ブロックチェーンシステムにおける匿名トークン付与に関する一考察

佐藤 哲平[1,a)]　江村 恵太[2]　面 和成[1,2]

概要：近年，Bitcoin や Ethereum を始めとした暗号通貨（暗号資産）は，市場の大きな時価総額や，スマートコントラクトの利用など，さまざまな面で注目されている．一方で，その匿名性から犯罪に利用されるケースやその価値上昇とともに サイバー攻撃の標的となるケースも増加している．2018 年に暗号通貨史上最大の被害額を記録した CoinCheck 社における流出事件では NEM 特有のモザイクという機能を利用して有志による流出通貨の追跡が行われ，これによりトークン付与による追跡の一定の効果が実証された．本論文では一定の匿名性を保った状態でトークンの付与，失効が可能で，さらに第三者機関によるトークン付与者の監査が可能なトークン付与手法について考察を行い、アカウンタブルリング署名を利用した手法を提案する．

キーワード：ブロックチェーン, トークン, 匿名性, アカウンタブルリング署名

A Consideration of Giving Anonymous Token on Blockchain System

Teppei Sato[1,a)]　Keita Emura[2]　Kazumasa Omote[1,2]

Abstract: In recent years, cryptocurrencies (crypto-assets) such as Bitcoin and Ethereum have attracted attention in various aspects, such as the large market capitalization and the use of smart contracts. On the other hand, it has been used for crimes due to their anonymity and it become a target of cyber attacks as their value increases. During CoinCheck incident, which recorded the largest amount of damagein cryptocurrency history in 2018, some volunteers had performed tracking leaked NEM using Mosaic, which is NEM-specific feature enables to generate and send self-made token on NEM blockchain. By this case, it is demonstrated that the use of token have a certain effect. In this paper, we propose a method of giving anonymous token on Blockchain system, which has audit function, by accountable ring signature.

Keywords: Blockchain, Token, Anonymity, Accountable Ring Signature

1. はじめに

近年，Bitcoin や Ethereum を始めとした暗号通貨 (暗号資産) は，市場の大きな時価総額や，スマートコントラクトの利用など，さまざまな面で注目されている．一方で，その匿名性から犯罪に利用されるケースやその価値上昇とともに サイバー攻撃の標的となるケースも増加している．

暗号通貨はブロックチェーンを基盤としており，非中央集権的であるため，取引の透明性や障害耐性などの利点がある一方で，アドレス間で人を介さず直接送金が行われることになり，現状では不正送金などの際にそれを第三者が止めることが実質不可能である．そのため流出が起こったあとの対策が必要とされており，その一つの手法としてトークンの付与が知られている．

2018 年に発生した CoinCheck 社における暗号通貨流出事件では当時の価値で約 580 億円の被害があり，暗号通貨史上最大の被害額を記録している．この流出事件では，流

[1] 筑波大学
University of Tsukuba
[2] 情報通信研究機構
National Institute of Information and Communications Technology
[a)] s1820583@s.tsukuba.ac.jp

出した NEM 特有の，モザイクという独自のトークンを作成，送信することができる機能を利用して，有志による流出通貨の追跡が行われた．この事例では「不信頼」を付与するトークンとしてモザイクの付与が行われた．追跡のためのトークンは 2 ヶ月程度で無効化されたが，それまでに取引所を介した大量の流出通貨の換金が明らかになっていないこと等から，この事例によりトークンを用いた流出通貨の追跡の一定の効果が実証されたものと考えられる．ただし，モザイクは NEM 特有の機能であるため他のブロックチェーンでは当然利用できない．またこの手法ではトークン発行者の信頼が担保されていないため正しくトークンが付与されているかわからないことや，トークンの送信者が特定されることによって，トークン付与に対する報復の可能性があるなどの欠点が存在する．

またブロックチェーンでは一般にアドレスに信頼を付与する仕組みが存在していない，そこで鈴木らの研究 [21] ではアドレスに対してトークンを利用して信頼性を与える手法を提案している．ただしこの手法においても，トークンの付与者が特定されることで，トークンを付与させようとする脅迫等が行われる可能性が存在する．単純な解決策として，リング署名 [13] 等を用いることで．トークン付与者を匿名にすることが考えられる．しかしこの場合，例えば信頼性を与えるトークンが一般ユーザにより悪用された場合，付与者の信頼性を担保するためには誰がそのトークンを発行したのかを特定する必要がある．しかしリング署名を単純に用いるとトークン付与者を特定することはできない．グループ署名 [7] を利用することで付与者の追跡が可能となるが，グループ管理者の存在がブロックチェーンの非中央集権性には適さない．

そこで本論文では，トークンの付与側に一定の匿名性をもたせ，トークン付与に対する監査が可能なトークン付与の方式を提案する．概要図を**図 1** に示す．

本論文の貢献は以下の通りである．

- 特定の暗号通貨に限らず，汎用的に利用可能なトークン付与手法を提案した．
- トークンの付与に一定の匿名性を持たせることで，トークン付与側のプライバシーに配慮した付与手法を考案した．
- トークン付与者を追跡することのできる監査機関を設置することで，信頼のあるトークンを実現した．

具体的には，リング署名とグループ署名の一般化であるアカウンタブルリング署名 [6] を用いることで上記の方式を構築した．アカウンタブルリング署名については 3 章を参照されたい．

2. 関連研究

2.1 Bitcoin アドレスに対する信頼性付与に関する研究

鈴木らの研究 [21] では，Bitcoin ネットワークにおいて

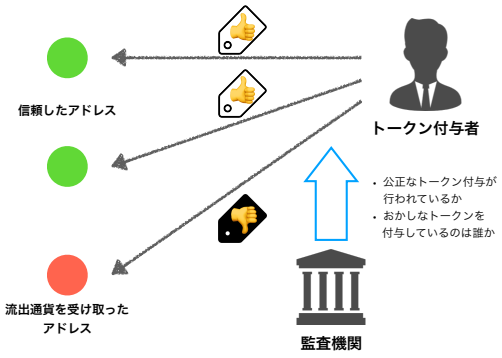

図 1 トークン付与の概要図

トークン付与によるアドレスに対する信頼性の付与を実現する手法の提案を行い，Bitcoin テストネットを利用してその検証実験を行っている．

この手法では，トークンを付与する権限のあるノードが持つ特定のアドレスからの送金を信頼付与のためのトークンとみなしていため，スマートコントラクト等が利用できないブロックチェーンにおいても利用することができるということが最大の利点である．その一方で，送金をトークンとみなすことで，トークンの付与を受けるアドレスが利益を得ることになる．これは信頼の付与の際は大した問題にならないが，不信頼の付与（つまり流出通貨の追跡にトークンを使う場合など）では，トークンの付与先が送金を受けることになるのは可能な限り避けたい問題である．

この手法では，トークンを付与したアドレスが特定される．これはトークンの信頼性にとっては必要なことであるが，一方でトークンの付与を行う者がトークンの付与を目的として脅迫を受けたり，ネガティブなトークンの付与によって恨まれたりするケースが発生することが考えられる．

2.2 トークンを用いた流出暗号通貨の追跡に関する研究

2018 年 1 月に発生した，CoinCheck 社より大量の NEM が流出した事件を受け，有志により，流出先を識別するための目印としてモザイクを用いた追跡がなされた．

佐藤らの研究 [20] では，NEM のブロックチェーンを分析し，流出した NEM を受け取ったウォレットの数・モザイク付与のタイムラグ・モザイクの付与率などを調査し，モザイクによる追跡の効果について評価を行った．

この事件において犯人は正規の取引所を介した流出通貨の利益化をほとんど行っておらず，このモザイク（NEM における独自トークン）による追跡の一定の効果があったことが実証されたものと考えられるが，モザイクは NEM 独自の機能であるため，同じ手法を他のブロックチェーンでそのまま使うことはできない．またこの事例では，有志がトークンの付与を行ったため，トークンの信頼性は直接は担保されていない．この事例の場合は流出の経路を流出

元までたどることでトークンが正当なものか確認することはできたが，それではトークンの意味がない．

暗号通貨の流出を完全に防ぐことは不可能であるため，トークン自体の信頼性が担保されたトークン付与の手法が必要である．また，複数の暗号通貨において利用できる事が望ましい．

2.3 匿名性を特徴とした暗号通貨（プロトコル）

ブロックチェーンでは，公開鍵に紐ついた「アドレス」と呼ばれる仮名を用いて，暗号通貨をやりとりしたり，ブロックチェーンの機能を利用することになるため，匿名性ではなく「仮名性」を持つと言われる．匿名機能をもたない一般的なブロックチェーンでは，記録されたそれぞれの取引履歴を紐付けることで，あるアドレスの取引の特徴や，複数のアドレス間での取引を追跡することなどが可能である．[14] これは取引の透明性などの観点から言えば利点とも言えるが，一方でプライバシーが守られないという欠点でもある．

そこでプライバシーに重点を置いた CryptoNote [17] というプロトコルが存在している．この手法では，リング署名とワンタイム鍵ペアを利用することで，送金の Untraceability（どのアドレスから送金が来たかわからない）と Unlinkability（任意の 2 つの Output が同じ先に送金されていることを証明できない）という 2 つの特徴をもって匿名性を実現している．

