# AI プロジェクト報告書

## ブロックチェーンと AI の融合領域創成研究

## ～Smart Blockchain の実現と応用を目指して～

令和２年８月

東京工科大学

コンピュータサイエンス学部

研究代表者　亀田弘之

## 1. 研究目的

ブロックチェーンは、Satoshi Nakamoto の論文(2008)により提案されたものであり、その歴史はまだ浅い。このことは、東京工科大学コンピュータサイエンス学部のようなまだ歴史の浅い大学においても、世界の最先端に飛び出す可能性があることを示唆している。このような考えのもと、下記の２項目を研究目的とする研究プロジェクト「ブロックチェーンと AI の融合領域創成研究　～Smart Blockchain の実現と応用を目指して～」を立ち上げた。

本研究プロジェクトの研究目的は、以下の２つである。

1. ブロックチェーンの実装および現実の運用場面において、人工知能（AI）技術を取り込み活用し、**従来よりも格段に優れたブロックチェーン実装・運用技術を実現**する。
2. 上述のブロックチェーン技術を活用し、日本社会に受け入れられ、かつ、価値創造を支援する**友好的人工知能（Friendly AI）の実現と応用分野の開拓**を目指す。

ブロックチェーンとは、分散型ディジタル台帳システムのことであり、理論的には安全なトランザクションを提供することのできる画期的な技術である。しかしながら、中央集権的なやり方ではなく、分散管理的に処理を行うため、例えばソフトウェアにバグにより不具合が生じた場合、その不具合に対処する責任主体が存在しないなどの問題点がある。このようにブロックチェーンには魅力的な利点がある反面、実装の方法に改善の余地があること、高度に複雑な IoT システム（SoS; System of Systems）上を流通することで生じ得る種々のセキュリティ上の問題が懸念されることなど、なおも研究すべき対象は多い。

このような状況に鑑み本研究では、文献を中心とする現状分析を網羅的に行うことでこれらの諸問題を具体化・明確化することを目指すとともに、人工知能技術を積極的に導入し、**従来のブロックチェーンよりも格段に優れた Smart Blockchain 実現の基礎を築く**ことを目指した。

一方、人工知能の分野は、かつての箱庭的な世界を対象とする研究から、実世界のビッグデータをリアルタイムに扱う研究段階に入って久しい。特に近年、深層学習（Deep Learning）を中心とする革命的とまで賞される画期的技術や、それらを活用した人工知能システム Watson（IBM）などが注目されている。しかしながら、如何にこれらの学習手法や AI システムがアルゴリズム的に処理性能的に優れていようとも、そもそも入力に利用されるデータ・知識に誤りが混入あるいは改竄されていたならば、その処理結果は、たとえ正確に処理されていたとしても直ちにその意味を失うことになる。誤った知識からは有用な知識・新なる知識は得られない。

この問題点を解決するために本研究では、ブロックチェーン技術を積極的に活用し、**データや知識の信憑性・信頼性・正確性を保証する仕組みとその限界を明らかにする**とともに、Blockchain3.0 における**“smart contract”の概念を基盤とする Friendly AI の実現と応用に関する研究テーマの創出**を目指した。

## 2. 研究計画

本プロジェクトの開始時のメンバーおよび活動計画は、以下の通り。

### (1) プロジェクトメンバー

プロジェクト代表者：亀田弘之

プロジェクト分担者：竹田昌弘，田胡和哉，岩下志乃，亀井聡，布田裕一，山元進，
宇田隆哉，柴田千尋，千葉康生，山口淳，相田紗織，喜多義弘

### (2) 活動計画

**I. 平成 29 年度（初年度）の活動：**

**【調査研究】**

・12 月　立ち上げのための前準備

・1 月　キックオフ会議（調査研究の分野の選定と調査担当の割り当て）

・2 月～3 月　文献を網羅的に調査。情報処理学会(東京)や電子情報通信学会(東京)に参加し、情報収集・意見交換する。成果は要約集(第一報)としてまとめ発信する。

**II. 平成 30 年度（2 年目）の活動：**

初年度の活動を発展させるとともに、新研究領域の創成を下記の要領で目指す。

**【調査研究(継続)】**

4 月～9 月　文献調査を継続的に実施する。学会等にも参加し、より多くの情報収を収集。

**【新研究領域の創成】**

前年度に得られた成果を元に、ブロックチェーンと人工知能の**融合領域を創成**する。

9 月～3 月にかけ以下の作業を集中的に行う。

1）ブロックチェーン関連の原理、アルゴリズム、コード実装に関する調査研究結果を精査し、**人工知能が有効に適用できる部分を探求**する。

2）人工知能システムにおいて、出力に対する**入力の信憑性・信頼性・正確性の影響**を定量的・実験的に探求するとともに、入力データ・知識に対してその**出所・存在を明示的に参照・証明できる仕組み（smart contract）**を実現する方法を探求する。

III. 平成 31 年度（3 年目）の活動：

最終年度は、得られた成果を国内外に発信する。具体的には以下の通り。

4 月～12 月にかけて以下のことに取り組む。

**【成果の発表・発信】**

１）この年までの成果を取りまとめ、**公開シンポジウムを開催**する。

２）得られた成果を**国際会議にて発表**する。

３）調査研究成果をもとに格段に優れた**新規プロジェクトを立案し、研究費獲得**を目指す。

## 3. 研究成果

本プロジェクトの真の目的は、本学コンピュータサイエンス学部が 21 世紀型社会に対して、新たな価値を継続的に発信する基盤を構築することであった。その 1 つのテーマとして、ブロックチェーンを取り上げ、これを人工知能と関連付ける研究を推進した。

その結果、以下のような成果を得ることができた。

### (1) 新たなブロックチェーン研究（主として、セキュリティに焦点を当てた研究成果）

- 監視カメラデータの偽造を防ぐための**データ保護手法**（宇田）

  概要：監視カメラの不正使用を検出し、監視カメラにより録画されたデータが偽造されることのないようにするための新たな手法の提案。

- ブロックチェーン技術を用いた **DNS キャッシュポイズニング**（布田）

  概要：DNS におけるキャッシュポイズニングをブロックチェーンの分散台帳と合意形成の機能を用いて検知するシステムを提案

- スマートコントラクトを用いた**電力取引システム**（布田）

  概要：スマートコントラクトを用いて電力取引を中央の機関にコントロールされずに、個々の需要者・供給者の電力取引を安全に実現できる電力取引システムの提案。

- 監査機能付匿名送金における監査者による**情報漏洩の被害軽減**（布田）

  概要：送受金の匿名性を高めた Zcash に対し、送受金に問題が発生した場合の対策として監査者による監査機能を導入する方式があるが、監査者に送受金の秘密情報が集中してしまう課題がある。その課題に対し、監査者を複数選定して、秘密情報を分散させる仕組みを追加した方式を提案。

- ProVerif を用いた CT 及び**ブロックチェーンの形式化**（布田）

  概要：ブロックチェーンの仕組みに関する計算機を用いた形式検証手法に関するもの。ブロックチェーンの木構造を、形式検証ツール ProVerif で形式化する方法を提案。

- ブロックチェーンを用いた **AI 推論信憑性維持・管理システム**（亀田）

  概要：来るべき AI を前提とする超スマート社会(Society5.0)へ向けて、AI 推論信憑性維持・管理システムの提案・考察を行うとともに、今後の方針について提案。

**(2) 授業改善への貢献**

- 大学院授業改善（布田）

  講義「情報セキュリティ応用」にて、ブロックチェーンの仕組みを解説

- 新たな卒業研究テーマの立ち上げ（細野）

  研究室において、ブロックチェーン技術を活用する研究テーマ「トラスト・ビルディング」を立ち上げ、3 人の学生が下記の卒業課題に取り組み中。なお、学生 3 名中内 2 名は本学大学院に進学予定（大学院入試受験済み）。

