

INPUT | OUTPUT

RESEARCH

Cardano Vision

Tech for Impact、2025年10月7日

Input | Output Research はじめに



Input | Output Research (IOR)は**Input | Output Group (IOG)**の研究部門であり、ブロックチェーン、暗号、分散システムの基礎研究および応用研究開発に専念している。

プルーフオブステーク型コンセンサスの**Ouroboros**、スケーラビリティの**Hydra**、ステークベースのしきい値暗号の**Mithril**など、**最先端のプロトコルレベルのイノベーションを提供**してきた実績を誇る。

コミュニティへの関与と現実世界への影響に重点を置き、**オープンな科学と分散化**に取り組む。



250+

査読付き
研究論文数

300+

IOR論文を共著している
研究者数

10,000+

論文ライブラリー全体の
引用数

➤ Input | Output Research 概要

- 現在、60を超えるオープンなR&D分野で3つの研究プログラムを管理
- Eurocrypt、Crypto、CCS (Computer and Communications Security) など、年間平均25の研究会議に出席
- [IOGのYouTubeチャンネル](#)で公開された研究動画は再生回数55,000回以上
- Cardano**5つの開発期**の発展の中心には約**50の論文**があり、今日のCardanoを実現

世界的な学術ネットワーク

IOの2つのR&Dチーム

30人以上の社内研究員 と各地の研究員との研究ネットワーク、ラピッドプロトタイピングと形式的証明に焦点を当てた35人を超えるアーキテクトとエンジニアからなる Web3イノベーション部門

Blockchain Technology

Laboratory (エディンバラ大、東京科学大、ワイオミング大)
業界や政府のパートナーと協力してブロックチェーン技術と分散システムに関する、業界に触発されたオープンアクセス研究を実施するネットワーク

IO Research Hubs (エディンバラ大、スタンフォード大)

ブロックチェーン技術の基礎問題に取り組み、ブロックチェーン業界の科学的知識と研究の蓄積を大幅に増やす



THE UNIVERSITY
of EDINBURGH



東京工業大学
Tokyo Institute of Technology



UNIVERSITY
OF WYOMING



Carnegie
Mellon
University



Stanford



組み込み型研究パートナーシップにより、分野を超えた最先端の専門知識を統合することができ、ブロックチェーン科学における組織横断的な研究とイノベーションを促進する。

➤ IORの方法論

基礎研究 (プレシード /SRL2まで)

IORが最先端の技術水準をも凌ぐアイデアを開発し、形式化。適切な要件の特定、固有のトレードオフや制限の特定、有意義な数学モデル、明確に定義された設計目標、厳密なセキュリティ証明に即した技術的な提案。

市場化まで3～5年

技術のイノベーション (シード /SRL4-5まで)

概念の軽量の検証を行う学際的なチーム。有望なアイデアを開発し、プロトタイプ、モデル、シミュレーションを通じて実現可能性を確立し、完全な実装の方向づけと検証に使用できる仕様を作成するための厳格な研究開発。

市場化まで1.5～3年

目標とする実装 (シード +/SRL 4-5以降)

IORが、イノベーションフェーズで開発された仕様に従って、目標とするプロダクション環境でソリューションを実装するエンジニアリングチームをサポートし、エビデンスに基づく高保証のエンジニアリングアプローチを確保。

市場化まで6～18か月

* SRL(ソフトウェア成熟度レベル)は、基本原理から商業化可能な段階まで、技術のライフサイクルの概要を示す。

ケーススタディ: Ouroboros

Ouroboros(ウロボロス)はCardano台帳の基盤として機能し、ブロック生成を管理し検証する最長チェーンのプルーフオブステーク型プロトコルを通じてブロックチェーンのコンセンサスを達成する。

2017年の初回実装 (Classic) 以来、これに続く各実装でプロトコルの強化と改良が行われてきた。Praosは稼働中、Genesisは開発中であり、Omegaは以下で提案されている。

Classic(クラシック)

プルーフオブステーク型プロトコルにおける重要な成果であり、オンチェーンで生成される公平なランダム性を用いたリーダー選出に基づき、最長チェーンコンセンサスを通じてセキュリティを保証。

Praos(プラオス)

リーダーの選出を秘匿し、前方秘匿性のある鍵変化型署名を使用することにより、適応型攻撃を防ぎブロック生成を保証し、セキュリティとスケーラビリティを強化。

Genesis(ジェネシス)