CryptoNote を利用する匿名性を特徴とした暗号通貨としては Monero[*1]が有名であるが，Monero では CryotoNote の他に RingCT という仕組みを用いることで送金の金額も秘匿した状態で送金が可能になっている．

3. アカウンタブルリング署名

本章では, リング署名 [13] とその改良であるアカウンタブルリング署名 [19] を紹介する．リング署名 [13] は Rivest, Shamir, Tauman によって提案された匿名性を持った署名方式である．各ユーザは自身で公開鍵と秘密鍵をセットアップ, 署名者は (自身の公開鍵を含む) 公開鍵の集合 (リング) を定義し, 自身の秘密鍵で署名を作成する．検証者は, 署名者がリングで定義されるユーザの集合に含まれることのみ検証できる．同じ署名者が複数回署名を生成しても署名者が同じか否かを判定できないという強い匿名性 (Unlinkability) を有し, また通常の署名同様に偽造不可能性が定義される．安全性の詳細は [5] を参照されたい．近年, 署名長がリングに含まれる公開鍵数の log サイズである効率的な方式が提案されている [3], [11]．類似技術であるグループ署名 [7] との大きな違いとして, グループ管理者の存在が挙げられる．グループ署名では, グループ管理者がグループ公開鍵と秘密鍵を生成, その秘密鍵を用いてユーザに署名鍵を発行する．署名検証時にはグループ公開鍵のみで検証することでユーザを特定することなく匿名で検証することができ, リング署名と同様に強い匿名性を有する．また有事の際にはグループ秘密鍵を用いて署名者を追跡することができる．

ブロックチェーンでは，トランザクションに対してアドレスに紐付いた秘密鍵を用いて署名を行う．アプリケーションによってはこの署名に匿名性が要求される．ブロックチェーンにおいては非中央集権性が求められるため, 自身で鍵をセットアップできるリング署名が, 特に暗号通貨分野で使用されている．ただし二重支払い防止のため, 匿名性を弱めたリンカブルリング署名 [12] が使用されている．リンカブルリング署名では, 同じリングに対して署名した場合に, その署名者が同じか否かが公開で検証可能である．ここで署名者の特定までは行うことができないことに注意されたい.[*2] 効率的な構成 [2] や, 一般的構成 [18] などが提案されている．なお CryptoNote [17] ではワンタイムリンカブルリング署名が使用されている．このワンタイムとは通常の署名とワンタイム署名との違いと同様, 各ユーザに対し, 1 度だけ攻撃者が署名オラクルに質問することが許される．安全性の詳細は [16] を参照されたい．

リング署名とグループ署名の一般化として, アカウンタブルリング署名が Xu と Yung により提案されている [19]．通常のリング署名と同様に, 各ユーザは自身で鍵をセットアップする．また追跡者と呼ばれるユーザも自身で鍵をセットアップする．署名者はリング署名を作成する際に指定した追跡者の公開鍵も入力として使用する．検証時にはリングに含まれる公開鍵の集合に加え, 追跡者の公開鍵を用いる．グループ署名と同様に, 追跡者は自身の秘密鍵を用いることで署名者を特定することができる．さらに追跡者の署名者特定が正当に行われたことを証明する機構 [4] を有し, さらにその証明を悪用した署名の乗っ取りの防止 [15] も考慮されている．具体的な方式として, 署名長がリングに含まれる公開鍵数の log サイズかつ標準的な DDH 仮定で安全な方式 [6], 墨塗り署名との関係性を示し, 署名長がリングサイズに依存せずコンスタント (ただし合成数位数) である方式 [10], 識別不能難読化を用いた方式 [9] が提案されている．

以下, Bootle ら [6] によるアカウンタブルリング署名のシンタックスを紹介する．安全性の定義は [6] を参照されたい．なお論文 [6] の匿名性の定義では, 追跡者は 1 名のみ定義され, その秘密鍵を攻撃者に与えない状況での匿名性が定義されている．しかし追跡者を指定可能という性質より, 複数の追跡者を仮定することが自然である．その際, 匿名性の定義を他の追跡者が指定された署名に対するものに

[*1] Monero: https://www.getmonero.org/

[*2] 追加の条件が揃うと署名者を特定可能なトレーサブルリング署名も提案されている [8].

