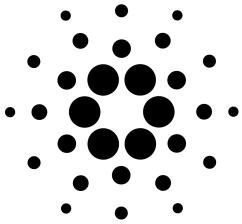

なぜカルダノを構築するのか

主観的アプローチ

チャールズ・ホスキンソン

<Charles.Hoskinson@iohk.io>

<C3A6 5E46 7B54 77DF 3C4C 9790 4D22 B3CA 5B32 FF66>

1.はじめに

動機

カルダノは**2015**年に仮想通貨の設計および開発のあり方を変えるために発足されたプロジェクトです。特定のイノベーションを超えた全体的な焦点は、ユーザーのニーズに応えられ、他のシステムとの統合を図れる、より調和のとれた、持続可能なエコシステムを提供することです。

カルダノは多くのオープンソースプロジェクトのように、包括的なロードマップ、また権威のあるホワイトペーパーの策定を行いませんでした。むしろ設計原則、工学的なベストプラクティス、また探求のための方法論を収集し、採用したのです。それには以下のものが挙げられます:

- 台帳システムと計算処理を別々の階層に分離する
- コアとなるコンポーネントをモジュール性の高い関数によって実装する
- 査読が行われる研究と競合する学者や開発小規模グループを作る
- **InfoSec**の専門家を早期に採用するなど学際的なチームを多用する

- ホワイトペーパー、実装、そしてレビュー中に発見された問題を修正するための研究を迅速に行う
- ネットワークを破壊することなく、導入後のシステムをアップグレードする機能を構築する
- 今後の研究となる分散型資金調達の仕組みを開発する
- モバイルデバイス上で安全に動作するための長期的な仮想通貨の設計の改善を行う
- 仮想通貨を運用および維持するために、ステークホルダー同士の関係を密接にする
- 同じ台帳システムで複数の資産を運用する必要性を認識する
- 従来のシステムのニーズに応えるために、オプションとしてメタデータを含むことができるようにトランザクションの抽象化を行う
- 約 **1,000** のアルトコイン から理にかなっている機能を学習し、採用する
- 最終的なプロトコル設計を決定するためにインターネット技術タスクフォース**(IETF)**に触発された規格駆動のプロセスを採用する
- 商業の社会的側面を探求する
- ビットコインから継承した基本原則を損なうことなく、規制機関が商取引と対話するための健全な妥協点を見つける

これらの個別のアイデアから、我々はカルダノの仮想通貨の探索およびに抽象化されたツールセットの構築に取り組み始めました。その研究成果は、**IOHK** の広範な論文のライブラリであり、近年のスクリプト言語の概要や、スマートコントラクトのオントロジー、**Scorex** プロジェクトなど多数あります。仮想通貨業界の異例、時には逆効果的な成長に見て取れる課題は以下の通りです。

第一に、成功を収めた**TCP/IP**などのプロトコルとは異なり、従来の仮想通貨には階層化がなされていません。これは、それが理にかなっているかどうかに関係なく、単一の台帳システムに記録やイベントに関する単一概念のコンセンサスを保持しようという願望があったためです。

例えば、イーサリウムは、世界の普遍的なコンピューターとなるために大幅な制限を行いましたが、明確な問題点を抱えており、価値を保存するシステムとしての能力を失う可能性があります。その経済的価値、維持費、法的規制、に関わらず、全ての人のためのプログラムが、最善と見なされるべきなのでしょうか。

第二に、主流の暗号学の研究において過去の業績がほとんど評価されていないことです。例えば、**Bitshares** の委任されたプルーフオブステークは**1980**年代以来知られている確実に結果を出力できるコイントスの技術 **(Rabin**および**Ben-Or**による発展的なペーパーを参照**)**を利用することによって、より確実かつ容易に乱数を生成できたでしょう。

第三に、ほとんどのアルトコインでは、将来的なアップデートに行う体制が整っていません(Tezos のような例外もあります) 。正常にソフトまたはハードフォークを行えるということは、仮想通貨 が長期的な成功を収めるためには極めて重要です。

当然のことながら企業は、ロードマップとその背後にあるアクターが不透明、小規模、または過激なプロトコルに何百万ドルものリソースをコミットすることはできません。根底にあるプロトコルを進化させるためには、社会的コンセンサスが成立可能なプロセスが必要となります。このプロセスが非常に厄介な場合、意識の分裂はコミュニティに破壊をもたらしかねません。

最後に、お金とは最終的には社会現象なのです。ビットコインとその同業者は、中枢アクターの匿名化および銀行離れを試みたことによって、その安定したアイデンティティとメタデータを放棄し、商業的なトランザクションとしての評判を失ってしまいました。中枢アクターが講じた解決策によってそのようなデータが追加されるということは、ブロックチェーンの本質である、監視能力、グローバルな可用性、そして普遍性を失ったことになります。

SWIFT、**FIX**、および**ACH**のような従来の金融システムは、トランザクションメタデータが豊富です。規制を行うには、アカウント間の取引だけではなく、関与するアクターの属性、コンプライアンス情報、疑わしいアクティビティの報告、およびその他の記録とアクションが要求されます。場合によっては、メタデータがトランザクション自体よりも重要となるのです。

したがって、メタデータの操作は、通貨の偽造やトランザクション履歴の書き換えと同様に有害であると結論づけることができます。またメタデータを自発的に取り入れているアクターを配慮しないことは、その行為の主流化およびに消費者保護に対して逆効果であるようにみえます。

終末の到来

我々の仮想通貨における先進的な探求は**2**つのプロトコルに集約されます。これらはそれぞれ、証明可能安全なプルーフオブステーク **[1]** **[2]** を用いた仮想通貨 **Cardano Settlement Layer(CSL)**、及びプロコトルの集合体である**Cardano Computation Leayer(CCL)** と呼ばれています。

我々は設計に際して、仮想通貨の社会的側面を受け入れ、階層化を行うことで資産の会計を複雑な計算処理から分離し、いくつかの不変の原則の範囲内で規制者のニーズに応えることに重点を置いています[1]。また必要に応じて、 査読によって提案されたプロトコルの検証を行い、正式な仕様に対するコードのチェックを行っています。

[1]リストは規制に関するセクションを参照

プルーフオブステーク

仮想通貨にプルーフオブステークを採用するということはその設計選定において疑問視されている設計上の選択肢です。しかし、我々はこれをあえて採用することにしました。というのも安全な投票を導入するためのメカニズムを追加でき、スケーリングを行える余地があり、かつよりエキゾチックなインセンティブの仕組みを取り入れられるためです。

我々のプルーフオブステークプロトコルはウロボロスと呼ばれ、エディンバラ大学の **Aggelos Kiayias** 教授が率いる**5**つの学術機関[2]の優秀な暗号学者のチームによって設計されました。ウロボロスがもたらすイノベーションとは 厳格な暗号化モデルを使用した安全証明だけではなく、多くのプロトコル構成の機能を強化できるモジュラーであり柔軟な設計です。

このモジュール化により、委任機能、サイドチェーン、閲覧可能なチェックポイント、シンクライアント用のより優れたデータ構造、様々な乱数生成方式、多様な同期方式など豊富な機能が実装可能となります。ネットワークは数千から数百万、さらには数十億のユーザーが関与により発展していくため、そのコンセンサスアルゴリズムの要件も変更されます。したがって、これらの変更に対応するために十分な柔軟性があることが不可欠であり、それによって仮想通貨を将来性のあるものにします。

お金の社会的要素

仮想通貨はお金が社会的コンポーネントであることの主要な例です。技術だけに焦点を当てて分析を行なった場合、ビットコインとライトコイン、イーサリアム と イーサリアムクラシックの間にはあまり差がありません。しかし、ライトコインとイーサリアムクラシックは共に巨大な時価総額と、堅牢で活発なコミュニティを有し、独自の社会的義務を負っています。

仮想通貨の価値の大部分は、コミュニティが通貨をどのように使用し、その進化にどの程度関与しているかで導き出せると主張できます。更に言えば、**Dash**などの通貨は、開発と資金調達の優先順位の決定にコミュニティが関わることのできるプロトコルを、直接システムに統合しています。

仮想通貨の多様性はまた、その社会的側面を明確にしています。哲学や金融政策に関する意見の不一致、あるいは開発チームの分裂は、コミュニティの断片化とフォークにつながりま

[2]コネチカット大学、アテネ大学、エディンバラ大学、オーフス大学、東京工業大学

す。しかし仮想通貨とは異なり、超大国の不換紙幣は、政治的変化や地域格差による通貨危機やキャピタルフライトが起きたとしても、生き残る傾向にあります。

したがって、仮想通貨業界には従来のシステムに欠落している要素があるようです。カルダノロードマップにもあるように、プロトコルのユーザーは、そのプロトコルの背後にある社会的な契約を理解するためのインセンティブを必要とし、生産的な方法で変更を提案する自由を持っていると我々は主張します。この自由は、市場がどのプロジェクトに資金を供給すべきか、どのように規制すべきかを決定するのか、価値交換システムなどあらゆる側面に及んでいます。これは中枢アクターや、特別な資格を有する潤沢な資産を有した少人数派などによって仲介されるものであってはいけません。

カルダノは、ユーザーのニーズに応えるために、**CSL**の上に構築されたオーバーレイプロトコルのシステムを実装します。

第一に、開発のブートストラップのために行なったクラウドセールの成功の有無に関わらず、調達資金は最終的には消滅します。加えてカルダノは、単調に減少するインフレおよび取引手数料が資金源となる分散型信託[3]を導入します。

全てのユーザーは、投票システムによって信託から資金を調達する資格を有し、**CSL**のステークホルダーは誰が受益者になるかを投票します。このプロセスによって誰が資金を受け取るべきかという議論が行われ、**Dash**など[]の財務システムを有する仮想通貨にみられる、生産的なフィードバックの循環を生み出すことができます。

資金調達の議論は、長期的及び短期的目標、仮想通貨の社会的契約、特定の提案における方針と価値創造の信念に対してその関連性を強制させることができます。これは、コミュニティが常にロードマップの可能性について評価およびに議論していることを意味します。

第二に、カルダノはソフトフォーク、ハードフォークの提案、正式に行うためにブロックチェーンに基づいた投票システムの導入を予定しています。ブロックサイズの議論をしているビットコイン、**DAO**フォークを行なったイーサリアムおよびその他の多くの仮想通貨は、長年、もしくは頻繁にプログラムコードの技術的および道徳的な方向について終わりのない議論を行ってきました。

これらの多くの意見の不一致、またそれによってアクションが取られたときに生じるコミュニティの破綻は、変更のための議論において正式なプロセスが欠如していたことが直接的な原因に違いありません。

[3]これは、財務システムとも呼ばれています

ビットコインユーザーが**Segregated Witness**を採用するためには誰を説得すれば良いのでしょうか。イーサリアムのコア開発者は**DAO**を救済する際に、コミュニティの感情を測定するにはどうすればいいのでしょうか。またコミュニティが分断すれば、その仮想通貨は永遠に修復不可能なのでしょうか。

最悪の場合、道徳的権限による行為とは、コミュニティの大半が望んでいるものではなく、単に開発者を味方にして、人脈とお金を持つ人に委ねられてしまいます。さらにインセンティブが悪い[4]ために、コミュニティの大部分がアクセス不能または離脱した場合、その行為が正当なものであるかどうかの真相を知ることは困難になります。

