

# Unichain

ホワイトペーパー（技術白書）

UniLab

2021 年 12 月 15 日（Version 2.0）

## 要旨

Unichain は、最先端技術の組み合わせであり、分散化とセキュリティを犠牲にせずに、1 秒あたり数千から最大数百万のトランザクションを処理できるスケーラビリティの高いブロックチェーンプラットフォームです。UniChain は general-purpose ブロックチェーンとして開発されており、誰もが自分のデジタル資産、アイデンティティ、プライバシーを完全に管理できるスマートソサエティー5.0 に分散型技術をもたらすことが目的です。また、誰も一人の管理者に操られることのない自由な金融システムを享受することができます。

UniChain は、Uniworld エコシステム[1]の1つの製品で、「人が創り出す全ての価値は人の幸せのためにあります」という理念を即して、UniDaoNetwork によって開発されました。Mainnet は 2020 年 6 月 4 日に公開されました。それ以来、数百のアカウント（ウォレットアドレス）が登録されており[2]、UNW（プラットフォームのネイティブトークン）は大規模なコミュニティや主要な取引所に広く受け入れられています。

## I. 序論

ブロックチェーン技術は現在ますます注目されています。ブロックチェーンとは、暗号通貨もさることながら、ポイントサービス（loyalty program）、ユーザーID 管理、物流、医療、保険、銀行などの多くの従来のアプリにも適用されます[3]。最初で最も有名なブロックチェーンであるビットコインは、人類初の p2p 電子マネーとして知られ、1 秒あたり約 3~7 トランザクション（TPS）を処理できます[4]。イーサリアムは、そ

れの上にスマートコントラクトと分散型アプリを構築できることで、ブロックチェーン 2.0 と呼ばれます。然しながら、イーサリアムは1秒あたり最大15 トランザクションしか処理できません[4]。最新の複数のブロックチェーンプラットフォームは、コンセンサスアルゴリズム (consensus algorithm) を調整すること (例: Proof of Stake, Proof of Authority…), またはシャーディングやマルチチェーンテクノロジーを利用することで、TPS を数百に伸ばすことを可能にしました。これらの上記のブロックチェーンは、実際のアプリケーションでは応用できないことは明らかです。なぜならば、ネットワークに参加する人が増えるほど、トランザクションが増え、トランザクションの確認を待つ時間が長くなります。拡張性 (スケーラビリティ) は、分散化とセキュリティに加えて、ブロックチェーンプラットフォームの最も重要な要素の1つです。また、実際に広く採用するには、ブロックチェーンプラットフォームの拡張性が高く、安価で、利用者にとって非常に使いやすくなる必要があると考えています。次のセクションでは、サイドチェーンアーキテクチャ、Dpos-HotStuff コンセンサスアルゴリズム、ブリッジプロトコル、ネイティブ機能とインセンティブモデルなどの従来のブロックチェーンの利点を組み合わせた新しいブロックチェーンプラットフォームを紹介します。これは Unichain と呼ばれます。

## II. Side chain architecture

Unichain にはマルチチェーンアーキテクチャを適用できます。その場合、主要かつ中心のチェーン(いわゆるルートチェーン)は Unichain であり、すべてのサイドチェーンのステート(取引ログ履歴)を検証し、それらを統合するために重要な役割を果たします。

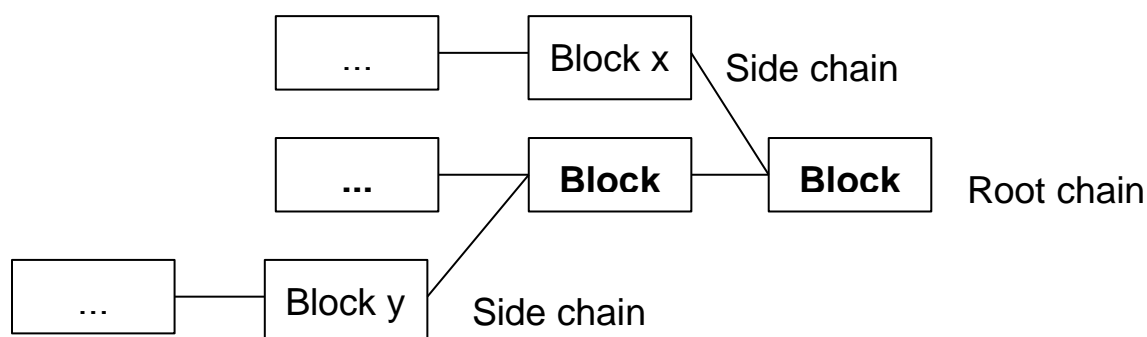


Figure 1. Side chain architecture

各サイドチェーンには、独自のブロックおよびトランザクションバリデーターがあります。全てのサイドチェーンは互いに独立しており、別個の元帳があります。例えば、チェーン X (図) で起こったことは一切チェーン Y に及ばず、その逆も同様です。この独立性により、プラットフォームを必要なだけ拡張（スケールアウト）できます。各サイドチェーンが 1 秒あたり約 1 万のトランザクションを処理できると覚えておいてください。したがって、100 個のサイドチェーンを備えたブロックチェーンプラットフォームは 1 秒あたり数百万のトランザクションに達します。

