ブロックチェーンを安全につなげる セキュリティ技術「コネクションチェーン」

Security Technology ConnectionChain for Securely Linking Blockchains

藤本　真吾　　小暮　淳

あらまし

仮想通貨の管理に使用されているブロックチェーンは，非中央集権的な運用によって複数のブロックチェーン参加者間の安全な取引を可能にする分散台帳技術として，多方面で活用が期待されている。ブロックチェーンの価値を高めるためには様々なブロックチェーンの連携が必要となるが，アプリレベルの連携ではシステム運用者による不正な操作が発生し得るなど，透明性が確保できない。また，このような一連の操作を実行した際に発生するエラーへの対処も必要になる。これらの問題に対して，富士通研究所では異なるブロックチェーンを安全に連携して動作させるためのセキュリティ技術として「コネクションチェーン」を開発した。

本稿では，コネクションチェーンの特長と試作システムを紹介する。

Abstract

Blockchain, which is used for the management of virtual currency, is raising expectations in many different fields as a distributed ledger technology that realizes secure transactions between multiple blockchain participants through decentralized operation. Increasing the value of blockchains requires linking various blockchains, but linking at an application level is insufficient to ensure transparency, as shown by the possibility of unauthorized operations by system operators. There is also a need to deal with errors that may occur when these operations are executed. In order to address these issues, Fujitsu Laboratories has developed Connection Chain, a security technology for securely linking and operating different blockchains. This paper presents the features of Connection Chain and its prototype system.

1. まえがき

ブロックチェーンは，仮想通貨の取引や記録データを安全に管理するための分散台帳技術（DLT：Distributed Ledger Technology）である。複数のブロックチェーン参加者（以下，プレイヤー）間における協調作業を実現するための技術として，金融以外の分野でもその活用が期待されている。

2009年の運用開始以来，ブロックチェーンを利用した仮想通貨の一つであるビットコインは現在まで一度も停止することなく稼働を続けている。仮想通貨に関しては，これまで仮想通貨取引所でのコインの消失や流出がたびたび報じられている。これらの事件はブロックチェーン自体に問題があったのではなく，システム管理者が正しく運用していなかったために発生したことが明らかになっている。このように，ブロックチェーンを安全に運用することは難しいため，プラットフォーム技術やクラウドサービスが多数用意されるようになってきている。

このような状況を踏まえて，富士通研究所は異なるブロックチェーンを安全につなげるためのセキュリティ技術である「コネクションチェーン」を開発した。

本稿では，まずブロックチェーンの仕組みと課題を述べる。次に，開発したコネクションチェーンの特長と実証実験のための試作システムを紹介する。

2. ブロックチェーンの仕組み

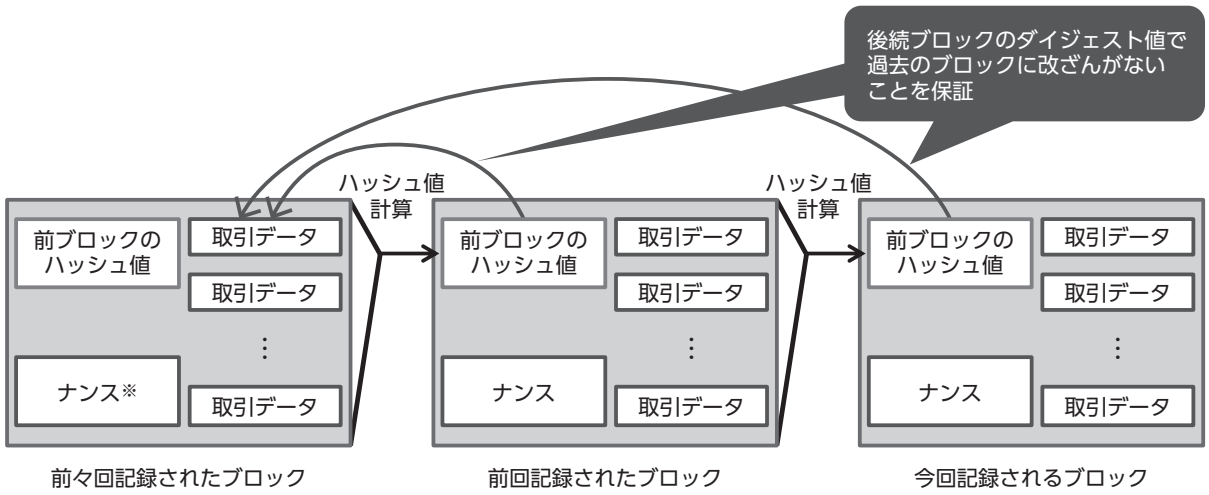
本章では，ブロックチェーンの仕組みについて述べる。

2.1 ブロックチェーンにおけるデータ記録

ブロックチェーンは，P2P（Peer to Peer）ネットワークで相互に接続されたノードと呼ばれるコンピュータで構成されている。各ノードが様々なデジタル資産を管理する台帳の複製を保持し合うことで，高い可用性を確保している。また，ハッシュ関数(注1)と公開鍵暗号技術(注2)を用いて，データの改ざん防止も実現している。

