everiToken 技術白書

v1.0, 2018 年 4 月 10 日

要点：

- この白書は、明示的又は暗示的な保証、証拠、予想などを表すものではありません。

- この白書に記載されている技術指標又は技術実現方法は、時間とともに変化する可能性があります。

- 技術チームは、いつでも解体又は再編成する可能性があります。したがって、コア技術者の離脱により、プロジェクトを完全に実施するのが不可能になる可能性もあります。

- この白書は原書です。プロジェクトチームとそのメンバーは、達成できない、又は完璧に達成できない項目については責任を負いません。

- この白書で言及されている Token は、実際には価値がありません。これは、以前に Token をデジタル暗号化で取得したことの証明に過ぎません。

- この白書に記載されている手法を使用して実行されるブロックチェーンまたはその派生品で発生する不都合は、プログラムによって自動生成された為、責任を負うことはできません。最終結果は、当ブロックチェーンを使用すると判断をした個人や組織の責任です。

- 誰でもこの白書の内容を変更又は悪質な非営利目的で使用することはあり得ます。この行為によるいかなる結果について責任を負いません。

目录

Token 経済時代とブロックチェーン 2
Token 経済時代の到来 2
我々の使命 4
既存技術の限界 4
イーサリアム：ERC20 / ERC721 4
EOS 5
要約 6
Token 発行と移転 6
Token 6
Token 発行と移転 7
合意アルゴリズムと燃料（EVT） 8
合意アルゴリズム 8
燃料（EVT） 8
権限管理 8
権限構造 9
シナリオ 1 10
シナリオ 2 11
シナリオ 3 13
技術の詳細 14
基本チェーン 14
データストレージ 14
権限管理 15
実行エンジン 16
結論 16

Token 経済時代とブロックチェーン

Token 経済時代の到来

2018 年 4 月、Bitcoin とブロックチェーンの基盤となるテクノロジーが世に紹介されて約 10 年になりました。我々が常に抱えている 1 つの疑問は、生産技術における革命と呼ばれるブロックチェーンが、導入されて以来世界経済に良い変化をもたらしたのかというものです。

データを見てみましょう：現時点では、ブロックチェーン上（以下「チェーン上」と省略）により管理されている世界各地の資産にあらゆる種類の代替通貨が存在し、総市場価値は約 3,000 億ドルです。チェーン上のこれらの資産は、一般的に、高い変動性と投機性によって特徴付けられ、世界経済に利益をもたらすにはほど遠いものです。実際、中本哲史をはじめとして、人々はこれらの「代替通貨」を支払い通貨として利用したいと考えていましたが、現在ではデジタル資産な為、通貨の役割を果たしていません。無価値の「代替通貨」を強調した結果、通貨主権など一連の困難な問題を引き起こしました。

実際、通貨は権力であり、通貨は政治であり、通貨の権力は国家に属していなければなりません。したがって、Token が通貨を置き換えることは非常に困難です。国家の認可と支援がなければ、いわゆる「代替通貨」は単に欺瞞に過ぎません。

一方、現在全世界の主流資産（有形・無形）はブロックチェーン下（以下「チェーン下」と省略）にあります。ブロックチェーンとこれらのチェーン下資産との間には基本的に交わりはありません。

しかし、Token は本当に単なる代替通貨ですか？違います。Token 本来の意味は「証拠、象徴」です。なので、「証書」という言い方が「代替通貨」より正確です。証書は、身分証明書から卒業証書、金銭、請求書、鍵、ポイント、カード商品券、株式から債券、社会すべての権利と利益を証書で表すことができます。

歴史を振り返ってみると、人間社会の文明全ては権利と利益を証明する事に基づいていると言えます。口座、所有権、資格、証明書などはすべて権利と利益の証拠の一部であります。 ユヴァル・ハラリが「サピエンス全史」で述べたように、ホモ・サピエンスが先立って人間文明を築いた根本的な理由は、上記の「架空事実」にあります。現在の権利証書には、偽造が容易、紛失しやすい、移転困難、簡単に複写して改ざん出来るなど数多くの問題があります。これらの権利と利益が全て電子化され、暗号が真正性、完全性、プライバシーを保護又は検証するようになれば、文明の非常に大きな改善になります。我々はそれを「Token 経済時代」と命名します。

証書は必ずしもブロックチェーン上で実行する必要はありませんが、ブロックチェーンは証書の為の信頼出来る確かな基盤になります。 したがって、証書が Token 経済時代のフロントエンド技術であれば、ブロックチェーンは Token 経済時代のバックエンド技術です。二つとも同様に重要です。

