Ολυμπιακοί Αγώνες
ΟΑ

全人民オリンピック・シャッフル

《OA白書》

ΟΛΥΜΠΙΑΚΟΙ ΑΓΩΝΕΣ

オリンピック精神·オリンピックの光

目次

はじめに.....3

1.プロジェクトの背景..... 5

1.1 業界の背景.....5

1.2 課題.....7

1.3 解決策..... 8

2、プロジェクトの説明.....11

2.1プロジェクトモデル..... 11

2.2 アプリケーションシナリオ..... 12

3、技術的実現.....17

3.1 OA の技術原理..... 17

3.2 ソリューション..... 17

4、ガバナンス構造..... 29

5.リリースノート 37

5.1OA コインの概要..... 31

5.2 リリースシナリオ..... 31

6.リスクのヒントと免責の説明.....32

6.1 免責事項..... 32

6.2 リスクに関する注意事項..... 33

概要

2020 年から、新冠の疫病は世界を席巻し、世界経済に大きな打撃を与え、各国民衆の生活様式も変えた。 ノーベル平和賞受賞者のマンデラ氏は、スポーツには世界を変える力があると語っていた。 世界が疫病のために再建された時、スポーツとオリンピック精神もその重要な役割を示した。 オリンピック主義はスポーツを通じてより良い世界を創造し、相互理解、友情、団結と公平な競争のオリンピック精神を提唱することを望んでいる。 世界人民が疫病に抵抗する中で示した勇敢な奮闘、粘り強さと団結互助もまさにオリンピック精神の生き生きとした描写である。

このような背景のもと、本プロジェクトチームと国際オリンピック委員会が共同で開発した OA（ギリシャ語では_λレンタルμπイタακ≦γνε、オリンピック）プロジェクトが誕生しました。 同プロジェクトはブロックチェーン技術に基づき、オリンピックのスポーツ精神の発揚、スポーツの質の向上、スポーツ文化の普及、慈善事業の発展、共有経済価値の創造を支えとするブロックチェーンプロジェクトである。 OA はブロックチェーンの非中心化、信頼性、スマートコントラクトなどの特徴を十分に応用し、オリンピック精神を駆動とするグローバルスポーツ生活プラットフォームの構築を目指している。 OA プラットフォームでは、産業チェーン上の各主体と個人は OA 上で情報伝送、正確なデータ、資産取引、資金分配などの活動を行うことができ、これらの行為はブロックチェーン技術の保護と奨励を受けている。

コア価値:非中心化、公開、透明性、公平性、共有

発展ビジョン:ブロックチェーン技術を全国民スポーツ・フィットネス分野に応用し、世界全国民スポーツ生活プラットフォームを構築する。

OA は 2 億枚のデジタル通貨を恒常的に発行する。 OA コインは、スポーツ分野におけ

る価値流通・取引媒体として利用することができ、記帳インセンティブだけでなく、一般的な等価物であるデジタルマネーとしても流通利用することができる。 OA コインを通じて、スポーツとオリンピック精神伝達業界の発展のために良好なデジタルサービスサポートを提供することができます。

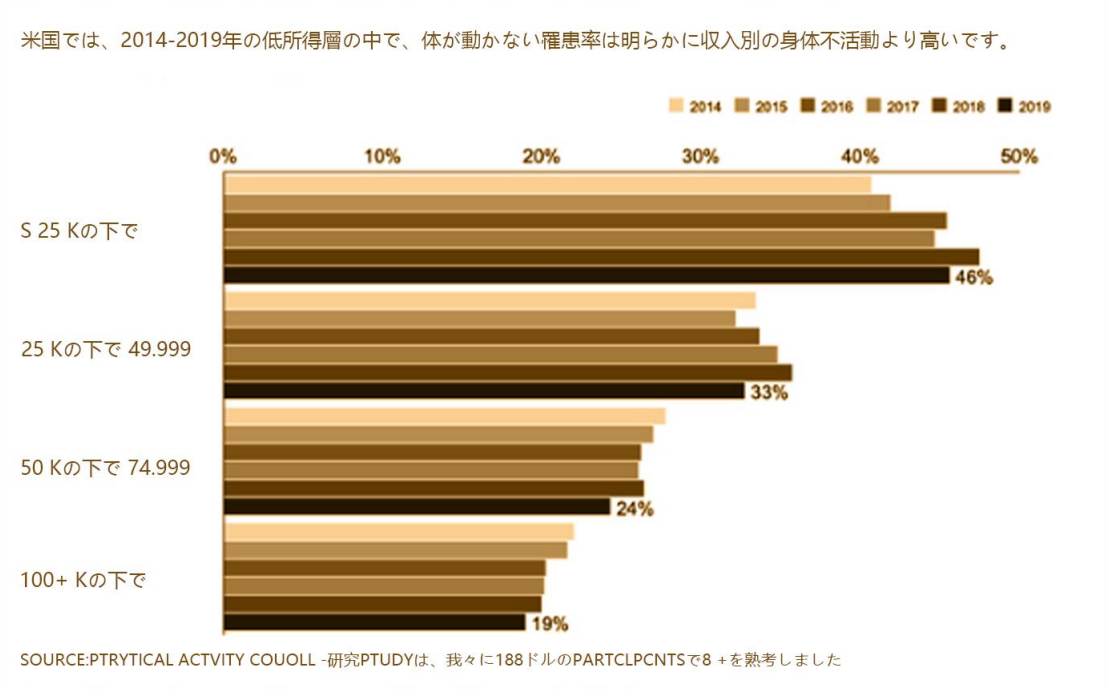
1.プロジェクトの背景

1.1 業界の背景

2020 年から、新冠の疫病は世界を席巻し、世界経済に大きな打撃を与え、各国民衆の生活様式も変えた。 ノーベル平和賞受賞者のマンデラ氏は、スポーツには世界を変える力があると語っていた。 世界が疫病のために再建された時、スポーツとオリンピック精神もその重要な役割を示した。 オリンピック主義はスポーツを通じてより良い世界を創造し、相互理解、友情、団結と公平な競争のオリンピック精神を提唱することを望んでいる。 世界人民が疫病に抵抗する中で示した勇敢な奮闘、粘り強さと団結互助もまさにオリンピック精神の生き生きとした描写である。

社交的な隔離、旅行の制限は人々の生活に多くの変化をもたらして、しかし更に多くの人もこの期間にスポーツの重要性を意識します:スポーツは人々に健康な体をもたらすだけでなく、更に絶えず挑戦に打ち勝つ自信と決意を強めることができます。 オリンピック憲章の冒頭にあるように、スポーツは人生の哲学である。 この特別な時期には、スポーツの生活哲学を学び、身につける理由がもっとあります。

新冠の疫病はより多くの家庭を低所得層に持ち込み、それによって個人の運動量の差を激化させた。 2019 年には、年収 2 万 5000 ドル未満の米国の回答者の 46%が運動不足だと答えた、 10 万ドル以上の収入を得た回答者のうち、運動をしない人は 19%にとどまった。 スポーツ業界は緊密に協力して、異なるグループに的を絞ったスポーツソリューションを提案すべきである。



図表 1-1:運動量と所得水準は正の相関関係にある

過去 1 年間では、デジタルスポーツおよびオンラインスポーツコミュニティは、社会的距離と在宅隔離の規定により急速に発展してきました。 デジタルスポーツは引き続き 2021 年と来年の人気トレンドとなり、伝統的なスポーツと相互補完し、ユーザー層を激励し、ロックする。

