2020 年 10 月 10 日（14:40 ~ 16:40）
日本経済学会パネル討論会
「デジタル通貨時代の金融経済」パネリスト報告

デジタル通貨、スマートコントラクト、プラットホーム

松島斉

東京大学大学院経済学研究科教授

はじめに...

貨幣には 2 つの形態がある

トークン型：　　コイン、キャッシュ
アカウント型：　　銀行口座預金

正当な支払いかどうかの確認方法に違いがある

トークン型：　　トークンが本物かどうかの確認
アカウント型：　　支払主が本人かどうかの確認
（要個人情報＋取引データ）

トークン貨幣の今昔

アナログ通貨：　偽造防止、交換手段（持ち運び）、
価値貯蔵（盗難防止）のコスト大
→ アカウント型にアドバンテージ

デジタル通貨：　コスト削減に成功
→ アカウント型からトークン型へ

民間団体はトークンを SDGs に利用する

地域通貨： コミュニティーの活性化、LETS

Feeding America： フェイクマネーを使って Food Banks に食料配分

特徴： 発行主体独自のミッション
独自の価値尺度、利用者制限

問題点： 不人気、利用者退出

→ より開かれた、営利的なネットワーク創りが必要
デジタル技術革新が追い風に

報告のテーマ

将来的なデジタル通貨の役割の重要性と影響力の大きさを
ブロックチェーン（特にスマートコントラクト）
を例に解説し、政策的含意を引き出す

Ⅰ．ブロックチェーン

オンライン分散型取引台帳

トークン（暗号通貨）の移動を時系列的に一本のチェーンとして記録

不正、改ざん（ほぼ）不可能

→ 法定通貨の裏付けなく価値発生

通貨の独立性、固有の価値尺度で決済

→ 民間通貨の躍進が期待

法定通貨との競争共生（Bitcoin）

Ⅰ．Ⅰ．スマートコントラクト

ブロックチェーンの重要な技術革新

Programmable Money（Ethereum）

「条件付き支払いルール」を
ブロックチェーン上に設置でき、
「自動的」に実行できる

∴　**Credible Commitment** が可能
（ただし支払いに関してのみ）

スマートコントラクトをブロックチェーンに設置：

「入力 A であれば、財布 X から財布 Y に 1 コイン移動」

「入力 A 以外（B）であれば、X から Y に 0 コイン移動」

その後オフチェーンからデジタル入力（A or B）：

スマートコントラクトにしたがって自動的にコイン移動

例：オフラインで X さんは Y さんから PC を 1 コインで購入する約束をする

PC が X さんに送られた場合	入力 A	→	1 コイン移動
送られなかった場合	入力 B	→	コイン移動せず

１．２．オラクル問題

オフチェーンとオンチェーンの連結性

オフチェーンから正直に入力させるにはどうしたらいいか？

解決方法：

- IOT　　オフチェーンにて連結の信ぴょう性について合意形成

- メカニズムデザイン（ゲーム理論）

  スマートコントラクトをインセンティブスキームとして設計する

  Matsushima and Noda “Mechanism Design with Blockchain Enforcement” (2020)

理論的な裏付け：Ethical Implementation Theory

標準的なメカニズムデザイン

利用者コミュニティーには利己的個人のみを仮定

配分と支払いを組み合わせれば正直入力のインセンティブを引き出せる

Abreu+Matsushima Mechanism, 1992

しかし支払いルールだけでは（つまりスマートコントラクトだけでは）

正直入力を一意均衡にすることはできない

↓

Ethical Implementation Theory

Matsushima “Epistemological Implementation of Social Choice Functions,” 2021.
Matsushima “Honest Community”, in preparation.

Ethical Implementation Theory とは

利用者コミュニティーにおいて利己的選好以外に
正直選好、敵対的選好も考慮される

Weakest Ethical Ties の仮定

“Adversarial is more likely than honest” and
“All parties are not honest”
never happen to be common knowledge.

→ **Selfish parties’ truthful reporting is the unique NE**
under some extended version of proper scoring rule.

