BULWARK
CRYPTOCURRENCY

Bulwark 仮想通貨白書

Bulwark Core Team
(Bulwark コアチーム）：

Eatbatterys (プロジェクト･コーディネーター)

Jack (マーケティング・ディレクター)

SerfyWerfy (ブロックチェーン・デベロッパー)

Frogman (コミュニケーション・リーダー)

Patrick (ブランドおよびデザイン)

Stu (エコシステム・デベロッパー)

Bulwark コアチーム

2017 年 12 月

私たち、Bulwark コアチームはこの白書に記載されたものは私たち独自のものであることをここに確認します。他の情報源から引用されたものは、それぞれ引用元を記載しています。

概要

Bulwark (ティッカー: BWK) は、コミュニティを主体としたコインです。このコインが創られた理由は、マスターノード・プライバシーコインが不公平な取引に利用されていることを危惧したためです。私たちの提供する、計画的で公平な市場投入計画により、賛同者は、初期段階から、この有益なプロジェクトに参加できます。私たちは、簡易な Value Proposition (バリュー・プロポジション)を提供し、過大なお約束はしません。私たちは、プライバシーコインを提供し、そのコインは、将来に渡って長期的に使えるもので、DASH と PIVX の成功事例を活用したものです。大仰なビジョンのもと、限られた人だけが恩恵を得るのではなく、私たちは、今利用できるプライバシーコインを、今使える環境で、長期的にサポートしていきます。しかし、私たちは革新的なことを何もしないというわけではありません。むしろ、大げさな夢物語ではなく、現実的なことを提供します。すでに世の中には、大量の仮想通貨が流通していますが、多くは、過大広告に踊らされ、しかも現実味には欠けています。私たちは、そのような、過大広告を掲げた、中身の欠如した通貨を作るつもりはありません。ICO の不在、Soft Launch Reward Ramp （ソフトローンチ報酬プログラム）、Premine（プリマイン、事前採掘）を最小限に抑えること、そして、採掘者を優遇したブロックリワードの配当、これらを基に、Bulwark の保有者は、プライバシーコインに好条件でアクセスすることができます。マスターノードと現存する最高のプライバシーコイン技術が融合し、そして、重要な Development ロードマップにアクセスが可能です。マスターノードは、公開された時点で、アクセス可能であり、機能しています。この機能は、このコインのビジョンの根本です。流通を安定させ、ネットワークを確実なものとし、さらに重要な機能を与えます。

謝意

Bulwark は、先駆者である Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash and PIVX チームの偉大な功績があってこそ、生まれました。オープン ソース ソフトウェアとその貢献者たちは、常に新たな更なる革新へと道を開いてきたのです。情報と知識が自由に構築されるとき、社会全体ははその恩恵を受けます。私たちもまた、その先駆者のおかげで、この発展し続けるエコシステムに貢献できることを心から感謝いたします。

目次

1 章

仮想通貨の歴史

1.1 背景

2009 年、ナカモトサトシは、商取引のビジョンを記した論文、「ビットコイン：P2P 電子マネーシステム」を発表しました。P2P 通貨システムは、ハッシュを基にしたプルーフオブワーク（PoW）によって保護されます。ネットワークは、進行中の ledger（ログブック、台帳）に、ハッシュを使ってトランスアクションをタイムスタンプします。これは、PoW を変更しない限り、変えることはできません。ノードは、貯められたハッシュの中から、最長のチェーンを選択し、これがイベントの証拠となります。ネットワークの５１%以上のハッシュが攻撃性を帯びないノードに制御されている限り、チェーンは最長であり続けます。（ナカモト　2009 年）

1.2 ブロック

ネットワークの各ブロックは、以下のもので始まります。その前のブロックのヘッダーの二重 SHA256 ハッシュコピーを含んだ、80 バイトのヘッダー、Merkle ルート（ブロック内で発生した全てのハッシュから派生した二重 SHA256）、POW が開始されたタイムスタンプ、このヘッダーのハッシュを目標とする難易度（より小さいか等しい必要があります。）、採掘者が目標とした難易度に到達した時点でのノンス。ブロック内のトランスアクションを変更しようとすると、ネットワークの採掘者によるブロックの拒否が発生します。（Bitcoin Core Team　2017）