強力なチェーン選択ルールを追加することで、可変的で動的な参加レベルの下でも、信頼できるチェックポイントなしで、参加者は起源/ジェネシスブロックからのブートストラップが可能に。

研究とイノベーション

IORは複数のイノベーションワークストリームをサポートしている。これには、Praosの高速決済と高スループット性能を大幅に向上させるつも含まれる。

Peras(ペラス)

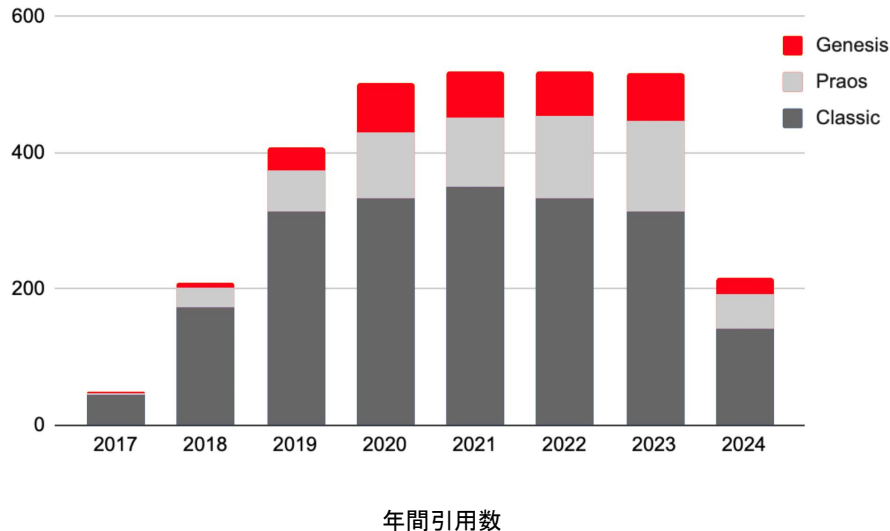
Cardanoの迅速な決済時間を改善することでブロックチェーンの持続可能性の最適化に焦点を当て、分散型ネットワークの長期的な存続性と効率性を確保。

Leios(レイオス)

ブロック伝播を最適化することでスケーラビリティを向上させ、最高のセキュリティを維持しながら、スループットの増加とネットワーク効率の改善を実現。

ケーススタディ: Ouroboros

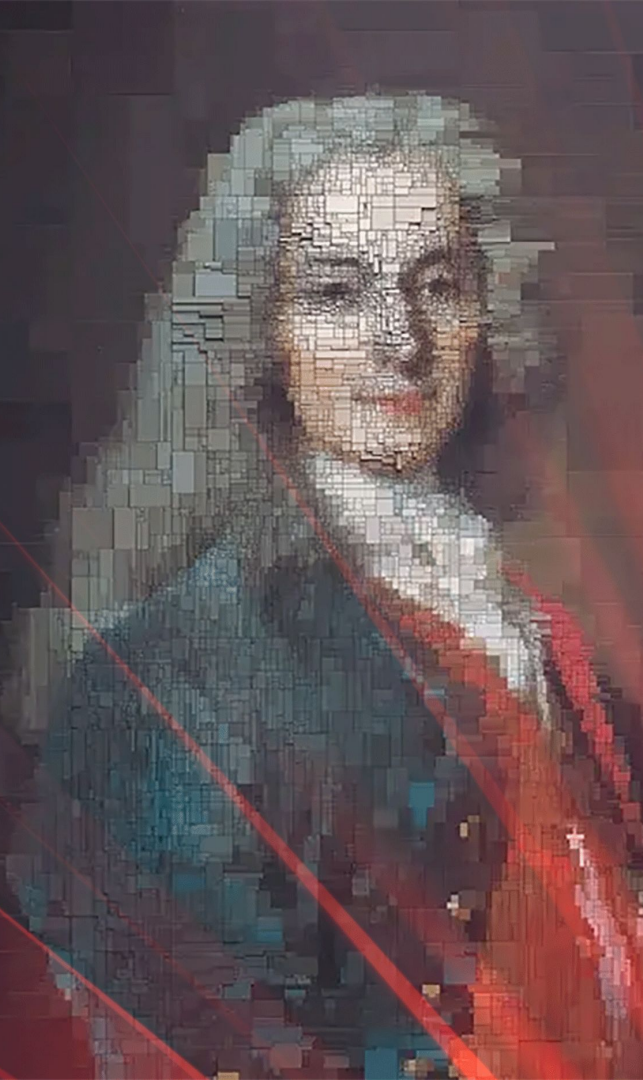
Ouroborosは、分散型台帳技術、特にプルーフオブステーク型プロトコルの開発と実行における、重要なイノベーションの成果を象徴する。



