SCIS 2021 2021 Symposium on
Cryptography and Information Security
On-line, Jan. 19 – 22, 2021
The Institute of Electronics,
Information and Communication Engineers

暗号資産の封印・償還における利用者の匿名性および特定・追跡性の考察

Consideration on User Anonymity and Identifiability/Traceability in CryptoAssets Sealing/Redemption

才所 敏明[*1] 辻井 重男[*2] 櫻井 幸一[*3]
Toshiaki Saisho Shigeo Tsujii Sakurai Kouichi

あらまし 暗号資産を台帳に登録する情報の内容により，資産移転記録方式と資産残高記録方式の 2 種に分類し，資産移転記録方式の主要な暗号資産 Bitcoin，Monero，Zcash を対象に，台帳に登録・公開される封印情報・償還情報に関する利用者の匿名性および特定・追跡性の現状を考察した．

利用者の匿名性に関しては，ゼロ知識証明を利用している Zcash が台帳に登録する情報の中に利用者識別情報を露出させることなく封印・償還を実現しており，匿名性が高い．

利用者の特定・追跡性に関しては，Monero では tracking key/鍵イメージ，Zcash では Incoming Viewing Key を利用者が提供することにより，台帳上の暗号資産/利用者識別情報と利用者の対応を特定可能であるが，未だ基本的な機能のみが実装されている状況で，利用者の特定・追跡性に関する具体的ニーズの明確化と共に，対応する技術・システム等の研究・開発が望まれる．

キーワード 暗号資産，資産移転，封印，償還，Bitcoin，Monero，Zcash，匿名性，特定・追跡性

Abstract Depending on the content of information to register CryptoAssets on the ledger, we classified CryptoAssets Management System(CAMS) into two types, Transaction based CAMS and Balance based CAMS. Then, we investigated the current status of user anonymity and identifiability/traceability on sealing/redemption information of Bitcoin, Monero, Zcash, which are major Transaction based CAMS. Regarding the anonymity of users, Zcash, which uses zero-knowledge proof, achieves sealing and redemption without exposing the user identification information in the information registered on the ledger, and is highly anonymous. Regarding user identifiability/traceability, by providing the tracking key/key image in Monero and the Incoming Viewing Key in Zcash, the received third party can identify the correspondence between the CryptoAssets/user identification information on the ledger and the user. However, only basic functions are implemented currently, it is desired to understand identifiability/traceability needs and to research and develop corresponding technologies and systems.

Keywords CryptoAssets，Sealing，Redemtion，Bitcoin，Monero，Zcash，Anonymity，Identifiability/Traceability

1 はじめに

Satoshi Nakamoto が 2008 年に投稿した論文（[5]）で公開し，2009 年に運用が開始された最初の暗号資産である Bitcoin 以来，多くの暗号資産が登場し，消滅した暗号資産もあるが，“All Cryptocurrencies”（[20]）のデータによると 2020 年 11 月 15 日現在，7671 個の暗号資産が公開され，活発な取引が行われており，暗号資産全体の時価総額は約 48 兆円となっている．その中でも暗号資産の元祖であるビットコインが現在も時価総額は 1

[*1] IT 企画 http://advanced-it.co.jp/
mail: toshiaki.saisho@advanced-it.co.jp
[*2] 中央大学研究開発機構 mail: tsujii@tamacc.chuo-u.ac.jp
[*3] 九州大学 大学院システム情報科学研究院
& サイバーセキュリティーセンター
(株) 国際電気通信基盤技術研究所
mail: sakurai@INF.kyushu-u.ac.jp

位であり，シェアも 65%前後を占めている．

多くの暗号資産は一定レベルの匿名性が確保されているが，プライバシーや個人情報の保護の観点からは不十分であり，匿名性が強化された暗号資産も提案されている．一方，暗号資産の匿名性の悪用も多発しており，安心・安全な社会，公平・公正な社会の実現には，利用者の特定・追跡性の保証もまた必要である．

なお，本稿で対象とする利用者の匿名性とは，暗号資産台帳に登録される資産移転情報から利用者の身元情報（実名，住所等）の把握が難しい性質を意味し，利用者の特定・追跡性とは，暗号資産台帳に登録される資産移転情報から利用者の実名の特定および利用者へのアクセスが容易な性質を意味している（図 1）．