1.3 ブロックチェーン

トランスアクションは、ブロックとして構成されます。時系列に従って並べられたブロックがチェーンとなったものがブロックチェーンです。ブロックチェーンはネットワークで起きたすべてのアクションを記録し続ける履歴となり、分散型コンセンサスモデルとしての役割を担います。ここで、すべてのトランスアクションがいつでも承認されることができます。(Crosby et al. 2015)

1.4 プルーフ・オブ・ワーク

プルーフ・オブ・ワークとは承認システムであり、採掘者が有形資源（電気、ハードウェアなど）を使って、任意の確率論“Word Puzzle (ワードパズル)”を解答しなくてはいけません。ブロックチェーンを変更するためには、すべてのプルーフオブワークを現時点まで完成させる必要があります。

(Okupski 2016)

2 章

Bulwark について

2.1 確かな基盤

全ての家は、確実な基盤の上に成り立ちます。Bulwark も同じです。Bulwark は、PIVX に基づいて作られており、その PIVX は、評価の高い Dash 仮想通貨を基に作られました。全ての履歴は、オリジナルである Satoshi Core につながりますが、それぞれのプロジェクトは、属するコミュニティの目的や考えによって、方向性が異なります。私たちは、先駆者のプラットフォームのプライバシーコインに焦点を合わせ、拡大していきます。その一方、新しい技術の模索、Bulwark を今日の技術プラットフォームに統合していくツールや機会を創造していきます。

2.2 コミュニティに特化したチーム

あるプロジェクトにとっては、コミュニティというのは、優先事項ではありません。Bulwark にとっての最優先はコミュニティです。Bulwark は、譲渡、コンテスト、活発な議論の場、初心者に対しての嫌がらせは厳禁など、あらゆるエンドユーザーのための仮想通貨であろうと努めています。私たちのメンバーは、ユーザー経験をさらに高めるために役立つスクリプトやガイドを作って貢献しています。

2.3 公平さと均衡

これを書いている時点で、似たような技術を使っている仮想通貨が多くあります。使われている技術は確実なものですが、それらの仕様やブロックチェーンパラメーターを注意深くみると、とても公平な取引とは言えないことがわかります。

2.4 Pre-Mine（事前採掘）の問題

2.4.1 事例：FooBarBaz Coin

昨今の仮想通貨業界では、遠い将来の任意の日付を選択し、その日付で流通しているコインの Pre-Mine の割合を決定しています。以下で、架空の FBC （FooBarBaz コイン）、Dash Fork というコインの例を見てみましょう。

- Block Reward（ブロック･リワード）: 15
- Block Time(ブロック・タイム): 2.5 分
- POW/Masternode Split（PoW/マスターノード・スプリット）: 50/50%
- Initial difficulty algorithm（初期のアルゴリズムの難易度）: KGW
- Subsidy decreases by 12% each year　（補助は毎年１２%減額）
- Maximum Coin supply（最大コインの供給量）: ~25 Million
- 2.5% pre-mine

この例では、2.5% Pre-Mine は 643,000 コインになり（～25 Million）、一見、理にかなったもののように見えます。PoW とマスターノードリワードのコインをデベロッパーの保有するコインと一致させるために、約 43,000 ブロックが必要となります。2.5 分/ブロックを目標として、採掘者は必要とされるコインを採掘するのに約１５０日（または丸７５日）必要とします。７５日後でも、デベロッパーは、既存するコインの総量の半分を保有していることになります。

2.5 より公平な代替案

Bulwark チームは上記の問題に気づき、公平であろうと決意しました。私たちの Pre-Mine、489,720 コイン（3.5%）は、12 日間強の PoW マイニング、または、全体のプロダクションとして、10 日間強で得られます。コアチームの保有するコインに関係なく、私たちのコインの市場価値が極端に下がることはないと安心してもらえればと思います。下図のとおり、両方のシナリオで 180 日間を例として比較しますが、違いは明確です。この課題に真摯に優先的に取り組むことにより、コミュニティ全体に利益をもたらす役割を果たすことを希望しています。

