everiToken

テクニカル ホワイトペーパー

バージョン 2.5

Zug, Switerzland

2018 年 9 月 25 日現在

免責条項

- この everiToken テクニカルホワイトペーパーあくまで情報目的です。
- このホワイトペーパーはあらゆる保証、証明、期待を表すものではありません。
- ホワイトペーパーに記載されている技術仕様または実装方法は今後変わる可能性があります。
- 我々テクニカルチームは随時解散または再編成する可能性があります。またコア技術者の人材喪失によりプロジェクトの失敗に至るかもしれません。
- ホワイトペーパーは「ありのまま」で提供されるテクニカルリビューです。プロジェクトチームとプロジェクトメンバーはホワイトペーパーの内容を実現できなくても責任を負いません。
- ホワイトペーパーに書かれている「トークン」は実用的な価値は一切なく、デジタル暗号化によって「トークン」を取得した証明にすぎません。唯一の目的は「トークン」の許可を確認することです。
- ホワイトペーパーに記載されている技術によって実行されるブロックチェーン、または派生イベントはプログラムによって自動的に生成され、我々はその結果に責任を負いません。 そのブロックチェーンを使用、または使用していない個人か組織の責任です
- 誰でもこのテクニカルホワイトペーパーのすべての内容を非商用で利用することができます。ただしテクニカルホワイトペーパー内容を変えないでください。また我々は使用したことによるいかなる結果についても責任を負いません。

everiToken

目次

パート I. 背景とビジョン

トークン経済の到来

2018 年 4 月現在、ブロックチェーン技術が発明されてから約 10 年間経っています。しかし 1 つの重要な疑問が依然として残っています。ブロックチェーン技術は、世界経済に価値を生むような生産革命を起こしていますか。
データを見てみると現在、ブロックチェーンで管理されている資産（以下、「チェーン上」と称する）は、基本的に様々なトークンであり、総市場価値は約 3,000 億ドルです。 これらのチェーン上資産は、高いボラティリティと強い投機の特徴があり、世界経済には新たな価値を生んでいません。中本哲史以来、人々はこれらの「トークン」を支払い通貨として使おうとしていますが現実、通貨ではなくデジタル資産の役割しか果たしていません。「デジタル通貨」は現実よりもただの名前にすぎないです。
通貨の発行は政治を具現化する重要な権利であり、財政は国家に属していなければなりません。したがってトークンが通貨を代替することは非常に困難です。国家の許可と支援がなければ、「デジタル通貨」はただの理想主義のに過ぎません。
一方、大半の主流グローバル資産（有形無形両方）はブロックチェーンを使わず（以下、「オフチェーン」と称する）、チェーン上の資産間との関わりは限られています。

しかし、トークンは本当に単なるトークンですか?
そうではないはずです。
トークンの本来の意味は「シンボル、シグナリング」であり、デジタル通貨ではなく証明書とみなされるべきです。身分証明書、卒業証書、アクセスキー、イベントチケット、カードクーポン、など様々な権利と利益の証明をすることができます。

歴史を振り返ってみましょう。
すべての文明は権利と利益の証拠に基づいています。口座、所有権、資格、証明書などはすべて権利と利益の証です。 Yuval Noah Harari が「サピエンス全史」で述べたように、「賢明な人類が立ち上がり、文明を構築するのは「架空の事実」のおかげである」と述べています。もしこれらの証明がすべてデジタル化し、信憑性と完全性が暗号により保護されたら人類文明に革命的な影響を与えるでしょう。我々はこれを「トークン経済」と呼びます。

ブロックチェーン上に証明書を実行することにより、従来の中央集権化モデルでは提供できない堅固な信頼基盤が出来上がります。証明書がトークン経済のフロントエンド経済ユニットならば、ブロックチェーンはフロントエンドと一体化したトークン経済のバックエンド技術です。

競合分析

トークン経済のために生まれたパブリックチェーンの everiToken には主に 2 つの競合、イーサリアムと EOS があります。SWOT 分析をします。

1. **デジタル権利と利益の証明:** 証明書は信用できるデジタル形式で本質的な価値（有形無形のいずれであっても）を表すものでなければならない。

2. **セキュリティ、暗号化、認可管理:** 証明書はプライバシー保護され、検証可能で、改ざん不可能、監視と暗号により保証され、認可された人のみが使用可能でなければなりません。

3. **交渉可能性:** 証明書は簡単に取引と交換することができなければならない。

上記の要求に応じてトークン経済の基本的なニーズを満たし、トークン管理と流通を促進し、トークン経済の技術基盤を構築するための一連の汎用ソリューションを提供します。
主に以下 3 つの特徴を実現しました。

- **高速で便利なトークン発行:** ユーザーは一切コードに触れる必要がなく、我々が提供する API（アプリケーション、ウェブページ、サードパーティアプリケーション用）を使用して独自のトークンを簡単に発行できます。

- **効率的なトークン転送:** 数百万トークンを数秒内同時に転送する事が可能です。

- **柔軟な認可管理:** 多人数保有、秘密鍵回復、多レベル権限、合法性、政府監視およびその他の複雑な要件をサポートし、認可管理など複雑なニーズを一つのプログラムにまとめました。

イーサリアムと EOS を見てみましょう:

イーサリアム: ERC20/ERC721

イーサリアムでトークン経済を実現するには、ERC20 と ERC721 のプロトコルに基づいてスマートコントラクトを開発するのが主な方法です。 ERC20 は FT（代替可能）、ERC721 は NFT（代替不可能トークン）をサポートしています。しかしこれらには大きな問題があります。

- **TPS**：現時点、Ethereum は毎秒最高 20 処理しかこなせません。これではトークン流通の実用的なニーズを満たすことができません。

- **費用**：Ethereum におけるスマートコントラクトの実行は、1 ステップごとにガスが消費されます。複雑なビジネスロジックを持つ関数（複数の人の保有、監視、合法性など）では、コストが高くなったりコントロールできなくなる可能性が生じます。

- **普及**：イーサリアム上でのトークン経済の実現はスマートコントラクトに基づいており、第三者アプリケーションを使用しないと非技術者がアクセスできません。

- **非標準化**：異なるスマートコントラクトは全く異なる開発アイデアに基づき、これらの仮想トークンのメタデータをつなぐのが困難です。これではトークン経済のエコシステム発展に貢献できず、ユーザーは統一プラットフォームで所有しているさまざまなトークン資産管理することができません。

EOS

EOS は 6 月 2018 日にメインネットを開始しました。 EOS はイーサリアムの問題に対処するのが目的なので、トークン経済の開発におけるイーサリアムの問題のいくつかを EOS で解決することは可能です。しかしこれでもまだいくつかの問題が残っています。

- **安全性**：

トークン取引は、非常に貴重で再生不可能な実物に使われている可能性があるため、セキュリティ上の問題は致命傷になります。スマートコントラクト開発は開発者のレベルに左右され、すべてのトークン開発者が十分なセキュリティ意識を持っていることは保証できません。

EOS のスマートコントラクトは、比較的新しくテスト段階にあるウェブアセンブリに基づいています。さらに、EOS のスマートコントラクトコードはチューリング完全であり、過度な権限を持っているため意図的ではないセキュリティ弱点が出現しやすいです。

大半の人はスマートコントラクト開発ができませんのでトークンを発行して転送をするには、第三者のアプリケーションを信頼する必要があります。資産の管理はユーザーの手元ではなく、第三者の保証に頼ります。