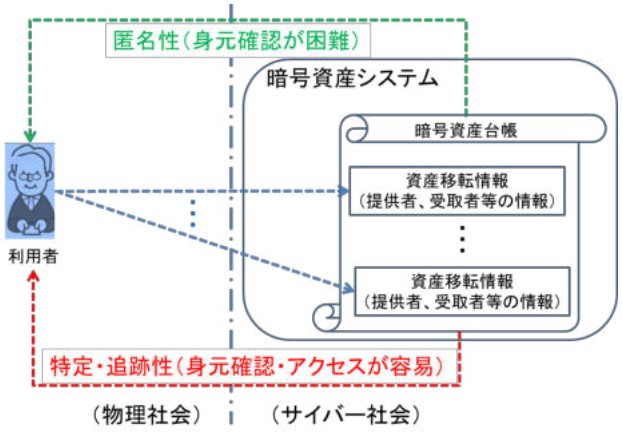

図 1　利用者の匿名性および特定・追跡性

本稿は，主要な暗号資産を対象に，資産封印・償還方式およびその結果として暗号資産台帳に登録される資産移転情報内の資産封印・償還情報を調査し，このような資産封印・償還情報からの利用者の匿名性へのリスク，利用者の特定・追跡の可能性の現状調査・分析を目的とする．

まず 2 章にて，台帳に登録され公開される情報の内容に基づく暗号資産の分類（資産移転情報の記録方式および資産残高情報の記録方式）を定義し，3 章にて，資産移転情報の記録方式を採用している主要な三つの暗号資産 Bitcoin（[6]），Monero（[8]~[10]），Zcash（[11]）のそれぞれについて，具体的な資産封印・償還方式，暗号資産台帳に登録される資産封印・償還情報および匿名性と特定・追跡性の現状・課題を報告する．その上で，資産移転記録方式を採用する三つの暗号資産において，台帳に登録される資産封印・償還情報からの匿名性および特定・追跡性に関し，比較・考察する．

2　台帳登録情報による暗号資産の分類

暗号資産のやり取りを担う暗号資産システムでは，暗号資産の移転を示す情報，提供者が示す①提供者の暗号資産提供能力の指定（提供者の情報）および②提供先および提供する暗号資産額の指定（受取者の情報）の妥当性を検証し，適切な移転であることが確認された場合は，提供者の暗号資産提供能力は減じられ，受取者の暗号資産提供能力は増加される．

利用者の暗号資産提供能力の管理方式として，大きく 2 種に分類できる．一つは，暗号資産の移転時に受取者が受け取る暗号資産をそのまま記録・管理し，提供の際にその暗号資産を指定する方式である．Bitcoin をはじめとする多くの暗号資産が採用している方式であり，本稿では資産移転記録方式（TCAMS：Transaction based CryptoAsset Management System）と称している（図 2）．もう一つは，資産移転の結果として更新される利用者の暗号資産残高（資産保有額）を記録・管理する方式である．Nano（[15]）や Hedera Hashgraph（[16]）等が採用している方式であり，資産残高記録方式（BCAMS：Balance based CryptoAsset Management System）と称している（図 3）．

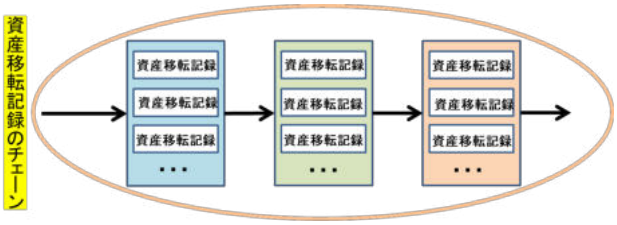

図 2　資産移転記録方式（TCAMS）

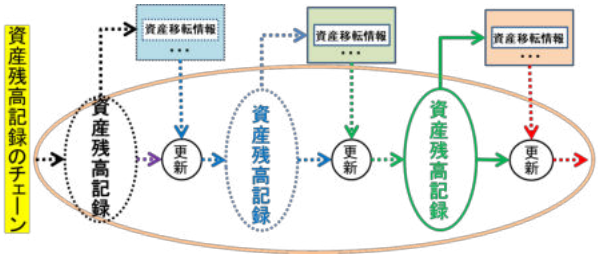

図 3　資産残高記録方式（BCAMS）

暗号資産システムの台帳に登録される情報は，資産記録・管理方式に依存する．一般的な資産移転記録方式 TCAMS の場合に台帳に登録される記録例を図 4 に示しており，資産残高記録方式 BCAMS の場合に台帳に登録される記録例を図 5 に示している．

図 4　台帳に登録される資産移転記録例

資産残高記録	
資産管理アカウント1	資産残高1
資産管理アカウント2	資産残高2
・・・	
資産管理アカウントn	資産残高n

図５　台帳に登録される資産残高記録例

３　資産移転記録方式暗号資産の封印・償還方式および匿名性と特定・追跡性の調査・分析

資産移転記録方式 TCAMS における暗号資産では，資産の提供者が提供先を示す情報を含むトランザクションを台帳に登録することにより資産の所有権が移転し，その後，資産の受取者が所有権を示す情報を含むトランザクションを台帳に登録することにより当該資産を使用することができる．資産の提供者が想定する受取者以外が受け取れないよう資産の提供先を指定する情報を封印情報，受取者が受取時にその資産の所有権を示す情報を償還情報と称している（図６）．

