Vol.2021-CSEC-95 No.22
Vol.2021-SPT-45 No.22
Vol.2021-EIP-94 No.22
2021/11/9

スマートコントラクトによるデジタル資産取引における プライバシに配慮した取引仲介の実現に向けて

藤本真吾 [1]　面和成 [2]

概要：ブロックチェーンの使途は，単純な所有権の移転から，複数の台帳を連動させて商品やサービスの購入を行う，などの，いわゆる商取引に適用範囲が広がりつつある．この交換取引を安全に実現する方法として，仲介処理が可能なスマートコントラクトの活用が期待されているが，現状のスマートコントラクトではこれを実現することが難しい．本論文では，デジタル資産取引の取引パターンをユースケースの分析からモデル化し，取引の仲介を行うスマートコントラクトの実現に向けたアプローチの提案を行う．

キーワード：ブロックチェーン，デジタル資産取引，モデル化

Consideration of privacy-conscious, smart contract-based trade intermediation between digital assets

SHINGO FUJIMOTO[†1]　KAZUMASA OMOTE[†2]

Abstract: Blockchains are expanding from ordinary cryptocurrency management to the trade of digital assets across different blockchain ledger, such as a purchase of goods. Researchers expect the smart contract to be used in this field, but it is still impossible to securely execute such trade with existing smart contracts. This paper will discuss the modeling for various patterns of digital assets trade and clarify the methodologies to enable secure, privacy-conscious trade mediation with extending the capability of smart contracts.

Keywords: Blockchain, Digital assets trading, System modeling **]

1. はじめに

ブロックチェーンの使途は，単純な所有権の移転から，複数の台帳を連動させて商品やサービスの購入を行う，などの，いわゆる商取引にまで適用範囲が広がりつつある．この交換取引を安全に実現する方法として，仲介処理が可能なスマートコントラクトの活用が期待されているが，現状のスマートコントラクトではこれを実現することが難しい．

本研究では，2 章でブロックチェーンとデジタル資産の現状について整理し，トークンエコノミーに関係する技術としてのブロックチェーンの特性と，トークンエコノミーの可能性を明らかにした．

具体的な本研究の貢献は，3 章で説明しているデジタル資産取引のモデル化と，続く 4 章での前章のモデルからデジタル資産取引仲介システムの検討を行った．

具体的な本研究の貢献は，3 章で定義しているデジタル資産取引のモデル化で，トークン化されたデジタル資産の取引を取引対象となるトークンの種別で整理し，各種トークンが持つ特性を利用して，想定される他トークンとの交換取引パターンをモデル化したことである．また，続く 4 章では，トークンエコノミーの実現に向けて，前章での取引モデルの分析結果から，トークン取引仲介システムに求められる機能要件を抽出し，スマートコントラクトにトークンエコノミーで新たに追加された機能要件に応じた拡張を行うアプローチで技術課題としてまとめている．

2. ブロックチェーンとデジタル資産取引

ブロックチェーンはもともと仮想通貨ビットコインの管理，運営のために考案された技術で，「取引履歴を暗号技術によって過去から 1 本の鎖のようにつなげ，正確な取引履歴を維持しようとする技術」とされている[1]. 昨今では，このブロックチェーンを発展させ，仮想通貨以外のデジタル資産管理や，ブロックチェーン上に実装されたスマートコントラクトの活用した，より複雑なデジタル資産管理システムの構築や，トークン化された異なるデジタル資産同士を交換する仕組みとしてトークンエコノミーが検討されている．

1 富士通株式会社
FUJITSU Limited
2 筑波大学
Tsukuba University

ⓒ2021 Information Processing Society of Japan

Vol.2021-CSEC-95 No.22
Vol.2021-SPT-45 No.22
Vol.2021-EIP-94 No.22
2021/11/9

2.1 ブロックチェーンの仕組み

仮想通貨ビットコインの管理・運用のために生まれたブロックチェーン技術ではあるが，現在ではビットコインの設計思想や機能を継承しながらも，用途別に独自進化したブロックチェーン基盤ソフトが数多く開発され，実際に運用されている．ブロックチェーンには，公開鍵暗号とハッシュ関数からなる電子署名技術と，Peer-to-Peer ネットワーク通信など，古くからある安定した技術が使われているが，そのユニーク性は，コンセンサスアルゴリズムを使った取引の非中央集権的な検証の仕組みにある．

