（日本銀行仮訳）

EUROPEAN CENTRAL BANK
EUROSYSTEM

BANK OF JAPAN

Project Stella：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

クロスボーダー取引における支払の同期化

2019 年 6 月

目次

１．　はじめに 1
２．　先行分析とステラ・フェーズ３の主な結果 4
２．１　台帳間の相互運用性に関する先行分析 4
２．１．１　中央銀行による主な研究成果 4
２．１．２　民間部門における主な取り組み 5
２．２　ステラ・フェーズ３の主な分析結果 6
３．　台帳間支払のプロトコル 9
４．　支払方法 15
４．１　Trustline 16
４．２　On-ledger hold/escrow using HTLC 19
４．３　Third party escrow 20
４．４　Payment channels 20
４．４．１　Simple payment channel 22
４．４．２　Conditional payment channel with HTLC 23
４．５　５つの支払方法における台帳の機能要件 24
４．６　まとめ 25
５．　実機検証 26
５．１　検証概要 26
５．２　中央集権型台帳での実験 27
５．３　分散型台帳での実験 28
５．３．１　ILP を用いない実験 28
５．３．２　ILP を用いた実験 29
５．４　異なるプラットフォーム間での実験 29
５．５　実験結果 30
６．　支払方法の評価 30
６．１　安全性 30
６．２　資金効率性 35
６．３　まとめ 36
７．　追加の検討事項 37
７．１　各支払の安全性と支払経路全体のアトミック性 37
７．２　台帳の処理速度や稼働時間による影響 38
７．３　フリー・オプション問題 39

※本稿は日本銀行および欧州中央銀行による報告書「Synchronised cross-border payments」（本文）の日本銀行決済機構局による仮訳である。

Project Stella

クロスボーダー取引における支払の同期化

１．　はじめに

分散型台帳技術（DLT）の登場に伴い、資金・証券決済を支える金融市場インフラについて活発な議論がなされている[1]。プロジェクト・ステラは、2016 年 12 月に開始された、欧州中央銀行（ECB）と日本銀行による共同調査であり、概念的な調査と実験を通して、DLT が金融市場インフラに対してもたらし得る潜在的な利点や課題を洗い出し、議論を促進することを目的としている。今次報告書（以下では、ステラ・フェーズ 3 と呼称する）は、これまで公表した２つの報告書――フェーズ１（DLT を用いた大口資金決済、2017 年 9 月公表）[2]とフェーズ２（DLT 環境における資金と証券の受け渡しを紐付ける DVP、2018 年 3 月公表）[3]――により得られた知見に基づき組み立てられている。ステラ・フェーズ 3 では、異なる通貨圏を跨ぐクロスボーダー支払に関する革新的な仕組み（ソリューション）について調査を行っている[4]。

クロスボーダー支払は、複数の法域を跨ぎ、多数の主体を経由する。クロスボーダー支払に対する需要が高まっている中、クロスボーダー支払は、国内支払と比べ、時間やコストがかかるという特徴がある[5]。とりわけ、情報伝達や電文の標準化が未整備である

---

[1] 他の中央銀行において行われた主な調査プロジェクトについては、日本銀行「決済システムレポート」（2019 年 3 月）参照。

[2] 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）。

[3] 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）。

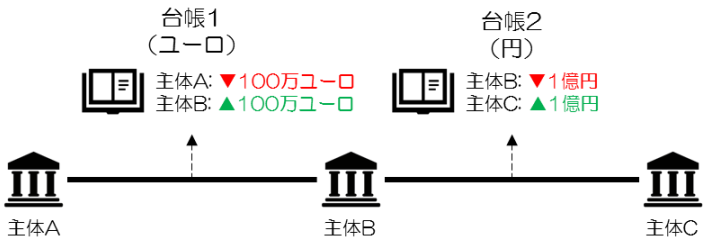
[4] 今次調査には、ECB（市場インフラ・決済総局）から Dirk Bullmann （チームリーダー）、Andrej Bachmann、Giuseppe Galano、Josip Kenjeric、Cedric Humbert、Anna Kearney、Diego Castejon Molina、日本銀行から岸道信（チームリーダー）、飛弾則雄、榎本英高、奥地俊夫、松嶋徹郎、松井茜美佳、小早川周司（明治大学教授および日本銀行ステラチームアドバイザー）が参加した。

[5] BIS 決済・市場インフラ委員会（Committee on Payments and Market Infrastructures＜CPMI＞）「クロスボーダーリテール決済」（2018 年 2 月）、および、同「コルレス銀行業務」（2016

ため、しばしば、システム間のシームレスな相互運用性が妨げられている。クロスボーダー支払にかかるこうした非効率性に対処する取り組みは行われているが[6]、安全性の観点からは、複数の台帳を経由することに伴う課題が残ったままである[7]。

図表 1 が示すように、クロスボーダー支払が完結する前に当事者が破綻した場合に、信用リスクが顕現化する可能性がある。この単純化された事例では、主体 A は、主体 B（例えば中継銀行）に 100 万ユーロを送金することを通じて、主体 C に 1 億円を送金しようとしている[8]。主体 B は、ユーロ建ておよび円建て台帳双方に口座を有しており、主体 A のために 1 億円を送金する。もし主体 B が 1 つ目の取引（例えば、主体 A から主体 B への 100 万ユーロの送金）が完了した後であるが、 2 つ目の取引が完了する前に破綻した場合には、主体 A は資金を失うリスクに晒される。こうしたリスクは、支払が同期化され、資金が固定されれば、削減可能である。しかし、現状では、こうした送金の同期化はほとんど実現していない。

【図表 1】クロスボーダー送金で信用リスクが顕現化する単純化された事例



こうしたことを背景に、ステラ・フェーズ 3 では、新たな技術を用いることにより、ク

年 7 月）参照。

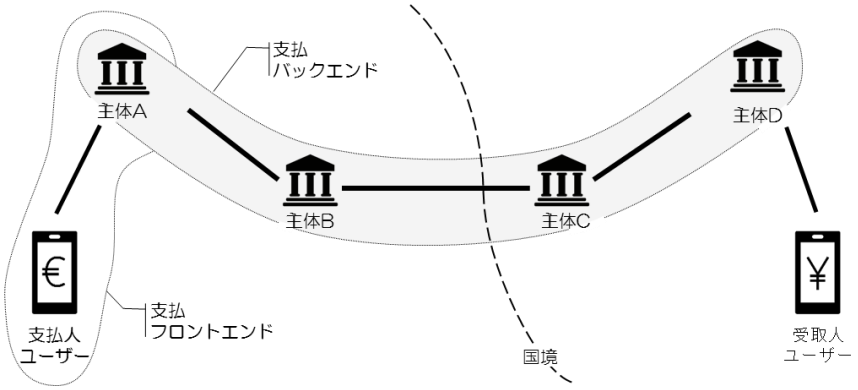
[6] 例えば、ISO 20022 の採用による電文フォーマットの標準化などが挙げられる。

[7] クロスボーダー支払は、送金の安全性や効率性を妨げる多くの要因を伴っている。例えば、法域間における法律や規制面での基準、複数通貨の利用や複数台帳が関係することに伴うインプリケーション等の差異などがあげられる。この共同調査は、複数台帳の関与に関する側面について分析している。

[8] ここでの数値例では、主体 B は 1 ユーロ ＝ 100 円で通貨を交換するものとする。

ロスボーダー支払が、特に安全性の面で改善しうるか検証している。具体的には、「台帳間支払のためのプロトコル」をベースに、①中央集権型台帳（民間銀行によって運営されている台帳や中央銀行によって運営されている即時グロス決済＜RTGS＞システムなど）と DLT 台帳の間、②DLT 台帳間、さらには、③中央集権型台帳間での、グローバルな相互運用性について分析している（図表 2）。

【図表 2】クロスボーダー支払方法のイメージ



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。プロジェクト・ステラは、金融市場インフラの分野における 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たものである。

第 2 章は、DLT の潜在的な利用に関する先行分析を確認しつつ、本調査結果の概要を示す。第 3 章では、「台帳間支払のためのプロトコル」の概念の概要と、当該プロトコルがどのように機能するのかにつき、詳細を説明する。第 4 章では、今回取り上げる支払方法と、各支払方法によってそれぞれ必要となる台帳の要件を示す。第 5 章では、当該プロトコルを用いて ECB と日本銀行の技術者が行った実験内容を示す。第 6 章では、特定の支払方法を安全性と効率性の面から評価する。第 7 章は安全性、効率性に止まらない観点に触れている。

２．　先行分析とステラ・フェーズ３の主な結果

２．１　台帳間の相互運用性に関する先行分析

幾つかの公的機関や民間機関では、異なる台帳の相互運用性を高め、クロスボーダー支払における決済の同期化を可能とするような、革新的なソリューションを探る試みが進められている。以下では、そうした取り組みの概要を幾つか紹介する。

２．１．１　中央銀行による主な研究成果

英国銀行（BOE）は、自ら運営する RTGS サービスの更新に係る調査の一環として、他の決済システムと RTGS との決済の同期化を含む幅広い相互運用性について、調査を行った[9]。具体的には、大口クロスボーダー支払のシナリオの下で、２つの異なる台帳間での同時決済について、実証実験（Proof of Concept）が行われた[10]。また、BOE は、同時決済のモデル案を示したが、そこでは、信頼された第三者が同時決済サービスを提供することが想定されている。同時決済サービスは、台帳間かつ通貨間で同時決済を実現しうるものとされている[11]。

カナダ中央銀行（BOC）とシンガポール通貨庁（MAS）は、ハッシュ・タイムロック・コントラクト（Hashed Timelock Contracts、以下 HTLC[12]）を用いて２つの DLT 基盤間の相互運用性に関する実証実験を行った。HTLC については、ステラ・フェーズ２において詳しく述べられている[13]。両行は、異なる DLT 基盤を用いた RTGS システム間のクロスボーダー大口送金についてシミュレーションを行った。