## チェーン間のコミュニケーション

サイドチェーンは、スマートコントラクトを介してルートチェーンや他のサイドチェーンとデータを交信します。Unichain で、チェーン間の繋がりには Uni ブリッジプロトコルと呼ばれるスマートコントラクトシステムによって可能となります。全てのサイドチェーンの資金はルートチェーンで保有されています。これにより、不正防止によって強制される状態遷移（state transition）を伴う各サイドチェーンでの預け入れと引き出しが可能になります。

各サイドチェーンは、ルートチェーンに独自のデータを全て開示しているわけではありません。代わりに、ブロックヘッダーのハッシュと少部の取引歴が送信されます。ルートチェーンに不正の証拠が送信された場合、そのブロックはロールバックされ、ブロック作成者はルートチェーンで管理されるスマートコントラクトシステムによって罰が科せられます。

Uni ブリッジプロトコルは、Unichain を他のブロックチェーンプラットフォームとの通信も可能にします。例えば、Unichain 上の情報やトークンはイーサリアム、ビットコイン、EOS などへ交転できます。

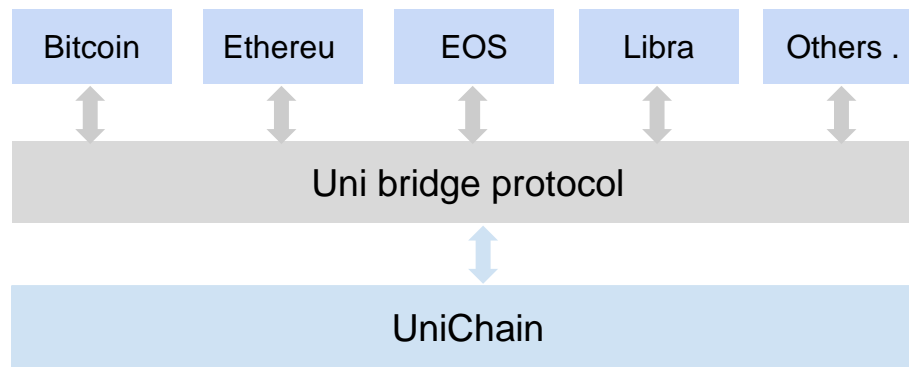


Figure 2. Uni bridge protocol

別のブロックチェーンプラットフォームのトークンに交換する場合、UniBridge プロトコルは分散型取引所として機能します。

### III. DPOS-Hotstuff コンセンサスアルゴリズム

コンセンサスは、あらゆるブロックチェーンプラットフォームに欠くことできないものです。ビットコインとイーサリアムにある一般的のコンセンサスアルゴリズムは、元帳の正確さを維持するために大量のエネルギーを消費するプルーフオブワーク（PoW）です。このようなコンセンサスアルゴリズムは、ブロックチェーンを完全に公的で分散化したものにしますが、大量トランザクションの処理に拡張することはできません。我がプラットフォームには Delegated Proof of Stake（DPOS）というコンセンサスを適用しました。DPOS は新しいコンセンサスアルゴリズムではなく、すでに Bitshare、EOS などに適用されています。しかし、私たちは DPOS を HotStuff [6] およびサイドチェーンアーキテクチャと組み合わせて、システムをスケーラブルにし、1 秒後にブロックのファイナリティに到達しようとしています。

#### *DPOS アルゴリズム*

DPOS は、ブロックチェーンで行われるトランザクションの representation を保証することによってブロックチェーンを保護するコンセンサスアルゴリズムです。DPOS は、民主主義を元にして開発されており、投票と選挙のプロセスを通じて、ブロックチェーンを集中化と悪意のある使用から保護します。Unichain で DPOS がどのように機能するかを説明する前に、いくつかの基本的な用語を下記に示します。

- Account (アカウント) : Account とは Unichain 上の一意の ID であり、各アカウントには一意のキーペアがあり。アドレスはブロックチェーン上のアカウントを指します。
- \* (キーペアとは秘密鍵と公開鍵を合わせた 2 つの鍵のこと)
- Uni トークン : Unichain およびその他のサイドチェーンのネイティブトークンです。
- ステークホルダー : トークンの残高が 0 以上あるアカウント。
- Node (ノード) : 通常のノードとは、誰でもダウンロードして実行できるソフトウェアのことです。ノードは元帳を保管し、トランザクションを検証および更新します。
- Witness ノード : Witness ノードは、1,000 以上の Unitoken を持つアカウントであると同時に、コミュニティから十分な票を受け取ったノードです。トランザクションとブロックは、Witness ノードによってのみ検証されます。