ブロックチェーンでは，記録の対象となるデータ（取引データ）を複数まとめた「ブロック」という単位で台帳に記録される（図-1）。各ブロックのデータは，ハッシュ関数で計算したハッシュ値で保護されるが，記録する取引データのほかに直前のブロック（前ブロック）のハッシュ値も含む。つまり各ブ

（注1） 出力されるハッシュ値の違いによってデータの改ざん検出を容易にし，整合性を保証できる技術。
（注2） 秘密鍵を所有するプレイヤーのみが署名でき，公開鍵で署名の正しさを検証できる技術。



※ブロック生成者が指定する特別な値。この値を変えることで，ブロック全体のハッシュ値を変化させることができる。

図-1 ブロックチェーンの仕組み

ロックに付与されたハッシュ値は，直前のブロックを間接的に保護することになる。この依存関係の連鎖により，ブロックチェーンに記録されたデータは多重に保護される。

2. 2 ブロックチェーンの特長

データを安全に管理するためのブロックチェーンの特長について述べる。

(1) P2Pによる信頼性の高いネットワークの構築

従来のデータ管理システムでは，システム管理者によって中央集権的なデータ管理が行われていたこともあり，データの改ざんや隠匿といった不正行為への対処が困難であった。ブロックチェーンでは，前回記録されたブロックのデータから算出されるハッシュ値のチェーンで取引データの改ざんを検出する。更に，取引を実行した結果を集約した台帳が各ノードに保持される。各ノードは，手元の台帳をほかの台帳と突き合わせて相互に監視することで，取引データに関する信頼性の高いネットワークを構築できる。

(2) 取引台帳の公開・共有

従来のデータ管理システムでは，データを台帳で共有する場合にデータの整合性を確保することが困難であった。一方，ブロックチェーンではP2Pネットワークを介して，全てのノードが台帳の複製を個々に保有しているため，各プレイヤーは手元の台帳でデータの整合性を確認できる。

(3) データ操作の検証強化

前述のように従来のデータ管理システムは中央集権的であるため，データ操作時に誤操作やシステム管理者による不正操作が発生することがあった。一方，ブロックチェーンには，複数の参加ノードに権限を分散し，あらかじめ決められた処理ルールに沿ってデータ操作を行う，スマートコントラクトと呼ばれる機能がある。この機能によって，各ノードで実行した処理結果を検証し，全てのノードの結果が一致したときにだけ台帳操作が反映される。

3. ブロックチェーン活用における課題

本章では，コネクションチェーンの開発の背景となった，ブロックチェーンの活用における課題について述べる。

3. 1 ブロックチェーン間連携の透明性確保

2018年4月時点で，世界で流通している仮想通貨は約1,500種類あると言われている。[(1)] 仮想通貨は，仮想通貨取引所を介して実際のお金を使った売買や，別の仮想通貨への交換もできる。関係省庁の指導のもと，仮想通貨取引所の登録制度などの運用上の法整備が進められてはいるが，仮想通貨の流出事件はたびたび発生している。

また，仮想通貨以外にも荷物の配送状況やデータコンテンツの利用権など，ブロックチェーンで管理されるデジタル資産の種類は増加している。このような資産の移転や交換を伴わない仮想通貨以外のデジタル資産の管理については，資産の状態の遷移が記録される。しかし，その記録の正当性はブロックチェーンの外で保証されることが多いため，厳密な運用ルールを決めることが難しい。その結果，ブロックチェーン間の連携において，行われている処理の透明性が確保できていない。

3. 2 台帳操作における例外処理

ブロックチェーンの種類にもよるが，ブロックチェーンにおける台帳操作が確定するまでには，一定の時間を要することが多い。また，プレイヤーが互いを信用できない場合であっても，複数のブロックチェーンをまたいで取引を行うことがある。このような場合，料金支払い能力の保証を得てから取引を開始し，取引全体の成否に応じて料金の収納や支払いの取り消しを行うエスクロー取引があると便利である。

