Steem

An incentivized, blockchain-based, public content platform.

November 2017

Abstract

Steem は暗号通貨の報酬によって、コミュニティ構築と社会的相互作用をサポートするブロックチェーンデータベースです。Steem は暗号通貨とそのコミュニティの構築から得た教訓と、ソーシャルメディアのコンセプトを組み合わせています。コミュニティ、通貨、または自由市場経済への参加を促す重要な鍵は、一人一人の貢献を一貫性を持って反映する公平な会計システムです。Steem はコミュニティに主体的な貢献をした無数の人々に、正確で透明性のある報酬を与えることを試みる初の暗号通貨です。

Table of Contents

はじめに	4
貢献の評価	5
貢献の方法	6
資本貢献	6
Steem (STEEM)	7
Steem パワー (SP)	7
Steem ドル (SBD)	8
主観的な貢献・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	11
コンセンサス・アルゴリズム	16
Steem におけるコンセンサス	16
取引手数料の排除	17
手数料の問題	17
マイクロペイメントに代わる帯域幅	20
パフォーマンスとスケーラビリティ	23
Reddit スケール	24
配分と供給	25
初期配分と供給	25
現在の配分と供給	26
Steem の力	27
マイクロペイメントは不要、チップは任意	27
価値はリンクにある	28
暗号通貨オンボーディング問題の解決	29
暗号通貨精算の問題の解決	29
	30
検索エンジン最適化による有機的な発見の解決	30
ブロックチェーンベースの帰属への移行	30
広告をブロックチェーンベースのコンテンツ報酬に置き換える	31
結論	31

はじめに

まとめると、ユーザーが作成したコンテンツは Reddit、Facebook、Twitter などのソーシャルメディア企業の株主に何十億ドルもの財産をもたらしました。2014 年 Reddit は、reddit.com に投稿や、コメント、投票によって貢献したすべての人が Reddit, Inc. の株式を公平に受け取った場合、プラットフォームが改善していくという仮設を立てました。*1 Steem は、価値のある貢献を提供する人々に、その価値の大部分を暗号通貨の報酬で返すことにより、ソーシャルメディアとオンラインコミュニティのサポートを目指しています。そしてこのプロセスを通じて、まだ暗号通貨経済に参加していない人々を含む、幅広い市場で通用する通貨を作り出します。

Steem の設計を導くために、いくつかの重要な原則が用いられました。最も重要な原則はベンチャーに貢献したすべての人が、ベンチャーから貢献に比例した所有権、支払い、または債務を受け取るべきだということです。この原則は、すべてのスタートアップ企業において、設立時およびその後の資金調達の場面における株式配分の原則と同じものです。

第二の原則は、すべての形態の資本が同じ価値を持つということです。つまり、貴重な時間を使い、コンテンツの制作とキュレーションに注意を向けて貢献する人は、貴重なお金を使って貢献する人と同じくらい価値があるということです。これはスウェットエクイティの原則であり*2、以前の暗号通貨で多くの場合に数十人以上の人々に提供することが困難であったコンセプトです。

第三の原則は、コミュニティがそのメンバーにサービスを提供する製品を作るということです。この原則は、信用組合や、食品生協、健康保険の例のように、製品やサービスをコミュニティの外に売るのではなく、コミュニティメンバーに提供するということです。

Steem コミュニティはメンバーに以下のようなサービスを提供しています:

- 1. キュレーションされたニュースと解説のソース。
- 2. 個別の質問に高品質な回答を得る手段。
- 3. US ドルにペッグされた安定した暗号通貨。
- 4. 無料の決済手段。
- 5. 他のメンバーにサービスを提供する仕事。

Steem の経済的インセンティブの意図的な再構築は、それ以前のソーシャルメディアや暗号通貨プラットフォームよりも、関係するすべての人々により公平で包括的な結果を生み出す可能性を持っています。本稿では、既存の経済的インセンティブを探り、Steem のインセンティブがどのようにしてほとんどの参加者にとってより良い結果をもたらすかということを証明します。

^{*1} Reddit's Cryptocurrency, Forbes, Erika Morphy, October 2014 http://www.forbes.com/sites/erikamorphy/2014/10/01/reddits-cryptocurrency-could-have-many-uses/#4e07b05332b9

^{*2} Sweat Equity, Investopedia http://www.investopedia.com/terms/s/sweatequity.asp

貢献の評価

Steem は、ソーシャルメディアベースの経済の採用と収益化に対する主要な障壁に対処するために一から設計されました。私たちは主要なソーシャルメディアプラットフォームを成長させたものと同じ技術によって、優れた暗号通貨をブートすることができると主張しています。暗号通貨によって可能になる経済的インセンティブは、新しいソーシャルメディアプラットフォームの成長を劇的に促進するでしょう。それは暗号通貨とソーシャルメディアの相乗効果であり、Steemに市場における強力な優位性を与えると考えられます。

Steem が向き合う課題は、個人の貢献を評価するためのアルゴリズムを導き出すことです。それはそれぞれの貢献の主観的な価値を公平に評価していると、コミュニティメンバーのほとんどが考えるものでなければなりません。完全な世界では、コミュニティメンバーは協力してお互いの貢献の評価と公平な対価を導き出します。実際には、利益のための意図的な操作を防ぐ方法で設計される必要があります。評価システムが広く悪用されると、経済システムの公平感においてコミュニティメンバーの信用を失わせる原因になります。

既存のプラットフォームは1ユーザ、1投票の原則で稼働しています。これはシビル攻撃によってランキングが操作される環境を作り出し、サービスプロバイダは積極的に悪用者を特定しブロックする必要に迫られます。その唯一の恩恵がウェブトラフィックや検閲であるため、人々は既にReddit や Facebook、Twitter の評価アルゴリズムの操作を試みています。

Steem プラットフォームの基本的なアカウントの単位は、STEEM という暗号通貨トークンです。 Steem は1 STEEM、1 投票に基いて稼働します。このモデルでは、アカウント残高によって評価されるプラットフォームへの貢献度が最も大きい人は、貢献の評価方法について最も大きい影響力を持ちます。さらに Steem はメンバーに、権利付与スケジュールに委ねられた STEEM によってのみ投票を認めています。このモデルでは、メンバーは STEEM の価値を長期的に最大化する方法で投票するという経済的インセンティブを持ちます。

Steem は比較的シンプルなコンセプトで設計されています:すべての人のコミュニティへの有意な 貢献は、その付加価値によって評価されるべきです。 有意な貢献をした人々が評価されるように なると、人々は貢献を継続し、コミュニティは成長していきます。コミュニティ内においてギブアンドテイクの不均衡は維持されません。最終的に、提供者は受け手をサポートすることに疲れ、コミュニティから離れていきます。

課題は、無数の人々へ拡大できる方法によって、どの貢献が必要とされていてその相対的な価値は どれくらいかということを識別可能なシステムを作り出すことです。

貢献度を評価し報いるための実績のあるシステムは自由市場です。自由市場は、誰もが互いに取引し、価値や損失によって報酬が割り当てられる単一のコミュニティとして見ることができます。市場システムは他者に価値をもたらす者に報酬を与え、生み出した価値以上に消費する者に罰を与えます。自由市場は様々な通貨をサポートし、お金は単に誰もが簡単に交換できる商品です。

自由市場が実績のあるシステムであるため、コンテンツの消費者が直接制作者に支払う自由市場システムを作ることは良いように見えます。しかし、コンテンツ制作やキュレーションに直接支払うことは非効率であり、実用的ではありません。ほとんどのコンテンツの値段は、経験的、財政的、そしてほとんどの読者がチップを払うことがないということに関連した機会費用に比べて非常に低いです。豊富な無料の代替物により、「有料の壁」を築くことは読者を逃すことになります。読者から著者へ記事毎にマイクロペイメントを実施する試みはいくつかありましたが、どれも普及していません。

Steem は経済の方程式を変更する事によって、あらゆる種類の貢献に効果的なマイクロペイメントを行えるように設計されています。読者は自身の財布から誰かにお金を出すべきかどうか判断する必要はなくなります。その代わりにコンテンツにプラスまたはマイナスの投票を行い、Steem はその投票によって個別の報酬を決定します。つまり、人々は親しまれ幅広く使われるインターフェースを使うことができ、また経験的、財政的、そして従来のマイクロペイメントやチッピングプラットフォームに関する機会費用の問題を気にする必要はなくなります。

Steem が貢献に支払いを正しく割り当てるためには、コミュニティメンバーからの投票が重要です。従って、投票は極めて重要な貢献であり、それ自体に報酬を与える価値があります。Slashdot などのいくつかのプラットフォームでは、誠実なモデレータをランク付けして報酬を出すメタモデレーション*3を用いています。Steem は一つのコンテンツの総合的なプロモーションに最も貢献した人に報酬を出すことを選択します。また、コンテンツ制作者に最終的に支払われた報酬に比例して投票者にも報酬が与えられます。

貢献の方法

このセクションでは、Steem の背後にあるアイデアと Steem コミュニティに有意義で測定可能な貢献をした人々への報酬について概説します。

資本貢献

コミュニティが資本を引き付けるために提供できる2つのものは、債権と所有権です。所有権を購入する人はコミュニティが成長するときに利益を上げ、コミュニティが縮小するときに損失を出します。債権を購入する人は一定の利息を保証されますが、コミュニティが成長することによって実現される利益を分かち合うことはできません。両方のタイプの資本貢献はコミュニティの成長と通貨の価値にとって重要です。さらに、所有権を保有するには流動と権利確定の2つの方法があります。権利確定した所有権は長期的な関係を作り、短期間に売却することはできません。

Steem ネットワークはこれらの異なる種類の資産を、Steem (STEEM)、Steem パワー (SP)、Steem

^{*3} Meta-moderation is a second level of comment moderation. Users are invited to rate a moderator's decision in order to improve moderation.

