

経済産業省委託調査事業

平成 30 年度産業技術調査事業

(国内外の人材流動化促進や研究成果の信頼性確保等に向けた大学・研究機関へのブロックチェーン技術の適用及びその標準獲得に関する調査)

報告書

平成 31 年 3 月

株式会社リクルート R&D

目次

1. はじめに.....	4
1.1. 実施概要.....	8
2. 用語集.....	10
3. 「学位・履修履歴証明」及び「研究データの信頼性確保」の現状.....	13
3.1. 「学位・履修履歴証明」テーマ.....	13
3.1.1. 学位や成績証明の管理における現在の規定.....	13
3.1.2. 既存技術の例.....	13
3.2. 「研究データの信頼性確保」テーマ.....	14
3.2.1. 既存技術の例.....	14
4. ブロックチェーン技術について.....	16
4.1. ブロックチェーン技術の特徴.....	16
4.2. ブロックチェーン技術適用の必然性の議論.....	17
4.2.1. 継続的なシステム運営に関する議論.....	17
4.2.2. データの真正性確保に関する議論.....	17
4.2.3. ブロックチェーンの永続性、移行に関する議論.....	17
4.2.4. データの登録、公開に関する議論.....	18
4.2.5. システム要件以外の点に関する議論.....	18
5. ブロックチェーン技術の活用例.....	19
5.1. 基本的な考え方.....	19
5.2. 「学位・履修履歴証明」テーマ.....	19
5.2.1. 基本概要.....	19
5.2.2. 適用案の例.....	20
5.3. 「研究データの信頼性確保」テーマ.....	22
5.3.1. 基本概要.....	22
5.3.2. 適用案の例.....	23
6. 標準化に関して.....	26
6.1. 標準化団体によるブロックチェーン技術における標準化の流れ.....	26
6.1.1. IEEE.....	26
6.1.2. IETF.....	27
6.1.3. ISO.....	27
6.1.4. ITU.....	28
6.1.5. W3C.....	28
6.2. ブロックチェーンプロトコル独自の標準化プロセス.....	28
6.2.1. EIP: Ethereum Improvement Proposal プロセス.....	29
6.2.2. EIP と BIP の例.....	31

7. 国際動向調査	32
7.1. 「学位・履修履歴証明」テーマ	32
7.1.1. 背景	32
7.1.2. 事例①「Blockcerts」	33
7.1.3. 事例②「University of Nicosia」	40
7.1.4. 事例③「Gradbase」	43
7.1.5. 事例④「University of Birmingham」	46
7.1.6. 事例⑤「Open University」	52
7.1.7. 事例⑥「uPort」	55
7.1.8. 事例⑦「e-scroll」	58
7.1.9. 総括	60
7.2. 「研究データの信頼性確保」テーマ	61
7.2.1. 背景	61
7.2.2. 事例①「Lyfescience」	62
7.2.3. 事例②「TrialChain」	68
7.2.4. 事例③「Enigma」	72
7.2.5. 事例④「Blockchain for Science」	75
7.2.6. 事例⑤「Data Management Hub」	78
7.2.7. 事例⑥「Dat」	79
7.2.8. 総括	80
8. ハッカソン開催	82
8.1. ハッカソン開催の目的	82
8.2. ハッカソン開催概要	82
8.2.1. 利用可能なブロックチェーンの選定について	82
8.2.2. 参加規約における工夫	83
8.2.3. スケジュール	83
8.2.4. ハッカソンに参加する関係者	84
8.2.5. 広報	85
8.3. 審査について	89
8.3.1. 基本方針	89
8.3.2. 審査方法	89
8.3.3. 審査基準	90
8.3.4. 審査表	91
8.3.5. 審査員	92
8.4. ワークショップの内容	93
8.4.1. ハッカソンテーマ関連ワークショップ	93
8.4.2. ブロックチェーン技術関連ワークショップ	95
8.5. 各参加チームの成果物	97
8.5.1. 「学位・履修履歴証明」テーマ	97

8.5.2. 「研究データの信頼性確保」テーマ.....	104
8.6. ハッカソン結果.....	110
8.7. アンケート結果の取りまとめ.....	112
8.7.1. 総合結果.....	112
8.7.2. 人材獲得における課題の分析.....	113
8.7.3. その他の意見.....	114
9. 総論.....	116
9.1. ブロックチェーン技術の実社会への適用について.....	116
9.2. 標準化について.....	117
9.3. 今後の取組における考察.....	118

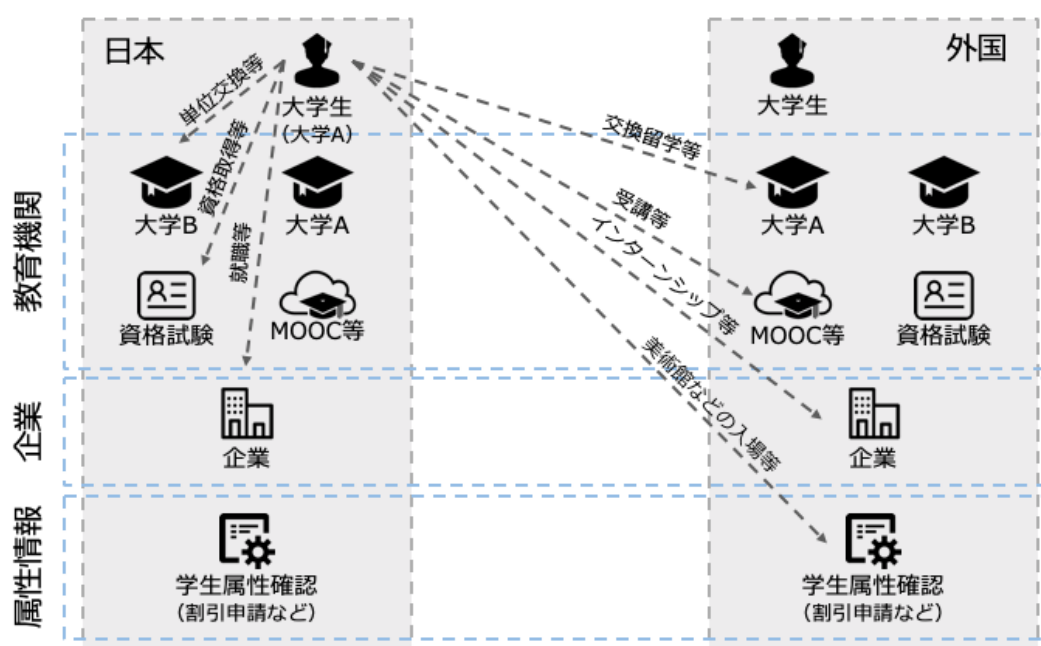
1. はじめに

～人材流動化や研究開発の現場における信頼ある基盤の構築を目指して～

現在、国際的な人材流動化を背景に、多様な学位・学修履歴や職歴等を有する諸外国からの留学生等が我が国の大学や企業等に出願・就労する機会や、我が国で発行された学位・学修履歴等を他国の大学や企業等から評価される機会が増加している。また、これに加えて次に掲げるような環境変化もあり、個人の属性を自己申告に頼る現状のみでは、これら属性情報を使用する側・使用される側ともに正當に活用することが今後困難となる恐れがある。

(1) 多様な学修形態の出現

単一の大学での座学形式の学修形態に加え、大学間の単位互換や交換留学、MOOC 等をはじめとするオンライン教育等多様な学修形態が出現。



図表 1 - 1 国内外における様々な学修や就労の機会が増え、学位・履修履歴の共有場面が増加¹

(2) 多様な就労文化及び就労形態の出現

情報通信分野をはじめとした技術革新等を背景として、産業構造が劇的に変化。これに伴い、転職や副業・兼業といった多様な働き方が普及。また、スタートアップへの就労やフリーランサー等、多様なキャリアパスが社会的に認知されてきている。

¹ 株式会社リクルート R&D 作成

(3) 海外の大学との合同交流プログラムの設置

例えば、文部科学省は欧州委員会教育文化総局と共同で、将来世代の人的交流の重要性を踏まえ、新たな学生交流プログラムを2018年7月に発表し、国を超えた交流を推進している²。

(4) 大学の統廃合における学位・学修履歴の管理

2018年生まれた子供たちが大学を卒業する2040年の大学進学者数は約51万人と、2017年と比較すると約12万人減少すると推定される。このことも鑑みて、文部科学省では、大学における教育・研究の質の保証の観点から大学の再編・統廃合に向けた検討が行われている³。具体的には、今後国公私の枠を超えた連携・統合に向け、「大学等連携推進法人（仮称）」の制度整備に向けた検討が求められている⁴。

(5) 大学内外の様々なコースやプログラムの修了証の信頼性の確保

大学内においても学部学科名の変更や統廃合、様々なコース・プログラム等が改廃されている。JMOC（日本オープンオンライン教育推進協議会※国内の大学における講義を配信、修了証を発行）のホームページ上で配信される講座の学習者数は50万以上に上る⁵。

また、我が国の研究機関や企業におけるデータ不正は年々増加傾向にあり、サイエンス誌によれば⁶、撤回論文が多い研究者上位10名のうち半数の5名が日本人となっている。これに加え、日本企業においてもデータ不正が現在頻発しており、学术界・産業界双方において、研究データの信頼性の確保は重要な課題となってしまっている。この状況を放置すれば、「Made in Japan」のブランド力が低下し、日本製だから安全・安心という仮説も成り立たなくなる恐れもある。

² 第1回日EU教育・文化・スポーツ政策対話の開催について（文科省）：http://www.mext.go.jp/b_menu/houdou/30/07/1406889.htm

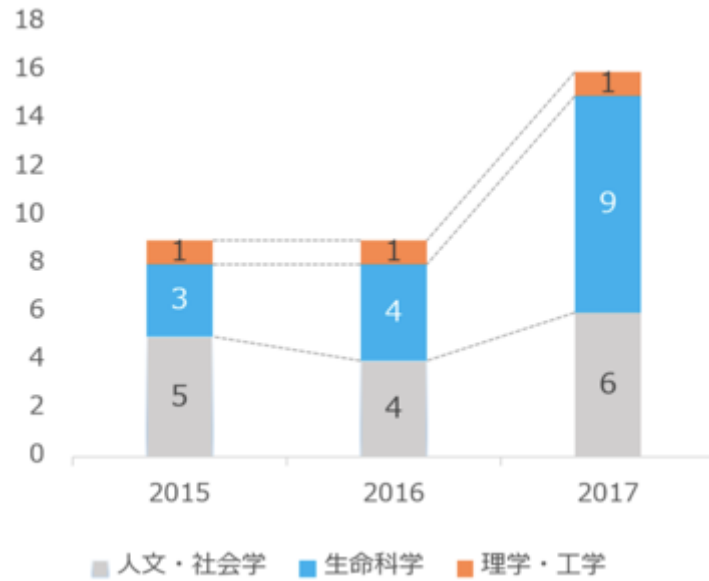
³ 大学への進学者数の将来推計について（文科省）：

http://www.mext.go.jp/b_menu/shingi/chukyo/chukyo4/042/siryo/_icsFiles/fieldfile/2018/03/08/1401754_03.pdf

⁴ 文科省の中教審・将来構想部会：http://www.mext.go.jp/b_menu/shingi/chukyo/chukyo4/siryo/1409589.htm

⁵ JMOC：<https://www.jmoc.jp/>

⁶ Researcher at the center of an epic fraud remains an enigma to those who exposed him：<https://www.sciencemag.org/news/2018/08/researcher-center-epic-fraud-remains-enigma-those-who-exposed-him>



図表 1 - 2 大学等の研究活動における不正⁷

企業名	概要
住友重機械工業株式会社	定期検査報告書において実際の検査結果と異なる内容の記載等の不適切行為 (2019年)
KYB株式会社	建築物用免震・制振用オイルダンパー検査工程における性能検査記録データの改ざん (2018年)
株式会社 TATERU	従業員が顧客から提供を受けた預金残高データを改ざんし、融資審査を通りやすくしていた等の不祥事 (2018年)
株式会社クボタ	鋼板等の生産設備で使用する消耗部品 (圧延用ロール) の検査成績書に実際の検査結果と異なる数値を記載するなどの不適切行為 (2018年)
日立化成株式会社	産業用鉛蓄電池の一部製品の検査成績書に不適切な数値の記載を行っていた等の不適切行為 (2018年)
三菱マテリアル株式会社	連結子会社である三菱電線工業株式会社、三菱伸銅株式会社におけるシール材の寸法、物性等の検査記録データの書き換え等の不適切行為 (2017年)

図表 1 - 3 企業におけるデータ不正⁸

このような中、透明性や耐改ざん性を確保しつつ、分散的にデータを持ち合う技術としてブロックチェーン技術が注目されている。当該技術については、スケーラビリティ等の課題があることを踏まえば未だ発展途上ではあるものの、各国でもその技術の適用可能性に向けた実証実験が進展中である。我が国においても、仮想通貨取引市場の活発化等と相まって、金融機関を中心にブロックチェーン技術の適用等に向けた研究開発や技術実証等の動きが活発化しており、国際競争力の観点からも、

⁷ 文部科学省公表事例に基づき経済産業省が集計。上記には、ねつ造、改ざんのほか、盗用による研究不正も含まれる。

⁸ Sustaina 企業不祥事・不正問題 検索：<https://www.sustaina.org/ja/scandals/?ScandalSearch>

我が国において当該技術を着実に育成し、標準化の取組やその普及へと確実に結び付けていく必要がある。

本調査では、上述の背景も踏まえ、「学位・履修履歴証明」及び「研究データの信頼性の確保」の2テーマにおいて、ブロックチェーン技術が既存技術と比べ技術的及び経済的優位性を保ちつつ適用される可能性及び国際的な標準化の取組等について勉強会において検討を深めていくとともに、両テーマに関し、文献等からブロックチェーン技術の適用に関する国際動向及び海外事例を調査する。また、ハッカソン開催を通じて、両テーマにおいて著しく変貌する国内外の社会環境に対応するための具体的かつ包括的な対応策について民間の知恵を活用して洗い出すとともに、実際の社会実装へとつなげていくことを目的とする。

1.1. 実施概要

合計4回の勉強会やハッカソンの開催、そして国際動向調査を通じて本調査を実施する。

勉強会の委員を「図表 1.1 - 1」に示す。

区分	氏名	所属
座長	楠正憲	Japan Digital Design 株式会社 CTO 政府 CIO 補佐官
委員	坂下哲也	JIPDEC (一般財団法人 日本情報経済社会推進協会) 常務理事 (担当: 電子情報利活用研究部認定個人情報保護団体事務局)
委員	砂原秀樹	慶應義塾大学大学院メディアデザイン研究科教授 /先導研究センター内サイバーセキュリティ研究センター センター長
委員	中村素典	NII (国立情報学研究所) 学術認証推進室 教授
委員	崎村夏彦	野村総合研究所 上席研究員
委員	岸上順一	室蘭工業大学 教授
委員	千葉吉輝	UMIN (大学病院医療情報ネットワーク) 研究センター所属 Japan CDISC Coordinating Committee (J3C) Vice Chair
委員	河合健	アンダーソン・毛利・友常法律事務所パートナー弁護士
委員	中山好彦	株式会社リクルートキャリア ビジネスディベロップメントスペシャリスト

※ 順不同・敬称略

事務局アドバイザー: 株式会社レピダム フェロー兼 OpenID ファウンデーション ジャパン理事の林達也

図表 1.1 - 1 勉強会の委員一覧

勉強会の実施概要を「図表 1.1 - 2」に示す。

回数	日程	場所	議題
第1回	2018年10月12日(金) 午後2時~4時	リクルート本社 (41F セミナールーム)	JIPDEC の推進する ISO TC307 の活動のご説明及び主に「学位・履修履歴証明」テーマにおける議論
第2回	2018年11月16日(金) 午前9時~11時	リクルート本社 (40F 会議室 OAK)	主に「研究データの信頼性確保」テーマにおける議論
第3回	2018年12月21日(金) 午前9時~11時	リクルート本社 (40F 会議室 OAK)	両テーマにおける議論及びハッカソン開催について議論
第4回	2019年3月1日(金) 午後2時~4時	リクルート本社 (40F 会議室 OAK)	ハッカソン及び勉強会の振り返り

図表 1.1 - 2 勉強会の実施概要

ハッカソンの開催概要を「図表 1.1 - 3」に示す

ブロックチェーンハッカソン 2019	
日時	2019年2月9日（土）、2月16日（土）～17日（日） ※ プロトタイプ制作の時間を確保するため、2月9日に開会式及びワークショップ、2月17日に審査・表彰と2週にまたがって実施
場所	Lifull Hub 東京都千代田区麹町 1-4-4
想定参加人数	参加者 70 人やサポート企業、審査員、運営及びその他の関係者
参加料	無料、但し参加条件について制限あり
プログラム内容	(1) テーマにそったアイデア出し及びプロトタイプ制作・発表 (2) サポート企業や団体によるワークショップ

図表 1.1 - 3 ハッカソン開催の概要

2. 用語集

「学位・履修履歴証明」及び「研究データの信頼性確保」へのブロックチェーン技術の適用可能性を整理する上でこの報告書内で用いる用語について「図表 2. 1-1」にまとめる。

用語	説明
IPFS	P2P ネットワーク上で動作する分散型のファイル管理システムのこと。HTTP を補完ないし代替するプロトコルとして開発が進められている。
ウォレット (wallet)	トランザクションを発行する際に利用される秘密鍵を管理する機能、アプリケーション。
オフチェーン	<p>ブロックチェーンと連携する実装、技術、仕組みの総称。オフチェーンに対して、ブロックチェーン自体の実装、技術、仕組みことをオンチェーンと呼ぶこともある。</p> <p>例えば、中央集権的に運営される仮想通貨取引所においては、一つ一つの仮想通貨の取引をブロックチェーンに書き込むのではなく、取引所内で管理されているブロックチェーンではないデータベースに登録されていることがあり、オフチェーンで管理していると言える。</p> <p>また、ブロックチェーンの機能向上等のために、ブロックチェーンと連携する別のネットワーク実装等を 2nd layer などと呼ぶこともあり、これもまたオフチェーンの例として取り上げられる。</p>
Open Badges	スキルと実績に関するメタデータが埋め込まれた検証可能なポータブルデジタルバッジである。これらは Open Badges Specification に準拠している。
OP_RETURN	ビットコイン上にビットコインの支払いとは無関係なデータを登録するために用意された演算子。
機械語	CPU が直接理解、実行できる言語のこと。0 と 1 の羅列で表現される。
クレデンシャル	主にセキュリティの分野で用いられる語で、ID やパスワードをはじめとする、ユーザの認証に用いられる情報の総称。
公開鍵	公開鍵暗号で利用される鍵のひとつ。 ビットコイン等、様々なブロックチェーンプロトコルにおいて、アドレスを導出するための元となる値として利用される。
コンセンサスアルゴリズム	ブロックチェーンを構成する各ノード間で行われる合意形成の方法のこと。具体例として、プルーフオブワーク (PoW) やプルーフオブステーク (PoS) 等があげられる。
真正性	利用者、プロセス、システム、情報等が本物であることを確実にするということ。
スマートコントラクト	ブロックチェーン上に登録されたプログラム。
solidity	Ethereum で利用されるスマートコントラクトを記述するためのプログラム言語。

ライフサイクル	データや証明書等の、発生から、活用、蓄積、保管、廃棄までの一連の流れ。
トランザクション	取引を実行したことを示すこと。 例えばビットコインであれば、ビットコインの所有者が他の人にビットコインを送ったと認めたことをビットコインネットワークに示すこと。
トランザクション手数料	マイナーに対して支払う、トランザクションを発行するための手数料。
ノード	ここではブロックチェーンを管理するために必要なコンピュータのこと。
ハッシュ関数	あるデータからハッシュ値を生成するための関数のこと。ハッシュ関数によってハッシュ化された値のことをハッシュ値という。ハッシュ化と暗号化は異なる点に注意。
ハッシュ値	ハッシュ関数から生成される暗号化や誤り・改ざん検出等に用いられる、あるデータからそのデータを要約する数列。
PtoP (P2P)	Point to Point の略。サーバやデータベースが存在せず、ネットワーク上で各コンピュータ同士が直接通信する形式の通信方法のこと。
プルーフオブワーク (PoW)	不特定多数の管理者が存在する状況下における合意形成（コンセンサス）の仕組み（コンセンサスアルゴリズム）のひとつ。
フルノード	全てのトランザクションデータを保有しているノードのこと。
プロトコル	一定の規格・ルール・手順のこと。プロトコルに従って計算処理を実行する、等のように用いられる。
マイナー	マイニングを実施するプレーヤー。
マイニング	トランザクションを検証し、ブロックに格納するために必要な計算作業のこと。例えばコンセンサスアルゴリズムとして PoW を導入しているビットコインであれば、マイニングに成功すると、報酬としてビットコインを受け取ることができる。
マークルツリー (Merkle Tree)	二分ハッシュ木とも呼ばれ、大規模データを効率的に要約し検証できるようにするデータ構造のひとつ。このデータ構造は木構造の一種であり、再帰的に一番下の葉ノードのペアから一つのハッシュ値を計算し、ハッシュ値が一つだけ残るまで続けて計算を実施する。
マークルルート (Merkle root)	マークルツリーにおいて、ハッシュ値計算を実施した最後に残るハッシュ値。
マークルパス (Merkle path)	特定の葉ノードからマークルルートまでどのようなルートでたどり着くかの情報。
マスターノード	各ノードを管理するための役割を担う親ノード。プライベート型のブロックチェーンの場合に必要なことが多い。
マルチシグネチャ、マルチシグ	トランザクションを発行するために必要な署名を複数人必要とするスキーム。
メタデータ	あるデータに付加されている、そのデータに関連した情報（データ）。

フォーク	ブロックチェーンの仕様を修正する際等に、古い仕様のままブロックが生成されて、新しい仕様のブロックの生成と並行して発生する分岐のこと。さらに、新しいブロックと古いブロックの間の互換性の種類によってソフトフォークとハードフォークに分類される。
ビットコインアドレス	ビットコインの受取人として様々な共有される鍵の識別子。
秘密鍵	公開鍵暗号で利用される鍵のひとつ。 ビットコイン等、様々なブロックチェーンプロトコルにおいて、トランザクションを発行する際に利用される。
ローカル	各人の所有するコンピュータのこと。ローカル上にデータを保存する、等のように使われる。
ワールドステート	Hyperledger を活用してトランザクションを管理するための格納庫のこと。ワールドステートは Hyperledger の重要な特徴。データを「キー」と「値（キーバリュー）」と呼ばれる形で保存し、現在の状態を容易に取得できるようにしている。ワールドステートを保存しているものは「キーバリューストア」と呼ばれる。

図表 2 - 1 用語集

3. 「学位・履修履歴証明」及び「研究データの信頼性確保」の現状

3.1. 「学位・履修履歴証明」テーマ

3.1.1. 学位や成績証明の管理における現在の規定

(1) 学位や成績証明に記載すべき事項

学校教育法及び関係政省令に具体的に記載すべき事項は定められていない。

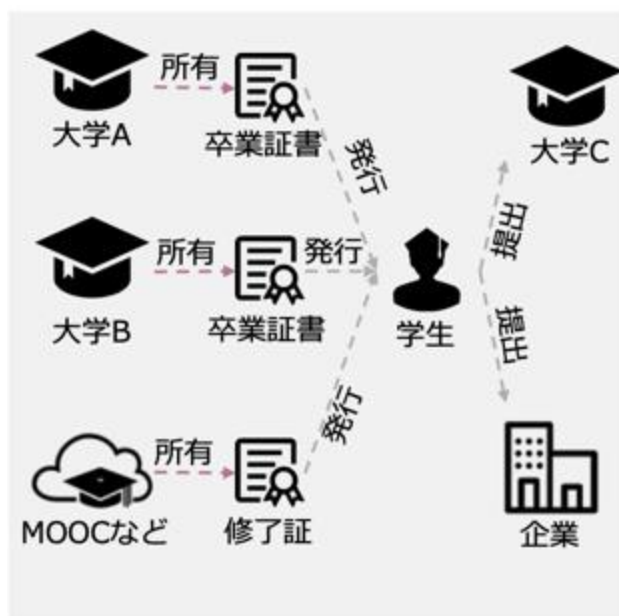
(2) 学位や成績証明の保存期間及び保存の形態

学校教育法施行規則（文部省令第11号）第28条第2項によると、卒業等の学籍に関する記録の保存期間は20年とされている。また、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（e-文書法）第3条、及び行政手続等における情報通信の技術の利用に関する法律第6条により、その保存形態は必ずしも書面による必要はなく電磁的記録でも可能となっている。また、これらの法令に定められている電磁的記録による保存方法はブロックチェーンによる記録を排除するものではないと考えられる。

3.1.2. 既存技術の例

(1) 大学等、学位や履修履歴の発行機関がデータを管理する例

データは発行機関のデータベースに保存されていて、個人は必要に応じて発行機関に問い合わせることで引き出すことができる。異なるデータ規格を共有する際にはデータの成形が必要になる。



図表 3.1 - 1 大学等の学位や履修履歴の発行機関がデータを管理⁹

⁹ 株式会社リクルートR&D作成

(2) 第三者機関によるデータの管理

高大接続ポータルサイト「JAPAN e-Portfolio」等、第三者機関によるデータの管理も実現されている。「JAPAN e-Portfolio」とは、文部科学省大学入学者選抜改革推進委託事業（主体性等分野）で構築・運営する、高校eポートフォリオ、大学出願ポータルサイトである。高校生は学校の授業や行事部活動等での学びや自身で取得した資格・検定、学校以外の活動成果をeポートフォリオとして記録し、将来的にはこのデータを大学入試時に利用することが可能である。



図表 3.1 - 2 eポートフォリオの仕組み¹⁰

(3) eLearning の修了証発行

現在、米国の主なグローバルMOOCプラットフォームであるCourseraやedX、Udacityはそれぞれ修了証を発行しているが、その形式等が異なり統一されていない¹¹。例えば、Udacityは「Nanodegree」というコンセプトを取り入れている反面、edXは無料のコースにお金を払わせることでCertificateの取得を可能とする形を取っている。また、そのプロバイダがなくなった場合の修了証の管理等については具体的な対策が定まっておらず、考える必要がある。

3.2. 「研究データの信頼性確保」テーマ

3.2.1. 既存技術の例

研究において一般的にかつ伝統的に利用されている研究活動の記録方法は、研究ノートを利用した方法である。研究ノートのページを破損、追加すると後に検出がある程度可能である。またソフトウェアプログラムのソースコードの履歴管理・変更を追跡するツールとしてGit等が存在しており、ソフトウェア開発だけではなく、他の用途にも転用されている。その他に、東京大学のUMIN（大学病

¹⁰ eポートフォリオの仕組み：<http://oraclemag.mobileclip.jp/entry/1693093>

¹¹ 文部科学省の「MOOC等を活用した教育改善に関する調査研究」：http://www.mext.go.jp/a_menu/koutou/itaku/_icsFiles/afieldfile/2015/08/14/1357548_02.pdf

院医療情報ネットワーク, University hosted Medical Information Network) や国立情報学研究所のRCOS (NII オープンサイエンス基盤研究センター) 等が研究データ管理基盤を提供している。

(1) UMIN

医療研究の国際標準化団体である CDISC (Clinical Data Interchange Standards Consortium) 基準に基づいたサービスを展開し、研究データの整合性確保による信頼性確保やデータの2次利用を促進。但し、データの真正性そのものを担保するものではない¹²。

- UMIN-INDICE (UMIN インターネット医学研究データセンター) : UMIN のサーバ及びデータ収集用ソフトを提供するサービスで、約 230 研究プロジェクト、累積病例登録数は約 560 万例に登る
- UMIN-CTR (UMIN 臨床試験登録) : 臨床試験登録サイトであり、研究費補助等で、厚生労働科学研究補助金のうちの介入を伴う臨床研究は、当サイトにおける臨床試験のデータ及び更新履歴の登録が義務付けられている
- UMIN-ICDR (UMIN 病例データレポジトリ) : 上記の CTR の追加機能として研究者が自身の実施した臨床研究症例の匿名化したオリジナルのデータセットを、研究者自身の同意のもとに UMIN サーバに保管・するもので、データ改ざん等を困難にし、研究におけるデータの整合性を確保している

(2) RCOS

学術論文や研究データが学术界及び社会で広く共有され、研究活動がオープンに実施されることを目指したスキームである。2019 年 3 月現在構築中の研究データ基盤 (下図) はデータ管理基盤、データ公開基盤、そしてデータ検索基盤の3つの軸を中心に設計されている¹³。



¹² 大学病院医療情報ネットワーク <http://www.umin.ac.jp/>

¹³ 国立情報学研究所オープンサイエンス基盤研究センター <https://rcos.nii.ac.jp/>

図表 3.2 - 1 国立情報学研究所オープンサイエンス基盤研究センターの構成¹⁴

4. ブロックチェーン技術について

4.1. ブロックチェーン技術の特徴

ブロックチェーン、特にパブリックブロックチェーン技術には、データの透明性の向上、中央管理者を必ずしも必要としない構造、データのトレーサビリティの確保、データの対改ざん性の向上、そして適用例によってはコストの削減の可能性がある等の利点がある。反面、発展途上の技術であり、秘密鍵の管理等、システム開発・運用に関する検討がまだ十分にされておらず、適用例によっては法律の整備が行われていない。

また、ブロックチェーン技術には、以下のような類型があり、システム構築時には、どのネットワークを採択するかを考える必要がある。

	パブリック型 (新しいネットワーク)	パブリック型 (既存のネットワーク)	コンソーシアム・プライベート型
基本概要	-パブリック型のオープンなブロックチェーンネットワークで、基本、誰もが自由に参加できる	-新たにネットワークを構築せず、Bitcoinといった既存のパブリック型ブロックチェーンネットワークを活用（例：MITのBlockcerts）	- ネットワークの参加者を選定し、書込みや読込み権限をコントロールできるネットワーク
メリット	-ネットワーク設計における柔軟性が高い - 参加者へのインセンティブ設計等を自由に設計することが可能	- 新規にネットワークを作る必要がないのでシステムの導入が容易	-ネットワークの参加者及び各参加者の権限のコントロールが可能 - 未許可の参加者が存在せず、参加者の数が限られているのでネットワークの変更が比較的容易
デメリット	-新たにネットワークを構築する必要があり、多くの技術面及び運用面におけるハードルを越える必要がある - 参加者の数が十分確保できないと、ネットワークとしての機能を失くなる可能性が存在する	-基盤となるネットワークに対するコントロールがほぼ不可能であり、ハードフォーク等ネットワークにおける大規模な変更がある場合には影響が生じ得る	-新たにパブリックネットワークを構成する時と同様、新たにネットワークを構築する必要があり、多数の技術面及び運用面におけるハードルを越える必要がある - インセンティブ設計が難しく、中央集権的なシステムとの間で優位性の比較を徹底させる必要がある

図表 4.1 - 1 ネットワーク構成の比較

¹⁴ 日本の研究データ基盤の構築：http://rcos.nii.ac.jp/item/2017/1215/AXIES2017_FE2.pdf

4.2. ブロックチェーン技術適用の必然性の議論

ブロックチェーンの性質の1つである「耐改ざん性」は、既存の他の技術でもある程度対応が可能である。例えば変更履歴を管理しているという点では、前後関係の整合性が確認できる Git 等でも耐改ざん性は保証される。つまり、耐改ざん性を持つ、トレーサビリティの確保が可能といった単純な理由でブロックチェーン技術の導入を決定するのではなく、実現するシステムの要件を決定後、その要件に適合する技術としてブロックチェーンが適切かどうかを考察する必要がある。そして実際にブロックチェーンを導入する際も、既存技術では存在しなかった以下のような考察すべき事項が存在するため、留意する必要がある。

4.2.1. 継続的なシステム運営に関する議論

既存のクラウドサービスであれば、サービス事業者自身がサービスを継続している限りスキームは維持し続けられるが、ブロックチェーンでは、多数のプレーヤーがノードを運営している前提で耐改ざん性等期待される効力を発する為、管理するプレーヤーが少なくなると持続が困難となる可能性がある。また、特権的なノードを持たない完全な非中央集権的なモデルの場合、膨大な計算力を持つコンピューター（ノード等）によるネットワークの乗っ取り防止策にも考慮する必要があると考えられる。

4.2.2. データの真正性確保に関する議論

プレーヤーの数を十分に確保する等、耐改ざん性が確保できるようになったとしても、ブロックチェーン技術は分散台帳にすでに格納されているデータにおいてのみ真正性を確保するものであり、登録するデータ自体の真正性を担保するものではない。一部の領域においては、計測器の IoT 化等により、生データを生成している箇所でデータを登録することにより真正性を確保することは可能と考えられるが、ブロックチェーン技術を用いてどの段階のデータの真正性を確保したいのかという点は慎重に検討を行う必要がある。

4.2.3. ブロックチェーンの永続性、移行に関する議論

ブロックチェーン技術自体はまだ歴史が浅く、その永続性に確信が持てる状況とは言えないため、チェーンの移行やアルゴリズムの移行に関する議論が必要である。このような議論を踏まえた上で、ブロックチェーン技術が長期的な運用が求められる研究データ基盤や学位・経歴データ基盤において、最も適切なプラットフォームかという議論は続けなければならない。現状においては、フォークを実施することでシステムのアップデートを行うためノード間の合意が必要になる。ノード間の合意が取れない場合、フォーク時に分裂騒動となり、システム全体の信頼性に影響を及ぼしている事案が見られるため、より安定的な移行方法について議論が必要である。

4.2.4. データの登録、公開に関する議論

ブロックチェーン技術を基にしたデータ基盤の構築において、データを透明性の高いパブリックネットワークに載せる場合、プライバシーの保護を視野に入れて設計をする必要がある。例えば、最初は限られた人々しかアクセスを持たないところに格納し、後から匿名加工したうえでパブリックネットワークに載せる仕組みを取り入れる等の工夫が不可欠になると考えられる。

4.2.5. システム要件以外の点に関する議論

システム要件以外（インセンティブ設計等）について検討する際には、ビットコインの事例が参考になると考えられる。具体的には、ビットコインではブロックの生成コストと検証コストの圧倒的非対称性によりマイナーに攻撃インセンティブを与えず、マイニング報酬により正しい振る舞いを行うことにインセンティブを与えている。このような IT システム外のシステムに影響を及ぼす設計こそ、ビットコインを特異にしていると考えられ、実際に通貨が存在しないブロックチェーンにおいても、システム要件以外の点に着目して議論する必要がある。

例えばブロックチェーンを利用して非中央集権のモデルにした場合には、「特定のプレーヤーがデータを独占するようなことがない」「スマートコントラクトにより特定プレーヤーによる恣意的なロジックの改ざんが困難である」という特徴を利用することで、従来は特定のプレーヤーに権限が集中せざるを得ないため実現が不可能であった業界統合的なプロジェクトの実現に対して心理的なハードルを下げる可能性があるのではないかと考えられる。

5. ブロックチェーン技術の活用例

5.1. 基本的な考え方

「学位・履修履歴証明」及び「研究データの信頼性の確保」は、それぞれ性質が異なるデータを扱っており、考慮する必要のあるポイントも異なるため、各テーマ個別に考察する必要がある。例えば、学位・履修履歴データにおいては、登録するデータ自体は学校や企業といった発行組織から組織的な検証を経た上でその担保のもとに発行されるのに対して、研究データにおいては、組織的な検証を必ず経ないために、データ入力時のミスによる誤りが生じやすい。米FDAは臨床実験データ管理の際のガイドラインを提示しているが、データ入力自体は人の手で実施される場合が存在するとしている

¹⁵。

5.2. 「学位・履修履歴証明」テーマ

5.2.1. 基本概要

大企業だけではなく、スタートアップといった規模の小さく、ライフサイクルが短い企業における就労がより一般化する中、履歴や勤務評定の正確な記録や証明の仕組みは今後さらに重要になると考えられる。また、履修履歴に関しては、現在よりも一層多くの大学や組織（MOOC等）間をまたがった単位取得により、卒業の要件を満たしていくことも可能となると考えられる。

したがって、将来的には経歴等については電子化して管理することが現実的とも考えられる。個人のデータの真正性が担保された状態で保管され、当該データを簡易に利用することが可能であれば、大学、企業、学生それぞれにとって、アナログで実施している現状と比較するとコストメリットやその他の様々なメリットが発生すると考えられる。また、「学位・履修履歴管理」とは、一般化すると個人の属性情報の管理とも言えるため、個人の属性情報管理フレームワークが実現できれば、様々な横展開の可能性が考えられる。なお、個人情報保護、プライバシー保護の観点から、管理されるデータの種類・内容、データの利用方法、第三者提供の枠組み等についての検討が必要なことはいうまでもない。

また、履修する講義のデータと実際の成績データ等を連携させることができれば、成績証明等に応用することが可能と考えられるが、評価を統合利用する際には、各組織間での評価基準の整合性を取る必要があり、各組織間で調整が必要である。よって当該スキームの構築には要件を詳細に設計する必要があり（例：証明書の失効条件を特定のイベントの発生とすることや、ID管理とデータ管理の方法の明確化等）、その要件に合う技術を模索しなければならない（必ずしもブロックチェーン技術でない可能性もある）。

¹⁵ Guidance for Industry Electronic Source Data in Clinical Investigations : <https://www.fda.gov/downloads/drugs/guidances/ucm328691.pdf>

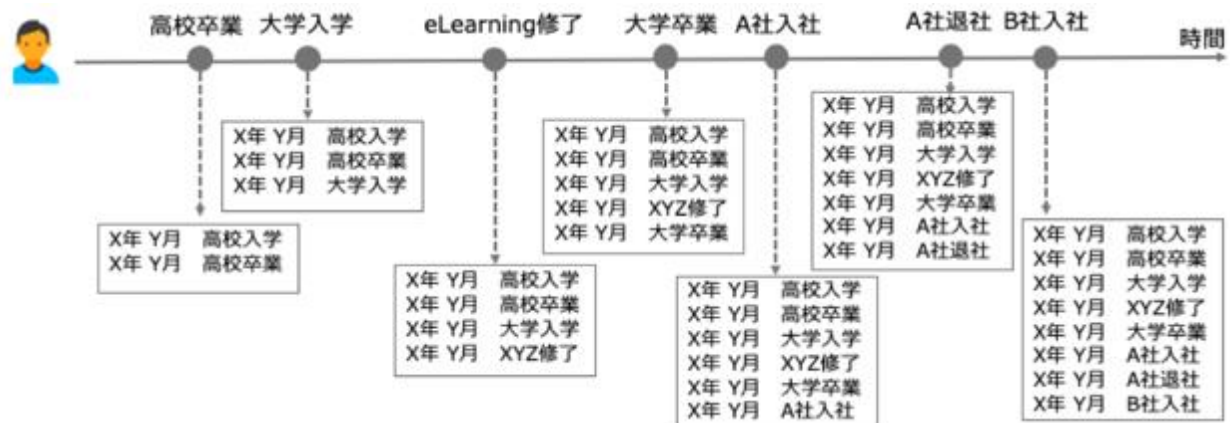
なお、以下のユースケースの通り、現状では学位・経歴データを活用する場面は必ずしも多くないと考えられるが、産業構造等の変化を踏まえれば、これらを利用する機会は今後増加するものと考えられる。したがって、真正性の担保された学位・経歴データは今後使用側・利用側双方にとって重要なことを見込まれ、今後、ルールの整備による強制力を設けたり、適切なインセンティブの付与を行ったり、もしくはその両方を用いたりする等の施策の必要性も考えられる。

- ユースケース①（学校）：小中高及び大学、大学院への進学時の一生約4～5回
- ユースケース②（会社）：就職及び転職。履修履歴や成績証明証は新卒採用のときのみ使用される（ただし、転職の場合、30代では約9割の人が2回以下の転職を経験している¹⁶⁾

5.2.2. 適用案の例

(1) 客観的データに限り分散台帳にて管理

学校の成績や会社の評価等組織ごとに判断基準が異なるデータを一律で直接比較することは困難であり、一律で評価するためには、各組織間で評価基準の整合性を調整することが必要である。したがって、ここでは学校の入学・卒業及びe-Learningなどの修了履歴、そして入社・退社などのファクトベースの客観的データのみを取り扱う基盤を想定した。



図表 5.2 - 1 ファクトベースの定性的データの取り組み例¹⁷⁾



図表 5.2 - 2 取り扱うデータの種類¹⁷⁾

¹⁶⁾ 年別別の転職回数と採用実態 by Recruit <https://next.rikunabi.com/tenshokuknowhow/archives/5883/>

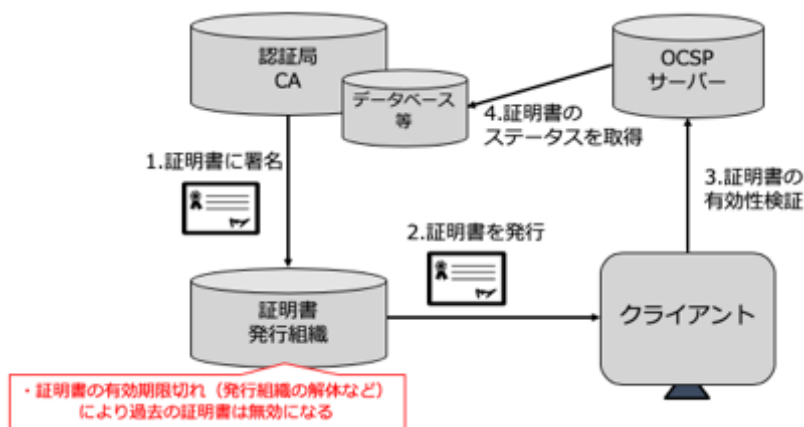
¹⁷⁾ 株式会社リクルート R&D 作成

(2) 過去に発行した証明書の有効性検証

証明書を長期的に検証することは中央集権的なシステムにおいても容易ではない。例えば、PKI の標準規格である X.509 は検証時点での証明書の正当性を確認する仕組みであり、証明書発行者が廃業した場合に、証明書が過去の特定の時点で有効であったかどうかを証明することは困難である。

この点、例えば一般社団法人日本データ通信協会タイムビジネス協議会では、信頼のおける時刻情報を考慮した情報通信基盤を整備する上で、現時点において電子認証局 (CA)、時刻認証局 (TSA) 等、既存の組織だけで解決が困難な課題があるとしている。具体的には、証明書を発行した TSA と TSA が利用する公開鍵証明書を提供する CA が廃業した場合の運用ルールに課題が存在し、証明書を検証するために必要となる CA の公開鍵証明書等の保存、公開を第三者機関により継続する制度づくりが必要と言及している¹⁸。

Certificate Transparency といった、証明書のライフサイクルを、ログを記録するサーバで管理する仕組みが存在するが、これは発行者に対する強制力が存在することにより成立している。ここにブロックチェーン技術を利用すれば、ルールによる強制力を必要とせずに過去に遡って証明書を検証できるスキームを構築できる可能性があると考えられる。

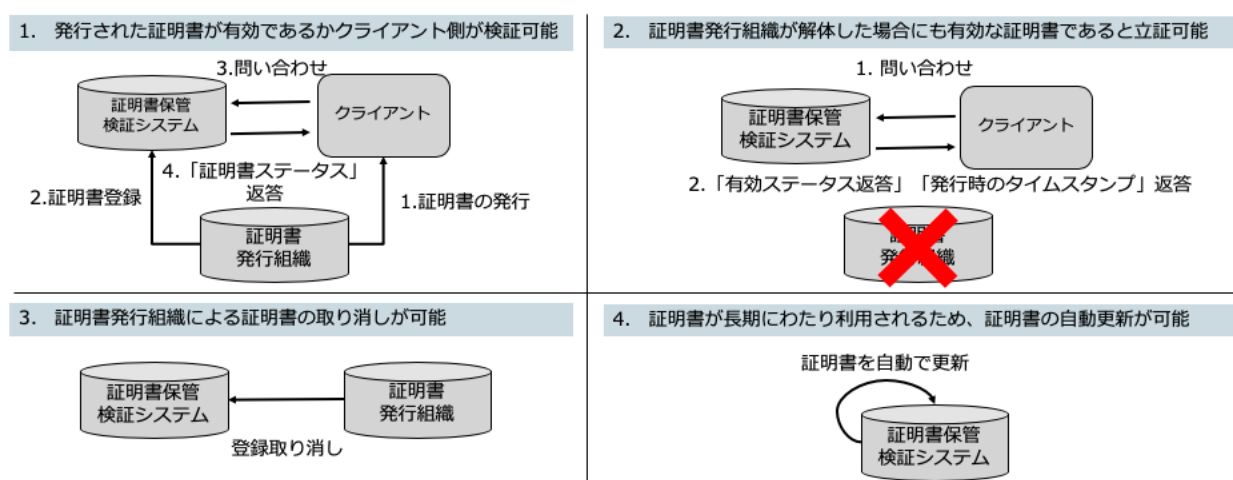


図表 5.2 - 3 既存の X.509 証明書の簡易証明フロー¹⁹

¹⁸ 電子証明基盤の構築に向けて～タイムスタンプの長期的証明力の考察と信頼できる基盤の提言～by タイムビジネス協議会 電子証明基盤検討 WG : https://www.dekvo.or.jp/tbf/data/seika/kiban_001.pdf