Tezos のような提案された仮想通貨は興味深いモデルを提供してくれます。**Tezo**では仮想通貨のプロトコルを**3**つのセクション（トランザクション、コンセンサス、ネットワーク）から成る法体制のように扱っており、改正を行うための正式なルールとプロセスがあります。しかし、インセンティブや、形式言語によって仮想通貨を正確にモデル化して変更を行う方法については、まだ多くの課題が残っています。

これには形式的な方式や、コンピューターが理解可能な仕様、あるいはこのプロセスを財務システムと併合することによって金融的インセンティブを高めることが解決策として考えられています。結局のところ、もし洗練された解決策を見出せない場合であっても、ブロックチェーンに基づいた投票システムによって、透明性があり、検閲を許容する方法でプロトコル変更を提案することができれば、そのプロセスの改善に繋がるはずです。

階層の設計 – Cardano Settlement Layer

偉大なプロトコルと言語を設計するときには、未来ではなく、過去に目を向けるべきです。歴史を振り返ると開放型システム間相互接続のような、理論的には完璧であるが、なんらかの理由で実現されなかった素晴らしいアイデアを数多く見出せます。また、**Javascript**や、**TCP/IP**などから生まれた幸運の産物もあります。

歴史から学んだ原則としては次のものが挙げられます:

1. 柔軟性から生まれた成果物から将来を予測することはできない
2. 複雑であるということは理論上素晴らしいが、実際にはシンプルである方が良い
3. 船頭多くして船山に登る
4. 標準規格が決定されると、それが最適であるかどうかに関わらず従ってしまう
5. 悪い考えであっても、意思が明確にあれば非常に良いものに進化することがある

[4]理性的な無知を参照

カルダノとは、その社会的性質を受け入れている金融システムです。システムには、柔軟性と特定のユーザーのトランザクションの任意の複雑さに対処する能力が求められます。もしそれらの要求に応えることができれば、数百万の同時トランザクションに対応するための膨大な計算処理、ストレージ、およびネットワーク・リソースが必要となります。

しかし豊富なノードから奪い、貧しい人々に与えるような、公正なネットワークを実現するためのデジタル化された分散型ロビン・フットはいません。また我々にはネットワークをより良いものにするために自己犠牲を払ってくれるような信頼できる人間を雇う余裕もありません。したがって、カルダノの設計には**TCP/IP**プロトコルの概念の**1**つである関心の分離を利用しています。

ブロックチェーンとは究極的には事実とイベント、そしてタイムスタンプを不変性と信頼性を持って記録し、それらに対して問い合わせを行うデータベースなのです。よってお金という観点から見れば、ユーザーが資産の所有権をブロックチェーン上で注文することと、これにプログラムの保存と実行によって複雑な計算処理を加えることとは、全く異なるコンセプトとなってきます。我々はアリスからボブへいくら送られたのか知りたいのか、それとも、その取引の背景を把握し、どれくらい送るべきなのかという決定に関与したいのでしょうか。

後者を選択することはイーサリアムが行なったように柔軟性があり、とても魅力的ですが、上記の設計原則を破ることになります。ストーリーを把握するということは、単一のプロトコルが任意のイベントおよびトランザクションを理解し、詐欺が行われた場合には仲裁を許可し、場合によってはトランザクションを取り消すことを意味します。

しかし設計者は各トランザクションに格納されるメタデータの設計において難しい決断を下す必要があります。アリスとボブの取引の背後にある物語のどのような要素が関連しているのか、それらは永遠に関連しているのか、いつデータを消去することができるのか、消去することが違法となることはないのかなどを考慮する必要があります。

加えて、いくつかの計算処理は、内密に行われるものです。たとえば、ある職場の平均給与を計算する場合、企業は各人の年収を公開しません。もしすべての処理が公にされるとしたらどうなるのでしょうか。また、この公共性によって 悪い結果へと導かれたら、どうなるでしょうか？

したがって我々は、会計処理とそれが行われる背景とを分離すべきであると判断しました。つまり、価値を計算の分離です。これはカルダノがスマートコントラクトに対応しないことを意味するわけではありません。逆に分離を明示的に行うことよって、スマートコントラクトの設計、使用、プライバシー、および実行をより柔軟に行うことができます。

カルダノにおいての公開台帳システムを担う階層は、**Cardano Settlement Layer (CSL)** と呼ばれます。**CSL**は会計処理を行うことが目的であるため、ロードマップには次の目標があります:

1. 次のスクリプト言語をサポートする。一方は価値の移動を行い、もう一方はオーバーレイプロトコルのサポートを強化するものである
2. **KMZ**サイドチェーン[5]が他の台帳システムと連携できるようなサポートを提供する
3. より高度なセキュリティのために耐量子コンピューター電子署名方式を含むあらゆるタイプの署名方式に対応する
4. 複数のユーザーの独自通貨に対応する
5. ユーザーがネットワークに参加するにつれ、システムの機能が向上する真の拡張性を実現する

スクリプト

まずもってスクリプト言語とは、台帳システム上のアドレス間におけるトランザクションにおいてその有効性を証明するために実行されるプログラムを意味します。イヴ(悪意のある者)がアリスの資産に不正アクセスする、あるいは誤って設計されたスクリプトによって無効の住所にお金を送ってしまい、資金が回収不能になるようなことは、スクリプトの設計者は望んでいません。

ビットコインなどのシステムは、非常に融通の利かない厳格なスクリプト言語を提供しているため、トランザクションを独自にプログラムすること、またそれを読み解くことは非常に困難です。加えて、**Solidity**などの一般的な言語によるプログラミングは、システムに複雑さをもたらす上に、ほんの一握りのアクターに対してのみ有益です。

よって我々は新しい言語を設計することにしました。これは**Simon**[6]と呼ばれており、言語を作成した**Simon Thompson**およびにそのコンセプトを生み出した**Simon Peyton Jone**から由来しています。**Simon**は[コントラクト構成法: 金融工学への探求]を基にしたドメイン特化言語です

主要な考え方は、金融取引は一般的に基本要素の集合から構成される、ということです[7]。金融関係の要素を定期的に寄せ集めれば、一般的なプログラマビリティでなくても、ほとんどすべてに通じるトランザクションをカバーする任意の大規模な複合トランザクションに対応することができます。

[5]**Kiayias、Zindros** と**Miller**氏の論文を近日公開予定
[6]これに関する詳細は、今後の仕様でリリースされます。言語の完全な対応は**2017**年第**4**四半期の**Shelly CSL**のリリースにて行う予定です
[7]**Project ACTUS** にてより詳細な記述があります

主な利点としては、セキュリティの向上とプログラムの実行が理解しやすいことです。これによってテンプレートの正確性を証明することができ、虚無から創出されたお金、トランザクション展性など問題のあるトランザクションの実行スペースを無くしてしまうことができます。また新しい機能が必要である場合、ソフトフォークを介して既存の拡張機能に追加することもできます。

つまり、オーバーレイプロトコル、従来の金融システム、および専用サーバーに**CSL**を接続する必要が常に存在します。したがって、我々は**Plutus**を汎用スマートコントラクト言語と相互運用性のための専用**DSL**として開発しました。

Plutusは、独自のトランザクションスクリプトを記述する際に使用できる **Haskell** の概念に基づいた型付きの関数型言語です。この言語は**CSL**において、サイドチェーンの仕組みなど別の階層と接続する必要がある複雑なトランザクションに対応するために使用されます。

サイドチェーン

サイドチェーンに関しては、カルダノはプルーフオブワークの証明の結果を基に**Kiayias**、**Miller**と **Zindros**氏 によって開発された新しいプロトコル(**KMZ**サイドチェーン)の対応を行います。このプロトコルに関する設計の詳細についてはここでの議論の範疇を超えています。しかし、そのコンセプトにより**CSL**から任意のカルダノ・コンピューテーション層やプロトコルに対応している他のブロックチェーンへの安全で非対話的な資産の移動を可能にします。

KMZサイドチェーンは、複雑な処理をカプセル化するための鍵となっています。規制要件、民間業務、堅牢なスクリプト言語、その他の特別の懸念については**CSL**ではブラックボックス化されています。しかし、**CSL**ユーザーは計算処理が完了すればその会計や資金回収能力について一定の保証を受けることができます。

署名

アリスからボブに安全に価値を移すためには、アリスは自身が資金を動かす権利を持っていることを証明する必要があります。この課題を最も直接的かつ確実に達成する方法として公開鍵証明方式が挙げられます。これはアリスが所有している秘密鍵と関連づけられた公開鍵が資金と結びつけられていることを意味します。

署名方式はさまざまなセキュリティパラメータと仮定によって、何百ものパターンがあります。それには楕円曲線に関連する数学的問題を使用する物もあれば、格子を用いて異種概念と結びついているものもあります。

抽象的な目標は常に同じです。解決が困難な問題が存在し、それに関する秘密の知識を誰かが持っていなければ解決できないということです。秘密の知識の持ち主は鍵ペアの所有者のはずであり、所有者は鍵ペアを使用できる唯一のエンティティでなければなりません。

署名方式を選択する際に、仮想通貨には**2**つの懸念があります。第一に、署名方式自体に長期的なセキュリティを行えるような耐久性が要求されます。**DES**など**1970**年代から**1980**年代にかけて使用されていた暗号方式は既に破られています。このため、署名方式の利用可能期間を想定しなければいけません。

第二に、特定の方式には、多くの企業、政府や他の機関で使用が好まれているか、場合によっては義務付けられているものがあります。たとえば**NSA(**アメリカ国家安全保障局**)**は **Suite Bプロトコルセット**を保有しています。**ISO**や**W3C**ワークグループにも標準化された暗号方式があります。

仮想通貨が単一の署名方式を採用した場合、その暗号がいずれ破られてしまうという運命を受け入れることとなり、また少なくとも**1**つのエンティティが法的または業界の制約により仮想通貨を利用できないという事態に陥る可能性があります。とはいえ仮想通貨は全ての署名方式を採用する訳にもいきません。その場合、クライアントは全ての方式に対して検証を行えるように開発しなければならないからです。

我々はカルダノ初期の署名方式として楕円曲線暗号、**Ed25519**曲線を採用することにしました。また**Khovratovich**博士と**Jason Law**の仕様[8]を使用することで**HD**ウォレットのサポートを行い、既存のライブラリを強化することも決定しています。

加えてカルダノを将来的に他の署名方式に対応させるつもりです。特に耐量子コンピューター電子署名方式である**BLISS-B**の統合には関心があります。また、従来の仮想通貨であるビットコインとの相互運用性を高めるために **SECP256k1** の統合も予定しております。

カルダノには特別な拡張機能があり、これによってソフトフォークを介して利用可能な署名方式を追加することができます。これらは必要に応じて、あるいはロードマップ[9]に計画されているメジャーアップデートにて追加されます。

[8]これは、カルダーノの**HD**ウォレットの実装に関するドキュメントです。我々の知る限りカルダノは**Ed25119**鍵を採用した**HD**ウォレットを初めてサポートする仮想通貨です。
[9]**cardanoroadmap.com** を参照

ユーザー発行資産 (UIA)

初期のビットコインでは、ユーザーが複数の通貨を同時に追跡するために、ビットコインの会計システムによって資産を発行して、管理できるようにしたプロトコルが急速に開発されました。これらのプロトコルはビットコインのネイティブなプロトコルに対応していませんでしたが、巧妙な手口により実装されました。

