Bitcoin Private
ホワイトペーパー

プライバシー革命

サトシが描いた 2018 年以降のビジョンを実現

2018 年 2 月

著者:

Bitcoin Private コミュニティ

Jacob Brutman 博士

Jon Layton

Christopher Sulmone

Giuseppe Stuto

Geoff Hopkins

Rhett Creighton

WWW.BTCPRIVATE.ORG

要旨

インターネットは、情報共有において歴史上最も大きな変化をもたらしました。容易にアクセスできる情報の蓄積には無数の利点がありますが、一方で人はそれと引き換えにプライバシーを犠牲にせざるを得ませんでした。あまりにも頻繁に、そしてエンドユーザーの誤りによるものでなく、第三者の不十分なセキュリティが侵害されて、機密情報が洩れ、盗まれてしまうのです。信頼できる仲介者がいなくても個人同士が自由かつ安全に取引できる、より良いシステムが必要です。Bitcoinの制作者であるサトシ・ナカモトのロードマップの真の実現であり、低料金で高速、そしてプライベートな取引ネットワークである新しい暗号通貨、Bitcoin Private をここに紹介します。Bitcoin Private は、Bitcoin と Zclassic とのフォーク-マージ(分派合流)による産物です。その結果生まれたBitcoin Private チェーンは、Bitcoin よりも大幅に手数料が安い上に、取引速度は 4〜6 倍速くなっています。最も重要なのは、元々Zcash Foundation によって実装され検証された守秘技術であるzk-SNARKs が組み込まれていることです。zk-SNARKs なら匿名かつ内密な取引が可能です。この点において Bitcoin Private は、他の守秘技術とは一線を画しています
Zclassic と Bitcoin の両者からなるこの UTXO(Unspent Transaction Output/未使用トランザクションアウトプット)セットが、この新しい元帳の初期コインとなります。これは、2,100 万枚のコインの内2,040 万枚がフォーク時に存在することを意味し、Bitcoin Private が暗号通貨界で最も低いインフレ率になるであろうことを保証します。このホワイトペーパーでは、Bitcoin Private とその技術的利点、商業的な適応性、および出来る限りコミュニティ主導で進められる今後の開発の可能性について説明します。

目次

1.序論

有史以来、大半において、取引は非公開かつ匿名で交わされてきました。取引情報は、送り方と受け取り方にだけ開示されていたのです。近年では、金融取引の大部分が技術の発達によってより容易になり、経済的な匿名性を維持することは難しくなっています。最も一般的な支払い方法（クレジットカード、デビットカード、アップルペイなど）により、取引のすべての情報はデジタル処理で保存されます。これらの取引方法には大きな利点がありますが、だからといって一般的な消費者の経済的プライバシーが度外視されるべきではありません。大きな金融機関内で起こる、個人情報や金融情報漏れの頻度を考えると、経済的プライバシー権が必要であることは明らかです。（注:1.2） その上、様々な金融機関では顧客データの販売が発覚し（注:3）、また法的根拠もなく、法に則った取引が阻害されているのです。（注:4）

2008 年 10 月、サトシ・ナカモトは、初めて暗号通貨の基礎を詳述した「Bitcoin: A Peer-to-Peer Electronic Cash System」という論文を公開しました。（注:5） サトシが目指したのは、第三者機関による取引の規制から解き放たれ、インフレが限定されていて、そして匿名性によって経済的自由を得られる通貨を作り出すことでした。2009 年に Bitcoin が生まれて以来、1000 種類以上の暗号通貨が生みだされ、大きく発展してきました。（注:6） 実際、多くの新しい暗号通貨は、取引速度と手数料の面で Bitcoin をはるかに凌駕しています。にもかかわらず、Bitcoin は先行者の優位を保ち、かつ多数のコインと交換できる基軸通貨であるため、依然として最も人気のある暗号通貨の地位を守り抜いています。

Bitcoin のブロックチェーンが長年に渡って成長した結果、明白な問題が起こり始めました。小さく固定されたブロックサイズ（これにより手数料が高くなってしまう）、ブロック生成時間の長さ（平均 10 分）、採掘難易度調整期間の長さ（2 週間毎）、高度な特定用途向け集積回路（ASIC）マイニングデバイス（鍵となるコンセンサスパラメーターであるアルゴリズム SHA-256 を迅速に算出する）によるマイニング(採掘)の集中化といった問題です。Bitcoin がこれらの問題に対処するためには、Bitcoin マイナー(採掘者)の 50%以上が実行中のコードの変更に同意する必要がありますが、そのような同意には至っていません。そのかわりに、Bitcoin のハードフォーク（Bitcoin Cash や Bitcoin Gold など）が起こり、技術的改良がなされました。たとえば Bitcoin Cash は、より大きなブロックサイズ（1MB に対して 8MB 以上）が可能になるように改良されているため、手数料が下げられ、取引の処理能が向上しています。しかしこれは、固定されたブロックサイズと「手数料市場」の欠如のために、コイン価格の将来性が損なわれてしまうことと引き換えでした。
Bitcoin のメモリプールの手数料市場は、お互いの機会コストに対して競い合うために、大なり小なり取引に挑みます。このことが所有権の価値を均等に高め、大きな需要を引き起こすのです。

Bitcoin Gold は別の道を選びました。ブロック生成時間を 2.5 分に短縮し、PoW アルゴリズムを ASIC マイニングへの耐性を備えた Equihash に切り替え、ブロック毎に発生する難易度調整アルゴリズムを強化したのです。
Bitcoin Gold は、GPU と相性の良い Bitcoin フォークコインとしての目標を大いに達成しましたが普及には及ばず、そして密かに事前に採掘されたコインを開発者達が確保したことは道義に反すると多くの人に指摘されています。(注:7) 優れた思想に基づいているにもかかわらず、2017 年第 4 四半期時点で、Bitcoin のフォークコイン群は暗号通貨市場で Bitcoin の後塵を拝しているのです。

サトシが描いたビジョンの中心では、多くの人々は匿名性を享受し、活用することができ、そして脱インフレという暗号通貨の技術特性を評価しています。「プライバシー権」は、自由世界では最高の権利であり(注:8)、サトシと暗号通貨コミュニティが定めた原則に欠かせないものです。サトシが描いた新しいデジタル通貨の世界では、経済的匿名性は大原則なのですが、依然として多くの人々は、ブロックチェーンの疑似匿名取引の交差点で右往左往させられています。さらに、巨大なデータや学習装置を駆使して、取引に関連する個人を特定する政府機関や民間組織も存在します。実際 2018 年 1 月時点で、BitFury には Bitcoin の取引の最大 15%を非匿名化する力があります。その数値は日を追う毎に増加し、この先数年で暗号通貨におけるその範囲は大きく変えられてしまうでしょう。(注:9) Bitcoin に匿名性が欠けてしまっていることは、作成者の意図を思うと皮肉ですが、対策は存在します。

さまざまな暗号通貨がこのプライバシー問題を解決しようとしています。これらの問題の多くは、難読化や TOR(The Onion Router)ノードによって匿名性を保証するオン・チェーン・トランザクション・システムのおかげで、さまざまな技術で折り合いをつけることができます。2014 年、MIT の研究者による革新的な研究論文で「zero-knowledge non-interactive arguments of knowledge」、すなわち zk-SNARKs が論じられました。(注:10) 注目すべきことに、zk-SNARKs を実装する暗号通貨は、シールド(遮蔽)された取引(完全に匿名で、取引や住所の残高が元帳に示されない取引)を可能にするのです。2016 年、この論文の著者は zk-SNARKs を最初に組み込んだ暗号通貨である Zcash を開発し、ローンチします。Zcash のコードには「開発者報酬」が組み込まれました。コミュニティが採掘したコインの 20%を、開発チームと初期の出資者が回収するためにです。Rhett Creighton は、マイナーのコミュニティに密着取材し、8 日後に Zcash をフォークすることを決断、開発者報酬を取り除いて Zclassic を作りました。この Zcash プラットフォームは、コミュニティ開発を通じて透明性を高めています。しかし残念なことに、Zclassic は、その素晴らしさを見出す元になった Zcash と同じ考え方に捕らわれてしまいました。開発者報酬がないと、開発が活発に進まないのです。ですが、このように活発でない開発に陥ることを防ぐ運営方法はいろいろあります。

Bitcoin と Zclassic の "フォーク-マージ"たる Bitcoin Private は、以前のフォークコインの挑戦、選択、失敗を認識しながら、Bitcoin ブロックチェーンに匿名性と、世界中での消費されやすさを加

えることを目指しています。これを達成するために、Bitcoin Private は、より大きなブロックサイズ（2MB）、より短いブロック生成時間（2.5 分）、およびマイニング時に GPU に優しく ASIC 耐性を備えたプルーフオブワーク・アルゴリズム、Equihash を採用しています。そして、この 2 つのコインを祖とするフォーク-マージの二重性によって、暗号通貨コミュニティの多くは、自分自身が Bitcoin Private に関わっていることに気付くでしょう。スナップショット(ある時点での残高確認)の後、ZCL（t 及び z アドレス）と BTC（segwit 及び normal アドレス）は、それぞれ同じアドレスに BTCP（いずれも 1：1）を受け取ります。これはこの種の初めてのフォークであり、オープンソースのブロックチェーンコミュニティはこの UTXO セットのマリアビティ(取引展性)を探り始めています。

表 1：Bitcoin Private、Bitcoin、Bitcoin Cash、および Bitcoin Gold の比較

	Bitcoin Private	Bitcoin	Bitcoin Cash	Bitcoin Gold
総供給量	2,100 万枚	2,100 万枚	2,100 万枚	2,100 万枚
匿名性	zk-SNARKs	x	x	x
ブロックタイム	2.5 分	10 分	10 分	2.5 分
ブロックサイズ	2MB	1MB	8MB	1MB
PoW アルゴリズム	Equihash	SHA256	SHA256	Equihash
難易度調整	ブロック毎	2 週間	2 週間	ブロック毎
事前採掘	x	x	x	○
コミュニティ主導	○	x	x	x
管理	○	x	x	x

2.フォークの方法論

Bitcoin Private では、2 つの暗号通貨の UXTO が1つのブロックチェーンに結合される「フォーク−マージ」が提案されています。zk−SNARKs と JoinSplit トランザクション(取引)が、この新しいブロックチェーンの基幹部であるため、正式にはこのチェーンは Zclassic ブロックチェーンから立ち上がることになります。ブロックチェーンの解明は、ポリマーの連鎖重合に喩えることができます。次のブロックを解くと、ポリマーチェーンの末端にモノマー(単量体)を添加したときにポリマーが拡張するように、ブロックチェーンが成長します。しかしながら、より長いポリマーチェーンは一般に、得られるプラスチックに耐久性の向上をもたらしますが、ブロックチェーンのサイズが増加すると、ストレージの消費量が増えるだけでなくノードの同期時間が大幅に長くなります。幸運なことに、このスナップショットは一時的に Bitcoin と Zclassic からアドレス状態を探るだけで、そのまま新しいチェーンへと運ばれます。このアプローチは効果的で、ブロックチェーンで必要なストレージを大幅に削減してくれます。この場合、157GB からたったの 10GB(ローンチ時)にまで短縮されるのです。さらに、Bitcoin Private クライアントは、ブロックチェーンのプルーニング(剪定)と、ユーザーの端末におけるブロックチェーンの負担を軽減するために、Electrum のような SPV(軽量ノード)をサポートします。

あらゆるフォークが対処しなければならない重大な問題は、元のブロックチェーン上の過去のフォークトランザクションが新しいブロックチェーン上で有効になってしまう、いわゆる「リプレイアタック」です。元のブロックチェーンからの正当性と独立性を保証するためには、すべてのコインフォークにリプレイ保護が不可欠なのです。Bitcoin と Zclassic のリプレイアタックから保護するため、Bitcoin Private は双方向再生保護機能を備えています。これは研究済みの問題で、上記のように双方向に組み入れられる、業界の標準的なアプローチです。Bitcoin Private には、Bitcoin Gold において十分に研究されており、うまく機能している業界の標準的アプローチ(SIGHASH_FORKID)が実装済みです。(注 11)

Bitcoin と Zclassic のスナップショットは、2018 年 2 月 28 日の午後 5 時(協定世界時)以降に最初にタイムスタンプされたブロックに設定され、フォーク/メインネットは約 2 日後にローンチします。ローンチ後、約 70 万の Bitcoin Private がマイニング可能と見られています。1.5625 Bitcoin Private である開始時のブロック報酬は、210,000 ブロック(約 1 年)ごとに半減期を迎え、半分になるように設定されています。しかし、この試みが失敗であると判明した場合、第 7 章に記した代替計画が実行されることがあります。

3.プルーフオブワーク：Equihash

冒頭で説明したように、Bitcoin のマイニングは GPU を軽く凌ぐ特別製の機器である ASIC で主に行われます。GPU と違って ASIC は入手が困難なため、Bitcoin マイニングの極端な集中化が起こっています。実際、Igor Homakov は、Bitcoin ネットワークのハッシュレート(採掘速度)の 60%以上を中国が占めていることを示唆しています。(注：12) 一方、ASIC 耐性アルゴリズムは、GPU が世界中で容易に利用できるようになるにつれて、分散化される可能性がはるかに高いのです。ネットワークハッシュの分散化により、ブロックチェーンの非集権化が大幅に進み、51%アタックの脅威が引き下げられ、マイニングによって生成された暗号通貨と集められた各種料金はコミュニティ全体に均一に分散されます。これにより、少数のマイナーがブロックチェーンの開発に大きな影響を与えること、及び大量の暗号通貨のマイニングよって市場を操作してしまうことが防止できます。

