# 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

才所 敏明[*1]　　辻井 重男[*2]　　櫻井 幸一[*3]

**概要**：資産の移転結果を示すブロックチェーンの匿名性要件を整理し，ブロックチェーンの匿名性を強化する主要な技術・プロトコル（CryptoNote，zk-SNARKs，Mimblewimble）を採用している代表的な匿名暗号資産 Monero，Zcash，Grin について，それぞれのブロックチェーンの匿名性要件への対応状況について報告する．一方，暗号資産の犯罪・不正利用防止・抑止あるいは第三者機関による監査を可能とするため，資産の移転に関わる利用者・移転資産額の特定・追跡性へのニーズも高まっており，Monero/Zcash/Grin における利用者・移転資産額の特定・追跡可能性の現状についても概要を報告する．

**キーワード**：仮想通貨，暗号通貨，暗号資産，匿名暗号資産，ブロックチェーン，CryptoNote，Monero，zk-SNARKs，Zcash，Mimblewimble，Grin，匿名性，特定・追跡性

# Considerations on anonymity of anonymous CryptoAssets (Monero / Zcash / Grin) blockchain

Toshiaki Saisho[*1]　　Shigeo Tsujii[*2]　　Kouichi Sakurai[*3]

***Abstract***: We define the blockchain anonymity requirements that indicate the result of asset transfer. And about representative anonymous encryption assets Monero (CryptoNote), Zcash (zk-SNARKs), Grin (Mimblewimble), we report investigation / examination result about the correspondence situation to anonymity requirements of each blockchain. On the other hand, there is a growing need for identifiability and traceability of users and transferred asset amounts related to asset transfer, in order to enable crime / abusive use / prevention of crypto assets and audits by third parties. In this paper, we also report the results of our study on the possibility of identifying and tracking the amount of users and assets transferred in Monero / Zcash / Grin.

***Keywords***: Virtual currency，Crypto currency，Crypto Assets，Blockchain，CryptoNote，Monero，zk-SNARKs，Zcash，Mimblewimble，Grin，Anonymity，Identifiability，Traceability

## 1. 暗号資産の概況

Satoshi Nakamoto が 2008 年に投稿した論文で公開し，2009 年に運用が開始された最初の暗号資産であるビットコイン以来，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”（[5]）のデータによると 2019 年 7 月 10 日現在，2264 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 355B ドルとなっている. 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 位であり，全体の時価総額の約 65%を占めている．図 1 に主要な暗号資産（時価総額のベスト 20）を示している．

| 順位 | 名称 | 記号 | 時価総額 |
|---|---|---|---|
| 1 | Bitcoin | BTC | $230,770,507,812 |
| 2 | Ethereum | ETH | $33,345,412,861 |
| 3 | XRP | XRP | $16,777,509,982 |
| 4 | Bitcoin Cash | BCH | $7,510,707,733 |
| 5 | Litecoin | LTC | $7,487,246,142 |
| 6 | EOS | EOS | $5,423,812,688 |
| 7 | Binance Coin | BNB | $4,591,788,731 |
| 8 | Tether | USDT | $3,826,998,216 |
| 9 | Bitcoin SV | BSV | $3,672,528,567 |
| 10 | TRON | TRX | $2,269,181,081 |
| 11 | Cardano | ADA | $1,993,993,065 |
| 12 | Stellar | XLM | $1,964,580,608 |
| 13 | Monero | XMR | $1,707,086,953 |
| 14 | UNUS SED LEO | LEO | $1,575,243,676 |
| 15 | Dash | DASH | $1,398,306,872 |
| 16 | NEO | NEO | $1,209,104,010 |
| 17 | IOTA | MIOTA | $1,095,114,011 |
| 18 | Chainlink | LINK | $1,089,556,852 |
| 19 | Cosmos | ATOM | $918,969,744 |
| 20 | Ethereum Classic | ETC | $875,490,153 |

**図 1　暗号資産時価総額ベスト 20**
**（2019 年 7 月 10 日）**

*1　（株）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

暗号資産は一般に匿名性が強く，マネーロンダリング等の不正・不法な目的に悪用される課題を抱えており，このような課題を克服した安心・安全な暗号資産への期待は強いと考えられる．

一方，プライバシー保護の観点からは，暗号資産の不十分な匿名性への懸念も強く，匿名性を更に強化した匿名暗号資産も多く登場してきている．

暗号資産全体の中で主要な匿名暗号資産 27 個（[6] で指定された匿名暗号資産に BEAM を加えた 29 個の内，[5] にデータが存在するもの）の 2017 年 7 月 10 日時点の時価総額は 3B ドルと推定され，現状，暗号資産時価総額全体の 0.9%程度となっている．図 2 に主要な匿名暗号資産（時価総額でベスト 10）を示している．

| 順位 | 名称 | 記号 | 時価総額 |
|---|---|---|---|
| 13 | Monero | XMR | $1,707,086,953 |
| 25 | Zcash | ZEC | $716,426,317 |
| 43 | HyperCash | HC | $194,272,844 |
| 55 | Bytecoin | BCN | $167,031,844 |
| 74 | Verge | XVG | $117,390,467 |
| 88 | Zcoin | XZC | $91,178,150 |
| 101 | Grin | GRIN | $66,960,442 |
| 107 | Electroneum | ETN | $62,559,652 |
| 119 | Enigma | ENG | $50,781,038 |
| 145 | Beam | BEAM | $38,514,322 |

**図 2　匿名暗号資産時価総額ベスト 10**
**（2019 年 7 月 10 日）**

## 2.　暗号資産の匿名性に関するリスク

### 2.1　暗号資産システムの匿名性に関するリスクの全体像

暗号資産システムにおける利用者の匿名性に関するリスクを図 3 に示している．このように，暗号資産を使用する様々の局面・過程で，匿名性に関するリスクは存在するが，本稿では，暗号資産の移転結果を示し，しかも広く公開される(5)の暗号資産ブロックチェーン（以下，単にブロックチェーンと表記）の匿名性を考察の対象とする．

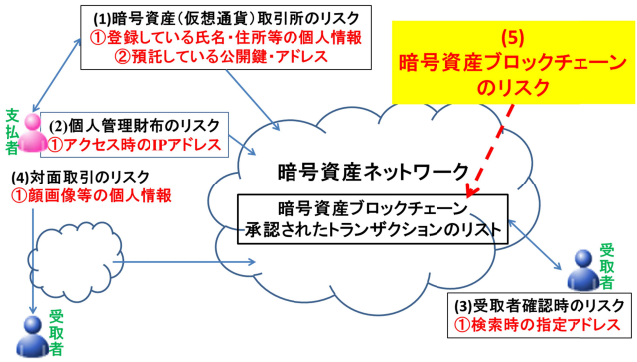


**図 3　暗号資産システムの匿名性に関するリスク**

### 2.2　ブロックチェーンの匿名性に関する要件

ブロックチェーンには暗号資産の個々の移転結果を示すトランザクションが登録されており，トランザクションには一般に図 4 に示す情報が登録されている．

| 入力関連情報 | | 出力関連情報 | |
|---|---|---|---|
| 入力項目１ | 使用する資産の指定（提供者のアドレス、金額等が指定されている位置） | 出力項目１ | 受取者の指定（受取者のアドレス等） |
| | 指定資産の使用権の証明（公開鍵、署名等） | | 提供額の指定（金額等） |
| 入力項目２ | 使用する資産の指定 | 出力項目２ | 受取者の指定 |
| | 指定資産の使用権の証明 | | 提供額の指定 |
| ・・・・・ | | ・・・・・ | |
| 入力項目ｎ | 使用する資産の指定 | 出力項目ｍ | 受取者の指定 |
| | 指定資産の使用権の証明 | | 提供額の指定 |

**図 4　トランザクションを構成する情報**
**（匿名性に関連する情報のみ）**

ブロックチェーンの匿名性は，利用者および利用者の資産額の特定不能性，利用者および資産の移転の追跡不能性と考えることができる．ブロックチェーンの匿名性に対するリスクは，ブロックチェーンを構成する個々のトランザクションに格納されている入力（提供）・出力（受取）情報，トランザクション間の出力（受取）・入力（提供）情報のつながりに関する情報，および移転する資産の額に存在し，ブロックチェーンの匿名性に関する要件は，次の 5 項目にまとめることができる．

**①Pseudonymity**

トランザクションには一般に暗号資産を提供する利用者（提供者）の識別情報，それを受け取る利用者（受取者）の識別情報が含まれている．

このような利用者識別情報から実在する利用者の実名等の推定が困難であるという要件を，Pseudonymity（利用者識別情報の仮名性），と定義する．

**②Unlinkability**

トランザクションの随所に格納されている利用者識別情報が同一の利用者に紐づけられていることが判ると，利用者の提供や受取の挙動の分析から利用者の推定に繋がる恐れがある．