我々の使命

人類の歴史の過程とブロックチェーン技術の進捗状況を分析した結果、次世代ブロックチェーン技術は以下、三つの側面を含む権利と利益を管理できる必要があります。

第一は、**電子著作権証明書**。証書は、資本の電子形式証拠でなければならず、権利、又は固有的かつ本質的な価値を表すものでなければなりません。

第二は、**暗号化および権限管理**。暗号によって保証される、証書の真正性、改竄性防止、プライバシー保護、権限管理、規制性および類似の能力。

第三は、**流通性**。証書が取引又は交換出来ることを意味する。

上記の要求に基づき、我々は、Token 経済時代の一般的な基本要求を満たし、Token の管理と流通を促進し、Token 経済時代の技術基盤を構築することを目的とした解決案を提案しました。

具体的には、上記の要求に対応する為、下記の 3 つの主な機能を実現しました。

- **迅速かつ便利なリリース Token**：ユーザーがコードを書く必要が無く、我々の API、又はアプリケーション (App、ウェブページ、またはサードパーティアプリケーション) を通じて独自の Token を公開できます。

- **Token の効率的な認証と流通**：Token 瞬時流通を実現し、何百万もの Token を同時に実行出来るようにしました。

- **柔軟な著作権管理**：簡易かつ洗練された統一モデルを使用して、権利管理、複数人物の共有、秘密鍵の取得、複数レベルの権限、コンプライアンス、政府監督、およびその他の複雑な要求を開発能力のないユーザーでも実現できます。

既存技術の限界

イーサリアム：ERC20 / ERC721

イーサリアムをベースにして Token 経済を実現する主な方法は、ERC20 および ERC721 協約に基づいてスマート契約を開発することです。その内の ERC721 は非均質性証書 (NFT) をサポートしているため、私たちの要求により近いものです。しかし、この方法には深刻な問題があります。

- **容量問題**：現在、イーサリアムは毎秒十何個かの取引しかサポートできません。これはチェーン上のすべての Token の実際の要求を完全に満たすことができません。
- **費用問題**：イーサリアムスマート契約を実行中あらゆる段階で Gas を消費します。複雑な事業論理（共通所有、規制、コンプライアンスなど）を実現するために、高い費用、又は制御困難という問題が発生します。
- **普及の難しさ**：イーサリアムの Token 経済の実装はスマート契約に基づいています。非開発者はサードパーティーアプリケーションに頼る以外上記は基本的に不可能です。
- **非標準化**：異なるスマート契約は全く違う開発観点を採用する可能性があるため、仮想 Token のメタデータが統一されていなく、全ての状況に適切な解決策が存在しません。これは無論 Token 経済の発展を助長しません。更に、ユーザーの為の独自の色々な種類の Token 資本を確認するための統一された方法が存在しません。

EOS

EOS は、2018 年 6 月にメインネットワークの立ち上げを発表しました。EOS はイーサリアムの改良版なので、EOS に基づいて Token 経済関連要求の開発を進めれば、Ethereum のいくつかの問題を解決することができます。但し、EOS を導入してもまだいくつかの問題があります。

- **安全性問題**：

1. Token 取引は非常に価値が高い、又は再生不可能な実体に対応する可能性があり、セキュリティ上の問題はないが、スマートコントラクトに基づく開発は開発者レベルによって制限されており、各タイプの Token 開発者が十分なセキュリティ意識を持っていることを保証するのは困難です。

2. EOS のスマート契約は Web Assembly に基づいていますが、これはまだテスト（Beta）段階で、完成までにはまだ相当の時間がかかる可能性があります。EOS のスマート契約コードはチューリング完全で、権限が大きすぎるため、セキュリティ侵害が容易に出来ます。

3. ほとんどの人はスマート契約を作成しません。Token の配分と管理を行う為には、第三者のコードに依存しなければいけません。最終分析では、資産の管理は自ら行うのではなく、第三者の管理の質に頼る以外は出来ません。

- **標準化されていない**：イーサリアムと同様に、異なるスマート契約によって管理される Token メタデータは、通信または相互運用できません。

- **規制、信用、コンプライアンス**：コードを読み取るに必要な非標準化と専門技術のため、政府が規制をするのは困難です。 また、一般人は、コードの信頼性を自身で完全に判断することができません。 これらの理由により、ブロックチェーンは一般人や政府に受け入れ難い状況になっています。

- **実装効率**：多様の要求を満たすために、EOS スマート契約には複雑な機能、多くのシステムモジュール、資源制限と分配の困難性など、システムの複雑さが大幅に増し、処理速度が低下しました。 異なるデータと機能との間の障礙の可能性を避ける為、マルチスレッド実行によって速度を上げることは容易ではなく、過大な資源の代償を払わなければいけません。 Token 経済にとって、これらの複雑な機能は過剰です。

- **普及困難**：現実の業務要求は複雑又は多変であり、一貫性がありません。開発されたスマート契約は、時間通りに経過観察するのが難しく、少数派の人々の要求を満たすことはできません。 これらは、Token 経済発展の障害になるでしょう。

要約

上記の考察に基づいて、我々はブロックチェーン技術発展に密接しながら新技術を導入し、基本から進み、ブロックチェーン技術を適用するに最適な方案を探索し、Token 経済開発のための新たなパブリックチェーンと生態系 everiToken を提案しました。 実在する世界全ての資産、証明書又はバウチャーなどは、Token 発行を通して**証明書電子化**を実現出来る可能性を持ち、その安全性、速度、及び相互流通性、又は追跡性を経験できます。

Token 発行と移転

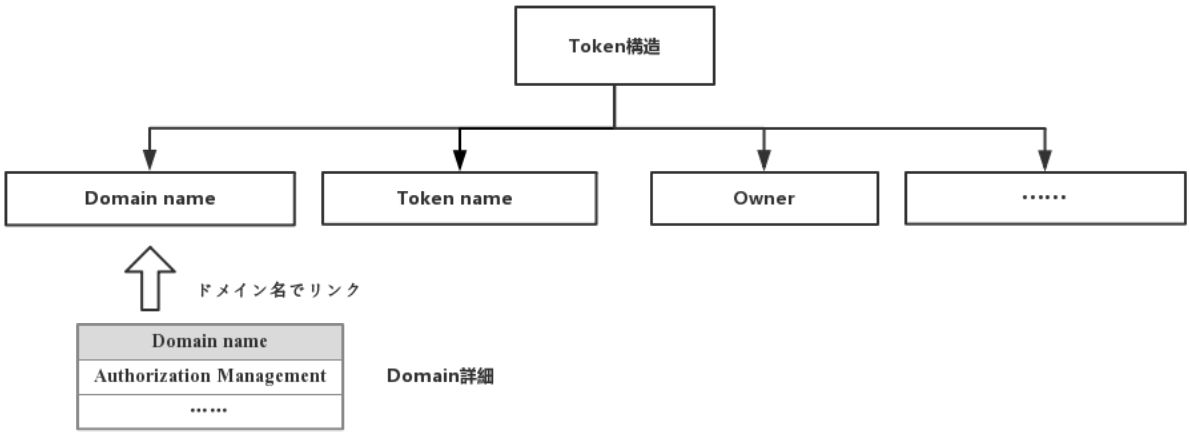
Token

我々は**証書**（Token）を、資産、特定の時間または場所の独占的な共有経済、または特定の人物が提供するタイムサービスを証明するものとして定義しています。 このシステムの Token とは全て非均質 Token（Non- Fungible Token）です。

各 Token は、一種の**ドメイン**（Domain）に属し、固有の**ドメイン名**によって認証されます。 同時に、発行者は各 Token に唯一無二の**名前**（Name) を設定することができます。この名前は独自の特殊な意味を持つことができます（典型的な例は、製品の国、製造業者およびその他の情報を含む製品のバーコードを Token の名前として使用することです）。

Token の **ID** は、**ドメイン名**と Token の**名前**を足した固有の物になります。

Token の基本構造を図で表すと：



Token ID は、唯一 Token を識別出来る**ドメイン名**と**名前**を Token の基本情報に格納する事の呼称です。 加えて、Token 所有者およびその他の重要な情報も記録します。

ドメイン情報は、Token のドメイン名を通して調べることができます。 ドメイン情報では、承認管理（Authorization Management）の一部およびその他の必要情報を記録します。

Token 発行と移転

誰もが独自の Token を発行する権利を持っています。Token 自体は価値がなく、その効用は Token 発行者の実際の信用によって裏付けられます。

Token が発行されれば、取引を通して他の人に移転可能です。我々のシステム内では、Token 移転後、Token **所有者**を変更しています。各 Token には Token 所有者がいます（1 人以上の所有者も可能です）。所有者を変更する必要がある際、Token の配布に参加しているユーザーは、電子署名に署名することで移転操作に同意します。everiToken ノードは、権限要件が満たされ、他のノードと同期されたことを確認した後、Token の所有権を変更します。移転時の権利管理については、**権利管理**に関する部分を参照してください。

"Token ベース"特徴を利用し、Token の移転は Token 所有者を変更するだけの簡易方法とし、既存のブロックチェーン技術を改善出来ました。システム内では、各 Token の移転は互いに独立しており、影響を及ぼさないため、自然的な同時処理が可能です。マルチコア CPU では、これにより、取引先を確認してブロックを作成する性能が大幅に向上します。Token に関連する機能に焦点を当て、不要な抽象化された層を効率化し、システムのパフォーマンスは従来のブロックチェーンに比べて大幅に向上しました。

合意アルゴリズムと燃料（EVT）

合意アルゴリズム

異なるノードで合意状況を達するために、BFT + DPOS 混成合意アルゴリズムを使用します。 絶対的な分散化は非現実的であると我々は信じています。 DPOS は、相対的な分散化を保証すると交換に、処理速度を最速化することができます。

具体的には、各投票期間の開始前に、各自が一定数のブロック生産者を選ぶことができ、選出された候補者は、ブロックの生産プロセスに参加し、会計を担当します。 これらのブロック生産者内部で、我々は BFT 合意アルゴリズムを使用してノード間の合意速度を上げました。

DPOS に基づくグラフェンプロジェクトは、安全で信頼性の高い BTS や EOS などのブロックチェーンシステムを支持しています。

燃料（EVT）

DDos などのシステムへの攻撃を回避する為、DPOS 投票に Stake を提供する為、会計担当者に妥当な報酬を与える為に、EVT を燃料として発行します。 すべての操作は EVT の一定額を手数料として請求します。この請求額の一部を、会計担当者の報酬として使用します。 請求された EVT は、悪質な攻撃を避けるためにのみ課金されるように自動的に調整され、ほとんどのユーザーの通常使用には影響しません。

EVT の生成および移転方法は、既存の主流のブロックチェーン代替通貨と同じです。

EVT は、会計担当者が提供する資源に報酬を与え、悪意のある行為を防止するためにのみ使用され、他の価値はありません。

権限管理

どのアカウントにも Token を発行する権限がありますが、異なるドメインの Token には異なる目的設定があります。 例えば、不動産の移転には政府関係機関の見直しと厳格な規制が必要であり；連鎖店の会員カードやクーポンはブランドの是認を得る必要があり；演奏会の有効チケットは見終わってしまえば無効になりますが、固定された一つの駐車スペースの所有者は、今月と翌月では別人かもしれません; 夫妻が共有している資産を取引する場合二人一緒に同意する必要がありますが、長年宝物のように保管した郵便切手を売る事を決心した場合、惜しむ気持ちを抑えて、分け与える勇気だけで十分です。

異なるドメインの Token の複雑な空間、時間、参加者の状況を満たすために、さまざまなシナリオで異なる要件を満たすための一連の権限管理フレームワークを導入しました。

Token 発行者は、Token 発行時にドメイン内の権限項目を選ぶことで、権限管理を行います。 everiToken システムには発行権（Issue）、移転権（Transfer）、管理権（Manage）の 3 つの権限項目があります。

権限構造

発行権（Issue）: ドメイン内の Token を発行する権限。

移転権（Transfer）：ドメイン内の Token を移転する権限。

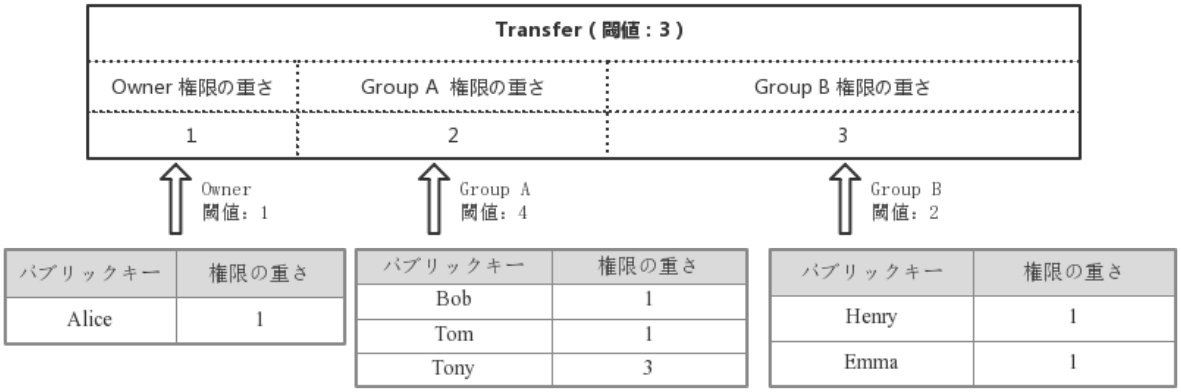
管理権（Manage）：ドメイン接続許可（権限管理などのパラメータを含む）を変更する権限。

どの権限も一つ、又は多数の群（Group）によって管理され、Token が発行される際、発行者は各権限下で各群の情報と権限の重みを指定する必要があります。各権限は閾値を設定する必要があります。あるドメインに置ける Token 操作の実行において、検証過程は、発行した群がその操作を実行する許可を持っている事を検証し、認可された群の権限の重さを足した結果が閾値を超えていた場合のみ、システムに受け入られます。このグルーピング設計は現実の様々な状況に対応し、柔軟な権限の重みと閾値の設定過程は、現実の複雑な要求の全てに対応します。

