OmiseGO
分散型取引所と支払のプラットフォーム

ジョセフ・プーン
joseph@lightning.network

OmiseGO チーム
omg@omise.co

2017 年 6 月 17 日

摘要

OmiseGO は分散型取引所、流動性提供者メカニズム、クリアリングハウスメッセージングネットワーク、そして資産を担保にしたブロックチェーンゲートウェイを構築している。OmiseGO は単一の当事者によって所有されていない。むしろ、参加者の振舞いを規制する認証者達のオープンな分散型ネットワークである。OmiseGO は参加者の市場での活動の規制を可能にするためのプルーフ・オブ・ステークブロックチェーンを作るため、プロトコルトークンの仕組みを用いる。この高パフォーマンス分散型ネットワークは法定通貨を担保にした発行者から完全に分散されたブロックチェーントークン（ERC-20 スタイルでネイティブな暗号通貨）まで資産クラス間での交換を規制する。他のほとんどの分散型取引所と違い、信頼されたゲートウェイトークンなしに他のブロックチェーンと複数のブロックチェーン間での分散型の交換を可能にするものである。市場は保管の分散と一層の市場活動の透明性を通じて、大きくスプレッドを低減し、市場の保障を促すことが出来るかも知れない。これは、スマートコントラクト、正しい注文書マッチングの市場での振る舞いを施行するプロトコルトークン、イーサリアムと結合したクリアリングハウス活動の外部による規制の新たな構築、そしてイーサリアムスマートコントラクトによる利用のための歴史的取引所データへのコミットメントを利用して達成される。

1 導入と問題定義

ブロックチェーンの主要な役割は、参加者のネットワーク間での複数間の合意連携の問題を解決することである。透明性、安心、そして施行を確保することにより、私達はこれまで不可能だった場面での複数間の合意を可能にできる。すべての当事者が運営が透明であるだけでなくメカニズムが多大な取り組みなしに変更されないことが保証されていることに安心する時、当事者達は連携により前向きである。参加者は将来において、単一の当事者が他の当事者にビジネスプロセスの変更や情報の非対称を通じて「高利の家賃徴収」を強制することが困難であることをより高度に保証される。別の言葉で言えば、どの単一の参加者もビジネスプロセスやメカニズム自体が他の単一の参加者によって所有されていないシステムの利用に前向きである。

決済処理業者、ゲートウェイ、そして金融機関の間で根本的な連携の問題がある。例えば、銀行の顧客が別のネットワークのマーチャントに支払いをしたいとする。従来、複数の決済ネットワークや金融機関を横断して互換な決済システム周りのエンジニアリングに多大な取組みが投入されていた。それらは通常、中央のカウンターパーティークリアリングハウスとのメッセージング

ネットワークやノストロ/ボストロ口座を通じたやり取りを管理するクリアリングハウスの設置によって構築された。FedWire, CHIPS, SWIFT, 各消費者カード決済ネットワーク、NSCC/DTCC, OCC, and ACH などを例として挙げることができる。これらのネットワークは現地/国内決済、国際決済、信用取引、株式/資産交換、デリバティブを含む異なる役割と機能を果たす。これらの集権型ネットワークはコントロールする主体がメカニズムを恣意的に変更することを可能にし、それは情報コスト、デュー・デリジェンス、すべての当事者間での契約の施行
など、相当の金額のトランザクションコストがかかる結果となる。

私達は、現在デジタル決済において、新たな決済プラットフォーム（Venmo、 Alipay）によるディスラプションの新興市場が存在すると確信している。これらのネットワークはネットワークを横断したやり取りを好まず、なぜならやり取りの施設への信頼にかなりの間接費がかかるからである。各当事者は中央の各カウンターパーティーを利用することを望まず、なぜかと言えばどちらの当事者も他方に従うことを望まず、ノストロ/ボストロ口座の利用には特別に作成された参加者間の契約を要するからである。大きなネットワークが彼らの持つネットワーク効果を保護するインセンティブを持つ一方、私達は e ウォレットのサービスの提供を望む主体のロングテールの存在を確信しており、それには複数の参加者間のより高度な連携を要する。これらの中規模の参加者はユーザビリティにおいて十分なネットワーク効果に達するため複数のネットワークを横断して価値を横断させることが出来るようになる。 これらの提供元向けのインフラと参照フロントエンドはこのネットワークにネットワーク効果をエンコードすることを可能にし、台頭しつつある e ウォレットの参加者が即座に高いネットワークユーティリティを作成することが可能になる。

ブロックチェーンは世界のビジネスプロセスを、単一で集権型の企業からオープンで分散型のコンピューティングネットワークへ外部化することを可能にする[1][2]。OmiseGO (OMG)は、これらの台頭する e ウォレット決済ネットワークを横断して決済を解決する助けになるため、市場の流動性、注文書マッチングと実行、クリアリングハウスによる保管、そして高スケーラビリティ決済を分散化するネットワークである。

従来単一の企業に置かれてきたビジネスプロセスを移すことにより、分散型高パフォーマンスオープンネットワークで e ウォレットの提供元にやり取りのプロセス全体を提供する事が可能である。

2 デザインアプローチ

最終状態の要件は、法定通貨の裏付けを持つ価値（ならびにネイティブでオプトインの暗号通貨のサポート）を保持する e ウォレットプラットフォーム向けの分散型メカニズムの構築である。e ウォレット法定通貨トークンは最大の効率のため、分散型の公開イーサリアム[3][4]チェーン（または他のあらゆる分散型暗号通貨）でやり取りの手段又は媒介としてイーサを用いる能力を持つ。私達はこれが、多くの e ウォレットプラットフォームにとって有用な役割を果すであろうことからより多くの分散型暗号通貨での活動と価値をもたらすことを確信している。

e ウォレットのやり取りを行うのはこの分散型ネットワークにとって中核の機能であるため、OmiseGO 上のブロックチェーン台帳は e ウォレットサービス（またはあらゆるユーザー/ノード）ごとに資金の残高を保持する必要がある。この台帳は多くのアセット/商品を横断して資金を保持出来なければならない。ただし、台帳を保持するだけでは、やり取りにおいて不十分である。メカニズムがこれらのアセット/商品をトレードすることが可能であることが必要である。

やり取りを実施するためには、注文はオープンな公設市場上で多くの異なるペアを横断して置かれることが必要である。これには、分散型の注文書とトレーディングエンジンが必要である。トレーディングエンジンは OMG ブロックチェーンにビルトインされ、注文は発行され、マッチはそれぞれのブロックの一部として、マッチした注文が一定の認証の確認数に達した時実行される。その結果は、e ウォレットプラットフォームが単一の主体への集中的な信頼なしに他の e ウォレットプラットフォームと交換できる、単一の当事者による非保管型の管理分散型取引所である。

ただし、数が多すぎるかも知れないので、e ウォレット法定通貨トークン間の直接の横断は望ましくないかも知れない。流動性のある市場向けに単一の選好なしに暗号通貨を用いることが必要になる。イーサリアムをスマートコントラクトへ結合する [5]（またはビットコインのようなトークンを結合されたクリアリングハウスへ）ことにより、イーサや他の暗号通貨よりも e ウォレットペアの発生を可能にし、流動性のある市場を作り出す（もし全てのペアが ETH と横断した場合、通貨のボラティリティが低ければスプレッドはもっと小さくなる）ためイーサを OMG チェーン上のアクティビティにロックアップすることが可能になる。とても小さいスプレッドを要する活動に関しては、一部の e ウォレットトークンがやり取りの横断のために利用されるようになるかもしれない。ただし、プログラム的裁定に関連する連携や信用の利点のため、決済において分散型トークンを使用する強いインセンティブがある。e ウォレット法定通貨トークンは必要に応じ、他の e ウォレットトークンを用いて横断する場合もあるが、スマートコントラクトの活動の短期の交換レートの変動に影響しない結合は主に ETH で行われる（例えば HTLC クリアリングハウス、流動性提供、そして OMG チェーン施行）。各暗号通貨を e ウォレットプラットフォームの裏付けとするのを可能にすることにより、プラットフォームがそれぞれの e ウォレットのやり取りの活動間で公平な場所であることが確保される。

これはロックアップされた資金のより大きい程度の流動性を要し、OmiseGO の分散型取引所は低額のやり取りのアクティビティのトランザクションに望ましくないかも知れない（例えば大量のマイクロ決済）。

２つの e ウォレット間の全ての決済が分散型取引所でのトレードを用いて行われなければならないとは限らない。e ウォレットがいくらかの準備金を他の e ウォレットの法定通貨トークンで持ち、ポピュラーな方向での金額の少ない送金で使用されるという期待がある。ライトニングネットワーク[6]などのような構築物は e ウォレットが高速の決済を推進するため残高を保持するとき決済がオフチェーンで起こるのを可能にする。実装は決済がビットコイン[7] とイーサリアム[8] を横断して発生することを可能にしており、e ウォレットの残高について OMG チェーンに容易にポートされることができる。

OmiseGO ブロックチェーンの構築の結果は、分散型取引所、暗号通貨（例えば ETH）マッチング、注文書、そして完全な保管(full-custody)の信頼なしのクリアリングハウスのサポートを持つ e ウォレットのやり取りを可能にすることである。

2.1 チャンネル向け分散型流動性ハブ

この構築物には、ビットコイン（やある程度までイーサリアム）等のさまざまな暗号通貨における決済チャネルに利用される分散型流動性プールの設置を可能にするという追加の利点がある。

各ブロックチェーン上の個別のトークン決済について、ノード認証/マイニング計算のプレッシャーを削減するためベースのチェーンに影響しないよう、ベースとなるブロックチェーン活動をスケールする必要がある。よって、ライトニングネットワークの活動(またはチャネルを使った似たような構築物)を行うことが必要である。しかし、ライトニングネットワークはネットワーク効果周りで大きなプレッシャーに直面するので、各流動性プールが単一の信用される主体に集中することを防止するのが望ましい。分散型クリアリングハウスと同じメカニズムを利用することにより、私達はより複雑なスマートコントラクトをサポートするトークン（例えばイーサリアム、ERC-20 のようなトークンなど）について単一の個人によって所有されないライトニングネットワークハブを作り出すことができる。単純なスマートコントラクトを持つ通貨については、ネットワーク上のすべてのノード（例えばビットコインネットワーク）が OMG チェーンへのゲートウェイとして振舞い、他の全ての参加者と再び横断することができる。これにより OmiseGO チェーンが、分散化を推奨する一方で多くのオンチェーン活動をオフロードすることが可能になる。

私達は、流動性の集中化における自然なネットワーク効果は、決定性/既知のコンセンサスルールを持つ分散型ステークチェーンによって低減されることが出来ると確信している。