2.5.1 両者の比較

図１他者（FBC）の方法論

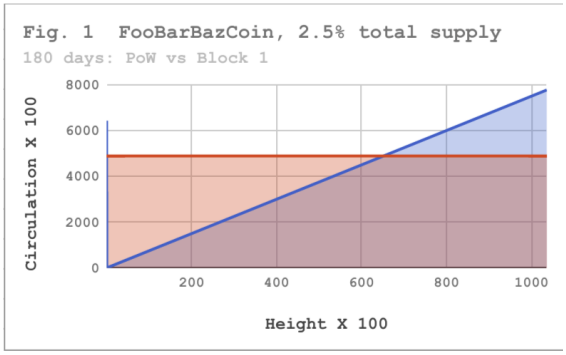
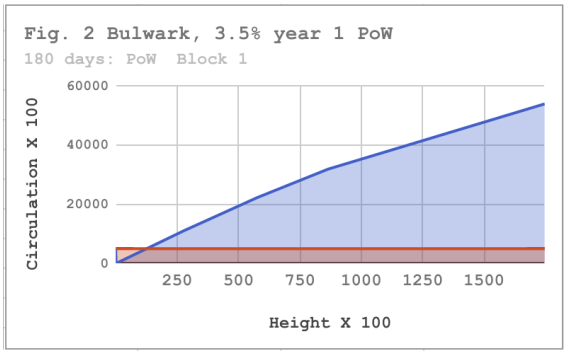


図２私たちの方法論



2.5.2 Instamine と私たちのアプローチ

Dash（Darkcoin）は Instamine の保護を必要とする興味深い事例です。コインが市場に投入された数日内に、全供給量の１０－１５%が、ある一部のユーザーに保有されてしまいました。（Wiecko 2017）この問題に対するアプローチは、二段階あります。私たちは緩やかな補助金を利用しました。最初の 960 ブロック(1 日目)がフルブロック報酬まで、直線を描いて増加し、ブロック報酬の１００%がその日も採掘者に向かうというものです。過去においては、とても小額のブロックリワードを与えられますが、それが突然フルブロックリワードにシフトします。プールは故意に DDoSED（サービス拒否）されたり、新しい採掘者が激増します。直線的に報酬が増えれば、採掘者やプールの運営者に金銭的利益を与えることを妨害する意味がありません。

2.5.3 ICO?ではなく IC-NO!

正直に認めてみましょう。私たちは絶えず ICO に提供されています。仮想通貨のエコシステムにおいて正当ではありますが、ほとんどの場合においては、ごく限られた人が恩

恵を受けられるだけです。Bulwark は、まずマスターノード・リワードを、そして、第二段階では、POS リワードを提供します。富の集中は巨大な市場変動を引き起こす可能性があります。ガバナンシステムは、最も初期の（そして最も富裕な）採用者のために有利に働く傾向があります。富の集中は全体として避けられませんが、私たちは、フィールドを公平にするために、あらゆる可能性を探っています。私たちは、他のプロジェクトに見られる富の集中を理想的に回避しながら、多くのユーザー間に Bulwark を広く配布することを奨励する公正なスタートの仕組み、スケールド・ブロック・リワード戦略を打ち出しました。

2.6 迅速さと機能性

90 秒のブロックタイム、マスターノード・コンセンサスとトランスアクション・ロッキング、合理的なエミッション・スケジュール、エコフレンドリーなステーキングと、Bulwark は迅速かつ機能的な仮想通貨を目指します。

3 章

ブロックチェーン・パラメーター

3.1 Bulwark の仕様一覧

Bulwark 仕様一覧

仕様 Specification	デスクリプター Descriptor
Ticker （ティッカー）	BWK
Algorithm （アルゴリズム）	NIST5
RPC Port	52541
P2P Port	52543
Block Spacing （ブロックタイム？）	90 Seconds （90 秒）
Difficulty Algorithm（アルゴリズム難易度）	Dark Gravity Wave v3.0
Block Size （ブロックサイズ）	1MB
Mined/Minted Maturity （採掘/Mint 成熟度）	67 Blocks (~100 Minutes)
Confirmation （確認）	6 Blocks (~9 Minutes)
Circulation (1 Year) （循環 1 年）	14,505,720 BWK
Circulation (5 Years) （循環 5 年）	27,668,220 BWK
PoW Period （PoW 期間）	≤ 345,600
PoS Period （PoS 期間）	≥ 345,601
Protocol Support （プロトコル・サポート）	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS, PIVX SeeSaw rewards.

