インターネット上の出版者とコンテンツ事業者がスマートなソーシャル通貨を利用できるようにするためのプロトコル

はじめに

Steem はパブリックアクセス可能で不変なコンテンツのためのスケーラブルなブロックチェーンプロトコル[*1]を提供します。それは高速で手数料不要のデジタルトークン (STEEM)[*2]によって、人々が自身の頭脳を用いて通貨を得ることを可能にします (“プルーフ・オブ・ブレイン” と呼ぶことができます)。プロトコルの 2 つの構成要素ブロックチェーンとトークンは、セキュリティ、不変性、寿命について相互に依存し、従って相互の存在に不可欠です。Steem は 1 年以上正常に動作しており、今やビットコインとイーサリアム両方の処理済みトランザクション数を越えています。[*3]

他のブロックチェーンと比較して、Steem はインセンティブを与える仕組みを持ち、プレーンテキスト形式のコンテンツを改変できない状態で格納する初のパブリックアクセス可能なデータベースとして頭角を現しています。このことから Steem は、あらゆるインターネットアプリケーションが最も価値のあるコンテンツを提供した者に報酬を与えつつデータを引き出し共有することができるパブリック出版プラットフォームとなっています。

暗号通貨の分野では、STEEM のユニークな特性によりビットコインやイーサなど他のものと比べて「スマート」と「ソーシャル」の両方を実現しています。これは新しい 2 つのトークンの機能に由来しています。1 つ目はコンテンツ作成とキュレーションへのインセンティブ付与に特化したトークンプールです (“報酬プール” と呼びます)。2 つ目はコンテンツの価値を評価してトークンを分配するために人々の知恵を活用する投票システムです。結合したこれらの 2 つの特性は、プルーフ・オブ・ワークにならってプルーフ・オブ・ブレインと呼ばれ、コミュニティの参加者にトークンを分配するために必要なヒューマンワークに重点を置いていることを表しています。プルーフ・オブ・ブレインは STEEM を、組み込まれた報酬システムによってコミュニティに価値を付加することを奨励することで、絶え間なく成長し続けるコミュニティを形作るためのツールとして位置付けています。

ブロックチェーンとトークン技術の向上に加えて、Steem は盗難アカウント回復[*4]、エスクローサービス、ユーザープロモートコンテンツ、評価システム、貯蓄アカウントなどの

---

*1 Delegated Proof of Stake Position Paper. Grigg, 2017.
https://steemit.com/eos/@iang/seeking-consensus-on-consensus-dpos-or-delegated-proof-of-stake-and-the-two-generals-problem

*2 To differentiate it from the term for its blockchain, the correct spelling of Steem's native digital token is STEEM.

*3 Transaction Volumes: Transactions Per Second Report. Steem Witness and user “@roadscape”.
https://steemit.com/blockchain/@roadscape/tps-report-2-the-flippening

*4 Stolen Account Recovery initiation for Steemit.com users: 07-13-2017
https://steemit.com/recover_account_step_1

ユーザーエクスペリエンスを強化する高度な機能を提供するシステムです。これらはすべてのトランザクションにおいて 3 秒の承認時間と手数料ゼロでユーザーに提供されています。これらによりインターネット上の出版者やコミュニティビルダーにスマートでソーシャルな通貨をもたらすという使命を支えています。

プルーフ・オブ・ブレイン：スマートでソーシャルなトークン

トークンベースのコミュニティに貢献するユーザーに報酬を出すシステムには、コンテンツの社会的価値を確立し評価する仕組みが必要です。これを “プルーフ・オブ・ブレイン” と呼びます。

報酬プール (“トークンはどこから来るのか？”)

Steem ブロックチェーンの最も革新的な (そして誤解されやすい) 側面の一つは、価値あるコンテンツの制作者にトークンを配布する “報酬プール” です。報酬プールが何かを理解するためにはまず、トークンを生み出す DPoS ブロックチェーンと PoW ブロックチェーンの違いを理解する必要があります。従来の PoW ブロックチェーンでは、トークンは定期的に生産されますが、ワークを実行しているマシンを持つ人々 (“マイナー”) にランダムに分配されます。