複数の利用者識別情報が，同一の利用者に紐づけられていることの推定が困難であるという要件を，Unlinkability（利用者識別情報間の非連結性），と定義する．

**③Untraceability between Transactions**

ブロックチェーン上のトランザクションに存在する利用者の識別情報に紐づけられた暗号資産は，保有者が新たなトランザクションにてその暗号資産の位置と所有権を示す利用者識別情報等を提示し，新たな受取者への提供に使用される．保有する暗号資産と提供に使用する暗号資産の

対応関係が判ると，利用者の暗号資産の受取・提供の流れが追跡でき，利用者の推定に繋がる恐れがある．

受取時の暗号資産と提供に使用する暗号資産との対応の推定が困難であるという要件を，Untraceability between Transactions（トランザクション間の暗号資産/利用者の非追跡性），と定義する．

**④Untraceability within Transaction**

トランザクションには一般に提供者と受取者の情報が格納されているが，暗号資産の提供者と受取者の対応関係が判るとそれぞれの利用者の推定に繋がる恐れがある．

トランザクション内の提供者と受取者の対応の推定が困難であるという要件を，Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性），と定義する．

**⑤Concealment of Amount**

暗号資産の提供額・受取額も，提供者，受取者の推定に繋がる恐れもあり，またプライバシー上の問題でもある．

暗号資産の提供額・受取額の推定が困難であるという要件を，Concealment of Amount（移転資産額の秘匿），と定義する．

## 3. 匿名暗号資産ブロックチェーンの主要な匿名化プロトコル

暗号資産のブロックチェーンは一般に匿名性が高いが，プライバシー保護および企業秘密保護の観点からは不十分であり，更に匿名性を強化した匿名暗号資産が多く登場してきている．

匿名暗号資産でブロックチェーンの匿名性を強化する技術は多く提案されているが，高い匿名性を実現するために提案されている代表的な技術・プロトコルは次の三つである．

**①CryptoNote**

CryptoNote は，提供者が使用する資産の特定を困難にするリング署名，受取者の特定を困難にするワンタイムアドレス，および資産の 2 重使用の検知の仕組み（鍵イメージ）から構成されるプロトコルである．移転資産額を秘匿する仕組みは含まれていない．

CryptoNote プロトコルベースの匿名暗号資産としては，Monero，Bytecoin，Electroneum，DigitalNote 等がある．

**②Zerocash**

Zerocash は，ゼロ知識証明 zk-SNARKs（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）を利用した，資産の移転に関わる情報を秘匿しつつ，その資産の移転が正当であることを第三者が検証可能な，プロトコルである．

Zerocash プロトコルベースの匿名暗号資産としては，Zcash，Zcash からフォークした Komodo 等がある．なお，Ethereum においても，匿名による資産の移転を可能とするために，zk-SNARKs が導入されている．

Zerocash プロトコルの前のバージョン Zerocoin プロトコルもゼロ知識証明を利用しているが，移転する資産の額の秘匿は行っていない．Zerocoin プロトコルベースの匿名暗号資産としては，Zcoin および PIVX 等がある．

**③Mimblewimble**

Mimblewimbe プロトコルは，Pedersen Commitment を利用した CT（コンフィデンシャルトランザクション）および CoinJoin の仕組みにより，利用者（提供者，受取者）および移転する資産の額を秘匿にしつつ，第三者による資産の移転の正当性検証を可能としている．

Mimblewimble プロトコルベースの匿名暗号資産には，Grin，BEAM がある．

**④その他**

ベスト 10 に入っている匿名暗号資産 Verge および Enigma はそれぞれ独自の方式を採用している．

Verge は，TOR/I2P による IP アドレスの秘匿や Wraith プロトコルによるトランザクションの暗号化による秘匿の仕組みにより，利用者の匿名性や提供者と受取者の対応の特定を困難にしている匿名暗号資産である．

Enigma は，sMPC（Secure Multi-party Computation）技術により，暗号化されたまま処理を実行し，計算に参加するノードに対しても元のデータを漏らさない秘匿性の実現の仕組みを目指したプロジェクトの匿名暗号資産である．

本稿では以下の章にて，①～③で示した高い匿名性を実現するために提案されている CryptoNote，Zerocash，Mimblewimble の各プロトコルを採用している代表的な匿名暗号資産 Monero，Zcash，Grin について，2 章で述べた匿名性要件との関係からそれぞれの匿名性の現状について考察する．また，それぞれの匿名暗号資産の移転に関わる利用者の特定・追跡や移転資産額の特定が可能な仕組みへの対応状況についても，整理し考察する．

