日本語訳

SHIELD,
暗号通貨の改善と問題解決

The SHIELD チーム

ShieldCoin@protonmail.com

https://ShieldCurrency.com

概要

SHIELDプロトコルは、ECDSをLamport、WinternitzまたはBLISSシグネチャに置き換え、アドレスを「耐量子化」します。 **SHIELD**は自立的な開発サイクルを整え、このホワイトペーパーで説明するSHIELDプロトコル及びその他のプロジェクトの開発を継続することができます。 **SHIELD**はマスターノードを利用したカスタムPoSスキーム（PoS Boo）を採用します。また、マスターノードは、PrivateSendやInstantSendなどの機能を実現します。

キーワード：SHIELD、耐量子、マスターノード、暗号通貨、ブロックチェーン、匿名

1. はじめに

SHIELDは、サトシナカモトのブロックチェーン技術（2009年のホワイトペーパーにより発表）に基づく暗号通貨です。数年前から、ブロックチェーン技術がますます採用されてきましたが、この技術が主流になるのを阻む多くの問題がまだ残っています。SHIELDはこれらの問題の多くを解決しようとしています。

2. 解決すべき問題

ビットコインは実装されたときは本当に革新的でした。そして、サトシが作ったもののかなりの部分は今日でも多くの暗号化通貨の中核にまだ使われています。彼の遺産の1つはブロックマイニングですが、より具体的には単一のアルゴリズムを使用したブロックマイニングです。その為特定のアルゴリズムに特化して効率的に実行できる特別なハードウェア（ASIC）が開発が推進され、GPUマイニングは時代遅れのものになりました。 最近の多くの暗号通貨が認識しているように、彼が下した決定のひとつの誤りは、マイニングは実際には公平ではないということです。これについては、第3章「PoWのマルチアルゴリズムのマイニング」を参照してください。

量子コンピュータはますます洗練されてきており、一般に公開される可能性もあります。研究者、政府、企業、一般の人々のどちらにしても、最終的に、量子コンピューティングが自己利益目的のある裕福なグループや個人に利用可能となるでしょう。私たちの生活を大きく改善することができる信じられないほどの新技術ですが、この技術を懸念せねばならない理由も多くあります。その理由のひとつは、将来の量子コンピュータは現代の暗号通貨を効率的にクラックすることができるということです。多くの暗号化通貨では、ブロックチェーンが破壊されてしまう可能性があるということです。この問題をどのように解決するかについては、第4章「耐量子性」に概説されています。

FacebookやGoogleのような大企業は、あなたが誰であり、何を望んでいるかを知ることが年々上手くなっています。これは（現時点では）大きな懸念ではないかもしれませんが、それは企業が私たちを常に監視している世界に私たちが住んでいることを意味します。それはそんなに悪いことではないかもしれませんが、それは手放しで喜べるものではありません。現在、大企業や政府があなたの支出習慣を追跡できないようにするため、ユーザーの匿名性を維持すると主張している多くの通貨があります。これらのコインのいくつかの問題は、彼らが主張しているほど効果的ではなく、スケーラビリティと実行可能性がほぼないと言っていいほど低いことです。第5章「匿名機能」では、ユーザーを匿名にする方法について詳しく説明します。

いくつかのアルトコインには本当に有望なロードマップがあります。信じられないほど才能のある開発者を擁しているコインもあります。しかし、資金がなければ、コインの開発を継続することは不可能となります。開発者がプロジェクトから何らかの収入を得ることができなければ、開発にフルタイムで従事することが大変困難になるでしょう。 そのような自体が発生することは絶対に避けねばならないので、SHIELD（およびSHIELD周辺のプラットフォーム）に資金調達をサポートするいくつかの機能を実装する予定です。この解決法については、第6章「資金調達」で読むことができます。

ビットコインと他の多くの通貨のもう一つの問題は、マイナーが電力を大量に消費するハードウェアを使って造幣と取引の確認をすることです。当時は本当に革新的でしたし、現在も問題なくいっているように見えますが、ブロックチェーン（ネットワークコンセンサスのためのPoWのみの機能を持つ）を維持する経済的および環境的コストは非常に高いです。これは、第9章「PoS Boo」で紹介するPoSスキームで解決されています。