---

[9] Bank of England「A blueprint for a new RTGS service for the United Kingdom」（２０１７年５月）。

[10] Bank of England「FinTech Accelerator Proof of Concept: exploring the synchronised settlement of payments using the Interledger Protocol」（２０１７年７月）。

[11] Bank of England「Call for interest: Synchronised settlement in central bank money」（２０１８年８月）。

[12] HTLC の詳細については、本報告書の 4.2 節および原文の別添１を参照。

[13] Bank of Canada、Monetary Authority of Singapore「Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies」（２０１９年５月）。

２．１．２　民間部門における主な取り組み

World Wide Web Consortium（W3C）内のコミュニティグループはインターレジャープロトコル（Interledger Protocol、以下 ILP）――異なる台帳間での支払を可能とするための規約（プロトコル）――の策定を進めている[14]。ILP は、ホワイトペーパー「A Protocol for Interledger Payments」（Thomas and Schwartz、2015）で開示された原案を基に、開発されている[15]。本報告書の第 3 章では、ILP の基礎概念をより詳細に説明している[16]。

Ripple 社は、xCurrent を開発した。xCurrent は、RippleNet と呼ばれるグローバルネットワークを通じて参加金融機関を接続する。xCurrent は、ILP を基礎に作成されており、これにより、参加者間の双方向の情報疎通と台帳間の支払の連携が可能となっている[17]。

SWIFT は、参加金融機関のために新たな標準的手法を構築した。これは、SWIFT gpi（SWIFT グローバル・ペイメント・イノベーション）と呼称され、コルレス銀行ネットワークを通じたクロスボーダー送金のスピード、安全性、透明性を向上させたものである。SWIFT gpi には、３つの主な特徴点がある。まず、①決済の進捗状況を即座にモニタリングすることが可能となるエンドツーエンドの追跡データベースである。次に、②参加金融機関、取扱通貨、カットオフタイムなどの実務上の情報を提供するディレクトリ機能である。これにより、最適な送金経路を見出せる。さらに、③ビジネス慣行を発展させるために、新たに作られたルールへの他の参加金融機関の順守状況を、参加金融機関に対して周知する機能である[18]。

---

[14] https://www.w3.org/community/interledger/

[15] https://interledger.org/interledger.pdf

[16] Ripple 社は、2017 年 6 月に開催されたインターレジャーワークショップにおいて、ILP の公開実験を行った。

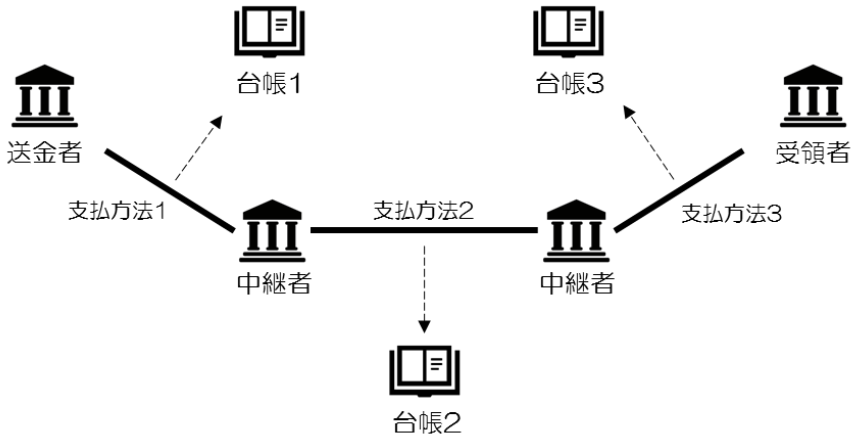
[17] https://ripple.com/files/ripple_solutions_guide.pdf

[18] https://www.swift.com/resource/swift-gpi-brochure

２．２　ステラ・フェーズ３の主な分析結果

ステラ・フェーズ 3 では、クロスボーダー支払（図表 3 の概念図参照）を改善するための――特に安全性の面からの――革新的なソリューションを検証した。ステラ・フェーズ 3 は、プロジェクト・ステラの下で先行して行われた実験及び概念的な調査の上に成り立っている。また、他の中央銀行や民間機関によるこれまでの研究も考慮している（2.1 節参照）。

【図表 3】クロスボーダー支払を構成する支払の流れ



ステラ・フェーズ２[19]では、HTLC を用いた台帳間の決済に関する新たな方法を明らかにした。これは、決済を同期化させることにより、信用リスクの軽減を図ることができる可能性がある。

ステラ・フェーズ 3 では、こうした分析の射程を拡充し、前述したホワイトペーパー「A Protocol for Interledger Payments」で紹介されたプロコルを研究し、台帳の　種類の違いに拘わらず、異なる台帳間での支払を同期するプロトコルを示すことを試みた[20]。

---

[19] 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）。

[20] DLT 台帳と中央集権型台帳への適用可能性が一連の実験で確認された。この点は、第 5 章でさらに説明する。

また、ステラ・フェーズ 3 は、異なる種類の台帳間の支払に利用しうる、多様な支払方法について、安全性、効率性の面から検証している。

これらの支払方法とは、以下のとおりである。

（1）Trustline とは、支払人と受取人との台帳外での取決めであり、受取人が予め定められた条件を充足した場合に、支払人は支払を行うことを約束するものである。未決済金額の合計は、支払人の受取人に対する仕向限度額を上回ってはならない。

（2）On-ledger hold/escrow using HTLC（以下 on-ledger escrow）では、条件付支払が台帳に記録され、受取人が予め定められた条件を充足した場合に台帳によって支払が確実に行われる。

（3）Third party escrow は、概念的には on-ledger escrow と類似しているが、条件付支払を確実に行うのは、台帳の機能に依るのではなく、支払人と受取人双方から信頼されている第三者に依存する。

（4）Simple payment channel は、支払人と受取人が、台帳上の共通の特別口座に預け入れた資金の範囲内で、台帳外で支払を行う取決め。両者は、特別口座の一定部分に対する取り分を表わす署名付き指図を交換することを約束する。台帳において決済されるのは、複数の 2 当事者間支払の最終ネットポジションである。

（5）Conditional payment channel with HTLCs（以下 conditional payment channel）は、署名付き指図を台帳外で交換する点で simple payment channel に似ているが、これに加えて、受取人が事前に定めた要件を充足したかどうかに基づき、台帳が支払を確実に行うメカニズムが備わっている。

これら 5 つの支払方法は、それぞれ異なった特徴を有している。それぞれの特徴は、①個別の支払が台帳上で決済されるか、あるいは台帳外で記録されるか、②資金が固定されるか特別口座に移されるか、③予め定められた条件が充足されたときに、支払が

確実に行われるか、④台帳に対して条件付支払の強制機能や署名付き指図の処理など、特定の機能要件はあるか、により整理できる（表１参照）。

【表 1】支払方法と台帳の特定の機能要件の概要

支払方法	台帳上／外	資金の隔離・固定	条件付支払の強制	台帳の特定の機能要件
Trustline	台帳外	無	無	無
On-ledger escrow	台帳上	有	有（台帳による）	有
Third party escrow	台帳上	有	有(第三者による)	無
Simple payment channel	台帳外	有	無	有
Conditional payment channel	台帳外	有	有（台帳による）	有

安全性について、ステラ･フェーズ 3 では、on-ledger escrow、third-party escrow、conditional payment channel は、取引プロセスにおいて自己の責任を完全に充足する取引当事者は、送金される額の元本を棄損するリスクに晒されないということが確認できた。

資金効率性については、これら 5 つの支払方法の中では、効率性の高い順に、①trustline、②on-ledger escrow および third party escrow、③simple payment channel および conditional payment channels とグループ化できる。Trustline は、支払がつけ払いのため、他の支払方法と比べて資金効率が高い。On-ledger escrow と third party escrow（１回の支払分のみの資金を固定）の資金効率性は総じて simple payment channel、conditional payment channel（payment channel で処理される全ての支払の所要資金を固定）よりも高い、との結論が得られた。

結論として、一連の支払を同期化し、資金を固定化する支払方法により、技術的な側面

からは、今日のクロスボーダー送金の安全性は改善することが可能であることを示唆している。もっとも、こうした新たな支払方法の導入を検討する前に、法律、コンプライアンス面での課題や、技術の成熟度や費用便益面での分析が求められる。

３．　台帳間支払のプロトコル

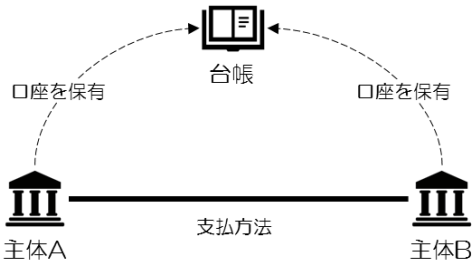
この章では、台帳間支払のためのプロトコルの考え方について述べる。台帳間支払のためのプロトコルとは、特定の台帳の形式に制約を受けず、これにより、送金者が異なる種類の台帳間で送金を行うことが可能となる。このプロトコルは、ホワイトペーパー「A Protocol for Interledger Payments」（Thomas and Schwartz、2015 年）で示された普遍的な[21]台帳間支払（universal interledger payments）についての提案と、その後のさらなる発展を下地にして組み立てられている。最近では、このプロトコル（Interledger Protocol、以下 ILP）に基づく要件は、W3C 内のコミュニティグループにより主に策定が進められている。最新版である ILP バージョン４（ILPv4）は、広く公開されている[22]。この章では、一般的な考え方と、それらがクロスボーダー支払のシナリオにどのように適用可能かについて述べることとする。

このプロトコルは、参加者、台帳、支払方法から構成されている（図表 4 参照）。

[21] ホワイトペーパーでは、Thomas and Schwartz（２０１５年）は台帳間支払にアトミックモードを提案していた。この点は、本報告書では、検証対象としていない。アトミックモードは廃止され、W3C 内のコミュニティグループは今では策定を行っていない。