カラーコインや Mastercoin (現在はOmniと呼ばれています) などのビットコインがオーバーレイされた仮想通貨のシンクライアントは、信頼できるサーバーに依存するように強制されました。また、トランザクション手数料はビットコインで支払わなければなりません。これらの性質に加えて、トランザクション承認に単一のパイプラインを使用することによって、ビットコインにおける複数の資産を運用することが難しくなると言えます。

ERC20 規格を採用した イーサリアム では、より豊富な機能があります。しかし、トランザクションの手数料には未だに**Ether**を必要とします。さらに、イーサリアムネットワークは、ERC20 によって発行されたトークンのニーズに応えるためのネットワーク拡張が上手く行えていません。

根本的な問題は、リソース、インセンティブ、そして関心という**3**つに分けることができます。リソースという観点からすれば、まったく新しい通貨を同じ台帳に追加するということは、バンド幅、メモリープール、およびブロック空間を共有する**2**つの独立した **UTXO**（未使用トランザクションアウトプット）セットを持つことを意味します。またこれらの通貨の取引を組み込むコンセンサスノードは、その責任を負うインセンティブを必要とします。加えて、その仮想通貨を利用しているすべてのユーザーが特定のエンティティの通貨に対して関心を持っているわけではありません。

これらの問題を踏まえて、複数の資産が運用可能である台帳の主要トークンが橋渡し通貨として効果的に機能し、それによって分散型市場の形成を可能にすれば、そのメリットは計り知れません。これによって、さらに機能を向上させるような特殊な目的を持った資産を発行することができます。例えば、融資および送金業務に役立つTetherやMakerDAOのような安定価値資産の発行です。

カルダノは複数の資産の相互運用を可能にするために実践的なアプローチを採用しています。最初の課題は、何千もの**UIA**のニーズに応えるために必要なインフラストラクチャを設計することです。これには以下のアップグレードが必要となります：

1. 大規模な**UTXO**の追跡を可能とする専用の認証データ構造
2. 膨大な量の保留中トランザクションを格納するための分散型メモリープール機能

3. 巨大なグローバルブロックチェーンを可能とするためにブロックチェーンの パーティション分割およびにチェックポイントの配置を行う
4. コンセンサスノードが異なるトランザクションセットに取り組むことに対するインセンティブの仕組み
5. ユーザーに任意の通貨の追跡を可能とする閲覧機能
6. **UIA**がネイティブの資産と同等のセキュリティを享受する
7. **UIA**と主要トークン間の流動性を向上させるような分散型市場を形成するための支援

正しい認証データ構造を発見するための予備的な取り組みにより、**IOHKとWavesのLeo Reyzinが共同開発した新しいタイプのAVL木**が考案されました。さらなる研究が必要となりますが、これはカルダノに後に導入されることになる基礎的なアップグレードです。

分散型メモリープール は、スタンフォード大学の **RAMCloud プロトコル**を使用して実装することができます。このプロトコルをカルダノのコンセンサス層へ統合することを検討するための実験は、**2017**年第**3**四半期に開始される予定です。

残りのトピックは今後の継続的な研究によって進められます。その成果如何によりますが、**2018**年に公開される**Basho of CSL**の時期に、我々はカルダノに**UIA**のためのプロトコルを実装する予定です。

拡張性

分散システムは、共通の目標を達成するためにプロトコルまたはプロトコル群を実行することに同意したコンピューター（ノード）の集合体によって構成されています。目標としては、**BitTorrent**プロトコルのようにファイルを共有することや、**Folding@Home**のようにタンパク質の折りたたみ構造を解析することなどが挙げられます。

最も効果的なプロトコルは、ネットワーク内のノードが増えるにつれ、より多くのリソースを獲得しています。たとえば、**BitTorrent**によってホストされているファイルは、多くのピアが同時にダウンロードしている場合、より高速にダウンロードを行うことができます。これはピアがリソースを提供すると共に消費しているためであり、これは分散システムに拡張性があると主張する際に挙げられる特性でもあります。

現在の仮想通貨に共通している設計課題は、これらが拡張するように設計されていないということです。たとえばブロックチェーンとは通常、ブロックの追加のみが行える連結リストです。ブロックチェーンプロトコルのセキュリティと可用性は、多くのノードがブロックチェーンデータの完全なコピーを所有していることに依存しています。つまり**N**個のノード間で**1**バイ

トのデータを複製する必要があります。したがって、ノードを追加することによってリソースが追加されるわけではありません。

トランザクション処理とシステム全体にメッセージを広めることにも同様のことが言えます。コンセンサスシステムにノードを追加したとしても、トランザクション処理能力が向上するわけでありません。それは同等の仕事を行うためにより多くのリソースを消費するということなのです。中継ネットワークの増加は、ネットワーク全体を最新のブロックと同期させるために、より多くのノードが同じメッセージを発信する必要があることを意味します。

このトポロジーでは、仮想通貨は従来の金融システムと同様の方法でネットワークを拡張することができません。これとは対照的に、従来のインフラストラクチャは拡張性が高く、処理能力とストレージ能力が桁違いにあります。より具体的には、ビットコインは、従来の金融システムに比べて非常に小さなネットワークでありながら、現時点での負荷の処理に四苦八苦している状態です。

カルダノの拡張性は、そのコンセンサスアルゴリズムによって可能となります。ウロボロスは、**Google** や **Facebook**[10] などの大規模なインフラストラクチャプロバイダのニーズに応えるために、過去**20**年間に開発された従来のプロトコルを実行できるコンセンサスノードのクォーラム（分散型システムにおいてトランザクション処理を実行するために必要なノード）を分散化された方法で選出することができます。

たとえばあるエポック（時代）のためにクォーラムを選出するということは、特定の期間において、台帳システムを維持するための信頼できる一定数のノードが存在することを意味します。複数のクォーラムを同時に選出し、一定数のトランザクションをそれぞれのクォーラムに割り当てることは大した問題ではありません。

同様の手法をネットワークの伝播やブロックチェーン自体の分割に適用することができます。現在のロードマップでは、拡張方式は**2018**年以降にウロボロスに適用され、**2019**年と**2020**年にも引き続き焦点が当てられることになっています。

カルダノ・コンピュテーション層

前述したように、トランザクションには**2**つのコンポーネントがあります。トークンを送信し、その流れを記憶する仕組みと、そのトークンの移動を制御するシステムです。後者には、テラバイトのデータ、複数の署名、特別なイベントが発生するような複雑なものもある一方で、単一の署名によって資産を別のアドレスに移動するような非常に単純なものもあります。

[10] **Elastico**や**ビットコイン-NG**など、同じ目的を達成しようとする独自の研究プロトコルもあります

お金の流れをモデル化する上での課題は、それがエンティティにとって内密なものであり、彼らがどのように利用しているのかを予測するのが非常に難しいということです。契約法からの教訓は、トランザクションが商業的現実と一致していないにも関わらず、アクター自身に自覚がないということです。我々は、一般に、この現象を「セマンティクス的ギャップ」[11]と呼んでいます。

何故仮想通貨は複雑性と抽象性を追い続けるべきなのでしょうか。これは本質的に実現不可能で、現実的に安直な考えに見えます。さらに、抽象化が進むにつれて、法的およびセキュリティ上のリスクも出てきます。

例えば、児童ポルノ、人身売買や国家機密の売却など、普遍的に違法または侮蔑的とみなされる多数の活動がインターネット上で行われています。堅牢な分散型インフラストラクチャを導入したところで、通常の商取引が享受するのと同等の検閲規制の枠内で活動するこれらのアクティビティに対してチャンネルを提供しているにすぎません。また、効率化を図るために連合化を促進するインセンティブがあるコンセンサスノードが、コンテンツを失ったことに対してその責任を負うべきかについては、法的には明確化されていません。

Tor運営者の訴追、Silk Road運営者の残酷な扱い、そしてプロトコル参加者の法的保護に関する明確な法律が全体的に欠如しているということは、不確実性がシステムに内在していることになります。十分に高度な仮想通貨がさらなる悪事に加担しかねないとは限りません(Ring of Gygesを参照)。仮想通貨を利用しているすべてのユーザーがウェブ上での最悪の行為を推し進めるか、少なくともそれを可能とすることは理にかなっていると言えるのでしょうか。

残念ながら、仮想通貨の設計者の考えに関する明確な答えはありません。これはどちらかといえば立場を選び、そのメリットを弁護することです。カルダノとビットコインの両者が持つ利点は、階層化を取り入れることで関心の分離を行なったということです。ビットコインでは、Rootstockがあります。カルダノにはカルダノ・コンピュテーション層があります。

前述で述べた動作を可能とする複雑な処理は**CSL**上では実行できません。**CSL**は、チューリング完全な言語で書かれたプログラムを実行する能力と、計算処理を計測するための何らかのガス経済を必要します。また、コンセンサスノードが自身のブロックにトランザクションを自発的に取り込む必要があります。

加えて、**CSL**の機能の制限することによって、ユーザーを合理的に保護することができます。これまでのところ、ほとんどの先進国の政府は、仮想通貨の使用または維持が違法行為であるという立場を取っていません。今後、大多数のユーザーは、デジタル決済システムと同等の能力を有する台帳システムを安心して維持できるようになるでしょう。

[11]**Loi Luu**らは[Making Smart Contract Smarter]においてこのギャップについて論じている。

能力を伸ばしたい場合には、**2**つの方法があります。**1**つはポーカーのように短期的に同じ目的を持った個人の集りであり、もう一方は、イーサリアムのような能力を持った台帳システムによって可能となります。どちらの場合においても、我々はイベントを別のプロトコルにアウトソーシングすることを選びました。

プライベートで短期的なイベントでは、ブロックチェーンパラダイムを完全に回避し、むしろ同じ目的を持った集団が任意に実行可能な専用の**MPC**プロトコルライブラリへの取り組みを制限するのが合理的です。計算処理とアクティビティは、プライベートネットワーク内で統合され、**CSL**は信頼できる掲示板、また必要に応じてメッセージを発信するチャンネルとして機能します。

ここで重要なのは意志とプライバシーについての同意があり、またそれらをカプセル化し得るということです。**CSL**は公園でプライベートなイベントを開催するような、ユーザーが出会い、コミュニケーションを行うことを用意とする専用のサイトを提供しないデジタルコモンズとして利用されます。さらに、専用**MPC**を利用することで、ブロックチェーンを膨張させずにレイテンシの低い対話が可能になります。これはシステムの拡張性に繋がります。

このライブラリに向けたカルダノの研究活動は、海外の科学者からの支援共々、東京工業大学の研究所にて集約されています。このライブラリはジェロラモ・カルダーノと同時代の数学者の名にちなんで「タルタリア」と呼ばれており、**2018**年第**1**四半期に初期実装を予定しております。

能力を伸ばす方法として２番目に掲げたケースでは、仮想マシン、一定数のコンセンサスノード、および**2**つのチェーン間の通信を可能にする仕組みが備わったブロックチェーンが必要となります。我々はイリノイ大学の研究チームと提携を結び、フレームワーク**K**[12]を用いてイーサリアム仮想マシンの厳格な形式化を行なっています。

この分析の結果から最終的には明確な操作的意味論と仕様によって正確に実装された強力な正確性を備えた分散型仮想マシン[13]を複製し、設計する最適な方法を導き出すことができます。つまり、仮想マシンはコードに記述されている通りのことを最小限のセキュリティリスクで実行するということです。

イーサリウムによって提案されたガス経済についてと、**Jan Hoffmann**らの資源認識**ML**のような、計算処理のための資源評価についての広範な研究とがどう関係しているかについては未

[12]**K**は**Grigore Rosu**教授らによって発明された言語に依存しないマシン実行可能セマンティクスのための普遍的なフレームワークです。我々の活動より前には、**C**、**Java**、**JavaScript**のモデリングに利用されています。
[13]これは異なるコンセンサスノードが別々のスマートコントラクトを実行することを意味しますこれはステートシャーディングとも呼ばれます

解決の問題が依然として残っています。また我々は、仮想マシンの言語依存性の程度についても関心があります。たとえば、イーサリアムプロジェクトでは、現在の仮想マシンから**Web Assembly**への移行を望んでいます。

次の段階は、分散アプリケーションによってサービスとして呼び出されるステートフルなコントラクトを表現するための合理的なプログラミング言語を開発することです。この課題に関して言えば、低保証アプリケーションには従来のスマートコントラクト言語である**Solidity**を対応させると同時に、正式な検証を必要とするより高保証なアプリケーションには**Plutus**と呼ばれる新しい言語を開発するというアプローチを採用しました。

Solidityに基づいたツェッペリンプロジェクトと同様に、**IOHK** もまたアプリケーション開発者が自身のプロジェクトで使用することのできる**Plutus**の参照ライブラリを開発します。また、**UCSD's Liquid Haskell**プロジェクトからの触発された正式な検証のための専門ツールの開発を行います。

コンセンサスの観点からすると、ウロボロスはスマートコントラクトの評価をサポートできるようにモジュラー方式で設計されています。したがって、**CSL**と **CCL**の両方が同じコンセンサスアルゴリズムを共有します。違いは、ウロボロスはトークン配布を介して許可型、無許可型の両方の台帳システムを許容することができるという点です。

CSLでは、**Ada**はトークン生成イベントによってアジア全体の購入者に配布され、最終的には流通市場で再販売されます。これは、**CSL**のコンセンサスアルゴリズムが、多様でより分散されたアクターまたは委任者によって制御されることを意味します。**CCL**では規制機関である委任者によって管理されている独自のトークンを発行することができ、これによって許可型台帳システムを構築することができます。

この柔軟なアプローチによって、**CCL**の異なるインスタンスがトランザクションの評価に関する異なるルールを採用することが可能となります。例えば、**KYC/AML**（顧客確認）データを提示できないユーザーに対してギャンブル活動に制限をかけることは、属性値がないトランザクションをブラックリストに載せることによって可能となります。

我々の最終的な設計目標は、信頼できるハードウェアセキュリティモジュール（**HSM**）をプロトコルスタックに追加することです。これらの機能をプロトコルに導入する際には、**2**つの大きな利点があります。まず、**HSM** を導入することによって大幅なパフォーマンス向上[14]に繋がります。これにはベンダーを信頼するという以外にセキュリティ上の懸念はありません。また、**Sealed Glass Proof (SGP)** を使用することにより、**HSM** は、データの検証後、悪意のある部外者にコピーまたはリークされることなく確実に破壊します。

[14]コーネル大学の http://hackingdistributed.com/2016/12/22/scaling-bitcoin-with-secure-hardware/を参照

後者に焦点を当てると、**SGP**は、コンプライアンスに革命的な影響を与える可能性があります。通常、消費者が身元を認証し、参加権を証明するための個人識別情報（**PII**）を提供する際、この情報は悪用されないことを前提として信頼できる第三者に引き渡されます。このようなアクティビティはもともと集中管理されているため、データ提供者は**PII**に対するコントロールを失い、管理者の管轄に基づくさまざまな規制の対象となります。

信頼できる証人を選出し、孤立領域基盤に**PII**を格納するということは、十分な能力の**HSM**を所有しているアクターが、検証者に身元を知られることなく、偽造不可能な方法で自身に関する事実を検証できることを意味します。これは、ボブはアメリカ市民ではないということ、アリスは、認定投資家であること、ジェームズは、米国の納税者であり、特定のアカウントに課税利益を送信する必要があることに対して検証が行えるということです。

カルダノの**HSM**戦略は、[インテル**SGX**](#)と[**ARM Trustzone**](#)を使用して、今後**2**年間に渡ってプロトコルの実装に取り組みます。どちらのモジュールも、ラップトップから携帯電話まで数十億個の消費者向けデバイスに組み込まれているため、消費者側ではこれを使用するために新たなデバイスを必要としません。どちらも、最大規模の資金提供を受けたハードウェアセキュリティチームの徹底的な審査、優れた設計、そして長年に渡る継続的な開発に基づいています。

規制

現代の金融システムの厳しい現実とは、その規模が拡大するにつれて、規制の必要性、または欲求が蓄積されていくことです。それは、一般的にはいくつかのアクターの怠慢または市場に潜む陰謀の結果です。

例えば、**1907**年恐慌では、貸し手の最終手段として**1913**年に連邦準備制度を創設しました。もう**1**つの例は、**1920**年代アメリカでの過剰投資によって財政が崩壊した大恐慌です。この崩壊により、同様の出来事を防ぐため、あるいは崩壊を招いたアクターの責任を問うために**1934**年に証券取引委員会が創設されました。

規制の必要性、規制対象の有効性について合理的な議論を行うことはできますが、規制の存在と政府がその施行に熱心に取り組んだことを否定できません。しかし、世界がグローバル化し、資産がデジタル化するにつれ、すべての規制機関は**2**つの課題に直面します。

第一に、複数の管轄区域を扱う際には、どの規制が優先されるべきなのでしょうか。単一のトランザクションが幾重もの国境を１分未満で越えるとき、ヴェストファーレンのような時代遅れの体制は一瞬で崩壊していたでしょう。単に地政学的に最も影響力のある地域が優先されるべきなのでしょうか。

第二に、プライバシー保護技術の向上はデジタル軍備競争を勃発させたために、トランザクションに参加者、または特定の資産を保有している人物を追跡するのがより困難になったことです。秘密が保持されている**12**つのパスフレーズ[15]で何百万ドルもの資産を管理できる世界では、効果的な規制をどのように実施するべきなのでしょうか。

あらゆる金融システムと同様に、カルダノプロトコルは公正かつ合理的であるかどうかを意識して設計する必要があります。我々は、個人の権利と市場の権利を分離することにしました。

個人は弾圧または資産を没収されることなく、自身の資金への独占的なアクセスを常に有するべきです。ベネズエラとジンバブエで腐敗した政治家が個人的利益のために主権を乱用しているため、全ての政府が信頼できるわけではなく、従ってこの権利は強く主張されなければなりません。仮想通貨は大多数の人々のために設計されなければなりません。

次に、歴史は決して改ざんすべきではありません。ブロックチェーンは、その不変性を保証します。歴史をロールバックする、あるいは公式記録を変更する力を導入することは、特定の人物や集団が利益をもたらすために、過去を変えようとする誘惑を誘発します。

また、お金の流れは自由でなければなりません。資本統制やその他の障壁は人権を制限することになります。それらを強制するのは無駄だとは言え[16]、生活資金を得るために自国の管轄外で働く最貧国の市民が多数いる世界経済において、資本の流れを制限することは、通常は、世界で最も貧しい人々に害を及ぼします。

これらの原則を踏まえれば、市場は個人とは明らかに異なります。カルダノの設計者は個人の権利を尊重する一方で、市場は公的に条件を主張する権利があり、個人がこの市場でビジネスを行うことに同意する場合、システム全体の完全性のためにその基準に従わなければなりません。

課題は常に施工コストとその実用性です。小規模かつ多管轄の取引に対して、詐欺または商事紛争に関する高保証の償還を提供することは、従来のシステムではコストがかかりすぎます。ナイジェリアの王子[17]に電信送金を行なったとき、通常その資金を返済してもらうのに通常は苦労することでしょう。

カルダノにとって、我々は**3**つのレベルから革新が行えると考えています。まず、スマートコントラクトを利用することによって商業関係の条件を上手く制御することができます。すべて

[15]**BIP39** https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki を参照
[16]キャピタルフライトの対策の一例として、Hawala Banking Systemを参照
[17]Advance-fee詐欺を参照

の資産がデジタル化され、**CSL**のみを用いて表現できる場合、詐欺のない商取引に対する強力な保証を得ることができます。

次に、**PII**の漏洩なしに、認証や信用アクターに利用できる**HSM**を用いて**ID**スペースを提供することによって、グローバルな評判システムを導入し、自動化された税務コンプライアンスを備えたオンラインゲームや分散型取引所などの低コストの規制された活動を実施できるようになります。

最後に、カルダノのロードマップには、ユーザーが書いたスマートコントラクトに可変性、消費者保護、仲裁機能を追加するために、スマートコントラクトと対話可能なカスタマイズが行えるモジュラー化された規制**DAO**の作成が記載されています。このプロジェクトについては、別の論文にて概説を行います。

なぜこのようなことを行うのか

カルダノは、仮想通貨業界内外の何百人もの有識者からのフィードバックを取り入れた長期プロジェクトです。そこでは、たゆまぬ取り組み、査読の積極的な使用、さらには偉大なアイデアの借用さえもが行われています。

残りのセクションでは、プロジェクトの中核的な要素であると我々が判断した特定の側面についてそれぞれ取り上げます。これにはカルダノの進化特有のものもあれば、仮想通貨業界の全体的なベストプラクティスの向上を期待して選ばれたものもあります。

あらゆる目標を取り上げ、すべてのユーザーを満足させるプロジェクトは存在しませんが、我々の目的は自己進化型財務スタックがどうあるべきであるかについてのビジョンを、それが欠如している管轄に提供することです。仮想通貨の本質は、従来の金融システムを混乱させることではありません。従来の金融システムでは、常に変化を吸収し、その形態と機能を維持することができます。

むしろ仮想通貨の設計者は、既存の銀行システムが高すぎて導入できず、**1**日の生活費が数ドルであり、安定したアイデンティティを持たず信用を得ることが不可能であるような地域に目を向けるべきです。

これらの地域において、支払いシステム、財産権、身分証明書、信用リスク、およびリスク保護を携帯電話で実行される単一のアプリケーションにまとめ上げることは、単に有用なだけではありません。それは人生を変えるほどのものです。我々がカルダノを構築する理由は、発展途上国のためのこのビジョンを提供する、少なくとも進展することに対して確実な見込みがあると判断したからです。

たとえ我々が失敗したとしても、既存の仮想通貨の設計、進化、資金提供の方法を変えることができれば、大きな成果を得たことになります。

2. 科学と工学

イテレーション開発

仮想通貨は、ソフトウェアとして実装されたプロトコルです。プロトコルとは単に参加者間の知的な会話です。ソフトウェアは究極的にはいくつかの目標を与えられたデータの操作です。しかし、信頼性が非常に高いソフトウェア及び有用で安全なプロトコルと、その逆のものとの違いは完全に人間的です。

優れたソフトウェアは説明責任、明確なビジネス要件、繰り返し可能なプロセス、徹底したテストと飽くなき反復を必要とします。優れたソフトウェアには、問題を解決できるシステムを適切に設計するための専門知識と、才能のある開発者が求められます。