このような時間のかかる取引やエスクロー取引では，一部の取引が成立しない場合も考慮する必要がある。この対応として，前述したスマートコントラクト機能を使って，成立しなかった取引を中止したり，取引そのものを元に戻したりすることが考えられる。しかし，本機能は単一のブロックチェーン上でしか動作しないため，複数のブロックチェーンをまたいだ取引を扱うことも，エラー発生時の例外処理を実行することもできなかった。

4. コネクションチェーンの特長

富士通研究所は，前章で述べた課題を解決するために，ブロックチェーンを安全につなげるセキュリティ技術であるコネクションチェーンを開発した。本章では，コネクションチェーンの特長を述べる。

4.1 透明性が高いブロックチェーン連携

筆者らは，異なるブロックチェーン間の連携処理の透明性を高めるため，単一のブロックチェーン上でしか動作しなかった既存のスマートコントラクト機能を調整した。そして，複数のブロックチェーンを連携させる拡張スマートコントラクトの実行をコネクションチェーンで実現した。

コネクションチェーンは，連携先ブロックチェーンの1ノードとして動作する連携ノードを持っている。連携ノードには，スマートコントラクトからの指示を受けて資産の移動などの台帳操作を行う機能と，連携先のブロックデータを受信して台帳操作の結果を証跡管理台帳に記録する機能がある。これによって，証跡管理台帳を見れば異なるブロックチェーンにまたがる一連の台帳操作を確認できる（図-2）。

4.2 エラー処理に対応したステート管理

コネクションチェーンでは，一部の取引が成立しなかった場合などの対応として，取引を保留状態にする機能を設けて，取引開始前の状態を復元できるようにしている。これには，第三者の仲介で安全に代金を支払う，預託支払いの概念を取り入れている。重要な点は，コネクションチェーンでしか操作できない口座を連携先のブロックチェーンに用意しておくことである。

これによって，支払いの保留が必要な場合には，本来の宛先に資産を移転する代わりに，コネクションチェーンが操作可能な預託口座に資産を移転する。そして，コネクションチェーンは，支払いの条件が満たされたかどうかを判断し，預託された資産を本来の移転先に移転するか，プレイヤーの口座に再度移転するかのいずれかの処理を自動で実行するようになっている。

5. コネクションチェーン技術の活用

本章では，コネクションチェーンを活用する際の具体例として，試作したシステムを紹介する。

5.1 仮想通貨決済システム

仮想通貨決済システムは，仮想通貨の交換機能を備えている。本システムの開発の背景として，特定の市町村で使用できる「電子地域通貨」がある。近年，電子地域通貨を発行して，地域住民による消費活動を促進する実証実験が数多く行われている。今回の実証実験で使用した試作システムでは，異なるブロックチェーンで管理されている地域通貨による支払いに対応した決済システムを実現する。この決済システムを利用すると，保有している電子地域通貨を利用地域外でも使えるようになる。

システムの利用者は，スマートフォンに特別なア

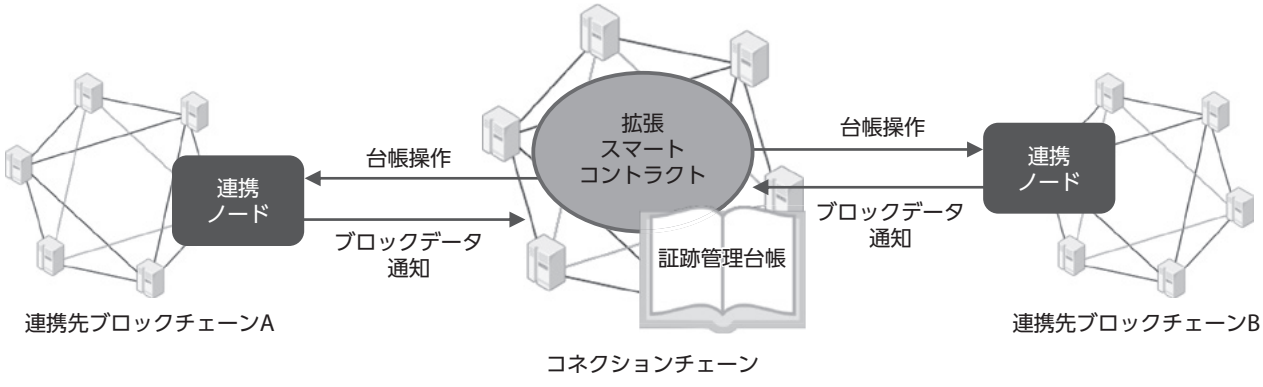


図-2　コネクションチェーンの拡張スマートコントラクト

プリをインストールすることなく，Webブラウザで電子地域通貨決済システムを利用できる。また，偽造対策に多大なコストがかかる印刷物の地域限定商品券を運用する場合に比べると，低コストで安全な運用が可能といったメリットがある。

例として以下に，電子地域通貨を運用している二つの商店街が連携して販促キャンペーンを実施するユースケースを説明する（図-3）。花子さんは，保有している電子地域通貨Aを使って，電子地域通貨Bを扱っているX書店で書籍購入を考えている。これを既存技術で実現しようとすると，花子さんは電子地域通貨の交換所で通貨を交換した後，X書店で支払うことになる。この場合には，花子さんはX書店への支払いのために，電子地域通貨Bを交換所から受け取るための口座を用意しなければならない。また，購入予定の書籍が売り切れていた場合に，交換後の地域通貨Bの使い道がなくなってしまうといった問題があった。

一方，試作した仮想通貨決済システムでは，「電子地域通貨B建ての料金支払いを電子地域通貨Aで行う」という拡張スマートコントラクトを実行すれば良い。花子さんは，電子地域通貨の移転の仕組みや変換レートを意識することなく，また電子地域通貨Bの口座を用意することなく，X書店で書籍を購入できる。

拡張スマートコントラクトの実行結果を記録したコネクションチェーンの取引記録を図-4に示す。この取引記録には，コネクションチェーンによって自動で実行される一連の操作の結果が，操作を行ったブロックチェーンにおける取引IDとタイムスタンプの組み合わせで記録されるため，いつでも取引内容の正当性を検証できるようになっている。