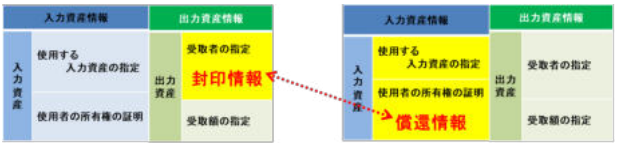

図６　封印情報と償還情報の対応

資産移転記録方式 TCAMS の暗号資産における利用者の匿名性，特定・追跡性は，台帳に登録され公開される，利用者を識別する情報を含む封印情報および償還情報，からの利用者の匿名性，特定・追跡性に大きく依存している．

本章では，資産移転記録方式 TCAMS を採用する三つの暗号資産 Bitcoin，Monero，Zcash について，資産封印・償還方式およびその結果として台帳に登録される封印・償還情報からの利用者の匿名性へのリスクおよび利用者の特定・追跡性の現状を報告する．

3.1　Bitcoin

Bitcoin の封印情報および償還情報は，スクリプトとして指定される．封印情報と償還情報の対応の妥当性は，それぞれのスクリプトから構成される検証スクリプトの処理結果の真偽により判定される．Bitcoin の封印・償還情報の指定方法には複数の方式が用意されているが，P2PKH および P2SH の 2 つの方式について調査を実施した．Bitcoin の標準的な封印・償還方式は P2PKH であり，2018 年 11 月頃までの 55 万ブロックのトランザクションの出力・入力の対応の調査の結果（[7]），実際に P2PKH が最も多く，P2SH が 2 番目に多い封印・償還方式であることから，P2PKH，P2SH を選定した．図 7 に，P2PKH，P2SH の封印情報，償還情報を示すスクリプトおよびその検証スクリプトを示している．

	封印情報 ←	→ 償還情報
P2PKH	OP_DUP OP_HASH160 <$PUBKEY_A$ HASH> OP_EQUAL OP_CHECKSIG	<SIG_A> <$PUBKEY_A$>
	<SIG_A> <$PUBKEY_A$> OP_DUP OP_HASH160 <$PUBKEY_A$ HASH> OP_EQUAL OP_CHECKSIG	
P2SH	OP_HASH160 <M-OF-N MULTI-SIG SCRIPT HASH> OP_EQUAL	OP_0 <SIG_1> <SIG_2> … <SIG_M> <M-OF-N MULTI-SIG SCRIPT> <M-OF-N MULTI-SIG SCRIPT> = OP_M <$PUBKEY_1$> <$PUBKEY_2$> … <$PUBKEY_N$> OP_N OP_CHECKMULTISIG
	<M-OF-N MULTI-SIG SCRIPT> OP_HASH160 <M-OF-N MULTI-SIG SCRIPT HASH> OP_EQUAL <SIG_1> <SIG_2> … <SIG_M> <M-OF-N MULTI-SIG SCRIPT>	

図７　P2PKH，P2SH における
封印・償還および検証のスクリプト

P2PKH（Pay to Public Key Hash）

P2PKH による封印・償還の仕組みを図 8 に示している．受取者（償還者）は受取に使用するワンタイム公開鍵を生成し，そのハッシュ値を提供者（封印者）へ連絡する．その受取者のワンタイム公開鍵のハッシュ値を封印情報とする出力を含むトランザクションを提供者が発行し，台帳に登録する．受取者は生成したワンタイム公開鍵に対応するワンタイム秘密鍵により，当該入力が含まれるトランザクションへの署名を作成し，ワンタイム公開鍵と署名を償還情報とする入力を含むトランザクションを発行し，台帳に登録する．

封印・償還の検証は，償還情報として指定されるワンタイム公開鍵と封印情報として指定されるワンタイム公開鍵のハッシュ値の対応の確認，償還情報として指定されるトランザクションへの署名のワンタイム公開鍵による署名検証により実施される．

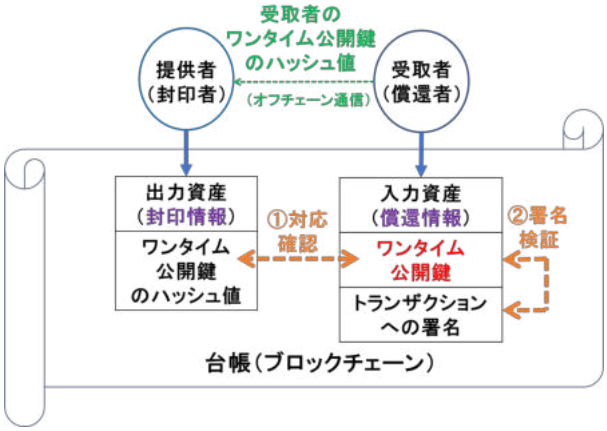

図８　P2PKH における封印・償還および検証

以上のように，P2PKH による封印・償還では，受取者のワンタイム公開鍵のハッシュ値，ワンタイム公開鍵そのもの，ワンタイム公開鍵に対応する秘密鍵によるトランザクションへの署名が台帳上に登録され公開されることになる．