3. PoWのマルチアルゴリズム

私たちは報酬の均等な配分の実現と51%攻撃に抵抗するために、複数のPoWアルゴリズムを改善しました。マルチアルゴリズムのマイニングは、ブロックに対して複数のタイプの処理ユニットのマイニングを可能とする方法です。私たちのアプローチは、GPUとASICの両方を含む多くの種類の異なるデバイスがSHIELDブロックチェーン上で一緒にマイニングすることを可能にします。アルゴリズムごとの報酬の分配は、ほとんどの場合、時間に対する総報酬の割合とほぼ同じです。たとえば、あるアルゴリズムの能力が300GH / sで、もう1つが50MH / sであっても、1時間で同じ金額のコインを受け取ることとなります。ブロックの配布方法によって51%攻撃の防御力が向上します。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、このような攻撃の実行に成功するためには、アルゴリズムごとにハッシュレートの51%が必要です。このシステムの重要な側面は、各アルゴリズムの難易度をどのように個別に調整するかということです。

難易度の調整は、Dashのために開発され、他のさまざまな暗号通貨で使用されている「Dark Gravity Wave v3」方式で運用されています。ネットワークハッシュスパイクやネットワークハッシュドロップを従来の難易度計算よりもずっと良く管理し、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すばやく採掘することを困難にします。

4. 耐量子性

SHIELDプロトコルは、特定のアドレスの耐量子トランザクション/アドレッシングです。他の暗号通貨は、ECDS（量子コンピュータを使用することで可能になるShorのアルゴリズム[9]に脆弱である）の使用のために、しばしば量子耐性がありません。我々SHIELDは耐量子にするために、Lamportシグネチャーやそれに類するスキームを使う予定です。 Lamportデジタルシグネチャーはハッシュ関数に基づいており、ハッシュ関数はShorのアルゴリズムに対して脆弱ではありません。 ECDSでは、トランザクションを送信するたびに、あなたのクラック可能な（いわゆるハッキング可能な）ECDS署名が公開されているため、あなたのアドレスは脆弱な状態で危険に晒されます。そのような署名をクラックすると、そのアドレスに関連付けられた資金への不正アクセスが可能になります。ハッシュはShorのアルゴリズムに対して脆弱ではないため、ハッシュに基づくデジタルシグネチャーは、この脅威に対して影響を受けるアドレスのセキュリティを向上させます。

5. 匿名機能

SHIELDのProject Perduは、最近計画の変更を受けたものです。もともと、暗号通貨バージ（XVG）のWraithプロトコル[6]を実装する予定でしたが、スペックが比較的低いため、代わりにDashによって開発されたPrivateSendを選択しました。私たちは既にマスターノードを実装する必要があるので、我々SHIELDにおいてはPrivateSendの方がうまく機能します。この変更により、ユーザーがInstantSendを選択すればトランザクションの速度を早める事ができます。改良されていますが、PrivateSendはトランザクションを完全にプライベートにするわけではないため、Zerocoin [5]またはzk-SNARKs [4] / zk-STARKが検討中です。これについては、次の四半期(1〜3月中)に詳しく説明します。

物理的匿名性のために、エンドユーザーのIPアドレスとロケーションを隠すTor [8] / I2P [7]ウォレット/ノードを使用します。

6. 資金調達

SHIELD自己資金調達は、マスターノードとマイニングブロック報酬の一部を使用することで機能すると考えています。これは開発チームを持続可能とするため、そしてマーケティングのためだけに必要な小さな割合です。また、開発者とユーザーの両方に役立つプラットフォームを作成したり、参加したりすることで、外部の資金源による支援を受けることになるでしょう。たとえば、私たちはプロジェクト推進を支援するコミュニティから多くの寄付を受けていますし、様々なマイニングプールからも支援を得ています。これがプロジェクトを半永久的に推進することをサポートしてくれるでしょう。現時点では、多くの競合する暗号通貨のようなICOやプレマインは行いませんでした。それより、私たちは、強いコミュニティを持つことが、より良い方法であると信じています。

7. セキュリティーの応用

SHIELDはセキュリティに一番重きを置いています。前述の耐量子性に関して多くの点を改善しようとしています。しかし、一般的に、脆弱なアプリケーションがブロックチェーンとやりとりする傾向があり、大抵の場合、UIに脆弱な部分が存在することがわかりました。これが要因となり、私たちが多くの独自のプロダクトをオープンソースコミュニティを使ってテストし、個別で試用をするペンテスターを集め、公式か非公式に関わらずアップデートを公表する前に全てのプログラミングコードを我々開発陣で逐一チェックする必要がある。

Discordボットを使用した経験から、安全なバックエンドを使用することで、フロントエンドへのリンクが安全なアプリケーションにおいて最も重要なものの1つであることがわかりました。