PoW 専用の暗号通貨とは異なり、Steem のトークンは 3 秒毎に 1 ブロックの固定レートで生成されます。これらのトークンは定義されたブロックチェーンのルールに基いて、様々なアクターに分配されます。コンテンツ制作者、証人、キュレーターなどのアクターはトークンのために特別な方法で競い合います。マイナーが純粋なコンピューターパワーで競い合う従来の PoW の分配方法とは異なり、Steem ネットワークのアクターはネットワークに価値を加える方法で競い合うようにインセンティブを与えられます。

新規トークンの生成比率は、2016 年 12 月から年間 9.5% に設定され、250,000 ブロック毎に 0.01% または毎年 0.5% ずつ減少します。インフレ率は約 20.5 年後に 0.95% に到達するまで減少し続けます。

毎年 Steem ブロックチェーンにより生成される新規トークン供給の内、75% がコンテンツ制作者やキュレーターに分配される “報酬プール” を構成します。15% は帰属するトークン保有者に分配され、10% は Steem の DPoS コンセンサスプロトコルでブロック生成に協力している証人に分配されます。

■コンテンツ制作者とキュレーターへの報酬

コンテンツを制作するユーザーは、新規ユーザーをプラットフォームに誘導する材料を作り出すだけでなく、既存のユーザーを魅了し楽しませ続けます。これにより、幅広いユー

ザーに通貨を流通させ、ネットワーク効果を高めることができます。コンテンツの評価と投票に時間をかけるユーザーは、最も多くの価値を付加しているユーザーに通貨を分配する上で重要な役割を果たしています。ブロックチェーンはこれら両方の活動に対し、ステークに重みを付けた投票システムによる集合知に基づいた価値に相関して報酬を与えます。

■報酬の配分を決定するためのステーク化したトークンによる投票

Steem は 1 STEEM、1 投票に基いて動作しています。このモデルでは、アカウントの残高によって測られるプラットフォームへの貢献度が最も高い人が、貢献度の評価方法に関して最も影響力を持ちます。ステークは購入することも獲得することもできます。ステークを共有する 2 つのアカウントと、同じステーク量を持つ 1 つのアカウントは同じ影響力を持つため、ユーザーは複数のアカウントを持つことによって付加的な影響力を持つことはできません。プラットフォームでの影響力を向上させる唯一の方法はステークを増やすことです。さらに、Steem は Steem パワーと呼ばれる 13 週間の帰属スケジュールに委ねられた STEEM によってのみ投票することが許されています。このモデルでは、メンバーには STEEM の長期的な価値を最大にするような方法で投票するための経済的なインセンティブがあります。

Steem ブロックチェーンの速度とスケール

Steem ブロックチェーンは既存のブロックチェーンで最も速く最も効率的なものの一つとなるために設計されています。それは Reddit よりも大きいソーシャルメディアプラットフォームで予想されるトラフィック量をサポートするために必要です。Steem はビットコインのトランザクション数を凌ぎ、毎秒 1 万件以上のトランザクションをサポートするように拡大可能です。

委任プルーフ・オブ・ステーク (DPoS)

多くのブロックチェーンはプルーフ・オブ・ワーク (PoW)[*5]がボトルネックとなり、世界の金融トラフィックの一部であるトランザクションを毎秒 3 件を超えるように拡張することができません。Steem は PoW によるものよりも遥かに大きいスケールと速度が必要であり、何十億ものユーザーに適したブロックチェーン基盤を構築するために、委任プルーフ・オブ・ステーク (DPoS)[*6]というあまり知られていないアルゴリズムを活用しました。

[*5] Bitcoin Scalability Problem
https://en.wikipedia.org/wiki/Bitcoin_scalability_problem

[*6] DPoS Whitepaper
https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

DPoS により、Steem ブロックチェーンは最小の計算負荷で新ブロックを 3 秒毎に生成することが可能になりました。このため、ブロックチェーンはより多くのトランザクションを処理し、コンテンツを含むより多くの情報を保持することができます。

ハードフォークが発生したときのルールを定めることにより、DPoS フレームワークで選出された証人は提案されたハードフォークを採用するかどうか迅速かつ効率的に判断できるため、Steem ブロックチェーンプロトコルは他のものよりも素早く進化することができます。Steem ブロックチェーンは既に 18 回のハードフォーク[*7]に成功しており、それぞれのハードフォークが起こったタイミングで 1 つのチェーンしか維持されていません。

