# Aurora
# ホワイトペーパー

# 概要

Aurora は、DPOS + BFT のコンセンサスメカニズムとコントラクトを「光速」の稼働率で適用することで、ゲーム、ビッグデータ、AI、IoT などの業界を繋ぎ合わせます。Aurora のスローガンは、「オーロラのように輝く素敵でカラフルなブロックチェーンワールドを構築すること」です。Aurora はインテリジェントなアプリケーション分離技術を提供し、マルチチェーン並列拡張を可能にすることで、セキュリティを維持しつつ極めて高い TPS を実現します。このようにして、Aurora はブロックチェーンの世界の飛躍を目指します。

以上を達成するために、Aurora は以下のような多くの技術を開発しました。

・DPOS＋BFT コンセンサスメカニズムは、迅速なコンセンサスメカニズムに基づいてフォークのリスクを低減します。
・P2P ステレオネットは、ネットワークレイヤーによる高速で安全な通信を可能にします。
・独自のアプリケーション分離技術とペンディングゾーンの適切な制御により、アプリケーション相互間における内部的な影響を防止できます。
・マルチチェーン並列動作及び水平拡張により、TPS を無限に増加できます。
・マルチアセットローンチ機能により、資産立ち上げの手順が簡素化され、メインチェーンのコインと同じレベルまで拡張する機能と高い処理速度が提供されます。
・アップグレード可能なブロックチェーンにより、自動アップグレード機能が提供されます。
・クラスタの自己グルーピング技術により、トランザクションの検証が可能になり、ユーザーのデータストレージコストが削減されます。

Aurora は、多くの既存ブロックチェーンが抱える問題点を解決することにより、動作速度を向上させ、またアプリケーションのためのブロックチェーンを開発することを目指しています。Aurora はあらゆる業界を繋ぎ、アプリケーションの開発を促進し、彩り豊かなブロックチェーンの世界の構築に貢献します！

# 各論

## 1　Aurora のバックグラウンド

ブロックチェーンは、新しい分散型インフラストラクチャであり、コンピューティングのパラダイムです。ブロックチェーンは、鎖状に連なるブロックというデータ構造を使用してデータの検証と保存をし、分散型ノードコンセンサスアルゴリズムを使用してデータの生成と更新をし、暗号技術を使用してデータの転送、データへのアクセス、スマートコントラクトのプロセスを保護し、自動化されたスクリプトを使用してコードを書き、データを処理する技術です。

ブロックチェーンは、信頼できるインターネット環境の始まりを象徴しています。ブロックチェーンは、ネットワーク上のピアツーピアに信頼を構築し、価値の移動のプロセスを第三者の仲介なしに透明かつ機密にする上で、非常に魅力的な技術です。

このメカニズムは共同決定されるものですが、個々の権利を保護することもでき、価値の交換の効率化とコストの削減につながります。

## 2　Aurora の目標

Aurora は、光速のコントラクトを作り上げ、またブロックチェーン上でのアプリケーションの作成を容易にするという使命を持っています。

私たちの中心的な目標は次のとおりです。

- 他の業界へのブロックチェーンの導入

  ブロックチェーンは、現状、デジタル資産の提供に使用されるのが最も一般的となっています。しかし、Aurora により、他の業界と密な関係を構築することが可能になります。Aurora は、企業がアプリケーションとルールをブロックチェーンに組み込むことを可能にしようとしています。Aurora は、アプリケーションのために生まれたものであり、アプリケーションの実装をサポートし、異なる業界をつなぐ架け橋になります。

- 完璧なスマートコントラクトの構築

  スマートコントラクトは、ブロックチェーンを他の業界に導入する上で必要不可欠です。コントラクトにとってパブリックチェーンがどれだけ役に立つかは、ブロックチェーンが他の業界とどれだけ密に繋がっているかと密接に関連します。下層レイヤー、高いレベルの自由度、透明性のあるコードを豊富に備えるコントラクトだけが、他の業界のニーズを満たすことができます。

- トランザクションスピードの向上

  多くのブロックチェーンが有する TPS の遅さは、これによりブロックチェーンと他の業界の融合が妨げられている、と長い間批判されてきました。そのため、Aurora はトランザクションスピードの高速化に重点を置いています。