修正する必要がある．この修正は容易であることから，以降本論文では複数の追跡者の存在を想定する．

Setup(1^λ) ：セットアップアルゴリズムはセキュリティパラメータ $\lambda \in \mathbb{N}$ を入力とし，共通パラメータ pp を出力する．

OKGen(pp) ：追跡者鍵生成アルゴリズムは pp を入力とし，追跡者の公開鍵 opk と秘密鍵 osk を出力する．

UKGen(pp) ：ユーザ鍵生成アルゴリズムは pp を入力とし，ユーザの公開鍵 pk と秘密鍵 sk を出力する．

Sign(opk, M, R, sk) ：署名生成アルゴリズムは opk，署名するメッセージ M，リング R，秘密鍵 sk を入力とし，リング署名 σ を出力する．なお sk に対応する pk が R に含まれると仮定する．

Verify(opk, M, R, σ) ：署名検証アルゴリズムは opk，M，R，σ を入力とし，1（署名が正当であることを示す）または 0 (署名が不当であることを示す) を出力する．

Open(M, R, σ, osk) ：追跡アルゴリズムは M，R，σ，osk を入力とし，署名作成者の pk および証明 π，または $\perp$ を出力する．

Judge($opk, M, R, \sigma, pk, \pi$) ：追跡証明検証アルゴリズムは opk，M，R，σ，pk，π を入力とし，1 (σ は pk に対応した sk で作成されたことを示す) または 0 を出力する．なお署名が不当，または $pk \notin R$ の場合，0 を出力するとする．

4. 匿名トークン付与の必要性・要件

4.1 トークンの利用

近年暗号通貨の価値上昇や，急速に増加した仮想通貨交換業者のセキュリティ対策不備等により，暗号通貨の流出事件が多発している．2014 年には Mt.Gox 社，2018 年の CoinCheck，Zaif などから当時の価値で数十億円以上の暗号通貨が流出しており，もちろん流出を未然に防ぐことは重要だが，流出が起こった際の対策について考えることも等しく重要であると言える．

2018 年の CoinCheck における流出事件では，NEM 特有のモザイクという独自のトークンを作成，送信することができる機能を利用して有志による流出通貨の追跡が行われた．この手法は CoinCheck のアドレスから流出した通貨を受け取ったアドレスに対して流出通貨であることを示すモザイクを送信することにより，目印をつけ，NEM を取り扱う取引所に対して他の暗号通貨や法定通貨との交換をしないよう警告するものであった．我々はこの事例によってトークンを利用した流出通貨の追跡手法の一定の効果が実証されたものと考える．この手法は 2018 年 3 月 20 日の NEM.io 財団の発表 [1] によりその無効化が開始されたことが明らかとなったが，その無効化までに正規の取引所を介した大量の通貨の換金があったことは明らかになっていないこと，犯人は最終的に正規の取引所ではなくダークウェブ上に独自の取引所を開設して流出通貨を交換する方法を取ったことなどから，流出通貨の直接正規の取引所を介した利益化を防ぐ手法としてこのトークン付与による追跡は一定の効果があったものと考える．

CoinCheck の例では「流出通貨を受け取ったアドレス」という不信頼の評価をアドレスに対して付与することで流出による被害を最小限に抑えようとした．一方で，鈴木らの研究 [21] のようにアドレスに対して信頼性を与え，ブロックチェーンの送金ネットワークの信頼性を向上させることにもトークン付与は利用が可能である．

4.2 トークンの実現方法

トークンの実現方法として考えられるものを挙げる．

- 独自トークンを発行できるもの
- スマートコントラクトによる実装
- 特定の条件を満たすトランザクションをトークンとみなすもの

4.2.1 独自トークンを発行できるもの

NEM や Counterparty などでは，標準でユーザが独自のトークンを作成・送信することができる機能をもっている．

4.2.2 スマートコントラクトによる実装

Ethereum ではスマートコントラクトを利用して実装することで，独自のトークンを作成することができる．またスマートコントラクトの実装次第で独自トークンにさまざまな機能を付加することが可能となっている．

4.2.3 特定の条件を満たすトランザクションをトークンとみなすもの

先の 2 つの手法では，ブロックチェーンが持つ特徴によりユーザがトークンを作成することが可能になっているが，それらと比較して低機能であったり他の特徴に重点を置いているブロックチェーンにおいても「広義のトークン」は実現可能である．その方法がこの「特定の条件を満たすトランザクションをトークンとみなすもの」である．ここで言う特定の条件は例えば以下のようなものやそれらを組み合わせたものが考えられる．

- 特定のアドレスから送信されている
- 特定の額の送金である
- 特定の鍵ペアによる署名が付与されている

この手法は他の 2 つと比較して，ブロックチェーンに内蔵された機能ではなく，トークンとするには利用者の合意が必要である．その一方で，この手法は多くのブロックチェーンに適用可能であるという利点がある．

4.3 現行の手法の問題点

現状でトークン付与をアドレスに対する信頼の付与や，特定の目的で目印をつける利用は手法が確立されておらず，有名な例が CoinCheck の際のもののみであるため，これを現行の手法として問題点を挙げる．

4.3.1 トークンの信頼性

CoinCheck の際の追跡におけるトークンの付与は有志によって行われたが，ここには付与されたトークンの信頼性の問題がある．有志により付与されたトークンはネットワーク参加者の合意がなく，またその付与が適切に行われているかどうか，どのような条件で付与が行われているのかが明確でない．付与されたトークンを信用しそれを元にした対策を行うかどうかは各取引所，ユーザ次第であるため，トークンやその付与自体の信頼性が担保され，その確認が容易であることが必要である．

4.3.2 トークン付与側のプライバシー

一方で信頼や不信頼の付与を行うトークン付与を行う際に，付与・失効した人が特定される場合，それらの操作を行う者のプライバシーが保たれないことによって公平なトークン付与の妨げになるという問題がある．これはつまり信頼の付与・失効，不信頼の付与・失効の際に，それを行うことで利益を得る，または不利益を被る組織などから脅迫を受けたり危害を加えられるようなことが起こる可能性があり，これにより公正で安全な運用が妨げられる場合が考えられるということである．ただし，単純にトークン付与に匿名性を持たせる場合，トークン付与者の不正・不当な付与に弱くなる．

4.4 匿名トークン付与の要件

以上のことから我々が実現を目指す匿名トークン付与の要件を以下に示す．

トークン付与の匿名性　トークンを付与した者が特定されない．ただし，一般アドレス（トークン付与を受けるアドレス）に関しては今回は考えない．

トークン付与の監査が可能　トークンの送信機関とは別にそれを監査する機関を設け，例えば信頼のトークンを付与されたアドレスによる不正や不信頼のトークンが不正に失効された場合など，トークン付与者の信頼に影響する事態が起こった際に，その監査機関がトークン付与者を追跡することが可能である．

5. 提案手法

本章では提案手法を示す．ただしこれ以降，「アドレス」はトークン付与を行う暗号通貨におけるアドレスを，「リング署名」はアカウンタブルリング署名 [6] を意味する．

5.1 提案手法の概要

提案する手法では，匿名かつ監査可能であることを実現するために，署名時に指定した追跡者のみが署名の署名者を追跡することができるアカウンタブルリング署名 [6] を使用する．また，この理由は 6.1.2 項で述べるが，トランザクションを送信する権限とトークンを付与する権限を分離するため，署名を生成するトークン付与者に対して，生成された署名をトランザクションに乗せてブロックチェーンネットワークに送信するトークン送信機関を設置することとしている．

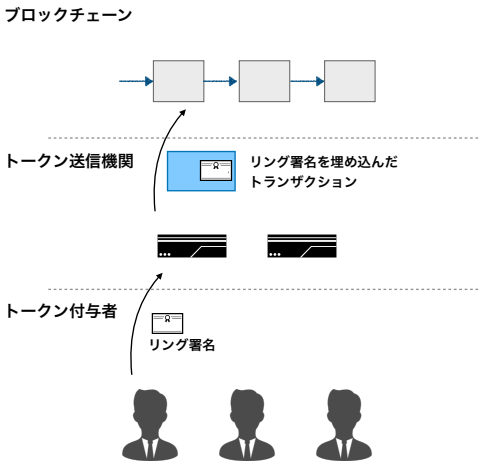

図 2　トークン付与の流れ

トークン付与者はトークンの内容 (信頼/不信頼の度合い，有効期限等) をメッセージとしたリング署名を作成しトークン送信機関に送信する．トークン付与機関が署名を確認し，送信機関のアドレスから付与対象のアドレスに対するトランザクションに署名を埋め込んで送信することでトークンの付与が完了する．

ある一般アドレスの信頼性を確認したい一般ユーザや取引所は，当該一般アドレスあてのトークン送信機関からのトランザクションを見つけて署名を検証することで，アドレスの信頼性を確認することになる．

この手法におけるトークンは，4.2 節における「特定の条件を満たすトランザクションをトークンとみなす」方式で実現しており，以下の条件を満たすことをトークンの条件とする．

- トークン送信機関のものとして公開されたアドレスから送信されている．
- トークン付与者のもとのして公開された検証鍵のみによって構成されたリングによる正当な署名が付与されている．
- 特定の監査機関がリング署名の追跡者に指定されている．

またトークン付与の流れを図 **2** に示す．

5.2 提案手法の登場人物

本節では，この手法の登場人物（一般ユーザ，トークン付与者，トークン送信機関，検証者，監査機関）について説明する．

一般ユーザ　トークンを付与される側の通常のユーザ．アドレス（一般アドレス）を持つ．

トークン付与者　トークンの付与先を決定して，トークン

（リング署名）を作成する，トークン付与の主体．リング署名の署名鍵を持つ．

トークン送信機関　トークンをトークン付与者から受け取り，トランザクションに埋め込んで送信する．トークン付与者の匿名性のために，トークン付与者からブロックチェーンにリング署名を中継する役割．トークン付与用のアドレス（トークン付与アドレス）を持つ．

