



VERGE

The most **privacy** focused cryptocurrency

BLACK PAPER

1. イントロダクション

ビットコインはインターネット上のトランザクションに内在する欠陥の解決策として、2009年に開発、リリースされました。サトシ・ナカモトが発表した論文（ホワイトペーパー）で、彼は以下のように言及しています。

「インターネット上の殆ど全ての商取引と、付隨するオンライン決済で、独占的な地位を持ち、"信頼できる仲介者"として、金融機関に依存せざるをえない状況になった。このシステムは上手く機能している一方で、金融機関をこのように信頼することで成立するシステムに内在する弱点は解決されていない。」

ビットコインは、2009年の誕生から今日まで、多様な商取引空間で採用され、急速な普及を続けています。

この急速な普及に伴い、ビットコインのトランザクション量も急増しました。ビットコインのトランザクション記録が保存されている、ブロックチェーン上では、トランザクションが承認されるまでの所要時間の長期化（トランザクションの渋滞・遅延）が生じ、トランザクション時間を短縮したいというユーザーの需要が、マイナーへ支払うトランザクション手数料の高騰に繋がってしまいました。このことは、現在のビットコインが直面する主な課題の1つになっています。

ビットコインを支える主要なイノベーションの1つとして、「非中央集権的(Decentralized)な構造」を挙げることができます。これは、法定通貨とは異なり、ビットコインは管理者及び支配権を持つ組織が存在しないということです。また、ビットコインのデータベースは単一障害点を持たない分散的な構成になっています。

この非中央集権性とは対照的に、ビットコインのエコシステムにおける実際のサービスやビジネスの殆どが、中央集権的な構造になってしまっていることは、ビットコインが直面している課題の一つです。

この中央集権的な構造に起因して、現在のオンライン上の商取引は、特定の所在地を持ち、個人所有の脆弱性が疑われるコンピューターの上で成立し、また、法制度からも複雑な影響を受けやすいです。

バージ（\$XVG）は、今日利用できる真に非中央集権的な暗号通貨の1つです。これは、バージの「ビットコインの理念と原則を継承しつつ、匿名性を実現する」という、強固なコミットメントに支えられています。

2. Tor (The Onion Router) の採用

Torという名前は、多層回路的特性を持つネットワーク上で、IPアドレスの追跡を困難にし、ユーザーの匿名での通信を可能にする「The Onion Router（オニオンルーター）」というソフトウェア開発プロジェクトの頭文字に由来します。

Torのネットワークは世界中のボランティアでノードを立てるユーザーの存在に支えられ、誰もが無料で利用することができます。このネットワークは世界中で7,000以上もの中継点から構成され、Torはこのネットワークを通してインターネット上のトラフィックをリレーするように捌き、ユーザーの所在地や利用状況を監視・解析しようとする者から隠すことができます。

Torのネットワークを通過するデータパケットを匿名化する、暗号化されたIPアドレスの複数の層はその名の通り、玉ねぎを彷彿とさせます。この構造が、ネットワークを通過する、データパケットの経路を完全に追跡することを不可能にします。

Torはインターネット上のユーザーの行動を監視しようとする者から保護し、ユーザーのプライバシー保護、通信における機密保持する自由と能力の確保を実現する事を目指しています。

オニオンルーティングは、通信プロトコルスタックのアプリケーション層を暗号化し、玉ねぎの皮のように複数の層を構成することで実装されています。

Torはデータを複数回暗号化します。このデータには次に送信されるノードのIPアドレスも含まれます。Torはこの暗号化されたデータを、連続的かつランダムに選択されたノードのリレーによって構成されるTorの仮想サーキットを通して送信します。

リレーを担うノードは受信した暗号化されたデータパケットのラッパー（層）を、送受信に必要な情報のみ復号化し、全体を再度新しいラッパー（層）で包み、暗号化した上で次のリレーに送信します。このようにリレーが続いた後に、リレーの終端を担うノードが、複数の層でラップされ暗号化されたデータパケットの最も内側にある、本来の送信先の情報が含まれる層を復号化し送信を行いますが、その際もノードが送信元のIPアドレスを知ることも、それを明かすこと也没有。

このように、Torのサーキットを通じて通信経路の一部が常に隠されることにより、送受信先の情報を頼りにネットワークの監視やノードの特定を試みる者に、その機会となるポイントを排除することを可能にしています。

3. I2P(The Invisible Internet Project)の採用

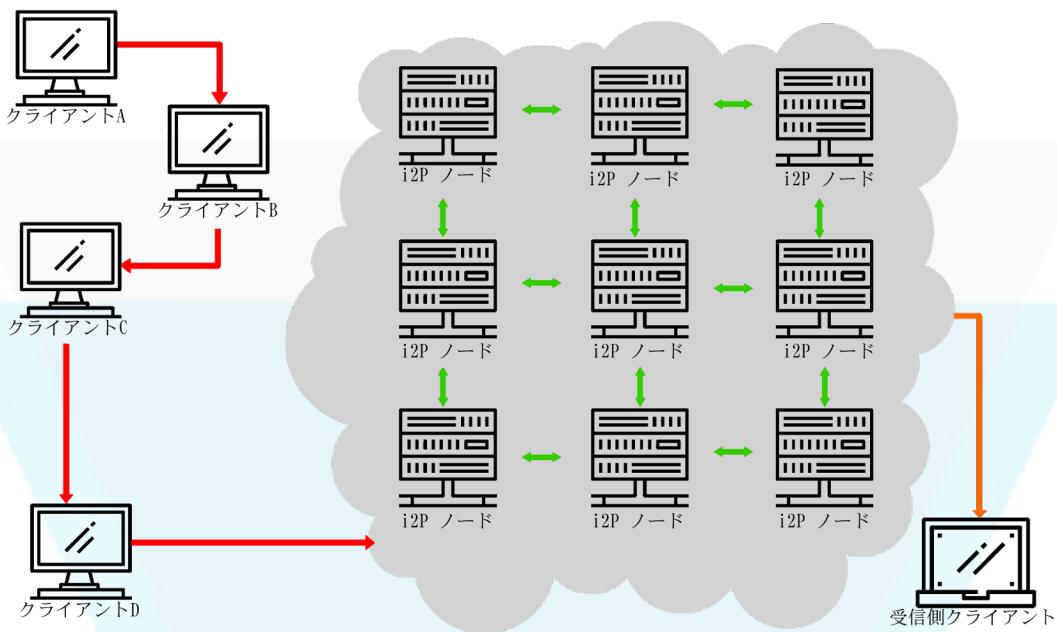
I2Pは元来、インターネット上で所在地を特定されずに、ホスティングサービスの提供を可能にすることを目的に開発されました。

I2PはTorと同様のメリットを数多く提供します。どちらも匿名での通信を可能にし、P2Pスタイルのルーティング構造を活用し、多層の暗号化を行っています。

一方で、I2Pは「インターネット内のネットワーク」として設計され (Figure2.1を参照) 、トラフィックはその境界に留まるという特徴があります。

I2Pは、Torのサーキットベースのルーティングとは対照的に、パケットベースのルーティングを実行します。このことは、インターネットのIPルーティングのような、通信の混雑やサービスの中止を回避する、ダイナミックなルーティングが可能になるというメリットをI2Pに提供します。これはネットワーク自体に高いレベルの信頼性と冗長性をもたらします。

図 2.1
I2Pトランザクションの仕組み



メモ：i2Pノードのホップは14秒ごとに発生します。

クライアントが初めて他のクライアントと通信を試みる時、クライアントは完全に分散化されたネットワークデータベースを参照します。

このネットワークデータベースはカデムリア・アルゴリズム[2]に基づき、その上で独自にカスタマイズされ構築された、分散型のハッシュテーブルです。

この参照は、他のクライアントのデータを受信する為のトンネルを効率的に発見する為に実行されます。また、クライアント間で送受信されるデータは、参照時に得た情報を含む為、一度発見することができれば、以降はネットワークデータベースに対して、この参照を行う必要はありません。

I2Pはipv6を活用した、高度な難読化を備えたトンネリングサービスで、ネットワーク上で送受信される全てのバージのデータを匿名化します。

各クライアントアプリケーションはI2Pルーターを備え、このルーターはいくつかのデータ送受信用トンネルを構築します。[2]

クライアントが別のクライアントにバージのデータを送信したい場合には、アプリケーションが送信用トンネルのひとつを通じて、他のクライアントの受信用トンネルのひとつをターゲットにして送信します。これを各々のノードが繰り返す事によって、最終的にデータが目的地に到達します。

I2PはTorと同じく、中央集権的なディレクトリサーバーに依存しません。I2Pは2つの分散型ハッシュテーブルを用いることでネットワークステータスを調整しています。

この分散型ハッシュテーブル（以下、DHT）は、分散型かつ非中央集権的な機構で、ハッシュ値とコンテンツを紐付けするために利用されます。

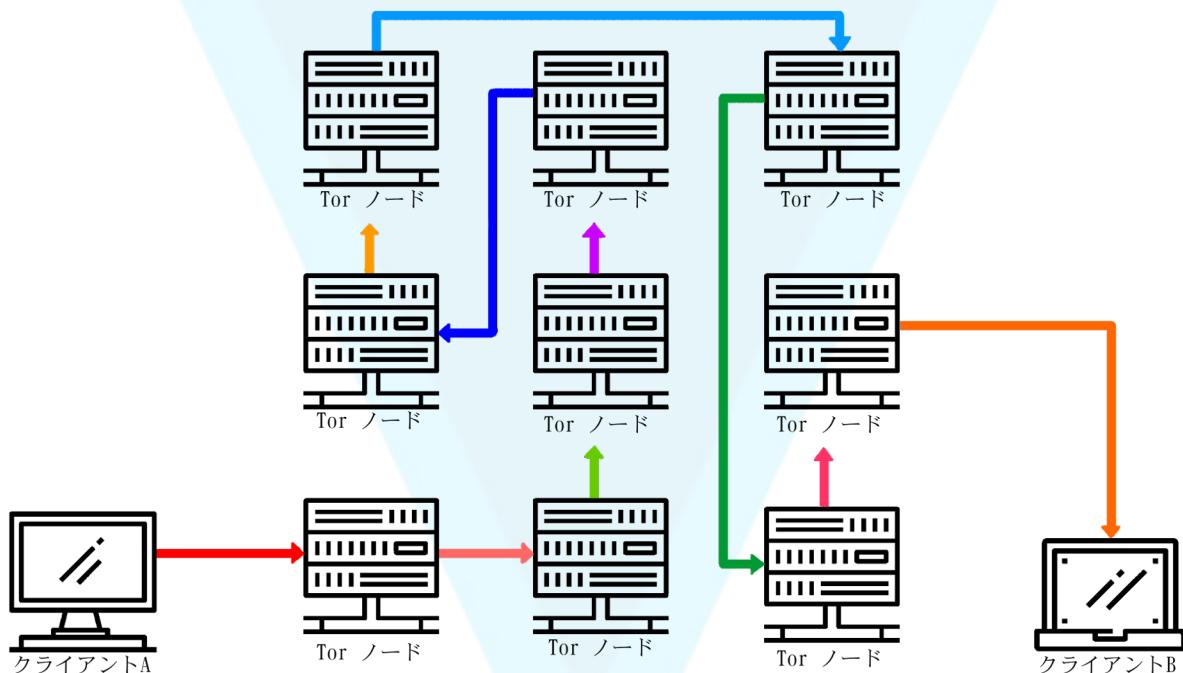
DHTの主要なメリットは、そのスケーラビリティ（拡張可能性）にあります。

成功するP2Pネットワークの条件は、コンテンツのデータサイズとトランザクションの共有性能が、必要に応じて継続的に拡張できることです。

更に、I2Pはルーティング情報を取得するためにディレクトリサービスに依存しません。その代わりに、それぞれのルーターが常に相互評価を行い、ネットワーク経路が動的に形成・更新されます。

最後に、I2Pはネットワーク上でデータを横断させるために、2つの独立した単信のトンネルを構築します。これはTorの単一の重層的なサーキット構造とは対照的です。（Figure1.1を参照）

図 1.1
TORトランザクションの仕組み



メモ：TORノードのホップは10分ごとに発生します。

4. Electrum ウォレット

バージのウォレットである「Electrum」の強みはスピードとシンプルさを、少ないリソース消費で実現していることです。

Electrumは安全なリモートサーバを使用し、これはバージのネットワークの最も複雑な部分を処理しています。また、秘密のシードフレーズを使ってユーザーがウォレットにアクセスできなくなった際に回復できる機能を備えています。更に、Electrumはシンプルで簡単に利用できるコールドウォレット機能を備えているので、ユーザーは保有しているコインの一部、もしくは全てをオフラインで保管することが可能です。

これらの機能に加えて、ElectrumはネイティブでTorとi2Pをサポートする数少ないウォレットの1つです。Torとi2PをElectrumに統合することによって、デスクトップ/モバイルでウォレットを使用する際に匿名性を実現することができます。IPアドレスとトランザクション情報は守られ、接続されるサーバーにも知られる事はありません。これは当然に、ユーザーのプライバシー向上に寄与しています。

また、Electrumはマルチシグネチャーに対応し、トランザクションの実行の際に、複数人の鍵を要求することが可能です。基本的なバージネットワーク上のトランザクションは「シングルシグネチャートランザクション (Single-Signature Transaction)」と呼ばれています。^[4] こう呼ばれるのは、単にトランザクションの実行の際に一人の署名を要求する為です。

この署名は、署名に紐付いたバージのアドレスの所有者の秘密鍵によって実行されます。Electrumのマルチシグネチャートランザクションでは、コインが転送される前に、複数人の署名が要求されます。バージネットワークも同様に、いかなるマルチシグネチャートランザクションの実行に際して、複数の異なるパーティのアドレスの提供を求めます。つまり、

“ひとつのElectrumウォレットがユーザーのコンピューターにあり、
仮にそのユーザーがスマートフォンのウォレットでトランザクションを実行する場合には、
双方のデバイスからの署名が得られないと、トランザクションは実行できません。
この仕様により、攻撃者は2つのデバイスへのアクセスを得ない限り、
そのアドレスからコインを盗むことはできません。”

Electrumウォレットの特徴

秘密鍵からのウォレットの生成

秘密鍵からウォレットを作成する為誤って鍵を紛失してしまった場合にもシードフレーズからウォレットを再生することができます。

インスタンツ・オン

クライアントはブロックチェーンをダウンロードすることなく、サーバーにブロックチェーン情報をリクエストすることのみが求められます。この為、遅延がなく、常に最新の状態を保つことが可能です。

トランザクションへのローカル署名

ユーザーの秘密鍵はサーバーに共有されることなく、トランザクションに署名することができます。よって、ユーザーはサーバーを信用する必要がありません。

プライバシー

Electrumサーバーはユーザーアカウントを保管しません。ユーザーは自らの秘密鍵をエクスポートすることも可能です。ユーザーは秘密鍵に対しての所有権を完全に保持します。

5. 複数のアルゴリズムのサポート

バージは複数のアルゴリズムをサポートする暗号通貨で、異なる種類のマイニングデバイスを所有するユーザーが平等にコインを獲得できるように設計されています。

バージは5つのハッシュ関数を1つのブロックチェーン上で統合している数少ない暗号通貨内の1つです。この事はセキュリティ向上に繋がるとともに、幅広いユーザーとデバイスがバージをマイニングすることを可能にし、結果として平等なバージの分配が確保されています。

バージの最大供給量は165億コインです。バージを他の暗号通貨から際立たせるのは、1つのブロックチェーン上で同時に機能する5つのPoWアルゴリズムです。

その5つは、Scrypt、X17、Lyra2rev2、myr-groestl、blake2sと呼ばれており、5つのアルゴリズム全てが、30秒のブロックタイムターゲットを持っています。計算の難易度はアルゴリズムのハッシュレートのみによって影響を受けます。この事もセキュリティの向上と、51%アタックを防止に寄与します。

6. Androidアプリへの TorとI2Pの統合

バージはモバイルにおける暗号通貨の世界で、第一線でイノベーションを起こしています。バージは2つのとてもユニークで初めてのタイプのandroidウォレットを開拓/開発しました。その1つはTorネットワーク上で、もう1つはI2Pネットワーク上でバージを扱います。

バージのTor/I2Pウォレットは匿名性という前提の上に構築されています。従って、それぞれのウォレットはユーザーの情報をブロックチェーン上に接続したり、ブロードキャストしたりする能力を備えていません。

トランザクションはサトシ・ナカモトの論文の中で紹介されているSPV (Simple Payment Verification) によって完了します。これは、ウォレットに「Proof of Inclusion (以下PoI)」という方法を用いてトランザクションを検証することを許可します。PoIは、全てのブロックチェーンをダウンロードすることなく、特定のトランザクションが特定のブロックに含まれているかを検証する方法です。(Electrumウォレットの機能に類似します)

SPVは瞬時に近い支払いの承認を実現します。なぜなら、SPVはブロックヘッダーのダウンロードのみをクライアントに必要とするからです。ブロックヘッダーは完全なブロックと比較して劇的にサイズが小さいので、非常に軽量なクライアントとして機能させることができます。

また、バージのモバイルウォレットは、4桁のピンコードや生体認証によるロック等、物理的にもセキュリティを向上させる為のレイヤーを備えています。

更に、バージのモバイルTor/i2Pウォレットは、P2Pトランザクションを、QRコードをスキャンすることで実行可能です。また、クライアントはペーパーウォレットからQRコードをインポートし、コールドウォレットから残高を引き出すことが可能です。

7. 今後の開発予定： Discord（ディスコード）& Telegram P2P

バージを用いたP2PのトランザクションはTelegram、Twitter、Discord等のプラットフォーム上でもサポートされています。また、SlackとSteamに対応すべく開発が進んでいます。Telegramは無料で利用できるクラウド型のインスタントメッセンジャーサービスで、Android、iOS、Windows Phone、Windows NT、macOS、Linuxをサポートしています。Telegramは「MTproto」と呼ばれる対称暗号化方式を採用しています。このプロトコルはNikolai Durovを含むTelegramの複数のデベロッパーによって開発され、「256-bit symmetric AES encryption」と「RSA 2048 encryption」、そして「Diffie-Hellman key exchange」をベースにしています。Discordは独自のフリーウェアVoIPアプリケーションで、暗号通貨の世界では広く利用されています。DiscordもTelegramのように、Windows、mac、Android、iOSをサポートし、ブラウザでアクセスできるウェブクライアントを有しています。これらのプラットフォーム上でバージP2P機能を実装することで、ユーザーはどこにいても即座に資金を送受信できるようになります。（クラウドベースの為、ウォレットをインストールしていなくても実行可能です。）

P2Pはユーザーにインターネットもしくはモバイルデバイスを通じて、コインを移動することを可能にするオンラインテクノロジーです。これらを実行する為にユーザーはオンラインでアプリケーションを利用します。Discord、Telegramアプリケーションの場合はbotを通じて、移動するコインの量を指示します。コインの受取者はユーザーネームのみで、送信者が送金を実行すれば、アプリケーション内でbotからの通知によってコインの受領を知ることができます。この際、受信用に新たに作成されたアドレスにコインでユーザーはコインを受領します。ユーザーはアプリケーション内で「withdraw（出金する）」などの簡単なコマンドをツイートやメッセージでbotに送信することができ、その後、新たに獲得したバージの受け取り方法の手順に促されます。このサービスは送信者に対して、送金したい金額と送信先の2つ以上の情報を一切要求しません。IPアドレスや所在地、名前と言ったプライバシーに該当する情報は、送金プロセスを通じて記録されることはありません。トランザクションの実行に際して、ユーザー個人を特定できる情報は完全に匿名な状態が保たれます。

バージはTwitter、Reddit、Internet Relay Chat (IRC)にP2Pソリューションを提供することを既に実現している数少ない暗号通貨です（Slack、Steamは開発中）。このようなP2Pサービスの提供はユーザーが日常的に利用しているプラットフォームでバージを送金することを可能にします。

8. レイス・プロトコル

レイス・プロトコルとは？

レイス・プロトコルが暗号通貨の歴史上、初めて実現するのは、「匿名性を担保しながら、パブリックなブロックチェーンとプライベートなブロックチェーンを選択できること」です。この革新的な新しいシステムを通じて、透明性と説明可能性に重きを置くユーザー、例えば小売店等のユーザーは、ブロックチェーン上で取引の内容を他のユーザーから確認できる状態にするオプションを持つことができます。レイス・プロトコルは、安全で堅牢な方法でXVGコインを送受信しながら、完全な匿名性が維持され、取引の内容は公開されているパブリックなブロックチェーンで捕捉される事はありません。今回のアップデートは「Stealth Addressing（ステルス・アドレッシング）」及び、最新のTor+SSLの統合を含み、core QTウォレットを使っているバージョンのユーザーを、現在稼働しているクリアネットから分離し、独占的に運営されている最新のTorネットワークに統合します。

そして前述の通り、ユーザーがパブリックかプライベート、どちらのブロックチェーンを通じて取引を行いたいのかに応じて、選択することができる機能が含まれています。洗練されたシンプルさを保ちながら、今回のレイス・プロトコルのアップデートによって、バージョンのユーザーがウォレットから（選択するための）スイッチを動かすだけで、ステルス・アドレッシングを利用することができます。更に、この取引はTorネットワークを経由し、ユーザーのIPアドレスは秘匿されます。

ディープ・ダイブ

ここからは鍵の合意に関する重要なコンセプト（「Elliptic Curve（楕円曲線暗号）」及びDiffie Hellman（ディフィー・ヘルマン））の説明を通じて理解を深めていきます。

鍵に関する合意とは？

鍵に関する合意とは、2人以上の当事者がシンメトリカルな暗号化を行う為に、1つ以上の鍵の中から、どの鍵から得た値を用いて計算を行うかということを合意する手続きです。どちらかの当事者が、一方的に「自身が所有する鍵から得られる値を用いる」と決定することはありません。つまり、どちらの当事者も最終的な値を決めるプロセスに関わります。また、ポイントとして、鍵の交換を目撃している者は最終的な鍵の値を知る術はありません。ここでも、この鍵の合意は原則として匿名であり、当事者は相手のアイデンティティを把握することはできません。

ディフィー・ヘルマン・アルゴリズムとは？

オリジナルなディフィー・ヘルマンの仕組みは値の大きな素数を法とした(素数で除した)整数の乗算処理を基本とします。この方式は以下のように行われます。まず値の大きな素数 p を用意し、 g を $\mathbb{Z}/p\mathbb{Z}$ の生成元とします。この g と p は公開されているものとします。いま X と Y が通信を行うとします。このとき X と Y はお互い秘密の値 a, b を選択します、この値は 0 以上 $p-2$ 以下の範囲からランダムに選びます。このように用意された値 (g, p, a, b) を当事者で交換しながら計算し算出された値を共通鍵暗号方式の鍵として使用します。（詳細な説明は[日本語版 wikipedia](#)を御覧ください）

楕円曲線ディフィー・ヘルマン鍵共有(EDCH)とは?

EDCH(楕円曲線ディフィー・ヘルマン鍵共有)はディフィー・ヘルマンのアルゴリズムをElliptic Curve (楕円曲線暗号)に適するように変更しています。これも鍵についての合意形成を行うためのプロトコルで、どのように鍵が生成され当事者間で交換されるかを定義します。この鍵を用いてどのように暗号化を行うのかは当事者次第ですが、EDCHは以下のような課題を解決するために実装されています。

例: AnthonyとBillyという2人の当事者がいます。この2人は情報を盗み見ようとするが解読はできないだろうと考えられる第三者がいる前提で安全に情報を交換しようとしています。

1. AnthonyとBillyはそれぞれの秘密鍵と公開鍵を生成します。
今、Anthonyの秘密鍵dAと公開鍵HA=dAGが存在します。また、Billyの秘密鍵dBと公開鍵HB=dBGが存在します。AnthonyとBillyは同じ有限体上のElliptic Curveに共通の基準点Gを持っています。
2. AnthonyとBillyはそれぞれの公開鍵であるHAとHBを安全ではないチャンネル上で交換します。第三者はこの公開鍵を傍受することはできますが、其々の離散対数問題を解かないと秘密鍵dAまたはdBに辿り着くことはできません。
3. Anthonyは彼自身の秘密鍵とBillyの公開鍵を用いてS=dAHBを計算します。Billyも同様の計算を行い、S=dBHAを導き出します。この「S」は両者で共有されています。

$$S = dAHB = dA(dBG) = dB(dAG) = dBHA$$

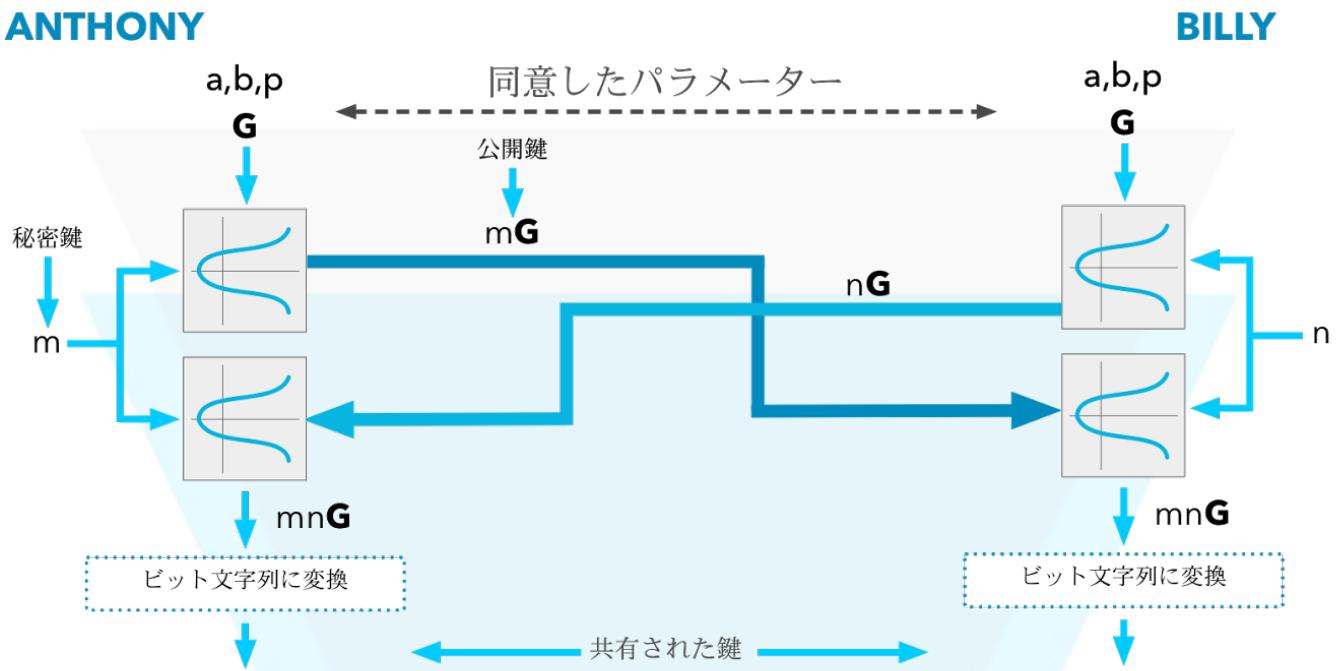
傍受した第三者は両者の公開鍵であるHAとHBを知っていても、共有の秘密である「S」を導き出すことはできないのです。

トランザクションの開始において、AnthonyとBillyは取引に用いるパラメーターを合意しなければいけません。ここでは、a、b、p、Gです。(Figure3を参照) 次にそれぞれがランダムな整数を生成し秘密鍵とします。この秘密鍵はAnthony側では「m」、Billy側では「n」とします。そしてそれぞれ、この値を乗算し基準点「G」を導き出し、この点が秘密鍵から導き出された公開鍵を表す値を持つ点になります。Elliptic Curve (楕円曲線暗号)については、それぞれの点がx座標とy座標を構成するということを覚えておいてください。

そして、AnthonyとBillyはそれぞれの公開鍵を交換し、自らの秘密鍵と受け取った相手の公開鍵を乗算します。この手続によって、双方にとって共有の新しい点が導き出されます。この点は鍵として利用可能なビット文字列に変換される為に存在し続けます。

注: 傍受を試みる第三者はこの交換された公開鍵や、パラメーターを知り得ますが、秘密鍵が分からぬ限りにおいて、当事者間で導き出した鍵に辿り着くことはできません。

図解3：ECDH



ステルス・アドレッシングとは？

ステルス・アドレッシングは送信者が「One time destination addresses（ワンタイム・ディスティネーション・アドレス）」を無限に生成することを許容します。この生成された使い捨てのアドレスを利用してことで、当事者は自身のオリジナルなウォレットのアドレスを介してやり取り（通信）する事はありません。そして、このアドレスは、受信者のみが使用し復元することができます。そして、当事者以外が両者のアドレスに紐付けることはできません。これを実現しているのは「Elliptic Curve（椭円曲線暗号）」と呼ばれる暗号学の仕組みです。※ 実際にステルス・アドレッシングを利用されているのは「Elliptic Curve Diffie Hellmann (ECDH)」です。この仕組によって、取引を行う者同士が、お互いの公開鍵を知っていれば、「当事者間で共有できる秘密の鍵」を生成することができます。この共有された秘密鍵は誰も、複製したり、当事者の公開鍵と紐付けしたりすることはできません。

バージのステルス・アドレッシングは95文字の文字列で、「public view key（パブリック・ビュー・キー）」と「public spend key（パブリック・スペンド・キー）」を含みます。AnthonyがBillyにXVGを送信する時に、AnthonyはBillyのパブリック・ビュー・キーとパブリック・スペンド・キーと、ある乱数を用いて、Billyが新しい「残高」を受け取る為に、ユニークなワンタイム・パブリック・キーを（ステルス・アドレス）生成します。誰もが、このワンタイム・パブリック・キーをブロックチェーン上で確認することができますが、AnthonyがBillyにXVGを送ったことは二人にしかわかりません。「残高」はこのように作成され、Billyは届けられた残高を、彼女のウォレットの「プライベート・ビュー・キー」を使ってブロックチェーンをスキャンニングしウォレットに取り込み、使用可能な状態にすることができます。一度、Billyのウォレットから発見されれば、彼女はワンタイム・パブリックキーに対応する「ワンタイム・プライベート・キー」を自ら計算し導き出し、紐づく「残高」を、彼女のウォレットのプライベート・“スペンド”・キーを利用して使用することができます。このプロセスはBillyのウォレットのアドレスとトランザクションを紐付けられることなく行われています。

キーに関する要点

1. オリジナルのパブリック・アドレスには当事者以外紐付けることはできません
2. 如何なるワンタイム・アドレスにも紐付きません
3. 受取人のみが、受け取った全ての支払を紐付けることができます
4. 受取人だけが、ワンタイム・アドレスに紐づく秘密鍵を導き出すことができます

ステルス・アドレッシングはユーザーが取引の度に「ワンタイムパブリックキー（使い捨ての公開鍵）」の生成を許容することで、ユーザーのプライバシーを向上させます。このワンタイムパブリックキーは、自動的に「誰が、新しい取引によって生じる残高（=アウトプット）を使用できるのか」を自動的に定義し記録します。ステルスアドレッシングは、ユーザーにパブリックなブロックチェーンの外で取引を行うことを適切に許容することで、この「残高」がユーザーのウォレットのアドレスに紐付けられる事を防ぎます。外部者は、「ユーザー間の資金の移動があったのか」を知る術はなく、ブロックチェーン上のトランザクションの記録を単純に見て、ウォレットのアドレスに紐付ける事もできません。例えば、AnthonyがBillyにXVGを送信したい時に、Billyが受け取った「残高」はBillyのパブリックなウォレットのアドレスに紐付けられる事はありません。ステルスアドレッシングは、資金を送信するユーザーが、ウォレットの中で取引の承認を確認することで、支払いが適切に行われた事を証明することができます。上記のケースではAnthonyは自身の支払いが完了したことをウォレットから証明できます。ここでも、Billyは自身にXVGが「いつ」そして、「送信されたこと」さえも誰も知ることができないと理解しているので、安心して取引をすることができます。

Tor + SSL 統合

以前から、バージのcore QTウォレット・ユーザーはクリアネットを利用していました。レイス・プロトコルでは、私たちは全てのQTユーザーをクリアネットからTorネットワークに移動します。Torは非中央集権的なネットワーク・システムで、ユーザーはランダムな複数のネットワークのリレーを経由して通信を行うことで、ユーザーのIPアドレスに関する情報を高度に難読化します。今回のTorの統合にはSSLによる暗号化も含まれており、暗号化されたセキュアなウォレット間の通信は、ウォレット間でやり取りされるデータが完全かつ秘匿された状態であることを確かにします。SSLによる暗号化は更に、ウォレット間を行き交うデータが途中で傍受されたり、改変されないことを確かにします。Torに関する追加の情報はブラックペーパーのセクション2に記載があります。

9. レイス・プロトコルの使用事例

看護学生で間もなく卒業を迎えるJessicaのケースです。彼女はあまりお金がなく、彼女にとって資金の流動性（お金を借りられること）は最も重要な事項です。Jessicaは最近、彼女のクレジットカードを使ってオンラインで買い物をしました。不幸にも、彼女の過ちによって、彼女のクレジットカード番号はスキミングされ、高価なハンドバッグを購入する為に使われてしまいました。カード会社は補償することに合意してくれたものの、新しいカードが届くまでには数日を要しました。この経験の後、彼女はお金に関するセキュリティは自分の責任で守る必要がある事を強く認識しました。この時、彼女はXVGの存在と、新プロトコル「Wraith プロトコル」によって、彼女がよく買い物するオンラインサイトで「Coinpayments.net」を通じて安全に支払いをすることが出来ることを知りました。彼女は取引を自分自身でコントロールし、恐れることなく取引を行うことができるようになりました。

次に、経営者のRandalのケースです。彼は自身の顧客の情報を守り、安全な取引を提供する事の重要性をとても強く認識しています。彼は、匿名の遺伝子検査をパーキンソン病や認知症等の病気を対象に検査サービスを提供している為、この点は特に重要です。顧客情報が漏洩する事は、彼のビジネスだけでなく、顧客の生活を脅かしかねません。彼は、多くの伝統的な経済取引の方法が、実際には情報漏えいを防ぎ、彼のビジネスと顧客を守ることを保証できない事を知り、彼はXVGを使って取引を開始しました。Core QTウォレットを通じてステルス・アドレッシングを利用できるようになったことで、彼は XVGで支払を受け付けるだけでなく、完全に匿名な検査サービスを提供できるようになりました。彼のビジネスは今、「情報が漏洩するリスクを冒すことなく、命を守る情報を提供する」事ができるのです。

10. アトミック・スワップ

アトミック・スワップは「クロス・チェーン・トレーディング」とも呼ばれ、XVGと今日、市場に流通する他の暗号通貨との互換性を実現します。アトミック・スワップはユーザー間で異なる暗号通貨を中心集権的な機関を介することなく、資金（コイン・トークン）を相互に送信する事を可能にします。バージはBIP65 にて、CheckLockTime Verify (CLTV) (Hash Time-Locked Contract. (HTLC)とも呼ばれます。) を実装します。HTLCは「hash-locks (ハッシュロック)」と「time-locks (タイムロック)」を用いる支払方法の1つで、この方法において、受取人に「期限までに、自らも支払をした事の証明証を発行した上で、相手からの支払を受領する事」を要求します。この条件を満たさない場合、受領する権利を喪失し、資金は支払者に返還されます。例えば、取引を行う当事者がともに正しいブロックチェーンにそれぞれのトランザクションを送信した時（ユーザーAはXVGをバージのブロックチェーン、ユーザーBはETHをイーサリアムのブロックチェーンに送信したとします）、受取人はシークレット・ハッシュ（これが前述の支払をした事の証明書に該当）を明らかにすることで、支払を受取る権利があることを主張することができます。この手続により、例え、2つの異なるブロックチェーンをクロスする取引であっても、2つのトランザクションを紐付けることが可能になります。もし、受取人がこのシークレット・ハッシュを明らかにしない場合、支払は無効になり、資金は支払者に返還されます。

アトミック・スワップの実装によって、ユーザーはアトミック・スワップをTorネットワーク経由で、レイス・プロトコルを用いて活用することができ、IPアドレスの難読化と個人情報の保護を確保しながら、XVGをクロスチェーンで送受信することができるようになります。更に、この実装はクロスチェーン取引のみならず、将来の「ライトニング・ネットワーク」の実装への足がけとなり、クロスチェーンでの取引の自動実行やトレーディングの実現にも繋がるでしょう。

11. 暗号化チャット: Visp

VispはP2P(peer to peer)のインスタント・メッセージ・システムです。最先端の暗号化技術を用いてユーザーのコミュニケーションにおけるプライバシーを保護しています。全てのメッセージはAES-256-CBCアルゴリズムによって証明された方法で暗号化されています。さらに、ノード間で分散され洗練されたトライック解析システムを用いる攻撃者から内容を推測されることを防ぎます。VispはElliptic Curve Digital Signature アルゴリズム (ECDSA=楕円曲線電子署名アルゴリズム) を用いています。これは、既に登場したElliptic Curve (楕円曲線暗号) の派生技術です。ECDSAによってユーザーはそのメッセージが正しい送信者から送信され、伝搬の過程で開封されたり、改変されていない確認を持つことができます。メッセージは以前から存在しているバージのネットワークを通じて伝搬されます。暗号化されたメッセージのコピーは48時間、各ノードに保管されます。

ステルス・アドレッシングによるトランザクションによって、ECDHによる鍵交換の方法で、秘密鍵が暗号化されて送受信者間で共有されることを可能にします。これには、メッセージに埋め込まれたデータと送受信者によって保有されているバージのステルス・アドレスの秘密鍵を利用しています。これにより、メッセージの伝搬において、受信者が誰か誰もわからないという状況を可能にします。このメッセージの送信はXVGを送信するように、受信者の公開鍵を保持する必要があります。この公開鍵とはバージのトランザクションが記録されているブロックチェーン上で、送金をしたことがあるユーザーであれば発見することができます。もしユーザーがまだ一度も送金をしたことがないアドレスにメッセージを送信したい場合は、この公開鍵の共有は手動で行われる必要があります。

バージはsecp256k1カーブをすべてのElliptic Curve関数用いています。これはビットコインで用いられているものと同様で、多くのアルトコインでも用いられています。この広範な利用と実績によっても、secp256k1が安全な方法ではないと言うことは難しいでしょう。また、メッセージはメッセージと一緒に送信された鍵によって署名されています。このことは、メッセージを受信したあなたに発信元について確信を持たせ、更にメッセージの送信者の公開鍵をメッセージから抽出することを許可することで返信に必要な情報をあなたに提供しています。

12. ブルーム・フィルター：BIP37

BIP37 (IP=改善提案) は主にSPVクライアントが主に利用しているフィルターで、クライアントが自身のアドレスにマッチするトランザクションとブロック・データの要約 (Merkle Tree=ハッシュ木) のみをリクエストする時に利用し、広義のトランザクション・スピードを向上させます。この改善提案では端末間でやり取りするデータの量を削減する新しいP2Pプロトコルを追加します。端末はバージョン・ハンドシェイク (2点間の通信路を確立した後、本格的に通信を行う前にパラメータを取り決めるなどの事前のやり取りを自動的に行うこと) を終えた後コネクションごとにフィルターを設定するオプションを有します。

13. 今後の開発予定：RSKスマートコントラクト

「RSK」という名で知られているRootstockは双方向ペグを行えるサイドチェーンで、バージネットワークと接続することで、スマートコントラクト機能を提供します。また、RSKはオフチェーンのプロトコルを用いて、ほとんど瞬時の決済を実現する事を可能にします。

RSKは独自のトークンを持たない、独立したブロックチェーンです。独自にトークンを持たない代わりに、既に存在するバージ（\$XVG）のようなトークンを利用します。RSKはスマートトークンをバージにペグするため、スマートトークンの価値はバージとまったく同じとなります。ユーザーはバージ及びRSKの2つのブロックチェーン間で自由にトークンを移動することができます。

スマートコントラクトの実行には手数料が必要です。スマートコントラクトを実行したいユーザーは保有するバージを預託すると、RSKのブロックチェーン上でロックされます。