① 利用者の匿名性

台帳上に公開される情報の中で，利用者（受取者）の匿名性を脅かすリスクが最も高いのは受取者のワンタイム公開鍵であるが，Bitcoin で一般的に使用されるワンタイム鍵ペア生成方法ではその生成過程で利用者固有の情報は使用されないため，生成されたワンタイム公開鍵からの利用者特定は困難である．P2PKH における利用者の匿名性は一定レベル実現済みと言える．

しかし，複数入力の暗号資産の場合は，それぞれがワンタイム公開鍵であっても，同一利用者のワンタイム公開鍵であること露呈することになり，利用者の匿名性を脅かすリスクとなる．

② 利用者の特定・追跡性

匿名性の場合と同様，受取者のワンタイム公開鍵が，受取者（利用者）の特定・追跡のための最も有力な情報ではあるが，匿名性の項目で記載したように，ワンタイム公開鍵から受取者(利用者)を特定することは難しい．

利用者の協力が得られ，利用者のワンタイム公開鍵を入手できれば，利用者の資産を特定できる．利用者にとっては，ワンタイム公開鍵群を第三者に提供しても，対応する資産の不正使用などのリスクは発生せず，資産の保全は保証される．なお，提供されたワンタイム公開鍵群が真に利用者のものであることは対応する秘密鍵群で作成される署名群の提供を受けることにより確認は可能であるが，利用者のワンタイム公開鍵群が網羅されているかどうかの判断は，提供を受けた第三者には難しい．

P2SH（Pay to Script Hash）

P2SH による封印･償還の仕組みを図 9 に示している．P2SH では，様々なスクリプトの使用が可能であるが，過半数を超え最も多く使用されている M-of-N マルチシグを調査の対象とした．

受取 G のメンバはそれぞれワンタイム公開鍵を生成し受取 G 代表者へ連絡，受取 G 代表者は集まったワンタイム公開鍵を使用し償還条件を作成しそのハッシュ値を提供者（封印者）へ連絡する．提供者は受け取った償還条件のハッシュ値を封印情報とする出力を含むトランザクションを発行し台帳に登録する．受取 G 代表者は受取時に生成するトランザクションのハッシュ値を受取 G メンバへ送り必要な数の署名を集め，償還条件と必要な数の署名を償還情報とする入力を含むトランザクションを発行し台帳に登録する．

封印・償還の検証は，償還情報として指定される償還条件と封印情報として指定される償還条件のハッシュ値の対応の確認，償還情報として指定される償還条件の充足情報（必要な数の署名等）が償還条件を真に充足するかどうかの確認により実施される．

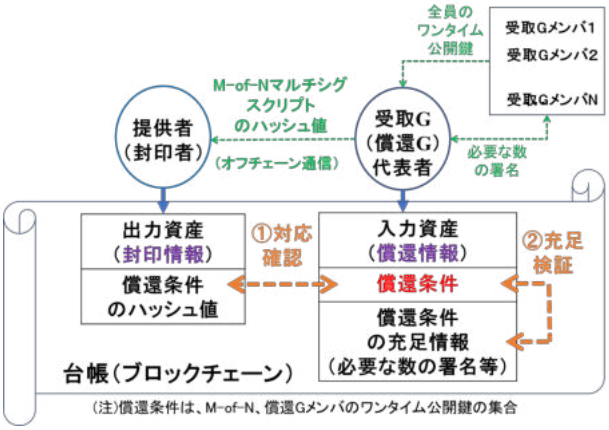

図 9　P2SH（M-of-N マルチシグ）
における封印・償還および検証

以上のように，P2SH（M-of-N マルチシグ）による封印・償還では，償還条件のハッシュ値，M-of-N の条件および受取 G メンバ全員の N 個のワンタイム公開鍵そのもの，受取 G メンバの M 人のワンタイム公開鍵に対応する秘密鍵によるトランザクションへの署名が台帳上に公開されることになる．

① 利用者の匿名性

台帳上に公開される情報の中で，利用者（受取 G メンバ）の匿名性を脅かすリスクが最も高いのは受取 G メンバのワンタイム公開鍵であるが，Bitcoin で一般的に使用されるワンタイム鍵ペア生成方法ではその生成過程で利用者固有の情報は使用されないため，生成されたワンタイム公開鍵からの利用者（受取 G メンバ）特定は困難である．P2SH における利用者の匿名性は一定レベル実現済みと言える．

なお，複数入力の暗号資産の場合のリスクは存在するが，それぞれの受取 G のメンバが異なる可能性もあり，また受取 G メンバの数により，同一利用者のワンタイム公開鍵かどうかの特定は難しく，P2PKH に比べリスクは非常に小さい，と考えられる．

② 利用者の特定・追跡性

匿名性の場合と同様，利用者（受取 G メンバ）のワンタイム公開鍵が，受取 G メンバ（利用者）の特定・追跡のための最も有力な情報ではあるが，匿名性の項目で記載したように，ワンタイム公開鍵から受取 G メンバ（利用者）を特定することは難しい．

利用者（受取 G メンバ）の協力が得られ，利用者のワンタイム公開鍵群を入手できれば，利用者が参加する受取 G の資産を特定できる．利用者にとっては，ワンタイム公開鍵群を第三者に提供しても，対応する資産の不正使用などのリスクは発生せず，資産の保全は保証される．なお，提供されたワンタイム公開鍵群が真に利用者のものかの確認には P2PKH の場合と同様の利用者の更なる協力が必要となり，また，利用者のワンタイム公開鍵群が網羅されているかどうかの判断は，P2PKH と同様，提供を受けた第三者には難しい．

3.2 Monero（RCTTypeSimple）

Monero においては，封印情報として受取者のワンタイム公開鍵が指定され，償還情報としては，受け取る暗号資産およびリング署名に組み込まれる複数のデコイ暗号資産の位置情報，指定された暗号資産に対応するワンタイム公開鍵群および受け取る暗号資産のワンタイム公開鍵に対応する秘密鍵から生成されるリング署名，受取者のワンタイム公開鍵・秘密鍵ペアから生成される鍵イメージが指定される．

封印・償還の検証は，封印情報として指定されるワンタイム公開鍵による償還情報として指定されるリング署名の検証，および償還情報として指定される鍵イメージによる資産の未使用確認により実施される（図 10）．

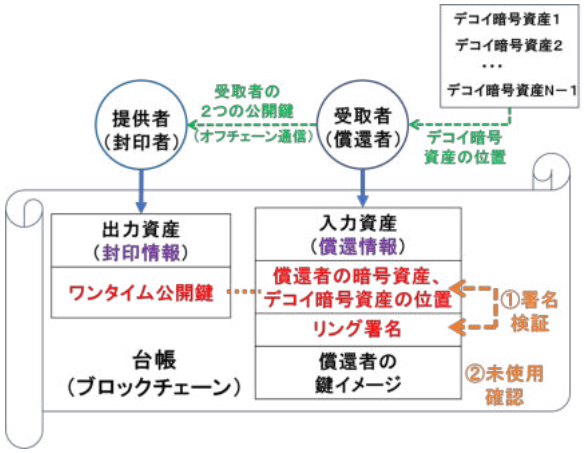

図 10　Monero における封印・償還および検証

以上のように，Monero では受取者のワンタイム公開鍵，リング署名に組み込まれるデコイ暗号資産のワンタイム公開鍵，リング署名，受取者の鍵イメージが台帳上に公開されることになる．

①　利用者の匿名性

台帳上に公開される情報の中で，利用者の匿名性を脅かすリスクが最も高いのは，Bitcoin の場合と同様，受取者のワンタイム公開鍵である．

Monero では利用者は View Key pair および Spend Key pair を保有し，両方の公開鍵は公開可能である．提供者は，受取者の 2 つの公開鍵と乱数からワンタイム公開鍵を生成し，封印情報として使用されている．

このように生成されたワンタイム公開鍵からの利用者の推定は困難であり，Monero における利用者の匿名性は一定レベル実現済みと言える．

また，実際に使用される受取者の暗号資産のワンタイム公開鍵の特定そのものも，現在は 10 個のデコイ暗号資産が利用されており一定レベルの困難化がなされている．

Bitcoin の場合と同様，複数入力の暗号資産の場合のリスクは存在するが，そもそもデコイ暗号資産により受取者の暗号資産に対応するワンタイム公開鍵の特定は難しく，複数の入力に対応するワンタイム公開鍵群の中からそれぞれの受取者のワンタイム公開鍵を特定するのは更に難しい．

なお，既に他のトランザクションの封印情報として台帳上に公開されているデコイ暗号資産のワンタイム公開鍵については，デコイ暗号資産として使用されることによる新たなリスクの発生は無いと考えられる．

②　利用者の特定・追跡性

匿名性の場合と同様，受取者のワンタイム公開鍵が受取者特定・追跡のための最も有力な情報ではあるが，匿名性の項目で記載したように，ワンタイム公開鍵から受取者（利用者）を特定することは難しい．