[22] https://interledger.org/rfcs/0027-interledger-protocol-4/

【図表 4】 2 つの主体の間のプロトコルの構成



ここでは、「台帳」とは、口座間での価値の移転や、残高を記録することに使用されるいかなるシステムにも用いられる、一般的な表現である。本報告書では、送金は台帳上に記録される一方、支払はつけ払いを含む概念であるため、台帳に記録されるとは限らない。「参加者」とは、 1 つ以上の台帳に口座を有し、台帳間の支払に参加する主体である。「支払方法」とは、台帳上で資金を支払い、債務を履行する上での特定の方法に関する参加者間の 2 者間合意を指す。支払方法の選択は、参加者の選好と台帳の機能に依存する。

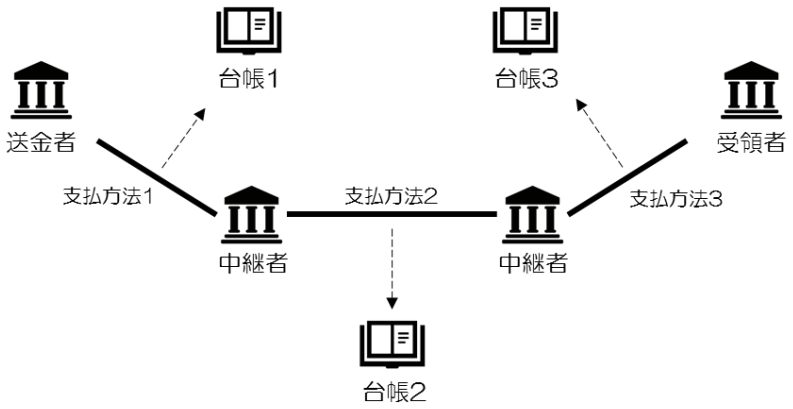
参加者は、ILP において、送金者、受領者、中継者という、3 つの役割を担いうる。「中継者」とは、2 つ以上の台帳に口座を有し、台帳間で支払を中継するための流動性を供給し、台帳間で支払を完了する上で重要な役割を果たす主体を指す。流動性供給者は、ある台帳における自己の口座への受入と他の台帳における自己の口座への支払を交換することにより、台帳間送金を実現する[23]。

単独の中継者が送金者と受領者の間で支払を連結させることができない場合、あるいは、同様のことが効率的な方法で行えない場合には、複数の中継者が 1 つの支払経路を構築することもありうる[24]。図表 5 は、 3 つの台帳と、流動性供給者の役割を果たす 2 つの中継者が一連の支払を構成している状況を例示したものである。

[23] 中継者が異なる通貨建ての台帳間で支払を行う場合、中継者は通貨の交換を行う。中継者はしばしば他の資料では流動性供給者と呼称される。

[24] 理論的には、台帳間支払における中継者の数は限定されない。

【図表 5】台帳間支払の経路の例



支払経路を構成するあらゆる個別の支払の成否は、受取人（受領者あるいは中継者）が、予め決められたタイムアウト前に暗号学的ハッシュ値の原像[25]を提示することに依存する。ハッシュ値は、支払の条件を定義することに使われ、これに対応するハッシュ原像は当該条件の充足の証跡となる[26]。単一のクロスボーダー支払の経路の中では、同一の暗号学的ハッシュ関数[27]、ハッシュ値、ハッシュ原像が使用されなければならない。

台帳間支払が開始される前には、原像とその暗号学的ハッシュ値は、受領者によって、任意の原像からハッシュ関数を用いてハッシュ値を導出することにより、生成される。ハッシュ値は、その上で、何らかの通信手段（Ｅメールなど）を利用して、送金者に対して、他の支払条件（金額、通貨、タイムアウト、受領者に関する情報）とともに共有されなければならない[28]。

---

[25] ハッシュ値はハッシュ関数を用いた計算値であり、原像はハッシュ関数の投入値である。

[26] 支払とタイムアウト到来前の暗号学的ハッシュ値にかかる原像の提示を結節させる考え方の基礎は、ステラ・フェーズ 2 で検証した、スマートコントラクトの特殊な形態である HTLC の概念から生まれたものである。

[27] ILP を策定したコミュニティグループは、SHA256 の利用を推奨。

[28] この点は、ILPv4 では、Simple Payment Setup Protocol と呼称される機能により達成しうる。

送金者、受領者間の初期段階での意思疎通ののち、台帳間支払は、主に２つの段階を経る。

- まず、支払人（送金人か中継者）は、利用される特定の支払方法に従い、受取人（受領者か中継者）への支払を準備する[29]。

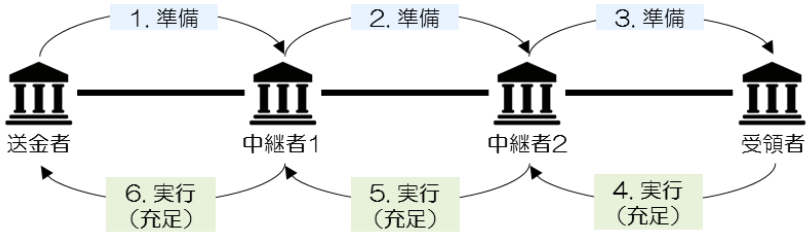
- これに続く段階では、３つのシナリオがあり、いずれも、準備された支払が実行されるか、中断されるかの結果となる。もし、ハッシュ原像がタイムアウトの前に受取人（受領者か中継者）から提示され、真正性が証明されれば、支払の条件は充足され、受取人への支払は実行される（充足シナリオ）。一方、真正な原像が提示されることなくタイムアウトが到来すると、支払は中断する（タイムアウトシナリオ）。また、受取人が支払を受付けないと、支払はタイムアウト到来前でも、中断されうる（拒否シナリオ）[30]。

図表 6 は、2 つの中継者が関与する台帳間支払が成功裡に実行されたケースを示している。送金者と中継者１、中継者２は、それぞれ、中継者１、中継者２、受領者への支払の準備を、この順番で行う。続いて、受領者と両中継者は、タイムアウト前にハッシュ原像を提示することにより支払条件を充足する。送金者と受領者間での取決め次第ではあるが、送金者による原像の保有は、受領者による資金の受領の証跡とみなされうる。

[29] 詳細は、第４章および原文の別添１を参照。

[30] 拒否シナリオは、初期のホワイトペーパーには含まれていなかったが、それは一連の支払が実行されるか、中断されるかしか想定されていなかったからである。受取人において、タイムアウトの到来を待つのではなく、送金を拒否することが可能であったとしても、受取人にとってそのようにふるまう経済的インセンティブはない。とはいえ、拒否シナリオは、参加者に対しては、オペレーション上の便益をもたらしうる。

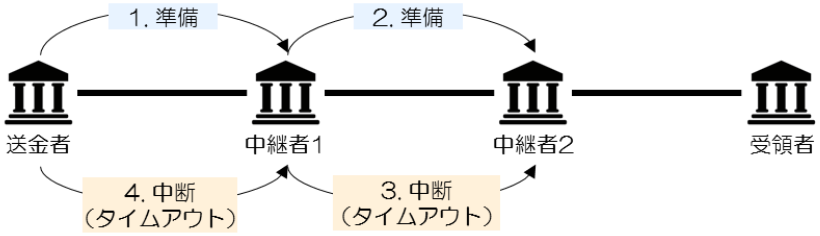
【図表 6】一連の支払の実行



矢印はある動作を起動した主体を起点としている。また、台帳の記載は省略している。同様の注記は図表 7 および 8 にも該当する。

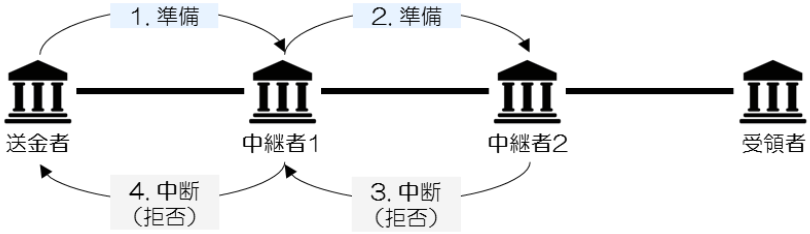
図表 7 に示すシナリオでは、支払は、一旦は準備されるが、タイムアウトの到来により中断される。送金者と中継者 1 は、それぞれ、中継者 1 と中継者 2 に対して、この順番で支払を準備する。その後、中継者 2 が動作を起こさず、ハッシュ原像をタイムアウト前に中継者 1 に提示しない場合には、中継者 2 および中継者 1 への支払は、この順番で中断される。

【図表 7】一連の支払がタイムアウトにより中断



図表 8 は、支払は一旦準備されるが、その後、中継者 2 による支払受領拒否に伴い、タイムアウト到来前に支払が中断されることを示している。送金者と中継者 1 は、それぞれ、中継者 1 および中継者 2 への支払を、この順番で準備する。その後、中継者 2 が支払受取を拒否することから、当該主体への支払は中断される。これにより、中継者 1 への支払も共に拒否されることとなる。