これは、smartXVG（XVGはバージのシンボル）として手数料の支払いに利用できるようにリザーブされます。言わば、手数料の支払いに必要なバージを当座預金口座に移し、該当する支払いに充当できるようにする、と表現することもできます。

ここで重要なのは、ユーザーによる簡単なスマートコントラクト、例えばトランザクションの実行前に複数人の署名を要求するマルチシグのような単純なコントラクトの実行は既にビットコイン上で実現されているということです。RSKをバージに実装することで、この既に実現されている単純なスマートコントラクトから、イーサリアムが提供するような完全なスマートコントラクトを実行できる、全く新しい次元のレベルに押し上げることができます。

この他にも、RSKの実装メリットとしてスケーリング性能向上に寄与することが挙げられます。RSKは現在、秒間400もの支払トランザクションを処理することが可能で、これは現在バージが実現している秒間100トランザクションの処理能力を大幅に上回ります。RSKの開発チームはより高い目標を持っており、「Lumino」と呼ばれるセカンドレイヤー技術を用いて、秒間2000トランザクションの実現を目指しています。LTCP(Lumino Transaction Compression Protocol)のホワイトペーパーによるとLuminoネットワークはオフチェーンの決済システムで、Luminoトランザクション圧縮プロトコルを使用しています。LTCPはビットコインのスケーリングの問題を解決する為にデザインされ、現在ライトコインでテストされている、ライトニングネットワークに類似するものと考える事ができます。

14. リファレンス

[1] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/bitcoin.pdf>

[2] I2P: A scalable framework for anonymous communication - I2P. (n.d.). Retrieved from <https://geti2p.net/en/docs/how/tech-intro>

[3] Multisignature - Bitcoin Wiki. (n.d.). Retrieved August 8, 2017, from <https://en.bitcoin.it/wiki/Multisignature>

[4] Voegtlin, T. (n.d.). Welcome to the Electrum Documentation! — Electrum 2.5 documentation. Retrieved August 8, 2017, from <http://docs.electrum.org/en/latest/>

他のリファレンス

Gribble, S., Brewer, E., Hellerstein, J., & Culler, D. (2000, October 23). Scalable, Distributed Data Structures for Internet Service Construction. Retrieved from https://www.usenix.org/legacy/events/osdi2000/full_papers/gribble/gribble_html/index.html

Anonymity and the Block Chain • IHB News™. (2014, November 18). Retrieved August 08, 2017, from <https://ihb.io/2014-11-17/news/anonymity-block-chain-13570>

Holden, E. (2017, July 18). An Introduction to Tor vs I2P. Retrieved August 08, 2017, from <https://www.ipvpn.net/privacy-guides/an-introduction-to-tor-vs-i2p>

Distributed hash table. (n.d.). Retrieved August 08, 2017, from http://infoanarchy.org/Distributed_hash_table

Scharr, J. (2013, October 23). What Is Tor - How Does Tor Work - How to Use Tor. Retrieved August 08, 2017, from <https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html>

Durumeric, Z., Wustrow, E., & Halderman, J. (2013). ZMap: Fast Internet-Wide Scanning and its Security Applications. Retrieved from <https://zmap.io/paper.pdf>

Voegtlin, T. (2015). Simple Payment Verification — Electrum 2.5 documentation. Retrieved from <http://docs.electrum.org/en/latest/spv.html>

SPV, Simplified Payment Verification - Bitcoin Glossary. (2017). Retrieved from <https://bitcoin.org/en/glossary/simplified-payment-verification>

<https://atlas.torproject.org/#search/flag:authority>

<http://torstatus.blutmagie.de/>

15. コントリビューター

As an open source project we find it very important to thank our contributors who have given us a helping hand in order for us to get to where we are today.

To that we say

Thank you

Translators

@tottokoproject

@Maeotsu_00

The Author

CryptoRekt

Verge Marketing Team

Core Marketing Team

CryptoRekt - The Hammer

Sasha Kolupaev - VP Of Operations

Maeotsu - Graphics and Marketing Lead: **Japan**

Greg Franko - Web Design and Marketing Specialist

Kieran - Marketing Specialist

Frank Dashwood - The Man | Marketing Strategist

@SpookyKid - Marketing Strategist

Rondoparisiano - Marketing Strategist

Cryptb - Marketing Strategist

Feyzi Ozsahin - Graphics Design and Marketing

@CYANO - Graphics Design and Marketing

Cees Van Dam - Social Media Expert

Patrick - International Project Manager

Contributors

@LuckLight - Community Manager

Harry - The Esskay, Software Developer

CryptoGrok - Marketing Advisor

Alexander Hourani - Marketing Lead: **Australia**

VergeKorea - Marketing Lead: **South Korea**

Lalo Trage - Marketing Lead: **Brazil**

Hristomir - Marketing Lead: **Bulgaria**

CapoDiCrypto - Marketing Lead: **Netherlands**

Frank v H - Marketing Contributor: **Netherlands**

Akshay P. - Marketing Contributor: **India**

Toko - Data Analysis Specialist: **Japan**

Kei Japan (Iero003) - Digital Marketing: **Japan**

ripplechan - GUNDAM: **Japan**

Simon Cheng - Marketing Lead: **China**

@TongTong9 - Marketing Contributor: **China**

@Dejvid - Marketing Lead: **Poland**

MXCSM - Marketing Contributor

Mr. Wolf - Official Verge Hype Man

Joaquin - Marketing strategist

SmartTrader - Marketing Advisor

Frank v H - Marketing Contributor: **Netherlands**

Michael Stollaire - Marketing Ambassador

@Dejvid - Marketing Lead: **Poland**

Jason (g0ldm0ney10) - Marketing Strategist

Emanuel Goldstein - Community Manager

Contact Info

[Twitter](#) [Telegram](#) [Slack](#) [Facebook](#) [IRC](#) [Reddit](#) [Steam](#) [Verge](#) [Discord](#) [BitCoinTalk](#)

[Radio Station](#)