図-4　地域通貨交換システムでの資産移転記録の例

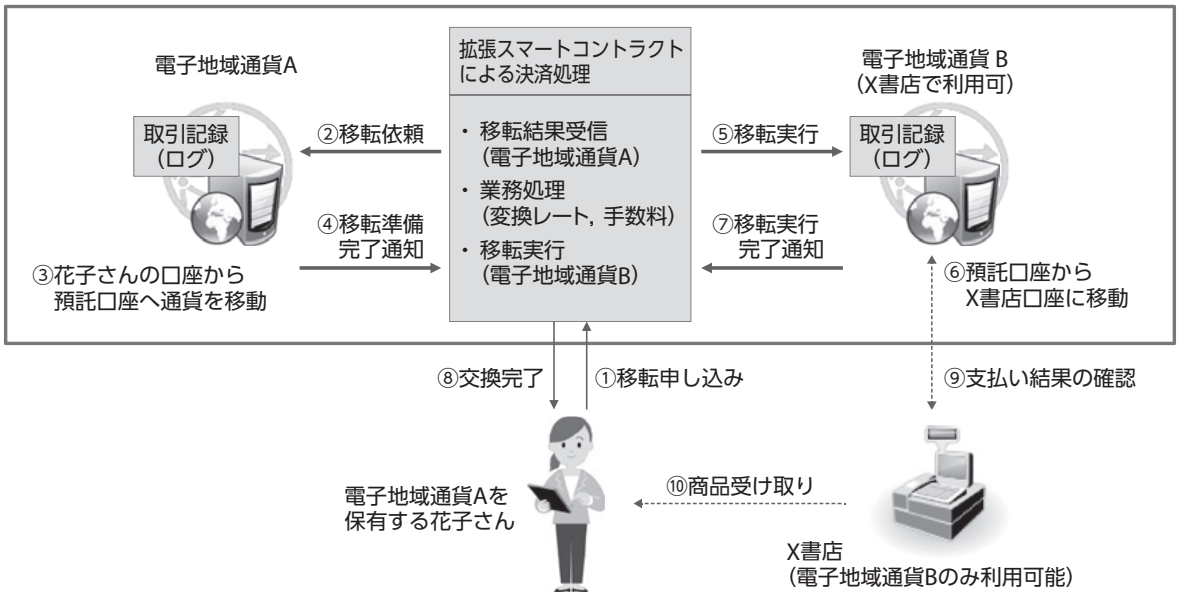


図-3　電子地域通貨の活用例

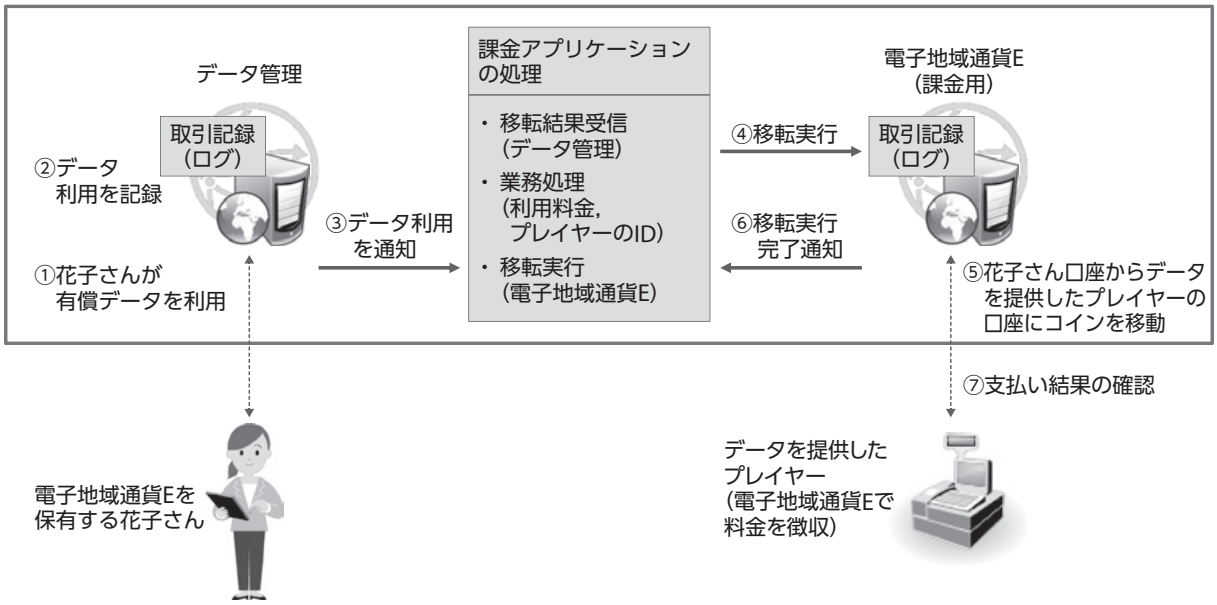


図-5　データ利用に連動した課金システム

また，何らかの理由でX書店が書籍を販売できない場合には，拡張スマートコントラクトが花子さんから預かった仮想通貨を花子さんの口座へ送り返すことで，購入を取り消すことも可能となっている。

5.2 データ利用に応じた課金システム

二つ目の試作システムでは，データの利用権を取引するブロックチェーンと課金用トークンを管理するブロックチェーンをつないで，データの利用量に応じた課金を実現した。

データの利用権を管理するブロックチェーンに対して，花子さんがデータの取得操作を行う。花子さんがデータの取得操作を行うたびに，データの利用権を取引するブロックチェーンには取引データが記録されるようになっている。このデータ利用権を管理するブロックチェーンと，課金用トークン（地域通貨E）を管理するブロックチェーンを，データの利用量に応じて課金するスマートコントラクトで連携させた。これによって，取引データが記録されるたびにコネクションチェーンが連携ノードの働きで検出する。その後，スマートコントラクトに設定された金額に応じて，課金用トークンを管理するブロックチェーンにある花子さんの口座から，データを提供したプレイヤーの口座へ資産の移転が自動的に実行される（図-5）。

6. むすび

本稿では，異なるブロックチェーンを安全に連携させる富士通研究所が開発したセキュリティ技術であるコネクションチェーンを紹介した。

ブロックチェーンは，複数プレイヤー間の安全な取引を可能にする技術であるため，プレイヤーの数が多いユースケースでこそ真価を発揮する。コネクションチェーンは，ブロックチェーンがもともと備えている特長を損なうことなく，より複雑なオンライン取引を安全に実現するための技術であり，ブロックチェーンの更なる可能性を引き出すことができる。今後も，実証実験によって実績を積み，実用化を目指すとともに共創型ビジネス実現に貢献していきたい。

参考文献

(1) 一般社団法人日本仮想通貨交換業協会：仮想通貨取引についての現状報告.
https://www.fsa.go.jp/news/30/singi/20180410-3.pdf

著者紹介

藤本　真吾（ふじもと　しんご）
（株）富士通研究所
セキュリティ研究所
ブロックチェーンの応用研究に従事。

小暮　淳（こぐれ　じゅん）
（株）富士通研究所
セキュリティ研究所
ブロックチェーンの応用研究に従事。