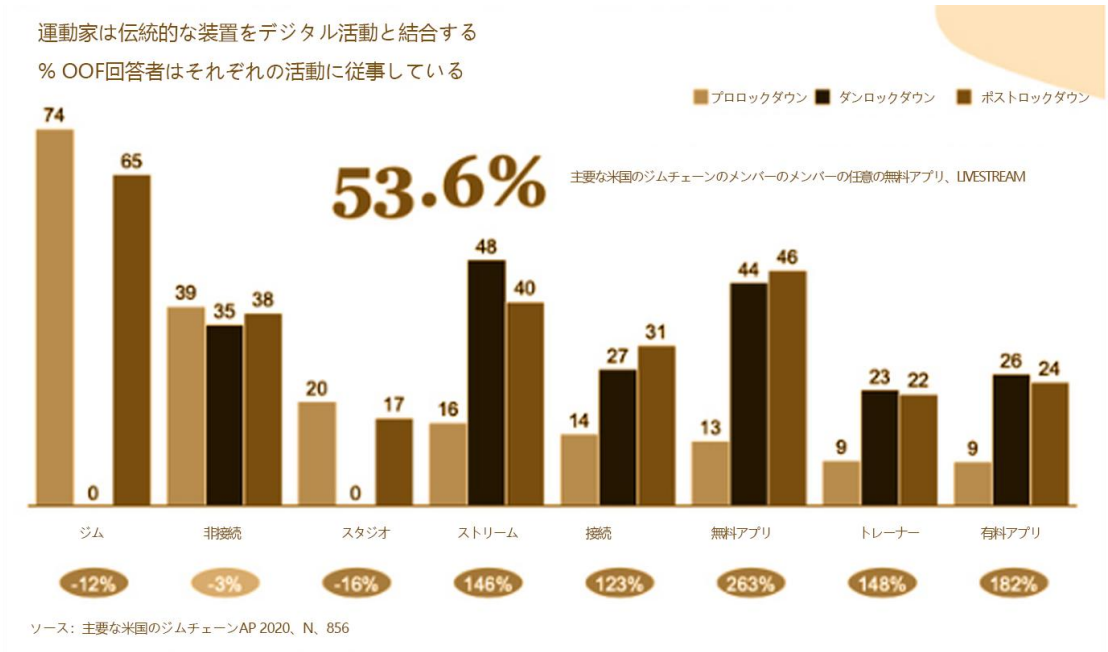


図 1-2:モーションスケールのディジタイズ

1.2 課題

ポスト疫病時代には、スポーツの経済的機能がさらに顕著になり、スポーツはこの危機の構成要素になるべきではなく、この危機を解決する有力な手段になるべきである。 スポーツは異なる社会、政治、宗教あるいは文化背景の参加者を一つに統合するツールになり、オリンピック精神の中で団結、平和、尊重の重要な原則も全世界で更に普及される。 しかし、現在の技術条件の下で、オリンピック精神の伝播と普及にはまだいくつかの問題が存在している

1、不健全な信頼システム:文化の伝播過程の中で、中心化システムの原因と監督メカニズムの不足のため、すべて信頼システムの不健全な問題が存在します。 これにより、情報伝達の歪み、公益寄付の減少、ユーザーの流出など、多くの問題が発生する可能性があります。

2、インセンティブの欠如:オリンピック文化の伝播分野では、ユーザーが資源を共有したり、資源に貢献したりする目的は主に収益のためではないが、長期的にインセンティブがなければ、このような行為も持続しにくく、市場は終始拡大しにくい。

3、標準化と大規模化の欠如:オリンピックの精神の核心は自強で、この精神を通じて人々に多くスポーツに参加させて、体を丈夫にすることができます。 しかしオリンピック文化の伝播は標準化と大規模化を実現する方法がない。 大多数の機構と組織はいずれも単独で戦い、協同革新発展できることはめったになく、競争構造が非常に分散し、内部摩擦が深刻になっている。

1.3 解決策

1.3.1 解決策

上記の問題は複雑に見えるが、糸を抜いて繭を剥ぎ、現象を通して本質を見ると、これらの問題の最終的な根源は 2 つの点にあることがわかる:

1、中心化組織がもたらす業界の不透明さ。 中心化された組織構造の下で、異なる主体の間の取引内容は外部の監督が不足して、相互の知る権利が不足して、必然的に価格が虚高になって、不良品を優良品の代わりにするなどの現象を招くことができます。

2、異なる段階における異なる取引主体間の相互信頼メカニズムが欠落している。 取引主体の間の信頼の欠如は、それによって取引コストの増加と取引効率の低下をもたらし、取引主体はこのようなマイナスの影響を相殺するために、各種の方式を通じて自身の収益を高め、自身のリスクを下げ、それによって各種の問題が現れ、更に重要なのは、環節の増加はこのような相互信頼の欠如による影響を更に拡大することである。

これらの問題を解決するためには、中心化された組織を打破し、取引主体を直接ドッキングさせ、効率性を高め、業界の透明性を高める必要がある。 しかし、これではさらに深刻な問題をもたらす--中心組織の制約がない下では、人類の従来技術条件は取引の相互信頼を維持することが難しい。 取引の相互信頼の問題は人類の誕生以来社会の発展に伴ってずっと存在して、人類は取引の相互信頼を実現するために大量の法律と技術の方面の制約条件を創立して、しかしずっと取引の詐欺の現象を根絶することができません。非中心化や弱中心化は取引をさらに混乱させ、従来の技術力やモデル改造による問題解決の道を塞いでしまう。 新しい技術概念を導入する必要があります。

1.3.2 ソリューション

ブロックチェーンは、データブロックを時系列に連続して組み合わせたチェーンデータ構造であり、暗号的に保証された改ざん・偽造不可能な分散型帳簿である。 客観的に見ると、ブロックチェーン技術の特徴は取引相互信頼問題の解決に決定的な役割を果たし、現在の健康と文化市場に存在する様々な問題を根本的に解決することができ、具体的には次のように現れている:

1、非中心化:非中心化の特徴に基づいて、ポイントツーポイントの取引が実現され、各取引主体はユーザーからインターネットサーバーまでブロックチェーンの1つのノードであり、ノードとノードの間で直接取引することができ、過度の段階を避けることができる。 また，ノードごとの履歴，フロー状況などの情報は変更不可能であり，取引双方の信頼性を大幅に向上させることができる。

2、安全性:産業チェーンでは、データはコア企業や参加企業によって分散的に孤立して記録され、中心化された帳簿に保存されることが多い。 帳簿上の情報が自己に不利な場合には、帳簿情報が改ざんされたり、無断で削除されたりするリスクがある。 ブロックチェーン技術のチェーン上のデータ改ざん不可とタイムスタンプを押す特性は、すべてのデータが改ざんされないことを保証する。 データの改ざんが不可能であるため、情報の非対称性が大幅に低減され、信用調査と企業間のコミュニケーションコストが削減されます。このアプリケーションは、企業間の信頼性を迅速に確立すると同時に、コア企業が負うリスクを分化させることができます。

3、情報の透明性:ブロックチェーンデータの情報が透明で、変更できないという特徴に基づいている。 各ノードは、データ・アプリケーションのトレーサビリティを確認でき

ます。 これにより、企業はデータ改ざんを行うことが不可能になり、ユーザーのセキュリティとプライバシーが十分に確保され、エクスペリエンスが大幅に向上します。

4、スマートコントラクト:ブロックチェーンで定義された規則の下で、産業チェーン全体の各取引主体はブロックチェーン技術を通じて自動的にスマートコントラクトを実行することができ、人為的に真偽を選別する必要がなくなり、管理コストと時間コストを大幅に削減することができる。 また、ノード間の自動取引の能力は全く新しいビジネスモデルを生み出すことができ、ネットワーク内の各ノードは独立したビジネス主体として機能することができ、非常に低い取引コストで、他のノードと自分のデータとリソースを共有することができ、これは新しいビジネスモデルの確立に大きな想像の余地をもたらす。

