X-CASHを通じた支払いを促進する グローバルブロックチェーンネットワーク

X-CASHチーム: G. CHAUMONT, P. BUGNOT, Z. HILDRETH

要約 - 2009年のビットコインの誕生とそれの普及以来、主流の視聴者による暗号通貨の毎日の使用を妨げる多くの障害が残されています。このペーパーは、X-CASHの背後にある概念を詳細に提示し、その課題をどのように克服する予定であるかを示します。このホワイトペーパーで説明されている重要な概念の1つは、ユーザー、商人、銀行の間の3重接続です。 X-CASHは、コストを削減しながらセキュリティを強化し、スケーラビリティと処理時間を保証することで、決済業界に革命をもたらすことを目指しています。
暗号化空間における規制のますます増加する要求に応えるため、X-CASHはネットワークの部分的な匿名性のアップグレードを開発しており、ユーザーは取引の詳細を公開するオプションを公開する予定です。これはブロックチェーンに追加データを含めることで可能になります。
X-CASHは、ブロックチェーンソリューションの企業ニーズに対応し、スケーラビリティに取り組む目的で、オペレーターがカスタムサイズの取引で独自のチェーンを運営できるサイドチェーンソリューションを開発しています。ネットワークのゼロ知識証明の性質のおかげで、参加者は、自分の身元を明らかにすることなく、またはコンテンツ自体を文書や情報を共有することができます。このソリューションの重要なビジネスケースの1つは、ネットワークが引き続きトランザクションを目撃する2つのエンティティ間の契約の隠れた署名です。取引の詳細と性質は、例えば法的目的のために、情報を明らかにする必要があるまで隠されています。
***Index Terms*—Blockchain, Cryptocurrencies, Payment Gateway, Crypto-to-Fiat Conversion Platform, X-CASH, Sidechains, Zero-Knowledge Proof.**

１）はじめに

実世界のデジタル支払いは、すでに全世界で毎年近くに500億件の取引と共通の練習している[1]。技術的な観点から信頼できるものの、現在のデジタル決済ソリューションは、0.1%から2%の範囲の商人に対する高い手数料を伴う。さらに、これらのソリューションには、顧客の観点からも、特に自国で使用されていない場合には、余分なコストがかかります。
同時に、cryptocurrenciesは2017年以来採用率が指数関数的になって大幅に増加している[2]。彼らは地理的制約を克服しましたが、毎日の支払いにはほとんど使用されません。いくつかの理由には、難しいFIAT変換、低いスケーラビリティ、高い転送コスト[3]、規制と透明性の欠如というグローバルな状況[4]が含まれます。
すべてがデジタル化される傾向にある企業、銀行、および機関は、法的な書類作成やあらゆるタイプの取引決済に関して、依然として時間と資金を消費する手順を使用する傾向があります。
X-CASHチームは、CryptonoteとMoneroのアルゴリズムから派生したサイドチェインネットワークソリューションを使用して、納税証明ネットワークを使用することにより、既存の支払いソリューションを混乱させる可能性が高いと考えています。完全な取引。

２）X-CASHプロジェクト

A.目標と私たちについて

X-CASH [5]は、フランスのパリに本拠を置く登録済みのfintechであり、2018年初めに開始されました。このプロジェクトは、自己資金を拠出しており、異なる背景を持つ3人のブロックチェーン愛好者（金融、エンジニアリング、コンピュータサイエンス）。 X-CASHの主な目標は、ブロックチェーン技術を使用して手数料や取引時間を削減するデジタル支払いと取引の決済に関するグローバルなソリューションを提供することです。
フランスに拠点を置く同社は、フランスとEUの既存規制および今後の規制をすべて遵守することを目指しています。同様に、X-CASHは既存の銀行システムと密接な関係を構築するために金融業界と緊密に連携します。これらのステップは、暗号化を主流採用にもたらすことを義務付けています。規制はユーザーと投資家の保護を確実にし、銀行は小売顧客の堅実な基盤のおかげで触媒として役立つことでしょう。

B.基盤技術

X-CASHは、CryptoNightハッシュ関数[8] [9]を使用して、Cryptonote [7]から派生したMonero v7 [6]のコアコードに基づいています。 X-CASHベースの開発を継続的に改善しアップデートしている実績のあるブロックチェーンのソースコードを使用するように選択されました。
Moneroの主な魅力は、プライバシーコインであるという事実です。それは、誰かがブロードキャストまたはトランザクションを送信できることを意味する難読化された公的元帳を使用し

ますが、外部のオブザーバはソース、伝えることはできません2つの金額、または宛先を。プライバシーは個人の財務を管理する上で重要な要素ですが、銀行や機関はトレーサビリティのために資金源を知る必要があります。したがって、X-CASHは、ユーザーに取引を公開するかどうかを選択させることを提案しています。
さらに、ブロックチェーンの同期化を他の暗号化の通貨より速くし、トランザクションの待ち時間を短縮するために、世界的な専用サーバーのネットワークが実装されています。これは、X-CASHコアの将来の改善の展開における重要な要素です。

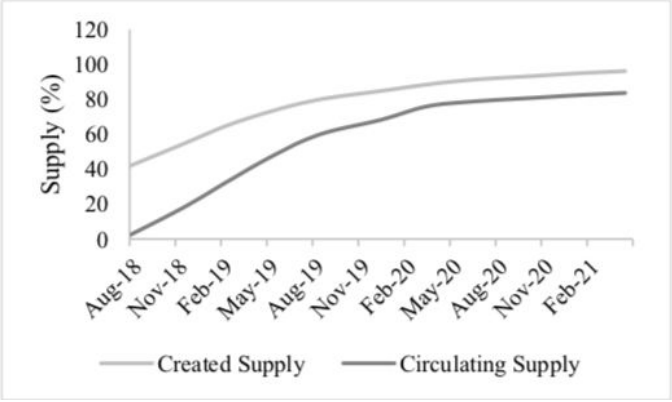
C.供給と排出の構造

X-CASHの総供給は、100,000,000,000（1000億XCA）である。
補給は次のようにして行われます。

- チーム専用の5%のうち、2%のコインが割り当てられています。残ったものは新しい参加者に提供されます。これらのコインの放出は、コインの時価総額に連動した厳しい条件のもとで行われます。
- 供給の10%は、チームの現在の給与、コインの開発、およびインフラストラクチャーの費用をカバーするために会社に提供されます。
- 総供給量の5%は現物市場価格に対して5〜30%の割引で、OTC取引を通じて民間投資家に売却される。この背後にある考え方は、コインスポット価格に影響を与えずにプロジェクトの初期段階で資金を調達することです（売却されたコインは権利確定期間の対象となります）。
- 供給の20%は20ヶ月間のエアドロッププログラムを通じて放出されます。このオプションは、コインをコミュニティに参加させながら鉱山設備を持たない人々に配布するための公平な方法であるため、これを選択しました。

現在の供給は毎月約4%増加し、2020年後半には供給の95%に達することになります。この時点で、X-CASH 2.0のリリースは既にPoSアルゴリズムで有効にされており、インフレ率は0,1-0,5%一定率に切り替える。
さらに、チームの割り当てられたコインのリリースは、コインの時価総額に応じて条件を受ける。実際には、1000万ドルの時価総額から始まり、その価値に10を掛けるたびに、チームの割り当てられたコインの20%がロック解除されます。これにより、パフォーマンスを重視し、コインを任意の期間ロックする代わりに、ハードダンピングを回避します。
ウォレットの資金を公的な住所で追跡する方法がないため、事前に払い出された資金は、一度四半期ごとに監査されます。独立した監査は、資金が分離財布に残っていることを確認します。このプロセスは、資金が銀行の金庫に保管された冷蔵財布に保管されるため、チームによって物理的に実行されます。
事前準備された供給は分離された口座に入れられ、徐々に循環に戻されるので、採掘された供給と実際の循環供給との間には相違がある。

右の図は、計画された循環供給の概要を時間で示しています。



D.創業チーム

X-CASHの創立チームは、合理的な目的でブロックチェーンテクノロジーを中心とした現実的なプロジェクトを開発するという共通の目標を持つ、学問的および職業的背景の異なる3人で構成されています。次のようにチームは次のとおりです。

Guilhem CHAUMONT

Chief Executive Officer

ギレムはblockchain技術と主流採用の間のギャップを埋めることを目的に、新たなcryptocurrencyを開始するために彼の仕事を残した元トレーダーです。ギルヘムは、2016年以来、2017年末に鉱業会社を設立する活発なトレーダーおよび投資家です。
ギルヘムは、Ecole Centrale de LyonのエネルギーエンジニアリングとHEC Parisの国際財務の2つの修士号を取得しています。ギルヘムは、最大手の銀行の2年のレートデリバティブ取引経験により、金融業界を動かす仕組みをよく理解しています。それ以前はCommissariatàl'Energie Atomiqueの原子力工学の学生研究員でした。

Zach HILDRETH

Chief Technology Officer

コンピュータサイエンスの学士号を取得するであり、ウェブサイト、ゲーム、およびソフトウェアをするフルスタックの開発者です。彼はまた、サイバーセキュリティを専門にしており、ブロックチェーン技術に興味を持ち始めました。彼は2013年から暗号侵害に投資し続けて以来、ブロックチェーンコミュニティに深く関わってきました。
Zachはまた、包括的な暗号化マイニングガイドの作者であり、最も活発なマイニングコミュニティの1つであるCTOです。

Paul BUGNOT

Chief Operating Officer

国立応用科学院でのナノテクノロジーの修士号で卒業後、ポールは、自動車のに対する特許弁護士として、その後、センターナショナルデRecherches Scientifiquesのリサーチエンジニアとして働いていました
業界。エキサイティングな機会を探して、フランスとヨーロッパでナノテクノロジーソリューションを提供する会社を担当しました。
新技術や新興企業に熱心なPaul氏は、X-CASHプロジェクトに参加しました。

E.ロードマップ

2018年の初めから2018年の9月まで：
開発の開始、主要なネットリリース、毎月の航空宇宙飛行の開始と交換リストX-CASHプロジェクトは2018年の第1四半期に急増しました。ブロックチェーンの最初の反復が迅速に導入されました。プロジェクトはその周りに建設されました。
その周りのウェブサイトと機能が開発され、最初のバージョンのGUI Walletが作成され、テストされて、技術に精通していないユーザーが1日目にウォレットを使用できるようにしました。6月の徹底した一連のテストとプロセス検証の後、X-CASHネットワークは7月31日に一般に公開されました。メインのネットリリースから3週間後、X-CASHの月間エアドップは8月21日に開始されました。 9月11日の最初の航空宇宙飛行の最後に、X-CASHは4つの為替リスティングで市場参入を発表しました。

Q3-Q4の終わり2018：
X-CASH 1.3 - 防弾および公的取引X-CASHプロジェクトの最初の主な更新は、防弾取引の実施です。防弾取引は、結果的に取引規模を縮小します。これにより、ブロックチェーンサイズの大幅な削減と取引手数料の削減が可能になります。同時に、取引の内容を公開する選択をユーザに与える公的取引が実施される。

Q4 2018 - モバイルウォレットのリリース
X-CASHの成功の鍵となる要素の1つは、一般の人々による使用です。この目的のために、ユーザはすべてのデバイスにわたって最も直感的かつ便利なインタフェースを必要とする。
GUIウォレットは、すべてのプラットフォームでシームレスに設計されています。デスクトップ、ラップトップ、モバイルデバイスのいずれの場合でも、同様のユーザーエクスペリエンスを全員に提供することです。
これらのモバイルウォレットのおかげで、ユーザは技術的なパラメータを心配することなく、自動的にネットワークに接続し、合理化されたユーザエクスペリエンスを提供します。

Q4 2018：第三者による商業的実施
X-CASH採用の他の要因の1つは、加盟店やサービスプロバイダーに直接支払うためにシステムを直接使用する可能性である。 APIは既にX-CASH支払いを統合するために第三者の加盟店に提供することができますが、主な目的はFiat通貨へのX-CASH変換を処理するインフラを構築することです。
これを可能にするために、X-CASHはフィアットへの商人の地位を簡単に清算して、支払いを別々に処理できるようにする市場作り活動を計画している。結局、X-CASHは商人にフィアットまたはX-CASHのいずれかを支払うオプションを提供できるはずです。 X-CASHの支払いには追加料金はかかりませんが、Fiatの支払いは30-50ベーシス・ポイント（bp）の範囲になります。

Q1 2019：X-CASH 2.0

現時点でX-CASHの最初のバージョンを正常に開始することに焦点を当てていたにもかかわらず、チームはブロックチェーンの未来を計画しています。 X-CASH 2.0は、API開発のスケーラビリティと基盤となる2つの重要なトピックに対処する必要があります。

3つの可能性があります：

•現在のコードを進化させる：これは、チームが集中している自然な道です。これは、cryptonoteとcryptonight PoWをコアコードとして維持しながら、プロジェクトが目標目標に徐々に到達するようにするインクリメンタルリリースから構成されています。 X-CASH 1.3の次のリリースは、9月末にセットアップされ、防弾取引を追加します。

•ゼロから新しい技術/コアコードを構築する：一定のサイズのブロックチェーンやブロックチェーン圧縮を含む新しいブロックチェーンコードを構築することは、エキサイティングな道ですが、開発には時間とリソースが必要です。

•既存のプロトコルにX-CASHを組み込む：X-CASHをより発展したブロックチェーンネットワークに実装することは、別の方法です。 Ethereumブロックチェーンの他の標準としてのERC20契約は興味深いかもしれませんが、現時点では実行可能ではありません。スケーラビリティにはまだ対応していないからです。同様に、EOSは、X-CASHプロジェクトが直面している課題への解決策を提供するソリューションを提供しています。結論は、技術は現時点では十分成熟していないが、平行した経験を実行し、それに応じてX-CASHの位置を改訂することは、その道筋を決めるのに役立つということです。

2018年9月初めの被験者の深い理解の後、現在のX-CASHコードの進化のための最初の解決法が選択されました。これにより、2019年初頭にPoSバージョンのCryptonoteがリリースされ、後でサイドチェーンソリューションが実装されます。

Q1 2019：
リテールバンキングプロトコルへのX-CASHの実装小売決済側では、究極の目標は、銀行口座からX-CASHを直接管理するオプションをユーザーに提供するために銀行と提携することです。
cryptocurrencyの需要はまだ成長しているように、これは、同様の銀行のための興味深い特徴だろうとありません。
銀行がまだクライアントに代わって責任ホルダーの役割を果たしているので、cryptocurrenciesを所有する直接的な解決策はまだ。
同時に、これにより、信用状や貸付契約などの銀行のブロックチェーンの実装が他のサービスと同様に可能になります。

Q2 2019：X-CASHにリンクされたデリバティブ商品
小売業者向けのX-CASHとFIATの間の変換は初日から競争力があるが、手数料を引き下げる改善の余地がある。
この目的のために、X-CASHは、X-CASHの流動性を高め、ユーザーが商人のポジションをより容易にヘッジすることを可能にするデリバティブ商品をリリースする予定です。

第一のステップは先物契約であり、ボラティリティの急上昇に対処するオプションをリリースすることを目指しています。
オールインでは、これらの機器を幅広く使用しているため、10〜35 bpの固定料金で販売者にプラグアンドプレイソリューションを提供できるはずです。

３）X-CASH 1.0：CRYPTONOTE ALGORITHM

A.作業証明（Pow）

ネットワーク参加者の作業量（ハッシュ）に基づいてブロックチェーンネットワーク全体でコンセンサスを達成するために使用されるアルゴリズムの一種です。ネットワークが潜在的なトランザクションを集約して次のブロックに追加する間、鉱夫はブロックのハッシュが特定のパラメータセット（通常は多数のゼロで始まるハッシュ）と一致するようにナンスを調整します。このプロセスは、マイニング方程式を満たすノンスをあらかじめ決定することができないため、多くの計算能力を必要とする。したがって、鉱夫はランダムまたは増分ノンスを試し、ハッシュを計算し、それらがパラメータのセットを満たすことができるかどうかを確認する必要があります。パラメータの集合は、ブロックを見つけるために計算される必要のあるノンストライ/ハッシュの数である難易度として知られているものに変換することができる。書面では、X-CASHネットワークの難しさは約186Mです[10]。ネットワークが60秒のブロックパラメータを満たすために毎秒約3Mのハッシュを計算していることを意味しています。
X-CASHは、ASICに耐性のあるMoneroの最新のCryptonote v1アルゴリズムを使用します。NiceHashに耐性を持たせるためにアルゴリズムを変更するかどうかについては、依然として内部的に議論されています。重要なネットワークハッシュレートの操作が行われない限り、現在のところ、NiceHashはネットワークコンピューティングパワーの流動性を向上させるため、このバージョンに固執することに決めました。

B.リングシグネチャ

Moneroのプライバシーの基盤となります。ビットコインのような公開トランザクションブロックチェーンでは、送信者の署名のみが追加されます。 X-CASHでは、すべての取引に最低2人の参加者が署名する必要があります。デフォルトでは、6人の参加者がトランザクションに署名し、真の送信者を識別することが難しくなります。将来のX-CASHの発展の中で、我々はUnique Ring Signature [11]を組み込む可能性についても検討している。

C.ステルスアドレス[12] [13]

送信者がワンタイムランダムアドレスを生成するように要求することにより、トランザクションにおけるプライバシーの追加層である。これは、パブリックアドレスがブロックチェーンに

記録されていないことを意味し、同様に、ブロックチェインエクスプローラを使用してパブリックアドレスバランスを表示する可能性がないことを意味します。リングシグネチャはトランザクションの履歴を追跡しないように見えるが、ステルスアドレスはトランザクションの詳細を隠すためのソリューションと見ることができる。セクションEは、余分な元帳を使用して追加のデータを保存することによって、ユーザーの裁量で匿名性を削除する方法を開発します。

D. Bulletproof Transactions [14] [15]

現在のアルゴリズムで使用されている範囲証明を置き換え、トランザクションサイズの縮小を可能にする。防弾は、取引の後ろの金額を隠して確認するために使用された数学的方法を置き換えることによって、範囲証明よりも改善されています。 X-CASHは、監査され、Moneroのネットワーク上に生存すれば、防御トランザクションを実装し、トランザクションサイズの80%の減少が予想されます。 Moneroのネットワーク上の防弾取引の現在の実装は2018年9月に予定されており、まもなくX-CASHに追加されます。

E.部分的な匿名性の実装暗号化空間におけるプライバシー

金融界と同様、非常に敏感なトピックです。このセクションの目的は、匿名性に関するX-CASH哲学の簡単な見通しを提供することです。

1）3種類のプライバシ情報の転送

（暗号化支払いなど）に関するトランザクションは、次の3つの主要コンポーネントに分けられます。

1. 送信者：トランザクションを開始しているユーザー
2. 受信者：トランザクションの恩恵を受けるユーザー
3. コンテンツ：財政支払いの場合に譲渡される金額は何ですか。

同様に、プライバシー情報は、3つの匿名層に分類することができます。

1. 完全な匿名性：を知る方法はありません鍵やパスコードなしで情報。
2. 部分的な匿名性：情報は追跡可能ですが基礎となる情報を隠す。最も良い例は、IBAN（銀行口座の住所）またはBTCの住所です。このアドレスは追跡可能であり、潜在的な送信者または受信者を表しますが、アドレスの背後にある最終情報、すなわちそれを制御する人間は隠されたままです
3. 匿名性はありません：固有の情報は直接誰にでもアクセス可能です。

これらの要素の組み合わせにより、ケース：

a）すべての情報に対する完全な匿名

トランザクションに埋め込まれた情報はすべて、一般ユーザーには表示されません。これは、Moneroを使用するすべてのCryptonoteコインの状態です。

b）間に送信者および/または受信者の部分的な匿名性

コンテンツが公開されている最も明白な使用例は、トランザクションの量が完全に表示されている間に送信者と受信者の両方が公開アドレスの後ろに隠れるビットコイントランザクションです。
Moneroコードの部分的な匿名性実装の目標は、ネットワーク上で取引するすべてのユーザーがこれらの2つの層を利用できるようにする必要から推進されます。これにより、プライバシーのニーズの大部分が満たされ、非公開トランザクションを実行するために必要な基礎基盤を提供しつつ、暗号世界での規制が増大するという話題が増えている[16] [17]。まもなく、すべての情報の匿名性がないなど、一部のケースではレビューするのが面白いかもしれませんが、すぐに実装する予定がないため、このドキュメントでは扱いません。

2）技術的実装部分

匿名取引の技術的実装のために選択されるソリューションは、展開の容易さ、コアコード自体のスケーラビリティ、機能、セキュリティのトレードオフです。ベースのMoneroコードをハードフォークするのを避けるために、X-CASHのコアコードのトランザクションコンポーネントを変更しないことが選択されています。これには、取引所、鉱山プール、商人、およびX-CASHネットワークに関与する他の関係者に、それを実装するかどうかの可能性を残すという利点があります。同時に2つのオプションがテストされています。第1のものは、分離された元帳に追加データを統合するものであり、第2のものはトランザクションブロック内のデータを含むものである。第1の解決策では、第2の元帳の情報が損なわれないことを保証するために、高いレベルのセキュリティを確保する必要があるという主な欠点の1つがあります。同時に、元のブロックチェーンのコアコードには影響がないため、最初のブロックチェーンの観点から追加のセキュリティ上の脅威はありません。

F.公的ノード同期能力に関して

ネットワーク容量を増加させるために、専用サーバ上で動作する公的ノードのネットワークがセットアップされている[16]。これは、地理的なカバレッジと帯域幅の容量が徐々に増加する3フェーズの展開から構成されます。

1）現在ライブ

現在のネットワークは、限定された地理的範囲を持つ15の専用サーバーで構成されています。サーバーの位置は、ユーザーの起源の最初の評価に基づいて決定されています。現在の場所には、米国、カナダ、フランス、ドイツ、ポーランド、中国、インド、日本、シンガポール、オーストラリアが含まれます。使用可能な総帯域幅は5 GB / Sです。これにより、1日あたり100,000ブロックの完全ブロックファイルの同期容量が可能になります。

2）Q4 2018

- サーバー数：30
- 帯域幅：10 GB /秒
- 追加場所：メキシコ、ブラジル、西ヨーロッパ、英国、ロシア、インドネシア、モロッコ＆SA

３）Q1-Q2 2019

- サーバー数：75
- 帯域幅：25 GB /秒
- 追加場所：アラスカ（米国）、残りのヨーロッパ、南コーラ、残りの南米およびタイ

４）X-CASH 2.0＆BEYOND：POS導入効率

スケーラビリティ、モジュール性という長期目標を達成するために、X-CASHネットワークは2つの重要なネットワークアップグレードを進めます。最初のものは2019年初頭に予定されており、コンセンサスアルゴリズムに変更が加えられる予定です。また、ネットワーク仕様に関して重要な一歩を踏み出すことができる新しい技術的特徴を提供する強い意欲もある：サイドチェーン。 X-CASH 2.0リリースでこの機能をリリースすることが強く望まれていますが、開発コストと時間を考慮し、仕様の一部を明確にする必要性を考慮すると、この機能は含まれる可能性が大きくなります後で。現在の目標は、2019年の終わりまでに、2019年第2四半期中にアルファ版を提供することです。

A. Stake Proof of Stake（PoS）

証拠は、ブロックチェーンネットワーク全体でコンセンサスを達成するために使用されるアルゴリズムの一種です。ネットワーク参加者のコイン（ステーク）の数。 PoWコンセンサスに対する主な利点は、コンピューティング/電力/エネルギー消費が高いPoSのハッシュを計算する必要性と比較して、デーモンを実行しているサーバに限られ、コンセンサスを生成することに限定されるエネルギー消費の削減である[17]。 20ノードのPoSネットワークは、現在のネットワークハッシュレート2と同等またはそれ以上のセキュリティレベルを達成し、消費電力は4kWで220kWです。
ブロック選択は、参加者の中からPoSアドレスで移転したステークに比例してランダムに選択されます。各ブロック選択プロセス中に、参加者は彼らがステークとその金額を所有していることを相手に証明しなければなりません。これは、ゼロ知識証明としてのリング署名の使用のおかげで、所有者に関する他の情報を明らかにすることなく達成されます。

B. Masternode X-CASH

DASH [18]と同様に、手数料や鉱業収入と引き換えにトランザクションを検証するマスターネットのネットワークを使用します。現在のマイニングプロセスと同様に、masternodeスキームには「dev」料金はありません。 masternodeの所有者に報酬の100％を残すこの決定は、masternodeの採用を奨励するために行われます。

1）支出と仕様Masternode

運営するために必要な最小限の株式について議論するとき、6/09/18 Asを実行するために必要なステーク、CryptonotevのX-CASHのNetwork Hashレートは2 MH / s

Masternodeは、2つの理由から、重要なエントリーの障壁となるはずです。最初の1つは、ネットワーク内のノードの速度と信頼性を高めるために、ネットワーク内のMasternodesの総数の制限です。最初のものにリンクされている2番目は、Masternodesのネットワークを「真の参加者」に保つ必要がある。これを実行する最善の方法の1つは、サーバー自体を実行するコストが重要でないように、株式を大幅に管理することです。 masternodeを実行するために必要な最小限のハードウェアに関する仕様を表現し、ネットワークの一部にすることを強制すべきかどうかについても議論されています。
依然として改正の対象となる100m XCASHの最小出資額は、現在のところ、masternodeの運用を決定している。チームのビジョンは、供給の約半分がmasternodeを走らせるべきであり、残りは真の循環供給であるということです。つまり、フルキャパシティーでは500個のMASternodeのネットワークを実行するために500億個のXCASHが使用されます。チームは、これが地方分権とネットワーク品質の間の良いトレードオフであると考えています。

タイプXCASHの普及に関する長期的な目標が達成された場合、XCASHマスターズの典型的な配布は次のようになります：

Type	Number of Masternodes
Governments	120
Corporations	150
Institutions	50
NGOs	30
Others	150

ステークスの低い人グループ化されたmasternodeに集まる。 masternodeの1%を所有することを可能にする最小ステークは、1m XCASHになります。このソリューションがX-CASH 2.0コードに直接実装されるのか、それとも市場にすでに存在する外部サービスプロバイダを通じて行われるのかについてはまだ検討中です[18] [19]。

2）投資収益短期的

供給の30%が採掘される間にPoSスイッチが行われるため、マスターノードを稼動させる大きなインセンティブが存在します。以下の表は、典型的なROIは、ネットワークMasternodesの仮定の下であるべきかを説明

XCASHにおける年率：Masternodesの推定数

Year	Estimated Number of Masternodes	Annualized ROI in XCASH (%)
2019	100	255%
2020	350	30%
2021	450	9%
2030	500	1%

2019年に観察された高いROIは、XCASH供給の大幅な削減（42%）を犠牲にして行われます。同様に、長期的には、masternodeを稼動するROIは大幅に低下するが、供給のインフレ率はゼロに近いことに留意することが重要である。したがって、これは、米ドルのインフレ率を1%上回る、masternode ROI（米ドル建て）を達成するという目標に合致するはずです。

C.サイドチェーン

1）仕様

サイドチェーンは、X-CASHネットワーク向けに計画されている最も重要なアップグレードの1つです。これは、メインブロックチェーンにコンテンツが記録されず、参加者の中でのみコンテンツが記録されるサイドチェーンを実行することから成ります[20]。安全性と信頼性を向上させるためには、X-CASH Masternodesをサイドチェーンに最低限必要とし、コンセンサスで最低33%の出資を残すことが義務付けられます。サイドチェーンの開始時に、各参加者は、サイドチェーンの中立化までメインチェーンの観点からロックされたままであるサイドチェーンに所定量のXCASHを転送することができます。サイドチェーン内では、参加者はステークを使用してサイドマスターネットを実行し、事前定義されたトランザクション仕様に従って取引を実行します。

2）トランザクションの仕様

サイドチェーンの重要な特徴と関心の1つは、トランザクションの詳細をパラメータ化する能力です。ユーザーは、料金、mixinの最小数、確認時間など、ほとんどのパラメータを変更できます。
サイドチェーンは、トランザクションの最大サイズを変更する可能性についての関心の大部分を見つけることができ、可変Xブロックを含めることができます。 Xブロックは、txに埋め込まれたデータの予め定義された余分なブロックであり、その特性（サイズに関して）もチェーンの開始時に定義される。一例は、契約データを共有するためのサプライヤと販売者間のサイドチェーンネットワークの作成です。トランザクションの特性はメインネットワークと同様のま

までですが、余分なデータブロックにより、任意のサイズ（たとえば10 MB）のデジタル署名された契約を追加することができます。すべてのデータは暗号化され、メインネットワークと同じステルスアドレスを使用してトランザクションが行われるため、トランザクションに関係する2者だけが他のユーザーに表示する必要があるまでコンテンツを知ることになります。興味深い重要なコンセプトの1つは、トランザクションは、まだ解読不可能であるが、すべての参加者によって目撃されタイムスタンプがつけられることである。

５）支払いゲートウェイと取引設定

ソリューションこのセクションでは、コアブロックチェーンネットワークの上に実装される2つのメインレイヤーについて説明します。最初のものは、顧客がX-CASHを使用して加盟店に支払う簡単なソリューションで構成されています。商人の視点から見ると、このソリューションは、従来の決済ソリューションの代わりに、減額手数料に焦点を当てて提示されます。

X-CASHプロトコルに組み込まれる第2の層は、新しいタイプのゼロ・ナレッジ・プルーフ・トランザクション決済です。機関、銀行、企業、個人は、マスターネットワーク上でサイドチェーンを実行することで、独自のブロックチェーンネットワークを実行し、XCASH支払いやさまざまな種類の情報を通じて価値を交換することができます。これらのサイドチェーンにはMoneroのコア原則も使用されるため、ユーザーは選択したオーディエンスに取引を表示/非表示するオプションがあり、ゼロ知識証明が可能になります。

A. XCASHからFIATへの変換プロセス

1）説明

XCASHからFIATへの変換プロセスは、XCASHコインをFIATの通貨に変換するためにX-CASHグローバルペイメントが提供するプラグアンドプレイソリューションとして記述できます。このソリューションの主な対象ユーザーは、オンライン小売業者です。このソリューションには、2つの主要コンポーネントがあります。最初のコンポーネントは財務で、2つ目は技術的なものです。変換プロセスは、X-CASHを（おそらく）他のaltcoinsに対して売買することを意味するため、より多くの取引所や1秒あたりの取引量のかなりの部分でかなりの市場深度を持つ必要があります。これは、XCASHを大量の多数の取引所に登録し、すべての市場でXCASHコインのマーケットメーカであることによって達成されます。暗号化通貨に関する規制の初期段階の性質のため、この活動はX-CASH開発を運営する同社の一部である可能性があります。近い将来、X-CASHの対象となるすべての情報に関して、この活動を中国の壁のある分離された会社に移すことが検討されます。
第2の層は、市場のコインの実際の流動化とFIAT通貨への変換を伴う技術的なものです。このプロセスはチームの裁量に委ねられており、いくつかのフォームを取ることができます。以下のサブセクションでは、典型的なプロセスは、顧客と販売業者の観点から、またバックエンドで起こっている清算プロセスから説明されています。

2）顧客の視点からのプロセス

- 顧客がカートをいっぱいにして、マーチャントのWebサイトの支払いボタンを押し、XCASH支払いソリューションを選択する
- 顧客はX（おそらく1または2）分の時間枠内でEUR相当のXCASHを送信する
- 支払い確認はレベル1の確認が満たされ、マーチャントのウェブサイトにリダイレクトされます。

3）マーチャントの見方からのプロセス

- マーチャントは、支払い確認が保留中の注文確認を受け取ります。
- マーチャントは、レベル1の支払い確認を受け取ります。
- 電子メールで顧客に注文を確認することができます
- 商人は、レベル3の支払いの確認を受け取り、商品を配達することができます
- 商人はトランザクションからFIAT通貨で資金を受け取ります

4）バックエンドの視点からのプロセス

- レベル1の確認支払いの受信します
- ALTと実行にX-CASHを変換するのに最高の市場の識別をショートFIATに対するALTの売却
- レベル3の支払いの確認が受けられ、FIATの加盟店への移転
- ALTとFIATの金額の調整

XCASHがALTコインに変換されるとき、ALTコインをFIAT通貨に短時間で変換して、市場リスク。変換は異なる取引所で行われる可能性が高いため、アセットを短期間で売却することが不可欠です。なぜなら、最終ステップは、ポジションを中立化するために売却された取引所にAltcoinを送信することにあります。

5）3段階確認プロセスブロックチェーン

取引は他の決済手段と比較して比較的高速ですが、依然として確認を受ける必要のある現金決済の世界とは互換性がありません。即時支払いと互換性を、ユーザーからのスムーズな処理を可能にするために、3つのレベルの確認が設定されます。

- レベル1は、トランザクションがネットワークにブロードキャストされ、mempoolに追加されたときに対応します。
- レベル2は、トランザクションがブロックに含まれている場合
- レベル3は、トランザクションがブロックに追加された後の一定数のブロック（確認）に対応します。

各レベルは、レベルが高いほど時間とセキュリティのトレードオフです拒絶/二重支出などを含む。ユーザの観点からは、放送が1〜3秒で行われるので、レベル1によって許容される瞬時にトランザクション時間を維持することが義務付けられている。同時に、これはブロックチェーンが依然として取引を含まないため市場リスクを伴うが、支払いをカバーするXCASHの清算が開始されている。最悪の場合のシナリオは、取引を拒否することであり（意図的な場合を除

き、限られた数の理由により発生する可能性があります）、FIAT通貨からXCASHへの換算が行われます。これは1〜2%の全体的なコストに変換されます。これは、積極的な発生見積もりで、1トランザクション当たり1〜2 bpのコストに100回転じます。

6）コストの要約

以下の表は、変換に伴うコストの概要を示すことを目的としています。

Item	Costs (bp)
XCASH/ALT Conversion	25
ALT/FIAT Conversion	5
FIAT Reconciliation	1
ALT Reconciliation	2
Short sell funding	0
X-CASH Fee	0
Total Costs	**33**

変換の重要なステップであるXCASH / ALT変換では、市場価格400satoshiを仮定すると、25bpのコストは控えめな見積りです。 XCASHごとにビッド・アスク・スプレッドを1 sat。
X-CASHは独自のマーケット・メーキング活動を行っているため、これらの数値よりも低い有効コストを達成することが期待されます。これらの市場コスト削減の目標は、より流動性の高いデリバティブの使用により達成される。

B.サイドチェーンネットワーク

1）説明サイドチェーンネットワーク

X-CASHネットワークに重要な追加機能を提供します。これは、誰もが独自のブロックチェーンネットワークを特定のブロック特性で開始できる可能性があります。その背後にある考え方は、大規模なブロックチェーンにトランザクションを記録しなくても、ブロックチェーンを使用する必要がある企業、機関、または政府にとって、簡単で適応性の高いソリューションを提供することです。さらに、ブロック数とトランザクションサイズの制限は、情報量を数kBに制限するため、ほとんどのプロフェッショナルエンティティによる主要なブロックチェーンの使用に対する重要な障壁となります。このため、企業のカスタマイズされたニーズに答える目的で、サブブロックチェーンネットワークのソリューションが開発されています。同時に、メインのブロックチェーンからのトランザクションを実行するためにサブブロックチェインを使用できるため、サブブロックチェーンネットワークはスケーラビリティの解決策になります。これは、主なブロックチェーンの手数料がマイクロペイメントを許可しない電子決済[21]に関して、特に大きな可能性を秘めています。

2）サイドチェーンネットワーク

a）情報ネットワーク情報ネットワーク

限られた参加者だけが取引を実行できるセミプライベートネットワークと見ることができます。しかし、サイドチェーンがメインチェーンのMasternodesを組み込んで動作させる必要があるため、ネットワークは完全にプライベートではありません。これらの理由から、それらも

公開されているが、アクセス権もビューキーも与えられていない場合、コンテンツはアクセス不可能なままである。
情報ネットワークの主な機能は、任意のtxブロックに追加情報を追加する可能性に依存します。チェーンの開始時に設定されたものの他に、追加されたデータのタイプまたはサイズに制限はありません。このソリューションは、（おそらく）企業や銀行のグループが文書とファイルを共有し、デジタル署名し、タイムスタンプを付けた簡単な方法になるように設計されています。このソリューションの背後にある2つの主な利点は、高速実行（分）と最小コストです（ハードウェアの観点からは、20ノードのサイドチェーンネットワークの年間コストは10,000ドル以下です）。
このテクノロジにはいくつかの潜在的なユースケースがあり、新しいアプリケーションを発見する必要があります。主要なを解決するためにサイドチェーンネットワークを運営する銀行のネットワークを想像することは可能取引です。この潜在的な用途は、金融サービス業界にとって最も有望なブロックチェーンアプリケーションの1つとして挙げられることが多い[22]。銀行と企業は、他のメンバーに開示する必要なしに信用状をデジタルで共有するネットワークを共有することもできます。同様に、妥当性の契約はサイドチェーンネットワーク上で交換することができます。これらの面では、主な挑戦は技術的なものではなく、これらの合意の法的性質の認識にある。

b）決済ネットワーク

X-CASHが牽引役を果たすようになると、特に決済ゲートウェイが成功しコスト効率が良いことが判明した場合、取引で急速に混雑することになります。このため、オフチェーン取引を有効にすることが不可欠であるか、取引手数料が徴収されるためマイクロペイメントが不可能になります。
これを行う方法の1つは、トランザクションの観点から同じ特徴を共有するサイドチェーンをメインチェーンとして作成することです。これらのチェーンの目的は、満足できるレベルのプライバシーを保証しながら、より低い地方分権化とコスト効率の間の最良のトレードオフを見つけることです。ある国で起こっている取引は、世界の反対側のサーバーによって目撃される必要はないと容易に主張することができますが、まだ支払レベルのチェーンを作成する必要があるかどうかはまだ決まっていません：地理的（国、都市地区等...）、セクシャル、または支払を取り扱う企業によって行われる。この最後の可能性の背後にある提案は、各銀行が独自のネットワークを運営できることであり、規制上の観点からも疑問を投げかけています。

６）デリバティブを通る液体の増加および揮発性の減少インストゥルメント

誘導体化装置を介して揮発性を低減VA6項で説明した手数料の主な要素の1つは、XCASHと他のaltcoinsとの間の市場の広がりです。このスプレッドは、ペアのボラティリティと流動性が密接に関連している2つの主要な情報源から発生します。

ボラティリティを低減する有効な方法の1つは、デリバティブ商品を導入することである[22] [23]。これはBitcoin市場でこれが目撃されているcryptocurrencyに特に当てはまります[24]。
X-CASHに関しては、2つのステップに分けることができる同様の目標があります。
最初のものは流動性を高め、大きなXCASHのFIAT変換への市場への影響を減らす先物商品の導入です。また、マーケット・メーキング・トレーディング・ブックのヘッジを容易にしながら、契約の解決を広げることができます。
第2の計画された手段は、オプションのリリースです。これらのデリバティブの目標は先物と似ていますが、長期的なボラティリティを保ちながらマーケットメイクの書籍を価格の急上昇から守ることも可能になります。全体として、これらの2つの商品の組み合わせは、XCASHからALTへの転換スプレッドのボラティリティを軽減し、中和しなければなりません。

７）結論

X-CASHプロジェクトは、cryptocurrenciesを使用して効果的な支払いソリューションを提供することを目指しています。このソリューションは、ユーザー、市場、商人を結ぶ使いやすいAPIとプラットフォームを開発することで、特に手数料の安さのおかげでデジタル支払いの標準になるように作られました。
その主な目的はネットワークのニーズを満たすことであるため、X-CASHはユーザーが取引の詳細を公開するための機能を統合します。これは、ブロックチェーン技術に関する拡大する規制を満たすための重要なステップとなります。
最後に、ネットワークを改善し、PoSに切り替え、サイドチェーンネットワークを有効にすることで、X-CASHは企業のゼロ知識証明情報システムに対するニーズを満たすと同時に、支払いグリッドのスケーラビリティに取り組んでいきたいと考えています。

８）バイオグラフィー

[1] Capgemini, "World Payments Report 2017," 2017.
[2] CoinMarketCap, "Global Charts - Total Market Capitalization," [Online]. Available: https://coinmarketcap.com/charts/
[3] bitcoinfees, "Historic daily average Bitcoin transaction fees (in dollars per transaction)," [Online]. Available:https://bitcoinfees.info.
[4] A. I. Joy, "THE FUTURE OF CRYPTO-CURRENCY IN THE ABSENCE OF REGULATION, SOCIAL AND LEGAL IMPACT".
[5] "X-CASH - Global blockchain network to receive & send payments across the world using cryptocurrency," X-CASH, [Online]. Available: https://www.x-cash.org
[6] T. M. Project.. [Online]. Available: https://github.com/monero-project/monero
[7] "An open-source technology and concepts for the cryptocurrencies of the future," [Online]. Available:https://cryptonote.org/

[8] M. J. T. N. N. A. M. J. Seigen, "CRYPTONOTE STANDARD 008 : CryptoNight Hash Function".
[9] "SHA-3," [Online]. Available: https://en.wikipedia.org/wiki/SHA-3
[10] X-CASH, "X-CASH Explorer," [Online]. Available: https://explorer.x-cash.org/.
[11] R. Mercer, "Privacy on the Blockchain: Unique Ring Signatures".
[12] R. M. Nicolas T. Courtois, "Stealth Address and Key Management Techniques in Blockchain Systems".
[13] Monero, "Monero - Stealth Addresses," [Online]. Available: https://getmonero.org/resources/moneropedia/stealthaddress.html.
[14] J. B. D. B. A. P. P. W. a. G. M. Benedikt Bünz, Bulletproofs: Short Proofs for Confidential Transactions and More.
[15] S. Noether, 07 12 2017. [Online]. Available: https://getmonero.org/2017/12/07/Monero-Compatible-Bulletproofs.html.
[16] Smartereum, "Japan's Financial Regulators want Cryptocurrency Exchanges to delist hard-to-track coins.," [Online]. Available: https://smartereum.com/11843/japans-financial-regulators-want-cryptocurrency-exchanges-to-delist-hard-to- track-coins/
[17] Cryptobriefing, "Privacy coins under threat regulation - Governments: Privacy Is Bad. Everyone Else: No It's Not.,"
[Online]. Available: https://cryptobriefing.com/privacy-coins-under-threat-regulation/
[18] X-CASH, "X-CASH - Official remote nodes," [Online]. Available: https://x-cash.org/remotenodes/
[19] BitFury Group, "Proof of Stake versus Proof of Work".
[20] D. D. Evan Duffield, "Dash: A Privacy-Centric Crypto-Currency".
[21] "CoinWatch," [Online]. Available: https://coinwatch.center.
[22] "MyNode," [Online]. Available: https://mynode.rocks/
[23] Forbes, "Explaining Side Chains, The Next Breakthrough In Blockchain," [Online]. Available:https://www.forbes.com/sites/shermanlee/2018/02/07/explaining-side-chains-the-next-breakthrough-in- blockchain/#795c287d52eb
[24] O. Hueber, "The blockchain and the sidechain innovations for the electronic commerce beyond the Bitcoin's framework".
[25] X-CASH, "Memo on sidechain network: characteristics, pricing and transaction output".
[26] Techcrunch, "Bank-based blockchain prokects are going to transform the financial services industry," [Online]. Available: https://techcrunch.com/2018/01/28/bank-based-blockchain-projects-are-going-to-transform-the-financial-services- industry/?guccounter=1.
[27] A. S. Nair, "Impact of Derivative Trading on Volatility of the Underlying: Evidence from Indian Stock Market".
[28] S. N. P. N. Drimbetas Evangelos, "The effect of derivatives trading on volatility of the underlying asset: evidence from the
Greek stock market".
[29] S. Shi, "The Impact of Futures Trading on Intraday Spot Volatility and Liquidity: Evidence from Bitcoin Market".

このドキュメントは https://x-cash.org/downloads/XCASH_Whitepaper_1.0.pdf を

Google翻訳で機械翻訳し、レイアウトを整えたものです。

正確な数値、情報は原文を参照してください。

作業者：.log#4329 (ディスコードID)

寄付：

XCA1WmkpvTrXKigzf1ydFLGrsWNayp3uSWTQdGfLXYC7GFsxM66crPaDUUsbP2FinENd9XGJSFLsGbv57F9UZ7Rr3eg6JbPG44

BTC: 31ifY5XfxdwUXiQshoG6xWDp2SehfcLQT4

エアドロップリファラル：

https://x-cash.org?ref=XCA1WmkpvTrXKigzf1ydFLGrsWNayp3uSWTQdGfLXYC7GFsxM66crPaDUUsbP2FinENd9XGJSFLsGbv57F9UZ7Rr3eg6JbPG44