有用で安全なプロトコル、特に暗号と分散システムを含むプロトコルは、より学術的で規格駆動のプロセスから始まります。プロトコルが有用であることを保証するためには、査読、無限の議論、トレードオフの確固たる概念が必要です。しかし、これだけでは十分ではありません。プロトコルを実装し、実際に使用し、テストしなければなりません。

仮想通貨業界特有の課題は、全く異なる**2**つの哲学が適切な弁証法を行わずに絡み合っているということです。我々の命題は、若さ、欲求、情熱に支えられたスタートアップの心構えである「迅速に行動し、破壊する」ことです。これに対する反対命題は、十分な資金と威信を享受しながら、業界の革新をニッチのようなものに入れ込んで確実にしようとする願望によって動機付けされた、慎重かつ系統的で、学問的なアプローチです。

その結果、多くの仮想通貨は、ほとんど意味のないホワイトペーパーによって策定されたか、または急いで書かれたプログラムコードです。現在、時価総額トップ**10**[18]の仮想通貨のいずれも、査読されたプロトコルに基づいてもいなければ、正式な仕様[19]からの実装も行われていません。

しかし、これらには数十億ドルの価値が絡んでいます。一度導入されると、仮想通貨に変更を加えることは非常に困難です。ユーザーは、安全なシステムの使用と、マーケティングの主張の正当性をどのように知ることができるのでしょうか。提案されたプロトコルが達成できない場合には、どうなるのでしょうか。

この命題の欠如にも関わらずプロセスのみが尊重されていることが、**IOHK**がカルダノを構築したかった主な理由です。我々の望みは、より効果的で、誠実かつ正直な方法で取り組む事例として参考となるプロジェクトを開発することでした。

目標は、ソフトウェアとプロトコル開発する上でのまったく新しい手法を提案するのではなく、素晴らしいソフトウェアとプロトコルがすでに存在することを認識し、その創造につながった条件を踏襲することです。次に、これらの案件をできる限り一般に知られるようにオープンソース化し、業界全体の利益となるよう参照可能にすることです。

事実と意見

もう一つの懸念は、事実と意見の境界線が曖昧なことです。この世には、何百ものプログラミング言語、数多くの開発パラダイム、プロジェクト管理に関する幾多もの哲学があります。学界は、ビジネス上の懸念や実用性から遠ざかっていることから、独自の課題を抱えています。

カルダノはまず、工学の観点から普遍的に有用であると認められる明らかな欠点を捕らえようと試みました。たとえば、暗号化システムと分散システムの両方が非常に複雑なトピックであるため、安直な行為によって恐ろしい間違いを犯した事例は数多くあります。したがって、これらの分野からの識見を必要とするプロトコルは、定評のある専門家によって設計され、他の専門家が審査を行うために提出される必要があります。

ウロボロスはこの分野において最初のケーススタディです。これは、公的に検証可能な出版履歴を持つ暗号学者達の大規模かつ多様なチームによって設計され、標準的な暗号プロセス、セキュリティの仮定、敵対的なモデルおよびその証明などに基づいて構築されました。これら

[18]時価総額による包括的なリストについては **www.coinmarketcap.com** を参照
[19]イーサリアムには、**Yellow Paper**と呼ばれる半正式な仕様があります。 ただし、**EVM**のセマンティクスは完全には規定されておらず、プロトコルの完全なる実装には不十分です。

の証明は学会への提出[20]およびに、ケンブリッジ大学の研究チーム[21]開発の定理証明システム**Isabelle**によって独自に検証されました。

しかし、この作業だけではその有用性を保証できません。いくつかの仮定を踏まえたセキュリティモデルの厳密なチェックを行なっただけです。有用性を実証するためには、プロトコルを実装し、テストする必要があります。我々の開発者は**Haskell**と**Rust**の両方で検証を行いました。この作業により、同期モデルに焦点を当てる必要があることが明らかになりました。これはウロボロス・プラオスの策定にもつながります。

このようなイテレーション開発が素晴らしいプロトコルを生み出すのです。それぞれのステップが新しい教訓をもたらし、前のステップの正しさの再確認を要求するからです[22]。プロトコルが正しく設計されていることを確認するのは費用と時間がかかり、時には非常に面倒であっても、必要とされています。

プロトコル 、特に何十億もの人々によって使用されるものは短命でもなければ、急速的に進化するわけでもありません。むしろ、それは何十年も利用されることを目的としています。今後**100**年間は利用されるであろう新しい金融システムを世界に押し付ける前に、設計者に対して厳しい要求を行うのが合理的でしょう。

関数型の罪

より偏見を伴った話題に話を移しますと，ツール，ソフトウェア開発に使用される言語と方法論は、客観的実在というよりも宗教的な摂理による成果物です。ソースコードは散文のようなものです。誰もが何が良いのかということに対して意見を持っています。時には伝える内容よりも、その伝達方法の方が重要である場合もあります。

我々は、他人には間違っていると受け取られかねないものを選ばなければなりません。しかし、我々の選択の背景には、その判断を正当化するための基盤があります。

カルダノを実行しているプロトコルは、純粋関数型言語である**Haskell**で実装されています。ユーザーインターフェイスは、**Electron**のフォークである**Daedalus**によってカプセル化されています。我々はできるだけ**Web**アーキテクチャモデルを採用し、データベースで**Key-Value**パラダイムを取り上げるために**RocksDB**を使用しました。

[20]カリフォルニア州で開催された**IACR**の**Annual Crypto Conference**の論文番号**71**
[21]ローレンス・ポールソン教授の監督下の **Kawin Worrasangasilpa** による
[22]少し話が逸れますが、これに関しては[ハルモス教授の数学の教科書の書き方についてのディスカッション]を是非ご覧になってください

コンポーネントレベルから見れば、この抽象化はメンテナンスがはるかに容易になり、より優れた技術が苦もなく導入され、また我々の技術スタックが**Github**と**Facebook**の開発成果に部分的に結びついていることを意味します。

WebGUIを使用することで、**React**を活用し、フロントエンドの機能を何十万人もの**JavaScript**開発者が理解できるツールを使用して開発することができます。**Web**アーキテクチャを使用するということは、コンポーネントをサービスとして扱うことができ、セキュリティモデルが分かりやすくなることを意味します。

プロトコル開発のために**Haskell**を採用することは、最も困難な選択でした。関数型言語の世界でも、選択肢は豊富にあります。より柔軟で不純な言語として、**Clojure**、**Scala**、**F#**のようなものがあります。これらの言語は、**Java**と**.NET**エコシステムの膨大なライブラリの恩恵を受けるとともに、機能プログラミングの最良の側面を確保しています。

Agdaや**Idris**のような学問指向の言語は、正確性に関して強力な検証を可能にする技術と密接に関連しています。しかし、彼らには手ごろなライブラリや、卓越した開発経験がありません。

カルダノでは、**Ocaml**と**Haskell**どちらかを選ぶことにしました。**Ocaml**は、素晴らしいコミュニティ、優れたツール、十分な開発経験、そして**Coq**による正式な検証に関する素晴らしい資産を持つ言語です[23]。では我々はなぜ **Haskell** を選んだのでしょうか。

なぜHaskellなのか

カルダノを構成するプロトコルは暗号学によって配布、バンドルされるため高度なフォールトトレランスを必要とします。最も好調な日でも、ビザンチンアクターが出現したり、不正な形式のメッセージが発信されたり、誤ったクライアントが意図せずにネットワーク上に何らかの騒ぎを起こしたりするかもしれません。

まず、**Quickcheck**などや、**Refinement Types**のような、より洗練された技術を容易に使用できる強力な型システムを採用でき、フォールトトレランスにある程度期待ができる言語を使いたいと考えました。**Haskell**と**Ocaml**等が前者を満足させるのに対し、**Erlang**スタイルの**OTP**モデルは後者を満たします。

[23]この点に加えて、**IOHK**は実際には**Ocaml**で**Qeditas**と呼ばれるプロジェクトを変名**Bill White**から継承し、実装しています

Cloud Haskellを導入したことで、**Haskell**独自の機能を維持しつつ、**Erlang**の利点の多くを獲得することができました。さらに、**Haskell**のモジュール性と合成性により、**Time Warp**というカルダノ専用の軽量ライブラリを使用することができました。

次に、**Haskell**のライブラリは、Galois、FP Complete、Well-Typedなどの商業用エンティティの広範な開発によって、ここ数年で大幅な進化を遂げました。結果として、**Haskell**を使用して本番レベルのアプリケーションを書くことができるようになりました。[24]

さらに、PureScriptの急速な進化は、**Clojurescript**が**Clojure**に与えたように、**Haskell**と**JavaScript**の間の必要不可欠な架け橋となっています。カルダノのブラウザ上での動作、またモバイルウォレットの開発には、**PureScript**が特に重要になると考えています。

加えて、依存関係の解消に関して言えば、**Haskell**は、過去数年間、**FP Complete**から強力な援助を受けて作り出され、容易に利用できるStackageを通して、Michael Snoymanのような技術者が達成した重要な社会的、技術的成果から恩恵を受けています。

また、適切に依存性を解決した上で、我々はソフトウェアのビルドを再現可能にすることを目指しています。つまり、同じ構成値と依存バージョンであれば、まったく同じ成果物が作成されるということです。**Stackage**を通して、我々はNixOpsを利用し、その再現性を獲得することができました。

最後に、**Haskell**に特化した才能ある開発者の人口は、他の言語と比較してもかなり大きく、彼らは学術的にも、業界的にも十分に訓練されています。また熟練の**Haskell**開発者の中にコンピューターサイエンスに関する豊富な知識を持っていない者はほとんどいないため、**Haskell**は優秀な人材を確保するためのフィルターとしても機能します。

正式な仕様と検証

証明可能な正しいセキュリティモデルを使用してプロトコルを開発することの強みは、敵対的なパワーの限度に関する保証を提供することです。プロトコルが守られ、証明が正しければ、敵対者には、プロトコルのセキュリティ性に違反することができないという約定が与えられます。

[24] **Bryan O'Sullivan**氏は、ここで**Haskell**の産業利用について素敵な話をしてくれています。

より深く洞察すれば、前述の主張の重要性がより明らかになります。敵は予想外に知的かつ有能である場合もあります。数学的モデルだけで彼らの攻撃を防ぎきれるというのは言い過ぎです。それは全く真実ではありません。

現実は、純粋なセキュリティと正常な動作の妨げとなる要因と環境をもたらします。実装が間違っている可能性があります。ハードウェアは、これまで考慮されていなかったベクトルからの攻撃を呼び込む可能性があります。セキュリティモデルが不十分であり、実際の使用に準拠していない可能性があります。

従って仕様、厳重性及びチェックがどれほどプロトコルに要求されているかについての判断が必要となります。例えば、SeL4 Microkernelプロジェクトのような試みは、曖昧さに対する徹底的な攻撃であって、**10,000**行未満の**C**言語のコードを検証するために、ほぼ**200,000**行の**Isabelle**コードを必要とする主要な例です。しかし、オペレーティングシステムのカーネルは、適切に実装されていないとセキュリティ上の深刻な脆弱性となりうる重要なインフラストラクチャです。

すべての暗号化ソフトウェアは同様の難題に取り組まなければならないのでしょうか。あるいは、同等の成果を生み出すことのできる、それほど厳重ではない手段を選ぶことはできないのでしょうか。また、それが実行されている環境に脆弱性があると悪名高い**WindowsXP**などであるならば、プロトコルを完全に実装しようとするのは無意味ではないでしょうか。

