M-020

スマートコントラクトを用いた位置情報交換インセンティブを有する紛失管理システム
Smart Contract-Based Lost Property Management System with Incentive of Information Exchange

内堀 健人† 梅澤 猛‡ 大澤 範高‡
Kento Uchibori Takeshi Umezawa Noritaka Osawa

1. はじめに

スマートフォンなどの端末を紛失した場合、GPS などにより最後に取得した位置情報を知ることで探す方法がある。通信機能を持たない所持品については、スマートタグと呼ばれる小型の Bluetooth Low Energy(BLE)ビーコンを使った紛失物検索サービスがあり、サービス利用者のスマートフォンがタグの信号を受け取った時の位置情報をサーバに集めることで紛失時に所持品を探す手がかりとすることができる[1][2]。このサービスは、多くのユーザが、他ユーザへタグの位置情報を送信することにかかる通信やバッテリー消費を忌避し、サービスが有効に働かないことがある。また、運営事業体がタグ情報や位置情報を集中管理しているため、単一障害点が生じることや、事業停止によりサービスが使えなくなる危険性がある。そこで、本研究では、代用貨幣であるトークンにより他ユーザのタグの位置情報の提供にインセンティブを与え、スマートコントラクト[4]により、位置情報とトークンの交換を自律分散的に自動実行するシステムを提案する。情報を分散管理することで単一障害点が生じることを防ぐことができる。

2. 提案システム

提案システムは、ユーザ間でのタグの位置情報とトークンの交換をスマートコントラクトによって自律分散的に処理する。ここで、インターネットを介した通信が可能なスマートフォンなどの機器を端末と呼び、所持品などに取り付け BLE などの信号を定期的もしくは適切なタイミングで発信し端末と通信できる機器をスマートタグと呼ぶ。端末が BLE などの信号を周囲に発信する場合には、スマートタグとしての役割を持つと考える。紛失時などに位置情報を取得する対象を単にデバイスと呼び、端末とスマートタグを含む。提案システムの概要を図 1 に示す。

端末は、自身のデバイス ID と位置情報をシステムに登録する。また、端末はスマートタグからの信号を受信した際に、端末の位置情報をスマートタグの位置情報と見なし、スマートタグのデバイス ID と位置情報をシステムに登録する。スマートタグは信号内にデバイス ID を含めて発信し、端末は受信した信号からデバイス ID を知ることができるとする。

2.1 インセンティブデザイン

従来のシステムでは、他ユーザのスマートタグから通信を受信した際に、システムにその情報を登録することはユーザの善意に頼っている。他ユーザのスマートタグをシステムに登録するためには、データ通信や端末のバッテリーを消費する必要があり、他ユーザのスマートタグからの信号受信に伴う登録を頻繁に行うことはユーザにとっては不利益である。このため、他ユーザの情報を処理しないように処理や通信を制限する行動が行われ、それによって、十分なデバイスの情報が収集できないことがある。

この問題を解決するために、提案システムでは、トークンと交換でデバイスの位置情報を取得することができ、デバイスの位置情報を求められた際に適切な位置情報を提供できた場合にトークンを取得できるようにする。これによって、自らのデバイスを紛失した際に位置情報を取得するためにはトークンが必要であり、そのトークンを取得するために他ユーザのスマートタグの位置情報登録を促すインセンティブを生じさせる。

さらに、支払われたトークンからシステムが手数料を得ることができるようにすることで、システムを維持するための費用を賄うことができ、自律分散システムとして機能させることができる。

2.2 スマートコントラクト

提案システムでは、ブロックチェーン上でスマートコントラクトが自律分散的に実行される。また、スマートコントラクトによって独自の代用貨幣であるトークンを作成し、管理することができる。

たとえば、Ethereum[4]ではチューリング完全なスマートコントラクトにより、自律的に機能する非中央集権型のアプリケーションの作成が可能である。また、標準規格に基づいてトークンを作成することで他トークンと互換性を持たせることができる。トークン を用いてユーザの一連の行動に対してインセンティブを設定することで、ユーザに積極的な行動を促すことができる。

2.3 管理される情報

提案システムは、ブロックチェーン上でユーザ情報とデバイス情報、デバイス位置情報を管理する。

ユーザ情報は、少なくともユーザ ID、所有するデバイス情報リスト、トークン残高を含む。それら以外に、ユーザの氏名や連絡先などの情報も必要に応じて管理される。個人情報などは暗号化などによる保護が必要であるが、従来の技術を適用することで可能であり、煩雑になるため本稿では触れない。

† 千葉大学大学院 融合理工学府 数学情報科学専攻
Division of Mathematics and Informatics Graduate School of Science and Informatics, Chiba University
‡ 千葉大学大学院 工学研究院
Graduate School of Engineering, Chiba University

デバイス情報は、少なくともデバイス ID、デバイスが属するユーザ ID、デバイス位置情報リスト、デバイス位置情報通知のために預けたトークンを含み、デバイス位置情報は、少なくとも位置情報、位置情報を提供したユーザ ID、位置情報提供日時の情報を含む。デバイス情報取得の際のトークンの支払いを確実にするためには、ブロックチェーンから支払いなしに位置情報などを取得できないように暗号化などが必要であるが、単純化のために本稿では省略する。

