2018 年 5 月

ポジションペーパー

2.1 版

目次

・

1. 要約

言語がスピーチを意味するのと全く同じように、通貨は経済を意味する。つまり、それは自然界で歴史的に起こってきた競争、借用機能、移動（翻訳）することで失われるものである。言語は、ユーザーの数とそれに付随する発音/読み書きされるもの量に直接比例して変化する。つまりそこには「トランザクション」が存在する。 それを生かし、絶滅から救うためには、それを循環させ、変化に適応するダーウィニズム的能力が必要である。ほとんどの方言が時間とともに定式化され、徐々に定着していったのと同じように、ほとんどの伝統的な通貨は自然に発達してきた。構築された言語は、世界的に成功すると言われていたにもかかわらず、うまく設計された機能や不規則動詞のようなものがないため失敗してしまった。

今や仮想通貨とブロックチェーンの世界に突入し、変化に適応する能力によって、プラットフォームがトランザクションの優先手段になることは明らかになりつつある。多くの既知のブロックチェーンは堅牢で不器用な設計であるが、Enecuum のプラットフォームは高度な適応性があり、真に分散化されており、参加者はプロトコルの変更をしなくても、望むままに新しい変更を選ぶことができる。ただし、必要に応じて、ブロックチェーンパラメータの変更は、修正されたプロトコルバージョンを使って導入することもできる。 以下のすべての技術的な説明は基本的に同じ考え方に則っている。つまり、我々は、プライバシー、セキュリティー、スケーラビリティの強化を信じ、さらに重要なことに、Enecuum を今後のブロックチェーンに変え、適応させる能力があると考えている。

It is being BUILT TO LIVE ON.

2. 免責事項

このホワイトペーパーおよびこのホワイトペーパーに関連して発行されたその他の書類は、Enecuum プラットフォーム（「Enecuum」）の意図された開発及び使用に関係している。これらは情報提供のみを目的としており、変更される可能性がある。

- **このホワイトペーパーにおける将来のプロジェクトについての説明**

このホワイトペーパーには、Enecuum HK Limited、香港有限会社(CR: 2562183)（以下「**当社**」）の理念に基づく将来的記述、ならびに当社が入手した情報による前提が含まれる。

このホワイトペーパーで想定されている Enecuum においては、主要なガバナンスや技術的機能を含むが、これに限定されないものが常に開発されており、更新されている。ENQ トークン（「**ENQ**」）は、実験プラットフォーム（ソフトウェア）の開発と使用を含み、かつそれに関連される、機能しない、もしくは目標が実現されない可能性のある技術もこのホワイトペーパーで規定される。

Enecuum が完了した場合、このホワイトペーパーに記載されているネットワーク設定と大幅に異なる可能性がある。この文書におけるいかなる計画、将来の見通しまたは見通しの達成または妥当性についての表明または保証はなく、この文書におけるいかなるものも将来の約束または表現に依拠していない。

- **規制された製品の不提供**

ENQ は、管轄区域内のセキュリティー、またはその他の規制製品となることを意図しない。

この文書は、セキュリティーまたはその他の規制製品の提供または勧誘、投資目的での宣伝、誘導、または勧誘を含まない。購入条件の文書は、ファイナンシャルサービスの提供用の文書、またはあらゆる種類の趣意書ではない。

ENQ は、プラットフォームまたはソフトウェア、または当社または他の企業またはプラットフォームに関連する知的財産、管轄内におけるその他の公的または民間企業、財団またはその他の法人における有価証券、株式、ユニット、ロイヤリティまたは資本、収益、利益または収入に対する権利を表すものではない。

- **このホワイトペーパーはアドバイスではない**

このホワイトペーパーは、ENQ を購入するためのアドバイスではない。契約や購買決定に関連して頼るべきではない。

- **リスク警告**

ENQ の購入と Enecuum への参加には、大きなリスクが伴う。

ENQ を購入する前に、他の文書に記載されているリスクを含め、リスクを慎重に評価し、考慮する必要がある。

- **当社の見解**

このホワイトペーパーに記載されている見解や意見は、Enecuum の見解と意見であり、いかなる管轄区域内の政府、準政府機関、行政機関、公的機関（管轄区域内の規制当局を含むがこれに限定されない）の公式の政策または地位を反映していない。

このホワイトペーパーに記載されている情報は、当社が信頼できると判断した情報に基づいているが、その正確性や完全性についての保証はない。.

- **英語がこのホワイトペーパーで認定された言語である**

このホワイトペーパーおよび関連資料は英語のみで発行されている。翻訳は参考目的のみであり、当社または他の人物によって認定されていない。翻訳の正確さと完全性について保証することはできない。このホワイトペーパーの英語版と翻訳版との間に矛盾がある場合は、英語版が優先される。

- **サードパーティーの提携または承認**

このホワイトペーパーにおける特定の企業およびプラットフォームへの言及は、例示目的のみのものである。任意の会社名および/またはプラットフォーム名および商標の使用は、それらの当事者のいずれかとの提携または保証を意味するものではない。

- **全ての必要な専門的アドバイスを取得する必要がある**

ENQ を購入するか、Enecuum ネットワークへの参加を決定する前に、必要に応じて弁護士、会計士、税務専門家および/またはその他の専門顧問に相談する必要がある。

3. 導入

2009 年 Bitcoin の創業以来、その基盤となるブロックチェーン技術は新しい世界経済の発展の展望を開いた。その後のスマートコントラクトの出現により、あらかじめ決められた条件での信頼性の高い自動取引が容易になり、この技術のアプリケーション潜在力が大幅に拡大した。ブロックチェーンは、貿易、金融市場、投票、さらには物流など、金融および経済活動の多くの分野に革命を起こすことができると確信している。

今日、ほとんどすべての主要機関が最高のソリューションを開発するために競争している。大手銀行と企業はコンソーシアムを形成しており、政府はこの技術をサポートするための適切な法的枠組みを作成する方法を模索している。

既存のソリューションと Ethereum が最も顕著なのは、すでにスマートコントラクトと組み合わせてブロックチェーン技術を適用するための十分な機会を提供していることである。それにもかかわらず、技術のさらなる開発と大衆化のためには、スケーラビリティ、セキュリティー、プライバシーという 3 つのカテゴリに分類される多くの問題を克服する必要がある。

3.1. スケーラビリティ

分散型ブロックチェーンシステムの欠点は、帯域幅が限られていることである。実際、分散台帳で利用されている既存のコンセンサス構築メカニズムのほとんどは、1 秒間に多数のトランザクションとネットワーク集中化の度合いとの間でトレードオフをしている[1]。したがって、処理されるトランザクションの数を増やしたいという要望は、しばしば、システムの信頼性へのリスクを増大させる。さらに、ブロックチェーンのサイズが大きくなるにつれて、より多くのディスクスペース、強力なインターネット接続、高い計算能力が必要になる。これらによって、フルノードの数が減少し、ネットワーク全体のセキュリティーに悪影響を及ぼすことがある(参照 5)。

3.2. セキュリティー

スケーラビリティに関連する問題に加えて、ブロックチェーンアーキテクチャ自体のさまざまな機能によって生成される多数の脅威がある。たとえば、PoW のトランザクション確認メカニズムは、一ヶ所でマイニング能力が高度に集中する可能性がある。たとえば、電気代が最も安い中国本土でビットコインのマイニング能力が集中しつつある。

この事実は、例えば「51%攻撃」を行う機会など、システムの集中化に伴うさまざまなリスクを大幅に増加させる。.

セキュリティーに対するもう一つの脅威は、ブロックチェーン自体よりも脆弱性やバグの影響を受けやすいスマートコントラクトに関連して発生し、ユーザーに数百万ドルの損失をもたらし、業界に損害を与えたこともある。我々は、スマートコントラクトの使用数は増え続けると予想しているが、弱点を特定する既存の方法はまだ不十分である。

最近の別の重要な問題は、集中化がブロックチェーンの方向性とコントロールに及ぼす影響である。これは、コアプロトコル[2]に修正を加えることができる少人数のグループの手に権限が集中する場合に発生する可能性がある。これらのグループの意見がコミュニティの利益に反する場合、安定した開発に必要なシステムの近代化プロセスを完全に麻痺させる紛争につながる可能性がある。またコミュニティとブロックチェーンの分裂につながる可能性がある(参照. 5)。

3.3. プライバシー

一部のブロックチェーンシステムは、すべてのトランザクションの透過性を目指している。しかし、この機能は商業的魅力を制限し、個人のプライバシーを侵害すると我々は考えている。分散型レジストリの主なメリットの 1 つは透過性だが、特に、ビジネスの取引相手、特定の金融取引、およびユーザーが秘密と機密を保持することを合法的に好む他の種類の取引間での転送に関しては、このプロパティは必ずしも望ましいものではない。

これは、数十の異なるプロジェクトに取り組んでいる多数の開発者が直面している問題であると我々は考える。その結果、さまざまな分野の特定のタスクを解決するために、より多くのアドホックブロックチェーンプラットフォームが毎日設計されている。これは、さまざまなタイプの分散型ネットワークの相互運用性に関連する別の問題と、それに取り組むために既に立ち上げられたいくつかのクロスチェーンプロジェクトを生み出している。

それにもかかわらず、1 つのプロトコルで上述した問題を効果的に解決する普遍的な解決策はまだ導入されていない。我々は、Enecuum がその解決策、つまり日常生活における分散レジストリ技術のすべての利点を完全に実現できる、基本的に新しい構造に基づくブロックチェーンシステムであると確信している。(参照. 5).

4. 製品説明

Enecuum は、次世代の分散型ブロックチェーンプラットフォームとして設計され、多数の安全でスケーラブルなブロックチェーンサービスと分散アプリケーションの実装を支援することのできる独自の機能を備えている。

Enecuum の他のプラットフォームと比較しての重要な利点の 1 つは、「HyperDAG」がトランザクションの保存と書き込みのためのデータモデルであり、柔軟な設定でブロックチェーン技術の実用的アプリケーションに新しい機会を提供することである。HyperDAG は、多数のトランザクションを安価かつ迅速に処理する機能を含む、潜在的なビジネス上のさまざまな問題を解決するルールを調整できる別個のブランチの作成をサポートしている。さらに、このソリューションは、スケーラビリティ問題の解決に成功した「シャーディング」技術を統合することを可能にする。

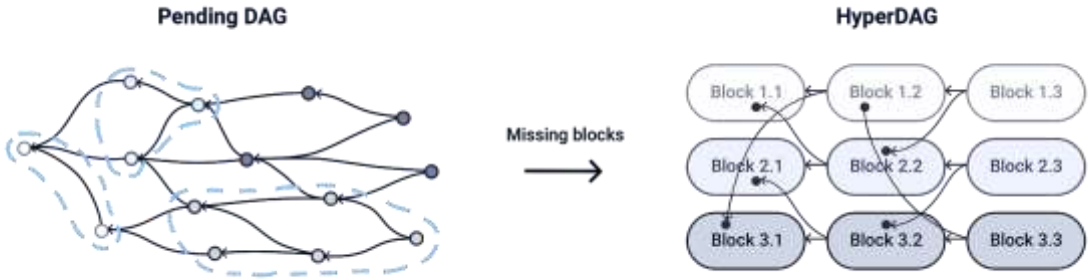

図 1. HyperDAG の一部として PendingDAG

Enecuum は、そのコンセンサスメカニズムの一部として、Proof-of-Work アルゴリズム（**「PoW」**）[3]、Proof-of-Stake アルゴリズム（**「PoS」**）[4]、Proof-of-Activity アルゴリズム（**「PoA」**）[5]を組み合わせたハイブリッドコンセンサスアルゴリズムを使用している。***PoA** は Enecuum を通じて実世界で初めて適用されることが提案されている。*コンセンサスメカニズムの組み合わせを利用することで、ネットワークに接続されているほとんどのデバイスからのトランザクションを確認することができる。その結果、システムの最大限の分散化が可能となり、Enecuum はさまざまな種類の攻撃に対して高い耐性を発揮できる。

Enecuum は、Enecuum プラットフォームで作動する「SHARNELL スマートコントラクト」[20]を開発した。これらのスマートコントラクトは、リニアロジックからなる公式とビジネスのみで構成されている。SHARNELL スマートコントラクトは、Enecuum の高いセキュリティレベルに貢献することを目指している。

リニアロジックは、潜在的な脆弱性、誤使用、凍結、デッドロック、およびシステム内の他の望ましくない問題を大幅に削減すると考えられており、システムに公開する前にスマートコントラクトの信頼性の高い自動証明を可能にする。

Enecuum のもう 1 つの利点は、適応性の高いシステムであることである。ユーザーは、開発に参加して、システム機能を向上させるための他の参加者の提案に投票することができる。システムパラメータの変更を考慮するには、以下の 2 つの方法がある。

- GitHub 上でのプロジェクトリポジトリを分岐し、プロトコルの修正版（経験豊富な開発者が使用する可能性が高い）を提示する。
- または、プロトコルの修正を必要としないネットワークパラメータの調整に投票する。

後者はシステムアーキテクチャによって提供され、ENQ のすべての保有者が使用できるもので、Enecuum で動作するように提案されたネイティブの暗号化デジタルトークンである。テスト期間の後、Enecuum のコンセンサスモデルへの変更をユーザーに提示する投票アルゴリズムが提案されている。テスト期間中、Enecuum チームは、テストとデバッグ用プロトコルの制御権を保持することを提案している。

Enecuum は、実行の安定性と副作用の可能性が低いために使用されるプログラミング言語である Haskell を使用して開発された。コア暗号化プロトコルとして Cryptonight [6]（Keccak + AES + X11）のカスタム版が選択された。これは、特定用途向け集積回路（「ASIC」）のデバイスに高い耐性があるためである。

ENQ は Enecuum のネイティブトークンである。ENQ は、システム特有のパラメータに従って生成されるように提案され、計算能力を費やす報酬として採掘者に支払われる。ENQ は無料で送受信が可能で、ネットワークへのスマートコントラクトの発行、スマートコントラクトの複雑な計算、カスタムマクロブロックや新しいトークンとブランチの作成、PoS マイニングへの参加などの支払いとしても使用できる。

4.1 トランザクション

我々の見解では、トランザクションを分散レジストリに格納するためには大きく 2 つのアプローチがある。

- ブロック（Bitcoin、Ethereum など）、
- 有向非循環グラフ（「DAG」）－（IOTA、Byteball、Universa）。

前者の利点は、ネットワーク内のすべてのノード間で 100%レジストリの複製を行うことによって達成される高い信頼性である。しかし、このアプローチでは、ネットワークの速度とスケーラビリティに一定の制限が課される。後者の DAG では、ブロックが存在せず、新しいトランザクションが発生するたびに、過去の複数のトランザクションを参照する。その結果、このタイプのレジストリは大量のトランザクションを迅速に処理できるが、セキュリティーのレベル如何ではコミュニティ内にある種の懸念が生じてしまう。

我々はこの 2 つのアプローチを組み合わせて、「HyperDAG」と呼ばれるトランザクションを登録するための抜本的に新しい方法を生み出そうと模索している。DAG との主な相違点は、システムに入るトランザクションは、直前のトランザクションひとつだけでなく、ブロック（図 2）に存在するグループも参照することができる点である。このように、HyperDAG は、両方のアプローチの利点をうまく組み合わせ、同時に、上述のような重大な欠点をなくすため、攻撃に対して高いレベルの暗号化プロテクションを備えつつ、毎秒何千ものトランザクションを処理できる。

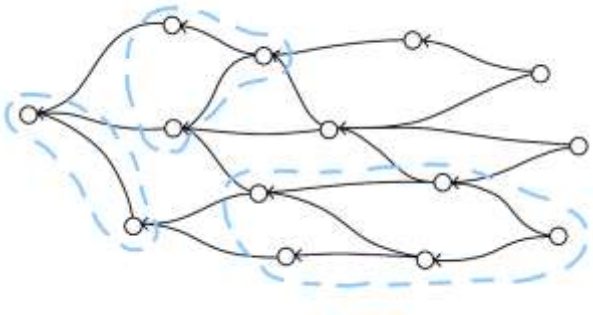

図 2. HyperDAG の原則：近くのトランザクションはブロックにグループ化

このようなトランザクションの方法は、分類、分析およびサンプリングのための膨大な機会を提供する。たとえば、1 つのネットワークのフレームに異なるブランチ（ブロックのチェーン）を作成し、シャーディング技術を適用してネットワークの速度を向上させ、すべてのノード間で 100%レジストリの複製を不要にすることが可能である。

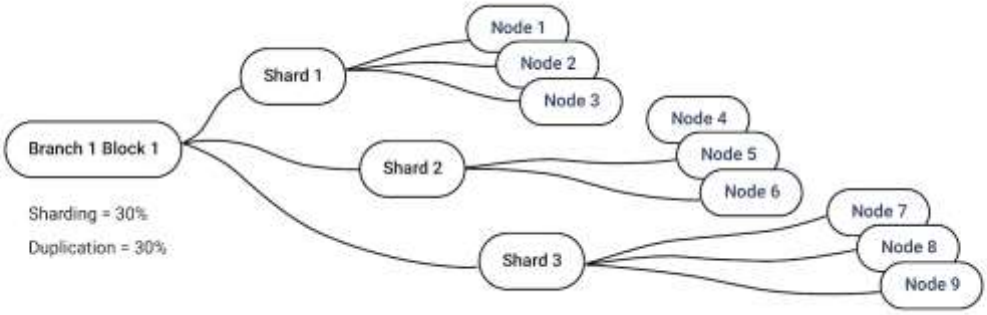

図 3. シャーディング

Enecuum では、トランザクションにいくつかのパラメータが存在する。つまり、重複、シャーディング、サービス品質（ここでは「QS」と呼ばれ、トランザクションの速度）である。重複はシステム全体のセキュリティーを向上させるが、ネットワーク速度を低下させる。シャーディングは逆である。デフォルトでは、重複は 30%、シャーディング – 30%、QS – 無しである。

これらの設定を変更するオプションは、システムの個々のブランチ内で容易なスケーラビリティとユニークなサービスの作成を可能にすることを目指している。

4.2 ブロック

HyperDAG がブロックの組み立てを開始するのに十分な数のトランザクションを蓄積する瞬間に、ブロック作成プロセスが開始される。各トランザクションの指定されたパラメータを分析することにより、採掘者はシステムの価値を判断し、対応するブロックに追加する。以前のトランザクション[MD1]への二重ハッシュタグの導入により、異なるトランザクションを含む *n* ブロックまでを一度にマイニングすることができ、本質的にトランザクションスループットを *n 倍*にすることができる。*n* の限界は動的であり、例えば *1000* とすると、結果として、*1000 x 62 x 40 = 2,480,000* トランザクション/秒、ここで 40 は最小ブロック内のトランザクションの最大数、*62* はトランザクションを検証する PoA チーム内（1 つのチームに 64 人のメンバー）のデバイスの数、そして *1000* は同時にマイニングされるブロックの数である。

Enecuum では、ブロックサイズは固定値を持たず、4KB から 4MB まで変化する。基本的に、最小サイズのブロックを作成し、動作あたりのスピードの遅れを最小にすることが可能である。また、ネットワークの負荷が増加するとブロックサイズも増加するため、ユーザーが 4 MB を超えるサイズのブロックを必要とする場合、システムも、任意の数のブロックをマクロブロックに結合させ、ブロックチェーン上に大量のデータを保存することを可能にする。

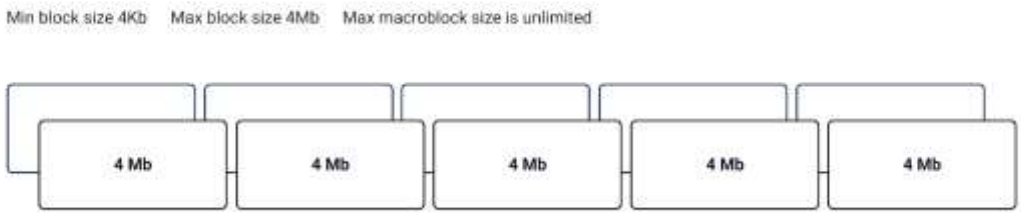

図 4. 可変のブロックサイズ

ビットコイン NG プロトコルは、ブロックの作成する間の時間を減らすために Enecuum マクロブロック[12]となるように設計されているため、マクロブロック内の各マイクロブロックはリアルタイムで作成され、出現後すぐにトランザクションをブロックチェーンに追加する。このように、マクロブロックが作成され、そのハッシュが見つけられ、ネットワーク上のすべてのノード間で同期されるまで待つ必要はなく、マクロブロック内で同時にマイクロブロックを生成することができる。

構造的には、ブロックは次の図に示す 3 つのメインセクションで構成されている。

図 5. ブロックの構造

4.3 ブランチ

HyperDAG を使用してトランザクションを保存および実行すると、同種のトランザクションのみを含むブランチ（ブロックのチェーン）を作成できる。各ブランチは、本質的に別々のブロックチェーンであり、同時に、システム全体の一部である。各ブランチは、新しいブロックの作成と確認のための特別な規則を指示することがある。ノードには全ての補助 Enecuum ブランチは重複しない。

概略的には、ブランチによるブロック割り当てのプロセスは、図 6 に示される通り。

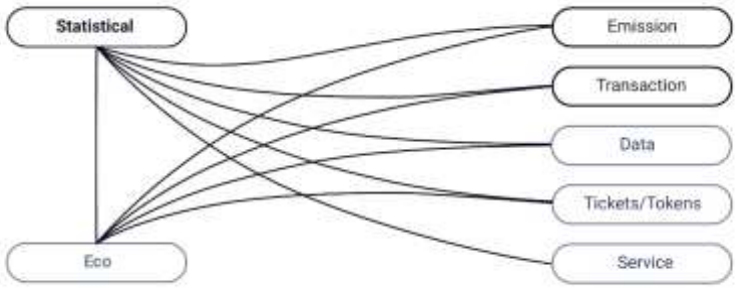

図 6. 異なるブランチへの異なるブロックの割り当て

システムの主要なブランチは以下の通り。

1. トランザクションブランチは、ENQ のユーザー間のすべての通常トランザクションを含むことを目的とする。

2. エミッションブランチは、新しい ENQ を生成するトランザクションをマイニング報酬として含むことを目的とする。

3. 統計ブランチはシステム内の操作に関する統計を蓄積し分析することを目的としており、このブランチには、ノードの総数、マイニング記録、ブロックサイズ、および PoA マイニング報酬の大きさを含む他のパラメータの複数のデータが含まれる。

また、Enecuum は、以下に説明する他のブランチの作成をサポートする。

1. エコロジーブランチは、検証に失敗した疑わしい操作やトランザクションを排除しようとする。たとえば、新しく作成されたウォレットが、異常な量のトランザクションを送信した場合、まず詳細な分析のためにエコロジーブランチに移動させる。

2. チケットブランチは、チケットを通じてさまざまなシナリオを導入する機会を提供する。チケットは、「チケットブランチ」(参照 4.6)と呼ばれる専用のプライベートブロックチェーンへのアクセスを可能にする。たとえば、ユーザーがチケットを作成し、そのチケットブランチにトークンを発行する場合、このチケットを含むすべての操作を暗号化して、この専用ブランチに保存することができる。さらに、これらのチケットブランチには独自のルールがある場合がある。たとえば、すべてのノードが有効であると認識された場合には、すべてのネットワークメンバー間でコンセンサスが必要ないため、トランザクションはより高速に処理できる。

3. サービスブランチは、ポーリング、測量、インスタントメッセージング、文書管理などの分散サービスを提供する。サービスブランチのトランザクションは追加情報を含むことにより、ブロックチェーンを使用して多数のビジネスの問題を解決するのに十分なレベルの柔軟性を実現する。

4. 分散リポジトリとして機能するデータブランチ。根底にある原則は BitTorrent プロトコルの原則と似ているが、従来のハッシングではなく、Enecuum は独自のソリューション(透明性のあるハッシュアルゴリズム)を提案している。BitTorrent ではできない、ハッシュテーブルをノード間で再ハッシュして再共有することなく、暗号化されたファイル内の任意のサイズの部分へのアクセスができるように設計されている。

4.4 ハイブリッドコンセンサスアルゴリズム(PoW, PoA, PoS)

Enecuum では、Proof-of-Work(**「PoW」**)、Proof-of-Activity(**「PoA」**)およびステークスオブ・ステーク(**「PoS」**)の 3 つのマイニングアルゴリズムの相互作用によってコンセンサスが達成される。この組み合わせにより、ネットワークセキュリティレベルとその速度の両方を大幅に向上させながら、高度なネットワーク分散を実現することができる。

Enecuum で実装されているトランザクション確認プロセスは、上記のアルゴリズムに対応する 3 つの段階に大別される。

第 1 段階:

第一段階には 2 つのアプローチがある。通常の方法は、PoW ネットワークに接続されている採掘者が、それぞれが、そのブロック用のさまざまなサイズのブロックハッシュを並列して計算する方法である。その計算の要件を満たすハッシュが見つかった後、採掘者はブロックをトランザクションで満たし、PoA 採掘者によるトランザクション検証が行われる第 2 段階用のネットワークに変換する。第 2 のアプローチは、PoW 採掘者がハッシュを計算し、マクロブロックを作成し、PoA 採掘者のチームがトランザクションを含むマイクロブロックで満たすためにそれを開いたままにすることである。

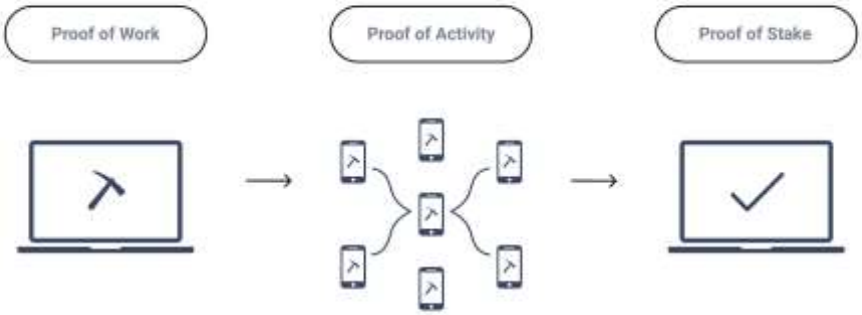

図 7. ハイブリッドコンセンサスアルゴリズム

第2段階:

第 2 段階では、チームに分かれた PoA 採掘者が、選択された PoW シナリオに応じて行動する。上記の最初の PoW シナリオの場合、変換されたブロックのヘッダー内のハッシュをチェックし、ブロック内のトランザクションを検証する。2 つめの PoW シナリオの場合、変換されたブロックのヘッダー内のハッシュをチェックし、マイクロブロックを作成し、トランザクションでそれを埋め、それを PoW 採掘者のマクロブロックに送る。最終的に、チームはそれぞれ 40 件のトランザクションを含む 62 個のマイクロブロックをマクロブロックに送る。その後、ブロックに含まれるトランザクションに応じて、PoA 採掘者はシステムのブランチの 1 つにそれを添付。ブロックハッシュが正確であることを確認するのに、大きな計算能力を必要とせず、この操作は、携帯電話のような単純なデバイスでさえも実行が可能である。

同じことがマイクロブロックの作成にも適用され、トランザクションとトランザクションの検証が行われる。PoA チーム形成のプロセスには、チームに入るためのハッシュを計算しなければならない。各チームは最大 64 の参加者を持つことができ、最高のコンセンサスセキュリティレベルを達成するために、ノードの地理的位置を含む他のいくつかのパラメータの分析に基づいて構成される。

第 3 段階:

第 3 段階では、PoS 採掘者はシステム内のすべてのウォレットの残高を継続的に再確認する。この活動のために、PoS 採掘者は、マイニング報酬の一部をエミッションからのパーセントの形で受け取れるようになっている。報酬は、採掘者の残高に応じて 2 つの方法で決められる。第一の方法は、採掘者がそれ以上報酬を得ることができない最小および最大のバランスの境界値を定める方法。第 2 の方法は、PoS 採掘者の残高が最小値から最大値の境界にまで増加するにつれて報酬が増加するという方法である。

有効なブロックを発見するとネットワークが新しいコインを直ちに生成する既存の報酬方法とは対照的に、Enecuum はこの段階でウォレット残高に追加されるマーク(参照 4.6)を平均して一日一回発行する。

このように、システムは、マイニングアルゴリズムに対する潜在的な攻撃に対しても保護されるのと同時に、計算容量の大部分を制御しようとする（例えば、ASICS を介して）。

デフォルトでは、マイニング報酬は参加者間で次のように分配される：PoA – 70%、PoW – 20%、PoS – 10%。しかし、統計的ブランチ(参照. 4.3)によって、システムはこの分配スキームをコントロールし、利益を乱用から保護することができる。

4.5 SHARNELL スマートコントラクト

Enecuum のスマートコントラクトは、JavaScript で書かれ、Google の V8 エンジンで実行されるようになっている。システムは 2 種類のコントラクトをサポートしている。

1. ビジネス指向の SHARNELL リニアロジックに基づいて、数式だけで構成される「軽い」（ロジカル）スマートコントラクト。リニアロジックは完全に予測可能であるため、潜在的な脆弱性の可能性は最小限に抑えられる。

ロジカルスマートコントラクトは、条件およびパラメータを含む「データカード」と、これらの条件およびパラメータを完全または部分的に達成および作動させることができるようにされた公式自体から構成されている。ロジカルコントラクトの各条件は、データカードに配置され、対応する記号が割り当てられる。

その後、契約条件を完全に反映した数式が作成される。π 計算システムは、計算を並行して実行するために使用される。

このタイプのスマートコントラクトは、マルチサイン、エスクローなどの最も一般的な操作とトランザクションを実行するのに理想的である。私たちのシステムの最初のバージョンでは、Petri Nets をベースにしたグラフィカルエディタを使って作成されることになっている。

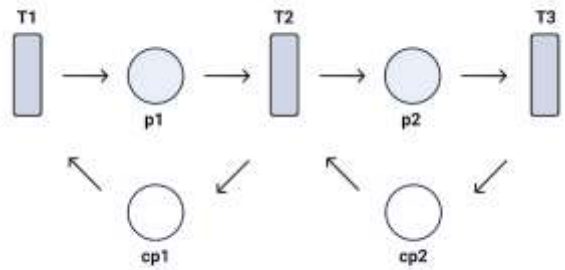

図　8. スマートコントラクト

2.「重い」スマートコントラクトには、科学計算やニューラルネットワークのトレーニングなど、より複雑な問題を解決するためのコードが含まれることが想定されている。これらは、計算用の支払いを伴うシステムの専用のブランチで実行される。このような計算用の支払いは、ENQ において、ユーザーが定義するレートで行われることになる。また、π 計算システムと、セッションタイプのチャネルシステムを使用することも提案されている。

4.6 チケットとマーク

前述のように、Enecuum は、「チケット」(「(最初の文字が大文字の)チケット」、(複数形の)「チケット」も同様)の概念をサポートすることを目指している。チケットは、トークンに類似した暗号の代わりであり、システム上のユーザーが誰でも作成できる。チケットは、ENQ の発行が意図されていない専用ブランチを作成するために使用される。チケットは、対応するブランチへのアクセスキーとこのブランチでのトランザクションの復号化キーの両方として使用され、Enecuum のユーザー間で自由に転送できる。

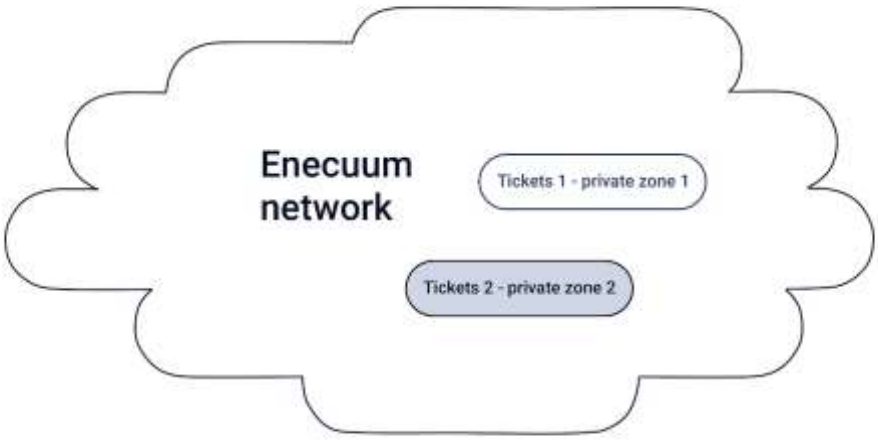

図 9. チケットとチケットブランチ
(グローバル ENQ ネットワーク, チケットブランチ#1, チケットブランチ #2)

チケットは、対応するチケットブランチで受け入れられる交換の基本的な媒体となる。これらのトークンの ENQ への変換は、対応するチケットを介して行われることが提案されている。

チケットブランチの主な目的は、ビジネスと顧客の間の容易な相互作用のためのブロックチェーンベースの柔軟な環境の作成を容易にすることである。

「マーク」は、Enecuum の機能を拡張することを目的とする別のツールである(ケースによって「マーク(単数)」または「マーク(複数)」)。マークは、トークン、取引、ウォレットにラベルを付けることを目的としており、個別のユニットとしては存在せず、必ず支払いユニットと結合している。マークは、タグ付けされたものの特定の機能を示すために使用され、規定された用語または特定のタスクの厳密な実行を保証する。マークは最終的かつ不可逆的である。つまり、それは変更できず、作成前に決定される。

Enecuum は、以下のタイプのマークを提供する。

·より高速なトランザクションを促進するトランザクションアクセラレーションマーク
·統計ブランチにおけるデータ蓄積時に ENQ に変換されるプルーフレムネレーションマーク(参照. 4.3).
·マークされたユニットに適用可能な動作のリストを制限し、対応するマークを含むウォレットにのみ移転できるようにするなど、支払いユニットにカスタムルールを適用するトークンラベリングマーク。この機能は、予算の効果的な管理、購買管理、および指定のローン管理をサポートする。

5. 問題と解決策

5.1. スケーラビリティ

オープンブロックチェーンシステムが直面する最も重要で典型的な問題の 1 つは、安価かつ安全に多数のトランザクションを容易にすることである。スケーラビリティは、この技術を世界規模で採用するために必須である。Bitcoin と Ethereum のスループットはしばしば、1 秒間に 50,000 回以上の処理が可能な VisaNet システム[14]と比較される。これは、最も人気のある仮想通貨の現在のスループットの数千倍も大きい。膨大なスピードでグローバルに伸びている仮想通貨ユーザーの数を考えると、現在の分散システムにおけるトランザクションのピーク時の料金は厳しいレベルに達する可能性がある。

ブロックサイズの単純な増加は問題の部分的かつ一時的な解決策であると我々は考えているが、基本的なスケーラビリティの問題は解決しない。現在、ブロック内のデータは永続的に格納されており、これは、ブロックチェーンのサイズが順調に拡大し続けることを意味する。 スループットの増加に伴い、そのサイズはさらに速いスピードで大きくなる。その結果、大企業のみがこの膨大なデータセットを保存して更新するのに十分なリソースを割り当てることができ、ネットワークの集中化を招く可能性がある。

HyperDAG (参照 4.1)を使用してトランザクションを記録し保存することにより、Enecuum はブロックチェーンを別々のブランチまたはそれらのブランチの一部によって提示されるいくつかの小さなパーツに分割し、並行して処理することを可能にするシャーディング技術の実装に理想的であると我々は考える。Enecuum は、さまざまなブロックサイズのシャーディングを組み合わせることで、システムのセキュリティーを危険にさらすことなく、1 秒間に数万件、数十万件ものトランザクションを効率的に処理できる。ほとんどの場合、最終的なコミッションはゼロまたは最小になる予定である。

さらに、システム内の潜在的に無数のブランチをサポートすることにより、独自のブロックチェーンやメインの Enecuum ブランチ上でより多くの作業負荷をかけることなく、さまざまな分散型ビジネスアプリケーションを作成することが可能となる。各ブランチは、サービス固有のニーズを反映するように個別に作られたカスタムルールを持つことができる。さらに、各ブランチは、システムのすべてのメンバーに対してオープンにするか、指定の参加者のリストを使いプライベートにすることができる。トランザクションスピードまたはブロックサイズを特定のブランチにおいてアップグレードする必要がある場合、コンセンサスルールを修正するために独自のノードを導入することもできるようにする。この場合の制約は、ブランチのノード容量のみである。

Enecuum のアーキテクチャーは、現在の CPU の性能向上と並行してプロトコルを拡張できる解決策である、潜在的に無限のサイズのマクロブロックをサポートすることを意図している。

5.2. セキュリティー

低い分散型の問題

第 1 世代のブロックチェーンシステムは、トランザクション確認のために PoW を使用していた。PoW は、「DoS」（Denial of Service）やスパムなどのさまざまなタイプの攻撃からブロックチェーンシステムを保護する際に実績があり、効率もよく信頼性の高いアルゴリズムである。 仮想通貨の人気と価値が高まるにつれ、PoW マイニングは数億米ドルが投資されたマイニングプロジェクトという大規模な事業に変わった。

中国の電力と人件費が低いことは、中国本土におけるマイニング能力の大規模な集約につながった。この状況では、大規模な採掘者がいることと「51%攻撃」の可能性が高まることが潜在的につながり、関連するブロックチェーンシステムセキュリティーが危険にさらされる。ASIC デバイスの登場は、恒常的にマイニング装置を使うことの経済的意味をなくし、大規模な投資家の手にマイニング能力をさらに集約させたため、この問題をさらに悪化させた[16]。

Enecuum における 3 タイプのマイニングとクリプトナイトの暗号プロトコルを組み合わせることで、地理的だけでなく、さまざまなデバイスタイプや人口統計的にも、システムの高度な分散化が実現できると考えられている。これらの機能により、Enecuum は最も安全な分散レジストリの 1 つになるだろう。それに加えて、ブロックチェーンステータスのデータを収集し分析するシステムに統計ブランチ(参照 4.3)があることで、Enecuum とそのユーザーは、すべての参加者のコンセンサスに影響を及ぼす度合いを均等に分散させることで、さまざまなタイプの潜在的な脅威から保護される。

スマートコントラクトの脆弱性

スマートコントラクトの発明は、仮想通貨業界全体に強力な影響をもたらしたが、今日まで、実装には多くの弱点がある。一旦スマートコントラクトがブロックチェーンに公開されると、修正のために閉じられるため、作成中にエラーが発生すると、さまざまな仮想通貨プロジェクトにおいてそのようなことは一度も起こってはいないが、ユーザーにとって数百万ドルの損失が発生する可能性がある。[16]

スマートコントラクトのセキュリティーを評価する既存の方法は、主にコミュニティにおける開発者による手動コード監査に帰着する。 スマートコントラクト作成とそのテストの方法は、非常に非効率的であるとされている。特に、作成されるスマートコントラクトの数が急速に増え、複雑さも増していることを考慮に入れるならなおさらである。スマートコントラクトの最も一般的なプラットフォームである Ethereum は、特定のプログラミング言語 Solidity [17]で記述することを推奨しているが、それはまだ開発者コミュニティでは人気がない。結果として経験豊富な Solidity 開発者が劇的に不足しており、問題を緩和することはできない。

SHARNELL スマートコントラクトの実装に使用されることが提案されているこのラインロジックは、この技術のセキュリティーを新しいレベルに引き上げようとしている。スマートコントラクトがブロックチェーン

に公開される前にすべてのスマートコントラクトに信頼性の高い自動テストを導入することを提案している。これは、エラーや潜在的な脆弱性の可能性を最小限に抑えることを目的としている。

さらに、SHARNELL スマートコントラクトで推奨される言語は、最も人気のあるスクリプトプログラミング言語の 1 つである JavaScript であるため、多くの専門家が SHARNELL スマートコントラクトの作成に携わる機会を得ており、それによってスマートコントラクトの開発コストを減らすことができる。

ブロックチェーンを介した権力集中

Bitcoin ネットワークの Segwit2x アップグレードの失敗と、Bitcoin Cash の作成におけるハードフォークが、コミュニティにおける潜在的な不一致を浮き彫りにしている[18]。残念ながら、Bitcoin のアーキテクチャーは、採掘者、開発者、および一般ユーザーが異なる動機を持ち、プロトコルを変更することについての見解を形成するという方法で準備されている[2]。競合する利益は、変化する市場状況への適応を減速させてしまう。解決しなければシステムが退化してしまう可能性がある。

Enecuum は、パラメータや新しい変更に関するユーザーの提案に対してオンチェーン投票を実施し、プラットフォーム改善プロセスに影響を及ぼす公平な機会をユーザーに提供することによって、この問題を解決しようとしている。 さらに、メインシステムブランチでのリリース前に補助ブランチの 1 つにおける潜在的な障害用の変更をテストできるため、変更の実装には安全なプロセスが必要である。

5.3. プライバシー

仮想通貨は匿名であり、それが故に違法行為を行うのは十分に容易であると一般的に考えられている。また、ネットワーク内のすべてのトランザクションが透過的でオープンであるにもかかわらず、実際の個人や企業は隠されているとも一般的に考えられている。しかし、これは全く正しくない。なぜなら、オープンブロックチェーンにおけるすべての操作でデジタルトレースが永遠に保持されており、このトレースで実行された詳細な分析により、高い精度で実際の取引相手を知ることができるからだ。したがって、侵入者が実際の人や会社と公共の住所を照合すると、重要な機密データにアクセスして修復不能な損害を引き起こす可能性がある[15] [19]。

チケットブランチ(参照 4.3)は、Enecuum ユーザーに個人情報開示のリスクを最小限に抑えるプライベートモードで取引を行う手段を提供しようとしている。 チケットは、 ブランチ内のトランザクションを暗号化するキーであるため、チケットの所有者だけが、その中で行われるトランザクションの詳細を見ることができる。また、チケットブランチは、特定のブランチ（チケットブランチ）で特定のトークンを発行できるようにしようとしている。そのようなトークンを Enecuum と交換する主な媒体である ENQ と交換する必要がある場合、チケットは交換に影響を与えるキーとなる。このようにして、チケットは、ネットワーク全体の容量を利用し、そのようなトランザクションが高速で行えるよう保証しようとし、チケットブランチ内で外部の目からトランザクションを確実に保護する暗号化キーとして機能する。

6. ユースケース

6.1 イニシャルコインオファープラットフォーム

このような Enecuum ブロックチェーンの高いスループットは、ネットワークのハングアップのリスクなしに、スタートアップがあらゆる規模で資金を調達できるようにすることを目的としている。したがって、最初のコインオファリング（「ICO」）の参加者は、ICO に参加することができ、迅速にトークンを受け取ることができる。 Enecuum のスマートコントラクトは JavaScript で実装されるため、どの Web 開発者にも簡単に書くことができ、作成コストが大幅に低下するだろう。さらに、リニアロジックを使用することで、スマートコントラクトのコードの潜在的な脆弱性を排除し、ハッキングのリスクを最小限に抑えることができる。

「キャンセルモデル」は、発行者が ICO の集合体をを段階的に実装し、プロセスのどの段階においても、参加者に資金を還元することを可能にする。トークンのシステム特有の表記法は、ERC-20 表記法と同様に、Enecuum に基づいて作成されたトークンを ICO 後の仮想通貨交換サービスに簡単に入力するためのものである。

トークン発行者は、トークンのユースケースの適切な設計を担当し、トークンがすべての適用される法的および規制上の義務を遵守することを保証する。

6.2 ファイナンシャルサービスと支払のインフラストラクチャー

Enecuum のチケットとマークを使用することで、銀行、政府機関、取引組織が受け取ったクレジットと予算資金の目標支出を確実に管理できるようにすることが我々の目標である。Enecuum インフラストラクチャーは、安全で効率的な支払いを可能にするように活用できる。

例えば、銀行は顧客のデータベースを有しており、そのデータベースは事業の性質（建設会社、産業機器供給業者など）に基づいて分類される。 銀行は、特定の明確なマークを持つトークンで顧客に特定のローンを発行することができる。顧客は、これらのトークンを使用して事前に決められた特定の組織にのみ支払い、発行されたローンの目的に応じてのみトークンを使用できる。

さらに、トランザクションに注釈を追加するできるようになれば、例えば、各顧客の履歴を保持するブロックチェーンベースの保険サービスを可能にする。このサービスは、スマートコントラクトによる自動計算を実行することによって、ブロックチェーンに直接ユーザーの評価を保存し、各ユーザーの保険の範囲に関する情報などを保存することができる。

6.3 分散コンピューティング

Enecuum は専用ブランチにおいて「重い」スマートコントラクトを実行できるようにすることを目指している。Enecuum はまた、主要な Enecuum ブランチに負荷をかけずに高い計算能力を必要とする複雑な計算を可能にすることを目指している。（ニューラルネットワークトレーニング、科学計算、レンダリングコンピュータグラフィックス、JS ライブラリなどに有効） ENQ でフレキシブルなレートで ENQ において行われる、このような「重い」スマートコントラクトを使用するための支払いは、Ethereum ブロックチェーンの取引価格のコンセプトと同じである。計算を実行する要求が作られると、顧客は価格を設定し、採掘者はタスクの計算能力を提供することが有益かどうかを決定する。採掘者が条件に同意した場合、顧客の資金は将来の支払いのためにスマートコントラクトによって予約される。タスクが完了し、有効な結果が出ると、資金は解放され、自動的に採掘者に転送される。

6.4 分散型ストレージ

シャーディング技術の適用とトランザクション重複パラメータの変更が可能になることで、ユーザーのデバイス上のディスクスペースを効果的に使用することができる。たとえば、4 人のユーザーがそれぞれ 5GB のスペースを提供し、複製およびシャーディングパラメーターが 50%に設定されている場合、ファイルの実効ストレージ容量は 10GB である。このパターンをネットワーク全体に外挿すると、「グローバル分散ディスク」のサイズは、データの可用性と十分な高速アクセスを維持しながら比例的に増加する。これは、将来、ユーザーが、分散ホスティング、クラウドデータストレージサービス、コンテンツ配信ネットワークなどのサービスを Enecuum ブロックチェーン上に構築する可能性を意味する。

また、SHARNELL スマートコントラクトとチケットをそのようなデータブランチ上に暗号キーとして適用すると、ユーザーはトークンで支払われた分散（および不変）コンテンツの有料アクセスサービスの複合体を作成できる。

6.5 マイクロトランザクションと IoT アプリケーション

Enecuum システムの作業負荷は、Eneecuum 上のユーザー数が増えるにつれて増加し、分散型アプリケーションは Enecuum ブロックチェーン上で開発される。しかしながら、Enecuum は、独自のコンセンサスルールセットを使用して別々のブロックチェーンブランチを作成できるようにすることで、メインシステムから作業負荷を取り除けるようにしている。これは、採掘者の活動を促進し、マイクロトランザクションサービスの実施に有益な条件を作り出すことを模索している。

Enecuum は、分散型マイクロトランザクションサービスのトランザクション手数料をゼロにし、一つのウォレットからの多数のマイクロトランザクションを含む集中型マイクロトランザクションサービスを行う場合、トランザクションあたりの手数料を非常に低くすることを提案している。たとえば、1 日に 10,000,000 件のトランザクションを、それぞれ 10 MB の大きなマクロブロックに簡単に記録することができる。手数料はブロックごとに計算されるため、トランザクションあたりの手数料は非常に低くなる。

我々はこれが Enecuum の機能を「モノのインターネット（IoT）」との関連において完璧な使用方であると確信している。様々なデバイス上の PoA マイニングのためのシンプルなクライアントの実装で、転送されるトランザクションの料金を完全にカバーすることができる。さらに、Enecuum ネットワークプロトコルは、それらの間にメッシュネットワークを確立することによって、そのようなデバイスの高い可用性を提供できるように設計されている。

7. 参考文献リスト

[1] P. Kasireddy, “Blockchains don’t scale. Not today, at least. But there’s hope.,”2017. [インターネット上]
https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a
[2] F. Ehrsam, “Blockchain Governance: Programming Our Future,” 2017. [インターネット上]
https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74
[3] A. J. Markus Jakobsson, “Proofs of Work and Bread Pudding Protocols (Extended Abstract),” 1999. [インターネット上].
http://www.hashcash.org/papers/bread-pudding.pdf
[4] V. Buterin, “What Proof of Stake Is And Why It Matters,” 2013. [インターネット上].
https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/
[5] C. L. A. M. M. R. Iddo Bentov, “Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake,” 2014. [インターネット上].
https://eprint.iacr.org/2014/452.pdf
[6] “CryptoNote Philosophy”. [インターネット上]
https://cryptonote.org/inside
[7] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [インターネット上]
https://bitcoin.org/bitcoin.pdf
[8] Ethereum Foundation, “Ethereum Homestead Documentation,” 2018. [インターネット上]
http://www.ethdocs.org/en/latest/
[9] IOTA Foundation, “The IOTA Developer Hub,” 2018. [インターネット上]
https://iota.readme.io/
[10] A. Churyumov, “Byteball: A Decentralized System for Storage and Transfer of Value,” 2016. [インターネット上]
https://byteball.org/Byteball.pdf.
[11] Universa Corporation LTD, “Universa Blockchain Platform Whitepaper,” 2017. インターネット上].
https://universa.io/files/whitepaper.pdf?v=1.3
[12] N. N. T. D. a. M. V. Ethan Heilman, “IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency,” 2017. [インターネット上].
https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md.
[13] A. E. G. E. G. S. R. v. R. Ittay Eyal, “Bitcoin-NG: A Scalable Blockchain Protocol,” 2015. [インターネット上]
https://arxiv.org/pdf/1510.02037.pdf
[14] J. Vermeulen, “VisaNet -- handling 100,000 transactions per minute,” 2016.[インターネット上]

https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-Per-minute.html
[15] P. Kasireddy, “Fundamental challenges with public blockchains,” 2017. [インターネット上]

https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428
[16] M. B. a. T. C. Nicola Atzei, “A Survey of Attacks on Ethereum Smart Contracts,” 2016. [インターネット上]
https://eprint.iacr.org/2016/1007.pdf
[17] “Solidity,” 2017. [インターネット上].
http://solidity.readthedocs.io/en/develop/
[18] J. J, “No SegWit2x Makes Bitcoin Cash Shine Amidst Crypto Bloodbath,” 2017. [インターネット上].
https://cointelegraph.com/news/no-segwit2x-makes-bitcoin-cash-shine-amidst-crypto-bloodbath
[19] J. Clifford, “Privacy on the blockchain,” 2017. [インターネット上]
https://hackernoon.com/privacy-on-the-blockchain-7549b50160ec
[20] “Deep Inference,” 2018. [インターネット上]
http://alessio.guglielmi.name/res/cos/