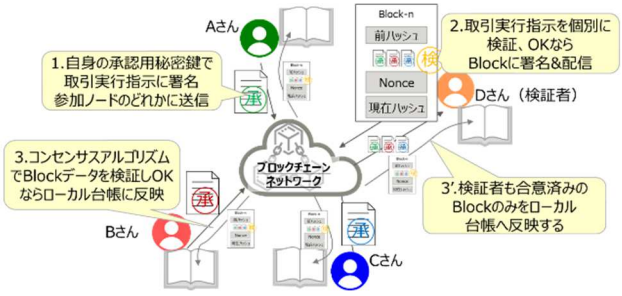


図 1：ブロックチェーンの仕組み

ブロックチェーン上で取引をしようとするユーザは，自身が発行する取引データ（例えばあるユーザのウォレット口座から別ユーザの口座への送金）に電子署名してから，P2P ネットワークに署名済みの取引データをブロックチェーンネットワークに参加するノード経由で送信する（図 1 のステップ 1）．次に，コンセンサスアルゴリズムの一部として規定された方法で，取引の検証者が選択され，選ばれた検証者は取引の正当性を検証する．このとき検証するのは，電子署名だけではなく，参加ノード間で同期している台帳に記録されている取引履歴と不整合がないか検査する．これは，取引につけられた署名が正しいものであっても，ウォレット口座の残高が送金予定額より小さかったり，二重取引をしていないかをチェックするためである．検証者が正当と判断した取引はブロックと呼ばれる取引データの集合に取り込まれ，他の参加ノードへ配信される（図 1 のステップ 2）．そして，そのブロックデータは，次に選ばれた検証者のチェック対象になっており，次の検証者が正しいと認めたブロックデータのみが台帳の同期対象になる（図 1 のステップ 3 とステップ 3'）．このようにして，ブロックチェーンではユーザと検証者が互いに監視しあうことで非中央集権な形の運営でも安全に取引が実行できている．

2.2 スマートコントラクトの仕組みと導入のメリット

「スマートコントラクトとは自動的な契約のことであり，契約とその履行条件をあらかじめプログラミングしておくと，契約条件が満たされた際に自動で取引が行われるような仕組み[2]」である．

スマートコントラクトは，ブロックチェーンネットワークで動作するプログラムであり，その取引プロセスを自動化できることから，決済期間の短縮や不正防止や，ユーザによる仲介が不要で運用コストを削減といった導入メリットがある．

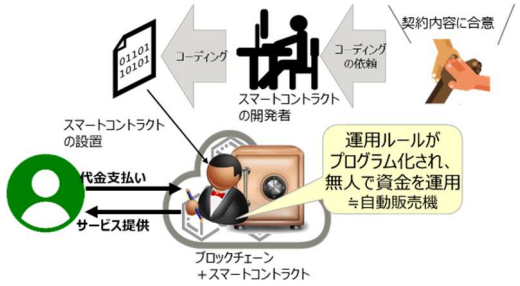


図 2：スマートコントラクトの仕組み

2.3 デジタル資産のトークン化とトークンエコノミー

ブロックチェーンによる「トークン化」が注目されている．トークン化（トークナイゼーション）とは，物理的な資産や仮想的な資産を，売買可能なデジタル単位に変換することで，トークン化により地域的な障壁や仲介者を排除し，資産を細かく分割できるとされている[3]．トークンには用途や性質が異なるさまざまなトークンがあるが，そのトークンが別のものに代替可能かどうか（ファンジビリティ）という観点では FT と NFT に分類できる（表 1）．

ここで注目すべきなのは NFT であり，「ブロックチェーンが持つ非中央集権や透明性，トレーサビリティ，関係者間の直接的な情報共有および管理，対改ざん性といった技術特性を備えていることに加え，固有性，取引可能性，相互運用性，プログラマビリティといった特性も併せ持っている[4]」ことで，従来は運用が難しかった“トークンエコノミー”の実現が期待されるからである．

トークンエコノミーとは，「トークンを用いた価値のエコシステムで，ブロックチェーンを基盤として個人や法人が資産を電子化（トークン）して運用することにより，多くの人や企業がその資産価値を新たに認識し，活用や拡張，交換などの循環が活発化し生まれる豊かな経済圏[5]」，とされている．一般的なデジタルコンテンツの流通では，コピーや改ざんが容易なため，現実の資産や販売物と比較して価値を持たせることが難しいが，NFT では暗号技術でコピーや改ざんを防止できるので，資産取引をデジタル空間で完結させることで，「（独自の取引市場がある）金（ゴールド）で株式を買う，といったイメージのユーザ体験に近く，取引の見た目上は，物々交換のような形になる[6]」．

