

ブロックチェーン技術を活用した 新たな銀行間決済の実現

Realization of New Interbank Settlement Platform Utilizing Blockchain Technology

谷内 圭 久保 竹清

あらまし

これまで、国内における商品などの決済は現金が主流であった。しかし近年、スマートフォンや電子マネーの普及に伴い、キャッシュレス化の機運が政府や産業界を中心に急激に高まっている。このような情勢の中、富士通は送金に着目し、2017年度にメガバンク3行と個人間送金の実証実験を行った結果、銀行間決済・資金清算を担う新たな仕組みが必要であるとの課題を認識した。今回、その解決に向けて、一般社団法人全国銀行資金決済ネットワークと共同でブロックチェーン技術を活用した仕組みを構築した。更に、銀行間決済専用のデジタル通貨を創出し、リアルタイムで銀行決済を行う仕掛けが有効ではないかと仮説を立て、各種検証に取り組んだ結果、一定の有効性を確認できた。

本稿では、ブロックチェーン技術を活用した新たな銀行間決済の実現に対して、前述した課題解決に向けた仮説検証の結果について述べる。

Abstract

Up until now, the mainstream method of settlement for merchandise in Japan has been cash. However, as smartphones and e-money have become increasingly widespread in recent years, movements toward going cashless led mainly by the government and industries have been growing. Given these circumstances, Fujitsu has placed focus on money transfers and conducted a field trial of person-to-person money transfers together with the three Japanese megabanks in FY2017. This resulted in the recognition of the need for a new system capable of interbank settlement and clearing funds. To provide a solution to the issue, we have cooperated with the Japanese Banks' Payment Clearing Network to work on the building of a system that makes use of blockchain technology. Moreover, we hypothesized the effectiveness of a system for creating a digital currency exclusively for interbank settlement for real-time bank settlement and, as a result, confirmed a certain level of effectiveness. This paper presents the results of the verification of the hypothesis for the resolution of the issue mentioned above in relation to realizing a new interbank settlement system making use of blockchain technology.

1. まえがき

近年、国を挙げてのキャッシュレス化の推進を背景に、様々な金融サービスが登場している。店舗やインターネットショッピングサイトなどで利用される決済と並んで注目されているのが、現金取り扱いに代わる送金であり、キャッシュレス化を推進していくに当たって、重要な領域であると考えられる。

富士通としてもこの領域に着目し、2017年度にメガバンク3行（株式会社みずほフィナンシャルグループ様、株式会社三井住友フィナンシャルグループ様、株式会社三菱UFJフィナンシャル・グループ様）とともに、個人間送金にフォーカスした実証実験を行った。その結果、銀行間決済・資金清算を担う仕組みが必要であるとの課題認識に至った。

本稿では、この課題の解決に向けて、一般社団法人全国銀行資金決済ネットワーク（以下、全銀ネット）と富士通が共同研究を進めている、ブロックチェーン技術を活用した新たな銀行間決済プラットフォームへの取り組み⁽¹⁾について述べる。

2. 実証実験の背景

送金とは、現金を手渡しするのではなく、銀行振込や現金書留、郵便為替などを用いて価値を送る方法である。近年では、2009年に成立した資金決済法によって、銀行以外の事業者が少額の送金サービスを行うことが解禁され、新たな送金手段の創出機会がもたらされている。

一般的に馴染みが深い送金手段としては、銀行振込と現金書留が挙げられる。しかし、前者は送金先の預貯金口座情報（金融機関名、支店名、預金種目、口座番号、口座名義人氏名）が必要となる。また、後者は取り扱いの性質上、郵便局窓口で受付が必要となる。このため、既存の送金手段では利用者にとって利便性が優れているとはいいがたく、利便性が高い新たなサービスが望まれている。

このような状況の中、富士通は2017年度にメガバンク3行とともに、ブロックチェーン技術を活用した個人間送金サービスの実証実験を行った。⁽²⁾ この実証実験では、送金対象である価値を預貯金と同

等のものと定義し、送金先指定に携帯電話番号を用いることとした。そして、従来の手段と比較して利用者の利便性が高められるかどうか、また個人間送金に伴い発生する一連の資金清算プロセスが問題なく成立するかどうか、といった観点で検証を行った。その結果として、個人間送金サービスとしての有用性・利便性が確認できた。