引用と採用

Cardanoブロックチェーンの基盤となるコンセンサス層として設計されたOuroborosプロトコルは、ルールとパラメーターを定義する。

Ouroborosの影響力を示すものとして、その論文は3,000回以上引用されており、このプロトコルはCardanoや、Polkadot、Mina、Horizenといった他の著名なブロックチェーンでも広く採用されている。



➤ Voltaire(ボルテール)期

CardanoのVoltaire開発フェーズは、ネットワークが自立したシステムになるために必要なフレームワークを完成させる。

投票およびトレジャリーシステムを導入することで参加者は自分のステークや投票パワーを活用してネットワークの将来を形作り、既存のステーキングおよび委任プロセスを基盤としCardanoを改善していくための提案をすることができる。

論文

- A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence
(暗号通貨のためのトレジャリーシステム: 優れたコラボレーティブインテリジェンスを実現)
- Updatable Blockchains(更新可能なブロックチェーン)
- SoK: Blockchain Governance(ブロックチェーンガバナンス)
- Reward Schemes and Committee Sizes in Proof of Stake Governance
(プルーフオブステークガバナンスにおける報酬スキームと委員会の規模)
- On the Potential and Limitations of Proxy Voting: Delegation with Incomplete Votes
(代理投票の可能性と限界: 不完全投票を伴う委任)
- Decentralized Update Selection with Semi-strategic Experts(半戦略的専門家による分散型更新選択)

仕様

- CIP-1694: An On-Chain Decentralized Governance Mechanism for Voltaire
(Voltaireのためのオンチェーン分散型ガバナンスメカニズム)

デジタル国民国家

IORは、Cardanoがより広範なブロックチェーンエコシステムとともに、分散型コンピューティングおよびストレージプラットフォーム、すなわち**世界OS (World's operating system)**へと進化することを想定している。ここでは、Web2のシームレスな接続感のごとく、ブロックチェーンネットワークが苦も無く相互運用できる。

このビジョンは、ブロックチェーンがID、ガバナンス、権力構造を定義する上で変革的な役割を果たす**デジタル国民国家**の出現をサポートする。戦略的研究アジェンダは、具体的な研究開発経路を示し、その目的、関連する技術的課題、およびその結果としてのCardanoの機能強化を詳述し、これらの進歩をリードするものとして自らを位置づけている。

- **相互運用性**: 開発者やビルダー向けのユーザビリティ、パフォーマンス、スケーラビリティ、セキュリティ、ユーティリティ
- **ID、ガバナンス、民主主義**: ID関連データでスマートコントラクトシステムを拡張
- **ユーザビリティ**: 開発者の生産性、運用効率、経済的な実行可能性
- **ユーティリティ**: 世界OSになるためには、膨大な計算力とデータが必要になる
- **コンセンサス**: ブロックチェーンの心臓部は、セキュリティ、パフォーマンス、信頼性に関するニーズをサポートするために進化を必要とする
- **トークノミクス**: 分散型システムとして、参加者はシステムに参加または利用するための適切な経済的インセンティブが必要
- **スケーラビリティ**: Web2アプリケーションに匹敵するレイヤー2プロトコル
- **ZK証明**: すべてのゼロ知識インスタンスに共通の技術コアを標準化
- **セキュリティ**: セキュリティに対する現在の脅威は、量子時代に劇的に増大する見込み

➤ Cardano Vision - 2030年の見通し



五か年戦略的研究アジェンダ。ビジョンフェーズとインパクトフェーズという各 2.5年間の2つのフェーズで構成され、連続的な年間または隔年の作業プログラムで編成されている。



Cardano Vision

Cardano Vision - 9つのテーマ別重点分野

➤ **Cardano Vision** - 9つのテーマ別重点分野

ブロックチェーンの約束を世界に届けるための、 9つのテーマ別重点分野にわたる野心的な研究アジェンダ

1. 世界OS
2. Ouroboros Omega
3. トークノミコン
4. グローバルID
5. Democracy 4.0
6. Internet Hydra-ted
7. インターチェーン
8. ゼロ知識のコア機能
9. ポスト量子の展望