3. ワークフロー

提案システムにおいて、ユーザ A がデバイスを紛失した場合を例に、(1)端末がスマートタグからの信号を受信した際に行われる処理、(2)紛失した際などにデバイスの位置情報を取得する処理、(3)紛失した際などにデバイスの情報更新通知を予約する処理、(4)紛失したデバイスが発見された際に予約されている情報更新通知を行う処理について、図 1 を用いて順を追って説明する。ユーザやユーザに属するデバイスはブロックチェーン上に登録済みとする。

3.1 スマートタグからの信号受信時

端末がスマートタグからの信号を受信した際(図 1- 3.1 項①)には、信号に含まれるデバイス ID と受信端末自身の位置情報をブロックチェーンに登録する(図 1- 3.1 項②)。デバイスがユーザ自身のものであっても、他ユーザのものであっても同様の処理を行う。この処理によって、ブロックチェーン上のデバイス位置情報を最新に更新することができる(図 1 上部の 3.2 項)。

後述の情報更新通知予約がされていない信号受信時には、位置情報は持ち主のユーザには通知されず、見ることもできない。位置情報は 3.4 項に示す通りトークンと交換で取得できる。

情報更新通知予約がされている場合には、報酬のトークンと引き換えに、最新情報をユーザに通知するスマートコントラクトが起動される。

3.2 デバイスの位置情報を取得

ユーザ自身が所有するデバイスの(最新もしくは履歴)位置情報を取得する要求をする(図 1- 3.2 項①)際には、報酬としてのトークンと交換に位置情報を取得するスマートコントラクトを実行する(図 1- 3.2 項②)。

トークンの額に応じて取得する情報を最新から過去のどこまでさかのぼるかを変化させるようなシステム運用ができる。

3.3 情報更新通知予約

ユーザが自身に属するデバイスの将来の情報を得たい場合には、将来の情報更新通知を予めトークンを預けることで予約することができる(図 1- 3.3 項①)。

また、必要な情報を取得でき、将来の通知が不要になった場合などには、情報更新通知を解除し、利用されずに残ったトークンの払い戻しをユーザは受けることができる。

3.4 予約された情報更新通知

情報更新通知予約がされている場合に、3.1 項の信号受信がされた際には、受信した情報が報酬と引き換えに、ユーザに通知される。預けたトークンから報酬分のトークンが差し引かれる。預けたトークンの量が不足している場合には通知されない。トークンの支払いが完了すると情報が開示され、ユーザは最新の位置情報を確認することができる(図 1- 3.4 項①)。その際に選択されたデバイス位置情報(図 1 上部矢印- 3.2 項)は、システムのデバイス情報に最新の位置情報として登録される(図 1 上部矢印- 3.4 項)。

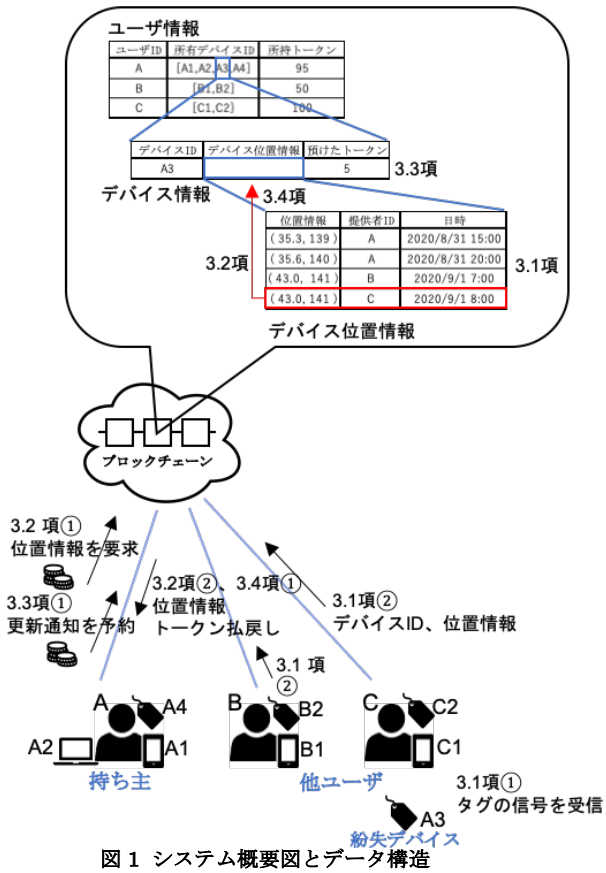

図 1 システム概要図とデータ構造

4. まとめ

インセンティブのために代用貨幣であるトークンを導入し、スマートコントラクトによってトークンとデバイスの位置情報などとの交換をトランザクションとして実行する紛失管理システムを提案し、その基本的な処理のフローを明らかにした。報酬の具体的な設計およびその自動調整法が今後の課題である。Ethereum によってアプリケーションを実装し、パフォーマンスおよび耐障害性を評価、検証する予定である。

参考文献

[1] MAMORIO, https://mamorio.jp/ . Accessed: 20.5.2020.
[2] Tile, https://thetileapp.jp/. Accessed: 20.5.2020.
[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,”2008, http://www.bitcoin.org/bitcoin.pdf. Accessed: 23.5.2020.
[4] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum Project White Paper, 2014, https://github.com/ethereum/wiki/wiki/White-Paper. Accessed: 23.5.2020.