（日本銀行仮訳）

プロジェクト・ステラ：日本銀行・欧州中央銀行による
分散型台帳技術に関する共同調査

分散型台帳環境における取引情報の秘匿とその管理の両立

2020 年 2 月

今回の報告書において示された分析および実験の結果は、中央銀行が運営する決済システムを含む既存の仕組みを置き換えたり、補完したりすることを意図したものではない。また、法律や規制上の観点は、本プロジェクトの射程外である。

要旨

分散型台帳上で取引情報を共有することにより生じるプライバシや秘匿性の課題に対して、過去数年にわたり、数々の手法が開発されてきた。これらの手法は、第三者の取引情報へのアクセスを制限する等の発想に基づいており、一般的に「プライバシ強化技術（privacy-enhancing technologies/techniques、以下 PET）」として知られている。

しかしながら、PET を用いて取引情報が秘匿化されると、取引確認のために第三者が取引情報を閲覧・解釈するのが困難になりうる。分散型台帳技術（DLT）に基づく決済システムのアカウンタビリティを確保するには、中央集権型のそれと同水準で取引が確認可能な仕組みを目指すべきである。これは、特定の決済手段が用いられる場合に限らず、ステーブルコインや中央銀行デジタル通貨など、さまざまなデジタル決済手段に当てはまる。こうしたことを背景に、ステラ・フェーズ 4 では、概念整理と実機検証を通して、分散型台帳環境において、いかにして取引情報の秘匿化と確認可能性を両立するかという問題に取り組む。具体的には、DLT に基づく金融市場インフラ（FMI）での取引を、PET で秘匿化する方法と、その確認を実効的に確保する仕組みについて調査する。

フェーズ 4 では、権限のない第三者から取引情報を秘匿化する手法のアプローチの違いに基づき、PET を 3 分類に整理している。共有先制御型 PET は、各参加者がネットワーク上の全取引の一部にしかアクセスできないようにする。非可読化型 PET は、暗号化技術を用いることで、第三者が取引情報を解釈できないようにする。関係性隠匿型 PET は、台帳に記録された送金者・受領者情報から、第三者が取引当事者を識別することを困難にする。

フェーズ 4 では、DLT に基づく FMI において、各 PET により秘匿化された取引情報の確認可能性を検証するための 3 観点――必要情報の取得の確実性、取得情報の信頼性、取引確認プロセスの効率性――を提案している。情報取得の確実性とは、確認者が取引確認に必要な情報を確実に取得できるかを示す。これは、確認者が、信用できる情報保有者（すなわち、DLT システムの中央集中的なコンポーネントまたは PET の特定機能を提供し、かつ必要情報を持っている信用できる第三者）または特定可能な参加者から必要情報を受領する場合に確保されうる。信頼性とは、確認者が取得した情報を用いて、秘匿化された取引情報を確実に解釈できるかを示す。確認者が信用できる情報保有者から情報を受領する場合、または、台帳に記録された情報を用いて取得情報の正確性を確認できる場合に信頼性は確保されうる。取引確認プロセスの効率性は、計算負担の度合いで示され、これはプロセス自体の実現可能性に関わる。

上記 3 観点をもとに PET ごとに取引の確認可能性を評価し、次のような場合に実効的

な取引確認が可能となる、との結果を得た。(1) 確認者が信用できる情報保有者から必要情報を取得する場合、または、(2)確認者が特定可能な参加者から必要情報を取得し、台帳に記録された情報を用いてその取得情報の正確性を検証可能であり、これらのプロセスを過大な負担なく実行可能な場合である。

フェーズ 4 は、実用化に際して、取引の秘匿性と確認可能性の両立に関する議論を展開するときの論点も提示している。第 1 に、信用できる情報保有者の存在は、ネットワークに対して単一障害点リスクをもたらしうることに注意が必要である。第 2 に、取引情報の秘匿性を強化するために複数の PET を組み合わせて使用することと実効的な取引確認の間にはトレードオフが存在しうる。第 3 に、本報告書で示したモデルを拡張して、複数のシステムの連携や階層型のシステムを考える際には、システム間で異なる規格やプロセスを調整する必要がある。最後に、システムがエンドユーザを含む場合には、エンドユーザ関連情報の秘匿性管理が複雑になりうるほか、取引確認の対象となる取引の決定方法についての適切な基準策定が必要となる。

目次

※本稿は日本銀行および欧州中央銀行による報告書「Balancing confidentiality and auditability in a distributed ledger environment」（本文）の日本銀行決済機構局による仮訳である。

1　はじめに

欧州中央銀行（ECB）と日本銀行は、過去数年間にわたり、プロジェクト・ステラにおいて、分散型台帳技術（DLT）が金融市場インフラ（FMI）に対してもたらしうる潜在的な利点や課題について共同調査を行ってきた。2016 年 12 月に開始されたプロジェクト・ステラは、概念整理と実機検証を通じて、FMI 分野への DLT の応用可能性に関する幅広い議論に貢献することを狙いとしている。これまでのフェーズでは、DLT に基づく市場インフラのパフォーマンスや耐障害性についての定量的結果を示し（2017 年 9 月公表）、また、異なる台帳間（DLT 台帳と中央集権型台帳の間を含む）や異なる資産間における支払の同期メカニズムについて調査した（2018 年 3 月、2019 年 6 月公表）[1]。

DLT は、多様なユースケースでの実装に向けて、ブロックチェーンコミュニティにより改善されてきた。また、さまざまな主体による取組みを通して、DLT に基づく資金・証券決済のプラットフォームを構築するための知見が得られてきた。これに関連し、分散型台帳上で取引情報を共有することにより生じるプライバシや秘匿性の課題に対して、数々の手法が開発されている。これらの手法は、第三者の取引情報へのアクセスを制限する等の発想に基づいており、一般的に「プライバシ強化技術（privacy-enhancing technologies/techniques、以下 PET）」として知られている[2]。

DLT を用いた FMI のアカウンタビリティを確保するためには、中央集権型の場合と同様に、取引の詳細を把握する権限のある第三者を置くなどの仕組みが必要になる。しかしながら、PET を用いて取引情報が秘匿化されると、情報の把握が制限されうるため、第三者による取引確認が難しくなる。本報告書では、権限のある第三者による取引情報の確認――すなわち、権限のある主体による秘匿化された取引情報の閲覧および解釈――が可能かを「確認可能性」という。

分散型台帳環境における取引情報のプライバシや秘匿性についての調査を、いくつかの中央銀行が公開している[3]。しかし、PET を用いて秘匿性が確保された取引情報（以下

---

[1] 日本銀行、ＥＣＢ「分散型台帳技術による資金決済システムの流動性節約機能の実現」（2017 年 9 月）、日本銀行、ＥＣＢ「分散型台帳技術による DVP 決済の実現」（2018 年 3 月）、日本銀行、ＥＣＢ「クロスボーダー取引における支払の同期化」（2019 年 6 月）。

[2] PET の定義は広範にわたる。European Union Agency for Network and Information Security (ENISA)「Readiness analysis for the adoption and evolution of privacy enhancing technologies」（2016 年 3 月）。

[3] Central Bank of Brazil「Distributed ledger technical research in Central Bank of Brazil」（2017 年 8 月）、Bank of Canada、Payments Canada、R3「Project Jasper: a Canadian experiment with distributed

「秘匿化された取引情報」）の第三者による確認可能性に関する研究や実験はほとんどみられない。

こうしたことを背景に、フェーズ 4 は、取引情報の秘匿化と確認可能性の両立についての洞察を提供することを目的とする。具体的には、分散型台帳環境で用いられるいくつかの PET を体系的に分類し、それらを用いて秘匿化された取引情報を DLT ネットワーク上の権限のある主体が実効的に確認可能かを評価する[4]。

第 2 章は、本報告書で分析のベースとして用いる、分散型台帳環境における抽象化された仮想 FMI モデルを説明する。第 3 章では、DLT の分野で用いられる、いくつかの PET について、秘匿性を高めるための基本的な性質を説明し、体系的に分類する。第 4 章では、第三者による取引情報の確認可能性を評価するための観点を提示し、それらの観点を用いて、秘匿化された取引情報が実効的に確認可能かを評価する。分析を裏付ける実験の概要を第 5 章で示す。

---

ledger technology for domestic interbank payments settlement」（2017 年 9 月）、Monetary Authority of Singapore、The Association of Banks in Singapore「Project Ubin Phase 2: re-imagining interbank real-time gross settlement system using distributed ledger technologies」（2017 年 11 月）、Bank of England「Chain -- fintech proof of concept」（2018 年 4 月）、South African Reserve Bank「Project Khokha: exploring the use of distributed ledger technology for interbank payments settlement in South Africa」（2018 年 6 月）、Federal Reserve Bank of Boston「Beyond theory: getting practical with blockchain」（2019 年 2 月）。

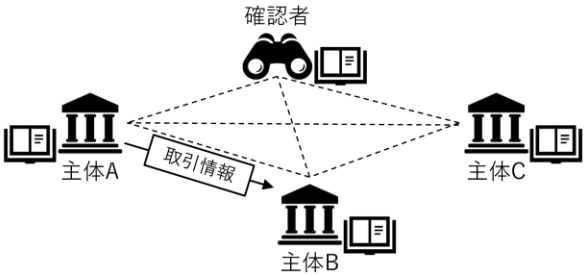
[4] 今次調査には、ECB から Dirk Bullmann （チームリーダ）、Andrej Bachmann、Diego Castejón Molina、Cedric Humbert、Naisa Tussi、Austeja Sostakaite、Giuseppe Galano（現イタリア銀行）、Kurt Alonso (ECB 情報システム総局)、日本銀行から岸道信（チームリーダ）、山田健、松嶋徹郎、北條真史、松井茜美佳、小早川周司（明治大学教授および日本銀行ステラチームアドバイザ）が参加した。

