

ジブレルネットワーク

2017年5月

第二草稿

YAZAN BARGHUTHI
yazan@jibrel.network

VICTOR MEZRIN
victor@jibrel.network

抜粋

ジブレルネットワークは、通貨、債券、およびその他の金融商品などの伝統的資産のデジタル化、上場および取引をブロックチェーン上で容易にすることを目的としています。ジブレル分散DAO、プラットフォームユーザーが現金、短期金融商品を入金したり、独自の暗号保管預託証券（CryDRs）を作成し、オンチェーン・オフチェーンアービトラージから利益を得ることを可能にします。デジタル通貨に過度にさらされた分散組織やファンドは、ポジションをヘッジし、安定した資産で資金を保護することができます。さらに、ジブレルは、伝統的なアセットバックトークンを活用して、取引、投資、ヘッジのためのツールとアプリケーションを構築するための完全なプラットフォームを開発者に提供します。

これに加えて、ジブレルは、ピアツーピア、ビジネス・ツー・ビジネス、または消費者から加盟店へのチャンネルを通じて、即時かつ手数料ほぼゼロで、Fiat to Fiatの送金取引やグローバルな支払いを可能にします。

このホワイトペーパーでは、ジブレルを構成するコアコンポーネント、その相互作用、および既存のインフラストラクチャを使用してネットワークを効率的に構築する方法を示します。

1.概要

2009年にBitcoinが登場して以来[1]、ブロックチェーンは世界に大きな価値をもたらしました。この新技術は、不変の分散型元帳でトランザクションを検証しコミットしたり、より広範に実装して分散型コンセンサスを達成することができます。

この信じられないほどイノベーションは、幅広い業種において、信頼をおける仲介業者、決済機関、および仲介のサービスプロバイダーの必要性を減らし、世界を変革しています。

しかし、大規模組織での採用が限定されているため、暗号化経済の価値の大部分は、ユースケースまたは地理的にサイロ化されています。さらに、これらのサイロによって課せられたボトルネックが伝統的資産とデジタル資産との間で変換する際の挑戦や制限の形で広がっているため、システム全体のリスクが広がっています。

伝統的経済と暗号通貨経済の切り離しを考えると、前者を悩ます課題のと同じ課題が後者に依然として残っています。伝統的資産とデジタル資産の相互交換を希望するユーザは、支払を処理するサービス、伝統的金融機関、暗号通貨交換所による利用料とタイムラグといった問題に直面しています。

さらに、伝統的資産の移動を迅速にほぼ制限なくできる従来の個人投資家や機関投資家は、その根本的な非互換性のために参入を断念しています - 最も顕著なのは、透明性の欠如と市場の極端な流動性です[2]。

最後に、クラウドセールス、分散ファンド、デジタル資産や暗号通貨を多く持ち、仮想通貨インベスターにより資金を調達する分散型組織は、伝統的資産への分散投資の方法が限られています。

取引を円滑するマイナーへの利益供与、価値の移転手段、投機的な投資ツール、そしてもっとも最近ではクラウドファンディングと分散組織とアプリケーション（例えば、分散コンピューティング[3]や分散ストレージ[4]）など、デジタル通貨が多面的な役割を持つという事実は、これらのリスクを高める。

伝統的金融では、さまざまな商品にとってこの機能が果たされ、それに応じて規制もあります。これが仕組的なリスクを管理するのに役立っています。分散規制コンセンサスプロトコルが完全に構築されるまで、暗号経済は安全性と詐欺のリスクに直面しています。規制のない取引、極端に流動性の高い通貨と、そのアーキテクチャの目的を超えた使用による起因するマーケットリスク、そして、スマートコントラクトでの締結され流動性の高いデジタル通貨で保存されたクラウドファンディングが仕組上のリスクを生み出します。

このホワイトペーパーでは、現在の環境の限界と課題を分析し、既存のインフラストラクチャを活用してすべてのステークホルダーにソリューションを提供するアプローチを提案します。

2. 伝統的資産によって裏付けられたトークン

ジブレルエコシステムの中核となるステークホルダーは、低送金手数料や即時転送などのブロックチェーンテクノロジーと暗号通貨によってロックされていない価値から利益を得ようとする非投資ユーザー、新興の暗号経済のハイリターンな利益を得ようとする従来の投資家、非匿名のクラウド投資家として、オンチェーンの安定した低利回り暗号資産のポートフォリオを多様化しようとする分散組織やファンド、暗号通貨投資家です。

伝統的金融商品の安定性をブロックチェーンにもたらすことで、すべてのステークホルダーのニーズを満たすことができます。これを実現するのが、トークンと伝統的資産をデザイヤーによる、トークンの価値を裏付けです。これにより、デザイヤーされたトークン（デザイヤートークン）は、通貨[5]やコモディティ[6]としての価値を表すことができます。

伝統的資産と原資産の所有権を表す発行トークンを保有する「保証機能」を開発することにより、幅広い通貨、商品、マネーマーケット商品およびその他の金融ツールをオープンに取引することができます。

3. システムアーキテクチャー

以下のセクションでは、ジブレルネットワークの主要コンポーネントと、伝統的資産を連携について概説します。

3.1 公開ブロックチェーン

別のブロックチェーンに依存することは、新たな課題と限界を突きつけますが、完全なクロスチェーン通信が可能になるまでは、初期バージョンのジブレルにはパブリックで安全なブロックチェーンが必要です。

3.2 暗号通貨の取引

暗号通貨取引は、エンドユーザーにローカル通貨の決済口座と、暗号化通貨を保持できるデジタルウォレットを提供しました。ユーザーは、デジタル通貨を購入、取引、または送信することができ、簡単に暗号通貨と通常通貨の交換を簡単にできます。

3.3 デザイヤートークン

デザイヤートークンは、伝統的資産に裏付けされたトークンです。保持している伝統的資産ごとに、紐づけされたトークンが作成されます。裏付け資産が売却されると、トークンは破棄されます。

3.4 保証機能

デザイヤートークンの価値を保持するために保証機能を設けます。保証機能は、伝統的資産を保有し、それに対応するデザイヤートークンを発行するだけでなく、その伝統的資産の所有権の解放・譲渡の代償としてトークンを償還し破棄するものです。

3.5 アプリケーションレイヤ、ライブラリ、テンプレート

デザイヤートークンが確立されたら、支払処理機能、送金口座、取引プラットフォームなど、その能力を活用する一連のアプリケーションを開発することができます。アプリケーション開発を容易にするために、ユーザーフレンドリーなライブラリとコードテンプレートを備えた専用アプリケーションレイヤを設けます。

3.6 所有権移転

デザイヤートークンが発行したら、裏付け資産は任意の暗号通貨と同様に容易に取引できるようになります。上位レベルのプロセスの概略を以下に示します。

1. ユーザーがFIATを保証機能に送る
2. 保証人がjFIATを返却する
3. ユーザーがjFIATでマーチャントに支払う
4. 加盟店がjFIATを償還する
5. 保証人がFiatをマーチャント口座に送る

紐づけトークンは保証機能により裏付けされ、将来の時点で裏付け資産との引き換えが可能であるため、トークンはシステム内に留まりオンチェーンやオフチェーンの支払いに利用できます。

3.7 料金

デジタルまたは伝統的資産の所有権の移転には手数料がかかります。

3.8 規制・監視

所有権や価値のオフチェーン移転を表すあらゆるオンチェーン取引は、国際および各国の規制を満たす必要があり、それに応じて管理する必要があります。

適切なガバナンスと監督を確実にするために、規制プロトコル・ガバナンスツールが必要です。

すべての取引はKYC / AML規則を満たさなければなりません。

4. ジブレルネットワークの実装

このセクションでは、各コンポーネントがジブレルネットワークでどのように実装されるかを概説します。

4.1 イーサリアムブロックチェーン

この選択されたブロックチェーンは、システムの参加者間の取引とマイニング報酬を切り離す必要があります。このため、イーサリアムはジブレルの基礎となるアーキテクチャの基盤を形成するのに適しています。マイニングの報酬はイーサリアムの「ガス」です。紐づけされたトークンはマイニングプロセスの一部にはなりません[7]。

ジブレルは、Bitcoinのオムニプロトコル上に構築するのにも適していますが、このアプローチはこのホワイトペーパーの対象外です。

4.2 暗号預託証券 (CryDR)

CryDRは、ジブレルが保有する、トークンの価値を裏付ける伝統的資産に紐づけされたトークンです。このホワイトペーパーでは、それらをjAsset (例: jUSD、jEUR、jGBP)と表記します。リリース時点で、ジブレルは6種類の決済通貨と2種類のマネーマーケット商品をサポートし、将来的には他の金融商品を追加する予定です。

4.2.1 通貨/Fiat

ジブルネットワークの最初のイテレーションでは、USD、EUR、GBP、RUB、CNY、AEDをサポートし、戦略的な取引パートナーとの連携が増えるにつれて、より多くの通貨をサポートすることを目指しています。

4.2.2 マネーマーケット商品

安定した低利回り資産はジブレルの中核であり、暗号投資家は米国財務省証券とゼロクーポン預金証書に紐づけされたトークン (テザートークン) を購入することができます。ジブルネットワークの最初のイテレーションでは、すべてのマネーマーケット商品に自動ロールオーバーまたはアキュラレートメカニズムが組み込まれます。つまり、満期の投資から得た金額は、自動的に同様の資産に再配分されます。同様に、配当または利息は、裏付け資産が満期になるか、または売却されるまで積立されます。将来のバージョンでは、マネーマーケットの商品は設定可能になりません。

4.2.3 その他の金融商品

将来的には、ジブレルプラットフォームは伝統的金融機関と連携し、上場株式やプライベートエクイティを含む他の金融商品の全面的なサポートも行います。

4.2.4 スマートコンプライアンス

CryDRは完全にプログラム可能であるため、規制に組み込むことができます。フィアット通貨は制限されませんが、他の資産の購入と再販はクラスと地域に完全に準拠するように制限する必要があります。このロジックは各CryDRに組み込まれています。

4.3 ジブレル分散型銀行 (DAO)

DAOは、所有者に代わって伝統的な資産を受領/保持し、それぞれのCryDRを発行します。それは所有者の財布に送られる。トークンを償還すると、トークンは破棄され、基礎資産はトークンホルダーに転送されます。

DAOは完全な分散化を目指していますが、伝統的金融機関とのフルチェーン連携が完成するまでは、大部分のシステムコンポーネントはオフチェーンで運用されます。オフチェーンアクティビティには、インプットと国際および各国の規制当局による監視が必要です。

これらの理由により、ステークホルダーのインターアクションは、透明性や信頼性を損なわないう、すべての規制に準拠するよう的確に管理される必要があります。これは、各地域の規制に準拠する専用の団体、アセットポータルにより可能になります。

4.4 アセットポータル

アセットポータルは、伝統的資産をオンチェーンのデジタル資産に変換するために必要な法的および財務的処理の実行に使用されます。

Fiatポータルはシンプルな暗号通貨取引です。既存の取引で戦略的パートナーシップを構築することと同時に、専用ジブル交換ネットワークを幅広い地域に構築することができます。さらに、ジブルのFiat保有の一部を取引所に保有することにより、取引にかかる時間と手数料を大幅に下げながら、流動的な取引を可能にします。

非Fiatポータルは、オフチェーン形式をとり、必要なデューデリジェンスを行い、非Fiat預金の所有権を持ちます。

ほとんどの地域では、アセットポータルには仲介業者と送金者のライセンスが必要です。規制が厳しい地域や、より微妙な金融資産を伴うケースでは、規制当局の関与や監督が必要になるかもしれません。

規制が進展するにつれて、アセットポータルは分散化され、コミュニティ主導型になります。機関投資家やその他の金融機関は、ジブレルプラットフォームを使用して、チェーン上に独自の伝統資産をリストすることができます。

4.5 ジブルネットワークトークン (JNT)

非Fiatポータルは、オフライン料金をFiat通貨に課金しますが、DAOのオンチェーン手数料および仲介手数料は、ジブレルネットワークトークン (JIB) で課せられます。

5. インフラストラクチャ

ユーザー残高やトランザクションなどの重要なデータはブロックチェーンに格納され、他のすべてのデータは開発サーバーでホストされます。

分散アプリケーションの迅速な開発を可能にするために、いくつかの開発環境、ツール、フレームワークがすでに開発されています[8]。ジブレルは、CryDRの普及を可能にするために、同様の開発コンポーネント、ツール、およびフレームワークを開発する必要があります。

インフラストラクチャは、オンチェーンAPIとオフチェーンAPI/ユーティリティの2つに必要となります。

5.1 オン・チェーン・インフラストラクチャー

ネットワークが効果的な動作に必要なのは4つの主要なスマートコントラクトだけです。

5.1.1 CryDRスマートコントラクト

DAOに登録された各資産は、スマートコントラクトで発行されるCryDRを有します。CryDRスマートコントラクトはERC-20に準拠します。ユーザーアカウント間でCryDRを転送することは、ウォレット間で他のERC-20トークンを転送することと似ています。

5.1.2 DAOスマートコントラクト

専用のDAOスマートコントラクトは、CryDRスマートコントラクトの業務を規制します。

5.1.3 取締役会スマートコントラクト (BODC)

理事会のスマート契約 (BODC) は、Jibrell DAO契約と相互作用し、影響を与える唯一のメカニズムです

BODCは投票システムを通じて管理されます。取締役員はイーサリアムアカウントを使って、BODCの決定に投票できます。プライベートキーの保管と使用は、メンバーの責任となります。理事会は暗号通貨の専門家と、金融サービスの専門家で構成するのが理想です。

図1. 暗号保管庫の領収書一般的なワークフロー

5.1.4 ヘルパー/ユーティリティ (補助スマートコントラクト)

また、補助的な機能、例えば、追加APIや異なるバージョンの契約書の切り替えなどの補助的な機能を有効化するために、異なる複数の補助的スマートコントラクトが必要で

す。

このホワイトペーパーのスコープを超えるため、ここでは詳細について言及しません。

5.2 オフ・チェーン・インフラストラクチャー

トランザクション、投資およびヘッジツールとしてのCryDRの普及を促進するために、アプリケーション開発者向けの使いやすいライブラリとコードテンプレートを公開します。

図2. ジブレル DApp APIワークフロー

5.2.1 ライブラリとテンプレート

開発者は既存ライブラリを使用してイーサリアムブロックチェーン (JS web3など) とやりとりできます。ジブラルは、このライブラリとコードサンプルをリリースし、DAOとCryDRスマートコントラクトのやりとりを簡素化します。

5.2.2 CryDRエクスプローラ

オープンソースのエクスプローラが作成され、ユーザーはCryDRメタデータを表示してBODCとやりとりすることができます。また、DAOによる裏付け資産の所有権を手動で確認することもできます。

5.2.3 取締役会ツールキット

ツールを作成し、CryDR Ltdの社内ITインフラストラクチャとイーサリアムブロックチェーンがインターフェースされます。特に、取締役会メンバーとBODCとの相互作用の組織化およびシステムの状態の運用的な監視のために利用されます。

6. スマート規制の実施

このセクションでは、CryDRの実装、ジブレルネットワーク内のスマート・レギュレーションとコンプライアンスの概要を説明します。

6.1 CryDRアーキテクチャ

CryDR自体は、イーサリアムブロックチェーンにデプロイされたスマートコントラクトです。堅牢でスケーラブルなシステムを容易にするために、CryDRは以下の複数の要件を満たす必要があります。

高い互換性：ERC20インターフェイスに既存のトークン管理ツールと互換性が必要です。

更新可能なビジネスロジック：進化する現実のルールや規制に追いつくために簡単にアップグレード可能できるようにします。

永続性：デプロイ後は永続的に稼働します。

移行可能性：イベントとストレージは別々に保存する必要があります。

相互作用：CryDRはお互いに相互作用できるようにします。

6.2 既存の方法論

これらの技術的要件は、現在のイーサリアムエコシステム内で利用可能なツールを使用して達成することは困難です。アップグレード可能なスマートコントラクトは実装するのが難しく、特定のツールや方法論が存在する一方で、それぞれ独自の制限があります。

6.2.1 EVM DELEGATECALL

第1のアプローチは、イーサリアム仮想マシン（EVM）におけるコード「DELEGATECALL」の活用です。

これはビジネスロジックを更新する強力なツールですが、欠点もあります。具体的には、一旦導入されると、元のスマートコントラクトのストレージ構造の維持に更新が必要なことです。そのため、このアプローチは単純なアップグレード可能な契約の実装でのみ使用でき、ジブレルのユースケースには使用できません。

6.2.2 スマートコントラクトブルーニング

もう1つの解決策は、契約のブルーニングし、同じアドレスで別の新しい契約を展開し、イベントと状態を保持することです。これはジブレルネットワークにとって理想的なソリューションですが、まだEVMに実装されていません。

6.3 ジブレルネットワークアプローチ

ジブレルを構築するには、単調でもホリスティックなソリューションが必要です。そこで、システム全体をデコンストラクトし、複数の洗練されたスマートコントラクトに分解することです。インターアクトしつつも、シームレスなアップグレードとアップデートをできるようになります。

より複雑な実装が必要になりますが、ジブレルDAppsに強力なバックエンドを提供します。

6.3.1 CryDR 3層システム

CryDRは、以下の重要なコンポーネントに分解されます。

ストレージ - すべてのデータを格納

表示 : サードパーティの契約とウェブアプリケーションのインターフェイス

コントローラ : コンプライアンスとビジネスロジックを実装し、ストレージを調整し、契約を表示する

図3階層構造

6.3.1.1 コンプライアンスの更新

この構造により、新しいCryDRコントローラ契約を簡単に導入し、この新しいコントローラを使用するためのビューおよびストレージ契約を設定することができます。

これにより、当社がスマート・レギュレーションと呼ぶ基本的なコンプライアンスとビジネス・ロジックのCryDRを簡単に更新することができます。

図4コントローラの更新

ジブレルネットワークは、ビジネスロジックの更新を可能にするプロセスを容易にすることで、現実の規制の変化に伴ってトークンのコンプライアンスを維持します。

6.3.1.2 インタフェースのアップグレード

このアーキテクチャーを使用して、トークン・インターフェイスをシームレスにアップグレードすることもできます。例えば、新しいトークン標準（例えばERC223）の追加サポートもできます。

図5アップグレードの表示

簡単に言えば、すべてのコンプライアンス対策は、スマートコントラクトを介してチェーン上で実施されるということです。

KYC / AML対策を実施するには、2つのソリューションを実装する必要があります。

データストレージ：ユーザーデータをチェーンに保存
ルールの実装：各トランザクションにKYC / AMLルールを適用

多くのプロジェクトが最初の課題に取り組んでいます。CivicやuPortなど。しかし、これらのソリューションは適応性があり、汎用性があるように構築されているため、機関グレードのKYC / AMLプロセスの必要性を十分に満たしていない一般ユーザー情報しか保存できません。

このため、ジブレルは、専用のジブレル KYC / AMLモジュールとサードパーティのソリューションの両方を利用できる専用のコンプライアンスAPIを構築します。

図7. ジブレル準拠API

このようなアップグレードを実行する場合、CryDRストレージは変更されず、また影響も受けません。

ビューはコントローラーの前に階層化されたレイヤーとして機能するため、更新中はすべてのイベントがそのまま残ります。実装されたコントローラーが接続されたすべてのビューをトリガーするので、クライアントはすべてのイベントを受け取ることができます。

図6. トリガイベント

6.3.2 スマート規則アーキテクチャ

KYC / AML対策を実施するには、厳密かつ詳細なアカウント許可制御が必要です。

スマートコントラクトは継承された制限があります。主に、設計上禁止されているサードパーティサービスへの呼び出しを使用して、オンチェーンデータにのみアクセスできます。

オフチェーンデータにアクセスするには、データをまず取引の形式でブロックチェーンにプッシュする必要があります。

6.3.3 ジブレルネットワークトークン (JNT) の役割

ジブレルネットワークの重要なビジネス要件は、すべてのCryDRが裏付け資産にテザーされていることです。これを達成するためには、オフチェーン資産をまず証券化しなければならないため、仮想為替通貨が必要となります。両方もネットワークとの取引だけでなく、支払いオフチェーン手数料もです。

既存の通貨 (BTC、ETHなど) は適切ではありません。なぜなら、これらの通貨の価格変動がジブレルネットワークのユーティリティと無関係であるからです。この切り離しは市場リスクと信用リスクを課します。また、ジブレルネットワークが将来的に専用チェーンを提供することを目指す場合、シームレスな移行プロセスを促進するために専用のトークンが必要になります。

CryDR自体は、現実世界の資産に縛られたままでなければならぬため、このソリューションには適していません。支払いの一部としてそれらを活用すると、別の切り離しが発生し、システムが不安定になります。

ジブレネットワークトークン (JNT) は、ネットワークの「燃料」または「ガス」として機能します。JNTは、ジブレと関連するジブレDAppsが提供するすべての機能にユニバーサルアクセスを提供します。

JNTは、コンプライアンスの層を追加し、すべてのCryDRが常にそれぞれの裏付け資産に拘束された状態を維持します。

図8. ジブレネットワークトークンの相互作用

7. 完全分散オペレーション

中長期的には、物理的資産をデジタル資産に変換するために必要な法的および財務的デューデリジェンスを実施するためにオフ・チェーン活動が必要となります。また、透明性と法令遵守を完全に確保するために、DAOを監督するために取締役会役員が必要となります。

長期的には、ジブレを分散自律組織にすることができるように、アセット・オーナーシップのオンチェーン検証を容易にするための規制が進化することが期待されます。

7.1 セルフサービスポータル

オンチェーンのコンピュータ処理能力や複雑なゼロ知識証明[9]を実装する実現可能性などの技術的限界と、関係ライセンスを取得するための規制上のハードルの克服したら、ジブレはセルフサービスポータル (ジブレネットワークと通信する従来の交換プラットフォーム) を運用する可能性があります。

これらのポータルの構築は、分散化を完全に達成するために重要です。

7.2 オンチェーンデジタルアイデンティティ/ KYC / AML
多くのオンチェーンのデジタルアイデンティティとKYCソリューションはすでに存在しますが、機能には限界があります。セルフサービスのポータルを実現するには、より高度な識別ソリューションが必要です。

7.3 取締役会DAO

業務が安定化したら、取締役会を解散し、DAOの業務を監督する自主的な規制機関に置き換えることができます。

8. ユースケース

容易に両替可能な従来のアセットバックトークンは、幅広いユースケースを提供します。

8.1 伝統的資産・デジタル資産取引所

伝統的資産とデジタル資産を自由に取引できるようにすることで、安定したデジタル資産を求めている投資家やエンティティに従来の投資手段を卸売し、機関投資家に対するリスクの低い、高いリターンを促進するプラットフォームが本質的に開発されます。

8.1.1 投資プラットフォーム

投資、マネーマーケットの商品や商品をDAOに入金し、その商品 (CryDR) を、分散型組織やファンドにプレミアムで販売することができます。

8.1.2 ヘッジ・トークン

分散自治組織と資金は、資金調達及安全であることを投資家に安心させるために、完全な透明性で、マネーマーケットのCryDRを購入してオンチェーンに保管することができます。分散型自律基金は、デジタルポートフォリオを補完し、暗号経済のデメリットから保護するために、幅広い伝統的資産から投資対象を選択することができます。

8.2 グローバル振り替え

アセットバックトークンを提供することにより、従来のアセット (特に安定性とグローバルな採用)、デジタル資産の不変性、振り替えの容易性、信頼性の両方をすべて備えたトークンを提供することができます。

これらのトークンを使用して、支払いゲートウェイ、送金チャネル、および他の送金転送ユースケースを実装することができます。

8.2.1 送金

ジブレは、トランザクションを実行するのに暗号通貨インフラを利用するFiat-to-Fiat振り替えを実現することで、送金を可能にしました。これによりユーザーは、デジタル通貨の低手数料を活用し、さらに伝統的資産の安全性と安定性を享受しながら、資金の追加したり、資金を世界中のどこかに移動したりできます。

8.2.2 ユニバーサルウォレット

通貨に依存しないウォレットを作成し、ユーザーが通貨間の両替や送金を、世界中のどこでも、どの通貨でも自由に行えるようにします。もちろん、これらには手数料がかかります。

8.3 国境を越えた支払い

同様に、ジブレは国境を越えた支払いを可能にします。

8.3.1 通貨API

裏付けとなるトークンを使用して、ジブレルはユーザーが通貨間で自由に両替できるようにする通貨APIを提供しません。

8.3.2 Merchant API

ジブレルは、どの通貨でも支払いを受け入れ、現地通貨で支払うことができる使いやすい支払いゲートウェイを簡単

にマーチャントに提供します。交換または手数料を払わずに。

ネットワークが確立されたら、加盟店は、ジブレルのライブラリとAPIを使用して、通貨に依存しない決済ゲートウェイをセットアップすることができます。

9. 参考文献

- [1] Nakamoto, Satoshi, *Bitcoin: A peer-to-peer electronic cash system*, 2008 - URL - {<https://bitcoin.org/bitcoin.pdf>}
- [2] Brennan and Lunn, Credit Suisse Equity Reports - *Blockchain - The trust disruptor: Shared ledger technology and the impact on stocks*, 2016 - URL {<http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf>}
- [3] Golem, *The Golem Project: Crowdfunding White Paper*, 2016 - URL {<http://golemproject.net/doc/DraftGolemProjectWhitepaper.pdf>}
- [4] Wilkinson, Shawn, *Storj Project: A Peer-to-Peer Cloud Storage Network*, 2014 - URL {<https://storj.io/storj.pdf>}
- [5] Tether Ltd, *Tether: Fiat currencies on the Bitcoin blockchain*, 2016 - URL {<https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf>}
- [6] Eufemio, Chng and Djie, *Digix: The Gold Standard in CryptoAssets*, 2016 - URL {<https://dgx.io/whitepaper.pdf>}
- [7] Buterin, Vitalik, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2013 - URL {<http://ethereum.org/ethereum.html>}
- [8] Solidity, *Solidity: A contract-oriented, high-level language for the Ethereum Virtual Machine*, Release 0.4.10 Documentation - URL {<http://solidity.readthedocs.io/en/v0.4.10/>}
- [9] Ben-Sasson, Chiesa, Garman, Green, Miers, Tromer and Virza, *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014 - URL {<http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf>}