- ブロックチェーンの抱える諸問題の解決

  Aurora は、アップグレード可能なブロックチェーンを構築し、指定された高さでの

自動アップグレード機能を実現します。また、クラスタのセルフグルーピング技術により、Auroraはユーザーのデータストレージコストを削減します。
このように、Auroraは、アプリケーションにブロックチェーンテクノロジーを実装する際に生じる様々な問題を解決し、ブロックチェーンエコロジーの構築を加速させます。

● アプリケーションへのブロックチェーンの迅速な実装の実現
Auroraは、理想と現実の結合、効率と実用性の共存に重点を置きます。 Auroraは、ブロックチェーンアプリケーションの実装を加速させるために、様々な種類のアプリケーションとブロックチェーンの深い統合を可能にします。

## 3 Auroraの技術的要素

### 3−1 DPOS＋BFTコンセンサスメカニズム

(1) DPOS（Delegated Proof of Stake）

DPOSコンセンサスメカニズムが高いトランザクション速度と高いTPSを備えていることから、多くのブロックチェーンプロジェクトが DPOS を採用し始めており、Auroraも同様にDPOSを採用します。
アカウントのAOA残高が500万AOA以上の場合、そのアカウントはAOAの代表者に立候補することができます。代表者候補のAOA残高が500万AOA未満の場合、その候補者は自動的に失格となります。すべてのAOA保有者がAOAの代表者候補に投票でき、得票数順に101の候補者が自動的に代表者として選出され、トランザクションの処理をします。投票者は、候補者1人につき一度だけ投票でき、最高で101票投票できます。 1AOAにつき1回投票でき、投票に使用されたAOAは投票終了するまでロックされます。

(2) BFT（Byzantine Fault Tolerance、ビザンチン障害耐性）

・DPOSにBFTを追加することで、効果的にフォークを回避できます。ブロック生成後に N回の承認を待つ必要がないため、速度が大幅に向上します
・Auroraは、UDPに基づくノード間のブロードキャストネットワークと、TCPに基づく代表候補間の長い接続を含む立体的なP2Pネットワークを構築します。上位のネットワークを介して、代表候補間で高速なBFTコンセンサスシステムを実現することができます。
・ステータスの記録と検証速度の向上のために、各ブロックの先頭にプロキシルートツリーが追加されます。

### 3−2 スマートコントラクト

クロスボーダーの法学者であるNick Szaboは、スマートコントラクトを、シェアホルダーが守る約束に基づく一連のデジタルな約束とプロトコルである、と定義します。

スマートコントラクトとは、情報を処理し、値を取得・送信するために使用されるブロックチェーンデータベース上で動作するプログラムです。

Auroraは、EVM仮想マシンと開発言語Solidityを用いてスマートコントラクトを作

成します。Aurora は、将来的には、Java、Go、および C ++に基づくスマートコントラクトに対応する予定です。

### 3−3　P2P ステレオネット

ブロードキャストネットワークは、異なるノード間に構築されます。代表候補者は、上位層のネットワークを介して直接接続を構築することができ、代表間の BFT メカニズムを迅速に実現することができます。

ネットワークレイヤーを使用することで、より迅速かつ安全な通信を実現します。

### 3−4　アプリケーション分離技術

検証済みのトランザクションは、ペンディングゾーンで処理されます。代表ノードは、トランザクションをそれが外部に出されるまでペンディングゾーンにパックします。

スマートスケジューリングペンディングゾーンの主な機能は次のとおりです。

まず、マクロの視点からは、異なる手数料、フロー、カテゴリのコントラクトをそれぞれ区別します。また、プロセスが公正であり、一部のコントラクト詰まりが他者に影響を与えないことを確認するために、ブロックチェーンへのトランザクションの記録が動的に制御されます。

次に、ミクロの視点からは、リアルタイムで各コントラクトを監視し、実際の状況に応じて調整を行うことができます。これにより、ブロックチェーンをより効率的なものにし、外部からの攻撃から保護します。

### 3−5　マルチアセットオファリング

メインチェーンを持つコインと同レベルの処理速度と拡張能力を提供することで、アセットオファリングの手続を簡略化します。

標準的なトークンオファリングでは、単純化され規制されたトークンオファリングの方法および手続が含まれます。他方でマルチアセットトークンオファリングでは、トークンをコントラクト上で直接使用することができ、他のコントラクトを導入する必要はありません。

### 3−6　マルチチェーン並列技術

マルチチェーン構造により、暗号化アルゴリズムとオンラインでの転送という制限があるシングルチェーン構造よりもトランザクションの処理を効率化することができます。

立体的 P2P ネットワークにより、クロスチェーンコンセンサスシステムが実現され、TPS が増加します。したがって、チェーンの数が増えるにつれ、ブロックチェーンの能力は無限に向上します。

### 3−7　アップグレード可能なブロックチェーン

ブロックチェーンの開発を犠牲にして強制的にフォークする場合を除き、ブロックチェーンがリリースされた後にブロックチェーンをアップグレードするのは困難です。

しかし、LLVM コンパイラでは、ブロックチェーンコードとコントラクトスクリプトがまとめられます。そして、すべてのクライアントは、アップグレードされたブロックチェーンが古いバージョンの特定のリンクに置かれた後に、共にアップグレードされます。

## 3−8　クラスタのセルフグルーピング機能

いずれかのノードがセルフグルーピング機能をオンにすると、ネットワーク内の特定のノードがクラスタ群を形成します。このクラスタ群は、トランザクションの検証とストレージに参加し、ユーザーのデータストレージコストを削減します。

ユーザーは、トランザクションの検証を通じて他のユーザーに協力することで、マイニングの仕組みに似た特別ボーナスを受け取ることができます。

## 3−9　量子耐性技術

量子計算は、量子情報の特殊性により、同時並行性という性質を有します。例えば、量子コンピュータが n 量子ビットのデータを処理する場合、実際には 2n のデータ状態を扱っています。このような同時並行性により、量子コンピュータは電子コンピュータにでは解決不能な問題を解決することができます。そのため、複雑な計算に基づく現在の公開鍵システムのセキュリティは、量子コンピュータの高度な計算能力により破られる危険性があります。

デコードに使用される最も一般的なアルゴリズムとして、Grover アルゴリズムと Shor アルゴリズムがあります。Shor アルゴリズムが、RSA、EIGamal、ECC、DH などの共通鍵の合意を攻撃できるのに対して、Grover アルゴリズムは、鍵の長さを半分に縮減することができます。したがって、量子計算の環境下では、RSA、EIGamal、ECC、DH を暗号方式として利用するのはもはや安全とはいえません。

国際的には、反量子暗号に関する研究は、主に、格子ベースの暗号、コードベースの暗号、多変量暗号およびハッシュベースの署名暗号に注目が集まっています。

格子ベースの暗号の問題の中心は、最短ベクトル問題（SVP）であり、これは格子システム内で最短の non-void ベクトルを見つけることです。これまでは、格子ベースの暗号を量子アルゴリズムでデコードできたことはありません。

以上のような量子コンピュータとの関係での安全性の観点から、Aurora は格子ベースの暗号を採用します。

## 3−10　クロスチェーン技術

現状では、ブロックチェーン同士を相互に接続することは不可能です。独立性が、異なるブロックチェーンが共に機能することを妨げます。しかし、Aurora は、無制限のバリューネットワークを獲得するために、クロスチェーン通信プロトコルやその他のクロスチェーン技術をサポートしています。

## 3−11　独自のマイニングメカニズム

ビットコインネットワークでは、マイニングノードが仕事量アプローチ（Proof of work）に基づいてトランザクションレコードを新しいブロックに独立して記録し、ビット

コインを報酬として獲得します。

マイニングの本質は、コミュニティメンバーの貢献度に応じて報酬を与え、参加を促すことにあります。

Auroraは、コードのアップグレード、バグの発見、効率化に資する提案の提供、コミュニティメンバー間で周知の情報の普及など、コミュニティーに貢献するあらゆる活動に対して報酬を付与します。

マイニングシステムは、最初のうちはブロックチェーンに書き込まれません。その代わりに、インセンティブを最大化できるルールが確定するまで、コミュニティでテストされ、最適化されます。

## 3－12　AOAトークンと手数料

AOAトークンは、Auroraの適切な機能を保証するものとして機能します。通常、AOAの手数料率は、攻撃からシステムを保護するために手数料率を急増する必要がある場合を除き、わずか0.0001です。

AOAトークンの発行総数は100億枚であり、そのうち26%は初期コミュニティメンバー、34%は投資家とパートナー、残りの40%はAurora Foundationの活動費、アチームメンバーとコミュニティ開発者への報酬、エコシステムの構築に使用されます。

# 4　ゲーム業界におけるAuroraアプリケーションの応用

## 4－1

(1) ゲームトークンのブロックチェーン化

ブロックチェーントークンは、ゲーム内においては、生産、取引、およびアカウント決済に使用されます。また、ブロックチェーントークンは、異なるゲーム上ではそれに応じて形を変えることができます。このオープンな経済システムでは、所有者はトークンについての完全な管理権を取得します。

(2) ゲームデータのブロックチェーン化

ゲームのアイテム、キャラクター、装備はすべてトークンによって定義されます。トークンは所有権を徴表するものであり、これにより所有者はゲームアイテム等をゲーム外で取引することができます。ゲームキャラクターや装備のブロックチェーン化は、ゲームの世界に革命をもたらします。そのため、ゲームの開発者、運営者、販売会社は、この変化に対応するためにゲームにおける自己の立ち位置を再定義する必要があります。ゲームは、最終的には、プレイヤーや開発者により装備の生産・使用のルールが決定されるコミュニティベースのものになるはずです。このような状況下では、ゲームの人気が高まり、その寿命が延びると考えられます。

(3) ゲームルールのブロックチェーン化

ゲームルールのブロックチェーン化により、ゲームの開発者やオペレーターによる恣意的なルール変更が不可能になるため、ゲームのアイテムや装備の生産の透明性が確保されます。このような透明性は、多くのゲームプレイヤーを引き付けるだけでなく、ゲーム開発者にも挑戦をもたらします。

## 4−2　IoT のためのアプリケーション

現在の IoT システムは、中央集権的なネットワーク管理アーキテクチャを利用しており、すべてのデバイスがクラウドサーバーを介して接続されています。しかし、分散型の IoT システムによれば、ブロックチェーンが、デバイス間のトランザクションと相互利用を促進するための基本的な枠組みを作り出すことができます。ネットワーク上の各デバイスは、独立して機能し、それ自体がマイクロビジネスとしてワークする実体を備えます。

## 4−3　AI や天文学などのハイテク分野への応用

AI や宇宙関連技術などのハイテク分野では、データのセキュリティとシナジーのバランシングに難航します。現在利用されている中央集権的なデータネットワークでは、クロスエリアシステムとマルチノードシステムの連携において問題があります。また、異なるデータネットワークシステム間の連携も完全には実現されていません。

このことからすると、ブロックチェーンにより、IoT 分野における技術革新を生み出すことができると考えられます。

## 4−4　サプライチェーン産業への応用

ブロックチェーン上のデータは透明性を有し、関係者全員の間で共有されます。サービスチェーン全体で完全で流暢なデータフローを形成するため、問題を発見し、時間内に解決することが容易になります。そのため、サービスチェーンの管理をより効率的に行うことができます。

## 5　Aurora のロードマップ

2018.3：Aurora が稼働を開始し、スマートコントラクトのためのオンラインプラットフォームと同期しました。
2018.5：アプリケーション分離技術とステレオネットを改善し、安全性と動作速度を向上させました。
2018.12：マルチチェーン並列技術、クラスタグルーピング機能、ブロックチェーンのアップグレード技術を完成させ、100 以上のアプリケーション及びブロックチェーンプロジェクトを実現します。
2019 年以降：量子耐性を実装し、明るく彩り豊かなブロックチェーンの世界を実現します！

## 6　コンタクト

ウェブサイト：www.aurorachain.io
E メール：official@aurorachain.io