## 4. Monero

Monero トランザクション情報に対する利用者の匿名性は，CryptoNote で提案された匿名化技術を改良し実現されている．採用されている主な匿名化技術は，ワンタイムステルスアドレス（ワンタイム公開鍵），Pedersen Commitment および MLSAG 署名を使用したリング CT（リングコンフィデンシャルトランザクション）である．

なお，Monero では，単一の提供資産の場合に使用される RCTTypeFull と複数の提供資産の場合に使用される RCTTypeSimple という二つのタイプのトランザクションが存在するが，本稿では複数の提供資産（入力）に対応する RCTTypeSimple トランザクションを調査対象としている．


**図 5　Monero（RCTTypeSimple）トランザクションを構成する情報（匿名性に関連する情報のみ）**

### 4.1　Monero の匿名性

RCTTypeSimple のトランザクションで構成される Monero ブロックチェーン（本稿では以下，単に Monero と表記）の匿名性について，以下，2 章でまとめた匿名性に関する要件ごとにまとめている．

**①Pseudonymity**

Monero では，利用者固有の 2 組の公開鍵暗号の鍵ペアが使用され，そのうちの 256 ビットの二つの公開鍵が利用者識別情報に該当する．二つの公開鍵は共に乱数から生成される秘密鍵経由生成され，その生成プロセスでは利用者固有の情報は使用されないため，二つの公開鍵（利用者識別情報）のいずれからも利用者を推定するのは難しく，一定の Pseudonymity 要件を満たしている．

**②Unlinkability**

Monero では，トランザクションでの受取者の指定には，上述の利用者固有の二つの公開鍵をそのまま使用するのではなく，二つの公開鍵とトランザクションごとに生成する乱数から新たな公開鍵を作成し使用する．このように受取者用公開鍵は毎回異なるため，ブロックチェーン上のトランザクション内に指定されている複数の利用者識別情報が同一の利用者に紐づけられていることを特定するのは困難で，一定の Unlinkability（非連結性）要件を満たしている．

**③Untraceability between Transaction**

Monero では，トランザクションで使用する暗号資産が特定されないよう，同時に⑤の暗号資産の移転額も秘匿できるよう，リング CT が採用されている．リング CT は，使用する暗号資産候補として未使用の暗号資産を多数指定し，どの暗号資産が使用されるかはわからないようにしつつも，一つの暗号資産が使用されることを保証することができる．また，使用暗号資産の鍵イメージの登録・利用により使用資産の特定を防ぎつつ，資産の 2 重使用のチェックを可能としている．

リング CT により Untraceability between Transaction（トランザクション間の暗号資産/利用者の非追跡性）要件に対応する仕組みは用意されているが，その要件への対応のレベルはダミーとして指定する未使用暗号資産の数に強く依存することになる．

**④Untraceability within Transactions**

Monero では，本要件のための個別の対策は行っていない．しかし，②のワンタイム公開鍵の使用による受取者を示す利用者識別情報からの受取者特定の困難化，および③のリング CT による提供者に対応する利用者識別情報の特定の困難化により，提供者と受取者の対応の特定を困難にすることができる．

しかし，③で述べたように Untraceability between Transactions 要件への対応レベルはリング CT で使用するダミーの暗号資産の数に依存し，Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性）要件への対応レベルもそれに準じたレベルとなる．

**⑤Concealment of Amount**

Monero では，リング CT により，個々の暗号資産の提供額，受取額を公開せずに，提供額の合計と受取額の合計が一致することを示すことができる．提供額・受取額の秘匿が可能となり，Concealment of Amount（移転資産額の秘匿）要件を満たしている．

### 4.2　Monero の特定・追跡性

上述のように，Monero は匿名性に関する 5 項目の要件は，リング CT で使用するダミーの未使用暗号資産の数に依存する要件もあるが，一定レベル満たしている．Monero からの利用者および利用者の資産額の特定，利用者および資産の追跡は困難であり，高い匿名性が保証された暗号資産である．

一方，Monero では，現在，特定・追跡を可能とする仕組みとして，ViewKey（参照鍵）の利用が推奨されている．Monero では，利用者固有の 2 組の公開鍵暗号の鍵ペアが使用され，一方の組の秘密鍵と他方の組の公開鍵の組から構成される参照鍵（View Key）をしかるべき第三者へ提供することにより，その利用者の暗号資産の提供・受取状況や

保有状況を把握することが可能となる．この仕組みは，第三者による監査や，捜査機関・徴税機関の調査への協力等での利用が想定されている．

Monero における特定・追跡性は，利用者の意思あるいは協力の元の特定・追跡性であり，協力を得ることが難しい犯罪者や悪意のある人を対象とした場合，その実効性は乏しい．Monero における特定・追跡性は，安心・安全な暗号資産として求められる特定・追跡の機能としては不十分であろう．

## 5. Zcash

Zcash は，最も匿名性の高い暗号資産と言われている．その匿名性は，資産の移転に関わる提供者，受取者，および移転資産額等を秘匿するシールドトランザクションとしてブロックチェーンへ登録することによる．シールドトランザクションであっても，ゼロ知識証明 zk-SNARKs（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）によって，トランザクションの第三者による検証（提供者，受取者，および移転資産額等の妥当性の確認）を可能としている．

なお，Zcash では，提供者，受取者，および移転資産額等が公開されるトランスペアレントトランザクションの使用も可能であり，またシールドトランザションには，Sapling および Sprout の 2 種の仕様が存在するが，本稿では最新の仕様である Sapling によるシールドトランザクションを対象とする．

| トランザクションに関する情報 | |
|---|---|
| 資産のバランス | Saplingによる使用資産額と提供資産額の差 |
| 使用資産情報 | 使用資産の数（n） |
| | 使用資産1 |
| | ・・・・・ |
| | 使用資産n |
| 提供資産情報 | 資産提供先の数（m） |
| | 資産提供先1 |
| | ・・・・・ |
| | 資産提供先m |

| 使用資産情報（1・・n） | |
|---|---|
| 使用資産額に対するコミットメント | 使用する資産（入力ノート：$(d, pk_d, v^{old}, rcm^{old})$）で指定されている金額に対するバリューコミットメント：$cv^{old}$ |
| 使用資産内容に対するコミットメント | 使用する資産（入力ノート）で指定されている内容に対するノートコミットメント$cm^{old}$が含まれるツリーのルート：rt |
| 使用資産内容に対するユニークなコード | 使用する資産の2重使用の検査に使用するユニークなコード（ヌリファイア）：$nf^{old}$ |
| 使用資産の使用権を示すのに使用される公開鍵 | 使用する資産の使用権を示す秘密鍵askをランダマイズし生成した秘密鍵rskに対応する公開鍵：rk |
| 使用資産の使用権の証明 | $cv^{old}$、rt、$cm^{old}$、$nf^{old}$、rk、および使用する資産（入力ノート）で指定されている受取者を示すワンタイム公開鍵$pk_d$、の正当性を示す証明 |
| 使用資産情報への署名 | rskによる署名（署名検証により、使用権を示す秘密鍵askの所有を証明） |

| 提供資産情報（1・・m） | |
|---|---|
| 提供資産額に対するコミットメント | 提供する資産（出力ノート：$(d, pk_d, v^{new}, rcm^{new})$）で指定されている金額に対するバリューコミットメント：$cv^{new}$ |
| 提供資産内容に対するコミットメント | 提供する資産（出力ノート）で指定されている内容に対するノートコミットメント$cm^{new}$の位置：$cm_u$ |
| 提供資産内容暗号化時の暗号鍵生成に使用される公開鍵 | 提供資産内容（出力ノート）の暗号化のために生成された秘密鍵eskに対応する公開鍵：epk |
| 暗号化された提供資産内容 | 受取者を示すワンタイム公開鍵$pk_d$およびesk、epk等から生成した暗号鍵$K^{enc}$により暗号化された提供資産内容（出力ノートのテキスト）：$C^{enc}$ |
| 暗号化された提供資産内容の復号を可能にする情報 | $cv^{new}$、$cm_u$、$cm^{new}$、提供資産内容の復号に使用する公開鍵epk等からランダムに生成される暗号鍵ockにより暗号化された$pk_d$およびesk |
| 提供資産情報の正当性の証明 | ノートコミットメント、バリューコミットメント、暗号化された提供資産内容（出力ノートのテキスト）の復号に使用する公開鍵epk等の正当性を示す証明 |

図６　Zcash（Sapling）トランザクションを構成する情報（匿名性に関連する情報のみ）

### 5.1 Zcash の匿名性

Sapling トランザクションで構成される Zcash ブックチェーン（本稿では以下，単に Zcash と表記）の匿名性について，以下，2 章でまとめた匿名性に関する要件ごとにまとめている．なお，Zcash ではブロックチェーンに登録される情報の他，資産の移転を示すノートに対するコミットメント（note commitment）および資産の 2 重使用のチェックに使用されるヌリファイア（nullifier）を管理しており，これらの情報を含めて，ブロックチェーンの匿名性に関する要件を考察する．

**①Pseudonymity**

Zcash では，Spending Key という利用者固有の秘密鍵が乱数により生成される．その SpendingKey から多数の秘密鍵・公開鍵が生成され利用者識別情報としても利用されている．SpendingKey の生成プロセスでは利用者の情報は使用されないため，Spending Key および SpendingKey から生成される鍵群から利用者を推定するのは難しく，一定の Pseudonymity 要件を満たしている．

**②Unlinkability**

Zcash では，トランザクションで指定する受取者（利用者）は，受取者固有の Spending Key から生成される受取参照鍵 ivk により受け取りの都度生成される Diversified Transmission Key から構成される Sapling Shielded Payment Address で指定される．このように受取者として指定する利用者識別情報は毎回異なる（ワンタイムステルスアドレス）ため，ブロックチェーン上のトランザクション内に指定されている複数の利用者識別情報が同一の利用者に紐づけられていることを特定するのは困難で，Unlinkability（非連結性）要件を満たしている．

**③Untraceability between Transactions**

Zcash では，トランザクションで使用する暗号資産（入力ノート）は受取者のみが復号できるよう暗号化された状態で指定されるため，第三者はその暗号資産の提供者，受取者を特定できない．一方，第三者は暗号資産の内容を確認できなくとも，使用者が指定した暗号資産を使用する権

利を保有していること（正しい受取者であること），指定された暗号資産が未使用であることを確認できる仕組みとなっている．受取時の暗号資産の受取者と使用する暗号資産の提供者との対応の特定を困難にすることができるため，Untraceability between Transactions（トランザクション間の暗号資産/利用者の非追跡性）要件を満たしている．

**④Untraceability within Transaction**

Zcash では，前述のように第三者はトランザクションで使用する暗号資産の内容を確認できないため，受取時の暗号資産の情報（受取者や受取額）は得られず，また提供する暗号資産の情報も暗号化されているため，提供先や移転資産額の情報も得られない．

以上のように，提供者と受取者の対応の特定を困難にする仕組みにより，Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性）要件を満たしている．

**⑤Concealment of Amount**

Zcash では，既述の通り移転資産額はすべて暗号化されている．また，Pedersen Commitment の利用により，個々の資産額は秘匿されつつ，当該トランザクションで提供者が使用する暗号資産の資産額と，受取者に提供される資産額の，それぞれの合計の差額が valueBalance に格納されており，他の方式による移転資産額との合算が可能で，第三者による提供額の合計と受取額の合計の一致の検証を可能としている．

提供額・受取額の秘匿が可能であり，Concealment of Amount（移転資産額の秘匿）要件を満たしている．

### 5.2 Zcash の特定・追跡性

上述のように， Zcash は匿名性に関する 5 項目の要件をすべて満たしており，高い匿名性が保証された暗号資産であり，利用者および利用者の資産額の特定，利用者および資産の追跡は極めて困難である．

一方，現在の Zcash の特定・追跡に関しては，それぞれの利用者固有の秘密鍵 SpendingKey より生成される受取参照鍵 ivk および提供参照鍵 ovk の利用が考えられる．ivk の利用により，その利用者が受け取る資産の情報（入力ノート）を全て復号でき，受取資産の情報（提供者，移転資産額）を把握することができる．一方，ovk の利用により，受取資産の情報（入力ノート）の他，提供資産の情報（出力ノート）を全て復号でき，提供先および移転資産額を把握できる．

Ivk，ovk を利用した利用者や資産の特定・追跡機能は，第三者による監査や，捜査機関・徴税機関の調査への協力等での利用が想定されている．このような Zcash の特定・追跡性は，利用者の意思あるいは協力の元の特定・追跡性であり，協力を得ることが難しい犯罪者や悪意のある人を対象とした場合，その実効性は乏しい．Zcash も Monero と同様，その特定・追跡性は，安心・安全な暗号資産として求められる特定・追跡の機能としては不十分であろう．

## 6. Grin

Grin は 2016 年に発表された Mimblewimble プロトコルを採用し 2019 年に登場した匿名暗号資産である．Grin トランザクション情報に対する利用者の匿名性は，Mimblewimble プロトコルにより実現されている．その特徴は，Pedersen Commitment を利用した CT および CoinJoin の仕組みにより，利用者（提供者，受取者）および提供する資産の額を秘匿にしつつ，第三者による資産の移転の正当性検証を可能としていることである．Grin では，CoinJoin の仕組みを利用し複数のトランザクションをブロックに格納する際，中間的な資産のやり取り（提供ー受取）は省略（カットスルー）され，あたかも一つの大きなトランザクションのようにブロックにまとめられている．

| ブロックに関する情報 | | | |
|---|---|---|---|
| カーネル オフセット | トランザクションカーネルオフセットの合計 | | |
| 入力情報 | 入力1 | 使用する出力1 (pedersen commitment) | 使用権の証明1 (signature for commitment with blinding factor) |
| | ・・・・・・・・・・・・・・ | | |
| | 入力n | 使用する出力n | 使用権の証明n |
| 出力情報 | 出力1 | 出力コミットメント1 (pedersen commitment) | 出力の非負の証明1 (range proof of output 1) |
| | ・・・・・・・・・・・・・・ | | |
| | 出力m | 出力コミットメントm | 出力の非負の証明m |
| トランザクション カーネル情報 | カーネル1 | カーネルエクセス1 (pedersen commitment) | トランザクション署名1 (signature for transaction with kernel excess) |
| | ・・・・・・・・・・・・・・ | | |
| | カーネルk | カーネルエクセスk | トランザクション署名k |

**図 7 Grin の統合されたトランザクション（ブロック）の情報（匿名性に関連する情報のみ）**

### 6.1 Grin の匿名性

Grin トランザクション情報に対する利用者の匿名性について，以下，2 章でまとめた匿名性に関する要件ごとにまとめている．

**①Pseudonymity**

Grin では，利用者を示すアドレス，固定のアドレスはもちろん，固定のアドレスから生成されるワンタイムアドレスも存在しない．Grin では受取者を示す秘密の情報が資産の移転の都度，乱数により生成され，その秘密の情報を知っていることが受取者の証明となる．乱数から生成されるその都度の秘密の情報がアドレスと考えることもできるが，いずれにせよ秘密の情報の生成には受取者（利用者）固有の情報は使用されないため，都度生成される秘密の情報（アドレス）から利用者を特定するのは難しく，一定の Pseudonymity 要件を満たしている．

**②Unlinkability**

Grin での暗号資産の提供者，受取者は，その暗号資産額を示すデータに内蔵される秘密の情報で指定される．利用者識別情報として使用される秘密の情報は，必要の都度に乱数より生成され毎回異なるため，ブロックチェーン上の

トランザクション内に指定されている複数の利用者識別情報が同一の利用者に紐づけられていることを特定するのは困難で，Unlinkability（非連結性）要件を満たしている．

**③Untraceability between Transactions**

Grin では，提供者は受け取った資産を提供資産としてそのまま指定する．結果として，受取資産と提供資産の対応は公開されることになり，Untraceability between Transactions の要件は満たしていない．

**④Untraceability within Transaction**

Grin では CoinJoin の仕組みを利用し，提供者と受取者の対応の特定を困難にするため，ブロック内のトランザクションを統合する．また，提供額，受取額の関係からトランザクションの再構成を防ぐべく，カーネルオフセットを導入している．

以上のように，提供者と受取者の対応の特定を困難にする仕組みにより，Untraceability within Transaction（トランザクション内の暗号資産/利用者の非追跡性）要件を満たしている．

**⑤Concealment of Amount**

Grin では，移転資産額はすべて Pedersen Commitment の利用により，個々の資産額は秘匿されつつ，当該ブロックで提供者が使用する暗号資産の資産額と，受取者に提供される資産額の，それぞれの合計の差額がカーネルオフセットに格納されており額との一致により，第三者による提供額の合計と受取額の合計の一致の検証を可能としている．

提供額・受取額の秘匿が可能であり，Concealment of Amount（移転資産額の秘匿）要件を満たしている．

### 6.2 Grinの特定・追跡性

Grin ブロックチェーンの匿名性は，匿名性要件の③の Untraceability between Transactions を満たしていないが，それでもかなり高い匿名性が保証された暗号資産であり，利用者および利用者の資産額の特定，利用者および資産の追跡は極めて困難である．

