

ブロックチェーンを用いた 金融取引における多角的検証方式の考察

米倉 裕貴* 藤本 真吾* 森永 正信*

概要： 近年、ブロックチェーンを活用した分散型金融プラットフォーム「DeFi」が注目を浴び始めている。DeFiでは、金融取引が透明性の高い状態で自律運用されることで、取引の手数料を削減し、資産の流動性を高めることが期待されている。我々は、DeFiにおける厳格なKYCやAML実現のための課題に着目し、課題解決の第一段階目としてHyperledger Fabricを拡張した方式を考案した。本稿では、方式の内容および拡張前と比較した考察や、今後の課題について述べる。また、DeFiへの適用例として、証券取引時の決済に関する評価用システムを紹介する。

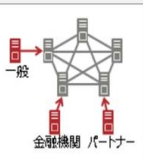
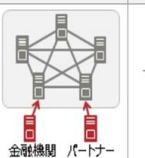
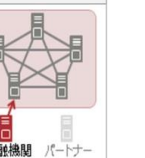
Consideration of Multi-verification Method in Financial Transaction using Blockchain

YUKI YONEKURA* SHINGO FUJIMOTO* MASANOBU MORINAGA*

キーワード ブロックチェーン、コンソーシアムチェーン、DeFi（分散型金融）、KYC、AML

1. はじめに

ブロックチェーンは、ネットワークに参加するノード間で取引を共有し、改ざん不能な形で共同管理することが可能な技術である。ブロックチェーンの様々な形態を図1に示す。Bitcoinのようなパブリックチェーンは管理者がおらず、不特定多数の参加者が参加可能である。一方、Hyperledger Fabricのようなコンソーシアム/プライベートチェーンは、特定の組織（ノード）のみが参加可能であり金融機関などでの利用が想定されている。

	パブリック	コンソーシアム	プライベート
			
管理者の有無	なし	あり (複数企業)	あり (単独)
BCN (※1) 参加者	不特定多数 (Permission less)	特定複数 (Permissioned)	組織内 (Permissioned)
合意形成の仕組み	PoW / PoS (※2) など (厳格な承認が必要)	特定者間のコンセンサス (厳格な承認は任意)	組織内承認 (厳格な承認は任意)
利用モデル	ビットコイン	金融機関などによる利用が想定されるモデル	

※1 BCN: ブロックチェーンネットワーク ※2 PoW: Proof of Work / PoS: Proof of Stake

図1: ブロックチェーンの様々な形態

(引用元: <https://www.fujitsu.com/jp/solutions/industry/financial/concept/blockchain/>)

そもそもブロックチェーンは、BitcoinやEthereumなどの仮想通貨分野を起点に普及し始めた。近年は、仮想通貨にとどまらず証券や不動産などの金融資産をトークン化して管理・取引する分散型金融プラットフォーム「DeFi」が注目を浴びている。DeFiは、以下の4つの基準を満たすプロジェクトのことを言う[1][2]。

- ・分散されたブロックチェーン上に、またはブロックチェーンを用いてサービスが構築される
- ・金融産業である
- ・共通の基準に準拠し、プロジェクト間の相互運用性を推進する
- ・3つのコア原則に従う（相互運用性とオープンソースであること、アクセシビリティと金融包摂、金融的な透明性）

DeFiでは、金融取引を透明性の高い状態で自律運用することで、取引の手数料を削減し、資産の流動性を高めることが期待されている。DeFiにおける金融産業はいくつかのカテゴリに分けることが出来る。代表的なものを以下に示す。

- ・レンディング（融資、貸付）
- ・ウォレット（仮想通貨、決済）
- ・セキュリティトークン（有価証券）
- ・バスケット取引
- ・DEX（分散型取引所）

レンディングは、近年急成長している分野で、資金の投資と借入れのマッチングをP2Pで行う。貸付の総額は数十億ドル以上となり、中でもMakerDAO[3]のステーブルコインDAIが有名である。

ウォレットは、よく知られたBitcoinやEthereumなどの仮想通貨を保管したり、送金や受金をしたりする際

* 株式会社富士通研究所 セキュリティ研究所
〒211-8588 神奈川県崎市中区上小田中 4-1-1, FUJITSU
LABORATORIES LTD., 4-1-1 Kamikodanaka, Nakahara,
Kawasaki, Japan.211-8588