🔪 世界OS (WOS)

スケーラブルで安全、実世界に適応したスマートコントラクト



- **WOS-1: 高価値アプリケーションのための DSL**
法律、トークン化、サプライチェーンの専門家が、コードを必要とすることなく信頼できるスマートコントラクトを設計できるようになるような新しいDSL(ドメイン固有言語)を構築。
- **WOS-2: ステートマシンコントラクト環境**
EasySMはステートマシンフレームワークを使用して Cardanoスマートコントラクトを簡素化し、DAppとHydraの開発をより速く、より安全に、より直感的に行う。
- **WOS-3: スマートコントラクトの形式検証**
Cardanoスマートコントラクトの正確性と安全性、高い信頼性を保証し、コストのかかるエラーを防ぐために形式証明を開発。
- **WOS-4: 分散型ストレージ**
ビザンチン耐性のあるストレージ層が、トランザクションを超えて Cardanoを拡張し、NFT、データ、DAppの安全な永続性を実現。
- **WOS-5: Pub/Subコミュニケーション**
DApp、コントラクト、SPOのメッセージングシステムを構築し、チェーン全体をスキャンすることなく効率的なコミュニケーションを可能にする。
- **WOS-6: 位置情報サービスとスマートコントラクト**
実世界の地理に対応できるスマートコントラクトを可能にしながら、回復力のためのグローバルなノード分散を保証。
- **WOS-7: 意図に基づく台帳と意思決定**
意図に基づくトランザクションは、ユーザーがスワップや手数料の支払いなどの目的を台帳で直接表現することで、より速く、より安く、より柔軟なインタラクションを可能にする。

➤ Ouroboros Omega(00)

Cardanoコンセンサスのスピード、スケール、回復性を向上



- **00-1V: Ouroboros Peras – ビジョン**
回復性を維持しながら、より迅速なファイナリティのために決済を加速し、よりスムーズなアプリ、クロスチェーン接続、より効率的なブロックチェーンを実現。
- **00-2: Ouroboros Leios**
Cardanoをノードリソースとともに成長させてスケーラビリティを向上させ、セキュリティを損なわずに高スループットを提供。
- **00-3: 公正なトランザクション処理**
コンセンサスに公平性を埋め込み、フロントランニングやキュー操作を防止してユーザーを保護し信頼を構築。
- **00-4: ビザンチン耐性のあるネットワーク**
攻撃や帯域幅制限からCardanoを保護し、信頼性の高いデータ拡散と包摂の参加を可能にする。
- **00-5: マルチリソースコンセンサス – Minotaur**
ステーキング、ワーク、リステイキングされたアセットをハイブリッドコンセンサスに統合し、新規および既存のチェーンの安全性と包摂性を向上。
- **00-6: ブルーフォブユースフルワーク (PoUW)**
最適化や機械学習などの意味のある計算を通じてブロックチェーンを保護し、セキュリティを生産的で持続可能なものにする。
- **00-7: 輻輳制御**
手数料体系を再設計して負荷がかかった状態でも予測可能で公平なコストを実現し、DeFi、決済システム、企業での利用をサポート。
- **00-8: Cardanoシャーディング**
ノード間で検証を分割することで真の水平スケーリングを実現し、低遅延を保ちながらスループットを向上させる。

トークンノミコン(TO)

Cardanoエコシステムのための持続可能なトークンエコノミーの設計



- **T0-1: トークノミクス設計**
ステーキング、トレジャリー、採用のモデルを構築し、Cardanoの長期的な経済安定と持続可能な成長を導く。
- **T0-2: 報酬の共有とトランザクション手数料**
SPOとデリゲーターのための、より公平で予測可能なインセンティブスキームの開発、分散性の強化、ガバナンスとMithrilのようなプロトコルにおける報酬の定義に関する研究。
- **T0-3: ステーブルコイン**
担保、アルゴリズム、ハイブリッドモデルのトレードオフを分析することで、Djedから多様なユーザーニーズに対応する新設計まで、Cardanoのステーブルコインエコシステムを強化する。

グローバル ID (GI)

ユーザーが制御し、プライバシーを保護するデジタル時代の ID



- **GI-1: 分散型 ID およびレピュテーション管理**

プライバシーを保護するデジタル ID およびレピュテーションシステムを開発し、安全なトランザクション、ガバナンス、クロスプラットフォームポータビリティを可能にしながら、ユーザーがデータを制御できるようにする。

7 Democracy 4.0 (D4)

Cardanoのためのスケーラブルで包摂的、安全なガバナンス



- **D4-1: 次世代のガバナンスプロトコル**
スケーラブルでプライバシーを保護し、コスト効率の高い投票システムを設計して、Cardanoに安全で将来の変化に対応できるガバナンスツールを装備する。
- **D4-2: ガバナンスインセンティブ**
包摂的で透明性があり、不正操作に耐性のあるガバナンスのために、公正な報酬モデルと予算モデルを開発。
- **D4-3: 意思決定ツールセット**
Cardanoコミュニティがガバナンスの決定を客観的に評価、比較、追跡するのに役立つ指標とモデルを構築。

➤ The Internet Hydra-ted (IHT)



Web2レベルのパフォーマンスを実現するための Hydraによるレイヤー 2スケーラビリティ

- **IHT-1: Hydra Tail**

HydraにZK-rollupを導入し、ゼロ知識証明とオフチェーントランザクションをバンドルして、負荷の軽減、資金とコントラクトのシームレスな移動を可能にする。

- **IHT-2: Inter-Head**

複数のHydraヘッドを安全で相互運用可能なチャネルネットワークにリンクし、グループ間の大規模で高速なオフチェーントランザクションを可能にする。

- **IHT-3: 最適化ツール**

流動性、ルーティング、同期の課題に対処することで、Hydraの実世界でのパフォーマンスを円滑にするツールを開発。

- **IHT-4: 監査ツール**

監査機能のオプションを Hydraに追加し、プライバシーと規制上の説明責任のバランスを取り、レイヤー 2ソリューションを金融機関でも使えるようにする。

インターチェン (IC)

Cardanoを他のブロックチェーンと接続するための安全な相互運用性



- **IC-1: ステート証明とブロックチェーンブリッジ**

証明とゼロ知識技術を使用してトラストレスなブリッジを開発し、中央集権的な仲介者に頼らずにアセット、コントラクト、データの安全なクロスチェーン転送を可能にする。

- **IC-2: プライバシー保護とクロスチェーン DApp および Oracle**

プライバシーを保護する計算機能と安全なオラクル統合によって Cardano のスマートコントラクトを強化し、プライバシー DeFi のようなスケーラブルで信頼性の高いクロスチェーンアプリケーションを可能にする。

- **IC-3: ライトクライアントインフラ**

ウォレットやアプリがフルノードなしで Cardano を使用できるようにする軽量で安全なクライアントを設計し、アクセスを分散化しながらサードパーティへの依存を軽減する。

- **IC-4.1: DApp トークノミクス**

DApp とパートナーチェーンの立ち上げフェーズのモデルを開発し、インセンティブ設計やエアドロップを導き、プロジェクトが持続可能な普及と独立を達成するのを助ける。

- **IC-4.2: コンセンサスイノベーション**

Cardano とパートナーチェーンの次世代コンセンサスを進化させる。BFT、ナカモト、DAG の研究と、証明やインセンティブを組み合わせ、より堅牢でスケーラブルなプロトコルを実現する。

🔪 ゼロ知識のコア機能 (ZK)

ゼロ知識証明によるプライバシーと効率性



- **ZK-1: ゼロ知識のコア機能**

アップグレード可能で、量子耐性を備えたモジュール式の Cardano用ZKツールキットで、ライトクライアントやブリッジからガバナンスや高度なスマートコントラクトまでのアプリケーションを可能にする。

7 ポスト量子の展望 (PQL)



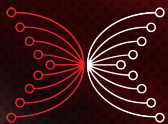
量子耐性のある、量子で強化された暗号技術で Cardanoに将来性をもたらす

- **PQL-1: ポスト量子の準備度**

署名、VRF、ランダム性などをカバーする完全な量子耐性暗号ツールキットを開発して、量子の脅威に対するセキュリティと効率を確保することで、Cardanoに将来性をもたらす。

- **PQL-2: ポスト量子の強化**

量子力学そのものが、一度きりで自己消滅する署名から、より強固なコンセンサスと鍵管理のための量子鍵配送に至るまで、どのようにブロックチェーンのセキュリティを向上させられるかを探求する。



INPUT | OUTPUT

RESEARCH

Thank you