SHIELD

FUTURE-PROOFING THE BLOCKCHAIN

概要

SHIELD プロトコルは楕円曲線電子署名を Lamport, Winternitz, または BLISS 署名に置き換えることで、P2P（ピアツーピア）アドレスに「耐量子性」を実現します。SHIELD プロトコルの持続的な開発と、このドキュメントに記載されたプロジェクトを促進していくことが、SHIELD の自律的な開発サイクルにつながっていきます。

SHIELDは、将来的にはマスターノードによるカスタムPoSスキーム(Pos Boo)を実装します。また、マスターノードはPrivate sendやInstant sendといったトランザクション機能を備えます。

キーワード：SHIELD, quantum-proof, masternodes, cryptocurrency, blockchain, privacy SHIELD currency, Lamport signatures, Winternitz signatures, BLISS signatures.

1.はじめに

SHIELDは2009年にサトシ・ナカモトにより開発されたブロックチェーン技術に基づいた暗号通貨（仮想通貨）です。

ブロックチェーンはその黎明から莫大な成長を遂げ、様々な産業での応用が行われています。しかし、ブロックチェーンが世間の主流となるためには克服しなければならない数々の大きな問題を抱えています。

SHIELD は世界で初となる真に安全かつ匿名な P2P 通貨となることでこれらの問題の解決を目指しています。SHIELD は 51％攻撃と将来脅威となるであろう量子コンピュータに対する耐性を有しています。SHIELD のトランザクションはとても高速で、送金手数料は最小限に抑えられています。

2.解決すべき問題点

ビットコインが世に出されたときは本当に革新的でした。サトシ・ナカモトが作り上げた基礎の多くは、今の暗号通貨でも使われています。その例の一つが単一のアルゴリズムを利用したブロックマイニングです。そのため、ある種のアルゴリズムに特化し、それを効率的に実行できるようなハードウェア(ASIC)が開発され、GPUマイニングは下火に成りました。ナカモト氏の開発デザインの欠点は、多くの暗号通貨で認識されているように、このマイニングの方法はすべての

参加者に対して「公平」なわけではない点です。詳細については「3. マルチアルゴリズムPoWマイニング」を参照してください。

量子コンピュータ技術は近年めざましく進歩しており、近い将来実用化されるでしょう。量子コンピュータの使用が研究者や政府、産業に制限されようと、いずれは営利目的の個人にも使われるようになるでしょう。この技術が人々の生活を大幅に向上させるのは疑いようもありませんが、懸念すべき事実もまたあります。その一つは、現在の暗号技術が量子コンピュータによるクラックに大変弱いことです。多くの暗号通貨が量子コンピュータによるブロックチューンの破壊を受ける恐れがあります。SHIELD が、この問題にどう対応するかは「4.耐量子性」を参照してください。

FacebookやGoogleのような大企業は、ユーザーが何者で、何を求めているかを知ることに非常に長けるようになりました。これは現時点では人々にとって大きな問題ではないでしょうが、これは企業組織が顧客を監視できるということです。最近、企業や政府がユーザーの消費活動を追跡できないようにして、ユーザーの匿名を守ると謳う暗号通貨が生まれています。ですが、それらの暗号通貨の多くは、謳い文句ほどの匿名性を保てていませんし、スケーラビリティと現実性にも欠けているか、未完成です。ユーザーの匿名性の維持に関しては、「5: プライバシー（匿名性）」を参照してください。

暗号通貨の中には、有望なロードマップを持つものがあります。驚くほど優秀で独創的な開発者を擁すアルトコインもあります。ですが資金が足りなければコインの開発は止まってしまいます。プロジェクトからの安定した収入がなければ、開発者がフルタイムに開発に取り組むことは難しいでしょう。私たちが心から我々の事業や目標を、そしてSHIELDコミュニティへの貢献を信じているのですから、こういった事態は避けねばなりません。暗号通貨のプロジェクトが直面しがちな資金の問題を解決するために、SHIELDとSHIELDプラットフォームに資金調達を助ける仕組みを組み込みました。詳しくは、「6: 資金調達」を参照してください。

さて、我々が見つけたもう一つの問題は「Proof of Work(PoW)」プロトコルを用いるビットコインや他の暗号通貨のマイナーがコインのマイニングとトランザクションの承認に 莫大な電気を消費することです。PoWはビットコインが開発された2009年の時点では革新的でしたし、今も稼働していますが、ネットワークコンセンサスをPoWプロトコルのみに頼るブロックチューンを維持する経済的なコストや環境コストは大きいですし、今後更に大きくなるでしょう。この問題は、Proof of Stake(PoS)スキームを用いることで解決できます。詳しくは「9: PoS Boo」を参照してください。

3. マルチアルゴリズムPoWマイニング

複数のPoWアルゴリズムの使用を通して、SHIELDはブロックチェーン上の均等な報酬の配分と51%攻撃への対策を実現しました。マルチアルゴリズムは複数アルゴリズムを提供することによって、様々なタイプのプロセッサーによるマイニングを可能とします。

我々のアプローチによって、SHIELDブロックチェーン上ではGPUとASICを同時に用いてマイニングを行うことが可能となります。アルゴリズム毎の報酬の配分は、時間に対する総ブロック報酬と比例しています。

例：x17アルゴリズムが300GH/sのネットワークハッシュを累積し、一方でblake2sアルゴリズムが50MH/sしか累積しなかった場合、両方のアルゴリズムで同量の時間当たりコインが配分されます。このような公平かつ平等なブロック配分システムによって51%攻撃に対する対策は強化されます。各アルゴリズムは独自の「スケジュール」に従います。つまり、51%攻撃に成功するには各アルゴリズムで51%のハッシュレートが必要となります。

このようなマルチアルゴリズムシステムの不可欠な要素として、各アルゴリズムの難易度を個別に調整している方法が挙げられます。難易度調整は「Dark Gravity Wave v3」スキーム(DGW)によって管理されています。もともとはDashのために開発されていますが、今では多くの暗号通貨に実装されています。DGWはネットワークハッシュのスパイク及びドロップを従来の難易度計算よりも効率的に管理し、悪意のあるマイナーがトランザクションを処理せずにコインを素早く採掘することをより困難にします。

4. 耐量子性

多くの既存の暗号通貨は、楕円曲線電子署名（Shorアルゴリズムに対し脆弱性を持つ）を用いているため耐量子性を持ちません。現在楕円曲線電子署名を使用しているトランザクションは、トランザクションの過程でユーザーのアドレスを公開し、クラッキングが可能な楕円曲線電子署名を外部に晒しています。そのような楕円曲線電子署名をクラッキングすることで、当該トランザクションに関わるあらゆる資産に対する不正アクセスを許すことになり、トランザクションの度に脅威にさらされることとなります。

SHIELDプロトコルはLamport署名、あるいは類似のスキームを導入することで、SHIELDネットワークのアドレス及びトランザクションに対し、耐量子性をもたらします。Lamport署名は

Shorアルゴリズムに対する脆弱性を持たないハッシュ関数に基づいているため、SHIELDユーザーに対しより一層のセキュリティをもたらします。

5. プライバシー（匿名性）

SHILEDのPerduプロジェクトは正しい道を進むために、先日見直しが行われました。当初のプランではVerge(XVG)で用いられているレイスプロトコルの実装が予定されていましたが、その相対的に仕様に不足がみられると判断され、Dashにより開発されたPrivateSendを実装することにしました。予定されているマスターノードの実装に鑑みても、PrivateSendを活用するという選択はより優位性を持っています。この変更により、InstantSendを用いたトランザクションの速度も向上されます。

ただし、PrivateSendの実装は改良ではあるものの、PrivateSend機能の実装だけではトランザクションを完全に匿名には出来ません。この問題に対処するために、Zerocoin または、zk-SNARKs/zk-STARKs の実装が検討されています。SHIELDの当項目に関わる詳細はQ2 2018に発表予定です。

ブロックチェーントランザクションの匿名性に加え、位置情報の匿名性を担保するため、SHIELDはエンドユーザーのIPアドレスと位置情報を匿名化するTor/I2Pウォレット/ノードを用います。

6. 資金調達

SHIELDの自己資金調達メカニズムは、マスターノード及びマイニングブロック報酬の一部（数パーセント)を使用する可能性があります。ただし、これは開発チームの活動を維持するためであり、残りの資金はマーケティング等に使用されます。また、開発者とユーザー双方に役立つプラットフォームの開発及び当該プラットフォームへの参画によって、外部の資金源からも支援を受けることとなるでしょう。一例ですが、SHIELDは多くの支援コミュニティから寄付を頂き、それによって開発の目標を期限通りに遵守してきました。さらに、SHIELDは様々なマイニングプールからも支援を受けています。

これらコミュニティによる支援は、SHIELDプロジェクトがロードマップを達成するための大きな力となります。SHIELDは、多くの競合する暗号通貨のようにICOやPremineを行いませんでした。

SHIELDでは、強く活発なコミュニティによってSHIELDがより有機的かつ最適な成長を遂げると信じています。

7. アプリケーションセキュリティ

セキュリティはこれからまでもこれからも常に SHIELD という通貨のコアとなる基本要素です。上述の耐量子性プロトコルの章で述べられている様に、我々は常に SHIELD のセキュリティ機能の改善に注力しています。

これまでの SHIELD の開発を通じて、私たちは数々のセキュリティ面の欠陥を発見してきました。その大多数は、ブロックチェーンとのやり取りを行う数多くのアプリケーションのユーザーインターフェースにおいて発見されています。これを理由として、私たちは我々独自のプロダクトのセキュリティを複数のレベルでテストすることを試みています。オープンソースコミュニティのリソースを活用することにより、ペネトレーションテスター（訳注：故意にアプリケーションへの攻撃を仕掛け、そのセキュリティを確認するプロセス）を集め個別のアプリケーションをテストし、開発チーム全員にコードをチェックさせ、理想的には（公式のアップデートの如何に依らず）、本番環境にアップロードする前に全ての新しいコードの組込みを承認するようにします。

我々の SHIELD Discord bot を用いた経験によると、セキュアなバックエンドに支持された、フロントエンドへのリンクが、安全なアプリケーションの最も重要な側面と考えています。

8. 統合（インテグレーション）

既存の、あるいは特定の目的を持って開発されているプラットフォームと新しい技術との統合は、SHIELD の究極的な適応性と汎用性を決定するのに無くてはならない要素です。我々は多くの人気かつ無料のプラットフォーム、例えば Discord, Twitter, Facebook 等、を SHIELD のユーザーエクスペリエンスを改善するために使用していきます。これらのプラットフォームとの統合はプラグインやボットの開発を通じて実現されます。これらが実現すると、ユーザーはウォレットアドレスを要求すること無く、友人、フォロワー、インフルエンサー等に送金をすることができるようになります。これらのプラットフォームとのより緊密な統合はプラットフォームに特化したウォレットの開発を含むことになるかもしれません。これによりユーザーは、ユーザーの SHIELD を使いたい時に、PC に存在するウォレットにアクセスするような必要性がなくなります。

より広範なレベルでの SHIELD の利用を促進するために、我々はネットワーキングや、外部の組織への接触を続け、SHIELD のユースケースを増やしていきます。こうして SHIELD の汎用

性を増していくことが、将来の SHIELD 価格の安定化をもたらすのに不可欠になります。

9.Pos Boo

Boo プロジェクトは、イーサリアムの PoS “Casper”をモデルとした、SHIELD 独自の PoS（Proof of stake）の仕組みです。Casper は PoSv3 において、悪意のあるステイカ―（通貨の保持者）を考慮に入れたリスクファクターを導入したことにより大きく前進しました。その前衛的なプロトコルの特徴が 51%攻撃などの攻撃を極度に難しいものにせしめました。例えば、悪意のあるステイカーは攻撃を仕掛けようとすると、発行済通貨の大多数を保持する必要があり、なおかつ攻撃に際してはそれらの通貨を全て失うリスクを負う必要があります。

取引完了の確認状態は主に、ステーキングとリスクファクターにより決定され、理論的には、51%を保有していたとしても攻撃を成功させる事を困難にしています。（Figure2 参照）
似たような攻撃がビットコインのような暗号通貨で行われた場合は大惨事が起きることになります。

プロジェクト Boo は今後取引の検閲の問題も解決していきます。PoW(Proof of work)においては、マイナーは特定のアドレスを含むブロックを採掘しない事を「選択」することが可能であり、それによりそのアドレスをネットワーク上から検閲できます（訳注：つまりネットワークを止めることが技術的には可能です）。PoS スキームにおいては、ブロック作成者はランダムに選ばれ、承認者は世界中に存在するために、特定のアドレスを検閲することは極端に困難になります。

10. 将来の展望

このホワイトペーパーを通じて、私たちはまだ最終的に決定されていないいくつかの特徴や仕様について論じてきました。Sharding や RSK スマートコントラクトなどは既にロードマップに置かれている一方で、このホワイトペーパーでは言及しませんでした。これは現在工数負荷の大きく、どのプロジェクトを採択していくか深く考える必要がある SHIELD プロジェクトの現状を反映しているためです。

このホワイトペーパーは SHIELD の今後の開発プランを完全に示したものではありません。SHIELD チームは今後親しみやすさや読みやすさを向上するため、また開発者が必要と感じた場合に、プロジェクトの詳細を提示するために、ホワイトペーパーの改訂を進めて行きます。

11. コアとなる仕様

要素	仕様
ブロックタイム	45 秒;(新たに鋳造されたコインが使用されるまでには)240 コンファメーションが必要。 SwiftTx/InstantSend
ブロック	500KB/Block
ブロックリワード	Figure1 参照
ブロック当たりのトランザクション	ワーストケース*:2777TX/Block ベストケース:14701TX/Block
一秒当たりのトランザクション	ワーストケース:61TX/秒 ベストケース:327TX/秒 詳細は Figure3 のグラフを参照
署名	楕円曲線 DSA (Lamport/Winternitz/BLISS オプションが使用可能)**
ミンティング(鋳造)	PoW(x17,blake2s, lyra2rev2, myriad-groestl, scrypt) Pos Boo (Quark*** hash and Slasher scheme)
マイニングフィー	0.05XSH per KB
プライバシー機能	Tor/I2p nodes, PrivateSend,Zerocoin****

*ベストケースとワーストケースはブロックのインプット/アウトプットにより決まります。これはインプットのほうがアウトプットよりもデータが重いためです。

**これから決定されます

***最終的な決定ではありません。

****最終的な決定ではありません。

参考文献

[1] Nakamoto, S. (n.d.). *Bitcoin*. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] Buterin, V. (2015). *Understanding Serenity...* Retrieved from https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/

[3] Vasin, P. (n.d.) *PoSv2* Retrieved from https://bravenewcoin.com/assets/Whitepapers/blackcoin-pos-protocol-v2-whitepaper.pdf

[4] Ben-Sasson, E(2014) *zk-SNARKs* Retrieved from http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

[5] cs.jhu.edu, (n.d.) *Zerocoin* Retrieved from http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf

[6] “CryptoRekt”, (2017) *Verge Blackpaper* Retrieved from https://github.com/vergecurrency/Verge-Blackpaper/blob/master/Verge-Anonymity-Centric-CryptoCurrency.pdf

[7] I2P, (n.d.) *I2P tech intro* Retrieved from https://geti2p.net/en/docs/how/tech-intro

[8] Tor, (n.d.) *Tor: The Second-Generation Onion Router Retrieved* from https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

[9] McAdam, S (n.d.) Shor’s Algorithm Retrieved from https://www.ma.utexas.edu/users/mcadam/monographs/Shor's_algorithms.pdf

Figures

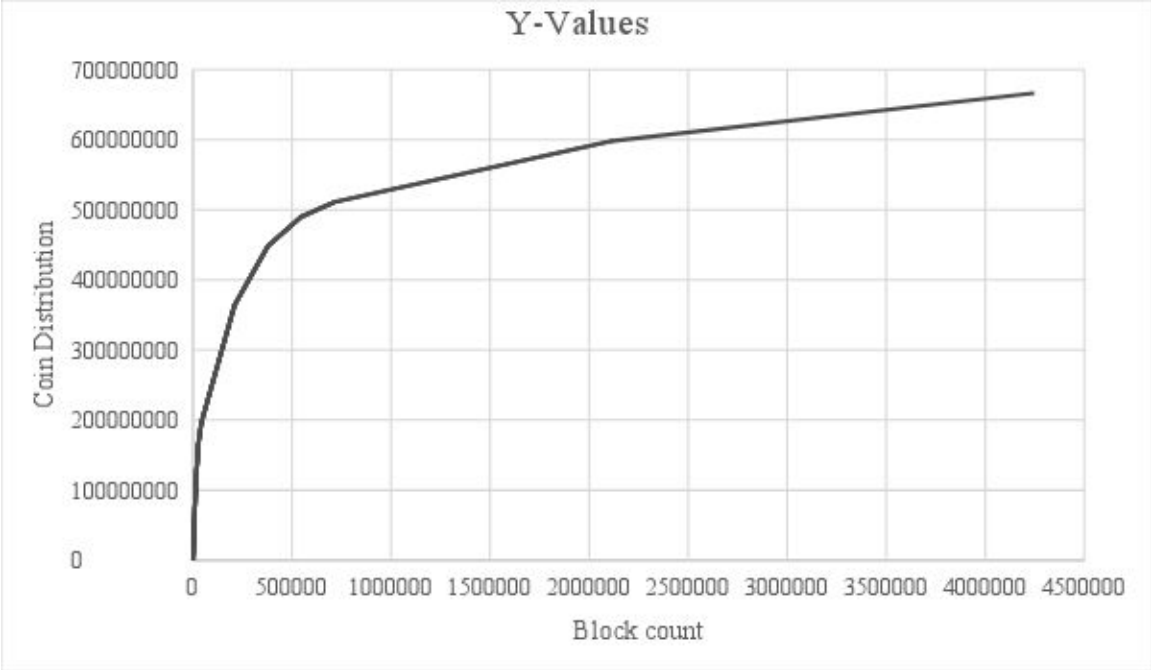

図 1. コインの配布 (y) ブロック数 (x)のグラフ

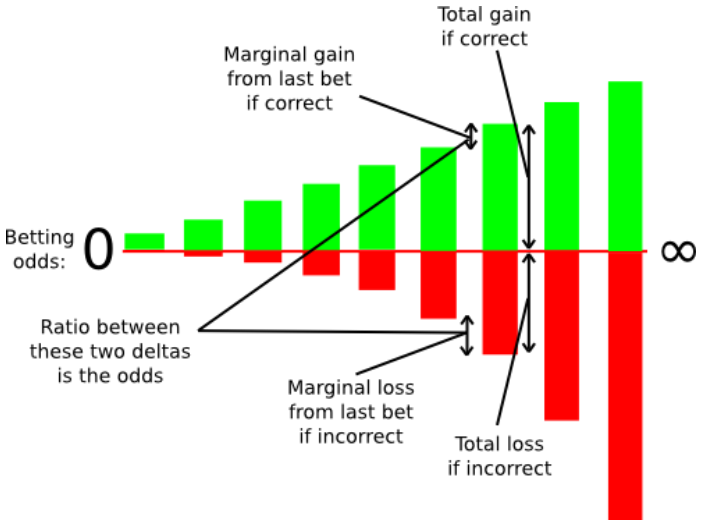

図 2. PoSキャスパーの賭けシステムの損失または利益のグラフ

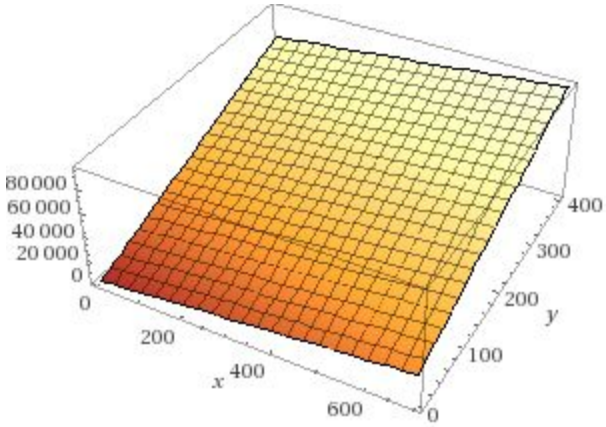

図3.入力（y）と出力（x）の3Dプロット。ここで、zはkBのサイズです。最悪の場合と最善のケースは常にZ = 500000です。これは、できるだけ多くのトランザクションを処理するためにブロックを埋める必要があるビットコインタイプのシナリオを前提としています。