既存の商取引の決済に通貨が用いられるのは，通貨に何にでも交換できて誰もが欲しがる価値があり，いわゆる「欲

ⓒ2021 Information Processing Society of Japan

Vol.2021-CSEC-95 No.22
Vol.2021-SPT-45 No.22
Vol.2021-EIP-94 No.22
2021/11/9

望の二重の一致（注a)」を不要にする機能が不可欠であったためである．「しかし，インターネットの普及で，今や二重の一致は奇跡ではなくなった．今後スマホ決済などによって売り手と買い手がインターネットで結ばれていけば，やがて物々交換や知識・労働の提供など，お金を用いない取引が拡大していくだろう[7]」といった予測もあるように，ブロックチェーンによるトークンエコノミーには新たな経済活動の実現手段としての期待がある．

表 1：トークンの分類

分類	定義	例
FT(Fungible Token)	ある資産を同じ種類かつ同じ価値をもつ別の資産と交換できるトークン	法定通貨，仮想通貨
NFT(Non-Fungible Token)	特別な価値を持つように設計されており，ユニークで，固有の価値を持ち，分割できず，相互交換もできないトークン	デジタルコンテンツの所有権（注b)，物理的な資産の所有権

3. デジタル資産取引のモデル化

本章では，デジタル資産取引を分類，類型化して，先に述べたトークンエコノミーを実現するための現状の課題を整理する．

3.1 トークンの分類

まず，トークンエコノミーのモデル化に先立ち，取引対象となるトークン化されたデジタル資産についてその性質による分類を行う．

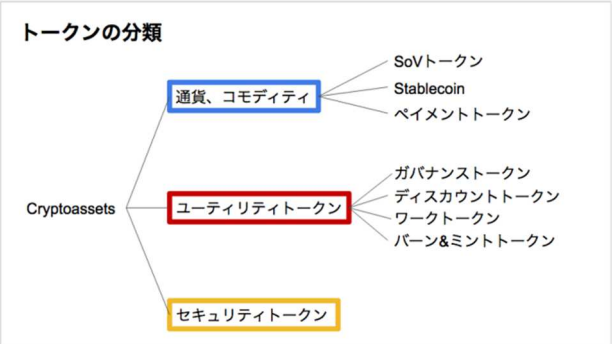


図 3：トークンの分類[8]

図 3 にあるようにトークンは用途によって大きく 3 種類に分類される．また，通貨，コモディティとユーティリティトークンでは，さらにその機能によってより詳細な分類が可能である(表 2).

表 2：トークンの用途による分類

	分類	定義	例
通貨，コモディティ	SoV トークン	SoV とは，Store of Value の略で，通貨の条件のうちの 1 つである価値貯蔵手段を意味し，完全に独立したアセットとして価値保存できるトークン．通貨価値の算出にはフィッシャーの交換方程式（MV=PQ）が用いられる．	Bitcoin, Monero, Zcash など
	Stablecoin (ステーブルコイン)	他の通貨を価値の担保としてボラティリティをなくしたもの．通貨の 3 条件のうちの価値の尺度や交換手段として使われる．	Tether, MakerDao, Libra など
	ペイメントトークン	支払い手段として用いられるトークンで SoV のような流動性や安定性がなく，ネットワーク経済圏の中での通貨として機能する．	
ユーティリティトークン	ガバナンストークン	ネットワーク運用や開発についての方針に関する投票権を決定するトークン．	
	ディスカウントトークン	ホルダーにプロジェクトが提供する資産を割引購入する権利を与える．	BNB トークンによる取引手数料の割引適用

a 互いに自分が欲しいものを持っていないと物々交換が成立しない，という問題

b デジタルコンテンツの所有権を NFT でトークン化することの法的な妥当性については結論が出ていない

ⓒ2021 Information Processing Society of Japan

Vol.2021-CSEC-95 No.22
Vol.2021-SPT-45 No.22
Vol.2021-EIP-94 No.22
2021/11/9

	ワークトークン	サービス提供を行う作業者が仕事の質を保証するために作業を始める前に保有トークンをステークし，仕事を正しく完了するとステークしたトークンが返還される．仕事が不十分と判断されたらステークしたトークンが没収される	Augur, Filecoin
	バーン&ミントトークン	バーンとミント(発行)によって通貨供給量を調整し，サービス需要と価格のインフレが比例するようにコントロールする．毎月一定量のネイティブトークンが新規に発行され，ネイティブトークンを購入したユーザーがサービスを利用すると所有するトークンがバーンされる．このとき同時に決済用トークン（例えば USD 建て）が発行され，サービス提供者に譲渡される．	Factom
セキュリティトークン		資産をトークン化して表現したもので，発行体が価値を担保するトークン．米国の基準では Howey テストの 4 条件を満たすことが必要[9]．ICO で発行されるユーティリティトークンとは違い，法令に従って発行・取引され，また(ホルダーの)権利が保証される[10]	デジタル債券, NFT(注c)

3.2 トークン取引のモデル化

3.1 章で整理されたトークンの分類について，既存の金融商品などから想定される他デジタル資産との取引パターンとしてモデル化する．

c 法令による規制でセキュリティトークンとみなされない場合もある．

(1) 通貨，コモディティの取引

通貨，コモディティに分類されるトークンには，SoV トークンなど市場での価格変動が大きいものが含まれる．SoV トークンの価格変動の大きさは投資目的では好まれるものの，別のデジタル資産との交換取引を行うトークンエコノミーでは，価格の変動が大きいことがデメリットになり使いにくい．逆に価格変動を低く抑えた，ステーブルコインやペイメントトークンは，別のデジタル資産の譲渡を受ける場合の決済手段としての使途が有望である．

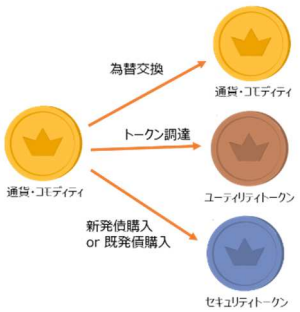


図 4: 通貨・コモディティのユースケース

(2) ユーティリティトークンの取引

ユーティリティトークンは，それ自体が資産価値を持つことはないので，ユーティリティトークンが起点となる交換取引は，購入済みのユーティリティトークンの払い戻し，もしくは保有するユーティリティトークンをサービス提供者へ譲渡してサービス提供を受ける使途が一般的と考えられる．

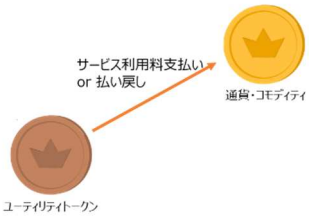


図 5: ユーティリティトークンの交換ユースケース

(3) セキュリティトークンの取引

セキュリティトークンはデジタル債券とも呼ばれ，既存金融商品である債券の役割[13]を代替するものである．出資の証拠であるセキュリティトークンが起点となる取引は，セキュリティトークン発行時に設定される償還期間満了に伴う通貨，コモディティへの償還が基本となる．これに加えて利子付き債では一方で，市場流動性を持たないユーティリティトークンとの交換が発生することは考えにくい．ところで，金融市場での債券の運用から類推すると，企業間での提携で株券や債券の交換が行われることがあるので，セキュリティトークン同士の直接交換も考慮が必要である．

ⓒ2021 Information Processing Society of Japan

Vol.2021-CSEC-95 No.22
Vol.2021-SPT-45 No.22
Vol.2021-EIP-94 No.22
2021/11/9

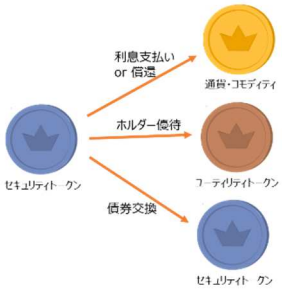


図 6：セキュリティトークンの交換ユースケース

4. デジタル資産取引仲介システムの検討

3 章でモデル化したトークンエコノミーのユースケースからデジタル資産取引における機能要件を抽出する．また，その機能要件を満たすようなデジタル資産取引仲介システムの実現検討を行う．