  1. 機器信用ネットワークの開発
  2. データ信用フレームワークの開発
  3. アイデンティティ信用プロトコルの開発

## 4. 今後に向けた提言など

**(1)振り返り**

本研究プロジェクトは、新規分野に教員の力を集約し一気に世界のトップに躍り出ることを目論んでいたものであるが、プロジェクト立ち上げ当時、学内には実践的教育プログラムや人工知能系の研究プロジェクトが同時多発的に立ち上がっていたため、教員の研究・教育のロードバランスを保つのが極めて困難であった。今後は、各教員の教育・研究の実態に合ったプロジェクトを立ち上げることで、より多くの優れた成果が得られると期待される。本研究プロジェクトにおいても、このような状況下でありながら、研究成果あるいは付録を一瞥すればわかるように、次へ向けての準備が確実にできている。このことは大いに評価されるべきものと考える。

**(2)提案**

【提案1】 現在、ブロックチェーンの研究分野では、実証実験を経て実用化へ向かって進んでいる。FinTech や電力供給の分野ではとりわけ関心が高いことを考えるならば、この分野へより多くの学生を送り込むための教育・研究体制を整える検討を早急にすべきであろう。

【提案2】 また、ブロックチェーンは、IoT(Internet of Things)に基づくビッグデータ、ビッグデータを背景とする人工知能（深層学習）などと密接に関わり合っている。本学コンピュータサイエンス学部は、その動向を先読みし、先進情報専攻と人工知能専攻とを立ち上げた。これは時宜にかなった正しい判断であったので、今後はこの両専攻が相互に刺激を与えながら発展していくための戦力を考える必要があると思われる。特に、これらの分野は進歩・変化が極

めて早いので、その動向を継続的に見極め、教育・研究を推進することが求められる。

【提案3】 本研究プロジェクトの成果・知見を基に、スマートキャンパス計画や八王子市を対象とするスマートシティ計画を立案・実施することも有効であろう。強く提案したい。

### (3)謝辞

最後に、本研究プロジェクトを支援してくださった軽部前学長に謝意を表するとともに、惜しみない協力をしてくださった学内外の関係者、とりわけ研究分担者の先生方には大いに感謝したい。

## 付録（論文発表、活動成果等）

### 学会発表

[1] Ryuya Uda, Data Protection Method with Blockchain against Fabrication of Video by Surveillance Cameras, Proc. Of The 2nd International Conference on Blockchain Technology, pp.29-33, 2020（ https://doi.org/10.1145/3390566.3391685 ）.

[2] 高橋幸宏, 布田裕一, 岡崎裕之, 鈴木彦文, ″ブロックチェーン技術を用いたDNS キャッシュポイズニング対策の検討″, 電子情報通信学会, 信学技報,ISEC2019-78, 107-112, 2019.

[3] 高橋幸宏, 布田裕一, 岡崎裕之, 鈴木彦文,″協調型DNSによるキャッシュポイズニングの検知″,暗号と情報セキュリティシンポジウム(SCIS) 2020, 4F2-3, 2020.

[4] 田付 洋大, 布田 裕一, 喜多 義弘, ″スマートコントラクトを用いた電力取引システム″, 電子情報通信学会, 信学技報, NS2019-161, 1-6, 2020.

[5] 金子 なのは, ″監査機能付匿名送金における監査者による情報漏洩の被害軽減″, 東京工科大学コンピュータサイエンス学部卒業論文, 2019.

[6] 荒井 研一, 岡崎 裕之, 布田 裕一, ″ProVerifを用いたCT及びブロックチェーンの形式化″, 暗号と情報セキュリティシンポジウム(SCIS) 2019, 4D2-2, 2019年1月.

[7] 亀田弘之, 相田紗織, ”ブロックチェーンを用いた AI 推論信憑性維持・管理システムの提案 － 人工知能活用社会へ向けての提言－,” 電子情報学会,ソサイエティ大会講演論文集, A-11-1, 2017

[8] 亀田弘之, ”Blockchain-based Artificial Intelligence Society,” 招待講演(武漢地質大学)、2018.

### 受賞

[1] サイバーセキュリティシンポジウム道後2020学生研究賞, 2020年2月. 学会発表[3]に対して受賞（ https://www.teu.ac.jp/information/2020.html?id=80 ）。