【図表 8】一連の支払が拒否により中断



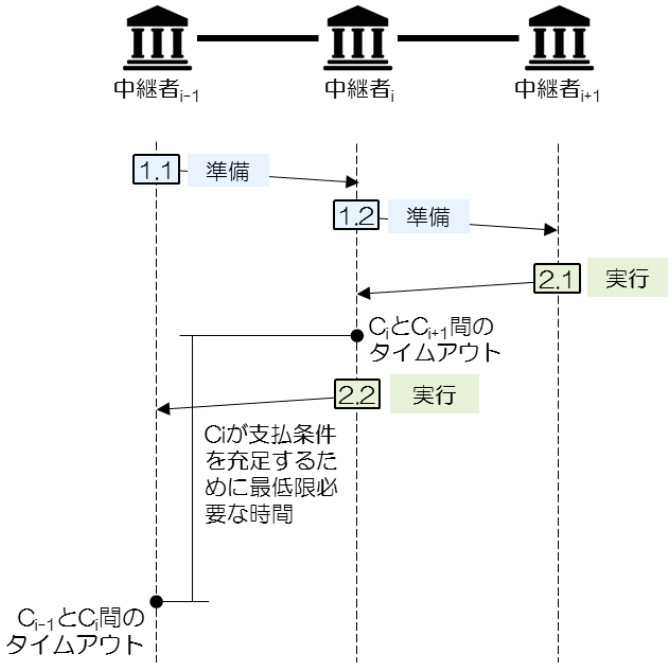
プロトコルに基づく支払プロセスでは、参加者間のほか、参加者と他の関連する主体との間の意思疎通が求められる[31]。これらの意思疎通には、支払経路如何で異なるものではなく、かつ、用いられた台帳や支払手段に依存しない、送金者と受領者間の初期段階での意思疎通のほか、支払経路中の各支払毎に異なる情報（例えば、手数料や個別の支払条件のタイムアウトなど）も含まれる。後者の情報については、以下の点に留意することが重要である。

- 中継者 C_{i+1}（あるいは受領者）と中継者 C_i との間の条件充足のためのタイムアウトは、C_i と C_{i-1}（あるいは送金者）との間の条件充足のためのタイムアウトより前であって、合理的な間をおいて設定されるべきである。これにより、C_{i+1} の条件充足後、十分な時間をもって、C_i は C_{i+1} から受領したハッシュ原像を提示することにより、要件を充足することが可能となる（図表 9 参照）。なお、受領者への支払のタイムアウトは、最長で、送金者と受領者との間で合意され、支払条件で特定されたタイムアウトと同時であることもありうる。

- C_{i-1}（あるいは送金者）と C_i 間の支払金額は、何らかの手数料や異なる通貨間取引であることを踏まえ、C_i と C_{i+1}（あるいは受領者）間の支払金額とは異なりうる。なお、受領者への支払額は、送金者と受領者との間で合意され、支払条件で定められた金額と同額以上であるべきである。

[31] 第 4 章でも述べる通り、これらは参加者が口座を有する台帳と、third party escrow の提供者を含む。

【図表 9】支払経路におけるタイムアウトの考え方



４．　支払方法

本章では、本報告書で扱う ILP の概念に準拠した、５つの支払方法を紹介する。これらの支払方法には、支払人と受取人の合意に基づき、受取人がタイムアウト前に原像を提示することで支払が実行される、という共通点がある。この特徴を持つ支払方法は、比較的広汎に存在し得る。本報告書で扱う支払方法の実現可能性は、台帳に関する特定の機能要件の有無および／または支払人・受取人間の信頼関係に依存する[32]。

本報告書で扱う支払方法は以下のとおり。

- trustlines
- on-ledger escrow using HTLC

[32] 支払方法の名称および説明は、ILP の Hashed-Timelock Agreements (HTLA) に基づく。
https://interledger.org/rfcs/0022-hashed-timelock-agreements/

- third party escrow[33]
- simple payment channel
- conditional payment channel with HTLC

支払方法についての以下の説明は、一連のクロスボーダー支払における参加者のうち、支払人と受取人を１組として捉えた場合のシナリオに基づく。また、支払人と受取人は、少なくとも１つの共通台帳に口座を保有し、それをある支払方法において使用することとする。

４．１　Trustline

Trustline は、支払人と受取人の信頼のみに基づいて実行される支払方法である。台帳上での決済は支払毎ではなく、つけ払い可能な金額の上限（仕向限度額）の抵触前に実行される。Trustline を用いた送金手順は、事前連絡段階、準備段階、決済段階の３段階に分けられる。

事前連絡段階：送金参加者（例：主体Ｂ）は、共通台帳に口座を保有する他の送金参加者（例:主体Ａ）との間で、主体Ａから主体Ｂへの仕向限度額を設定することで、trustline を開設できる[34]。

準備段階：支払人は、支払の準備としてハッシュ値やタイムアウトなどのメッセージを受取人に送る。Trustline の取引状況を示す未決済金額の合計は、各送金参加者のデータベースに記録される。十分な与信枠があるか、仕向限度額に抵触しない限り、技術的

[33] 現行の仕様である ILPv4 は、HTLA の主要な支払方法と追加的な支払方法（third party escrow、notarised payment channel、third party payment channel）を区別している。追加的な支払方法は支払人と受取人が信頼する第三者に頼る。これらの追加的な支払方法では、台帳に関して追加の機能要件が不要と推測されるため、ここではその典型的な例として third party escrow を取り上げている。

[34] あらかじめ主体Ａが主体Ｂに、台帳上で仕向限度額相当を支払うことで trustline を設定することも可能。一方のみが相手を信頼する場合には、trustline の設定方法が重要になることもある（trustline の設定方法が当事者間の信頼関係に影響を及ぼすことはない）。

には、trustline は双方向の支払に利用できる。主体Aがハッシュ値を用意のうえ準備を行い、主体Bが原像をタイムアウト前に主体Aに提示すると、trustline 上での主体 B の残高はつけ払い金額分増加（主体Aの残高は減少）する。一方、主体 B がハッシュ値を用意のうえ準備を行い、主体Aが原像をタイムアウト前に主体 B に提示すると、trustline 上での主体 A の残高はつけ払い金額分増加（主体 B の残高は減少）する。ただし、この段階では支払は決済されない。

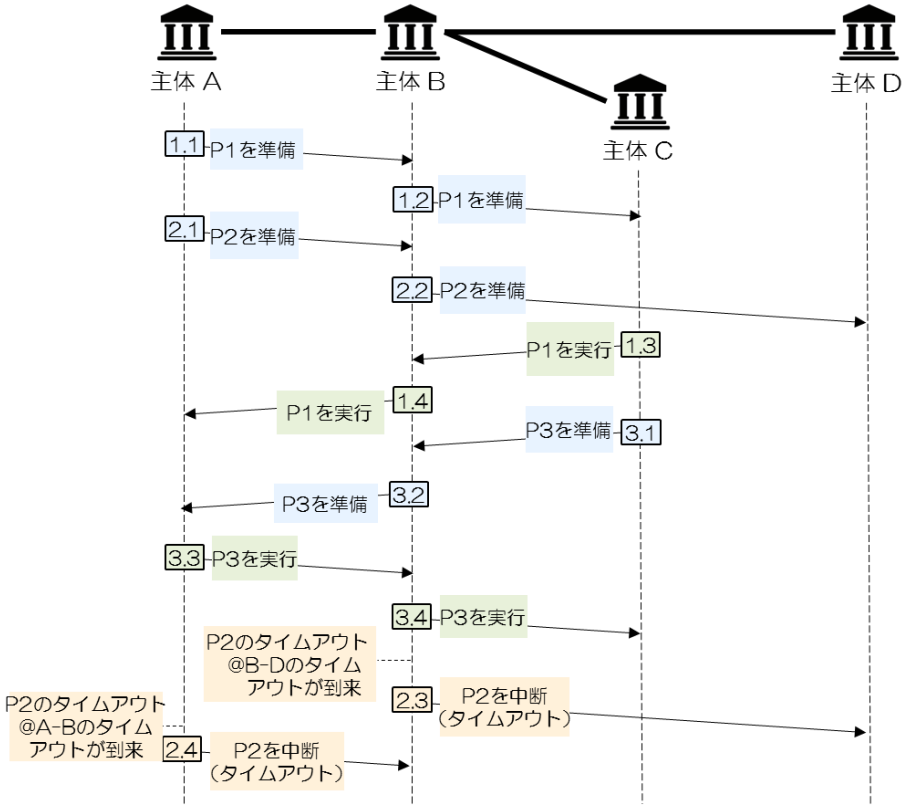
決済段階：未決済金額の合計は、台帳上での資金移動により決済される。

Trustline における台帳の機能要件は、資金移動の機能のみである。よって、送金参加者はいかなる種類の台帳でも trustline を利用できる。

Trustline は台帳外での支払方法であり、支払の度に台帳上で決済する必要がない。そのため、十分な与信枠があるか、仕向限度額に抵触しない限りつけ払いができる。また、残存債務の決済後はつけ払いを再開できる。Trustline では、台帳の有無、処理能力や処理時間に関わらずつけ払いを指図できる。

Trustline などの台帳外での支払方法を示す例として、図表 10 では 4 人の送金参加者間（主体 A～D）で複数支払が同時に行われる（一部は実行、残りは中断）場合を紹介する。支払経路が複数あるが、 A B間の支払には常に trustline が使われることとする。支払の詳細は図表 10 のとおり。

【図表 10】同時支払の例



支払経路	送金者	受領者	金額	原像/ハッシュ値
P1	A	C	50	S1 / H1
P2	A	D	10	S2 / H2
P3	C	A	12	S3 / H3

主体Aの主体 B に対する仕向限度額は€100.00 とする。A B間のネッティング契約により、trustline の取引状況は表２のとおり更新される。

【表 2】同時支払における trustline の取引状況

項番	事象の説明	A - B 間の trustline の取引状況			
		A が支払可能な金額	B が支払可能な金額	A → B への準備	B → A への準備
	当初の状況	€100.00	€0.00	€0.00	€0.00
1.1	P1 を準備	€50.00	€0.00	€50.00	€0.00
2.1	P2 を準備	€40.00	€0.00	€60.00	€0.00
1.4	P1 を実行	€40.00	€50.00	€10.00	€0.00
3.2	P3 を準備	€40.00	€38.00	€10.00	€12.00
3.3	P3 を実行	€52.00	€38.00	€10.00	€0.00
2.4	P2 を中断	€62.00	€38.00	€0.00	€0.00

４．２　On-ledger hold/escrow using HTLC

On-ledger escrow は、台帳により強制力を持つ条件付支払を可能にする支払方法である。支払人の資金は、事前に決定された条件が充足されるまで台帳に固定される。HTLC は、受取人がタイムアウト前に原像を提示することにより、資金が確実に受取人の口座に移されると規定している。原像がタイムアウト前に提示されなかった場合、資金は支払人に戻される[35]。

HTLC を採用した条件付支払では、初めに暗号学的ハッシュ関数を用いて資金を一定期間固定する。タイムアウトやハッシュ値は各支払の支払人によって設定される。タイムアウトまでは、受取人により事前に決定された条件（資金の固定に使われたハッシュ値と整合的な原像の提示）が充足された場合にのみ、資金が受取人の口座に移される。一方、タイムアウト前に条件が満たされなかった場合、資金は支払人に戻される[36]。

[35] 実装に依っては、支払人がタイムアウト後に台帳に指示を送り、資金の払い戻しを請求する場合もある。

[36] On-ledger escrow を用いた支払が受取人に拒否される場合（拒否シナリオ）において、台帳での資金固定期間を短くするため、資金は受取人の要請に応じて支払人に戻される、という追加の契約を結ぶこともできる。

On-ledger escrow を利用するには、HTLC 機能をサポートし、処理可能な台帳が必要である。台帳の機能要件の詳細は原文の別添 1 を参照。また、各支払は台帳上で決済されるため、台帳が利用可能である必要があるほか、資金移動の処理時間や処理量は台帳の処理能力や処理時間に大きく左右される。

４．３　Third party escrow

Third party escrow は、支払人と受取人から信頼されている第三者を活用することで、on-ledger escrow と概念的に類似した資金移動を行う支払方法である。

初めに、支払人は支払に関する情報を、台帳のオペレーターとは別の、支払人と受取人から信頼されている第三者に送り、資金をその第三者が保有する口座に送る。受取人がタイムアウト前に原像を提示すると、第三者は特別口座に移していた資金を受取人に送る。タイムアウト前に原像が提示されなかった場合、資金は支払人に戻される[37]。

Third party escrow における台帳の機能要件は、資金移動の機能のみである。よって、送金参加者はいかなる種類の台帳でも third party escrow を利用できる。もっとも、third party escrow は支払を台帳上で決済するため、台帳と第三者が利用可能である必要があり、資金移動の処理時間や処理量は、台帳と第三者の処理能力や処理時間に左右される。

４．４　Payment channels

Payment channel は、２者間での複数支払を合算でき、最終的なネットポジションのみを決済する支払方法である。この支払方法は、共通台帳に口座を保有する２者間で利用されるが、支払は台帳外で実行される。Payment channel を用いた支払手順は、事前連絡段階、準備段階、決済段階の３段階に分けられる。

---

[37] Third party escrow を用いた支払が受取人に拒否される場合において、第三者による資金固定期間を短くするため、資金は受取人の要請に応じて支払人に戻される、という追加の契約を結ぶこともできる。

事前連絡段階：支払人と受取人の一方または両方が、一時的な特別口座に特定の額を預け入れることで、payment channel が開設される。

準備段階：支払は、特別口座の資金の持ち分についての署名付き指図を送ることで実行される。資金の持ち分は payment channel の取引状況として表される。署名付き指図は送金参加者と台帳により照合でき、台帳により確実に実行される。新しく署名付き指図が送られると持ち分が更新され、過去の署名付き指図は効力を失う。支払の際は特別口座からの資金移動はせず、直接双方で署名付き指図を送る。なお、payment channel は、特別口座での持ち分がマイナスでない限り、双方向の支払に利用できる[38]。

決済段階：最終的なネットポジションを示す最新の署名付き指図に基づいて、持ち分見合いの資金が配分される。その後、両者間の特別口座と payment channel は閉鎖され、payment channel の決済は完了し、取引関係は終了する。Payment channel の閉鎖は、送金参加者間の争いの際など、協力関係なく一方的に行われる場合と双方の合意をもとに協力して行われる場合がある。

台帳には、payment channel 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、署名付き指図は台帳外で直接双方に送られる。これにより、支払は台帳の有無、処理能力や処理時間に関係なく実行できる。なお、争いの際は台帳が必要となる場合も考えられる。

Payment channel における台帳の機能要件は、payment channel の機能をサポートし、送金参加者が合意した最終的なネットポジション（最新の取引状況）の決済を強制する機能である。Payment channel はこうした台帳を用いたときに限り実装できる。

[38] 本報告書では、双方向かつ対称的な payment channel を扱う。この場合、資金は双方向に移動可能で、両参加者が取引状況について同じ情報を記録することにより、署名付き指図は両者に有効である。一方向の非対称的な payment channel も存在し、それらは本報告者が示す要件や処理フローとは異なる。

Payment channel では、受取人が支払人に対して原像を提示すると、支払人が特別口座の持ち分を変更する署名付き指図を出すこととなる。以下の節では、simple payment channel と conditional payment channel の２種類の payment channel を紹介する。

４．４．１　Simple payment channel

Simple payment channel の場合、受取人がタイムアウト前に原像を提示すれば、支払人は、特別口座の持ち分を変更する署名付き指図を送ることを約束する。署名付き指図を受け取ると、特別口座における受取人の持ち分が増加する。支払人による原像とハッシュ値の速やかな照合や、原像の提示見合いに約束した署名付き指図を送付することについて、台帳には強制力がなく、支払人の裁量で行われる。したがって、この支払方法では、支払人が約束を守るという信頼に基づいて支払が実行される。

Simple payment channel は trustline と違い、最新の payment channel の取引状況に基づく決済を強制する台帳に対して、送金参加者はいつでも署名付き指図を送ることができる。

技術的には、simple payment channel で使用する台帳は、payment channel の機能があれば追加の要件はない。

表３は simple payment channel を使った際の支払を示す。4.1 節のとおり、ＡＢ間の支払には simple payment channel が使われ、初めに主体 A が特別口座に€100.00 預け入れるとする。取引状況は表３のとおり更新される。

【表 3】同時支払における simple payment channel の取引状況

項番	事象の説明	A – B 間の simple payment channel の取引状況[39]		Simple payment channel の支払指図で扱われていない分	
		A の持ち分	B の持ち分	A → B への支払の準備	B → A への支払の準備
	当初の状況	€100.00	€0.00	€0.00	€0.00
1.1	P1 を準備	€100.00	€0.00	€50.00	€0.00
2.1	P2 を準備	€100.00	€0.00	€60.00	€0.00
1.4	P1 を実行	€50.00	€50.00	€10.00	€0.00
3.2	P3 を準備	€50.00	€50.00	€10.00	€12.00
3.3	P3 を実行	€62.00	€38.00	€10.00	€0.00
2.4	P2 を中断	€62.00	€38.00	€0.00	€0.00

４．４．２　Conditional payment channel with HTLC

Conditional payment channel は、支払人と受取人が台帳外で署名付き指図を送るという点で simple payment channel と類似しているが、この署名付き指図は台帳によって確実に実行される HTLC を用いている。また、conditional payment channel では、支払条件の充足が一参加者に依存しないため、両者間に信頼関係がある必要がない。

Conditional payment channel は simple payment channel と違い、HTLC を用いた署名付き指図により、payment channel の取引状況が更新される。よって、台帳が利用可能であれば、送金参加者はいつでも最新の署名付き指図を台帳に送り、台帳外の HTLC（署名付き指図）を、概念上は 4.2 節と同一の、台帳上の HTLC に変えることができる。

[39] 事前連絡段階で準備された資金は、取引参加者の誰か（支払人、受取人、支払人に関わらず主体Ａ、支払人に関わらず主体Ｂ）または第三者に割り当てられるが、これは主体Ａと主体Ｂの信頼関係に依る。本報告書では、特定の simple payment channel の設計を扱う。この設計では、受取人が支払人を信用し、準備資金は署名付き指図によって常に支払人の残高に割り当てられるため、事前連絡段階での残高は変わらない。

技術的には、conditional payment channel で使用する台帳は、payment channel の機能に加えて、HTLC を処理する機能が必要だと考えられる。

Conditional payment channel の機能を明らかにするため、4.1 節のとおり、A B 間の支払には conditional payment channel が使われ、初めに主体 A が特別口座に €100.00 預け入れるとする。取引状況は表４のとおり更新される。

【表 4】同時支払における conditional payment channel の取引状況

項番	事象の説明	A - B 間の conditional payment channel の取引状況			
		A の持ち分	B の持ち分	HTLC を用いた A → B への指図	HTLC を用いた B → A への指図
	当初の状況	€100.00	€0.00	€0.00	€0.00
1.1	P1 を準備	€50.00	€0.00	€50.00	€0.00
2.1	P2 を準備	€40.00	€0.00	€60.00	€0.00
1.4	P1 を実行	€40.00	€50.00	€10.00	€0.00
3.2	P3 を準備	€40.00	€38.00	€10.00	€12.00
3.3	P3 を実行	€52.00	€38.00	€10.00	€0.00
2.4	P2 を中断	€62.00	€38.00	€0.00	€0.00

４．５　５つの支払方法における台帳の機能要件

支払方法に利用する全台帳は、支払処理のためのユーザー認証や口座間での資金の授受といった、基本的な機能を備えている必要がある。加えて、前節までで紹介したとおり、いくつかの支払方法には台帳に対して特定の機能要件がある。よって、そうした支払方法は、要件を満たす台帳に口座を保有する送金参加者にしか利用できない。特定の機能とは、HTLC や payment channel の処理に関するものである。

- HTLC の処理能力には、特定の期間資金を固定し、HTLC が規定する条件の充足により資金を移動する機能が含まれる。

- Payment channel の処理能力とは、台帳外で合意した最新の署名付き指図のとおりに持ち分を配分するよう、一方の者（または両者）が決めた時点まで資金を固定する機能。

これら 2 機能の詳細は原文の別添 1 を参照。

４．６　まとめ

本章では、本調査で検討した 5 つの支払方法の特徴を紹介した。これらの支払方法の特徴は、①個別の支払が台帳上で決済されるか、あるいは台帳外で記録されるか、②資金が固定されるか特別口座に移されるか、③予め定められた条件が充足されたときに、支払が確実に行われるか、④台帳に対して条件付支払の強制機能や署名付き指図の処理など、特定の機能要件はあるか、という点で表 5 のとおり纏められる。