3.2 スロースタート

私たちの公平なスタートは以下のコード・スニペットを提供します。(クレジット: ZCash)

```
        int64_t nSlowSubsidy = 50 * COIN;

        if (nHeight < 960 / 2) {        // If block height less than 480,
           nSlowSubsidy /= 960;         // Set nSubsidy to .05208333
           nSlowSubsidy *= nHeight;     // Multiply present height by .
05208333
        } else if (nHeight < 960 {      // ex: Block 200, BR will be
10.41666600
            nSlowSubsidy /= 960;        // Credits: ZCASH Team
            nSlowSubsidy *= nHeight;
```

3.3 Dark Gravity Wave 3.0

Dark Gravity Wave は Bulwark によって開始当時から使われており、PoW の難易度を

変更する手段として使われます。簡単な“Moving Average”を使用しますが、これは Nethash に反応して、数ブロック以内に、増加するか、ドロップオフするかを決めます。これは Multipool に引き起こされがちな”Stuck block effect” を減らし、意図的に計算能力を増加して数ブロック以内よりも早く問題を解決するのを防ぎます。

4 章

ブロック・リワード

4.1 PoW ブロック・リワード

Subsidy（補助）	Block（ブロック）	PoW	MN	Circulation（循環）
489720	1	100%	NA	489200
~25(avg)	2-960	100%	NA	513150
50.000	961-28800	80%	20%	1391950
50.000	28801-57600	75%	25%	2831900
50.000	57601-86400	66.6%	33.3%	4271850
43.750	86401-172800	50%	50%	8565056
37.500	172801-259200	50%	50%	11801306
31.250	259201-345600	50%	50%	14501275

PoW ピリオド・ブロック・リワード仕様

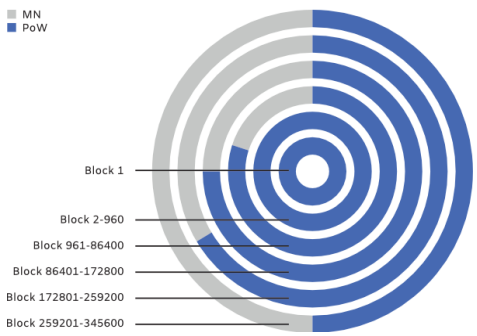


図 4.1: PoW ピリオド・ブロック・リワード　Period Block Reward

4.2 PoS ブロック・リワード

PoS ピリオド・ブロック・リワード仕様

Subsidy（補助）	Block（ブロック）	Budget（予算）	PoS/Masternode	Note
25.000	345601-432000	10%		Year 2
21.875	432001-518400	10%		Year 2
18.750	518401-604800	10%		Year 2
15.625	604801-691200	10%		Year 2
10.250	691201-777600	10%		Year 3
10.938	777601-864000	10%		Year 3
9.3750	864001-950400	10%		Year 3
7.8120	950401-1036800	10%		Year 3
6.2500	1036801-1123200	10%		Year 4
5.4690	1123201-1209600	10%		Year 4
4.6880	1209601-1296000	10%		Year 4
3.9060	1296000-1382400	10%		Year 4
3.1250	1382401-1468800	10%		Year 5
2.7340	1468801-1555200	10%		Year 5
2.3440	1555201-1641600	10%		Year 5
1.9530	1641601-1728000	10%		Year 5

1.6250	1728000+	10%	以下 同様

5 章

NIST5 ハッシュ

5.1 NIST5 を使用する理由

NIST5 は、2014 年 TalkCoin によって名を知られるようになりました。NIST5 のハッシュアルゴリズムは、まだそれほど広く使われていません。NIST5 は、一般のハードウェア、CPU、AMD 、NVidia GPU などでの採掘が可能です。NIST5 は、ほかのメモリーハードアルゴリズムのように ASIC 耐性があるわけではありませんが、システムの安定性を高めるため、そしてほかのメモリーハードアルゴリズムに比べて、消費電力を減少させるために交換することは可能と思われます。ファームウェアのアップデートとして、NIST5 サポートが ASIC に追加されるとき、それが PoW 期間が終わる前であれば、アルゴリズムを交換する用意はあります。必要であれば、コミュニティで多数決をとります。PoW 期間は短く、アルゴリズムを交換する意欲があるので、ASIC 製造者との間に問題が起きることはありません。

5.2　5 つの最終候補（NIST　SHA-3 コンペティション）

NIST5 に使われる、5 つのハッシュアルゴリズムは、NIST ハッシングコンペティションのファイナリストです。(Chang et al. 2012)　以下にブロックがハッシュされた順に最終候補を挙げます:

Blake (Aumasson 2013), **Grøstl** (Gauravaram1 et al. 2012), **JH** (Wu 2012), **Keccak** (Bertoni et al. 2012), and **Skein** (Ferguson et al. 2010)

5.3 新しい SHA-3 スタンダード

Keccak が最終的に勝利し、新しい SHA-3 ハッシュ機能に名づけられました。ほかの 4 つのアルゴリズムは（技術的に安全と考えられているにも関わらず）マイナーな技術面において審査で数ポイントを失いました。新しい SHA-3 スタンダードとほかの 4 つの最終候補を組み合わせることで、迅速、安全そして、確立されたハッシュアルゴリズムを提供できると考えています。

5.4 採掘ソフトウェア

この原稿を書いている時点で、採掘者にはいくつかの選択肢があります。

名前	プラットフォーム	リンク
SGMiner-5.0	OpenCL	GitHub
ccminer-2.2.2	CUDA	GitHub
cpuminer-opt	CPU	GitHub

6 章

特徴

6.1 マスターノード Masternodes

マスターノードは、特に、Bulwark ネットワークに使われるコンピューターの分散ウェブです。マスターノードは重要なネットワークの役割があり、ブロックリワードの一部も受け取ります。コインの供給の安定、トランスアクションの処理、ネットワークの保護によって、Bulwark のエコシステムを支えます。マスターノードは 5000BKW を必要とし、操作するのには特別な技術知識は要りません。

6.2 難読化/コイン・ミクシング

Bulwark は難読化を特徴としています。CoinJoin を基にしていますが、オリジナルに更に改良を加えています。分散したコイン･ミクシングによって行われ、マスターノードがこれを簡単にします。これはトランスアクションのプライバシーを更に強化します。完全な保護ではありませんが、ノード･ミクシングによる難読化はスタンダードなビットコインのトランスアクションよりははるかに優れたものです。たとえば、全てのビットコインのトランスアクションは公です。Bulwark は、悪意を持つものは、操作中のマスターノードの 50%をコントロールしなくてはいけません。それでも、８ラウンドの難読化をされた一つのトランスアクションを特定できるチャンスは 0.5%以下にしかなりません。（Kiraly 2017b）これは重要な特徴で、トランスアクションをプライベートにしたい BWK ユーザーにとっては、非常に高いレベルで匿名性を確保できます。

6.3 SwiftTX

SwiftTX はマスターノードを供給しますが、これによりトランスアクションの権限を同意し、ロックします。トランスアクションがネットワークに提出され、マスターノードがそのトランスアクションを確認します。マスターノードがトランスアクションの有効性を確認したあと、ブロックチェーンにロックされます。従来のシステムに比べ格段に早いスピードでトランスアクションを処理できます。（例：ビットコインは、複数の確認に 10 分のブロックタイムを必要とします。）SwiftTX は複数のトランスアクションの処理を可能にしており、それもネットワーク上のブロックが同じインプットで採掘さ

れる前に処理が可能です。このシステムは Dash の InstandSend に基づいています。（Kiraly 2017a）

6.4 Sporks

Bulwark ネットワークは、Sporking として知られる多層のフォークメカニズムを使用しています。これにより BWK ネットワークは、ロールアウト中に起こる、予想外のネットワークのフォークを最小限に抑えながら、新しい特徴を実行することが可能になります。Spork の変化はネットワークにより展開可能であり、必要に応じてオン・オフにすることが可能ですが、ノード・ソフトウェアのアップデートは不必要です。（Strophy 2017）この特徴は特に有益で、ネットワークが脆弱性の保護に迅速に対応できます。

6.5 TOR & IPV6 マスターノード

Bulwark ユーザーは、それぞれのオニオン・アドレスあるいは IPV6 アドレスからのフルノードやマスターノードを使うことができます。私たちは TOR ネットワークを強化するために TOR ノードをフルで加えるように改良してきました。Bulwark ユーザーは TOR モードのみでも使うことが可能です。TOR マスターノード独自の特徴は、あなたのマスターノードを TOR の隠れた役割として利用できることです。TOR ノードを利用することで、ユーザーはマスターノードを自宅のネットワークで利用することができます。それぞれのロケーションや自宅のネットワークを公になる恐れはありませんので、攻撃や妥協を心配する必要もありません。

6.6 コミュニティの重要性と管理システム

Bulwark コミュニティはプロジェクトの長期的な成功のために最も大切な要因です。最も重要なのは、コミュニティがコインの将来をコントロールできることです。PoW のフェーズが終了する時には、バジェット・スーパー・ブロックをネットワーク上でアクティベートする予定です。このスーパーブロックは、毎月支払われ、コミュニティは、Bulwalk の発展、ブランド、コミュニティ・イベントに関する全ての要因をコントロールできます。このシステムのアクティベーションを遅らせることで、さらに必要なフレームワークを発展させて、ユーザーエクスペリエンスをポジティブなものとし、採掘者とマスターノードへのブロックリワードを最大とすることができます。

提案を創造し、提出するのにはいくつかのプロセスがあります。各ステップはそれぞれ完全に終了しなくてはいけません。各ステップを終了できなかった場合、その提案がアクティベートされることはまずありません。基本的なアウトラインは以下のとおりです。

・Discord でチャットを始め、経験のあるユーザーと話をします。反応が良好であれば、次のフェーズに進みます。

・いくつかのソーシャルメディアをつかって、ディスカッションをして、フィードバックを得ます。Bulwark のユーザーは多様に富んでおり、様々なレベルの参加者がいるので、これらのユーザーベースからフィードバックを得るのは、時間と労力がかかります。ディスカッションを記録し、引用を正式な Pre-proposal（予備/事前提案書）に記入してください。引用の数が多いほど好ましいです。

・コミュニティやデベロッパーからの提案に耳を傾けてください。あなたの提案に対する、他の人の考えや意見も柔軟に取り入れてください。

・Burwalk のウェブサイトに行き、Governance->Pre-Proposal をクリックして、Pre-Proposal を作成してください。上記のステップで行った全てのディスカッションからの引用を記入してください。あなたの Pre-Proposal を、ブロックチェーンの投票に提出する正式書類のように、慎重に作成してください。

・上記のステップを完了したら、ブロックチェーンにあなたの提案を提出します。２つの費用が必要です。一つは提出時に払うもの、もう一つは投票料で、デベロッパーに支払われますが、ブロックチェーンにあなたの提案を反映させてアクティベートさせるための費用です。提案料は返金不可ですが、投票料は、あなたの提案が承認され、アクティベートされる時に支払います。

・全ての人は、2 つの必要費用の返還を含め、提案を調整することができます。正式な提案書に、費用の返還を請求する旨を記入してください。

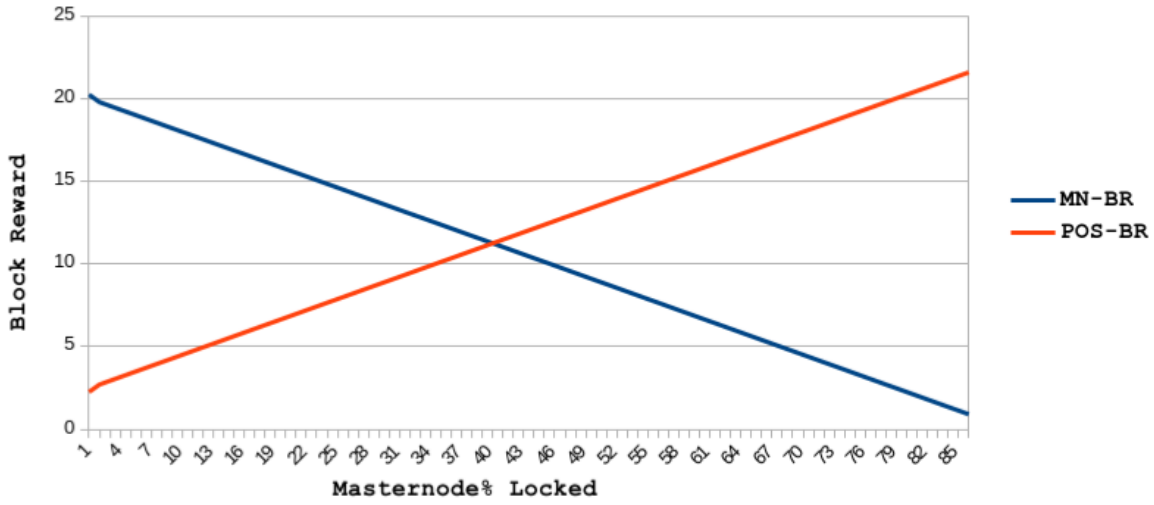
・あなたの考えが賛成票を集められるよう、話した全ての人とコンタクトを取り続けてください。資格のあるマスターノードの１０%があなたの提案に賛同すれば、その提案は承認されます。１０%の賛同票を得るのは簡単ではありません。熱心さ、十分な情報提供、敬意を持った態度で、票を獲得できるよう努力してください。

6.7 SeeSaw PoS/マスターノード・リワード

私たちは、PIVX（jakiman 2017）によって一般化された SeeSaw リワードシステムを採用することに決めました。 SeeSaw リワードシステムは、9：1 のブロック報酬率（マスターノード優先）で始まり、循環している４１．５%のコインがマスターノードにロックされるまで、ステーキングとノードオペレーター間の報酬の比率をスムーズに調整します。この時点で、コイン単位で見れば、ステーキングリワードはマスターノードリワードをわずかに上回ります。私たちが SeeSaw がステーキングリワードをわずかに優遇する理由は、大きな価格変動と低い流動性のような問題を回避したいためです。これは循環型供給の非常に高いパーセンテージでノードに固定されたコインに影響を与えるからです。この戦略は、コイン供給へのアクセスに対するユーザーの不満を軽減し、私たちのネットワークの重要性を維持できます。私たちのゴールの一つは、匿名の商取引のため、プラットフォームを十分にサポートすることです。Bulwark を使用し、保有する人にとってトランスアクションは最も重要です。

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



7章

7章　今後

7.1 Bulwark ツール・チェスト

Bulwark ツールチェストは、コード・スニッペット、API、図書館、原稿、知識のコレクションです。デベロッパーは、これらのツールを無償で使うことができます。私たちは、これらのツールをデベロッパーに提供することは、大工に必要な道具を貸して、傑作を作り出せるよう、手を差し伸べるのと同意と思っています。

7.2 プライバシーとソフトウェアの強化

私たちは新しいプロトコルを採用してユーザーベースのプライバシーを獲得しようとしています。現在検討している選択肢がいくつかあり、2018 年前半に内部テストと開発を始める予定です。例を挙げると：

・I2P プライバシー･ネットワーク

・ゼロ・コイン・プロトコル、または Stealth addressing （私たちが、この性能を確信したときに採用します。）

・私たちのコードベースをビットコインのメインラインに近く同期化する。

・QT wallet を簡素化/アップデート

・Libtox の統合

・Bulwark wallet の仮想化/コンテナ化をし、保護を更に強化する

7.3　Bulwark の保護ホームノード

私たち、CAD のスペシャリストと、小さな自己完結型の Bulwark ホーム･ノードを設計しています。ユーザーは、これをそれぞれのホームネットワークに接続し、Web UI を使って設定できます。私たちが目指している機能は以下の通りです。