4.1 トークンエコノミーにおけるユースケースの分析

トークンエコノミーのユースケースと，既存金融サービスや関連法令への配慮からトークンエコノミーに関するデジタル資産取引への機能要件を抽出し，表 3 にまとめた．

表 3：ユースケースから抽出した機能要件

ユースケース	機能要件	備考
（共通）	・取引履歴の記録	・取引当事者以外には取引内容の秘匿が必要 ・監査目的での取引チェック機能が必要
為替交換	・為替レート設定 ・AML チェック	・市場流動性が高いトークンを扱うため取引の追跡性に関するプライバシへの配慮が必要 ・AML 対策のため取引口座開設時のユーザ身元調査がなされていることを前提とした
トークン調達	・トークン価格設定	
新発債購入	・トークン価格設定 ・出資者（セキュリティトークンのホルダー）属性情報のチェックと記録	・法令対応に必要な出資者属性情報について取引前のチェックと記録が必要（居住国，口座情報，投資適格性など）
既発債購入	・約定情報設定 ・新ホルダーの属性情報のチェックと記録	・約定情報のうち譲渡価格は取引毎に違うが，当事者以外には秘匿が必要
サービス利用料支払い	・利用料金設定	・サービス提供の成否判定が必要
払い戻し	・払い戻しレート設定	・当事者以外には払い戻された資産の移転先情報の秘匿が必要
利子支払い	・利払いステータス記録 ・利息の支払い請求	・利子支払い後も所有権は残るので利払記録と所有権を紐づけた記録が必要 ・ブロックチェーンにはタイマー処理がないため ST ホルダー自身による利息の支払い請求が必要 ・当事者以外には利息送金先情報の秘匿が必要
償還	・償還ステータス判定	・償還満了日までは償還の実行禁止が必要

ⓒ2021 Information Processing Society of Japan

Vol.2021-CSEC-95 No.22
Vol.2021-SPT-45 No.22
Vol.2021-EIP-94 No.22
2021/11/9

ホルダー優待	・優待ステータス判定 ・優待ルール設定	・優待によるトークン発行後も所有権が残るので，トークン発行履歴を ST の所有権情報と紐づけた記録（優待ステータス）が必要
債券交換	・交換レート設定	

上記の機能要件抽出ではトークンエコノミー特有の機能要件として「取引当事者以外には取引内容の秘匿が必要」と，「監査目的での取引チェック機能が必要」という一見相反した要件が挙がっている．

特に，コモディティ，通貨に分類されるトークンが関わるトークン交換取引については，その市場流動性の高さからトークンのウォレット口座番号が公開されていると，口座に紐づくユーザの購買行動の追跡が可能になるため，ブロックチェーン台帳を利用することの最大のメリットである取引の透明性は担保しつつ，ウォレット口座情報などの個人情報につながる情報は，取引の当事者以外には秘匿する必要があることがわかった．

また，さらに，既存のブロックチェーン連携では取引が電子署名のチェックなどの暗号技術でのチェックで十分だったが，トークンエコノミーのトークン交換では，トークンが持つ特性に踏み込んだチェックが必要であることもわかった．

具体的には，セキュリティトークンの発行，運用で，トークン発行体の属する各国の，資金洗浄などの犯罪防止や，外国籍投資家の出資比率への規制などの法令遵守が求められるため，トークンホルダー情報の参照や，記録が必要となることが判明した．

さらに，セキュリティトークンには利払日や償還日などの時間と連動したイベントと連動した運用ルールがあるが，既存のスマートコントラクトでは時間連動イベントの処理は苦手なのでその対応も必要となる．

4.2 デジタル資産取引仲介の実現に向けた課題

前章での機能要件分析の結果を踏まえて，トークンエコノミーの実現に必要な機能要件を備えたスマートコントラクトによるデジタル資産取引におけるプライバシに配慮した取引仲介システムの提案を行う．

ブロックチェーン取引において，当事者以外に信頼がおける信頼点となる存在がスマートコントラクトである．このスマートコントラクトの処理において，台帳上に記録されていない情報はすべてオラクル情報(注d)とみなされ判断の基準に取り込めない．一方で，トークンエコノミーでの交換取引ではトークンの管理には直接関係しない，台帳外の情報参照や，証跡としての安全な記録メディアが必要である．このようなブロックチェーン間連携を実現する技術のひとつとして異なる種類のブロックチェーン台帳同士を連携専用のブロックチェーンで統合管理する ConnectionChain 技術[14]を開発しているが，今回の検討で抽出された機能要件のうち以下のような機能要件を満たしていない：①取引の追跡性に関するプライバシへの配慮
②オラクル情報（法令対応に必要な出資者属性情報など）のチェック
③ブロックチェーンにはタイマー処理がない

この中でもプライバシへの配慮は，トークンエコノミーに特有の機能要件で，ビジネス上の理由から取引上の秘密やプライバシの保護が期待されるため，秘匿しなければいけない情報が存在する．その一方で，セキュリティトークンでは法令遵守の観点で，秘匿性と両立される形で取引の監査性を同時に満たす必要がある．