【表 5】支払方法と台帳の特定の機能要件の概要

支払方法	台帳上／外	資金の隔離・固定	条件付支払の強制	台帳の特定の機能要件	
				HTLC の処理能力	Payment channels の処理能力
Trustline	台帳外	無	無	無	
On-ledger escrow	台帳上	有	有（台帳による）	有	無
Third party escrow	台帳上	有	有（第三者による）	無	
Simple payment channel	台帳外	有	無	無	有
Conditional payment channel	台帳外	有	有（台帳による）[40]	有	有

[40] 台帳による条件付支払の強制は、payment channel が閉鎖された場合にのみ起こる。

５．　実機検証[41]

５．１　検証概要

ステラ・フェーズ 3 では、Interledger ホワイトペーパーで普遍的な台帳間支払（universal interledger payments）として紹介された考えを用い、異なる台帳を跨いだ送金の同期の実現可能性を確かめる実験を行った。ILP はホワイトペーパーに最も関係が深い仕様の１つであるが、ILP を用いるものと、用いないものの両方が行われた。ILP を用いない送金の実験では DLT 台帳間の送金が行われた一方、ILP を用いた実験は DLT 台帳間、中央集権型台帳間、DLT 台帳と中央集権型台帳の間で行われた。実験で得られた知見は、本報告書で示された概念研究の主な結果を補っている。なお、性能に関する実験は本実験の対象外である。

利用可能な ILP のオープンソース実装は、Interledger.js[42]と Hyperledger Quilt[43]が認められる。Interledger.js は Interledger のプロトコルスタックの JavaScript 参照実装で、活発な開発者コミュニティが異なったブロックチェーンを用い、異なるソリューションについて取り組んでいる。Hyperledger Quilt は Interledger のプロトコルスタックの Java 実装で、現時点では Hyperledger プロジェクトの傘下で萌芽期にある。本実験では、文書の利用可能性を主な理由として、Interledger.js が採用された。

ILP の仕様はホワイトペーパー[44]の公表後、現在は W3C の Interledger Payments Community Group のもとで発展している。2019 年 5 月時点で最新のプロトコールは ILPv4 である。それにもかかわらず、我々の実験では、古く、廃止された ILP （ILPv3）が採用された。ILPv4 に対応したオープンソースの中央集権型台帳の実装が、実験時には利用できなかったことがこの選択の主な理由である。

---

41 実験の詳細は原文の別添 2 参照。

42 https://github.com/interledgerjs/

43 https://github.com/hyperledger/quilt/

44 https://interledger.org/

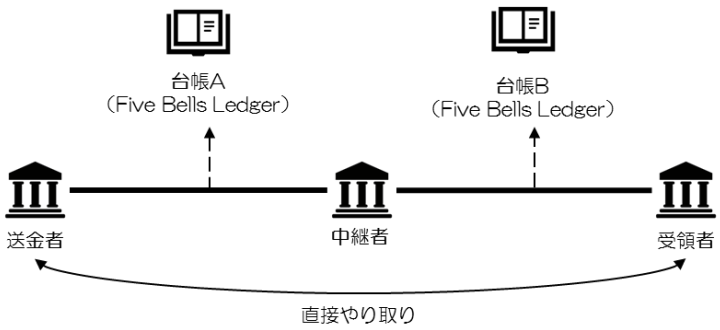
特に、中央集権型台帳の例として、ILPv3 の実装から Five Bells Ledger が選ばれた。そのソースコードは Interledger.js の一部として公開されており、その ILP プラグイン（台帳と通信するためにクライアントが利用する小規模なソフトウェア）ともども利用可能である。

DLT 台帳としては、Hyperledger Fabric がプロジェクト・ステラの前フェーズと同様に採用された。しかしながら、その ILP プラグインは今回の実験において新規に実装された。Five Bells Ledger が on-ledger escrow をサポートしていたため、Hyperledger Fabric の台帳でもこれを実装した。

５．２　中央集権型台帳での実験

中央集権型台帳間での決済の同期を確認するために、ILP を用いて実験を行った。中央集権型台帳として Five Bells Ledger[45]が、クライアントアプリケーションが Five Bells Ledger につなぐためのプラグインとして ilp-plugin-bells[46]が、採用された。この実験では、on-ledger escrow による決済の同期が中央集権型台帳間で ILP を用いて誤りなく行いうることが確認された。

【図表 11】　中央集権型台帳での実験時の構成



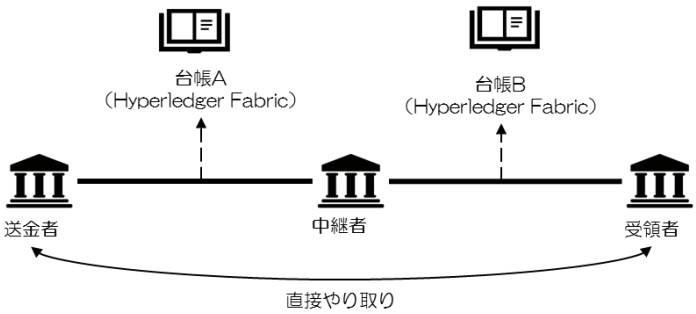
[45] https://github.com/interledger-deprecated/five-bells-ledger

[46] https://github.com/interledger-deprecated/ilp-plugin-bells

５．３　分散型台帳での実験

プロジェクト・ステラの前フェーズと同様に、DLT での実験では、Hyperledger Fabric が用いられた。ステラ・フェーズ 2 では Hyperledger Fabric のバージョン 1.1.0-alpha が用いられたが、今回はバージョン 1.2.1 が用いられた[47]。

【図表 12】 DLT 台帳での実験時の構成



５．３．１　ILP を用いない実験

この実験では、台帳 A にのみ口座を持つ送金者から、台帳 B にのみ口座を持つ受領者へ、両台帳に口座を持つ中継者を経由して送金された。異なる台帳間での決済の同期は、あらかじめ期待されていた通り、ILP を用いずとも誤りなく行われた。具体的には、送金者から中継者と、中継者から受領者への送金予定の資金を、同じハッシュ値を使用する on-ledger escrow を用いて固定し、同じ原像を用いて資金を払出した。

この実験において、中継者は外国為替に関するクライアントアプリケーション実装を全く行っていないが、中継者の送金額と受入額の比率を変更することでこれを実現出来るだろう。

[47] Hyperledger Fabric Client SDK for NodeJS が本実験では用いられた。

５．３．２　ILP を用いた実験

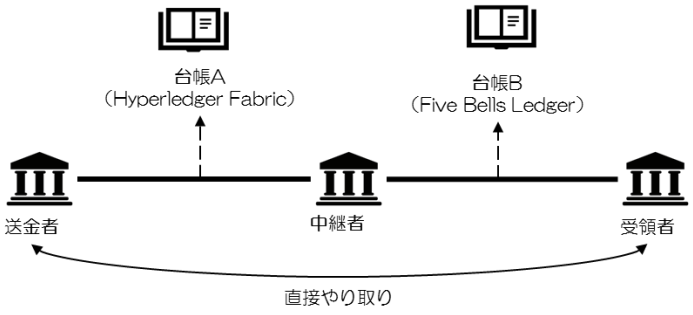
DLT 台帳での実験を行うために、いくつかの機能[48]を Hyperledger Fabric 台帳に実装するとともに、参加者が ILP に従って台帳に接続できるようにプラグインも実装した。実験では２つの異なる台帳で on-ledger escrow を用いた決済が同期されうることが確認された。

５．４　異なるプラットフォーム間での実験

ILP が台帳の技術に依存していないことを確認するために、Five Bells Ledger を用いた中央集権型台帳と、Hyperledger Fabric を用いた DLT 台帳を跨ぐ支払について実験を行った。具体的には、Hyperledger Fabric の台帳（台帳 A）にのみ口座を持つ送金者から、Hyperledger Fabric の台帳と Five Bells Ledger の台帳（台帳 B）の両方に口座を持つ中継者を経由し、Five Bells Ledger の台帳にのみ口座を持つ受領者に対し、資金が送られた。

下図で、台帳 A は 5.3.2 節の台帳 A と同一である。また、台帳 B は 5.2 節の台帳 B と同一である。我々は 5.3.2 節の中継者アプリケーションに対し、プラグインを追加した。ILP のインターフェースが標準化されていたため、台帳やプラグインへの修正を行う必要はなかった。

【図表 13】　異なるプラットフォームでの実験時の構成



[48] ハッシュ関数は ILP と互換性があるように作成された。本実験では、SHA256 が用いられた。

５．５　実験結果

複数パターンの決済の同期の実験が行われ、成功裡に終わった。この中には DLT 台帳間、中央集権型台帳間、DLT 台帳と中央集権型台帳の間で ILP を用いた場合の決済の同期が含まれている。ILP は Interledger のホワイトペーパーで紹介されている送金プロトコルの仕様である。ILP を用いない DLT 台帳間の決済の同期も実現可能なため、決済の同期に ILP の使用は必ずしも必要ではない。それにもかかわらず、ILP は異なる種類の台帳の抽象化を助け、それゆえ標準化の利点をもたらしうる。

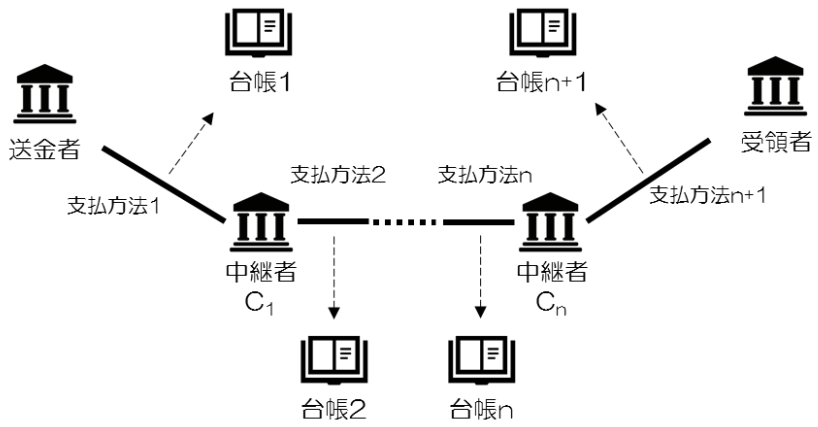
６．　支払方法の評価

本章では、それぞれの支払方法の安全性および効率性について評価する。第 4 章で紹介した支払方法を使うことで、支払を同期できるものの、支払の同期自体は、必ずしも支払が信用リスクのない、安全な形で行われることを保障するものではない――支払は、取引の手順における自身の責任を完全に果たした送金参加者（送金者・受領者・中継者）が当該送金にかかる信用リスク（送金額の一部または全額を失うリスク）に晒されないことを保障できる場合に、安全と見做せる。安全性は、異常シナリオを用いて評価する。その後、資金効率性についての簡単な分析も行う。

６．１　安全性

本節では、送金者が受領者に向けて中継者 C_1、C_2、…、C_n を経由した支払を行うケース（C_1 は送金者から資金を受け取り、C_n が受領者に資金を送る）について検討する。送金者・中継者・受領者ともに、第 3 章で説明されているプロトコルに従うものとする。

【図表 14】一連の支払のイメージ



台帳間支払のためのプロトコルでは、C_{i-1} から C_i への支払は C_i から C_{i+1} への支払の後に行われると想定されている。この場合、C_i から C_{i+1} への支払が行われた後に C_{i-1} が破綻すると、C_i は損失を被り得る[49]。従って、我々は「C_i が C_{i+1} に対して支払を行った後、C_{i-1} から資金を受け取る前に、C_{i-1} が支払不能に陥る[50]」という異常シナリオに基づき、それぞれの支払方法の安全性について評価する。

この評価に際して、我々は下記の前提条件が満たされているものと仮定する。これらの前提条件が満たされていない場合、どの支払方法を用いたとしても、安全に支払を行うことはできない。

I.　支払経路内の全ての送金参加者は経済的インセンティブに従って行動する。

[49] これは、当プロトコルとは違い、C_{i-1} から C_i への支払が C_i から C_{i+1} への支払の前に行われる、現在のクロスボーダー送金の多くとは、対照的である。C_{i-1} から C_i への支払が C_i から C_{i+1} への支払の前に行われる場合、C_{i-1} の破綻は C_i にとってはリスクをもたらさないが、法的取決め次第では、C_j（$j \leqq i-2$、C_j は送金者であり得る）にとってリスクをもたらし得る。

[50] C_{i-1} と C_{i+1} は、それぞれ送金者、受領者であり得る。

II. 送金参加者が台帳に開設した口座に預けた資金は安全でなければならない。これは、支払プロセスの最中に台帳が破綻する場合、支払方法に関係なく、資金が失われてしまう可能性があるからである[51]。

III. 送金参加者が口座を開設している台帳は、送金が問題なく行われるために必要な責任を全うする点について、信頼できる必要がある[52]。

IV. 資金を固定する台帳は、十分な処理速度および稼動時間を確保している。

V. 送金プロセスに関与する送金参加者および台帳は、第 4 章にて規定された能力[53]を具備し、送金における自身の責任を全うすることができる（4.1～4.4 節に記述された支払手順を厳しいストレス時にも履行可能である）[54]。

VI. 受取人（受領者および中継者）は、支払手順上、必要なときにのみ、必ず原像およびその他の重要情報を開示できるよう、十分なセキュリティおよびその他の能力を備えている必要がある。

---

[51] Third party escrow が用いられている場合、third party escrow の提供者の破綻時に安全に支払が行われるかは、特別口座への預入のプロセスにおいて、支払人・受取人に対して当該提供者が賠償責任を負うか否かで異なる。本報告書において取扱われている third party escrow の手法では、支払人が送金資金を提供者の口座に送金することで資金を固定しているため、提供者が破綻すると支払の安全性が損なわれる。一方、払出のためには支払人・受取人双方の署名が必要な台帳上の共同口座に支払人が送金資金を送ることで資金を固定し、提供者は支払人・受取人の代理人として、台帳に対して資金を固定・払出するための指図を発出するような third party escrow の手順も検討可能かもしれない。この方式の場合、提供者は支払人・受取人に対して賠償責任を負うことはない。

[52] もし仮に信用できない場合、送金参加者はそもそも当該台帳に口座を開設しないだろう。

[53] これは、送金参加者が信頼できるような同期された時間管理メカニズムを具備していることを含む。

[54] 従って、受取人が不可抗力によりタイムアウトまでに原像を提示することができないようなシナリオは、受取人が前提条件 V に規定されている自身の責任を全うできなかった場合と考えられ、今回の評価の対象外となっている。

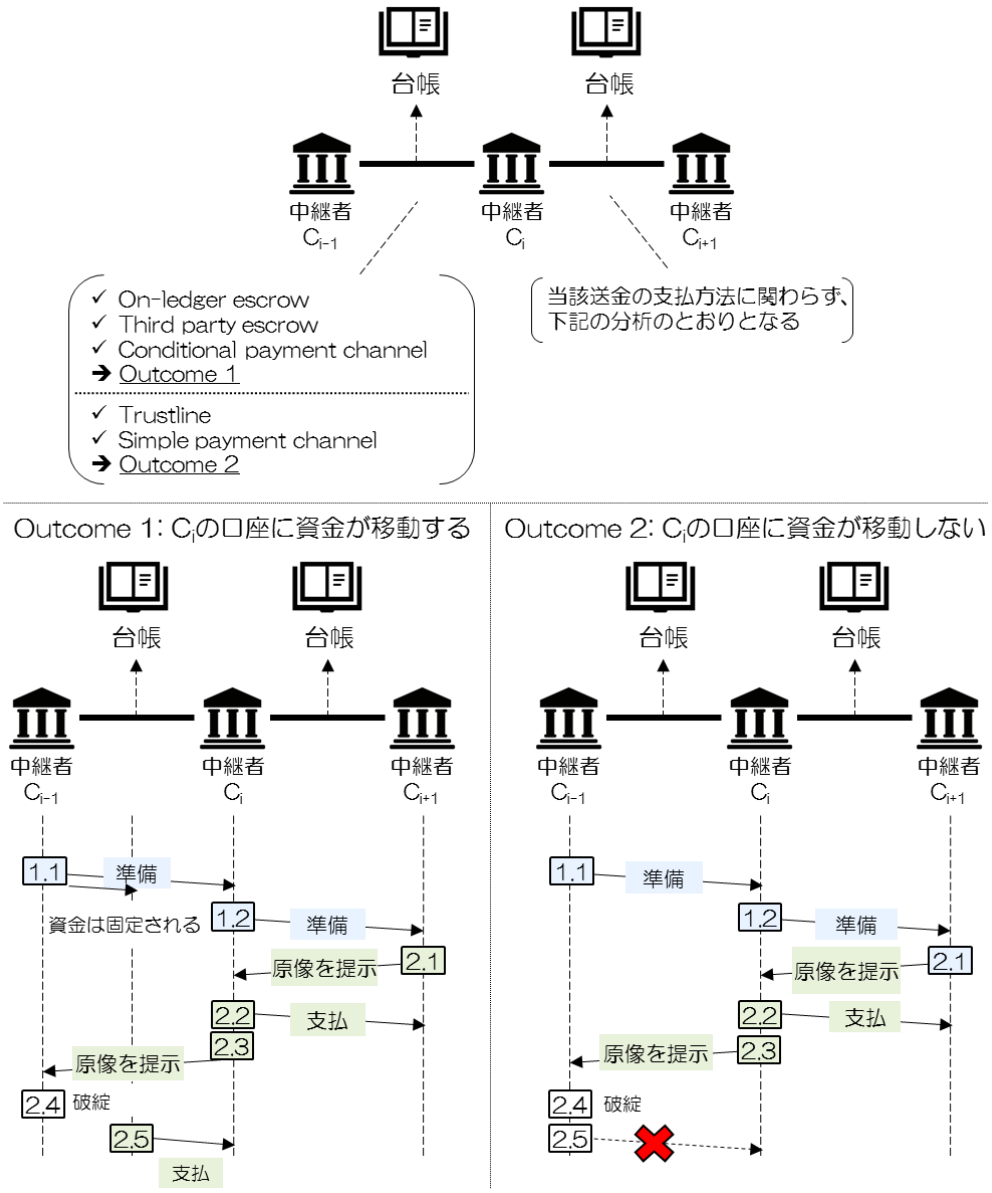
VII. 固定された資金は支払人の破綻からは隔離される。

VIII. Third party escrow の提供者は、上記の前提条件のうち、台帳に関係するものを満たしている。

上記のシナリオにおいては、用いられている支払方法によって、C_i が資金を C_{i-1} から受け取れるかは異なる。すなわち、C_i は on-ledger escrow、conditional payment channel、または third party escrow が用いられている場合には、資金を受け取ることができるが、trustline または simple payment channel が用いられている場合には、資金を受け取れない可能性がある。

これは、前者の支払方法では、C_{i-1} の破綻前に資金は信用リスクから隔離される形で固定され、かつ受取人が支払条件を満たしたか否かに従って、送金がなされるような強制の枠組みが存在する一方、後者の支払方法では、支払はあくまで C_{i-1} による約束に依存しているためである（図表１５参照）。

【図表 15】カウンターパーティーが破綻するシナリオ



Conditional payment channel（Outcome1）については、送金に用いられる資金は、payment channel が開設された段階で既に台帳により固定されている点に留意。

Trustline と simple payment channel は、上記の異常シナリオにおいて、どちらが用いられても送金の安全性は保障されないが、C_i が被る可能性がある損害額については差異がある。すなわち、simple payment channel が用いられている場合には、C_i は最新の取引状況に反映されていない受取額を失う可能性があるが、trustline が用いられて

いる場合には、C_{i-1} に対する全ての与信を失う可能性がある[55]。

６．２　資金効率性

次に、それぞれの支払方法を用いた場合の資金効率性について評価する[56]。本報告書で検討している 5 つの支払方法は、資金効率性の高い順に、①trustline、②on-ledger escrow および third party escrow、③simple payment channel および conditional payment channel に分けることができる。

Trustline は、5 つの支払方法のうち、唯一の事後確保型である。Trustline を用いる支払人は、資金を事前に用意する必要がなく、受取人と相互の支払をネッティングできるため、この支払方法は、最も資金効率性が高い。

残る 4 つの事前確保型支払方法のうち、on-ledger escrow と third party escrow は、simple payment channel と conditional payment channel 対比で基本的に資金効率性が高い。これは、前者の支払方法では、支払人が送金の都度、資金を固定する一方、後者の支払方法では、支払人は payment channel を開設している期間中、個別の送金よりも大きな額（もしくは同額）[57]の資金を固定する必要があるためである[58]。

---

[55] C_n（受領者に資金を送る中継者）が受領者から原像を受け取った後で、かつ、受領者が資金を受け取る前に破綻するケースについては、追加的な検討が必要である。

[56] 送金に用いる口座のファンディング方法や、複数の台帳に預けた資金の調整方法等、流動性管理にかかる考察は行っていない。こうした流動性管理策は、資金効率性に影響するものの、個別の支払方法の特性とは無関係であることから、支払方法の差別化には役立たないため、考慮外としている。

[57] もし 1 件の送金のみを対象として payment channel が開設され、送金が行われた場合、payment channel と on-ledger escrow または third party escrow との間の資金効率性の差は減る。

[58] この評価は、前提条件 IV（資金を固定する台帳は、十分な処理速度および稼動時間を確保している）が満たされていると仮定したうえで行われている点には留意。また、技術的には、送金参加者間で合意に基づき、payment channel にて固定されている金額を必要に応じて増やしていくことは可能であるが、これは台帳外で支払を行うという payment channel の利便性を損な

これを説明するために、支払人が午後 1 時に資金 1 単位、午後 2 時に資金 3 単位を支払うケースを考えてみよう。もし支払人が payment channel を用いるならば、午後 1 時より前に全 4 単位の資金を準備する必要がある。これに対し、支払人が on-ledger escrow または third party escrow を用いるならば、支払人は午後 1 時までに 1 単位、午後 2 時まで追加で 3 単位、用意できればよい。

６．３　まとめ

6.1 節の安全性についての分析により、我々は、取引の手順における自身の責任を完全に果たした送金参加者（送金者・受領者・中継者）が当該送金にかかる信用リスク（送金額の一部または全額を失うリスク）に晒されないことを保障できる、安全な支払方法を明らかにした[59]。これらの安全な台帳間送金を保障する支払方法は、on-ledger escrow、conditional payment channel、および third party escrow である（Default-resistant Conditional Transfers ＜DCT＞）。送金参加者は、自身の責任で trustline や simple payment channel を採用可能だが、支払人の破綻リスクに晒されている点について意識すべきである。

資金効率性については、6.2 節の分析を通じ、5 つの支払方法のうち、trustline の資金効率性が最も高く、また、on-ledger escrow と third party escrow の資金効率性は、simple payment channel と conditional payment channel よりも高いことを示した。

上記の分析結果は、表６のようにまとめられる。

うことから、本報告書では考慮の対象外とする。

[59] Interledger ホワイトペーパーで提唱されたプロトコルに基づいた台帳間送金において、全ての送金参加者が自身の責任を全うする場合、送金者は、用いられる支払方法に関係なく、信用リスクに晒されない点には留意。異常時シナリオで検討したとおり、用いられる支払方法次第で信用リスクに晒されるのは、受領者および中継者である。

【表 6】評価結果一覧

支払方法	安全性	資金効率性
On-ledger escrow using HTLC	高い	中程度
Third party escrow	高い	中程度
Conditional payment channel with HTLC	高い	低い
Simple payment channel	低い	低い
Trustline	極めて低い	高い

注： 安全性については、「高い」は DCT、「低い」は送金参加者が最新の取決めに反映されていない受取額を失う可能性がある支払方法、「極めて低い」はカウンターパーティーに対する全ての与信を失う可能性がある支払方法に付与されている。資金効率性については、「高い」は事後確保型の支払方法、「中程度」は事前確保型のうち、送金の都度、資金を固定する支払方法、「低い」は事前確保型のうち、個別の送金よりも大きな額（もしくは同額）が必要である支払方法を示している。

７． 追加の検討事項

本章では、台帳間支払のためのプロトコルに関連すると思われる３点を検討する。具体的には、①各支払の安全性と支払経路全体のアトミック性という、２つの関連するも異なる概念、②第６章における支払方法の評価では考慮していない台帳の処理速度や稼働時間による制限の影響、③第６章で挙げた前提条件が全て満たされ、かつ、支払の安全性が損なわれなくとも起こり得る、「フリー・オプション問題」について検討する。

７．１ 各支払の安全性と支払経路全体のアトミック性

第６章では、送金参加者が用いる各支払方法の安全性を分析した。各支払の安全性は、支払経路全体のアトミック性とは異なる。支払経路全体のアトミック性は、各支払について、他の支払が全て行われない限り実行されない場合に実現していると言える[60]。

[60] 支払経路全体のアトミック性が支払の安全性を確保する訳ではないため、本調査では支払経路全体のアトミック性の分析は行っていない。

支払経路全体のアトミック性は、各支払が安全に実行される場合にのみ実現する。これを説明するにあたり、6.1 節の異常シナリオを考える。第６章で挙げた前提条件を踏まえ、支払経路内の全支払に安全な支払方法が用いられる場合、債務不履行による異常シナリオにおいても全支払が実行される。これは、受領者により送金が開始されれば、送金参加者（債務不履行者やそれに対する債権者も含む）は支払を実行すると考えられるからである。受領者が送金を開始しない場合、支払経路内の全支払はタイムアウトにより中断される。

一方、同上の異常シナリオにおいて支払経路内で安全でない支払方法が用いられる場合には、アトミック性は実現しない可能性がある。もっとも、この場合にも安全な支払方法を用いた支払については実行され、資金は安全であると考えられる。

なお、第６章における支払方法の安全性評価は、いくつかの前提条件を踏まえている点に留意する必要がある。それらには、支払経路内の全ての送金参加者は、経済的インセンティブに従って行動すること（前提条件 I）や、資金を固定する台帳は、十分な処理速度および稼動時間を確保していること（前提条件 IV）が含まれる。これらの前提条件が満たされない場合、各支払は安全でなくなるため、支払経路のアトミック性は、その中で用いられた支払方法に関わらず保証されなくなる。

７．２　台帳の処理速度や稼働時間による影響

第６章では、台帳は十分な処理速度と稼働時間を確保していることを前提とした（前提条件 IV）。しかし、一般的には、送金参加者はタイムアウトを設定する際には、台帳の処理速度と稼働時間を考慮する必要がある。具体的には、利用する支払方法に台帳が関与する場合（on-ledger escrow、third party escrow や conditional payment channel）には、その処理速度や稼働時間を勘案して、タイムアウトを設定する必要がある。

支払経路内で、１つの支払に対し、処理速度が遅く稼働時間が短い台帳が関与する支払方法を用いた場合、他の支払のタイムアウトの設定に影響する可能性がある。例えば、C_i と C_{i+1}（C_{i+1} は受領者の場合もある）の支払に非常に遅い台帳が使われ、C_j（$j<i$、C_j は送金者の場合もある）は C_i、C_{i+1} 間を経由して自身の支払を行うことを予想する場

合を考える。C_j は C_{j+1} とのタイムアウトについて、C_i、C_{i+1} 間で遅い台帳を用いた支払が実行されるのに十分なタイムアウトを設定する（さもなければ、原像をタイムアウト前に C_{i-1} に提示するのは困難だと想定する C_i は、この送金に参加することを引き受けないだろう）。

タイムアウトを短くするためには、①台帳が関与しない支払方法（trustline または simple payment channel）を用いるか[61]、②台帳の処理速度および／または稼働時間を改善する必要がある。但し、trustline や simple payment channel を利用する場合には、送金資金の安全性が損なわれるため、信用リスクが高まることに留意すべきである。

７．３　フリー・オプション問題

「フリー・オプション問題」とは、異なる台帳間や通貨間での支払において、送金参加者が晒される為替リスクを指す。支払準備の際、送金参加者は、ある通貨建ての特定額を別の通貨建ての相当額と引き換えに支払う責務を負う。この責務は、悪意のある送金参加者に悪用される可能性がある。

図表 16 は送金開始後に送金者と受領者が共謀し、中継者の流動性を拘束する例を示す。この例では、受領者には、①支払を実行（充足）するか、もしくは、②タイムアウト前に拒否またはタイムアウトが到来して支払を中断するか、の選択肢がある。これにより、共謀者は為替レートに応じて、中継者の契約上の義務を悪用できる。すなわち、共謀者は、為替レートが自身に好都合な場合にのみ支払を実行し、さもなければ、支払を中断する。

現在のところ、このフリー・オプション問題は未解決のままであり、インターレジャーの策定を進めるコミュニティにおいて議論が活発に行われている。この問題は、プロトコルの設計により発生するため、第６章で挙げた前提条件が全て満たされている場合に

[61] この場合、台帳が関与しない支払方法を用いた送金手順は、十分な速度で行われなければならない。

も発生する。なお、この問題は、支払の安全性に直接的なリスクをもたらすものではない。また、送金参加者が、中継者の契約上の義務を悪用し、潜在的な利益を享受することよりも、風評リスクを重視する場合には、フリー・オプション問題は発生しないと考えられる。

【図表 16】「フリー・オプション」の悪用例