Bitcoin の場合と同様，Monero においても利用者の協力が得られ利用者のワンタイム公開鍵群を入手できれば，利用者の資産の保全を保証しつつ，利用者の資産を特定できるが，提供されたワンタイム公開鍵群が真に利用者のものかの確認は必要であり，また利用者のワンタイム公開鍵群が網羅されているかどうかの確認は難しい．

Monero ではワンタイム公開鍵生成プロセスの特徴から，利用者から View Key pair および Spend Key pair に対応する tracking key の提供を受けた第三者は，利用者の View Key pair および Spend Key pair により生成されたワンタイム公開鍵および対応する資産のすべてを特定できる．また，特定できたワンタイム公開鍵に対応する鍵イメージの提供を受けることにより，対応する資産の使用済み/未使用の判断が可能で，利用者の資産保有額の把握も可能である．

tracking key および鍵イメージだけでは当該利用者が受け取った資産を使用することはできないため，対応する資産の不正使用のリスクは発生せず，利用者は資産を保全しつつ監査等の目的のために第三者へ提供することができる．

なお，利用者は View Key pair および Spend Key pair を複数組保有することも可能で，利用者の Monero 資産総額の特定は，台帳上に登録されている情報のみでは不可能である．

3.3 Zcash（Sapling）

Zcash では，封印情報として暗号化された Note Plaintext を指定する．Note Plaintext は，受取者の Diversifier of Shielded Payment Address，受取者の受取額，Trapdoor of Note Commitment，受取者へのメモ等から構成されている．出力資産に含まれている Value Commitment, Note Commitment 等の他の情報が Note Plaintext の内容と整合していることを確認できるゼロ知識証明も出力資産に含まれている．

Zcash の償還情報として，Note Commitment が格納されている Note Commitment Tree の anchor，Note の Nullifier，Expanded Spending Key 等による署名が指定されている．また，Note Commitment Tree の anchor，Note の Nullifier および入力資産に指定されて

いる Value Commitment の正当性を確認できるゼロ知識証明も入力資産に含まれている．

封印・償還の検証は，償還情報として指定される Note Commitment Tree の anchor を利用し Tree State 内の Note の存在の確認，償還情報として指定される Note Nullifier が Nullifier Set に含まれていないことによる Note の未使用の確認，償還情報として指定される Expanded Spending Key から生成された秘密鍵に対応する公開鍵による署名検証による所有権の確認により実施される（図 11）．

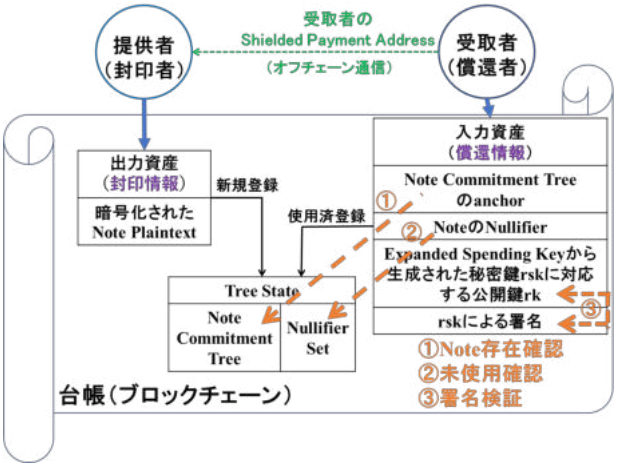

図 11　Zcash における封印・償還および検証

以上のように，Zcash においては，暗号化されている Note Plaintext, ハッシュ関数を利用し生成される Value Commitment，Note Commitment，Nullifier，乱数を利用し生成される公開鍵等が，台帳（あるいは台帳経由参照可能な場所）に登録され公開されることになる．

① 利用者の匿名性

Zcash の場合，台帳に登録される利用者に関する情報はすべて，暗号化，ハッシュ化，ランダム化された情報であり，封印・償還情報が利用者の匿名性を脅かすリスクは存在しないと考えられる．

複数入力の暗号資産の場合も，Zcash では新たなリスクは発生しない．

② 利用者の特定・追跡性

上述のように，Zcash では台帳に登録される利用者に関する情報はすべて，暗号化，ハッシュ化，ランダム化された情報であるため，利用者の特定・追跡の手掛かりとなる情報は存在しない．受取者（利用者）を特定することは難しい．

Zcash では，利用者から利用者のマスター秘密鍵である Spending Key から生成される Incoming Viewing Key の提供を受け取った第三者は，当該利用者が受け取った資産の特定，資産の使用済み/未使用の判断が可能で，資産保有額の把握も可能である．また，Incoming Viewing Key だけでは当該利用者が受け取った資産を使用することはできないため，資産の不正使用のリスクは発生せず，利用者は資産を保全しつつ監査等の目的のために第三者へ提供することができる．しかし，Note の一部に組み込まれている memo（提供者から受取者へのメッセージ）も Incoming Viewing Key で復号され第三者に開示されることになり，注意を要する．