- **非標準化：**イーサリアムのように、異なるスマートコントラクトのメタデータをつなげることができません。

- **規制、信用、法律：**非標準化なコードを理解するには専門知識が必要なため、政府が規制しにくくなります。同様に、非開発者は、プログラムを信用できるかどうか判断するのが難しく、ブロックチェーンが普通の人や政府受け入れられにくい可能性があります。
- **実行効率：**多様なニーズを満たすために、EOS のスマートコントラクト機能は複雑です。システムモジュールが多数にあり、資源のスケジューリングと配布は困難です。システムの複雑さが増すのと同時に処理速度も低下します。また様々なデータや関数間に問題が発生する可能性があるため、単にマルチスレッドを利用して速度を上げるのは困難であり、スケジューリングコストも高くなります。しかしこれらの複雑な機能はトークン経済には非常に重要です。

- **大衆化：**世界経済のビジネスニーズは複雑で変化しやすく、一貫性が欠けています。しかし、スマートコントラクトは開発とテストに時間がかかり、短期間で市場の多様化に対応しにくいです。これではトークン経済の発展に支障が出ます。

everiToken と競合の主な違いは、他のブロックチェーンはスマートコントラクトを使用しているのに対してセーフコントラクトを使っているところです。つまり、everiToken はチューリング完全ではなく、everiToken が満たすことができない複雑なアプリケーションシナリオが存在します。 しかし、everiToken はトークンエコノミーでの要求の 95%を満たすことができ、最も安全で、親しみやすいパブリックチェーンであります。また、一般利用者にはほぼ無料で提供します。

OT（機会と脅威）

everiToken のこれらの強みに加えて everiPass / everiPay QR コードを生成時に使われる EvtLink 標準を作ります。 everiPass / everiPay は everiToken パブリックブロックチェーンを利用して**対面型マイクロペイメント**のために生まれた決済プロトコルです。
everiPay / everiPay には **QR コード**生成の標準と通信プロトコルの定義が含まれ、そのほかにもこれらの 5 つの特性を持ってます：

即時クリアランス、取引は瞬時に決済となります。
地方分権化、P2P 決済、非中央集中型プラットフォーム、チェーン上のデータを改ざんすることができなく、誰もが価格設定に参加することができます。
最高の安全性、ブロックチェーン内のデータとコンテンツは、ユーザーの財産セキュリティの保護を最大限にするために、偽造または改ざんすることはできません。
互換性、everiPass / everiPay は、everiToken でサポートされているすべてのトークンに利用できます。通貨だけでなく、トークンやポイント、ドアを開く鍵まで、スマートフォンだけでどこでも利用できます。
便利性、インターネットに接続できなくても決済できます。

上記の 5 つの特性に基づいて、everiPass / everiPay は、最も安全で、最も便利なサービスを対面型で提供します。

しかし、いくつかの脅威は依然として存在します。イーサリアムと EOS もトークンエコノミーのパブリックチェーンになることができます。 もしイーサリアムがシャーディングのような方法で TPS を大きく高めることができれば強力なライバルになります。また、スマートコントラクトは現在多くの問題を抱えていますが、時間の経過とともに欠陥の多くが解決されるとイーサリアムと EOS の競争が高まる可能性があります。実際、イーサリアムは現在より多くの注目とユーザーを持っています。なので everiToken はイーサリアムのエコシステムと実用アプリケーションの発展に非常に注目しています。

まとめ

上記の分析に基づいて、我々はブロックチェーンアプリケーションに最適な新しいコンセプトを設計し、トークンエコノミーの開発のための新しい公開チェーンとエコシステム **everiToken** を提案します。 実世界の資産、証明書、バウ

チャーは、トークンの発行によって**デジタル化**され、かつてないセキュリティ、スピード、ネットワーク互換性が出来上がり、誰もが簡単に利用できるようになるます。

パート II. everiToken の技術

セーフコントラクト

スマートコントラクトは理論上、仲買人なしに商品やサービスの分散型取引を促進する手段です。 しかし現時点スマートコントラクトは、不適切な実装や論理的なエラーから生じるセキュリティ弱点が非常に多くロックアウト、アクセス漏洩、間違ったプログラム終了処理などが発生してます。そのため残念ながらスマートコントラクトは従来の契約や取引手段よりも信頼性が低いと見なされます。
everiToken は API レイヤーを使用してセーフコントラクトという新しいコンセプトを紹介します。直接コードで実装する代わりに、トークンの発行や転送などの処理にセーフコントラクトを使用します。 セーフコントラクトは機能をコアニーズのみに削減することで、利用可能な API 関数を徹底的にテストすることができ、すべてのチェーン上転送の安全保証ができます。セーフコントラクトはチューリング完全ではないですが、API 通じて必要な機能の大半を達成しトークン発行者必要に応じてオフチェーンのサービスを提供できます。
さらに、セーフコントラクトには高いアクセスビリティと TPS の利点があります。API を組み込むことで、ブロックチェーン導入用のコードを 1 から実装する必要がなく、既存システムのワークフローに簡単に統合することができます。また API を使用することによりさまざまなトランスレーションタイプを簡単に識別ができ、各独立したトークン転送をより高速（5000 TPS 以上）な並列処理をすることができます。

データーベース

EOS はロールバック操作をサポートする Boost.MultiIndex ベースメモリデータベース（Chainbase）を使用していますので、すべてのコントラクト処理結果はメモリデータベースに保存されます。コントラクトコード異常時に分岐や復旧時のロールバックをサポートするためには、各操作のロールバック用の余分なデータを記録する必要があります。すべてのデータはメモリに保存されて処理されるため、時間の経過とともにユーザーと転送数が増加すると、メモリに対しての要求が大幅に上がります。これではブロック生産者のメモリ容量に対する要求が非常に高くなってしまいます。さらにプログラムがクラッシュまたは再起動すると、全てのメモリデータが失われます。データを復元するには、ブロック内のすべての操作を繰り返す必要がありコールド起動時間が長く実用

的ではありません。
我々は EOS のメモリデータベースを利用しながら、RocksDB をベースにしたトークンデータベースを開発しました。以下の強みがあります：

- RocksDB は非常に成熟した産業レベルの Key-Value データベースで、完全に検証されており Facebook のコアクラスターにも使用されています

- RockDB は LevelDB に基づいており、LevelDB よりも優れたパフォーマンスと豊富な機能を提供します。また Flash や SSD などの低レイテンシストレージにもコア最適化されています。

- 必要に応じて RocksDB をメモリデータベースとして使用もできます。

- RocksDB ベースのアーキテクチャはバージョンのロールバックと永続性を支持しており、パフォーマンスへの影響は極めて低いです。

私たちのトークンデータベースは基盤となるストレージエンジンに RocksDB を使用しています。パフォーマンスを最大限に引き出すためにトークン関連の操作を完全に最適化し、低コストでロールバックを達成できます。さらにトークンデータベースはデータの永続性、量的バックアップ、増分バックアップなどのオプション機能があり、コールド起動などの問題を解決できます。
everiToken の操作は非常に抽象的であるためタイプは既知で制限され各操作に必要な情報は最小限です。したがって EOS などのシステムに比べて余分な部分が少なくブロックサイズも小さくなります。

トークンベース

概要

トークン経済のために生まれた everiToken は独特のトークンベースマネジメントメソッドを使用してます。
トークンは中央銀行が発行したデジタル通貨や暗号通貨(ビットコインや ETH など）とは異なります。
トークンは「特定のエンティティが提供する特定の資産、期間、場所、またはタイムサービスに経済的独占シェアを持つ証拠」と定義します。トークンは代替可能トークンと代替不可能トークンの 2 種類に分けられます。アプリケーションのシナリオや構造にはいくつかの違いがあり我々の分析によると、代替不