∴ オラクル問題は、非常に弱い社会的関係資本の下でも
メカニズムデザインによって解決できる

Ⅰ．３．プライバシー

ブロックチェーン　　Public 型、Private 型、Consortium 型
Validators（取引の承認者、マイナー）全員にスマートコントラクトの中身が筒抜けである

解決方法：　　抽象的入力にする（Encryption, Mechanism Design）
∴　当事者にだけ意味がわかる
∴　取引データはオンチェーンとオフチェーンのデータの組み合わせによって生み出される

Ⅰ．４．スマートコントラクトの用途制限

不正な取引や契約にも利用されうる

スマートコントラクトからは不正か否か判別できない（∵抽象的入力）

ＰＣ　→　不正な品物（ドラッグ、マネーロンダリング）
ただしオフチェーンで足がつきやすい

ＰＣ　→　不正な行動（サボタージュ、カルテル）
オフチェーンでも足がつきにくい

∴　用途を制限しないと実社会に悪影響

∴　信頼機関（プラットホームプロバイダーなど）による
事前審査が不可欠

Ⅰ．５．デジタル法廷

裁判所の役割の一部を
自前のスマートコントラクトに代行させることができる
→　コスト大幅削減
司法コストゼロ、一期一会 OK

→　デジタル法廷の提案

Matsushima and Noda “Mechanism Design with Blockchain Enforcement” (2020)

デジタル法廷とは？

オフライン（実社会）の契約は自動化できない。
司法コストが高いため、オフラインの契約は
実質的には口約束である。そこで、

オフラインの契約の際
オフラインの契約とは別に
「オフラインの契約の違反者に罰金を科すための罰金ルール」を
スマートコントラクトとして
ブロックチェーン（オンライン）に設置しておく
∴　スマートコントラクトが裁判所の代わりになる
裁判の自動化！

Digital Courts went viral.

A digital court for a digital age

Researchers devise a way to perform legal functions with blockchain technology

Research news

Division for Strategic Public Relations | Graduate School of Economics / Faculty of Economics

April 6, 2020

In a move to save time, money and effort, economics researchers utilized existing blockchain methodologies to create what they call a digital court. This would provide enforcement of contracts wherever a traditional legal court would currently settle disputes. Examples of areas which could make use of this would be auctions, business contracts and sales. As it is based on existing technology, it could be implemented right now.

The digital court could open up commercial opportunities to those who cannot access traditional legal services. Image CC-0

Blockchain technology has great potential to impact many areas of life, commerce in particular. Put simply it is a way to ensure that information can be recorded in such a way that it cannot be manipulated afterwards. Blockchain is what is known as a distributed ledger, that is, there is no central authority, it is peer-to-peer, and its most famous application at this time is the online currency bitcoin. However, people find other uses for it.

Professors Hitoshi Matsushima from the Department of Economics at the University of Tokyo and Shunya Noda from the Vancouver School of Economics at the University of British Columbia, in Canada, have come up with a mechanism which uses blockchain to settle legal disputes without the need for an otherwise costly legal process. This is an extension to existing ideas for smart contracts which exist without central administration, but which until now have not found an application in the more general field of legal enforcement.

１．６．まとめ

ブロックチェーン、スマートコントラクト、デジタル法廷は
無限の可能性

ただし課題も山積

Proof-of-Work：グローバルコモンズの悲劇

国際協調が不可欠：

環境負荷の大きいシステム（PoW など）の制限

環境負荷の小さいシステム（PoS など）の実装支援

２．デジタル通貨の差別化

プラットホームプロバイダー（Data Intermediary）が
自前のデジタル通貨を作って
自身のプラットホーム内で独自の取引サービスを創発

貨幣の機能＋データ仲介機能
→　独自のサービスを創発
（FB, Alipay, …）

貨幣の機能： 価値尺度、取引手段、価値貯蔵

＋

データ仲介機能： Network Externalities, Algorithm, Smart Contract, Privacy, Matching, Recommendation, Prediction, Reputation Building, ICO, Finance, …

→ 独自の取引データを獲得でき自身のプラットホーム内で占有できる
cf. クレジットカードによる銀行口座決済（外部に取引データ漏洩）

→ クロスボーダーなプラットホーム間の差別化競争

→ セグメンテーション（ボーダーレスなデジタル通貨圏）
利用者は複数のプラットホーム（トークン）を自由に使い分けることができる

３．デジタル社会：
法定通貨と民間通貨の関係

中央銀行の金融政策：

アカウント型へのインフルエンスが中心
完全兌換な銀行預金が前提
No-Question-Asked（NQA）、Rigid Regulation

CBDC の導入：

「アナログ→デジタル」化の直接的メリット
CBDC（あるいは銀行預金）で貯金し、随時引き出して民間トークンを購入
→民間トークンへのインフルエンスチャネル
しかし民間サービスの代替は不可
No “NQA” Discipline

通貨独立性：　独立性は民間通貨の役割と不可分の関係にある

互換性は民間発行主体の裁量下にある：

完全不換：　Feeding America、SDG s

不完全兌換：　交換レート変動

Bitcoin, Ether, …

価値の不安定性

ステーブルコイン：　固定レート、規制なし

ワイルドキャット

総じてデータ独占のメリット（Innovation）とデメリット（Welfare distortion）あり

これらの課題解決に対し CBDC はどのような意義をもつと考えられるのか？？

以上