Unichain には、デフォルトで 33 個のアクティブな witness ノードがありますが、将来的にその数を増やす予定です。Witness ノードになるには、ステークホルダーは少なくとも 1,000 Unitoken (UNW) をアカウントに預け入れてから、トランザクションをブロードキャストして Witness 候補として登録する必要があります。他のステークホルダーは、それぞれが持っているトークン数に基づいた投票力で、Witness ノードに投票します。投票数が最も多い上位 33 人の候補者が Witness ノードになります。投票プロセスは、エポックと呼ばれる 7,200 ブロックごとに繰り返されます。各エポックでは、一つごとの witness ノードが約 218 ブロックを生成する能力があります。

### ***監視ノードが Unichain でブロックを生成する方法***

選挙プロセスの後、33 の投票された witness ノードがブロックを作成し始めます。従来の DPOS アルゴリズムはラウンドロビンでブロックを生成します。例：ブロック  $n$  は witness ノード  $n$  によって生成されます。

$$Witness \in \{1, 2, 3, n - 1, n\}$$

$$Block \in \{1, 2, 3, n - 1, n\}$$

このプロセスは予測可能であり、一部の不誠実な witness ノードによって破られる可能性がある。ブロックが予測可能なターンを生成することを防ぐために、私たちは、すべての witness ノードが同数のブロック（各エポックに 218 ブロック）を生成することを保証しながら、ブロックを生成する witness ノードをランダムにするメカニズムを提案します。

witness をランダムに選択するアルゴリズム

$$\begin{aligned} \text{Witnesses} &\in \{1, 2, 3, n-1, n\} \quad n = 33 \\ \text{magicNumber} &= \text{hexToIn}(\text{last10Digit}(\text{previousBlockHash})) \\ \text{index} &= \text{magicNumber} \bmod 33 \\ \text{Witness} &= \text{Witnesses}[\text{index}] \end{aligned}$$

前のブロックハッシュは処理計算時にのみ認識されるため、magicNumber は不明な番号であり、したがって次に選択された監視者は秘密のままです。前述の定式により、ブロックを作成するために 1 人の監視者を n 回選択することができるから、218 回の限定を超える可能性があります。この問題を解決するために、監視者が生成したブロックの最大数に達すると、ランダム選択プールから削除され、他の監視者にチャンスが与えられます。

## ***Hotstuff***

HotStuff は、Libra プロジェクトで利用された部分同期モデル (partially synchronous model) 用の Byzantine fault-tolerant（ビザンチン障害耐性、及び BFT）プロトコルのリーダーベースのレプリケーションです。これにより、通信の複雑さがレプリカの数で線形になります。HotStuff は、BFT 通信をメッシュからリーダーに依存するスターネットワークに変更しました。

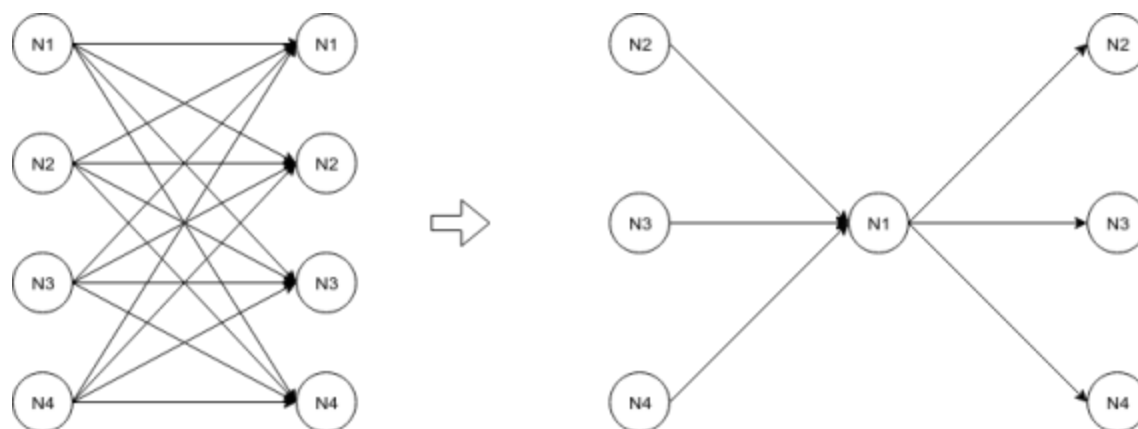


Figure 3. BFT' mesh vs. HotStuff' s Star network

従来のPBFT (Practical Byzantine Fault Tolerance) は、2 ラウンドのメッセージ交換を利用します。最初の段階では、 $(n - f)$  の票で構成されたクォーラム証明書 (QC) を生成することにより、提案の一意性を保証します。第2段階では、次のリーダーがレプリカ達に安全な提案に投票するよう説得できることが保証されます。新しいリーダーが情報を収集してレプリカ達に提案するためのアルゴリズムは view-change と呼ばれます。従来の BFT の2つの段階に基づいた view-change は、バグが発生しやすく[5]、複雑な通信です。BFT の各提案には、 $O(n^3)$  つのオーセンティケーターの通信フットプリントが発生します。単一のコンセンサス合意に至る前に  $O(n)$  回 view-change が発生した場合に送信されるオーセンティケーターの総数は  $O(n^4)$  です。