一つの群は、企業、政府部門、財団、または友人間で構成された少グループ、あるいは個人を表すことができます。一つの群はその群特有のパブリックキーと群内全ての構成員の権限の重みを表す構成表を持ち、唯一、群内全ての権限を持つ構成員の同意を合計した値が予め設定した群の閾値を超えた場合、群が操作を承認したと認められます。同時に、パブリックキーをもつ群内の人物、又は組織は群内の構成員と権限の重さを変更する操作を認可出来ます。この群内構造を**群内自治（Group Autonomy）**と呼びます。

各群は最初に作成された際、自動的にその群の ID を生産し、発行者がドメイン権限を設定した時、群内の自律規制構造を利用し、既に存在する群 ID を使い、直接群を他の権限構造システム内に移動する事が出来る為、各群を容易に再利用出来ます。

Token 所有者は Token 所有者の集合である特殊な Owner という名称が固定された群に所属します。この群の特徴は各 Token が異なる可能性がある事で、発行操作の認可条件は、全ての構成員の同意です。もし構成員各人の権限の重さを 1 とするならば、閾値は群内の構成員の数になります。以下の図を例とすると：



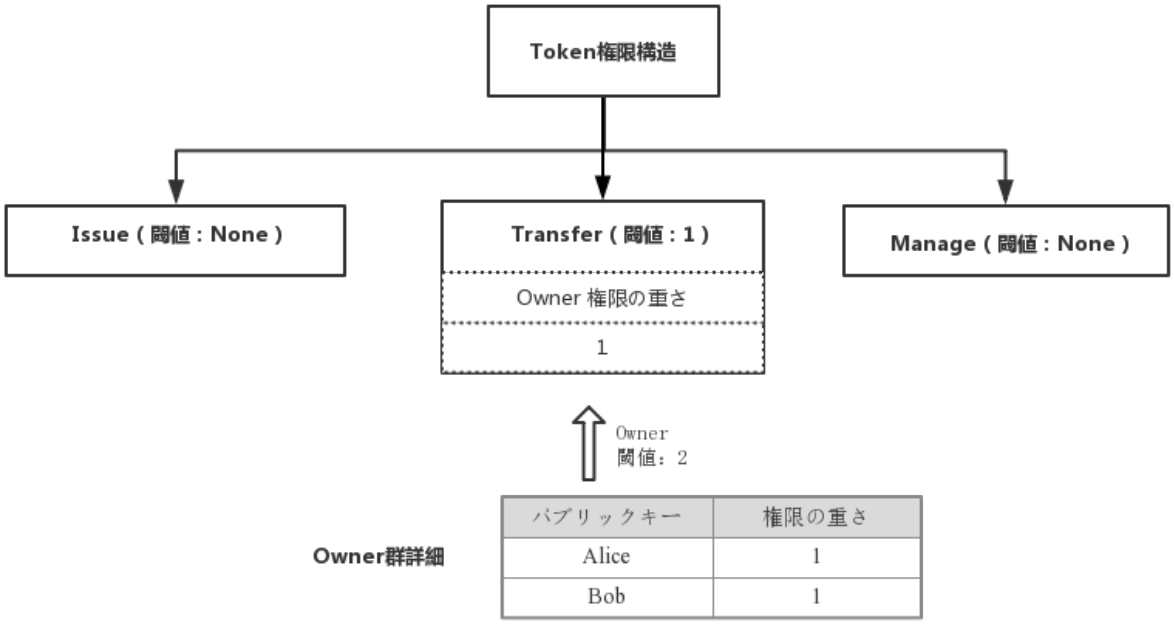
この図は、あるドメイン内の Transfer 権限を表しています。閾値は 3 として、Owner，Group ***A***、Group ***B*** の 3 つのグループがあります。各群の権限の重さ (それぞれ順番に 1、2、3) に基づいて、閾値を満たすには、Owner と Group ***A*** は共同発行を必要とし、Group ***B*** は単独発行出来ます。

各群の説明として、Owner が発行する為には Alice のパブリックキーだけを必要としますが；Group ***A*** が閾値を満たし、発行する為には少なくとも Bob と Tony、又は Tony と Tom の共同発行を必要とし；Group ***B*** が閾値を満たし、発行する為には Henry と Emma 全ての認可を必要とします。

下記ではいくつかの例を使って権限管理の利便性を証明します。

シナリオ 1

現実では Token の所有者はおそらく一人ではなく、多数です。例として、夫妻 (Alice と Bob) が一緒にペットの犬を飼っていたなら、犬を現在取引するには夫妻両方の同意を得てから、この犬の Token を発行します。構造は次の通りです：



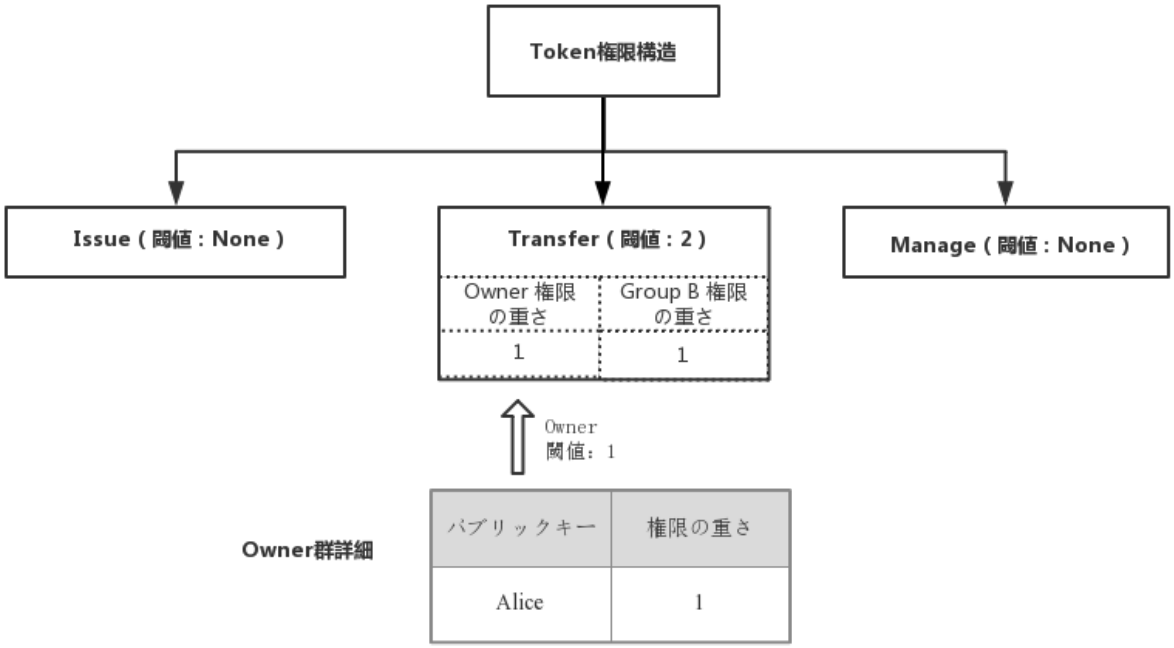
発行者 (Alice、Bob 両方とも可能) は、この Token の所有者を Alice と Bob の間で共同所有する事を設定します。権限管理の点では、余分な変更や要求を省く為、発行者は Issue と Manage の権限を空白に設定します。こうすれば、このドメインの管理構造を二度と追加、又は変更出来ません (どの群も権限を持ち合わせていません)。Transfer 権限内 (権限に続くカッコ内の数字が閾値を表し、群に続くカッコ内の数字が権限の重さを表しています) では、Owner しかいません。Alice と Bob が同時に移転操作に同意した場合のみ、この操作はシステムに受け入れられます。

Alice 又は Bob、どちらかのシークレットキーだけで署名されている場合、システムはサービスを拒否しエラーメッセージを表示します。

シナリオ 2

Alice が購入した、会社 B 発行のとある金融 Token は安全性保証とリスク管理の要求を満たす為に、会社 B はどの Token の取引も会社側の確認、加えて取引一部の手数料を受け取る事を要求します。

このドメインの Token 構造は次のとおりです：



Alice はこの Token の所有者ですが、もし Token の所有権を移転する場合、Owner 群 (すなわち、Alice 自身) 署名合意以外に、Group B の許可を得る必要があります。Group B は会社 B が金融 Token 移転の管理をする為の群です。Alice がこの Token を転送する際、会社 B に手数料を払う必要があり、支払いと同時に、会社 B は Token 移転操作を検査でき、確認後、Group B の署名合意 (第三者サービスを利用) を通して、最後に移転操作がシステムによって認識されます。

このメカニズムに基づけば、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、会社 C がパスワードにより保護されたサービスを提供すれば、Alice はシークレットキーを忘れるか無くすことで自身の Token を失う事を恐れて、ドメインの Transfer 権限を：所有者 (1)、Group C (1) とし、同時に閾値を 1 に設定するとします。このような状況では、もし Alice が自身のシークレットキーを忘れ、Transfer 群の権限を取得することができなくても、会社 C を通して、Alice 本人であると証明ができ、そこから Group C の認可権限を得ることができます。こうすれば、Alice は類似の Token を自身のアカウントに移転し、自身のシークレットキーを再取得できます。