可能トークンはトークン経済でより広範な役割を果たすと思います。したがって代替不可能トークンから始めます。

代替不可能トークン (NFT)

代替不可能なトークンを理解するために一つ例をみてみましょう。現実の世界ではビーチのすべての石は異なる重量、外観、石質を持っています。 2 つ同じ葉っぱが存在しないように、2 つの同一の石はありません。その上、2 つの石を簡単に組み合わせることはできないので、すべての石は「分割できなく」、「合体できない」とします。

ブロックチェーンの一例は、かつてはブロックチェーンの世界で大ヒットしたゲーム CryptoKitties です。 各猫には固有の数字と属性があります。

NFT トークンは現実世界での唯一無二な石、またはブロックチェーン上の猫に似ています。現実世界では自然に違いが生じ、我々のシステムにも同じような特性があります。

一般に NFT トークンは異なるタイプに応じて異なるカテゴリーに分けられます。 同じ種類の NFT トークンを分類してドメインを形成することができます。トークンに集中することにより、everiToken は高い標準化の実現ができます。

ユーザーが発行したカスタムトークンはすべて同じ構造です。各トークンは特定のドメイン（トークンの種類）に対応する 1 つのドメイン名を含み、発行者はドメイン内でユニークなトークン名を決めます。トークン名は通常、何か特別な意味を表します。例えば製品のバーコードは、原産国および製品の製造元に関する情報を含む命名規則として使用されています。各トークンはドメイン名とトークン名によって決まりますので唯一無二になり、所有権に関する情報も含まれるため各トークンに少なくとも 1 人の*オーナー*います。

前述したように、トークンの **ID** は、**ドメイン名**と**トークン名**によってユニークに定められます。図 1 はトークンの基本構造です。トークン ID の他に、トークンオーナーとその他必要情報も保存されます。

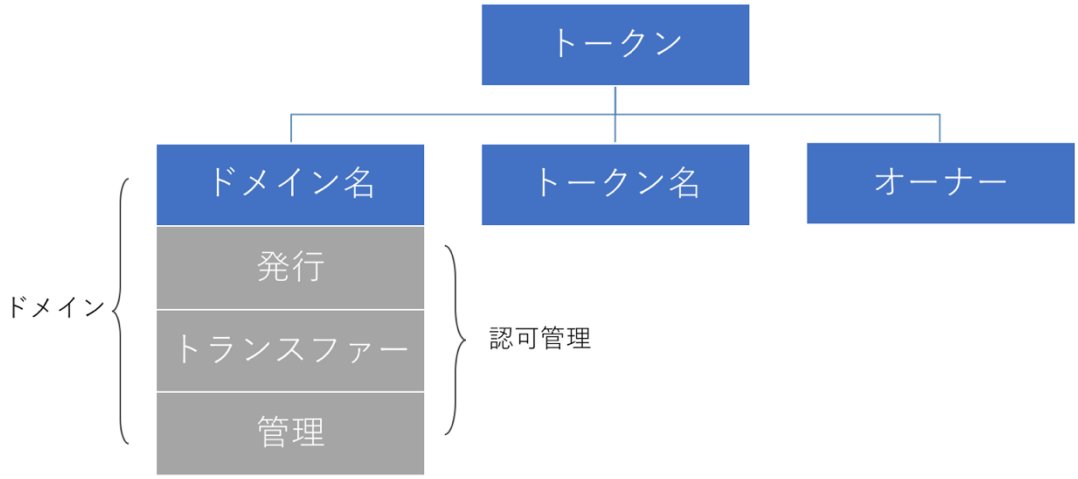


図 1. everiToken のトークン構造

各ドメインの詳細はドメイン名によって確認することができます。 ドメインには認可管理情報も記載されています。
誰もが自分のトークンを発行する権利があるのでトークン自体に価値はなく、その発行者の現実世界の信用によって保証されます。新しいトークンが発行されると、トランザクションで他人に転送することができます。NFT の場合トークンが変わるのはトークン所有権を変更することになります。すべてのトークンには**オーナーグループ**があります（1 人以上のオーナーが存在する場合もありえます）。 オーナーグループの変更が必要な場合、トークンの流通メンバーがデジタル署名することで操作確認ができ、everiToken ノードがトランザクション認可条件を満たしていることを確認してトークンのオーナーグループが変更され、 他のノードと同期されます。

承認管理

everiToken システムには、認可管理に 3 種類の権限（発行、転送、管理）があります。
（1）「**発行**」はドメイン内でトークンを発行する権利です。
（2）「**転送**」はドメイン内のトークンを転送する権利です。
（3）「**管理**」は認可管理、その他のパラメータ、ドメインを変更する権利です。
図 2 のように各権限はツリー構造により成り立っているため、**権限ツリー**と呼びます。各権限は根ノードに必要最低限値があり、1 つ以上のアクターに接続されています。

アクター

アクターはアカウント、グループ、オーナーグループの 3 種類に分けられます。アカウントは個々のユーザー、グループ複数のアカウント、オーナーグループは特別グループです。

グループは特定のクラブ、会社、政府機関、財団、または個人を表します。グループにはグループの公開鍵、各メンバーの公開鍵、各重量が含まれています。操作を承認したグループ内のメンバーの承認合計重量がグループ必要最低限値を満たした時のみ操作は承認されます。

同時にグループの公開鍵を保持するメンバーはグループメンバーと重量の変更を認可することができます。このメカニズムを「**グループの自律性**」と呼びます。

グループが作られますと、システムは自動でグループ ID を生成します。発行者がドメイン内の認可管理を決める際、グループ ID を権限システムに直接参照すればできます。グループの自律性により各グループは再利用でき、非常に便利です。

トークンオーナーにはオーナー名に固定されたトークンオーナーの集まりの特別グループがあります。このグループの特徴は各トークンが異なる点とグループ承認条件は全員同意です（グループ内各一人の重量は 1 であり、必要最低限値はメンバー数）。

管理

認可は初期設定でトークン発行者になり、各認可は少なくとも 1 つのグループに管理されます。トークン発行後、発行者は各グループの情報、重量、権限、必要最低限値を設定します。誰かが特定のドメインで操作を実行する前にまず操作グループに十分な重量があるかどうかを確認し、必要最低限値を超えた場合にのみ認可されます。このグループ化設計は現実世界の様々なケースに適しており、柔軟な重量と必要最低限値の設定はあらゆる複雑なニーズを満たします。図 2 は一つの例です。

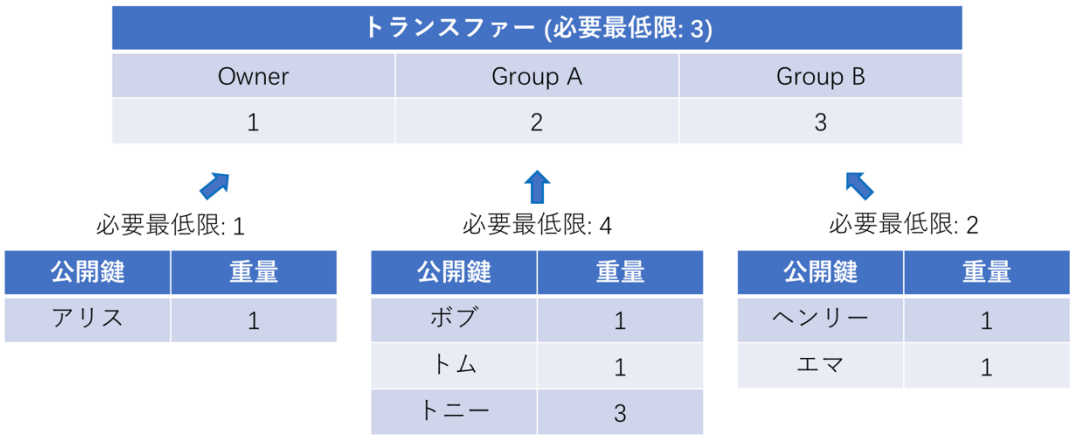


図 2. 認可の転送

図 2 はドメイン内の認可転送を示しています。必要最低限値は 3 でありオーナー、グループ A、グループ B の 3 つのグループが存在します。オーナー、グループ A、グループ B は各グループ転送必要最低限値を満たしているため単独で認可をすることができます