カルダノは、以下の点に関して妥協を行いました。まず、暗号技術と分散コンピューティングの複雑な性質のために、検証は非常に繊細で、長く、複雑で、時には至って専門的になる傾向があります。これは、人間によって行われる検査が退屈でエラーを起こしやすくなることを意味します。したがって、コアインフラストラクチャを網羅するために作成されたホワイトペーパーに示されている重要な証明はすべてコンピューターでチェックする必要があると考えています。

次に、**Haskell**のコードが当社のホワイトペーパーに正確に対応しているかの検証には、LiquidHaskellを介した**SMT**証明者とのインターフェースと**Isabelle/HOL**のいずれかを選択することができます。

SMT（充足可能性モジュロ理論）ソルバーは、等式または不等式を満たす関数パラメータを見出す、あるいはそのようなパラメータが存在しないという課題に取り組みます。De MouraとBjørnerが議論したように、**SMT**の使い道は様々ですが、重要な点は、これらの手法が強力であり、バグやセマンティックエラーを劇的に減らすことができることです。

一方、Isabelle / HOLは、実装の特定と検証の両方に使用できる表現力豊かで多様なツールです。**Isabelle**は、高次論理構造を扱う包括的な定理ソルバーであり、検証に使用される集合やそ

の他の数学的オブジェクトを表現することができます。そのような制約を伴う問題に取り組むために**Isabelle**は**Z3 SMT**検証システムと統合しています。

どちらのアプローチも有益であるため、両者を段階的に採用することにしました。人間によって記述された検証は、**Isabelle**でコード化され、その正確性を確認し、それによって我々のシステム化された検査の要件を満たしたことになります。そして、**2017**年と**2018**年にかけてカルダノに実装されているすべての本番コードに**Liquid Haskell**を徐々に追加する予定です。

最後に、正式な検証は、検証している仕様と利用できるツールセットと同じくらい優れています。**Haskell**を選択する主な理由の**1**つは、それが実用性と理論の適切なバランスを保っているためです。ホワイトペーパーから得られた仕様は、**Haskell**のコードによく似ており、この**2**つを関連づけることは、命令的な言語で行うよりもはるかに容易です。

適切な仕様をキャプチャし、アップグレード、バグ修正などの変更が必要なときに仕様を更新することは未だに困難ですが、それによって**Haskell**の評価が落ちるようなことはありません。開発者が証明可能安全性の基盤を構築することに苦労しているなら、理論上提案されているものを実装しなければなりません。

透明性

仮想通貨の開発および工学について議論する際の最後の論点は、どのようにプロジェクトの透明性を確保するかということです。設計上の決定とは、開発者の夢に出てきて突然具現化するような、明解な論理値や、エーテルのような非現実的なものではありません。これらは過去の過ちから得た経験、討論、教訓などから生まれたものです。

課題は、完全に透明な開発プロセスが、議論に影響を及ぼし、証拠に基づくものよりも大げさになることです。エゴがコミュニティを勝ち取ろうと試みます。また愚かであるという恐れがあると、会話は無力化し、非生産的なものとなってしまいます。

さらに部外者が、自身に興味のあるトピックのみを取り上げるために会話をすり替えようとするかもしれません。各人が求めているものはそれぞれ異なるからです。

恐れることなく自由に表現しながらも、進捗を開発者に任せているような、委託されたコミュニティが開発プロセスの必要性に関する透明性のバランスを保つためにはどのようにすれば良いのでしょうか。

カルダノでは、指揮監督のもとで規格駆動のプロセスを行う方法を採用することにしました。コミュニティは理論とコードがよく考えられ、検証されており、それによって開発者が解決したと主張するような物事が、実際に解決されているかどうかを確認する必要があります。

そのために査読は、科学的要素を完全に満たしていなければなりません。なぜなら、それはまさにこの目的のために設計され、そして現代の世の中を切り開いてきたからです。

コードについては意見が分かれます。カルダノでは、カルダノ財団を**IOHK**の成果物の最終審査員として選任しました。特に、彼らには以下の任務が委ねられています。

1. カルダノ**Github**に含まれるソースコードに対して定期的にレビューを行い、その品質、テストカバレッジ、適切なコメントと完全性を確認する
2. カルダノ全てのドキュメントに対してレビューを行い、その正確性、有用性を確認する
3. 科学者によって作成されたプロトコルが実装されているという主張に対して検証を行う

この務めを果たすために、**IOHK**は定期的でタイムリーな報告書を財団およびその代理人に提出し、審査を行ってもらいます。財団は、少なくとも四半期ごとにカルダノのコミュニティへの開発監視報告書をリリースする予定です。

この最初の取り組みに関しては、分散型プロジェクトがどのように説明責任を果たすかについて、より幅広い会話が開始される予定です。信頼できる第三者からの開発監督は、開発者が確実に軌道に乗るようにするための強力なツールですが、プロジェクトが常に実現されることを完全に保証するには不十分です。

このため、財団は**CSL**に財務システムを統合後、**IOHK** と共同開発された正式仕様に基づいた代替クライアントを構築する開発チームの奨励を行います。開発の多様性は、単一のアイデアや開発者によってモノカルチャーが形成されるのを回避するために、イーサリウムプロジェクトで使用された素晴らしい技法でした。

仕様に関しては、**WC3**と**IETF**に準拠した標準プロセスから得られる豊富な知識があります。最終的には、カルダノの各プロトコルを統合するには、学術的な作業やソースコードとは独立した仕様が必要となります。むしろ、それは**RFC**のような適切な形式である必要があります。

カルダノ財団の中核となる教義の**1**つは、カルダノプロトコル専用の標準化団体として機能し、カルダノに関連する規格の更新、追加、変更についての意見交換の場を設けることです。**IETF**を通じてインターネット（標準の製品）が、どのようなコアプロトコルを使用するかについてコンセンサスを得ることができるのであれば、専門の機関が同様の結果を導き出すと仮定することも理にかなっています。

最後に、これらの議論をブロックチェーン上でホストされている分散したエンティティとして検討することは興味深いものです。この概念は自律分散組織（**DAO**）と呼ばれ、この分野に関する予備作業が現在進行中です。**IOHK**はカルダノを利用するエンティティのために必要に応じて使用できる参照**DAO**モデルを開発し、カルダノ財団にはこれを自身が定めた基準に基づいて採用する決定権があります。

3. 相互運用性

壮大な思い違い

金融と商取引の包括的なアイデアは、究極的には人々の長年の努力の末に作り上げられたものです。この世には悪い結果が生じた場合に償還請求を行うためのエレガントな言語、意味を汲み取るための正確なツール、無限に発展する技術や、平等な取引を繰り返し模索した結果成立した法律が存在します。事実、初期の書面のいくつかは商業契約でした。

論理や、コンピューター操作、あるいは非情な力を携えた政府の手先の関与を排除したとしても、人間的要素を取り除くことはできません。それは仮想通貨に対する壮大な思い違いです。これらは人間が関わる現実とは往々にして隔てられています。

人々は間違いを犯し、心変わりします。また彼らは、自分が同意しているビジネス関係を完全に理解しているわけではありません。人々は欺かれ、詐取されるのです。個人および国家規模で状況が変化し、それらには独自の解決策が必要されます。念のために言っておきますが、ほとんどの契約には不可抗力条項が含まれます。

しかし仮想通貨は公平性や人々が奮闘する様を考慮しない法制度に完全に縛られている無神経で電子化された判事と雇い入れ、人間への理解、思いやり、判断を捨てようとしています。人類が自分たちの目的のためにルールを変えようと試みてきたことを考えれば、不正に加担しないシステムの存在は非常に新鮮です。

しかし、ユーザーがこれらの新しいシステムを従来の金融システムと融合させる必要があるとすれば、どうなるのでしょうか。また、これらを現代社会で活用するためにはどうすれば良いのでしょうか。たとえば、土地登録などの財産権は、物理的な世界のものです。よって土地のトークン化を行なった場合、その管轄の管理者の承認が必要となります。

別の例を挙げると、金塊は自分で動くことができません。電子化された判事が判決を下しても、人間がそれを受け入れない限り強制することはできません。また、電子台帳が現実とはかけ離れたものになっているかもしれません。

したがって、プロトコル設計者は、自身の仮想通貨と現実世界との関与をどの程度許容するべきかを決定する必要があります。柔軟性が高いほど、絶対的なものに対する忠実の度合いは

低くなります。消費者保護が強化されるほど、ロールバック、払い戻し、履歴の編集を行うための仕組みが増えることになります。

このセクションと次の規制に関するセクションでは、カルダノのこのトピックへ対する実践的アプローチについて説明します。相互運用性の観点から、議論すべき**2**つの大きな分野があります。従来の金融システム (非仮想通貨世界) との相互運用性、そして、他の仮想通貨との相互運用性です。

レガシー

フィンテックは単一の規格または共通の言語で構成されていません。アプローチ方法、決算および清算を担当しているエンティティ、ビジネスプロセス、会計に関わっているドメイン、変革、価値の移動には多様性があります。

単一の技術が優れているだけで、他のエコシステムが敗北を認め、アップグレードを示唆するのは理不尽です。たとえば、多くの人々はリリースしてから**16**年が経過している**WindowsXP**を未だに使用しています。この悲しい状況は**Macintosh**にも同様のことが言え、**1984**年にリリースされた初期型**Macintosh**を**2000**年になっても使用している人々がいました。

消費者行動はさておき、一般的に企業のアップグレードサイクルはさらに遅くなります。多くの銀行は今もなお**Cobol**で書かれたバックエンドを利用しています。インフラストラクチャが機能し、ビジネス要件を満たしていれば、コンプライアンスやセキュリティの問題以外でソフトウェアやプロトコルのアップグレードを行うインセンティブはほとんどありません。

まずカルダノでは、従来のシステムとカルダノとを橋渡しすることが何をもたらすのかを明確にする必要があります。相互運用性についてある程度確かなものを保証するためにはどのようなシステム、エンティティおよびプロトコルを目指すべきなのでしょうか。これらの架け橋は連合化または分散化することができるのでしょうか。あるいは取引所のように、ハッカーや、悪意のある所有者、また過激な規制機関のターゲットとなるシステム上の欠陥の中枢となってしまうのでしょうか。

カルダノには**3**つの懸念があります。まず、情報の表現とその正確さに対する信頼性です。次に、価値とそれに関連する所有権の表現です。最後に、エンティティの表現と、特定のユーザーがそのようなエンティティからどの程度信頼されているかです。

有用であるためには、伝統的な金融界とカルダノの間で情報と価値が自由に行き来する必要があります。そしてその評価を構築し、償還のための基盤を形成するために結果を記録しなければなりません。しかしそのようなことは本質的には、関与するアクターが主体となって管理

しているのがほとんどです。ブロックチェーン上でそれらをエンコードすれば、世界規模かつ永続的なものとなるでしょう。

加えて、従来の世界では価値は常に自由に動かせるわけではありません。禁輸、制裁、資本統制、司法行為により資産が凍結する可能性があります。また相互運用が可能であるためには、価値が漏出するような常に開放された逃し弁を作ってはいけません。