上述の内容からわかるように、センターへの移動、安全性、情報の透明性、スマートコントラクトなどの特徴は、異なる段階の取引主体間の相互信頼問題を根本的に解決しており、このような解決方案は基礎技術から完成したものであり、現在のオリンピック精神の伝播とスポーツ生活分野における問題を解決する上で決定的な意義がある。

2、プロジェクトの説明

2.1プロジェクトモデル

このような背景のもと、本プロジェクトチームと国際オリンピック委員会が共同で開発したOA（ギリシャ語では_λレンタルμπイタακ≦γνε、オリンピック）プロジェクトが誕生しました。 同プロジェクトはブロックチェーン技術に基づき、オリンピックのスポーツ精神の発揚、スポーツの質の向上、スポーツ文化の普及、慈善事業の発展、共有経済価値の創造を支えとするブロックチェーンプロジェクトである。

発展ビジョン:ブロックチェーン技術を全国民スポーツ・フィットネス分野に応用し、世界全国民スポーツ生活プラットフォームを構築する。

OAでは、各主体は情報伝達、資産取引、振替、デジタル資産分配などの活動を対等に行うことができ、これらの行為はブロックチェーン技術に基づく保護と奨励を受けている。 全世界のオリンピック精神の伝播を激励する。 また、デジタル通貨の応用により、運動効率を大幅に向上させ、オリンピックを中心とした慈善サービスを充実させることができ、市場はさらに繁栄するだろう。 その上で、オンラインモール、コミュニティサービス、スポーツクイズなどの派生サービスが誕生する。

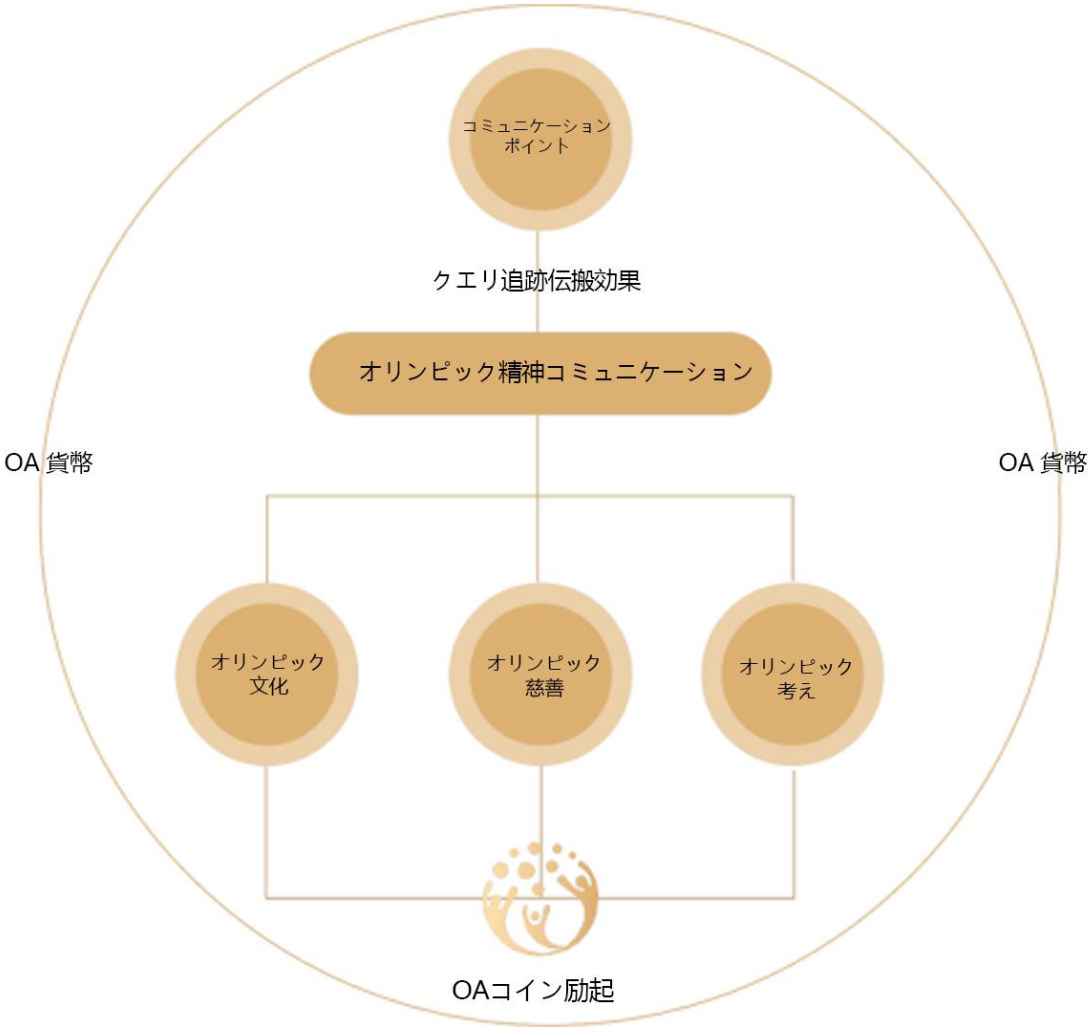
図 2-1:OA のパターン

2.2 アプリケーションシナリオ

OA プラットフォームには、次のようなさまざまなアプリケーションシナリオがあります:

2.2.1 オリンピック精神の伝播

伝統的なモデルの下で、オリンピック精神の伝播は多層の段階を経なければならず、過程の中で情報の歪みの問題が発生する可能性が高く、最終的にオリンピック精神の伝播の効果に影響を与える。 OA では、ブロックチェーン技術の非中心化と高度な安全性の特徴により、オリンピック精神は文化、慈善、クリエイティブなどの様々な形式でバリアフリーに伝播することができる。 さまざまな企業、組織、個人が配信のノードとなり、すべてのデータがリンクされて情報が歪まないようになります。同様に、配信に貢献した人にはデジタル資産のインセンティブが与えられます。 この方法を通じて、オリンピック精神の伝播効率は大幅に向上し、より多くの人がオリンピック精神の核心に触れ、世界の貧しい後進国が自分のオリンピック精神とオリンピック援助を確立し、積極的にスポーツと生活を一体化し、世界を戦乱の苦しみ、疫病の害から守ることができるようになる。 特に、五輪委員会は定期的に OA コインを通じて後進国への援助と慈善活動を。

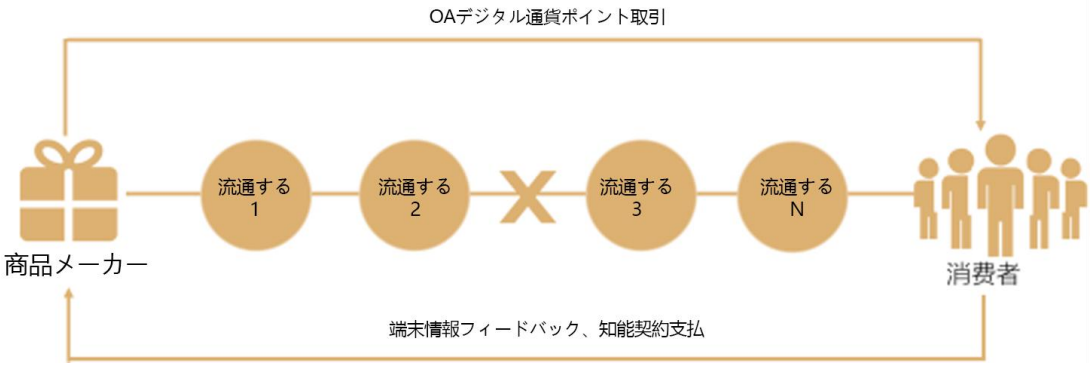


図表 2-2:オリンピック精神の伝播

2.2.2 オンラインビジネス城

ユーザーは OA コインを受け取ると、OA のオンラインモールで、スポーツ・フィットネス器具の購入、スポーツ会場の消費時間、スポーツウェアなどの取引や交換を行うことができる。 従来の技術条件では、商品取引は複数の段階を経なければならず、各段階はコストを増加させなければならず、情報は極めて不透明であった。 一方、OA オンラインモールは、低コスト、透明性、便利な取引プログラムを取引当事者に提供することができ、非中心化とスマートコントラクトの特徴を通じて、ポイントツーポイントの取引を可能にし、メーカーはエンド消費者と直接取引することができ、取引効率を大幅に