オーナーグループは Alice のみによって認可され、グループ A は少なくともボブ＋トニーまたはトム＋トニーの認可で必要最低限値（4）を満たすことができ、グループ B は必要最低限値（2）を満たすためにはヘンリーとエマの両方の認可が必要です。

どのユーザーもトークン発行する権利がありますが各ドメインのトークンターゲットシナリオは異なります。たとえば財産移転は、厳格な監視を受けている政府関係機関によって審査されなければならなく、チェーンのメンバーシップカードとクーポンには同社ブランドの認可が必要です。コンサートチケットはコンサートを過ぎたら無価値になりますが、駐車スペースのオーナーは時間とともに変化する可能性があります。

トークンを発行する時トークン発行者はドメイン内のアクセス許可を設計することによって、認可管理を実装できます。以下のシナリオは認可管理の利便性を示しています。

図 3 は、everiToken の認可管理メカニズムを使用して複雑な問題を解決する方法の例です。

（アメリカ例）

某会社は新築オフィスビルを建設し、建物の財産権を 1000 トークンとして発行したいと考えています。同社は、これらのトークンを発行し維持する SPV（特別目的事業体）を設立しています。現実では不動産トークンの発行と転送

は、地方財産局(Local Property Bureau)の審査と承認を受ける必要があります。各地方の基準に基づいて発行され、トークンの詳細（合計数、発行者、権限管理構造など）は公式のプラットフォーム上に表示されます。中央財産部(Central Property Department)は地方財産局とオーナーを制限し管理する権限が最も高い。

図 3.認可管理の構造

ドメイン内の発行者とトークンの最初のオーナーは SPV であり、グループ S は SPV を表し、グループ L は地方財産局を表し、グループ C は中央財産部を表します。

ほとんどの場合トークン転送にはオーナーと地方財産局（合計 3 で必要最低限値を満たす）の許可が必要です。このプロセスでは転送業務は地方財産局によって監査されます。中央財産部は裁判所、関係部門の判決、または審査の後、法的相続人にトークンの所有権を転送することがあります。

トークン ID の一部が失われた場合（発生する可能性は高い）、もしくは SPV と他のトークンオーナー両方がトークン追加に同意した場合、発行機関に追加のトークンを発行させることができます。さらに認可管理構造は極端なケースにも対応しています。たとえば法務局がこのタイプのトークンの流通を一時的に凍結する必要がある場合、管理権限があれば転送許可の必要最低限値を大幅に上げることにより、ドメイン内全トークンの転送を止められます。

代替可能なトークン (FT)（ポイント）

発行

誰もがシンボル登録後にポイントを発行することができます。ユーザーはこのシンボルでトークンの総数を設定できます。総数を設定しない場合は現時点で発行するトークン数を設定する必要があります。

転送

秘密鍵を持つ人はトークンを他人に転送することができます。

その他詳細

各アカウントは保持する異なるシンボルのトークン数を記録します。各シンボルのトークンは基本情報を保存する独立キー値があります。ユーザーは他の秘密鍵に指定されたシンボルとトークン数を転送する権利を与えることもできます。この機能はトークンアローワンスと呼ばれ、トークン交換の際に使用できます。

トークンベースのトランザクションモデル

概要

everiToken は、代替不可能トークンに**トークンベース**のトランザクションモデルを使用します。

トークンベース元帳の場合、トークン ID と所有権の記録が最初に発行された時点で作成され、その後新しい所有権が無制限に追加されます。これは代替不可能トークンには非常に効率的な方法です。この目的のために特に索引付きトークン・データベースを設計したのでトークンの情報の更新と照会は非常に高速です。

トークンベースのトランザクションモデルは everiToken のコアメンバーによって考案され、代替不可能トークンを everiToken 上で完璧に動作することが証明されています。 everiToken は、すべての巻き戻し不可能なブロック上でアクションを実行しているときにのみに状態を変更する状態マシンと考えられます。everiToken のようなトークンベースのトランザクションモデルに基づくブロックチェーンでは、データベースをトークン DB とブロック DB の 2 つに分けることができます。トークン DB とブロック DB の両方がバージョン化された DB であることにより、ブロックがまきもどした場合の高速ロールバックできます。everiToken ではトークン DB に RocksDB を使用しています。

トークン DB

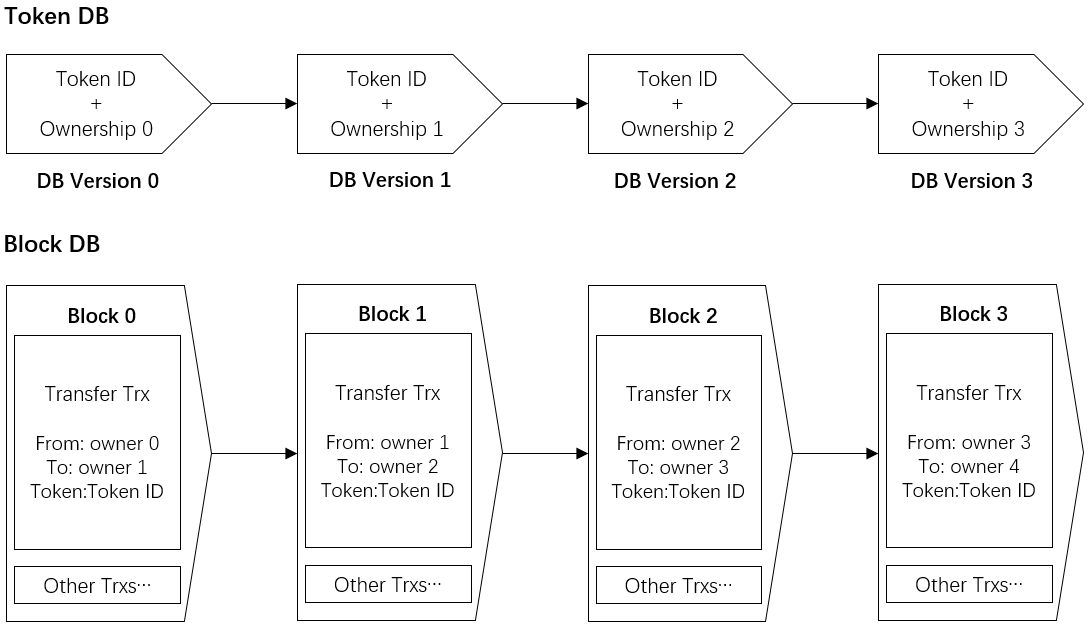
トークン DB はトークンの所有権やチェーン上の代替可能なトークンの残高など、ブロックチェーンの最新ステータスをすばやく見つけるためのインデックス付き DB です。トランザクションを実行すると DB のオーナーが変更されます。トークン DB はデータ追加のみができるデータベースなので、新しいデータが追加されると DB のバージョンが増加し、古い値はすぐに削除はされま