最後に、エンティティのブランドと評判は、商業関係における基盤の**1**つです。ブランドを確立、維持、修復するためのマーケティングキャンペーンには、毎年数十億ドルが費やされています。人または団体に関して誹謗、虚偽、または誤解を招く主張がなされた場合、法的訴訟を求める権利を有します。とは言え、ブロックチェーンは歴史を曲解することなく永久的に保存しようとします。

我々がプログラミング言語を選択したのと同様に、カルダノがこれらの問題を普遍的に解決する理想的な方法は皆無です。むしろ、支持された意見になびくしかありません。

この情報の流れは信頼できるデータフィードと呼ばれています。それには情報源とコンテンツがあります。情報源には信頼の概念と誠実さを維持するかまたは欺くかのインセンティブがあります。コンテンツは任意にエンコードできます。

プロトコルスタックで**Trusted Hardware**の対応を行う予定があることから、**Ari Juel**教授の**Town Crier**プロトコルをサポートすることしました。信頼できる情報源の存在を前提とすると、**Town Crier**はスマートコントラクトや他のアプリケーションで使用できる安全なウェブスクレイピングを可能とします。

Emurgo、**IOHK**、カルダノ財団が情報源のブートストラップリストを提供することになっています。今後これらのリストはカルダノの財務システムから派生した仕組みをコミュニティが利用することによって精緻なリストに置き換えられます。我々の希望は、評判システムが良好なデータフィードによって実現し、それによって徐々に信頼性と忠実性を向上させ、肯定的なフィードバックグループを形成することです。

価値の表現は、より複雑なトピックです。情報は、正確性、適時性、完全性が確立されていれば、プロトコルは信頼性が高い、決定論的な振る舞いをします。一方、価値はより繊細です。

一度トークン化されると、価値は一意のオブジェクトのように動作するはずです。情報はコピーして渡すことができますが、何かの所有権を表すトークン（たとえば所有権の証明書）は、**2**つの異なる台帳に複製して取引することはできません。この行為は、システムの完全性を破壊することになります。

従来のシステムとの相互運用性においてトークン化された価値を扱う上での課題は、トークンが台帳間を移動する際に信頼性、監視能力が変更されることです。たとえば、ボブがビットコインを所有していて取引所に預けた場合、ボブは取引所の台帳にて自身の所有権を主張していることになります。**MtGOX**の場合には、台帳は現実に沿うことなく、ユーザーは全てを失いました。

この問題は、従来の金融システムが仮想通貨内で発行されたトークンを認識する必要性が生じる際にさらに複雑になります。前述のように、企業はソフトウェアのアップグレードや新しいプロトコルへの対応に対して否定的です。このような状況では、明確な解決策を見出すことが困難になります。

カルダノでは、ユーザーに取引に関する豊富なメタデータを添付するオプションを提供し、それらを利用する業界標準が策定されることを期待しています。既に時代遅れの金融プロトコルをアップグレードするために**Interledger**ワークグループ、**R3Cev**らによる研究成果、国際的な義務づけなどいくつかの進展がありました。

しかし、従来のシステムから仮想通貨の台帳に送られてきた価値を定量化し、その有効性を証明する方法については、未だに課題があります。たとえば、ボブが銀行のオーナーで、ドルで裏付けされたトークンを発行した場合、彼はカルダノでのユーザー独自通貨のように、自身のトークンを台帳に送るためにいつでも両者をつなぐことができます。

カルダノは所有権を正確に追跡し、タイムスタンプや監査機能などの機能を提供してくれますが、仮想通貨はボブを正直な銀行家にすることはできません。彼は自身のドルトークンを実際のドルで裏付けしないことによって部分準備銀行を運営することができます。この詐欺は、ドル自体が電子台帳[25]によって占められているトークンでない限り、仮想通貨によって検出することはできません。

最後に、インターネット上のエンティティの表現は、インターネットが発明された頃から存在する古典的なネットワーク問題です。大学、企業、政府機関、そして任意のユーザーは、なんらかの身元確認を行う必要があります。

そこで、ウェブの**公開鍵インフラストラクチャ（PKI）**や**ICANNのDNSシステム**のような実用的で集中化された解決策が実装されました。現代のウェブを我々が享受していることを考えると、これらの解決策は拡張性及び実用性の両方を兼ね備えています。しかし、これらは企業がビジネス行うべきなのかを判断する際に必要な信頼性、信用性、及びその他のメタ特性など、より商業的なデータを提供できるわけではありません。

[25]一方、電子台帳の場合、プルーフオブリザーブは、仮想通貨のみが唯一正直な取引所として機能する巧妙な方法として提案されています。

EBayのような多面的なマーケットプレイスの運営は、取引を完了するためのフレームワークと共に、メタデータをいくつか提供するビジネスモデルを構築しました。コンテンツ、イベント、ビジネスの品質に関する評判は、信頼された情報源からの評価によって大きく影響されることがよくあります[26]。

評価が特定の情報源に左右されるという問題はカルダノにも起こりうることです。カルダノの目標の一つは、発展途上国のための金融スタックを提供することです。これを達成するための鍵となるのが、一度も会ったことのないアクターとの信頼を確立する能力です。

あるエンティティの良し悪しが、コミュニティ全体としての実際のやりとりから導き出された有機的なプロセスではなく、単一のエンティティまたはエンティティのコンソーシアムによって分類される場合、彼らは自らの判断基準に基づいて任意のエンティティをブラックリストに載せることができます。この力は、プロジェクトの価値観に反しており、仮想通貨の利用を大幅に妨げます。

幸いにも、財務に利用される投票システム、信頼できるデータフィードのリストに情報源を追加する方法、プロトコルのフォークに利用している仕組みは、評判システムを確立するために再利用できます。これはオープンな研究領域であり、カルダノのより基本的な要素が定着した**2018**年から**2019**年の間に、分散型評判システム、すなわち信頼できるウェブにオーバーレイプロトコルを提供する予定です。

仮想通貨との相互運用性

分散型台帳については、その相互運用性ははるかに容易です。各台帳には、それぞれのコンセンサスアルゴリズムに関するネットワークプロトコル、通信規格、およびセキュリティの仮定があるため、その定量化は容易に行うことができます。

情報の移動は、外部ネットワークに接続してメッセージを変換することによって確立されます。価値は、中継システム、アトミッククロスチェーン取引、または巧妙なサイドチェーンの仕組みを通じて動かすことができます。中央集権的な管理機関がないため、エンティティの単一表現でさえも、信頼できる開発者、マイナー、その他の実力者のメタ議論を制限します。

カルダノでは、**Kiayias**、**Miller**、**Zindros**氏が開発した新しいサイドチェーンプロトコルの統合を行います。これは、プロトコルに対応する**2**つのチェーン間での価値の移動を安全かつ非対話的に行う方法を提供してくれます。この仕組みは、**CSL**と**CCL**の階層間で価値が移動するための主要な方法となります。

[26]これらの評価は、コンテンツ自体の作成にも影響します。Rotten Tomatoesが映画業界にどのような影響を与えたかについてのこの興味深い記事をご覧になってください。

他の仮想通貨については、価値とユーザーベースでカルダノが成長していくにつれて、連合化された相互関係が形成されるはずです。この成長を促進するために、カルダノ**SL**は相互運用性スクリプト用の制限されたバージョンの**Plutus**をサポートしています。これらのニーズに応えるための新たなトランザクション方法は**Shelly**およびそれ以降のリリースで追加されます。

ダイダロスの迷宮

他の通貨との相互運用性は、グローバルな視点から来ています。専門的なプロトコル、新しいタイプのトランザクション、信頼性を評価するシステム、および情報の流れは、単一のゲートキーパーまたはユーザーを対象としたものではいけません。むしろ、誰でも自由に閲覧できるものでなければならないのです。

しかし、もしカルダノがユーザーによって必要不可欠なプロトコル、トランザクション、またはアプリケーションに対応していなければどうなるのでしょうか。我々は見向きもされなくなってしまうのでしょうか。**Web**は、**1990**年代に同様の懸念に直面しました。

幸い、**Web**はこれに対して**2**つ解決策を見出しており、仮想通貨にもそれらを講じることができます。**JavaScript**の導入により、どんなウェブサイトでも任意の機能を追加することができるプログラム機能が提供されました。また、ブラウザプラグインと拡張機能を導入することで、ユーザーがそれらをインストールできるカスタム機能が追加されました。現代の**Web**は、両方のアプローチを採用したことにより発展してきたのです。

イーサリアムは、ユーザーがそのブロックチェーンのサブプロトコルをスマートコントラクトとして埋め込むことを可能とするような前者のアプローチを採用しました。カルダノは、**CCL**のパラダイムを通じてこの機能をサポートしています。しかし、カスタム拡張機能についてはどうでしょうか。

わかりやすい例としては、仮想通貨のトレーダーが挙げられます。**DM**（**Decentrialized marketplace**）と呼ばれる、様々な仮想通貨を取り扱っている分散型市場を想像してみてください。トレーダーは、**DM**に作用する戦略を自動化したいと考えています。

断片化されたエコシステムでは、トレーダーは仮想通貨ごとに数十のクライアントをインストールし、自動取引を調整するために各クライアントとの対話を可能とするカスタムソフトウェアを作成する必要があります。また、クライアントが**1**つでも更新されると、ソフトウェアが破損する可能性があります。さらに、トレーダーがそのソフトウェアを販売したい場合はどうすればよいでしょうか。

Webの拡張モデルを利用し、様々な仮想通貨のインターフェースを**Web**スタックに取り込めることができれば、トレーダーのタスクは劇的に改善するのではないでしょうか。これが実現すれば、普遍的なインターフェースが確立され、インストールはワンクリックとなり、ソフトウェアの配布は、**Chrome**ウェブストアのようにモデル化することができます。

カルダノでは、ウォレットのフロントエンドに**Electron**を利用することによって、このパラダイムを実験することにしました。これは**Github**によって管理されているオープンソースプロジェクトであり、**Node**と**Chrome**の両方の技術を組み合わせたものです。カルダノが組み込まれた**Electron**アプリケーションはダイダロスと呼ばれています。

ダイダロス[27]の第**1**世代は、消費型パスワードや**BIP39**など、業界標準となっている多くの会計およびセキュリティ機能をサポートする**HD**ウォレットとして機能することでしょう。後の世代では、ダイダロスは普遍的な統合**API**と**SDK**を備え、ストア機能が搭載されたフレームワークとして開発されることでしょう。

技術革新としては、プログラマーが**JavaScript**、**HTML5**、**CSS3**を使用してアプリケーションが構築可能であり、またアプリケーション間の通信に統一された回線を利用することによって、開発が容易に行えることです。暗号化、分散ネットワークの管理、データベースの仕組みなど、複雑な動作を取り除くことで、開発者はユーザーエクスペリエンスとアプリケーションのコアロジックに専念することができます。

ダイダロスを普遍的なフレームワークとするために、そのロードマップと進化は、カルダノからある程度独立しています。**2017**年ではこれらは密接に関連していますが、将来的には、カルダノはダイダロスユーザーのためのアプリケーションの**1**つとなるでしょう。また、インテル**SGX**のみで実行可能な普遍的なキー管理サービスなど、非常にユニークな機能も模索しています。