2　DLT に基づく FMI の抽象モデル

本章では、PET が用いられうる、DLT に基づく FMI の抽象モデルを導入する。同モデルでは、さまざまな主体が取引情報を分散的に記録・共有するネットワークを構成する、と想定する（図表 1）。このモデルは、中央集権型 FMI モデルのもとで取引情報が記録・保管・共有される既存のアプローチとは対照的である（図表 2）。DLT に基づくモデルでは、参加主体が各自の DLT ノードを運用し、これを通じて取引の処理および取引情報の保管・閲覧が行われる。

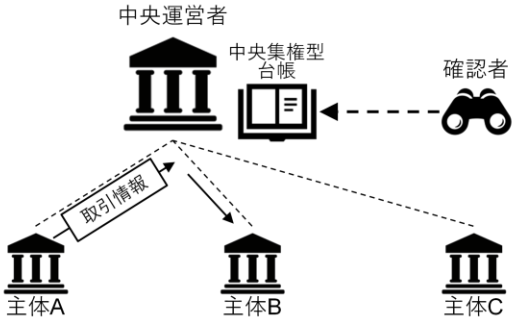
また、ネットワークには参加者のほか、取引確認の権限を与えられた単一または複数の主体（確認者[5]）が存在し、その主体は台帳上の取引情報の閲覧および解釈により取引確認を行うこととする[6]。本報告書はバックエンドの仕組みに焦点を当てているため、ネットワークの参加者間で行われる取引のみを分析対象とする。よって、エンドユーザ（例：各参加者の顧客）はモデル中に登場しない。

【図表 1】DLT に基づく FMI モデル



注：各参加者は、取引関連情報を各自の台帳に保管し、他の参加者とその情報を共有する。

【図表 2】中央集権型 FMI モデル



注：中央運営者は、取引情報を保管する中央集権台帳を持ち、参加者による台帳へのアクセスを管理する。

---

[5] 本報告書では、単一の確認者を想定している。DLT ネットワークに複数の確認者が存在する場合には、実効的な取引確認を確実に行うための仕組みが構築されている必要がある。例えば、①取引情報のすべてが少なくとも 1 先の確認者には確認可能な仕組みや、②ある取引に対する確認責任がどの確認者にあるのかをすべての確認者が把握する仕組み、③確認者間の共有データベースを持つこと等で、必要に応じて確認者や他主体間で取引関連情報を共有する仕組み、が挙げられる。

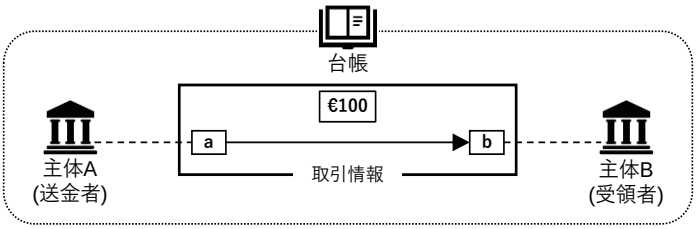
[6] 理論上、取引情報の確認を取引検証プロセスに組み込むことも可能であるが、このアプローチは今回の報告書の射程外である。ECB「Exploring anonymity in central bank digital currencies」（2019 年 12 月）参照。

DLT に基づく FMI モデルは、パーミッションド型ネットワーク[7]であり（プライベートネットワークなどとも呼ばれる）、ネットワークに参加するすべての参加者は、ネットワークの参加条件（規則）に従い、自らが負う責任を果たすことが期待される。また、規則に準拠した基本的な機能を DLT ノードに実装し、取引には所定のフォーマットを使用することが求められる。こうした規則に従わない場合、その参加者はレピュテーションリスクに晒されるだけでなく、ネットワークへのアクセス権を失うなどの制裁の対象となる可能性がある。

本報告書では、DLT に基づくモデルにおける参加者管理やガバナンス等のシステム管理者が行う役割は、主な焦点ではなく、モデルを簡略化する観点から取り扱わない。取引検証者の役割については、参加者またはその権限を与えられた主体が担い、必要に応じて本報告書の関連部分で言及している。

また、取引情報には、簡略化の観点から、取引当事者（送金者・受領者のアドレス等の参加者識別子＜ID＞）と取引額のみが含まれることとする。取引情報にエンドユーザやスマートコントラクト[8]に関する情報を含めることで、DLT に基づくモデルを充実させることもできるが、第 4 章の主な結果への実質的な影響がないため、それらは含めないこととする。図表 3 は、主体 A（送金者）が主体 B（受領者）へ 100 ユーロを送金する場合における台帳上の取引情報を示す。

【図表 3】秘匿化されていない取引情報



注：点線はアドレス（a、b）とそれらを用いる取引当事者（A、B）間の結び付きを示す。

2.1 FMI の抽象モデルにおける秘匿性

取引データの秘匿化や保護に関する現在の議論には、さまざまな用語と定義が用いられ

[7] パーミッションド型ネットワークは、DLT ネットワークにおける設計の 1 つであり、ネットワークに参加するには、他の参加者または、システム管理者が存在する場合はシステム管理者により、権限を付与される必要がある。

[8] スマートコントラクトとは、参加者の契約上の義務を DLT 上に置き換える際に用いるための方法であり、契約条項が自動的に履行されるようにするものである。

ている。本報告書では、「秘匿性」とは、それが確保された際に権限のない第三者（図表 1、図表 2 が示す主体 C）が（主体 A、B 間の）取引情報の閲覧および解釈ができない状態を指す。ここでいう「閲覧」とは、第三者が取引情報の存在を認識できる状況を示し、「解釈」とは、第三者が取引情報の閲覧のみならず、実際の取引額や送金者・受領者を特定できる状況を指す。

中央集権型モデル（図表２）では、取引情報の秘匿性は、取引情報を管理する中央運営者によって確保され、各参加者はアクセス権限のある情報しか入手できない。すなわち、中央運営者が権限のない第三者による取引情報の閲覧を効果的に防いでいる。DLT に基づくモデル（図表１）では、情報が分散的に保管・共有されているものの、中央集権型モデルと同水準の秘匿性が確保される必要がある。

2.2 FMI の抽象モデルにおける取引情報の確認可能性

本報告書では、取引情報の確認可能性とは、確認者による実効的な取引確認――すなわち、確認者としての責任を果たすための取引情報の閲覧および解釈――が可能かを表す[9]。

中央集権型モデルでの取引確認は、中央運営者が確認者の要請に基づき取引情報を開示することで可能となる。これは、中央集権型モデルでは、取引情報が中央運営者に対しては秘匿化されていないため可能となる。

中央運営者が存在しない DLT に基づくモデルにおいても、同水準の取引確認が可能な仕組みを目指すべきである[10]。そのために、確認者は、（ネットワーク参加者を通じて台帳にアクセスするケースも考えられるが、）自ら DLT ノードを運用すると想定される。しかしながら、PET を用いて取引情報が秘匿化されると、確認者による取引確認が難しくなる。これは、PET によって、確認者を含む第三者に対して取引情報が閲覧不能になる、または閲覧可能でも解釈不能になるためである。従って、PET によっては、秘匿化と確認可能性を十分に両立させることが困難になる。

---

[9] 加えて、確認者は、必要に応じて各参加者が適切に顧客確認とアンチマネーロンダリングを行っているか検証することもありうる。この目的のため、各参加者は、顧客 ID を台帳上の口座情報と紐づけ、確認者と顧客情報を共有できる体制を持っている必要がある。しかし、この体制は DLT ネットワーク外に構築される可能性が高いため、本報告書では取り扱わない。

[10] BIS 決済・市場インフラ委員会『金融市場インフラのための原則』（2012 年）において、秘匿保持と監査可能性は、FMI の情報セキュリティの目標・方針が適合すべき基準の一つである旨が言及されている（説明 3.17.12 参照）。

3　DLT におけるプライバシ強化技術

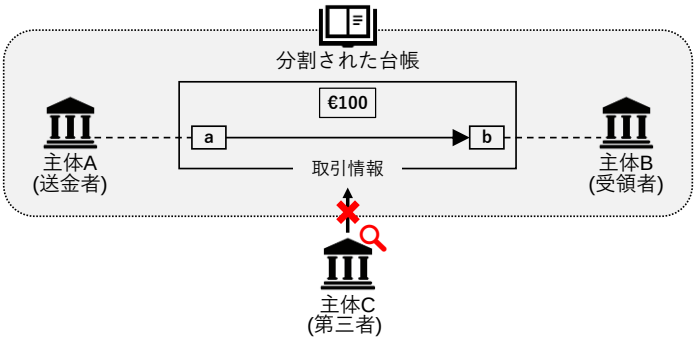
分散型台帳上で取引情報を共有することで生じるプライバシや秘匿性の課題に対応する数々の手法が登場している。取引情報の秘匿性を高めるための改善案については、研究や実用化に向けたプロジェクトにてますます検討が進んでいる。

本章では、DLT ネットワーク上で取引情報の秘匿性を強化することを目的とする技術や手法――いわゆる PET――をいくつか紹介する。各 PET の基本的な性質を説明しつつ、秘匿性を強化する手法のアプローチの違いに基づき、PET を 3 種類に分類する。本報告書において、DLT ネットワーク上で PET を適用する際、すでに取引情報には基本的な仮名化[11]が施されているとする。本報告書で解説する PET は、個別に適用されるのみではなく、秘匿性を高めるために、組み合わせて適用することが可能であることに留意すべきである。