HotStuff は3フェーズのコアを中心に展開し、新しいリーダーは単純に知っている限り最も高い QC を選ぶことができるようになっています。これは、リーダーの承認を全く必要とせず、フェーズで投票した後にレプリカ達が「考えを変える」ことを可能にする第二フェーズを導入しています。これにより、上記の複雑さが軽減され、同時にリーダー交代プロトコルもかなり簡略化されます。

Protocol	Authenticator complexity		
	Correct leader	view-change	$f$ leader failures
DLS	$O(n^4)$	$O(n^4)$	$O(n^4)$
PBFT	$O(n^2)$	$O(n^3)$	$O(fn^4)$
SBFT	$O(n)$	$O(n^2)$	$O(fn^2)$
Tendermint/Casper	$O(n^2)$	$O(n^2)$	$O(fn^2)$
<b>HotStuff</b>	$O(n)$	$O(n)$	$O(fn)$

## HotStuff における各フェーズ

- pre-commit フェーズ：リーダーは現在のプロポーザルに対する prepare-vote を受け取ると、それが prepareQC に結合され、ネットワーク上のすべてのノードに pre-commit を通知する。
- commit フェイズ：リーダーは  $(n-f)$  個のノードから precommit 票を受け取り、precommitQC メッセージに結合し、ネットワーク上の全ノードに通知する。レプリカはこのメッセージを受信すると、状態遷移リクエストを固定し、コンセンサス決定に至ることができるようにする。
- 決定フェーズ：リーダーはネットワークから十分な commit 票を受け取ると、すべての commit を CommitQC に結合し、決定メッセージをネットワークに流します。ネットワーク上のレプリカ達は決定メッセージを受信し、状態遷移を実行し、状態をコミットして次の view を開始する。

## パイプライン化された HotStuff

HotStuff には、準備（正式なフェーズではない）、プレコミット、コミット、決定という、常に同じフェーズが存在する。流れの構造としては、他のノードがメッセージに投票し、リーダーが投票をまとめ、他のノードに通知します。これらのフェーズは統一的に表現することができ、パイプライン化することができます。



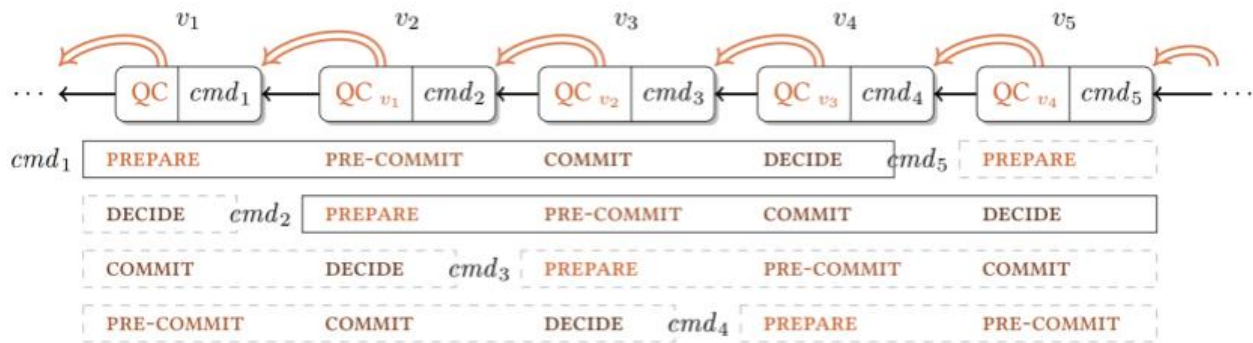


Figure 4. The pipeline HotStuff

## IV. UniChain のネイティブ機能

ネイティブ機能は、UniChain の特別な機能の 1 つです。これは、暗号化にあまり詳しくない利用者が、中間アプリケーションを使用したり、深い技術的な知識を持ったりしなくても、簡単にブロックチェーン技術を利用できるようにするものです。例えば、農民（普通の人）でさえも Unichain ツールのウェブアプリをいくつかクリックするだけで、トークンの作成やデジタル資産を分散型元帳に登録できます。

### ネイティブトークン(URC-30)

URC-30 は、イーサリアムネットワークの ERC-20 規格に類似しています。異なるのは、ERC-20 はスマートコントラクトシステムによって管理されており、すなわち技術的なユーザーによって開発・展開されなければならない点です。一方、URC-30 は、VM の上で実行されるネイティブコードです。誰でもウェブやモバイルアプリケーションのインターフェースにパラメータ入力することでトークンを作成することができます。また、URC-30 の特徴は、ユーザー同士が URC-30 トークンを交換する際に、UNW（ガス代）という取引手数料がかからず、トークン自体から手数料が算出されることです。

