



Viacoinホワイトペーパー

Viacoin開発チーム
2017年9月12日

最終更新: 2018年3月17日

要約

Viacoinは、2014年に作成されたオープンソースの暗号通貨です。本通貨は、拡張版120バイトのOP_RETURNを持ち、埋め込み型コンセンサスをサポートする **[bitcoin2008]** ビットコインプロトコルの流れを汲んでいます。Viacoinは、AuxPoW(Auxiliary proof of work)とも呼ばれるスクリプトマージマイニングを採用しており、ビットコインの25倍のトランザクション速度を持ちます。Viacoinのマイニング報酬は6ヶ月ごとに支払われます。最大供給量は、2317万6392.41459枚です。マイニング報酬を最小限に抑えているため、Viacoinは低いインフレ率を保っています。Viacoinのブロック報酬は低いので、採掘者はマージマイニング(AuxPoW)を介して、採掘におけるインセンティブを受け取ります。Viacoinは現在、最も大きいマイニングプールの1つであるF2Poolによって、非常に高いハッシュレートで採掘されています。その他には、Kimoto Gravity Well(DarkGravityWave)で指摘される脆弱性を修正する採掘難易度調整アルゴリズムや、一度に29のソフトフォークの実行を許容するVersionbits、Segwit、そしてLightning Networkなどの機能を採用しています。

注記: ホワイトペーパー、参照文献、設計は研究および開発段階で、変更される可能性があります。



Viacoin Whitepaper

1. スクリプト

暗号学において **[scrypt]** スクリプトとは、コリン・パーシバル(Colin Percival) 氏によって作成された、鍵導出関数に基づいたパスワードのことを指します。 同アルゴリズムは、大量のメモリを要求することによって、大規模なカスタムハードウェア攻撃を行いにくくするよう設計されました。 2012年、同アルゴリズムは、情報RFCとなるように意図した、インターネット標準化への草稿としてIEFTが公開しましたが、そのスクリプトは現在、Viacoinのような暗号通貨がフルーフオブワークシステムとして使用しています。

スクリプトはメモリハードの鍵導出関数であり、評価するために大量のランダムアクセスマトリクスが必要とします。これによって、特定用途向けカスタムハードウェア(ASIC)の実装により多くのVLSI領域が必要になり、Viacoinの採掘を目的とした機器の開発は採算が取れないものとなります。スクリプトアルゴリズムの要件は、メモリに収容される擬似ランダムビットの大量の配列と、これから生成された鍵です。 同アルゴリズムは、時間と記憶域のトレードオフ(TMTO)に基づいています。 ASICにおける利点は、Viacoinではビットコインと比較して10倍減少します。

スクリプトは以下のパラメータを使用して、導出鍵を生成します。

- パスフレーズ: ハッシュする文字列
- ソルト: スクリプト関数に付与されるランダムな文字列
- N: メモリ/CPUコストパラメータ
- P: 並列化パラメータ
- R: ブロックサイズパラメータ
- dkLen: 意図された鍵長。バイト表示の導出鍵

`kd = scrypt(P, S, N, P, R, dkLen)`

Viacoinパラメータ: N=1024、R=1、P=1、S= 256ビットのアウトプットを出すランダムな80バイト



Viacoin Whitepaper

2. マージマイニングAuxPoW

Viacoinの**[auxpow]**マージマイニングは、他の**[scrypt]**スクリプトコインのマイニングパワーを再利用してViacoinブロックチェーンのセキュリティを強化することを目的とします。また、採掘者はこれにより、一度に一つ以上のブロックチェーンを採掘することが可能です。例えば、Viacoinやライトコイン、またはその他のスクリプトコインを、どちらのハッシュレートにも大きな影響を及ぼすことなく、Viacoinと一緒に同時に採掘することができます。

採掘者が貢献するすべてのハッシュは、両方の暗号通貨のハッシュレート合計に加算され、結果としてブロックチェーンの安全性を高めます。AuxPoWブロックはビットコインブロックと似ていますが、2つの違いがあります。- まず第一に、AuxPoWのブロックヘッダーのハッシュは、ブロックチェーンの難易度を満たしていません。 第二に、AuxPoWは、ブロックを作成した採掘者が親ブロックチェーンでマイニングを行った、という補足的なデータ要素を持ち、それがauxブロックチェーンの難易度を満たします。