 $https://en.wikipedia.org/wiki/Meta-moderation_system$

ドル (SBD) と呼びます。

Steem (STEEM)

Steem は Steem ブロックチェーンの基本的なアカウントの単位です。他のトークンの価値はすべて STEEM の価値に由来します。STEEM は流動的な通貨であり、従って取引所で売買することが可能で、また他のユーザーへの支払い方法として転送することが可能です。

Steem パワー (SP)

スタートアップ企業には長期的な資本投入が必要です。スタートアップ企業に投資する人は、株式を売却して利益を現実のものとするまでに数年間待つことを想定しています。長期的な投資がなければ、追加発行した株式を売ることによって資金調達しようとするスタートアップ企業は、資金を引き上げようとしようとしている既存の株主と競合することになります。賢明な投資家は資本貢献によって起業を成長させたいと考えますが、新しい資本が撤退しようとしている人に与えられると、成長は起こり得なくなります。

コミュニティが長期計画を立てるためにも、長期的な関係を持つことには大きな価値があります。 また、ステークホルダーの長期的な関係は、彼らに短期的なポンプよりも長期的な成長のために投 票するように促します。

暗号通貨の世界では、投機筋は主に短期的な成長を予期するものに基いて通貨から別の通貨へと移行していきます。Steem は主に長期的な観点を持つ人々によって所有され、完全に制御されるコミュニティを築きたいと考えています。

ユーザーは STEEM を 13 週間の権利付与スケジュールに委ねることができ、プラットフォーム内で付加的な利益を得ることができます。13 週間の権利付与スケジュールに委ねられた STEEM は Steem パワー (SP) と呼ばれます。SP 残高は自動的に繰り返される変換要求を除いて、転送や分割はできません。つまり、SP は暗号通貨取引所で容易に取引できるものではありません。

ユーザーがコンテンツに投票したとき、報酬プールの分配への影響力は保有する SP の量に比例します。より多くの SP を持つユーザーは報酬の分配により多くの影響力を持ちます。つまり、SP は Steem プラットフォーム内で、保有者に排他的な権限を認めるアクセストークンです。

また、SP 保有者は権利が続いている SP 残高に対して利息を支払われます。年間 15% のインフレ で SP 保有者に利息が支払われます。受け取る利息の量は、すべてのユーザーが権利確定させた総 SP 量に対する相対的な保有 SP 量に正比例します。

STEEM から SP への移行は「パワーアップ」と呼ばれ、SP から STEEM への移行は「パワーダウン」と呼ばれます。パワーダウンした SP は、パワーダウンが始まって 1 週間後から、13 等分の支払いで 13 週間に渡ってユーザーの元へ返ります。

Steem ドル (SBD)

安定性はグローバル経済が成功するための重要な要素です。安定性がなければ、世界中の人々は商業と貯蓄に対して認知コストを低くすることはできませんでした。安定性が経済を成功させるための重要な要素であることから、Steemドルは暗号通貨の世界と Steem ネットワークを使う個人に安定性をもたらすための試みとして設計されました。

Steem ドルはスタートアップ企業の資金調達によく使われるコンバーチブルノートと同じ仕組みで作られています。スタートアップの世界におけるコンバーチブルノートは、将来(典型的には資金調達の時に)決定されるレートで所有権に転換できる短期債権型証券です。ブロックチェーン上のトークンはコミュニティにおける所有権とみなすことができますが、コンバーチブルノートは他の商品や通貨建ての債権とみなすことができます。コンバーチブルノートの規約により、保有者は最小の通知によって公正な市場価格で、保証されたトークンに変換することができます。トークンに変換可能なドルを作成することにより、ブロックチェーンはトークンホルダーの利益を最大化しながらネットワーク効果を高めることができます。

Steem ドルは Steem Blockchain Dollars の頭文字から SBD で表されます。SBD を作成するには、信頼できる価格フィードと悪用を防止するためのルールが必要です。信頼できる価格フィードを提供するには3つの要素を必要とします:不適切なフィードによる影響を最小化することと、不適切なフィードを生み出すコストを最大化することと、タイミングの重要性を最小化することです。

不正なフィードを最小化する

SP の保有者は価格フィードを公開する証人と呼ばれる人を選出します。選出された証人は、フィードの質に関心のある人々からおそらく信頼されていることでしょう。選出された人々に報酬を支払うことによって、Steem はフィードを作成する権利を得るための市場競争を作り出します。フィード作成者への支払いを大きくするほど、誤情報を公開することによって失うものも大きくなります。

信頼を得て選出されたフィード作成者たちにより、フィードの中央値によって変換に実際に使用される価格を導き出すことができます。この方法では、少数のフィード作成者が異常値を与えた場合には、彼らの評価に影響を与えつつも、実際の中央値への影響はほとんどありません。

また、すべてのフィード作成者が誠実であっても、過半数のフィード作成者が自身でコントロールできない事象の影響を受ける可能性はあります。Steemネットワークはコミュニティが積極的に問題解決に取り組みつつ、短期間のフィード中央値の異常は容認するように設計されています。修正に時間のかかる問題の1つの例に、短期間の市場操作があります。市場操作は長期間維持するのが難しくお金がかかります。もう1つの例を挙げると、集中型取引所の障害、または取引所から異常なデータが公開されることです。

Steem は、3.5 日間の価格中央値を用いることで短期間の価格変動を排除します。公開フィードの中央値は毎正時にサンプリングされます。

価格フィードの異常が中央値を取る時間枠の半分未満である限り、変換価格への影響は最小限に抑えられます。フィード異常が発生した場合、ネットワーク参加者は実際の変換価格に影響を及ぼす前に異常フィードの作成者への投票を外すことができます。恐らくもっと重要なことは、フィードが価格に影響し始める前に、フィード作成者に問題を検出して修正する機会を与えることです。

3.5 日の枠により、コミュニティメンバーには問題が起きてからおよそ 1.5 日の対応期間が与えられます。

タイミング攻撃を軽減する

市場参加者はブロックチェーンの 3.5 日間の中央値による変換価格が反応するよりも早く情報を得ることができるでしょう。トレーダーがこの情報を用いてコミュニティに負担を強いて利益を得ることもあり得ます。STEEM 価格が急騰した場合、トレーダーは最小限のリスクで、古い低い価格で SBD の変換を要求し、STEEM を新しい高い価格で売るということもできるかもしれません。

Steem はすべての変換要求を 3.5 日遅らせることで条件を平等にします。このため、トレーダーもブロックチェーンも変換が実行される時点における価格について優位性のあるどのような情報も持っていません。

変換の悪用を最小限に抑える

もし双方向に自由に変換できるならば、価格を変えずに大量のトレードを行えることから、トレーダーはブロックチェーンの変換レートを利用することができるでしょう。価格の大幅な上昇を見たトレーダーは、高値で SBD を変換し (この時最もリスクが高い)、補正された後に再変換することでしょう。Steem プロトコルは SBD から STEEM への変換のみを許可することによって、この種の悪用からコミュニティを守ります。

ブロックチェーンは SBD の作成方法とそのタイミング、及び誰が手にするかを決定します。これにより SBD 生成率が安定し、悪用手段の大部分を排除します。

所有権への持続可能な債務比率

トークンが全体供給量の中における所有権とみなされる場合、トークン変換可能ドルは債権と見なされます。所有権への債務比率が大きすぎると、通貨全体が不安定になる可能性があります。債権の変換はトークンの供給を劇的に増やし、次にマーケットで売られ、価格を抑制します。その次の変換では更に多くのトークンの発行が必要となります。放置すると、負債の山の裏で無価値な所有権を残してシステムは崩壊します。所有権への債務比率が高くなるほど、新規の投資家は投資したくなくなっていきます。

STEEM の急激な価格変動は、劇的に所有権への債務比率を変える可能性があります。ブロックチェーンは所有権への債務比率が高くなりすぎることを防止するために、債務水準が 10% を越える場合、SBD 変換で得られる STEEM を削減します。SBD 債務額が STEEM の時価総額の 10% を越えたとき、ブロックチェーンは変換により生成される STEEM 量が時価総額の 10% 以下になるよ

うに自動的に引き下げます。これにより、ブロックチェーンの所有権への債務比率が 10% を越えることは決してありません。

STEEM 生成の計算で使用されるパーセンテージの下限は、すべての未処理の SBD と SP の (現在のレート / フィードによって決定される) STEEM 値を含む供給量に基いて決められます。

利息

SBD は保有者に利子を支払います。利率は変化する市場の状況に対応するために価格フィードを公開するのと同じ人々が設定します。すべての債権は貸し手にリスクを与えます。SBD を精算せずに保有している人は、コミュニティに効果的に1ドル分の価値を貸しています。保有者は、将来のある時点でSBD を1ドルで買う誰かや、変換して得た STEEM を買う投機家や投資家がいることを信じています。

STEEM や SP の保有者は、コミュニティメンバーが SBD を保有しようとする際に影響力を得ます。この影響力は成長によって増大し、また成長にも貢献します。STEEM の価格が下がり希薄化が進むと、保有者は苦しむことになります。暗号通貨プロジェクトは、資本によりネットワークを信頼するユーザー数の増加による利益は、最終的には景気後退時の希薄化よりも多くの価値をもたらすことを示しています。