3.1　共有先制御型 PET

取引情報の秘匿化は、取引を把握する必要性に応じて取引情報が参加者間で共有されるように DLT ネットワークを設計することで実現できる（図表 4 参照）。共有先制御型 PET が使用された環境下では、全参加者が閲覧可能な全取引情報が記録される共有台帳は存在しない。その代わりに、各参加者は全取引の一部が記録される台帳（全取引が記録される台帳の部分集合）のみを持つ。従って、ある取引（主体 A、B 間の取引）について、閲覧権限のない第三者（主体 C）は、その取引の存在そのものを認識できない。

【図表 4】共有先制御型 PET



[11] 仮名化とは、参加者の個人情報が各参加者に紐付けられることを防ぐために、それらの情報を偽装する手段であり、DLT ネットワークで広く利用される。ネットワーク参加者は、通常、一意な識別子である仮名を持つ。仮名には参加者に関する情報は含まれないことが多いが（通常、ランダムな文字列を用いる）、仮名を用いるだけでは十分な秘匿性は得られない。

3.1.1 Corda における共有先制御手法

パーミッションド型 DLT 基盤である Corda は、取引情報の共有先を効果的に制御するネットワーク設計を特徴としている。共有先の制御は、閲覧が許可された参加者間でのみ取引情報が共有されるように、ネットワーク上で参加者が通信することで実現される[12]。Corda では、事前に決められた特定の参加者のみが特定の通信に参加し、ネットワーク内のその他の参加者はその通信が行われていることを認識しない。

取引情報の共有先が制御されている一方、Corda のネットワークには notary と呼ばれるネットワーク上のサービスが存在し、これは、取引情報を受領し二重支払いが行われていないことを保証する。Notary には、validating notary と non-validating notary の 2 種類がある。Validating notary はすべての取引情報を受領し、二重支払いの確認に加えて取引の検証も行う。Non-validating notary は取引情報の一部のみを受領し、完全な取引情報は取引検証を行う参加者間でのみ共有される[13]。

3.1.2 Hyperledger Fabric における共有先制御手法

パーミッションド型 DLT 基盤である Hyperledger Fabric では、チャネル機能を通じてネットワークレベルで取引情報の共有先制御ができる。この機能により、ネットワークはそれぞれが台帳の部分集合を持つサブネットワークに分割され、すべての取引情報を記録する共有台帳は存在しない[14]。

参加者は、特定のチャネルの台帳上で取引を行い、かつその台帳の記録を保持するために、ネットワークによって認証・認可される必要がある。それゆえ、参加者は自身が参加しているチャネル上の取引のみ閲覧できる。さらに、本報告書執筆時点での Hyperledger Fabric の実装（v.1.4）では、全チャネルの取引情報は、取引順序を整理するために ordering service と呼ばれるネットワーク上のサービスに送信される。

3.1.3 ペイメントチャネル

ペイメントチャネル[15]は DLT ネットワーク上の資金を DLT ネットワークの外で取引で

---

[12] M. Hearn「Corda: a distributed ledger」（2016 年 11 月）。

[13] 検証を実施する参加者のノードは、過去に行われた取引の秘匿情報を知ってしまう可能性がある。これを防ぐためには、chain snipping などの追加の手法を実装することができる。

[14] https://hyperledger-fabric.readthedocs.io/en/release-1.4/channels.html を参照。

[15] ペイメントチャネルに関するより詳細な説明については、日本銀行、ECB「クロスボーダー取引における支払の同期化」（2019 年 6 月）を参照。

きるようにすることで、秘匿性を強化する仕組みである[16]。ペイメントチャネルにより、参加者は個々の取引をネットワーク全体にブロードキャストすることなく、台帳外で取引可能となる。

2 参加者間でペイメントチャネルを確立（開設）する際には、一方あるいは双方が特定の額の資金（表 1 中では主体 A、B がそれぞれ 50 ユーロ）を、一般的には、台帳上の一時的な特別口座に預け入れる。参加者は特別口座の資金の持ち分を変更する指図をやり取りすることで、台帳外において 2 者間で取引できる。ペイメントチャネルが閉鎖されると、預け入れた資金が閉鎖時点の両者のネットポジションに基づいて分配される。共有台帳にはペイメントチャネルの開設と閉鎖のみが、特別口座からの資金移動という形で記録されるため、第三者は送金者と受領者の仮名とネットされた取引額（主体 A が主体 B から 30 ユーロを受取った）を確認できる。しかしながら、台帳外で実施された個々の取引は当事者以外の参加者からは確認できない。

複数の 2 者間ペイメントチャネルはペイメントチャネル・ネットワークを形成しうる。そこでは、参加者 2 先が 2 者間ペイメントチャネルを持たずとも、中継役の参加者を通して取引を実施することが可能になる。中継役の参加者が、他の全参加者との 2 者間ペイメントチャネルを持つ中心的な主体である場合には、この参加者はペイメントチャネル・ハブとみなせる。しかしながら、秘匿性に関しては、ペイメントチャネル・ハブは取引を中継する際に取引情報（取引額や取引当事者）の閲覧が可能である。

ペイメントチャネルは、ビットコインやイーサリアムなどのパブリック型ブロックチェーンにて実装されている（それぞれ、ライトニングネットワーク、ライデンネットワークと呼ばれる）。

[16] DLT ネットワーク外で取引を実行することで秘匿性を強化する他の方法としては、サイドチェーンの構想がある。

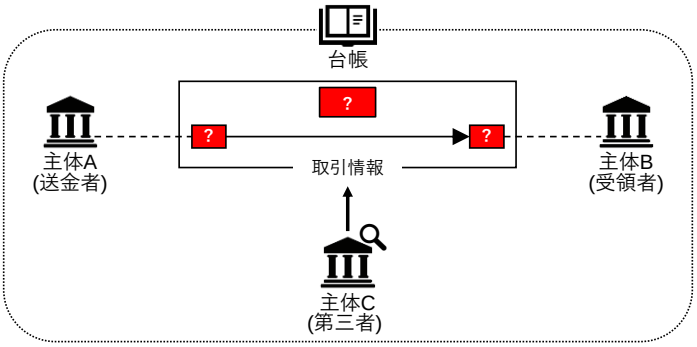
【表 1】主体 C からみた取引情報の例

閲覧可能な情報 （台帳上取引）	閲覧不可能な情報 （台帳外取引）
開設取引 A →特別口座（€50） B →特別口座（€50）	
	A→B (€20)
	B→A (€40)
	B→A (€10)
閉鎖取引 特別口座→A (€80) 特別口座→B (€20)	

3.2 非可読化型 PET

取引情報の共有先制御がなされず、全取引情報を記録する単一の台帳を参加者が共有する場合には、個々の取引単位での秘匿性強化のために PET を用いることができる。ネットワーク上の全参加者が全取引を閲覧可能でありつつも、種々の暗号技術を用いて権限のない第三者（主体 C）が取引の詳細を解釈することを防ぎ、結果として取引情報を非可読化する（図表 5）。

【図表 5】非可読化型 PET



3.2.1 Quorum におけるプライベート・トランザクション

DLT 基盤である Quorum[17]のネットワークでは、パブリックとプライベートの 2 つの異なる取引機能がある。プライベート・トランザクションは Quorum における追加機能であり、参加者は、これを用いることで権限のない第三者に対して取引情報を解釈不能に

[17] Quorum はパブリック型ブロックチェーン基盤のイーサリアムをベースにしつつ、パーミッションド型ネットワーク上での取引実施を目的に設計されている。

できる[18]。本機能は、事前設定にて、参加者が取引当事者を指定することによって利用可能となる[19]。プライベート・トランザクションで行われる取引は、指定された当事者のプライベート台帳に保存され、パブリック台帳には、その取引の存在を証明するためのハッシュ値および送金者情報が記録される。これにより、権限のない第三者が取引内容を完全には解釈することなく、プライベート・トランザクションが実行できる。

3.2.2 Pedersen commitment

Pedersen commitment は、送金者が送金額に対応するコミットメントを作成し、送金額の代わりにコミットメントを共有することを可能とする、暗号化の要素技術の 1 つである[20]。コミットメントはネットワーク上で定義されたパラメータと送金者自身が選んだパラメータによって作成される。

取引当事者は、Pedersen commitment を用いて、共有台帳上の取引額を第三者に解釈できないコミットメントに置き換えられる。一方で、この技術では送金者と受領者の情報は解釈可能なままとなる。Pedersen commitment により、取引に含まれる入力額と出力額が等しいことを、その値を明らかにせずに検証可能になる。Pedersen commitment は、暗号学上、全秘匿と計算拘束を満たし、これは、コミットメントを解釈するためにはそれを作成したときに用いたパラメータの情報が必須であり、後からその値を変更できないことを意味する。

Pedersen commitment は、Elements における Confidential Transaction など、いくつかのプロジェクトで実装されている。Pedersen commitment の詳細については、第 5 章を参照のこと。

3.2.3 ゼロ知識証明

ゼロ知識証明（Zero-knowledge proof、以下 ZKP）は、当事者が、ある情報を知っていることを、その情報を知っているという事実以外の情報を開示せずに証明できるという、暗号学的な手法である。DLT ネットワークにおいては、取引情報そのものを開示せずに検証可能な秘匿化された取引を作成するために、ZKP が用いられる。取引当事者は秘匿

---

[18] 他方、パブリック・トランザクションで行われる取引情報は、すべてのネットワーク参加者による解釈が可能である。

[19] ここでのハッシュ値は、ある入力から一方向性関数によって計算される値である。ハッシュ値から元の入力値を取得することは不可能である。

[20] T. P. Pedersen「Non-interactive and information-theoretic secure verifiable secret sharing」(1991 年)。

化された取引情報を台帳上に記録することにより、第三者からの解釈を不可能にした取引を行える。

この手法をもとに、いくつかの実装、特に、送金者とその他の参加者間で、取引の検証に際して対話を必要としないものが開発された。非対話型の ZKP の実装を効率的に実施するために、zero-knowledge Succinct Non-interactive ARgument of Knowledge（zk-SNARK）が提案されている。これは、ZKP に基づくアプリケーションを開発するための方式であり、信頼された主体が秘密のパラメータを用いて 2 つの公開パラメータ（証明鍵と検証鍵）を生成する準備作業が必要となる。ここで、証明鍵は、送金者が完全に秘匿化された取引情報を共有する際に使用され、検証鍵は、その取引情報を検証する際に用いられるものである。

イーサリアムや Quorum などのいくつかの DLT 基盤で、zk-SNARK に基づくアプリケーションが実行可能となっている。また、DIstributed Zero Knowledge は、スケーラビリティを改善している[21]。さらに、zero-knowledge Scalable Transparent ARguments of Knowledge[22]は、信頼された当事者による準備作業を必要とせずに取引が検証可能となることを目的としている。

---

[21] H. Wu、W. Zheng、A. Chiesa、R. A. Popa、I. Stoica「DIZK: a distributed zero knowledge proof system」（2018 年）。

[22] E. Ben-Sasson、I. Bentov、Y. Horesh、M. Riabzev「Scalable, transparent, and post-quantum secure computational integrity」（2018 年 3 月）。

BOX：スマートコントラクトの秘匿化

本報告書は、DLT に基づく FMI モデル上で参加者が取引を行う場合の決済プロセスのみを扱っている。本モデルをさまざまな金融アプリケーションに拡張するにあたっては、スマートコントラクトの利用が考えられる。本章にて紹介した PET のいくつかは、スマートコントラクトの処理内容の秘匿性を高めるために利用することが可能である。

Merkelized Abstract Syntax Tree（MAST）[23]は、スマートコントラクトの処理内容の非可読化を可能とする手法の 1 つである。MAST の設計により、処理内容に含まれる条件分岐を木構造として表現することが可能となる。特定の条件が実行されない限り、それに対応する分岐は非可読のままとなり、条件が実行された場合にのみ、その分岐内の処理内容が開示される[24]。

3.3 関係性隠匿型 PET

共有台帳上で閲覧可能な送金者/受領者情報と、実際に取引を行った送金者/受領者の関係性を切断するために、PET を適用できる[25]。図表 6 にて示すように、関係性の切断は、（i）実際の送金者（図表 6 中の主体 A）および/または受領者（主体 B）と記録された仮名（a と b）、または、（ii）送金者と受領者の間の取引関係[26]、に対して行われる。これにより、権限のない第三者（主体 C）は、取引情報を閲覧でき、取引額を解釈できるものの、取引当事者を識別することが不可能となる。

---

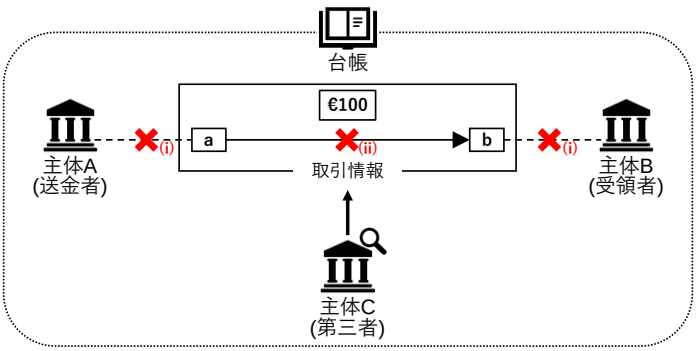
[23] J. Rubin、M. Naik、N. Subramanian「Merkelized Abstract Syntax Trees」（2014 年）。

[24] 特に、相互に合意したスマートコントラクトの実行に際しては、さらに秘匿性を高める別の手法を利用することが可能である。例として Schnorr 署名は参加者の署名を集約するために用いることができ、その結果、実行された分岐の詳細を非可読化することができる。G. Maxwell、A. Poelstra、Y. Seurin、P. Wuille「Simple Schnorr multi-signatures with applications to Bitcoin」（2018 年 5 月）を参照。

[25] ここでも、取引情報は共有先を制御されておらず、参加者は全取引を記録する 1 つの台帳を共有していることを想定している。

[26] 実際には、送金者から発出される取引と受領者に到着する取引とを個々に追跡することで、関係性を復元することが可能となりうるため、取引関係の切断による秘匿性の確保は不十分な可能性がある。S. Steinbrecher、S. Köpsell「Modelling unlinkability」（2003 年）を参照。

【図表 6】関係性隠匿型 PET



3.3.1 ワンタイムアドレス

参加者は、各取引に対してそれぞれ異なる仮名――すなわちアドレス（ワンタイムアドレス）――を用いることで、自身の ID が自身の関わったその他の取引と関連付けられることを防げる（図表 6 中の（i）の方法）。この手法は広くさまざまなプロジェクトで用いられている[27]。ワンタイムアドレスは秘匿性を強化するために利用できるものの、各参加者が多数のアドレスと各アドレスに対応する秘密鍵を扱うため、それらの管理は無視できないほど複雑になる。

決定性ウォレットは、この欠点に対応する最も一般的かつ効率的な手法である。これは、1 つの起点から多数のアドレスを決定的に生成することを可能とし、アドレス管理の複雑さを軽減することに繋がる。決定性ウォレットにより生成された個々のアドレスの間には、明らかな関係性は存在しないため、第三者が、これらのアドレスが使用された取引を関連付けることは困難である。

決定性ウォレットのうち、階層型決定性（hierarchical deterministic、以下 HD）ウォレットは最も実用的な手法である。HD ウォレットにおいては、ある生成元を用いてマスタ秘密鍵/公開鍵のペアを生成し、そこからすべての鍵ペアが、階層的な木構造の形式で導出される。このほか、CryptoNote のように公開鍵と秘密の値をもとに取引固有の鍵を生成する手法もある[28]。HD ウォレットの詳細については、第 5 章にて解説する。

3.3.2 ミキシング

ミキシングは、複数の参加者間の取引関係を切断するために、複数の取引を混合する手法である（図表 6 中の（ii）の方法）。ミキシングの結果として共有台帳に記録される混

[27] 例としては、ビットコインやイーサリアム、リブラが挙げられる。

[28] https://cryptonote.org/cns/cns006.txt を参照。

合された取引は、複数の送金者と複数の受領者がいることを示し、第三者にとっては元の取引当事者の組み合わせを特定することが困難となる（表 2)。一般的に、より多数の取引を混合することにより、取引当事者の組の数が多くなるため、秘匿性の水準はより高いものになる。

ミキシングは、中央集中型のミキシングサービス提供者を経由するものと、peer-to-peer（P2P）に基づいて実行されるものがある。前者では、参加者が実際の取引情報をその提供者に送信する必要があるため、サービス提供者が参加者に信頼されている必要がある。後者では、参加者は中央集中型のミキシングサービス提供者を頼る必要がなくなるが、同時に取引を実行する他の参加者を見つけることが課題となる。

ミキシングが用いられると、中央集中型と P2P 型のいずれについても、取引額は解釈可能な形式で台帳上に記録される。従って、同額の取引の数が限られている場合には、取引当事者は互いに関連付けられる可能性がある。この欠点を克服するために、ミキシングは、Pedersen commitment 等の取引額を秘匿化する手法と組み合わせて実装されることがある。現在、いくつかのミキシングのプロトコルやサービス提供者が存在している。

【表 2】主体 C からみたミキシング使用前後の取引情報の例

ミキシング使用前

送金者	取引額	受領者
a	€100	b
d	€100	f
e	€100	g

ミキシング使用後

送金者	取引額	受領者
e a d	各々 €100	b g f

3.3.3 リング署名

リング署名は、実際の署名者が誰であるかを開示せずに、その署名者が署名者グループに属していることを証明するデジタル署名の一種である（図表 6 中の（ii）の方法）[29]。

DLT ネットワークにおけるリング署名の基本的な性質は、送金者が、異なる複数の参加者（リングメンバと呼ぶ）の公開鍵を集めたうえで、自身の秘密鍵と集めた公開鍵を用いて取引に署名することを可能にする点である。第三者はリングメンバの 1 人が取引に署名したことは分かるが、その署名者を識別することはできない。

しかしながら、リング署名が使用された際、ミキシングと同様に取引額（および受領者

[29] リング署名の概念は D. Chaum、E. van Heyst「Group signatures」(1991 年)および R. L. Rivest、A. Shamir、Y. Tauman「How to leak a secret」(2001 年)。

の仮名）は解釈可能な形で台帳に記録される（表 3)。入力額として用いられる取引額の情報は、実際の送金者を特定するために利用されうるため、通常リング署名は、秘匿性を強化するために、Pedersen commitment 等の取引額を秘匿化する手法と組み合わせて実装される。

【表 3】主体 C からみたリング署名が使用された取引情報の例

送金者	取引額	受領者
a d e	€100	b

3.4 まとめ

本章では複数の PET を、秘匿化する手法のアプローチの違いに基づき 3 つに分類した。取引に関連する情報の閲覧および解釈がどの程度可能かは、各 PET によって異なる。表 4 は、取引情報について、第三者が閲覧・解釈可能かをまとめている。複数の PET を組み合わせて使用することにより、より高い水準の秘匿性が確保されうることに留意する必要がある。

【表 4】権限のない第三者からの取引情報の閲覧および解釈可能性

分類	PET	取引情報		
		送金者	受領者	取引額
共有先制御型	Corda における 共有先制御手法	不可		不可
	Hyperledger Fabric に おける共有先制御手法	不可		不可
	ペイメントチャネル	可		不可*
非可読化型	Quorum における プライベート・トランザクション	可	不可	不可
	Pedersen commitment	可		不可
	ゼロ知識証明 （送金者、受領者、取引額を非可読化）	不可		不可
関係性隠匿型	ワンタイムアドレス	不可		可
	ミキシング	不可		可
	リング署名	不可	可	可

*ネットされた取引額のみ閲覧および解釈可能。

4　秘匿化された取引情報の確認可能性

分散型台帳システムにおいて秘匿性を強化するために PET が用いられると、取引情報の確認可能性を確保することが困難になりうる。本章では、第 2 章で提示した DLT に基づく FMI モデルを基に、秘匿化された取引情報を実効的に確認できるかを評価する。本分析は、DLT ネットワークにおける取引情報の秘匿性とその管理に関する議論への貢献を目的とする。

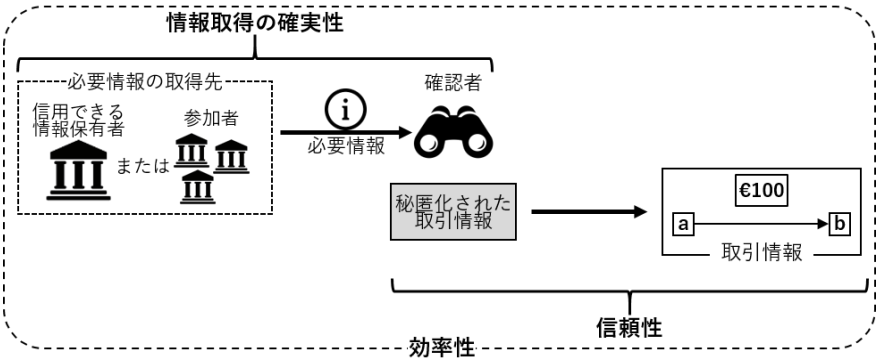
PET を実装する方法はさまざまであるほか、本報告書で取り上げている PET のいくつかは、今も開発途上である。このため、取引確認の具体的な方法およびその実効性は、ネットワークにおける PET の実装次第であり、各 PET に関する評価結果は、断定的なものではない点に留意すべきである。

本章は、まず、秘匿化された取引情報が実効的に確認可能かを評価するにあたって鍵となる観点を提案する。そのうえで、特定の PET の仕組みについて、これらの観点に基づき評価する。さらに、実用化に際しての追加的な論点について述べる。

4.1　確認可能性を評価するための 3 観点

本報告書は、秘匿化された取引情報の確認可能性を評価するための 3 つの観点を提案する。これらの観点は、取引確認プロセスの一般的な流れに対応したものである（この点は、図表 7 で図示され、以下で詳述される）。3 観点は、評価に用いられる順に、(1) 必要情報の取得の確実性、(2) 取得情報の信頼性、(3) 取引確認プロセスの効率性、である。ある構成の DLT システムがこれらの観点を満たしている場合、実効的な取引確認は可能である。

【図表 7】取引確認の大まかな流れと 3 観点



4.1.1 必要情報の取得の確実性

第 1 の観点は、必要情報の取得の確実性である。この観点では、確認者が取引確認を行うために必要な情報を取得できるかについて検討する。PET が用いられると、確認者は、取引情報を閲覧できない（共有先制御型 PET)、もしくは取引情報を解釈できない（非可読化型 PET または関係性隠匿型 PET)。この結果、確認者は、取引確認を行うために追加的な情報（以下「必要情報」）を他の情報保有者から取得する必要がある。情報保有者としては、ネットワーク上に存在する「信用できる情報保有者」および参加者が挙げられる。

信用できる情報保有者は、DLT システムの設計上存在するコンポーネント（例えば Corda における notary）または PET の実現に必要な信用できる第三者（例えば中央集中型ミキシングサービス）であり、かつ確認者が取引情報を確実に解釈するために利用できる必要情報を保有しているものを指す。信用できる情報保有者および参加者は、制裁またはネットワークへのアクセス権の喪失といった強制力のある枠組みに裏打ちされた、ネットワーク規則によって、確認者への協力を求められうる。

必要情報の取得の確実性は、信用できる情報保有者による確認者への必要情報の提出が求められる取引確認プロセスにおいては満たされる。信用できる情報保有者が存在しない場合には、確認者は必要情報の提供を参加者（特に取引当事者）に頼る必要がある。多くのケースにおいては、参加者はネットワーク規則を遵守し、確認者に必要情報を提出すると想定される。もっとも、参加者が確認者に必要情報を提出しないケースにおいては、確認者は当該参加者を特定し、強制的に情報を取得する必要がある。確認者が実際の取引情報を保有する参加者の特定が可能（以下「特定可能な参加者」）な場合には、強制力をもって情報提供を求められるため、情報取得の確実性は満たされる。一方、特定可能な参加者以外の参加者から情報を取得する必要がある場合は、情報取得の確実性は充足されない[30]。

---

[30] 取引情報の確認を取引検証プロセスに組み込んだ DLT システムもデザインできる。こうすることで、用いられる PET に関係なく、情報取得の確実性のみならず信頼性も確保されうる。しかし、こうしたアプローチは、即時の取引確認を必要とし、確認者が積極的に DLT システムの運営に関わることになるため、第 2 章に記述されているとおり、本報告書の射程外としている。なお、取引検証時に、取引の確認そのものではなく、確認可能性のみをチェックする DLT システム設計も提案されている（ECB「Exploring anonymity in central bank digital currencies」（2019 年 12 月）および K. Naganuma、M. Yoshino、H. Sato、T. Suzuki「Auditable zerocoin」（2017 年）を参照)。

4.1.2　取得情報の信頼性

確認者が必要情報を取得可能なときには、第 2 の観点が適用されうる。この観点は、取得情報の信頼性に着目するものであり、取得情報を用いることで、確認者が実際の取引情報を確実に入手できる場合において、信頼性が確保されているとみなされる。

情報取得の確実性についての評価と同様に、確認者が信用できる情報保有者から必要情報を取得する場合には、取得情報の信頼性は満たされる。信用できる情報保有者が存在しない場合には、確認者は特定可能な参加者から必要情報を取得しなければならない。取得された情報の信頼性が確保されるためには、取得情報の正確性の検証に利用できる取引記録が、確認者が閲覧可能な形式で共有台帳上に存在する必要がある。このような取引記録が存在しない場合、取得情報の信頼性は確保されない。

4.1.3　取引確認プロセスの効率性

情報取得の確実性と信頼性に加え、取引確認プロセスの効率性について検討することは、取引確認の実現可能性を確かめるうえで重要である。効率性は、確認者や参加者、その他の関係者（信用できる情報保有者等）が消費するリソース（例えば計算能力、データ容量、通信帯域）で測ることができる。秘匿化された取引情報の確認のために消費されるリソースは、DLT システムの構成によって異なるほか、利用可能な技術の変遷に伴い変化しうる。

概念的には、取引確認プロセスが過度の計算能力を必要とする、または確認者と参加者が取引ごとに情報のやり取りを必要とするようなネットワーク構成や確認プロセスとなっている際は、確認プロセスは十分に効率的ではないと考えられる。確認者が取引額を大量の取りうる値の中から見つけなければいけないような極端なケースにおいては、取引確認が実行不可能となるかもしれない。確認者が信用できる情報保有者から必要情報を取得すると、参加者と情報のやり取りをする必要がないため、取引確認プロセスは概して十分に効率的と考えられる。確認者が特定可能な参加者から必要情報を取得する場合、効率性はネットワークの構成により異なりうる。取引確認プロセスにおいて存在する情報保有者と 3 観点からの評価は、表 5 のとおりまとめられる。

【表 5】情報保有者別の 3 観点の評価

情報保有者	情報取得の確実性	信頼性	効率性
信用できる情報保有者	有	有	有
特定可能な参加者	有	共有台帳上に取得情報の正確性の検証に利用できる取引記録が存在するかによる	DLT システムおよび PET の構成による
その他の参加者	無	—	—

4.2 3 つの観点に基づく評価

本節では、特定の構成の PET について、上述の 3 観点に基づき評価する。この検討は、第 2 章で提示した DLT に基づく FMI モデル上で利用されうる、一部の PET 構成に対象を絞っており、網羅的ではない。従って、別のモデルのもとで同様の検討を行うと、異なる評価結果になる可能性がある。

4.2.1 Corda における共有先制御手法

Corda では、validating notary または non-validating notary の活用を含め、いくつかの異なるシステム構成が可能である。Corda の設計上、すべての取引に関する情報が notary に共有される。また、確認者は、参加者から取引情報の送信を受ける observer node[31]を運用することもできる。

Validating notary は取引情報を解釈可能な形式で受領し、当該取引を検証する[32]。Validating notary の検証を受けていない取引は有効とはみなされない。確認者が信用できる情報保有者の役割を担っている validating notary から必要情報を取得する場合、情報取得の確実性、信頼性、および十分な水準の効率性が確保されると考えられる。

Non-validating notary は取引情報を解釈できない形式で受領するものの、当該情報の送信者情報については解釈可能な形式で保管する[33]。確認者は、取引確認にあたって参

[31] 複数の DLT 基盤において、確認者が利用する DLT ノードに必要情報が共有される仕組みを構築することで、取引情報の確認可能性を確保しようという共通の発想が認められる。こうしたノードは一般的に、supervisory node または observer node と呼ばれている（例えば、https://docs.corda.net/tutorial-observer-nodes.html や Federal Reserve of Boston「Beyond theory: getting practical with blockchain」（2019 年 2 月）を参照）。

[32] https://docs.corda.net/key-concepts-notaries.html を参照。

[33] 前掲脚注参照。

加者から必要情報を取得する必要があるものの、non-validating notary に保管されている情報を用いることで、取得情報の正確性を検証できるほか、非協力的な参加者を特定できる。このため、non-validating notary を取引確認プロセスに用いると、validating notary を信用できる情報保有者として利用するのに比べて効率性は落ちるものの、情報取得の確実性と信頼性は確保される。効率性を改善するため、確認者は observer node を運用して non-validating notary とともに利用することも可能である。これは、参加者ノードの設定により、observer node をすべての取引情報のやり取りに含めることで実現されうる。

4.2.2 Hyperledger Fabric における共有先制御手法

Hyperledger Fabric では、各チャネルで行われた取引情報がすべて ordering service に送信されるため、確認者はこれを通じて必要情報を取得することができる[34]。Ordering service は信用できる情報保有者とみなすことができ、従って、情報取得の確実性、信頼性、および十分な水準の効率性が確保される。

上記プロセスの代わりに、確認者はネットワーク上で observer node を運用することもできる。ネットワークの設定により、当該ノードが全チャネルに参加し、個別の取引情報が共有されるようにすることで、確認者は必要情報を取得することが可能になる。この場合、情報取得の確実性および信頼性は確保される。効率性に関しては、確認者は observer node を運用することで多少の追加的負担を負うことになる。

4.2.3 ペイメントチャネル

ペイメントチャネルでは、ペイメントチャネルの開設・閉鎖にかかる取引情報のみが台帳に記録され、個別の取引情報は記録されないため、確認者は、取引当事者から取引情報を共有される必要がある。取引当事者は開設・閉鎖取引において解釈可能な形式で記録されるため、情報取得の確実性は確保される。しかし、確認者は取得情報について、あるペイメントチャネルで行われた全取引をネッティングした額が開設・閉鎖取引の額に対応するかは確認できるものの、個別の取引情報が正しいかは検証できない。従って、信頼性は確保されない[35]。

---

[34] 本報告書執筆時点でのバージョンでは、取引情報は解釈可能な形式で ordering service に伝達されている。

[35] 実際は、ペイメントチャネル・ネットワークでは送金が複数の中継者を介して行われることが多い。こうした送金では、取引確認の複雑性が増す可能性がある。

ネットワークにペイメントチャネル・ハブが存在する場合、当該ハブが信用できる情報保有者の役割を担い、すべての取引情報を確認者と共有することが想定できる。このときは、情報取得の確実性および信頼性は確保される。さらに、参加者が確認者に対して取引情報を提出する必要がないため、この取引確認方法は十分に効率的と考えられる。

4.2.4 Quorum におけるプライベート・トランザクション

Quorum におけるプライベート・トランザクションでは、取引情報のハッシュ値および送金者情報が共有台帳に記録される。確認者は、送金者情報に基づき、当該参加者から取引情報の提出を受けると、台帳に記録されたハッシュ値と照合することでその正確性を検証することができる。従って、この取引確認プロセスでは、情報取得の確実性と信頼性が確保される。一方で、確認者と参加者の間で必要情報のやり取りが必要とされるため、効率性は低下する。

効率性を向上させるための有効な手法として、observer node の使用が挙げられる。参加者ノードの設定により、すべての取引情報が observer node に送信されるようにすることで[36]、参加者が追加的な負担を負うことなく、十分な水準の効率性が確保された取引確認プロセスを確立できる。

4.2.5 Pedersen commitment

Pedersen commitment を用いると、取引当事者に関する情報は確認者にとって解釈可能である一方、取引額はコミットメントに置き換えることで非可読化される。このコミットメントを解釈するために、確認者は取引当事者から blinding factor および/または取引額を共有される必要がある。

Pedersen commitment は送金者・受領者の情報は解釈可能なため、情報取得の確実性は確保される。加えて、確認者は取得情報からコミットメントを計算し、台帳に記録されたものと照合することによって、取得情報の正確性を検証することができるため、信頼性も確保される。Blinding factor と取引額が確認者に共有されている場合、取得情報からコミットメントを求める際の計算負担は極めて小さいため、取引確認プロセスは十分に効率的だといえる。他方、確認者が blinding factor のみ共有され、取引額が取りうる値の個数が限定されていない場合、確認者は取引額を総当たり方式で計算する必要が

[36] 「always-send-to」オプションを有効にすることで、送信者が取引情報の共有先として特段設定せずとも、全プライベート・トランザクションの情報が observer node に共有される（https://github.com/jpmorganchase/tessera/wiki/Configuration-overview を参照）。

あるため、所要の計算負担は大幅に増大する。従って、効率性の観点から、確認者は blinding factor と取引額の共有を要求すると考えられる。Pedersen commitment を使用した取引情報の確認にかかる実機検証については、第 5 章を参照のこと。

4.2.6　ゼロ知識証明

ZKP の実装にはさまざまなものがあるため、3 観点からの評価は具体的な実装方法によって異なる。ZKP を用いて送金者・受領者情報が秘匿化される場合、確認者は共有台帳に記録された情報から取引当事者を特定することはできない。従って、情報取得の確実性は確保されない。あるアプリケーションでは、指定された第三者に対して、実際の取引情報を閲覧可能にする機能（viewing keys）が開発されているものの、確認者がこの key を参加者から共有される必要がある限りにおいては、情報取得の確実性は確保されない[37]。

4.2.7　ワンタイムアドレス

本手法は、台帳に記録される各取引で異なるアドレスを用いることを可能にする。従って、確認者は、すべてのアドレスを取引当事者と紐付ける必要がある。このためには、参加者が確認者にそれぞれの取引で用いたアドレスを共有する必要がある。もっとも、参加者が使用したアドレスを確認者に共有しなかった場合、確認者が当該参加者を特定するのは容易ではない。このため、情報取得の確実性は確保されない。第 5 章では、HD ウォレットを用いて生成されたワンタイムアドレスの取引確認にかかる実験について詳述している[38]。

4.2.8　ミキシング

ミキシング（中央集中型および P2P 型）を用いると、混合し集約された取引のみが台帳に記録される。中央集中型ミキシングサービスが用いられる場合、ミキシングを提供する主体は参加者から受領した実際の取引情報を保持している。確認者は当該主体を信用できる情報保有者として扱い、送金者・受領者を紐付けるための情報を提供させるこ

---

[37] ZKP は取引情報の一部を非可読化するために用いることも可能である。

[38] 同一の参加者が使用したとみられるワンタイムアドレスをみつける手法（address clustering）や、それらのアドレスを実際の参加者に紐付ける手法（address tagging）が存在する。もっとも、こうした手法の取引確認への応用は、本報告書の射程外としている。Address clustering や address tagging についての詳細は、M. Spagnuolo、F. Maggi、S. Zanero「Bitiodine: extracting intelligence from the Bitcoin network」（2014 年 3 月）を参照。

とができる。よって、情報取得の確実性と信頼性は確保されうる。加えて、この取引確認プロセスは参加者からの情報提供を必要としないため、十分な水準の効率性も確保される。

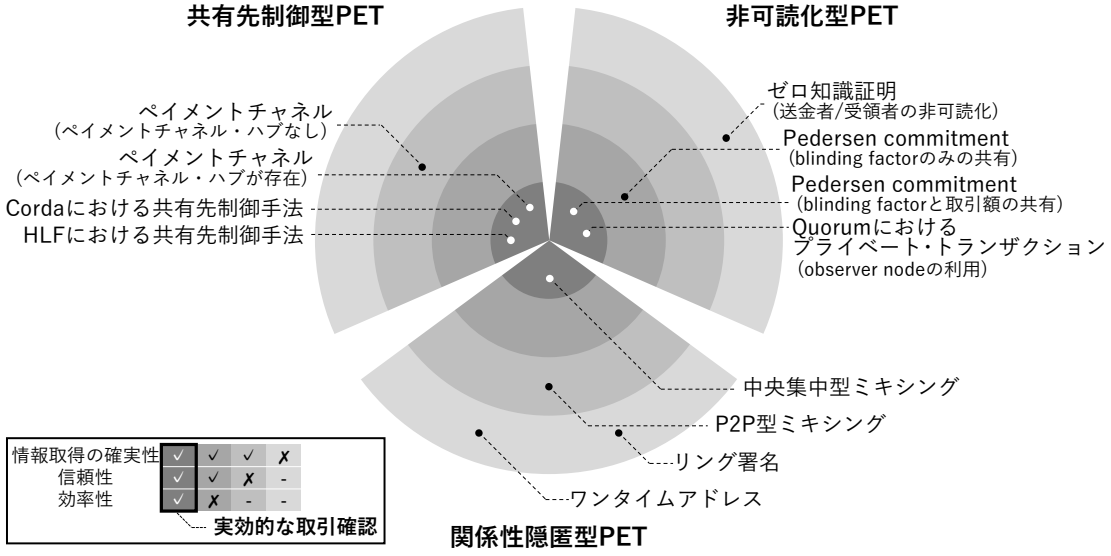
ミキシングが P2P 方式で行われる場合、確認者を含む第三者は、台帳に記録された情報からは参加者間の取引関係を確定することができない。このため、確認者は特定可能な参加者に実際の取引関係に関する情報を提供させることはできるが、取得情報の正確性を検証する術を持たない。従って、情報取得の確実性は確保されるものの、信頼性は確保されない。

4.2.9　リング署名

リング署名は、送金者・受領者の取引関係を切断することで秘匿性を確保する。確認者は、台帳上に記録された取引情報を閲覧できるものの、署名した可能性のある参加者の集合（リングメンバ）から送金者を特定することはできない。送金者はリングメンバの許可を得ることなく当該メンバの公開鍵を使用できるため、第三者が送金者を特定するための証跡は残らない。従って、リング署名が使用されている場合には、情報取得の確実性は確保されない。

図表 8 では、各 PET における一部の取引確認プロセスを 3 観点から評価した結果についてまとめている。

【図表 8】一部の取引確認プロセスに対する評価結果



4.3 実用化に際しての追加的論点

本節では、実用化に際してさらに検討されるべき論点を提示する。

4.3.1 信用できる情報保有者を活用する際の論点

本章で実効的な取引確認が可能と評価された PET 構成のいくつかは、必要情報を集中的に保管する、信用できる情報保有者を活用している。DLT システムに存在する中央集権的なコンポーネントまたは信用できる第三者を情報提保有者として活用することは、実効的な取引確認のために満たすべき 3 観点からの評価のすべてにおいて明確な利点があるものの、こうした主体は取引確認プロセスの単一障害点になりうる。さらに、こうした主体はネットワークの単一障害点にもなるため、分散型システムのメリット（例えば頑健性や可用性）を打ち消す可能性もある。

PET の実行を可能にする単一の主体が存在する場合、当該主体の機能不全は秘匿性が確保された取引の実現に支障をきたす。さらに、すべての取引情報を保管している単一の主体が存在する場合、セキュリティ違反によって全参加者の取引の詳細情報が漏えいする危険性がある。DLT の運営にあたって重要な単一のコンポーネントが存在する場合、このコンポーネントの障害は DLT ネットワーク全体の機能性を毀損しうる。

4.3.2 PET を組み合わせて使用する際の論点

第 3 章で述べたとおり、取引情報の秘匿性を強化するために複数の PET が補完的に使用されるケースがある。もっとも、PET が組み合わせて使用される際には、秘匿性の強化と実効的な取引確認の間にトレードオフが発生しうる。取引確認プロセスの効率性が低下する可能性があるほか、情報取得の確実性と信頼性が毀損される可能性がある。下記では、一例として、Pedersen commitment と HD ウォレットを組み合わせて使用するケースについて簡単に考察する。

Pedersen commitment は取引額を非可読化する一方、HD ウォレットは取引情報に使用されている仮名と送金者・受領者との関係性を切断する。これらの PET を組み合わせて使用することで、取引情報の秘匿性は強化される。Pedersen commitment が単体で使用されていると、確認者は取引当事者を特定することが可能だが、これを HD ウォレットと組み合わせることによって、参加者が確認者に協力しない場合に確認者が取引当事者を特定できない可能性が生じる。このため、この組み合わせにおいては、情報取得の確実性は確保されない。

4.3.3　複数のシステム間の連携、階層型のシステム、エンドユーザの導入にあたっての論点

本報告書は、単一の DLT ネットワークにおいて取引が行われる単純なモデルを仮定している。実用化に際しては、複数のシステムを跨いだ取引や階層型のシステムでの取引にも適用可能とするために、このモデルを拡張する必要がある。こうした拡張は、特にシステム間・階層間で取引情報の秘匿性および確認可能性について異なる要件設定がなされている場合に、追加的な課題を生じさせうる。システム内では秘匿化と確認可能性を両立しつつ、システム間の異なる規格やプロセスを調整する必要がある。

本報告書は、バックエンドの仕組みについて検討しており、エンドユーザは考慮の対象外としている。エンドユーザが導入されると、台帳に記録されるエンドユーザ関連情報の管理が複雑になりうるほか、取引確認の対象となる取引の決定方法についての適切な基準策定が必要となる。

4.4　まとめ

PET を適用している DLT システムにおける取引情報の確認可能性を評価する際には、必要情報の取得の確実性、取得情報の信頼性、取引確認プロセスの効率性、の 3 観点から行うことができる。実効的な取引確認が行われるためには、DLT システムは各観点において、十分な評価を得る必要がある。これらの観点は、取引情報の秘匿化と確認可能性を両立するような DLT システムの設計に関する議論において参照できる。

これら観点から取引確認プロセスを評価すると、PET の実装方法によって確認可能性の度合が異なることが分かる。一方では、取引確認が不可能なものがあり、もう一方では実効的な取引確認が可能なものがある。実効的な取引確認は、(1) 確認者が信用できる情報保有者から必要情報を取得する場合、または、(2) 確認者が特定可能な参加者から必要情報を取得し、その取得情報の正確性を台帳に記録された情報を用いることで検証可能で、これらのプロセスを過大なリソースを消費せずに実行可能である場合に可能となる、との結果を得た。

これまでの評価に基づき、PET の分類ごとに、取引可能性にかかる特徴を演繹することができる。共有先制御型 PET では、確認者が取得情報の正確性を検証するために利用できるような、すべての取引情報を記録した共有台帳が存在しない。このため、実効的な取引確認のためには、確認者が分割された台帳のすべてから情報を取得するか、全取引情報を情報保有者から取得する必要がある。非可読化型 PET では、非可読化された取引情報が共有台帳に検証可能な形式で記録されている。従って、実効的な取引確認の

ためには、必要情報の取得の確実性を確保することが鍵となる。関係性隠匿型 PET の特徴は、共有台帳に記録された取引情報から、取引関係を識別できないようにする点にある。従って、実際の送金者・受領者およびその取引関係についての情報を保管し、確認者に共有するための仕組みの整備が、実効的な確認のための必須要件となる。

本章では、実用化に際しての追加的な論点も提示した。信用できる情報保有者の存在は、ネットワークに対して単一障害点リスクをもたらしうる。取引情報の秘匿性を強化するために PET を組み合わせて使用することと実効的な取引確認の間にはトレードオフが存在しうる。複数のシステムの連携、階層型のシステム、エンドユーザの導入のためにモデルを拡張することで、追加的な課題が生じうる。

5 PET に関する実機検証

本章では、Pedersen commitment と HD ウォレットについて、それらの動作原理と技術特性を解説し、第三者による取引確認可能性の観点から実施した実機検証の内容を紹介する。これらは、非可読化型と関係性隠匿型の基本的な概念を代表する PET であり、さまざまなプロジェクトで利用されている。第 4 章で論じたとおり、実効的な取引確認は、Pedersen commitment が用いられる際は可能である一方、HD ウォレットが用いられる際は、必要情報の取得の確実性が確保されないため、困難である。ステラ・フェーズ 4 では、これらの PET が用いられた DLT ネットワーク上で、実効的な取引確認プロセスを設計可能であるかを確認するために、実機検証を実施した。以降の節で、これら 2 つの PET について、理論的に説明したうえで実機検証の結果を解説する。

5.1 Pedersen commitment

Pedersen commitment は非可読化型に分類される PET である。第 3 章で説明したとおり、本手法は取引額を秘匿するために用いることができ、さまざまな DLT 上の支払・決済アプリケーションで活用が可能である。本章における実機検証の解説では、UTXO に基づくシステムを想定している[39]。

5.1.1 技術的解説

Pedersen commitment は、複数の取引額のコミットメント（取引額から計算される暗号値）の和が、それぞれの取引額の和から求まるコミットメントに等しいという基本的な性質を持つ。すなわち、2 つの値 v_1 と v_2 について、コミットメント C が $C(v_1) + C(v_2) = C(v_1 + v_2)$ を満たすということである。

この性質に基づき、一連の取引額 $\{v_i\}$ が $v_1 + v_2 = v_3 + v_4$ を満たすとき、これらの取引額に対応するコミットメント $\{C_i\}$ が $C_1 + C_2 = C_3 + C_4$ を満たすように計算できる（以下では単純化のために $1 \leq i \leq 4$ と仮定する）。これにより、送金者は取引額をコミットメントに置き換えることで、実際の取引額を開示することなく検証可能な、秘匿化された取引情報を作成できる。

Pedersen commitment の一般的な実装では、コミットメントは、4 つの異なるパラメ

[39] Unspent transaction output（UTXO）は、取引額を表現する形式の 1 つである。各取引は単数または複数の入力額と、単数または複数の出力額を持ち、取引は、入力額の合計値と出力額の合計値に基づいて検証される。

ータを用い、楕円曲線暗号に基づく計算によって作成される。これらのパラメータのうち G と H は、楕円曲線上の 2 つの異なる生成元であり、一般的に DLT ネットワークの構築時に選択される。これらの生成元がネットワークの全参加者に共有されることで、コミットメントによる取引を検証することが可能になる。3 つ目のパラメータ bf は blinding factor と呼ばれ、送金者によって選択される。最後のパラメータが秘匿すべき取引額 v である。これら 4 つのパラメータを用いて、コミットメントは以下のように計算される。

$$C = bf \cdot G + v \cdot H$$

Pedersen commitment は以下の特徴を有している。フェーズ 4 では、これらの特徴について実機検証を通じて確認した。

- Blinding factor を適切に選択することにより[40]、一連の取引額 $\{v_i\}$ からコミットメント $\{C_i\}$ を計算でき、第三者は $v_1 + v_2 = v_3 + v_4$ が満たされていることを、各取引額を用いずにコミットメントのみを用いて検証できる。
- $v_1 + v_2 \neq v_3 + v_4$ であるような取引額に対して、$C_1 + C_2 = C_3 + C_4$ を満たすような $\{C_i\}$ を計算することは、計算量の観点から実行不可能である。従って、取引情報に不正な取引額を含めることは不可能である。
- もしも取引額に負値が含まれていたとしても、$v_1 + v_2 = v_3 + v_4$ を満たす限りは各コミットメントを計算でき、負値が含まれていることは完全秘匿される。従って、出力額に負値を含めることで、入力額の合計値よりも大きな出力額が得られる取引を作成することが可能となる[41]。
- $H = x \cdot G$ を満たす x が存在し、これは離散対数と呼ばれる。x の算出は計算量的に実行不可能であるが、もし仮にある参加者が x を知り得た場合、拘束性と呼ばれる Pedersen commitment の安全性の条件が失われ、コミットメントに含まれる取引額の書換えが可能になる[42]。

---

[40] コミットメントの和が和のコミットメントと等しくなるためには、各 blinding factor を $bf_1 + bf_2 = bf_3 + bf_4$ を満たすように選択しておく必要がある。

[41] 負値の取引額を含めるような不正を防ぐため、実際には、Pedersen commitment は範囲証明と呼ばれる仕組みと組み合わせて利用される。

[42] 実際には、G と H は、離散対数の仮定が破られないことを参加者が確認できる方法で決定される。一般的には、これらパラメータを計算するプロセスが公開されていることで、確認ができる。計算するプロセスが公開されていない場合、参加者は、パラメータを決定した本人が離散対数 x を知っている可能性を疑うことになる。

5.1.2 Pedersen commitment における取引確認

Pedersen commitment における取引の確認可能性は、コミットメントを解釈し、秘匿化された取引額を検証するための確認者の能力と定義できる。実機検証では、確認者がコミットメントで隠された取引額を確認する方法を分析した。コミットメントを解釈するためには、確認者は blinding factor および/または秘匿化された取引額に関する情報が必要となる。フェーズ 4 では、参加者が確認者と共有する情報の種類に関する 3 つのシナリオを定義し、実機検証を通じてその実行可能性を分析した。

- 確認者が blinding factor と実際の取引額の両方を受領した場合、取得した情報の正確性を常に確認できる。従って、取得情報が正確であれば、取引確認は可能となる。
- 確認者が blinding factor に対する公開鍵（$bf \cdot G$）と実際の取引額を受領した場合、情報の提供者から、bf を用いて作成された署名も受け取り、取引額の正確性を確認する必要がある[43]。取得情報が正確であれば、取引確認は可能となる。
- 確認者が（i）blinding factor もしくは（ii）blinding factor の公開鍵と署名のみを受領し、取引額が含まれていない場合、コミットメントに含まれる実際の取引額を即座に見つけることはできない。総当たり方式による取引額の推測は可能ではあるが、取引額が取りうる値の個数が限定されていない場合では、計算するのに相当の時間がかかる。

実機検証にて検討した取引確認のシナリオについて、第 4 章で論じたとおり、取引の確認可能性の観点では、必要情報の取得の確実性と取得情報の信頼性は確保されていると想定できる。しかしながら、確認者の計算負担を考慮すると、取引確認プロセスの効率性に差があることがわかる。確認者が (i) blinding factor と取引額、または (ii) blinding factor の公開鍵と署名、取引額を受領した場合、計算負担は極小であり、取引確認プロセスは十分に効率的であるとみなせる。一方、確認者が blinding factor のみを受領し、かつ取引額が取りうる値の個数が限定されていない場合、より大きな計算負担がかかり、取引確認プロセスが十分な効率性を持って実施できないことが予想される。

5.2 HD ウォレット

HD ウォレットは、関係性隠匿型に分類される PET である。ワンタイムアドレスの優れた管理機構である HD ウォレットの基本思想は、1 つの秘密の値から無数の鍵を導出する鍵生成機能である。HD ウォレットはビットコインの開発コミュニティにより提案・

---

[43] ある C と任意の v に対して、公開鍵（$bf \cdot G$）自体は誰でも計算することができる（$bf \cdot G = C - v \cdot H$ の計算が可能であるため）。そのため、確認者は送金者が bf を知っているかどうかを確認する必要がある。

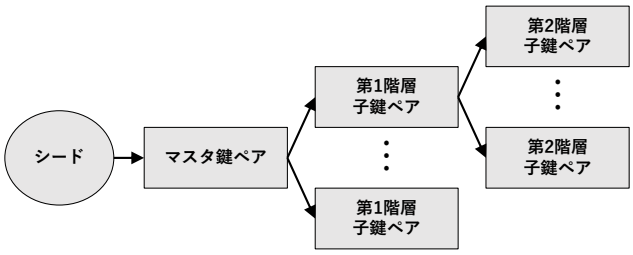
定義され[44]、さまざまなウォレットアプリケーションで実装されている。

5.2.1 技術的解説

HD ウォレットにおいて、すべての鍵は一つの生成元（シード）から導出される（図表 9)。まず、シードに適切な変換を施し、その他の鍵導出の起点となるウォレットのマスタ秘密鍵を生成する。このマスタ秘密鍵を用いることで無数の鍵が導出され、導出されたそれらの鍵はさらに無数の鍵の導出に用いられる[45]。より一般的には、HD ウォレット内の任意の鍵は、無数の子鍵を生成するための親鍵とみなすことができる。従って、HD ウォレットは大量の鍵を木構造の形式で保持することを可能にするとともに、ウォレットの所有者はシードとそれぞれの鍵の導出パス[46]のみを管理しておけばよい。

鍵導出には、通常鍵導出と強化鍵導出の 2 種類の方法が存在する。通常鍵導出には、秘密鍵導出と公開鍵導出の手法があり、そのうち通常公開鍵導出では、親秘密鍵の情報を用いることなく、親の拡張公開鍵のみを用いて子公開鍵を導出できる。このため、第三者に秘密鍵の情報を一切伝えることなく公開鍵（アドレス）情報の一部を伝える必要がある際には、通常公開鍵導出を用いることが推奨される。強化鍵導出は、ウォレットの所有者が秘密鍵をより安全に導出する方法として利用される。以下では、通常公開鍵導出を用いた取引確認の手法について議論する。

【図表 9】HD ウォレットにおける階層的な鍵導出



フェーズ 4 では、以下で述べる HD ウォレットの機能・特徴について、実機検証を通じ

---

[44] BIP-0032（https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki）および BIP-0044（https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki）を参照。

[45] 鍵導出は、親鍵自体に加えて、追加的な情報を用いることで実行される。鍵と追加情報を含めたものを「拡張鍵」と呼ぶ。

[46] 導出パスは導出木における位置を表す索引である。例えば、「m/1/2/3」という導出パスは、「マスタ鍵の 1 番目の子鍵の 2 番目の子鍵の 3 番目の子秘密鍵」を表す。ここで、「m」で始まるパスは秘密鍵を指し、「M」で始まるパスは公開鍵を指す。また、パスにアポストロフィ（'）が付記された箇所は強化鍵導出によって、付記されていない箇所は通常鍵導出によって、鍵が導出されたことを示す。

て確認した。

- 複数個の単語[47]をもとにシードを生成し、シードを変換することでマスタ秘密鍵を導出する。
- 強化鍵導出、通常秘密鍵導出、通常公開鍵導出の 3 つの機能を実装する。
- 通常鍵導出にて、親の拡張公開鍵に加えて子秘密鍵が 1 つでも漏洩すると、その親秘密鍵から導出される全情報が明らかになってしまうという欠点を確認する。なお、この欠点は強化鍵導出では生じない。

5.2.2 HD ウォレットにおける取引確認

第 4 章にて論じたとおり、HD ウォレットにおいては、必要情報の取得の確実性が保証されないため、実効的な取引確認はできない。この点は、ある参加者が取引で使用したすべての仮名（公開鍵/アドレス）を確認者は特定できるかという観点で行った実機検証を通じて確認した。秘密鍵を第三者に共有すべきではないため、フェーズ 4 では、親の拡張公開鍵から子公開鍵を導出できる通常公開鍵導出を前提として実機検証を行った。ある参加者の拡張公開鍵を確認者が持っていれば、子公開鍵を導出し、それらの鍵が用いられた取引の確認ができるようになる。

情報取得の確実性の観点から HD ウォレットの確認可能性を分析するため、フェーズ 4 では以下のシミュレーションを実施した。

- ある参加者が HD ウォレットを用いて多数のアドレスを生成し、それらが個々の取引で用いられた状況を想定する。本検証では、200 個のアドレスをいくつかの法則に従って生成した。
- 拡張公開鍵と導出パスが確認者に共有された場合、確認者はすべてのアドレスを復元し、それぞれの取引情報を実効的に確認できる。
- 導出パスを除く拡張公開鍵のみが確認者に共有された場合、確認者は導出される可能性のあるアドレス（約 20 億個のアドレスが 1 つの親拡張公開鍵から導出可能）をすべて生成し、それぞれの取引で使われたアドレスと照合する必要がある[48]。この計算には取引確認の実施が非現実的なほど、長時間の計算およびそれに伴う計算負担がかかることを確認した。
- 仮に、取引に用いられたアドレスが確認者に共有された拡張公開鍵から導出された

---

[47] BIP-0039（https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki）を参照。

[48] 特定の状況下では、確認者が参加者による鍵導出の法則性を発見し、取引確認が実施可能となりうる。

ものではなかった場合、確認者には取引当事者を特定するための有効な手段がない。

これらの実機検証の結果から、参加者が確認者に協力しなかった場合（例えば、何らかの理由で、共有した拡張公開鍵から導出されたものではないアドレスを使用した場合や、導出パスを共有しない場合）には、情報取得の確実性が確保されないことは明確である。これは、確認者には特定の参加者が使用したすべてのアドレスを確実に生成することができないからである。実効的な取引確認のためには、確認者が取引当事者を特定できるように、参加者が鍵を導出し使用する仕組みが必要である。