向上させ、取引コストを削減し、市場フィードバック情報をタイムリーに取得することができます。 また、スマートコントラクトにより、すべての費用が約定内容に基づいて自動的に実行され、双方が多くの労力と時間を費やす必要がなくなり、双方の取引の効率が大幅に向上する。



図表 2-3:OA オンラインモール

2.2.3 コミュニティサービス

OA はユーザーコミュニティを構築し、多くのスポーツ愛好家、クラブ機構、スポーツ会場運営者がオリンピック分野の各種問題を自由に討論し、オリンピック精神やスポーツ知識などを相互に交換できるようにする。 また、スポーツ・フィットネスは専門性が高く、長期的な社会関係を構築できる分野であることを考慮すると、OA はコンテンツ公開モジュールをオープンし、ユーザーはプラットフォーム上でオリジナルコンテンツを公開し、他のユーザーが関連知識を学習するのを助けることができ、知識に価値があると感じたユーザーはこれらのコンテンツに対して賞金をかけて購読し、公開者の行動を奨励することができる。 すべての報酬は OA デジタル通貨で支払われます。

図表 2-4:OA コミュニティサービス

2.2.4 スポーツクイズ

スポーツクイズはスポーツ業界において非常に重要な分野であり、ブロックチェーンの各種技術特性に依拠して、OA プラットフォームは公開・公平・公正な透明化クイズメカニズムを実現し、すべてのスポーツクイズプロジェクトはスマートコントラクトの作用の下で全世界のユーザーに開放され、非インタラクティブ乱数アルゴリズムを使用して懸賞の絶対的公平を保証している。 さらに重要なのは、OA プラットフォームを通じてブロックチェーンを媒体に世界中のユーザーがクイズサービスの購入やボーナス決済を簡単かつ迅速に行うことができることだ。 従来の技術条件であった外貨両替の非効率性や地下銭荘での為替レートの高さはなくなるだろう。 利用者は OA コインを利用すれば、自国通貨と同じように任意の国のスポーツクイズサービス（OA プラットフォームにログインしていれば）を購入することができ、賞金も瞬時に入金することができる。

図表 2-5:スポーツクイズ

以上をまとめると、オリンピック精神の存在がある限り、OA の存在価値や意義があることがわかります。 さらに重要なことに、このプロジェクトはオリンピック委員会に裏書として依存しているので、世界のオリンピックスポーツ業界では、OA の着地と応用に十分な価値のサポートを提供するために、私たちは非常に多くの応用シーンを想像することができます。

3、技術的実現

3.1 OA の技術原理

OA は既存のブロックチェーン技術を基礎として改良を行う革新的なブロックチェーン技術プラットフォームで、DAPP のワンストップ開発をサポートするだけでなく、異なるチェーンのシームレスな融合相互作用をサポートし、機能が完全で、システムが豊富で、可塑性が強いなどの特徴がある。

OA はグローバルなパブリックチェーンを目指して設計されています、 P2P ネットワーク転送プロトコル、PAOS コンセンサスアルゴリズム、スマートコントラクト、仮想マシンテクノロジーをサポートし、複数の署名を使用して同じファイルに複数の秘密鍵を使用して署名することで、ファイルアクセスのセキュリティレベルを向上させます。取引匿名保護にはリング署名テクノロジーを使用します。マルチチェーン融合により、OA と他のチェーンの相互作用を迅速かつ簡単に行うことができます。 サービス層はブロックチェーンに格納されたデータを簡単に加工処理し、DAPP に対して様々なアプリケーションに必要なサービス呼び出しインタフェースを提供する。

3.2 ソリューション

3.2.1P2P 通信技術

OA ネットワークは、インターネット上で取引を行うプロトコルのセットである OA プロトコルによって実現される P2P ポイントツーポイントネットワークである。 このプロトコルは、人々が分散ネットワーク内で価値を移転することを可能にし、お金のメールを送信することができるようにします。 実際、OA ネットワークプロトコルの目的は、ネットワーク全体のノード間で取引情報の一貫性を迅速に実現することであり、これは

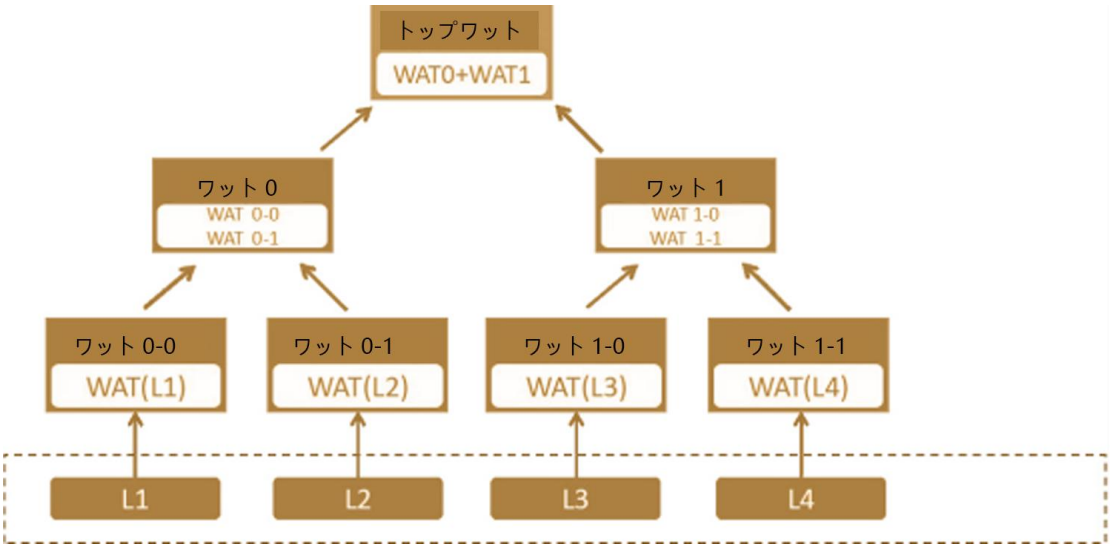
コンセンサスプロセスの基礎を提供する。

3.2.2 二重側鎖

当社の構想では、OA は、さまざまなブロックチェーン技術をリンクする新しい基盤技術プラットフォームを構築し、信頼に基づく価値をさまざまなブロックチェーンシステムで流通させることができます。

OA はブロックチェーンと DAG システムの二重側鎖である。 ブロックチェーンベースおよび非ブロックベースの分散システム情報と価値との相互接続を実現する。 その中、OA はクロスプラットフォームの価値相互通信の媒体であり、OA プラットフォームはもともとクロスプラットフォームの情報交換の媒体である。 OA システムの設計特性に基づき、OA はシード設計段階でブロックチェーンベースのシステム（UTXO ベースと Account Based ベースを含む）と DAG ベースの分散帳簿情報の読み取りを考慮しています。 将来的には OA に基づいてブロックチェーンと DAG システムとの間で明（White）暗（Black）トークンを直接送信または受信することが可能になる。 同時に、OA クライアント間のゼロ知識証明に基づく完全に暗号化された通信や、他のシリーズのエキサイティングな機能も可能になります。

ビットコインやエーテル坊などの伝統的なブロックチェーンはメルケル木のような二分木に基づくデータ構造を採用している：



OA の技術チームはビッグデータ、クラウドコンピューティング、暗号学、ブロックチェーン分野で長年培ってきた技術専門家で構成されており、OA は福利厚生という 2 つの全く異なる基礎データ構造システム間のチャネルを計画し、基礎技術層で主流のブロックチェーン技術標準と互換性を持たせる。

3.2.3 コンセンサスアルゴリズム

1、コンセンサスの基礎

OA チェーンでは，ノードは軽ノード，全ノードの 2 つのタイプに分類される。 ライトノードはコンセンサスに参加せず、ハッシュツリーが自身に関連するトランザクションデータのみを保存する。 全ノードはコンセンサスに参加し、発生したすべてのトランザクションデータを保存します。

OA チェーンの中で、3 種類の取引類型が存在する:普通取引、契約取引、暗号化取引、普通取引直接入庫。 契約取引はスマートコントラクトと仮想マシンによってトリガーされ、安全性が高く、自律性があるなどの特徴がある。 暗号化取引ではリング署名などの技術を使用し，暗号化取引のデータがコンセンサスで一致した後，スマートコントラク

トを使用して入庫操作を行うとともに，ダブルフラワーの問題を回避するために，より多くの処理方法を提供する。

2、特徴

- 大容量のデータスループット:OA のスループットは 1,000 本/秒に達することが実証されています。
- 取引速度が速い:新ブロックの生成時間は 2-10 秒で、ビットコインの 10 分やエーテル坊の 1 分に比べ、商業化事業の着地が大幅に促進された。
- 高いフォールトトレランス:ビットコインと同様に 50%のフォールトトレランスをサポートしており、攻撃者にとっては、取引データの帳簿を変更するために 50%の費用がかかります。
- 取引料金の低さ:1 取引当たりの取引料金は極めて少ないため、電子決済はクロスボーダー振替や頻度の高い小額決済などの分野で異彩を放っている。
- 高いセキュリティ:総合的なテクノロジーの活用により、セキュリティが大幅に強化されています。 スマートコントラクト、仮想マシン、リング署名、暗号化アルゴリズムなどがあります。

3、コンセンサスプロセス

OA ネットワークは 2~8 秒ごとに新しいブロックを生成し、新しいブロックは PAOS と呼ばれるコンセンサスメカニズムを使用して取引コンセンサスを行い、新しいブロックがネットワーク全体で承認される過程はすべてのネットワークノードがコンセンサスを行う過程である。 コンセンサスは 2 段階に分けて完成され、第 1 段階は取引セットのコンセンサスを達成することであり、第 2 段階は新たに生成されたブロックを提案し、最終的にコンセンサスされたブロックを形成することである。 取引セットを達成するため

のコンセンサスはラウンドごとに行われ、各ラウンドで次の操作が行われます:

- 各ノードは、コンセンサスの開始時にコンセンサスを必要とする取引をできるだけ多く収集し、「候補セット」に入れる。
- 各ノードは、信頼ノードリスト内の「候補セット」を和セットし、各トランザクションに投票する。
- UNL におけるサービスノード取引の投票結果は，一定の投票比率に達した取引は次のラウンドに進み，比率に達しなかった取引は破棄されるか，次のコンセンサス過程の候補セットに入る。

最終ラウンドでは、80%以上の投票が行われたすべての取引は、合意された取引セットに配置されます。 ビットコインと同様に、トランザクションセットも Merkle ツリーデータ構造を採用しています。 トランザクションセットが形成されると、各ノードは新しいブロックのパッケージングを開始します。ブロックのパッケージングは次のように行われます:

新しいブロック番号、コンセンサス取引セットの Merkle 木の根 Hash、親ブロック Hash、現在のタイムスタンプなどの内容を一緒にして、ブロックハッシュを計算する。 各ノードは、自身が生成したブロックハッシュを可視ノードにブロードキャストする。 ノードは、すべての信頼できるリスト内のノードからブロードキャストされたブロックハッシュを収集した後、 各ブロックハッシュの発生回数（すなわち、各ノードがブロックハッシュを「投票」した回数）は、自ノードが生成したブロックハッシュと組み合わせて計算され、あるブロックのハッシュの割合が閾値（一般的に 80%）を超える場合には、そのブロックハッシュはコンセンサスが通過したブロックのハッシュであるとみなされる。自ノードが生成したブロックハッシュが同じであれば、自ノードがパックしたブロック

は確かであり、新たに合意されたブロックであり、直接ローカルに保存され、状態が更新される。 本ノードによって生成されたブロックハッシュがコンセンサスによって通過されたハッシュと異なる場合には、ブロックハッシュが正しいノードに行って新しいブロック情報を要求し、ローカルに記憶し、現在の状態を更新する必要がある。

上記リンクにおけるブロックハッシュの発生回数（投票割合）が設定された閾値を超えていない場合には、条件が満たされるまでコンセンサスプロセスを再開する。 これで、1つのブロックのコンセンサスプロセスが終了し、次のコンセンサスプロセスが開始される。

3.2.4 デジタル・ゲートウェイ

OA デジタルゲートウェイは、OA システムへの資金の輸出入です。 これは、各国の法貨やビットコインなどの仮想通貨を問わず、様々な通貨を OA システムに注入したり、OA システムから引き離したりすることができる仲介者のようなものです。（英語） これにより、たとえ 2 人が互いに信頼のない見知らぬ人であっても、2 人が同時に同じゲートウェイを信頼していれば、2 人間の振替を行うことができる。

「ゲートウェイ」を大手銀行や大手金融機関が担当していれば、この信頼チェーンは容易に構築できる。 「ゲートウェイ」の導入により、利用者間の振込が知人間にとどまらず、見知らぬ人同士でも可能になることが解決された。

OA デジタルゲートウェイアルゴリズムは、ゲートウェイ間の最短経路を探索し、中間ゲートウェイが存在する限り、商品の交換が成功するような信頼チェーンを形成することができる。 次の図 Alex のエージェント AgenOA は Beth のエージェント AgB を信用していない可能性があるが，双方を信用している第三者エージェント AgC が存在する可能性があり，Alex のエージェントは第三者エージェントに借りがあるという 2 つのツケ

が生じる。 第三者エージェントは Beth のエージェントに借りがある。 第三者エージェント Agent C は取引の処理を担当し，第三者エージェントにより異なる通貨交換をサポートするブリッジを形成することができ，稲妻ネットワークを融合することにより秒単位の支払いを実現することができる。