に用いる電子的な「財布」にあたり、DeFi のエコシステムには欠かせないものと言える。

セキュリティトークンを扱うシステムは STO システムと呼ばれ、SPIN[4]や Polymath[5]に代表される。主に株式などの有価証券をトークン化しブロックチェーン上で流通、管理するものである。金融商品取引法に準拠するためにトークン発行や投資への参加が厳しく制限されている。

バスケット取引は、Facebook の libra[6]に代表され、複数種類の通貨・トークンをまとめて新しいトークンとして流通するものである。

DEX（分散型取引所）は、資産を個人で管理しユーザー同士で直接やり取りすることの出来る取引所である。分散型の取引所では秘密鍵を個人で管理するため、取引所がハッキングされても資産が盗まれない。EtherDelta[7]や Openledger[8]が有名である。

2. DeFi における課題

仮想通貨での出資を募集する ICO（Initial Coin Offering）が資金洗浄などの犯罪の温床になったこと反省から、規制当局は DeFi での KYC（Know Your Customer：本人確認）や AML（Anti Money Laundering：資金洗浄）を強化しようとしている。日本では、2018 年 11 月に改正された犯罪収益移転防止法（犯収法）において、取引所や銀行、証券会社など各種金融機関に例えば以下を義務付けている[9]。

第 4 条：取引時に確認が必要な取引（本人特定事項、取引目的、職業/事業内容、実質的支配者、資産・収入状況）

- ① 仮想通貨取引を継続・反復して行うことなどを内容とする契約の締結（アカウント開設契約など）
- ② 200 万円を超える仮想通貨の売買・交換（ハイリスク取引）
- ③ 10 万円を超える仮想通貨の移転

第 8 条：疑わしい取引の届出義務

この KYC や AML には個人情報の収集が必須であるが、個人情報であるが故に各金融機関は他社が持つ情報を活用することができていない。また、KYC や AML 以外にも DeFi が取り扱う金融取引では、各種金融機関の管理している秘密情報によって承認すべきか否かの判断が必要なケースが多い。

このようなケースの一例として、セキュリティトークンを扱う STO システムが挙げられる。セキュリティトークンは 2019 年 12 月に改正された金融商品取引法（金商法）[10]によって株式や債券と同じ第一項有価証券に分類され、仮想通貨よりも厳しく規制されている。こういった金商法の規制に対応するため、STO システムに求められる具体的な要件として以下が挙げられている[11]。

- ・適切な機関による厳格な KYC の実施
- ・適格性要件の判断に必要な情報収集
- ・適格な投資家リストの作成、メンテナンス
- ・適格な投資家リストの取引アドレスと本人の結合
- ・トークン流通前の適格な投資家リスト参照
- ・適格な投資家リスト以外の者への流通制限

適格性要件の判断に必要な情報や、適格な投資家リストは証券取引所や証券会社、銀行など各金融機関が保持しているが、各々が非公開な基準に基づいて判断しており、お互いに公開できない。よって、各金融機関は取引の検証に参加できず、適格な投資家リスト以外の者への流通制限を行う際、監査組織の権限によってリアルタイムに取引を強制的にキャンセルする必要がある（図 2）。

ここで挙げたような問題は、DeFi により資産の流動性が高まることで、さらに顕著に現れるであろう。

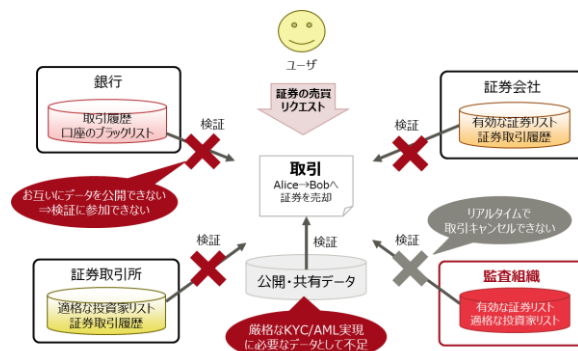


図 2：証券取引、決済における KYC や AML の課題

一方、先に挙げたコンソーシアムチェーンは、取引に関与するプレイヤーによる共同運用であり、取引の信頼性を向上することが期待される。コンソーシアムチェーンを DeFi のインフラとして適用すると、KYC や AML に関する問題の解決につながる可能性がある。具体的には、ノードとしてコンソーシアムチェーンに参加する各金融機関が取引に紐づく個人情報をもとに取引を承認/拒絶し、全体として取引の可否を決議することにより、各々の権限のもとでのセキュアな取引の運用が可能となり得る（図 3）。