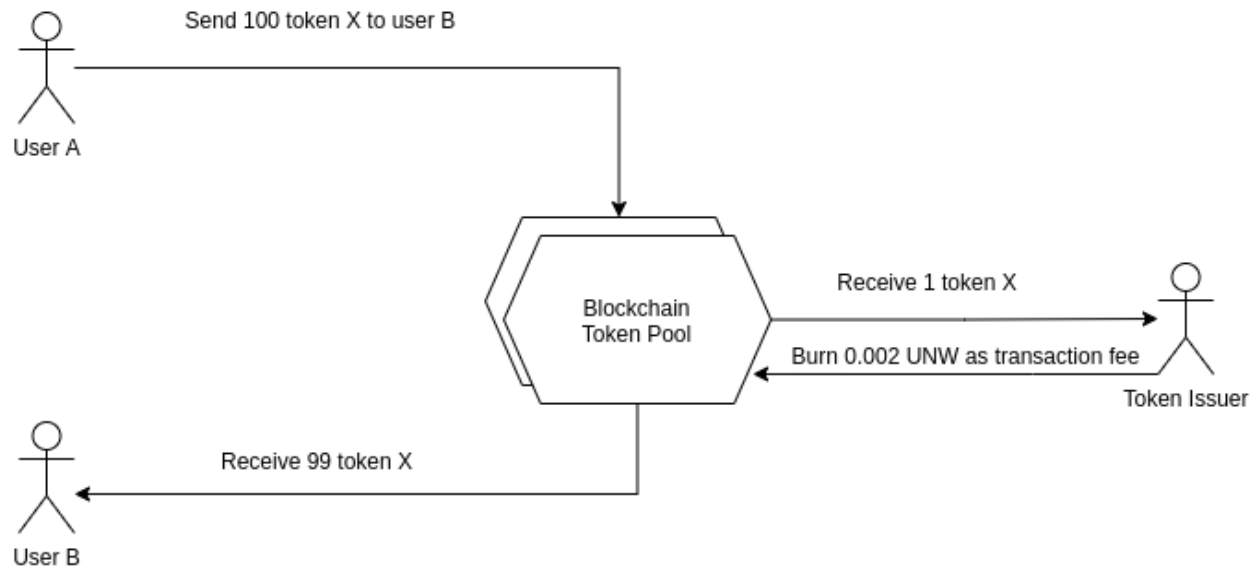


Figure 5. Urc-30 token fee mechanism

URC-30 規格 は以下の function を備えています。

- トークンを作成する
- トークンを送信する。
- トークンをミント（トークン所有者のみが循環を増加させるためにこれを行うことができます）。
- トークンをバーン（トークン所有者のみが循環を減少させるためにこれを行うことができます）
- トークンプールフィーを寄付する。
- トークンの所有権を譲る。
- フューチャートークンを送信する。
- フューチャートークンを請求する。
- トークンのパラメータを更新する。

**ネイティブ NFT (URC-721/URC-1155)**

UniChain は ERC-721/ERC-1155 の規格に準拠し、ネイティブ NFT(Non-fungible token) をサポートします。トークンは UVM (UniChain VM - Ethereum の EVM のようなもの) の上で実行され、スマートコントラクトシステムは一切も必要としていません。

この機能により、ユーザーは一般的なウェブ/アプリのインターフェースを使用して、デジタル資産を表す任意の NFT トークンを作成でき、UniWallet [7]の助けを借りて、デジタル資産を視覚的に表示できます（例えば、画像、ビデオ、3D アバター、その他 Uni NFT 標準に沿った資産の形などで）。