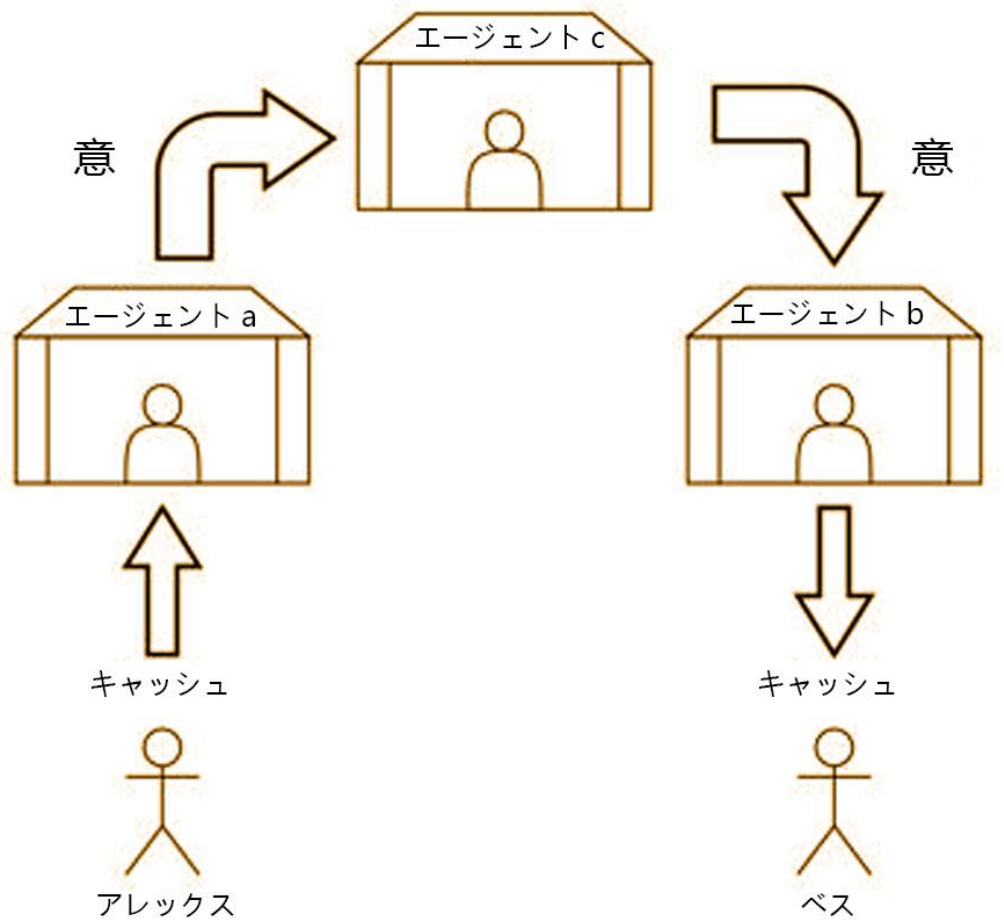


図 3-1:ゲートウェイの相互作用

ブロックチェーンゲートウェイは本質的に BTC と ETC に基づく決済記帳システムであり、商人の注文システムとドッキングし、Token に転送すると自動的に伝票を報告することができ、会員に大量に Token に転送して Token を送信することもサポートし、バックグランドで手動で大量に Token に転送することもサポートし、API で自動的に Token に転送することもサポートしている。

3.2.5OA スマートコントラクト

OA は、仮想マシン(OAVM)を介して、スマートコントラクト機能の実装において、コンピュータストレージアーキテクチャのような階層化の考え方を採用しています。 スマートコントラクトは法律の契約言語に近く、安全性が高く、スマートコントラクトの手数料は契約が占めるバイトに基づいて計算される。 OA のスマートコントラクトは、記述的で完全なブール文で構成されているので、従来の法的契約言語により近く、ブール演算、数学演算、さらにはデータストレージなどをサポートしています。 OA は、一般的に使用される宣言されたスマートコントラクトのテンプレートを提供し、ユーザーが使用したり、カスタマイズされたニーズに合わせて改善したりすることで、コントラクトの導入の難易度とエラー率を削減します。

スマートコントラクトモデルは次のとおりです:

["contract template", [

"hash of unit where the template was defined",

{param1: "value1",param2: "value2"}]]

OA にはスマートコントラクトモジュールパッケージが内蔵されており、モジュール構造から見ると、OA スマートコントラクトモジュールは対外サービスモジュール（例えば RPC モジュール）と基礎設備モジュール（例えばネットワークモジュール、ストレージモジュール、アカウントモジュールなど）の間にあり、ストレージモジュール、基本暗号化アルゴリズム、アカウントモジュール、ネットワークモジュールなどのその他のモジュールはスマートコントラクトの基礎サポートを提供する。

スマートコントラクトは、上位アプリケーションによって定義され、インタプリタによって解釈され、記憶モジュールによって記憶され、OA スマートコントラクトモジュー

ルパッケージによって演算される。 OA スマートコントラクトインタプリタは、複数の高度なプログラミング言語をサポートします。 アプリ開発者は、使い慣れた言語を使って OA スマートコントラクトを設計することができます。

3.2.6 非対話型乱数生成アルゴリズム

非対話型乱数生成アルゴリズムとは、乱数シードの生成に参加するためにユーザが追加のカスタマイズ情報を提供する必要がないアルゴリズムである。 我々は，スポーツクイズの公平性を十分に考慮して，ハードウェアシードによって生成された乱数を適用し，システムの安全性を確保した。 次の図は、OA の非対話型乱数生成プロセスを示しています:

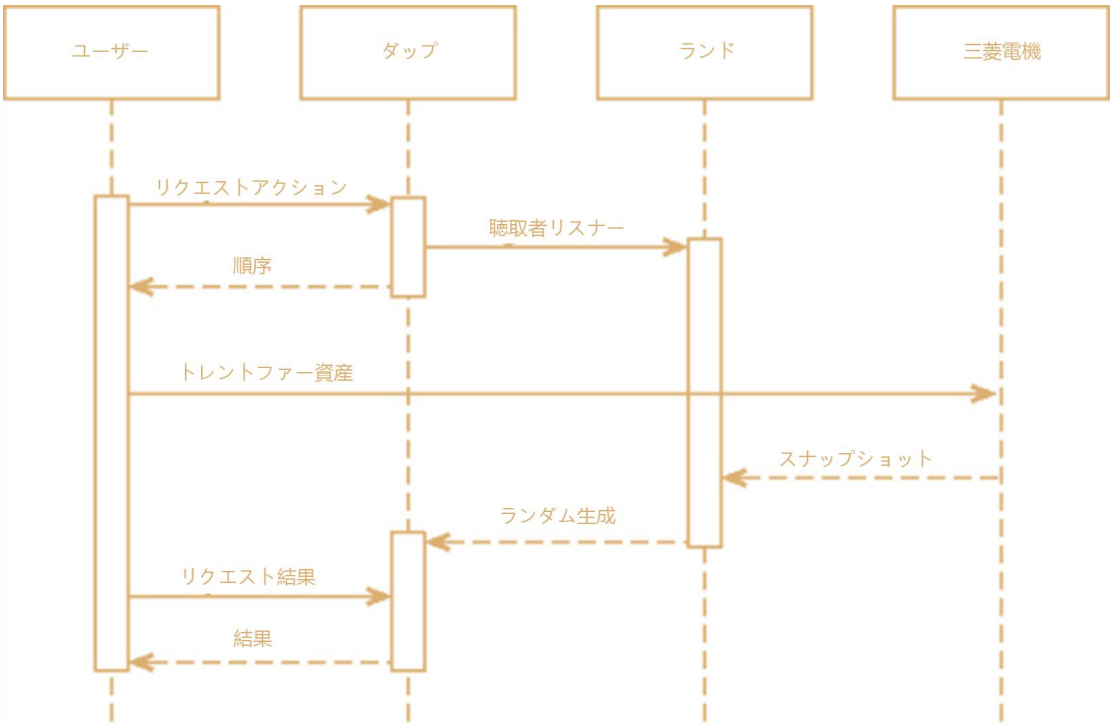


図 3-2:OA 非対話型乱数生成プロセス

- ユーザは OA サービスに登録を要求し、OA サービスは登録ユーザのチェーン上の行動を監視する。

- ユーザはパスワード生成要求を1回開始し、この要求はOAのノードによって検証された後、Snapshotの形式でブロックチェーン帳簿に記入される。
- OAは、帳簿中の当該取引によって生成されたSnapshot情報をリアルタイムで傍受し、当該SnapshotのID値を乱数シード seedとして取得する。
- 特定の乱数生成器randを選択し、乱数r=rand（seed）をユーザに生成する。

ここで、各スナップショットは、対応する要求、検証ノードの署名、検証ノードの最後のスナップショットの3つの部分で構成され、スナップショットの内容をハッシュしたHash値がスナップショットIDとなります。 これは、要求の発信者も検証者も一方的にスナップショットIDの値を予測して改ざんする方法がないことを意味し、スナップショットIDを乱数シードとして使用することは安全である。

乱数を生成した後，使用時にその有効性を検証する必要がある。 OAでは，トランザクションに対応するSnapshotを直接問い合わせ，Snapshotの内容をハッシュしてSnapshot IDを取得し，そのIDを乱数シードとして乱数を生成し，取得した乱数と比較することで，その乱数が有効であるか否かを検証することができる。

3.2.7 量子計算耐性

現在のビットコインに代表されるブロックチェーンシステムでは、 SHA-256ハッシュ計算とECDSA楕円曲線暗号はビットコインシステムの最も基本的なセキュリティィを構成しています、 しかし量子コンピュータ技術が進歩していく中で、 特にショアアルゴリズムを典型的に代表する量子アルゴリズムの提出、相関演算操作は理論上で指数レベルから多項式レベルへの転換を実現することができて、これらの古典的なコンピュータにとって十分に「困難」な問題は必ず予測できる将来に実型量子コンピュータに解読される。

暗号化アルゴリズム	タイプ	作用	潜在量子コンピュータ能力脇衝撃
AES	対称鍵	暗号化	鍵の長さを増やす
SHA-2,SHA-3		ハッシュ機能	より多くの出力が必要
RSA	公開鍵暗号化	デジタル署名鍵の生成	安全性を失う
ECDSA,ECDH（エリプソイド	公開鍵暗号化	デジタル署名鍵の生成	安全性を失う
DSA（有限体密度）	公開鍵暗号化	デジタル署名鍵の生成	安全性を失う

既存のブロックチェーンシステムの大部分は楕円曲線デジタル署名方案 ECDSA を採用しているが、量子コンピュータの下で ECDSA 署名アルゴリズムに対して非常に効率的な SHOR 攻撃アルゴリズム、Shor アルゴリズムは大整数分解、離散対数逆求めるなどの困難な数学問題の解決に適しているため、ECDSA 署名アルゴリズムは量子攻撃の下でかなり安全ではない。 OA は格理論に基づく署名アルゴリズム NTRUSign-251 を採用しており、アルゴリズムの具体的な実現フローは次の通りである:

1. 鍵生成

つの多項式 f および g は、f および g の係数における 1 の個数がそれぞれ d f および d g であるように、リング R 上で選択される。 そして，f と g から公開鍵を計算する。 h: h = Fq * (mod q)

多項式（F，G）を解くことで、式 f 下 G−F 下 g=q を満たす

そして F≒f，G≒g である。

2. 署名プロセス

メッセージ M は HASH 変換されて多項式（m1，m2）に変換され、ここで、多項式 m1，m2 は共にリング Rq 上の 1 つの多項式である。 ループ上の多項式 A，B，a，b は、次の条件を満たすように計算されます:

G * m1 − F * m2= A + q * B

−g * m1 − f * m2 = a + q * b

そして、A 及び A の各項の係数が、−q/2 より大きくかつ q/2 より小さい条件を満たすことが要求される。 多項式 s を計算するには、次の手順に従います:

s = f ∗ B + F ∗ b(mod q)

s は平文 M を公開鍵 h を用いて計算した署名である。

3. 検証プロセス

メッセージ M はハッシュ変換されて多項式（m1，m2）に変換され，検証対象署名 s と公開鍵多項式 h から計算される。

t = s ∗ h(mod q)

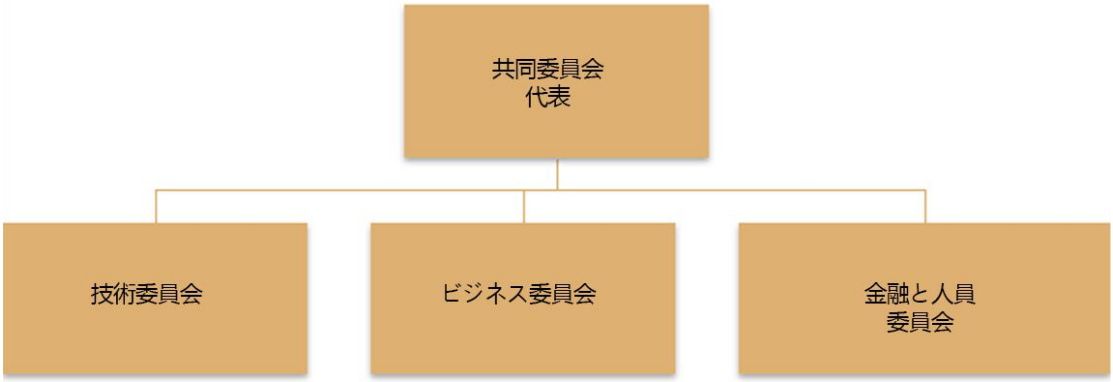
t = g ∗ B + G ∗ b(mod q)

多項式（s，t）と多項式（m1，m2）との間の距離 m1−s+m2−t を計算し、距離が Norm Bound より大きい場合には検証に失敗し、それ以外の場合には検証に合格して署名は有効である。

要約:NTRUSign−251 署名アルゴリズムの安全性は、最終的に 502 次元整数格子における最短ベクトルを求める問題と等価であることが知られている、 一方、格子中の最短ベクトル問題は SHOR 攻撃アルゴリズムの下では無効であり、量子コンピュータの下では他の求解高速アルゴリズムもなく、現在の最良のヒューリスティックアルゴリズムも指数関数的であり、NTRUSign-251 署名アルゴリズムを攻撃する時間複雑度は約 2168 であるため、NTRUSign-251 アルゴリズムを採用した OA は量子計算の下で SHOR アルゴリズム攻撃に抵抗することができる。

4、ガバナンス構造

OA プロジェクトの持続可能性と管理の有効性を確保するため、OA チームは OA 財団を設立し、財団の組織と活動を規範化し、財団、関連収益者、ユーザーの合法的な権益を維持し、財団はシンガポールの憲法、法律、法規、規則、ポリシーを遵守しています。OA 財団の下には、技術委員会、ビジネス委員会、財務および人事委員会、共同代表委員会が設置されており、重要事項は、技術委員会、ビジネス委員会、財務および人事委員会によって選出された共同代表委員会によって決定されます。 共同代表委員会会長は共同代表委員会によって選出され、日常事務管理を担当する。



図表 4-1:組織構成

1. 共同代表委員会は、最高意思決定機関であり、その機能には次のものが含まれる:

(1) OA 管理規程の変更、

(2) OA 定款の実施の監督、

(3) 共同代表委員会の会長及び各職能委員会の長の選任又は解任、

(4) 重要な意思決定を制定又は修正する。

共同代表委員会のメンバーの任期は 5 年であり、共同代表委員会のメンバーの任期が満了すると、技術委員会、ビジネス委員会、財務および人事委員会の再投票により 5~20 名のメンバーが選出されます。選出されたメンバーは財団を代表して重要かつ緊急の意

思決定を行い、在職中に与信調整を受ける必要があります。

2. 技術委員会:

OA 技術委員会は基礎技術開発、各製品開発、審査、管理業務などを担当する。 具体的な内容は次のとおりです:

（1）コード管理、コード開発、コードテスト、コード監査、コードオンライン、脆弱性修復など。

（2）プロジェクト追跡会議を開催し、プロジェクトの進捗とニーズをコミュニケーションする。

（3）OA 技術の応用シーンを掘り起こし、商業的な着地を実現する。 コードのオープンソース審査では、パブリックチェーン、アライアンスチェーンのオープンソース、プライベートチェーンはオープンソースでないことを許可することができる。

3、ビジネス委員会:

（1）OA 技術の普及、原チェーン制品の普及、各種資源のドッキングなどを担当する。

（2）OA ブランドイメージを形成し、各管理制度を確立し、健全化する。

（3）広報を担当する。 理事会の評判に影響を与える事象が発生した場合には、内部監査評価を経て、委員会による広報対応を統一的に行う。

4、財務及び人事委員会:

（1）報酬管理、日常運営費用審査などを担当する。

（2）関連文書の起草、審議、会議のスケジュールなど、各種行政系事務を担当する。

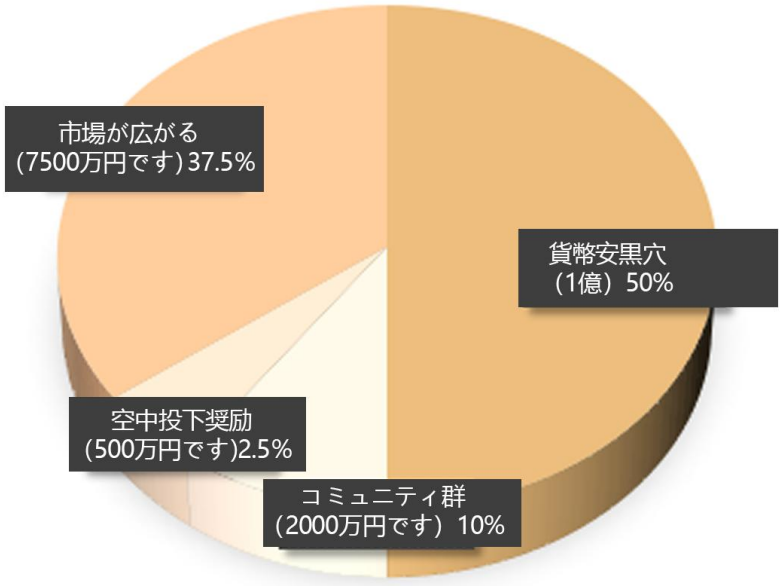
5.OA コインの概要

5.1OA コインの概要

OA コインは脱中心化運動生活生態系の稼働を駆動する血液である。 主に世界のスポーツ・フィットネス分野の開発、保護、支払いなどの場面に応用されている。 今後、各企業や個人が OA に基づいてさまざまなサイドチェーンとアプリケーションを開発することを奨励します)。その際、異なるサイドチェーンとアプリケーション間のデータ相互作用、スマートコントラクトの実行、および各段階の資産と情報データの交換は OA コインを消費し、OA コインは生態系全体の基礎デジタル通貨となります。

5.2 リリースシナリオ

OA デジタル資産の総発行部数は 2 億枚で、発行計画は以下の通りである:



図表 5-1:リリースシナリオ

原価格:0.01 USDT

1 日 1 回:スイス・ローザンヌ時間 12:00~15:00

6.リスクのヒントと免責の説明

6.1 免責事項

このドキュメントでは、プロジェクトに関連する情報のみを提供します、 本書またはドキュメントに記載されているいかなる内容も、証券、先物取引、オプション、その他の金融商品の購入、販売の勧誘、提案、またはいかなる国・地域のいかなる人に対する投資助言またはサービスの提供、または提供とはみなされません、 本書に記載されている内容は、投資助言や有価証券の適用に関する助言を構成するものではありません。 過去の業績は必ずしも将来の業績を示すものではありません。また、本書に記載されている予測、市場の見通し、予測は、一定の前提に基づく将来予想に関する記述であり、実際に発生する事象を示すものではありません。

両替意思者は、自ら意思決定した後に両替を行う場合には、当該リスクを完全に受け入れなければならず、かつ、自らそのために相応するすべての結果又は結果を負担することを希望しなければならない。 財団およびチームは、以下を含むがこれらに限定されない、OA プロジェクトへの参加に起因する直接的または間接的な損失を一切負担しないことを明確に表明している: 因为用户交易操作带来的经济损失;

- 個人の理解によって生じたいかなる誤り、過失又は不正確な情報、
- 個人が各種ブロックチェーン資産を取引することによる損失及びそれによるいかなる行為。

6.2 リスクに関する注意事項

OA 開発および運用チームは、OA の開発、保守、および運用には無数のリスクが存在し、その多くはチームの管理を超えていると信じています。 このホワイトペーパーで

説明されていることに加えて、OA の購入者は、OA が暗号化されたデジタルパスであるというリスクをよく読み、理解し、慎重に検討する必要があります。 OA の交換は投資ではなく、私たちは OA が必ず付加価値を持つことを保証することはできません、ある場合には価値が下がる可能性があります、OA を正しく使用していないユーザーは OA を使用する権利を失う可能性があります、甚だしきに至っては彼らの OA 口座を失う可能性があります。 財団およびチームのスポンサーは、OA 交換のリスクを希望ユーザーに明確にしています。希望ユーザーは、参加した時点で、次のリスクを明確かつ完全に理解しているとみなされる必要があります:

情報開示のリスク:OA は、このホワイトペーパーの発行日まで継続的に改善されており、哲学的な考え方、コンセンサスメカニズム、推論アルゴリズムとコード、およびその他の技術的な詳細とパラメータが頻繁に変更され、更新される可能性があります。 このホワイトペーパーには OA に関する最新の主要情報が記載されていますが、完全なものではありません。 また、OA 開発および運用チームによって、特定の目的のために随時調整および更新されます。 OA 開発・運用チームは、開発における OA の技術的詳細を参加者に通知する能力や義務を有しておらず、情報開示の不十分さは避けられず、合理的である。

市場競争によるリスク:ブロックチェーンは非常に競争の激しい分野であり、数千のチームが異なるプロジェクトを計画し、開発に着手しており、競争は残酷になるでしょうが、この時代には、どんな良い概念、スタートアップ企業、さらには成熟した企業もこの競争のリスクに直面しています。 しかし、私たちにとって、これらの競争は成長の原動力となっています。

法的・ポリシー上のリスク:OA プロジェクトは様々な国の当局によって規制される可能

性があり、暗号通貨の発行には非常に革新的であるため、世界のほとんどの国で法律の空白があり、業界には非常に大きな法律および政策の不確実性が存在しています。

価格変動リスク:公開市場で取引される場合、暗号化されたパスは通常、価格の変動が激しい。 短期的には価格変動が頻繁に発生する。 この価格はビットコイン、エーテルコイン、ドル、またはその他の法貨で計算される場合があります。 このような価格変動は、市場の力（投機的な売買を含む）、規制政策の変化、技術革新、取引所の利用可能性、およびその他の客観的な要因によって引き起こされる可能性があり、このような変動は需給バランスの変化を反映している。 OA プロジェクトの開発・運営チームは、いかなる二次市場におけるパススルー取引についても責任を負わない。 OA 通貨の取引価格に係るリスクは、取引者自身が負担する必要があります。