報酬が低くても、他のスクリプトコインと一緒に無料で採掘できるため、Viacoinの採掘におけるインセンティブは十分にあります。 Viacoinの原動力はブロック報酬によるものではないため、マージマイニングをサポートしていない他の暗号通貨に比べて低いインフレ率を保てます。

3. Dark Gravity Wave

[darkGravityWave] Dark Gravity Wave (DGW) は、オープンソースの難易度調整アルゴリズムです。 DGWは、X11/ダークコイン/ダッシュの開発者および作成者であるエヴァン・ダッフィールド (Evan Duffield) 氏によって創生されました。 同アルゴリズムは、Kimoto Gravity Waveアルゴリズムにおけるタイムワープ攻撃などの欠陥を指摘するために設計されました。

Dark Gravity Waveが初めて導入されたのは、ダッシュ(ダークコイン)です。 DGWは、複数の指標関数的移動平均線と

単純な移動平均線を使用し、再調整のメカニズムを円滑にします。

公式:

$$2222222 / (((\text{Difficulty} + 2600) / 9)^2)$$

最新のバージョンはDark Gravity Waveバージョン3であり、有名なKimo Gravity Wellアルゴリズムと比較して、リターゲティングが精度を増しています。



Viacoin Whitepaper

4. Segwit

Viacoinは【segwit】Segwit (BIP 141)を採用しています。Segregated Witnessは取引サイズを縮小し、UTXOの拡大に対処します。Segregated Witnessは、witnessデータが取引から分離された取引フォーマットのことです。- また、1ブロック当たりのトランザクション処理能力を2~3倍に増加しつつ、同時に新しいノードに対するブロック同期の速度を向上することを目的とします。

しかし、ViacoinにSegwitを実装する主な目的はキャパシティの増加ではなく、属性を修正し、スクリプトのアップデートを容易にするためです。Viacoinの属性の修正を行うことで、【atomic】アトミックスwapや、双方向ペイメントチャネル、Lightning Networkなどの追加機能が搭載でき、ビットコインとの相互運用性を向上させることができます。

Segwitにはスクリプトに対するバージョニングが含まれ、これにより、Segwitを使用しないトランザクションでは通常ハードフォークが必要になるオペコードも、代わりに使用できます。オペコードのスクリプト変更が容易になれば、Viacoinの進化も容易になります。これにより、Schnorr署名、サイドチェーン、MASTなどの機能が追加できるようになります。

5. The Lightning Network

【lightningNetwork】Lightning Networkは、Viacoinブロックチェーンの一層上で稼働している転送ネットワークであり、ブロックチェーン内でスマートコントラクトを使用して参加者のネットワークにおける即時支払いを可能にします。- これは、トランザクションの大部分をコンセンサス台帳の外に出し、支払いチャネルに移動することで、トランザクション処理能力を桁違いに向上することを可能にします。つまり、同ネットワーク上で、1秒当たり数百万から数十億のトランザクションができるということです。これは、従来の支払い方法を圧倒するキャパシティです。- これは、当事者が双務ステートフル契約を結ぶオンチェーンスクリプトをサポートすることで可能になりました。双務ステートフル契約とは、デジタル署名を共有することによりステートを更新でき、ブロックチェーンに証拠を発行することで終了できる契約です。

Lightning Networkの手数料は非常に低額です。Lightning Networkは、少額のトランザクションにとって魔法の解決策のようなものです。- Lightning Networkは新しい種類の商取引を可能にします。多くの関係者と支払いチャネルを開くことで、Lightning Networkの参加者が他人の支払いに対するルーティングの中心になることができ、完全に接続された支払いチャネルの構築に繋がります。支払いは、デクリメント時限錠によって不可分性を強化するスクリプトを用いて強制されます。



Viacoin Whitepaper

もう一つの利点として、アトミッククロスチェーントランザクションの可能性が挙げられます。これにより、ユーザーは、Viacoin、ビットコイン、ライトコイン、そしてその他Segwitコインの取引を瞬時に行うことができ、非常に効率的かつ分散化された取引、または分散化型の「Shapeshift.io」を可能にします。

6. Schnorr署名

Schnorr署名アグリゲーションは、今後の開発予定の一部です。この機能はビットコインにおいても、より効率的なアルゴリズムであるという理由から、ECDSAの後継として提案されています。近年まで、Schnorr署名をViacoinやその他多くの暗号通貨に実装するのは、ハードフォークなしには不可能でした。今やそれがSegwitの属性をもつてすれば、可能になりました。すべての署名データは、witnessに移動されます。現在Viacoinは、あるアウトプットから他のアウトプットに対する転送を承認するために、所有権のゼロ知識証明として楕円曲線DSA(ECDSA)を使用しています。2015年、ダニエル・J・バーン斯坦氏は、楕円曲線上の署名のようなSchnorrを使用することを提案しました。

それには以下のようない点があります。

- 標準的仮定において立証可能な形で安全
- 属性への耐性
- ハッシュ関数の衝突に対する抵抗力
- 2~3倍の高速化を実現するバッチ認証
- ネイティブk-of-kマルチシグネチャ...

Schnorr署名はバッチ認証をサポートしています。つまり、単体ではなく、複数の公開鍵メッセージ署名の組み合わせがある場合、グループとしてその信頼性を確認でき、個別に認証するよりも速く処理できます。ブロックは認証を行う署名の大きな塊であるため、この方法は最適と言えます。



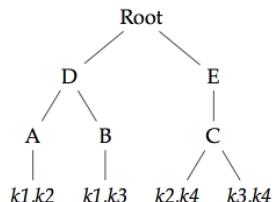
Viacoin Whitepaper

Schnorrのアイデアであるネイティブk-of-kマルチシグチャは、複数の鍵を一つの鍵にまとめ、そのすべてが署名していることを証明できます。複数人で鍵の合計に対する有効な署名を作成することができます。下図のU1、U2、U3は、ユーザーです。これらすべてがk1、k2、k3のノンスを生成するラウンド、そして対応するパブリックポイントのR1、R2、R3を算出するラウンドの二つのラウンドを持つ相互作用スキームがあります。これらは互いに交信し合い、合計して総合的なRの値を出します。- この総合的なRの値は各鍵を用いてこのノンスに署名し、S1、S2、S3を生成します。そして、これらすべてのSの値を合計して、鍵の総和に対して有効である最終的なS. A署名を作成します。これは、k-of-kマルチシグチャの利点を持ちます。

$$\begin{array}{c|c} U_1 \rightarrow k_1, R_1 & U_1 \rightarrow (R, s_1) \\ U_2 \rightarrow k_2, R_2 & U_2 \rightarrow (R, s_2) \\ U_3 \rightarrow k_3, R_3 & U_3 \rightarrow (R, s_3) \end{array} \longrightarrow R \longrightarrow \begin{array}{c} (R, s) \end{array} \quad (1)$$

k-of-kではない場合でも、他のポリシーを持つどの鍵の組み合わせも署名できます。必要なのはマークルツリーと、すべての葉ノードが署名できる鍵の組み合わせを持つマークルツリーを構築するためのSchnorrの機能です。これらはまとめてハッシュされる必要があります、ルートがアドレスになります。OP_CHECKSIGとOP_CHECKMULTISIGは、公開鍵をスタックし、認証されたインプットを非線形化して関連付け、トランザクションに対する結合した署名を生成します、結果として、ブロックサイズを20%縮小させることができます。

4のうち2 (k1...k4)
 O(1) 認証時間
 O(log n) 署名サイズ
 O(n) 署名時間



一つのトランザクション内で、すべての署名に対してアグリゲーションを行うことが可能です。その裏にあるアイデアは、Viacoinノードのようなシステム認証がすべてのトランザクションの各インプットに対して一つの鍵を算出することを可能にするというものです。



Viacoin Whitepaper

7. 非アトミックフラッシュ

システムを強固にするため、ディスク上のステートはブロックと一致しなくてはいけません。ウォレットの予期しないシャットダウンには、再起動後にウォレット内でロールバックまたはロールフォーワードを行い、ディスクの一貫性を保つことができます。通常、キャッシングが溜まつた時はいつでも、フラッシュが強制されます。起動時にこれが発生する場合は、フラッシュの間にクラッシュしたこと意味します。この場合、続行する前に内部でブロックをロールバック/ロールフォーワードして、ディスクの一貫性を保ちます。