Bitcoin Private は、Alex Biryukov と Dmitry Khovratovich によってルクセンブルグ大学でプルーフオブワーク(PoW)メカニズムとして開発され、高く評価されている Equihash PoW アルゴリズムを使用します。(注:13) 他の ASIC 耐性 PoW アルゴリズムとは異なり、Equihash は「バースデー・プロムレム(誕生日問題)」とこれを解決するために使われる拡張ワグナーアルゴリズムに基づいています。さらに、Equihash は「メモリ・ハードネス(メモリ硬度)」を特徴としており、これによりメモリ使用量と速度低下という著しいコンピューター演算のペナルティをもたらされます。この Equihash の特徴は、ASIC が GPU や CPU に対抗するために多くのメモリを実装するものであるため、Equihash の ASIC 耐性を強固にします。メモリ硬度は、悪意あるプログラムによって乗っ取られたコンピューター群による CPU マイニングを防ぐことはできませんが、非常に多くのメモリが消費されることで、感染した PC の持ち主がパフォーマンスの急激な異変に気づき、感染を取り除くために必要な措置を講じることになるだろうと元の論文の著者たちは論じています。

4.透明性 対 シールドされた取引

Bitcoin Private は、透明性を持つ取引システムとシールド(遮蔽)された取引システムという 2 つの取引システムの融合です。透明性を持つ取引システムは、Bitcoin と同じ原則（入金、出金、金額、サイン）で動きます。すべての資金、行き先、金額の情報源は、ブロックチェーン上に透明性を伴って保存されます。反対に、シールドされた取引では、これらの詳細が JoinSplit というブロックの特別な区域に暗号化されます。 これらの取引の検証は可能ですが、第三者には判読できません。シールドされた記録が使われる時、ブロックチェーンの整合性は zkSNARKs と呼ばれる特別なゼロ知識証明アルゴリズムによって維持されます。(注 6) このアルゴリズムは、シールドされた各転送の出金額と入金額の合計を表示すべく一連の演算を実行します。次に送金者は、入力記録のプライベートキーを所持していることを証明し、支出権限を与えます。最後に、入力記録のプライベートキーが、プライベートキーを知らない何者かに取引が変更されないように、取引全体を暗号化します。(注 : 14) この全方法論は Zcash の信頼性の高い設計によって成立しています。Zcash のローンチ時には、ゼロ知識証明とプライベート取引に必要な鍵が生成され、その後破壊されたのですが、これは「セレモニー」と呼ばれました。（注:6） これにより、システムは「CMA(chosen message attacks/選択暗号文攻撃)と呼ばれる暗号解読法に対する強力な一度の偽造不可能性」を保証することができるのです。(注:10)

5.自発的マイナー供出プログラム

Bitcoin Private の保守と開発用の基金を作るために、「Voluntary Miner Contribution Program(自発的マイナー供出プログラム)」が立ち上げられました。このプログラムでは、合計 50,000 の Zclassic がハッシュ・パワーを通じて Bitcoin Private の基金に供出されるまで、62,500 の Bitcoin Private がマイナー達に競りに出されました。このプログラムにおけるマイナーへの配当は、次の式で算出することができます。

P=Zm*62,500/Zp

P はマイナーへの配当、Zm は各マイナーが採掘した Zclassic、Zp はプール全体で採掘された Zclassic の合計です。62,500 Bitcoin Private はフォークで生成され、各マイナーから提示されるウォレットアドレスに送られます。このプログラムのために作られたプリフォーク ZCL マルチシグウォレットには、総額 5 万の Zclassic が入っていて、開発、奨励金、継続的なマーケティング、そしてコミュニティによる Bitcoin Private の全体的な発展のための基金を設立するために、BTCP にフォークされています。これは、元の Zclassic が抱えた開発が活発でなくなってしまう問題に対処するためのいくつかの方法の内の 1 つなのです。