ChainBase

ChainBase[*8]はブロックチェーンスタックのデータベース部分であり、2016 年に Graphene[*9]に置き換えられました。ChainBase はロード時間と終了時間が速く、データベースへの並行アクセスをサポートし、以前のものよりもクラッシュに対して堅牢です。また、データベースの破損頻度も少なく、データベース全体の状態を瞬時に “スナップショット” することができ、同じメモリからの RPC リクエストを処理することができます。

AppBase

AppBase はマルチチェーン FABRIC を作成する最初のステップです。AppBase は、専用のプラグインとして付加的な非コンセンサスブロックチェーンを作成することにより、Steem ブロックチェーンの多くのコンポーネントをモジュール化することを可能にしています。これらのプラグインはブロックチェーン全体を再生する必要が無いため、より迅速に更新することができます。これにより、steemd[*10]はより効率的で維持拡大が容易になります。

事実上、AppBase は様々なコアや異なるコンピュータ間であっても、Steem ブロックチェーンの様々な部分を整備することができます。これはそれぞれのコアを必要とするよりも遥かに効率的で、ネットワークのそれぞれのコンピュータでブロックチェーン全体を維持します。ブロックチェーンのモジュール化により、コンピュータのモジュール性を最大限に活かすことができます。これは完全に並列化され、完全に最適化されたブロックチェーンを作るための長いプロセスで不可欠なステップです。

---

*7 https://steemit.com/steemit/@steemitblog/proposing-hardfork-0-20-0-velocity

*8 ChainBase Release https://steemit.com/steem/@steemitblog/announcing-steem-0-14-4-shared-db-preview-release

*9 Graphene Documentation http://docs.bitshares.org/

*10 The component of the Steem blockchain framework responsible for processing transactions and the distribution of rewards.

Steem のプラットフォーム機能

Steem ブロックチェーンはデジタルトークン処理システムであるとともに、メインストリームのソーシャルメディアプラットフォームであるという 2 つの目的を果たします。ブロックチェーンによって提供される機能は、両方の目的をサポートするために必要なもので、ユーザーにプラットフォームの両方の側面を使用することで世界クラスのエクスペリエンスを提供します。

コンテンツアプリケーションのために設計されたプリミティブ

Steem は様々なコンテンツを公開し、プレーンテキストとしてブロックチェーンの不変な台帳に直接的かつ永久に格納するユニークな機能をユーザーに提供します。ブロックチェーンに格納されると、開発者がビルドするためのデータが公開されます。開発者は利用可能な API によってブロックチェーンのコンテンツと直接対話することができます。ブロックチェーンプリミティブの一部はアカウント名、投稿、コメント、投票、アカウント残高から作成することができます。

ネイティブネームシステム

ビットコインやイーサリアムなどの多くのブロックチェーン技術が使用しているウォレットアドレスは歴史的に長いランダムな文字列や数字列で構成されています。しかし、これらのウォレットアドレスはユーザーが記憶から長い文字列のアドレスを思い出すことができないため、典型的なオンラインソーシャルメディアのコンテキストにおいて他のユーザーと取引することを難しくしています。Steem ブロックチェーンは参加者のユーザー名をウォレットアドレスとして使用します。ユーザーはトークンを送ろうとするときにこれらのアドレスを記憶から検証することができるため、参加者のユーザーエクスペリエンスを強化することができます。

Steem ブロックチェーンドル (SBD)

暗号通貨を知った多くのユーザーは、プラットフォームから与えられた “魔法のインターネットトークン” がどのようにして実際の価値を持つのかを理解するのに苦労します。メインストリームのユーザーが慣れ親しんだ従来の法定通貨のシステムと、プラットフォームから与えられた暗号通貨トークンのギャップを埋めるために、Steem ブロックチェーンドル (SBD) という新しい通貨が作られました。

SBD トークンはちょうど 1USD にペッグされるように設計されているため、受け取ったユーザーはその価値を “実質 1 ドル” としてどのくらいの価値があるのかを知ることがで

きます。また、SBD トークンは、USD に対する相対的なアカウント価値を維持しようとするユーザーに比較的安定した通貨を提供します。より詳細な技術的説明は Steem テクニカルホワイトペーパーにあります。*[11]

分散取引所

Steem ブロックチェーンは BitShares 取引所*[12]のような分散トークン取引所を提供します。取引所でユーザーはパブリックな分散ピア・ツー・ピアマーケットで STEEM と SBD をトレードすることができます。ユーザーは買い注文と売り注文を出すことができ、注文のマッチングはブロックチェーンにより自動的に実行されます。また、ユーザーがマーケットを分析できるようにパブリックアクセス可能なオーダーブックとオーダー履歴があります。ユーザーはブロックチェーン API を用いて取引所と直接対話することも、Steemit.com のような GUI を用いることもできます。*[13]

エスクローによる支払い

ブロックチェーントランザクションの不可逆性は重要なセキュリティ機能です。しかし、他のユーザーにトークンを送る場合に、他のユーザーが契約を完了しない場合に取り戻す方法がないため、快適ではないケースが多くあります。Steem ブロックチェーンは、ユーザーがエスクローサービスとして指定された第三者によって互いにコインを送る方法を提供します。エスクローサービスとして働くユーザーは、契約の条件が満たされているかどうかを判断し、受領者に資金を送るか、送金者に返金するかを決定することができます。

階層的プライベートキー構造

Steem は低セキュリティと高セキュリティのトランザクションを容易にする今までにない段階的プライベートキーシステムを採用しています。低セキュリティトランザクションは投稿やコメントなどソーシャルのものが多いです。高セキュリティトランザクションは転送やキーの変更が多いです。これにより、ユーザーはキーに対して、それぞれが許可するアクセスに応じて異なるセキュリティレベルを実現することができます。

プライベートキーは、ポスティング、アクティブ、オーナーです。ポスティングキーは投稿、コメント、編集、投票、resteem*[14]、そして他のアカウントをフォロー/ミュートす

---

*[11] Steem Whitepaper
https://steem.io/SteemWhitePaper.pdf

*[12] Bitshares Decentralized Exchange
http://docs.bitshares.org/_downloads/bitshares-general.pdf

*[13] Steemit.com Currency Market
https://steemit.com/market

*[14] "Resteem" is the term used in the Steem blockchain for when a user shares the content with their followers.

ることができます。アクティブキーは資金転送、パワーアップ/ダウントランザクション、Steem ドル変換、証人投票、マーケットへの発注、ポスティングキーのリセットなど、より注意を要するタスクのためにあります。オーナーキーは必要な時だけ使用するためのものです。これは、オーナーキーを含むアカウントのすべてのキーを変更することができ、アカウント回復において所有権を証明できるため、最も強力なキーです。理想的には、オフラインに保管し、アカウントのキーを変更する必要がある場合や、ハッキングされたアカウントを回復する必要があるときだけ使用します。

また、Steem は 3 つのキーを暗号化するマスターパスワードを使いやすくしています。ウェブサービスは必要なプライベートキーで復号化や署名を行うことでマスターパスワードを使用することができます。マスターパスワードにより、ユーザーは不適切なキーが他のサーバーに転送されないようにすることができ、特定のサービスを信頼することができます。それにより、クライアント側の安全な署名環境を維持しながらユーザーエクスペリエンスを向上させることができます。

マルチシグ権限

Steem ブロックチェーンは権限を複数のエンティティに分割することを可能とし、複数のユーザーが同じ権限を共有したり、トランザクションを有効にするために複数のエンティティを要求したりすることができます。これは BitShares[*15] と同じ方法で行われ、各パブリック/プライベートキーのペアは重み付けられ、権限には閾値が定められます。トランザクションを有効にするためには、重みの合計が閾値以上になるために十分なエンティティが署名する必要があります。

複数の報酬受取人

任意の投稿について、報酬に金銭的関心を持つ人が多数いる場合もあります。これは、著者、共著者、参照元、ホストプロバイダー、ブロックチェーンのコンテンツを埋め込んだブログ、ツール制作者などを含みます。投稿やコメントを作成する際に使用されるウェブサイトやツールには、コンテンツからの報酬が様々な関係者の間でどのように分割されるのかを設定する機能を持つものがあります。これにより、様々な形式のコラボレーションが可能になります。また、Steem ブロックチェーン上に構築されたプラットフォームがユーザーから報酬の一部を集めることも可能です。

[*15] Bitshares Flexible Identity Management
http://docs.bitshares.org/_downloads/bitshares-general.pdf

スマートメディアトークン (SMT)

スマートメディアトークンは Steem ブロックチェーン上に構築可能なネイティブトークンです。STEEM は最初の SMT です。スマートメディアトークンプロトコルは、人々が STEEM と同様の特性を持つトークンを作成し、web 全体を通してコンテンツウェブサイトやアプリケーションの収益化することを目的としています。それは様々なオンラインコミュニティのビジョンにあわせてインセンティブを与えるようにカスタマイズすることによって、STEEM の成功を様々なウェブサイトやアプリケーションに再現します。詳細な技術情報はスマートメディアトークンのホワイトペーパーにあります[*16]。

盗難アカウント回復

ユーザーのアカウントがハッキングされた場合、プライベートオーナーキーでキーを変更されてしまう可能性があります。攻撃者がプライベートオーナーキーを盗み出し、アカウントのパスワードを変更してしまった場合、Steem の業界初の盗難アカウント回復プロセスに 30 日以内に有効であったプライベートキーを提出し、アカウントのコントロールを取り戻すことができます。これは Steem へのアカウント登録サービスを提供している個人または企業によって提供されます。登録者がユーザーにこのサービスを提供することは必須ではありませんが、これにより登録者のユーザーエクスペリエンスの価値を高めることができます。

タイムロックによるセキュリティ

ユーザーのアクティブまたはオーナーキーが盗まれた場合、攻撃者はアカウントのすべての資金にアクセスすることができます。ブロックチェーンのトランザクションは不可逆であるため、盗まれた資金を取り戻す方法はありません。

Steem ブロックチェーンはユーザーが STEEM や SBD を貯蓄アカウントに入れることができるようにしているため、3 日間を待たなければ資金を引き出せない可能性があります。また、13 週間の帰属スケジュールで保持されている STEEM は、最初の 7 日を待ってから毎週 1/13 の比率でしか引き出すことができません。これらのタイムロックは、攻撃者がユーザーの資金のすべてにすぐにアクセスすることができないようにすることによって、アカウントの所有者にすべての資金が引き出される前にアカウントのコントロールを取り戻す時間を与えます。

[*16] Smart Media Tokens Whitepaper
https://smt.steem.io/smt-whitepaper.pdf

無料操作の帯域幅制限

証人にはすべて新しく生成されたトークンで支払われるため、ブロックチェーンを稼働させるための料金をユーザーに請求する必要はありません。料金を請求する唯一の理由は、ブロックチェーンのパフォーマンスに潜在的に影響する程の不当なトランザクション量をユーザーが完了させないための抑止です。

システム使用に合理的な制限を設けるため、各ユーザーは制限された帯域幅を与えられます。ユーザーがトークンの転送、コンテンツの投稿、投票などのブロックチェーン操作を行うと、帯域幅の一部が消費されます。ユーザーに割り当てられた帯域幅を超えた時、更なる行動を行うには帯域幅が再チャージされるまで待つ必要があります。

帯域幅制限はネットワークの使用状況によって調整されるため、ネットワーク使用率が低い場合は帯域幅の割り当ては大きくなります。アカウントに割り当てられる帯域幅は、アカウントが持つ Steem パワー量に正比例します。そのため、ユーザーは Steem パワーを追加で手に入れることによって、いつでも帯域幅の割り当てを増やすことができます。

結論

Steem ブロックチェーンとトークンによって提供されるユニークな報酬とインセンティブプログラムは、Steem をメインストリームユーザーの暗号通貨への究極の入り口とするように設計されました。ブロックチェーンのパフォーマンスは、通貨とプラットフォームを広く普及させることを念頭に置いて設計されています。超高速な処理時間と無料のトランザクションの組み合わせにより、Steem は世界中の人が使用する主要なブロックチェーン技術の一つになることができます。