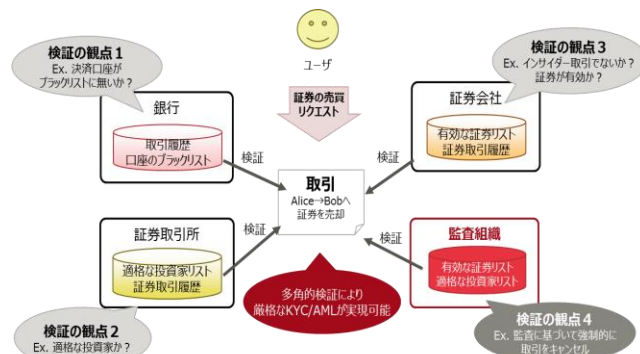


図 3：コンソーシアムチェーンによる KYC や AML の課題解決可能性

しかし、従来のコンソーシアムチェーンは、参加する全てのノードが同一のロジック¹やデータを用いて取引を承認/拒絶することにより取引の正当性を担保するセキュリティモデルである。そのため、参加する各ノードが異なるロジックやデータを用いて取引を承認/拒絶し、各々の承認/拒絶結果をもとに全体として取引を決議することはプロトコルの最適化を含め実現が難しい。

3. コンソーシアムチェーン (Hyperledger Fabric) を拡張した多角的検証方式

DeFi 実現における前述の課題解決に向けて、コンソーシアム関係者間の承認ワークフローをコンソーシアムチェーンの取引実行プロセス上で実現する多角的検証方式を考案した。また、本方式は、Hyperledger Fabric(v2.0.0)[12][13]を拡張することで実装できるように設計した。以下で拡張の方法を紹介し、STO システムへの適用と拡張前と比較した際の課題について考察する。

3.1. Hyperledger Fabric (v2.0.0)について

Hyperledger Fabric は、linux Foundation が開発するコンソーシアム型ブロックチェーン基盤の OSS である (以下、HLF)。HLF は、「Fabric-CA」、「Peer」、「Orderer」によって構成される。システム構成を図 4 に示す。

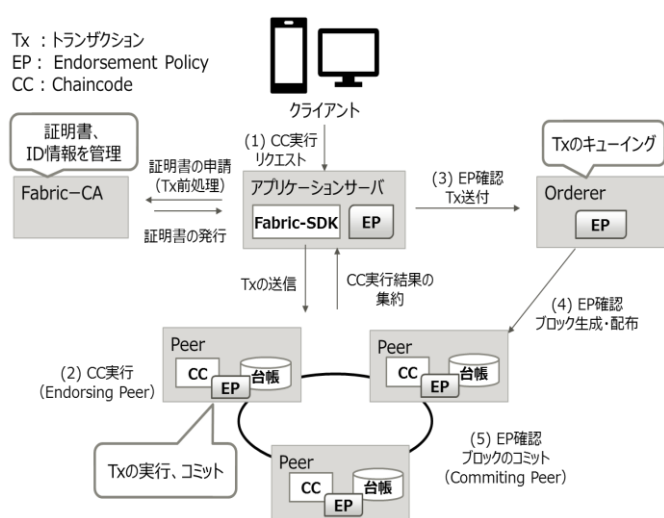


図 4: HLF のシステム構成

Fabric-CA は、複数のノード (Peer, Orderer) が属することのできる組織 (Organization) という独自の概念に基づくメンバーシップ証明書の管理 (発行や無効化など) を行う。組織ごとに取引の発行やアクセスに関する権限を設定することができる。

Peer は、一般的なブロックチェーンノードに対応す

るノードである。台帳 (ブロックチェーン, World State と呼ばれるブロックチェーンの状態管理用データベース) を保有し、Chaincode と呼ばれるスマートコントラクトを配備する。取引の実行時には、Endorsing Peer が Chaincode を実行し、Committing Peer が取引の検証を行う。

Orderer (Ordering Service) は、取引を調停し順序性を担保する特別なノードである。複数の Orderer 間でコンセンサスによりリーダーノードを決定し、リーダーノードがブロックの作成と全 Peer へのブロック配布を行う。