価格フィードの設定

賢明な読者は、有限供給量の有利子資産が、同じ資産において利益を得る他の機会に応じて、基本的な資産よりも高値または安値で取引されることを認識しています。USドルにペッグされた資産に高い金利が支払われると、Steemドルの供給が減少し、1ドルの価値がなくなるまで多くの人々が人々が値を競り上げるでしょう。経済学において国際金融のトリレンマ*4として知られる原則は、以下の3つを同時に実現することは不可能であることを述べています:

- 1. 安定した為替レート
- 2. 自由な資本移動
- 3. 独立した金融政策

Steem のフィード作成者が、Steem ドルの作成と破壊を可能にすると同時に、金利を完全に制御することを可能にする独立した通貨政策を目指すならば、彼らは問題に直面するでしょう。トリレンマによると、Steem ドルは資金移動を制限するか、対ドルの不安定な為替レートを受け入れるか、金利の制御を限定的とする必要があります。

Steem フィード作成者にとって最も重要なことは、SBD と米ドル (USD) の間で安定した 1 対 1 の変換を維持することです。SBD が常に \$1.00 以上で取引されている場合は、利息の支払いを停止する必要があります。 利率 0% の債権に対してプレミアムを要求し続けている市場においては、コミ

^{*4} The Impossible Trinity, economic theory https://en.wikipedia.org/wiki/Impossible_trinity

ュニティが考えている債権よりも信用を拡大したいと言うのは安全です。これが起こると、SBD は \$1.00 以上の価値を持ち、マイナス金利を課す以外にコミュニティができることは殆どありません。

所有権への債務比率が低く、SBD が \$1.00 未満で取引されている場合は、利率が引き上げられます。これは人々に SBD をもっと保有するように促し、価格を支えます。

SBD が \$1.00USD 未満で取引され、所有権への債務比率が高い場合は、SBD あたりに与えられる STEEM が増えるようにフィードを調整します。これは SBD の需要を増やし、同時に所有権への債務比率を下げ、SBD を USD と等価に戻します。

Steem が新しく生成する SBD 量よりも STEEM 価値の成長速度が高いと仮定すると、所有権への債務比率は目標比率以下を保ち、すべての人が利息の利益を得られます。ネットワークの価値が横ばいまたは下落している場合、利息の提供は所有権への債務比率を悪化させるだけです。

実際、フィード作成者は USD との安定したペッグを維持するために通貨ポリシーを設定する責任を委ねられています。この力を悪用すると、STEEM の価値を傷つけることになるため、SP の保有者は上記の規則に従って価格フィードと利率を調整することを期待できる証人に投票するのが賢明です。

所有権への債務比率が危険なほど高くなり、市場参加者が変換要求を避けている場合は、変換する SBD に支払われる STEEM の比が大きくなるようにフィードが調整されます。

利率のポリシーまたは STEEM/SBD 変換比率に対するプレミアム/ディスカウントの変更は、短期的な市況に対応しようとすることよりも、長期的な平均偏差の反応を測りながら緩慢に行われるべきです。

これらの規則により、\$1.00 で購入した SBD を保有することによって損失が生じないという信頼を市場参加者に与えられると確信しています。私たちは通常の市況の下で SBD が、\$0.95 から \$1.05 の狭い範囲で取引されることを全面的に期待しています。

主観的な貢献

主観的なプルーフ・オブ・ワークは、マイニングのような完全に _ 客観的な _ プルーフ・オブ・ワークシステムを改善した通貨を分配するための別のアプローチを提示します。 _ 主観的な _ プルーフ・オブ・ワークを実装した通貨の適用は、十分に定義された目的を持つどのようなコンセプトのコミュニティ構築にも適用できるためため、 _ 客観的な _ プルーフ・オブ・ワークシステムよりも遥かに広範です。個人がコミュニティに参加する際、彼らは特定の一部の考えに賛同し、コミュニティの価値や目的を強化するために投票することができます。

実際、評価される仕事の基準は完全に主観的であり、その定義はソースコードの外に存在します。 あるコミュニティは芸術家や別の詩人、別のコメディアンに報酬を与えたいと望むかもしれません。他のコミュニティは慈善目的や政治的な課題の前進のために報酬を出すことを選ぶかもしれません。 各通貨が到達する価値は、特定のコミュニティ内部における影響の需要と、各コミュニティがどこまで大きくなるかという市場の予測に基づきます。従来のシステムとは異なり、主観的なプルーフ・オブ・ワークは価値のあるどんなものの開発にでも資金を集めることを可能とし、従来は収益化できなかった時間の収益化を可能にします。

通貨の分配

人々が暗号通貨コミュニティに関わるには2つの方法があります: _ 買うこと _ と _ 働くこと _ です。どちらの場合でも、ユーザーは通貨に価値を与えます。しかし、大多数の人々は _ 余分なお金 _ よりも _ 自由な時間 _ を持っています。実際の _ お金 _ はないが、 _ 時間 _ ならば豊富にある貧しいコミュニティの通貨を立ち上げるという目標を想像してみてください。人々が他の人のために働くことでお金を得ることができれば、公正な会計 / 通貨システムによって促進された相互交換を通して自ら価値を高めることになります。

一般に公平と認識される方法によって、可能な限り多くの人々に通貨を分配することは困難なこととされています。客観的なコンピュータアルゴリズムによって完全に評価することが可能なタスクは本質的に限られており、一般的に言えば、外部の利益は制限されます。ビットコイン形式のマイニングの場合、特別なハードウェアが生産され、より効率的なアルゴリズムを開発するために時間を費やすことになります。それは素数を見つけるために役立つかもしれませんが、社会や大規模な通貨保有者コミュニティに意味を持つ価値を提供することはありません。さらに重要な事は、規模の経済と市場の力は最終的に、この手の流通に参加する専門家を除いたすべての人を排除してしまうことです。結局、計算ベースのマイニングは、計算に必要な電気代やハードウェアの開発にお金を払う必要があるため、_ 買うことによる参加 _ の別の形に過ぎません。

すべての人に参加とお金を稼ぐことの均等な機会を与えるには、人々には働く機会を与える必要があります。課題は個人が提供する仕事の相対的な質と量をどのように判定するのかということと、何百万人ものユーザーに効率的に報酬を分配する方法です。これにはスケーラブルな投票プロセスの導入が必要です。特に、資金を分配する権限は分散し、可能な限り分権的である必要があります。

何百万人ものユーザーに報酬を出すための最初のステップは、実際に行われた仕事の量やユーザーの投票方法とは無関係に一定額の通貨を分配することです。これは、疑問を_「支払うべきか?」から「誰に支払うべきか?」」に変えます。また、お金が流通し、最も多くの_仕事_に「入札」する人へ売られていることを市場に知らせます。これはビットコインが最も難しいハッシュを見つけた人に 50BTC を与えることと似ています。ビットコインのように、すべての仕事は支払いの前に行われていなければならず、将来の仕事の約束の上で推測により支払われるべきではありません。

次のステップは、間接的にポジティブな _ あること _ をしている人も含めて、何かをしているすべての人に報酬を出すことです。これは、すべての行われた仕事をランク付けし、その値に比例して分配することによって成し遂げられます。市場の競争が激しくなるほど、同じ報酬を得るのが難しく(より高い質または量に)なります。

通貨分配の投票

分配する決められた量のお金があり、しかも将来の価値と通貨の有用性に長期的に強い関心を持つ者が、どのように配分するかを決めなければならないということを想定してください。権利を持つすべてのユーザーは誰が最も良い仕事をしたのかについて票を投じ、結局のところ、1日分のお金は投票に比例して分配され、正味1票の賛成票を持つすべての人が何かを得られるようになります。

単純な投票プロセスは N 人の囚人のジレンマ*5を生み、それによって個々の投票者は、コミュニティの大きな目標に反して自分自身のため投票するインセンティブを持ちます。もし、すべての投票者が自分自身に投票してから離脱すると、通貨はやがて流通しなくなり、通貨全体がネットワーク効果を得られなくなります。一方、1 人の投票者だけが離脱した場合は、その投票者は通貨の全体価値にはほとんど影響を与えずに不相応な利益を得ることができます。

■投票の濫用

誰がどのくらいのお金を持っているのかに関わらず、常に同じくらいの財産を持つ人々がたくさんいます。最も裕福な人であっても、次に豊かな2人を合わせたのよりも多くを持つということは滅多にありません。さらに、コミュニティに多額の投資をしている人々は、自身のために投票システムを操作しようとすることによって、最も多くを失うことになります。それは企業のCEOが給料の支払いをやめてしまうようなもので、そのとき彼はすべての利益を自分の懐に収めることができます。誰もが他の会社で働くために去っていき、会社は無価値になり、残ったCEOは裕福にはならず破産します。

幸運にも、多くの投票が集中している作品は、最も吟味 (宣伝) されることにもなります。_ 否定的な投票 _ を追加することにより、多数の小規模なステークホルダーは、共謀集団や離脱する大規模ステークホルダーの投票力を無効化することが可能になります。さらに、大規模ステークホルダーは濫用によって通貨の価値が下落した場合、自身への投票によって得られるものよりも多くを失います。実際、誠実な大規模ステークホルダーは、小さな貢献に投票するよりも濫用を監視し否定投票を使用するようになる可能性が高いです。