せん。古いバージョンを使用してロールバックすることができます。その場いいブロックが巻き戻され、ガベージコレクトされます。

ブロック DB

ブロック DB は、チェーン上の巻き戻し不可能なブロックをすべて集結する役割を果たします。 各ブロックには、実行されたアクションの名前とパラメータ、ブロック上の署名、その他情報など、すべての詳細が集結されます。

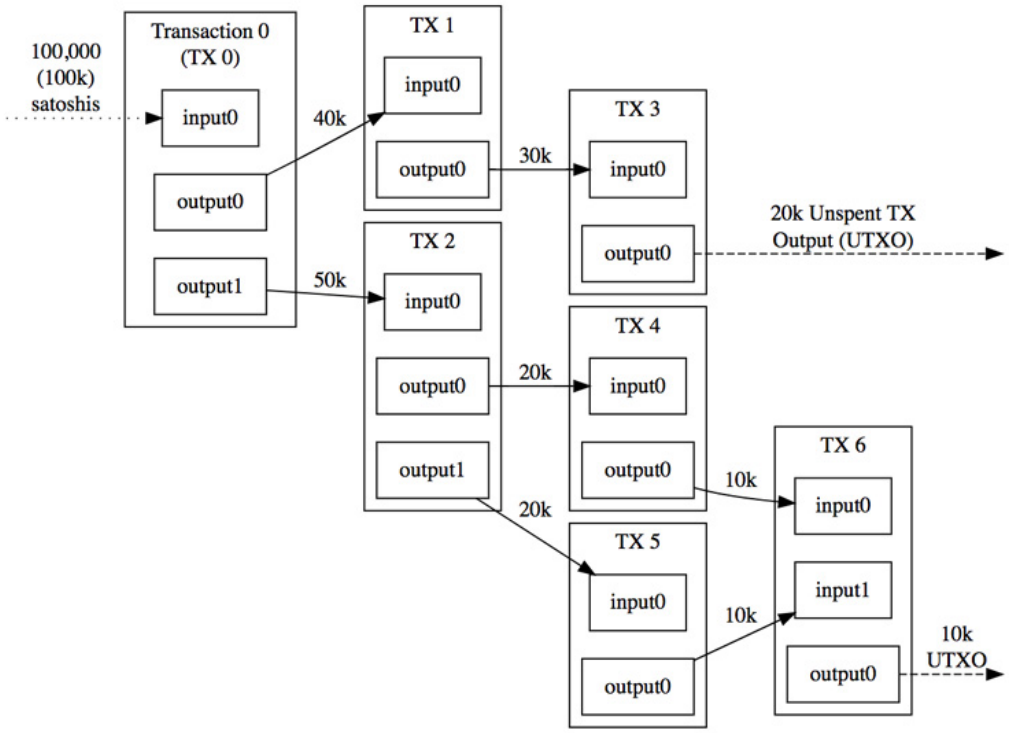
こちらのグラフは、代替不可能トークンのために 2 種類のデータベースがどのように連携するのかを示しています:



他のトランザクションモデルとの比較

a）UTXO

UTXO モデルでは各トークン所有者は、前の取引のハッシュ値と次の所有者の公開鍵（アドレス）をデジタル署名し、これらをコインに追加することによって、所有しているコインを他人転送します。 このメカニズムは本質的には、トークンの所有者が実際に所有していないトークンのインプットとアウトプットの連続違反ですが、特定の数のトークンの出力を所有することにより、新所有者がそれをインプットとして署名すれば同じくアウトプットを所有することになります。



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

(bitcoin.org の図を使用してます)

ご覧のように、UTX は特定のインプットが明らかね一度しか使用できないため、二重支出を避けるのに最適です。しかし、それにはいくつかの欠点があります。

- BTC は代替不可能トークンの一種ではなく、代替可能トークンです。すべての UTXO に固有の ID を保持しても意味ないです。（everiToken はそれをは代替不可能トークンに移します。）

- UTXO は一回限りのものです。 膨大な量の UTXO を保存するためのコンピューティング資源やディスクボリュームの無駄です。

b）残高ベース

残高ベースの取引モデルは銀行と同様です。 あなたは銀行で口座を作り、その口座にお金を貯め、引き出したり振り込んだ時のは口座の残高を変更します。 UTXO のようなものはなく、より効率的です。なぜなら、データベース内の数字のみを変更するからです。 しかし明らかに代替不可能トークンには適していません。

セキュリティ

everiToken はトークン関連の機能に集中し、重要ではない抽象化レイヤーを簡素化したことにより効率と安全性の両方を改善しました。 everiToken のトークン種類は非常に豊富で理論上無数ですが、統一されたトークン構造によりシステムと第三者機関は原則に従って監査することができます。システムはスマートコントラクトの 1 つの形式を認識するだけなので、複雑な監査とセキュリティが必要ないです。

スクリプト（everiSigner）

everiSigner はオフライン署名ツールです。ブラウザーのアドオン内で全ての署名プロセスが実行されますので秘密鍵が漏洩する心配はありません。ウェブサイトはセキュリティを高めるために新しいチャネルを作成した後 everiSigner と接続し、署名するコンテンツをチャネルに渡してから everiSigner は署名されたデータを返します。

秘密鍵紛失

認可管理に基づいて第三者は多くのサービスを提供することができます。例えば C 社はパスワード保護専門サービスを提供しており、アリスはトークン秘密鍵を忘れるのを恐れています。アリスはドメインの転送許可をオーナー(1)とグループ C（1）に与え、必要最低限値を 1 に設定します。こうすればアリスが秘密鍵を紛失し、トークンの管理権を失ってしまった場合でもグループ C を通じて再びトークンのアクセスを持てます。

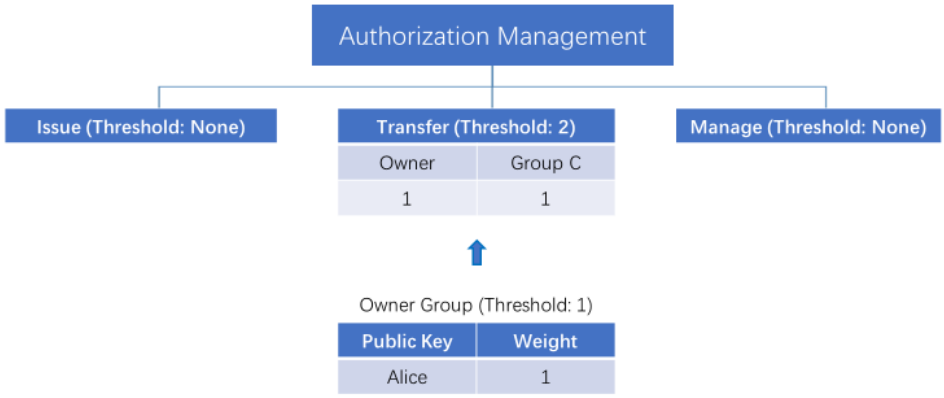


図 4.会社 C は秘密鍵復元サービスを提供

もちろんグループ C はアリスのトークンを盗むことができますが、すべての操作がチェーン上記録されるため C の信頼性が損なわれます。

コンセンサス

everiToken のコンセンサスアルゴリズムは BFT-DPOS を導入してます。 DPOS はブロックチェーン上のアプリケーションの性能条件を満たせることが証明されています。このアルゴリズムでは EVT トークンを保持する人は、継続的承認投票システムを通じてブロック生産者を選択することができます。誰でもブロック生産に参加することができ、トークンオーナーの投票を十分に得られればば、ブロック生産する機会が与えられます。
everiToken はブロックを精確に 0.5 秒ごとに生成し、どんな時でも 1 人だけのブロック生産者がいます。スケジュール時間内にブロックが生産されない場合そのタイムスロットのブロックはスキップされます。 1 つ以上のブロックがスキップされますとブロックチェーンに 0.5 秒以上の空きができます。
everiToken のブロックは 180 のラウンドで生産されます（12 ブロック x15 生産者）。各ラウンドの初めに、違う 15 人のブロック生産者が EVT オーナーの投票よって選べられます。選べられた生産者らは 11 人以上の生産者が同意した順序で生産スケジュールができます。
生産者がブロックを逃し、過去 24 時間以内にブロックを生産しなかった場合、ブロックを再び生産開始する意思をブロックチェーンに通知するまで外されます。信頼性が低いと判明した生産者にスケジューリングを組み込まないことでスキップされるブロックの数を最小限に抑え、ネットワークがスムーズに動きます。
ビザンチン将軍問題はすべての生産者がブロックに署名できるようにすることで解決されます。11 人の生産者が特定のブロックに署名するとそのブロックは不可逆であるとみなされます。悪質な生産者は、同じタイムスタンプまたはブロックの高さを持つ 2 つのブロックに署名をして暗号証拠を生成する必要があります。このモデルでは 1 秒以内に不可逆的コンセンサスが達成されます。

その他技術詳細

ベーシックチェーン

私たちは既に存在する技術を一からは作りません。「先生を超える生徒」になるために、既存のパブリックチェーンシステムの優れた部分を取り入れます。EOS は現在最高の設計、最先端の実用的なブロックチェーンプラットフォームの 1 つであり、コード構造も優れているため、ベーシックフレームワークを everiToken のコードベースとして使用しています。

私たちは everiToken のトークン流通のためのあらゆる操作の実装を独自に開発しました。同時にトークンベースという点に集中し、パフォーマンスを向上させるために EOS のデータ構造を最適化しました。
このような実践には多くの利点があります：

- EOS はベーシックフレームワークはきちんとテストされてます。DPOS やその他のコアメカニズムは BitShare のようなプロジェクトでも万全にテストされています。

- ベーシックフレームワークを再利用することで作業負荷の一部を減らし、everiToken に関連する操作の最適化にもっと集中することができます。

- オープンソースコミュニティー精神として EOS の Github にベーシックフレームワークの改善を提出する予定です。

EOS ではブロックチェーン操作（アクション）には 2 種類あります。 1 つ目は C ++で書れたバイナリコードに直接コンパイルされるネイティブコードです。2 つ目はウェブアセンブリまたは JIT コンパイル後に実行されるコードに基づいています。 我々は 2 つ目のタイプを除去しすべてのコードをネイティブで実装しました。

承認操作

everiToken の承認オペレーションは主にマルチサイン、重量計算、必要最低限値設定などが含まれます。各トークンの転送は独立しているので異なるトークンの転送作業を並列して実行できます。また各グループの認可グループは独立しているため、異なるグループ間の発行や管理そうさを並列して実行することもできます。

各操作はデータパケットと署名リストで構成されています。認可確認各所名を検証するだけで署名間に相互関係はないので並列で実行できます。

実行エンジン

everiToken システムでは各トークンの操作が完全に独立しているため並列処理にはパーティションの追加負担がかかりません。トークンの操作種類は限られ、コードは組み込まれているため、各操作を繰り返しテストすることにより

システムの安定性は保証できます。

everiToken は各ブロックの製造プロセスを準備、転送、終了の 3 段階に分けてます。新しいドメインを作成してトークンを発行するとき、システムは操作の正確性を保証するために準備段階で処理されます。次に最高のパフォーマンスを維持するために、トークンオーナーの変更と配布の操作は並列処理されます。終了段階ではエラー対処に集中して結果の正確性を維持します。

トランザクション中断
中断されたトランザクションは複数の遅延後に完了するトランザクションを指します。通常の一時停止していないトランザクションは一度に完了し、トランザクションがサブミットされるとすべての条件が満たされなければなりません。例えばすべての署名者が一緒に署名する必要があるとします。しかし現実では複数のトランザクションが一貫のプロセスで完了します。トランザクションの参加者は、同時に署名することができないと想定できます。中断されたトランザクションは、トランザクション全体が成功するまで署名を一つずつ承認することができます。

EvtLink / everiPass / everiPay

everiPay / everiPass
everiPay / everiPass は、everiToken パブリックブロックチェーンを使用して対面型マイクロペイメントのために生まれた支払い方法です。

EvtLink には、QR コード生成の標準と通信プロトコルの定義が含まれています。
EvtLink / everiPass / everiPay のハイライトは次のとおりです：

- **即時クリアランス**、取引は瞬時に決済となります。

- **地方分権化**: P2P 決済、非中央集中型プラットフォーム、チェーン上のデータを改ざんすることができなく、誰もが価格設定に参加することができます。

- **最高の安全性**: ブロックチェーン内のデータとコンテンツは、ユーザーの財産セキュリティの保護を最大限にするために、偽造または改ざんすることはできません。

- **互換性**: everiPass / everiPay は、everiToken でサポートされているすべてのトークンに利用できます。通貨だけでなく、トークンやポイント、ドアを開く鍵まで、スマートフォンだけでどこでも利用できます。

- **便利性**: インターネットに接続できなくても決済できます。

- **速い:** everiToken は高い TPS を達成しており、機器やネットワークの状況を考慮して 1〜3 秒以内にトランザクションを完了できます。

- **標準化**：ウォレット側からの技術とは異なり、EvtLink は生態系全体のために作られたクロスウォレット、クロスチェーン、クロスアプリ標準です。アプリを使用して作成または解析することができます。

上記の 7 つの特徴によって everiPay / everiPass は最も安全で、最も便利で楽しいサービスを対面式で提供することができます。

everiPay / everiPass の場合、受取人は EvtLink の解析と everiToken へのトランザクションのプッシュをサポートするアプリを使用する必要があります。エンジニエア向けに使いやすい API やコード例を提供するのは簡単です。これはお店が AliPay / WeChat サポートを追加するのと似ていますが、それよりはるかに簡単です。

受取人 QR コード

受取人の QR コードは everiPay と比べて機能は少ないです。たとえば、支払いを行うにはインターネットに接続し、支払人と受取人は手動で金額を入力します。支払いが自動的に完了したときは通知は送られません。

ただし、受取人はこの支払い方法をサポートするアプリを使う必要はありません。実際、受取人がする事は携帯電話でウォレットを使って支払いを受けたかどうかを確認するだけです。非常に小さな店や個人の利用に適しています。可能限り、支払人は QR コードの代わりに everiPay を使用することをお勧めします。

EvtLink の技術の仕組み

EvtLink は、everiPass / everiPay の実行に使用される QR コードの形式です。everiToken パブリックチェーンは、everipass と everipay のアクションを使って

evtLink のトランザクションを実行します。 EvtLink を表す構造体 evt_link も提供しています。

everiPay / everiPass 支払いの技術的プロセスは次のとおりです：

1. 支払人は使用する一種のトークンを選択するとウォレットに支払人の署名と支払用トークンのシンボルが含まれた一連のダイナミック QR コード 128 ビット LinkId が表示されます。関連するトランザクションが実行されない限り、QR コードが変わっても LinkId は変わりません。こうしないと二重支払いのリスクが生じます。チェーンは同じ LinkId を持つ EvtLink 上 2 以上のアクションは許可しません。