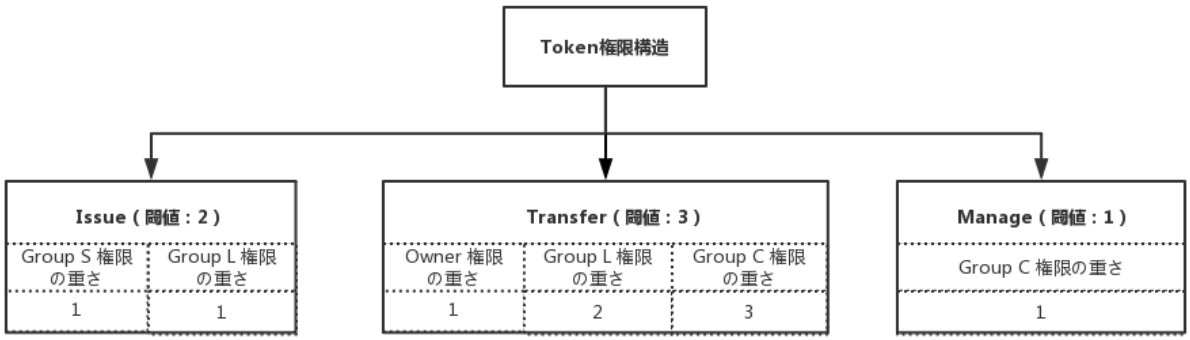
当然、Group C が悪意を持ち、Alice の Token を移転する事は出来ますが、全ての操作がチェーン上に記録される為、信頼性のある会社 C にとって、それは無価値の行為です。

シナリオ 3

ここでは、everiToken の権限管理メカニズムで解決できる複雑な問題を表すために、最も複雑なシナリオを紹介します。

会社は新しいオフィスビルを建設し、建物の財産権のために 1000 Token を発行することを望んでいます。これらの Token を発行、又は維持する為に SPV を設定しました。不動産 Token の発行と移転は、地方不動産局によって審査と承認される必要があり、当地の規則に従った場合のみ発行する事が出来、その後公式プラットフォームで建物の Token の詳細（総数、発行者、権限管理構造など）を表示します。さらに、地方不動産局と保有者を制限し管理するために最高権限を持つ中央不動産局の徹底した規制があります。

このドメインの権限構造は、下記の図のようになります：



ドメイン内の最初の発行者と Token 所有者を SPV として、Group ***S*** は SPV、Group ***L*** は地方不動産局、グループ C は中央不動産局を表します。

一般的に、Token の移転は、元の所有者と地方不動産局の署名で十分です。この過程中、地方不動産局は移転過程を見直します。 Token 所有者の死亡や秘密鍵の紛失などの予期していない状況では、裁判所または関係部門の審査を経て中央不動産局が決定を下し、Token の所有権を正当な後継者に移転することができます。

誤って Token ID の一部を失った（発生する可能性はあります）、又は SPV や他の Token 所有者が新しい Token を発行することに同意したとしても、中央不動産局は既所持の Issue 権限を通じて実際の要求を満たすために新しい Token を発行することができます。さら

に、例えば、中央不動産局が Token の流通を一時的に停止する必要がある場合などの非常に特殊な状況下では、既所持の Manage 権限によって Transfer 権限の閾値が変更され、ドメイン内の全ての Token 発行が凍結されることがあります。

技術の詳細

下記は技術者の為に書かれているので、それ以外の人は飛ばしても大丈夫です。

基本チェーン

我々は同じシステムを再構築するつもりはありません。したがって、私たちは、「青は藍より出でて藍よりも青し」を達成するために、既存のパブリックチェーンシステムの優れた部分を多く吸収しました。 EOS は現在、優れたコード構造を持つ最も高度で実用的なブロックチェーンプラットフォームの 1 つと考えているため、コードベースとして EOS の基本構造を採用しました。

これにより、私たちは everiToken における Token 流通のための各操作の実装を独自に開発し、高度に最適化しました。 同時に、Token ベースの特性を踏まえて、EOS のデータ構造を最適化してより良い性能を得ました。

このアプローチには多くのメリットがあります：

- EOS は完全かつ十分にテストされた基本構造を持っています。 DPOS やその他のコアメカニズムも同じく、BitShare のような項目で完全にテストされています。
- 基本構造を再利用することで、一定量の作業負荷を減らし、everiToken 操作の最適化により集中することができます。
- 使用過程中、オープンソースコミュニティーの精神に沿って、我々の基本構造の改善策を EOS コードに提供します。

EOS には二つの形式のブロックチェーン操作（Action）があり、一つはネイティブコードという、C ++で書かれたコードで、直接バイナリーコードにコンパイルされます。 もう一つは、Web Assembly 又は JIT コンパイル後に実行されるコードです。 我々は二つ目の操作を無効化し、全てのコードを Native で実現しました。

データストレージ

EOS には、Boost.MultiIndex ベースのロールバック操作をサポートするメモリーデータベ

ースがあります (主に Chainbase)。 すべての契約操作データの結果はこのメモリーデータベースに存在します。 フォーク時のロールバックを支持する為、加え、契約コード異常時の復旧の為、各操作中ロールバックの為にデータを追加記録する必要があります。さらに、すべてのデータはメモリーに格納され、処理されますが、ユーザーの増加と時間の経過に伴い、メモリー増量の需要が増加することが予想されます。 これは、ブロック生産者のメモリー容量に対する高い要求です。 プログラムがクラッシュまたは再起動すると、すべてのメモリーデータが失われます。 データを復元するには、すべてのブロックの全操作をもう一度繰り返す必要がある為、長いコールドスタート時間が発生します。

我々は EOS メモリーデータベースを維持しながら、RocksDB を基盤とした Token データベースを開発しました。このデータベースにはいくつかの利点があります：

- RocksDB は成熟した産業基準の Key-Value データベースで、Facebook の中核群内で完全に検証され、使用されています。
- RockDB は LevelDB に基づいて開発されており、LevelDB と比較してより優れた性能と豊富な機能を提供します。同時に、純粋なメモリーの為に、フラッシュや SSD などの低レイテンシストレージ状況をコア最適化しました。
- 必要に応じて、RocksDB をインメモリーデータベースとして使用できます。
- RocksDB ベースの構造上、当然、バージョンのロールバックと永続性をサポートし、パフォーマンスへの影響は最小限に抑えます。

我々の Token データベースは、基盤となるストレージエンジンとして RocksDB を使用しています。トークン関連の操作では、性能を最大限に引き出すために調整しています。この手法を使用すると、低コストでロールバックを実現できます。また、Token データベースは、コールドスタートなどの問題を解決するために、データの永続性、定量バックアップ、増分バックアップなどの機能のオプションを提供します。

everiToken での操作は非常に抽象的であるため、操作が非常に少なく、各操作に必要な情報量も非常に少なく、EOS などの一般的なシステムに比べて冗長性が非常に低く、ブロックの長さも短くなります。

権限管理

everiToken の権限管理には、主に複数署名、権限の重要度計算、閾値設定などが含まれます。各 Token の移転は互いに独立しているため、異なる Token の移転操作は並列実行できます。各 Group の権限群も互いに独立しているため、発行と管理、どちらの操作も異なる

群間で並列実行できます。

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。 権限認証時、各署名を検証するだけで、署名に関連性が無いため、並列実行できます。

実行エンジン

EOS の実行エンジンはチューリング完全なスマート契約コードをサポートする必要があるため、その実装は複雑で、並列操作は特に実現するのが困難です。これには多くの要因が存在します：

- ブロックチェーンの読み書きの操作は、契約コードによって決定されます。各操作には、矛盾するアカウントやデータが含まれる場合があります。データ間の障害を避けるためには、データを正しく分割し、並列および直列実行を正しい方法で処理する必要があります。これを実現するのは複雑です。
- 各操作の並列ロールバック要求の可能性があるため、データベースの要求が難しくなります。 EOS の既存の Chainbase はこの機能を支持していません。この機能を正しく実装するには、時間と大規模なテストが必要です。

したがって、EOS の技術白書では、EOS の公式バージョンが開始された際に、並列機能が支持されていないことが明確に述べられています。

everiToken システムでは、各 Token 変更操作は完全に独立しているため、並列処理にはパーティショニングの追加負担がかかりません。さらに、Token 操作のタイプが限られていて、コードも組み込まれている為、各タイプの操作が繰り返しテストされている限り、システムは安定している可能性が高いです。

everiToken は、各ブロックの製造プロセスを 3 つの段階：準備段階、移転段階、および最終段階に分割します。新しいドメインを作成して Token を発行するとき、システムは正しい操作を保証するために、準備段階中に順次ドメインを処理します。Token 所有者の変更、発行およびその他の操作は、最高性能を実現するために並列処理されます。最後に、例外を最終段階で集中的に処理し、結果を保持します。

結論

Token 経済時代が近づいていますが、イーサリアムや EOS のスマート契約は、Token 経済

には適していません。

everiToken はブロックチェーン技術をベースとした「Token ベース」に基づいて、トークンの発行、流通、検証のための専門システムを構築しています。システムは、チューリング完全性の一部を犠牲にしましたが、システム内の抽象度を減らし、速度、安全性、相互運用性、安定性、規定を改善し、より効率的な実行能力を実現しました。これを通して、世界全ての人に理解し、想像し、交流し、互いに真の価値を伝えることを可能としました。

同時に、デジタル世界と現実世界の媒体として、everiToken は誰もが技術によってもたらされる利便性を経験できるように、現実世界の難事を解決するためにブロックチェーン技術の実用的な要求を満たすことを目指し、 社会全体の効率性、加え信頼までに至るコストを削減し、ブロックチェーン技術を原点時の概念に復旧させます。