なお，Grin のブロックチェーン/トランザクションには，特定･追跡の仕組みは用意されていない．資産移転の都度，移転資産額のデータに受取者を示す利用者識別情報（乱数により生成される秘密の情報）が内蔵される．この秘密の情報を提供することにより，提供資産額，受取資産額を第三者が確認可能となるが，未使用資産の場合，第三者に使用されてしまうリスクも発生し，第三者への提供は難しい．Grin では，安心・安全な特定・追跡性のための仕組みの導入は当面は行わないようであるが，安心・安全な暗号資産として求められる特定・追跡の機能への対応は将来必要となろう．

## 7. おわりに

**(1)匿名暗号資産のブロックチェーンの匿名性**

代表的な匿名暗号資産 Monero（RCTTypeSimple），Zcash（Sapling），Grin のブロックチェーン/トランザクションはいずれも高い匿名性であることを確認した．その中でも Zcash（Sapling）が最も匿名性が高く，Monero（RCTTypeSimple），Grin，の順に匿名性が高い，と考えられる．

しかし，暗号資産システムの匿名性は，資産の移転結果を示すブロックチェーン/トランザクションのみならず，暗号資産システムを利用する様々の局面で必要となるプロセスにおける匿名性にも依存している．実際，暗号資産システムアクセスのためのネットワーク接続時の情報を利用した匿名性への攻撃が試みられている．今回の調査の対象外ではあるが，ネットワーク利用時の匿名性を高める技術として，Tor，Loki，Dandelion 等が提案されている．暗号資産システムとしての匿名性の検討においては，暗号資産システムを利用する様々の局面で必要となるプロセスにおける匿名性の検討が必要である．

**(2)匿名暗号資産のブロックチェーンの特定・追跡性**

代表的な匿名暗号資産 Monero（Sapling），Zcash（RCTTypeSimple），Grin のブロックチェーン/トランザクションの特定・追跡性に関する仕組みは，皆無またはごく限られた機能の仕組みに限られているのが現状である．

特に Grin については，その特徴機能であるカットスルーにより，ブロック内での提供，受取でクローズしている出力情報，入力情報は完全にブロックチェーンから抹消され，資産の移転が記録されないことになる．このことは，監査や不正･不法な取引の追跡を困難にすることが懸念される．

安心・安全な暗号資産システムとしては，確実な匿名性と共に，暗号資産に関する監査性や不正・不法な利用の抑止のための，確実な特定・追跡性の仕組みの提供が必要であろう．

既に，匿名性と特定・追跡性の両立に向けた仕組みや仕組みを組み込んだ暗号資産も提案され始めてはいるが，多くの主要な暗号資産では未だ構想段階である．今後，社会のコンセンサスを得ながら，匿名性と特定・追跡性の両立に向けた仕組みの更なる研究開発が展開され，安心・安全な暗号資産の早期の実現・普及が期待される．

**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.

[2] 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.

[3] 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.

[4] 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”, 2001.
https://bitcoin.org/bitcoin.pdf

[6] All Cryptocurrencies
https://coinmarketcap.com/all/views/all/

[7] Top 28 Best Privacy Coins 2018
https://kingpassive.com/best-privacy-coins-2018/

[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] Nicolas van Saberhagen, ″CryptoNote v2.0″, 2013.
https://cryptonote.org/whitepaper.pdf

[13] Adam Back, “bitcoins with homomorphic value (validatable but encrypted)”, 2013.
https://bitcointalk.org/index.php?topic=305791.0

[14] Greg Maxwell, ″Confidential Transactions″, 2016.
https://people.xiph.org/~greg/confidential_values.txt

[15] Gregory Maxwell, Andrew Poelstra,” Borromean Ring Signature”, 2015.
https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf

[16] SHEN NOETHER,“RING CONFIDENTIAL TRANSACTIONS”, 2015.
https://eprint.iacr.org/2015/1098.pdf

[17] 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

[18] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova, “Pinocchio: Nearly Practical Verifiable Computation”, 2013.
https://eprint.iacr.org/2013/279

[19] Andrew Poelstra, “Mimblewimble”, 2016.
https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf

[20] Gregory Maxwell, “CoinJoin: Bitcoin privacy for the real world”, 2013.
https://bitcointalk.org/index.php?topic=279249.0

[21] Daniel Wilczynski, “Greg Maxwells Roadmap for Bitcoin Scaling”, 2015.
http://www.danielwilczynski.com/maxwells-scaling-roadmap

[22] 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

[23] Christina Garman, Matthew Green, Ian Miers,“ Accountable Privacy for Decentralized Anonymous Payments”, 2016.
https://eprint.iacr.org/2016/061.pdf