見方によっては、このプログラムは、Bitcoin Private コントリビューションチーム(開発チームの中に存在するチーム)が激しく反対している概念である「プレマイン(事前採掘)」と見ることができます。しかし、プレマインは一般的に中心グループによって直接的に実施されますが、今回はそうではありません。この例では、マイニングコミュニティは、Bitcoin Private の早期入手と引き換えに、資金を供出することを自ら選択することができるのです。さらに、オークションのような形式のこのプログラムのために、マイニングコミュニティは寄付され集まった各 ZCL にどれだけ価値があるのかを見立てることができるのです。(上記の方程式を参照) このタイプのフリーマーケット方法論は、サトシが描いた本来の Bitcoin のビジョンの核となるものです。これらの基金は、為替待機(50%)、開発(25%)、マーケティング(15%)、その他/運営(10%)に使用されます。

6.財務管理

財務管理委員会には、コミュニティから 3 人、マイニングコミュニティから 2 人が集められ、BTCP 開発者コミュニティ LLC(有限責任会社)として設立されました。発表時には、Jacob Brutman 博士（運営担当）、Giuseppe Stuto（マーケティング担当）、Peter Hatzipetros（ジェネラル・カウンセル/法務のトップ）がコミュニティを代表し、Adib Alami と Evan Darby がマイニングコミュニティを代表しています。また、委員会の内規も用意されています。（注：15）

7. Bitcoin Private の未来

全面的な匿名性の改善は、Bitcoin Private プロジェクトの重要な一部です。現在、zk-SNARKs は取引にサインする際にかなりの RAM と CPU を費やし、処理に数分かかることもあります。フォーク後の最初の改善点の 1 つは、現在 Zcash コア開発チームによって開発中の「Jubjub」と呼ばれる新しい苗木です。（注:16） この新しい苗木は、zk-SNARKsプライバシーコインのシールドされた取引の速度と使いやすさを大幅に向上させます。Bitcoin Private の匿名性を改善するもう一つの方法は、現在開発中の ″Dandelion″プライバシープロジェクトを活用することです。（注:17） この手法には、 ″stem″（取引）と ″fluff″（難読化）が含まれます。どんな難読化の手続きも本質的には zk-SNARKs より安全性が低くなってしまいますが、Bitcoin Private の透明性の高い取引とシールドされた取引の両方に Dandelion の難読化を追加することで、全面的な匿名性を向上させることができるのです。

Bitcoin Private のブロックチェーンを改善することは、プロジェクトにとって非常に重要です。ソフトフォークを可能にするために BIP9 がブロックチェーンに組み込まれ、そして改良されています。（注:18） 改善のための適切なコーディングが終了した後、マイナー達はチェーンコードの変更を受け入れる準備ができていることを知らせるように求められます。マイナーの 95%が変更を受け入れると、「ロックイン(実装)」され、ソフトフォークが完了します。しかし、マイナー達が指定された期間内に準備状況を知らせなかった場合、ソフトフォークは失敗し、変更は行われません。Bitcoin Private プロジェクトの支援と開発は、マイニングプールドミネーション(寄付)以外の方法で、継続的に資金が集まるかどうかにかかっています。しかし、Bitcoin Private コントリビューションチームは、それを支持するという民主的な投票をせずに、コミュニティへ課税することに強く反対しています。したがって、BIP9 を介して最初に提案された変更の 1 つには、基金収集パラメーターが含まれています。これによってマイナー達は、プログラムの将来の成功を確実にするために自分たちが寄付する妥当な金額を選ぶことができます。

第 2 章で述べたように、フォーク後に残っているマイニング可能な Bitcoin Private が少ないために、ネットワークのハッシュレートが極端に低くなるなど、いくつかの問題が起こる可能性があります。可能な解決策は、フォーク前からまったく動かされていないコインをある時点で取り除いてしまうことです。この策が実行された場合、フォークされてから動いていない Bitcoin Private コインの約 0.14%が 2 年間にわたって毎日削除されることになります。このシナリオでは、Bitcoin Private コインは、動いていないコインを持つすべてのウォレットで均等に削除されます。ハードフォーク以降動いていない Bitcoin Private の各ウォレットは、2 年間に渡り、1 日当たりそのコインの約 0.14%を失うことになるのです。この方法によって、マイナーのためにかなりのコインが解放され、同時にユーザーには自分のフォークされたコインを動かす十分な時間が与えられます。さらに、日々の削除の割合が低いので、時価総額に与える影響は抑えられるはずです。

代替手段として、BithereIn Private には、Ethereum と同じ方法で将来の重要な開発を可能にするための「ディフィカルティ・ボム（困難な爆弾）」が実装されています。（注:19） 使われると、ディフィカルティ・ボムが旧来のブロックチェーンコードに適用され、継続的な改善のためには新しいコードベースを採用するべきだということにマイナー達が思い至ることになるのです。この方法は最後の手段とみなされ、極端な状況下でのみ使用されます。もしかすると、この爆弾は、Decred のような特徴的なシステム(それに限定されるわけではありませんが)など、新しい管理方法を導入させるかもしれません。（注:20） これによって、Bitcoin Private ブロックチェーンのさらなる非集権化と分散化が可能になることでしょう。現在、ディフィカルティ・ボムの爆発は 2019 年 3 月 2 日に設定されていますが、ハードフォークによってこの日付をいつまでも延長することができます。最初の半減期がディフィカルティ・ボム爆発の前後に来るかもしれず、半減期による低インフレ化が成功しなかった場合、ディフィカルティ・ボムによって変更が行われることになるでしょう。

8. 商用利用

今日、支払い手続きは Bitcoin の最も目覚ましい使用事例の 1 つになっています。加盟店が BitPay などの Bitcoin の決済会社を使うことで、2017 年には 10 億ドル相当を越える取引が行われた可能性があります。この決済会社のウォレットユーザー達は月額 10 億ドル以上の資産を確保し、月額 15 億ドル以上を自分のウォレットから他者のウォレットに送金します。(注:21) インターネットは新しく、そして革命的な支払い方法をもたらしましたが、暗号通貨もまた同じことを成し遂げようとしています。

消費者は、商品やサービスと引き換えに対価を支払う際に、ある程度利便性を求めており、これがウェブ決済一般化の要因です。その利便性の要求に加えて、ウェブ取引に伴う匿名性の想定レベルというものがあります。残念なことに過去 20 年間以上にわたって、インターネットのクレジットカード取引を追跡し、消費者のオンライン「プロフィール」(人物情報)を作ることで利益を得る事業体が存在しています。(注:22) これは恐るべきプライバシーの侵害であり、消費者が暗号通貨でオンライン取引をしたいと考えざるを得ない大前提でもあります。にもかかわらず、最も一般的な暗号通貨の技術的設計では、このプライバシー侵害をブロックチェーン上で見抜くことはできないのです。(注:14) ですが Bitcoin Private なら、zk-SNARKs トランザクションによって消費者の匿名性に関する必要性を満たすことができます。

Bitcoin Private はデジタル資産の直取引および商取引に大きな役割を果たします。売り主には、テスト済みであり安全で、かつ広く採用され、立証可能な匿名性と非公開性という利点が追加された暗号通貨技術が提供されます。おそらく何百から何千ものごく一般的な使用例が、Bitcoin Private の商業利用にもたらされることでしょう。他の z プロトコルコインでもこの役割を果たすことができますが、広く一般に選ばれたり成功したりしたコインはありません。これは、シールドされた取引の CPU とメモリへの要求が高いためです。 しかしながら、苗木 "Jubjub"のリリースは、モバイルでのシールドされた取引をも可能にします。Bitcoin Private コントリビューションチームは、この暗号通貨が主流派に受け入れられ、広く普及することを強く望んでいます。 ですから売り主が使いやすい、シールドされた取引サービスが新しい苗木の直後にリリースされる予定です。標準的な Web の売り手の使用例に加えて、実店舗でもモバイルウォレットプラットフォームが使われるかもしれません。実店舗用アプリケーションを使った透明性のある取引やシールドされた取引で、Bitcoin Private が貯めておかれたり送金されたりするのです。さらに、同じプラットフォームをどんなユーザーでも使用することができ、一店舗に限定されません。現時点で既に Bitcoin Private は、さまざまな売り主や商人達から、商品の支払いオプションとして使いたいというアプローチを受けています。これら商取引の一部は Bitcoin Private 基金に集められ、マイニングでの資金調達の必要性がなくなるのです。

9.コミュニティ主導のプロジェクト

ユーティリティトークンでもコインでも、多くの暗号通貨プロジェクトは、自分たちがコミュニティ主導でありオープンソースであると主張しています。これはある程度は真実ですが、一般的にはプロジェクトの将来全体をコントロールする中心的な開発チームが存在します。コミュニティが実際にプロジェクトをコントロールするという例外はほとんどありません（例えば Decred）。開発チームは依然として閉鎖的であることが多いのです。コミュニティのメンバー達が該当するコードの変更を提案したとしても、その要求は顧みられないことがあります。Bitcoin Private プロジェクトには、2018 年 2 月 6 日現在、100 人以上の参加者がいて日々拡大し、真のコミュニティ活動を実現しています。

Bitcoin Private が他のコミュニティコインと一線を画す、様々な取り組みが実施されています。例えば、世界中の多言語使節プログラムが立ち上がり、コミュニティのメンバーは Bitcoin Private を広め、コミュニティを拡大するのに積極的に取り組んでいます。さらに Bitcoin Private は、誰もが申し込み可能な「開発者コール」を開設しました。これによってブロックチェーンテクノロジーに初めて触れる人でも、プロジェクトに有意義な方法で貢献することができるでしょう。未経験者はこの開発者プログラムを学び、ブロックチェーンテクノロジーやエンジニアリングに習熟することができます。これらの 2 つのプログラムを合わせると、数日のうちに 100 人以上の新しい参加者が現れ、デイリーコントリビューションチームが 300 人を超える規模に拡大しました。Bitcoin Private コントリビューションチームのこの規模は、コミュニティ主導という思いに対してプロジェクトが献身的であることを表すものであり、チームが知る限り他の暗号通貨が達成できていない偉業でもあります。これは、Bitcoin Private の開発が本当に分散化された性質であることを示しています。

10.結論

Bitcoin Private は、様々なコミュニティによって開発され、維持されている暗号通貨です。世界中のチームメンバーが毎日、このプロジェクトを成功させるために協力しています。彼らはなぜそうしているかと言うと、サトシが描いた速く、低料金で、分散されていて、プライベートな取引が可能という金融的自由のビジョンを、このプロジェクトが実現すると信じているからです。Bitcoin Private は BIP9 ソフトフォーク提案を早々に内包することで、将来的な開発が可能になりました。仕込まれたディフィカルティ・ボムは、BIP9 が有効ではないと判明した場合、代わりの管理方法を発展させることでしょう。Bitcoin Private の商用アプリケーションは、世界規模の高速な取引から地方商店での買い物まで数多くあります。Bitcoin Private を支える献身的な貢献者達と Zclassic のシールドされた取引技術との組み合わせは、明らかにあてにならないブロックチェーンのプライバシーを新時代へと導くことでしょう。

11.謝辞

私達は、マイナー供出プログラムを通じて多大な寄付をしてくれているマイニングコミュニティに感謝の意を表したいと思います。私達はまた、日夜働き続けるチームを支えてくれたカフェインの分子に感謝します。コーヒーなしに、このプロジェクトは不可能でした。私たちの驚くべき開発チームにもたくさんの感謝を。あなた達は私達が頼みにする、このプロジェクトの基盤です。最後に、Bitcoin Private コミュニティの全員に感謝します。あなた方はこのプロジェクトの中枢であり、あなた方がいてくれてこその私達なのですから。

12.参考文献

注:1 Dutch Banks Tax Agency Under DdoS Attacks a Week after Big Russian Hack Reveal. https://www.bleepingcomputer.com/news/security/dutch-banks-tax-agency-under-ddosattacks-a-week-after-big-russian-hack-reveal/ (Accessed Feb. 5, 2018).
注:2 The Biggest Data Breaches of the 21st Century. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the21st-century.html (Accessed Feb. 6, 2018).
注:3 What Chase and Other Banks won't Tell you about Selling your Data. https://www.forbes.com/sites/adamtanner/2013/10/17/what-chase-and-other-banks-wont-tellyou-about-selling-your-data/#5eacaaf62c41 (Accessed Feb. 5, 2018).
注:4 Santander Totta has no Known Legal Basis to Block Bitcoin Related Transactions says Portuguese Consume Watchdog. https://www.ccn.com/santander-totta-has-no-known-legalbasis-to-block-bitcoin-related-transactions-says-portuguese-consumer-watchdog/ (Accessed Feb.5, 2018)
注:5 Nakamoto S.; (2008) Bitcoin: A peer-to-peer electronic cash system.
注 :6 List of Cryptocurrencies. https://cryptocurrencyfacts.com/list-of-cryptocurrencies/ (Accessed
Feb. 5, 2018).
注:7 Premine Endowment. https://bitcoingold.org/premine-endowment/ (Accessed Feb. 2, 2018)
注:8 Brandeis, L.; Warren, S.; (1890) The Right to Privacy.
注:9 "BitFury Group De-Anonymizes Over 15% of the Bitcoin ... - The Merkle." 11 Jan. 2018, https://themerkle.com/bitfury-group-de-anonymizes-over-15-of-the-bitcoin-network-with-newblockchain-analysis-tool/ (Accessed Jan. 30, 2018).
注:10 Ben-Sasson, E; Chiesa, A; Garman, C.; Green, M,; Miers, I.; Tromer, E.; Virza, M. (2014) Zerocash: Decentralized Anonymous Payments from Bitcoin.
注:11 Interpreter.cpp. https://github.com/BTCPrivate/BitcoinPrivate/blob/6b6abb3d121ba5231e5d775e9e2287dbbf7687f6/src/script/interpreter.cpp#L1089 (Accessed Feb. 9, 2018)
注:12 Homakov, I. (2017) Stop. Calling. Bitcoin. Decentralized. https://medium.com/@homakov/stop-calling-bitcoin-decentralized-cb703d69dc27 (Accessed Feb. 4, 2018)
注:13 Biryukov, A.; Khovratovich, D.; (2016) Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem.
注 :14 Zcash - How zk-SNARKs works in Zcash. https://z.cash/technology/zksnarks.html (Accessed Feb. 3, 2018).