2. 支払人のウォレットは有効な取引 ID を取得するまで、get_trx_id_for_link_id という API を連続で呼び出すことにより、LinkId に関連するトランザクション ID を継続的に照会します。その後ウォレットは次に QR コードを表示する時には違う LinkId を表示します。ウォレットはこのトランザクション ID を照会することによってトランザクション結果を表示する必要があります。支払人のウォレットは取引を直接送信する必要はありません。

3. 一方受取人は電話、スキャナまたはスマートゲートウェイを使用して QR コードをスキャンします。 EvtLink をスキャンして解析した後、アクションでラップされチェーンにプッシュする必要があります。その後、すべてのチェーンノードが結果を同期され get_trx_id_for_link_id は 404 の代わりにトランザクション ID を返します。

base42 エンコーディング

Base42 はバイナリから文字列へ変換のためのエンコーディングです。 これは 16 進数エンコーディングに似ていますが、代わりに 42 をそのベースとして使用し、それに合わせて別のアルファベットを使用します。 アルファベットは QR コードのエンコード文字と同じですので、base42 でエンコードされた文字列を QR コードにエンコードすると効率的です。それにより QR コードのサイズが小さくなるかもしれません。

everiToken では Base42 を利用して EvtLink のコンテンツをエンコードします。

パート III. 経済モデル

燃料(EVT)

EVT 燃料は DDoS などのシステム攻撃回避、DPOS の投票権、生産者への合理的な報酬役割を果たします。everiToken 上すべての操作に EVT をサービス料として課金されます、生産者の報酬になります。請求される EVT 数は自動に変わります。サービス料は主に悪意のある攻撃を防ぐためのもので、ほとんどのユーザーの通常使用に支障はありません。
EVT の生成と転送方法は主流の仮想通貨と同じです。 EVT はプロデューサのブロック生産への報酬と悪意行為を防ぐためのみに使用されるので他の価値はありません。

コアチームには 1 億 5,000 万 EVT（合計 15%）が与えられます。
コミュニティコア貢献者には、1 億 5,000 万 EVT（合計 15%）が与えられます。
プレースメントには 7 億回の EVT（合計 70%）と設定されています。

サービス燃料コスト=燃料使用量×R

この式の燃料使用量は特定のアクションを使うための価格です。価格の単位は EVT で R は**調整率**です。 BP ノードはチェーンが忙しい状態または攻撃されている時に、自動的に**レート上げ**をします。 もちろん EVT の価格が高すぎる場合は**レート下げ**もします。R は 15 BP の中央値として計算されます。
チェーンのユーザーが API を初めて呼び出すときに R は 1 になります。BP 影響で R に変動がなければ呼び出し完了します。R が変わった場合は BP の応答された R から呼び出しが失敗と判断されます。ユーザーは再び呼び出し直すことができます。
例えば creatingAccount API を呼び出す価格を 2 EVT とします。
通常ユーザーは 2 EVT で CreatingAccount API を呼び出すことができます。
BP が R = 1.1 にレート上げされますと価格は 2.2 EVT に変わります。
すべてのブロック生産者の中央値が R となりますので、 3 人の生産者が R を 1.15、5 人が 1.2、2 人が 1.1、2 人が 1.3、1 人が 1、1 人が 1.4, 1 人が 1.45 とすると、R の最終値は 1.2 になります。

固定 EVT

固定 EVT は EVT に似ていますが転送できません。燃料代のみに使用できます。ユーザーはいつでも EVT を固定 EVT に 1 対 1 のレートで交換できます。**固定 EVT は通貨ではない**ため、安全上固定 EVT を誰かにエアドロップするのに向いています。

EVT を使用して燃料代を請求することもできるため EVT を固定 EVT に交換することはお勧めしません。EVT を固定 EVT に交換する際、固定 EVT は自動的に受信機にバインドされるため、**固定 EVT** と名付けました。

固定 EVT は特定のアカウントに属し他人に転送することはできませんがエアドップするのは可能な上、便利で安全です。企業や組織は EVT を固定 EVT に変換して特定のアカウントに投稿することができます。しかしその後固定 EVT を再度転送することはできません。

ペイヤーは取引の支払い用アカウントです。 everiToken はユーザーが取引でペイヤーを指定できますのでアカウント作成に便利です。

安全のためペイヤーは取引に追加の署名が必要です。

ペイヤーが設定されている場合、燃料費に固定 EVT で支払いはできません。

各ドメインには固定 EVT 用の特別残高があります。

チェーンはドメイン内のトークン転送や破棄などの処理に固定 EVT バランス（ゼロでない場合）を優先して消費します。

ユーザーは EVT でドメイン内の固定 EVT 残高を前払いすることができます。

追加 EVT 発行

毎年追加の EVT を発行します。

- $R = \begin{cases} 0.05 - 0.005 \times Y & (0 \leq Y \leq 5) \\ 0.02 & (6 \leq Y) \end{cases}$
- Y は現在の年からチェーン作成年を引いた数です。
    - Yは0から年々増加します
- 発行される数は$(1 + R)$ × 現在通貨量.

その他情報

ブロックプロデューサ（BP）

- BP 数：15

EOS とは違い、BP を増やすとコストも増加するため私たちは EVT を BP ではなく、コミュニティにより多く提供したいと考えております。分権には 15 個の BP で十分です。

- 初年度に BP は発行された EVT の 1%、2 年目には 0.9%を得られます。

エスクロー会社

everiToken はトークン ID 以外、現実世界でトークンが示している資産やコインについては何も知りません。トークンの価値はエスクロー会社によって支えられます。これらのエスクロー会社はトークンの発行中に追加署名を加えることができるのでトークンを署名した会社に社会信用があればトークンも信用されます。SSL のようなものです。

パート IV. エコシステム

ツール

everiSigner アドオン

everiSigner はオープンソースのアドオンで、ユーザーは everiToken アプリケーションをブラウザで直接アクセスできます。everiSigner には安全に異なるサイトでのアイデンティティ管理と、ブロックチェーントランザクションを検証するための UI を提供してます。さらにユーザーの秘密鍵を保存し、EVT、ETH、EOS、その他プラグインともコンパチブルです。

everiWallet

everiWallet は、everiSigner アドオンに基づくウォレットです。詳細はこちらをご覧ください。https://www.everiwallet.com/

EVTJS

EVTJS は JavaScript 用 everiTokenAPI バインディングライブラリで、NodeJS とブラウザ両方をサポートしてます。また everiSigner もサポートされてますので、このライブラリを使い everiToken 上のウェブアプリケーションを簡単に作れます。詳細はこちらをご覧ください。https://www.github.com/everitoken/evtjs

evtScan

evtScan は everiToken のブロックチェーンブラウザです。誰でも everiToken TestNet（および今後のメインネット）のノードによって生成された全てのブロックに関する特定のリアルタイム情報（チェーン上のトランザクション、アカウント、グループ、ドメインの詳細、統計および分析など）を検索できます。開発者は evtScan を使い情報がチェーンに正しくリンクされているかどうかを効率的に確認できます。ユーザーは evtScan でトランザクションの真正性を検証できます。詳細はこちらをご覧ください。https://evtscan.io/

アプリケーションシナリオ

トークン経済のネットワークではブロックチェーンが発行、取引の確認、会計、和解、清算を記録します。上流から下流まで発行者、取引所、流通経路、公証プラットフォームなどすべての機関は役割に応じて everiToken の公開チェーンを使用できます。
トークン関連のコア情報のみがチェーンに記録されます。信頼問題は取消不能性と不正行為に生じる膨大な費用により解決されます。オリジナルのモジュールでトークン経済ニーズの大部分を満たしているため、大勢の方にすぐに使っていただけます。短期的に everiToken は今後パートナーシップのため以下の 3 つのアプリケーションシナリオに集中します。

クーポン

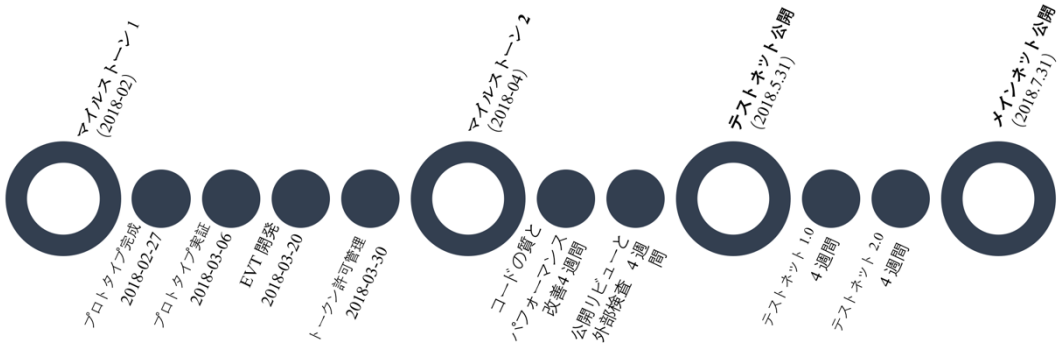
EveriToken は North American House Buyers（住宅取引システム www.beimeigoufang.com）のクーポンシステムを構築しています。 NAHB は everiSigner を使用してサブユーザー（登録された家の売り手または代理店）が NAHB 署名付きのさまざまなクーポンを発行できるようにウェブプラットフォームを提供しています。プラットフォームはすべてのクーポントークン関連の発行、転送、管理、検証などの操作を簡単に実行できるように、everiToken API が提供されています。サブユーザーとエンドユーザー（住宅購入を希望するユーザー）は全ての操作をウェブ上でこなせます。発行記録は全部 everiScan で追跡できるので余分のクーポントークンを発行することはできません。クーポントークンは実用的価値が高いです、たとえば 100 ドルのクーポンは家を購入する際、10 倍の 1000 ドル割引になったりできます。NAHB、サブユーザー、エンドユーザーらはみんな従来のクーポントークン化により流通が高まるので得します。

ゲームプロトコル

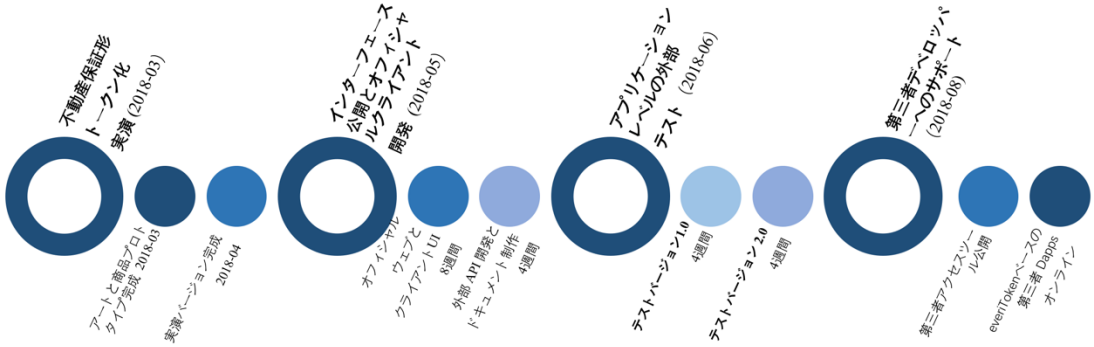
FastX も everiToken のパートナーです。 FastX はイーサネットの遅い処理速度に対処するために、Ethereum ベースのゲーム用プロトコルを提供し、ユーザーはゲームデータステータスをスマートコントラクトにロックすることができます。同時に FastX はサブチェーン上でも同じ情報を生成し、完全なゲームデータがメインチェーンとは定期的な更新する事で処理速度を大幅に高めています。EveriToken は、高い安全性、便利な転送機能、簡単な管理機能を備えているため、ゲームプロトコルのサブチェーンとして使用できます。すべてのゲームデータの変化は everiToken チェーンに直接記録されます。ゲームのデータ全部を保存する必要はなく、Token 関連の情報の最も重要な部分のみセーブするのが好ましいです。

タイムライン

パブリックチェーン開発 スケジュール



アプリケーション レイヤー 開発 スケジュール



パート V. まとめ

Token 経済時代は間も無く到来しますが Ethereum と EOS のスマートコントラクトは Token 経済の開発には適していません。

トークンベースのブロックチェーン技術を目指して、everiToken はトークンの発行、転送、検証が誰にでも簡単にできる特化システムを構築しました。システムは Turing 完全ではありませんが、システム内の抽象度も低下しました。よって処理スピード、セキュリティ、相互運用性、安定性、監視しやすさを向上させました。世界中の誰もが効率的にデジタルで価値を理解、創造、交流することができるようになります。

創業者たち

CAI Hengjin, 首席科学官

2005 年から武漢大学コンピュータサイエンス学部教授および博士号アドバイザー、中国科学アカデミーの先端技術の深セン研究所マルチメディア技術センター客員研究員、Global FinTech Lab 専門家、中国 AI とビッグデータ委員会の専門家委員を務める。サービスサイエンス、AI、ブロックチェーン技術に携わり、「機械の登場前：人間の意識と知性の始まり」という書籍を出版。 WU Wenjun 人工知能科学技術賞受賞。武漢 Yellow Crane Talents Plan の初回選考に選ばれ、2012 年に武漢大学で教育への貢献が評価され大統領賞受賞した。専門アドバイザーとしてマイクロソフト Imagine Cup、マイクロソフトモルガンスタンレー Cup of High Performance Computing in Finance、インテル Cup National Collegiate Software Innovation コンテスト、中国大学生起業家精神コンテストなど、中国および世界中の有名大会で生徒をサポートし 80 以上の賞を受賞。

Brady Luo, CEO

Brady はブロックチェーン技術に基づいたグローバルトークン経済を信じています。 北京航空航天大学大学院電気工学学部とブランデイズ大学の金融大学院卒業。オックスフォード大学のサイードビジネススクールでブロックチェーン戦略を勉強。上海 1000 人の計画（ベンチャーグループ）の第三バッチに選ばれた起業家。以前はニューヨークオッペンハイマーファンドで代替資産投資（CDO ベースの資産証券化）と日本最大の金融グループ三菱 UFJ 証券（東京本社と上海）に勤めていた。

Bozhen Chen, COO

Bozhen は政府プロジェクト運営に豊富な経験を持ち、強力な執行、コミュニケーション、PR スキルを持つ。アストン大学経営学科理学士。過去に電子商取引プロバイダ、アパレルサプライチェーン B2B サービス、社会貢献ショー

トビデオ、政府 e コーマスプロジェクトなど参画。Internet Conference と Tongxiang 電子商取引公共サービスセンターの永続的ホスト。国家の農村青年リーダー、2017 年最も美しい浙江青年リーダータイトルを獲得、青年インターネット起業家サービスセンターのディレクター。

Ceeji Cheng、CPO

10 年以上のフルスタックデベロッパーの開発経験を持ち起業家精神とチームマネジメント経験が豊富。かつて国家情報学オリンピックリーグで一位を獲得。以前はスタートアップの CTO、共同創業者などを務める。

Harry Wang、CTO

Harry は 10 年以上のシステム開発経験を持つ。以前は上海 Tianfeng 証券会社で働き技術パートナーとして私募に参加し、量的取引システム開発を担当。