暗号資産Moneroの匿名性を支える技術

花村 直親[1]

,

概要：匿名性を主たる特徴とした暗号資産である Monero について、匿名性を実現する手法と解決するプライバシー課題に基づいた分類と調査を行った。まず暗号資産におけるプライバシー課題を分類し、次に各プライバシー課題に Monero が対応する匿名性機能の分析を行うことで Monero の解決する課題を定義した。最後に匿名性の実現手法について、組み合わされた技術要素を分解することで Monero が匿名性を実現している方法を検討した。

キーワード：Monero, 暗号資産、匿名性、リング署名

Privacy Enhancing Technology in Monero

Naochika Hanamura[1]

,

Abstract: This work examines privacy method and privacy issues Monero, which is crypto asset whose main feature is anonymity. First, we classify privacy issues in crypto assets. Second, we defined privacy issues which Monero would solve by analyzing the anomynity function that Monero corresponds to each privacy issue. Finally, we considered the method which Monero realizes anonymity, by decomposing the combined technical elements.

Keywords: Monero, Cryptoassets, Privacy, Ring Signature

1. はじめに

ブロックチェーン技術は暗号資産を支えるテクノロジーとして広く注目を集めている。ブロックチェーンは不特定多数の参加者がいる状態においても動作するシステムとして、Bitcoin[1] のアイデアと共に発表された。

Bitcoin は 2009 年に稼働してから年々多くの人がネットワークに参加して価値を増やし、暗号資産の時価総額を掲載しているサイトである CoinMarketCap[*1]によると 2.2 兆ドル以上の時価総額を持つようになった。Bitcoin 以外にも Litecoin[*2]、Ethereum[*3]など多くのブロックチェーンが存在しており、決済に使いやすくすることを目的にしたものや、チューリング完全性のあるプログラムをブロックチェーン上で動かすスマートコントラクト機能を用いているものなど、Bitcoin とは異なる課題に対応している。Bitcoin の持つ課題の 1 つにプライバシーの問題がある。Bitcoin はアドレスやトランザクションが透過的であり、取引の履歴が参加者から見えているため、アドレス間の関係性が判明する手がかりとなる。例えば、1 つのアドレスの所持者が判明した場合、そのアドレスと取引のあるアドレスについて、その所持者と関係や取引関係のある人間であることが推測できてしまう。このようなプライバシーの課題を解決するためにトランザクションが匿名性を持つ

[1] naomasabit@gmail.com

[*1] https://coinmarketcap.com/ 2022 年 1 月閲覧

[*2] https://litecoin.org/

[*3] https://ethereum.org/en/

暗号資産として Monero[*4]が存在する。

Monero は Bitcoin をベースにプライバシー問題に対応した暗号資産としてコンセプトが発表され [2] 開発された。執筆時点における Monero の時価総額は 41 億ドルになる。CoinMarketCap[*5]によると、掲載されている 6500 以上の暗号資産の中で 42 位の市場規模で、これは Zcash[*6]や Grin[*7]など、匿名性を持つ暗号資産の中でも最大の市場規模である。

Monero はアドレス間取引に関わる項目について匿名化を施し、アドレス間の関係性が推測されないようにしている。これにより、取引の当事者以外にはどのアドレスとの取引や取引金額は秘匿しながら、正しく暗号資産が送金されたことの検証は行えるようにしている。

しかし、匿名性を持つ暗号資産は、脱税や、犯罪取引に利用される社会問題も存在している。2020 年にはランサムウェアの Sodinokibi の運営するグループは、匿名性の高い手段として、要求する身代金の支払手段に Bitcoin から Monero を変更した[*8]。また、2020 年にはアメリカ内国歳入庁が、匿名性を持つ暗号資産は不法行為に使われる主要な手段となりつつあり、Monero のトランザクションを追跡するためのツールを公募した。[*9] 日本国内においては、一時期匿名性を持つ暗号資産が暗号資産取引所で扱われていたが、マネーロンダリングなどの懸念を背景に、業界団体の自主規制によって現在は取り扱われていない。

匿名性を持つ暗号資産について、プライバシーの側面と悪用される脅威の側面について理解し、脅威を緩和するための方法を考えるためには、技術の課題、限界、発展してきた軌跡を理解することが必要である。本調査では早くから匿名性に着目し、暗号資産の中でも時価総額が最大規模にまで広がった Monero について、(1)Monero が担保する匿名性の性質、(2)Monero が匿名性を技術的に担保している手法、(3)Monero が匿名性を発展させてきた方法と歴史、の理解を提供することを目的とする。

1.1 貢献

本レポートでは、以下の貢献を行った。

- ブロックチェーンにおけるプライバシー課題を整理し、Monero が採用している技術による解決策と紐付ける分析を行った
- Monero が匿名性を技術的に担保している手法を整理した
- Monero が採用している技術の変遷について整理した

1.2 レポートの構成

本レポートでは、第 2 章で Bitcoin の概要と、暗号資産におけるプライバシー課題を体系的に整理し、Monero の解決するプライバシー課題を分析する。第 3 章では、送金アドレス、着金アドレス、送金額の匿名化についてそれぞれ詳説を行い、Monero がどのように匿名化を実現しているかを述べる。最後に、第 4 章では本レポートで触れた内容をまとめる。

2. 暗号資産におけるプライバシー課題の定義と Monero における解決手法の分析

2.1 Bitcoin の概要とプライバシー側面

Bitcoin は Nakamoto[1] によって 2008 年に発表され、2009 年 1 月 3 日より動作しているピア・ツー・ピアネットワーク上で動作する通貨システムである。Bitcoin は、簡単にはコインの所有者から次の所有者への取引の連鎖と捉えることができる。Bitcoin ネットワークへの参加者は署名鍵とペアになるアドレスと呼ばれるフォーマット化された公開鍵を持つ。アドレスからの送金指示はトランザクションと呼ばれ、各トランザクションにおいて、コインの所有者は送金のために、所有アドレスに対応する署名鍵を使用して、コインを受け取ったトランザクションのハッシュと次の所有者の公開鍵に署名を行う。所有者は署名鍵で署名を行ったトランザクションをネットワーク上に放流する。

また、Bitcoin では所有者が送金したコインを再度送金しようとした場合、どの取引が先に行われたかを判断することで二重支払を防ぐことができる。マイニングと呼ばれる計算プロセスによってトランザクションはブロックにグループ化され、ブロック内に含まれるトランザクションにタイムスタンプが付与され、取引の有効性を証明する役割を果たす。ブロックはそれ自体が連鎖構造を持ち、各ブロックは前のブロックを参照することで、前のブロック中のトランザクションの有効

[*4] https://www.getmonero.org/
[*5] https://coinmarketcap.com/ 2022 年 1 月閲覧
[*6] https://z.cash/
[*7] https://grin.mw/
[*8] https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-to-stop-taking-bitcoin-to-hide-money-trail/
[*9] https://beta.sam.gov/opp/3b7875d5236b47f6a77f64c19251af60/view

性を強化する。このプロセスにより、ブロックチェーンと呼ばれる構造が生成され、ネットワークの参加者はブロックに含まれるトランザクションを全て参照することができる。

即ち、アドレス間のトランザクションは公開されており、取引履歴の追跡検証が可能な状態になっている。また、アドレス自体は仮名 (Pseudonym) 化されており、実世界のアイディンティティと結びついていない。しかし、アドレスは往々にしてコインの着送金のため、インターネットなどを通じて所有者によって公開される。ネットワークに公開されているトランザクション情報を基に各アドレスについて分析し、アドレスの所有者のアイデンティティを組み合わせればアドレス間の関連性や取引の活動を把握することができるという研究結果が報告されており [3][4][5]、Bitcoin の仮名性だけでは匿名化に不十分であることが示されている。

2.2 暗号資産におけるプライバシー課題の定義

本項では暗号資産におけるプライバシー課題について確認する。Feng らはブロックチェーン上のプライバシーとしてアイデンティティのプライバシー（Identity Privacy)、取引のプライバシー（Transaction Privacy）の 2 つを提唱している [6]。アイデンティティのプライバシーは、アドレスと所有者のアイデンティが結びつかないことの保証である。Bitcoin のように暗号資産アドレスが仮名化されていても、取引の振る舞いなどからアドレス所有者やその属性を推測可能である。例えば一部の暗号資産取引所の送金アドレスは複数人の暗号資産をまとめて保管している。まずその取引所のユーザーとなって出金指示を行うことで出金トランザクションを辿れば取引所の出金アドレスを特定できる。その出金アドレスとトランザクションを送り合っているアドレスを探せば、その暗号資産取引所が所有権を持つ可能性のあるアドレスを芋づる式に推測できる。取引のプライバシーは、トランザクションの内容が取引関係者以外に知られないことである。取引金額、取引の頻度、取引相手についてその取引関係者以外から把握できないことである。Bitcoin のようにトランザクションが透過的であると、取引金額、取引の頻度、取引の当事者について第三者から把握できてしまう。

Feng らの提案したプライバシー課題の他に、暗号資産においてはトランザクション経路のプライバシー課題が存在する。アイデンティティのプライバシーと取引のプライバシーが保たれていても、トランザクション経路が公開されていると、経路を辿ることでコインの取得元を辿ることができる。もし、あるコインの過去の取引の性質が判明すると、現在のコインにおいても過去の取引の影響を受ける事が生じる。これは、ブロックチェーン上の暗号資産において重要な性質を表すどのコインも等価であるという性質 (Fungibility) が保証されない。

また、この性質を利用して、経路に問題のあるコインを大量のアドレスに散布する事でブロックチェーンのネットワーク自体を汚染し暗号資産の価値を既存させる攻撃なども考えられる。Monero の性質を表すにあたってトランザクション経路のプライバシーは重要な性質を表すことから、Feng らの定義に加えて本レポートではこれもプライバシー課題として扱う。

Monero の開発コミュニティでは、送金手段として Bitcoin を利用する場合、匿名性がない事が問題になる事例があると指摘している。[7]

Monero によって例示されている Bitcoin のプライバシーが問題になる事例について、上記 3 つの課題分類に当てはめると以下のようになる。

アイデンティティのプライバシーが問題になる事例

- Bitcoin を送金手段として利用するとき、取引相手がトランザクションを追うとアドレスと残高が知られることになり、取引相手が多額の残高を狙っていた場合襲われる可能性がある。

これは実際の取引に Bitcoin を利用した際、アドレスと使用者が紐づいてしまうアイデンティティのプライバシーに該当する問題である。匿名性の観点においては実際の取引に利用する際にアドレスと使用者が紐づかないことが望ましい。

取引のプライバシーが問題になる事例

- ビジネスを営んでおり、取引先にアドレスを指定して支払いを依頼する場合を考える。取引先は指定された受取アドレスから相手がどれくらいの残高を持つかを確認でき、交渉材料にすることができる。また、Bitcoin のアドレスで今までに受け取ったすべての他の支払いを見ることができるので、他業者との価格交渉を見ることができ、交渉を有利に進められる。

これは公開されているアドレスから取引の当事者以外にも過去の取引が判明してしまう、取引のプライバシーに関わる問題に該当する。こちらも取引の当事者以外に取引詳細が判明しない事が実際の利用においては望ましい。

トランザクション経路のプライバシーが問題になる事例

- 自分がビジネスで販売していて代金として Bitcoin を受け取った時に、取引相手が犯罪活動に関わっていた場合、犯罪者への資金提供といういわれのない疑いを受ける可能性がある。

Bitcoin においては、トランザクション経路の関係性が秘匿されていない以上アドレス間を辿っていくことでコインの入

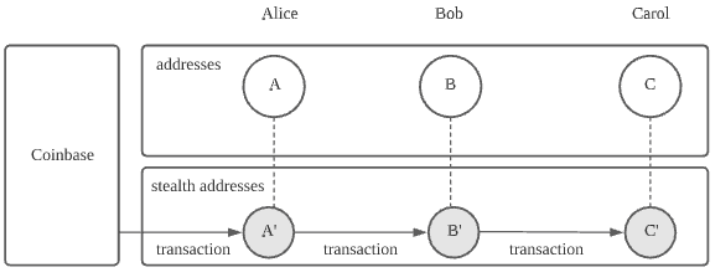

図 1　ステルスアドレスを用いるトランザクションの遷移

手経路を把握できる。これは、過去の取引のトランザクションが犯罪行為によって得られたものであることが判明した場合、受け取り手に特に落ち度がなくとも、入手経路によって現在の取引とコインの価値が影響を受けるという問題に該当する。また、過去に犯罪者に利用されたコインとその他のコインは同価値ではなくなる Fungibility への影響を示唆している。

これらのように取引のプライバシー、アイデンティティのプライバシー、トランザクション経路のプライバシーに対して Monero が課題視し、対応する機能を実装している。ただし Monero はプライバシーの課題について触れているが、第三者から取引の内容や関係者への検閲性は下がり、犯罪取引への利用が行われやすくなる副作用については触れていないことには注意が必要である。本来はプライバシーを確保しつつ、犯罪取引が起きた時などに身元の検証を行えるプロトコルの提案など、プライバシーを強化することの副作用への対応が望ましい。

2.3　Monero のプライバシー課題に対応する機能の分析

前節で暗号資産で取引のプライバシー課題、アイデンティティのプライバシー課題、トランザクション経路の課題がある事を確認した。Monero はこれらの課題について、以下 3 つの技術で対応している。

- 着金者の情報と取引に関与したアドレスを秘匿するステルスアドレス
- 送金者の情報とトランザクション経路を秘匿するリング署名
- 送金額を秘匿する Confidential Transaction

前節で取り上げたプライバシー課題との対応を分析した結果を表 1 に整理した。本節では、それぞれの対応機能を概観し、プライバシー課題に対応している方法を確認する。

表 1　Monero の課題対応する機能

プライバシー課題	対応機能	対応手法
取引のプライバシー（着金者）	ステルスアドレス	ダミーのアドレスを用意して取引に関与した本物のアドレスを秘匿する
取引のプライバシー（送金者）	ステルスアドレス	ダミーのアドレスを用意して取引に関与した本物のアドレスを秘匿する
取引のプライバシー（送金者）	リング署名	送金用の署名をしたアドレスを隠蔽する
取引のプライバシー（送金タイミング）	リング署名	送金の流れを秘匿する
取引のプライバシー（送金額）	Confidential Transaction	ダミーの金額を用意して送金額を秘匿する
アイデンティティのプライバシー	ステルスアドレス	ダミーのアドレスを用意して取引に関与した本物のアドレスを秘匿する
トランザクション経路のプライバシー	リング署名	トランザクションの送金の流れを秘匿する

ステルスアドレス

ステルスアドレスは、着金者に対しダミーのアドレスを用意して取引に関与した本物のアドレスを秘匿するアイデアとして発表された [2]。送られたコインが次に送金される時には着金者のステルスアドレスからであるため、結果的に着金者のアドレスに加えて送金者のアドレスも秘匿される。

図 1 はステルスアドレスを用いて、Alice、Bob、Carol のアドレスをトランザクションが遷移していく状況を表している。まず Alice がマイニングを成功した報酬は Coinbase から Alice のダミーのステルスアドレスに払い出される。次に Alice は Bob のダミーのステルスアドレスを用意して送金先に指定する。Bob も同様に Carol のダミーのステルスアドレスを用意して送金先に指定する。トランザクションの送金先にダミーのアドレスを経由することで、本当の着金アドレスはネッ

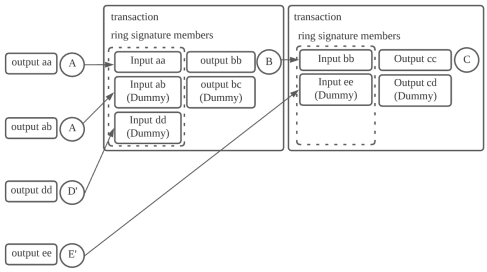

図 2 リング署名を用いるトランザクションの遷移

トワークに秘匿される。Monero のホワイトペーパーでは送金者を隠蔽することを主眼に置いた技術として提案されているが、実際にはダミーの着金アドレスから送金されるため送金者、着金者情報共に秘匿される。

リング署名

Monero で送金者の匿名性を担保する手法としてリング署名が利用される。リング署名は Rivest らによって提案され [8]、複数の公開鍵を持つ参加者がいることによって管理者なしに署名者を秘匿することができる。リング署名には多くの派生系が存在するが、初期の Monero では藤崎らの Traceable Ring Singature[9] を活用している。

送金者が送金毎にダミーの秘密鍵と公開鍵を作成し、リング署名を行うことで送金元のアドレスと送金コインに該当する UTXO を秘匿する。ステルスアドレスで送金者、着金者は秘匿できるがコインの送金履歴自体は秘匿されない。また、コインの送金時に、ある所有者の複数の UTXO が同時に利用されるケースがある。トランザクション自体は公開されているため、同時に動いた複数の UTXO は同じ所有者であるという関係が推測されてしまう。また、ステルスアドレスだけではどの UTXO が送金されたかは公開されているが、ワンタイムリング署名で送金 UTXO を秘匿するため、送金タイミングを秘匿して取引のプライバシー課題に対応することが可能である。

図 2 はリング署名を用いて、A,B,C の順に送金をしていく様子を表している。トランザクションは Input,Output の集合として表される。A は output aa を用いて、B に output bb として送金する。その際、この送金に関係ない output ab と D のステルスアドレスが持つ output dd をダミーの input として混ぜ、D のステルスアドレスの公開鍵をリング署名のメンバーとし、output にもダミーの output bb として混ぜる。B が C に送金する際も、同様に E のステルスアドレスの公開鍵をリング署名のメンバーとし、C への output cc、ダミーの output cd を作る。C の output cc の送金元を追おうと試みると、実際には aa → bb → cc の流れだが、ab → bb → cc, dd → bb → cc, ee → cc の経路も存在し、経路が難読化される。これはリング署名のメンバーが多ければ多いほど経路が難読化される。これによって犯罪利用歴のあるコインを偶然受け取った場合など、送信経路によって価値が毀損されるという Fungibility の問題に対応できる。

Monero では当初 Traceable Ring Singature[9] を用いた署名をワンタイムリング署名と名付けて採用していたが、2017 年 10 月のアップグレードで MLSAG と呼ばれるリング署名を考案し利用するようになった [10]。MLSAG の詳細は 3.2.2 項にて述べる。

Confidential Transaction

Confidential Transaction は、Maxwell によって提案された、送金額をネットワークに秘匿したまま着金者に伝える手法である [11]。Pedersen Commitment を暗号資産の送金に応用した手法で、。送金額を秘匿する事で取引のプライバシー課題に対応できる。

Confidential Transaction は当初の Monero には組み込まれておらず、2017 年 10 月のアップデートで Monero に導入された。Confidential Transaction は、当初 Monero に採用されていたワンタイムリング署名にそのまま適用すると、送金者の匿名性が失われるおそれがあったことから、リング署名手法を MLSAG として刷新し、RingCT(Ring Confidential Transactions)[10] と呼ばれる複合技術として導入された。

次章では、各プライバシー課題に対応する手法を実現する詳細について述べる。

3. Monero における匿名性の実現手法

2 章では Monero が暗号資産におけるプライバシー課題に対応するアプローチを分析検討した。本章では実現手法の詳細について述べる。

3.1 ステルスアドレス

ステルスアドレスは Monero はユーザがアドレスを公開しながらも、着金元・送金先との結びつけが不可能な送金を可能にする手法である。ステルスアドレスは、一度限りの使い捨てアドレスを経由することによって実現する。本節では具体的にステルスアドレスがどのように動作するかを Alice が Bob に送金したい場合を例に取り検討する。

Monero の仕様として公開鍵、秘密鍵は view key,spend key というそれぞれの鍵の組み合わせ、計 4 つの鍵で表現される。また、署名手法は EdDSA[12] を利用している。Bob の公開鍵は (A, B) の組み合わせとなる。本節で出てくる用語を以下のように定義する。

- G: EdDSA のベースポイント;
- A: Bob の view key の公開鍵
- B: Bob の spend key の公開鍵
- a: Bob の view key の秘密鍵
- b: Bob の spend key の秘密鍵
- H_s: ハッシュ関数
- r: Alice が計算するランダムな数値。ステルスアドレスの鍵のシードとなる
- x: Alice が r から計算するステルスアドレスの秘密鍵
- P: Alice が r から計算するステルスアドレスの公開鍵

(1) Alice は送金先である Bob の公開鍵 (A, B) を確認する

(2) Alice はランダムな数字 r を作成し使い捨ての秘密鍵とし、Bob の公開鍵 (A, B) と組み合わせて宛先のステルスアドレスの公開鍵 $P = H(rA)G + B$ を計算する。

(3) Alice は宛先ステルスアドレスの公開鍵 P を宛先のキーとして扱い、$R = rG$ をトランザクション内に包含する。R は r に対する公開鍵の関係性にあたる。

(4) Alice は宛先がステルスアドレス P としたトランザクションを送る。トランザクションには使い捨ての公開鍵 R が内包されている。

(5) Bob は、自分の秘密鍵 (a, b) を用いて全てのトランザクションを検証し、$P' = H_s(aR)G + B$ を計算する。もし Bob が宛先であるトランザクションがあった場合、$aR = arG = rA$ であるため $P' = P$ が成り立ち、受取人が自身であることを証明できる。各等式についての理由は以下に示す。

(a) $aR = arG$ について。 R は Bob の秘密鍵の一部 a とランダム数 r とベースポイント G を掛け合わせた数値であり、R は rG に等しいため成り立つ。

(b) $arG = rA$ について。 aG は Bob の秘密鍵 a とベースポイント G の掛け算の数値であり、Bob の公開鍵 A と等しい。そのため、arG は rA に等しい。

(c) $P' = P$ について。 $P' = Hs(aR)G + B$ で、$P = Hs(rA)G + B$ であり前式 a,b より $aR = arG = rA$ であるため、$P' = P$ となる。

(6) ステルスアドレスの公開鍵は $P = H_s(rA)G + B$ であることから、ステルスアドレスの秘密鍵 x は $P = xG$ より、$x = H_s(aR) + b$ となる。即ち、Bob の秘密鍵 (a, b) を用いて x は計算できる。Bob は計算された x を使ってトランザクションに署名することで、受け取ったコインを使うことができる。

上記よりランダム値 r と Bob の公開鍵 (A, B) より、ステルスアドレスの公開鍵 P、秘密鍵 x は定義される。ブロックチェーン上に残る送金記録は使い捨てのステルスアドレス P に送ったもので、本来の着金者である Bob のアドレス (A, B) は秘匿されることとなる。

3.2 リング署名

トランザクション経路のプライバシー課題、送金タイミングのプライバシー課題に対応するためにリング署名を Monero は実装している。Monero に利用されているリング署名は変遷しており、本節では、初期の Monero が利用していたワンタイムリング署名、RingCT の導入によって刷新された MLSAG について解説する。

3.2.1 ワンタイムリング署名

Traceable Ring Signature[9] を基にしたワンタイムリング署名プロトコルを Monero は実装している。ワンタイムリング署名は、（GEN、SIG、VER、LNK）の 4 つのアルゴリズムで実施され、本項ではそれぞれのアルゴリズムを確認する。

- GEN アルゴリズム: ステルスアドレスの仕組みで見たように、送金者はランダムな数字である使い捨て秘密鍵 $x \in [1; l-1]$ と、x に対応する公開鍵 $P = xG$ を用意する。G はベースポイントのため公開パラメータである。さら

に送金者はキーイメージ $I = xH_p(P)$ を計算する。このキーイメージ I は、二重送金を防ぐために LNK アルゴリズムで用いる。

- SIG アルゴリズム: メッセージ m、公開鍵 $\{P_i\}_{i \neq s}$ のセット S', ペア (P_s, x_s) から、署名 δ と集合 $S = S' \cup \{P_s\}$ を生成する。送金者は、署名のために他のユーザの公開鍵群 P_i のうちから n 個のサブセット S'、自分の秘密鍵、公開鍵ペア (x, P) および キーイメージ I を選択する。$0 \leq s \leq n$ であり送金者の秘密鍵のインデックスが s とする（その公開鍵は P_s と表す)。署名者はランダムな $\{q_i | i = 0...n\}$ と、$\{w_i | i = 0...n, i \neq s\}$ を $(1...l)$ から取り、次の変換を行う。

$$L_i = \begin{cases} q_i G, & (i = s) \\ q_i G + w_i P_i, & (i \neq s) \end{cases} \tag{1}$$

L_i はランダムなパラメータ q_i が用いて計算され、自身以外のインデックスについては公開鍵情報を用いて計算されている。

$$R_i = \begin{cases} q_i H_p(P_i), & (i = s) \\ q_i H_p(P_i) + w_i I, & (i \neq s) \end{cases} \tag{2}$$

R_i はランダムなパラメータ q_i と公開鍵 P_i を用いて計算され、自身以外のインデックスについては公開鍵 P_i と I 情報も用いて計算されている。次のステップでは、非対話型ゼロ知識証明の課題を計算する。メッセージ m と、計算した L_i と R_i の配列をハッシュ化したものを c とする。式で表すと $c = H_s(m, L_1, ...L_n; R_1...R_n)$ となり、その後、署名者は以下の変換を行う。

$$c_i = \begin{cases} w_i, & (i \neq s) \\ c - \sum_{i=0}^{n} c_i \bmod l, & (i = s) \end{cases} \tag{3}$$

$$r_i = \begin{cases} q_i, & (i \neq s) \\ q_s - c_s x \bmod l, & (i = s) \end{cases} \tag{4}$$

結果の署名は $\delta = (I, c_1, ..., c_n, r_1, ...r_n)$. となる。

- VER アルゴリズム: メッセージ m、セット S、署名 $\delta = (I, c_1, ..., c_n, r_1, ...r_n)$ から、署名を検証して真偽を判定する。検証者は L'_i と R'_i を計算し、それぞれ L_i と R_i と一致するか検証する。

$$\begin{cases} L'_i = r_i G + c_i P_i, \\ R'_i = r_i H_p(P_i) + c_i I, \end{cases} \tag{5}$$

以下は検証プロセスである。$L'_i = L_i$ が成立することを以下に示す。
$i = s$ の場合、 (1), (2) より

$$\begin{aligned} L_i &= L'_i \\ q_i G &= r_i G + c_i P_i (\because L_i = q_i G, L'_i = c_i P_i) \\ (q_i - r_i) G &= c_i P_i \\ (q_i - q_i + c_i x) G &= c_i P_i (\because r_i = q_i - c_i x) \\ c_i x G &= c_i P_i \\ c_i P_i &= c_i P_i (\because xG = P) \end{aligned}$$

$i \neq s$ の場合、

$$\begin{aligned} L_i &= L'_i \\ q_i G + w_i P_i &= r_i G + c_i P_i (\because L_i = q_i G + w_i P_i, L'_i = r_i G + c_i P_i) \\ q_i G + w_i P_i &= q_i G + w_i P_i (\because c_i = w_i, r_i = q_i) \end{aligned}$$

となり、$L'_i = L_i$ が成立し、
次に、$R'_i = R_i$ が成立することを以下に示す。$i \neq s$ の場合、

$$
\begin{aligned}
R_i &= R'_i \\
q_i H_p(P_i) + w_i I &= r_i H_p(P_i) + c_i I (\because R_i = q_i H_p(P_i) + w_i I, R'_i = r_i H_p(P_i) + c_i I) \\
q_i H_p(P_i) + w_i I &= q_i H_p(P_i) + w_i I (\because c_i = w_i, r_i = q_i)
\end{aligned}
$$

で等式は成立する。
$i = s$ の場合、(6) より

$$
\begin{aligned}
R_i &= R'_i \\
q_i H_p(P_i) &= r_i H_p(P_i) + c_i I (\because R_i = q_i H_p(P_i), R'_i = r_i H_p(P_i) + c_i I) \\
(q_i - r_i) H_p(P_i) &= c_i I \\
(q_i - r_i) H_p(P_i) &= c_i x H_p(P) (\because I = x H_p(P)) \\
(q_i - q_i + c_i x) H_p(P_i) &= c_i x H_p(P_i) (\because r_i = q_i - c_i x) \\
c_i x H_p(P_i) &= c_i x H_p(P_i)
\end{aligned}
$$

で等式は成立する。よって、VER アルゴリズムにおいては公開パラメータ c_i, r_i, c, G, P_i から、署名者しか知らない非公開情報である q_i 、w_i から作られた R_i、L_i の検証を行える。次に、検証者は LNK アルゴリズムを実行する。

- LNK アルゴリズム:$L = \{I_i\}$ と、キーイメージの集合を L とおく。キーイメージ I が過去の署名で使用されていないかどうか（L に存在しないか）を確かめる。暗号通貨の世界においては、トランザクションの再利用をしていないことを確かめるのが二重送金を防ぐ手段となる。Monero において、自身の残高証明は自身の秘密鍵によって行われるが送金はワンタイム秘密鍵 x によって行われる。ワンタイム秘密鍵は使い捨てで二度使われないため、ワンタイム秘密鍵 x に対応するアドレス P から送ることができるトランザクションは 1 度だけで I は一度しか使われない。L にすでに I があることは、同じワンタイム秘密鍵で x で 2 つ以上の署名が作成されたことを意味し二重送金と見なされる。

3.2.2 Multilayer Linkable Spontaneous Anonymous Group（MLSAG）

初期の Monero では上記ワンタイムリング署名を送金者の秘匿方法として用いていたが、Linkable Spontaneous Anonymous Group（LSAG）[13] を基にした Multilayer Linkable Spontaneous Anonymous Group（MLSAG）を導入した。

LWW の LSAG では、署名者が識別不能である匿名性 (Anonymity), 同一の署名者による署名がリンク可能であるリンク性（Linkability）、署名者がグループメンバーの協力がなくとも署名可能である自発性（Spontaneity）をそろえたリング署名である。リングメンバーを n 人の時、$n-1$ 個の公開鍵と、署名者の秘密鍵、公開鍵各々 1 つずつでリングを作る。公開鍵は署名者が自発的に選択できる。リングを形作る公開鍵セットのハッシュ値と署名者の秘密鍵からキーイメージを作成し、キーイメージを用いることで、同一の公開鍵セットを使った署名同士について、同じ署名者が署名していることのリンクを検証できる。Back によって、Traceable Ring Signature[9] の代わりに LSAG を利用できることが指摘され [14]、Monero のリング署名への利用が模索された。

MLSAG は LWW の LSAG に改良を加えて応用している。まず、LWW の LSAG はキーイメージをリングを形作る公開鍵セットのハッシュ値から取得しているが、MLSAG では署名者の秘密鍵からキーイメージを生成するようにしている。[14] 署名者の秘密鍵からキーイメージを生成することで、ワンタイムリング署名で見たように二重送金の検証として利用することができる。また、LSAG では 1 参加者につき 1 つの公開鍵だったが、1 参加者につき m 個の公開鍵を持ってリンクする。これによって、後述する RingCT における Confidential Transaction の導入に利用できる。

MLSAG では、n 人の署名者が m 個の鍵をそれぞれ持つ。署名者の署名鍵を $x_j (1 \leq j \leq m)$ とし、ランダムな数値 α_j、リング参加者数 n 人にそれぞれ m 個分のダミー公開鍵 $\{P_i^j\}_{i=1,...,n}^{j=1,...,m}$, ランダムな数値 $s_i^j (j = 1, ..., m, i = 1, ..., \hat{\pi}, ...n)$ を用意する。これらを用いた MLSAG の署名方法を以下に述べる。
(1) π を署名者のインデックスとおき $L_\pi^j = \alpha_\pi^j G, R_\pi^j = \alpha_\pi^j H_p(P_\pi^j)$ を計算する $(1 \leq j \leq m)$

(2) 次に L_π^j, R_π^j から $c_{\pi+1} = H(m, L_\pi^1, R_\pi^1, ..., L_\pi^m, R_\pi^m)$ を計算する
(3) $c_{\pi+1}$ をもちいて $\pi+1$ 番目について、$L_{\pi+1}^j = s_{\pi+1}^j G + c_{\pi+1} P_{\pi+1}^j$, $R_{\pi+1}^j = s_{\pi+1}^j H_p P_{\pi+1}^j + c_{\pi+1} I_j$ を計算する
(4) 2 同様に $L_{\pi+1}^j, R_{\pi+1}^j$ から c_{j+2} を計算する
(5) 3 同様に $c_{j+2}, s_{j+2}, P_{j+2}, I$ から L_{j+2}, R_{j+2} を計算する
(6) 4,5 を繰り返して $L_{\pi+n-1}^j, R_{\pi+n-1}^j, c_\pi$ まで計算したら、s_π^j を $s_\pi^j = \alpha_\pi^j - c_\pi x_j modl$ となるように調整する。(l は ed25519 の定数である素数。)
(7) 最終的な署名内容を $(I_1, ...I_m, c_1, s_1^1, s_1^m, ..., s_n^1, ..., s_n^m)$ としてまとめる

図 3 は MLSAG の計算過程を表現したもので、リング状の署名になっていることがわかる。Monero ではこの MLSAG をリング署名に用いることで、送金者の匿名性を担保し、後述する RingCT における Confidential Transaction の導入に適用させている。

手順 6 で計算した s_π^j が、手順 1 で計算した L_π^j, R_π^j になるための等式変換を式 3.2.2, 式 3.2.2 に示す。

$$
\begin{aligned}
L_\pi^j &= s_\pi^j G + c_x P_x^j \\
L_\pi^j &= (\alpha_\pi^j - c_\pi x_\pi modl) G + c_\pi P_\pi^j \\
L_\pi^j &= \alpha_\pi^j G - c_\pi x_\pi modl G + c_\pi P_\pi^j \\
L_\pi^j &= \alpha_\pi^j G - c_\pi P_\pi^j + c_\pi P_\pi^j \\
L_\pi^j &= \alpha_\pi^j G
\end{aligned}
$$

$$
\begin{aligned}
R_\pi^j &= s_\pi^j H(P_\pi^j) + c_\pi I_j \\
R_\pi^j &= (\alpha_\pi^j - c_\pi x_\pi modl) H(P_\pi^j) + c_\pi I_j \\
R_\pi^j &= \alpha_\pi^j H(P_\pi^j) - c_\pi x_\pi modl H(P_\pi^j) + c_\pi I_j \\
R_\pi^j &= \alpha_\pi^j H(P_\pi^j) - c_\pi I_j + c_\pi I_j (\because I_j = xH(P_\pi^j))
\end{aligned}
$$

3.3 コンフィデンシャルトランザクション

3.3.1 Confidential Transaction

ここまでで送金者と着金者を秘匿するための手法について解説してきた。本章では送金、着金額を秘匿するためのコンフィデンシャルトランザクション [11] について解説する。2015 年 6 月に Maxwell より発表されたアイデアであり、2017 年 1 月には Monero にも実装された。(送金者情報の秘匿と組み合わせてリングコンフィデンシャルトランザクション [10] という名前で導入されている) コンフィデンシャルトランザクションは、Pedersen Commitment[15] を元にしたアイデアである。

楕円曲線暗号のベースポイント G から

$H = topoint(SHA256(ENCODE(G)))$

を計算する。$topoint()$ は引数が楕円曲線上にある事を検証する関数である。さらに、blinding factor と呼ばれる秘密の数字 x と金額 a を用いて以下式で commitment C を求める。

$C = xG + aH$

Pedersen Commitment は元の数値を知らせる事なく、加算結果同士を検証することができるアイデアである。コンフィデンシャルトランザクションにおいては、Bitcoin のトランザクション形式である UTXO モデル [1] に組み合わせて応用する。UTXO モデルは input となる金額が複数、output となる金額が複数あるトランザクションモデルであり、各 input/output が UTXO と呼ばれる。input が送金、output が着金に相当する。

UTXO モデルにおいては、input と output についてそれぞれの合計が一致しなければならない。コンフィデンシャルト

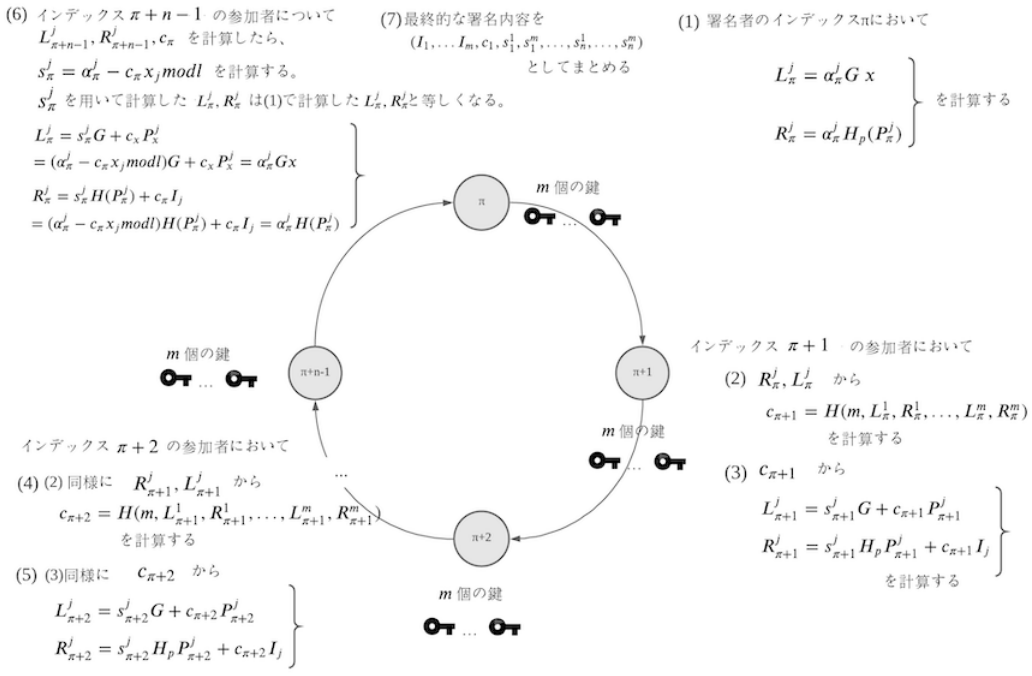

図 3 リング署名を用いるトランザクションの遷移

ランザクションにおいては、それぞれの金額は秘匿されるが、commitment で金額を表現することで、合計額が一致することは表現できる。図 3.3.1 は UTXO モデルにおいて commitment による秘匿前（上）と秘匿後（下）を表した図である。秘匿後について、個々の金額はわからなくとも、合計額の一致は確認できる。

しかし、input と output 合計が同一である事は証明されていても、着金者にとっては $C = xG + aH$ から金額を復号できなければいくら受け取ったが分からない。C,G,H は公知であるが、a を着金者に伝えるために、送金者は Elliptic Curve Diffie Hellman 鍵交換を用いて、着金者の公開鍵と送金に用いる blinding factor x から shared secret s を作成し、$s + a$ を

トランザクションにセットして公開する。着金者は受け取った $s+a$ から a を計算する事で着金額を知る事ができる。s を持たない送金者、着金者以外に a は分からず、送金者と着金者だけの間の秘匿化が完成する。

Input	Output
a_address 1.5coin b_address 2.5coin	c_address 3.5coin d_address 0.5coin

Input	Output
a_address xG + 1.5H b_address xG + 2.5H	c_address xG + 3.5H d_address xG + 0.5H

Range Proof

Confidential Transaction を扱う際の課題として、もし負の数が紛れている場合にも合計が一致してしまう。例えば、1.5coin と 2.5coin が input として送金に使われたが、-5coin と 9coin が output として着金にすると 9coin の UTXO が生まれ、着金者は 9coin を自由に利用できてしまう。つまり、$(1.5+2.5)-(-5+9)=0$ が成立してしまう。プログラム実装において正の値しか入力が認められていなくとも、大きな値をわざと入力してオーバーフローをかけることで負の値を入力してコインを増やす悪用が考えられる。そのため秘匿された金額がオーバーフローを起こさない範囲内であることを証明できれば負の値を利用した悪用を防ぐ事ができる。

秘匿された金額がオーバーフローしない範囲内であることを commitment から証明するために、commitment が 0 か 1 に対する commitment であることは証明できることを利用する。金額 a が 0 の場合 $C=xG+aH=xG$ であり、C に対する署名を依頼する事で x の保持者は 0 に対する commitment を証明できる。

金額 a が 1 の場合、$C=xG+aH=xG+1H$ である。ここで、$C'=(xG+1H)-1H=xG$ を導入すると、こちらも C' に対する署名を依頼する事で x の保持者は 1 に対する commitment を自明に証明できる。

これらの 0 か 1 に対する commitment である事を証明する性質を用いて、[0,2^n] の範囲内である事が証明できる。5 桁の C を 2 進数で表現し、$CN=0$ を C の N 桁目について 0 の commitment である事を示すとき、例えば以下を示せば、C が 00000 から 11111 の範囲内であることを示す事ができ、即ち 10 進数において $[0,2^5]$ の範囲であることは示せる。

$C1=0or1, C2=0or1, C3=0or1, C4=0or1, C5=0or1$

0 か 1 に対する commitment である事が証明可能な事は既に見てきたので、この式は成立し $C>0$ は表現できる。confidential transaction では更に効率的な計算を行うためにボロミアン・リング署名 [16] を用いる。この例で見た 5 桁の C の range proof は 2 進数であったが、4 進数で表現すると、$CN=0or1or2or3$ を証明することになる。$CN=0or1or2or3$ の時、$C0$ の値の範囲は自明に以下 4 パターンに定まる。

$$C0 = xG \tag{6}$$
$$C0_1 = xG + 2^5 H \tag{7}$$
$$C0_2 = xG + 2^{10} H \tag{8}$$
$$C0_3 = xG + 2^{15} H \tag{9}$$
$$\tag{10}$$

それぞれの $C0_n$ を公開鍵、x を秘密鍵としてみなして 4 つの鍵によるボロミアン・リング署名を適用することで、$C0$ に対して $C0_n$ のいずれかを用いていることを証明できる。この手法が range proof である。

3.3.2 RingCT

RingCT[10] は、Confidential Transaction と MLSAG を組み合わせた総称である。Confidential Transaction を導入すると、3.2.1 項で述べたワンタイムリング署名では匿名性を毀損してしまう。Confidential Transaction では、それぞれのアウトプットについて、実際の総金額の代わりにコミットメント C_{output} を設定する。それぞれのインプット C_{input} があり、

$\sum_{C_{input}} - \sum_{C_{output}} = 0$

を成り立たせるが、ワンタイムリング署名で単純に送金者を秘匿したとしても、それぞれの送金コミットメントのアウトプットと等しいコミットメントのインプットを抽出してトランザクションの関係性を追跡することが可能となってしまい送金者の匿名性が毀損される。そのため、式 3.3.2 に表すようにコミットメントのインプットとアウトプットの差分が zG になるようにダミーのコミットメントを用意し、アウトプットとインプットのコミットメントとの関係性を秘匿する。4

$\sum_{C_{input}} - \sum_{C_{output}} = zG$

各メンバー π において $z_\pi G$ を計算する。ここで、$z_\pi G$ は公開鍵、z_π は署名鍵の関係性になる。MLSAG は、π メンバーそれぞれに対して複数のベクトルの鍵を計算するが、コミットメントの差分 zG も鍵とみなしてベクトルに加える。

以下の式 3.3.2 は、コンフィデンシャルトランザクションと MLSAG を具体的に組み合わせた場合の RingCT の手順である。

- $(P_\pi^1, C_\pi^1), ..., (P_\pi^m, C_\pi^m)$ を、アドレス・コミットメントの組とする
- 送信先のアドレスとコミットメントの組を $(Q_i, C_{i_{out}})$ とする
- リングは、$R = \{\{(P_\pi^1, C_\pi^1), ..., (P_\pi^m, C_\pi^m), (\sum_{j=1} C_1^j - \sum_i C_i)\}, ..., \{(P_{\pi+n-1}^m, C_{\pi+n-1}^m), (\sum_{j=1} C_1^j - \sum_i C_i)\}\}$ と表せる。$(\sum_{j=1} C_\pi^j - \sum_i C_i)$ は $z_\pi G$ である。
- $(Q_i, C_{i_{out}})$ のハッシュ値 m をメッセージとして、MLSAG 署名を作成する
- 各 $C_{i_{out}}$ に対して range proof を計算し、アンダーフローを起こさないことを保証する

なお、RingCT を採用することで、必然的に各メンバーの署名鍵に相当するベクトルは複数になる。LWW の LSAG では各メンバーに対して 1 つの鍵の署名であるため、LWW の LSAG で処理すると複数のリング署名を作成する必要があり、計算量が増加する。そのため、各メンバーで複数の鍵でのリング署名を作れる処理できる MLSAG の方が適した署名方式として採用されている。

4. 結論

本レポートでは、Monero の匿名性について、解決課題、実現のための技術要素、発展してきた軌跡を整理した。Bitcoin における匿名性の課題をもとに、プライバシー課題の分類とそれを解決するために Monero が採用している手法を分類した。さらに、各手法について技術要素を分解することで Monero が匿名性を実現している手法を検討した。また、Monero が独自に応用した手法である RingCT などについて実現を支える技術要素についても詳細を検討することができ、全体を通して匿名性を実現するための技術理解を提供した。

本レポートで扱えなかった点を挙げると、Monero は 2020 年 10 月のアップグレードで、CLSAG?と呼ばれる手法を採用した。CLSAG は MLSAG を改良した手法で、MLSAG との違いはデータ容量の削減が主になるため、匿名性に着目した本論文では扱わなかったが現在の Monero を支えるという点で重要な技術である。

本レポートではプライバシーの強化と悪用の脅威の関係性について主として論じてはいないが、1 章にて述べた通り、プライバシーを強化することで、犯罪などに悪用される副作用効果は存在する。必要な時に第三者から身元の検証ができるなど、プライバシーの強化と悪用の脅威への副作用効果への対応を行うプロトコルなどが望ましい。Monero はすでに独自の匿名性をもった暗号資産として一定の地位を成しているが、プライバシーと悪用防止を両立する暗号資産の実現はこれ

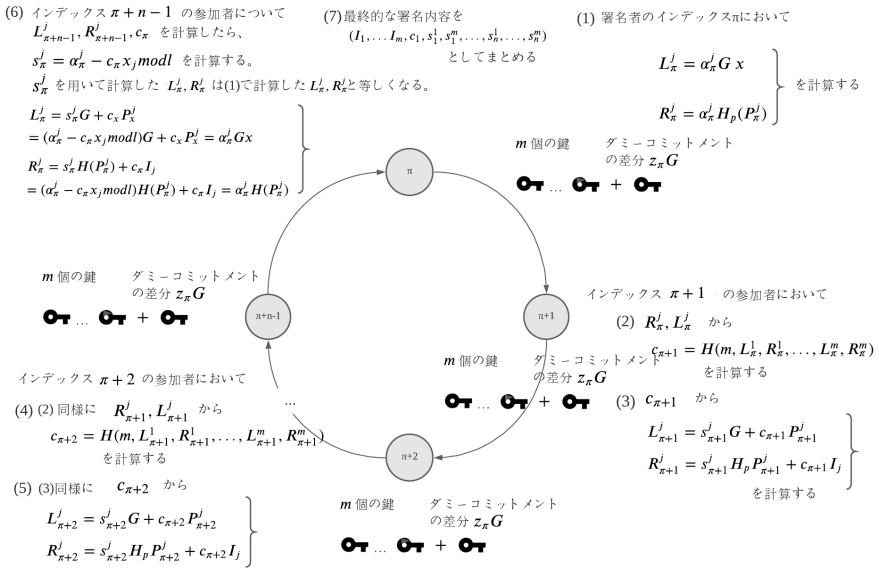

図 4 MLSAG にコミットメント zG を含めた図

から解決が待ち望まれる。

参考文献

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.com/bitcoin, 2008.

[2] Nicolas van Saberhagen. Cryptonote v 2.0. 2013.

[3] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, pp. 1318–1326, 2011.

[4] Steven Goldfeder, Harry Kalodner, Dillon Reisman, and Arvind Narayanan. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *arXiv*, Vol. 2018, No. 4, pp. 179–199, 2017.

[5] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A fistful of Bitcoins: Characterizing payments among men with no names. *Communications of the ACM*, Vol. 59, No. 4, pp. 86–93, 2016.

[6] Sherali Zeadally Muhammad Khurram Khan Neeraj Kumar Qi Feng, Debiao He. A survey on privacy protection in blockchain

system. *Journal of Network and Computer Applications*, Vol. 126, No. 9, pp. 45–58, 2019.

[7] The merits of monero: Why monero vs bitcoin. https://www.monero.how/why-monero-vs-bitcoin.

[8] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '01, p. 552–565, Berlin, Heidelberg, 2001. Springer-Verlag.

[9] Eiichiro Fujisaki and Koutarou Suzuki. Traceable Ring Signature. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *Public Key Cryptography – PKC 2007*, pp. 181–200, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[10] Shen Noether, Adam Mackenzie, and The Lab. Ring confidential transactions. *Ledger*, Vol. 1, pp. 1–18, 12 2016.

[11] Gregory Maxwell. Confidential transactions. https://elementsproject.org/features/confidential-transactions/investigation, month = , year = 2015,.

[12] Daniel J Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-Speed High-Security Signatures. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, pp. 124–142, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[13] Joseph Liu, Victor Wei, and Duncan Wong. Linkable spontaneous anonymous group signature for ad hoc groups. Vol. 2004, p. 27, 07 2004.

[14] ring signature efficiency. https://bitcointalk.org/index.php?topic=972541.msg10842017msg10842017. (Accessed on 02/07/2021).

[15] Torben Pryds Pedersen. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pp. 129–140, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.

[16] Gregory Maxwell and A. Poelstra. Borromean ring signatures . 2015.