¹⁹ 株式会社リクルート R&D 作成

過去に遡って証明書を検証できるスキームを構築するには以下4つの要件が必要だと考えられる。



図表 5.2 - 4 必要と想定される要件²⁰

5.3. 「研究データの信頼性確保」テーマ

5.3.1. 基本概要

文部科学省は「研究活動における不正行為への対応等に関するガイドライン」において、不正行為の種類として以下を定義している²¹。

- **【捏造】** データを改変もしくは都合の悪いデータを排除すること
- **【改ざん】** 研究資料・機器・過程を変更する操作を行い、データ、研究活動によって得られた結果等を真正でないものに加工すること
- **【盗用】** 他の研究者のアイデア、分析・解析方法、データ、研究結果、論文又は用語を当該研究者の了解又は適切な表示なく流用すること

複雑かつ多様な研究プロセス上には研究データ不正が発生する状況が複数存在すると考えられる。例えば、データの測定値自体が正確なのかどうか、測定方法が正しいかどうか、等様々な観点があり、研究プロセスや研究データの全体のライフサイクルを理解した上で、どの工程にブロックチェーン技術を適用することが可能かを考察する必要がある。

研究履歴の保存手段である研究ノートと、実験を実施した時に発生する未加工な生データは、相関関係があると考えられるため、スマートコントラクト等を使用し、改ざんできない仕組みでデータを保存することができれば、ブロックチェーン技術の適用は、研究データの不正防止においてメリットがあると考えられる。但し、例えば、実験で取得した画像データも加工が可能である為、計測機器から

²⁰ 株式会社リクルート R&D 作成

²¹ 研究活動における不正行為への対応等に関するガイドライン http://www.mext.go.jp/b_menu/houdou/26/08/_icsFiles/afieldfile/2014/08/26/1351568_02_1.pdf

データを取得して直接データベースに登録する等を実施せず、人の手によりデータの登録を実施した場合、単体で真正性が担保されるとは言い難い。

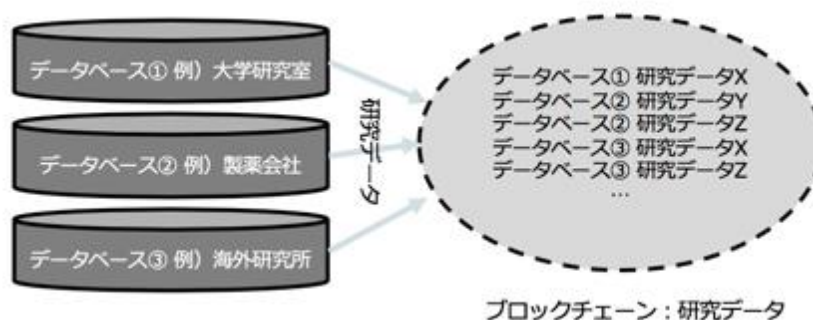
その他にもブロックチェーン技術を基盤とする研究データのソリューションの構築にあたり、考慮すべき事項も複数存在する。例えば、データの種類が複数存在する場合、それに携わるステークホルダーも複数存在するため、そのステークホルダー間の利害関係の調整や、運用する際の共通ルールを定める必要がある。また、研究データが個人情報に関係する場合、プライバシーの保護等の倫理的課題も存在し、データの開示範囲に関して綿密に設計する必要がある。さらに臨床研究の場合には、そのデータが公開されるのは研究結果の発表後であることが多いため、研究の初期の段階から研究データをパブリックネットワークに公開する構想は現実的ではなく、研究活動を実施している期間は限られた人々しかアクセス権を持たない領域に格納し、研究結果の発表後にパブリックネットワークに公開する仕組みにする必要があると考えられる。

既に UMIN 等の研究活動の管理システムを利用する必要がある臨床研究や大規模な研究の研究者は継続して当該管理システムを利用する可能性が存在する。しかしながら、その他の殆どの研究者にとっては専用の研究活動の管理システムを利用すること自体が単純に面倒であると考えられ、それぞれの研究者にとってインセンティブが確保されない限り管理システムは利用されない可能性が高い。また、簡便に利用可能であることも重要な要素であり、特別な操作を実施することなく利用できるものである必要があると考えられる。

5.3.2. 適用案の例

(1) データベースとしての適用例

大学の研究機関、製薬会社、海外の研究所、UMIN 等のデータベース等のデータプロバイダから研究活動で計測、保存された未加工の生データを、分散ストレージやブロックチェーンに格納することで、改ざんが困難なストレージ内に情報を残すことができるため、遡ってのデータの改ざんは困難になると考えられる。

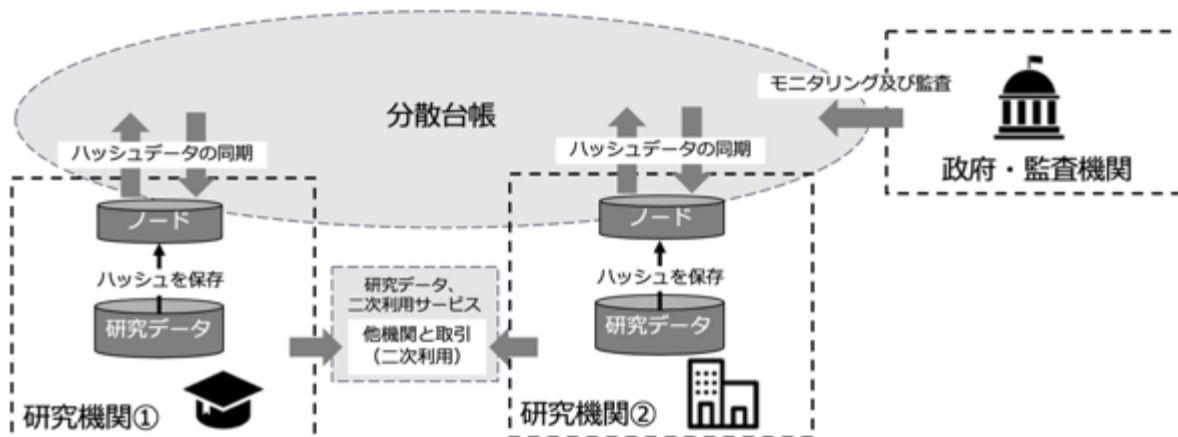


図表 5.3 - 1 データベースとしての適用例²²

²² 株式会社リクルート R&D 作成

この適用例におけるブロックチェーン技術の適用可能性としては、国や属性が異なるデータプロバイダのデータを登録する際に、特定の中央集権的機関への依存を最小化することができることや、生データをハッシュ化した値で保存する場合には、データを誰かが所有することなく、解読不可能な形式で保存することで、データ共有に対するハードルを下げるることができることがあげられる。

また、格納するデータの種類によって、以下2つの活用案を考えることができる。1つ目は、研究データ自体は各研究機関で管理し、研究データのハッシュ値だけをブロックチェーン、分散ストレージ上に登録するという構想である。



図表 5.3 - 2 研究データのハッシュ値だけをブロックチェーン上に登録する²³

利点：

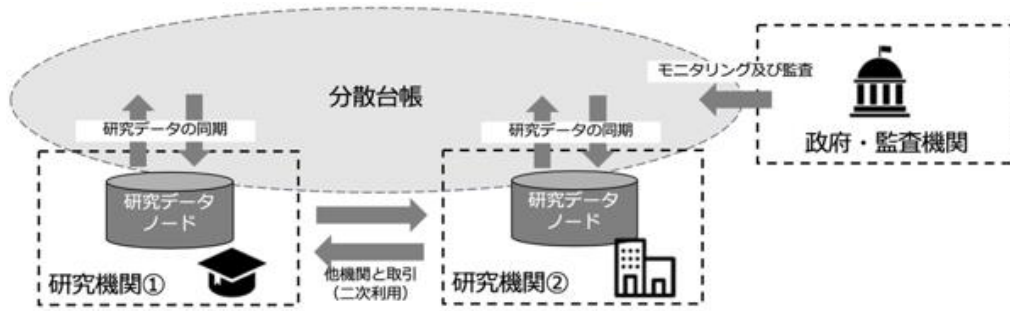
- ハッシュ値を保存するため、各ノードの容量が比較的小さい
- 未加工の生データ自体は、各研究機関で保存するため、プライバシーに関する心理的障壁が低いと考えられる
- 推測不可なハッシュ値を保存するため、既存のパブリックブロックチェーンを利用できる可能性がある

課題：

- データの二次利用を実施する場合は、別途システムを構築する必要がある
- 生データの情報を変更するとハッシュ値が変更されてしまうため、データ運用ルールを厳密に定める必要がある

2つ目の構想としては、全ての研究データをブロックチェーン上で管理することが考えられる。

²³ 株式会社リクルート R&D 作成



図表 5.3 - 3 全ての研究データをブロックチェーン上で管理²⁴

利点：

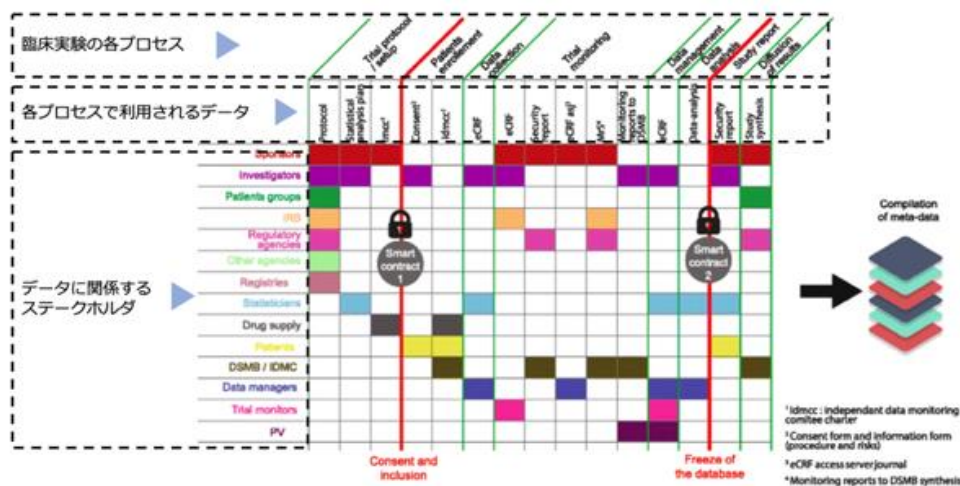
- データの二次利用に関して、スマートコントラクトを用いて秘匿取引が可能である

課題：

- アクセスコントロールが可能なコンソーシアムチェーンの構築が必要な可能性がある
- 全データを各ノードで保存するため、各ノードのデータ容量が膨大になる
- 全データを分散して保存するため、プライバシーに関する心理的障壁が存在する

(2) スマートコントラクトを利用した適用例

ブロックチェーンのスマートコントラクト技術を活用し、研究プロセスの各工程においても検証を実施しながら進む基盤が考えられる。例えば、必要な研究データの種類や質が揃わない場合、次のプロセスに移行しないロジックをスマートコントラクトとして組み込むことで、研究プロセス全体における整合性の向上に繋げる。



図表 5.3 - 4 スマートコントラクトを利用した適用例²²

上の図では臨床実験の各プロセスで利用されるデータが、どのステークホルダーと関係するかをマッピングしている²⁵。

²⁴ 株式会社リクルート R&D 作成

²⁵ Blockchain technology for improving clinical research quality: <https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z>

6. 標準化に関して

6.1. 標準化団体によるブロックチェーン技術における標準化の流れ

以下に示すとおり、各種国際標準化団体に置いてブロックチェーン技術関連の標準化の動きはあるものの、標準化の策定までは至っていない。

組織名	プロジェクト名 (グループ)	トピック
IEEE Standards Association	The IEEE Blockchain Initiative	IEEE ブロックチェーンのプロジェクト及び活動の拠点：スタンダード、教育、会議等主要な委員会でサポートされている包括的なプロジェクト
IETF : The Internet Engineering Task Force	Decentralized Internet Infrastructure Proposed RG	分散化技術に関する研究課題を調査する。ユースケースやベストプラクティスの開発等を活動の目的としている
ISO : International Organization for Standardization	ISO/TC 307	現在 8 個のグループによって構成されたブロックチェーンと DLT の標準化プロジェクト
ITU : International Telecommunication Union	Focus Group on Application of Distributed Ledger Technology	DLT ベースのサービスの標準化ロードマップを策定し、ITU、その他の標準開発機関、フォーラム、及びグループで進行中の活動をサポートする
W3C : World Wide Web Consortium	The Web Ledger Protocol	DLT システムにおけるデータモデルやシンタックス概要

図表 6.1 - 1 標準化団体におけるブロックチェーン標準化の動き

6.1.1. IEEE

組織名	プロジェクト名	グループ	検討内容
IEEE Standards Association The IEEE Blockchain Initiative	P2418.1 - Standard for the Framework of Blockchain Use in Internet of Things (IoT)		Internet of Things (IoT) アプリケーションにおけるブロックチェーンの使用、実装、及び対話のための共通のフレームワーク
	P2418.2 - Standard Data Format for Blockchain Systems		ブロックチェーンシステムのデータフォーマット要件
	P2418.3 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture		農業における DLT システムの使用、実装、及び対話のための共通フレームワーク
	P2418.4 - Standard for the Framework of Distributed Ledger Technology (DLT) Use		自動運転車における DLT システムの使用、実装、及び対話のための共通フレームワーク

	in Connected and Autonomous Vehicles (CAVs)	
	P825 - Guide for Interoperability of Transactive Energy Systems with Electric Power Infrastructure (Building the Enabling Network for Distributed Energy Resources)	分散型電源によってトランザクティブなグリッドサービスを実行するためのガイド

図表 6.1 - 1 IEEE におけるブロックチェーン標準化の動き

6.1.2. IETF

組織名	プロジェクト名	グループ	検討内容
IETF : The Internet Engineering Task Force	Decentralized Internet Infrastructure Proposed RG		<p>分散化技術に関する研究課題を調査する。 ユースケースやベストプラクティスの開発等を活動の目的としている</p> <ul style="list-style-type: none"> ・ユースケースとその具体的な要件を分散して実装することについて調査（理解、文書化、調査）する ・スケーラビリティ、パフォーマンス、セキュリティ等のインターネットレベルの問題に焦点を当てて、特定のユースケースのソリューションを検討して評価する ・技術的ソリューションとベストプラクティスを開発し文書化する ・スケーリングの問題について、コンポーネントが欠落しているかどうかを判断するツールとメトリックを開発する ・IETF の将来の作業項目を整理する

図表 6.1 - 2 IETF におけるブロックチェーン標準化の動き

6.1.3. ISO

組織名	プロジェクト名	グループ	検討内容
ISO : International Organization for Standardization	ISO/TC 307	ISO/TC 307/CAG 1	Convenors coordination group
		ISO/TC 307/JWG 4	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
		ISO/TC 307/SG 2	Use cases
		ISO/TC 307/SG 6	Governance of blockchain and distributed ledger technology systems

		ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems
		ISO/TC 307/WG 1	Foundations
		ISO/TC 307/WG 2	Security, privacy and identity
		ISO/TC 307/WG 3	Smart contracts and their applications

図表 6.1 - 3 ISO におけるブロックチェーン標準化の動き

6.1.4. ITU

組織名	プロジェクト名	グループ	検討内容
ITU : International Telecommuni- cation Union	Focus Group on Application of Distributed Ledger Technology (FG DLT)		DLT ベースのサービスの標準化ロードマップを策定し、ITU、その他の標準開発機関、フォーラム、及びグループで進行中の活動をサポートする <ul style="list-style-type: none"> ・ DLT ベースのアプリケーションとサービスを識別して分析する ・ グローバル規模でのアプリケーションやサービスの実装をサポートするベストプラクティスとガイドランスを作成する ・ ITU-T 研究グループにおける関連する標準化作業の道筋を提案する

図表 6.1 - 4 ITU におけるブロックチェーン標準化の動き

6.1.5. W3C

組織名	プロジェクト名	グループ	検討内容
W3C : World Wide Web Consortium	The Web Ledger Protocol	W3C Blockchain Community Group	DLT システムにおけるデータモデルやシタックスの概要
	Decentralized Identifiers	Credentials Community Group	検証可能な「自己主権」デジタル識別のための新しい識別子の概要

図表 6.1 - 5 W3C におけるブロックチェーン標準化の動き

6.2. ブロックチェーンプロトコル独自の標準化プロセス

ブロックチェーンにおいては、ISO 等の標準化に先駆けて、Bitcoin や Ethereum は独自の標準化プロセスを、それぞれ Bitcoin Improvement Proposal (BIP) ²⁶、Ethereum Improvement Proposal (EIP) ²⁷ という名称で実施している。

²⁶ BIPs : <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki>

²⁷ EIPs : <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1.md>

BIP と EIP はどちらも三種類の提案から構成されている。

(1) プログラムコードに関する提案

A Standards Track BIP (Bitcoin の場合)、A Standards Track EIP (Ethereum の場合) と呼ばれるものであり、ブロックチェーン自体やスマートコントラクトの標準実装に関する内容の提案である。
※Ethereum の場合は、アプリケーションレベルのスタンダードである ERC (Ethereum Request for Comments) が策定されており、トークンのスタンダードである ERC20 や代替不可能 (non fungible) なトークンのスタンダードである ERC721 等が存在する。

(2) 一般的なガイドラインに関する提案

A Informational BIP (Bitcoin の場合)、A Informational EIP (Ethereum の場合) と呼ばれるものであり、この提案は、必ずしもコミュニティのコンセンサス又は勧告を表すものではないため、提案を適用するか否かはユーザの自由判断である。

(3) プロセスに関する提案

A Process BIP (Bitcoin の場合)、A Meta EIP (Ethereum の場合) と呼ばれるものである。主に BIP 及び EIP 自体の実施プロセスについての提案であり、この提案をユーザは無視できず、遵守する必要がある

6.2.1. EIP: Ethereum Improvement Proposal プロセス

EIP は Ethereum Github 上で管理されており、プロセスは下記ルールによって実施される。

ルール	実施事項
EIP 作成者 (チャンピオンとも呼ばれる)	EIP を特定のフォーマットに沿って記述し、フォーラムで議論し、議論のコンセンサスを構築する
EIP 編集者 (Vitalik Buterin 氏等)	<ul style="list-style-type: none">・ EIP が規格に沿っているか、議論の状況をチェックする (アイデアに技術的側面があるか、タイトルは正確か、フォーマットに沿っているか等)・ チェック後、EIP 番号を付与し、対応する Pull Request をマージしてステータスを変更する・ EIP 編集者はあくまで管理や編集を実施するだけで、EIP それ自体の評価はしない。「The editors don't pass judgment on EIPs. We merely do the administrative & editorial part.」
Ethereum Core Developer	EIP の実装をチェックする

図表 6.2 - 1 EIP プロセスにおけるルール

また、正常に EIP プロセスが完了した場合、下記ステータスで EIP は遷移する。



図表 6.2 - 2 EIP プロセスにおけるステータス

ステータス	説明
WIP : Work in progress	<ul style="list-style-type: none"> ・ EIP 作成者が、コミュニティにアイデアの提案を実施し、最初の Pull Request を作成した状態 ・ 「幅が広すぎる」「重複した内容」「技術的に適切でない」「動機が適切でない」「下位互換性に対応していない」「又は Ethereum の考え方に従わない」場合は、EIP 編集者によって Pull Request が却下される
Draft	<ul style="list-style-type: none"> ・ WIP から EIP 編集者のチェックをパスした状態。EIP の番号が EIP 編集者によって付与されている ・ 議論が成熟し次のステータスに進めると判断した場合、EIP 作成者が再度 Pull Request を作成する ・ Draft にまだ重要な変更があると考えられる場合は、EIP 編集者によって Pull Request が却下される
Last Call	<ul style="list-style-type: none"> ・ 重要な変更や技術的な指摘が存在しないかチェックしている状態 ・ 重要な変更や技術的な指摘が存在しない場合は、次のステータスに移行する ・ Ethereum Core に関する EIP の場合、次は「Accepted」にステータスが移行する ・ Ethereum Core に関する EIP で無い場合、次は「Final」にステータスが移行する
Accepted	<ul style="list-style-type: none"> ・ Ethereum Core Developer によって実装を検証している状態 ・ Ethereum Core に関する EIP の場合は、少なくとも 3 つの実行可能な Ethereum クライアントで実装する必要がある
Final	<ul style="list-style-type: none"> ・ EIP の実装が完了し、コミュニティによって採用されると、ステータスは「Final」に変更される

図表 6.2 - 3 各各ステータスの説明

他の EIP 作成者から、EIP の所有権を引き受けることも可能である。その場合は元の EIP 作成者と、EIP 編集者にメッセージを送信し、権利を引き継ぐ。もし元の EIP 作成者が返信を返さない場合は、EIP 編集者が一方的に (unilateral) に決断を下す。

6.2.2. EIP と BIP の例

番号	内容及び経緯
BIP141 ²⁸	<ul style="list-style-type: none"> ・ トランザクションの情報から署名 (Witness) を分離 (Segregate) する提案 ・ Bitcoin のスケーラビリティの問題への対応の1つ
ERC20 ²⁹	<ul style="list-style-type: none"> ・ Ethereum スマートコントラクトのプラクティスであった Standardized_Contract_APIs に記述された一要素である Transferable Fungibles (Also known as tokens, coins and sub-currencies.) を Ethereum 版 RFC である ERC (Ethereum Request for Comments) にリライトした規格である ・ トークンの移転等に関する状態や関数が記述されている。 ・ ERC20 はトークンに関する基本的な機能の実装提案であったため、ERC20 の発表後、様々な特性を持つトークンの規格が多数提案された。
ERC721 ³⁰	<ul style="list-style-type: none"> ・ ERC20 のトークンは代替可能 (Fungible) でそれぞれが同一 (Identical) なものである ・ それに対して、トークンが代替不可能 (Non Fungible) でそれぞれが唯一 (Unique) な証書 (Deed) として発表されたのが ERC721 である ・ NFT (non-fungible token) と呼ばれ、区別可能であり、権利の移転追跡が可能なことから下記のような利用手段が考えられている。 <ul style="list-style-type: none"> - 物理的な財産 - 住宅、絵画のような芸術品 - デジタル上の収集物 - ゲームアイテム、トレーディングカード - ネガティブな意味をもつ資産 - ローン、負債、その他責務

²⁸ BIP141 : <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>

²⁹ ERC20 : <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>

³⁰ ERC721 : <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md>

7. 国際動向調査

7.1. 「学位・履修履歴証明」テーマ

7.1.1. 背景

「学位・履修履歴証明」のデジタル管理における社会的ニーズは日本だけでなく世界的に求められており、ブロックチェーン技術の適用可能性が検討されている。産業構造や働き方が急速に変化に伴い、学位履修履歴・職歴をどのように真正性を保ち、偽造や改ざんされた証明書を見破るのか、以下の海外事例を元に考察を深めていく。

いくつか本事業において議論した内容と各事例における見解に関して乖離が発生している箇所が存在している。ただ国際動向調査としては各プロジェクトの見解を事例としてそのまま記載している。

国名	プロジェクト名	テーマ	概要
アメリカ	Blockcerts	ブロックチェーン基盤の卒業証明書を管理するアプリケーションプラットフォーム	ブロックチェーンに卒業証明書等を記録し、第三者が卒業証明書の検証可能。オープンソースのライブラリ、ツール、モバイルアプリケーションで構成。
キプロス	University of Nicosia	ブロックチェーン基盤の卒業証明書	ビットコインを採用したブロックチェーン基盤のデジタル証明書を卒業生に配布。卒業生が秘密鍵を保持しないシステム設計を考案。
イギリス イタリア	Gradbase	ブロックチェーン基盤の卒業証明書サービスとビジネス展開	ロンドンとミラノに拠点を持つ企業。ブロックチェーン基盤のデジタル卒業証明書のサービスをローンチ。
イギリス	University of Birmingham	Blockcerts のシステム改善	Blockcerts のシステムにマルチシグを取り入れることで、セキュリティの向上ができると提案。
イギリス	Open University	OpenBadge を利用したブロックチェーン基盤の属性情報の登録	open badge をスマートコントラクトで制御し、個人の情報をブロックチェーンに登録。企業とのマッチングができるプラットフォームを提案。
アメリカ	uPort	自己主権型アイデンティティのプラットフォーム	資格や職歴、学歴等あらゆる記録をブロックチェーン上に記録し、保持者本人が責任を持って所持できる自己主権型アイデンティティプラットフォームの提案。

マレーシア	e-scroll	ブロックチェーン基盤の卒業証明書	NEMを採用したブロックチェーン基盤のデジタル証明書を卒業生に配布。マレーシアの6つの大学が関連したコンソーシアム型ブロックチェーンを実装。
-------	----------	------------------	--

7.1.2. 事例①「Blockcerts」

(1) プロジェクトの概要

Blockcerts³¹は、MIT Media Labを中心にLearning Machine社³²と開発されたブロックチェーン基盤のプラットフォームで卒業証明書を管理するプラットフォームである。ブロックチェーンに卒業証明書等を記録し、第三者が卒業証明書の検証をする。卒業証明書だけでなく資格等も管理することができ、発行機関を介さずに資格や卒業証明書が偽造ではなく特定の発行機関が作成したことを証明することが可能である。

Blockcertsは、オープンソースのライブラリ、ツール、モバイルアプリケーションで構成されており、卒業証明書の保有者中心の分散型エコシステムを実現している。オープンソースである

Blockcertsは、バーミンガム大学やバーレーン大学、マルタ共和国等あらゆる機関や国に採用され実証実験が行われている。

(2) プロジェクトの背景

ブロックチェーンの分散台帳技術を活用することで、卒業証明書の偽造の防止、卒業証明の問い合わせを無くし卒業したことを簡単に第三者に証明できるようになると考えられる。

現在でも、資格証明書は成果や会員である証として運用されているが、ほとんどの証明書はアナログで運用されていることが多い。例えば、大学の卒業証明書は、紙で発行されることが多いため、本人が本物の証明書を持参したとしても、それが本物であるかは大学に問い合わせをしなければ受け取った側には判断できない（問い合わせを行ったとしても、個人情報保護の観点から教えてもらえない可能性も存在する）。また、卒業証明書を偽造する例も多発しており、精巧な模倣技術に加え、大学機関によりフォーマットも異なることも相互に関係してあらゆる面において運用が上手くできていないのが現状である。

Blockcertsの最初の開発に携わった人物の一人であるMIT Media LabのPhilipp Schmidt氏は、非公式な学習履歴の検証及び管理においてブロックチェーン技術利用の検討を始めた³³。彼は資格証明のプラットフォームにおいてブロックチェーンを使用する理由を「資格は金融資本ではなく社会資本

³¹ Blockcerts : <https://www.blockcerts.org/>

³² Learning Machine社 : <https://www.learningmachine.com/>

³³ リクルートR&Dとのインタビューにて

の一種の通貨として考えることができるからだ。」と話をしており、「ブロックチェーンは暗号通貨ビットコインのような通貨としての利用がベストだと知られている。しかし、本質はトランザクションを分散台帳に記録することである。そして、耐久性や透明性があり、タイムスタンプを持ち、非中央集権であることが特徴である。これらの特徴は、金融取引の管理にも同様に資格証明システムにも役立つと考えられる」と主張している³⁴。

しかし、本質はトランザクションを分散台帳に記録することであり、耐久性やタイムスタンプ機能、透明性があり、そして非中央集権であることである。これらの特性は、金融取引の管理にも同様に資格証明システムにも役立つと考えられる」と主張している³⁵。

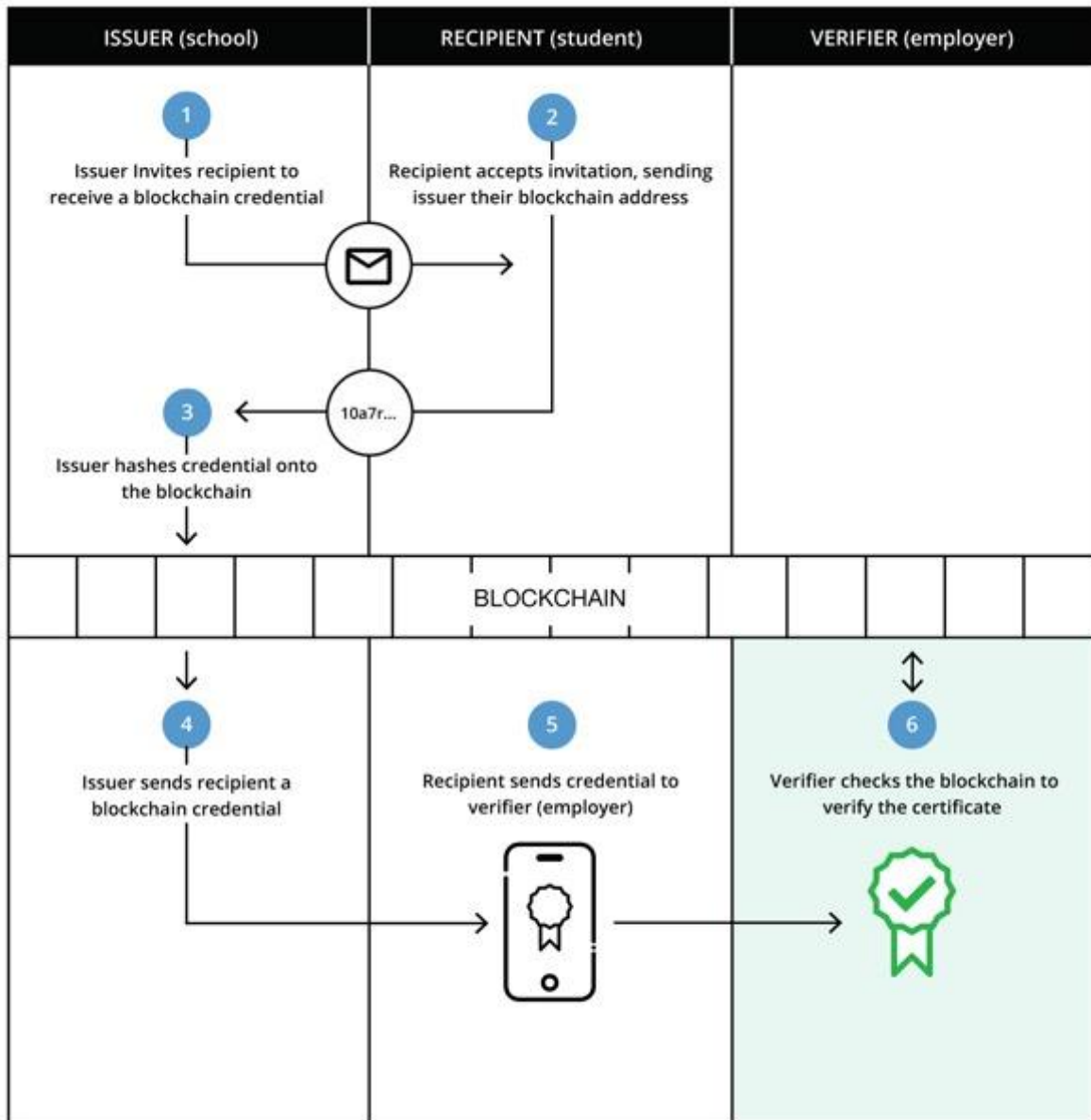
(3) 仕組み

基本フロー

Blockcerts はプロトコルとしてビットコインとイーサリアムを用いている。ブロックチェーンの耐改ざん性の性質や分散台帳技術等を利用することにより、卒業証明書の偽造の防止、卒業証明書の問い合わせを無くし簡単に卒業したことを第三者に証明できるシステムを提案している。具体的には、卒業予定の生徒はスマートアプリケーション「Blockcerts Wallet」をダウンロードすることにより、大学からブロックチェーン基盤のデジタル卒業証明書を受け取り、Blockcerts wallets から確認できる。就職活動等の際は、企業に対しても、情報をシェアすることができ、企業は専用の確認サイトから卒業証明書の真正性をチェックすることができる。

³⁴ Credentials, Reputation, and the Blockchain : <https://er.educause.edu/articles/2017/4/credentials-reputation-and-the-blockchain>

³⁵ Credentials, Reputation, and the Blockchain : <https://er.educause.edu/articles/2017/4/credentials-reputation-and-the-blockchain>



図表 7.1 - 1 Blockcerts のワークフロー³⁶

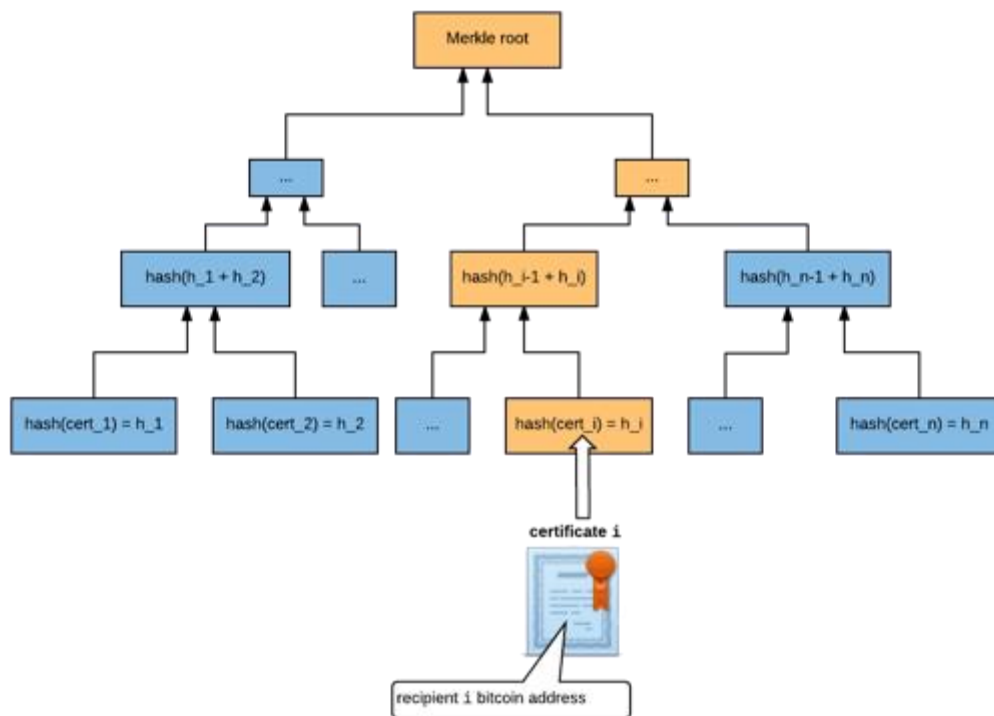
- 1) 発行機関（学校）は受取人（生徒）にブロックチェーン基盤上にクレデンシャルを付与するための招待メールを送る。
- 2) 招待を受けた受取人（生徒）は、招待の受諾又は却下の意思決定をする。受諾した場合は、受取人（生徒）自身のブロックチェーンアドレスを発行機関（学校）に送る。
- 3) 発行機関（学校）はブロックチェーンでクレデンシャルをハッシュ化する
- 4) 発行機関（学校）は、それを受取人（生徒）に送る。
- 5) 受取人（生徒）は、クレデンシャルのハッシュ値を受け取り、卒業の証明をする際に企業に共有をすることができる

³⁶ Blockcerts のワークフロー：<https://www.blockcerts.org/guide/>

- 6) 企業はブロックチェーンに問い合わせることで真正性の確認ができる。検証用のウェブサイトから参照できる³⁷。

ブロックチェーンに登録されているデータの内容

ブロックチェーンに卒業証明書を書き込む場合、2つのパターンがある。1度のトランザクションを使って1つの卒業証明書を発行するか、複数の卒業証明書を1つにまとめて発行する方法である。ブロックチェーンに情報を格納する場合には、トランザクション手数料が都度発生するため後者の手法が適切であると考えられる。発行機関は、複数の卒業証明書のハッシュ値を用いた Merkle Tree を作り、トランザクションのアウトプットに OP_RETURN を利用して Merkle root を登録する。



図表 7.1 - 2 Merkle Tree³⁸

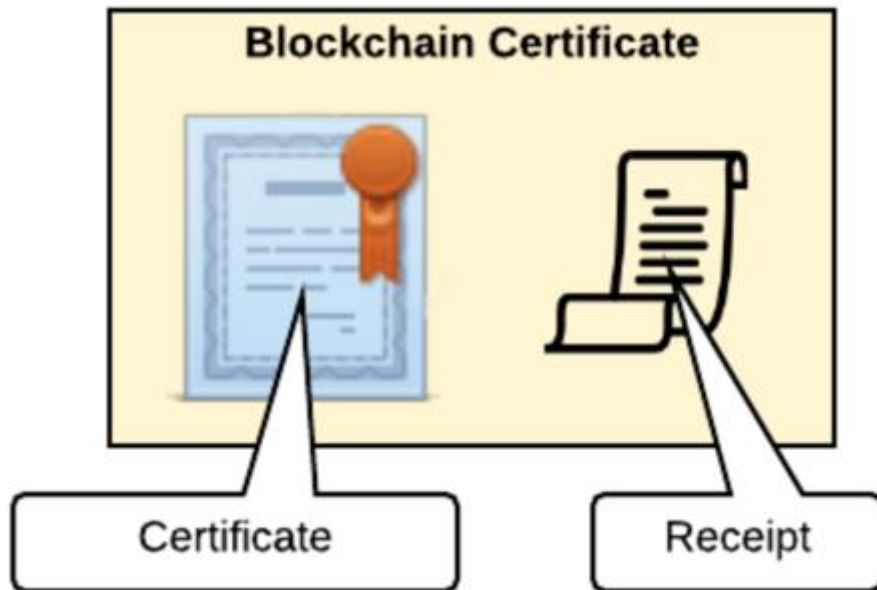
卒業証明書を複数纏めたものをバッチと読んでおり、卒業証明書は受取人の情報を含んでいる。発行機関は、それぞれの卒業証明書をハッシュ化し、Merkle Tree の中でそれらを結びつける。Merkle Tree の Merkle root は 256bit のハッシュ値で、ブロックチェーン上に発行される。そのトランザクションのアウトプットを Transaction structure (トランザクション構造) と Blockcerts は呼んでいる。卒業証明書が Merkle Tree に含まれていることを証明するために、受取人に与えられたブロックチェーン証明書は、Merkle Proof Signature Suite 2017 (サイン証明)³⁹の規格に準拠している。バ

³⁷ 検証用のウェブサイト: <https://credentials.mit.edu/>

³⁸ <https://github.com/blockchain-certificates/cert-issuer>

³⁹ Merkle Proof Signature Suite 2017: <https://w3c-dvcg.github.io/lds-merkleproof2017/>

ツチのサイズはビットコインネットワークによって 100KB のトランザクションの大きさに制限される。これは、バッチにつき最高およそ 2000 人の卒業生の量を保存できる計算である。



図表 7.1 - 3 Blockcerts の卒業証明書の構成⁴⁰

上記の「図表 7.1 - 3」で表しているように、ブロックチェーン基盤の卒業証明書の構成は、卒業証明書とレシートがある。レシートは以下のデータを含む。

- Merkle Tree に格納されているトランザクション ID
- ブロックチェーン上に期待される Merkle root
- 受取人の証明書の期待されるハッシュ値
- 受取人の証明書から Merkle root への Merkle path。図表 7.1 - 2 にてオレンジでハイライトされた path

これらは検証プロセスを通じて、以下の項目を検証することが可能である。

- 証明書のハッシュ値が受取人の値と合致するか
- Merkle path が確かなものであるか
- ブロックチェーン上に格納されている Merkle root が発行されてから改竄されていないか

尚、卒業証明書は以下のデータを含む。

- 受取人の名前
- 発行機関
- 発行した日付等の基本情報

⁴⁰ <https://github.com/blockchain-certificates/cert-issuer>

卒業証明書の発行プロセス

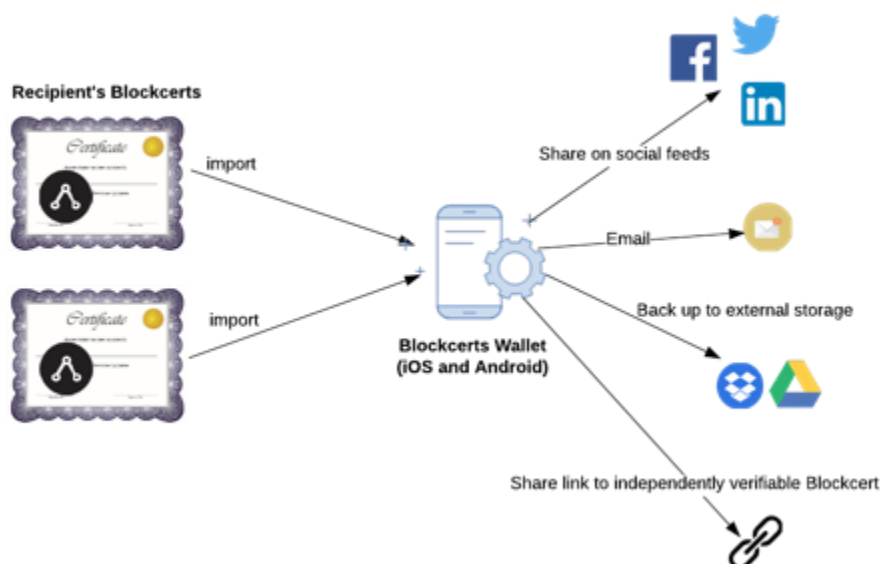
- 1) 受取人の名前と発行機関、発行した日付等の基本情報を含んだデジタルファイルを作成する。
- 2) 発行機関の秘密鍵で卒業証明書に署名し、その署名を卒業証明書自体に追加する。
- 3) ハッシュ値を作成する。このハッシュ値は、誰も改ざんでしていないことを証明するために使用される。
- 4) 最後に、何月何日に何某さんに特定の証明書を発行したというステートをブロックチェーン上に記録を記入するために再び発行機関の秘密鍵を使う。

ブロックチェーンに格納された卒業証明書は以下の項目を検証することが可能である。

- 証明書が誰に発行されたか
- 発行期間は誰なのか
- 証明書自体の内容が有効であるかどうか

第三者への共有

Blockcerts は、作成されたブロックチェーン基盤の卒業証明書を持ち主自身のアプリケーションから他者に簡単に共有することができる。多くのアプリケーションに対応しており、SNS や email、クラウドサービスや検証した Blockcerts のリンクをシェアすることもできる。



図表 7.1 - 4 Blockcerts の共有フロー⁴¹

⁴¹ Blockcerts の共有フロー : https://www.blockcerts.org/guide/recipient_experience.html

検証プロセス⁴²

企業等の第三者は卒業生から提出された卒業証明書が本物であるかどうかを検証する必要がある。Blockcerts は、発行された卒業証明書を指定のサイトにアップロードすることで卒業証明書が偽造されていないか等をチェックすることができる。

検証する項目は以下の 4 つである。

- 卒業証明書の整合性
- 卒業証明書の権限
- 発行機関によって失効されていないか
- 有効期限が過ぎていないか

卒業証明書の整合性

卒業証明書の整合性では、卒業証明書が改ざんされていないかを 3 つのステップで検証する。

- 1) 証明したい卒業証明書が Merkle Tree 内に存在するのを確認する。
- 2) レシートとアップロードされた卒業証明書のハッシュ値が一致する確認する。
- 3) ブロックチェーントランザクションの値と卒業証明書の Merkle root の値が一致する確認する。

1) で卒業証明書の存在を確認し、2) と 3) で、Merkle Tree 内にある卒業証明書が検証したい卒業証明書と一致しているかを判断している。

卒業証明書の真正性

トランザクションに署名する秘密鍵が発行者のものであるかを確認すること、トランザクションが発行された時点で有効であったことの 2 点を確認することによって検証できる。