注:15 BTCP Developer Community, LLC Bylaws. https://btcpfoundation.org/bylaws.pdf

注:16 What is Jubjub? https://z.cash/technology/jubjub.html (accessed Feb. 1, 2018).

注:17 Bitcoin Developers Reveal Roadmap for 'Dandelion' Privacy Project https://www.coindesk.com/bitcoin-developers-reveal-roadmap-dandelion-privacy-project/ (accessed Feb. 5, 2018).

注:18 BIP9. https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki (Accessed Feb. 7,2018)

注:19 What is the Ethereum Difficult Bomb. https://themerkle.com/what-is-the-ethereum-difficultybomb/ (accessed Feb. 5, 2018)

注:20 Decred Documentation. https://docs.decred.org/ (Feb. 1, 2018)

注:21 Bitcoin Transactions aren't as Anonymous as Everyone Hoped. https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-aseveryone-hoped/ (Accessed Feb. 5, 2018)

注:22 Google Now Tracks Your Credit Card Purchases and Connects them to its Online Profile of you. https://www.technologyreview.com/s/607938/google-now-tracks-your-credit-card-purchasesand-connects-them-to-its-online-profile-of-you/ (Accessed Feb. 5, 2018)

13.重要な開示およびその他の情報

特に明記されていない限り、すべてのコンテンツはオリジナルであり、Bitcoin Private によって調査、制作されています。Bitcoin Private の明示的同意なしに、どのような形式であってもこのコンテンツのいかなる部分も複製することはできません。

この文書は情報提供のみを目的としたものであり、販売を目的としておらず、提案や勧誘が違法となる範囲における、どのような証券類の売買をも目論んだものではありません。本文書に記載された情報は財務上の決定を下すには不十分であり、ここに記載されている情報をそのような目的の根拠として用いるべきではありません。このホワイトペーパーは個人的な推奨を構成するものではなく、読者の特定の投資目的、財務状況、またはニーズを考慮したものではありません。読者は、本文書のアドバイスや推奨が自身の状況に対して適当であるかを考慮し、必要に応じて税務を含む専門的アドバイスを求めてください。本調査で参照されている暗号通貨の価格と価値、及びそれらから得られる収入は変動する可能性があります。過去の業績は将来の業績の目安ではありません。将来の収益は保証されず、元本の損失が発生する可能性があります。為替レートの変動は、特定の投資の価値または価格、またはそれに伴う収益に悪影響を与える可能性があります。Bitcoin Private について提供される情報は、Bitcoin Private コインの投資、税務や法律相談、勧告、または売り出しや購入の勧誘を意図したものではなく、そのように解釈、使用すべきではありません。

本書内の特定の記述は、Bitcoin Private の見解と将来の予測に基づいており、実際の結果や業績、または出来事が記述または暗示されたものと大きく異なる原因となりうる既知および未知のリスクと不確実性を伴います。文脈により先見的である記述に加えて、かもしれない(may)、だろう(will)、すべきである(should)、であっただろう(could)、ありうる(can)、期待する(excepts)、計画する(plans)、意図する(intends)、予測する(anticipates)、信じる(believes)、見込む(estimates)、見通す(predicts)、可能性(potential)、計画された(projected)、継続する(continue)及び同様の表現は将来の予測に関する記述であることを示しています。Bitcoin Private は、ここに記載された将来の予想、予測に関する情報を更新する義務を負いません。Bitcoin Private は、ここに記載されている情報の正確性に十分な注意を払っていますが、Bitcoin Private の正確性、確実性または完全性に関して、明示もしくは暗示を問わずいかなる表明及び保証（第三者に対する責任を含む）も行いません。