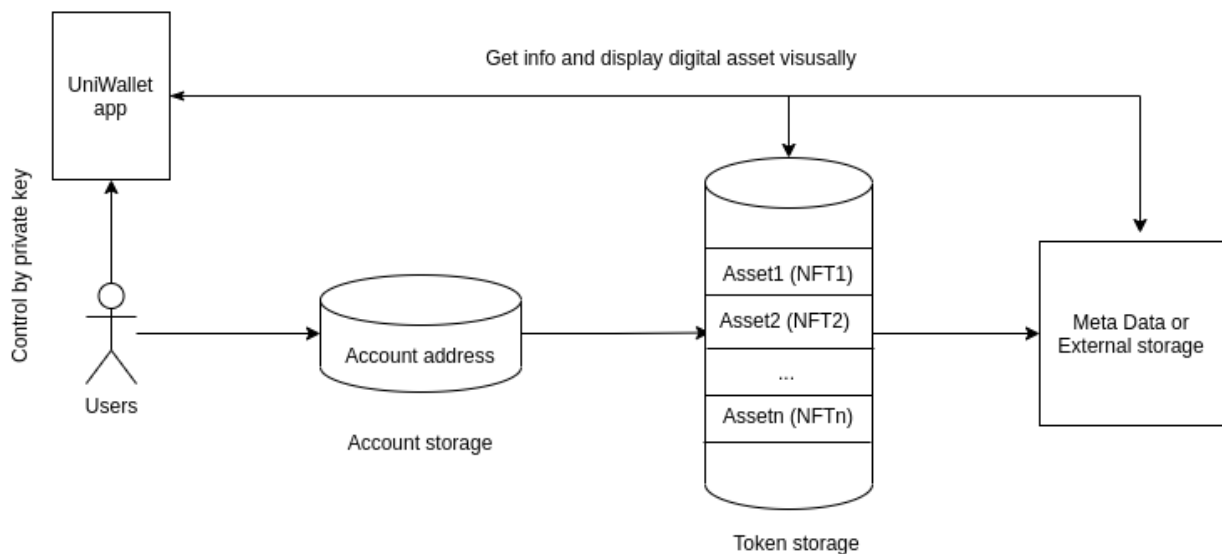


Figure 6. Native NFT token in Unichain

### その他のネイティブ機能

UniChain には、その他多くの機能が一定の規格に準拠し、ユーザーに利便性をもたらす限り、追加される予定です。これらのネイティブ機能は、ブロックチェーン技術を利用する際のミドルウェアや複雑さを解消するものです。

## V. Unichain エコシステムとインセンティブモデル

前述の通り、UniChain は UniWorld エコシステムの製品です。UniChain を利用する他の多くの UniWorld 製品は、UniChain ネットワーク上のサイドチェーンとなります。これらのチェーンは互いに繋がり、補完し、また共有することになります。

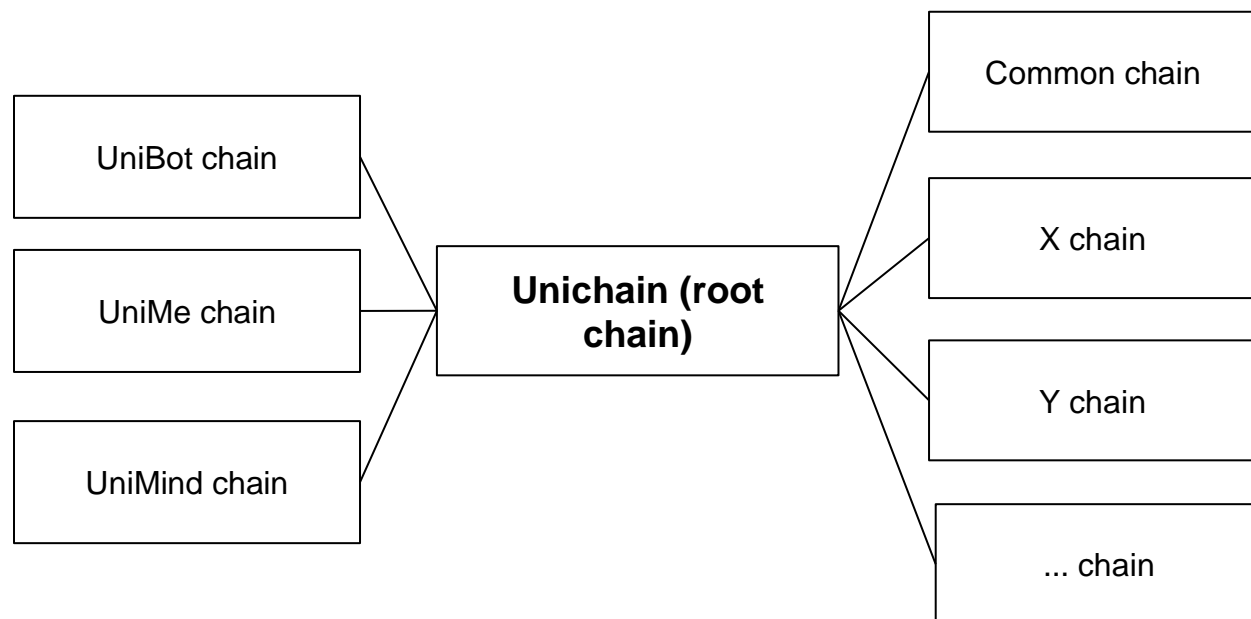


Figure 5. Unichain ecosystem

- UniBot (<https://unibot.org>) チェーンは、Chat bot アプリケーション専用のブロックチェーンです。チャットボットの検証、オンライン決済履歴の保存、不正取引からの保護などのためにスマートコントラクトを導入しています。

- UniMe (<https://unime.world>) は、安全なエンドツーエンドの暗号化を利用したチャット（および音声/ビデオ通話も可能）のモバイルアプリケーションです。また、マルチチェーンウォレットとブロックチェーンハブを統合しているため、ユーザーはたった一つのアプリで多くのタイプのブロックチェーンとやり取りすることができます。

- UniMind は、人工知能技術向けの製品です。これは、最も話題となる 2 つの技術トレンドを組み合わせた、初めてのブロックチェーンです。

- Common chain は、金融、ゲーミングなど、その他のアプリケーション用のチェーンです。
- X, Y, Z ... チェーンとは、その他の目的のために作られたチェーンでです。

UniWorld トークンは Unichain の主要なトークンですが、各サイドチェーンはそのチェーン内のスマートコントラクトにより独自のトークンを作成することができます。特に、UniWorld トークン (UNW) はすべてのチェーンに対して有効なトークンであり、チェーン同士をつなぐ媒体となります。UniWorld トークンは、ネットワークをスパマーから守るための取引手数料の支払いや、Unichain の取引プラットフォームで他のトークン (コイン) との交換にも利用されます (UniWorld トークンを交換手数料として利用する場合、手数料は 80%削減されます)。

## **新しいサイドチェーンを作成する手順**

ウォレットに指定されたトークン残高さえ用意すれば、誰でも新しいサイドチェーンを作成することができます。現在、最低 250,000UNW が必要です。以下は、K さんがサイドチェーンを作成する手順です。

- K さんは新しいウォレットを作成し、250,000 以上の Unitoken を自分のウォレットに入金する。
- K さんは新しいサイドチェーンの作成をリクエストする特別なトランザクション (ルートチェーン上のスマートコントラクトを呼び出すトランザクション) を作ります。このトランザクションは 250,000UNW を要し、バーンアドレスに直接バーンされます。
- K さんのトランザクションはルートチェーンのバリデータ (監視者) によって検証され、K さんは条件を満たしたと確認された上、取引は有効となり、元帳に無事に追加され、K さんは chainID を受け取ります。

- Kさんは受け取った chainID でサイドチェーンを作成します。この時、サイドチェーンのメンバーは一人（つまり K さん）だけであり、K さんはこのチェーンの作成者です。
- K さんは、新しいサイドチェーンに参加し、スマートコントラクトを運用、展開し、そのチェーンを K さんの目的のために使用するという人を誘っていきます。

## ***Witness ノードになる手順***

すべてのステークホルダーは、witness 候補になることができます。witness ノードになるには、ステークホルダーは自分のウォレットに最低でも 1000UNW を持っていないければなりません。次のステップは、ステークホルダー K さんが witness になる手順を説明します。

- K さんは 1000UNW を K のウォレットに入金する。
- K さんは witness ノードになるためのプロポーザルトランザクションを作成する。witness 作成の為のトランザクション手数料は 1000UNW となり、バーンウォレットアドレスに直接バーンされる。
- K さんのトランザクションが有効であれば、K さんは witness 候補として挙げられ、投票プロセスを待つことになる。
- 他のステークホルダーはプール内の witness ノードの一覧を見て、信頼できると感じたノードに投票を行うようになる。投票力はステークホルダーのトークンの総数次第です。
- 最も高い投票数を得た 33 の witness 候補が公式の witness となり、他の候補はまだプールに残っていて次の投票プロセスを待つか、代替 witness となる（選択された witness ノードが故障したり指定時間内にブロックを生成したりできない場合など）。

## ***インセンティブモデル***

UniChain では、ユーザーによる投票と、Witness ノードによる取引やブロックの検証・生成を奨励するために、それぞれに報酬の仕組みを設けています。報酬は 6 時間（選挙時間）ごとに積算されます。報酬を受け取るアカウントは以下の通りです。

- アクティブな Witness ノード(33 ノード)。
- 候補者ノード(55 人)。
- Witness ノードや候補者ノードに投票した人。

なお、アクティブな Witness ノードは、候補者のノードでもあります。

## 報酬の計算

報酬は 6 時間ごとに集積されるため、その間の報酬の計算のし方を説明します。

- アクティブな Witness ノードの場合：各ブロックの報酬は 1UNW です。ブロック時間を 3 秒とすると、アクティブな Witness ノードの報酬合計は  $1 \times 6 \times 60 \times 60 / 3 = 7,200$  UNW です。しかし、アクティブな Witness ノードは特定の比率で報酬を投票者と共有するので、個々のアクティブな Witness が受け取ることができる実際の報酬は  $0.2 \times 7200 / 33 = 43.6$  UNW です（比率は 20% : 80%と仮定します）。

- 候補ノードの場合：55 個の候補ノードが 6 時間ごとに 7363UNW の受け取りを共有します。個々の候補ノードが受け取ることができる実際の報酬は、候補ノードが受け取った票数とその投票者との分配率に依存します。その額は以下の式で計算されます。

$$candidateReward = ratio_{candidate} * 7363 * \frac{vote_{candidate}}{vote_{totalNetwork}}$$

分配率は 0.2（20%）、投票数/total\_network\_votes は 1/55（平等投票）と仮定すると、報酬は  $0.2 \times 7363 \times 1/55 = 26.7$  UNW となります。

-投票者の場合：

アクティブな Witness ノードに投票があった場合、報酬は以下のように計算されます。

$$reward = (1 - ratio) * 7200 * \frac{vote}{totalActiveVote * 33}$$

候補ノードに投票があった場合、報酬は以下のように計算されます。

$$reward = (1 - ratio) * 7363 * \frac{vote}{totalNetworkVote}$$

なお、アクティブな witness ノードは候補ノードでもあるため、ユーザーがアクティブな witness ノードに投票した場合、両方の報酬を得ることができます。実際の報酬は、証人ノードとネットワーク全体における証人比率と投票数により、時間経過とともに変化します。

### トークンをバーンする仕組み

他のブロックチェーンプラットフォームとは異なり、Unichain におけるトランザクションの手数料はブロックを発生した方（つまり、Witness ノード）に直接送られるわけではありません。代わりに、それは特別なアドレス（U000000000000000000）に送られます。このアドレスの秘密キーは誰も知らないため、トークンがバーンされていることと言う意味です。トークンをバーンすることで、UniWorld トークンの価値は将来的に高まります。下表は、トランザクションのタイプによって、どれだけのトークンがバーンされるかを示します。

トランザクションのタイプ	バーンされる手数料 (Uni トークン単位)
トークンをアカウントに送金する	0.000267
Witness ノードに登録する	1000
新しいサイドチェーンを作成する (ネイティブ機能)	5000
トークンを作成する	500
スマートコントラクトの function を呼び出す	スマートコントラクトの複雑さに応じて計算される



## VI. UniChain の仕様

- ブロックタイム：1～3 秒
- 1 秒あたりのトランザクション数（TPS）：1 チェーンあたり 5,000 件
- ブロック確認（ファイナリティ）：1 秒～3 秒
- ネイティブトークン：UniWorld Token（UNW）。
- トークン総数：1,000,000,000（10 億トークン）。
- トランザクション手数料：計算複雑さに基づき、一般的なトークン送金には 0.000267 UNW の手数料がかかる。
- コンセンサス・アルゴリズム：DPOS-HotStuff
- Witness ノード数：55 ノード、33 アクティブ、22 オルタネート。
- スマートコントラクト言語：現在 solidity をサポート。（将来的には Nodejs と Java をサポートする予定）。
- デジタルシグネチャーのアルゴリズム：ECDSA。
- マルチチェーン：対応可能
- クロスチェーンコミュニケーション：対応可能

以下は、いくつかの一般的なブロックチェーンと UniChain を比較したものです。

Technical Spec	Bitcoin	Ethereum	IOTA	EOS	UniChain
Consensus algorithm	PoW	PoW	Tangle	DPOS-BFT	DPOS and Hotstuff
Transactions per second (TPS)	3	15	300	Thousands	Millions
Block time (second)	600	15	NA	~1	~1-3

Confirmation time (in seconds)	1800	150	NA	~1	~1-3
Smart contract	x	✓	x	✓	✓
Multi chain	x	x	x	x	✓
Cross chain communication	x	x	x	x	✓

## VII. 結論

このホワイトペーパーでは、多くの最先端技術の組み合わせとして、Unichain を紹介してきました。私たちは、Unichain が実際のアプリケーションの要件（スケーラビリティ、分散化、セキュリティ、およびユーザーフレンドリ）を満たす最も強力なブロックチェーンプラットフォームの1つであると考えています。私たちの目標は、Unichain を暗号通貨のためだけでなく、世界中のあらゆる分散型アプリケーションに利用されるようにすることです。

## VIII. 参考資料

- (1) Uniword ecosystem (<https://uniworld.io>) including UniBot (<https://unibot.org>), UniMind, UniLab, UniChain (<https://UniChain.world>), UniCom (<https://mia.world>) ...
- (2) <https://uniscan.world> UniChain scan (or explorer <https://explorer.unichain.world>) to explore blockchain details such as the account, block, transaction ...,
- (3) Shiroq Al-Megren, Shada Alsalamah, Lina Altoaimy, Hessah Alsalamah, Leili Soltanisehat, Emad Almutairi. Blockchain Use Cases in Digital Sectors: A Review of the Literature

- (4) Dejan Vujičić, Dijana Jagodić, Siniša Randić. Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview
- (5) Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan Gueta, Ittai Abraham. HotStuff: BFT Consensus with Linearity and Responsiveness
- (6) Ittai Abraham, Guy Gueta, Dahlia Malkhi, Lorenzo Alvisi, Ramakrishna Kotla, and Jean-Philippe Martin. 2017. Revisiting Fast Practical Byzantine Fault Tolerance. CoRR abs/1712.01367 (2017). arXiv:1712.01367
- (7) UniWallet (<https://uniwallet.world>)