
VERGE
The most privacy focused cryptocurrency
BLACKPAPER

1.0 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、付随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。

2.0 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、それを明かすこともありません。

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。

3.0 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、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断を回避する、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。

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。

4.0 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可能です。

インスタント・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可能です。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。

5.0 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の内の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。

6.0 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可能です。

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。

7.0 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。

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

Telegram及びDiscordでのP2Pのトランザクションのサポートは現在開発中で、8月中のリリースを予定しています。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はフリーウェアの 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。これを実行する為に、ユーザーはオンラインでこれらの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、ユーザーはbot機能を通じて、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から通知を受けることによってコインの受領を知ることができます。

この際、受取者は受信用に新たに作成されたアドレス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の説明を受けることが可能です。
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、名前といった、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)、 Slack、そしてSteam等に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。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。

9.0 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.ivpn.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/

10. 0 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

O.G Verge Development Team

Sunerok
Gfranko
CryptoRekt

Contributors

Core Marketing Team

@Spookykid
@CryptoRekt
@gfranko
@Crypto_K1NG
@JtheLizzard
@lucklight
@Cryptonator92
@feyziozsahin
@Slemicek
@Trilla6six6
@Dabbie USA
@Cyrus7at
@Thehunter9 Netherlands
@GGWeLost
@Jeanralphio69
@Crypth
@deheerlen
@Twomanytimes
@ScagFX
@TraderNILW

Github Contributors

Sunerok
Gfranko
CryptoRekt
Mkinney
badbrainIRC
Grinfax
Swat69
NeosStore
Koenwoortman
Hellokarma
Kirillseva
Fuzzbawls
Buzztiaan
Spiralmann666
stshort
alcy0ne
chisustation
ShapeShifter499
Infernoman
pallas1
bearsylla
2Dai
31percent
Racoooon
ceasarpolar
enewnanwebdev
giovanni1186
labelmeagod

Contact Info

Twitter Telegram Slack Facebook IRC Reddit Steam Verge Discord BitCoinTalk Radio Station