HYCON ホワイトペーパー

INFINITY プロジェクト

要旨

本ホワイトペーパーでは、以下の 3 段階で展開する INFINITY(インフィニティ)プロジェクトのビジョンの要点から述べる：1)「HYCON(ハイコン)」コイン、2) カスタマイズ可能なエンタープライズブロックチェーンソリューションを提供する INFINITY プラットフォームオープンソース、3) 分散型暗号通貨取引所。ただし、本ホワイトペーパーの主題は、SPECTRE プロトコルを用いることで安全性を保ちながら高速処理が可能な暗号通貨である「HYCON」の詳細分析を提供することである。既存の暗号通貨の多くが抱える課題や限界の事例と共に、

「HYCON」コインが提供するソリューションについて以下に明示する。更に、「HYCON」の技術仕様書を公開し、SPECTRE とプロジェクトへの実装に関する簡潔な解説も加える。

序論

> 「...何千年にも渡り人類にとって最も多用途で長期的に使用されたテクノロジーのひとつである現金は、今後 15 年で大きく変化し最終的に 1 と 0 の電子ストリームに完全に置き換わるだろう。」
>
> **The Economist (2007)**

今日の電子商取引及びモバイルバンキング業界では、お金とは誰かが所有している何らかの有形物を、インターネット上を移動するデジタル番号に変換したものである。そして自然な流れとして、暗号で保護されたデジタルコードの文字列としてのみ存在する「暗号通貨」と呼ばれる新しい形式の通貨が誕生した。デジタル通貨革命は、Satoshi Nakamoto と名乗る依然正体不明の人物がビットコインホワイトペーパー [19]を発表した 2008 年に始まった。

今日、新しい暗号通貨が毎日のように発表されているが、どの通貨もブロックチェーンという技術構造を基盤とする統一概念を共有している。

ブロックチェーン自体は、最初に生成されたブロックから今この瞬間までシステム上で行われた全取引を、記録及び保持している共有の公開取引台帳である。台帳、つまり上記で説明したブロックチェーンは、連結リスト、またはブロックの連結により構築され、各ブロックは一定数の取引を含み、ネットワークによって特定の期間で認証される。

INFINITY プロジェクトでは、既存のブロックチェーンテクノロジーが抱える課題に対処するために設計された「HYCON」という新たな暗号通貨を発表する。以下に、対処すべき課題に焦点を当てた既存のブロックチェーン開発の概要、INFINITY プロジェクトの目的、「HYCON」が既存のブロックチェーンの限界をどのように克服するのか、及び「HYCON」の技術仕様書を提示する。

既存のブロックチェーンテクノロジーの考察

考察にあたり、これまでに最も広く使用され、ブロックチェーンテクノロジーの実装に関し既に十分研究されている、ビットコインとイーサリアムのブロックチェーンに焦点を当てる。

Yli-Huomo らの研究[31]は、ブロックチェーンテクノロジーの最近の研究及びブロックチェーンをベースとするシステムに特有の制限に関し、包括的な概要が述べられているため、研究する際に有益な基準点となる。Yli-Huomo らの研究はすべてビットコインブロックチェーンについて考察した論文に焦点を当てたものであるが、述べられている研究結果は本考察に広く適応できる。主に使用した考察基準は Swan[29]より引用したものであり、同様に本考察にも適応可能である。

本研究では既存のブロックチェーンシステムにおける以下の 7 つの制限に焦点を当てる:

- スループット
- レイテンシ
- サイズとバンドワイズ
- セキュリティ
- 無駄なリソース
- ユーザビリティ
- バージョニング、ハードフォーク、マルチプルチェーン

スループット

ビットコインのような代表的なブロックチェーンは、取引認証に 10 分以上を要し、最大スループットは毎秒取引回数 7 回で、現状は毎秒 4 回程度である。イーサリアムは毎秒 10 回以上を処理可能で、認証時間はビットコインネットワークに比べ 10 倍速い。しかし、これらブロックチェーンのスループットのベンチマークとして VISA ネットワークと比較することで現在抱える制限が理解しやすくなる：VISA ネットワークは数秒で取引認証が可能で、毎秒平均取引回数 2,000 回、最大毎秒 65,000 回を処理する。[30]これらのメトリクスが、今日最も利用されているブロックチェーンネットワークにおけるスループットに関し、VISA のような従来の集中型決済ネットワークに大きく劣ることを示している。

ブロックチェーンネットワークのスループットを制限する主な要因は、ノード間のレイテンシである。ビットコインに採用される予定のライトニングネットワーク[22]、既にイーサリアムブロックチェーンのマイクロバージョンとして運用されているライデンネットワーク[23]など、この問題を解決する可能性のある試みはこれまでもあったが、現実的且つ長期的なソリューションにはまだ到達していない。

レイテンシ

上述の通り、ネットワークの最大スループットはノード間のレイテンシによって制限されるため、レイテンシとスループットは制限因子として密接に関係している。ノード間のレイテンシが高い場合、古いブロックでマイニングする可能性が高くなる。ビットコインネットワークを例に説明すると、各ブロックがノードの 50%に伝播する平均所用時間はたった 2 秒以下であり、約 13 秒後にはノードの 90%に伝播する(2017 年 4 月現在)[4]。イーサリアムでは、ノードの 50%に伝播する平均時間は 1 秒以下であり、約 10 秒後にはノードの 90%に伝播する[11]。

ビットコインでは、ブロックのマイニング時間とネットワーク伝播時間の比が大きいので、ノード間のレイテンシが大きな制限要素ではない。イーサリアムではブロック間の伝播時間がより短いので、無駄な時間がより問題視されがちである。しかしイーサリアムは、GHOST プロトコル [27]に基づくアルゴリズムを使用して、高レイテンシ、またはブロック間の伝播時間が遅いことにより生じる並列チェーンではなく、最長チェーン上でのマイニングを奨励している。

サイズとバンドワイズ

サイズとバンドワイズに関して以下の２点に注目して考察する必要がある。ブロックチェーン全体を表す物理データと、ネットワーク経由で送信される個別ブロックのサイズである。新しいブロックをマイニングしてブロックチェーンネットワークと関連させることができるフルノードの要件は、ブロックチェーン全体のローカルコピーを維持することであり、ローカル台帳を保管する為に必要なストレージ容量はチェーン上のブロック数と直接比例する。故に、もしブロックチェーンが非常に大きくなり、ごく少数のノードしかブロックを処理できなくなると、より強い中央集権に向かうリスクがある[15]。更に、利用可能なバンドワイズの制限を超える取引ボリュームになると、ブロックサイズにより課されるハードキャップと相まって、マイニング手数料が著しく高騰する可能性がある。その結果、より多くの取引を処理する為、ブロックサイズを大きくする、またはブロック伝播時間を短くする為のコアプロトコル変更に繋がる可能性がある。そして一般的に望ましく思われないが、最終的に必要なプロトコルアップグレードを実行するハードフォークをせざるを得なくなる。

セキュリティ

ハッキングされにくいという事が、プルーフオブワークブロックチェーンテクノロジーの最大のセールスポイントのひとつである。悪意のあるユーザーが既にブロックチェーン上に存在するデータを改ざんするには、当該ブロックだけではなく、関連する後続の全ブロックのプルーフオブワークをやり直す必要がある。確実に攻撃する為に必要なコンピューターリソースはネットワークの 51%のハッシュパワーと同等である為、「51%攻撃」と呼ぶ。しかし、ネットワークの 51%を所有して得られるマイニングの利益の方が、不正行為によって得られる利益よりも大きい為、現実には起こり得ないと考えられている。

次に考えられる攻撃はシビル攻撃と呼ばれる。シビル攻撃とは、悪意のある組織が複数の不正 ID をネットワーク上に存在させ、都合の良いようにネットワークを操作しようとすることである。ビットコインのようなプルーフオブワークを利用したシステムでは、新しいブロックを見つける為に使えるハッシュパワーによって、ネットワークに及ぼす影響力が決定する。つまり、異なる２つの ID のマイナーを装うとハッシュパワーも分割される為、結果としてメリットがないのである。

しかし、ブロックチェーンネットワーク上のユーザーの資金を攻撃する手段は、他にもいくつか存在する。大抵のユーザーは中央集権型取引所が発行するプライベートキーのストレージを安全であると信頼しているが、ハッキングされた場合、ウォレットへのアクセス情報及び保管している暗号通貨が盗まれる可能性がある。

ブロックチェーンスペースのもうひとつのセキュリティリスクは、スマートコントラクトの実装時に発見されるコーディングエラーである。特に有名で且つうまくスマートコントラクトを悪用された事例としては、2016 年 6 月 17 日に起こった「The DAO 事件」として現在知られている。攻撃者はスマートコントラクトに実装されているコードの小さな欠陥を利用して、約 50 億~60 億円相当のイーサを獲得した。そして最終的には、議論の的となるハードフォークに繋がり、イーサリアムのネットワークが 2 つに分岐、イーサリアムクラッシックが生まれる結果となった。[2]

無駄なリソース

ビットコインブロックチェーンによる電力、更には環境への影響は非常に大きい。現在、ひとつの取引を認証する為に必要な電力は 249kWh であり、継続的にビットコインブロックチェーンに新しいブロックを追加しているマイナーが年間に使用する電力は 32TWh を超えると推定される。[6] イーサリアムの方が利用者は少ないが、エネルギー消費量、そして環境へのインパクトは大きい。[7]実際、ビットコインとイーサリアムネットワークを両方維持する為に必要な電力量を合わせると、ニュージーランド全土の年間電力使用量に匹敵する。現在プルーフオブワークブロックチェーンから移行する動きがあり、イーサリアムのプルーフオブステークへの移行発表が最も有名である。

ユーザビリティ

ビットコインブロックチェーン上では、ブロックの一部として約 10 分毎に取引は公開されるが、各取引が公開した後に認証が可能になるまで通常 50 分またはそれ以上待つのが通常である。これを現実に例えると、お店で食料品を選び、支払いが処理されるまで 1 時間並んで待つようなものである。このような現状では、明らかに現実的な使用事例にはなりえない。

次に、ビットコインや多くの暗号通貨で特有な懸念点として挙げられるのは、匿名性、またよくあるケースとして偽名利用の点である。取引は公開され、ブロックチェーンの全参加者と共有されるが、アルゴリズムがユーザーの「プライベート」取引から取引データを抜き出してデータ分析することが可能な事も踏まえた上で、取引は慎重に行う必要がある。実際の例とし

て、ユーザーが母親にお金を送金する場合を想定すると、取引情報に基づき以下の情報が確認できる：1) 現在各ユーザーが送金、そして受領したビットコインの量、及び各アドレスの全取引履歴、2) 履歴の各時点での各アドレスの残高、3) 各ユーザーが資金を送金、または受領したことのある他の相手のアドレス。基本的に、取引の送金者と受領者は他者の資金移動履歴を見ることができ、特定のアドレスと個人をリンクすることができれば、購入した物、賭けた物、誰が「匿名の」サポートを受けたか等も知ることができる。アメリカの FBI が既に何度も証明しているが、実際ビットコインは完全に匿名ではない。おそらく多くのユーザーにとって、経済状況の透明性はビットコインを利用する際の最も大きなデメリットのひとつであるが、問題解決策が研究されている。例えば、ZCash に組み込まれているプライバシーメカニズムであるzkSNARKS[24](ゼロ知識暗号化)などのソリューションが生まれ、Metropolis (Byzantine) アップグレード時にイーサリアムに導入されている。

バージョニング、ハードフォーク、マルチプルチェーン

ブロックチェーンの分岐の主な問題は、コンセンサスとセキュリティの喪失である。極端であるが、全世界で利用可能な計算能力の 100%を使用する非常に拡張したブロックチェーンと、利用可能な計算能力の 1%を必要とする異なる 100 のチェーンを例として比較する。

最初の例の場合、51%攻撃は公正なノードで維持されたチェーンを上回るため使用可能な計算能力の 51%を保持する必要があるが、分裂したケースでは、全世界で利用可能な計算能力の 0.51%だけで各チェーンを改ざんできる。

ブロックチェーンは、公正なノードの計算能力の合計が不正なものよりも上回ることで保持される、というコンセンサスに基づいている。分岐によりチェーンが分裂し計算能力が減少すると、最低限必要なリソースが少なくなるため攻撃は成功しやすくなる。

ハードフォークは、一般的には望ましくないが、プロトコルコンセンサスが喪失したことが原因で生じることが多い結果のひとつである。ブロックチェーンエコシステムのステイクホルダー間で生じるイデオロギーの違いが、チェーンの分裂や分岐の原因となることがある。最も有名な事例が、ビットコインのスケーリング問題、及び迅速で安い電子キャッシュ手段として利用できないことによるビットコインキャッシュの分離と、先に述べた、ブロックチェーンの原則は変わらずにイーサリアムから分岐したイーサリアムクラッシックがある。ハードフォークは常に議論を引き起こす訳ではなく、2017 年のイーサリアム Metropolis アップグレードのようにブロックチェーンシステムのコアプロトコルを変更する為に行われる場合も多い。ハードフォーク後は、オリジナルチェーンに適応されたハッシュパワーが全てそのままである場合もあるが、イデオロギーに関連するハードフォークの場合、競合する 2 つのチェーンに分裂するため、セキュリティは低下し攻撃されやすくなる。

INFINITY プロジェクト - コアゴール

INFINITY プロジェクトを構築において、以下重要な 2 点について取り組んだ:

✓ 現在既存の暗号通貨が持つ制限に対し、何が市場のニーズやウォンツであり、どのようにソリューションを提供できるか？

✓ 暗号通貨がより広く採用されて経済活動に組み込まれる為には、どのような特性が必要か？

これらの点を念頭に置いて、ビットコイン、イーサリアム、今後伸びていく可能性のある様々なアルトコインを含む既存のブロックチェーンの徹底分析を行い、各プロジェクトの長所と短所を明らかにしようとしが、上記に挙げた 2 点に完全に対応できるプロジェクトを見つけることは困難であった。

従って、INFINITY プロジェクトチームとして目的達成の為、より多くの現実的なケースに適応できる新しいテクノロジーとアルゴリズムの研究に着手した。同時に INFINITY プロジェクトの基本フレームワークの設計を開始し、以下の通り５つのコアゴールを設定した：

INFINITY プロジェクト **-** コアゴール

1. 暗号通貨に対する実際の市場ニーズの確認
2. 適応性のある暗号通貨の開発
3. ユーザー主体のブロックチェーンプラットフォームの創造
4. 適応性のあるイノベーションを促進するエコシステムの開発
5. 暗号通貨の分散型取引手段の調査

コアゴール **1 -** 市場ニーズの確認

最近、数多くのブロックチェーンプロジェクトが大きく注目されているが、世界規模で電子商取引に浸透している暗号通貨は存在しない。より正確には、多くの暗号プロジェクトと現実のソリューションには依然大きな隔たりがある。現在、暗号通貨の受け入れや採用がオンライン業者の非常に小さいグループやごく少数のその他サービスに限定されている理由は、事実上デジタル通貨の選択肢としてビットコインやその他既存の暗号通貨に完全に頼ることが不可能だからである。

これを克服して使用事例や採用を増加、そして促進させる為、特定分野やコミュニティの専門家及びディベロッパーと共同作業を行い、全てのユーザーに有益で市場に適した通貨開発の成功を目指す。

INFINITY プロジェクトチームが提起した重要な 2 点のひとつである「市場が求めているユーザー主体の通貨とは何か？」に答える為に、市場と開発の相互観点から理想的なソリューションとなる、必要なコアブロックチェーンテクノロジーを定義しなければならない。よって

INFINITY プロジェクトチームは、新しい暗号通貨を開発する際の最初の主要成功要因 (KSF) を、市場が求める現実的なソリューションを提供する事を前提とした設計及び実装、と位置付けた。

コアゴール **2 -** 適応性のある通貨

INFINITY プロジェクトチームは、既存の暗号化プロジェクトの多くで採用されているモノリシック通貨開発という従来の観点から脱却し、多様な通貨モデルを組み込むことができる適応性のある実装プラットフォームのコンセプトを導入するとした。

このコンセプトをさらに発展させ、「Hyper-connected Coin」(HYCON)を考案した。このコインは初めから、高速、安価、スケーラブル、安全に配慮し、様々な現実的シチュエーションで採用及び使用できるように設計されている。

基礎となる INFINITY ブロックチェーンは、互換性のあるモジュール構造で設計されており、特定のニーズに合わせた基礎テクノロジーの採用や変更を容易にする。

コアゴール **3 -** ユーザー主体のプラットフォーム

おそらくビットコインが起こしたパラダイムシフトの最も重要な点のひとつは、安全で分散的な電子価値交換を促進したこと、つまり誰でも利用できるよう公開し、銀行を経由せずに支払いを行うという、これまで非現実的だった概念の新たな扉を開いたことである。

しかし、多くの暗号通貨の概念レベルから実際の UI 及び UX に至るまで途方もなく高いラーニングカーブが、より幅広い分野での適応性を妨げる主なハードルのひとつとなっている。INFINITY プロジェクトでは、より簡単で使いやすいプラットフォームに加え、直感的に使えるウォレットと相互作用する取引プラットフォームを提供し、これらのハードルを下げていく。最終的な目標は、より多くの人がこのブロックチェーンテクノロジーの起こしたパラダイムシフトの恩恵を活用できるようにすることである。

コアゴール **4 -** 適応性のあるイノベーション

INFINITY プロジェクトの開発に際し最も重要な側面のひとつは、どうやってより多くの人々、企業、政府、NGO などに対してブロックチェーンテクノロジーの活用を促進するかであった。従って INFINITY プロジェクトチームは、既存の多様なブロックチェーン、プラットフォーム、暗号通貨の研究から考案された、適応性のあるブロックチェーンプラットフォームコンセプトである INFINITY プラットフォームの導入を研究している。

INFINITYプラットフォーム研究の目的は、直感的に使用でき多様な手段に実装できるプラットフォームを創造することである。 INFINITYプラットフォームの使用例としては以下が含まれる。高速で安価に使用できる価値交換手段である HYCON に基づく安全な暗号通貨の実装；情報セキュリティを強化し、より効率的なデータのストレージとトランスミッションを促進する分散型企業台帳の創造；証券取引所への暗号化セキュリティの導入。今後新たな使用事例やINFINITYプラットフォームを使用したイノベーションの範囲は幅広く、これからのユーザーが必要とするブロックチェーンソリューションの柔軟性に十分対応できる。

コアゴール **5 -** 安全な分散型取引所

INFINITY プロジェクトで積極的に行われている研究分野は、ユーザーに分散的な方法で異なる暗号通貨に交換できる機能を提供することである。現在の取引所は、安価で迅速に暗号通貨取引を行う為に中央集権的方法に依存しているが、この場合ユーザーは所有している従来通貨及び暗号通貨を中央集権取引所に委託することになる。

残念なことであるが、大量の取引がこれらの取引所を経由しているにも関わらず、これらの取引を実行するソースコードは公開されていないことが多く検証することができない。実際悪意のある操作により、取引所からユーザーの暗号通貨が盗まれるという事件は世界中でたくさん起きている。今日の中央集権取引所に保管されているユーザーの資金と情報は、今後も狙われる可能性がある。

INFINITYプロジェクトの今後の研究の一部として、真の流通貨幣を目指して HYCON にアトミックスワップの概念を融合する予定である。HYCON を経由し他の様々な暗号通貨と取引可能となり、取引手数料はネットワークを保護するマイナーに分配される。アトミックスワップにより相手の暗号通貨支払いが証明されるまで HYCON のエスクローを保留することができるため、HYCON や他の暗号通貨の P2P 取引の信用リスクを補うことができる。

HYCON TECHNICAL 技術仕様書

特性	仕様
ハッシュ関数	Blake 2b
コンセンサスプロトコル	SPECTRE
チェーン構造	有向非巡回グラフ(DAG)
ブロック速度	1000ms
マイニング方式	PoW

BLAKE 2B ハッシュアルゴリズム

BLAKE ハッシュ関数は、SHA-3 基準を指定した NIST ハッシュ関数コンテストの最終選考に残った。[1] BLAKE ハッシュ、特に後続するバリアント (2b, 2s)はマルチコアプロセッサ向けに最適化され、同等の安全性を保持しながら毎秒より多数のハッシュ化が可能である。

コンセンサス - SPECTRE プロトコル

ビットコインブロックチェーンのコンセンサスに利用されているナカモトプロトコルに対して、HYCON はコンセンサスを保持する為に SPECTRE と呼ばれるプロトコルを実装している[26]。SPECTRE は、対をなす取引であることを確認する為のブロックペア間の投票アルゴリズムを採用して、ブロックチェーンを有向非巡回グラフ(DAG)の形式へ、すなわちブロック x < ブロック y または ブロック y < ブロック x へと一般化する。SPECTRE プロトコルの全説明はホワイトペーパーの範囲を超えてしまう為、投票ルールの基本概要を以下に示す。

投票ルール

SPECTRE の投票ルールは、プロセスを視覚的に表示したものを参照すると理解しやすくなる。また投票はノード間でやりとりされることはなく、投票への参加を明示する必要もないことも補足する。むしろ投票はブロックにより行われ、投票方法はブロックの DAG 構造で決定する。

SPECTRE の投票プロセスに利用される基準は以下の通りである; 重要な概念は過去(x)と未来(x)であり、x から接続可能なブロックと先に存在したブロックとして x を参照するブロックである。さらに具体的に述べると、x が過去(y)の場合ブロック y は未来(x) である。また、バーチャル(G)というバーチャルブロックは、DAG 全体を過去とする仮定に基づいたブロックである。

ブロック z は、ブロック x か y に投票する：

1. z が 未来(x) にあるが未来(y)にない場合、x を選択して投票する。
2. z が未来(x)と未来(y)にある場合、過去(z)のバーチャルブロックの投票に基づく予測で再帰的に投票する。
3. z が未来(x)にも未来(y)にもない場合、ブロックの集まりである未来(z)の過半数の投票に基づき投票する。
4. z が過去(バーチャル(G))のバーチャルブロック、つまり過去=DAG 全体の場合、DAG の過半数投票に従って投票する。
5. z=x または z=y の場合、y が未来(x)でない、またはその逆という前提で、自身が正しいと投票する。

SPECTRE プロトコルを DAG 事例へ適応

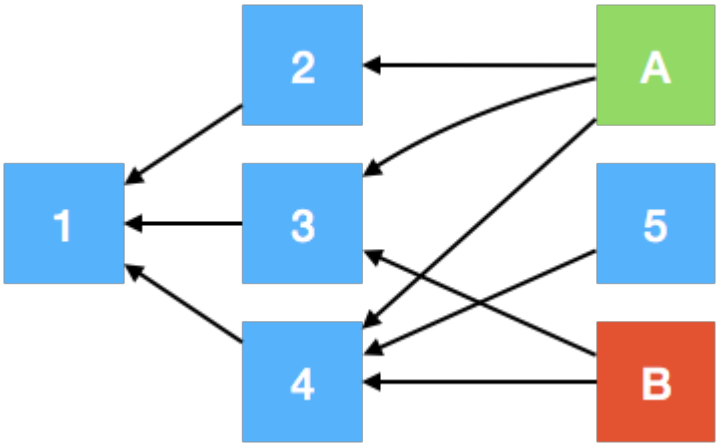
SPECTRE の適応を事例と投票プロセスの進行状況の図を用いてプロトコルの動きを段階的にわかりやすく説明する。特定の事例は SPECTRE ホワイトペーパーから直接引用した。[25]

事例 - 二重支払い

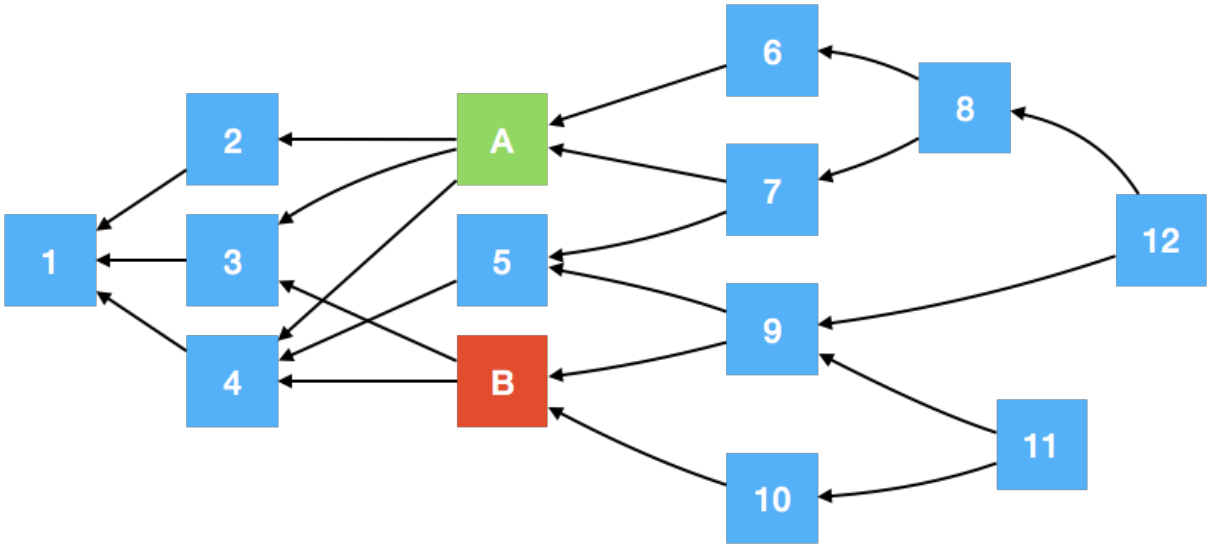
取引 t1 を含むブロック A と、対立する取引 t2 を含む 2 番目のブロック B による最も単純なケースについて考察する。これらの対立は、悪意のある操作、または単に異なるマイナーが同じ取

引手数料を回収しようする場合など、ノード間のレイテンシにより取引が 2 回公開された場合が考えられる。2 つのブロックは異なる過去と未来を持つため、DAG の構造によって二重支払いは別に解決される。

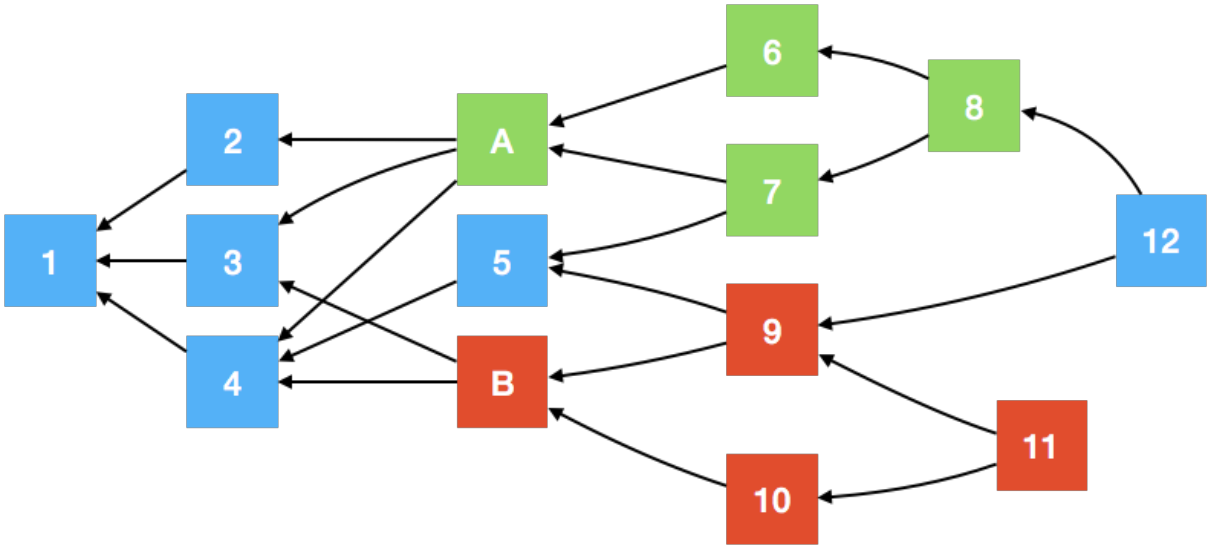
本例では、以下に示す通りブロックＡとブロックＢはブロック５とほぼ同時に公開される。



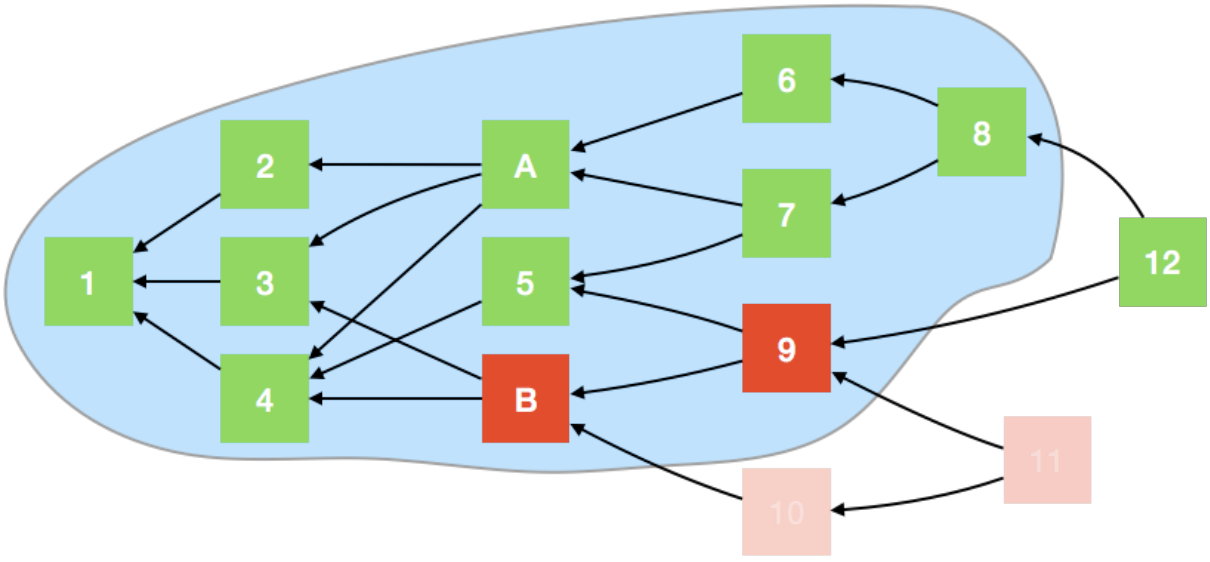
この段階では、対立する両ブロックを参照する後続のブロックが公開されていないため、システムは二重支払いを認識していない。しかし、DAG 構造が展開してブロックが追加されると二重支払いが発覚し、どちらのブロックが先であるか確定する為に DAG 構造の分析が行われる。



上図では、ブロック 12 は AB 間の二重支払いを認識した最初のブロックである。上述のルールに従って投票は以下のように集計する。ブロック 6、 7 、8 は、ブロック B が過去に存在しない為ブロック A に投票する。同様に、ブロック 9、10、11 は、同じ理由でブロック B に投票する。



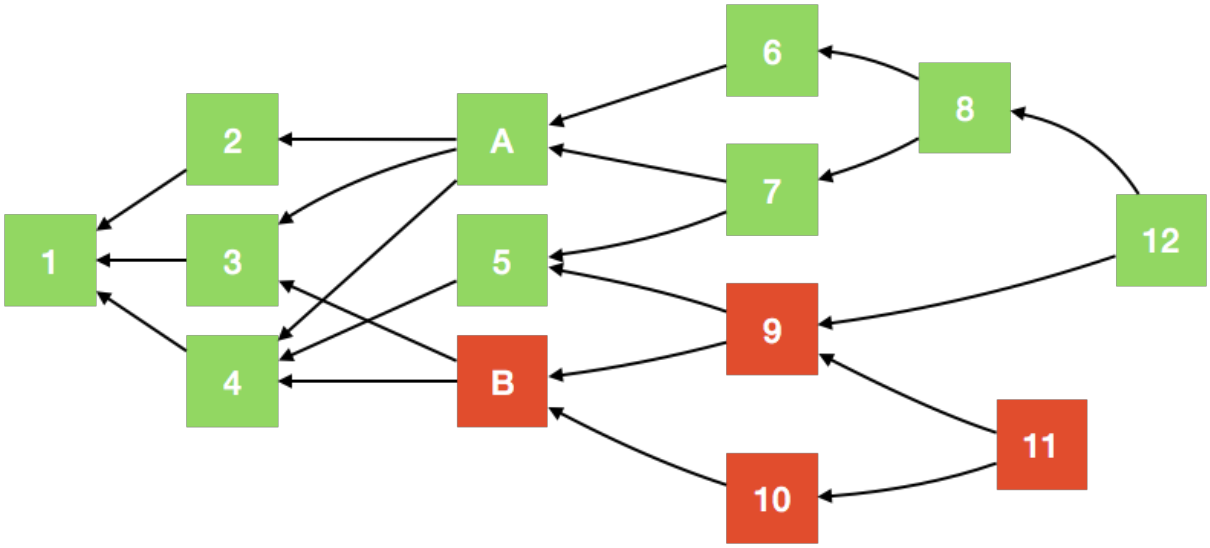
ブロック 12 は過去の再帰呼び出しに基づき投票する。ブロック 10 と 11 は過去(12)に含まれない為、ブロック 12 の投票に影響しない。ブロック 12 の投票範囲を以下に示す。



ブロック 1 - 5 は未来(A)にも未来(B)にも存在しないので、各々の未来の多数決と同様に投票する。再帰的な投票の場合、これらのブロックは全て、未来にブロック A に対しより多くの票を有するので、ブロック A に投票することになる。ブロック 12 の過去はブロック A に対する 9 票とブロック B に対する 2 票を含むので、ブロック 12 はブロック A に投票する。票が同数だ

った場合、ブロック 12 が決着を付け、全サーバーがブロック 12 の投票を認証できるようになる。過去(12) だけが 12 の投票を判定できるので、その投票が覆ることはない。

DAG の投票プロセスの続きは残りのブロックの未来次第である。ブロック 12 の投票が認証されると、7、8、12 の投票が 9、11 の投票を上回ったためブロック 5 は A を選んで投票する。ブロック 4 は、ブロック A、5、6、7、8、12 が A に投票し、ブロック B、 9、10、11 が B に投票したことから A に投票する。ブロック 3、 2、1 の場合も同様に A に投票する。この投票手順により、最終的に A が 10 票、B が 4 票となる。



特にここで説明した様な単純なケースにおける SPECTRE の興味深い特徴は、他のブロックチェーンテクノロジーに使われている最長チェーンを採用するモデルが再現されていることである。1 -> 12 のルートで A を通過する場合と、同じルートで B を通過する場合を比較すると、1 -> A -> 12 のルートは 1 -> B -> 12 のルートより長い。つまり、長い方のチェーンが勝つのである。

DAG と ブロックチェーンの比較

ブロックチェーンの代わりに DAG を使うメリットは第一にスピードである。既存のブロックチェーンの場合、前のブロックのハッシュを参照して、新しくマイニングされたブロックはブロックチェーンの最後尾に接続されるが、DAG に新しく追加されるブロックは現在の DAG の複数の先端を参照する。この仕組みにより、チェーンが分岐するリスクなく異なるノードから同時にブロックが公開できる。新しいブロックは複数の前歴を同時に追加することが出来るため、マイナーはブロックが孤立する心配をすることなく、マイニング報酬を得ることができる。問題が起こるとすれば、ノードが同時に別の場所で取引を公開した時であり、二重支払い

に繋がる可能性がある事である。SPECTRE を使うと、どのブロックも孤立することなく、どの取引が拒否されたかのコンセンサスを得ることが可能である。

INFINITY SPECTRE 実装

SPECTRE の投票手順には十分なリソースが必要である為、実装には慎重な管理が必要である。最初のプロトタイプは開発の利便性のため Python で書かれていたが、INFINITY SPECTRE 実装の最終版は、C、C++、Rust などの言語で書かれ、データ構造とメモリ管理の完全な制御が維持でき、より良いパフォーマンスが可能である。

ネットワークインフラ - Node.js, Typescript

この設定をシステム構成に使用するメリットは、非同期動作を可能にする Node.js の組み込みサポートである。Node.js によりクロスプラットフォーム「ノンブロッキングイベント I/O」が可能になり、個々のコンポーネントが通常の一連操作から外れた操作の結果を待つことができるのである。待機中のコンポーネントは、実行を許可する他のコードをネットワークからメッセージを受信する、またはユーザーが入力するなど、特定のイベントが発生した場合にのみ作動する。 [20]
強力な型検査の結果、Javascript を基礎とする Typescript の使用が決定した。Javascript の型付け版を使用することで、明確に定義されている型によって単純なプロセスをデバッグしつつ、開発チームは Node.js が提供する非同期性を活用したプラットフォームを構築することができた。Typescript ファイルは実行する前にコンパイルが必要であるが、多くのシンタックスエラーやタイプエラーはコンパイルの段階で簡単に見つけることができ、Javascript アプリケーションのデバッグプロセスで通常行われるような入り組んだコールバックを手順を踏んで探らなくてもよい。

シリアライゼーション - プロトコルバッファ

ブロックチェーンシステムでは、ネットワーク上に任意の時点で任意の数のメッセージが存在する。そこで、ノードソフトウェアがそのデータを一貫性のある正しい方法でデコードできることが重要である。Google が開発したプロトコルバッファ[14]を使用することで、異なるプラットフォームで使用できる一貫性のあるメッセージ定義が可能になり、INFINITY ブロックチェーンを実行するノードを複数のプログラム言語で開発することができる。シリアライゼーションレイヤーは言語にとらわれない為、クロスプラットフォームアプリケーションで非常に使いやすい。プロトコルバッファも後方互換性と前方互換性があるため、アップデートの際にハードフォークよりもソフトフォークだけで済む可能性が増す。更に、他の開発者と HYCON ネッ

トワークを通じて協力することができるので、第三者ソフトウェアにも容易に互換性を持たせることができる。

マイニング

ブロックを公開するには、現存する大多数の暗号通貨と同様にプルーフオブワークが必要である。マイナーは、DAG 先端のハッシュ、ブロックに含まれる取引のマークルルート、現在の難易度を超えるハッシュが計算されるまで置き換わるノンスに基づき、次のブロックのハッシュを計算する。SPECTRE の考案者は、このプロトコルを使えば毎秒 10 ブロックが実行可能であると述べているが、HYCON はまず毎秒 1 ブロックを目標にする。現在のプロトタイプではプルーフオブワークを使用しているが、ビットコインやイーサリアムのネットワークを保護する為に大量の電力を消費することがわかっているため、代替案を検討している。あまり有名ではない方法だが、マイナーが大量のデータを事前に計算して保管しておき、必要なソリューションをそのファイルから探して現在の課題を克服する方法である、プルーフオブスペース[32]が候補として挙がっている。この場合ほとんど電力を使わず、バーストコインとスペースミントで既に効果が実証されている。

同期

HYCON はネットワークの初期同期の際にヘッダーファーストアプローチを採用する。最初の起動時とその後に続く起動時に、特定のブロックの高さ(現在はローカルデータベース内の最大のブロックの高さで格納されている)に続く、ブロックの高さを含んだヘッダーの数を確認するメッセージが接続されているピアに送信される。これらのヘッダーを受信するとブロックが認証され、もしローカルデータベースから欠落している場合、接続されたピアから全ブロックデータが要求される。受信したブロックは受信時に再び検証され、認証された場合はデータベースに追加される。ブロックは親ブロックがこのプロセスに含まれる場合にのみデータベースに追加される為、必ず逐次プロセスとなる。

結論

本ホワイトペーパーの考察は、INFINITY プロジェクト全体の基盤となる既存の暗号通貨の限界を調査検討することから始まった。INFINITY プロジェクトのビジョンは、幅広い分野への適応を可能にするべく、高速、安全、スケーラブルで且つユーザー主体のブロックチェーンと暗号通貨エコシステムを提供することである。当社は、SPECTER プロトコルと BLAKE-2b ハッシュアルゴリズムの組み合わせを通じて、安全かつ迅速に処理される新しい暗号通貨を提案す

る。上述の手段を適応することにより、HYCON という暗号通貨と INFINITY プロジェクトは、グローバル暗号通貨業界に有益で他にはない付加価値を提供する。

参考文献

[1] Blake2.net. (2017). BLAKE2. [online] Available at: https://blake2.net/ [Accessed 16 Oct. 2017].

[2] CoinDesk. (2016). Understanding The DAO Attack - CoinDesk. [online] Available at: https://www.coindesk.com/understanding-dao-hack-journalists/ [Accessed 20 Nov. 2017].

[3] Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G. and Song, D., 2016, February. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security (pp. 106-125). Springer Berlin Heidelberg.

[4] Decker, C. (2017). BitcoinStats. [online] Bitcoinstats.com. Available at: http://bitcoinstats.com/network/propagation/ [Accessed 10 Nov. 2017].

[5] Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on (pp. 1-10). IEEE.

[6] digiconomist.net. (2017). Bitcoin Energy Consumption. [online] Available at: https://digiconomist.net/bitcoin-energy-consumption [Accessed 16 Nov. 2017].

[7] Digiconomist. (2017). *Ethereum Energy Consumption Index (beta) - Digiconomist*. [online] Available at: https://digiconomist.net/ethereum-energy-consumption [Accessed 8 Dec. 2017].

[8] The Economist. (2007). The end of the cash era. [online] Available at: http://www.economist.com/node/8702890 [Accessed 27 Sep. 2017].

[9] Ethereum Blog. (2014). Toward a 12-second Block Time - Ethereum Blog. [online] Available at: https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/ [Accessed 27 Sep. 2017].

[10] Etherscan.io. (2017). Ethereum Average BlockSize Chart . [online] Available at: https://etherscan.io/chart/blocksize [Accessed 16 Nov. 2017].

[11] Ethstats.net. (2017). Ethereum Network Status. [online] Available at: https://ethstats.net/ [Accessed 16 Nov. 2017].

[12] Goland.org. (2017). How to make block chains strongly consistent – Stuff Yaron Finds Interesting. [online] Available at: http://www.goland.org/why_block_chains_are_strongly_consistent/ [Accessed 27 Sep. 2017].

[13] Goland.org. (2017). The block chain and the CAP Theorem – Stuff Yaron Finds Interesting. [online] Available at: http://www.goland.org/blockchain_and_cap/ [Accessed 27 Sep. 2017].

[14] Google Developers. (2017). Protocol Buffers | Google Developers. [online] Available at: https://developers.google.com/protocol-buffers/ [Accessed 20 Oct. 2017].

[15] James-Lubin, K. (2015). Blockchain scalability. [online] O'Reilly Media. Available at: https://www.oreilly.com/ideas/blockchain-scalability [Accessed 16 Nov. 2017].

[16] Koteska, B., Karafilovski, E. and Mishev, A. (2017), Blockchain Implementation Quality Challenges: A Literature Review : Proceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications, Belgrade, Serbia, 11-13.9.2017.

[17] Malanov.A, (2017). Six main disadvantages of Bitcoin and the blockchain. [online] Kaspersky.com. Available at: https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/ [Accessed 16 Nov. 2017].

[18] Motherboard. (2017). One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week. [online] Available at: https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change [Accessed 20 Nov. 2017].

[19] Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

[20] The NodeSource Blog - Node.js Tutorials, Guides, and Updates. (2014). Why Asynchronous?. [online] Available at: http://nodesource.com/blog/why-asynchronous/ [Accessed 16 Nov. 2017].

[21] Park, J.H. and Park, J.H., (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry, 9(8), p.164.

[22] Poon, J. and Dryja, T.. (2016). The Bitcoin Lightning.network [online] Available at: https://lightning.network/lightning-network-paper.pdf.

[23] Raiden-network.readthedocs.io. (2017). Raiden Specification — Raiden Network 0.2.0 documentation. [online] Available at: https://raiden-network.readthedocs.io/en/stable/spec.html [Accessed 7 Dec. 2017].

[24] Reitwiessner, C. (2017). zkSnarks in a Nutshell [online] Available at: http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf [Accessed 23 Nov. 2017].

[25] Sirer, E.G. and Song, D., 2016, February. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security (pp. 106-125). Springer Berlin Heidelberg.

[26] Sompolinsky, Y., Lewenberg, Y. and Zohar, A., 2016. SPECTRE: A Fast and Scalable Cryptocurrency Protocol. IACR Cryptology ePrint Archive, 2016, p.1159.

[27] Sompolinsky, Y. and Zohar, A., 2015, January. Secure high-rate transaction processing in bitcoin. In International Conference on Financial Cryptography and Data Security (pp. 507-527). Springer, Berlin, Heidelberg.

[28] Son, M. (2017). Bitcoin's Rise Happened in Shadows of Finance. Now Banks Want In. [online] Bloomberg.com. Available at: https://www.bloomberg.com/news/articles/2017-10-05/bitcoin-s-rise-happened-in-shadows-of-finance-now-banks-want-in [Accessed 7 Dec. 2017].

[29] Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[30] VISA (2017). Visa Inc. Facts & Figures . [online] Available at: https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-facts-figures-jan-2017.pdf [Accessed 20 Nov. 2017].

[31] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), p.e0163477.

[32] Dziembowski, Stefan; Faust, Sebastian; Kolmogorov, Vladimir; Pietrzak, Krzysztof (2015). "Proofs of Space". 9216: 585–605.
Available at: https://eprint.iacr.org/2013/796.pdf