なお，Zcash では，利用者は複数のマスター秘密鍵を保有することも可能で，利用者の Zcash 資産総額の特定は，台帳上に登録されている情報のみでは不可能である．

3.4　Bitcoin，Monero，Zcash の比較

① 匿名性について

本章の調査・分析結果の要点を図 12 にまとめている．

	匿名性へのリスクが想定される台帳登録・公開情報	利用者の確実な匿名性の観点からのリスク
Bitcoin（P2PKH）	利用者（償還者）のワンタイム公開鍵とそのハッシュ値	複数の入力資産指定の場合の、ワンタイム公開鍵間の連結性
Bitcoin（P2SH）	利用者を含む受取Gのメンバのワンタイム公開鍵とそのハッシュ値	複数入力指定の場合に同様のリスクは存在するが、P2PKHに比べ小さい
Monero	利用者（受取者）のワンタイム公開鍵（受取者のワンタイム公開鍵の特定はデコイ暗号資産の数に応じ困難）	複数の入力資産指定の場合の、指定された複数のワンタイム公開鍵間の連結性（但し、償還者のワンタイム公開鍵の特定はデコイ暗号資産の数に応じ困難）
Zcash	匿名性へのリスクが想定される台帳登録・公開情報は無い（利用者に関する情報は、暗号化、ハッシュ化、ランダム化されている）	―

図 12　“利用者の確実な匿名性”の観点からのまとめ

一般に，利用者の匿名性については多くの暗号資産が，最初の暗号資産である Bitcoin に倣い，利用者識別情報の仮名性，ワンタイム性を採用し，同程度の匿名性を実現している．（但し，今回の調査の対象外である資産残高記録方式（BCAMS）の暗号資産の中には Bitcoin より匿名性のレベルが低いものも存在する．）

確実な匿名性の実現には，台帳上に利用者の情報を露出させない方式が必要であり，にもかかわらずトランザクションの正当性を第三者が検証できる仕組みとしてのゼロ知識証明の活用は今後も増加するものと考えられる．

② 特定・追跡性について

本章の調査・分析結果を図 13 にまとめている．

	可能な方法	できること（できないこと）	リスク
Bitcoin（P2PKH、P2SH）	利用者によるワンタイム公開鍵の提供	＊ワンタイム公開鍵で受け取った資産の特定、使用済み/未使用の特定 ＊資産保有額の把握（すべてのワンタイム公開鍵を提供した場合）	＊利用者の提供情報が正しいかどうか
Monero	利用者によるワンタイム公開鍵の提供	＊ワンタイム公開鍵で受け取った資産の特定（当該資産の使用済み/未使用の特定は不可）	＊利用者の提供情報が正しいかどうか
	利用者による tracking keyおよび鍵イメージの提供	＊受け取った資産の全ての使用・未使用の特定、資産保有額の把握	
Zcash	利用者による Incoming Viewing Keyの提供	＊受け取った資産の全ての特定および資産保有額の把握	＊利用者提供情報が正しいかどうか ＊利用者宛メッセージ開示のリスク

図 13　利用者の特定・追跡性に関する機能比較（現状）

Bitcoin の場合，第三者は利用者よりワンタイム公開鍵の提供を直接受けることにより，ワンタイム公開鍵に対応する利用者を特定できるが，その他の方法は用意されていない．

Monero については，Bitcoin と同様に利用者による第三者へのワンタイム公開鍵の提供によりワンタイム公開鍵

に対応する利用者の特定は可能であるが，利用者による View Key pair および Spend Key pair に対応する tracking key の提供により，第三者による利用者の一連のワンタイム公開鍵および受取資産を特定できる仕組みが用意されている.

Zcash についても Monero と同様，利用者による利用者のマスター秘密鍵である Spending Key に対応する Incoming Viewing Key の提供により，第三者による利用者の一連の受取資産を特定できる.

以上のように，今回調査した３つの暗号資産システムでは，利用者の協力が得られる場合においても，封印・償還される資産の受取者（利用者）の特定・追跡については，基本的な仕組みのみが用意されているのが現状であり，利用者の協力が得られない場合の特定・追跡性に関しては特段の配慮は一切なされていないのが現状である.

４　おわりに

本稿では，資産移転記録方式（TCAMS）の主要な暗号資産 Bitcoin，Monero，Zcash について，それぞれの封印情報・償還情報からの利用者の匿名性および特定・追跡性に関する調査・考察を報告した.

匿名性については，暗号資産の多くは強く意識しており，それぞれ対応を工夫しているが，第三者に対する匿名性の確保のためには台帳上で公開される封印情報・償還情報には利用者の特定につながる情報を露出させない方式が望ましく，匿名性の強化には暗号化＋ゼロ知識証明が今後も活用されることになろう.