・安定したインターネット接続があれば、Fully Onionized マスターノード（またはフルノード）は、TOR hidden service を使って設定することは簡単です。

・オプションとして、TOR ネットワーク全体を向上させるリレーとしての機能。

・VPN および／または Proxy は、TOR/I2P ネットワークと通して、ホームインターネット･トラフィックにルートをつなげることに使えます。

・Bulwark ステーキングは、仮想化かアドオンデバイスで可能。

分散化の考えのもと、３ D でプリント可能なファイルと、全てのソースコードがコミュニティに無償で与えられます。

7.4 私たちのブランドの拡張

私たちは、ブランドを拡張し続け、同じビジョンや理想を持つ、ハードウェア・ヴェンダーやシステム・インテグレーターとも連携する意図を持っています。5 年以内には、私たちの Bulwark という名前は、仮想通貨の名称のみでなく、プライバシー、保護、そしてユーザーのフリーダムへの敬意を表す言葉であってほしいと思います。Bulwark の主な目的は、プライバシーを通して、選択の自由を供給することです。

7.5 デザインとビジュアル

リサーチと開発を通して、Bulwark のビジュアル･デザイン･ランゲージを作ります。これにより、Bulwark は仮想通貨の市場において、競合社から一線を隠した存在になります。当社の設計チームは、現在の UI/UX/ブランディングを革新し、実験し、最終的に優れた設計を作り出す予定です。目的は、最良のユーザーエクスペリエンスを可能にするメディアと、革新的で美しい美学を探して、最終的に優れたデザインを実現します。これは競合他社を調査し、現在の技術動向と基準を守り、エンドユーザーに新しいエキサイティングなビジュアルを提供するよう絶えず努力して行われます。

8 章

結論

8.1 要点

Bulwark はプライバシー志向のコインで、マスターノード、コントロール、進化し続けるエコシステムのツールを伴っています。このプロジェクトは、公平なローンチ、コインの広い流通を目的に始まりました。スロースタート、ブロック·リワードの分割、ハッシュ·アルゴリズムは、計画的に取り入れられましたが、これらはコミュニティに機会を与えるものです。Bulwark は数多くの重要なプライバシーコインの特徴を備えて始まりました。開発チームは、新しい特徴を取り入れるのに忙しく働き、技術を改良し続けています。Bulwark はプライバシーを通じて、選択肢を与えられるように目指し、努力しています。

8.2 今後の方向性

マスターノード・プライバシーコイン・エコシステムは、膨大な数のコインで溢れかえり、その多くは、ハイリターン、不可能なゴールで満ちた巨大なロードマップ、マーケティングに焦点を合わせていますが、価値を提供することに焦点を合わせることはありません。Bulwark は、その正反対であろうとしています。必要最小限のマーケティング、実際の価値の提供をします。現在と今後のプロジェクトのゴールは、具体的、測定可能、達成可能、関連性のあるもの、時間的に可能なものである、というフォーマットに従います。

参考文献

Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Available at: https://131002.net/blake/blake.pdf.

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Available at: https://keccak.team/files/Keccak-submission-3.pdf.

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Available at: https://bitcoin.org/en/developer-reference#block-headers.

Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Third-round report of the sha-3 cryptographic hash algorithm competition. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Available at: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family. Available at: http://www.skein-hash.info/sites/default/files/skein1.3.pdf.

Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2012. Grøstl – a sha-3 candidate. Available at: http://www.groestl.info/Groestl.pdf.

jakiman, 2017. PIVX purple paper. Available at: https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf.

Kiraly, B., 2017a. InstantSend. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend.

Kiraly, B., 2017b. PrivateSend. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend.

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf.

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Available at: https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf.

strophy, 2017. Understanding sporks. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks.

Wiecko, R., 2017. Dash instamine issue clarification. Available at: https://dashpay.atlassian.net/wiki/spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification.

Wu, H., 2012. The hash function jh. Available at: http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf.