと呼ばれる [6]．Bitcoin では二重払いを防ぐためにブロックチェーンと呼ばれる，公開台帳の仕組みを取り入れている．**図 3** にブロックチェーンの例を示す．この図のように，ブロックチェーンは承認されたトランザクションが含まれるブロックによって形成されるチェーンの構造をしている．このブロックに含まれたトランザクションは承認されたとみなされる．二重払いを防ぐために，ブロックは簡単に生成できないようにする必

要がある．そこで Bitcoin では PoW (Proof-of-Work) と呼ばれる仕組みでこれを実現する．ブロックの生成は採掘者と呼ばれるユーザによって行われ，解くのは難しいが検証するのは容易な暗号パズルを解くことに等しい．より具体的には，採掘者は前のブロックの参照，未承認のトランザクションと共に SHA-256 のハッシュ関数に入力したときの出力値が難易度によって定まる値よりも小さくなるようなナンス値を探すことである．この難易度はネットワーク全体でいずれかの採掘者が約 10 分に 1 回解けるように自動的に調節される．そしてブロック毎の難易度の合計が最大 (≒ 最長のブロックチェーン) に含まれるトランザクションが承認されたとみなす．採掘者がこのプロトコルに従うように，Bitcoin では最初にブロックを生成した採掘者に対して，新しく発行される BTC に加え，そのブロックに含まれる全トランザクションの取引手数料を報酬として与える．この仕組みにより攻撃者が二重払いのために過去の承認されたトランザクションを無かったことにし，それが含まれるブロックを改竄しようとすると，そのブロックを解き直す必要がある．さらにブロック生成には前のブロックのハッシュ値が必要であるため，攻撃者は最長のブロックチェーンになるまで後続のブロックもすべて解き直す必要がある．これは攻撃者が採掘者全体において圧倒的な計算能力を保持する必要があり，現実的でない．

商品所有権管理システムを構築するためには，Bitcoin における “通貨” を “商品” に変えればよい．この概念は既に存在しカラードコイン (CC: Colored Coin) と呼ばれている．例えば，CC は車や家といった財産，株などのアセットを発行するために用いられる．[11, 12] といったほとんどの CC は，Bitcoin のシステム上に構成され，より具体的には Bitcoin において送金のために満たすべきルールを記述できるスクリプト機能を利用している．CC を利用してサプライチェーンにおけるコンテナの入出荷イベント管理を行う手法が提案されている [13]．しかしながら，この手法は本研究で想定している商品所有権管理システムに必要ないくつかの要件を満たしていない．例えば，所有権を移行するためにはわずかながらも送金を行う必要があり，プロトコルに従うことで各パーティは金銭的に損をする．したがってプロトコルに従った場合，そのパーティにインセンティブを与える必要がある．これを従来提案されている CC で行うことは困難である．そこで，提案システムを構築するためには，ブロックチェーンを利用しつつ，任意のアルゴリズムを記述可能なチューリング完全なプラットフォームが必要である．

4.2 Ethereum

Ethereum はブロックチェーンを用い，チューリング完全性をサポートする仮想通貨である [14]．Bitcoin と同様に，暗号パズルに基づくブロックチェーンによるトランザクションの取引履歴の管理を行う．チューリング完全性をサポートするために，Ethereum では 2 つのアカウントの種類が存在すう．一方は EOA (Externally Owned Account)，他方は CA (Contract Account) と呼ばれる．EOA は単にそのアカウントの残高を管理するが，CA はアルゴリズムを表現するためのコードとストレージ領域を持ち，EOA もしくは CA からメッセージを受け取ると記述されたコードが実行される．

CA に記述されたコードは採掘者によって実行される．したがって，チューリング完全性をサポートするということは，攻撃者が採掘者に対して無限ループのように延々と計算をさせることを可能とする．これを防ぐために，送金者はストレージの内容を変更するような全てのコードの実行に対してコードの実行量に応じた “gas” と呼ばれる実行手数料を払う必要がある．この gas が実行途中で切れた場合には，コードの状態は実行前に戻されるが，消費した gas は送金者には返却されない．また Bitcoin と同じく，手数料は最初の暗号パズル解読者に与えられる．

Ethereum においてコードの記述をするために，Solidity と呼ばれるスクリプト言語が一般的に使用される[*1]．Solidity で記述されたコードは CA が実行できる形式にコンパイルされる．したがって，提案システムは Solidity によって記述し，Ethereum 上で稼動させることが可能である．次の章では本システムについて詳細に説明する．

5. 提案システム

本章ではまずシステムに必要な条件を挙げ，Ethereum 上で実装したシステムに関して主な部分を説明する．そして提案システムを用いて各パーティがどのように所有権を移行・証明を行い，偽物商品の検知を行うのかについて述べる．

5.1 システムに必要な条件

提案システムの詳細なプロトコルを説明する前に，必要な条件を示す．

(1) 正規の製造者のみが製造した商品 (EPC) の最初の所有者となること
(2) 各製造者は自社の商品の所有権のみを持つこと
(3) 1 商品に対して 1 人のみが所有権を持つこと
(4) 製造者は本システムを利用し正しくプロトコルに従うパーティにインセンティブを与えること

1 つ目の条件は攻撃者が不正に商品の所有権を主張することを防ぐために必要である．2 つ目の条件は，ある製造者が他社の商品の所有権を最初に主張することを防ぐ．さらに 3 つ目の条件によって，同時に 2 人以上がある商品の所有権を主張できないようにする．これにより，ある消費

[*1] https://github.com/ethereum/solidity

者が商品を購入しようとした際に，小売店がその商品の唯一の所有者であることを確認できる．また 4 つ目の条件により，正しく所有権を移行した際に発行されるトランザクション手数料に加え，いくらかのインセンティブを送金者に与える．インセンティブは本システムにより利益を獲得できる製造者によって支払われる．これにより各パーティが正しくプロトコルに従うことを可能とする．

5.2 実装 CA

上記の要件を満たす 2 つの CA を実装し，提案システムを構築する．それらを MM(ManufacturersManager) および PM(ProductsManager) と呼び，MM は製造者に関する情報を管理 (製造者のアドレスと EPC に含まれる製造者コード company prefix の登録など) し，PM は製品の情報を管理 (商品の登録，所有権の移行・所有者の確認など) する．本論文においては，コード全体のうち，主要な部分のみコードを記述し，解説を行う．

5.2.1 ManufacturersManager

提案システムにおいて，製造者の登録を担う信頼できる第三者機関の存在を仮定する．これは攻撃者が正規の製造者になりすまして製造者登録を行うことを防ぐためである．この機関として EPC の company prefix を扱う GS1 (Global Standard One) が考えられる．

以下に MM において製造者の情報を管理するためのデータ構造を示す．

```
struct ManufacturerInfo {
  uint40 companyCode;
  bytes32 companyName;
  uint expireTime;
}

mapping (address => ManufacturerInfo) manufacturers;
```

このようなデータ構造に対し，信頼できる第三者機関のみが製造者の情報を登録できるように，以下の関数を定義する．

```
function enrollManufacturer(address m,
  uint40 companyCode, bytes32 companyName,
  uint validDurationInYear) onlyAdmin {
  manufacturers[m].companyCode = companyCode;
  manufacturers[m].companyName = companyName;
  manufacturers[m].expireTime = now +
    validDurationInYear;
}
```

5.2.2 ProductsManager

PM は各商品の状態を管理する CA である．商品の情報のデータ構造を以下のように定義する．データ構造は，(i) 現在の所有者である owner，(ii) 商品が配送中もしくは譲渡中である場合に受領予定のパーティを記述した recipient，(iii) 商品の現在の状態 (輸送中，リコール中など) を表す status，(iv) 製造された日時 creationTime，(v) 商品が過去に何回輸送されたか nTransferred の 5 つの項目からなる．これらのデータが必要な理由は後程説明する．

```
enum ProductStatus {Shipped, Owned, Disposed}

struct ProductInfo {
  address owner;
  address recipient;
  ProductStatus status;
  uint creationTime;
  uint8 nTransferred;
}

mapping (uint96 => ProductInfo) products;
```

製造者が自社の商品の最初の所有権を登録できるように以下の関数 enrollProduct() を定義する．より具体的には，checkAuthorship() において EPC に含まれる company prefix が製造者 (mmAddr) のものであるかを確認する．

```
function enrollProduct(address mmAddr, uint96 EPC)
  onlyNotExist(EPC) onlyManufacturer {
  ManufacturersManager mm =
    ManufacturersManager(mmAddr);

  if (mm.checkAuthorship(EPC)) {
    products[EPC].owner = manufacturer;
    products[EPC].status = ProductStatus.Owned;
    products[EPC].creationTime = now;
    products[EPC].nTransferred = 0;
  }
}
```

商品の所有権を移行するために，2 つの関数 shipProduct() および receiveProduct() を定義する．shipProduct() はある商品の現在の所有者が次の所有者に所有権を移行する際に使用される．一方，receiveProduct() は商品の受領者が確かに商品を受領し，所有権の移行を了承する際に使用される．このように所有権の移行を行う際に所有権を移行する側と受領する側で関数を分けることにより，商品を配送したが受領側が受け取っていないような状況において所有権だけが移行される事態を防ぐことが可能である．同様の理由により，商品を管理するためのデータ構造において owner と recipient を分けている．

Ethereum では，トランザクションの発行毎に手数料が必要となる．したがって，現在の所有者が受領者に商品を所有権を移行する際に，shipProduct() を行うことを怠る可能性がある．この事態を避けるために，本システムではインセンティブを取り入れる．すなわち，商品の所有権

が正しく移行された際には，その商品の製造者がその報酬を shipProduct() の発行者に支払う．しかしながら，悪意のある 2 パーティによって，所有権の移行を繰り返すことでインセンティブを得続けることを避けるために，所有権の移行に対するインセンティブを与える回数に上限 MAXTRANSFER を設定する．具体的に transferReward および MAXTRANSFER をどの程度に設定すべきは，今後の研究課題とし，ここでは議論しない．

```
function shipProduct(address recipient, uint96 EPC)
  onlyExist(EPC)
  onlyOwner(EPC)
  onlyStatusIs(EPC, ProductStatus.Owned) {
  if (recipient == products[EPC].owner) {
    throw;
  } else {
    products[EPC].status = ProductStatus.Shipped;
    products[EPC].recipient = recipient;
  }
}

function receiveProduct(uint96 EPC)
  onlyExist(EPC)
  onlyRecipient(EPC)
  onlyStatusIs(EPC, ProductStatus.Shipped) {
  products[EPC].owner = msg.sender;
  products[EPC].status = ProductStatus.Owned;
  products[EPC].nTransferred =
    products[EPC].nTransferred + 1;

  if (products[EPC].nTransferred <= MAXTRANSFER) {
    msg.sender.send(transferReward);
  }
}
```

5.3 各パーティの手続き

図 4 に提案システムの概要を示す．図において，製造者が製造者情報を登録を信頼できる第三者 A に要求し，商品を登録，配送，所有権の移行を行うところまでを説明する．

(1) 製造者 M は enrollManufacturer() を MM に対して発行し，自社の EPC に含まれる company prefix とアドレスの登録を行う．

(2) 製造者 M は製造した $N_{products}$ 個の商品に対して，固有の EPC $\mathtt{EPC}_i$, $(1 \leq i \leq N_{products})$ を割り当て，それぞれの RFID タグに書き込む．さらに，それらの最初の所有権を登録するため，enrollProduct() を商品毎に発行する．

(3) 製造者 M は商品を発送後，recipient に受領者のアドレスを指定した上で shipProduct() を商品毎に発行する．

(4) 受領側 (配送業者 D, 小売店 R, 中古品店 S, 消費者 C 等) は商品を受け取った後，商品に付加された EPC を RFID リーダを用いて読み取り，リーダのアプリケーションが自動的に receiveProduct() を発行する．これにより，M が指定した recipient と受領者のアドレスが一致した場合のみ，所有権が受領側に移行される．

(5) 受領者はさらに他のパーティに商品を輸送する際には，上記の手続き 2 から 4 までを行い，所有権を移行させる．

5.4 プロトコルの正当性

本節では，提案システムによって偽物検知ができる理由を説明する．より具体的には，正規のパーティが本システムを利用する限り，攻撃者は偽物を製造する経済的利点が無いことを示す．

ここで，攻撃者が製造する偽物は本物の商品と同じ EPC が書き込まれた RFID タグが付加されているとする．さらに，消費者は中古品店等でブランド品の購入を検討していると仮定し，購入したい商品が偽物であるかを購入前に確認したいとする．消費者は PM にその EPC の現在の所有者を確認し，現在購入を検討している販売者のアドレスと一致するかを確認する．一致しない場合，この販売者がその商品の所有権を持っていないために，購入を事前に中止することが可能である．

次に攻撃者が正規の商品とその偽物を所持している場合を考える．この時，攻撃者にとって偽物を製造する経済的な価値がないことを示す．商品購入者は，商品を購入と同時にその商品の所有権が自身のアドレスに移行されていることを確認できる．ここで攻撃者が偽物を配送したとしても，正規の攻撃者は以後保持している正規の商品の所有権を主張することができない．したがって，例え攻撃者が正規品を保持していたとしてもその所有権がないため，正規品はその価値を失う．一般的に偽物は正規の商品よりも格安で販売されるため，結果として攻撃者は損失を被る．このことから，攻撃者にとって偽物を製造する経済的な価値がないことがわかる．

5.5 提案システムの利点

提案システムの利点は大きく 2 つある．1 つ目は例え正規の RFID タグが複製され，偽物に付加されたとしても偽物検知が可能である点である．したがって，本システムによってポスト・サプライチェーンにおいても偽物の検知が可能となる．2 つ目は，従来手法と異なり，各パーティは商品の入出荷の度に RFID タグの内容を更新する必要がない．RFID タグは一般的に読取・書込エラーがあり，また書込は読取と比較して時間が掛かるため [4], この利点は大

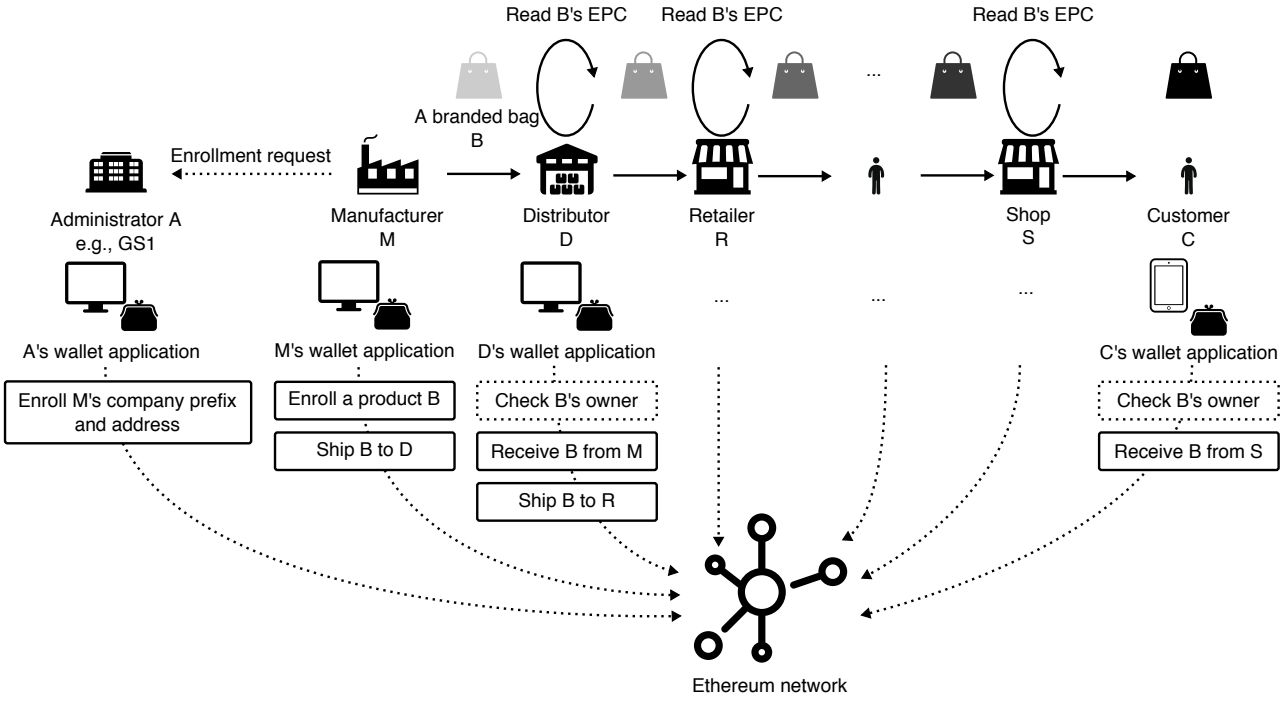

図 4　提案システムの概要.
Fig. 4　A detailed proposed POMS.

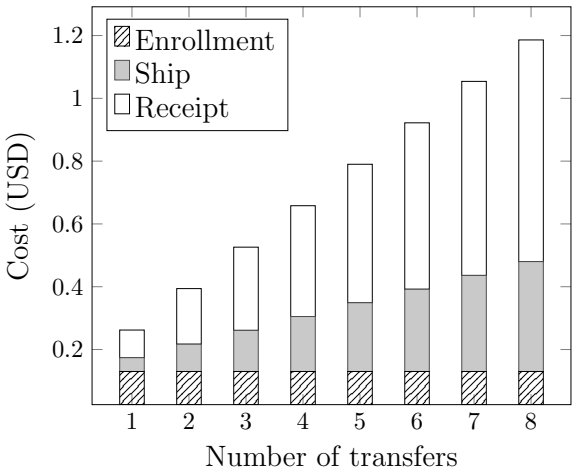

図 5　所有権の移行回数に対する 1 商品の所有権を管理するコスト.
Fig. 5　Operation cost for managing a product's ownership.

きな利点である.

6. 特性評価

提案したシステムを用いて商品の所有権を管理した場合にどの程度のコストが必要であるかを評価する．提案システムを Ethereum 上で実装した場合，商品の最初の所有者の登録 (enrollProduct())，所有権の移行 (shipProduct(), receiveProduct()) 毎にコードのオペレーションに応じて gas が必要となる[*2]．例として，SHA3 を一度計算するために 20gas 必要である．Ethereum のテスト環境ツールの testrpc[*3] を用いてそれぞれに必要な gas 量を算出する．この gas 量を公開されている換算レートを利用し[*4]，実通貨 (米ドル) に換算して評価する．評価の時点における換算レートは 1 gas = 0.000001443 米ドルであった.

図 5 に 1 つの商品の所有権を移行させた回数に対する必要な管理コストを示す．各関数の実行に必要なコストは固定であるため，コストは所有権の移行回数に対して線形に増加することがわかる．6 回程所有権を移行させた場合でも 1 米ドル以下である．このことから高級品の所有権管理においては有効である．一方で日用品に対してはそのコストが占める割合が大きいため不適である．しかしながら，日用品のような商品に対しては偽物を製造する経済的な利点は低いと言えるため，実用的には問題にならないと考えられる.

7. 結論

本論文では，偽物商品流通防止に向けた商品所有権管理システムを提案した．提案システムにおいては，各商品毎に所有権の移行履歴をブロックチェーンを利用して管理することで，ポスト・サプライチェーンにおける偽物検知を可能とする．本システムの特徴として，正規の RFID タグが複製され，偽物に付加されたとしても偽物検知が可能である点である．本システムをブロックチェーンを用いた分散アプリケーションプラットフォームである Ethereum に

[*2] http://ether.fund/tool/gas-fees

[*3] https://github.com/ethereumjs/testrpc

[*4] https://www.coingecko.com/en/price_charts/ethereum/usd

おいて実装し，1 つの商品の所有権の管理コストが 1 米ドル程度であることを示した．

参考文献

[1] Avery, P.: *The economic impact of counterfeiting and piracy*, OECD Publishing (2008).

[2] Staake, T., Thiesse, F. and Fleisch, E.: Extending the EPC network: the potential of RFID in anti-counterfeiting, *ACM Symposium on Applied Computing*, pp. 1607–1612 (2005).

[3] Elkhiyaoui, K., Blass, E.-O. and Molva, R.: CHECKER: On-site checking in RFID-based supply chains, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, pp. 173–184 (2012).

[4] Zanetti, D., Capkun, S. and Juels, A.: Tailing RFID tags for clone detection, *Network and Distributed System Security Symposium (NDSS)* (2013).

[5] Shi, J., Kywe, S. M. and Li, Y.: Batch clone detection in RFID-enabled supply chain, *IEEE International Conference on RFID*, pp. 118–125 (2014).

[6] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008).

[7] Michael, K. and McCathie, L.: The pros and cons of RFID in supply chain management, *IEEE International Conference on Mobile Business (ICMB)*, pp. 623–629 (2005).

[8] Angeles, R.: RFID technologies: supply-chain applications and implementation issues, *Information Systems Management*, Vol. 22, No. 1, pp. 51–65 (2005).

[9] Huang, J., Li, X., Xing, C., Wang, W., Hua, K. and Guo, S.: DTD: A novel double-track approach to clone detection for RFID-enabled supply chains, *IEEE Transactions on Emerging Topics in Computing*, Vol. Preprint, No. 99, p. 1 (2015).

[10] Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X.: The Tangled Web of Password Reuse., *Network and Distributed System Security Symposium (NDSS)*, Vol. 14, pp. 23–26 (2014).

[11] Charlon, F.: OpenAssets/open-assets-protocol: Technical specification for the Open Assets protocol, a Bitcoin based colored coins implementation., `https://github.com/OpenAssets/open-assets-protocol` (2013).

[12] Rosenfeld, M.: Overview of colored coins, *White paper, bitcoil.co.il* (2012).

[13] Christidis, K. and Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things, *IEEE Access*, Vol. Preprint, pp. 1–11 (online), DOI: 10.1109/ACCESS.2016.2566339 (2016).

[14] Wood, G.: Ethereum: A secure decentralised generalised transaction ledger, *Ethereum Project Yellow Paper* (2014).