HLF のトランザクションの流れは以下である。

- (1) クライアントは、取引 (トランザクション) の提案を Endorsing Peer 宛に送付する。
- (2) Endorsing Peer は、Chaincode を実行してトランザクションをシミュレートし、実行結果に署名をしてクライアントへ返却する。
- (3) クライアントは、Chaincode に設定された Endorsement Policy² が満たされることを確認し、トランザクションを Orderer へ送付する。
- (4) Orderer は、Endorsement Policy が満たされることを確認の上トランザクションをキューイングしブロックを作成する。コンセンサスによりリーダーノードを決定し、リーダーノードが作成したブロックを Committing Peer へ送付する。
- (5) Committing Peer は、受け取ったブロック内の各トランザクションについて、Endorsement Policy および自身の台帳との整合性を確認したうえでブロックをコミットし自身の台帳へ書き込む。

3.2. Hyperledger Fabric の拡張

本方式では、HLF v2.0.0 へ次の 2 つの拡張を行った。

1. それぞれの Peer で、同一の処理ロジックで取引実行を行う Chaincode に加え、ESCC plugin³ に Peer 毎の取引検証処理を追加
2. Endorsement Policy を拡張し、Endorsement が必要な Peer の ID を設定。また、Peer ごとに検証内容や検証の重みなどメタデータを格納可能な形式に変更 (以下、合意 Policy と呼ぶ)

拡張後のシステムの全体構成を図 5 に示す。

¹ 取引や契約の条件確認や履行を行うプログラム。スマートコントラクトを指す。

² トランザクションをコミットするために必要な Peer からの Endorsement を Organization 単位で Chaincode に設定する。(例: Org 1 Admin の Peer の Endorsement が必要)

³ ESCC は Endorsement System ChainCode の略。

Peer の Endorsement 後の処理をカスタム (golang の plugin) で実装可能。

デフォルトでは署名機能のみ実装。

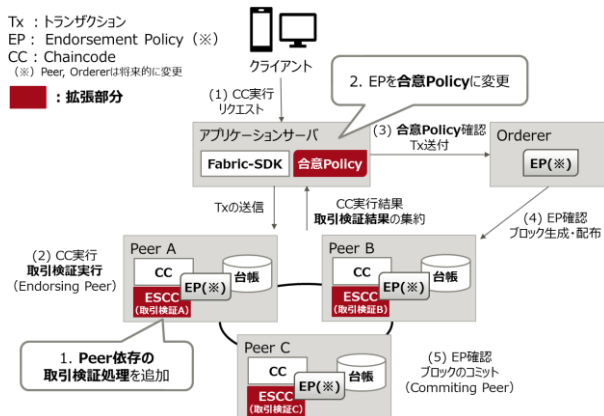


図 5：本方式の構成

従来の HLF から拡張した部分は、ESCC plugin の取引検証処理および合意 Policy のみであり、本方式を実装時に HLF のソースコードを修正する必要はない（図 5 白抜き文字）。合意 Policy に含まれるメタデータについては、必要に応じて検証内容の正当性確認や検証結果の重み付けなどを行う拡張も可能である。