発行機関によって失効されていないか

発行機関によって失効されていないかの検証は、卒業証明書の ID で検証できる。執行されている場合は、卒業証明書の ID に紐づけて失効と失効理由を記載してブロックチェーンに書き込まれる。そのため、ID に紐づけられている内容を確認することで失効されているかを判断できる。

有効期限が過ぎていないか

卒業証明書は ISO-8601 の規格に準拠した失効の日付を含ませることができる。

有効期限の検証は、入力された時刻と現在の時刻を比較することで検証する。

⁴² Verification Process: <https://github.com/blockchain-certificates/cert-verifier-js/blob/master/docs/verification-process.md>

以上の方法で、卒業証明書が改ざんされていないか、発行機関が正しいか、その有効性を検証することができる。

7.1.3. 事例②「University of Nicosia」

(1) プロジェクトの概要

キプロス共和国のニコシア大学は、ブロックチェーンに関する様々なオンライン・オフライン教育を提供している。また、ビットコインで学費を支払うこともできる等、他にはあまり例を見ないような試みを先行的に取り組んでいる。同大学では、学位や卒業証明書もブロックチェーン基盤のデジタル証明書で授与している。システム設計において、生徒が秘密鍵を所持しなくても運用可能である点が特徴である。

ニコシア大学は秘密鍵を学校側が管理し、PDFとして卒業生に渡すためアプリケーションをスマートフォンに入れる必要がない設計になっている。この点において秘密鍵を紛失した場合、卒業生であることを証明できなくなるような課題を解消している。しかし、検証により証明される内容は、その卒業証明書が改ざんされていないことと、ニコシア大学が発行したものであるということであり、その卒業証明書の保持者であるかの確認は、顔写真付きの公的な証明書で検証内容と一致するかを確認する必要があると考えられる。また、ニコシア大学が存在するときは卒業証明書を再発行可能であるが、もし存在しなくなった場合、検証は可能であっても再発行が不可能になる可能性がある。

(2) プロジェクトの詳細⁴³

このプロジェクトは、卒業証明書をブロックチェーン基盤のデジタル証明書として発行することを目的にしている。第三者はニコシア大学に問い合わせをせずにその場でその卒業証明書が本物であることを検証できる仕組みになっている。また、卒業生は秘密鍵を持たない設計になっているという特徴がある。秘密鍵を卒業生が管理する Blockcerts の場合では、生徒は自身の wallet を持ち、アプリケーションに所有権を持たせた卒業証明書を発行しているが、ニコシア大学は、大学側が秘密鍵を発行、管理し、配布しているので別途の wallet が必要ない。また、これにより、卒業生が自分の卒業証明書を紛失した場合でも再発行することが可能である。

ブロックチェーンのプロトコルはビットコインを採用しており、卒業証明書の格納には Merkle Tree を使用している。これは、トランザクション手数料のかかる可能性のあるブロックチェーンにおいて、大きなコスト削減に繋がるためである。

⁴³ University of Nicosia Blockchain Initiative : <https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain>

また、ブロックチェーンで卒業証明書を発行するメリットとして、第3者機関からの卒業証明書に関する問い合わせの量を削減できた点が挙げられる。これまでは、メールや電話によってアナログな対応をしていたという。専用のオンラインサイトにデータをアップロードすれば、その場で検証結果が返ってくる。

このシステムにおいて、ニコシア大学は仮に大学がなくなったとしても、卒業証明書の検証ができる仕組みとなることを期待している。但し、ニコシア大学が閉鎖すると、同大学が卒業証明書の検証のために運用しているウェブサイトもなくなる。その場合、卒業生は卒業証明書の検証ができる手段がなくなり、卒業した事実の証明ができなくなると考えられる。その解決策として、同大学は Facebook や LinkedIn 等あらゆるオンラインサイトからも検証できるよう専用サイトを用意している。

(3) 仕組み

卒業証明書の発行

- 1) 卒業証明書のメタデータを用意する。このメタデータは機械語で書かれたもので人は読めないようになっている。このメタデータには発行機関とビットコインアドレス（公開鍵）が含まれている。また、検証の際に有効性を判断する情報として名前等の個人データを入れることもできる。
- 2) 数千もの卒業証明書を Merkle Tree に格納し、それぞれの格納場所は Merkle root によって位置関係を把握できる。
- 3) それから OP_RETURN とニコシア大学の識別子、Merkle root の3つの要素を含むトランザクションを作成し、トランザクションを Bitcoin ノード（できればローカルノード）に送信し、トランザクション ID を返す。
- 4) 最後に PDF のメタデータを変更しないように、トランザクション ID や root hash 等の情報を追加する。この時、情報が追加されるのでハッシュ値が変更されるが、構造を保った状態でその追加情報だけを削除すれば元のハッシュ値に戻る。このハッシュ値の性質を利用することにより検証を可能にしている。
- 5) Merkle root の構造に格納させたデータの内容や値が少しでも書き換えられると全体の整合性が合わなくなりシステムエラーとなるため、改ざんが非常にしにくいシステムになっていると考えられる。

卒業証明書の検証

- 1) オンライン検証ができるウェブサイトへ接続し、卒業証明書をアップロードすることで検証を開始する。
- 2) 発行の手続きの際に最後に追加した情報を取り除く。PDF のハッシュ値と登録されているハッシュ値を比較し一致していれば改ざんされていないことになる。

- 3) トランザクション ID から Merkle root と OP_RETURN を含んだトランザクションを取得する。ここで認証情報のハッシュ値が実際にブロックチェーンから取得した Merkle root の一部であることを検証する必要がある。この検証のため、卒業証明書のハッシュ値を使用し、抽出されたメタデータからの Merkle proof を使用して、Merkle root を再構築する。それが OP_RETURN から得たものと同じであるならば、卒業証明書が改ざんされていないこと、そしてニコシア大学から発行されたものであると証明することができる。

再発行

再発行は生徒が学校に問い合わせをすることで学校側が再発行し、取得できるようになっている。

(4) University of Nicosia の Blockchain Initiative のディレクターを務める Soulla Louca 教授とのインタビュー内容

Q：ニコシア大学のブロックチェーンのイニテシアティブに関して

A：キプロスのニコシア大学はコンピューターサイエンス領域に置いてブロックチェーン技術をいち早く取り入れた。実際、ブロックチェーン技術の教育機関として授業料を暗号通貨ビットコインで支払える。また、ブロックチェーンを専門とする修士号が取得可能で、世界で最も人気のあるブロックチェーンの参考書の一つの「Mastering Bitcoin」の著者である Andreas Antonopoulos 氏が講師を務めるコース等を提供している。オンラインコースにおいては世界中から受講生が集まってきており、ブロックチェーンを基盤としたデジタル卒業証明書を発行している。

他にも、ブロックチェーン基盤のデジタル証明書のプラットフォームに関して他の大学や企業と連携している。例えば、UAE との間でプロジェクトが始まっており、EU のいくつかの大学とも話し合いをしている状況である。また、EU 最大のリサーチ・イノベーションプログラムである Horizon2020 を通じた支援を受けており、2,000 人の参加者が集まったブロックチェーン技術カンファレンスの開催もしている。

Q：ブロックチェーン基盤のデジタル証明書について

A：デジタル証明書を格納するためのプロトコルはビットコインを選択している。MIT の Blockcerts と似ているが、いくつか異なる点がある。実際、Blockcerts よりも早くプロジェクトが始まっている。Blockcerts と似ている部分は、1 度に 1000 以上の卒業証明書を格納するために Merkle Tree を採用している点である。これはビットコインのトランザクション手数料を最小限に抑えるためである。大きく異なる部分としては、2 つある。1 つは、秘密鍵の管理の必要性がない点があげられる。もう 1 つは、名前や誕生日のような他の個人情報を追加した学位情報の証明書の PDF ファイルのハッシュ値を格納している点である。学生は複数の PDF ファイルを持つことができ、企業等にその PDF ファイルを提出することで、企業側はその PDF ファイルを検証することができる。

プロトコルはビットコインであるが、イーサリアムのような他のプロトコルに変換することは難しい。今後の課題としては、スケーラビリティの問題に対処し、多くの大学や企業の間で標準を確立することである。

7.1.4. 事例③「Gradbase」

(1) プロジェクトの概要

Gradbase⁴⁴は、ロンドンとミラノに拠点を持つ企業である。大学を中心にブロックチェーン基盤の卒業証明書を提供し、様々な課題を解決している。ここでは、企業としてどのようにブロックチェーン基盤の卒業証明書を運用し、サービスを提供しているのか、2つの大学の事例を挙げることで、人件費の削減やマネタイズ、その他の利点について紹介する。

(2) 仕組み

Gradbase は、大学が卒業証明書を発行する際のプロセスにおける課題の解消を目指す企業である。卒業資格をブロックチェーン上で管理し、卒業資格の証明書を QR コードとして発行することで、信憑性の検証を可能にしている。検証は、Gradbase によって発行された証明書が、ビットコインのブロックチェーンを採用して発行したトランザクションと一致するかどうかで実施することが可能である。発行された QR コードは、LinkedIn 等で活用することができ、SNS 上のプロフィール情報の信憑性向上にも寄与できると考えられる。

以下に、GradBase を使用した卒業証明書の検証方法の説明と、実際に行ったデモの様子を掲載する。

- 1) QR コードが発行された卒業証明書を用意する
- 2) 専用のアプリケーションで QR コードを読み取る
- 3) 卒業証明書の内容が改ざんされていない場合、検証が完了する
- 4) 卒業証明書の内容が開示される

⁴⁴ Gradbase : <https://gradba.se/en/>

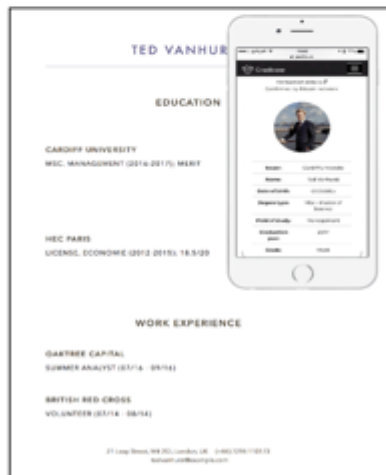
① Gradbaseで発行されたQRコード付き卒業証明書

② QRコードをスマートフォンで読み込む



③ 検証が完了するとページが切り替わる

④ 内容を確認する

図表 7.1 - 5 Gradbase の検証⁴⁵

(3) サービス内容について

現在、イタリアの Talent School Innovation School とイギリスの University College London で GradBase のサービスが、試験的に使用されており、以下の利点を享受できると考えられる。

- 1) 卒業証明書の信憑性を確認したい場合、卒業証明書の発行者に対して毎回連絡する必要性がなくなり、また、発行者の管理コストも削減できる
- 2) ブロックチェーンに卒業資格の情報を記録することで、改ざんが困難な状態で管理することが可能であるため、学位詐称の問題を解決できる
- 3) ブロックチェーンを活用することで、特定の管理者による不正を防止することができる
- 4) ブロックチェーンには、サーバダウンの概念が存在しないため、記録したデータは 24 時間 365 日検証可能である

⁴⁵ <https://gradba.se/en/>

GradBase の独自調査によると、卒業証明書の発行者が負担する管理コストは、GradBase のサービスを使用することで大幅に削減することができるという。1つの例として、イギリスを拠点とする大学の卒業証明書の管理コストを取り上げる。この大学では、毎日外部から請求される卒業証明書の検証処理を、3人の正社員を雇用することで実施しているという。正社員の平均給与は年間約 31,000 ポンドと推定され、3人分を合計すると 93,000 ポンドのコストとなる。他方、GradBase の場合、1件の卒業証明書の検証につき 2 ポンド必要である。毎年約 5,000 件の検証が行われると前提すると、年間 10,000 ポンドのコストが発生するといえるので、これを単純に 93,000 ポンドから引くと、約 80,000 ポンド以上のコスト削減が期待できると考えられる。また、これまで数週間の期間を必要としていた大学に対する卒業証明書の発行プロセスも、GradBase によって瞬時に実行することが可能になるという⁴⁶。

(4) インタビュー

GradBase CEO である Alberto 氏にインタビューを行った。

Q: 会社とサービスの概要について

GradBase はロンドンとミラノの2つの拠点を持っている。このプロジェクトは Alberto 氏が Imperial College London に在学中に始まったという。証明書やポートフォリオには、メールによって送られる唯一無二の QR コードが存在する。ポートフォリオは証明書のリストとして構成され、所有者は GradBase が運営するポートフォリオサイトにログインできるという。そこで、各証明書の QR コード又はポートフォリオ全体の QR コードをダウンロード可能であるという。各証明書の発行者は、ビットコインもしくはイーサリアム のウォレットを所持する必要がある。

Q: ビジネス面について

GradBase は現在、University College London と政府支援コンソーシアムのコーディング機関と共に、試験的なプログラムを実施中であり、イタリアのミラノでも Talent School Innovation School と共に研究を進めている。また、GradBase は、talent.io のようなリクルーターと積極的に連携することで、証明書の検証ツールとしてのプラットフォームを実装している。GradBase は、LinkedIn のプロフィールにおける専門的なスキルや経験に対して QR コードを埋め込もうとしている。これにより、それぞれの人材が持つスキルや経験が正しいものであるかどうかを確認することができるのだという。しかしながら、証明書を検証する上で、各国における使用言語の違いが障壁になると考えられる。例えば、採用場面において、雇用主が自身の国以外の言語で書かれた証明書を検証することは困難な状態になっている。なぜなら、そもそも証明書を読むことができず、仮に読むことができたとし

⁴⁶ Gradbase Medium post: <https://medium.com/gradbase-blog/how-top-universities-in-the-uk-could-be-70k-better-off-every-year-with-blockchain-based-diplomas-ba8224c79fd5>

ても、情報の信憑性を確かめる方法がないのである。この問題に対しては、デジタル証明書による解決が期待できると考えられる。

7.1.5. 事例④「University of Birmingham」

(1) プロジェクトの概要

バーミンガム大学⁴⁷は MIT Media Lab の Blockcerts を改善し、卒業証明書の認証と卒業証明書失効の信頼性の向上を目指した論文⁴⁸を発表している。卒業証明書の改ざんや第三者からの検証コストの改善等、長年問題視されている。これらの問題を解決することを期待して様々なプロジェクトが立ち上がっているが実際の運用までは至っていないと考えられる。バーミンガム大学の取り組みでは、MIT Media Lab の Blockcerts に対して独自のマルチシグ機能を実装し、運用上の安全性等の向上を目指した。

(2) プロジェクト詳細

卒業証明書の偽造問題は教育業界における長年の課題となっている。MIT Media Lab は、ブロックチェーン上にローカルファイルのハッシュ値を書き込むことによりこの問題に対してアプローチをしている。しかし、この MIT Media Lab の Blockcerts にも課題が残っており、バーミンガム大学では独自に改善案を提案し、Blockcerts ver1.0、Blockcerts ver2.0 を比較検討することにより、それぞれの優位性を明らかにしている。

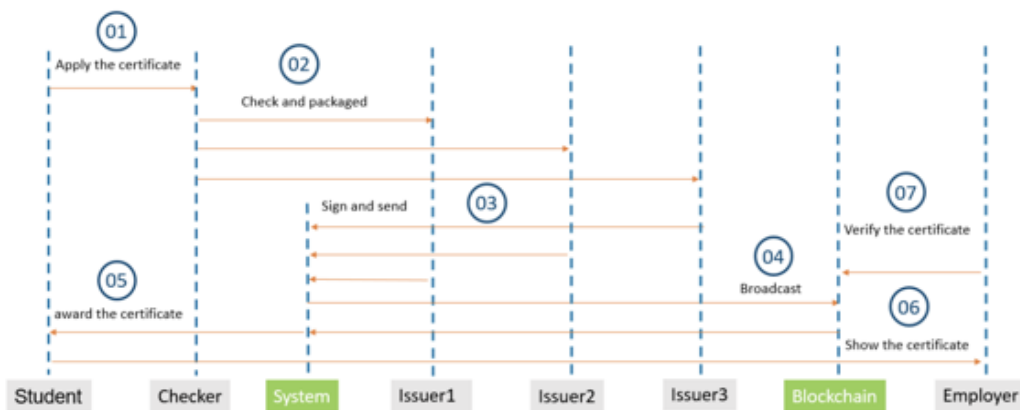
主な改善案として、Blockcerts はブロックチェーンに卒業証明書を記述するのに必要な署名が1つであるのに対して、バーミンガム大学の場合は、複数の機関が署名するマルチシグの仕組みを採用している。これは、セキュリティのシステム改善を目的にしていると考えられる。

「図表 7.1 - 6」は、プロトタイプのワークフローを表している。マルチシグの仕組みを取り入れることによって、本来1つしかなかった issuer(発行機関)が3つに増えていることが確認できる。

⁴⁷ University of Birmingham Blockchain Laboratory: <http://www.bccert.org/>

⁴⁸ Blockchain based Academic Certificate Authentication System Overview:

<https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf>



図表 7.1 - 6 ワークフロー⁴⁹

プロトタイプワークフロー

- 1) 生徒は学校に対してクレデンシャルを渡す
- 2) 学生の情報をチェックし、クレデンシャルとブロックチェーントランザクションをパッケージ化する
- 3) 教育機関のメンバーがプライベートキーで署名をする
- 4) 署名後、ブロックチェーンにブロードキャストする
- 5) 生徒は JSON 形式のデジタル卒業証明書を受け取る
- 6) 生徒は就職活動の際に、企業に対してデジタル卒業証明書を提出する。
- 7) 企業は、受け取ったデジタル卒業証明書をブロックチェーンに問い合わせ、検証する

※ブロックチェーンにブロードキャストする仕組みは、Blockcerts と同様に Merkle Tree を利用している。

(3) マルチシグの実証実験

バーミンガム大学では、マルチシグの性質の確認とセキュリティに関する評価を実施している。ここでマルチシグとは、 $M | N$ の条件を満たす署名が必要な仕組みである。N はトータルの公開鍵の数で、M は最低必要な秘密鍵の数を示します。M は変数で N は定数になる。

実験を 2 つ実施している。

実験 1

実験内容は、以下の通りである。

- 1) 公開鍵 M の数を、5, 7, 9, 11 とする 5 つのグループを作成する

⁴⁹ ワークフロー <https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf>

- 2) それぞれのアドレスを a0, a1, a2, a3, a4 とし、その全てに対して 2 つの秘密鍵が必要なマルチシグの条件を定義する
- 3) 2 つの秘密鍵を使用して全ての未処理のトランザクション文字列に署名し、指定されたアドレスへの支払いを行うためにそれらをブロードキャストできるか測定する

結果は以下の「図表 7.1. - 7」の通り、全ての条件に置いてトランザクション処理が成功したという結果が返ってきた。

Addresses	Required Number M	Total number N	Executed results
a0	2	3	Accepted
a1	2	5	Accepted
a2	2	7	Accepted
a3	2	9	Accepted
a4	2	11	Accepted

図表 7.1 - 7 実験 1 の結果⁵⁰

実験 2

実験 1 に対して、公開鍵 M の数を 7 に統一し、秘密鍵 N の数を 1 から 6 の範囲で変更した。このとき、署名する秘密鍵の数は 2 つである。結果は以下の表 2 の通りとなった。

Addresses	Required Number M	Total number N	Executed results
a0	1	7	Accepted
a1	2	7	Accepted
a2	3	7	Rejected
a3	5	7	Rejected
a4	6	7	Rejected

図表 7.1 - 8 実験 2 の結果⁵¹

これら 2 つの実験結果は、マルチシグの具体的な性質を示すことに他ならない。つまり、N の数に関わらず M の数が指定の数に揃えば、トランザクションの処理が実行されるということである。

マルチシグを使わない Blockcerts の場合、秘密鍵が漏洩したり紛失したりした際に対処できなくなってしまう。しかし、この問題に対してバーミンガム大学のアプローチであれば、対処することが可能であると考えられる。もし、7 つ用意している秘密鍵のうち 2 つが漏洩したとしても、残りの 5 つの秘密鍵を使うことで、漏洩した秘密鍵のアカウントを削除するといった対処ができると考えられるからである。

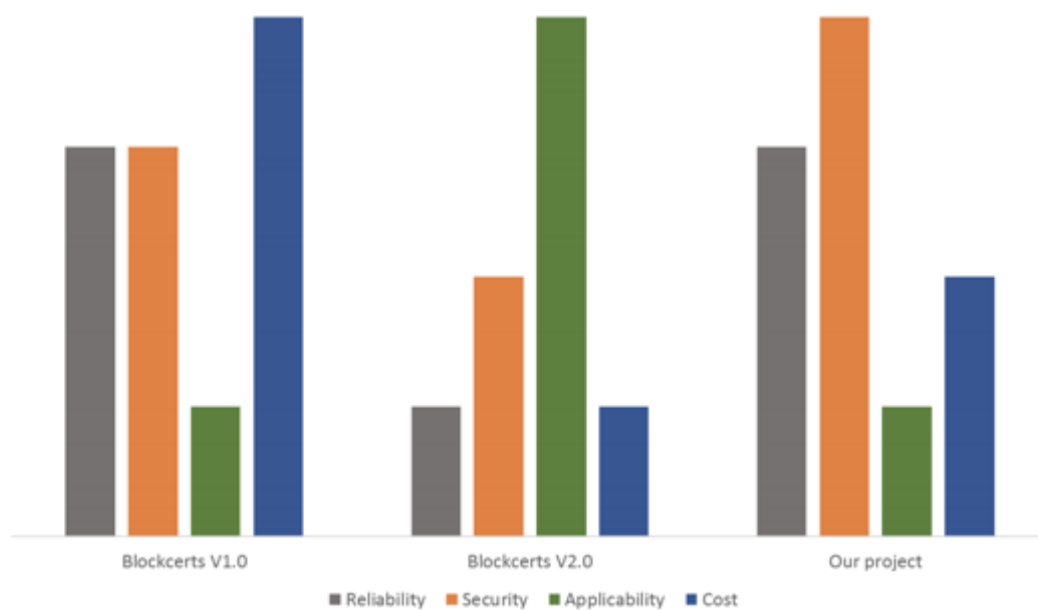
⁵⁰ 実験 1 の結果 <https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf>

⁵¹ 実験 2 の結果: <https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf>

よって、 $M > N / 2 + 1$ でマルチシグの値を設定することは、セキュリティの向上に繋がるとバーミンガム大学は結論づけている。

(4) 比較検証

バーミンガム大学は、信頼性(reliability)、セキュリティ(security)、適用可能性(applicability)、コスト(cost)の4つの指標でBlockcerts v1.0、Blockcert ver2.0、バーミンガム大学のプロジェクトをそれぞれ比較し、検証を実施している。



図表 7.1 - 9 3つのプロジェクトの比較表⁵²

信頼性(reliability)の指標は、Blockcertsv1.0とバーミンガムのプロジェクトは同じ評価となっているが、Blockcertsv2.0は低評価になっている。この理由は、前者の2つは全てをビットコインブロックチェーン上で行っているためであると考えられる。Blockcerts v2.0は、固定URLに基づく卒業証明書失効リストを採用している。両者を比較した場合、ビットコインのトランザクション状態は、URLを介して証明書を照会するよりも安定していると考えられるのである。

セキュリティ(security)の指標では、バーミンガム大学のプロジェクトが最も高い評価となっている。その理由は、ブロックチェーン内のトランザクションの検証が安定し、失効したアドレスもウォレット内に存在することにより、安全であると判断できるためである。Blockcerts ver1.0の証明書

⁵² 3つのプロジェクトの比較表 <https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf>

状態照会サービスはインターネット上に存在するため、ハッキングされる危険性を排除できない。また、最もセキュリティ上の観点で問題を抱えていると判断された Blockcerts ver2.0 は、発行機関が全ての秘密鍵を保管している点が理由であると考えられる。

適用可能性 (applicability) の指標では、Blockcerts ver2.0 の評価が高くなっている。これは、Blockcerts ver2.0 が既に一般的に広く受け入れられているためである。

コスト (cost) は、Blockcerts ver1.0 が最も低い評価を受けている。その理由は、卒業証明書を失効させるのに少なくとも 2 回分のトランザクション手数料が必要であるからである。一方、Blockcerts ver2.0 はトランザクション手数料を発生させない点で最もコスト効率がいい。バーミンガム大学のプロジェクトは、卒業証明書を失効させるごとに 1 回のトランザクション手数料が必要である。

以上より、このプロジェクトの目的であったセキュリティ上の向上に関しては、Blockcerts を超えたとバーミンガム大学は言及している。

また、バーミンガム大学は以下の SWOT 分析を実施している。

<p>STRENGTHS</p> <ul style="list-style-type: none"> ➤ Proposed an innovative BTC address based solution to revoke a certificate which is more reliable. ➤ Utilizing multi-signature rather than the single private key makes the academic certificates issuing progress more secure. ➤ The authentication data of the credential which published to blockchain is immutable, trustful and verifiable. ➤ The new approach of authenticating the certificate(scan the QR code) simplified the workflow to efficient and economical. ➤ The core data of the credential is secure and private even the blockchain technology crashes in the future. 	<p>OPPORTUNITIES</p> <ul style="list-style-type: none"> ➤ The Blockchain technology has evolved and has given various opportunities for other industries such as banking and finance, manufacturing, healthcare. Blockchain has the potential to transform education industries(academic certificate as an example) and make processes more efficient, transparent democratic and secure. ➤ The Blockchain is intended to help us create the digital relationship that will reshape the world of business and transform the old order of human affairs for the better. ➤ At the university, the blockchain technology can not only be used at the certificate authenticating, but also be used at the statement of official documents or files and other areas.
<p>WEAKNESSES</p> <ul style="list-style-type: none"> ➤ In the phase of the multi-signature, the member of the academic committee member needs to remember the private key. However, the private key is a format of some irregular hexadecimal characters which is hard to remember. ➤ In the phase of broadcasting the certificate authentication data to the blockchain, the university should pay a few mining fees for the miner to confirm it on the blockchain. ➤ The broadcasting API using in our project has a potential that it is not available in the future. 	<p>THREATS</p> <ul style="list-style-type: none"> ➤ Nowadays, the applications related to the blockchain technology are still in the experimental phase. ➤ The blockchain technology is not widely accepted by the public now since most of the people trust 3rd organization. ➤ Our project is based on the Bitcoin blockchain, the maintenance of which relies on thousands of participants in the cryptocurrency ecosystem. Admittedly, it is imprudent to assume that the Bitcoin would work well continuously in the future because multiple types of stakeholders influence the blockchain ecosystem or business model.

図表 7.1 - 10 バーミンガム大学のプロジェクトの SWOT 分析⁵³

⁵³ バーミンガム大学のプロジェクトの SWOT 分析: <https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf>

7.1.6. 事例⑤「Open University」

(1) プロジェクトの概要

OpenUniversity⁵⁴は、イギリスの通信制の公立大学である。1969年に設立されて以降、アカデミックコースを1,000個以上提供し、現在も20万人近くの学生が在籍しているという。

この大学の研究機関である Knowledge Media Institute (KMI)⁵⁵は、3年前にブロックチェーンの研究グループを発足した。

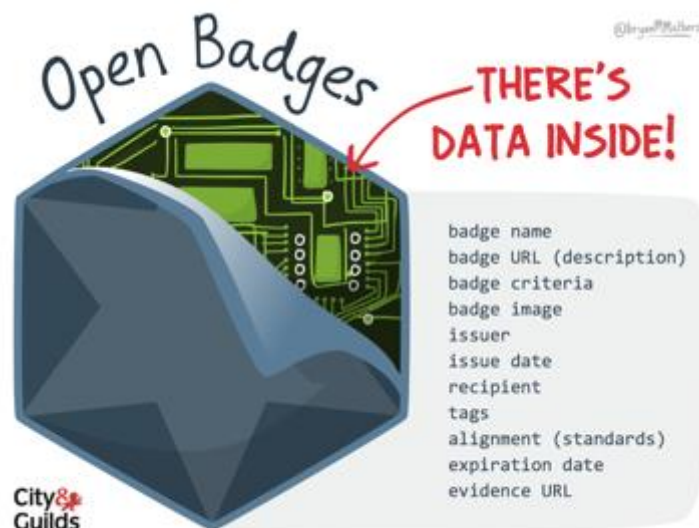
研究目的はブロックチェーンの教育への適用可能性の検証である。OpenBadges⁵⁶の規格に準拠し、個人の学位や資格をインターネット上に公開し、企業に対して最適な人材を見つけやすくするマッチングサービスの実証実験を行なっている。

(2) プロジェクトの詳細

Open University のプロジェクトは、個人の学位や資格に相当するメタ情報を Open Badges に準拠した状態でブロックチェーンに記録している。

Open Badges⁵⁷とは、Open Badges Specification⁵⁸に準拠している規格のことである。スキルや実績に関するメタ情報を格納し、検証可能なポータブルデジタルバッジとして機能する。Open Badges は、Web 上で管理・共有できる。

Open Badges のイメージを「図表 7.1 - 11」で示す。



図表 7.1 - 11 Open Badges のイメージ⁵⁹

⁵⁴ Open University: <https://blockchain.open.ac.uk/>

⁵⁵ Knowledge Media Institute (KMI) : <http://kmi.open.ac.uk/>

⁵⁶ Open Badges 2.0: <https://medium.com/openbadges/open-badges-2-0-b7f67d2c3191>

⁵⁷ Open Badges : <https://openbadges.org/>

⁵⁸ Open Badges Specification : <https://github.com/IMSGlobal/openbadges-specification/issues>

⁵⁹ Open Badges のイメージ : <https://openbadges.org/get-started/issuing-badges/>

学位・資格等に相当するバッジは、以下のような情報を格納することができる。

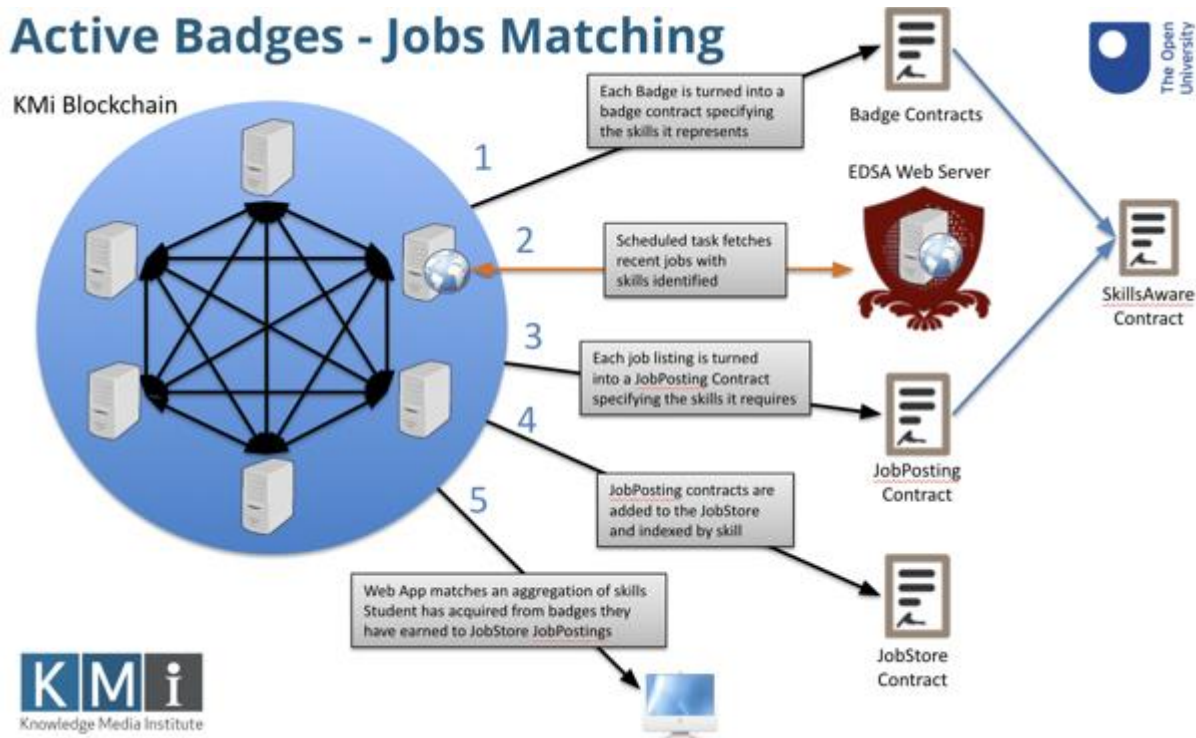
- バッジの名前
- バッジの URL (説明)
- バッジの評価
- バッジの画像
- 学位・資格等の発行者
- 発行日
- 学位・資格等の受取人
- タグ
- 規格
- 有効期限
- 証拠になる URL

また、Open Badges には extension の機能も存在するため、追加情報を格納することも可能である。追加情報として発行者はプロフィールを作成できるため、公式な機関も非公式な機関も、Open Badges を発行することができる。

Open Badges によって、これまで評価されていなかった様々な教育機関の資格に価値を与え、バッジを集積させることができるようになったと言えるだろう。Open University では、この性質を利用することで、個人のもつ学位や資格等のスキルと企業の求める求人のスキルの、マッチングを実現するサービスの実証実験を行なっている。

このマッチングサービスでは、学位や資格の情報を Open Badges に準拠した状態でブロックチェーンに記録し、バッジとして発行している。バッジはスマートコントラクトによって制御され、ウェブサイト上で表示、検索可能な状態で管理する等、企業が求めるスキルとその人の経歴やスキルのマッチングを図ることも可能である。

(3) 仕組み



図表 7.1 - 12 基本フロー⁶⁰

- 1) Badge Contracts は、学位や資格等のスキル情報が格納されたバッジを発行することで、SkillsAware Contract に継承する
- 2) EDSA WEB API を使用し、定期的にジョブを確認するスケジュールを組み込む
- 3) 企業の求人情報は JobPosting Contract に変換され、SkillsAware Contract に必要なスキルとして登録される
- 4) JobPosting contracts は JobStore Contract に追加され、スキルを検索できるようにインデックスが付与される
- 5) 最後に、ブラウザに学生が獲得したバッジを集約し、それらを JobStore Contract に追加された求人情報とマッチングさせる

主要な Contract の役割

- JobPosting Contract は、EDSA から取得した求人情報を保持する。
- SkillsAware Contract は、badge contract と Job Posting Contract の両方に継承され、それぞれのスキルリストを保持する役割を担う。
- JobStoreContract は、全ての求人情報を保持しつつ、スキルごとに検索できるようインデックス付けされる。

⁶⁰ ハッカソンで実施したワークショップにて投影された資料より抜粋

学生が使用するツールとしてブラウザを採用しているのは、badge contract に JobPosting Contract の情報が含まれると、コードが solidity のバイナリの許容範囲を超えてしまうため、ブロックチェーンに記録できない状況になってしまうことが理由であるという。なお、将来的には Hyperledger でこの実証実験を再試行する可能性があるとしている。

最後に、マッチングサービスの実際のブラウザ画面を以下に掲載する。インターフェースには、顔写真等の個人情報と資格情報が掲載され、Full Match to Skills や Partial Match to Skills の欄に、求人情報と本人のスキルによるマッチング結果が表示されるシステムとなっている。



図表 7.1 - 13 学生が実際に使用するブラウザ画面⁶¹

7.1.7. 事例⑥ 「uPort」

(1) プロジェクトの概要

uPort⁶²は資格や職歴、学歴等あらゆる情報をブロックチェーン上に記録し、学位や資格等を所有する本人が、自身で管理可能な自己主権型アイデンティティの取組を実施しているオープンソースプロジェクトである。uPort は、スマートコントラクトとライブラリ、そしてモバイルアプリケーションの3つで構成されている。

⁶¹ ハッカソンで実施したワークショップにて投影された資料より抜粋

⁶² uPort.me: <https://www.uport.me/>

モバイルアプリケーションはユーザの鍵を保持する役割を果たす。スマートコントラクトは、端末を紛失した場合に持ち主のアイデンティティを復元するための役割を果たす。最後、ライブラリは、uPort を使ってサードパーティ製品を開発可能にする役割を果たす。

(2) プロジェクトの詳細

uPort は「すべての人に分散型アイデンティティを提供する」ことを目的とした、オープンソースの分散型アイデンティティフレームワークである。自己主権型アイデンティティと呼ばれる、個人が中央集権的な組織に縛られずに自らアイデンティティを管理する世界の実現を目指している。そのため uPort の提供するアイデンティティ（以下「uPort アイデンティティ」⁶³）は、様々な形式に対応できるように設計されている。例えば、個人やデバイス、エンティティ、機関といったものがあげられる。uPort アイデンティティは自己主権型であるため、アイデンティティの持ち主が自身で全て管理し、検証の際に中央集権的な第三者が不要な設計となっている。

uPort アイデンティティは、複数のスマートコントラクトによって制御されている。スマートコントラクトに対して、秘密鍵の管理やデータ格納の仕方等、様々な機能を組み込んでいる。

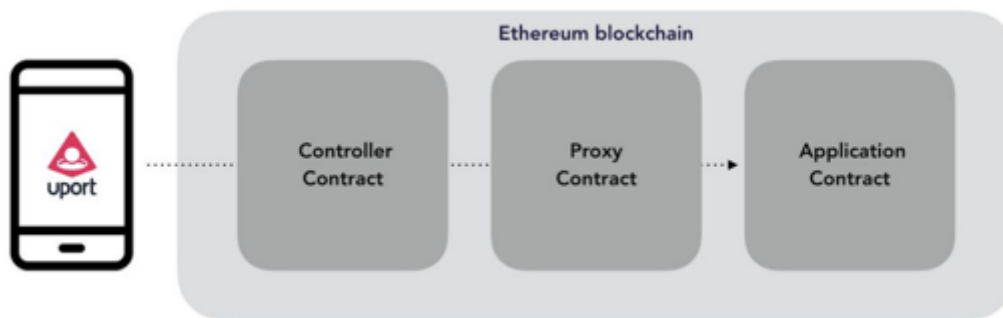
(3) 仕組み

uPort アイデンティティの中核を成すのは、uPort ID である。この uPort ID は、Controller Contract と ProxyContract によって制御され、登録した学位・資格等の情報に紐づいている。この uPortID は、登録する情報ごとに作成され、ProxyContract のアドレスによって管理されている。また、Controller Contract のみが Proxy Contract を呼び出すことができるという。

新規に uPort ID を作成する手順を以下で紹介する。

- 1) ユーザが使用する uPort モバイルアプリケーションで、非対称の新たなキーペアを作成する。
- 2) 新しく作成された公開鍵への参照を含む、Controller のインスタンスを作成するトランザクションを、Ethereum に送信する。
- 3) 作成した Controller Contract アドレスへの参照を含む、新たな Proxy が作成される。

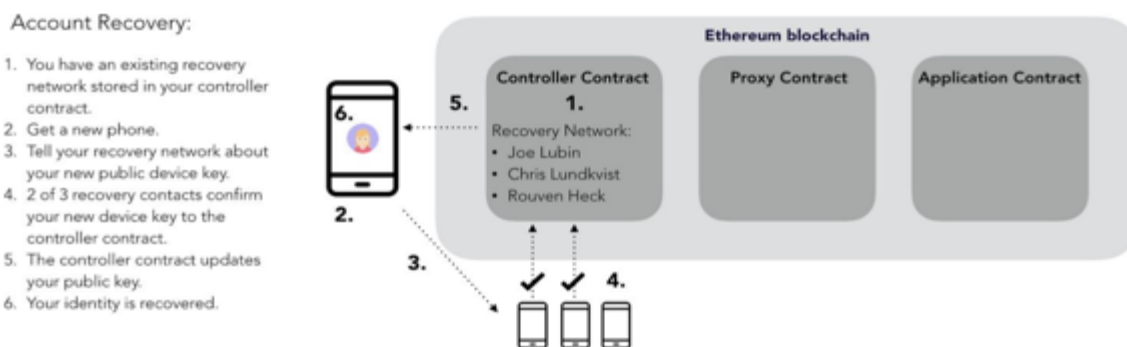
⁶³ UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY: http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf
A First Look at Identity Management Schemes on the Blockchain: <https://arxiv.org/pdf/1801.03294.pdf>



図表 7.1 - 14 スマートコントラクトのアーキテクチャ⁶⁴

ProxyContract に uPortID を持たせる目的としては、秘密鍵を紛失した場合に対応するためであると考えられる。ProxyContract を参照するためには、スマートフォン等のデバイスに保管されている秘密鍵を参照しなければならない。しかし、もし秘密鍵を保管していたデバイスを紛失した場合、uPort ID の参照ができなくなるのである。

この問題に対して uPort は、ControllerContract に uPort ユーザのアカウントの復元を目的とした、リカバリーデリゲートのリストを作成できるようにすることで対応している。このリストは、本人の知り合い等を複数人設定し、そのうち特定の人数以上が復元を承認した場合のみ、紛失した秘密鍵を新しく作成した公開鍵に置き換えることができるという。このプロセスにより、ユーザは秘密鍵を紛失した場合でも、永続的に uPort ID を維持することができると考えられる。



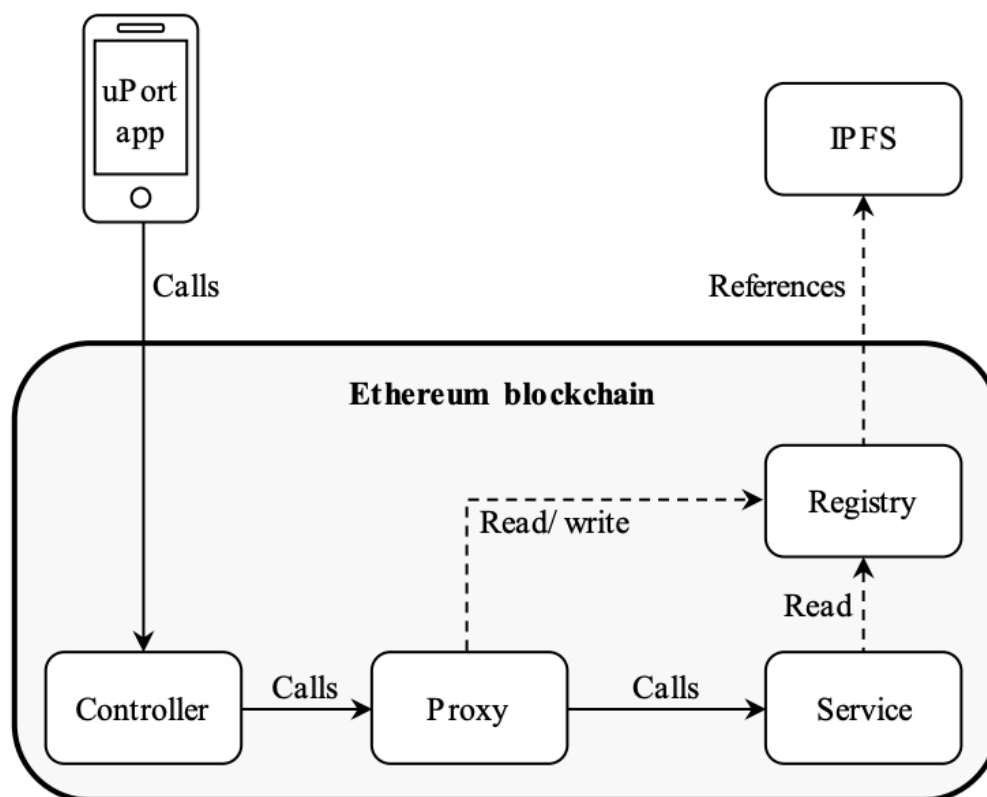
図表 7.1 - 15 アカウントの復元フロー⁶⁵

最後に、スマートコントラクトで管理するデータの向きや不向きについて説明する。スマートコントラクトでは、学位や資格情報等の大量のデータを管理するのは不向きであると考えられる。そのため uPort では、グローバルな情報を保管するスマートコントラクトとして、Registry Controller を活用する設計となっている。データ自体は IPFS と呼ばれる分散ファイルシステムに格納し、暗号化ハ

⁶⁴ スマートコントラクトのアーキテクチャ : http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

⁶⁵ アカウントの復元フロー : http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

ッシュの仕組みを活用することでファイルを安全に管理することができる。RegistryにはJSON属性構造のハッシュ値のみを格納する。



図表 7.1 - 16 全体フロー⁶⁶

7.1.8. 事例⑦「e-scroll」

(1) プロジェクトの概要

e-scroll⁶⁷は、ブロックチェーン基盤の卒業証明書を発行することで、学位の真正性を確保するために発足されたプロジェクトである。マレーシアの Ministry of Education (MoE) を中心に国内の6つの大学と連携することで、学位の管理等を行うコンソーシアム型のブロックチェーン基盤を構築している。

(1) 背景

マレーシアでは、不正な学位や卒業証明書が闇市場で販売されるという問題が深刻化しており、大学の発行している認定資格の評判と完全性を守るための措置を講じる必要があると判断。マレーシアの大学では、卒業生を確認するために世界中から数千件に及ぶ要請を受けているが、そのプロセスは依

⁶⁶ 全体フロー : <https://arxiv.org/pdf/1801.03294.pdf>

⁶⁷ Ministry of Education in Malaysia : <https://www.moe.gov.my/index.php/en/arkib/pemberitahuan/2018/4587-kenyataan-media-kpm-lancar-sistem-e-scroll-menggunakan-teknologi-blockchain-atasi-masalah-ijazah-palsu>

然として電話や電子メールで行われており、非常に効率が悪いといえる。そのため、Ministry of Education (MoE) を中心にマレーシアの6つの大学で構成された、コンソーシアム型のブロックチェーンを活用することで、問題の解消や業務の効率化に取り組んでいる。このブロックチェーンは、マレーシア国際イスラム大学 (IIUM) の教授が率いるグループと、資産の真正性と所有権を保護することを可能にするソリューションプロバイダーである LuxTag⁶⁸との連携によって構築されている。プロジェクト名は e-Scroll であり、プロトコルは NEM を採用している。

(3) インタビュー

Q: e-scroll がどのようなサービスについて

A: このシステムは、学生の身元をプライベートブロックチェーンのパブリックアドレスに結び付けることによって、ブロックチェーン公証の概念を活用する。生徒の情報をシステムに入力し、各生徒にブロックチェーンアドレスを発行。これらのブロックチェーンアドレスのパブリックアドレスは、大学の卒業証書に追加される。その後、パブリックアドレスとプライベートブロックチェーン上のすべての詳細を指す QR コードを読み取ることができるアプリケーションを作成。これには、過去の卒業生リストのデータ操作を防ぐための大学の卒業証書の作成に関するタイムスタンプが含まれる。その後、雇用主（又は証明書を検証したい一般市民）は、実際の大学の卒業証書のデータが、ブロックチェーンの情報と一致しているかどうかを検証できる。

Q: NEM の Apostille の基盤について

LuxTag の技術は、我々が特許を取得した NEM の Apostille⁶⁹における拡張版に相当。

Q: コンソーシアム型のブロックチェーンを採用した背景

システムをコンソーシアムで実装する必要はないが、1つのプラットフォーム上でシステム上の統治教育機関（マレーシアでは、教育省）への可視性を高めることを強くお勧めする。マレーシアの事例では実装していないが、MoE に大学発行の証明書への署名を要求する等、マルチシグを使用するようにシステムを設計できる。

このコンソーシアムはまた、彼ら全員が潜在的に独自のブロックチェーンノードを実行しているので、より強固で安全なシステムを提供し、不正なノードによる攻撃が発生する可能性を減少できる。さらに、1つのコンソーシアムでシステムを構築することで、e-scroll 以外にも、支払いシステムやマイクロコースのトークン化、教育資金の調達、及び LuxTag とは無関係に大学が開発できる多くの新たな活用事例が生まれてくることを期待。

⁶⁸ LuxTag : <https://luxtag.io/>

⁶⁹ Apostille : <https://nem.io/project/apostille/>

このシステムは大学ごとに別々のネットワーク上で実行可能だが、ブロックチェーンによってセキュリティプラットフォームの将来的な使用例が提供され、ロックが解除されない。マルチシグの場合、大学の卒業証明書の発行が許可されている人、及び卒業証書発行を承認する必要がある人が業務ルール通りに処理することを管理できる。

Q: コンソーシアム型のブロックチェーンとしてマルチシグを採用している場合、6大学で署名をし合って対応しているのか

システムを稼働させるために必要な、最小限の大学の数は定義されていない。私たちの役割は、システムを安全に稼働させるために、プラットフォームに対して新たな大学を継続的に追加し続けること。データの管理については、データに関する業務上のルールを用意すること、必要に応じてデータを暗号化すること、新たなデータを追加する署名を所有すること、といった様々な管理方法を大学と連携して行うことになる。

7.1.9. 総括

海外においては学位履修履歴・職歴の真正性の確保や偽造・改ざんの防止を狙い、複数のブロックチェーン技術の導入事例が存在している。学位履修履歴・職歴に対するブロックチェーンの活用ポイントは、「改ざんが困難」「検証プロセスの簡略化、分散化」であると考えられる。Bitcoin等の基盤を利用することにより、大学自身が廃校になった場合にも学位のデータを保持し続けることが可能になり、ブロックチェーン技術の基盤を用いて発行された証明書は、世界中から検証することができる。電話やメールで発行機関へ問い合わせをし、検証を行っていたプロセスが、特定のウェブサイトにデジタル証明書をアップロードするだけで可能になった。また、偽造された証明書の検出もブロックチェーン上に登録された情報を照合することで可能になっている。

今後のより大規模な社会実装に向けた課題として、「忘れられる権利」や「利用しているブロックチェーン自体が終了した際のマイグレーション」「秘密鍵の管理」等が挙げられる。また、現状、各大学がそれぞれ違うブロックチェーンプロトコルや技術を利用している他、今後も様々なソリューションが創出されてくると想定される中、標準化等を通じて利用環境を整備する必要があると考えられる。

7.2. 「研究データの信頼性確保」テーマ

7.2.1. 背景

本章では、オープンサイエンス及びオープンデータ構想が一般化していくに伴い、研究プロセスがどのように変貌していくのか、データ不正問題はどのように解決されていくのか、以下に掲載する海外事例を元に考察を深めていく。今回調査した海外事例の選択基準は、次の通りである。

- 解決する課題が明確に述べられているもの
- 提供するソリューションが研究データの抱える課題を解決し得ると考えられるもの
- 大学や公的機関を含む何らかの組織及び人物が関係しているもの
- プロジェクトの概要が既に公開されているもの

また、研究データと一口にいても、科学分野や臨床試験、バイオメディカル領域等多岐に渡るため、海外事例ごとに、解決を目指す課題やプロジェクト開始背景をそれぞれ記載している。

いくつか本事業において議論した内容と各事例における見解に関して乖離が発生している箇所が存在している。ただ国際動向調査としては各プロジェクトの見解を事例としてそのまま記載している。

国名	プロジェクト名	テーマ	概要
アメリカ	TrialChain	バイオメディカル領域における研究データの管理	プライベートチェーンである MutliChain とパブリックチェーンである Ethereum を組み合わせることにより、秘匿性と耐改ざん性及び処理速度を確保した、ハイブリッド型のブロックチェーンプラットフォーム。
アメリカ	Enigma	プライバシーを保護した状態でのデータ管理	暗号化した状態でスマートコントラクトを実行可能。秘匿性の高い研究データの管理に利用される可能性が高い。
ドイツ	Data Management Hub	科学分野における研究データの管理及び二次利用の効率性・再現性の向上	研究データの二次利用やアクセシビリティを実現するためのデータ管理ソリューション。スマートコントラクトを活用することにより、多様化するステークホルダーの役割分担が明確化させることも期待できる。
ドイツ	Blockchain for Science	科学分野におけるデータ改ざんからの保護	信頼できる特定の第三者によって保護されたパブリック型のブロックチェーンを採用。研究データを研究者自身に帰属させ、出版社等による不正の防止を目指す。

不明 (アメリカ の非営利団 体が後援)	Dat	分散化されたデータガバ ナンスの構築	特定の管理者が不在の状態デジタルデータを 共有可能なプロトコル。リンクの破損や書き換 えによるデータの紛失を防ぐことができる可能 性が考えられる。
カナダ	Lyfescience	臨床試験における研究デ ータ管理	臨床試験におけるデータ管理の煩雑化やコスト の肥大化を解消するために、スマートコントラ クトを活用。データ転送の合理化や人力による データ入力ミス削減を目指す。Hyperledger Fabric を採用。

7.2.2. 事例①「Lyfescience」

(1) プロジェクトの概要

現在、臨床試験に実施するには数多くの障壁が存在しているといわれている。例えば、地理的に分散した複数の利害関係者間における合意形成をはじめ、厳格な管理体制や情報共有の不確実性等があげられている。また、データ管理における中央集権性やデータアクセスの複雑性、情報漏洩に対する監視体制の欠如も問題といえるだろう。これらの問題が存在している結果、臨床試験を実施する際に必要なコストは年々膨れ上がり、悪循環に陥っているといわれている。

この問題を解決するために、ブロックチェーンを活用した Lyfescience 社⁷⁰の開発が進み、PhUSE EU Connect⁷¹2018にてその論文発表している。Lyfescience 社では、製薬会社やその他の臨床試験関係者が被験者のデータや調査結果を安全かつ分散的に収集・管理する方法を実現するために、スマートコントラクトを使用して最適化及び自動化する方法を提供しようとしている。また、The Linux Foundation が主催するオープンソースのエンタープライズ向けブロックチェーンである Hyperledger を使用して、この概念を実証している。ブロックチェーンを活用することで、臨床試験におけるデータ転送の合理化や、臨床試験参加者間でのリアルタイムなデータアクセスの実現、手作業によるデータ入力ミス削減、及び臨床試験監査とコンプライアンスプロセスの簡素化を実現できると考えられる。また、臨床試験に留まらず、ブロックチェーンは医療領域のエコシステム全体における、コラボレーションの実現とデータ共有の新たな方法を提供する可能性がある。

(2) プロジェクトの詳細

現状の環境下で臨床試験を実施するには、地理的に分散している複数の利害関係者によるコミュニケーションの円滑性や高いレベルを維持した監視体制、情報共有の正確性といった困難を極める要素が必要になるという。また、以下のような課題も解決できていないといわれている。

⁷⁰ LyfeScienc : <https://www.lexjansen.com/phuse/2018/tt/TT11.pdf>

⁷¹ PhUSE EU Connect : <https://www.phuse.eu/>

データ管理

- データのアクセス権は、データベースの管理者に委ねられている。
- 研究所やベンダー等、様々なデータソースを元にデータが作成されている。データは多種多様なシステムに格納されているため、必要なデータに繰り返しアクセスするのが非常に困難。従って、ごく単純な調査をするだけでも、レポートを作成するのに膨大な時間がかかっている。
- データ管理体制がアナログであるため、データ入力が手作業になっている。多くの調査担当者は、データをリアルタイムで分析するためのツールを持っていない。
- 規制緩和が進まず、データの使用に関する適切な権限が調査担当者に与えられていない。

データの共有とセキュリティ

- 機密情報の漏洩や詐欺、悪用防止の体制が不十分。
- 複数人によるデータの検証ができていない。
- データを共有する際に、該当する当局の規制に準拠した方法であるか確認する必要がある。

被験者データの登録

- 適切なボランティアを活用し続ける体制が整っていない。
- 被験者に対するインセンティブが不足しているため、研究参加の意義が感じられない。
- 被験者の安全性の確保体制が十分ではない
- 被験者が、被験者として参加したいと思っても、研究そのものを見つけることが困難。

悪循環にあるコスト

先述の問題を解消できないために、臨床試験を実施する際に発生しているコストは日々膨れ上がっているという。臨床試験の複雑さは増すばかりであり、比例してコストが肥大化している現状であると考えられる。そして、結果的に新たな革新性のある発見が誕生しにくくなるという、悪循環な状態に陥っていると考えられる。

この問題に対して、本プロジェクトは以下のブロックチェーンの特徴が活用できると考えている。

データの不変性

ブロックチェーンでは、各ブロックはハッシュ関数を使用して相互にリンクされている。いずれかのブロックのデータが改ざんされると、それ以降の全てのブロックのハッシュ値を更新しなければならない。この改ざん作業は確率論的にも証明されているため、臨床試験で扱うようなデータを記録しておくには、ブロックチェーンは最適であるという。

分散性及び非中央集権

ブロックチェーンは特定の権限によっては制御されない。臨床試験及び製薬業界におけるこの利点は、以下の通りであるという。

- データの複製：ブロックチェーンに記録されるデータは、多数のノードが全く同一のものを管理できる。
- 権限付与と所有権：ブロックチェーンのような分散されたシステムを活用することで、研究者自身が最新データを保持できる。

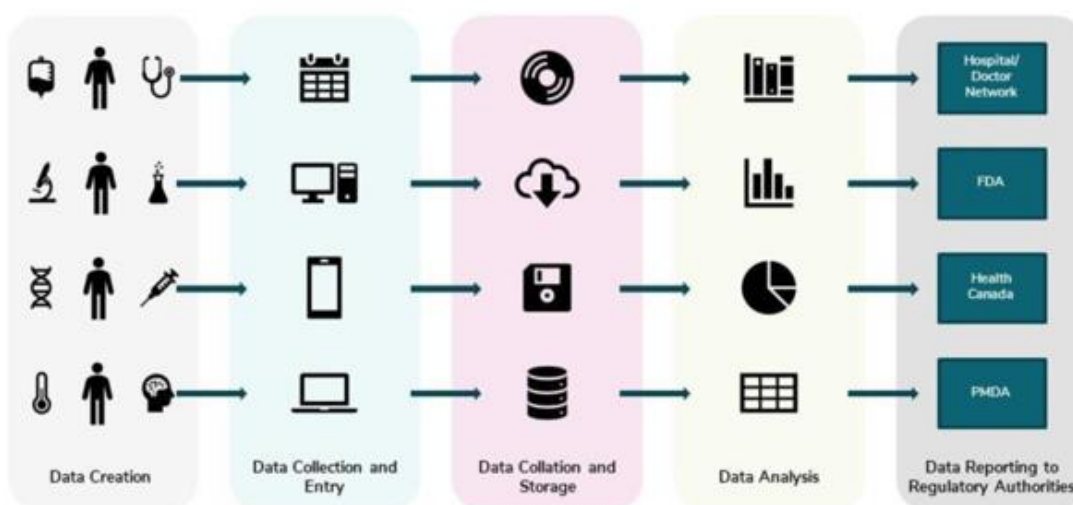
これにより、研究者がデータにアクセスする方法を確実に制御することができると考えられる。医療及び臨床試験等の分野では、プライベート型のブロックチェーン（以下プライベートチェーン）を活用することが望ましいという。プライベート型のブロックチェーンは、パブリック型のブロックチェーン（以下パブリックチェーン）の抱える、以下の3つの課題を解決すると言及している。

データのプライバシー

パブリックチェーンとは異なり、データはパブリックノードには保存されず、ネットワークの一部を構成する組織の管理するノードにのみ保存される。プライベートチェーンを使用することで、許可された組織及びエンティティだけがネットワークに参加することができ、ネットワーク上で特定の作業を実行できる。

コストとスピード

パブリックチェーンの管理には大量の電力消費が必要である。そのため、パブリックチェーンでの取引は遅くなり、コストも高くなる。プライベートチェーンの場合、パブリックチェーンと比較して高速かつ安価に運用することができる。

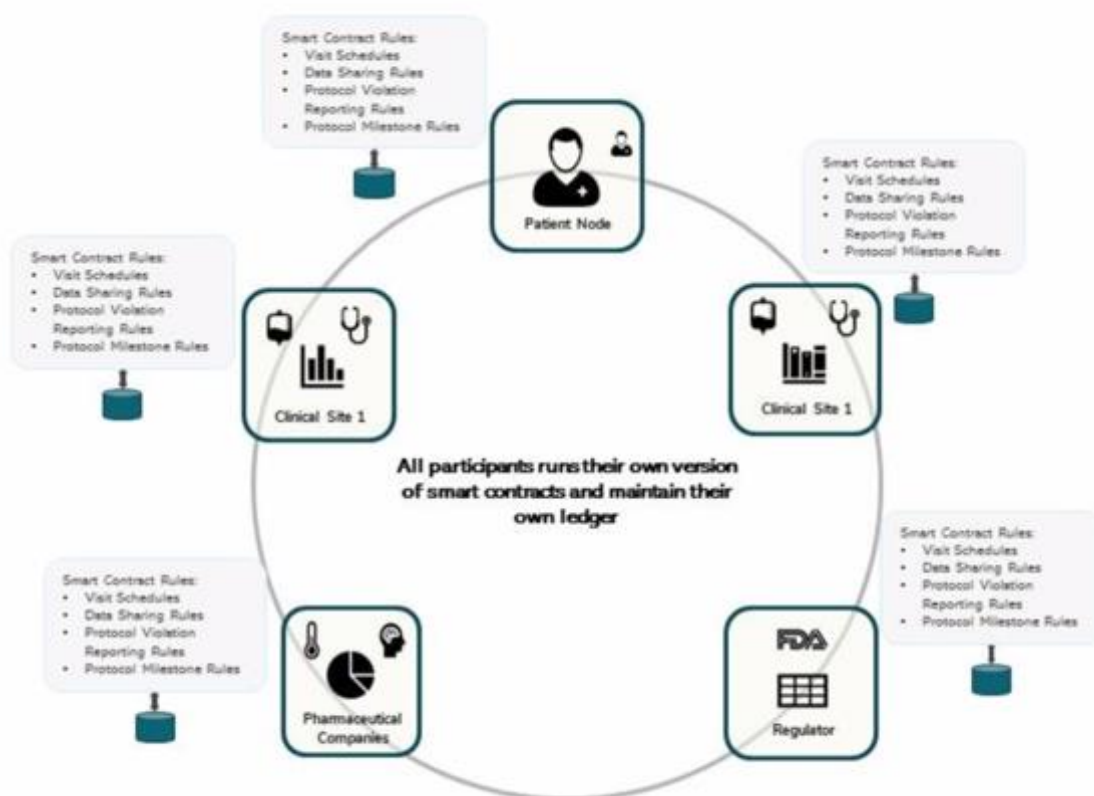


図表 7.2 - 1 臨床試験の様々な作業は互いに独立して行われている⁷²

⁷² <https://www.lexjansen.com/phuse/2018/tt/TT11.pdf>

まず、データは病院やスマートデバイス等の複数チャンネルから、複数の被験者に対して作成される。次に、作成されたデータが収集され、複数の組織ごとに完全に分離したデータベースに入力される。その後、複数の組織が独自のインターネット環境で、独自の方法及び独自の形式でデータを照合して保存する。そして、各組織内でデータが独自に分析され、最終的に結果のみが規制当局に提出されているという。Lyfescience 社の提案は、プライベートチェーンを活用し上記の問題を解決するためのソリューションであり、その特徴としては、以下があげられる。

- 臨床試験プロトコルに基づく、プログラム可能なスマートコントラクトを使用して、分散方式で臨床試験を実施できる。
- すべての利害関係者が、独自のローカルバージョン（プライベートチェーン）を更新でき、独自のバージョンのスマートコントラクトを実行できる。
- 組織内のノードは、独自のコンセンサスアルゴリズムを介して同期される。



図表 7.2 - 2 プライベートチェーンを構成するエンティティ⁷³

当該ソリューションの主な構成要素は以下である。

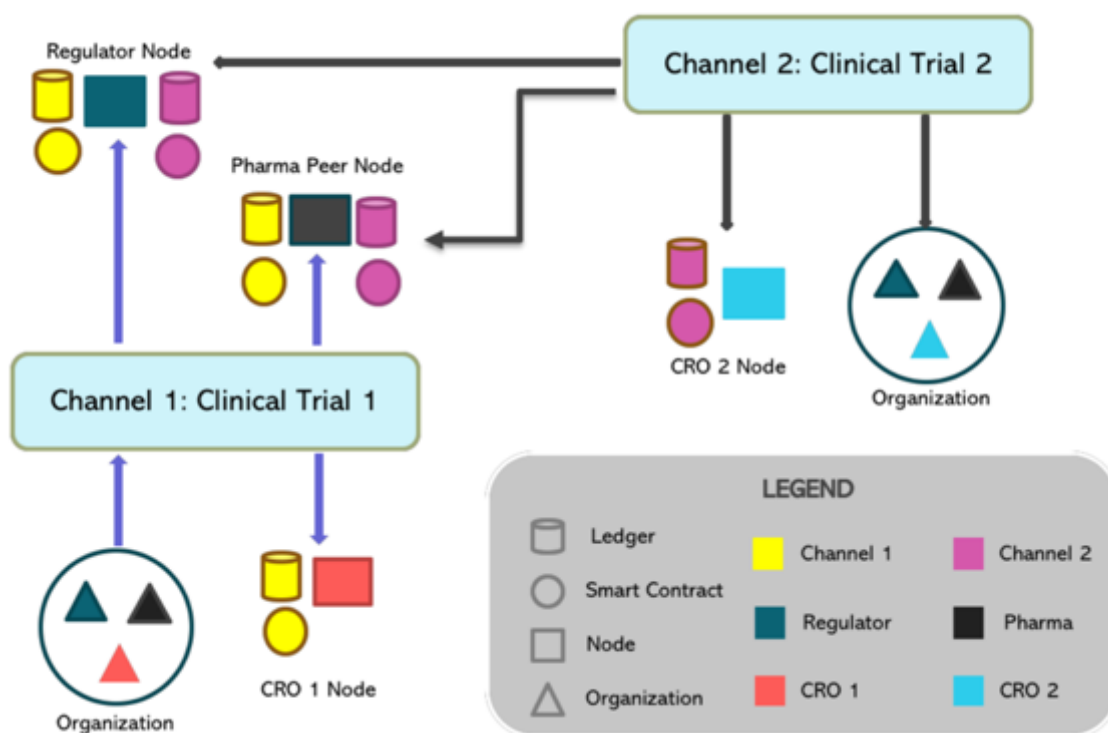
⁷³ <https://www.lexjansen.com/phuse/2018/tt/TT11.pdf>

組織内のノード

ここでいう組織とは、ネットワークに参加している事業者（製薬会社や規制当局、病院等）を意味する。

チャンネル

チャンネルは、各組織が内部で作成できるプライベートチェーンを意味する。各チャンネルには、複数の組織や異なる ID、データへのアクセスルール等を設定することができる。各チャンネルはプライベートネットワークとなっており、データはチャンネル内の参加者間でのみ共有される。



図表 7.2 - 3 2つのチャンネルから構成されているネットワークの例⁷⁴

上記の例においてチェーンには、2種類のデータの型を格納できる。1つ目はトランザクション履歴である。トランザクション履歴は、ネットワーク上の全てのトランザクション履歴のログを意味する。トランザクション履歴は、ネットワーク内の許可された全ての参加者を、リアルタイムで表示するために使用できる。2つ目はワールドステートである。ワールドステートは、チェーンの最新状態を管理する。新たなトランザクションが合意されて追加される度に、ワールドステートには最新のトランザクションが反映されるようになっている。

⁷⁴ <https://www.lexjansen.com/phuse/2018/tt/TT11.pdf>

ここからは、どのように臨床試験における課題を解決するのかについて説明する。

プロトコルの遵守と違反の検知

同社のアプローチは、データ管理におけるコンプライアンスを向上させることでプロトコルからの逸脱を防ぎ、監査を迅速化するスマートコントラクトを通じて、プロトコルをデジタル化する。例えば、被験者からの（デジタル署名を介して）同意がない場合、被験者のデータは入力できないようにする、といったスマートコントラクトを作成できる。また、一度被験者が同意した後に同意を撤回した場合、被験者によって再度同意があるまで、被験者データを更新することはできない、といったルールを決めることもできる。

データ共有や規制当局との連携

規制当局は、Lyfescience社のネットワーク上でノードとして機能するため、臨床試験の作成及び共有プロセス全体への即時アクセスと可視性を享受できる。規制当局は、独自のバージョンのチェーンを保有しているため、データ収集を他の製薬会社やヘルスケア事業者に依存する必要がなくなり、柔軟性の向上やコンプライアンス要件の緩和を実現できる。

被験者のプライバシー

プライベートチェーンは、データの安全な転送を可能にする。例えば、被験者が臨床試験の終了時に、自身のデータの所有権を即時取得できるように、スマートコントラクトを作成することが可能である。

最後に、臨床試験におけるブロックチェーン活用の際に浮上するであろう課題について、以下のよう
な点が考えられる。

- レガシーな既存 IT システムとの統合困難性
- 経験・知識共に豊富なブロックチェーンコンサルタント、プログラマ、インフラエンジニアを見つけるのが困難
- 規制が未整備な状況であるため、不確実性が充満している
- スマートコントラクトは法的強制力を有していないため、スマートコントラクトの執行力の欠如が懸念される
- オフライン環境でのデータ収集が困難
- 初期の導入コストが高い
- 最新のテクノロジーに対する業界の受容性の欠如
- 相互運用が不可能な複数のブロックチェーンが実装されると、エコシステムが細分化され、普及が制限される可能性がある

最新のテクノロジーに対する不信感と、変化に対する寛容性に適応するには、全ての利害関係者からの合意とそのため多大な努力が必要不可欠である。

7.2.3. 事例②「TrialChain」

(1) プロジェクトの概要

バイオメディカル領域における研究データの管理には、一般的に提供されているようなアプリケーションが使用されている。このようなアプリケーションには、特定の提供者及び管理者が存在するため、潜在的な不正が存在していないとは決して言い切れない状態であると考えられる。こういった問題に対しブロックチェーンのような新しい暗号技術を活用することで、データの不正操作や改ざんといった潜在的リスクを軽減し、研究データの信憑性を高めることができると考えられる。

TrialChain⁷⁵は、MIT 出身の Shada Alsalamah 氏と、MIT の教授であり Media Lab Entrepreneurship Program の Director を務める Alex 'Sandy' Pentland 氏によって構想された。TrialChain は、中国の北京にある NCCD が抱えるデータ管理問題を解決するために開発された。バイオメディカル領域における研究データは、秘匿性が高くパブリックチェーンに記録するのは適していないといえる。そのため、既存プライベートチェーンである MultiChain を採用することにしたという。研究データをプライベートチェーンである MultiChain に記録し、そのハッシュ値を TrialChain が受け取り、パブリックチェーンである Ethereum に記録するようにしている。こうすることで、研究データ自体の秘匿性は確保しつつ、ハッシュ値をパブリックチェーンに記録することによるデータの改ざんを困難にしている。

(2) プロジェクトの詳細

中国の北京にある National Center for Cardiovascular Disease (NCCD) は、2014 年に China PEACE Million Persons と呼ばれるプロジェクトが発足して以降、計 200 万人を超える患者のデータを管理してきた。このデータには、患者のアンケートの回答結果から医療機関の情報、エコー図、ゲノムシーケンスといった膨大な種類と量が含まれていると公表している。そのため、当然ながらデータ管理には厳格なガバナンス体制が必要となっている。

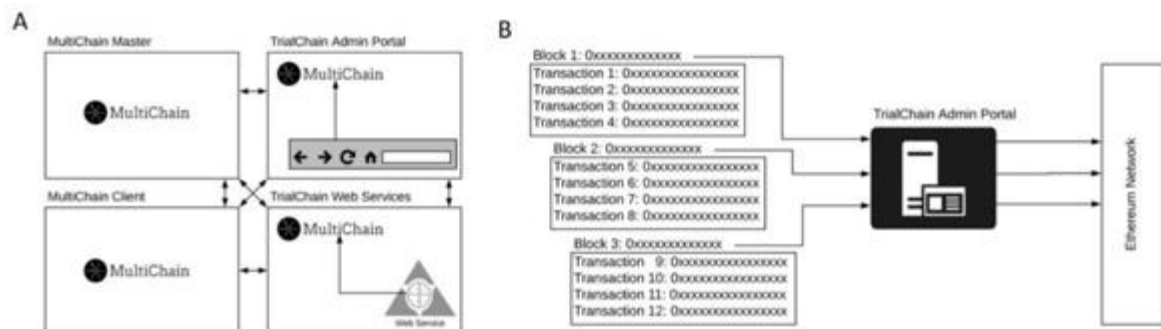
TrialChain はこの NCCD が抱えるデータ管理の問題を解決することをきっかけに誕生した。具体的には、NCCD の管理するデータサイエンスプラットフォーム (NDSP) に統合される形で誕生し、分散データ管理用の Hadoop クラスタと次世代シーケンス (NGS)、分析用の高性能コンピューティング (HPC) クラスタで構成されている。

⁷⁵ TrialChain : <https://arxiv.org/pdf/1807.03662.pdf>

TrialChain を構築する上で、収集したデータをログとして記録しておくためのプライベートチェーンが必要となり、既に存在していた MultiChain を活用することにしたという。プライベートチェーンの利点は、ネットワークに参加しているノードを承認できたり、ノードに特定の権限を付与することができたりする点にある。MultiChain はリモートプロシージャコール (RPC) のエンドポイントを公開することができる仕組みになっている。これはネットワーク内でのノード同士のやり取りに使用される。ネットワーク内のマスターノードは、TrialChain コンポーネントによる RPC を経由した接続に対して許可を与えることができるように構成されている図表 7.2 - 2 (A)。

先述の通り、MultiChain のクライアントノードは、マスターノードよりネットワークへの接続許可を管理されている。こうすることで、各アプリケーションを独立して動作させることができ、ノードに障害が発生した場合に備えてデータを各ホストに複製しておくことができるという。また、ノードの追加や削除、権限の変更等の全てのトランザクションはブロックチェーンに記録される。

MultiChain はプライベートチェーンである MultiChain に記録するデータの検証を行うために、プライベートブロックの状態を定期的に Ethereum に送信するよう設計されている。図表 7.2 - 4 (B) プライベートチェーンとパブリックチェーンの統合を実現するために、ローカルの Ethereum ノードを使って同期し、パブリックチェーンとプライベートチェーンの相互通信を可能にした。



図表 7.2 - 4 TrialChain のワークフローと一般的な Ethereum ネットワークとの統合⁷⁶

A) マスターノードが最初に立ち上がりブロックチェーンが作成されると、デフォルト権限が割り当てられる。その後、クライアントノードをローカルに追加したり、マスターノードによる適切な承認を得ることでリモートスポットにノードを追加したりできるという。TrialChain のサービスとしては、MultiChain のクライアントノードと共に個々の Docker コンテナ内に配置されることで、ローカルからの接続機能とデータ複製機能を提供する。

B) TrialChain の管理ポータルは、現在のチェーン状態 (state) を表す最新のブロックハッシュ値を、Ethereum のパブリックネットワークに対して定期的に同期する役割を担う。

⁷⁶ <https://arxiv.org/pdf/1807.03662.pdf>

プライベートチェーンとパブリックチェーンの検証作業が開始されると、パブリックチェーン側の Web アプリケーションによってプライベートチェーンとの接続が実施され、プライベートチェーンの最新のブロックハッシュを取得する。続いて、提供された外部 URL もしくはローカルの Geth ノードの JSON RPC API ポートを通して、Ethereum のパブリックネットワークとの接続が確立される。最後に、ローカルのブロックハッシュとその他のメタデータを含むトランザクションが作成され、ローカルの秘密鍵で署名される。

プライベートチェーンに記録するデータの検証を行うためのトランザクションでは Ether を必要としないが、Ethereum のパブリックネットワーク上でマイナーが検証を行うための Ether はわずかながら必要になるという。

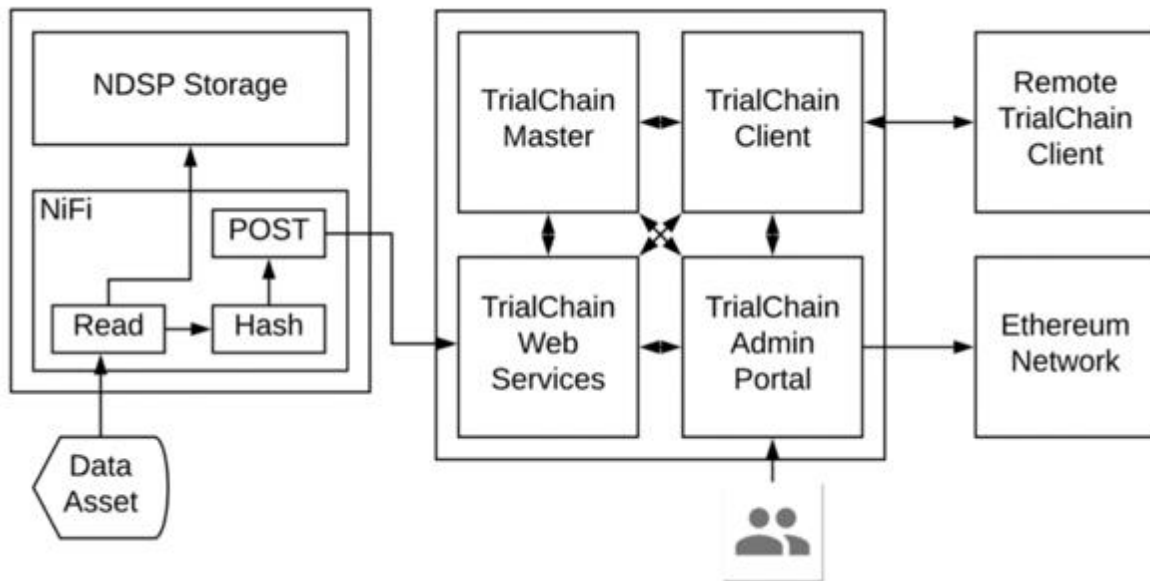
トランザクションに必要なコストは取引の前に試算されるため、残高が不足している場合には取引を実施することはできない。また取引実施後でも、ネットワークの接続を確立できない場合や取引のリクエストがハッシュ値を返さない場合等には、トランザクションは取り消される仕組みとなっているとのことだ。トランザクションの送信に成功すると、Web アプリケーションによって現在の時刻や送信されたブロックハッシュ値、トランザクションハッシュ値、及びウォレットアドレスをローカルの postgres データベースに記録する。

TrialChain のような新しいアプローチによって、研究結果を作成する際に使用するデータの信憑性を高めることができると考えられる。また、プライベートチェーンとパブリックチェーンを統合することで、ブロックチェーンを活用する際のコストを削減しつつ、依然として高いレベルの透明性と信頼性を実現することができるだろう。

プライベートチェーンである MultiChain は、ビットコイン等の一般的なブロックチェーンと同様、プルーフオブワークのコンセンサスアルゴリズムを採用し、トランザクション履歴を検証するためのノードで構成されているという。MultiChain はパブリックチェーンとは違い、マスターノードとして明示的に指定されているノードが存在し、マイニングの参加承認やブロックチェーンに記録されているデータへのアクセス許可を管理している。プライベートチェーンを利用することにより、実行に必要なソフトウェアを特定のバージョンに留めておくことができるようになる。そのため、パブリックチェーンの開発に必要なコンポーネントのアップグレードが必ずしも必要ではなくなると考えられる。また、トランザクションを処理するためのコストは、ブロックチェーンを作成する際に任意に設定することができるため、コンピューティングリソースを維持するためのコストだけでなく、トークンの使用料を無料にすることも可能であるという。

トランザクションを迅速に処理するために必要なコンピューティングリソースは、標準的な商用のデスクトップと小型の仮想マシンで実現可能であるという。なお、ブロックチェーン上のデータがプラ

イベントネットワークの外に拡散されることはないため、機密性の高いデータを記録することができると考えられる。



図表 7.2 - 5 TrialChain のアーキテクチャとワークフロー⁷⁷

TrialChainにデータを記録した後、ファイルのハッシュ値がTrialChainに送信され、ファイルそのものはNDSP内に保存される。TrialChain内の状態は、定期的にEthereumのパブリックネットワークに同期される。ユーザは管理ポータルを介してネットワークの状態とファイルの信頼性を確認することができ、リモートクライアントはデータの配布が行えるよう設定することもできるという。

プライベートチェーンの最新のブロックハッシュ値は、定期的に（一日に一回）Ethereumのパブリックネットワークにブロードキャストされる。Ethereumのパブリックネットワークを破壊することは事実上不可能であるため、プライベートチェーン内の全てのデータが、Ethereumのパブリックネットワークにブロードキャストされて以降、データが改ざんされていないことを検証することができるという。

NDSPでは、マスターノード以外にも外部ネットワークのノードも容易にサポートすることができるとのことだ。異なるインセンティブを持つ他のノードを同じネットワークに置くことで、個々の利害関係者による不正行為を防ぎ、共同作業間での信頼性を築くためのメカニズムを提供している。

バイオメディカル領域における価値の高いデータと臨床試験におけるデータ検証の必要性を考慮すると、ブロックチェーンによる管理システムが必要になると、彼らは考えている。バイオメディカルに限らず、現代社会は膨大な量のデータで溢れているため、意図的又は偶発的なデータ操作の発生リス

⁷⁷ <https://arxiv.org/pdf/1807.03662.pdf>

クは、ブロックチェーン等の技術的な手段によって軽減する必要があるという。ブロックチェーンは、データを管理する際に発生する全ての潜在的なリスクを解決できる訳ではないが、研究スポンサー及び一般の人々に対して、研究データが適切に使用されているということを証明できると考えられる。

7.2.4. 事例③「Enigma」

(1) プロジェクトの概要

現代社会におけるアプリケーションは、ユーザから膨大なデータを取得し、取得したデータに対して広範な分析をかけている。ここで問題なのが、秘匿性の高いデータが非常に多いという点と、秘匿性の高いデータを処理するために重厚なシステムを構築する必要があるという点である。また、秘匿性の高いデータを、特定の管理者が自由に収集し閲覧、分析することができてしまっている点も、非常に大きな問題として議論されるべきである。この問題に対して、ブロックチェーンによるアプローチが活発な動きを見せているものの、現在のブロックチェーンはプライバシーに全く対応できていないだけでなく、重い計算処理には適していないのである。

Enigma⁷⁸は、秘匿性の高いデータのプライバシーを保護しつつ、高速に計算処理ができる分散型のコンピューティングネットワークである。Enigma で処理されるデータは、事前に暗号化された状態で、複数のノードに対して分割して送信されるという。各ノードは、送信されてきたデータを閲覧することなく処理することができるといわれている。Enigma で処理するためのデータは、分散型オフチェーンハッシュテーブル (DHT) に格納される。このデータは、本来の持ち主以外が閲覧することができないため、データのプライバシーを保護することに繋がるだろう。また、全ての処理をブロックチェーン上で行わず、オフチェーンを活用することで大量の計算処理を実現するという。

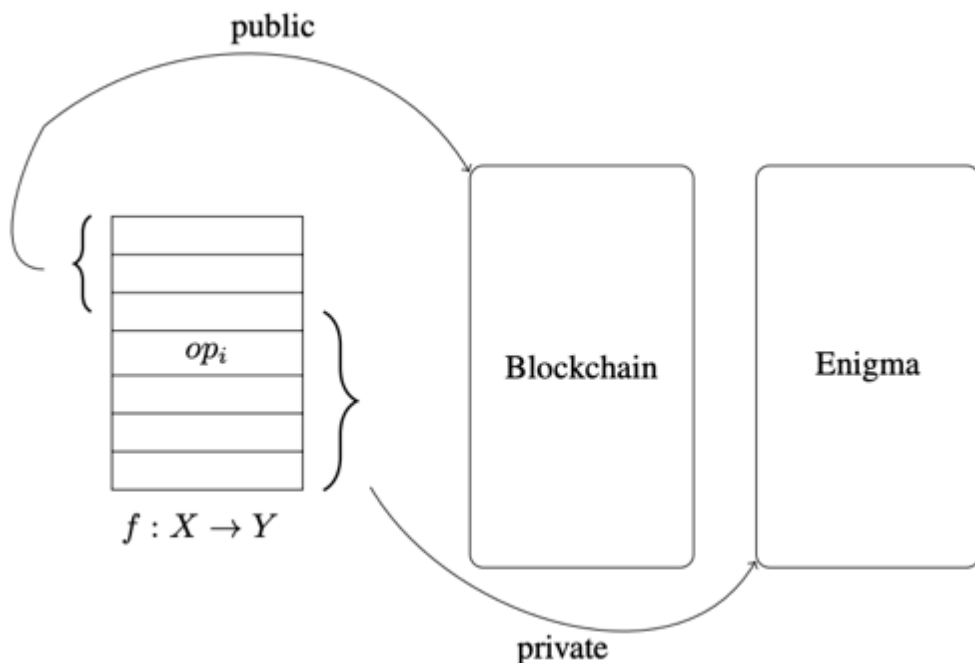
(2) プロジェクトの詳細

Enigma は、プライバシーが保護された状態でデータを処理することができる分散型コンピューティングプラットフォームである。安全なマルチパーティ計算方式 (sMPC 又は MPC) を使用することで、特定の管理者を排除した状態で計算処理を行うことができるといわれている。データは、Enigma を構成するノード間でばらばらに分割され、他のノードに情報を共有せずに計算処理を行うことができる。具体的には、特定の管理者がそのデータ全体にアクセスするのではなく、不特定多数の管理者がそれだけでは無意味なデータの断片を所持することになる。Enigma では、一般的なブロックチェーンとは少し異なり、計算処理とストレージをネットワーク内の全てのノードが担うわけではない。小さなサブセットのみがデータの異なる部分に対して計算処理を実行していくことになっている。すなわち、各ノードは生のデータ自体にアクセスすることなく、データの断片のみを受け取って計算処理

⁷⁸ Enigma : https://enigma.co/enigma_full.pdf

を行うことができる。こうすることで、プライバシーを守りつつ、重い計算処理でも速く実行することができるのだという。

現在のアプリケーションの多くにおいては、データの共有は不可逆的なプロセスとなっていることも問題だと考えられる。データが一度送信されると、それを取り戻したり送信先の使用方法を制限したりすることができないのである。Enigma におけるデータへのアクセス方式では、元データの所有者以外には誰も生のデータを見ることができないようになっているという。そのため、可逆的かつ制御可能なデータ共有が可能なのである。この仕組みは、データ分析に対する現在のアプローチを根本から変えることになる可能性がある。



図表 7.2 - 6 Enigma のコード実行モデル⁷⁹

Enigma は、パブリックチェーンとオフチェーンのハイブリッド型を採用しており、計算処理がネットワーク全体に効率的に分散されるように設計されている。図 2.5.2-1 のように、スマートコントラクトをパブリックとプライベートに分割して実行することで、プライバシーと検証性の両方を維持しながら、実行時間の短縮化を図っているという。

Enigma におけるオフチェーンネットワークは、以下の問題を解決すると公表している。

⁷⁹ https://enigma.co/enigma_full.pdf

ストレージ

Enigma には、データのリファレンスは格納するがデータそのものは格納しない。データそのものは、ブロックチェーンを介してアクセス可能な分散型オフチェーンハッシュテーブル (DHT) に格納される。その際、格納されるデータはクライアント側で事前に暗号化される。

プライバシーを保護する処理

Enigma ネットワークでは、いずれのノードも生のデータにアクセスすることなくコードを実行することができる。これは、現在の中央集権型システムを代替する上で非常に重要である。

大量の処理

プライバシーが論点にならない場面においても、現状のブロックチェーンでは、多くの複雑なトランザクションを処理できないという問題が存在する。Enigma では、オフチェーンを活用することで大量の計算処理を可能にしている。

Enigma は、暗号通貨やブロックチェーンに該当するものではないため、インセンティブ設計はマイニング報酬ではなく手数料に基づいており、ノードは計算リソースを提供するために必要になるという。フルノードは安全性を確保するためのデポジットを管理するために必要とされ、万が一悪意のあるノードが発生した場合に罰することのできる権限を持つとのことである。

各ノードが、ネットワークへの参加やデータの保存、計算処理の実行を行うには、全てのフルノードが事前にデポジットをプライベートコントラクトに送信しておく必要がある。各ノードでの計算処理が完了すると、プライベートコントラクトは正当性と公平性が確保されていることを検証する。特定のノードが悪意のある行動を起こしたことが判明した場合、デポジットが没収される設計となっているため、悪意のある行動を事前に防ぐ力学が働くだろうと考えられる。

ストレージの利用やデータ検索、計算処理等の際に発生するネットワーク内の全てのリクエストには、Ethereum におけるガスの概念と同様の固定費用 (手数料) が必要になるという。ただし、全ての計算が全てのノードによって実行される Ethereum とは異なり、Enigma では異なるノードが異なる処理を実行するため、貢献度に応じて報酬を調整する必要があると考えられる。チューリング完全なプラットフォームでは、発生するリクエストの正確なコストを事前に計算することはできないため、計算処理が完了すると、各リクエストのコストは、各ノードが保有しているアカウントの残高から差し引かれることになる。当然、アカウントの残高を上回るコストが必要なリクエストは処理されない。

また、データストレージの使用量には有効期限が存在する。アカウント残高が少なすぎる場合、ストレージ内のデータに対するアクセスが制限され、追加資金が入金されない限り、データは一定期間経過後に削除される仕組みになっているという。

7.2.5. 事例④「Blockchain for Science」

(1) プロジェクトの概要

科学分野に限らず、現在のあらゆる分野の研究結果の事実データや研究者の考察は、最終的に世の中に出出版物として発信する組織の手に委ねられているといわれている。というのも、現在のデジタルデータ管理の仕組みでは、データが改ざんされないということを保証することができない状態である。例えば、膨大な時間をかけて研究したデータを何百ページにも及ぶ論文にまとめたとしても、最終的に出版する組織にデータが渡って以降のプロセスには、研究者が介在することができないという。そのため、データを渡してから改ざんされてしまった場合に、気付くこともできなければ、何百ページにも及ぶデータを改ざんされたところで、該当箇所がどこであるかすら容易に検知することができない。

ブロックチェーンを活用すれば、デジタル資産の不変性と透明性を確保することができる。これは、研究データを本当の持ち主に帰属させることも意味するだろう。Blockchain for Science⁸⁰では、信頼できる特定の第三者によって保護されたパブリック型のブロックチェーンを活用するという。Blockchain for Science に実際に保存されているデータは、信頼できる特定の第三者が管理できるわけではないとのことだ。データはあくまでも研究者に帰属させるという。ブロックチェーンには、現実世界とブロックチェーン上のデータの整合性をどのように確保するのか、という課題が存在する。そのため、Blockchain for Science では特定の第三者を信頼することで解決しようとしているという。

今後、科学分野に限らず、多くの分野でブロックチェーンを活用した研究データの保護が実現すると考えられる。

(2) プロジェクトの詳細

現在、科学者たちの研究結果の正当性や考察は、最終的に世に出版する役割を担う組織に委ねられているといわれている。要するに、科学者たちが提出した研究結果が、世の中の目に触れるようになるまでに、出版者の手によってデータが改ざんされている可能性があるということである。この問題に対しては、ブロックチェーンを活用することで研究作業の大部分を研究者自身に帰属させることができるだろう。これは「無駄を減らし、より多くの研究結果の正当性を保証する」という可能性があることを意味している。またそれ以上に、余計な負担を減らすことで科学的プロセスを加速させ、真のイノベーションを刺激することにも繋がると考えられる。

今後の研究実験においては、実験作業とデータ収集を除く研究プロセスの全ての作業が、ブロックチェーン内で行われるようになる可能性が考えられる。データやテーマの匿名性、計算処理、研究評

⁸⁰ Blockchain for Science : <https://www.blockchainforscience.com/2017/02/23/blockchain-for-open-science-the-living-document/>

価、及び研究資金の分配等は、タイムスタンプが付与されることでわかりやすくオープンな状態で、外部からの検証が可能になるとされる。

Blockchain for Science によると、図 7.2-7 のように、ブロックチェーンはいくつかのグループに分類することができるという。

		Who can use?	
		Public	Private
Who secures?	Permissioned	Science!	Some banking, supply chain, healthcare, IoT, ...
	Permissionless	Bitcoin, Ethereum,

図表 7.2 - 7 科学分野における最適なブロックチェーンの種類⁸¹

まず、以下に説明するように、誰がブロックチェーンを管理しているかという観点で分類することができるという。特定の管理者が存在しないブロックチェーン(Permissionless)は、ネットワークへの攻撃を防ぐために、内在的な価値を有するトークンを活用した経済的な力学を利用する。これは、Proof-of-work や Proof-of-Stake と呼ばれる。特定の管理者が存在するブロックチェーン(Permissioned)は上述の仕組みを必要としないという。なぜなら、ブロックチェーンを管理するための信頼できる明確な管理者が存在するからであるとのことだ。ここで重要なのは、特定の管理者が存在するブロックチェーン(Permissioned)においても、ブロックチェーンで管理されているデータを特定の管理者が制御できるわけではないということだという。ブロックチェーンによって定義されたプロトコルを超えた範囲で、検証又は承認することはできないとのことである。

次に、パブリックかプライベートかという観点で分類することができるという。これは、実際に誰がブロックチェーンを使用できるかといった観点による分類であると考えられる。誰もがブロックチェーンにアクセスできるのか、それとも特定の誰かだけがアクセスできるのかということの意味する。ただし、実際の使用状況に応じて権限を設定することができるため、この分類は少し粗くなってしまうだろう。なお、この分類方法では、ブロックチェーン内のデータに対する閲覧性については言及していないという点に注意が必要である。例えば、パブリックブロックチェーンを使って非公開な研究データを管理することもできるのであるという。

⁸¹ <https://www.blockchainforscience.com/2017/02/23/blockchain-for-open-science-the-living-document/>

従って、科学分野におけるデータ管理のためには、信頼できる特定の第三者によって保護され (permissioned)、誰もがデータにアクセスできるパブリックな形態が最も適しているといわれている (図表 7.2 - 7)。なお、Blockchain for Science に実際に保存されているデータについては、特定の第三者が管理することはできないという。政府や他の団体が Blockchain for Science にあるコンピュータを利用して研究結果を改ざんすることはできないということである。

Blockchain for Science のまとめた、科学と知識の想像におけるブロックチェーンの活用方法が図表 7.2 - 8 である。

実験を除く研究サイクルの多くの部分において、ブロックチェーンを活用することができるという。すなわち、研究サイクルにおけるデータ収集作業以降、全てが不変で透明になり、外部からの検証が可能な状態となると考えられる。これにより、研究サイクルの大部分が科学的な自己添削の対象となり、より多くの研究結果が再現可能で、真実かつ有用なものになる可能性が浮上するという。



図表 7.2 - 8 研究サイクル⁸²

(既出のアイデアや概念を緑色、新たに導入したアイデアを黄色で示している)

ブロックチェーンの根本的な課題の一つは、現実世界とブロックチェーン上のデータの整合性の問題であるといわれている。要するに、ブロックチェーンをどのようにして現実世界と連動させるのかということである。この問題の一例として、研究データを収集する研究者、現実世界と連動させるためのセンサー等を信頼する必要がある点があげられるという。また、実験における研究者と被験者の身元が、ブロックチェーン上でどのように確認されるのかという問題もあげられるだろう。この問題へ

⁸² <https://www.blockchainforscience.com/2017/02/23/blockchain-for-open-science-the-living-document/>

の対処としては、特定の研究機関あるいは研究者の大規模データベースを保有する他の組織によって確保される可能性が考えられる。

ブロックチェーンは、最終的な出版物だけでなく、研究サイクルを科学的な自主管理型に移行させることができ、「価値を高め、無駄を減らす」ために活用することができるという。従って、真に革新的な研究を支援するために使用することもできると考えられる。

7.2.6. 事例⑤「Data Management Hub」

(1) プロジェクトの概要

今日の、科学分野における研究データの管理実態には、非常に多くの課題が存在しているといわれている。例えば、アイルランドでは、研究者の80%が研究を終えて学術論文を発行してから、わずか3年でそのデータを管理する権限を失うことになっているといわれている。また、2015年には、200人以上の研究者が既に発表済みの研究を意味なく繰り返し、再現性があるかどうかを確認していると公表されている。研究データは実証実験の基礎にあたる部分であるため、正しくてかつ見つけやすい状態で管理しておくことが重要なのであると考えられる。また、再利用が可能なデータは、科学分野の発展、すなわちオープンサイエンスを促進するために欠かせない要素となると考えられる。

現状は、研究データ管理のための最適なソリューションは存在していないといわれている。GitHubやDropboxのようなツールは、一般的なサービスであるため、秘匿性の観点から研究データの管理には適していないだろう。生のデータはCDやDVD、USB等に保存され、一定の時間が経つと忘れられる存在となっている。これらの課題が積み重なった結果、研究者たちはデータ管理に疲弊しているのが現状であるという。

Data Management Hub⁸³(以下、DaMaHub)は、オープンライセンス技術であるIPFSとブロックチェーンを活用した、科学分野における研究データの信憑性とアクセシビリティを実現するソリューションである。DaMaHubは、次世代の研究者たちのために、研究の再現性をも実現すると考えられる。

オープンサイエンスを実現するためには、データ管理の作業を研究者たちの日々のワークフローに適合させる必要があるだろう。DaMaHubは、研究者のコンピュータ上のローカルクライアントに分散型オープンサイエンスプラットフォームを組み合わせた形で開発された。ローカルクライアントを使用することで、データの秘匿性を担保しつつ、安全に研究者同士で共有ができるようになる。また、データのバージョン管理や簡単なアーカイブも可能となっているという。

⁸³Data Management Hub Executive Summary : <https://github.com/DaMaHub/v0.01/blob/master/ExecutiveSummaryDataManagementHub.pdf>
Data Management Hub Vision : <https://github.com/DaMaHub/vision>

DaMaHub では、既存の研究基盤と新しい技術(IPFS、ブロックチェーン、DAT、分散 ID 等)を組み合わせたプロトコルを開発し、研究データをより FAIR(Findable, Accessible, Interoperable, Re-usable/Reproducible)な状態にすることを目指しているという。アカデミックのエコシステムの中に分散技術の概念を取り入れることで、既存のエコシステムを全て代替するのではなく、足りない部分を補完しようと試みていると考えられる。

FAIR の各要素はそれぞれ次のように実現するという。Accessible : 学術記録は信頼できるノード (図書館や研究センター、インフラプロバイダー等) との共同ネットワークを通じて、オープンで恒久的なアクセスが可能になる状態の実現を目指す。Interoperable : IPFS に格納されているコンテンツに相互運用性を持たせるために、データモデル及びその他の関連技術をカスタマイズすることで、規格を統一している。Findable : コンテンツアドレスが指定されたデータパッケージに、エンコードされたセマンティックを索引付けすることにより、照会及び検索する方法、要するに見つけやすさを実現する。Re-usable/Reproducible : これら 3つの要素を実現することができれば、データを再利用可能な状態で管理することができ、重複する無意味な研究を減らし、オープンサイエンスの発展に貢献することができると考えられるだろう。

また、スマートコントラクトを活用することで、研究者間の役割分担を明確にすることができると考えられる。そしてこれにより、プロジェクトへのさらなる貢献を促進することができるようになることも考えられる。トークンで表現された科学的なエコシステムを通して、研究に資金を提供する新たな手段が登場する可能性も浮上するだろう。いずれこのプロトコルには、任意の共同研究サイクルにおける何かしらのアプリケーションが実装されることになるといわれている。

7.2.7. 事例⑥「Dat」

(1) プロジェクトの概要

インターネットの普及により、HTTP や FTP といった様々なプロトコルが整備され、膨大な量のデータがオンライン上で共有されるようになった。しかしながら、これらのプロトコルには、データのバージョン管理やコンテンツアドレッシングをサポートする仕組みが備わっていない。そのため、オンライン上でデータが共有された際に、リンクが破損したり中身が書き換えられたりといった問題が発生した場合でも、対処することができていない状況になっていると考えられる。その結果、出版された科学分野の学術論文等において、データの参照元が消えてしまっていたり、事実と異なる内容で拡散されていたりといった問題が起きてしまっているといわれている。AWS や Google Drive のような既存のクラウドストレージサービスでは、データの可用性は保証しつつも、中央集権的な管理体制であるがために、帯域幅によって送信できるデータのサイズが制限されたり、送信コストが高価になってしまったりする。

今後は、分散型のデータ共有の仕組みが普及し、データの送信速度は劇的に速くなり、帯域幅の問題も解消され、送信コストも大きく削減されるようになるといわれている。また、リンクが破損した場合に即時検知する仕組みも備わり、なおかつバックアップからの自動復元も可能になると考えられる。

この分散型のデータ共有の仕組みを実現するのが Dat である。Dat プロトコルを通して共有される全てのデータは、公開鍵によって暗号化されるという。自身の公開鍵を任意の送信相手に伝えることによって、送信相手はデータを閲覧することができる。すなわち、公開鍵を知らない人物には、自身のデータは閲覧されないのである。公開鍵の所有者であれば誰でも、送られてきたデータが、公開鍵と対になる秘密鍵の所有者のものであることを確認することができる。

Dat⁸⁴は、ノードのネットワークの中で、保有するデータの一部を交換し合うように設計された PtoP 型のプロトコルである。ノードは、ネットワークに参加後すぐに他のノードからデータを取得し、ネットワークを構成する一部となる。ネットワーク内では、全てのノードが同一のデータを保有しているわけではない。そのため、特定のデータが必要になった場合には、ネットワーク内でそのデータを保有しているノードを探し出す必要がある。ノードは IP とポートを利用して探すことができ、ノードが見つかるとそのノードに接続することでデータを取得することができる。全てのノードが同一のデータを保有しているわけではないものの、複数のノードで1つのデータを保有するため、万が一いずれかのノードからデータが消えてしまったとしても、ネットワーク内の他のノードからデータを取得することができる。

Dat は、既存の様々なシステムに足りない機能を補う形で設計されているという。例えば、バージョン管理システムである Git は、ソースコード等のテキストデータの変更履歴を、効率的にダウンロードするためのプロトコルを提供しているが、大きなサイズのデータには適していないと考えられる。従って、Git-LFS のようなソリューションでは、Git プロトコルではなく HTTP を使用している。しかしながら、データ送信の帯域幅を確保するためのコストは、リポジトリの所有者が負担する形となっている。Dat を使えば、PtoP 型のプロトコルによってバージョン管理ができる状態で、大きなサイズのデータも最小限のコストで送信することができるという。

7.2.8. 総括

様々な分野における研究データの信憑性確保や不正防止のために、ブロックチェーンを活用した新たな取組が進められている。研究データ管理に対するブロックチェーンの活用ポイントは、「改ざん検知による不正防止」、「プライバシー保護及び秘匿性の高いデータの管理」、「データ共有のガバナ

⁸⁴ Dat : <https://docs.datproject.org/>

ンス構築」等であると考えられる。ブロックチェーンを活用することで、データ改ざんの即時検知が容易になり、研究データを研究者自身に帰属させることができるようになるだろう。また、ライフサイエンス領域における患者のプライバシー保護も期待できると考えられる。これは、ブロックチェーンに使用されている公開鍵暗号を使用することで実現可能とされる。

一般的に、研究データは膨大な量になることが多く、全てのデータを永久に管理しておくことが困難であったが、この課題もブロックチェーンによって解消されることが考えられる。従来は一箇所で集中的にデータを管理していたが、ブロックチェーンのような PtoP 型のデータ管理方式を採用することで、物理的な制約からも解放されるのである。そして結果的には、データの参照元が削除される他、誤って書き換えられたりすることによる、データの紛失といった問題をも解消することができるだろう。

先述の海外事例からも分かる通り、研究データ管理におけるブロックチェーンは、コンソーシアムチェーン又は、プライベートチェーンとパブリックチェーンを組み合わせたハイブリッドチェーンであることが多くなっている。この理由としては、ブロックチェーンそのものが発展途上の技術である中、研究データのような秘匿性の高いデータを管理するには、現状のパブリックチェーンは適していない点等が考えられる。

8. ハッカソン開催

8.1. ハッカソン開催の目的

今回のハッカソン開催の目的は、「学位・履修履歴管理」及び「研究データの信頼性確保」の2テーマにおいて、ブロックチェーン技術の様々な可能性を発掘し、我が国における人材流動化促進のための社会基盤や信頼できる研究基盤を構築するための具体的かつ包括的な対応策について民間の知恵を活用して洗い出すことである。また、参加者には社会的な課題をより深く理解して頂き、技術的な解決策にとどまることなく、実際の社会実装へと繋がるようなアウトプットの創出を期待する。

8.2. ハッカソン開催概要

- 運営体制
 - 主催：経済産業省
 - 事務局：株式会社リクルート R&D
 - 運営協力：株式会社 LongHash、株式会社 LIFULL
- 日時：2019年2月9日（土）、2月16日（土）～17日（日）
- 場所：Lifull Hub (<https://hub.lifull.com>) 東京都千代田区麹町 1-4-4 1F, 2F, 8F
- 参加人数
 - 申込者数：142名
 - 運営による参加者選定者数：106名
 - 最終参加人数：98人
 - 社会人：73人
 - 学生：25人
- 参加チーム数：22チーム
 - 学位・経歴証明テーマ：13チーム
 - 研究データの信頼性確保テーマ：9チーム
- 参加料：無料
- 集客方法
 - 仮登録：connpassで募集（2019/12/27～2019/1/17（22日間））
 - 本登録：Eventbriteで募集（2019/1/17～2019/1/31（15日間））

8.2.1. 利用可能なブロックチェーンの選定について

現在既に多数のブロックチェーンプロジェクトが存在しているが、今回のハッカソンにて利用可能なブロックチェーンプロトコルには関連省庁の規制等も鑑みて制限を設定した。

まず、パブリックのブロックチェーンプロトコルは、資金決済法に基づく登録仮想通貨交換業者が取り扱う仮想通貨の基盤となっているプロトコルに限定した。

また、Hyperledger や Miyabi 等のプライベートブロックチェーン技術の利用においては、特に資金決済法等の影響を受けないため、ハッカソンの参加規約に記載の知的財産の規定に抵触しない限り参加者が希望するプロトコルを利用可能とした。

8.2.2. 参加規約における工夫

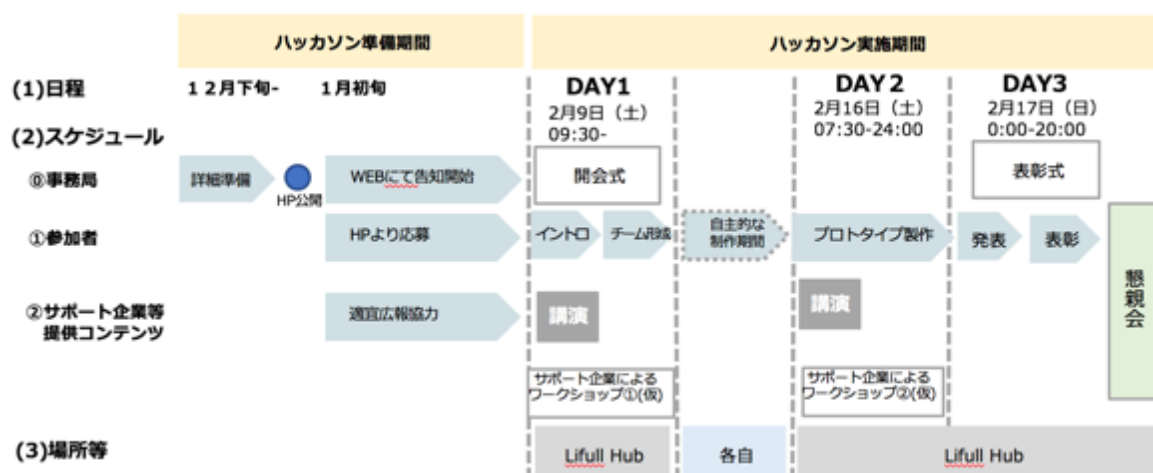
本ハッカソンへの参加及び受賞した事実が資金決済法等に違反する行為に用いられることを防ぐため、参加規約に下記条項を記載するとともに、ホームページ等でも FAQ を通じて参加者への周知を行った。

(1)利用するブロックチェーンの選定について：「エアドロップを通じて取得したトークンを含み、世の中に出ているトークンで日本で仮想通貨交換所で取り扱いがないものを用いてはならないものとする。ただし、ハッカソンを通じて新たにトークンを生成・作成する場合にはこの限りではない。」

(2)ハッカソン参加後の宣伝について：「参加者は、参加者が制作した成果物をもとに将来、新商品・サービスを開発する場合、本イベントへの参加や受賞した事実を Technical whitepaper 等を通じて自由に利用することができるものとする。但し、国内外でのトークンを用いた資金調達における募集・販売に関わる勧誘に用いることをしてはならないものとする。」

8.2.3. スケジュール

(1)ハッカソン開催における全体のスケジュール



図表 8.2 - 1 ハッカソン開催の全体スケジュール

(2)ハッカソン当日のスケジュール

時間	2月9日(土)	時間	2月16日(土)	時間	2月17日(日)
9:30 - 10:00	受付	7:30-8:00	受付	7:30 - 8:00	受付
10:00 - 10:15	オープニング (経済産業省)	8:00 - 8:30	オープニング	8:00 - 11:00	朝食及びワーク
10:15 - 10:30	事務局説明 (リクルート)	8:30 - 10:00	朝食及びワーク	11:00 - 12:30	昼食及び制作物提出 期限
10:30 - 12:30	サポート企業による ワークショップ	10:00 - 12:00	サポート企業による ワークショップ、 又はワーク	12:30 - 14:00	1次審査
12:30 - 14:00	チームビルディング 及び昼食	12:00 - 13:00	昼食	14:00 - 14:30	最終審査 結果発表
14:00 - 18:20	サポート企業による ワークショップ、 又はワーク	13:00 - 17:00	サポート企業による ワークショップ、 又はワーク	14:30 - 17:15	最終審査及び 表彰式及び クロージング
18:20	クロージング	18:00 - 22:00	夕食及びワーク	17:15 - 20:00	ネットワーキング
18:20 - 19:00	片付け及び完全撤収	22:00 -	夜食及びワーク	20:00 - 21:00	片付け及び完全撤収

図表 8.2 - 2 ハッカソン当日のスケジュール

8.2.4. ハッカソンに参加する関係者

(1)参加者

- 概要：実際にハッカソンに参加する参加者
- 参加日：ハッカソン開催期間中の全日参加（3人以上のチームに限って、半数以下のメンバーはリモートでの参加が可能）

(2)審査員

- 概要：1次審査及び最終審査の審査員
- 参加日：主に最終日の午後から。但し、ハッカソン開催期間中、必要に応じていつでも参加

(3)スピーカー

- 概要：ワークショップの講演者
- 参加日：初日及び二日目のワークショップの提供時や最終日の懇親会等に参加

(4)見学者

- 概要：役所関連や大学関連の関係者
- 参加日：主に初日及び最終日参加

(5) プレス

- 概要：取材を目的とするメディア関係者
- 参加日：初日のオープニング及び最終日の2次審査から懇親会に参加

(6) 運営要員

- 定義：ハッカソン運営のための経産省、リクルート、運営協力社からの要員
- 参加日：ハッカソン開催期間中の全日

8.2.5. 広報

(1) プレスリリース

- 2018年12月27日、Connpass上で仮登録用のサイトのオープンと同時に経済産業省からプレスリリース (<http://www.meti.go.jp/press/2018/12/20181227004/20181227004.html>)
- 2019年1月18日、Eventbrite上で本登録用のサイトのオープンと同時に株式会社リクルートからデジタルPRプラットフォームにてプレスリリース (<https://digitalpr.jp/r/31020>)

(2) Eventbrite 上の本登録用サイト

当初は本登録用には独自 URL を取得し、新たにホームページを開設し、受付を行う予定であったが、一時的利用のホームページにおける独自 URL の取得・運営におけるセキュリティの観点からの懸念により、Eventbrite を利用することに決定。ホームページ用に作成したデザインをそのまま Eventbrite にて再現することとした。

以下に実際の日本語版・英語版のホームページデザインのスナップショットを掲載する。



図表 8.2 - 3 Eventbrite サイト（日本語版）のスナップショット

Blockchain Hackathon 2019

Leveraging blockchain technology to manage degree, course history, job history, and research data to build a trusted platform to serve increased talent mobility and research development |

7th Feb
9:30am - 1A:00pm


Hackathon Day1

14th Feb
9:30am - 22:00pm

Hackathon Day2

17th Feb
8:00am - 20:00pm

Hackathon Day3



70⁺

Participants

10⁺


Support companies

10⁺


VIP guests

BACKGROUND

This event will be held in light of two recent developments in today's society.



As technological revolutions such as artificial intelligence ushered in an era when the industrial structure is rapidly changing, an increasing number of people are choosing diverse workstyles; changing workplaces and taking up side jobs. The aging society combined with falling number of children will likely prompt more academic institutions to form partnerships or merge. As the mobility of human resources rise and diverse ways of learning and working become more common, there are concerns that the existing system may no longer be able to sufficiently verify individuals' academic degrees and professional credentials.

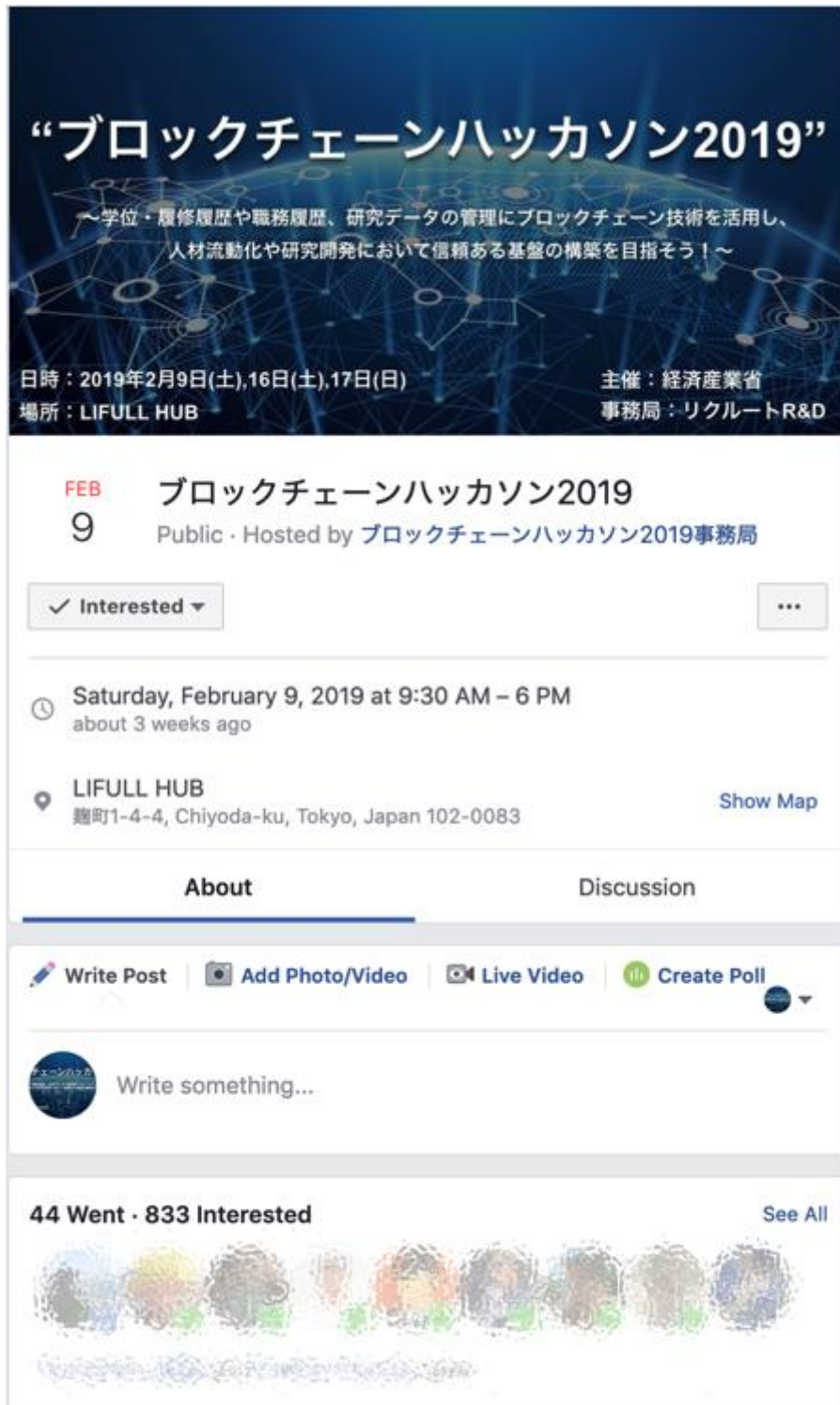


In Japan, we have seen a rise in data fraud at research institutions as well as businesses. In 2017, the number of fraud cases in the academic field doubled from the previous year, while many Japanese firms were also faced with data-rigging scandals. The issue of data fraud has been put on the front burner at both academic institutions and businesses.

図表 8.2 - 4 Eventbrite サイト (英語版) のスナップショット

(3) ソーシャルメディアの活用

Facebook、Twitter を活用した広報を行う。以下に、Facebook のイベントページ及び Twitter 活動のスナップショットを掲載する。



図表 8.2 - 5 Facebook のイベントページのスナップショット
(800 人を超える方々に興味を持って頂いた)



図表 8.2 - 6 Twitter のアカウント情報のスナップショット

(4) 関係者による広報

その他、ソーシャルメディアでの投稿や他のイベントでの告知等、審査員やサポート企業等の関係者も積極的に広報活動に参加。

8.3. 審査について

8.3.1. 基本方針

今回のハッカソンでは「学位・履修履歴管理」及び「研究データの信頼性確保」の2テーマにおけるブロックチェーン技術の適応可能性を検討し、社会実装に繋がるアイデアやアウトプットを発掘することをゴールとした。そのため、審査においては技術的観点からの完成度だけではなく、上記のテーマが有する社会的課題に対して実行・実現可能性の高いアイデアやアウトプットが提示できているか等を総合的に判断するものとした。

8.3.2. 審査方法

審査は1次審査及び最終審査に分けて、ハッカソン最終日である2月17日（日曜日）の午後に実施した。

1次審査では全審査員の中から6名が担当し、3名ずつ2グループを組成。合計22チームを2つのグループに分け、グループごとに11チームずつデモ試演及びインタビューを通じて審査を実施した。1次審査は各グループの審査員が話し合い、最終審査進出チームを決定した。

最終審査に進出したチームは全審査員の前でプレゼンテーション及び質疑応答を行い、各審査員は審査票（点数表）を用いて審査を実施した。



1次審査の様子（グループA）



1次審査の様子（グループB）



最終審査の審査員（最前列）



最終審査の様子

8.3.3. 審査基準

審査は以下の5つの基準に沿って実施。尚、1次審査及び最終審査とも同じ審査基準を用いて審査を行った。

- ① 問題着眼点・着想点（着想した問題が明確で新しく、その問題の解き方が斬新か）
- ② 実行・実現可能性（実際に世の中で利用される可能性が高いサービスか）
- ③ 完成度・動作性（コンセプトで提示された機能が実装されているか）
- ④ プレゼンテーション力（端的に問題点、解決方法、実装が語られているか）
- ⑤ ハッカソンテーマへの適合性（「学位・履修履歴・経歴の管理」及び「研究データの信頼性確保」テーマに沿ったアイデアやアウトプットで、テーマ特有の課題を解決しているか）

但し、ハッカソン開催の時点にて国内の登録を受けた仮想通貨交換業者で取り扱いのない仮想通貨及びトークン（例：EOS や QTUM）を扱っているチームは、1次審査でその内容に関係なく最終審査に進出できないものとした。

8.3.4. 審査表

項目	観点	採点基準及び点数（0点～5点）
ハッカソンのテーマへの適合性（5点）	<ul style="list-style-type: none"> ・「学位・履修履歴・経歴の管理」及び「研究データの信頼性確保」テーマ特有の課題を解決しているか ・本ハッカソンのテーマに特化した観点の例： <ul style="list-style-type: none"> ○ Private key の管理や、ユーザビリティ等の課題を現実的な方法で解決しているのか ○ 証明書の発行者・利用者・受領者等、ステークホルダーの観点が適切に反映されているか ○ 手入力等によるミスが発生する可能性を考慮しているか（即ち、データの真正性を確保しているか） 	<ul style="list-style-type: none"> 5点：テーマ関連の、新しい課題を解決している 3点：テーマ関連の課題を解決している 0点：テーマ関連の課題に触れていない
問題着眼点・着想点（5点）	<ul style="list-style-type: none"> ・着眼・着想した問題が明確で分かりやすいか ・その問題の解き方が斬新で面白い、又は技術的に優れているか 	<ul style="list-style-type: none"> 5点：問題点が新しい、解き方が新しい 3点：問題点が明確 0点：問題点が分からない、解き方が分からない
実行・実現可能性（5点）	<ul style="list-style-type: none"> ・アイデアやアウトプットを実際に実現できるか ・実際に世の中で利用される可能性の高いサービスか ・スケーラビリティが高いか 	<ul style="list-style-type: none"> 5点：実行可能性が高く、多くのユーザに使ってもらえるサービスになり得る、このままサービスになる 3点：ユーザに使ってもらえるサービスになり得る 0点：ユーザが不明確である
完成度・動作性（5点）	<ul style="list-style-type: none"> ・アイデアやアウトプットを実際に実現できるか ・実際に世の中で利用される可能性の高いサービスか ・スケーラビリティが高いか 	<ul style="list-style-type: none"> 5点：コンセプトで提示された機能に触って体験できる、デモ動作が確認できる 3点：部分的又は、動画上では正常に動いている 0点：本当に動作しているかどうかわからない
プレゼンテーション力（コミュニケーション力）（5点）	<ul style="list-style-type: none"> ・端的に問題点、解決方法の内容が語られているか ・会場の笑いを誘う等、会場の注意を引きつけたか ・質疑応答に適切に対応できたか ・時間配分がうまくできたか 	<ul style="list-style-type: none"> 5点：問題点及び解決方法の提示、インパクトのあるデモで且つ時間内に収まった 3点：問題点や解決方法の提示、デモが時間内に収まった 0点：内容が伝わらなかった、時間内に説明が終わらなかった

図表 8.3 - 1 審査に用いられた審査表（点数表）

8.3.5. 審査員

氏名	所属
楠正憲 (審査委員長) (1次・最終審査)	JapanDigitalDesign株式会社 CTO ISO/TC307 ブロックチェーンと電子分散台帳技術に係る専門委員会 国内委員会委員長
江草陽太 (最終審査)	さくらインターネット株式会社 執行役員技術推進統括担当
村井宏行 (最終審査)	株式会社リクルート R&D 投資室長
河合健 (最終審査)	アンダーソン・毛利・友常法律事務所 パートナー弁護士
岸上順一 (1次・最終審査)	室蘭工業大学 教授 W3C (World Wide Web Consortium) ボードメンバー
坂下哲也 (1次・最終審査)	一般財団法人日本情報経済社会推進協会 (JIPDEC) 常務理事
鈴木絵里子 (最終審査)	FrescoCapital パートナー Mistletoe 投資部ディレクター
谷口耕平 (1次・最終審査)	株式会社 Chaintope BlockchainEngineer GoBlockchainEngineeringCommunityco-founder
千葉吉輝 (最終審査)	UMIN (大学病院医療情報ネットワーク) 研究センター J3C (JapanCDISCCoordinatingCommittee) ViceChair
平野淳也 (1次・最終審査)	株式会社 HashHub COO
福泉武史 (最終審査)	ソフトバンク株式会社技術戦略統括 IT サービス開発本部長
富士榮尚寛 (1次・最終審査)	伊藤忠テクノソリューションズ株式会社 西日本ビジネス開発チームチーム長代行 一般社団法人 OpenID ファウンデーション・ジャパン 理事

※ 順不同・敬称略

図表 8.3 - 2 審査員リスト

グループ A	グループ B
楠正憲 富士榮尚寛 平野淳也	岸上順一 坂下哲也 谷口耕平

※ 順不同・敬称略

図表 8.3 - 3 1次審査員のグループ

8.4. ワークショップの内容

英国・アイルランド・キプロス・ドイツ等、実施された団体から、実際の適用事例についてご紹介頂くと共に、イーサリアムやNEM、Hyperledger等の技術的なワークショップを実施。結果として、開催ワークショップで紹介されたコード等が実際に活用されるケースもあった。

8.4.1. ハッカソンテーマ関連ワークショップ

(1) Digital Certificates for academic and professional history

- 日付：2月9日（土）
- 長さ：40分
- 参加人数：全員
- 講演者（所属）：Ms. Soulla Louca (Professor, Director, Blockchain Initiative at University of Nicosia(キプロス))
- 概要：耐改ざん性を持ち独自に検証可能な記録の発行プロセスが、ブロックチェーンによってどのように変革されるのかという内容。具体的には、ニコシア大学ブロックチェーンイニシアチブによって設計され開発されたユースケースを紹介した。

(2) OpenBlockchain: How the Open University is applying Blockchain Technology to Adult Education

- 日付：2月9日（土）
- 長さ：40分
- 参加人数：全員
- 講演者（所属）：Ms. Michelle Bachler (Open University(英国) Research & Innovation Software Manager)
- 概要：Open UniversityのKnowledge Media InstituteとOpenBlockchainイニシアチブについて紹介。ブロックチェーンがどのように高等教育を変えることができるかというビジョンについて説明し、ブロックチェーン技術がそのビジョンの構築にどのように機能するかを確認するために、これまでブロックチェーン技術の実証実験事例を紹介。また、Institute of CodingプロジェクトとQualichainの下でチームが行っている最新情報を共有した。

(3) 組織におけるアイデンティティ管理に関する基本的な考え方

- 日付：2月9日（土）
- 長さ：40分
- 参加人数：全員
- 講演者（所属）：富士榮尚寛様（一般社団法人OpenIDファウンデーション・ジャパン理事）
- 概要：今回のハッカソンでは、学位や経歴等を含む属性の集合体であるアイデンティティを扱うため、デジタル・アイデンティティとは何であり、どのように管理するべきかを知って

おく必要がある。本ワークショップではデジタル・アイデンティティの管理に関する基本的な考え方と今後解決していくべき課題について説明した。

(4) A Deep Dive into Open Blockchain Experiments

- 日付：2月9日（土）
- 長さ：90分
- 参加人数：13名
- 講演者（所属）：Ms. Michelle Bachler（Open University(英国) Research & Innovation Software Manager)
- 概要：OpenBlockchainの技術的な面を紹介、参加者には、ブロックチェーン技術を用いた認証に関するハンズオンに参加した。

(5) Data, Policies and Algorithms

- 日付：2月9日（土）
- 長さ：50分
- 参加人数：30名
- 講演者（所属）：Mr. Denis Parfenov（Data Management Hub Founder, Open Data Governance Board member(アイルランド)）
- 概要：アイルランドにて市民のデータを非公開にし、政府データの公開を手助けしている事例を紹介。Data Management Hubは科学的データを検証、発見可能な形式で保存するためのデータストレージプラットフォームを設計及び開発しており、アルゴリズムが世界規模で人類に役立つと考えている。

(6) Free Q&A Session

- 日付：2月16日（土）
- 長さ：50分
- 参加人数：5名
- 講演者（所属）：Mr. Denis Parfenov（Data Management Hub Founder, Open Data Governance Board member(アイルランド)）
- 概要：Data Management HubのDenisさんへの自由Q&Aセッション。

(7) Blockchain and Cryptoeconomy for Science

- 日付：2月16日（土）
- 長さ：60分
- 参加人数：18名

- 講演者（所属）：Dr. Sönke Bartling (Founder of Blockchain For Science(ドイツ), Lecturer at CODE.University)
- 概要：ブロックチェーンが研究と知識創造のために必要な技術を説明。例えば、分散データ市場やプライバシーを考慮したデータの使い方、アイデアへの投資のための方法、研究データと新たな科学的資金調達方法等に関する取組を説明した。



ワークショップの様子①
(組織におけるアイデンティティ管理に関する基本的な考え方)



ワークショップの様子②
(How the Open University is applying Blockchain Technology to Adult Education)

8.4.2. ブロックチェーン技術関連ワークショップ

(1) 簡単に利用でき堅牢な NEM ブロックチェーン・初心者向けワークショップ

- 日付：2月16日（土）
- 長さ：160分
- 参加人数：20名
- 講演者（所属）：木村優様、松原正佳様（LCNEM株式会社 代表取締役、NEM Foundation）
- 概要：NEMを使うことでトークン発行や使い切りのマルチシグネチャ等、通常はプログラミングが必要な機能が、標準機能としてWebAPIで利用できる。低い開発コストで簡単に導入できるNEMブロックチェーンの初めて触れる方向けのワークショップ。アポストイーユ（公証機能）の解説・NEMブロックチェーンのIntroduction・環境構築について説明した。

(2) Ethereum の概要及びハンズオンワークショップ

- 日付：2月16日（土）
- 長さ：160分
- 参加人数：52名
- 講演者（所属）：谷口耕平様（株式会社 Chaintope Blockchain Engineer）

- 概要：Ethereum に始めて触れる方に向けた、ブロックチェーンの基礎から DApp の開発までを通して体験できるワークショップ。開発の言語及び環境として Solidity、Truffle を使い Metamask と連携して動作する DApp のサンプルプロジェクトを動かしながら解説。未経験の方がハッカソンでスタートダッシュを切れるようにサポートできるセッションを行った。

(3) コンソーシアム型ブロックチェーン及びHyperledger Fabric

- 日付：2月16日（土）
- 長さ：50分
- 参加人数：18名
- 講演者（所属）：田中健介様（株式会社NTT データ IT サービス・ペイメント事業本部方式基盤統括部課長代理）
- 概要：前半は、コンソーシアム型ブロックチェーンの特徴と活用のポイントについて簡単に歴史を振り返りながら解説。後半は、非常に強力ですがやや複雑な「Hyperledger Fabric」の構成と処理の流れについて説明。コンソーシアム型ブロックチェーンの理解を助ける初級～中級者向けのワークショップを行った。

(4) Ethereum Identity: ERC-725

- 日付：2月16日（土）
- 長さ：50分
- 参加人数：35名
- 講演者（所属）：真木大樹様（BlockBase 株式会社 代表取締役）
- 概要：ERC725 は人物だけでなく組織やデバイス、ソフトウェア等様々なものにアイデンティティを付与することができる Ethereum の規格の一つである。技術的な概要だけではなく、ユースケースや、実際に運用していくために解決すべき課題等も含めて考察するワークショップを行った。

(5) Ethereum Getho

- 日付：2月16日（土）
- 長さ：50分
- 参加人数：16名
- 講演者（所属）：佐藤大輔様（株式会社 Popshoot Co-Founder & CTO）
- 概要：twitter を使ったアイデンティフィケーションを実現するコントラクトのデプロイと実行を getho 上で実行し、Web アプリケーションを立ち上げ、正常に動くか検証。イーサリアムでスマートコントラクトの開発を行ったことがある人や DApp 開発をしてみたい人が対象となるワークショップを行った。

(6) NEM Wallet を作ろう！

- 日付：2月16日（土）
- 長さ：60分
- 参加人数：11名
- 講演者（所属）：中川祥平様（NEM Foundation）
- 概要：NEM を使って簡単な Wallet を作るハンズオンのワークショップを行った。



ワークショップの様子①
(Ethereum の概要及び
ハンズオンワークショップ)



ワークショップの様子②
(Ethereum Identity: ERC-725)

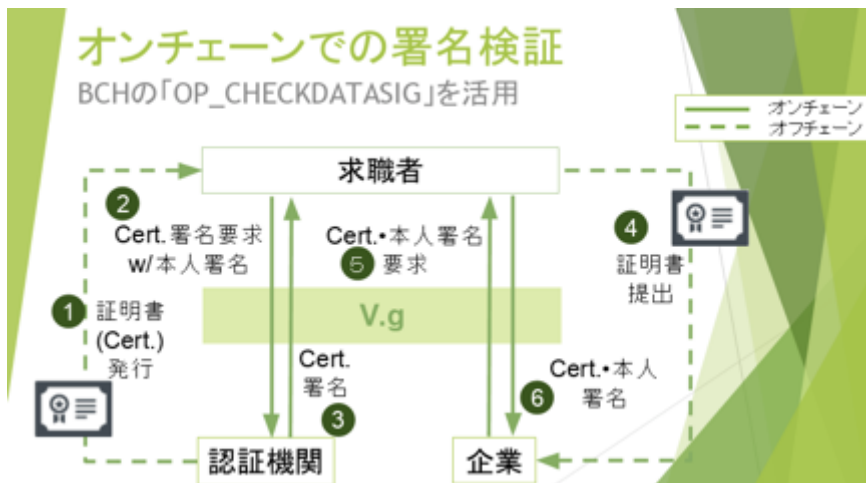
8.5. 各参加チームの成果物

ここでは各チームからの成果物を紹介する。テーマごとのチーム番号順に並べている。

8.5.1. 「学位・履修履歴証明」テーマ

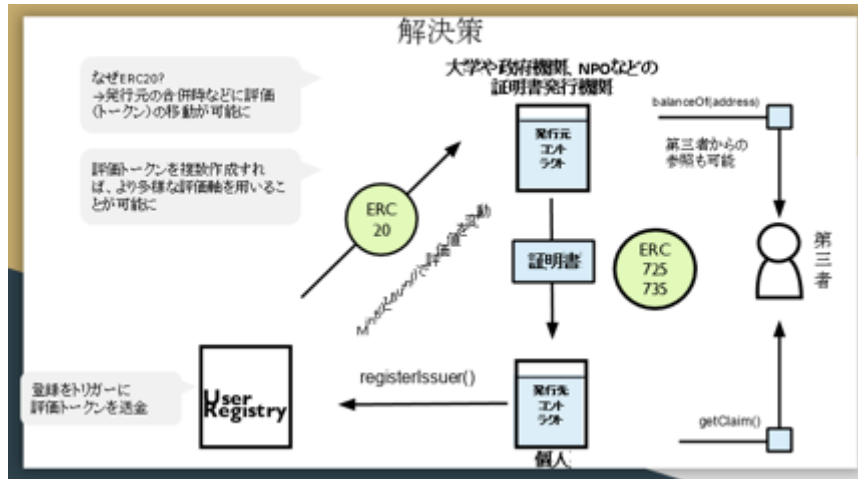
(1) チーム名：team-green

- チームメンバー数：5人（社会人：4人、学生：1人）
- 参加形態：個人参加チーム
- 内容：BCH で実装した、オンチェーンでの証明書発行サービス



(2) チーム名 : ryo0301

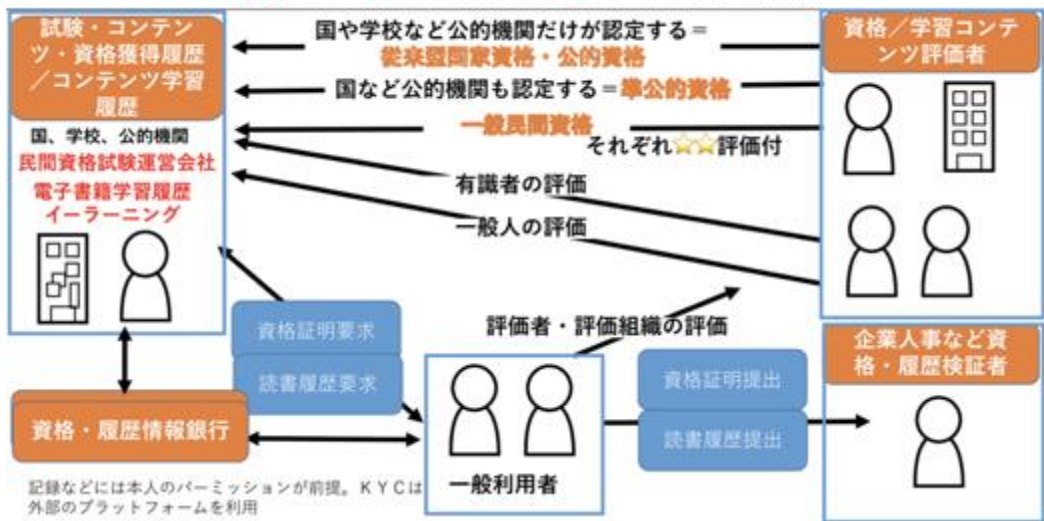
- チームメンバー数 : 3 人 (社会人 : 2 人、学生 : 1 人)
- 参加形態 : チーム参加
- 内容 : ERC725, 735 を利用した、証明発行と評価者の評価連動システム



(3) チーム名 : OVP (Open Verifiable Platform) ※優秀賞

- チームメンバー数 : 5 人 (社会人 : 4 人、学生 : 1 人)
- 参加形態 : 個人参加チーム
- 内容 : ERC725 、 ERC735 を利用した、資格・学習履歴の公的・準公的認証を実現する分散型資格・履歴証明ネットワーク。ERC735 で発行する認証情報 (クレーム) の評判を管理する ERC1757 を Ethereum コミュニティに提案
- 実施スキーム :
 - 資格情報を公的資格、準公的資格、一般民間資格と区分し、それぞれの認定機関を誰でも評価することにより信頼できる資格かどうかを蓄積
 - ERC725 のスマートコントラクトを自身のアイデンティティとしてデプロイする
 - 認証情報は ERC735 にて管理し、ERC725 スマートコントラクト上に紐付け
 - ブロックチェーン技術により、証明の情報を分散台帳 (IPFS) に格納することによる耐改ざん性の向上や、ERC725 及び ERC735 を利用し、第三者機関を不要とする分散型資格・履歴証明の実現を狙う。また、認証そのものに関する評判を管理することで (ERC1757)、第三者機関を介さずに「本当に国家資格であるか」や「本当にその学校が存在しているか」等が明示できるようになる他、変貌していく社会的ニーズに合わせて民間の資格を準公的資格とみなせる仕組みが構築できると考えられる。
- 検討事項 :
 - KYC については外部のプラットフォーム利用を前提
 - 実際に Ethereum Improvement Proposal (EIP) に対して提案を実施、標準化を目指す

Open Verifiable Platformの全体像



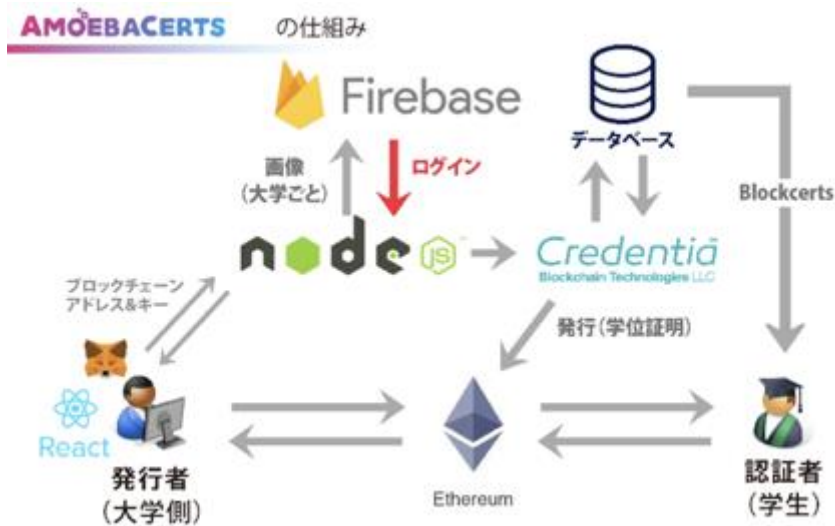
(4) チーム名：株式会社 SKILL

- チームメンバー数：5人（社会人：5人）
- 参加形態：チーム参加
- 内容：Ethereum で実装した、職歴管理と職歴リファレンスシステム



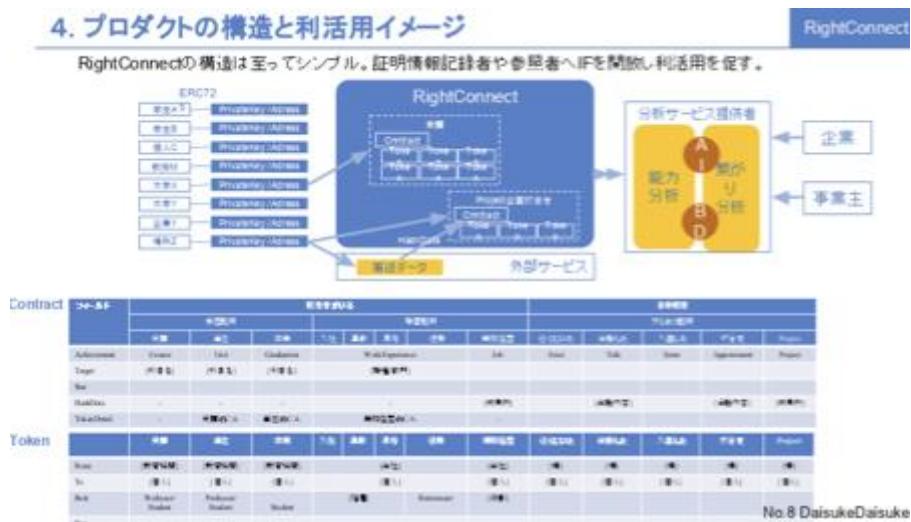
(5) チーム名：AMOEBACERTS

- チームメンバー数：5人（社会人：5人）
- 参加形態：チーム参加＋個人参加チーム
- 内容：Blockcerts をベースに多様な証明書発行が可能になるサービス



(6) チーム名 : DaisukeDaisuke

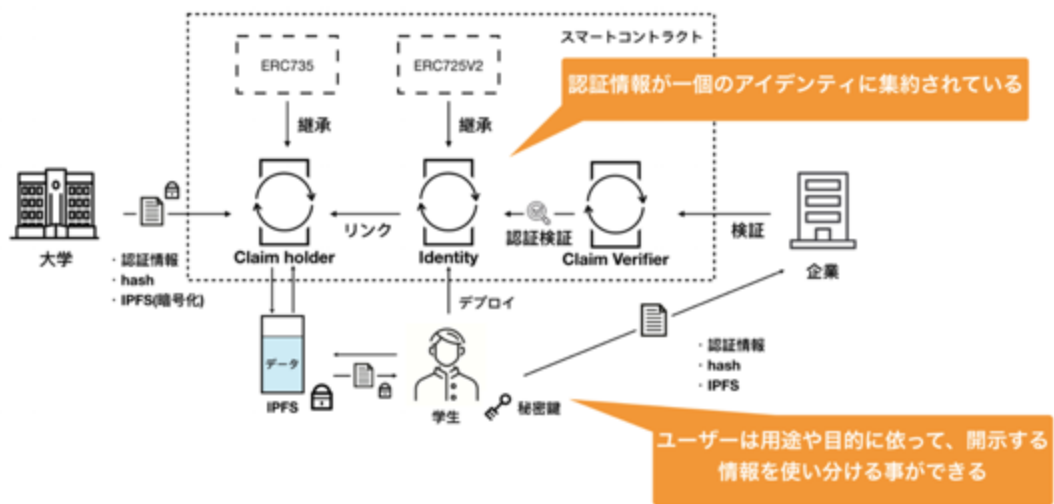
- チームメンバー数 : 5 人 (社会人 : 5 人)
- 参加形態 : 個人参加チーム
- 内容 : 個人の証明情報の蓄積により、人材発掘等に活かすサービス



(7) チーム名 : DigiD ※最優秀賞

- チームメンバー数 : 4 人 (社会人 : 3 人、学生 : 1 人)
- 参加形態 : チーム参加
- 内容 : ERC725V2、ERC735 を利用して、公開鍵がアイデンティティとなるような世界を作ること を目的としたプラットフォーム
- 実施スキーム

- 学生は ERC725V2 のスマートコントラクトを自身のアイデンティティとしてデプロイ。秘密鍵は学生が保持し、公開鍵を大学が保持、認証情報をその学生の公開鍵を用いて暗号化して管理
- 大学が発行する認証情報は ERC735 にて管理し、ERC725 スマートコントラクト上に紐付けされる
- 認証情報は分散台帳上（IPFS）に登録されているため、データの耐改ざん性を高めている。また、ERC735 を利用した認証情報が、ERC725 を用いて学生本人主導の分散アイデンティティとして一元的に管理することが可能になるため、個人の価値向上をも狙う。更に、この基盤を利用することで、大学が統廃合により無くなった場合でも、情報は存続可能になると考えられる。
- 検討事項
 - 個人情報保護については、今後の検討事項としている。個人情報をハッシュ化することで個人の特정이実質できない状態には近づけるが、現状は明快なガイドラインが存在しない。更に、オンチェーン上で管理する情報を適切に選別する他、削除できるオフチェーンのストレージを有効活用する等、「忘れられる権利」の課題を克服する必要がある。
 - 秘密鍵の紛失対策としては、マルチシグを利用し、ユーザが鍵を紛失した際には運営側が対応することで復帰可能としている



(8) チーム名 : Little eArth

- チームメンバー数 : 3 人 (社会人 : 3 人)
- 参加形態 : チーム参加
- 内容 : エンジニア向け有償トレーニング修了証の管理・発行サービス

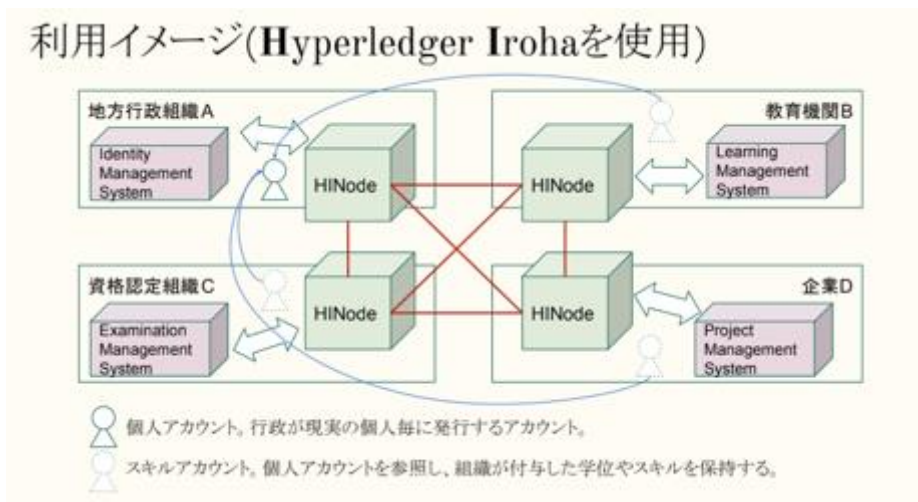
Solution



- Blockchain上に発行情報を記録し、簡易に真正性を確認できる修了証
- Ethereum上に修了証発行データを記録
- 紙の修了証にURLと復号鍵を印刷
- システムにてEthereumより発行データを読み出し
- 印刷された復号鍵で発行データを復号し、真正性を確認

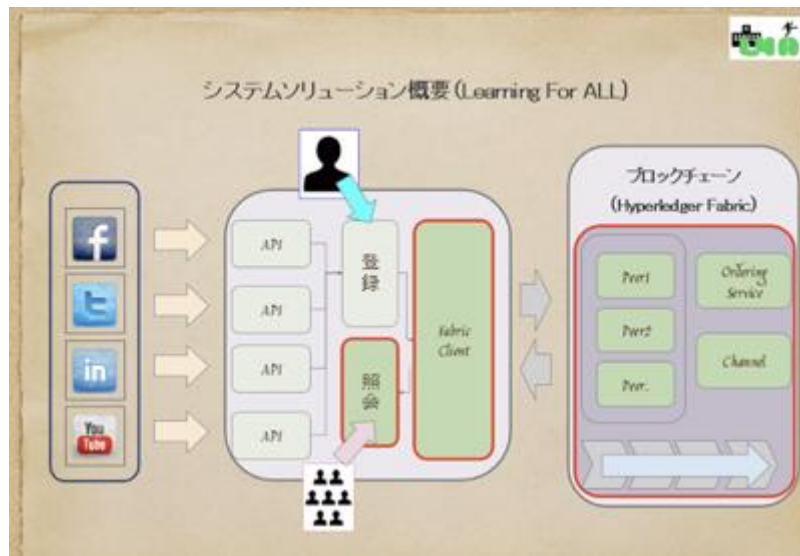
(9) チーム名：わかば

- チームメンバー数：5人（社会人：2人、学生：3人）
- 参加形態：チーム参加
- 内容：自分のスキルの証明、個人のキャリアの検索ができるサービス



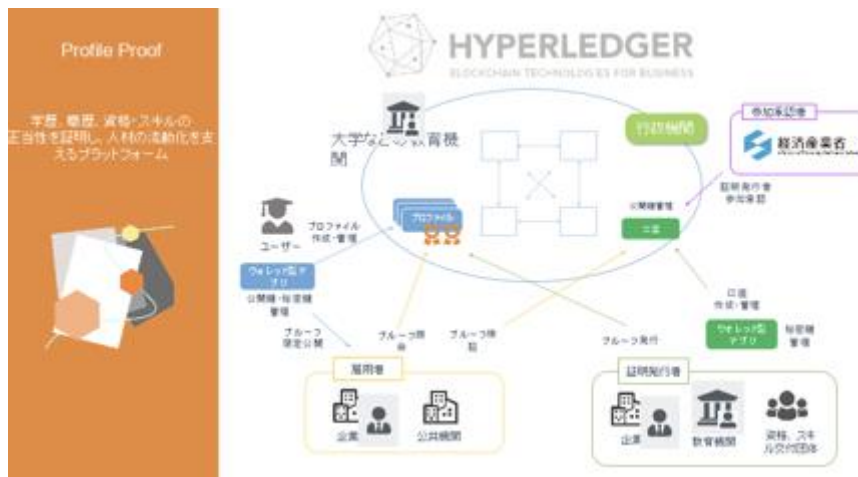
(10) チーム名：森田

- チームメンバー数：5人（社会人：4人、学生：1人）
- 参加形態：個人参加チーム
- 内容：SNS等のインフォーマルな学びの記録サービス



(11) チーム名 : KIOS

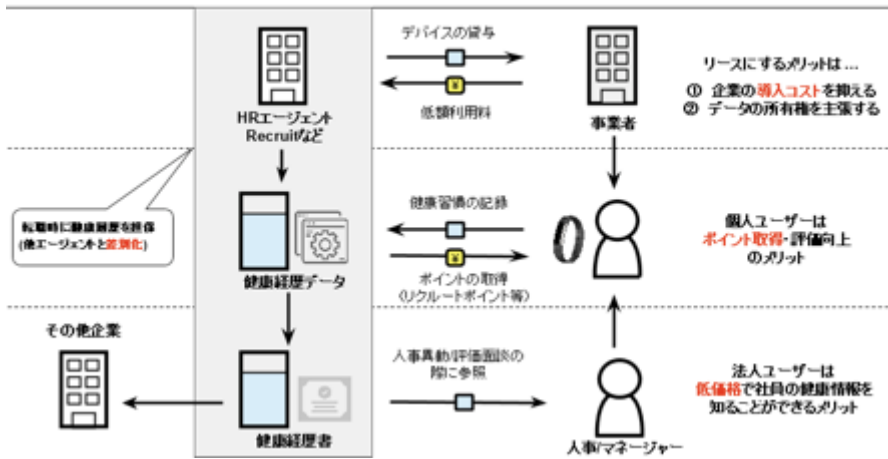
- チームメンバー数 : 4 人 (社会人 : 4 人)
- 参加形態 : チーム参加
- 内容 : 各自の学歴等が 1 つのプロファイルとなり参照できるサービス



(12) チーム名 : HealMes

- チームメンバー数 : 6 人 (社会人 : 4 人、学生 : 2 人)
- 参加形態 : チーム参加
- 内容 : Fitbit を使って健康データを取得し、各自の健康データを利用してトークン発行や人事評価等を行えるサービス

ステークホルダー UX



(13) チーム名：sola (辞退)

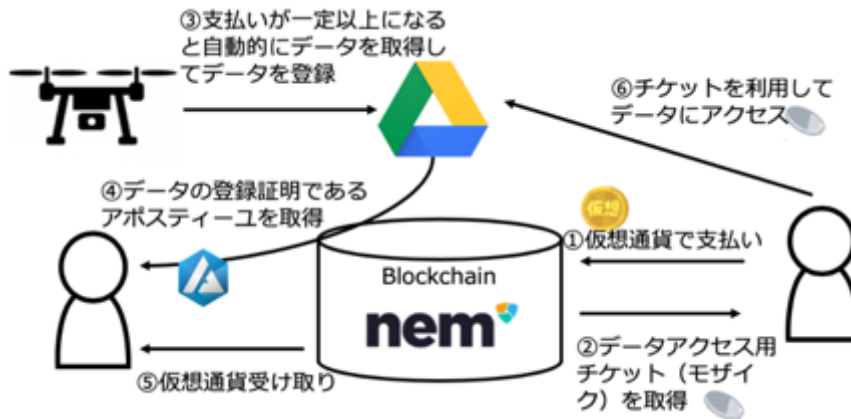
- チームメンバー数：3人 (社会人：1人、学生：2人)
- 参加形態：チーム参加

8.5.2. 「研究データの信頼性確保」テーマ

(1) チーム名：Authorized Moment ※アーリーエッジ賞

- チームメンバー数：5人 (社会人：2人、学生：3人)
- 参加形態：個人参加
- 内容：研究プロジェクトのための仮想通貨によるクラウドファンディング機能を提供し、完全自動化ドローン等によるデータ不正排除や実験結果公証における未改ざんデータを証明するシステム「ソラノメ」
- 実施スキーム
 - 改ざんのされていない動画・画像データを利用したい研究者は自身の Google アカウントでサービスにログイン、利用したいプロジェクトに割り当てられているウォレットに仮想通貨 (今回は NEM) を支払う。
 - 支払い元のウォレットへ電子チケットが届く。
 - プロジェクト記載の実施額まで仮想通貨が集まると、ドローン可動準備。
 - ドローンが作動し、撮影された画像・動画データがリアルタイムでサーバー上に集まる。その後、サーバー側で自動的にブロックチェーンに書き込み、公証機能 (アポステーユ) 登録。
 - ウォレット側に電子チケットを持つユーザーの Google ドライブアカウントに上記の公証されたデータと証明書が共有される。
 - 公証検証機能で、該当データが改ざんされていないものが保証される。

- 検討事項
 - ドローン完全自動化に対して、さらなる安定性やトラブル対策などを継続的に議論する必要がある。
 - ハッカソン後にドローンを360度カメラに置き換えたものを構築中であるが、環境や需要に合わせて入力ソースや排出データを検討してゆく必要がある。



(2) チーム名：六

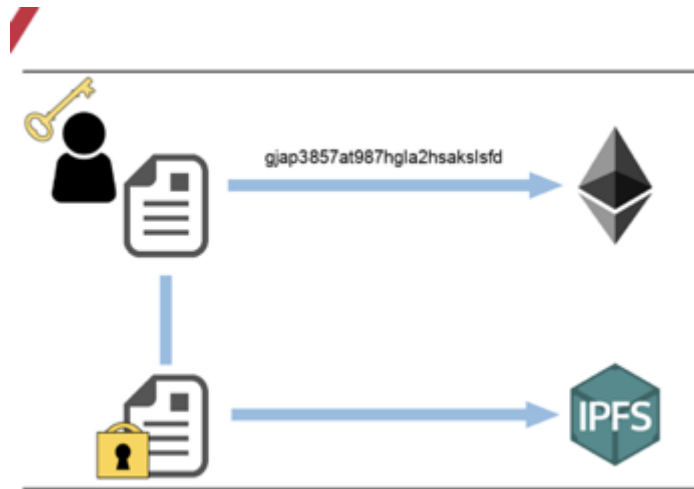
- チームメンバー数：3人（社会人：1人、学生：2人）
- 参加形態：チーム参加
- 内容：論文の剽窃チェックをハッシュ化を用いて安全に行うサービス

研究成果公開の Contract



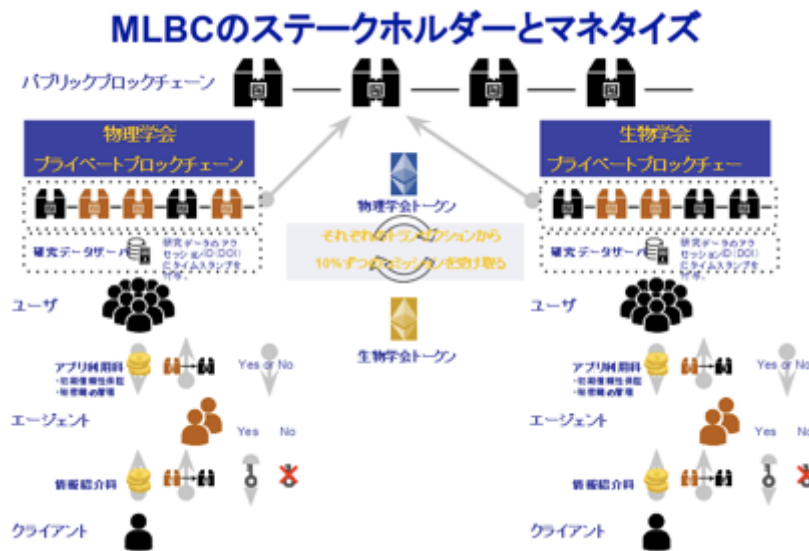
(3) チーム名：Acompany

- チームメンバー数：5人（社会人：1人、学生：4人）
- 参加形態：チーム参加+個人参加チーム
- 内容：研究データの非改ざん性の証明サービス



(4) チーム名 : Multi Layer Block Chain (MLBC) Group

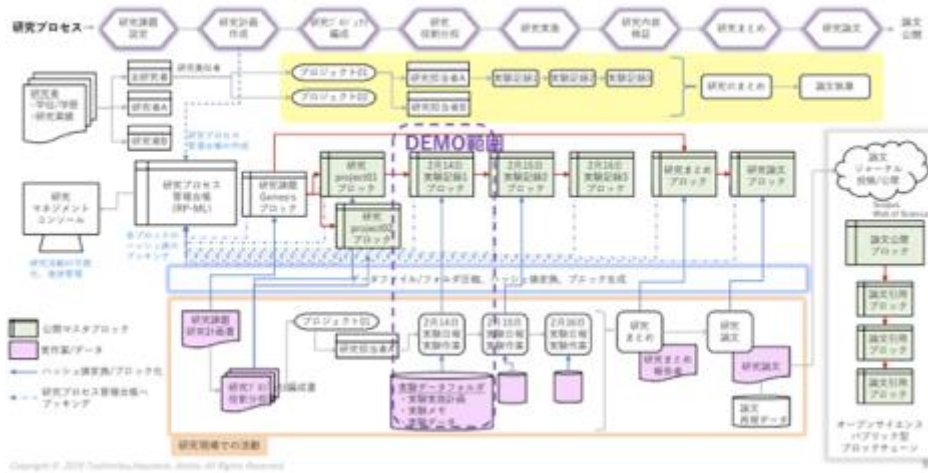
- チームメンバー数 : 5 人 (社会人 : 4 人、学生 : 1 人)
- 参加形態 : チーム参加 + 個人参加チーム
- 内容 : 複数のチェーンを利用し研究の不正防止や異分野の研究との協業を促進するサービス



(5) チーム名 : Kame27s

- チームメンバー数 : 3 人 (社会人 : 3 人)
- 参加形態 : チーム参加
- 内容 : 研究プロセス/データの公開、共有、可視化を促進するサービス

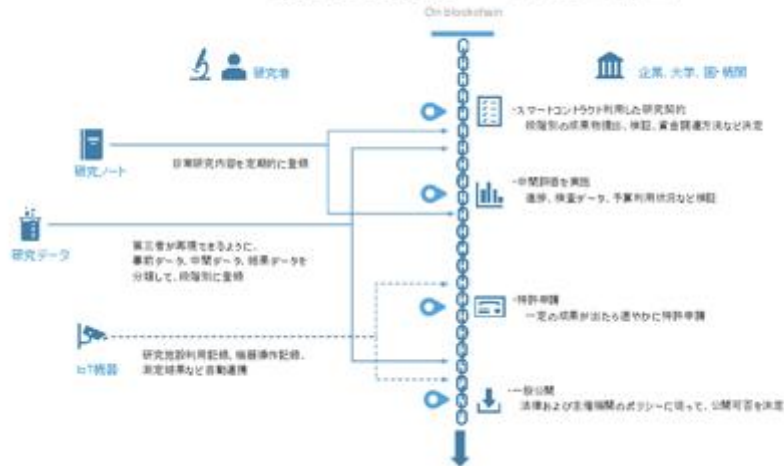
研究データブロックチェーンマネジメントプライベートチェーン (プライベートチェーン)



(6) チーム名 : YYit

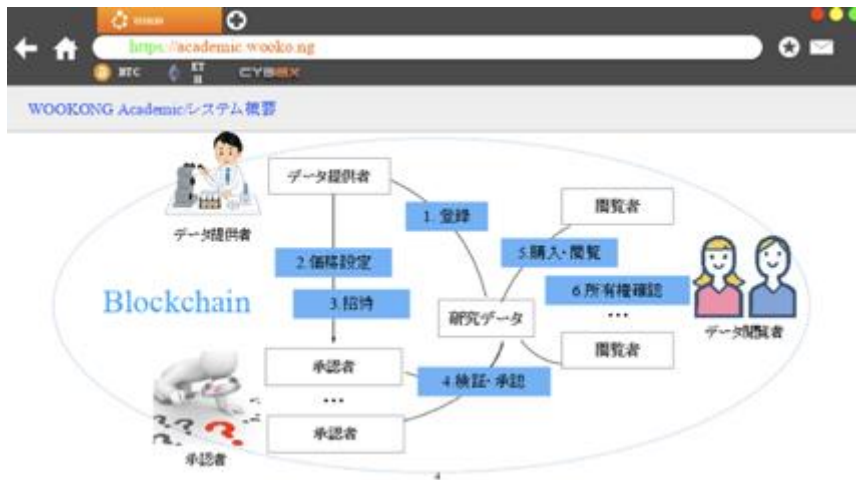
- チームメンバー数 : 5 人 (社会人 : 5 人)
- 参加形態 : チーム参加
- 内容 : IPFS で実装した、研究データの管理サービス

ご提案の研究プロセスの全体図



(7) チーム名 : チーム 20

- チームメンバー数 : 5 人 (社会人 : 5 人)
- 参加形態 : チーム参加
- 内容 : 研究データの検証、閲覧をシームレスに行えるサービス



(8) チーム名：FUJIIWASETOTANA

- チームメンバー数：4人（社会人：3人、学生：1人）
- 参加形態：個人参加チーム
- 内容：人工知能を用いたミスデータの検出サービス

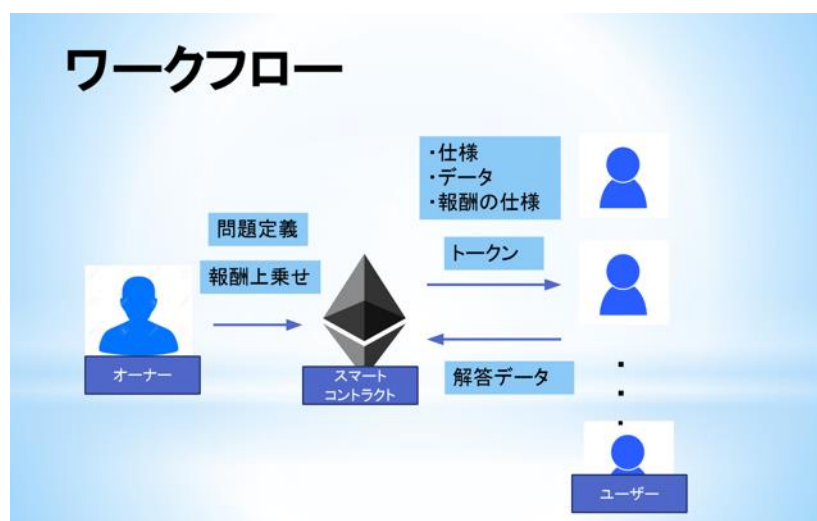
提案するシステムの流れ



(9) チーム名：egateam ※最優秀賞

- チームメンバー数：6人（社会人：4人、学生：2人）
- 参加形態：個人参加
- 内容：臨床試験における解析工程のアウトソースプラットフォーム
- 実施スキーム
 - 臨床試験登録体制や症例データの登録体制については、UMIN等既存の組織で対応可能であるためブロックチェーンは不要だと判断
 - それ以外の工程の中で、解析工程については「第三者のチェックが必要（現状されていない）」「作業が膨大」等の理由により適応可能性があると考えられる

- 解析工程の依頼内容をブロックチェーンに公開してネットワーク参加者へ作業依頼し、ネットワーク参加者が解析業務とその検証作業を行う。その報酬としてトークンを受け取る
- ブロックチェーン技術により、適切なインセンティブ構造を設計、解析工程を全世界の第三者解析技術者に依頼すること（分散化）が可能になり、解析工程の信頼性向上に繋げることが可能だと考えられる
- 検討事項
 - 機密性の高い解析データをどのようにプラットフォームに共有するのか検討が必要
 - 解析結果の検証に対する合意形成のプロセスについて、業務の実情に合わせた仕組みを考える必要がある

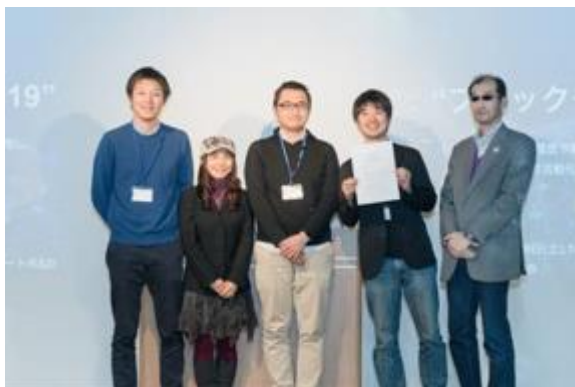


8.6. ハッカソン結果

最大、テーマごとに最優秀賞（産業技術環境局長賞）を1チーム、優秀賞を2チーム、アーリーエッジ賞（学生チームや斬新なアイデアを提案したチームに対して授与）を最大4チームに授与する予定。審査の結果以下のような授与結果となった。

(1) 学位・履修履歴管理テーマ

賞名	受賞チーム	チームメンバー
最優秀賞 (産業技術環境局長賞)	DigiD	真木大樹 浅田真理 田中康平 山村賢太郎
優秀賞	OVP	堀鉄彦 渡辺彰吾 荒巻陽佑 Kamol Mavlonov 須賀祐治
アーリーエッジ賞	該当チーム無し	n/a



最優秀賞：DigiD



優秀賞：OVP

(2) 研究データの信頼性確保テーマ

賞名	受賞チーム	チームメンバー
最優秀賞 (産業技術環境局長賞)	egateam	恵上裕介 伊藤光佑 野上慎一郎 田中翔 新井賢太郎 松本駿
優秀賞	該当チーム無し	n/a
アーリーエッジ賞	Authorized Moment	會田昌史 高梨美佳 橋本豪 山本裕貴 Vu Thuy Trang



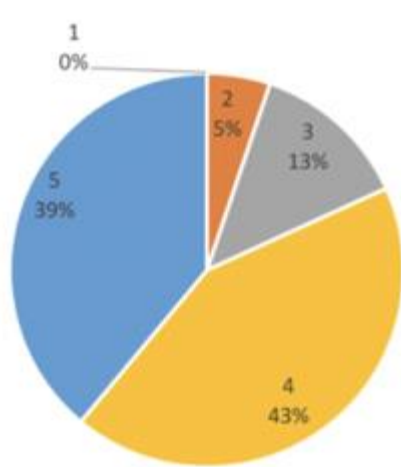
最優秀賞：egateam



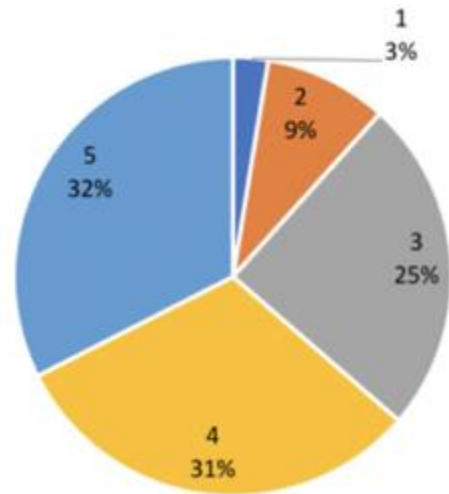
アーリーエッジ賞：Authorized Moment

8.7. アンケート結果の取りまとめ

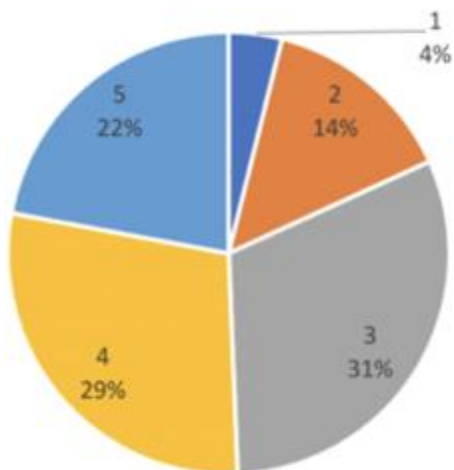
8.7.1. 総合結果



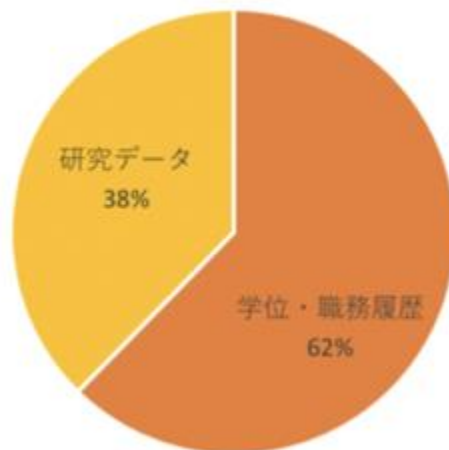
1: 全く満足していない ~ 5: とても満足
図表 8.7 - 1 総合的な満足度



1: 全く満足していない ~ 5: とても満足
図表 8.7 - 2 ワークショップ満足度

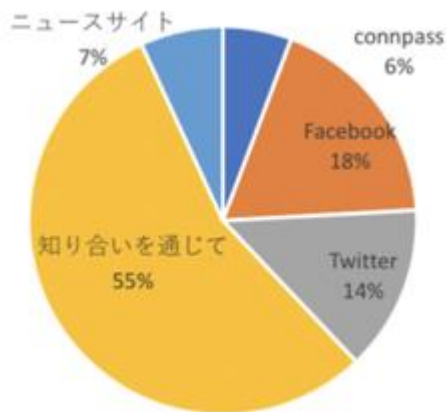


1: 全く満足していない ~ 5: とても満足
図表 8.7 - 3 運営への満足度

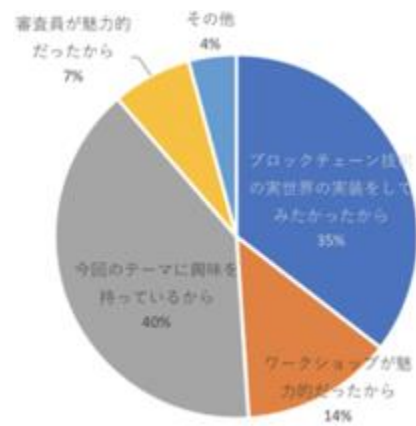


図表 8.7 - 4 テーマ選定の割合

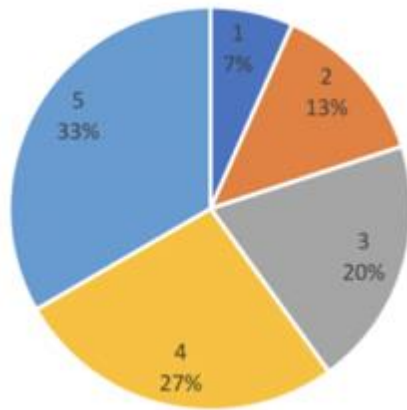
8.7.2. 人材獲得における課題の分析



図表 8.7 - 5 ハッカソンのことを知った経緯



図表 8.7 - 6 参加のきっかけ



(3年以上を5)

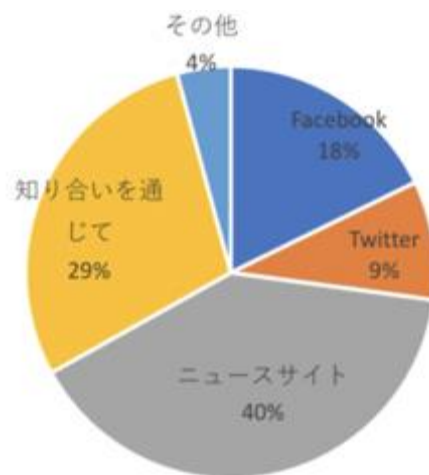
図表 8.7 - 7 ブロックチェーンに関する経験



図表 8.7 - 8 ブロックチェーン普及に当たって日本で不足しているもの



図表 8.7 - 9 ブロックチェーン普及に当たって日本の環境で優れているもの



図表 8.7 - 10 ブロックチェーンに関する情報源

8.7.3. その他の意見

(1) 今後の経済産業省のブロックチェーン領域における活動についてどのような活動を期待しますか
(抜粋)

- ブロックチェーン企業のハブとなるコミュニティ運営
- 開発企業のサポート（複数あり）
- 省内での実際に利用して、発信すること
- 業界のサポートと金融庁と連携したスピーディな法整備。世界水準での取り組み。本当に日本は遅れています
- 今回のようなハッカソンを定期的 to 開催し、広く PR していくこと（複数あり）

(2) 今後、国や社会からどのようなサポートが必要と感じていますか（抜粋）

- サンドボックス拡充（複数あり）
- 規制緩和（複数あり）
- 法整備（複数あり）
- 開発資金提供（複数あり）
- 開発企業と教育機関のマッチング
- 官民関係なくブロックチェーン技術の正しい理解
- 環境整備、実証実験のサポート（複数あり）

(3) 総合的な満足度に関する具体的な事項（抜粋）

- ワークショップは別日程で良かったのではないのでしょうか（複数あり）
- チーム分けにもう少し介入いただいても良かった。バランスを取るため。
- 技術的に興味はあったが、専門分野とは違うので触手が伸びない状態だったので、学ぶ切っ掛けになった。また、実際にモノを作る必要があったので、自身の動機づけにもなった。感謝しています。
- この先学習する必要のあるブロックチェーン技術を具体的なハンズオンで学ぶことができたから
- テーマが非常によかった。実装して終わりではなく運用面まで考える必要があり刺激になった

(4) 今回テーマを実装するにあたっては解決できなかったが、今後解決すべきと感じた課題はありますか

- サービスとしてユーザに提供できるレベルに落とし込む工夫
- 信頼性が低いデータが紛れることへの漠然とした不安と、それでも問題が生じにくくする対策の検討

- 社会実装をいかにやり遂げるか。一般ユーザに届くサービスをつくるのが大切でそのための工夫
- UXを担保しつつブロックチェーンアプリケーションを構築すること
- ブロックチェーンの特性をどの分野でどのように活用しマネタイズするかです
- 何故ブロックチェーンを利用するかということ
- プライバシーの保護
- 本人であることの証明
- 秘密鍵を安全に保持、管理、利用する方法
- 研究データはパブリックに公開されるべきなのか
- データを入力する側の信頼性の担保
- 現実の世界とのつなぎ込みの部分、運用の部分に最も時間をさきました。
- 秘密鍵をなくした場合等想定外の出来事に対する対策

(5) 実装を考えるうえで難しいと思った、ないし悩んだ論点について教えて下さい (抜粋)

秘密鍵の管理方法

- プライバシーとデータライフサイクル
- 学位証明書の導入事例をつくることです
- IPFS だけだと足りない機能があり、拡張か強化した技術探したい
- ブロックチェーンの一般への理解の浸透、既得権益企業がブロックチェーンに抱えるジレンマを乗り越えるか。
- 社会適応させる時の法律的な壁。技術に法律が追いついていない。
- メタマスクウォレットを使うとユーザビリティが下がる
- 知る権利、忘れられる権利、忘れられない権利、等矛盾した権利の共立
- 個人情報の保護とのバランス

9. 総論

ブロックチェーン技術は取引の信頼性を確保するため、中央集権的な第三者機関を不要とする可能性を有する。そのため、ブロックチェーン技術は欧州をはじめとした国際的な個人情報保護に関する法整備の動き等とも連動し、今後の社会システムを大きく変貌させる可能性を有する。また、我々の社会基盤が一層情報化社会へと進むにつれて、ブロックチェーン技術の適用可能性は十分に検討価値があると考えられる。

実際に、今回の調査事業の一環で実施した勉強会においても、「学位・履修履歴証明」及び「研究データの信頼性確保」の両テーマにおけるブロックチェーン技術の適用可能性のある領域が議論された。また同じく本調査事業の中で両テーマに特化し実施したハッカソンでは、想定を上回る方々の関心を集めることができた。まさに今後爆発的に普及する技術の萌芽期を迎えている可能性があると言えるだろう。

他方、その適用可能性のある領域におけるブロックチェーン技術利用の必然性を考える事は極めて重要であるという認識と共に、ハッカソンの参加者からは次の課題点が共有されている。これらの課題に加え、その他の潜在的な課題を順次解決していくことが今後社会実装に向けて必要である。

- 技術面：①秘密鍵の安全な管理・利用の方法、②そもそものデータを入力する際の信頼性確保の方法等
- 経済面：①高いUXの実現、②ブロックチェーン技術利用の必然性、③マネタイズモデル等
- 制度面：①プライバシーの保護、②知る権利や忘れられる権利との整合性等

9.1. ブロックチェーン技術の実社会への適用について

ブロックチェーン技術はまだ発展途上の技術ではあるが、要件によっては様々な適用例が考えられる。まず、「学位・履修履歴証明」テーマにおける適用例として、勉強会では発行体や検証機関を喪失した時の検証におけるブロックチェーン技術の適用可能性に着目した他、ハッカソンではユーザ自身によって自身のアイデンティティを管理できる仕組みである「DID（分散化ID）」という最新の関連技術について複数のチームから提案がなされた。「研究データの信頼性確保」テーマにおいても、長期的な実現可能性として研究活動の解析工程における適用可能性が議論された。

海外に目を向けると、すでに様々なブロックチェーン技術の取組が始まっている。米国のMITでは2017年に一部の修士課程修了者に対してブロックチェーン技術を利用したデジタル修了証授与に関して実証実験を実施。2018年からは卒業生全員に対して該当デジタル修了証授与をオプションとして提供し始めている他、キプロスのUniversity of Nicosiaでも学位の発行をブロックチェーン上で実施している。また、ドイツのData Management Hubでは研究データに特化した分散データ基盤で、

研究データの検索、アクセス、再利用等が可能な基盤を構築している等、海外では数多くの先行事例が紹介されている。

但し、社会基盤として実世界に導入するに当たっては、ブロックチェーン技術の可用性についてより深く考える必要がある。例えば、学位や経歴等の証明においては、50年、60年といった人生の長い時間軸におけるブロックチェーン技術の可能性を検討する必要がある。ブロックチェーン技術だけでなく、クラウド等の技術はまだその歴史が浅く、長期的なデータの管理や認証における基盤として適当かどうかの判断をすることは困難である。従って、ある特定のブロックチェーン基盤から異なるブロックチェーン基盤へのマイグレーションといったチェーンアジリティやアルゴリズムアジリティにおける理解を深め、全く新しいシステム基盤へのマイグレーションの可能性についても検討をしながら進める必要がある。

9.2. 標準化について

ブロックチェーン技術の標準化について国際標準化団体による標準化の動きはあるものの、まだ進捗状況としては初期段階であり、例えばISOではTerminologyを定義している段階と言える。他方、実際の実装にて使用される標準規格の策定には、オープンソース手法を基本とするコミュニティやコミュニティの中心となるコアデベロッパーによる独自の標準化プロセスが使われている。

例えば、イーサリアムではEIP (Ethereum Improvement Proposal の略でイーサリアムのシステム全体の様々な改善提案に関わるプロセス) やERC (Ethereum Request For Comments の略でトークンやスマートコントラクトといったアプリケーションレベルの標準仕様の提案に関わるプロセス) といったプロセスで技術仕様を改善し、標準化を行なっている。ビットコインでも類似プロセスであるBIP (Bitcoin Improvement Proposal) 等が存在する。このような標準化プロセスは実際の実装をベースとしたものであり、採択されるものは単純に標準化されるだけでなく、コミュニティから広く使われる技術仕様となる。

但し、現在当該プロセスにおける我が国の影響は決して大きいとは言い難い状況である。今後、そのコミュニティへの貢献度を上げることで、標準化そのものに対する影響だけではなく、実際世界中で使われていくブロックチェーン技術においても影響力が高められると考えられる。国内主導で行われる標準化は、海外のユーザからは結局使われないケースが多々あり、すでにグローバルのコミュニティが標準策定を行なっているブロックチェーン技術の標準化においては、我が国からのエンジニアがうまく連携し積極的に参加をすることが極めて重要だと考えられる。

9.3. 今後の取組における考察

イノベーションが起きるためには4つの条件が揃わないといけないと言われている。まず、①新しく切り開かれる領域であること、次に、②十分な資金が集まっていること。さらに、③リスクがあるチャレンジが可能であること、最後に④自由活発な議論が行えることである。今回の調査事業の中で開かれたハッカソンは資金に関する条件以外が揃った場合であったが、このような環境においても実際に21のアプリケーションが生まれることが確認できたことは重要な成果に考えられる。

前述の通り、ブロックチェーン技術の適用を検討する上で、該当適用例におけるブロックチェーン技術利用の必然性を考慮する必要がある。例えば、SQL データベース等の既存技術と単純に比較した場合、すでに既存技術に慣れているユーザからすると、ブロックチェーン技術の妥当性を見出すのは難しい。但し、様々な実証実験を重ねていくことで、多様な可能性が生まれ、既存技術とは違う分類として今は考えられないブロックチェーン技術の必然性が生まれてくる可能性もあると考えられる。

このような社会環境を組成するために、また、海外ではすでに複数の適用事例が実施されていることもあり、我が国においてもこのような動きに遅れず、むしろ先導していくためには、今後次の取組が必要と考えられる。

まず、「学位・履修履歴・職歴管理」及び「研究データの信頼性確保」テーマにおけるブロックチェーン技術の先行的な導入に向けた検討をより深化させるため、学校や企業等市場の積極的な参加の下、今回開催したハッカソン等の実証実験を実施できる環境を官民が連携して整備すること。

また、世界中のブロックチェーン技術適用の動きと歩調を合わせるためにも、我が国の技術者コミュニティに対して今回のようなハッカソンといったきっかけを提供しつつ、技術仕様の策定といった今後のブロックチェーン技術の標準化に貢献できる環境を整備すること。

最後に、今回のような調査事業が単純な報告書の提出で終わらないよう、1、2年後に、今回生まれた21のアプリケーションが実際どのような成果を出すことができたのか、何をエンハンスすべきだったのか、また今後の運用についてどのような工夫が必要なのか等を振り返ることが重要になってくると考えられる。

平成30年度産業技術調査事業

(国内外の人材流動化促進や研究成果の信頼性確保等に向けた大学・研究機関への
ブロックチェーン技術の適用及びその標準獲得に関する調査)

報告書（概要版）

2019年3月

株式会社リクルートR&D

アジェンダ

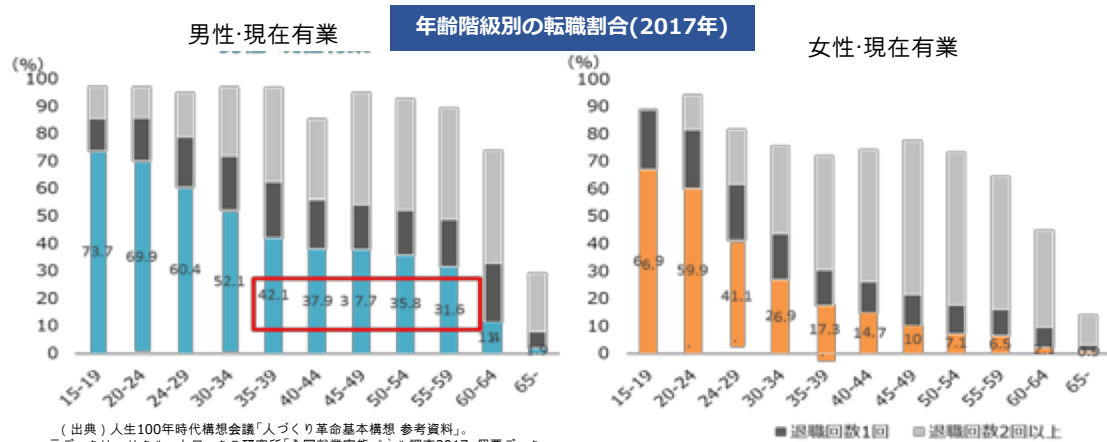
1. 本調査事業の背景及び目的	3P
2. ブロックチェーン技術の活用案	6P
3. 標準化に関して	9P
4. 国際動向調査	10P
5. ハッカソン開催概要及び主な成果物の紹介	12P
6. 総論	20P
Appendix	23P

1-1 「学位・履修履歴証明」テーマに置ける社会的背景

急速な技術革新を背景とし人材流動化を前提とした学習履歴・学位の真正性確保が求められる時代へ

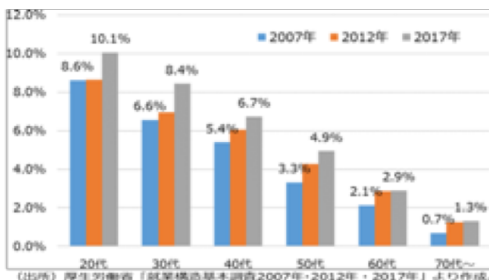
- AIを始めとした技術革新を背景として、**産業構造が速くかつ劇的に変化**する時代となり、転職や副業・兼業といった多様な働き方が広まってきたところ。
- 学位授与機関においては、少子高齢化を背景に、学校間の連携や統合が今後加速していく見込み。今後人材の流動化も進み多様な働き方が普及する中、例えば**存続しなくなった大学やスタートアップでの学位・経歴等の真正性を確保し、これらをむしろ積極的に活用していくうえでも、学位・経歴等に関する新たな信頼性確保の仕組みが必要**と考えられる。

①多様な働き方の普及



(出典) 人生100年時代構想会議「人づくり革命基本構想 参考資料」。
元データは リクルートワークス研究所「全国就業実態パネル調査2017」個票データ。

年代別の副業希望者割合(2017年)



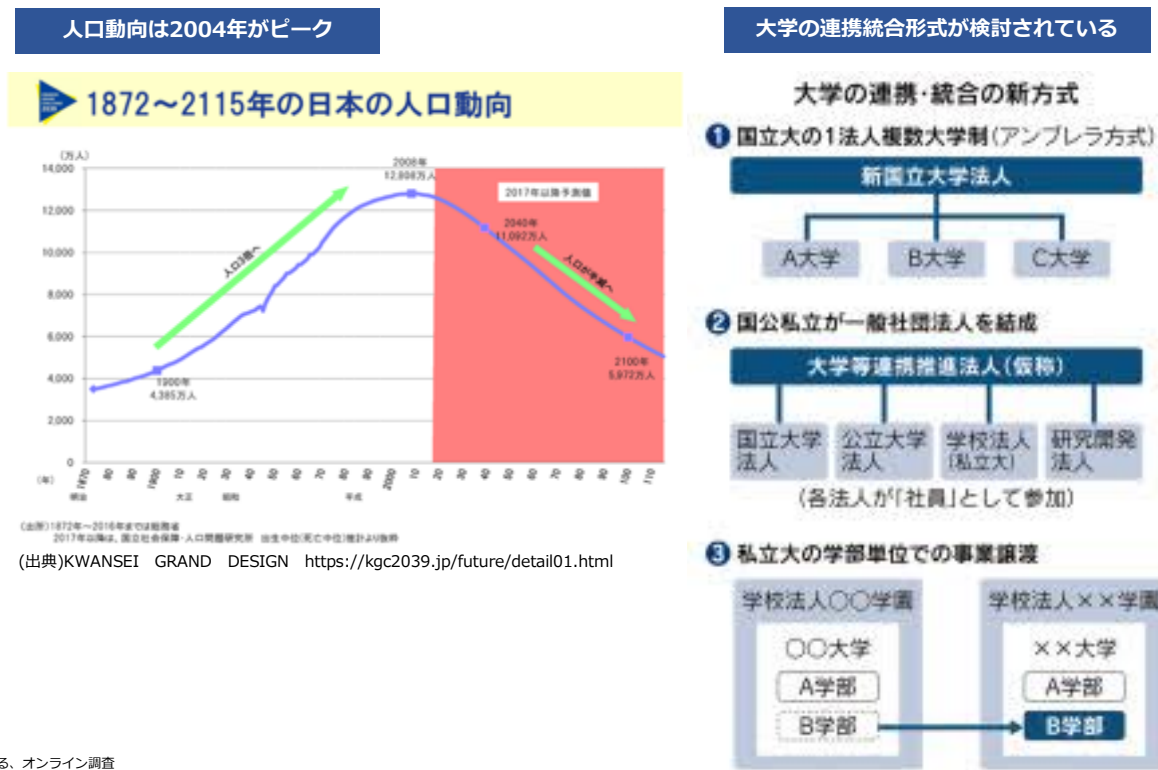
(出所) 厚生労働省「就業構造基本調査2007年・2012年・2017年」より作成。

フリーランス人口の増加



(出所) 株式会社ランサーズ「フリーランス実態調査 2018」
(注) 1) 過去12か月に仕事の対価として報酬を得た全国の20-69歳男女に対する、オンライン調査(有効回答数3,096人)をもとにフリーランス規模を想定。
2) 括弧内は、労働力人口に対する比率。
3) アメリカの調査は「Freelancing in America」に基づく。

②学位授与機関の連携・統合が進む



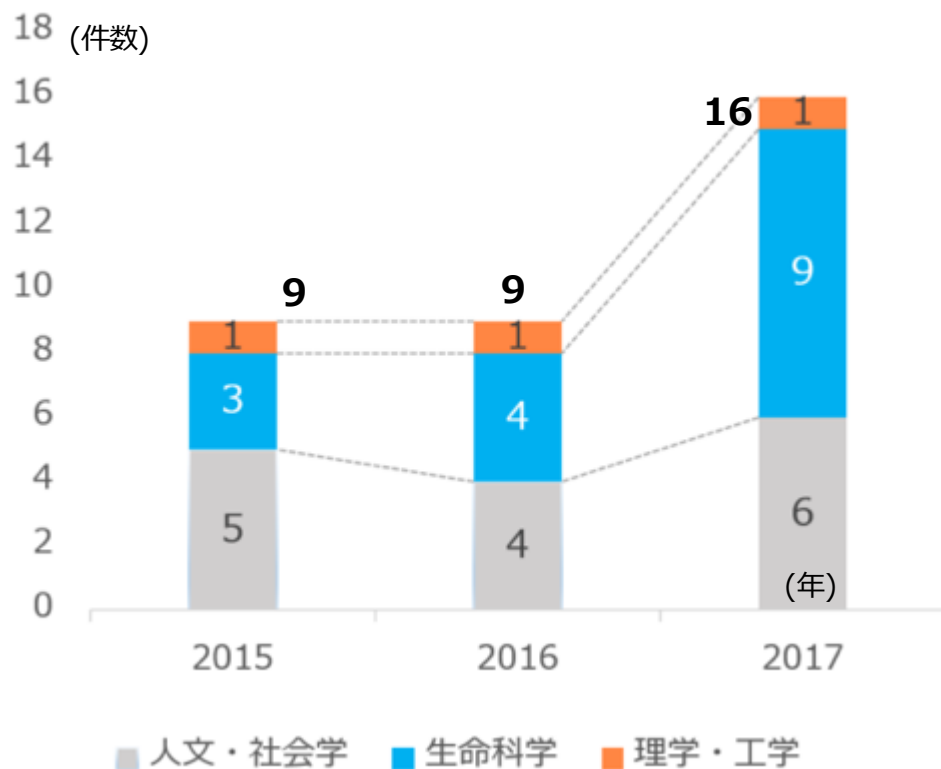
(出典) KWANSEI GRAND DESIGN <https://kgc2039.jp/future/detail01.html>

(出典) 日経新聞 2018/11/26 15:24時点
<https://www.nikkei.com/article/DGXMZO38171810W8A121C1CR8000/>

1-2 「研究データの信頼性確保」テーマに置ける社会的背景 研究データ等の不正に関する状況（研究機関・企業）からデータの真正性が求められる時代へ

- 我が国の研究機関や企業におけるデータの改ざん等の**データ不正は年々増加傾向**。
- サイエンス誌によると、撤回論文が多い研究者上位10名のうち半数が日本人であり、かつ日本企業においてもデータ不正が頻発するなど、**学术界・産業界双方においてデータ改ざん等が問題となっており、産業競争力を低下させる恐れ**⁽¹⁾。

大学等の研究活動における不正⁽²⁾



企業におけるデータ不正⁽³⁾

○近年の主な事例

企業名	概要
住友重機械工業株式会社	定期検査報告書において実際の検査結果と異なる内容の記載等の不適切行為（2019年）
KYB株式会社	建築物用免震・制振用オイルダンパー検査工程における性能検査記録データの改ざん（2018年）
株式会社TATERU	従業員が顧客から提供を受けた預金残高データを改ざんし、融資審査を通りやすくしていた等の不祥事（2018年）
株式会社クボタ	鋼板等の生産設備で使用する消耗部品（圧延用ロール）の検査成績書に実際の検査結果と異なる数値を記載するなどの不適切行為（2018年）
日立化成株式会社	産業用鉛蓄電池の一部製品の検査成績書に不適切な数値の記載を行っていた等の不適切行為（2018年）
三菱マテリアル株式会社	連結子会社である三菱電線工業株式会社、三菱伸銅株式会社におけるシール材の寸法、物性等の検査記録データの書き換え等の不適切行為（2017年）

(1) Researcher at the center of an epic fraud remains an enigma to those who exposed him: <https://www.sciencemag.org/news/2018/08/researcher-center-epic-fraud-remains-enigma-those-who-exposed-him>

(2) 文部科学省公表事例に基づき経済産業省が集計 ※上記には、ねつ造、改ざんのほか、盗用による研究不正も含まれる。

(3) Sustaina 企業不祥事 不正問題 検索: <https://www.sustaina.org/ja/scandals/?ScandalSearch>

1-3 ブロックチェーン技術の可能性及び本調査事業の目的

- データの透明性の向上やトレーサビリティの確保、改ざん防止などを特徴として有する**ブロックチェーン技術は、経済活動の基盤となる取引相手の信頼性を確保する技術**として近年注目を集めており、**中央集権的な第三者機関を不要とする可能性**がある。
- ブロックチェーン技術は、幅広い分野で社会システムを変換させる可能性がある**ことが指摘されているが、先に示した社会的背景を踏まえれば、「**学位・履修履歴証明**」及び「**研究データの信頼性確保**」といったテーマにおいても、**本技術を適用できる可能性がある**と考えられる。

現在



中央集権型の信頼性確保の仕組み

- ポイント発行者：前払式支払手段の電子マネー管理
- エスクロー機関：Eコマース等の電子商取引管理
- 登記簿管理者：土地登記等の権利所有者管理
- 仲介者：シェアリングエコノミーのマッチング管理
- 中央銀行：通貨の発行主体であり、通貨の管理

2025年以降



分散型



IBM社資料をもとに経済産業省で加工

調査の目的

「学位・履修履歴証明」

「研究データの信頼性の確保」

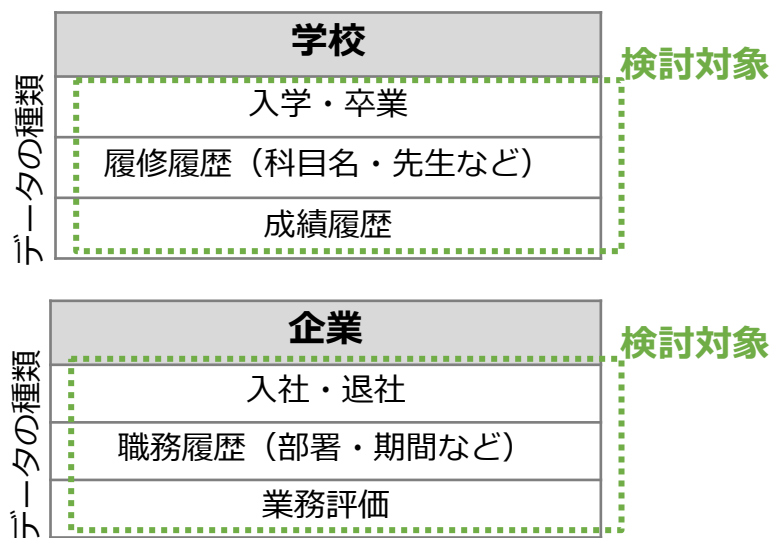
- 上記の2テーマにおいて、ブロックチェーン技術の可能性及び国際的な標準化の取組等についてブロックチェーン技術である必然性を厳しく精査しつつ検討を深める。
- また、ハッカソン開催を通じて、実際の社会実装へと繋がるようなアウトプットの創出を期待する。

(出典) 平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備
ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

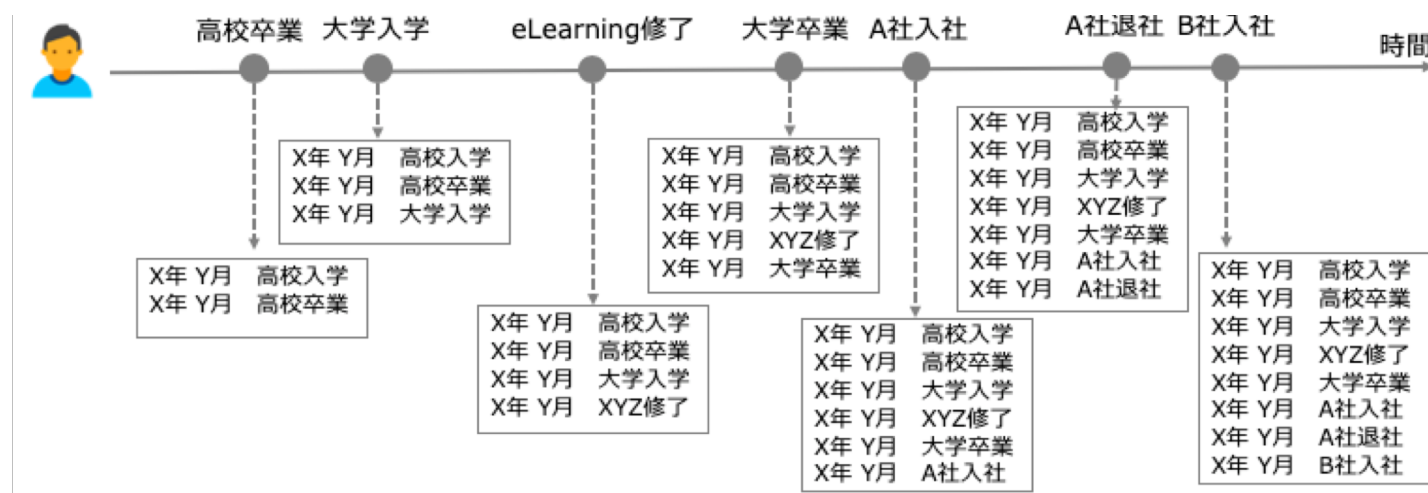
2-1-1 「学位・履修履歴証明」のテーマ：活用案と想定される課題①

- 学校への入学・卒業やe-Learningなどの修了履歴、そして企業への入社・退社などの**ファクトベースの客観的なデータをブロックチェーン上に格納すること**を想定。格納されたデータは、個人がシステム上から直接、特定の企業等に開示できるようにする。多くの参加者を得られれば、**信頼ある人材基盤が構築され、全世界において円滑な人材流動化が実現**。
- ブロックチェーン上に載せるデータの種類の種類は、本活用案における検討すべき課題の一つ。例えば、学校の成績や企業における評価などは組織間で判断軸が異なり、一概に比較できない。

①本活用案における検討対象のデータの種類（学校・企業）



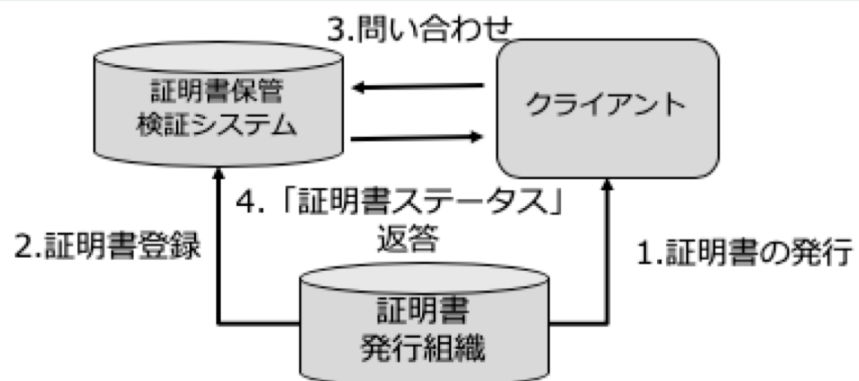
②ブロックチェーン上に格納される客観的なデータの例



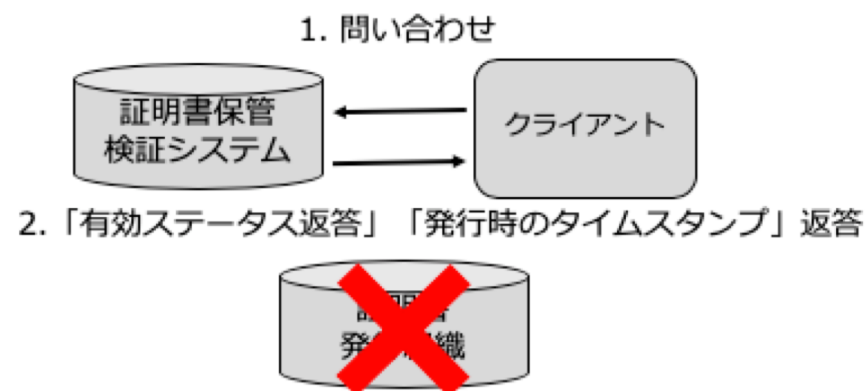
2-1-2 「学位・履修履歴証明」のテーマ：活用案②

- 証明書の真正性を長期的に検証することは現在の仕組みだけでは解決困難な課題として認識されている⁽¹⁾。
- 中央集権的な仕組みで多く用いられているPKI（公開鍵暗号基盤）の標準規格であるX.509は、検証する「時点」での証明書の正当性を確認可能にする仕組みであり、その「時点」で過去に発行した証明書の発行者が不在の場合は、証明書の真正性の正しい検証が不可能である。したがって、**過去に遡って証明書の真正性を正しく検証できるスキームを構築するには以下4つの要件が必要**だと考えられる。
- PKIの永続のための手段として、**その「時点」のPKIスナップショットをブロックチェーンに載せること**が考えられる。

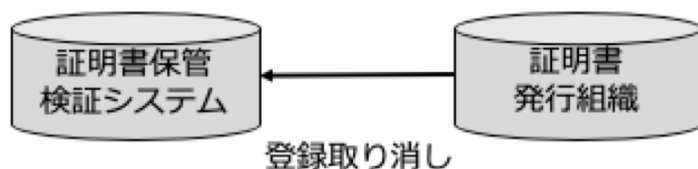
1. 発行された証明書が有効であるかクライアント側が検証可能



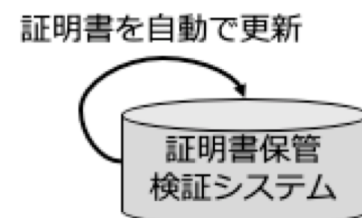
2. 証明書発行組織が解体した場合にも有効な証明書であると立証可能



3. 証明書発行組織による証明書の取り消しが可能



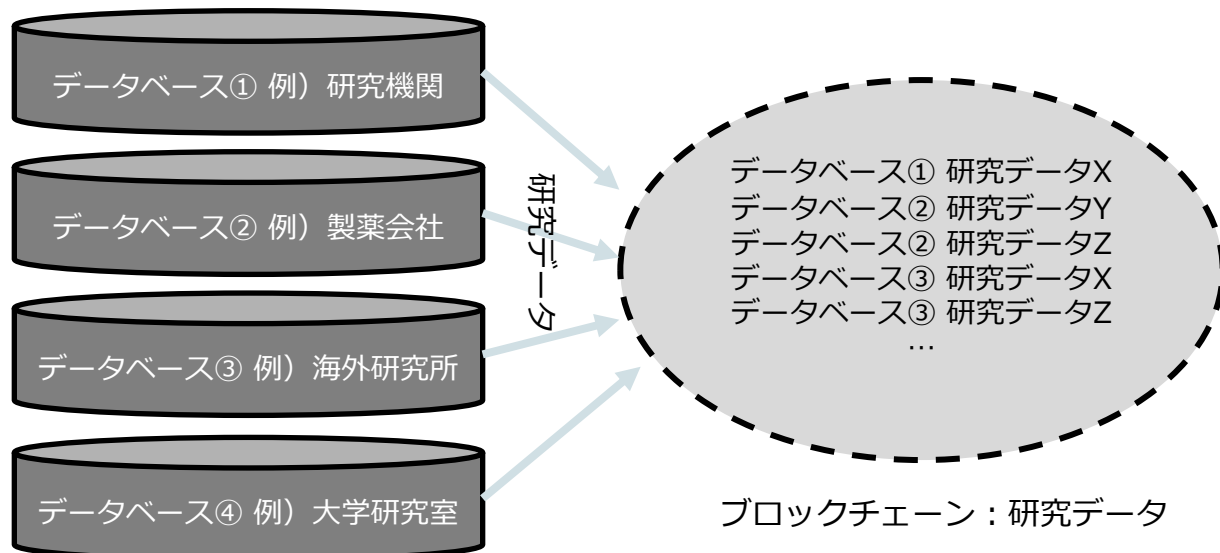
4. 証明書が長年にわたり利用されるため、証明書の自動更新が可能



2-2 「研究データの信頼性確保」のテーマ：活用案

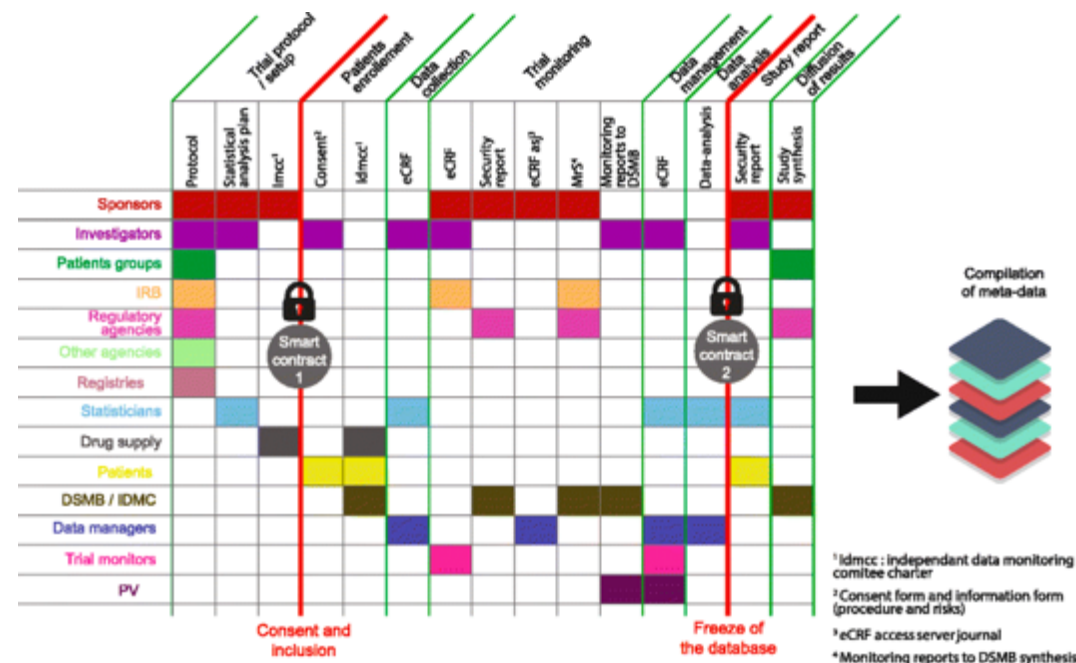
活用案①

- 概要：**(1) 大学等の研究機関、製薬会社など研究データを有する民間企業、海外の研究所などのデータプロバイダから、研究の生データ（ハッシュ値等）を分散台帳に格納することで、改ざん不可能な台帳内に情報を残すことができるため、遡ってのデータの改ざんができなくなる、(2)例えば「臨床研究法」の適用分野等、既に中央集権的なデータベースが構築されている分野以外の領域から実施することを想定。
- ブロックチェーン技術の適用可能性：**(1) 国や属性が異なるデータプロバイダのデータを取り込む際に、特定の中央集権的機関への依存が少なく済む、(2)ハッシュ値での保存であれば、データを誰かに所有させることなく、分散化した形で所有することで、データ共有に対するハードルを下げる事が可能（Appendix A参照）



活用案②

- 概要：**ブロックチェーンのスマートコントラクト技術を活用し、研究プロセスそのものにおいても検証を行いながら進む基盤を想定。例えば、必要な研究データの種類や質が揃わない場合、次のプロセスに進まないようなスマートコントラクトを組むことで、研究プロセス全体における整合性の向上に繋げる（Appendix B参照）



(出典) Blockchain technology for improving clinical research quality : <https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z>

3-1 標準化に関して

ブロックチェーンの標準化については、国際標準化団体における標準化の動きと、民間のオープンソースのコミュニティによって運営される独自の標準規格構築の動きが存在。現在は、**主に後者の民間における標準規格化（例えば、イーサリアムのERC-20）の動きが活発。**

標準化団体によるブロックチェーン技術における標準化の流れ

- 国際標準化団体によるブロックチェーン技術の標準化の動きはあるものの、まだ具体的な標準化の動きには至っていない。例えば、W3Cにおいてはユースケースなどは時期尚早という風潮があるほか、ISO/TC307においても標準化には時間が必要だとの認識から、Terminologyから着実に固めていく方針（Appendix C参照）

ブロックチェーンプロトコル独自の標準化プロセス

- ISOなどの標準化に先駆けて、BitcoinやEthereumは独自の標準化プロセスを、それぞれBitcoin Improvement Proposal (BIP)、Ethereum Improvement Proposal (EIP) という名称で実施している（Appendix D参照）

4-1 国際動向調査：学位・履修履歴管理

海外の大学や企業において、ブロックチェーン技術の活用事例が確認されている

アジア

- **マレーシア：**
 - Ministry of Education (MoE) の主導で国内の6つの大学を結び、学位の管理などを行うコンソーシアム型のブロックチェーン基盤e-scrollの構築を発表⁽¹⁾

アメリカ

- **アメリカ合州国**
 - MITでは2018年の卒業生に対して、紙ベースの学位と共にDigital Certificateの受領オプションを提供⁽²⁾
 - Blockcertsはブロックチェーン基盤の学位認証ソリューションを提供。MITやイギリスのUniversity of Birminghamなどがこれを導入⁽³⁾
 - ConsensysのプロジェクトであるuPortでは、分散型のアイデンティティ管理システムを提供⁽⁴⁾

ヨーロッパ

- **イギリス：**
 - University of BirminghamではAcademic Certificate Authentication Systemの構築及び検証実験を実施⁽⁵⁾
 - Open Universityは、同大学のMOOCプラットフォーム（FutureLearn）にて、ブロックチェーン基盤上でマイクロ単位を発行⁽⁶⁾
 - GradBase社は、CertificateもしくはCertificateのポートフォリオが検証できるQRコードを発行、ユーザーはそのQRコードを自由に共有⁽⁷⁾
- **キプロス：**
 - University of Nicosiaでは、ブロックチェーンのコースを修了した学生に対し、ブロックチェーン基盤のAcademic Certificateを発行⁽⁸⁾

(1) Ministry of Education in Malaysia : <https://www.moe.gov.my/index.php/en/arkib/pemberitahuan/2018/4587-kenyataan-media-kpm-lancar-sistem-e-scroll-menggunakan-teknologi-blockchain-atasi-masalah-ijazah-palsu>

(2) MIT News: <http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017>

(3) Blockcerts : <https://www.blockcerts.org/>

(4) uPort: <https://www.uport.me/>

(5) University of Birmingham: <https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf>

(6) OpenUniversity: <https://blockchain.open.ac.uk>

(7) Gradbase: <https://gradba.se/en/>

(8) University of Nicosia : <https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain>

4-2 国際動向調査：研究データの信頼性確保

- ヨーロッパやアメリカを中心に、サイエンス系におけるブロックチェーン技術の多様な適用可能性が試されている

研究サイクル



研究サイクルにおける多くの部分（オレンジ色）において、様々なブロックチェーン技術の適用可能性が検討できると考えられる

海外プロジェクトの例

ドイツ

- **Blockchain for Science** ⁽¹⁾：ドイツをベースとし、研究領域における様々なブロックチェーンの適用可能性を研究。2018年11月にベルリンで第1回Blockchain for Scienceカンファランスを主催し、ハッカソンも開催
 - Smart Privacy：スマートコントラクトを使って被験者のデータ管理を行うことで、例えば、誰が、いつ、どの程度の期間でデータを閲覧可能かなどをコントロール
 - Internet of Research Things：研究デバイスからのデータを直ちにブロックチェーンに記録することでデータの改ざんを防ぐ
- **Data Management Hub** ⁽²⁾：ドイツをベースとする研究データに特化した分散データ基盤で、研究データの検索、アクセス、再利用などが可能な基盤構築を目指す

アメリカ合衆国

- **MIT OPEN TrialChain** ⁽³⁾：臨床試験におけるデータ共有基盤。利用者はクエリを同基盤に投げることで、被験者の情報が匿名化された安全な答えを得ることが可能
- **Enigma** ⁽⁴⁾：Enigmaプロジェクトでは秘匿した状態でデータ操作が可能となるシステムを公開
- **Dat** ⁽⁵⁾：分散型のデータ共有の仕組みであり、Datプロトコルを通して共有される全てのデータは、公開鍵によって暗号化される。自身の公開鍵を任意の送信相手に伝えることによって、送信相手はデータを閲覧可能

カナダ

- **Lyfescience** ⁽⁶⁾：製薬会社やその他の臨床試験関係者が被験者のデータや調査結果を安全かつ分散的に収集・管理する方法を実現するため、スマートコントラクトを使用して最適化および自動化する方法を提供

(1) Blockchain for Science : <https://www.blockchainforscience.com>

(2) Data Management Hub : <http://damahub.org/>

(3) MIT OPEN TrialChain: <https://www.media.mit.edu/projects/open-trialchain/overview/>

(4) Enigma: <https://enigma.co>

(5) Dat <https://datproject.org>

(6) Lyfescience: <https://lyfescience.com/>

5-1 ハッカソン開催の背景及び実施結果

実施背景：ブロックチェーンにおける社会実装の現状

- 現状はユーザー側・ベンダー側ともに各種PoC（※）により、主として技術的な課題を洗い出している状況（コスト効率化の検討までには至らず）。（※）Proof of Concept（概念実証）
- この原因として、①ブロックチェーン技術そのものが発展途上であること（安全な鍵管理手法等）、②安全な形式でのブロックチェーンの高速化や適用範囲の拡大のモデル構築・技術開発が進んでいないこと、③必要な法整備が行われていないこと、④ブロックチェーンに関する技術者等の人材が不足していること、等が挙げられる。

「学位・履修履歴管理」及び「研究データの信頼性確保」テーマにおいて、社会実装に向けた様々な可能性を発掘、技術的・社会的課題を理解すると共に、我が国におけるブロックチェーン技術の人材育成を目的にハッカソンを開催

実施結果、期待を上回る調査結果を獲得

- 当初予定した募集人数は70名であったが、その2倍を超える142名が応募。最終的には98人が参加。22チームから21のアイデアや成果物が発表され、ブロックチェーン技術の課題への理解を深化させると共に、上記両テーマにおける社会実装への可能性を確認。
- ハッカソン期間中に、参加チームからイーサリアムの国際コミュニティに対して標準規格への提案が行われる等、今後のブロックチェーン技術の国際標準化を我が国が先導して貢献していくための糸口を確認。

5-2-1 ハッカソン開催の概要

(1) 開催概要

- 日時：2019年2月9日（土）及び2月16日（土）～17日（日）
- 場所：Lifull Hub（東京都千代田区麹町1-4-4 2F）
- 参加料：無料、ただし参加条件並びにプロトコル等について制限有り（※）既存のトークンを利用する場合には、金融庁の登録を受けた仮想通貨交換取引業社で取引がされている仮想通貨及びトークンのみ利用可能

(2) 表彰

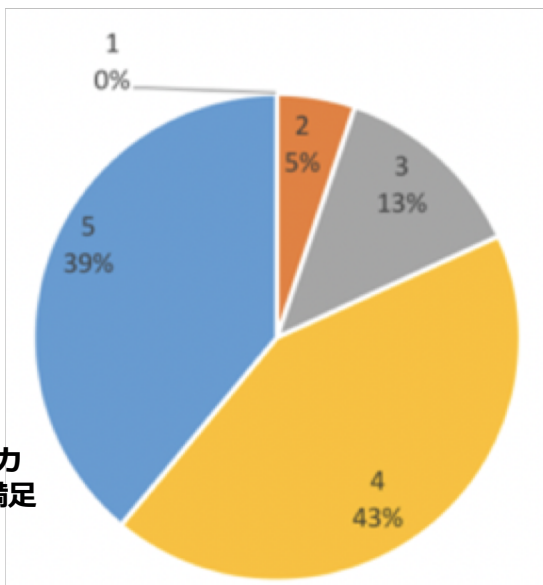
- 学位・履修履歴管理テーマ
 - 最優秀賞（産業技術環境局長賞）：1チーム
 - 優秀賞：1チーム
- 研究データの信頼性確保テーマ
 - 最優秀賞（産業技術環境局長賞）：1チーム
 - アーリーエッジ賞：1チーム

（※）アーリーエッジ賞：学生チームやアイデアが斬新なチームに対して授与

(3) 参加者の統計及びアンケート結果

- 全体応募者数：142名（1月31日正午〆切）
- 事務局による参加選定者数：106名
- 参加決定者数：98名（学生：25名、社会人：73名）
- チーム数：22チーム
 - 学位・経歴証明テーマ：13チーム
 - 研究データの信頼性確保テーマ：9チーム

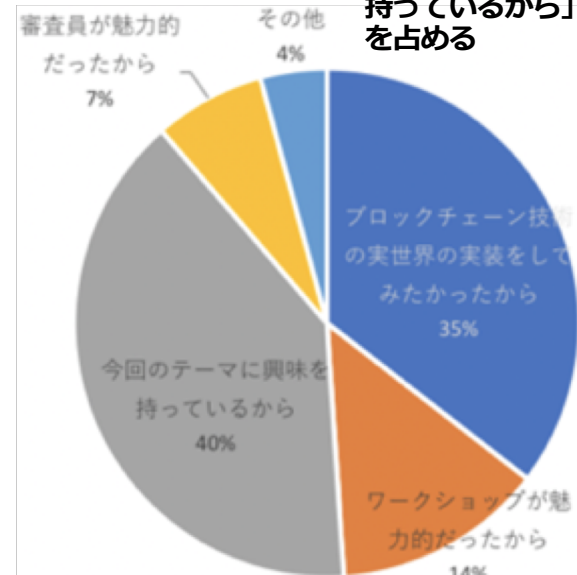
82%がハッカソン参加に満足している



総合的な満足度

（1：全く満足していない～5：とても満足）

「ブロックチェーン技術を実世界で実装してみたいから」及び「テーマに興味を持っているから」が75%を占める



参加のきっかけ

5-2-2 ハッカソン開催の概要

(4) 審査基準

① 問題着眼点・着想点

—着想した問題が明確で新しく、その問題の解き方が斬新か

② 実行・実現可能性

—実際に世の中で利用される可能性が高いサービスか

③ 完成度・動作性

—コンセプトで提示された機能が実装されているか

④ プレゼンテーション力

—端的に問題点, 解決方法, 実装が語られているか

⑤ ハッカソンテーマへの適合性

—「学位・履修履歴・経歴の管理」及び「研究データの信頼性確保」テーマに沿ったアイデアやアウトプットで、テーマ特有の課題を解決しているか

(5) 審査員リスト

氏名	所属	審査
楠正憲 (審査委員長)	JapanDigitalDesign株式会社 CTO ISO/TC307ブロックチェーンと電子分散台帳技術に係る専門委員会 国内委員会委員長	1次・最終審査
江草陽太	さくらインターネット株式会社 執行役員技術推進統括担当	最終審査
村井宏行	株式会社リクルート R&D投資室長	最終審査
河合健	アンダーソン・毛利・友常法律事務所 パートナー	最終審査
岸上順一	室蘭工業大学 教授 W3C (WorldWideWebConsortium) ボードメンバー	1次・最終審査
坂下哲也	一般財団法人日本情報経済社会推進協会 (JIPDEC) 常務理事	1次・最終審査
鈴木絵里子	FrescoCapital パートナー Mistletoe 投資部ディレクター	最終審査
谷口耕平	株式会社Chaintope BlockchainEngineer GoBlockchainEngineeringCommunityco-founder	1次・最終審査
千葉吉輝	UMIN (大学病院医療情報ネットワーク) 研究センター J3C (JapanCDISCCoordinatingCommittee) ViceChair	最終審査
平野淳也	株式会社HashHub COO	1次・最終審査
福泉武史	ソフトバンク株式会社技術戦略統括 ITサービス開発本部長	最終審査
富士榮尚寛	伊藤忠テクノソリューションズ株式会社 西日本ビジネス開発チームチーム長代行 一般社団法人OpenIDファウンデーション・ジャパン 理事	1次・最終審査

※ 順不同・敬称略

5-2-3 ハッカソン開催の概要

(6) ワークショップ開催及び参加者数

英国・アイルランド・キプロス・ドイツにおいて、ブロックチェーン技術の活用実績のある団体等から、実際の適用事例についてご紹介いただくと共に、イーサリアムやNEM、Hyperledger等の技術的なワークショップを実施。ハッカソンの参加者に対し、アイデアや技術的なアドバイスを提供。

実施日	ワークショップのタイトル	講演者及び所属
2月9日	組織におけるアイデンティティ管理に関する基本的な考え方	富士榮尚寛 一般社団法人OpenIDファウンデーション・ジャパン理事
2月9日	OpenBlockchain: How the Open University is applying Blockchain Technology to Adult Education	Michelle Bachler Open University(英国) Research & Innovation Software Manager
2月9日	Digital Certificates for academic and professional history	Soulla Louca Professor, Director, Blockchain Initiative at University of Nicosia(キプロス)
2月9日	Ethereumの概要及びハンズオンワークショップ	谷口耕平 株式会社Chaintope Blockchain Engineer
2月9日	簡単に利用でき堅牢なNEMブロックチェーン・初心者向けワークショップ	木村優、松原正佳 LCNEM株式会社 代表取締役、NEM Foundation
2月9日	Data, Policies and Algorithms	Denis Parfenov (Data Management Hub Founder, Open Data Governance Board member(アイルランド))
2月9日	Ethereum Getho	佐藤大輔 株式会社Popshoot Co-Founder & CTO
2月9日	コンソーシアム型ブロックチェーン及びHyperledger Fabric	田中健介 株式会社NTTデータ ITサービス・ペイメント事業本部方式基盤統括部課長代理
2月9日	Ethereum Identity: ERC-725	真木大樹 BlockBase株式会社 代表取締役
2月16日	A Deep Dive into Open Blockchain Experiments	Michelle Bachler Open University(英国) Research & Innovation Software Manager
2月16日	Free Q&A Session	Denis Parfenov Data Management Hub Founder, Open Data Governance Board member(アイルランド)
2月16日	NEM Walletを作ろう!	中川祥平 NEM Foundation
2月16日	Blockchain and Cryptoeconomy for Science	Dr. Sönke Bartling Founder of Blockchain For Science(ドイツ), Lecturer at CODE.University

5-3-1 「学位・履修履歴証明」テーマ成果物の紹介（最優秀賞） 《学位や在学期間のポートフォリオを一括管理するシステム》

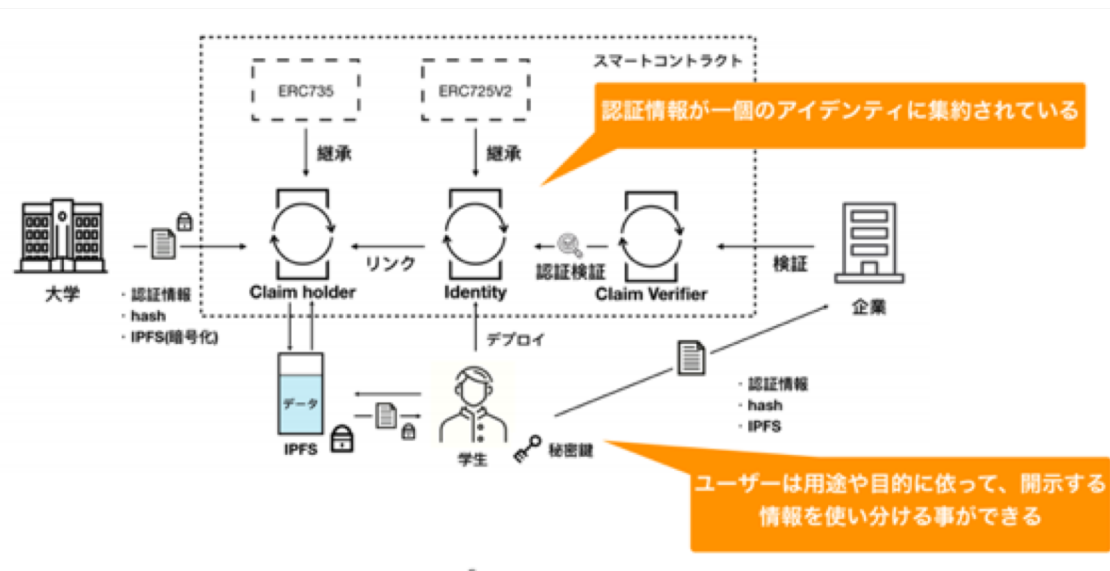
概要

- チーム名：DigiD
- チームメンバー数：4人（社会人：3人、学生：1人）
- テーマ：学位・履修履歴管理
- 参加形態：チーム参加

内容

- ERC725V2、ERC735を利用して、公開鍵がアイデンティティとなるような世界を作ること目的としたプラットフォーム

実施スキーム



- 学生はERC725V2のスマートコントラクトを自身のアイデンティティとしてデプロイ。秘密鍵は学生が保持し、公開鍵を大学が保持、認証情報をその学生の公開鍵を用いて暗号化して管理
- 大学が発行する認証情報はERC735にて管理し、ERC725スマートコントラクト上に紐付けされる
- 認証情報は分散台帳上（IPFS）に登録されているため、データの耐改ざん性を高めている。また、ERC735を利用した認証情報が、ERC725を用いて学生本人主導の分散アイデンティティとして一元的に管理することが可能になるため、個人の価値向上をも狙う。更に、この基盤を利用することで、大学が統廃合により無くなった場合でも、情報は存続可能になると考えられる

5-3-2 「学位・履修履歴証明」テーマ成果物の紹介（優秀賞） 《オープン型資格・履修履歴プラットフォーム》

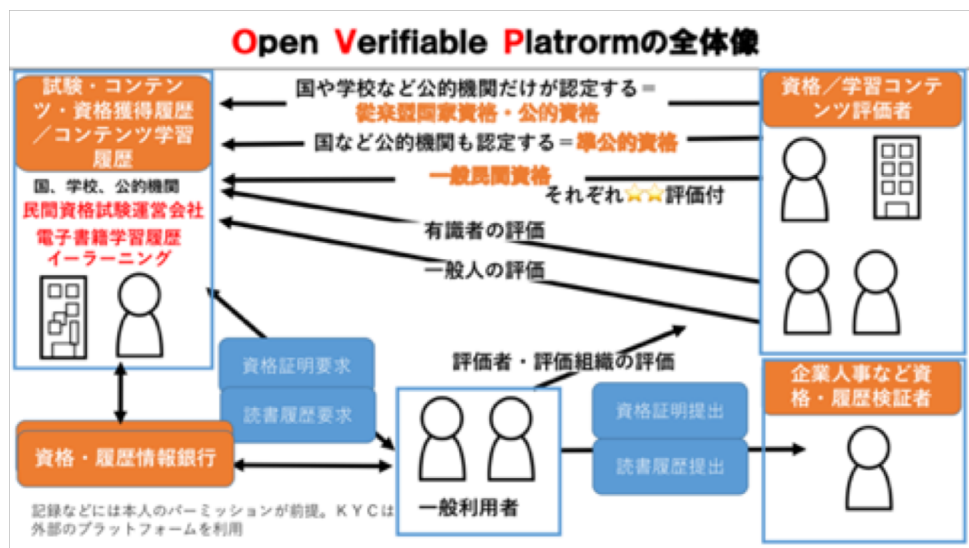
概要

- チーム名：OVP (Open Verifiable Platform)
- チームメンバー数：5人（社会人：4人、学生：1人）
- テーマ：学位・履修履歴管理
- 参加形態：個人参加

内容

- ERC725、ERC735を利用した、資格・学習履歴の公的・準公的認証を実現する分散型資格・履歴証明ネットワーク
- ERC735で発行する認証情報（クレーム）の評判を管理するERC1757をイーサリアムのコミュニティに提案

実施スキーム



- 資格情報を公的資格、準公的資格、一般民間資格と区分し、それぞれの認定機関を誰でも評価することにより信頼できる資格かどうかを蓄積
- ERC725のスマートコントラクトを自身のアイデンティティとしてデプロイする
- 認証情報はERC735にて管理し、ERC725スマートコントラクト上に紐付け
- ブロックチェーン技術により、証明の情報を分散台帳（IPFS）に格納することによる耐改ざん性の向上や、ERC725及びERC735を利用し、第三者機関を不要とする分散型資格・履歴証明の実現を狙う。また、認証そのものに関する評判を管理することで（ERC1757）、第三者機関を介さずに「本当に国家資格であるか」や「本当にその学校が存在しているか」等が明示できるようになる他、変貌していく社会的ニーズに合わせて民間の資格を準公的資格とみなせる仕組みが構築できると考えられる

5-3-3 「研究データの信頼性確保」テーマ成果物の紹介（最優秀賞） 《臨床研究の解析アウトソーシング分散プラットフォーム》

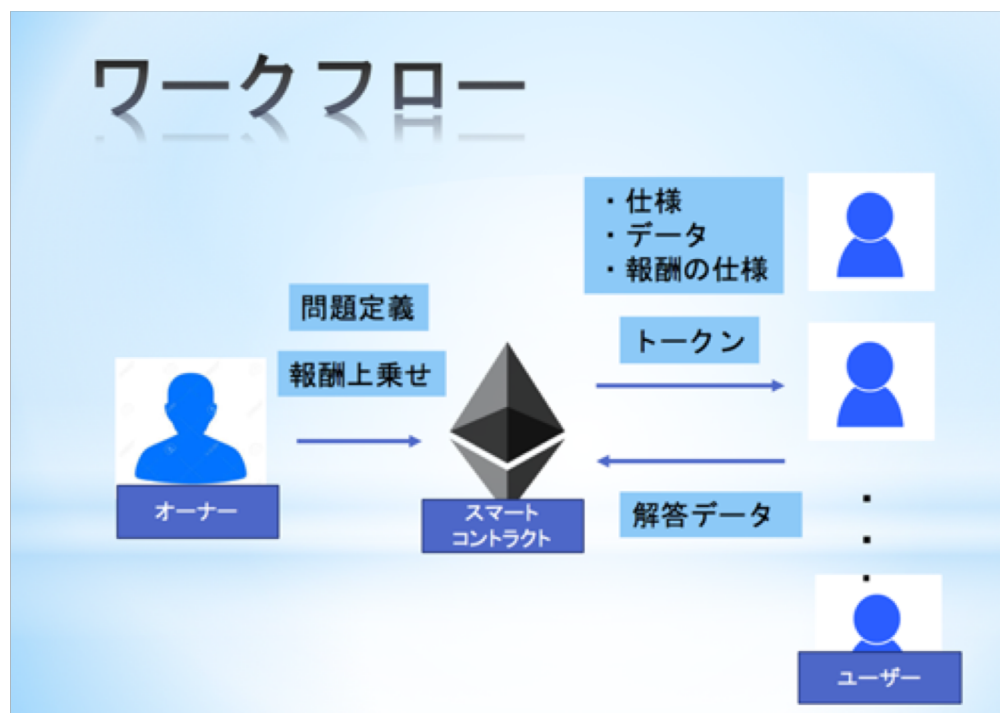
概要

- チーム名： egateam
- チームメンバー数： 6人（社会人： 4人、 学生： 2人）
- テーマ： 研究データの信頼性確保
- 参加形態： チーム参加 + 個人参加

内容

- 臨床試験における解析工程のアウトソースプラットフォーム

実施スキーム



- 臨床試験登録体制や症例データの登録体制については、UMIN等既存の組織で対応可能であるためブロックチェーンは不要だと判断
- それ以外の工程の中で、解析工程については「第三者のチェックが必要（現状されていない）」「作業が膨大」等の理由により適応可能性があると考えられる
- 解析工程の依頼内容をブロックチェーンに公開してネットワーク参加者へ作業依頼し、ネットワーク参加者が解析業務とその検証作業を行う。その報酬としてトークンを受け取る
- ブロックチェーン技術により、適切なインセンティブ構造を設計、解析工程を全世界の第三者解析技術者に依頼すること（分散化）が可能になり、解析工程の信頼性向上に繋げることが可能だと考えられる

5-3-4 アーリーエッジ賞受賞成果物の紹介

《研究の信憑性を確保し、世界中の研究者が継続利用可能なドローンプラットフォーム》

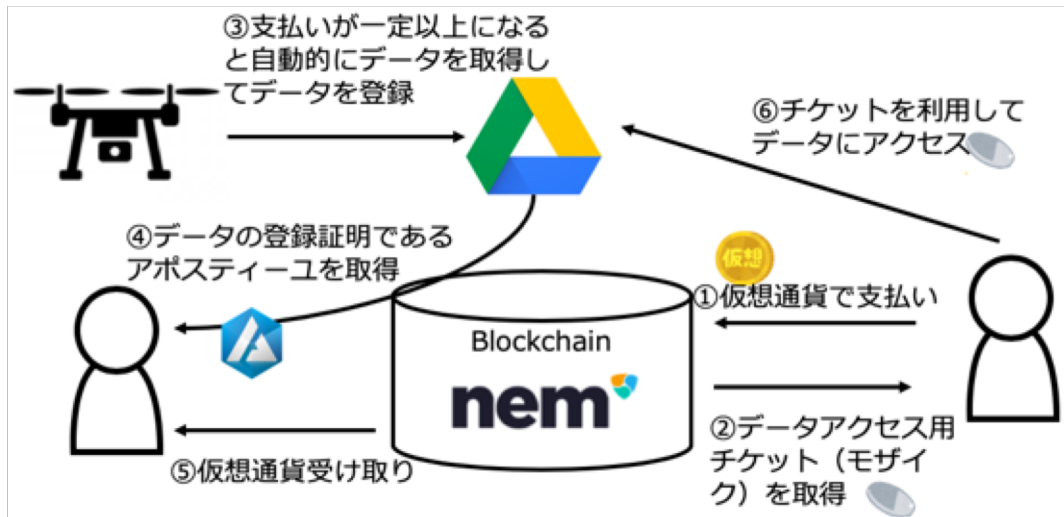
概要

- チーム名： Authorized Moment
- チームメンバー数： 5人（社会人： 2人、 学生： 3人）
- テーマ： 研究データの信頼性確保
- 参加形態： 個人参加

内容

- 研究プロジェクトのための仮想通貨によるクラウドファンディング機能を提供し、完全自動化ドローン等によるデータ不正排除や実験結果公証における未改ざんデータを証明するシステム「ソラノメ」

実施スキーム



- 改ざんのされていない動画・画像データを利用したい研究者は自身のGoogleアカウントでサービスにログイン、利用したいプロジェクトに割り当てられているウォレットに仮想通貨（今回はNEM）を支払う
- 支払い元のウォレットへ電子チケットが届く
- プロジェクト記載の実施額まで仮想通貨が集まると、ドローン可動準備
- ドローンが作動し、撮影された画像・動画データがリアルタイムでサーバー上に集まる。その後、サーバー側で自動的にブロックチェーンに書き込み、公証機能(アポストリーユ)登録
- ウォレット側に電子チケットを持つユーザーのGoogleドライブアカウントに上記の公証されたデータと証明書が共有される
- 公証検証機能で、該当データが改ざんされていないものが保証される

6-1 総論

- 取引相手の信頼性を確保するために、多大なコストを払って構築してきた中央集権的な第三者機関を不要とするブロックチェーン技術は、欧州における個人情報保護に関する法整備の動き等とも連動し、今後の社会システムを大きく変容させる可能性を有する。この期待感からか、本調査事業の中で実施したハッカソンは、想定を上回る方々の関心を集めて開催され、インターネット萌芽期と同様、まさに**今後爆発的に普及する技術の萌芽期を迎えている可能性**もある。
- 他方、ハッカソンに参加した多くの参加者が言及しているとおり、
 - 技術面からは、①**秘密鍵の安全な管理・利用の方法**、②**そもそものデータを入力する際の信頼性の確保の方法**等
 - 経済面からは、①**高いUXの実現**、②**ブロックチェーン技術利用の必然性**、③**マネタイズモデル**等
 - 制度面からは、①**プライバシーの保護**、②**知る権利や忘れられる権利との整合性**等克服すべき課題も多く、**これら課題を順次解決していくことが社会実装に向けては必要**となる。
- 海外に目を転じれば、「学位・履修履歴・職歴管理」及び「研究データの信頼性確保」双方において、複数の適用事例が生まれてきているのは事実であり、我が国においても、こうした動きに遅れず、むしろ先導していく上では、今後次の取組が必要と考えられる。
 - ✓ 第一に、「学位・履修履歴・職歴管理」及び「研究データの信頼性確保」テーマにおけるブロックチェーン技術の先行的な導入に向けた検討をより深化させるため、学校や企業など市場の積極的な参加の下、今回開催したハッカソンなどの実証実験を実施できる環境を官民が連携して整備すること。
 - ✓ 第二に、世界中のブロックチェーン技術適用の動きと歩調を合わせるためにも、我が国の技術者コミュニティに対して今回のようなハッカソンといったきっかけを提供しつつ、技術仕様の策定といった今後のブロックチェーン技術の標準化に貢献できる環境を整備すること。

6-2 総論：ブロックチェーン技術の実社会への適用について

ブロックチェーン技術の適用可能性

ブロックチェーン技術は発展途上の技術ではあるが、要件によっては様々な適用例が考えられる。実際の社会実装に必要な要件及び課題の分析、その他ブロックチェーンの持続性の担保等が必要である。

「学位・履修履歴管理」テーマ

- 既存の仕組みでは困難である「**発行者が不在となった場合に、その発行者によって過去に発行された証明書を正しく検証すること**」において適用が可能であると考えられる。
- ハッカソンにおいて複数のチームが取り上げたDID（※）に関する取組については、秘密鍵の管理等の課題はあるものの、**ユーザー自身によって自身のアイデンティティを管理する今までにない仕組み**であり、適用可能性について継続的な議論が必要になると考えられる。（※）Decentralized ID（分散型ID）

「研究データの信頼性確保」テーマ

- 国内外の一部組織においては、信頼性がある程度確保された中央集権的なシステムが稼働しているが、そのシステムがコスト優位性をもって正常に機能している限り、ブロックチェーン技術を無理に適用する必要はないと考えられる。
- ハッカソンでは、現状中央集権的なデータベースが存在しない、研究活動の「解析工程」に着目したプロジェクトが存在したが、同様に**研究活動におけるその他の工程における適用可能性**について継続的な議論が必要になると考えられる。

海外の事例

海外では様々なブロックチェーン技術の適用事例が紹介されてきている。今後、各事例における課題を洗い出し、解決策を議論していく必要がある。

「学位・履修履歴管理」テーマ

- キプロスのニコシア大学など**既に学位の発行をブロックチェーン上で実施している大学が存在しており、大学が廃校になったとしても学位のデータを残すことが可能となっている。**
- ブロックチェーンにアクセスする運営を当該大学だけが実施している状態では、大学の廃校とともにユーザー用のウェブサイト等がなくなってしまう。この場合、実質的に継続運営が困難であるため、**運営自体も分散して実施することが必要**となっている。

「研究データの信頼性確保」テーマ

- ヨーロッパを中心とした団体であるData Management Hubなどでは、**IPFSを基盤とし、研究データの検索やアクセス、再利用などが可能な研究データに特化した分散データ基盤構築**を目指している。
- 一度ブロックチェーンに格納されたデータの耐改ざん性は向上するものの、**データの真正性そのものを確保するものではない。**

6-3 総論：今後の標準化における考察

ブロックチェーン技術における標準化の動向

- ブロックチェーン技術の標準化について、国際標準化団体による標準化の動きはあるものの、**進捗状況としては初期段階であり**、例えばISOではTerminologyを定義している段階にある。
- その一方で、オープンソース手法を基本とするブロックチェーン技術においては、**コミュニティやコミュニティの中心となるコアデベロッパーによる独自の標準化プロセスが存在する**。
- 従って、**国際標準化団体による標準化のみならず、ブロックチェーンのコアデベロッパーなど民主導の標準化プロセスにも注視していくことが必要である**。

ブロックチェーン開発コミュニティによる標準化

- 例えば、**イーサリアムではEIP**（Ethereum Improvement Proposalの略でイーサリアムのシステム全体の様々な改善提案に関わるプロセス）や**ERC**（“Ethereum Request For Commentsの略でトークンやスマートコントラクトといったアプリケーションレベルの標準仕様の提案に関わるプロセス）**といったプロセスで技術仕様を改善し、標準化を行っている**。**ビットコインでも類似プロセスであるBIP**（Bitcoin Improvement Proposal）が存在する。
- このような標準化プロセスは実際のインプリメンテーションをベースとしたものであり、採択されるものは単に**標準化されるだけではなく、コミュニティから広く使用される技術仕様**となる。
- しかしながら、現在、**本プロセスにおける我が国の影響は決して大きいとは言い難い状況**。今後、貢献度を上げることで、標準化そのものに対する影響だけではなく、**実際世界中で使われていくブロックチェーン技術において影響力を高められる**と考えられる。

想定される今後の必要なアクション

- 今回のようなハッカソンや、オープンソース開発環境の強化、ブロックチェーン技術における教育といった、**我が国の技術者コミュニティが世界のブロックチェーン開発コミュニティに対してより容易に貢献できるようにきっかけの提供**。例えば、今回のハッカソン開催中にERC-1757（Reputation Mechanism to Claim Issuers）が提案されたが、多くの日本人エンジニアはコミュニティに参加するための作法を知らないのではないかと考えられ、きっかけを与えることで国際社会への提案力を増すことが可能に。
- ISOやW3Cといった国際標準化団体で行われている標準化の動きとEIPやBIPといった民間の標準化プロセスにおける橋渡しの役割を官民連携で担う。

ハッカソン期間中に参加者から提案されたERC-1757

yujisuga commented 10 days ago • edited ▾

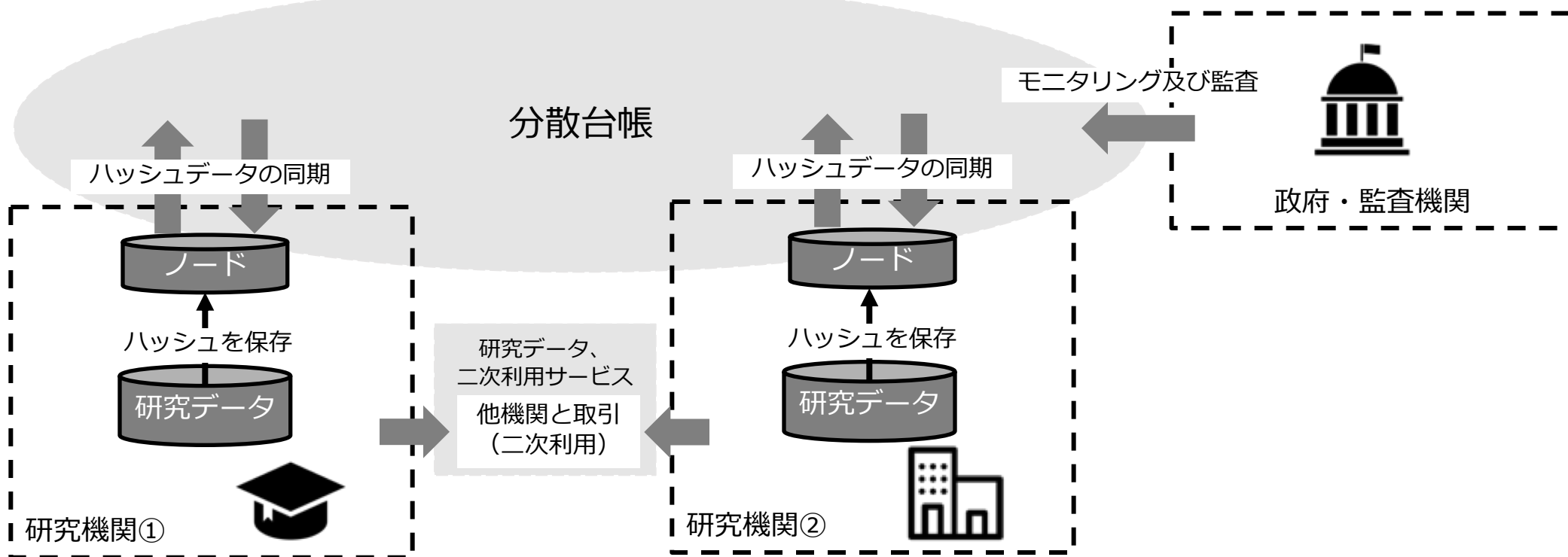
```
eip: 1757
title: ERC: Reputation Mechanism to Claim Issuers
author: Yuji Suga (@yujisuga) >
discussions-to: to-be-assigned
status: Discussion
type: Standard
category: ERC
created: 2019-02-17
requires: ERC725, ERC735
```

Appendix

[Appendix A] 「研究データの信頼性確保」テーマにおける活用案①

概要

研究データ自体は各研究機関で管理し、研究データのハッシュ値だけをブロックチェーン上に登録する

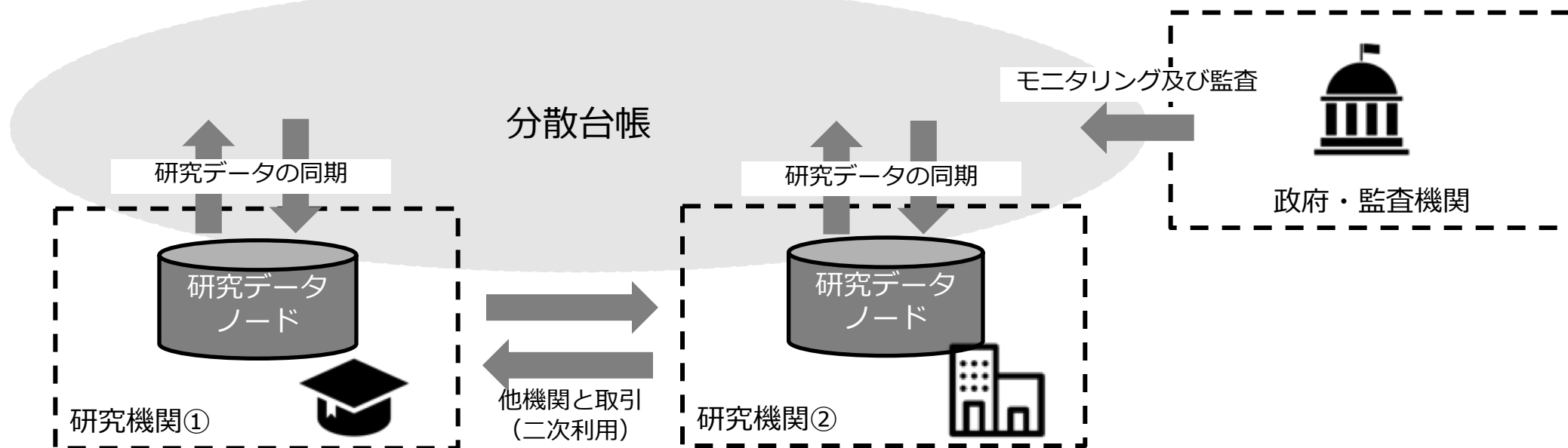


- ・ **利点** : (1) ハッシュ値を保存するため、各ノードの容量が比較的小さい、(2) 生データ自体は、各研究機関で保存するため、プライバシーに関する心理的障壁が低いと考えられる、(3) 推測不可なハッシュ値を保存するため、既存のパブリックブロックチェーンを利用できる可能性がある
- ・ **課題** : (1) データの二次利用に関して、別途システムを構築する必要がある。(2) 少しでも情報を変更するとハッシュ値が変更されてしまうため、データ運用ルールを定める必要がある

[Appendix A] 「研究データの信頼性確保」テーマにおける活用案②

概要

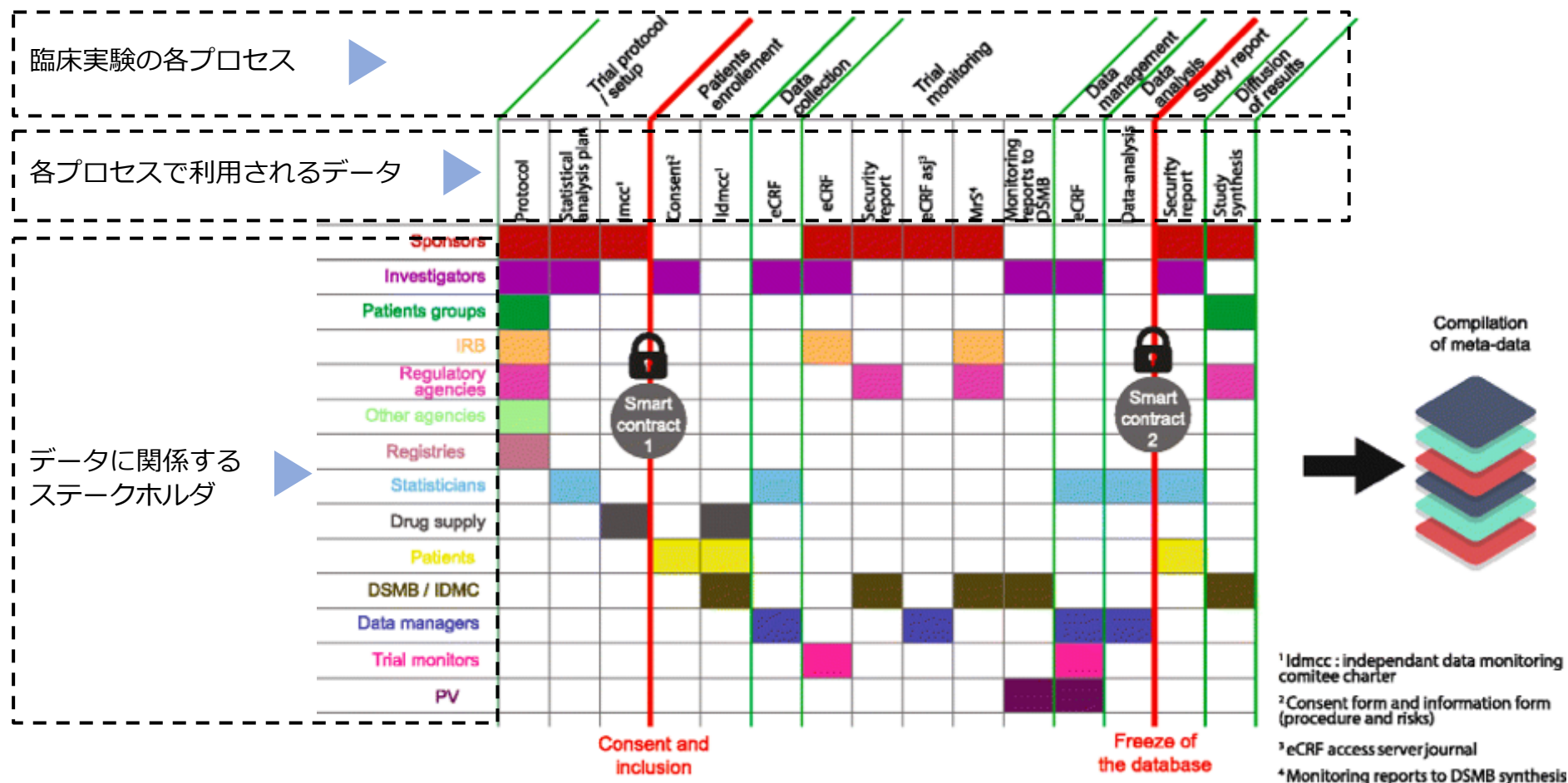
全ての研究データをブロックチェーン上で管理する



- ・ **利点** : (1) データの二次利用に関して、スマートコントラクトを用いて秘匿取引が可能である
- ・ **課題** : (1) アクセスコントロールが可能なコンソーシアムチェーンの構築が必要な可能性がある、(2) 全データを各ノードで保存するため、各ノードのデータ容量が膨大になる、(3) 全データが分散するため、プライバシーに関する心理的障壁が存在する

[Appendix B] Clinical Trial Complex Data Workflow

下図では臨床実験の各プロセスで利用されるデータが、どのステークホルダーと関係するかマッピングして、各プロセスにおけるスマートコントラクトの導入例も併せて示している⁽¹⁾



(1) Blockchain technology for improving clinical research quality : <https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z>

[Appendix C] 標準化団体による標準化 (1/6)

組織名	ISO : International Organization for Standardization	IEEE Standards Association	W3C : World Wide Web Consortium	ITU : International Telecommunication Union	IETF : The Internet Engineering Task Force
プロジェクト名 (グループ)	ISO/TC 307	The IEEE Blockchain Initiative	The Web Ledger Protocol	Focus Group on Application of Distributed Ledger Technology	Decentralized Internet Infrastructure Proposed RG
トピック	現在8個のグループによって構成されたブロックチェーンとDLTの標準化プロジェクト	IEEEブロックチェーンのプロジェクト及び活動の拠点：スタンダード、教育、会議など主要な委員会でサポートされている包括的なプロジェクト	DLTシステムにおけるデータモデルやシンタックス概要	DLTベースのサービスの標準化ロードマップを策定し、ITU、その他の標準開発機関、フォーラム、及びグループで進行中の活動をサポートする	分散化技術に関する研究課題を調査する。ユースケースやベストプラクティスの開発等を活動の目的としている

[Appendix C] 標準化団体による標準化 (2/6)

組織名	プロジェクト名	グループ	検討内容
ISO : International Organization for Standardization ⁽¹⁾	ISO/TC 307	ISO/TC 307/CAG 1	Convenors coordination group
		ISO/TC 307/JWG 4	Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques
		ISO/TC 307/SG 2	Use cases
		ISO/TC 307/SG 6	Governance of blockchain and distributed ledger technology systems
		ISO/TC 307/SG 7	Interoperability of blockchain and distributed ledger technology systems
		ISO/TC 307/WG 1	Foundations
		ISO/TC 307/WG 2	Security, privacy and identity
		ISO/TC 307/WG 3	Smart contracts and their applications

(1) ISO/TC 307 : <https://www.iso.org/committee/6266604.html>

[Appendix C] 標準化団体による標準化 (3/6)

組織名	プロジェクト名	グループ	検討内容
IEEE Standards Association The IEEE Blockchain Initiative ⁽¹⁾	P2418.1 - Standard for the Framework of Blockchain Use in Internet of Things (IoT)		Internet of Things (IoT) アプリケーションにおけるブロックチェーンの使用、実装、及び対話のための共通のフレームワーク
	P2418.2 - Standard Data Format for Blockchain Systems		ブロックチェーンシステムのデータフォーマット要件
	P2418.3 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture		農業におけるDLTシステムの使用、実装、及び対話のための共通フレームワーク
	P2418.4 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Connected and Autonomous Vehicles (CAVs)		動運転車におけるDLTシステムの使用、実装、及び自対話のための共通フレームワーク
	P825 - Guide for Interoperability of Transactive Energy Systems with Electric Power Infrastructure (Building the Enabling Network for Distributed Energy Resources)		分散型電源によってトランザクティブなグリッドサービスを実行するためのガイド

(1) Standards - IEEE Blockchain Initiative (IEEE) : <https://blockchain.ieee.org/standards>

[Appendix C] 標準化団体による標準化（4/6）

組織名	プロジェクト名	グループ	検討内容
W3C : World Wide Web Consortium	The Web Ledger Protocol ⁽¹⁾	W3C Blockchain Community Group	DLTシステムにおけるデータモデルやシンタックス概要
	Decentralized Identifiers ⁽²⁾	Credentials Community Group	検証可能な「自己主権」デジタル識別のための新しい識別子の概要
ITU : International Telecommunication Union	Focus Group on Application of Distributed Ledger Technology (FG DLT) ⁽³⁾		<p>DLTベースのサービスの標準化ロードマップを策定し、ITU、その他の標準開発機関、フォーラム、及びグループで進行中の活動をサポートする</p> <ul style="list-style-type: none"> ・ DLTベースのアプリケーションとサービスを識別して分析する ・ グローバル規模でのアプリケーションやサービスの実装をサポートするベストプラクティスとガイダンスを作成する ・ ITU-T研究グループにおける関連する標準化作業の道筋を提案する

(1) The Web Ledger Protocol 1.0 (W3) : <https://w3c.github.io/web-ledger/>

(2) Decentralized Identifiers : <https://w3c-ccg.github.io/did-spec/>

(3) Focus Group on Application of Distributed Ledger Technology (ITU) : <https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx>

[Appendix C] 標準化団体による標準化 (5/6)

組織名	プロジェクト名	グループ	検討内容
IETF : The Internet Engineering Task Force ⁽¹⁾	Decentralized Internet Infrastructure Proposed RG		<p>分散化技術に関する研究課題を調査する ユースケースやベストプラクティスの開発等を活動の目的としている</p> <ul style="list-style-type: none"> ・ユースケースとその具体的な要件を分散して実装することについて調査（理解、文書化、調査）すること ・スケーラビリティ、パフォーマンス、セキュリティなどのインターネットレベルの問題に焦点を当てて、特定のユースケースのソリューションを検討して評価する ・技術的ソリューションとベストプラクティスを開発し文書化する ・スケーリングの問題について、コンポーネントが欠落しているかどうかを判断するツールとメトリックを開発する ・IETFの将来の作業項目を整理する

(1) Decentralized Internet Infrastructure Proposed RG : <https://datatracker.ietf.org/rg/dinrg/about/>

[Appendix C] 標準化団体による標準化 (5/6)

組織名	プロジェクト名	グループ	検討内容
	BITA : The Blockchain in Transport Alliance ⁽¹⁾		貨物業界のブロックチェーン基準と教育の発展のためのフォーラムを作成 ブロックチェーン技術の開発に関心がある貨物技術業界の有力企業を結集することを目標とする
	MOBI : Mobility Open Blockchain Initiative ⁽²⁾		自動車業界のグローバル・コンソーシアム

(1) BiTA (Blockchain in Transport Alliance): <https://bita.studio>

(2) MOBI (Mobility Open Blockchain Initiative): <https://www.dlt.mobi/>

[Appendix D] EIP: Ethereum Improvement Proposalプロセス (1/4)

◆BIPとEIPはどちらも三種類の提案から構成されている

プログラムコードに関する提案

A Standards Track BIP (Bitcoinの場合)、
A Standards Track EIP (Ethereumの場合)
と呼ばれる

ブロックチェーン自体やスマートコントラクトの標準実装に関する内容の提案である

※Ethereumの場合は、アプリケーションレベルのスタンダードであるERC(Ethereum Request for Comments)が策定されており、トークンのスタンダードであるERC20や代替不可能 (non fungible) なトークンのスタンダードであるERC721等が存在する

一般的なガイドラインに関する提案

A Informational BIP (Bitcoinの場合)、
A Informational EIP (Ethereumの場合)
と呼ばれる

この提案は、必ずしもコミュニティのコンセンサスまたは勧告を表すものではないため、提案を適用するか否かはユーザーの自由判断である

プロセスに関する提案

A Process BIP (Bitcoinの場合)、
A Meta EIP (Ethereumの場合)
と呼ばれる

主にBIP及びEIP自体の実施プロセスについての提案であり、この提案をユーザーは無視できず、遵守する必要がある

[Appendix D] EIP: Ethereum Improvement Proposalプロセス (2/4)

EIPはEthereum Github上で管理されており、プロセスは下記ルールによって実施される⁽²⁸⁾

ルール	実施事項
EIP作成者 (チャンピオンとも呼ばれる)	EIPを特定のフォーマットに沿って記述し、フォーラムで議論し、議論のコンセンサスを構築する
EIP編集者 (Vitalik Buterin氏など)	EIPが規格に沿っているか、議論の状況をチェックする (アイデアに技術的側面があるか、タイトルは正確か、フォーマットに沿っているか等) チェック後、EIP番号を付与し、対応するPull Requestをマージしてステータスを変更する EIP編集者はあくまで管理や編集を実施するだけで、EIPそれ自体の評価はしない 「The editors don't pass judgment on EIPs. We merely do the administrative & editorial part.」
Ethereum Core Developer	EIPの実装をチェックする

似たような議論がないか下記フォーラムで議論した後、提案することが推奨されている

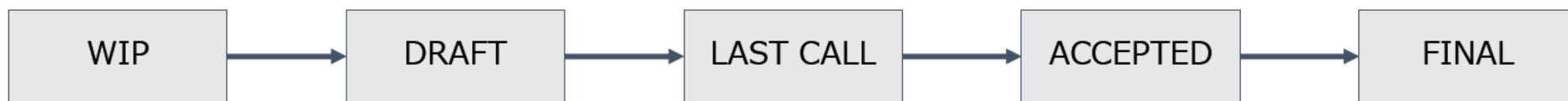
- Ethereum subreddit
- Issues section of Ethereum Github repository
- Ethereum Gitter chat rooms

(1) EIPs : <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1.md>

[Appendix D] EIP: Ethereum Improvement Proposalプロセス (3/4)

◆EIPのステータス

- 正常にEIPプロセスが完了した場合、下記ステータスでEIPは遷移する



◆権利の移譲について

- 他のEIP作成者から、EIPの所有権を引き受けることも可能である
- その場合は元のEIP作成者と、EIP編集者にメッセージを送信し、権利を引き継ぐ
- もし元のEIP作成者が返信を返さない場合は、EIP編集者が一方的に (unilateral) に決断を下す

[Appendix D] EIP: Ethereum Improvement Proposalプロセス (4/4)

◆各ステータスの説明

ステータス	説明
WIP : Work in progress	<ul style="list-style-type: none"> EIP作成者が、コミュニティにアイデアの提案を実施し、最初のPull Requestを作成した状態 「幅が広すぎる」「重複した内容」「技術的に適切でない」「動機が適切でない」「下位互換性に対応していない」「またはEthereumの考え方に従わない」場合は、EIP編集者によってPull Requestが却下される
Draft	<ul style="list-style-type: none"> WIPからEIP編集者のチェックをパスした状態。EIPの番号がEIP編集者によって付与されている 議論が成熟し次のステータスに進めると判断した場合、EIP作成者が再度Pull Requestを作成する Draftにまだ重要な変更があると考えられる場合は、EIP編集者によってPull Requestが却下される
Last Call	<ul style="list-style-type: none"> 重要な変更や技術的な指摘が存在しないかチェックしている状態 重要な変更や技術的な指摘が存在しない場合は、次のステータスに移行する Ethereum Coreに関する EIPの場合、次は「Accepted」にステータスが移行する Ethereum Coreに関する EIPで無い場合、次は「Final」にステータスが移行する
Accepted	<ul style="list-style-type: none"> Ethereum Core Developerによって実装を検証している状態 Ethereum Coreに関する EIPの場合は、少なくとも3つの実行可能なEthereumクライアントで実装する必要がある
Final	<ul style="list-style-type: none"> EIPの実装が完了し、コミュニティによって採用されると、ステータスは「Final」に変更される

[Appendix D] BIPとEIPの例

番号	内容及び経緯
BIP141 ⁽¹⁾	<ul style="list-style-type: none"> トランザクションの情報から署名 (Witness) を分離 (Segregate) する提案 Bitcoinのスケーラビリティの問題への対応の1つ
ERC20 ⁽²⁾	<ul style="list-style-type: none"> EthereumスマートコントラクトのプラクティスであったStandardized_Contract_APIs⁽⁴⁾に記述された一要素であるTransferable Fungibles (Also known as tokens, coins and sub-currencies.) をEthereum版RFCであるERC(Ethereum Request for Comments) にリライトした規格である⁽⁵⁾ トークンの移転等に関する状態や関数が記述されている
ERC721 ⁽³⁾	<ul style="list-style-type: none"> ERC20のトークンは代替可能 (Fungible) でそれぞれが同一 (Identical) なものである それに対して、トークンが代替不可能 (Non Fungible) でそれぞれが唯一 (Unique) な証書 (Deed) として発表されたのがERC721である NFT(non-fungible token)と呼ばれ、区別可能であり、権利の移転追跡が可能なことから下記のような利用手段が考えられている。 <ul style="list-style-type: none"> 物理的な財産 — 住宅、絵画のような芸術品 デジタル上の収集物 — ゲームアイテム、トレーディングカード ネガティブな意味をもつ資産 — ローン、負債、その他責務

(1) BIP141 : <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>

(2) ERC20 : <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>

(3) ERC721 : <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md>

(4) Standardized_Contract_APIs : https://github.com/ethereum/wiki/wiki/Standardized_Contract_APIs

(5) Ethereum Request for Comments (ERCs) and Ethereum Standards (ESDs) #16 : <https://github.com/ethereum/EIPs/issues/16>