8. 統合

新規または既存のプラットフォームに新しいテクノロジーを統合することは、その最終的な有用性および適用性を決定する際に影響を与える可能性があります。私たちはDiscordやTwitterのような一般的で無料の多くのプラットフォームを使用して、ユーザーエクスペリエンスを向上させます。私たちは、Disord、Twitter、Facebookなどのプラットフォーム用のプラグインと 'ボット'を開発することでこれを行います。この統合によって、SHIELD（XSH）を、送金先のWalletアドレスを要求する事なしに、送金する機能ができるようになります。この統合には、これらのプラットフォーム用のウォレットも含まれている可能性があります。この方法では、SHIELDを使用するために専用のウォレットをPCに置く必要さえありません。

統合は一般消費による使用実例を増やして行きます。つまり統合は、ネットワーキングと組み合わせることで、SHIELDの使用者や使用実例を拡大するための非常に重要な部分です。したがって、これらの要因を増やすために多くの関連ビジネスにコンタクトを取る計画です。これにより、価格の安定性がさらに高まり、より多くの適用性が得られるようになります。

9. PoS Boo

SHIELD Booは、PoSキャスパーに基づいた私たち独自のPoS方式です。 このキャスパー方式は、悪意のあるステイカーのリスクファクターの導入により、 "POSv3" [3]を最大限に改善します。このシステムは、51%の攻撃のような攻撃を実行することをかなり困難にするような進歩的なものです。このような攻撃を開始するときには、発行されているすべてのコインの大半が必要になります。また、そのような攻撃を実行しようとすると、そのコインをすべて失う可能性もあります[2]。最終的には主にステークとリスク要因によって決まります。その理由は、Bitcoinのようなコインにおいては非常に恐ろしい状況である、５１%のシェアを持った強力な攻撃であったとしても、攻撃を成功させることが困難となるからです（図2）。

PoS Casper/Booが解決するもう一つの問題は、トランザクションの検証です。 PoWを使用すると、ブロック・マイナーは特定のアドレスを含むブロックをマイニングしないように「選択」することができる。そこで、PoS Casper/Booによってそのアドレスをネットワークから検証します。ブロック作成者はランダムに選択され、検証ツールはこのPoSスキームではグローバルなので、ネットワークからのアドレスを検証することは非常に困難です（報酬を多く貰おうとしてネットワークを強制しようとすると、ほぼ確実に持分を失うことになるでしょう）

10. 将来の展望

第5章でお気きになったように、まだ完成していない将来実装する可能性のある機能や仕様について説明します。ロードマップにSHIELDの将来持ちうる可能性のある特徴と

して、「シャーディング」や「スマートコントラクト」がありましたが、このホワイトペーパーには記載されていません。これは、SHIELDの多くが依然として重い開発と慎重な検討の下にあるためです。

将来、私たちの変更に応じて、このホワイトペーパーを更新するか、新しいホワイトペーパーを作成します。このホワイトペーパーはSHIELD開発計画の決定版ではありません。さらに、このペーパーでは、近づきやすさ、読みやすさを向上させる複数の改訂版を用意し、項目ごとに必要となる詳細を提供していきます。

11. 中核となるスペック
注意：以下のスペックは将来計画中のものを含みます。
私たちは以下のスペックをSHIELDの中核として使います。

項目	スペック
ブロック時間	45秒; 240検証; SwiftTx/InstantSend
ブロック	500kB/block
ブロック報酬	図１参照
トランザクション/ブロック	最低のケース：2777 tx/block　最適のケース：14701 tx/block
トランザクション/秒	最悪のケース：61 tx/s　最適のケース：327 tx/s 図３のグラフを参照
署名	ECDSAと選択可能なLamport/Winternitz/BLISS 署名
造幣	x17, blake2s, lyra2rev2, myriad-groestl, そしてscryptを使用したPoW。 Quark[1] hash と Slasher 方式を使ったPoS Boo。
トランザクションマイニング報酬	0.05 XSH/kB
匿名機能s	Tor/I2P nodes, PrivateSend, Zerocoin

1

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

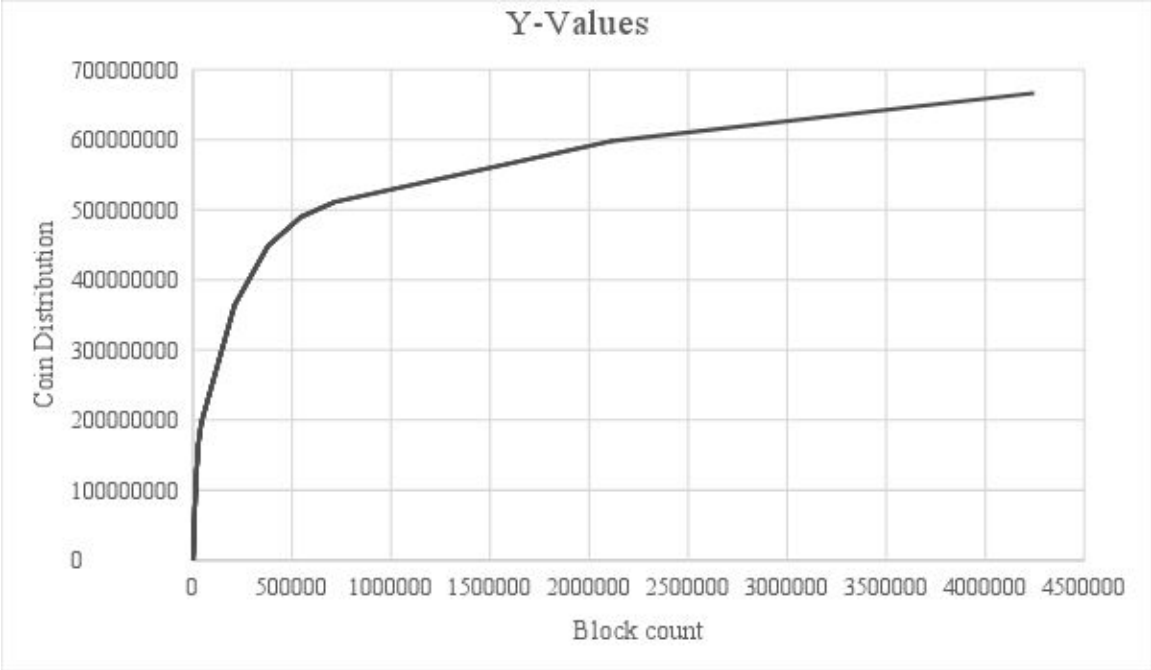

図 1. コインの配布 (y) ブロック数 (x)のグラフ

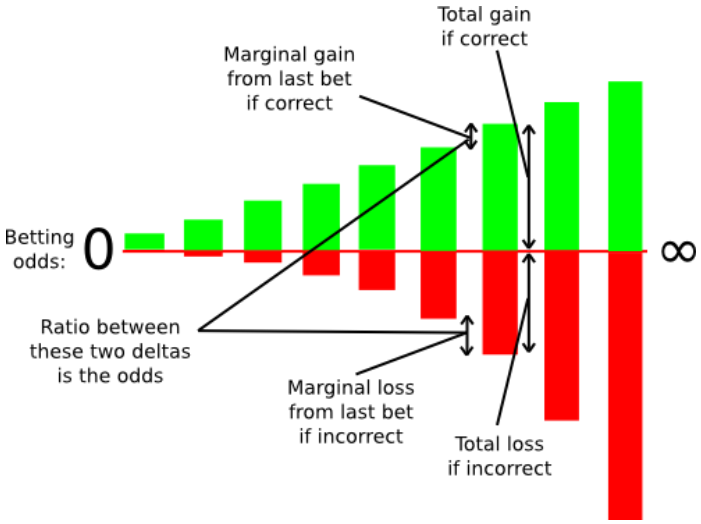

図 2. PoSキャスパーの賭けシステムの損失または利益のグラフ

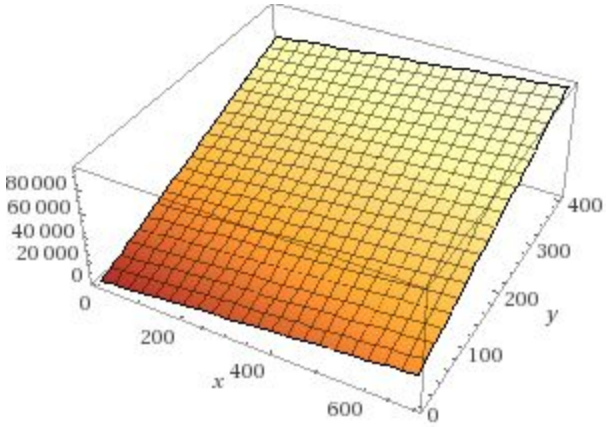

図3.入力（y）と出力（x）の3Dプロット。ここで、zはkBのサイズです。最悪の場合と最善のケースは常にZ = 500000です。これは、できるだけ多くのトランザクションを処理するためにブロックを埋める必要があるビットコインタイプのシナリオを前提としています。