特にイーサリアム（そして他の完全な機能を持つスマートコントラクトがスクリプトされる各ブロックチェーン）において、全ての参加者は単一の各資金のプールとして運営される ETH スマートコントラクトへのチャネルを設定する。OMG チェーンの状態は参加者の現在の残高を反映する。これはあらゆる参加者によるこのネットワークへの流動性の提供、その OMG チェーンのコンセンサスルールに基づく配分を可能にする（時間をかけたテスト/認証の前にこの構築が成功した場合、このブロックチェーンが暗号通貨空間から予備の流動性を吸い上げるのを防止するため初期において制限される場合がある）。これらの資金はよって、OMG チェーン上のあらゆる流動性活動に利用することができる。

3.ブロックチェーンの概要とメカニズム

上のメカニズムは（特に状態について）かなり多くの活動を要し、現時点において全ての活動がイーサリアムのメインチェーンで起こるのは適切でなく、ただし行われる構築は公開イーサリアムチェーンでのトレード活動を OMG チェーンによって提供されるコントラクトの実行のインプットと結合することであろう。

私達は主にイーサに裏付けられたトークン/資産クラスを横断したトレードを可能にするため、他の各ブロックチェーンにフックするブロックチェーンを構築している。個別のチェーンの視点からは、私達はコントラクトの状態が OMG チェーン自体の活動によって結合されたスケーラビルなブロックチェーンを構築している。他の各チェーンでの活動は BTC Relay[9]と似た（ただし異なる構築の仕方）インターチェーンのコミットされた証明を通じて OMG チェーン上で、イーサリアムに提示することによりこのチェーンと連結することができる。OMG チェーンは（他のチェーンでの活動を含む）全ての参加者の行動による活動を認証する。別の言い方をすると、OMG トークンの役割は計算と施行の提供である。トークン自体がこのブロックチェーン上での活動の証書として振舞い、不適切な活動はトークン/証書が OMG チェーン上でバーンされる結果となる。深く施行を行うカスタムチェーンを作成することにより、私達はコンセンサスルールが高パフォーマンス活動に最適化されたシステムを構築することができる。

デザインはやや遅めの決済で高速実行とクリアリングへ最適化する。将来のバージョンは OMG チェーンの分割(sharding)を含むかも知れないが、最初のバージョンはブロックの伝播における高スループット能力を仮定する。

OMG トークンを所有していることで、このブロックチェーンをコンセンサスルール内において認証する権利を買うことができる。決済、やり取り、トレード、そしてクリアリングハウスの利用を含む（がそれに限定されない）ネットワーク上のトランザクションフィーは、結合したコントラクトの状態を施行する落ち度のない認証者に与えられる。

トークンはユーザーへ認証を提供する責務/コストとともに、このネットワークからのフィーから派生した価値を持つ。このトークンは、低コストな攻撃を防ぐため価値を持っていなければならず、それはこのネットワークでの施行に必要である。

一定分を再移譲の前に毎回削減する事が必要な、認証のサードパーティへの委譲を可能にすることは私達のロードマップにあるかも知れない（正確なメカニズムはセキュリティのモデリングについてまだ指定されていない）。

これは高パフォーマンスシステムとして設計されるので、証明を通じてリンクされた（linked-via-proof）ブロックチェーンの構築が必須である。私達はこのシステムが大量のトランザクションを扱うことができることを期待し、よって最終的配信はイーサリアム上のみで行う。クリアリングと決済は OmiseGO ブロックチェーン上で発生する。コンセンサスルールはこのプルーフ・オブ・ステークネットワークで施行される。このネットワークのコンセンサスルールの一部として、全ての OMG (Omise GO)の認証者がイーサリアムネットワークも稼働し、並行して認証することが要求され、結果イーサリアムはブロックチェーン間の認証において「第一級市民」となる。

BLS 署名（あるいは Schnorr）が計画するイーサリアム/ERC-20 結合と引出のような機能が近い将来イーサリアム上で有効になることが仮定される。各暗号通貨にとって、これらのトークンは保管されているわけでなく、（信用されるゲートウェイをベーすとして必要とするリップルなどの取引所プラットフォームと違い）スマートコントラクトにロックされている。また、指名された集中型認証セット（例：リップル）に依存しない。

OMG ブロックチェーンはイーサリアムチェーン上での注文の実行のマッチングと管理を行う。OMG 上の活動が、認証者活動もまたネイティブイーサリアムスマートコントラクトを通じてイーサリアムチェーン上で施行されることを確保する。ビットコインやビットコインに似たシステムについては、私達はライトニングネットワーク上のクリアリングハウスネットワークを通じたトレードを認める。このブロックチェーンはコミットされた証明を通じてこのネットワーク上の活動を施行する。イーサリアムのネットワークほど堅牢でない一方で、ほぼ即座の OMG チェーンで編成された活動のフルノード認証なしのクリアリングと決済が可能である。将来においてブロックチェーンの再組織を認めないノードについて部分的認証を行うことを予定している。再組織をサポートするブロックチェーンのネイティブ SPV 認証はセキュリティの理由からこのネットワークでは許可されていない。

コンセンサスメカニズムとセキュリティプロパティの詳細な記述は Exonumia Labs, Inc のジョセフ・プーンによって、（現在執筆中の）近日公開予定の論文で提供される（2017 年夏を予定）。この論文内の説明（とその結果 OmiseGO によって用いられる実装）はおそらく多くのオープン

ソーストークンプロトコルブロックチェーンプロジェクトにとって役に立ち、分散型データ処理のためのインセンティブの創出やブロックチェーン間の金融活動など、台頭しつつある各チェーンのために新たな構造を提供するかも知れない。私達は OmiseGO とその分散型取引所がプロトコルトークンの生態系全体をを刺激し立ち上げることができるベースレイヤー技術/インフラストラクチャの提供への途において重要な中核となることを望んでいる。OmiseGO の最初のバージョンは Tendermint コンセンサスのいくつかの側面を利用するかも知れない。

3.1 ライトクライアントによる検証

OmiseGO が多数のトランザクションを扱う能力を持つ高パフォーマンスネットワークとして構築される一方、部分的認証並びに外部スマートコントラクトの施行のためライトクライアントの証明を生み出すことが必要になる。

ブロック毎のコミットされたトランザクションのマークル木並びに最近のブロックの状態へのコミットメントが含まれる。どのノードによっても、最近のブロックの状態のコミットメントとその時からの全てのブロックのダウンロードによって現在の状態が取得されることができる。

最近のブロックの状態は最近の状態のツリーを含むので、クライアントはチェーン全部をダウンロードすることなく最近のコミットメントののビューを得ることが出来る。再組織と停止攻撃に対して十分な経済的インセンティブがあるためそれが可能であることに注意のこと。OMG チェーンは結合した証明を通じたブロックの再組織にインセンティブを与えないよう設計されているが、ブロック確認の必要性周りの保証を提供しない。現行の SPV ビットコイン認証の実装と似て、検閲のリスクに関してフルノードに一定の信用が与えられている。私達はトランザクションの出来高をかんがみ、コミットされたブルームマップが分散型取引所にとって可能となることを期待しない。ライトクライアントは十分な数の認証者がトランザクション並びにフルノードから取得されたあらゆる部分的データを処理した事を認証できる。OMG チェーンのスマートコントラクトの構造のため、クライアントがイーサリアムチェーン上でも活動を認証することが強く推奨される。

4 e ウォレット

OmiseGO は決済をサポートする一方、特定の e ウォレット決済提供者(EPP)内の決済処理の仕組みとして設計されていない。単一の EPP 内での連携の問題は存在せず、連携の問題は主に EPP 間に存在すると私達は考えている。ただし、EPP 間のトランザクションの必要のため、決済活動はブロックチェーン上で行われることができる。このブロックチェーンは EPP が OmiseGO 上でのトークン発行を提供することを可能にする。これはプラットフォーム上で、または（ロイヤリティポイントなど）あらゆる資産クラスについて法定通貨に裏打ちされた法定通貨建ての通貨を可能にする。OmiseGO は誰でもアセットを発行できるオープンなシステムであるが、正しい発行/監査を保障するのは個々のユーザー（またはユーザーを代表して振舞う EPP）に任されている。これは、発行を可能にするスクリプト（と秘密鍵）に帰属する発行の作成によって達成される。別のアプローチとして、イーサリアム上で ERC-20 トークンを発行しスマートコントラクトでロックアップして OmiseGO チェーンで扱うことができる。これは現行の ERC-20 トークンを OmiseGO チェーンで扱うために行われるのと似たアプローチである（REP、 GNT 等）。

デフォルトの設定では、利用のし易さの目的で EPP がユーザーの代わりに資金を直接保持していると仮定されている。これは Coinbase や今日の多くの集中型取引所のような完全保管の暗号通

貨ウォレットと似ている。これはブロックチェーン活動にならないので、EPP が自身のネットワーク内で手数料無料のトランザクション構成すること可能にする。しかし、EPP から直接引き出し彼らが発酵したトークン（例：法定通貨）を OmiseGO チェーン上で取引するのも可能かもしれない（しかし送金は、EPP の保管アカウント内でオンチェーンで移転しない場合、オンチェーンフィーの結果となるかもしれない）。これは分散型の送金や、一部の EPP のニーズ（自身のネットワーク内でのゼロフィートランザクション）を満たすことを可能にする。EPP は多くのホスティングされた暗号通貨ウォレットと似た集中型のソフトウェアを提供する場合があり、これはデプロイの時間を大きく削減し、ネットワーク間を横断する決済のみが EPP のインフラストラクチャでホスティングされる。サードパーティも将来において、EPP 残高をオンチェーンで保持できる分散型ウォレットを開発することができる。

e ウォレットプラットフォームをブロックチェーンの一部として構築することにより、直接法定通貨に裏打ちされたトークンを OMG ブロックチェーン上で分散型通貨やプロトコルトークンと交換することが可能である。

4.1e ウォレットによる順守

トークンの発行者から証明書を必要とする送金の制限は、（分散型暗号通貨ではなく）発行者の方針によって発行されたトークンについて認められる。EPP は証明書に署名する前に KYC(顧客を知る)認証を必要とする場合がある。制限には証明書の保持者のみへの移転の制限やフロー・コントロール（フローするアカウント毎の送金とその特定の発行されたトークンについての最大アカウント残高の制限）が含まれる。これは、これらの制限をフラグしないトークンにも、分散型暗号通貨にも適用されない。発行したトークンについてライセンスと順守を確保するのは各 EPP の責任である。

5 分散型取引所

e ウォレットのやり取りのプラットフォームの中心の部分は分散型取引所である。これは EPP が発行したトークンをサポートする一方、分散型暗号通貨間でのトレードもサポートする。

分散型取引所は、異なるベースの価値の表示を持つかもしれない e ウォレットのやり取りに理想的かもしれず、もし同じベースで取引しているとしても、異なるカウンターパーティリスクやコストがある。同じものに裏付けられていたとしても、e ウォレット A は e ウォレット B と異なる。その理由から、適切な市場の運営には流動性市場が必要である（交換レートの違いがわずかだとしても）。

分散型取引所は当初、毎ラウンドごとに取引所でのマッチングが発生するバッチオークションの構造を使用する。特定のラウンド（ブロックの高さ）を受け入れるか、注文が満たされるまでオープンな注文をラウンドに残しておくことが可能である。バッチオークションは発注することを可能にし、実行は特定の間隔ごとに即座である。この構造は分散型ネットワークでのより高い保障とパフォーマンスを可能にする。注文は注文書に残る場合があるが、実行は EMV カード端末と同等の速度である（コンセンサスメカニズムの一層の研究が必要）。特定の利用ケースに速度が充分でない場合、EPP が高速トランザクションをサポートしたい他の EPP の残高を保持する責任を負う（より高いスプレッドを請求する場合がある）。これは毎日の少額の購入に利用でき、より高価値の購入は分散型取引所経由である。

レイテンシーの低い高頻度の注文実行が行えるのが望ましい一方、分散型ネットワークでそうすることには大きな障害がある。実行がそれぞれの時点で発生するのは注文マッチングの必要な機能である。実行が単一の「エンジン」で発生しなければ、シビル攻撃や単一当事者への信頼への可能性を開く。もし誰かが多くの場所で発注と実行を行えるなら、本当の発注のコミットメントは発生しなかったー容易にネットワークを「シビル」し、自身で実行されたふりをすることができる。加えて、信用されてない実行の発生場所において、スマートコントラクトと外部的に使用するティッカーを作成するーこのネットワークの必須機能ーのは不可能である。このネットワークの目的は群を抜く価値交換および決済プラットフォーム（高ボリューム低価値ネットワークではなく）となるというゴールを念頭にデザインされている。

高速実行ならびに低レイテンシーを可能にする別の選択肢としては、外部の集中型の場所を認めることである。しかし、これはに実行おいて単一の主体への信頼を確立する。トレードの流動性が（決済の集中化よりずっと強く）自然に集中化するにつれ、重大な信頼/連携の問題があり、最終的には現行の暗号通貨取引所に見えるようになる（唯一の違いは保管がないこと）。しかしながらこの構造は、主要な単一の信頼される提供者上でトレードしたくないという連携の問題の解決を必要とする参加者の間の連携の問題を解決しない。OmiseGO の分散型取引所のゴールは、透明で既知の実行の振る舞いを持つことである。私達は、信頼される非保管実行が分散型実行エンジンの補完として信用できる選択肢であると確信しており、将来これらのプラットフォームもサポートするかも知れない。成熟した分散型取引所には非保管の信頼される実行環境に比べ、スマートコントラクトのための分散型オラクルとして用いることができるという利点がある。

この分散型取引所は高パフォーマンスを出すよう設計されており、注文はプルーフ・オブ・ステークネットワーク上で伝播する。十分な参加者がブロック確認を持つ注文を持つ時、注文は注文ブックに置かれる。特定のバッチ実行時点の注文書は、そのバッチ実行の時点まで実行されないすべての注文の実行中のタリーである（なのでブック上でマッチする注文がある）。最初の設定には透明な注文が含まれるが、目隠しをされた発注が行われ、その後追加の注文は受け入れられず、目隠しする鍵が発注した参加者によってリリースされ、最後に一定時間後実行される模造コインのような構造を行うことが可能である。最初のバージョンは完全に透明なシステムを用いるであろう（バッチ実行フォーマットが敵対行動を一定分低減させる）。

その結果は、トレードの実行は主にプルーフ・オブ・ステーク分散型取引所である単一の「エンジン」上で発生するが、実行のルールが透明で検証可能であることが確保されているシステムである。

5.1 イーサリアムトレード

OMG は最大の効率とセキュリティのために公開イーサリアムブロックチェーンのフルノード認証を要するので、イーサリアムブロックチェーン上で OMG チェーンの状態に基づき資金をロックするコントラクトを作成するのが可能である。これらの資金は今や結合されロックされており、その活動は OMG チェーンによって施行される。注文が実行される時、イーサリアム側で資金をアンロックするために証明が提供される。

この構造は近い将来 Schnorr または BLS 署名がイーサリアム上で提供される事を仮定する。トランザクションは OMG チェーンの活動を追跡し、決済がイーサリアムチェーンに届けられる前に一定の「満期」の確認を必要とする。資金は依然としで OMG で決済され、トレードの継続のため残高は更新される。決済がイーサリアムで発生するのは最後のデリバリーについてのみであ

る。OMG チェーンの振る舞いはイーサリアムチェーン上での決済の振る舞いを施行する。非敵対的環境では、ユーザーが直接、証明なしに支払いを提供でき、もし決済が一定のブロック成熟の後争われない場合、ブロックチェーンによる証明/計算の必要なく支払われるライトニングのような構造が利用可能である。支払いが OMG の状態と一致しないような事があった場合、誰でも証明を提供でき、送信者の残高はその分カットされる。これはイーサリアムチェーン上でより大きな計算と帯域の効率を可能にする。

この OMG チェーン上の構造は、イーサリアムの取引、イーサリアムに類似のチェーン、そして結合されたスマートコントラクトを用いる ERC-20 に類似したイーサリアムが発行するトークン向けである。

5.2 他の取り組みとの比較

トレードは金融活動の基本的な側面である。これまでに他の暗号通貨取引所の構造を構築する取り組みがあったことは驚きではない。

Poloniex のような集中型の完全保管暗号通貨取引所は高パフォーマンスだが、責任ある保管と正直な注文の実行について単一の当事者への信頼に依存する。

リップル(XRP)のようなネットワークはコンセンサスへの到達について信頼される指名された認証者に頼っており、これはゲーム理論的には変更不可能な集合に収束する。加えて、リップルのトレード機能は自身のプラットフォームで発行されたアセットをトレードすることに依存し（保管の選択に関して重大な問題がある）、一方分散型取引所は発行されたゲートウェイなしにイーサやビットコインをトレードできない。

多くの EVM スマートコントラクトをを用いた分散型取引所プラットフォームは直接オンチェーンで行うこと（不可避的に全てがイーサリアムネットワーク上で行われることになり、ブロックチェーンを横断した活動を許さない）か単一のエンジンなしにオフチェーンで行うことに頼っている。OMG チェーンはネイティブの暗号通貨について、完全保管の発行されたアセットの利用なしにチェーンを横断（例:ETH-BTC）して稼働するよう設計されている。

新興のネットワークも分散型取引所に関連する設計を提供するかも知れない（例： Cosmos）。これらのネットワークはまだ十分にデプロイされていないので、違いを適切に比較、評価する事は出来ない。

5.3 ビットコインクリアリングハウス

一方、ビットコインやビットコインに類似したシステムについては、クリアリングハウスによってシステムの外部と結合したアセットを用いて BTC のトレードと他の類似のブロックチェーンも可能なシステムの作成が可能である。

本質的に、この構造はクリアリングハウスハウスが、ビットコインのようなブロックチェーンを持つ分散型取引所を可能にするため活動が OMG チェーンによって結合、施行されるオラクル[10]として稼働するのを可能にする。これは Tier Nolan[11]の仕事、外部の取引実行エンジンに基づく高速分散型取引所の実施から更に積み重ねたものである。

クリアリングハウスは支払がビットコインブロックチェーン上で発生するのを確保するため用いられる。私達は、外部のシステムを攻撃するためビットコイン採掘者がコンセンサスと互換しないが SPV 証明で有効であるブロックを生成する「反対の」インセンティブを防ぐため SPV 証明の代わりにクリアリングハウスを利用する（自身のチェーンへの再編成攻撃は高くつくが、外部への攻撃は安い）。

ビットコインに類似のシステムについては、このシステムは展性の修正（例：SegWit）か、P2SH/BIP-66/CLTV/CSV の組み合わせが透明なアドレスだけで利用可能であることを要する。

ビットコインでコントラクトの状態を複雑に施行するのは現在不可能なので、クリアリングハウスは必要である。これらのクリアリングハウスはプレイメージやハッシュを生成することによりビットコイン（またはビットコインに類似の）チェーン上での活動を開示する責任を持つ。ハッシュはクリアリングハウスによる活動にコミットされ、結合される。もし間違ったプレイメージをリリースしたり、OMG チェーンへプレイメージを開示するのを拒んだ場合、誰でも不正行為の証拠を提供でき、クリアリングハウスはカットを受ける。

これにはクリアリングハウスがビットコイン側で資金を利用できること、並びに OMG チェーン上での結合のために資金を利用できることを要することに注意のこと。結合された金額については、これは資金がクリアしてビットコイン側で決済されるまでのみ続く。なので、理想的には大きな資金の額を要しない。

クリアリングハウスはライトニングチャンネルを運営するが、チャンネルの彼らの側で資金を保持するだけでなく、複数の予定された資金（ETH で保持）が OMG チェーン上で流れる（例えば資金の流れについて三倍、彼らは口座において交換レートの変動について責任がある。）

図 1: アリスとボブはキャロル（クリアリングハウス）とライトニングネットワークチャンネルをビットコインブロックチェーン上で持っている。支払いのプレイメージ R がキャロルによって生成され、プレイメージのリリースは OmiseGO チェーン上の結合されたコミットメントによって施行される。

アリスがビットコインを売却したい、そしてボブがビットコインを購入したい、なおかつ両者がキャロル（クリアリングハウス）とチャンネルを開いていると仮定する。3 者とも OMG チェーン上にあり、キャロルをクリアリングハウスの仲介者として受け入れ指名する。もし両者が受け入れ可能として指名した場合、送金が複数のクリアリングハウスを経由して起こる場合があること、そしてトレードはトレードの参加者の間で受け入れ可能なクリアリングハウスが交差した時のみ発生することに注意のこと。

クリアリングハウスのキャロルはイーサリアムで「スマートコントラクト」と OMG チェーンのコンセンサスルールにより決定されたスマートコントラクトにより資金をロックし、キャロルは特定のハッシュ H（現時点でキャロルだけが知っているキャロルのプレイメージ R によって生成されたもの）の署名された証明を提供する。彼女が責任を持つ BTC での対応する値と署名とともに、彼女はハッシュ H を提供する。これは OMG チェーン上（そしてキャロルに落ち度がある場合イーサリアムスマートコントラクト）で証明として利用することができる[12]。

アリスがビットコインを売却したい時、彼女はキャロルが提供した H の値のリリースを条件とする HTLC の決済を作成する。同様に、ボブがビットコインを受け取りたい時、キャロルはキャロルがボブに提供する H の値のリリースを条件とする HTLC を送信する。

これらの H の値は OMG チェーン上で特定の人々と紐付けられ、資金は今や分散型取引所上で実行されるのに利用可能である。

トレードが OMG 分散型取引所で実行される時、例えばアリスが BTC を売って ETH を得、ボブが BTC を買って ETH を払う時、トレードは今や OMG チェーン上でクリアされる。全員がトレードを実行する責任と義務を持つ。

アリスとボブが OMG チェーン上にトレードを実行した該当する H について R プレイメージをリリースするのはキャロルの責任である。ボブはこの情報を用いて、ビットコインチェーンで資金を引き出すことが出来、キャロルは今やアリスから資金を引き出す権利を持つ。

もしキャロルが OMG チェーンへ適切な時間内に R プレイメージをリリースすることを拒否した場合、彼女の資金はカットされ、ETH はアリスと（または）ボブに提供される（交換レートの変動を低減しキャロルが不適切な行動を取らないディスインセンティブのため、ペナルティとともに）

もしキャロルが間違って R の値をリリースした場合、証明がどの当事者によっても OMG チェーンに提供されることができ、キャロルは罰せられ、資金はクリアリングハウス取引所コントラクトが H バリューでロックされた当事者に渡る。

クリアリングハウスは参加者（アリス、ボブ）と直接つながっている必要はなく、彼らはルーテッドネットワークを通じて支払うことができ、よって資本の効率を最大化出来る。

クリアリングハウスは全ての活動において彼らの利用にフィーを課金することができる。

クリアリングハウスが支払を行えることにはいくらかの信用が介在するが、彼らの活動での信用の最小化がある（彼らの活動は OMG チェーン上で結合されているので）。

付言しておくと、この構造は外部化された結合を通じた HTLC の高速失効にも有用であり、非常に高速、分単位のタイムアウト期限を持つ支払いを構築する方法足りうる。クリアリングハウスによって施行される結合された情報のリリースのために、クリアリングハウスがビットコインをロックすることを要しない。この構造のさらなる説明は別のペーパーに予定されている。

OMG チェーンが強く再組織を妨げるという理由のみでこれが可能であることに注意のこと。

最終結果は、ビットコインの外で分散型取引所を持つ能力である。ビットコインネットワーク上での参加者の活動が経済的インセンティブを持ってビットコインを扱うクリアリングハウス経由で外部の分散型取引所によって施行されるので、また、外部の状態経由で施行されたプレイメージのリリースがビットコインがプロトコルトークンブロックチェーンでのトレードに用いられるのを可能にするので、私達はこれが新たな構造であると確信している。

5.4 スマートコントラクトデータフィード

コンセンサスルールとして、最近のトレード実行の売買高加重平均価格（VWAP）が計算され OMG ブロックチェーン上で定期的に発行されている。

これは外部コントラクトが取引実行価格と取引高のマークル木の SPV 証明を利用するのを可能にし、望ましくはスマートコントラクトでの大きい生育可能性を作り出す。

図 2: データフィードへの定期的なコミットメントが OmiseGO ブロックチェーンに存在するであろう。これはブロックチェーンヘッダでのマークルルートコミットメントを通じた外部認証を可能にする。トレードのデータフィードには人気の交換ペアと最後の取引価格、取引高、そして各種 VWAP 状態（様々な時間とブロックの高さ）が含まれる。

どの取引所でも、主要な機能は注文ブックの管理と実行だけでなく、各サードパーティシステムが利用できる機能を持つことである。これはサードパーティシステムがこの情報を用いることができること、そして参加者が単一の場所で活動を概観するのを可能にする。あらゆる種類の（スマート）コントラクトの交換レート/値付けメカニズムの基盤が必要なので、このシステムへのアクセスはこれのデータフィードとして取引所を用いている外部コントラクトの参加者が取引の実行についてより大きい安心と透明性を得るのを可能にする。これにより各コントラクトの参加者が分散型取引所の振る舞いとアクセスの知識のもとコントラクトを作成するのが可能になる。もし参加者がスマートコントラクト上の値付けの基盤として OmiseGO チェーンの価格のオラクルフィードを用いる場合、彼らはより大きい OMG チェーン上で発注する際に実行されるという安心を持つことが出来る。これは一層のスマートコントラクトの採用により、大きな OMG チェーンのネットワーク効果を生み出す。

6.ライトニング流動性プロバイダ

資本流動性のネットワーク効果周りで集中化のプレッシャーについて基本的な懸念がある。多くがライトニングネットワークが一握りのノードに集中し、「家賃を取り立てる」可能性を持つという懸念を持っている。ライトニングネットワークは流動性の非常に高いノードについてこのような「家賃の取り立て」を回避するよう設計されている。しかし、よく接続されたノードを持つことの最適な利点がある。

上の節にあるクリアリングハウスに似て、ノードが OMG チェーン上で活動を結合でき、OMG チェーンが流動性の非常に高い単一のライトニングハブとして振る舞うことができるメカニズムを構築するのは可能である。

ETH や ETH に類似のチャンネルについては、直接スマートコントラクトにロックすることが可能である。BTC ベースのチャンネルに関しては、可能だが、チャンネル参加者の活動は OMG チェーン上の ETH に裏打ちされた債券によって施行される。支払いは OMG チェーンじょうの参加者へと送信され、出て行く活動はこのチェーン上のコミットメントを通じて施行される。

OMG プラットフォームが成熟するまでの間、多過ぎる資本がこのシステムに割り当てられるのを防ぐため、制限は必要である。それにより、クリアリングハウスと分散型取引所に資金利用可能性のインセンティブを与える巨大な流動性プールの作成が可能となる。

7. OmiseGO トークンへの経済的影響

トランザクションフィーは OmiseGO チェーンにネイティブである。認証者はこのブロックチェーン上の活動を認証することで手数料を受け取る。

支払いややり取りの手数料は、このネットワーク上の活動の支払いに、そして正直な活動にインセンティブを与えるため用いられる。

結合にはコストがかかり、このネットワーク上で他の代わりに結合する人々、例えばクリアリングハウスはおそらく手数料を課金する。

8. 制限

このネットワークはオープンなネットワークであり、正確なトレード活動には、目隠しされたコミットメント/入札としてでも、分散型取引所上の活動が最終的に公開となることが必要である。新しい暗号方式が SNARKS 経由で可能である一方、今の所高取引高のトレードネットワークには低速かつリソースを消費し過ぎる。（発行されたトークンについて AML/KYC の構造のオプション付きの）ネイティブに匿名のネットワークなので、私達は現在パフォーマンスと速度の面で最適化を行っている。

他のチェーンの SPV 認証は再構成を妨げないブロックチェーンの場合セキュアでないと仮定される。再構成を認めるチェーンについては、そのチェーンのフルノード認証か、HTLC クリアリングハウスの構築が必要である。これは、イーサリアムが今後より高い信頼性を持ち、ファイナリティ周りの保証を行う（現行のプルーフ・オブ・ステーク研究）ことを仮定するものである。

これらのテクノロジーは新しいもので、まだテストされていない。私達は逆境的な設定で最大限のセキュリティで構築することに最善を尽くす一方、適切な理解に現実世界での人間の行動が関わる利用ケースが必要な、これらのメカニズムのセキュリティモデルをモデリングしている
チェーン間のやり取りにおいてエラーをロールバックするのは難しく、重要な分散型のブロックチェーンを横断した活動を行っている時、一回あたり必要最小限をこのチェーンに投入すべきである。最初のバージョンは逆境的な設定の場合堅牢さの点で不足かもしれず、攻撃（特に DoS 攻撃）はソフトウェア開発が進むにつれ解決するので、私達は低めの数値を試すことを推奨する。デザインのパフォーマンスと現実世界での振る舞いの影響はまだ明確でない。

このネットワークの参加者が長期的にどのような価値を引き出すことができるか、未だ明確になっておらず、この空間での競争に影響される場合があり、またこの領域はまだ技術面の探索が進んでいないので、認証者として参加することについて保証は提供されない。

クリアした（が未だ決済していない）送金の合計価値は、どの時点でも、合計の認証者達の結合した価値より低くなければならない。追加の額を結合することは可能だが、トークンの合計価値が十分に高い場合必要ないかも知れない。このシステムに固有である施行メカニズムの更なるモデリングが必要である。

究極的にこのビジョンの実行は OmiseGO チームが責を負い、この文書の作者は OmiseGO チームを構成せず、技術的ガイドラインとアーキテクチャの提供についてのみ責任を負う。

9. 結論

e ウォレットプラットフォームの人気が台頭する中、サイロ・ネットワーク（他と連携を適切に取らないネットワーク）が問題となっている。これは法定通貨トークンにとって暗号通貨との相互互換性とともに、分散型ネットワークを横断してやり取りするユニークな機会を生み出す。

この分散型のやり取りのネットワークを構築するには、発行されたトークンの支払いとやり取りに適切なブロックチェーンを必要とするだけでなく、これらの活動をサポートする分散型取引所や良く機能する流動性プールを作成するインセンティブも必要とする。

いずれ、これらの発行されたトークンは（ユーザー所有の鍵も含め）漸近的に完全な分散型に近づいていき、それにより個人の働きが最大化される。これは支払いのやり取りのビジネスプロセスに透明性を作り出すだけでなく、ビジネスプロセスそのものの所有を単一の信頼される主体から除くことで達成できる。OmiseGO は個人から発行者まで、各ステークホルダーが社会の金融メカニズムに対しはるかに大きな安心を得ることを可能にする。

10 謝辞

この論文へ貢献してくれた Piotr Dobaczewski、並びにインプットとフィードバックをくれたリック・ダッドリーとヴィタリック・ブテリンに感謝したい。

11 ライセンス

参考文献

[1] Fred Erhsam. Blockchain Tokens and the dawn of the Decentralized Business Model. https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f.
[2] Fred Erhsam. Tokens, Why How. https://www.youtube.com/watch?v=rktHO5R8Y9c.
[3] Ethereum. Ethereum. https://ethereum.org/.
[4] Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. http://szabo.best.vwh.net/formalize.html, Feb 2015.
[5] Nick Szabo. Formalizing and Securing Relationships on Public Networks. http://szabo.best.vwh.net/formalize.html , Sep 1997.
[6] Joseph Poon and Tadge Dryja. Lightning Network. https://lightning.network/lightning-network-paper.pdf, Mar 2015.
[7] Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, Oct 2008.
[8] Raiden. Raiden Network. https://raiden.network/.
[9] Joseph Chow. BTC Relay. http://btcrelay.org/.
[10] Bitcoin Wiki. Using external state. https://en.bitcoin.it/wiki/Contract#Example_4:_Using_external_state
[11] Tier Nolan. Re: Alt chains and atomic transfers. https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949.
[12] Ilja Gerhardt and Timo Hanke. Homomorphic Payment Addresses and the Pay-to Contract Protocol. http://arxiv.org/abs/1212.3257, Dec 2012.