人々をシステムの濫用から守るために _ 否定的な投票 _ の使用には、ある個人が他のすべての人を犠牲にして利益を上げていると認識されたとき多くの人々が持つ _ クラブメンタリティ _ を利用します。クラブメンタリティ (カニ精神) は通常、近視眼的な人々が善良な人々を抑えつけることを指しますが、それはまた善良な人々が悪い人々を抑えることをも可能にします。クラブメンタリティの唯一の「問題」は、誰かが他の人の支出で利益を得ていると人々が _ 誤って信じている _ 場合です。

バケツの中のカニの話*6

^{*5} N-Person Prisoner's Dilemma

https://cs.stanford.edu/people/eroberts/courses/soco/projects/1998-99/game-theory/npd.html

^{*6} The Story of the Crab Bucket

ある男が浜辺を歩いていると、サーフフィッシングをしている別の男がいて、その横には餌の入ったバケツが置いてありました。彼が近付くと、餌のバケツには蓋がなく生きたカニが入っていることがわかりました。

「なぜカニが逃げないように餌のバケツに蓋をしないのですか?」と彼は言いました。

「あなたはわかっていない」と男は返事をしました。「バケツの中に1匹のカニがいる場合は、そのカニは間違いなく素早く這い出してしまうでしょう。ですが、バケツの中にたくさんのカニがいる場合は、一匹が側面を這い登ろうとすると、それを他のカニが掴み、元の場所へ落としてしまいます。そしてそのカニは他のカニと同じ運命を辿るでしょう」

つまり、それは人々についても一緒です。1人がなにか違うことをしたり、評価を上げたり、自身を向上させたり、環境から逃げ出したり、大きな夢を見たりしようとすると、他の人々はその人を引き戻して運命を共にしようとします。

「濫用」を排除することは不可能であり、それを目標にするべきではありません。システムを「濫用」しようとしている人でさえ、仕事をしているのです。彼らが濫用や共謀に成功することで得た報酬は、少なくとも、従来のビットコインマイニングやマイニングプールを介した集団マイニングで採用されたやらせ仕事のシステムとして、通貨を分配する目的のためには価値があります。必要なことは、濫用が横行しすぎないようにし、コミュニティと通貨を支える本物の仕事へのインセンティブを損なわないようにすることです。

コミュニティ通貨構築の目標は、より多くの「カニをバケツに入れること」です。すべての濫用を排除するために極端な対策を行うことは、数匹のカニが逃げ出さないようにバケツに蓋をしようとすることであり、その代償としてバケツに新しいカニを追加することを困難にしてしまいます。壁を滑りやすくし、カニに他のカニが逃げ出すのを阻止する力を与えるだけで十分なのです。

レート制限投票

濫用を最小化するための主要部分は、投票のレート制限です。個々のユーザーは、1日に限られた数の作品しか読んで評価することができません。それ以上の頻度で投票しようとするのは、自動化や潜在的な濫用の兆候です。レート制限により、より高頻度で投票するステークホルダーの投票は低頻度で投票するステークホルダーの投票より少なくカウントされます。複数のアカウントにトークンを分割しようとしても、影響力も分割されるため、正味の影響力が増加することも、投票に課されるレート制限を回避することもできません。

ユーザーには一定の投票力が割り当てられます。与えられた作品にどれくらいの報酬プールを割り当てるのかを決定するには、投票力にユーザーが持つ権利トークンを乗じます。投じられたすべての票は残っている投票力の割合を使用します。ユーザーはより多くの投稿に投票することもできますが、各投票は価値が薄くなり、最大の投票力を再び得るには長い時間がかかるようになります。投票力は1日に20%の固定速度で充填されます。

支払いの分配

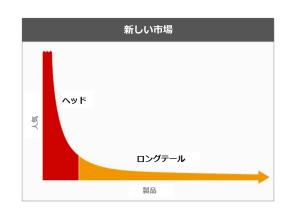
Steem の報酬システムの主な目標の一つは、インターネット上に最高の議論を作り出すことです。 毎年、年間インフレの 75% がコンテンツを投稿、投票、そして議論するユーザーに分配されます。 ビットコインの規模では、トップ貢献者には毎日数百万ドルが与えられる可能性があります。

実際の分配はユーザーの投票パターンに依存しますが、報酬の大部分が最も人気のある投稿に分配 されるだろうと私たちは考えています。

ジップの法則* 7 は驚くべき範囲の実世界の現象を非常によく特徴付けている経験的な法則の一つです。それによれば、大きな集合を大きさや人気で整理すると、2番目の要素は1番目のもののおよそ半分の程度になり、3番目のものは1番目のもののおよそ $^1/3$ の程度になります。一般に、k番目の項目は1番目のもののおよそ $^1/k$ の程度になります。

価値の大まかな尺度として人気を取ると、個々の項目の価値はジップの法則で与えられます。つまり、100 万の項目があれば、最も人気のある 100 の項目が全体の価値の 1/3 に寄与し、次の 10,000 が別の 1/3、残りの 989,900 が最後の 1/3 になります。n 個の項目の集合の価値は $\log(n)$ に比例します。

この投票と報酬分配の効果は、良いコンテンツ に大きな報酬を与える一方で、ロングテールの 貢献をする小規模なプレイヤーにも報酬を出すことです。



この経済効果は宝くじに似ています。それは人々が投票を得る確率を過大評価し、報酬の期待値以上の仕事をし、それによってコミュニティのために行われる仕事量を最大化します。すべての人が「何かを獲得する」という事実は、カジノで人々が賭け続けるのと同じ心理を刺激します。換言すれば、小さい報酬によって、もっと大きい報酬を得ることが可能だという発想が強くなります。

支払い

投稿が支払いを受けるとき、50%SBD と 50%SP の形を取ります。Steem パワーはユーザーに投票 と取引の力を与え、SBD は安定した通貨ですぐに利益を与えます。既に長々と議論したように、SP は短期的な売却ではなく長期的な保有を促すように設計されています。これは多くのユーザーに、プラットフォームの長期的な成長に強い関心を持つように促します。

また、ユーザーは支払いの 100% を SP で受けることを選べるほか、投稿の支払いを辞退すること

^{*7} Zipf's Law

もできます。ユーザーが投稿の支払いを辞退すると、支払われるはずのお金は報酬プールに残り、 他のユーザーに分配されます。

コンセンサス・アルゴリズム

コンセンサスはコミュニティが広く認識され、一定量の情報について明確な合意に達するプロセス です。誰が何を所有しているのかについてコンセンサスに至るために、社会が開発した様々なアル ゴリズムが存在しています。地球上のすべての政府は、全住民が憲法に記された一定の規則を遵守 することに合意することによる、原始的なコンセンサス・アルゴリズムです。政府は裁判所、裁判 官、陪審員を設置し、客観的な事実を解釈して最終的な決定を下します。殆どの場合、人々はそれ が誤りであっても決定に従います。

暗号通貨で使用されるアルゴリズムはコンセンサスに至るための良い方法を提供します。個人から の暗号で署名された証言は、事象の絶対的な全体的順序を確立する公開台帳に記載されます。決定 論的コンピュータアルゴリズムはこの台帳を処理して、普遍的に受け入れられる結論を導き出しま す。コミュニティのメンバーが処理アルゴリズムに合意している限り、アルゴリズムの結果は信頼 できます。

主要な考慮点は、どの証言が公開記録に受け入れられるのかを決定することです。システムは検閲 の可能性を最小限にするように設計されるべきです。公開台帳における検閲は、誰かに選挙で投票 させないようにすることと似ています。どちらの場合も個人は全体的なコンセンサスに影響を与え ることができません。

Steem におけるコンセンサス

概念的には、Steem で採用されたコンセンサス・アルゴリズムは、世界中の企業で採用されている コンセンサス・アルゴリズムに類似しています。Steem の将来的な価値に強い関心を持つ人々は、 公開記録に責任を持って証言を含める個人を選ぶように投票します。投票は各個人が持つ既得権に 比例して重み付けされます。

暗号通貨の世界では、公開記録は一般に _ ブロックチェーン _ と呼ばれます。 _ ブロック _ は署 名された取引の集合です。

Steem ではブロック生成はラウンドで行われます。各ラウンドで21人の証人が選ばれ、取引のブ ロックの生成と署名を行います。これらの証人の内20人は承認投票で選ばれ、1人はトップ20に 入れなかった各証人から総投票数に比例して時分割されます。21人のアクティブな証人が毎ラウ ンドシャッフルされ、1人の証人が特定の証人によって生成された1つ前のブロックを常に無視し 続けることを防止します。ブロックを逃し過去 24 時間以内に生成していない証人は、ブロック署 名キーを更新するまで無効になります。

このプロセスは最高の信頼性を提供するのと同時に、トップに立つのに十分な投票を得られるほど の人気があるかどうかに関わらず、誰もがブロック生成に参加できるという可能性を保証するよう 16

に設計されました。人々には選出されたトップ 20 の証人による検閲に打ち勝つための 3 つの選択 肢があります: トップ 20 に入らないすべての人と一緒に辛抱強く待つか、もしくは SP を購入して投票の力を増すか。一般に、検閲は選出された証人が仕事を失うための近道となります。従って Steem ネットワーク上では重要な問題になることはまずありません。

アクティブな証人は事前にわかっているため、Steem は 3 秒毎にブロックを生成するように証人をスケジュールすることができます。 証人は NTP プロトコルでブロック生成を同期させます。 このアルゴリズムの変形は BitShares ネットワークで 1 年以上使用されており、信頼性が証明されています。

取引手数料の排除

Steem はネットワークに貢献する人々に報酬を出すために尽力します。人々がコミュニティとやり取りをする度に課金するのは逆効果になるでしょう。

現在、ブロックチェーン技術は取引手数料によってスパムを防止しています。これらの手数料は少額取引における既知の問題すべてを被り、ブロックチェーンが少額の取引に使用されるのを阻みます。真に分散化したアプリケーションは、集中化された競合相手と競争するには、ユーザーに外見上は無料であるように見せる必要があります。本稿では手数料の必要性を排除するための Steem におけるアプローチを概説しており、それによって以前は困難であった分散化アプリケーションを広い範囲で可能にします。

手数料の問題

ブロックチェーンは分散化されたネットワークであり、すべての取引はすべてのピアに発信されます。時々生成されるブロックは、保留中の取引の一部または全部を含みます。すべてのブロックチェーンは、悪意あるユーザーが無意味な取引でネットワーク容量を消費し尽くしてしまうのを防ぐための解決策を見つける必要があります。無意味な取引は他の意味のある取引が処理されるのを阻み、最終的にネットワークを破壊します。

これまでのほとんどのブロックチェーンが採用した解決策は、最低限の取引料金を課すことです。ネットワークへの攻撃を高価で無益なものにするには僅か数セントの手数料で十分です。このアプローチはスパム問題を解決しますが、新しい問題をもたらします。すべての電子メールに少額の料金を課すことでスパムメールの問題を解決しようとすることを想像してみてください。誰も電子メールを使わなくなるでしょう。

マイクロペイメントはうまくいかない

取引に手数料を課すことの基本的な問題は、マイクロペイメント、特に価値の低いユーザー行動に 対するものが機能しないことです。すべての取引に手数料がかかる場合、分散ネットワークが処理 できる取引の種類が制限されます。手数料の必要性に関してどのような合理的な議論が行われたとしても、ユーザーは自分のすべての行動に対して少しずつ出費があるということを嫌います。

私たちが毎日使用するウェブサイトが、アカウントのパスワード変更を行う毎に手数料がかかるということを想像してみてください。ユーザーは一定のものが無料であることを期待しています。ある行動に少額の手数料がかかるかどうかをユーザーに判断させることは、ユーザー離れの原因となる懸念を生みます。取引は決断を必要とするほど価値があるわけではありませんが、自動化できるほど小さい価値というわけでもありません。どんなに小さいものであっても、それを買う決断をする際はある程度の不安があります。それはユーザーインターフェースやかかる時間に由来するものではなく、まさに決断する行為そのものに由来します。

マイクロペイメントは、すべての支払いと同様に比較を要します: _ 「X には Y の価値があるか?」 _ ユーザーが何も考えずに承認できる取引だけが、コストがかからないものですが、それは取引ではありません。そのため、この事実によって作られた取引の精神的なコストには、最適化によって除去しきれないものがあります。

- クレイ・シャーキー*8

金融決済の世界では、取引が手数料に対して高額であり、買い手は既に購入を決断しているため、 少額の手数料が容認されています。潜在的なブロックチェーンアプリケーションの世界は、単なる 金融決済よりも遥かに大きく、必要な取引にユーザーが手数料を容認しないようなものを多数含み ます。

BitShares、Nxt、Ripple、Counter Party、Stellar のようなシステムはすべてユーザーがブロックチェーン上に指値注文を置くことができ、そのすべてがユーザーの行動に対して少額の手数料を課します。その後、ユーザーが注文を取り消そうとすると、もう一度手数料が課されます。Ethereum のようなシステムはマイクロペイメントを全く新しい段階にします: 計算毎の課金。分散型検索エンジンが検索毎に少額の手数料を課す場合に Google からユーザーを引き込むのに苦労するだろうということと同じ理由で、これらのすべてのシステムは新しい主流ユーザーを引き込むのに苦労しています。それはサービスがどれほどすばらしいかということとは関係ありません。人々は一定のものが無料であることを期待しています。これはユーザーが別の料金体系の下でより全体的な支払いを終わらせたとしても当てはまります。

手数料は参加の障壁

どのような手数料も新規ユーザーの参加の障壁となります。Ethereum を体験するにはまず ETHトークンを取得する必要があります。Ethereum 上で分散アプリケーションを構築しようとする人は、顧客にコストを転嫁する必要があります。暗号通貨の購入は簡単な作業ではなく、10 ドル未満の金額にはほとんど意味がありません。つまり、新しい分散アプリケーションを試してみたい新規ユーザーは、まず 10 ドルを手放すことに納得しなければなりません。

^{*8} Clay Shirky, The Case Against Micropayments http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html

手数料の変更

時間とともにネットワークは手数料を調整しなければなりません。これは、トークン価値の上昇または容量の増加によって起こることがあります。ユーザーは予測可能な料金と保証されたサービスを好みます。使用料の多い時間に動的に手数料を変更することも可能ですが、ユーザー・エクスペリエンスの低下を招きます。

シビル攻撃

集中型ウェブサイトは帯域制限や ID 認証によってスパムを防ぎます。reCAPTCHA*⁹のような単純なものでも偽アカウントの作成を制限するのには十分です。誰かがアカウントを悪用すると、集中型ウェブサイトは自由にアカウントをブロックできます。

分散型システムでは、ユーザーを直接 BAN することや、集中型プロバイダが reCAPTCHA をホストしてアカウントの帯域制限を行うことはできません。実際、ユーザーを検閲できないことがブロックチェーン技術のセールス・ポイントの一つです。

完全準備 vs 部分準備

町内すべてのケーブルを所有し、いつでも提供できる帯域幅には上限があるインターネットサービスプロバイダ (ISP) 協同組合のようなブロックチェーンを考えてみましょう。街に住む人々は ISP の株を買うことができ、その代わりに有効な帯域幅の一部を利用する権利を得ます。

ISP には「完全準備」システムまたは「部分準備」システムの2つの選択肢があります。完全準備システムでは、各ユーザーは最大帯域幅から所有する株に比例したほんの一部しか利用できません。誰もが同時にインターネットを使用しているわけではないため、町のネットワークは十分に活用されないでしょう。

部分準備システムでは、すべてのユーザーが同時にインターネットを使用していない限り、各ユーザーはいつでも使う権利のある帯域幅より多くを利用できます。部分準備の運用上の問題は、想定よりも多くの人々が同時にネットワークを使用しようとした場合に常に輻輳が発生することです。 ISP には輻輳時に帯域幅を優先順位付けする方法が必要です。最も極端な場合、ネットワークが完全に輻輳している場合は完全準備システムに戻す必要があります。課題は適切な部分準備率を設定することです。

^{*9} reCAPTCHA, Easy on Humans, Hard on Bots https://www.google.com/recaptcha/intro/index.html

マイクロペイメントに代わる帯域幅

マイクロペイメントにおける問題の解決策は_動的部分準備_の実装です。このモデルでは、ブロックチェーンは輻輳時にネットワークの準備率を自動的に調整します。ブロックチェーンは短期的な需要の急増に対して十分なヘッドルームを残すように目標利用量を設定します。需要の高まりが長引く場合、ブロックチェーンはステークあたりの最大帯域幅を減らします。需要の高まりが終わり容量に余剰がある場合は、ブロックチェーンは緩やかにステークあたりの帯域幅を増やします。

個々のユーザーが使用する帯域幅は、ユーザーが使用量を時間シフトできるように適切な長期間に渡って測定する必要があります。ユーザーはログインしてから一度に多くのことを行い、そしてログアウトするという傾向があります。つまり、彼らの短時間の帯域幅は、長期間で見た帯域幅よりも遥かに大きく見えます。時間窓を拡大しすぎると、準備率は短時間の急増に対して十分な早さで調整することができず、また時間窓が短すぎると通常のユーザーにはクラスタ化された利用量の影響が大きすぎます。

私たちの見積りでは、ユーザーの毎週の平均帯域幅利用量を測定すれば十分です。ユーザーが取引に署名する度に、その取引は各個人の移動平均に組み込まれます。ユーザーの移動平均が現在のネットワーク制限を超過すると、平均が制限値を下回るまで取引は遅延します。

容量の影響

ブロックチェーンの容量には上限があるとは限りません。インターネットインフラの技術力の範囲内で、ビットコインのブロックサイズを 10MB に拡大して最小の必要残高を 1/10 に減らすことができます。現在、ビットコインは毎秒 3 トランザクションをサポートしています。別実装では毎秒1000 トランザクション以上が可能です。

手数料との比較

25 ドル相当の BTC を持つユーザーが、毎週取引を行い 0.04 ドルの手数料を毎回支払っていると 仮定すると、そのユーザーは毎年 2 ドル以上の手数料を支払うことになります。ユーザーはただ手 数料を取り戻すためだけに、その 25 ドルで 8% の収益率で稼ぐ必要があります。ユーザーがとに かくブロックチェーン上に自身のお金を貯めようとしていたとすると、25 ドル相当の BTC を持つ このユーザーは手数料ベースのアプローチよりも帯域制限アプローチを選んで年間 2 ドルを節約します。175 ドルの場合、毎日取引することができて、また年間 14 ドルを節約できます。

アカウント作成

Steem の残高を公知としたアカウントベースのシステムは、帯域幅ベースのレート制限アルゴリズムの実装を単純にします。残高が週に1回取引するために必要な最小値を下回るアカウントは取引できません。これは、すべての新規アカウントにはこの最小残高以上の資金が必要であるというこ

とを伴います。また、少額の取引をしようとしているユーザーは、大きい残高を保有しアカウント を再利用している限り、それが可能です。

ネットワーク使用率の低い時に作成された低残高のアカウントは、使用率が高くなった場合にアクセスできなくなる可能性があります。その資金は、大き目の残高を一時的にアカウントに委託することによっていつでも回収することができます。

ハングアップするアカウント数を最小にして合理的なユーザー・エクスペリエンスを維持するには、すべての新規アカウントは毎週の取引に必要な最小残高の10倍を持ってスタートするべきです。この方法により、需要が10倍に増加してもアカウントは使用可能なままです。

シビル攻撃の可能性があるため、初期アカウントの残高はトークン生成からではなく、アカウント 作成ユーザーから付与しなければなりません。

最小残高の正当化

ユーザーが最小残高を維持しなければならないというコンセプトは、ユーザーの価値から自然に生じます*10。事業を営んでいる人なら誰でも、各ユーザーには大きな価値があることを知っています。企業はユーザー獲得のために 30 ドルから 200 ドルを出費しています。ユーザーに直接支払うこともあれば、広告費として支払うこともあります。また、ユーザーベースを手に入れるためだけに企業を丸ごと買うことさえあります。企業はユーザーを獲得した後には、他の手段で収益化する間ユーザーを引き止めるために、多くの _ 無料サービス _ を提供することがよくあります。

Ripple はアカウント資源の使用にあわせて変化する最小残高を使用し *11 、新規アカウントはこの最小残高以上の資金を入手する必要があります。現在、この最小残高は約0.15ドルであり、私たちが毎週1回の取引を自由にできる残高として見積もった0.10ドルを上回っています。

ブロックチェーンは最小残高を要求するシンプルなプロセスによって、ユーザーあたりの最小価値を決定することができます。ブロックチェーンに新しい顧客を呼び込みたい企業は、ユーザーのアカウントに取引を可能とするための最小残高を事前に入れておくことができます。新規登録ユーザーに比較的大きい料金 (1.00 ドル) を要求すると、無料アカウント提供者はブロックチェーンに登録する前に、各アカウントの質と唯一性を検証しなければなりません。

最小残高を維持するということは、残高から得られる利子で取引手数料を払うということと実質的に同じことです。最小残高は比較的短い期間において手数料を支払うのに十分な利子を得るのに必要な残高です。

幸い、最小残高は1ドル程度に低くすることができ、これはユーザーの理解を得られるものです。 利子を得られないということによる機会費用には少額手数料とは違って認知コストがなく、よりユーザーに受け入れられやすいものです。

^{*10} Forbes, Tristan Louis, "How Much is a User Worth?" http://www.forbes.com/sites/tristanlouis/2013/08/31/how-much-is-a-us

^{*11} Ripple, Account Reserves https://ripple.com/build/reserves/

アカウントの事前資金として使用された STEEM は、新規アカウントにパワーアップされます (つまり、Steem パワーに変換されます)。新規アカウントの資金として使用された SP の一部は、アカウント作成者から委託されたものであることがあります。ユーザーが SP を委託されると、投票や大域幅においてその SP を自身のもののように使用できますが、SP の所有権は委託したユーザーに残ります。ユーザーはいつでも委託を取り消すことができます。冷却期間をおいてから、SP はアカウントに戻ります。

手数料との相対的な効果

帯域制限と手数料の効果を比較するには、2つのシステムが攻撃者の意図的なネットワーク・フラッディングに対してどのように反応するのかを考慮する必要があります。ビットコインにおいては、1万ドルを持つ攻撃者は一つ一つのブロックをすべて埋めることによって丸一日サービスを中断することが可能です。一つ一つのブロックに動的な部分準備帯域制限を行うシステムでは、同じ攻撃者はサービスを中断させることができません。

より極端な場合では、攻撃者が全体の 1% のコインを持っているとすると、攻撃者は 6000 万ドルを持っていると推定できます。そのような攻撃者は、マイナーが手数料や容量を増やさない限りビットコインのブロックチェーンを 16 年間止めることが可能でした。取引毎の手数料を 15 ドルに引き上げたとしても、攻撃者はネットワークを 16 日間フラッドさせたままにすることができます。

帯域制限の手法では、ネットワークをフラッドさせる目的ですべてのコインの 1% を持つ人は、30 秒未満しかその目的を果たせません。

賃借 vs 購入 vs タイムシェア

家を所有する人はその家を無料で使用できる権利を期待します。あるグループが家を共同で購入した場合、それぞれが持つ家の所有権の比率に応じて家を使う権利があるということを期待しています。手数料ベースのブロックチェーンは家をオーナーから借りるようなものであり、帯域制限はオーナー間のタイムシェアのようなものです。

複数の人で家を所有する場合、各個人はどのように家をタイムシェアしたいかを決めなければなりません。家の50%を所有しているが年に1回の週末にしか使用しない人は、使用していない時間に使用する人からの支払いを望むかもしれません。これは手数料ベースシステムの考え方です。

一方、家の 50% を所有する人は、将来的に家の需要が増加し権利を高く売ることができるのではないかという思惑を持っています。家を使用する以上に所有しているオーナーは不動産投機家になります。この考え方では、彼らは賃料よりも好評を集めます。

分割した所有権の価値は、その所有者に潜在的に与えられる時間の量に由来します。家の 1% を所有し年に 1 回の週末に利用することが、分割した所有権の最小の価値です。ただし、所有権者の半分が週末に利用しない場合は、タイムシェアの価値は年に 2 回の週末に上がります。そのようなアクティブでないユーザーが代わりに未使用時間を賃貸することを選択した場合、年間 1 回の週末に戻ります。そのような未使用のタイムシェアを使用したい人々に販売した場合、タイムシェアの価

値は 50% に下落します。集めた賃料が下落した価値より大きくなければ、タイムシェアの所有者 は経済的な計算を誤っています。

この理論的解釈によって私たちは、手数料ベースのシステムはユーザーにとって高くなりすぎるか、共同所有者にとって収益性の低いものになると推測します。一人一人の小規模な所有者は、小さいタイムスライスを貸すことで利益を得ることが可能ですが、その場合は他のすべてのタイムシェア所有者にとって負担となります。実際、タイムシェアの価値の下落によるコストは、すべての所有者が被ることになりますが、利益は所有分を貸すことにした一人の所有者に集約されます。

このことから、ブロックチェーンはすべてにおいて使用料を取らないのが最も普及すると私たちは結論づけました。帯域制限の代わりに使用料を課す場合は、十分なタイムシェアを購入し、それを一回使用する権利を得るのに十分な期間保有することを約束するということと同等でなければなりません。

つまり、取引手数料は毎週1回取引を行うために必要な最小アカウント残高と等しく、週末には返却される必要があります。毎週1回の取引を行うことができる最小アカウント残高が1ドルであると仮定します。1ドルの残高を持つ人が1度に5回の取引を行いたいと望む場合は、その取引の前後の週に残高を5ドルに増やす必要があります。

理論的には、ユーザーが必要なステークを借りられるマーケットが作られます。実際には、ユーザーが望む使用率に対応したタイムシェアを簡単に売買できるようにすることの方が効率的です。言い換えれば、少額ローンの交渉のコストは、毎週の最大使用量に対応した残高を維持することのコストよりも大きいということです。

分散型のトランザクション帯域制限により、あらゆる使用場面でマイクロペイメントが必要なアプリケーションでは実現できなかったような、新しい種類の分散型アプリケーションが可能になります。この新しいモデルにより、アプリケーション開発者はユーザーに対して、取引に手数料を課す時と場合を決めることができます。

パフォーマンスとスケーラビリティ

Steem ネットワークは BitShares と同じ技術である Graphene の上に構築されています。Graphene は分散ネットワーク上で毎秒 1,000 トランザクションを維持できることが実証されています。Graphene はサーバー容量と通信プロトコルの比較的単純な改善によって容易に毎秒 10,000 トランザクション以上に拡張することができます。

Reddit スケール

Steem は Reddit よりも大きなユーザーベースを扱うことが可能です。2015 年に Reddit には 870 万人のユーザーがいて、毎秒 23 コメントを作成していました *12 。それはユーザーあたり年間平均 83 コメントです。7,300 万件の最上位投稿があり、毎秒平均 2 件の新しい投稿がありました。約 70 億の投票があり、平均投票量は毎秒 220 件でした。合計すると、Reddit がブロックチェーン上で稼働していた場合、平均で毎秒 250 トランザクションが必要になります。

この業界トップのパフォーマンスを得るために、Steem は毎秒 600 万トランザクションを処理できる LMAX Exchange*13から学んだ教訓を取り入れました。教訓には以下の重要なポイントがあります:

- 1. すべてをメモリに保持する。
- 2. コアビジネスロジックをシングルスレッドにする。
- 3. 暗号化操作 (ハッシュと署名) をコアビジネスロジックの外に置く。
- 4. バリデーションを状態依存と状態費依存の確認に分割する。
- 5. オブジェクト指向のデータモデルを使用する。