一方で、各利用者の預貯金口座間の送金において、以下のような課題が見つかった。

- ・銀行間をまたいだ送金発生に対して、決済尻^(注1)の算出（クリアリング）とそれに基づく清算依頼処理（セトルメント）が必要。
- ・清算を効率的に行うためには、各銀行が相対処理を行うのではなく、清算の起点となる銀行が必要。
- ・送金後の現金引出機能の提供を想定する場合、送金タイミングと清算処理タイミングのズレから生じる決済リスク（決済資金ショート）への対応が必要。

3. 新銀行間決済プラットフォームの可能性検証

今回の実証実験では、以下の仮説に基づいて、前述した課題解決の可能性を検証した。

(1) 決済を実施する手段として、銀行間決済専用デジタル通貨（以下、決済用デジタル通貨）を創出。

(2) 各銀行は決済尻の算出と清算を行わず、銀行間をまたいだ送金が発生するたびに決済を実行。

この仮説に基づいた銀行間決済を採用することで、各銀行はクリアリングとセトルメントを意識する必要がなくなる。また、決済用デジタル通貨の直接流通によって、決済リスクが軽減される。この仕組みを担うシステムが新銀行間決済プラットフォームであり、最終的なイメージは送金サービスにおけるRTGS^(注2)の実現である。

決済用デジタル通貨を実装する際には、その性質

(注1) 銀行間をまたいだ送金に対して、算出された銀行単位の受払差額。

(注2) Real-Time Gross Settlementの略。取引1件ごとに銀行間決済を行い、決済リスクを回避する仕組み。

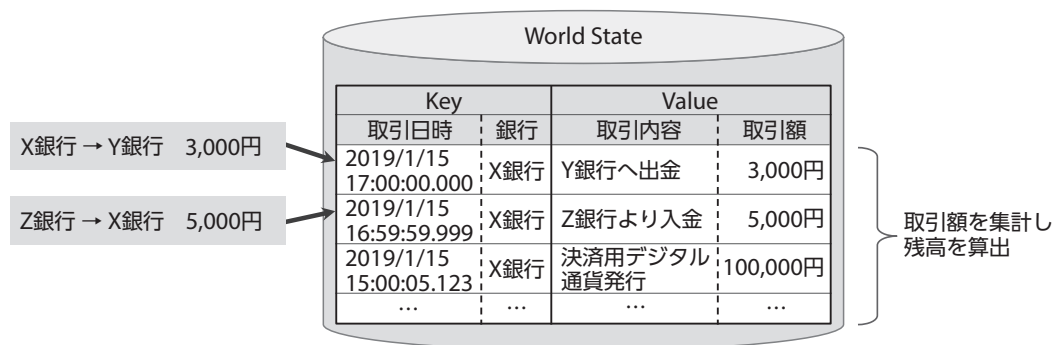


図-1 本検証のデータ構造

上、取引の完全性および価値そのものの厳密な管理が求められる。これらの要求事項を実現するに当たっては、ブロックチェーン技術の持つ特長に着目し、その採用を試みた。

この取り組みでは、新しい銀行間決済の実現をテーマに、ブロックチェーン技術を適用した場合の機能面の検証および可用性、性能、セキュリティといった非機能面の検証を行った。

4. 適用技術

2009年のビットコインの誕生以降、ブロックチェーンの領域では様々なフレームワークが登場している。今回の検証では、数あるブロックチェーンフレームワークの中でも、多数のOSS（Open Source Software）開発の実績を持つThe Linux Foundation⁽³⁾が主催するHyperledgerで、エンタープライズ用途に開発されているHyperledger Fabric⁽⁴⁾の適用を試みた。また、計画当時（2018年7月）に最新のバージョンであったV1.2を利用した。

Hyperledger Fabricは、台帳としてWorld Stateと呼ばれるKey-Valueストア^(注3)を持ち、取り扱いデータの格納先として機能する。今回の銀行間決済のユースケースにおいては、取り扱いデータとして決済用デジタル通貨の残高および取引履歴がある。一般的には、残高を「Key：銀行」「Value：決済用デジタル通貨残高」の形式で管理することが考えられる。

(注3) KeyとValueの組み合わせによって値を読み書きできるデータベース。

しかし、Hyperledger Fabricでは特定のKeyに対する更新処理が短時間に集中した場合には、データの整合性を確保するために受付単位の中で最初の更新処理のみを有効とする、排他制御の仕様を有している。今回検証する性能要件を鑑みると、排他制御の仕様に抵触しており、多数の処理が排他され無効化してしまう可能性が高いと推測した。そのため、本検証ではWorld Stateに残高を保持するのではなく、「Key：取引日時＋銀行」「Value：取引内容＋取引額」のように、一意のKeyを持つ取引履歴を記録するデータ構造とした（図-1）。残高は取引のたびに取引履歴から算出する方式とし、排他制御への抵触を回避することとした。

5. 実証実験の実施内容と確認観点

今回の検証では、検証用に開発した新銀行間決済プラットフォームと2017年度に開発した個人間送金システムを連動させることで、個人間送金から銀行間決済に至る一連の流れを検証可能とした。具体的には、利用者がスマートフォンを利用して個人間送金を行い、その送金が銀行をまたがる場合に、新銀行間決済プラットフォームによるRTGSが正しく機能するかどうかを確認するものである（図-2）。

検証において、機能面、非機能面のそれぞれで確認の観点を設定した。機能面においては、前述したRTGSが正しく機能するかどうかを、(1) 新銀行間決済プラットフォーム上での残高不整合の発生有無、(2) 実証実験参加者における取引履歴の欠損有無の二つの観点について、日次で検証した。また、

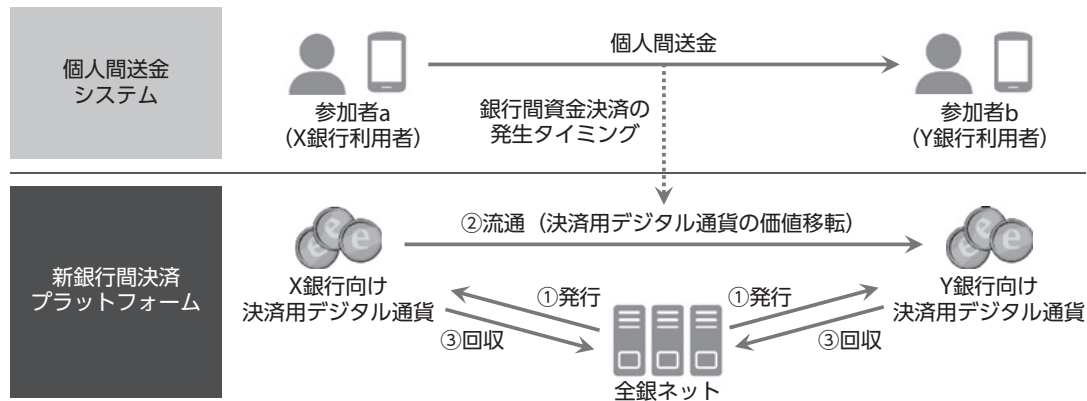


図-2 実証実験の概要

非機能面においては、可用性評価として「単一障害点^(注4)の排除可否」、性能評価として「1,000 tps^(注5)の実現可否」、セキュリティ評価として「Hyperledger Fabric上のデータ改ざん検知・復旧可否」を観点として設定し、実機検証を行った。なお、性能評価の目標値である1,000 tpsは、当該ユースケースの実現に当たって必ずしも十分な値とは言えないが、まずは当面クリアすべき目標値として関係者の認識の下で定めた。

6. 検証の結果と評価

本章では、前章で述べた検証の結果とその評価について述べる。

まず、機能面の結果評価を述べる。日次の残高不整合確認および取引履歴の欠損確認においては問題が発生することなく、RTGSによる新しい銀行間決済プラットフォームとして機能したと言える。また、付随的な評価ではあるが、本検証で開発したシステムによって、2017年度の実証実験で見つかった各利用者の預貯金口座間の送金に関する課題を解消し、個人間送金を含めた銀行間決済の一連のフローが成立することを確認できた。

次に、非機能面の検証においては、ブロックチェーンが持つ高可用性、高耐改ざん性が有効であることを確認できた。一方で、性能に関してはいく

つか課題が明らかになった。非機能面の評価結果の課題について、以下に述べる。

6.1 可用性評価

Hyperledger Fabricを用いたシステムにおいて、単一障害点を排除可能であることを確認した。本検証システムでは、EP/CP（Endorsing Peer/Committing Peer）、CA（Certificate Authority）、OS（Ordering Service）、Kafka、ZookeeperなどのHyperledger Fabricの各機能サーバ、およびHyperledger Fabric外に配置した業務サーバ、DBサーバにおいて、冗長化構成を採用した。その中で、それぞれ単一障害が発生した場合、あるいは全サーバで同時に単一障害が発生した場合において、業務継続が可能であることが確認された。

一方で、Hyperledger Fabricの機能サーバにおいては、縮退運転^(注6)時に縮退割合以上にスループット性能が劣化する事象が確認された。調査の結果、Hyperledger Fabricの仕様として、停止サーバの検知・切り離し機能が具備されていないことが判明した。このため、障害が発生してサーバが停止している状態においても通信が行われ、その結果としてタイムアウトが発生するまで待ち合わせする挙動になる。これが原因で、スループット性能が劣化していた。この事象は望ましい状態ではないが、サーバ復旧時に自律的な業務復帰が期待でき、異常時の運用オペレーションを不要とする効果も考えられる。

(注4) 停止した場合に、システム全体の停止をもたらす箇所。

(注5) Transaction per secondの略。ピーク時における1秒あたりの銀行間決済件数。

(注6) システムの機能や性能を部分的に停止させた状態で、稼動を維持すること。

これについては、運用設計と併せて総合的に検討すべきであると考える。

6.2 性能評価

本検証システムにおいては、銀行間決済単体処理（個人間送金処理を除く）で目標とした1,000 tpsの処理速度を達成した。一方で、管理系機能において決済用デジタル通貨の残高照会レスポンスにおいて、以下のような課題があることが分かった。

本検証システムでは、前述したとおり取引履歴を管理し、残高自体は必要なタイミングで算出するという方式を採用している。算出対象となる取引履歴が急激に増加した場合、これに比例して計算量（回数）が増加するため、結果として残高照会のレスポンスが遅延するという事象が発生する。この問題は、残高照会時のレスポンス遅延にとどまらず、銀行間決済のレスポンスやスループットの性能にも影響するとも考えられる。その理由は、銀行間決済の前処理として、送金額に対して決済用デジタル通貨の残高が不足していないかどうかをチェックする必要があるためである。この事象については、取引履歴情報の保持管理方法の見直し、あるいはそもそもの処理方式の見直し含めて検討する必要がある。

6.3 セキュリティ評価

ブロックチェーンネットワークに参加しているサーバ間での合意形成が行われずに、Hyperledger Fabricの台帳が改ざんされた場合であっても、改ざんされていないサーバ間で合意形成ポリシー^(注7)を満たす状態が維持されていれば、改ざんの検知・復旧が可能である。

例えば、3台のサーバでブロックチェーンネットワークを構成し、合意形成ポリシーを2に設定した場合を考える。3台のうち、改ざんされたサーバが1台、改ざんされていないサーバが2台存在したとすると、ブロックチェーンネットワークは以下の挙動をとる。

(1) 参照処理

- ・改ざんされたサーバの値は採用されない。
- ・値の不一致を知らせる警告ログが出力されるた

め、改ざんされたサーバの存在の検知が可能。

(2) 更新処理

- ・改ざんされたサーバの値をベースとした合意は形成されない（却下される）。
- ・値の不一致を知らせるエラーログが出力されるため、改ざんされたサーバの存在が検知可能。

また実際には、改ざんされたサーバが保有する値は、取引が行われるタイミングで改ざんされていないサーバが保有する正常値によって上書きされることで、全体復旧がなされる。

7. むすび

本稿では、ブロックチェーン技術による、新たな銀行間決済プラットフォームへの取り組みを紹介した。

今回の実証実験をととして、ブロックチェーン技術を活用した新たな銀行間決済の仕組みの有効性を確認することができた。その一方で、新たな課題も明らかになった。富士通はこれらの課題に対して、今後も最新技術の動向をフォローしつつ、解決に向けて精力的に取り組んでいく。また、今後も先進技術へのチャレンジを続け、新たな銀行間決済プラットフォームの可能性を検討するとともに、新しい金融サービスの創出への取り組みを通じて、社会変革の一助となるよう邁進していく。

参考文献

- (1) 富士通：ブロックチェーン技術を活用した新たな銀行間決済の実証実験を実施。
<http://pr.fujitsu.com/jp/news/2018/10/29-1.html>
- (2) 富士通：メガバンク3行とブロックチェーン技術を活用した個人間送金サービスの実証実験を実施。
<https://pr.fujitsu.com/jp/news/2017/10/10-2.html>
- (3) The Linux Foundation.
<https://www.linuxfoundation.jp/>
- (4) Hyperledger Fabric.
<https://www.hyperledger.org/>

(注7) 合意形成に必要な最低限の承認数。

著者紹介



谷内 圭 (たにうち けい)

富士通（株）
第一システム事業本部
金融業種向けデジタルビジネスの創出
に従事。



久保 竹清 (くぼ たけきよ)

富士通（株）
第一システム事業本部
金融業種向けデジタルビジネスの創出
に従事。