ところで，このような秘匿性と監査性を両立させる技術として ZKP(ゼロ知識証明)技術がある．このゼロ知識証明技術を使えば，取引内容のうち公開が必要な情報と，秘匿が必要な情報を選択して台帳上で共有できる可能性がある．しかし，ゼロ知識証明では証明を検証する側にも安全な鍵管理や安吾処理が求められるため，そのままスマートコントラクトで利用できないという問題が存在する．

そこで，この研究での次のステップとして，既開発の ConnectionChain に以下に挙げる機能拡張を行い，トークンエコノミーに対応したデジタル資産交換を行う取引仲介システムの開発を行う予定である：

① ゼロ知識証明に必要な鍵管理機能
② 交換取引に関するオラクル情報の管理機能
③ 時間駆動型のイベント処理機能

図 7 に検討中のスマートコントラクトによるデジタル資産取引におけるプライバシに配慮した取引仲介システムのアーキテクチャを示す．

dスマートコントラクトに外部のサードパーティ製サービスから与えられる情報で，ブロックチェーンと外の世界をつなぐ役割を果たす．

ⓒ2021 Information Processing Society of Japan

Vol.2021-CSEC-95 No.22
Vol.2021-SPT-45 No.22
Vol.2021-EIP-94 No.22
2021/11/9

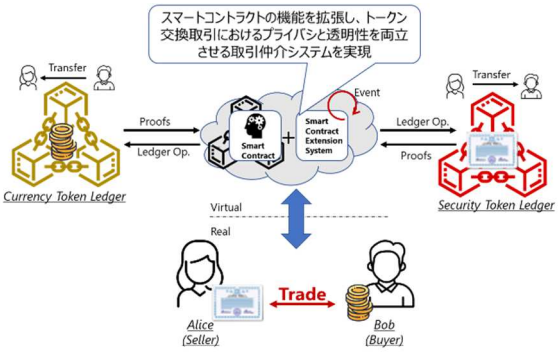


図 7：トークン取引仲介システムのアーキテクチャ

5. まとめ

本論文では，ブロックチェーンの新たな使途としてトークンエコノミーに焦点を当て，トークンの種別の性質からトークンエコノミーのユースケースで想定される交換取引のパターンから取引モデルを提案した．また，提案モデルの分析結果から，スマートコントラクトの機能拡張によるトークン交換取引の仲介システムの実現にむけたアプローチを提案した．

今後は，本論文で検討したアプローチに沿って，スマートコントラクトの機能を拡張し，提案したアーキによるデジタル資産取引仲介システムの設計，および試作に研究をすすめる予定である．

参考文献

[1] “ブロックチェーンって何？”．https://www.zenginkyo.or.jp/article/tag-g/9798/, （参照 2021-10-15）．
[2] “【スマートコントラクト】特徴やイーサリアムの事例を紹介”. https://udemy.benesse.co.jp/development/blockchain/smart-contract.html, （参照 2021-10-15）
[3] “「トークン化」の仕組みとは”．https://coinpost.jp/?p=234391, （参照 2021-10-15）.
[4] “NFT（非代替性トークン）を活用したデジタル世界の未来”. https://www.pwc.com/jp/ja/knowledge/column/disruptive-technology-insights/blockchain-featured1.html, （参照 2021-10-15）．
[5] “プレスリリース：ブロックチェーン推進協会(BCCC)がトークンエコノミー部会を新設”．https://prtimes.jp/main/html/rd/p/000000007.000035659.html, (参照 2021-10-15).
[6] “究極のフィンテックは「物々交換」？”．https://www.sbbit.jp/article/fj/39629, （参照 2021-10-15）．
[7] “キャッシュレスの次は「マネーレス」が到来する”．https://president.jp/articles/-/31561?page=2, （参照 2021-10-15）
[8] “トークンモデルの分類”. https://chainscape.co/articles/62, （参照 2021-10-15）．
[9] “セキュリティトークンの概説と動向”．https://www.jri.co.jp/MediaLibrary/file/column/opinion/pdf/12671.pdf, （参照 2021-10-15）．
[10] “基礎から学ぶ STO　～仕組みと魅力～”．https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&cat1=home&cat2=none&dir=info&file=home_sto_summary.html, （参照 2021-10-15）．
[11] “初めてでもわかりやすい用語集：債券”．https://www.smbcnikko.co.jp/terms/japan/sa/J0067.html , （参照 2021-10-15）．
[12] S. Fujimoto, Y. Higashikado and T. Takeuchi, "ConnectionChain: the Secure Interworking of Blockchains," 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019, pp. 514-518, doi: 10.1109/IOTSMS48152.2019.8939267.

ⓒ2021 Information Processing Society of Japan