8. カラードコイン

Viacoinのスクリプト言語では、アセット操作の命令を示すことが可能な、ブロックチェーン上にある少量のメタデータを保存できます。Viacoinのトランザクションは、Xユニットの新しいアセットが発行されたこと、そしてViacoinのアドレスに入金されることをエンコードできます。カラーリングという言葉は、コインの額面価格に「色をつける」という概念から生まれました。Viacoinに色をつけることで、企業の株式や物理的な商品のように、ユーザーが取引したいと考える多様な資産に相当するトークンに変換できます。→ 「カウンターパーティ」と非常に似ていますが、主な違いがいくつかあります。まず、Viacoinブロックチェーン(例: NXT)を使用する点です。

そして、補助貨幣は発行しません(例: Counterparty、Mastercoinなど)。メタデータは、通常OP_RETURNオペコードの一つに格納される、**[coloredCoins]** カラードコイントランザクションに意味を持たせます。OP_RETURNを含むアウトプットは、マーカーアウトプットと呼ばれます。このマーカーアウトプットは、ゼロまたはゼロ以外の値を持つことができます。マーカーアウトプットはOP_RETURNオペコードから始まり、その後に任意のオペコードのシーケンスが続けます。このシーケンスは、解析可能なオープニアセットマーケットペイロードを含んだPUSHDATAオペコードを含む必要があります。アセット数量のリスト欄は、アセットの各アウトプットの数量を決定するために使用され、各整数はLEB128エンコーディングを使用しています。これが9バイトを超えた場合、そのマーケットアウトプットは無効と見なされます。一つのアウトプットに対する最大アセット数量は、263 - 1ユニットです。カラードコインの**[openAsset]** オープニアセットプロトコルは、Viacoinプロトコル上に実装されます。Viacoinのプロトコル自体を変更する必要はありません。



Viacoin Whitepaper

9. MAST [マークル化抽象構文木]

[MAST] MASTは、部分的にハッシュ化した形でViacoinトランザクションの認証スクリプトを保管し、ノードがマークルツリーと交信することを可能にします。「支払い時、ユーザーは実行しているブランチ、そしてブランチに接続しているハッシュを固定サイズのマークルルートに提供するだけで良い。」これによりロック解除のスクリプトのスタックを $O(n)$ から $O(\log n)$ (nはスクリプト内のブランチの数を意味する)に減らすことができる。また、今のところスクリプトのサイズやオペコードの実行数の制限が原因で実現できない複雑な解除条件も設定が可能になる。さらに、未実行ブランチを隠すことでプライバシーが向上し、少額のコスト、または追加コスト無しで任意のデータを含められるようになる」。

MASTは、ブロックチェーンに大きな負荷をかけることなくスマートコントラクトの作成を可能にするため、重要であると言えます。通常、スマートコントラクトはすべてブロックチェーン上に表示され、容量をとります。MASTを用いれば、完了したスマートコントラクトのみを開示するだけによく、ノードはマークルツリーの最上層を読むだけでいいため容量を節約することができます。これはイーサリアムのスマートコントラクトに類似しますが、違う点があります。イーサリアムは直接VM(仮想マシン)にアクセスしますが、VIAはRootStock(RSK: ルートストック)を通してVMにアクセスします。RSKは、本来イーサリアムがなるべきはずだった、分散型かつチューリング完全なスマートコントラクトプラットフォームを目指しています。

10. Viacoin RSK スマートコントラクト

[rootstock] Rootstockは、双方の互換性を持つスマートコントラクトプラットフォームです。スマートコントラクトを活用するということが、同プラットフォームの概念です。Rootstockは、Rootstock Virtual Machineというチューリング完全な仮想マシン(しかもイーサリアム仮想マシンとも互換性があります!)を稼働しており、Solidityでコンパイルされたスマートコントラクトを実行できます。Viacoinを用いたマージマイニングも可能で、これによりRSKブロックチェーンはViacoinと同等のセキュリティレベルを実現できます。オンチェーンでは1秒当たり約2000トランザクション、オフチェーンでは約2万トランザクションを処理する予定です。



Viacoin Whitepaper

11. 匿名取引

[styx] Tumblebitに基づいたViacoin用追跡不能な匿名アトミックペイメントハブ。

<https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf>