Wrapped Tokens

あらゆる資産をトークン化するための、複数機関フレームワーク

Whitepaper V0.1
Oct 5th 2018

Kyber Network
BitGo Inc
Republic Protocol

概要

ERC20トークンの普及に伴い、Ethereumエコシステム上のデジタルトークンが重要なアセットクラスとして登場しました。これらのトークンは、ブロックチェーンやEthereumが実現すべきである通貨数や所有者、鋳造数、速い承認時間、トランザクション詳細やスマートコントラクト執行などの透明性の面での利点を享受しています。Ethereumブロックチェーン上のこれらのトークンはいくつか多様な機能を提供します。この論文では、特にアセットバックトークン、もしくはラッピングしたトークンについて焦点を当てます。これらのトークンの価格は、それを裏付ける資産の価格を反映しているため、それらは「ステーブルコイン」と呼ばれます。アセットバック・トークンは通常、2つの異なる手法で実現されます。

- **Algorithmic** - これらはEthereum上のいくつかのトークンが採用しているメカニズムであり、トークン価格と法定通貨価格を合致させるため需要と供給がスマートコントラクトにより制御されている方法です。いくつかの事例としては、Dai, Basis, Carbon, Nubitsがあります。

- **Centralized** - 資産は、保管資産の存在を証明する組織によって保管されます。これはTether, True USD, USDC (USD), Digix (gold), Globcoin (法定通貨のミックス), AAA reserve (国債) のケースです。

Wrapped tokens はCentralizedモデルを採用します。しかし、全てを一つの機関に依存するのではなく、ネットワーク上の異なる役割を持つ複数機関のコンソーシアムを作ります。このホワイトペーパーでは、スケーラビリティ、トラスト、規制、ガバナンスなどの課題に対処できるアセットバック・トークンを発行するためのフレームワークを提案します。私たちがローンチする最初のwrapped token はBitcoin (BTC) に裏付けられたERC20トークンとなり、”Wrapped BTC” (WBTC) と名付けます。集権的ソリューション (USD) とは異なり、WBTC はBTCチェーン上に公表される準備金の証明により完全に説明されます。

WBTCを使うために、いかなる派生トークンも求められませんし、ブロックチェーン手数料以外の手数料はありません。WBTCはシンプルな連合ガバナンスモデルを使い、ユーザビリティの向上に努められています。

ユースケース

トークン化

アセットのトークン化により、以下が可能になります。

- トランザクションスピードの向上
  Ethereumブロックは約15秒ごとに作成され、公正な取引のトランザクションは取り消されないという信頼を5分たらずで得ることが可能です。このスピードはBitcoinや金、法定通貨を自然に取引するに比べると高速です。

- 仲介者の減少
  ブロックチェーン上の資産の大きなメリットの一つは、仲介者のいない取引が可能であることです。これらの取引はアトミックスワップや分散型取引所プロトコル、lightningやraiden形式のチャネルを通して完了します。

- セキュリティの向上
  トークン化により、ユーザーは資産の秘密鍵を完全にコントロールできます。鍵を保有したくないユーザーは、資産を取引所からセキュリティに特化したカストディアンに移すことでリスクを低減できます。

- ユーザビリティ
  このERC20標準は、多数の機関やプロジェクトにより採用されます。これにより、ユーザーは自身のトークン化資産を保有している間、多様な取引所、ウォレット、Dappsを活用することができます。さらに、トークンは素早く、24時間いつでも移動できます。

- 透明性の向上
  トークン総数、トークン作成トランザクション、トークン除去トランザクション、トークン保有者数、そして転送ルールはパブリックブロック・エクスプローラーで誰もが確認できます。このレベルの透明性は、通常は法定通貨やコモディティ、株式で見ることはできません。

分散型取引所やdappsにおける流動性

今日の分散型取引所で取引される大多数のERC20は、ETHではなくBTCにより行われています。ほとんどの分散型取引所は ETH/Token のみサポートしており、 BTC/Token のトレードはサポートされていません。Wrapped tokensはそのギャップを埋め、分散型取引所にさらなる流動性を提供できることになります。加えて、他の分散型アプリケーションやプロトコル(ファンド、融資、決済) はBTCトークンがもたらす多大な流動性へのアクセスを持つことになり、大きな利益を得ることができるでしょう。WBTCにより、スマートコントラクトの簡単な創造をBitcoinに持ち込みます。

法定通貨トークンのメリット

法定通貨に裏付けられたトークンにより、トレーダーは価格の乱高下の心配なく、資産を暗号通貨に反映させる安全な方法を取ることができます。これは、法定通貨を直接転送することのできない集権的取引所や分散的取引所にいるトレーダーにとって特に便利です。法定通貨に裏付けられたトークンは、暗号通貨が伝統的ファイナンスを置き換える世界を実現します。重要なことに、このトークンは買い手と売り手が交換レートや税金 (USでは、買い手は購入時点で計算されたキャピタルゲイン税を支払う必要があります。) を気にせずeコマースで使うことができます。

暗号通貨間の相互運用性

今日の暗号通貨数の拡大を見る限り、それぞれは通貨交換のいくつかの側面にフォーカスしています。例えばトランザクション処理能力、プライバシー、低手数料、スマートコントラクトの能力、ノードとマイナーの分散化などです。ラッピングのフレームワークは、Bitcoinなどの他の暗号通貨をEthereum上で容易に表現できるようにし、Ethereumブロックチェーンのすべての機能がそれを向上させます。ユースケースの一つは、イニシャル・コイン・オファリング (ICO) で、wrapped Bitcoin トークンをデポジットしてもらい直接トークンを鋳造、資金調達することです。将来的には集権的取引所や暗号通貨を受け入れるその他の機関は、複数の暗号通貨ノードを維持する必要なく、単にEthereum上で開発すればよいことになります。

オンチェーンによる施策執行

トークン化により、オンチェーンによる施策執行もできます。オンチェーンでの施策執行はルールをより透明にし、執行を一つの主体に頼る必要がなくなります。資産の種類によっては、資産移転や取引に関するルールの服従を強制する必要があります。例えば証券では、ホワイトリスト、保有期間やアイデンティティ管理が求められます。

共通の問題

スケーラビリティ

2018年1月、Ethereum上のガスリミットの最大値はブロック当たり800万ガスを越えています[1]。この制限はハードウェアとソフトウェア共通に当てはまります。多くのスケーラビリティソリューションが提案されていますが、多くは開発者の顕著な努力を要求し (state channels)、もしくは実用的なものに開発するには早すぎるものになっています (plasma, sharding) 。競争が起こる期間 (人気ICOやCryptoKitties) はガス価格が高騰するため、これはネットワーク内のDappsとユーザーが抱える問題です。今年7月初めには、中国の取引所のFcoinがトランザクション手数料の最高値を引き起こしました[2]。

トラスト

アセットバック・トークンは通常、資産を保有する機関へのトラストが求められます。これは運用においてトラストを最小限に抑えようとする暗号通貨の哲学に反します。いくつかの答えるべき重要な質問は以下にあります。

- 資産保有者は管理にあたり、既存の法的枠組みから認定されているのか？
- カストディアンは任意の量のトークンを作成可能か？
- カストディアンはどのようにして、管理下にある資産保有を証明するのか？

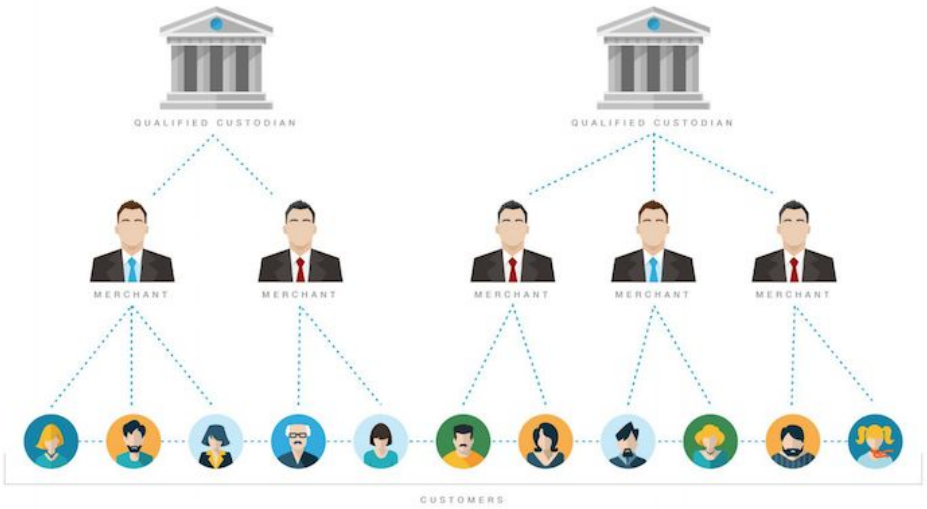
規制

アセットバックトークンの保管者は、資産を保持するためにライセンスを取得する必要があります。このライセンスは、資産保管場所やカストディアンの地理的管轄により変更する可能性があります。カストディアンは、1:1の裏付けが欠如すれば全システムを毀損してしまうため、定期的に保管資産の存在を証明しなければなりません。KYCとAMLの規制も、アセットバック・トークンに関わるユーザーに適用されます。これらの制約は購入、償還、トークン転送などの全てに課せられる必要があります。

ガバナンス

システムに複数のステークホルダーがいる際、トークンに加えられる変更にいかに対処するか、というガバナンス上の課題があります。ほとんどのアセットバック・トークンは、トークンを統治するルールやスマートコントラクトの変更をカストディアンに完全に依存しています。通常はICOの場合、トークン発行者はプロトコルの変更に完全なコントロールを握っています。ユーザーが投票権を持つ自律分散型イニシャル・コイン・オファリング (DAICOs) のようなケースもありますが、投票率の低さという課題に直面しています[3]。

実装とテクノロジー



主要な役割

- カストディアン - 資産を保管する機関。WBTCの場合BitGo[4]が役割を果たします。カストディアンはトークンを鋳造する鍵を保有します。

- マーチャント - 鋳造された wrapped tokens を受け取り、またはバーンする機関。マーチャントは wrapped token を配布する重要な役割を担います。WBTCの場合、最初はKyber[5]とRepublic Protocol[6]が担います。各マーチャントは新しい wrapped tokens の鋳造を開始するためと、 wrapped tokens のバーンのための鍵を保有します。

- ユーザー - wrapped tokenの保有者。ユーザーは wrapped tokens を他のEthereumエコシステム内のERC20トークンと同じように、転送したり取引することができます。

- WBTC DAO メンバー - コントラクトの変更やカストディアンとマーチャントの追加/削除は、マルチシグコントラクトで制御されます。マルチシグコントラクトの鍵の保有者は、WBTC DAO機関の一員となります。

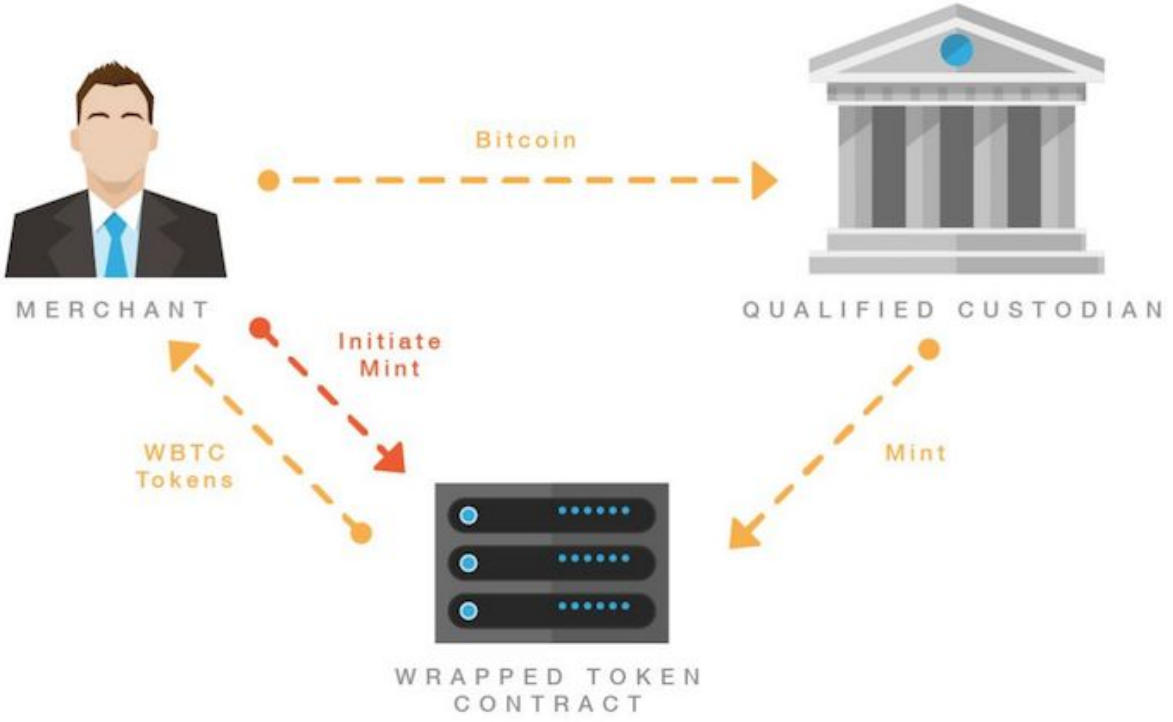
カストディアンは、保管資産と wrapped tokens をマーチャントと交換します。これは2つのタイプのトランザクションを通して行われます。鋳造 (wrapped tokensの創造) とバーン (wrapped tokens 供給量の減少) です。これらのトランザクションは一般公開され、誰でもブロックエクスプローラーを通して確認できます。最初の交換が終われば、マーチャントは wrapped tokens のバッファを維持し、それによりユーザーとの交換に応じます。鋳造とバーンはオフラインの鍵と署名が求められるため時間がかかりますが、この2ステップの鋳造プロセスは、ユーザーが wrapped tokens を得る時間を減少させます。

カストディアン・コールドウォレットセットアップ

カストディアンには全てのマーチャントのため、一つのコールドウォレットが求められます。コールドウォレットは、マルチシグネチャを使い、全ての鍵は常にオフラインでカストディアンに管理されています。コールドウォレットからは、ホワイトリスト上のマーチャントのアドレスにのみ、オンチェーンで送金できます。全ての鋳造とバーンのトランザクションは、カストディアンへの提出から48時間以内に完了する見込みです。複数のカストディアンが存在する場合、一つのコールドウォレットでは保留中の wrapped tokens の償還に応じる十分な資金がない可能性があることに注意してください。

鋳造

鋳造とは、新たな wrapped tokens を作成するプロセスを指します。ラッピングフレームワーク内での鋳造は、カストディアンにより完了されなければなりませんが、マーチャントにより “開始” される必要があります。ユーザーが鋳造に関与しないことは重要な点です。これはマーチャントとカストディアンの間で完了される一連のトランザクションです。



WBTC鋳造のシーケンス

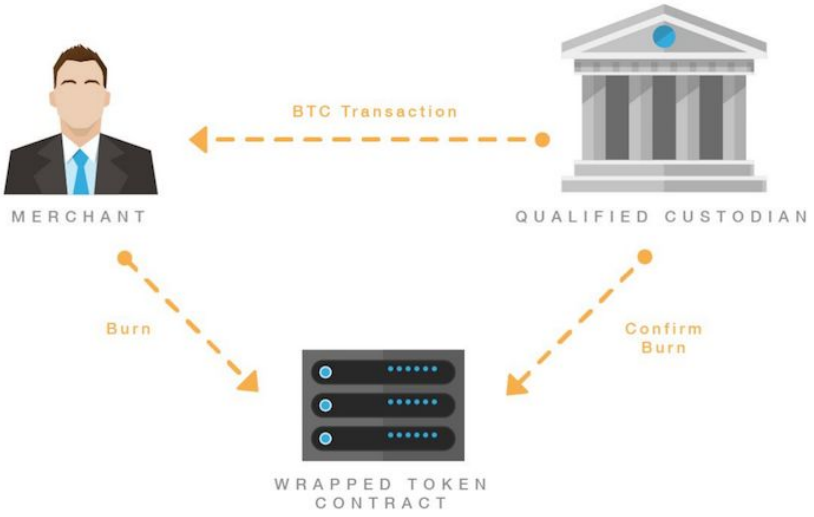
- マーチャントはカストディアンに、Ethereumチェーン上のマーチャントアドレスに X WBTC を鋳造する許可を与えるトランザクションを開始します。
- マーチャントはカストディアンに X BTC を送金します。
- カストディアンはBTCトランザクションの6承認を待ちます。
- カストディアンは新しい X WBTCトークンをEthereumチェーン上に創り出します。

ユーザーがWBTCトークンを受け取る際のシーケンス

- ユーザーはマーチャントへ、 wrapped tokens をリクエストします。
- マーチャントは求められるAML, KYCを手続きし、ユーザー識別情報を得ます。
- ユーザーとマーチャントはアトミックスワップを行うか、もしくはBitcoinを受け取るマーチャントとWBTCを受け取るユーザーの間でトラストある交換を行います。

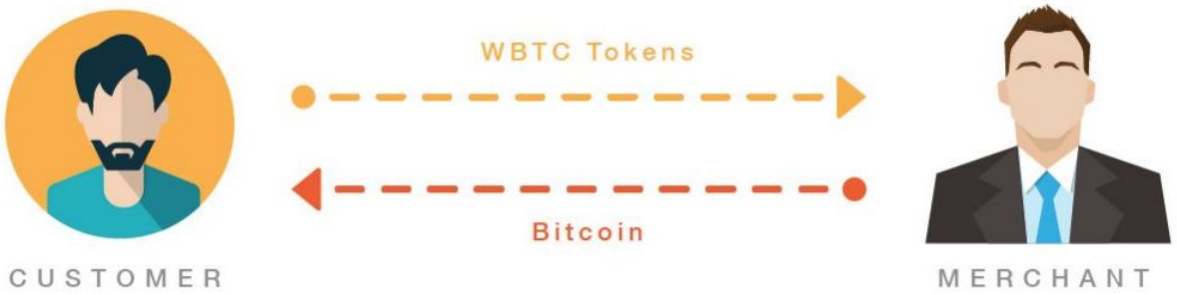
バーン

バーンとは、WBTCトークンをBTCに償還するアクションを指します。マーチャントのアドレスのみが、wrapped tokens をバーンできます。そのために、Ethereumチェーン上からその量のトークンをバーンするための、コントラクト内の “burn” ファンクションが呼び起こされます。それにより、マーチャントのWBTC残高 (オンチェーン) から差し引かれ、WBTCの供給は減少します。



WBTCトークンをバーンするの際のシーケンス

- マーチャントは X WBTC をバーンするバーントランザクションを作ります。
- カストディアンはETHトランザクションの25ブロック承認を待ちます。
- カストディアンはコールドストレージからX BTCをマーチャントのBitcoinアドレスに解放します。



ユーザーがBitcoinを受け取る際のシーケンス

- ユーザーはマーチャントからのトークン償還をリクエストします。
- マーチャントは求められるAML, KYCを手続きし、ユーザー識別情報を得ます。
- ユーザーとマーチャントはアトミックスワップを行うか、もしくはBitcoinを受け取るユーザーとWBTCを受け取るマーチャントの間でトラストある交換を行います。

オンチェーン転送の規制

トークンにより、トークン転送に関して制限がある可能性があります。WBTCの場合は転送に制限はありません。

ガバナンス

wrapped token コントラクトは、メンバー追加や排除の際にDAOメンバーからの署名が求められるマルチシグコントラクトにより統治されます。全てのカストディアンとマーチャントがDAOメンバーですが、しかしカストディアンやマーチャントでなくとも、他の機関もメンバーに参加できます。 “M of N” 署名がコントラクトに利用されます。ここではMがマルチシグの必要数で、Nはメンバーの総数です。MとNの値は、セキュリティに加え、容易なメンバー追加/削除も念頭に置きつつ、メンバー間相互で決定されます。

wrapped tokens のためのサイドチェーン

最初は、WBTCはEthereumメインネット上でローンチされます。メインネットチェーンは、取引所ネットワークやブロックエクスプローラー、ウォレットやその他Dappsが豊富にあるため、簡単にアクセスできて便利です。トークン化の主要な利益の一つは、トランザクションコストの低価格化です。しかしEthereumの人気やDapp開発スピードが上がれば、wrapped tokens のトランザクションコストはメインチェーンで行うには低価格とは言えないポイントまで届いてしまうでしょう。ラッピングフレームワークで複数の機関と協力することで、現実的なスケーラブルソリューションのデプロイを可能にし、トランザクション処理能力を高めることができます。

これは、DAOメンバー間で実行される既存のソフトウェア (parity-bridge) である、ペッグされたサイドチェーンを使うことで可能になります。このチェーンは、Aura コンセンサスアルゴリズム[8]を使う自身の proof of authority ネットワーク[7]で動きます。ブロックは4秒ごとに予測可能かつ効率的に作成されます。現在、すでにこのようなチェーン (Kovanテストネット) があり2017年3月から稼働しています。wrapped tokens は、双方向のマルチシグウォレットをメインネットとサイドチェーン上で作ることにより、メインとサイド間でペッグされます。サイドチェーンはEthereumに求められるスケーラビリティにより多く応えます。wrapped tokens をサイドチェーン上で取引、転送するメリットはいくつかあります。

- 最小限の開発コストでスケールできる (同じEVMで)
- 専用にすることで高まる処理能力 - 異なるブロックチェーンには異なるハードウェア、そして潜在的な proof of authority (PoA) の利点 (より速いブロック生成)
- 既存のクライアントやウォレットの簡単なサポート
- チェーンは他の “うるさい隣人” から自由に活動できる
- 最小限のトランザクションコスト (スパムを避けるための)

バリデーター (ブロック生成者) は wrapped パートナーと、地理的に分散されたいくつかの本籍/政府を代表する信頼ある主体により選ばれます。バリデーターはメインとサイドチェーン間の双方向ペッグを維持します。両方のチェーンで wrapped token の価値をペッグするため、私たちはメインネットとサイドチェーンで使われるマルチシグニチャコントラクトを提案します。

- EthereumメインネットからEthereumサイドチェーンに送信する:
    - メインネットアドレスからメインネット・マルチシグアドレスへ送信
        - マルチシグアドレス上で “sendToSidechain” メソッドをコールし、サイドチェーン上の宛先アドレスを引数として指定してその量を送ることを推奨する。
        - メソッドなしに送信した場合、サイドチェーン上の宛先アドレスは送信元アドレスと同じであると想定される。
    - イベントはメインネット上に作られ、送信を記録する
    - 署名者はメインネット上のトークンを “ロック” する
    - “承認期間”のあと、サイドチェーン上のマルチシグの権利者はメインネットの送信イベントを検証でき、低い手数料でサイドチェーン上の宛先アドレスへ出金可能。
- ETHサイドチェーンからETHメインネットへ送信する:
    - 同一 (対称)

WBTCはサイドチェーンの初めての資産となり、共に働くこれらの構成のコンビネーションを活用し、エコシステムを作り出すことになります:

- ノードソフトウェアと設定
- ブロックエクスプローラー
- ウォレットプロバイダー
- ブロックバリデーター
- マルチシグ権利者

インセンティブ

トランザクションには、ブロックバリデーターへの支払い、そしてサイドチェーンをスパムを防ぐ目的で1Gweiの最小限のガス価格が課せられます。バリデーターは、Dappごとにオフチェーンでインセンティブを受けたり、もしくはブロック報酬を得ることができます。サイドチェーン上のEtherのディストリビューション/マネジメントの詳細はまだ決定していません。

アトミック・スワップ

アトミック・スワップは、WBTCとBTCを交換するためにマーチャントとユーザー間で活用されます。もしユーザーがWBTCやBTCをより速く受け取りたい場合、マーチャントを通してトラストある交換もできます。

KYCが完了すれば、BTCをWBTCへアトミックな交換をするためにユーザーがマーチャントと行うステップは以下になります:

- ユーザーは、シークレットとそのハッシュを生成し、オフチェーンでマーチャントへ渡します。ユーザーとマーチャントは受信アドレス (ETHとBTC) などの詳細に合意します。

- ユーザーはマーチャントのBitcoinアドレス、ユーザーのアドレス、シークレットのハッシュ、有効期限を設定し、Bitcoin HTLC (Hashed Time Lock Contract) を作ります。これは、ユーザーが X BTCを得るP2SHアドレスを作るために利用されます。

- 6承認の後、マーチャントはユーザーのEthereumアドレス、マーチャントのアドレス、シークレットのハッシュ、有効期限を設定し、Ethereum上にHTLCコントラクトを作ります。そして、マーチャントは X WBTC をアトミック・スワップコントラクトに転送します。

- ユーザーは X WBTC をアトミックスワップ・コントラクトからユーザーのEthereumアドレスに動かすために、シークレットを明かします。

- マーチャントはBitcoinをP2SHアドレスから動かすためにシークレットを使用します。

- ユーザーが有効期限内にWBTCを動かさなかった場合、トランザクションは実行されず、ユーザーはBTCの返却を要求できます。

いくつかの重要な点を以下に並べます:

- アトミックスワップ・コントラクトをデプロイしてWBTCを送るためには、トランザクション手数料がかかります。従って、ユーザーはスワップを始める前にアトミックスワップ手数料を支払う必要があります。

- アトミックスワップは時間がかかり、BTCとETHチェーンの双方で複数トランザクションが必要です。ユーザーは、BTCがマーチャントアドレスに送信され、Bitcoinネットワーク6承認後にマーチャントがユーザーにWBTCを送る、というトラストを使った交換をするオプションを選択できます。これはマーチャントへのトラストを含みますが、素早く安価です。

WBTC VS アトミックスワップ

アトミックスワップは、ユーザーが BTC - ETH トレードのみを求めるのであれば、WBTCなしで実現できます。これらはKomodoプラットフォーム[9]のメカニズムによって説明されている分散型取引所で行うことができます。しかしWBTCは、DAPPsと他のエコシステムの相互作用ために不可欠なETHチェーン上のBTCを現すことに注意が必要です。アトミックスワップとWBTCを比較する際に考えるべき、いくつかのトレードオフを以下に列挙します:

- アトミックスワップをする場合、誰もが価格発見を経なければなりません。wrapped tokens の価格発見は、既にあるWBTCを得た後に、分散型取引所でトレードされる間に起これば十分です。

- アトミックスワップの技術は既存のウォレットや分散型取引所でサポートされる必要があります。wrapped BTC はERC20トークンに対応しているあらゆるウォレットで活用可能です。

- 全てのトランザクションがETHチェーン、次にBitcoinチェーンと複数の承認が必要であり、非常に遅くなってしまいます。 (反対にWBTCは、最初の鋳造/トークン化に時間が必要ですが、それ以降はETHチェーンで簡単にトレードできます。)

- 分散型取引所でアトミックスワップを行うことは、個別にデポジットとアトミックスワップ手数料がかかります。これはユーザーが通貨を交換するたびに不便となります。

手数料

WBTCをユーザー間で転送する際は、ネットワーク手数料以外にコストはありません。ネットワーク内のそれぞれの主体が手数料を得るには、3つの方法があります:

- カストディアン手数料: マーチャントがwrapped tokens を鋳造もしくはバーンした際にカストディアンが得る手数料
- マーチャント手数料: ユーザーが資産を wrapped tokens と交換したマーチャントが得る手数料

- サイドチェーントランザクション手数料: この料金は、主にサイドチェーンのスパムを防ぐことを目的としています。 これは、サイドチェーン上のノードを実行しているすべての機関で等しくシェアされます。

法的拘束力

カストディアンとマーチャント間の契約

ユーザーはトークンの鋳造とバーンのプロセスに関与せず、信頼ある機関の間でのみ行われます。マーチャントはユーザーの識別情報をセキュアに保有することが求められます。カストディアンは四半期ごとに資産状況の詳細を公表せねばならず、タイムリーに鋳造とバーンを行わなければなりません。この基準に達していない場合、ネットワークから排除される要因となります。

ネットワーク内には複数のカストディアンが共存可能である点に注意してください。しかしそれは、ネットワークに関与することによるリスクが高まることが理由です。異なる機関でマルチシグウォレットを保有するカストディアン方式も、将来的には可能です。運用上では、鋳造/バーン/監査には多くの調整と時間が必要になるでしょう。カストディアン間のセキュリティ違反は信頼の喪失を招き、大量の出金を引き起こすでしょう。マーチャントのセキュリティ違反の場合、全ての未払いトークンはカストディアンによりバックアップされているため深刻さは和らぎますが、ユーザーの KYC/AML データの喪失が考えられます。

トラストモデル

資産が盗難されたり、1対1の裏付けに不誠実な行動を起こす可能性もあるので、wrappedフレームワーク内のカストディアンを信頼することが必要です。しかし、wrappedフレームワークではいくつかの方法により、トラストを最小限に抑えることを意図しています。

- 四半期ごとの監査は外部の第三者により実施され、全ての鋳造されたwrapped tokensに対し、全カストディアンが保管する資産が同等量保たれているかを確認します。WBTCの場合、準備金の証明はbitcoinが保管されているアドレスの署名を公開することで示されます。

- カストディアンは自身のみでトークンを鋳造することはできませんが、鋳造のためにマーチャントに開始を要請することができます。従って、新たなトークンの作成はカストディアンとマーチャント双方の関連が必要です。

- ユーザーはカストディアンとの通信から隔絶されており、一連のマーチャントを通す他ありません。個人のマーチャントは信頼される必要はありませんが、全てのマーチャント全体としては信頼される必要があります。

- 関わる機関の既存の信頼性は、このフレームワークに関連する全ての機関にとって重要です。

透明性

wrapped token の機能には、完全な透明性があります。以下にあるように、ネットワークの全詳細はダッシュボードに反映されています。

- ネットワーク内で異なる役割を果たす機関の名前と詳細

- 鋳造とバーン注文の状態 (保留、進行中、キャンセル、完了)

- カストディアンに保管される総BTC量

- ネットワーク内のWBTCの量 (同等か、保管されるBTCよりわずかに少ない)

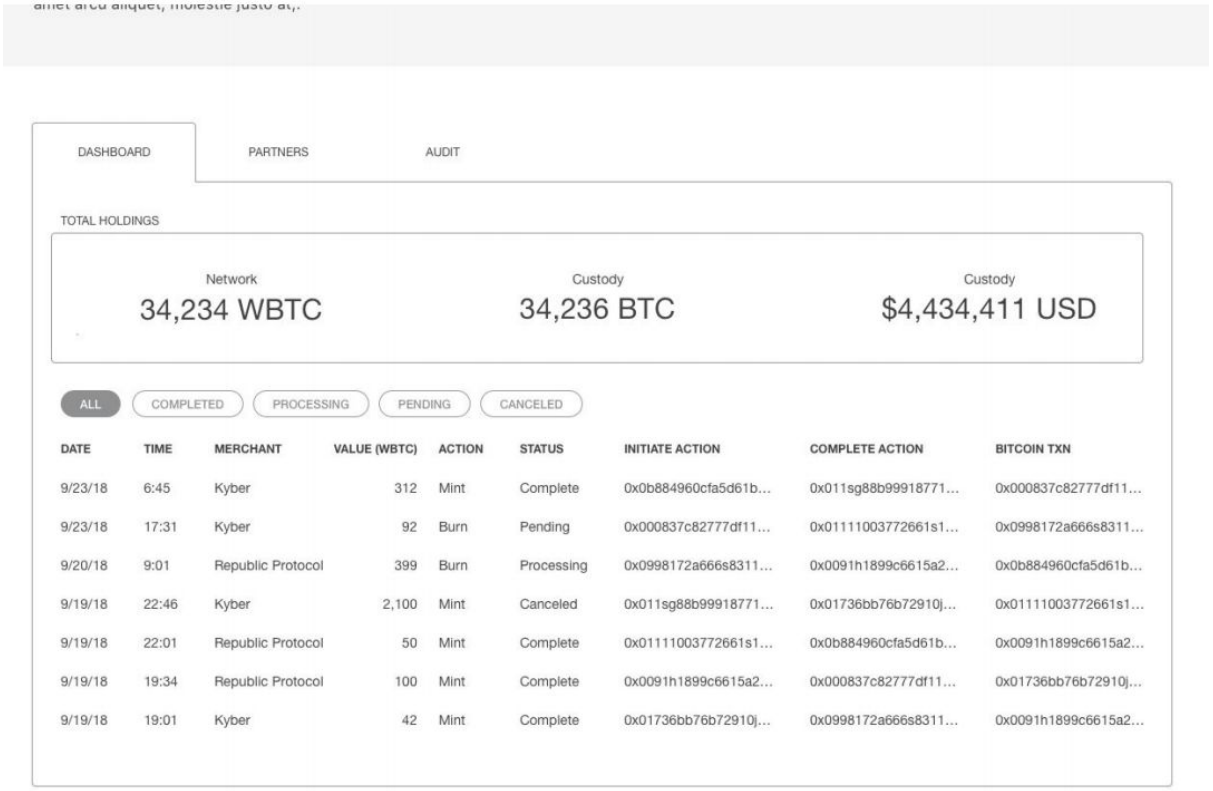
- カストディアンがBitcoinの鍵を持っていることを証明する、トランザクションの形での四半期ごと監査

- マーチャントとカストディアンのEthereumアドレス

- カストディアンがコントロールする、各マーチャントと関連するBitcoinアドレス

- ブロックエクスプローラー上のオープンソースのトークンコントラクトコードや、デプロイされたコントラクトへのリンク

ダッシュボードがどのようなものになるか、サンプルがあります。



結論

wrapped tokens を通して、資産をイーサリアム上でもっと交換可能で表現しやすくできるソリューションを提案します。国際的な流動性、フラクショナルオーナーシップ、スマートコントラクトのプログラマビリティやトランザクション手数料の減少は、トークン化の主要な利益です。WBTCはそれらの最初のトークンとなり、DappsがBitcoinにアクセスすることを簡単にします。全てのトランザクションやコントラクトと監査は公表されており透明性が確保され、ネットワーク全体の信頼を実現します。フレームワークはまた、アセットバック・トークンが過去に直面してきた共通の課題のために、暗号通貨業界の複数の機関が多様な役割で対応する道を与えます。

用語集

カストディアン - 資産を保管する機関または主体。WBTCの場合、BitGoが役割を持つ。カストディアンは、トークン鋳造のための鍵を保有する。

マーチャント - 鋳造された wrapped tokens を受け取り、バーンする機関または主体。マーチャントは wrapped tokens 分配の重要な役割を果たす。WBTCの場合、最初は Kyber と Reppublic Protocol が役割を持つ。各マーチャントは、新たなトークンの鋳造を許可するため、そしてバーンするための鍵を保有する。

ユーザー - wrapped token の保有者。ユーザーはイーサリアムエコシステム内の他のERC20トークンと同じく、 wrapped tokens を転送したり取引できる。

KYC (Know your customer) - FINCEN と OFAC Required Guidelines は、機関の顧客がOFACの制裁下にないこと、銀行秘密法の規則違反を行っていないこと、マネーロンダリングに関与する関与することがないことを確認することを求めている。

AML (Anti money laundering) - 洗浄された違法資金を標的とする規制当局 (アメリカ財務省を含む) により強制される、規則と規制。

WBTC (Wrapped Bitcoin) - Ethereum上の、Bitcoinと1:1の裏付けがあるERC20 トークン

参考

[1] - https://etherscan.io/chart/gaslimit
[2] - https://www.coindesk.com/ethereums-growing-gas-crisis-and-whats-being-done-to-stop-it/
[3] - https://cointelegraph.com/explained/what-is-a-daico-explained
[4] - https://www.bitgo.com
[5] - https://https://kyber.network
[6] - https://republicprotocol.com
[7] - https://paritytech.github.io/wiki/Proof-of-Authority-Chains
[8] - https://wiki.parity.io/Aura
[9] - https://komodoplatform.com/atomic-swaps/