特定・追跡性については，多くの暗号資産で対応はこれからである．利用者として登録時に身元確認を行うこととか，身元情報登録機能を用意し，利用者の判断で登録，必要な第三者へ提供する等の仕組みを用意している暗号資産も見受けられるが，まだまだ本格的な対応とはいいがたい状況である.

今後，安心・安全な暗号資産システムとして求められる利用者の特定・追跡性に関する要件を整理しつつ，暗号資産システムとしてはその要件への対応策を検討する必要があろう.

謝辞

本研究の一部は，JSPS 科研費 基盤(B) JP18H03240 の支援を受けている.

参考文献

[1] 才所敏明，辻井重男，櫻井幸一，“暗号資産台帳の匿名性と特定・追跡性についての考察”，2020 年電子情報通信学会ソサイエティ大会.

[2] 才所敏明，辻井重男，櫻井幸一，” 匿名暗号資産（Monero/Zcash/Grin）ブロックチェーンの匿名性に関する考察 ”，コンピュータセキュリティシンポジウム 2019（CSS2019）.

[3] 才所敏明，辻井重男，櫻井幸一，” 暗号仮想通貨における匿名化技術の現状と展望 ”，情報処理学会第 81 回全国大会, 2019.

[4] 才所敏明，辻井重男，櫻井幸一，” 仮想通貨の匿名性の現状と課題”，暗号と情報セキュリティシンポジューム（SCIS2019），2019.

[4] 穴田啓晃，櫻井幸一，“ブロックチェーンの暗号論的要素技術の分類”，SCIS2018.

[5] 宇根正志，“暗号資産における取引の追跡困難性と匿名性：研究動向と課題”，金融研究/2019.7. http://www.imes.boj.or.jp/research/papers/japanese/kk38-3-4.pdf

[5] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. https://bitcoin.org/bitcoin.pdf

[6] Mastering Bitcoin https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf

[7] Stefano Bistarelli，Ivan Mercanti，Francesco Santini, "An Analysis of Non-standard Transactions", 2019. https://www.frontiersin.org/articles/10.3389/fbloc.2019.00007/full

[8] Monero：Privacy in the blockchain　v1.0 https://eprint.iacr.org/2018/535.pdf

[9] Zero to Monero: First Edition https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf

[10] Mastering Monero https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf

[11] Zcash Protocol Specification https://www.btrade.co.kr/btrade_res/20180507145055652.pdf

[12] Grin Whitepaper https://www.allcryptowhitepapers.com/grin-whitepaper/

[13] Serguei Popov，“The Tangle”，April 30, 2018. Version 1.4.3.

https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
[14] Anton Churyumov, "Byteball: A Decentralized System for Storage and Transfer of Value", 2016. https://obyte.org/Byteball.pdf
[15] Colin LeMahieu, "Nano: A Feeless Distributed Cryptocurrency Network", 2018. https://nano.org/en/whitepaper
[16] Leemon Baird, Mance Harmon, Paul Madsen, "Hedera: A Public Hashgraph Network & Governing Council", 2019. https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf
[17] Aidos Kuneen − A Blockless and Anonymous Cryptocurrency for the Post-Quantum Era −, Aidos Developer & Aidos Foundation, 2018. http://www.aidoskuneen.com/files/adk_whitepaper.pdf
[18] DERO PROJECT WHITE PAPER, 2018. https://dero.io/attachment/Whitepaper.pdf
[19] Tangram: An Introduction, 2018. https://tangrams.io/wp-content/uploads/2018/12/Tangram_An_Introduction-2018-12-19-03-27.pdf
[20] All Cryptocurrencies https://coinmarketcap.com/all/views/all/
[21] Nicolas van Saberhagen, "CryptoNote v2.0", 2013. https://cryptonote.org/whitepaper.pdf
[22] Andrew Poelstra, "Mimblewimble", 2016. https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf
[23] Gregory Maxwell, "CoinJoin: Bitcoin privacy for the real world", 2013. https://bitcointalk.org/index.php?topic=279249.0
[24] Gregory Maxwell, Andrew Poelstra, "Borromean Ring Signature", 2015. https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf
[25] SHEN NOETHER, "RING CONFIDENTIAL TRANSACTIONS", 2015. https://eprint.iacr.org/2015/1098.pdf
[26] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer, "From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again", 2011. https://eprint.iacr.org/2011/443
[27] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova, "Pinocchio: Nearly Practical Verifiable Computation", 2013. https://eprint.iacr.org/2013/279
[28] DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843
[29] Christina Garman, Matthew Green, Ian Miers, " Accountable Privacy for Decentralized Anonymous Payments", 2016. https://eprint.iacr.org/2016/061.pdf