これらの単純なルールに従うことで、Steem は最適化開発に多大な労力を費やすことなく毎秒 10.000 トランザクションを処理することができます。

インテルの OptaneTM テクノロジー*¹⁴が導入されてから、すべてをメモリに保持することはますます容易になっています。Steem に関連したすべてのビジネスロジックをシングルスレッドで処理し、すべての投稿をメモリに保持して高速にインデックス作成をするということを、コモディティハードウェアでできなけれなりません。Google もまたインターネット全体のインデックスを RAM に保持しています。ブロックチェーン技術を用いると、データの損失を防ぐために多数のマシンにデータベースを複製することは容易です。OptaneTM テクノロジーが普及することで、RAM がさらに高速化し、持続性が得られます。つまり、Steem は未来のアーキテクチャによって拡大できるように設計されています。

^{*12} Reddit Statistics, Number of Users and Comments per Second http://expandedramblings.com/index.php/reddit-stats/2/

^{*13} Martin Fowler, The LMAX Architecture http://martinfowler.com/articles/Imax.html

^{*14} Introducing Intel Optane Technology – Bringing 3D XPoint Memory to Storage and Memory Products https://newsroom.intel.com/press-kits/introducing-intel-optane-technology-bringing-3d-xpoint-memory-to-storage-and-memory-products/

配分と供給

初期配分と供給

Steem ネットワークは通貨供給量 0 の状態で始まり、プルーフ・オブ・ワークによってマイナーに およそ毎分 40 STEEM の比率で割り当てられ、さらにコンテンツとキュレーションの報酬プール に毎分 40 STEEM が蓄えられました (合計で毎分 80 STEEM)。その後、ネットワークは SP に変換したユーザーに報酬を出し始めました。この時点で、STEEM は以下のような様々な貢献への報酬の複合効果により、およそ毎分 800 STEEM の比率で増加していました:

貢献への報酬:

- キュレーション報酬: 毎ブロック 1 STEEM、または年間 3.875% のいずれか大きい方
- コンテンツ作成報酬: 毎ブロック1 STEEM、または年間3.875%のいずれか大きい方
- ブロック作成報酬: 毎ブロック 1 STEEM、または年間 0.750% のいずれか大きい方
- 864,000 ブロック以前の POW に含まれる報酬: 毎ブロック 1 STEEM (毎ラウンド 21 STEEM の付与)
- 864,000 ブロック以降の POW に含まれる報酬: 毎ブロック 0.0476 STEEM (毎ラウンド 1 STEEM の付与) または年間 0.750% のいずれか大きい方
- 流動性報酬: 毎ブロック 1 STEEM (毎時 1200 STEEM の付与) または年間 0.750% のいずれ か大きい方

パワー報酬

■ Steem パワー報酬: 上記の報酬によって作成された各 STEEM に対して、9 STEEM がすべての Steem パワー報酬者の間で分割されました。

SBD 運用:

■ SBD 報酬: 証人が設定した APR の割合で SBD が作成され、SBD 保有者に SBD が支払われました。

SBD 運用の効果により全体的な供給像が複雑になり、SBD のセクションで議論したように、フィードレートの影響や SBD 報酬によって STEEM の大規模な作成や破壊が起こる可能性があります。その他、未請求の報酬 (例: 喪失ブロックのブロック報酬) や放棄されたアカウントなどの小規模の複雑な効果も存在します。

現在の配分と供給

2016 年 12 月にネットワークのハードフォーク 16 から、Steem は年間インフレ率 9.5% で新しいトークンを作成するようになりました。インフレ率は 250,000 ブロックごとに 0.01%、年間およそ 0.5% 減少します。全体のインフレ率が 0.95% になるまで、インフレ率はこのペースで減少し続けます。これはハードフォーク 16 が有効になってからおよそ 20.5 年かかる予定です。

新しいトークンの 75% は報酬プールに蓄えられ、投稿者とキュレーターで分割されます。新しいトークンの 15% は SP 保有者に付与されます。残りの 10% はブロックチェーンを動かしている証人に支払われます。

トークン生成率の影響

インフレモデルのコインは持続可能ではないとよく言われますが、現実に数え切れないほどの例が あり、通貨量は確かに意味がありますが、その価値に直接的かつ即時的な影響はないことが知られ ています。

2008 年 8 月から 2009 年 1 月にかけて、米国の通貨供給量 *15 は 8710 億ドルから 1 兆 7370 億ドルまで増加し、増加率は年間 100% を超え、その後の 6 年間は年 20% で増加し続けました。米国の通貨供給量は 7 年足らずで 4.59 倍に増加しました。その間、政府の物価指数 *16 によると、商品やサービスに対するドルの価値は 10% 未満の下落でした。この実例は、供給量は価格の一要素でしかないことを示しています。

ビットコインが誕生してから最初の 2 年間で、ネットワークは年間 100% を越えるインフレ率を維持しました*17。最初の 5 年間で 10% 以上、最初の 8 年間で 10% 以上でした。全体として、Steem のコンテンツやキュレーション、ブロック生成に資金を供給するための「支出」総額は年率 10% 未満に抑えます。

STEEM のようなデジタル商品の価格は、供給と需要の両方で動きます。長期的な保有者が撤退すると、市場の STEEM 供給が増えて価格は下落します。新しい長期保有者が STEEM を買って SP に変換すると、この下向きの圧力は打ち消されます。市場の投機家が将来の市場価格の予測に基づいて流動的な STEEM を売買することにより、さらに供給と需要が増加する可能性があります。

https://research.stlouisfed.org/fred2/graph/?s%5B1%5D%5Bid%5D=AMBNS

http://data.bls.gov/cgi-bin/cpicalc.pl?cost1=1&year1=2008&year2=2016

^{*15} United States Money Supply, 2009

 $^{^{*16}}$ CPI Inflation Index, United States Dollar 2008-2016

^{*17} Bitcoin Annual Inflation Rate, Bitcoin Talk Forum https://bitcointalk.org/index.php?topic=130619.0

Steem の力

Steem はユーザーの貢献 (投稿と投票) 全体の価値が、個々の合計よりも大きいことを認識しています。単一のコメントにはほとんど価値はありませんが、数百万ものキュレーションされた投稿の価値は何百万ドル、あるいは何十億ドルにもなる可能性さえあります。単一の投票には僅かなキュレーション価値しかありませんが、数十億の投票によるキュレーションは非常に効果的です。キュレーションのないコンテンツには限られた価値しかありません。インターネットのすべてのコンテンツにリンクがなかったとすると、Google は有用な検索結果を作り出すのに苦労したでしょう。それは情報の間のリンクであり、大きな価値をもたらすものです。

全員が利益を得ているため、全員が支払うべきです。言い換えれば、個々のユーザーが支払いを求められることはなく、代わりに Steem に価値をもたらすすべてのものに対して報酬を出すべきです。私たちがしなければならないことは、どのユーザーがソーシャルネットワークに価値をもたらす貢献をしたか、どのユーザーがそうでないかを確認することだけです。

まとめると、Reddit のユーザーは毎秒 220 回の投票を行い、毎秒 23 件の投稿を作成しています。 Reddit には 5 億ドル *18 から 40 億ドル *19 の価値があります。これはそれぞれの投票と投稿に 0.06 ドルから 0.50 ドルの価値があると仮定し、Reddit の価値が主に過去 1 年間のアクティビティによるものとした場合です。 Reddit の価値の大部分は、過去 1 週間以内に行われたリアルタイムに近い議論であり、それは新しいアクティビティの価値を劇的に高めると主張することができます。人は、人々が去年いた場所ではなく、人々が今いる場所に行きます。

マイクロペイメントは不要、チップは仟意

既存の暗号通貨とソーシャルメディアプラットフォームを統合する試みは、ユーザーが他のユーザーに支払うことができるようにすることに焦点を当てています。多くのサービスではチップを導入しようとしています。それは、チップを簡単にすることで、多くの人がそれを使うようになるという理論です。他のサービスでは、宣伝やコンテンツのランキング強化のために支払わせようとしています。また、記事がどれだけのチップを得られるかについて小規模の予測市場を作ろうとしているものもあります。

これらのアプローチはすべてマイクロペイメントに要約されます。それらは誰が支払うかということだけが異なります。それらはどれもマイクロペイメントを支払う人の参加不足に悩まされています。コンテンツ制作にインセンティブを与えることを求めている企業家は、誰が支払うかに焦点を当てており、明らかな実態を見逃しています:すべての人がすべての人の行動から利益を得ている

^{*18} Reddit Valuaton, Newsweek, 2014

http://www.newsweek.com/investors-think-reddit-worth-500-million-26

^{*19} Worth of Web, March 2016

http://www.worthofweb.com/website-value/reddit.com/

のだから、考え様によって、すべての人が支払うか、または誰も支払わないべきです。

Steem はユーザーが投稿に投票しコミュニティがお金を支払うため、完全にマイクロペイメントを回避しています。ユーザーが投稿に投票したかどうかに関わらず同じ金額が使われ、そのお金は投票者から支払われたものではありません。

経済的な決断に伴う精神的なエネルギーは、多くの人にとって参加への障壁となります。

私たちは情報が爆発的に急増するデジタル時代において、オンラインにアクセスすることについて既に毎日多数の選択肢に迫られており、私たちがその上でしなければならない決断は、単に私たちが直面している不確実性と不安に追加されるだけです。マイクロペイメント・サポーターは、簡略化された実装によってマイクロペイメントの介入を最小限にしユーザー・エクスペリエンスを向上させられると考えています。しかし、その議論は意思決定プロセスに二重規範を作成するだけです [2]。取引は同時に、意思決定の理由として十分な価値を持つことと、意思決定を自動化できるほど価値を小さくすることはできません。ユーザーが何も考えずに承認できる取引は無料のものだけです。そのため、どのような正の価値を持つマイクロトランザクションも、意思決定のために必要な精神的コストを負担することになります。さらに、精神的な取引コストは実際にはある閾値まで上昇し、マイクロペイメントをより一層不利益なものにする現象となります。例えば、今日の新聞のコピーが 1 ドルであるということは簡単にわかりますが、読者がそれぞれの記事や言葉の価値を判断するのは非常に困難であり不安を伴うでしょう。そのようなジレンマは、すべてのオンラインコンテンツが構成要素に分割され、個々の価値がマイクロペイメントのシステムによって決められる場合にのみ、反復し増幅されます。

-マイクロペイメント: 実現可能なビジネスモデル*²⁰

Steem においては、マイクロペイメントはコンテンツ制作者に支払われますが、コンテンツに投票する人は支払いません。代わりに、報酬の費用は新しいトークンで支払われます。システムに参加し、誰かに支払うために投票する人は、スタート時に持っていたものよりも多くのお金を持ってシステムから撤退することができます (Steem システムの市場価値が一定であると仮定した場合)。言い換えれば、Steem によって提供されるマイクロペイメントソリューションは、ユーザーモデレートによるコンテンツを持つ多くのウェブサイトと同様のユーザー・エクスペリエンスを提供します。

さらに、Steem は支払うべき人を見つけ出す人にも支払います!このような考え方は革命的です。

価値はリンクにある

コンテンツ間のすべてのリンクを削除した場合、インターネットはその価値の大部分を失います。 Google が 1600 万件の結果から最高のアップルパイのレシピを見つけ出すことができるのは、ウェ ブページ間の結びつきのおかげです。リンクがなければ、Google が持つ情報は単語の出現頻度だけ

^{*20} Micropayments: A Viable Business Model http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html

になります。

リンクは様々な形式をとることができ、時間をかけて最適化されていきます。ユーザーがソーシャルネットワークのコンテンツに投票する度に、ユーザーをコンテンツの間に繋がりが増えます。これにより、コンテンツを通じて消費者と制作者の間に次々とリンクができていきます。繋がりが多くなるほど、ネットワークの情報価値は大きくなります。それは価値をもたらす相対的で意図的な情報の繋がりです。

ソーシャルネットワークは、繋がりの量と質を最大化したコンテンツの集まりから抽出した価値を最大化することができます。キュレーションコンテンツは高コストで時間がかかるものであり、リンクがなければコンピュータで行うことは不可能に近いものです。Steem は、新しいコンテンツを最初に見つけて確認したユーザーに報酬を与えます。

キュレーションにインセンティブを与えることにより、Steem ネットワークは膨大なコンテンツから最も価値のある情報を抽出するための自動化アルゴリズムを用いることができます。

暗号通貨オンボーディング問題の解決

暗号通貨に参入するのは容易ではありません $*^{21}$ 。ある人がビットコインを見つけてそれを試してみたいと思ったとすると、取引所に登録してクレジットカードや電信送金でアカウントに入金しなければならないことがすぐにわかります。お金と 2 種類の ID が必要だとすれば、Facebook の普及率はどうなっていたでしょうか?

Steem は、すべての人がシンプルですが価値のある仕事をすることによって報酬を得られるようにすることで、この問題を解決しました。これは STEEM トークンを広く普及させます。これは暗号通貨がネットワーク効果を持つため有益なことです (例えば、ユーザーが多いほど便利になります。より極端な例として、Satoshi がビットコインの 100% を自身で持っていた場合を考えると、ビットコインは無価値です)。

暗号通貨精算の問題の解決

使いにくいまたは売ることができない通貨にはほとんど価値がありません。1ドル相当のビットコインを手にした人はそのビットコインを売るのに1ドル以上のコストがかかることに気づくでしょう。彼らは取引所にアカウントを作成し、KYC認証を行い、手数料を支払う必要があります。少額の暗号通貨は、わざわざ拾うことのない小銭のようなものです。

商店はユーザーに、暗号通貨を有形の商品やサービスに簡単に交換できるようにする方法を提供します。商店は口座の単位、通常ドルに固定された通貨を求めます。価格が変動しやすい通貨を導入するのには多大な経費がかかります。

^{*21} Dailydot, Jon Southurt, April 2015 http://www.dailydot.com/opinion/bitcoin-cryptocurrency-adoption-hard

商店は売上を増加させるためならどのような通貨も受け入れます。SBD のような安定した通貨とともに大きなユーザーベースを持つことは、商店の参入を容易にします。導入店舗の存在は、取引所の使用に煩わされることなくシステムから資金を引き出すための出口となり、システムを改善します。

Steem プラットフォームに参加することによって得た少額の暗号通貨を精算できる別の方法は、他の人に _ チップを渡す _ ことです。これはウェイターにチップとして小銭を残すようなものです。多くの人が少額のチップを残していけば、合わせるとそれは大きな金額になります。あなたもウェイターもチップから利益を得ることができます。

検閲

Steem は世界中の法域にいる承認によって運営されている分散型ネットワークです。すべてのユーザーの行動はブロックチェーン上で記録、公開されており、誰でも検証が可能です。つまり、STEEM 保有者によって評価されるコンテンツを検閲できる単一の実体は存在しません。

steemit.com のような個々のウェブサイトは、自身のサイト上でコンテンツを検閲することも可能ですが、ブロックチェーン上で公開されるコンテンツは本質的にブロードキャストされており、世界中にあるミラーで引き続き利用可能です。

言論の自由は他のすべての自由の基礎であり、言論の自由に対するいかなる侵害もコンセンサスに至る唯一の平和的な方法、議論の根底を崩します。自由な議論がなければ、投票者には十分な情報が与えられず、十分な情報を持たない投票者は社会にとって投票権を失うことよりも脅威になります。検閲は公開討論を制限することによって投票を盗む手段です。Steem は自由な言論と自由な社会の構築を可能にすることを約束します。

検索エンジン最適化による有機的な発見の解決

ほとんどの暗号通貨はネットワークを積極的には利用していない人にとってはほとんど価値を生みません。対照的に、Steem はコンテンツを生み出し、ユーザーに共有するように促します。このコンテンツは検索エンジンによってインデックス化され、最終的に非常に多くの消極的なユーザーに価値をもたらします。この検索トラフィックは Steem ネットワークの有機的な宣伝を作り出し、ネットワーク効果を高めます。

ブロックチェーンベースの帰属への移行

インターネットは世界で最も容易に情報を配信するための代表的な媒体です。とは言え、それは自身のコンテンツを持ち、適切な帰属によって共有しているコンテンツクリエイターにとっては恐ろしい場所にもなります。現在のソーシャルメディアプラットフォームにおいては、帰属が一晩中失われることもあります。投稿された動画や画像はクリエイターの同意やクリエイターへの配慮なし

に、複製および再共有されます。

ブロックチェーンベースのソーシャルメディアでは、クリエイターや著者はコンテンツのオリジナル性の証明を公開記録とタイムスタンプで示すことができます。クリエイターが許可や帰属なしに再共有する人に対処したい場合、ブロックチェーンベースの記録は、コンテンツがどのユーザーからどの時間に投稿されたものかということの公開証拠を提供します。将来、ブロックチェーンベースの帰属は、政府が信憑性を認めて裁判所において重要性を持つようになり、コンテンツクリエイターにとって自身の作品の管理における大きな力になるかもしれません。

ほとんどすべてのブロックチェーンにタイムスタンプサービスを構築することは可能であり、ビットコインネットワーク上でこの種のサービスを作ろうという取り組みがいくつか存在します。ですが、Steemではコンテンツ発信者は「ファーストクラスの市民」であり、この分野において利点があります。 – Steem ブロックチェーンは、コンテンツ発信に使用するために基礎から作り上げられており、コンテンツクリエイターが他の Steem ユーザーが使うのと同じオーサリングツールを使用して投稿するだけで、特定の時点においてコンテンツの正当性を検証できるブロックチェーンです。

広告をブロックチェーンベースのコンテンツ報酬に置き換える

ほとんどのコンテンツの収益化モデルでは、コンテンツクリエイターは様々な形の広告を活用しています。多くのクリエイターは広告が消費者にとっての作品の価値を低下させることを認識していますが、それでもクリエイターは多くの場合に、彼らの時間に対して収益化による見返りを求める必要があります。広告は諸刃の剣です:広告によりクリエイターは最も容易にお金を得ることができます。広告がなければ収益化は困難ですが、コンテンツはより鮮やかになります。

Steem に接続するソーシャルメディアに投稿したクリエイターは、ただ Steem コミュニティから作品が認識される (または、「いいね」をもらう) だけで収益化することができます。ブロックチェーンベースの報酬は完全にデジタルであり、仲介者はいません。従って、ブロックチェーンベースのコンテンツ報酬による収益化は、広告による収益化よりも迅速であり、遥かに使用も容易なものになるはずです。

結論

Steem は暗号通貨とソーシャルメディア業界の両方の最も良い面を組み合わせることで、両者の課題に取り組むために設計された新しい試みです。Steem はソーシャルメディア業界にはない方法で、コンテンツクリエイターとインターネット読者に稼ぐ機会を提供します。Steem では、各個人は貢献度に直接相関した報酬を実際にオンラインで得ます。それらの報酬は、市場の価格発見と Steem の流動性によってドルの価値を持ち、Steem を保有する人々は、持たない人よりも大きい収益力を持つ可能性があります。