検証者　一般アドレスに付与されたトークンを検証する．現実であればさまざまな機関や人がこの「検証者」になりうる．例えば，とある一般アドレスに対して送金を行う際にその信頼性を確認したい他の一般ユーザ，自分あての送金を行った一般アドレスに「盗難された通貨であることを示すトークン」が付与されていないかを確認したい仮想通貨取引所などである．

監査機関　トークン付与の公正でない場合などにリング署名の署名者を追跡し，監査を行う機関．リング署名の追跡者のための鍵を持つ．

5.3　提案手法の流れ

本節では，提案手法を「準備，トークン付与，トークン検証，監査」の 4 段階に分けて説明する．

5.3.1　準備

- トークン付与者: それぞれ，リング署名の鍵ペアを生成し，検証鍵を公開する．
- トークン送信機関: トークン付与アドレスを生成し，アドレスを公開する．
- 監査機関: リング署名の追跡者用の鍵を生成し，公開鍵を公開する．

5.3.2　トークン付与/失効

(1) トークン付与者: 特定のフォーマットに従ったメッセージに対してリング署名を生成, トークン送信機関に署名を送信する．

(2) トークン送信機関: 受け取った署名を検証し正当なものであれば，トークン付与対象の一般アドレスに対するトランザクションに署名を埋め込み，トランザクションを送信する．

ただし，リング署名のメッセージの内容はトークン付与の場合とトークン失効の場合で，それぞれ以下の様な項目を持つ．

- トークン付与
  - 付与を示すフラグ
  - 信用レベル (信頼なのか不信頼なのか，どの程度の信頼/不信頼なのか)
  - 有効期限
  - 流出した通貨を受け取っていることを示すメッセージ
- トークン失効
  - 失効を示すフラグ
  - 失効したいトークンが付与されたトランザクションのハッシュ

また，トークン送信機関が行う検証の項目は以下のとおりである．

- 署名自体の検証
- リングに含まれる検証鍵が，すべてトークン付与者のものか
- 正しい監査機関の公開鍵が指定されているか
- 有効期限内のトークンであるか

5.3.3　トークン検証

(1) 検証者: トークンを確認したい一般アドレスに対するトランザクションをトークンの有効期限に当たるブロックまでさかのぼって確認する．

(2) 検証者: トークン付与アドレスからのトランザクションが存在しており，当該トークンの失効を示すトランザクションが付与以降に存在していなければ，そこに埋め込まれたリング署名を取得する．

(3) 検証者: リング署名を検証し正当なものであれば，メッセージを取り出し，トークンがアドレスに付与した情報を確認する．

ただし，検証者が行う検証の項目は，トークン送信機関が行うものと同一のものとする．

5.3.4　監査

匿名トークン付与の監査では，リング署名の作成時に指定された監査機関のみがそれを行うことができる．リング署名の機能によりリング署名の署名者が誰かを暴露することで，監査機関はトークン付与者によってトークン付与が公正に行われているかどうかを確認する．

5.4　提案手法の実現可能性

5.4.1　本手法を適用可能なブロックチェーンの条件

本手法を適用可能なブロックチェーンの条件は，「リング署名サイズのデータをトランザクションに埋め込むことができる」ということである．

群要素のサイズを $\mathbb{G}$，群の位数を q，リングサイズを N とした場合，今回利用したアカウンタブルリング署名の署名サイズは以下の式で与えられる [6].

$$(\log_2 N + 12)\mathbb{G} + \frac{1}{3}(3\log_2 N + 12)\mathbb{Z}_q^*$$

例えば，$N = 11$，使用する楕円曲線を Curve25519 と仮定した場合の署名サイズはおよそ 1.4kB であり，ブロックチェーンに十分格納可能なサイズである．

5.4.2　トークン送信機関がトークン付与を拒否できる問題

本手法では，トークン付与の権限とトランザクションを送信する権限を分離し，それぞれトークン付与者とトークン送信機関にもたせている．トークンはトークン付与者が作成したリング署名をトークン送信機関がトランザクションに埋め込みブロックチェーンに記録することで初めてその効果が発生するが，トークン付与者はトークン送信機関

にトランザクションの送信を強制する事はできず，トークン送信機関はトークンの付与を拒否することが可能である．トークンの拒否は，例えばトークン送信機関とトークン付与対象の一般アドレスが利害関係にある場合などに起こりうる．

ただし，図 2 に示したとおり，トークン送信機関は複数存在し，どのトークン送信機関からトランザクションが発行されたかどうかは意味を持たないため，トークン付与者はトークンの付与が一定時間確認できなければ他のトークン送信機関に依頼することで拒否を回避してトークンを付与することが可能である．

5.4.3 トークン付与のためのアドレスについて

鈴木らの提案するトークン付与手法 [21] では，トークンの付与を行う「特権ノード」がトークン付与のための「付与用アドレス」とトークン失効のための「失効用アドレス」の 2 種類のアドレスを管理する必要がある．

提案手法では，トランザクションに埋め込むリング署名のメッセージに「トークン付与/失効を示すフラグ」が入ることで，トークン送信機関はトークン付与アドレス 1 種類のみを管理することになる．

6. 考察

6.1 今回の手法にたどり着くまでの試行錯誤

6.1.1 単純に CryptoNote の署名方式をアカウンタブルリング署名に入れ替える

まず我々は第三者による監査が可能な匿名トークンを実現するために，匿名性が強い暗号通貨である Monero 等で利用される CryptoNote プロトコルで利用されるリング署名の方式を，署名時に指定した追跡者が署名の署名者を追跡することのできるリング署名であるアカウンタブルリング署名に入れ替えることを考えた．CryptoNote でも監査の機能は存在しているが，それはブロックチェーンの外で秘密鍵の一部を渡すというものが必要であり，監査を誰がするかという部分までは検証不可能である．一方でアカウンタブルリング署名では，署名作成時に追跡者の公開鍵を指定し，検証時にその公開鍵が使用されるため，この署名をブロックチェーンに記録することで追跡者の情報も同時に記録されることになり，正しい監査機関を指定しているかという部分も誰もが確認できるため，トークンとしての有効性が高いと考えた．

しかし，そもそもすでに匿名性を持つブロックチェーン上では，一般アドレスも匿名になってしまい，トークンの所持を証明する機構が別途必要になる．また不信頼のトークンにおいては，その所持を証明するモチベーションがないため，トークン付与の効果がなくなってしまう．そこで匿名性を持たないブロックチェーン上で匿名トークンを実現する手法を考案する方針とした．

6.1.2 代表アドレスの秘密鍵をトークン付与者が共有する

匿名性を持たないブロックチェーン上で匿名トークンを実現するために重要なことは，トークン付与者らがそれぞれでトランザクションを送信するためのアドレスを持つと，アドレスとトークン付与者が 1 対 1 で紐付いてしまうため，匿名が実現できないということである．それを解決するため，トークン付与者が 1 つのアドレス (代表アドレス) の秘密鍵を共有し，共有しているトークン付与者全員がその代表アドレスからトークン付与のためのトランザクションを送信するというナイーブな手法が考えられる．

この手法では，トークン検証の際の「トークンを確認したい一般アドレスに対するトランザクションを確認する.」という手順において，確認すべきトークン付与アドレスが少なくなるという利点がある．その一方で，秘密鍵を共有するため，代表アドレスにトランザクションの手数料などのために保有されている通貨を秘密鍵を共有する誰でも不正に引き出すことが可能であるという脆弱性が存在している．

我々はこの欠点が致命的であると考えたため，トークンを付与する (リング署名を生成する) 権限とトランザクションを送信する権限を分離した今回の提案手法にたどり着いた．

6.2 提案手法によるブロックチェーンへの影響

ブロックチェーンを利用した暗号通貨の一つの特徴が非中央集権である．提案手法では，トークン付与者が参加者の合意によらない独自の指標で特定のアドレスを評価している．

しかしながら，提案手法におけるトークン付与者は，ブロックチェーンによって公式に用意・設定されるものではなく，SSL/TLS 証明書と同様に，あくまでサードパーティによるサービスとして提供されるものという想定である．つまりそれぞれのトークンを信用するかどうかはユーザ次第であり，それぞれのユーザが複数ある付与者のトークン付与の基準や条件などに応じて付与されているトークンを信頼するかどうか決めることになる．

またこの手法は，トークン付与者の作成したリング署名を，トークン送信機関のアドレスからブロックチェーンに送信することで匿名性を実現している．そのため署名方式等，利用するブロックチェーン自体に手を加える必要がなく，トークンを利用しない一般ユーザにとっては無視できる，影響を与えない手法である．

よって，本手法はブロックチェーンに大きな影響は与えない．

7. まとめ

本研究では暗号通貨のアドレスに対して，信頼や不信頼を付与するためのトークンについて考察を行い，手法を提

案した．

提案した手法では，トークンの付与側に一定の匿名性をもたせ，トークン付与に対する監査が可能なトークン付与の方式を，アカウンタブルリング署名を用いて実現した．トークン付与者のプライバシーが守られることで公正なトークン付与を可能にし，トークン付与が不正に行われた場合の署名者の追跡も可能としている．

一方でこの手法では，トークンの有効期限が短いとトークン付与の回数が増えることによる手数料コストが増大し，トークンの有効期限が長いと検証者が遡るブロック数が大きくなり検証のコストが増大する．そこで妥当なトークンの有効期限の見積もりが今後の課題である．

謝辞　本研究成果の一部は，JSPS 科研費 19H04107 の助成を受けたものである．

参考文献

[1] : Coincheck Hack Update: Removal of Mosaic Tagging System, https://medium.com/nemofficial/coincheck-hack-update-removal-of-mosaic-tagging-system-18b4157ff060. Accessed : 2018-04-11.

[2] Au, M. H., Chow, S. S., Susilo, W. and Tsang, P. P.: Short linkable ring signatures revisited, *European Public Key Infrastructure Workshop*, Springer, pp. 101–115 (2006).

[3] Backes, M., Döttling, N., Hanzlik, L., Kluczniak, K. and Schneider, J.: Ring Signatures: Logarithmic-Size, No Setup - from Standard Assumptions, *EUROCRYPT*, pp. 281–311 (2019).

[4] Bellare, M., Shi, H. and Zhang, C.: Foundations of Group Signatures: The Case of Dynamic Groups, *CT-RSA*, pp. 136–153 (2005).

[5] Bender, A., Katz, J. and Morselli, R.: Ring Signatures: Stronger Definitions, and Constructions without Random Oracles, *J. Cryptology*, Vol. 22, No. 1, pp. 114–138 (2009).

[6] Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J. and Petit, C.: Short accountable ring signatures based on DDH, *European Symposium on Research in Computer Security*, Springer, pp. 243–265 (2015).

[7] Chaum, D. and van Heyst, E.: Group Signatures, *EUROCRYPT*, pp. 257–265 (1991).

[8] Fujisaki, E. and Suzuki, K.: Traceable ring signature, *IEICE transactions on fundamentals of electronics, communications and computer sciences*, Vol. 91, No. 1, pp. 83–93 (2008).

[9] Kumawat, S. and Paul, S.: A New Constant-Size Accountable Ring Signature Scheme Without Random Oracles, *Inscrypt*, pp. 157–179 (2017).

[10] Lai, R. W. F., Zhang, T., Chow, S. S. M. and Schröder, D.: Efficient Sanitizable Signatures Without Random Oracles, *ESORICS*, pp. 363–380 (2016).

[11] Libert, B., Peters, T. and Qian, C.: Logarithmic-Size Ring Signatures with Tight Security from the DDH Assumption, *ESORICS*, pp. 288–308 (2018).

[12] Liu, J. K., Wei, V. K. and Wong, D. S.: Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract), *ACISP*, pp. 325–335 (2004).

[13] Rivest, R. L., Shamir, A. and Tauman, Y.: How to leak a secret, *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 552–565 (2001).

[14] Ron, D. and Shamir, A.: Quantitative analysis of the full bitcoin transaction graph, *International Conference on Financial Cryptography and Data Security*, Springer, pp. 6–24 (2013).

[15] Sakai, Y., Schuldt, J. C. N., Emura, K., Hanaoka, G. and Ohta, K.: On the Security of Dynamic Group Signatures: Preventing Signature Hijacking, *Public Key Cryptography*, pp. 715–732 (2012).

[16] Torres, W. A. A., Steinfeld, R., Sakzad, A., Liu, J. K., Kuchta, V., Bhattacharjee, N., Au, M. H. and Cheng, J.: Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0), *ACISP*, pp. 558–576 (2018).

[17] Van Saberhagen, N.: CryptoNote v 2.0 (2013).

[18] Wang, X., Chen, Y. and Ma, X.: Generic Construction of Linkable Ring Signature, *ISC* (2019, to appear). Available at `https://eprint.iacr.org/2019/371`.

[19] Xu, S. and Yung, M.: Accountable Ring Signatures: A Smart Card Approach, *CARDIS*, pp. 271–286 (2004).

[20] 佐藤哲平，今村光良，　面和成：コインチェック事件における流出 NEM の追跡に関する実態調査 (情報セキュリティ)，電子情報通信学会技術研究報告= IEICE technical report: 信学技報，Vol. 118, No. 30, pp. 35–41 (2018).

[21] 鈴木明日香，佐藤哲平，　面和成：ビットコインにおけるユーザへの信頼性付与の手法，電子情報通信学会技術研究報告, vol. 119, no. 143，pp. 29–34 (2019).