アプリケーションサーバ、Peer の内部詳細を図 6 に示す。また、各コンポーネントの説明を表 1 に示す。

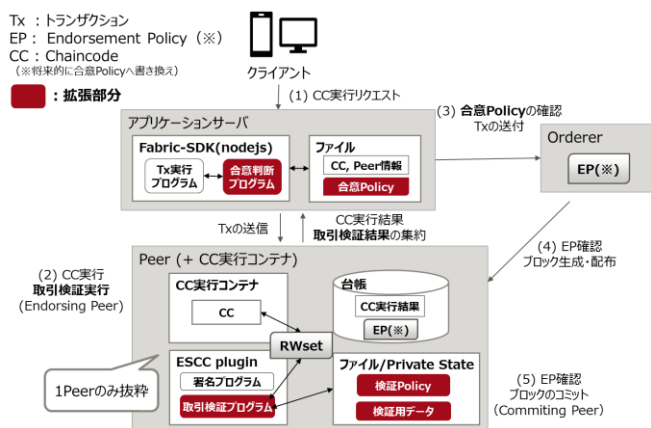


図 6：アプリケーションサーバ、Peer の詳細

表 1：拡張により追加したコンポーネント

コンポーネント	説明
合意判断プログラム	Chaincode 実行結果および取引の検証結果を収集し、合意 Policy により取引の合意判断を行う。
合意 Policy	Endorsement Policy を拡張、Chaincode ごとに設定する。現状、Endorsement が必要な Peer の ID を設定。Peer ごとに検証内容や検証の重みなどメタデータを格納可能。
取引検証処理 (ESCC plugin)	Chaincode 実行時に生成される WorldState に格納する情報 (RWset) から取引情報を参照。また、取引情報、検証用データ、検証 Policy を参照し突き合わせることで取引の検証を行う。取引検証結果に署名し、合意判断プログラムに渡す。
検証 Policy	取引情報、検証用データについて、設定値（文字列/数値）および検証 NG とする条件（設定値と一致/大なり/小なり）。
検証用データ	取引検証用のデータ。暫定でファイルに記載しているが、外部 DB や Private State からの参照も可能。

図 6 において、白抜き文字が従来の HLF から拡張した部分であり、各拡張部分について詳細な説明を表 1 に示している。アプリケーションサーバに付属の合意判断プログラムは、合意 Policy に従って各 Peer から収集した取引検証結果に基づいた合意を行う。また、Peer 内 ESCC plugin に実装された取引検証処理が検証 Policy、検証用データに従って個々の取引検証を実行する。拡張後のトランザクション実行シーケンスは以下である。

- (1) クライアント（アプリケーションサーバを経由）は、トランザクションの提案を Endorsing Peer 宛に送付する。
- (2) Endorsing Peer は、Chaincode を実行してトランザクションをシミュレートする。このとき、ESCC plugin の取引検証プログラムは RWset 経由で取引情報を参照し検証用データ、検証 Policy と突き合わせて取引を検証する。署名済みの Chaincode 実行結果に加えて、取引検証結果をクライアントへ返却する。
- (3) クライアントは、合意判断プログラムによって合意 Policy が満たされることを確認し、トランザクションを Orderer へ送付する。
- (4) Orderer は、Endorsement Policy*が満たされることを確認の上トランザクションをキューイングしブロックを作成する。コンセンサスによりリーダーノードを決定し、リーダーノードが作成したブロックを Committing Peer へ送付する。
- (5) Committing Peer は、受け取ったブロック内の各トランザクションについて、Endorsement Policy*および自身の台帳との整合性を確認したうえでブロックをコミットし自身の台帳へ書き込む。

3.3. 従来技術との比較と考察

2 章で挙げた STO システムに求められる要件に照らし合わせて、本方式を拡張前の HLF と比較した。結果を表 2（次頁）に示す。本方式では、ノードごとに異なる取引検証を行うことにより、各機関が独自の観点で判断した適格な投資家リストをもとに取引の厳格な検証および監査機関による取引の強制キャンセルが可能となる。

また、本方式がブロックチェーン上で行われることにより次の付加価値が得られる。

- ・取引の実行・検証処理実装の開発コストを削減（スマートコントラクトやプラグインの実装で実現可能）
- ・関係者間での取引実行、取引検証を 1 つのトランザクションで効率よく実現（スマートコントラクトによる取引実行結果、ESCC による取引検証実行結果を 1 回の通信でまとめて収集可能）

* 将来的に合意 Policy への置き換えを行う。

表 2：拡張前の HLF と提案方式の比較

要件	拡張前	提案方式	備考
適切な機関による厳格な KYC の実施	×	○	提案方式では、KYC に必要な情報を各機関に保持したまま厳格な検証が可能
適格性要件の判断に必要な情報収集	×	○	提案方式では、他社に公開したくない情報を半断に用いることができる
適格な投資家リストの作成、メンテナンス	○	○	各機関がリストの作成とメンテナンスを行う
適格な投資家リストの取引	○	○	各機関が持つリストと取引アドレスを照合する
トークン流通前の適格な投資家リスト参照	×	○	提案方式では、トークン流通前に各機関が保持するリストに照合して厳格な検証が可能
適格な投資家リスト以外の者への流通制限	×	○	提案方式では、監査ノードによる強制的な取引のキャンセルが可能

一方、拡張前のコンソーシアムチェーンと比較すると本方式には課題もある。本方式では、ノードごとに異なる取引検証を行うことにより、取引検証に関する単一障害点耐性（CFT：Crash Fault Tolerance）、ビザンチン耐性（BFT：Byzantine Fault Tolerance）、透明性が損なわれている。CFT については、同一の取引検証を行うノードを冗長化して対処可能であるが、BFT や透明性についてはノードごとに異なる処理を行い、お互いにデータやロジックを非公開とすることから現状対処できていない。これらの課題を解決することで、ノード間の取引検証に対する信頼が担保できれば、本方式の価値がさらに高まると考えている。

4. DeFi における適用例（証券取引時の決済）

前章で説明した多角的検証方式の DeFi への適用例として、証券取引時の決済に焦点を当てて試作した評価用システムについて紹介する。本システムは、複数のブロックチェーンを安全に連携可能なブロックチェーン技術「コネクションチェーン」[14][15]を用いて試作したが、多角的検証方式は一般的なコンソーシアムチェーンを用いたシステムでも適用可能である。システム外部から取引を投入するコンソーシアムチェーンに実装するのが適している（コネクションチェーンは、複数のブロックチェーンに投入する取引をまとめて外部から受け付け、処理を行う）。

本システムは、証券管理ブロックチェーン、暗号通貨管理ブロックチェーン、コネクションチェーンから成る。証券管理ブロックチェーンは、証券の発行および取引など諸々の管理を行うブロックチェーンである。また、暗号通貨管理ブロックチェーンは Bitcoin や Ethereum のような暗号通貨を管理するブロックチェーンである。本

システムでは、簡単のためにこれらのブロックチェーンは HLF 基盤上のスマートコントラクト（Chaincode）で実装した。コネクションチェーンは、証券管理ブロックチェーンにおける証券取引と暗号通貨管理ブロックチェーンにおける決済処理を安全に連携することで、証券取引時の決済を一連の取引として実行可能とする。

多角的検証方式は、コネクションチェーンに適用する。コネクションチェーンの各ノードには、証券取引・決済の関係者（銀行、証券取引所、証券会社、監査組織、仮想通貨取引所）を割り当てる。各関係者は、自身の持つ取引履歴やブラックリストをもとに証券取引と決済に関する取引を多角的に検証する。こうすることで、証券取引や決済に潜むインサイダー取引やマネーロンダリングなどの不正な取引を事前に防ぐことが出来る。本システムの構成を図 7 に示す。

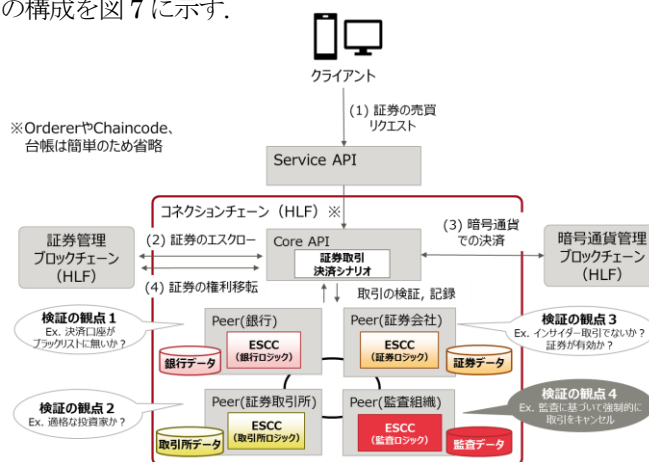


図 7：評価用システムの構成（証券取引時の決済）

図 7 において、コネクションチェーンの Core API と呼ぶアプリケーションサーバが証券取引および決済のリクエストを受け付け、証券取引・決済シナリオ（図中の(2)~(4)の処理手順を定めたもの）に従って証券管理ブロックチェーンおよび暗号通貨管理ブロックチェーンに対して処理を依頼する。これらの処理を、1つの取引としてまとめてコネクションチェーンの台帳に記録する。本システムにおける証券取引、決済のシーケンスは以下である。

- (1) クライアントは、証券の売買リクエストを Service API を介して Core API へ送付する。クライアントから送付されたリクエストは、コネクションチェーンの台帳に記録されるが、このときコネクションチェーンの各 Peer が取引の多角的検証を実行する。ここでは、全ての Peer が検証 OK としない限り(2)以降の処理は実行せずエラー内容がクライアントに通知される。
- (2) Core API は、証券管理ブロックチェーンに対して証券のエスクロー（売り手口座からエスクロー口座への一時的移転）リクエストを送付し、証券管理ブロックチェーンにて当該処理を実行する。証券管

理ブロックチェーンへのリクエストとレスポンスは、随時コネクションチェーンの台帳に記録される。

- (3) Core API は、暗号通貨管理ブロックチェーンに対して暗号通貨での決済（証券の買い手から売り手への支払い）リクエストを送付し、暗号通貨管理ブロックチェーンにて当該処理を実行する。暗号通貨管理ブロックチェーンへのリクエストとレスポンスは、随時コネクションチェーンの台帳に記録される。
- (4) Core API は、証券管理ブロックチェーンに対して証券の権利移転（エスクロー口座から買い手口座への移転）リクエストを送付し、証券管理ブロックチェーンにて当該処理を実行する。証券管理ブロックチェーンへのリクエストとレスポンスは、随時コネクションチェーンの台帳に記録される。

(3)または(4)にてエラーが発生した場合は、Core API によって(2)の処理が逆向きに実行（エスクロー口座から売り手口座への移転）されエラー内容がクライアントに通知される。

5. まとめと今後の課題

本論文では、DeFi（分散型金融）における厳格な KYC や AML を実現するための方式を考案した。具体的には、HLF を拡張し関係者間の承認ワークフローを取引実行プロセス上で実現可能とするものである。また、STO システムの要件という観点で本方式を拡張前の HLF と比較し、本方式が有効であることを確認した。さらに、考察の結果として次の課題があることが分かった。

① 取引検証に対する BFT の確保

② 取引検証に対する透明性の確保

今後は、これらの課題を解決する方向で引き続き検討を進めていく予定である。また、本方式の DeFi における適用例として、証券取引時の決済に関する評価用システムを紹介した。DeFi 以外のユースケースへの適用についても並行して検討を行う予定である。

参考文献

- [1] Medium.com, Opening #DeFi, available at: <https://medium.com/defi-network/opening-defi-42a5afdb71e0> (accessed May. 8, 2020)
- [2] DeFi – An Open Community of Decentralized Finance Platforms, available at: <https://defi.network/> (accessed May. 8, 2020)
- [3] Maker, A better money – Digital currency that can be used by anyone, anywhere, anytime ,available at: <https://makerdao.com/en/> (accessed May. 8, 2020)
- [4] Spin, Spin - Ride The Moment, available at: <https://www.spin.app/> (accessed May. 8, 2020)
- [5] Polymath, Security token solutions start here, available at: <https://polymath.network/> (accessed May. 8, 2020)
- [6] libra.org, Libra – A New Global Payment System, available at: <https://libra.org/en-US/?noredirect=en-US> (accessed May. 8, 2020)
- [7] EtherDelta, etherdelta.com, available at: <https://ethersdelta.com/> (accessed May. 8, 2020)
- [8] OpenLedger, Transform your business with blockchain, available at: <https://openledger.info/> (accessed May. 8, 2020)
- [9] e-Gov, 犯罪による収益の移転防止に関する法律（平成十九年法律第二十二号）, available at: https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=419AC0000000022 (accessed May. 8, 2020)
- [10] e-Gov, 金融商品取引法（昭和二十三年法律第二十五号）, available at: https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=323AC0000000025 (accessed May. 8, 2020)
- [11] KPMG ジャパン, セキュリティトークンの動向 IV. セキュリティトークンの仕様, available at: <https://home.kpmg/jp/ja/home/insights/2019/01/security-token-offering-20190131.html> (accessed May. 8, 2020)
- [12] Hyperledger 2020, A Blockchain Platform for the Enterprise – Hyperledger Fabric, available at: <https://hyperledger-fabric.readthedocs.io/en/release-2.0/> (accessed May. 8, 2020)
- [13] GitHub, GitHub – hyperledger/fabric at release-2.0, available at: <https://github.com/hyperledger/fabric/tree/release-2.0> (accessed May. 8, 2020)
- [14] 藤本真吾, 鎌倉健, “ブロックチェーンの安全な連携方式の提案”, SCIS2018
- [15] 東角芳樹, 竹内琢磨, 藤本真吾, 森永正信, “パブリックチェーンとコンソーシアムチェーンとの安全な連携方式の提案”, SCIS2019