結局のところ、我々プロトコル設計者は、すべてのニーズに応えることができません。ダイダロスの柔軟性と、**CCL**で実行されるステートフルなスマートコントラクトを組み合わせることによって、我々の設計上の決定から除外されたものを実装できると期待しています。また我々は、すべての仮想通貨がより良い相互運用性とセキュリティを享受できるような規格がダイダロスから実現されることを望んでいます。

[27] これは既に[daedaluswallet.io](daedaluswallet.io)で入手可能です

4. 規制

虚偽の二分法

規制とは気まぐれで不可解なものですが、これを腐敗とそれを告発する検察官との華麗なる繰り返しの物語の比喩として推論することができます。規制は弁護士の道具です。しかし、すべての道具と同様に、それらは粗雑で、古いか、もしくは単に誤用されるかもしれません。

仮想通貨は人間の有様や物語の反復パターンを変えるわけではありません。最善を尽くしたとしても、詐欺、悪意のある者、最悪の事態などは常に存在します。仮想通貨は人間の判断を無視することができますが、その性質を取り除くことはできません。

仮想通貨の設計者は、規制者が悪事を修正するためにどのようなツールキットを提供するべきかについての立場を選ぶ必要があります。仮想通貨は規制と通貨における失敗の産物[28]であるため、独自の課題に直面しています。

文化的に、多くの仮想通貨は、政府の行動が腐敗、不適切、または無効であると見なしています。したがって、規制者や弁護士が過ちを正すための特別な措置を提供することに対してほとんど敬意を払いません。この行為は、仮想通貨の存在意義に反しているためです。

一方、**2009**年**1**月**3**日にプロトコルが開始して以来、**10%**以上のビットコインが紛失及び盗難被害に遭いました。**2017**年**6**月**30**日現在、その被害額は**40**億ドルを超えます。この数字には詐欺や、ずさんな**ICO**によって失われたビットコイン、またその他のトークンが含まれていません。

また、プライバシーに関する問題があります。マクロ規模では、価値は規制、豊富なメタデータがあり、法執行機関、政府機関、国際的な規制機関によって積極的に監視されている特別なチャンネルを通じて流れています。これはしばしば紛失騒ぎに揺れる現金の世界ではよく行われることです。しかし世界がデジタルマネーに移行するにつれ、価値の紛失は徐々に減少しています。[29]

[28]実際、ナカモトサトシ氏はタイムズ紙の見出しを引用したものをビットコインのジェネシスブロックに埋め込んでいます。*タイムズ紙、2009年1月3日「銀行の第2次救済措置の危機」*
[29]読者は、**David Wolman**氏の**The End of Money**を是非読んでみてください。それは現金消滅への国際的な動きを網羅しています。

よって仮想通貨が存在しなかった場合のパラダイムは、金融プライバシーをソーシャルメディアコンテンツのように扱う世界になっていたでしょう。そこにはプライバシーもなければ、システムから逃れることもできません。したがって、我々には明示的な二分法を生み出すジレンマがあります。

仮想通貨の設計者は、その原則を放棄し、管轄のいかなる要求にも応じてしまうことで、ユーザーのプライバシーと完全性を損なうかもしれません。また設計者は、現代のベストプラクティスや法律を無視した、より原理的ながらも無政府主義の哲学を採用することができます。

カルダノでは、この物語が想像力の欠如によってもたらされた、誤った二分法であると感じています。現実には、ほとんどのユーザーは市場に存在するルールを気にしていません。彼らは通常、単一または複数のアクターが自己利益のために突然ルールが変更されることを懸念しています。また彼らは、誰に特権が与えられているのかが不透明であると、不安になります。

我々は、個人と市場の権利を区別する必要があります。仮想通貨が世界的に普及していることを考慮すると、権利は可能な限りユーザー指向である必要があります。

プライバシーは合理的であり、その管理はゲートキーパーではなく、ユーザーによって行われなければなりません。また、価値の移動は自由であり、ユーザーの同意なしに突然没収されるようなことはあってはいけません。

市場の観点からすれば、市場はデータの使用方法、資金の取り扱い方、およびユーザーが規則を遵守していることについて透明性を確保する必要があります。さらに、ユーザーが同意した後は、不都合故に突然規則を変更することはできません。また取引先にも確実性が必要です。

しかし、抽象的なものから具体的なシステムを生み出すにはどうすれば良いのでしょうか。また、実用的かつ合法的なものとは一体どのようなものなのでしょうか。我々はその解決策をメタデータ、認証、コンプライアンスおよびに市場**DAO**の**3**つのカテゴリに分けて考察しました。

メタデータ

何らかの行為を記録することは、それを取り巻くメタデータよりも味気ないときがよくあります。例えば、デンバー市からボルダー市へ運転したというのは行為です。一方、デンバー市からボルダー市へフェラーリ**488**を時速**190**キロで運転したことはメタデータとなります。これはトヨタプリウスで時速**50**キロの運転を行うこととは明らかに異なります。

金融取引もなんら変わりありません。ある行為に関するメタデータは、エコノミスト、税務機関、法執行機関、企業およびその他のエンティティにとって非常に重要です。残念ながら紙幣に基づいた従来の金融システムでは、ほとんどの消費者は、トランザクションのメタデータがどれほど豊かであるか、また誰と共有されているかを知りません[30]。

カルダノは、ユーザーのトランザクションに関するメタデータを税務機関または特定のアクターと共有する必要があることを認識していますが、その共有にはユーザーの同意が不可欠に違いありません。

また、ブロックチェーンシステムは、監査能力、タイムスタンプ、および不変性を提供することによって、不正行為や、浪費、濫用などを排除する大きな力を持っています。したがって、いくつかのメタデータは、カルダノブロックチェーンに投稿される必要があります。

難しいのは、我々のブロックチェーンに負荷をかけないような正しいバランスを見つけることです。この懸念から、我々は実践的なアプローチを採用しました。

まずダイダロスは、今後**12**ヶ月間にわたって、トランザクションおよび財務活動を分類するためにさまざまな機能をサポートします。これらのメタデータは、ユーザーの必要に応じてエクスポートし、共有することができます。さらに、このデータは、専門的な目的（税務会計など）のためにサードパーティのアプリケーションで操作することもできます。

次に、ハッシュや暗号化された値を含んだ特別なアドレスへの対応を検討しています。この構造により、ユーザーはメタデータを公開せずにブロックチェーンに投稿することができます。もしデータを共有したければ、トランザクションが享受する監査能力、不変性、タイムスタンプの保証などをそのデータは保持することができます。

我々は既に属性値を持つアドレス構造を導入しています。現在それは、ウォレットの高速リカバリーに利用される暗号化された**HD**ウォレットツリー構造のコピーを格納するために使用されています（これに関しては**HD**ウォレットのドキュメントを参照してください）。後のバージョンではこの構造が一般化されることでしょう。

認証とコンプライアンス

[30]よりマクロな視点では、**Juan Zarate**は[Treasury's War]において、このデータが反テロリスト活動のためにアメリカ合衆国財務省がどのように利用しているかについての記述を行なっています。これは、現在のグローバル金融市場の構造が地政学的目的のためにどのように使用できるのかについての包括的な見解を提供してくれます。

トランザクションに密接に関連するのは、それを行う権利と資金の所有権に関する話題です。例えば、何かを買うのに十分な資金があるにも関わらず、その購入が制限されるかもしれません（例えばアルコールの年齢制限です）。

所有権と資金源は、顧客確認による規制を行う際に確認する最も基本的なデータです。銀行や取引所のような貨幣サービス事業が新しい顧客の口座を開設するときは、通常、顧客とその資金源に関する基本的な情報を収集する必要があります。

技術的な課題は、法的に要求された情報を提出する過程で、それがどのように利用、保管、または破棄されるのかについての保証が一切ないことです。コンプライアンス情報は商業的に貴重な情報です。よって、なりすましのために盗まれる、あるいは規制の許容範囲内で転売されるかもしれません。

カルダノでは、可能な限り革新を行いたいと考えています。プロトコルのソフトウェア側では、コンプライアンス情報の受信者が許容範囲内で行動することを保証するものはほとんどありません。しかし、プロトコルのハードウェア側では、**Trusted Hardware**であるインテル**SGX**や他の**HSM(**ハードウェアセキュリティプロトコル**)**を活用することによって、特定のポリシーを強制できます。

加えて、我々は**Sealed Glass Proof**と共有ポリシーを併用する試みを行なっています。これによってコンプライアンス情報を検証者に安全に送信することができ、検証者は送られてきたポリシーに従わなくてはなりません。我々は、両方を統一する規格が出現すると考えており、この方法によって顧客データの損失が防止され、検証者のリスク低減に繋がると考えています。

この成果によって、我々がカルダノで提案した価値と計算処理を分離するという階層モデルもうまく機能します。コンピューテーション層が規制機関（取引所やカジノなど）によって運用されているならば、コンプライアンスチェックを実施し、場合によっては税金の制度をユーザーに強制する必要があるでしょう。

SGPを使用することによって、ユーザーは個人識別情報がインターネット上で漏洩する、あるいはコンピューテーション層のコンセンサスノードによって保存されるという心配をすることなく、資金と一緒にその情報を送ることができます。さらに、コンピューテーション層は、取引を行なっているすべてのユーザーが認証済みであり、合法であるという確実性を得ることができます。

このパラダイムは、規制されたエンティティ間の顧客情報の相互運用も可能にします。取引所は、これらの安全なチャンネルを通じて顧客の残高と、アカウント情報を即座に転送できます。また、規約に従ってデータを規制機関と共有することもできます。

この技術のベータテストは、**2018**年中旬に実施される予定で、カルダノは**2018**年後半から**2019**年にかけて研究成果の統合を目指しています。このタイムラインは、ハードウェア上でコードが実行されるように、**ARM**および**Intel**と提携を結ぶことを前提としています[31]。

マーケットプレイス DAO(分散型自律組織)

先ほどのセクションでは、外部システムの存在を仮定した上での情報の生成と、その流れについて説明を行いました。従来の金融システムとの相互運用性を保証するために、これらの機能は必要不可欠ですが、ブロックチェーンに基づいた規制には対応していません。

スマートコントラクトは全く新しい類の商業システムを可能にします。そこでは取引関係は決定的、かつ自己強制的であり、曖昧さがないものです。これらを用いて仲裁、イベント駆動型の返金、特殊な条件を満たした上での事実の暴露など、任意に複雑な構造のマーケットプレイスのルールを作成することができます。

我々はこれらのスマートコントラクトによって施行された構造を、マーケットプレイス**DAO**と呼んでいます。特別なプロトコルの対応や台帳に可変性を取り入れる必要はありません。むしろ、これらは相互依存しているスマートコントラクトの集合によって構築することができます。

アーキテクチャ上のコンセプトは、契約法とビジネスのベストプラクティスからインスピレーションを得た商業用テンプレートのコレクションを設計することです。これらのテンプレートを開発者のスマートコントラクトに結びつけることで、市場に特定の規則を設けることができます。

たとえば、開発者が**CCL**で**ERC20**トークンを発行してクラウドセールを実施したいとします。マーケットプレイス**DAO**はそのクラウドセールのため立ち上げることができ、その利用規約はパラメータ化、もしくはボランティアや法的基準に従って定めることができます。払い戻し、資金の再配分、支払いの凍結などは、開発者の**ERC20**コントラクトを継承することによって実施できます。

この取り組みから、消費者保護を確実に行うためには市場をどのように管理すべきかについてのマクロな議論を展開することができます。また、ニューハンプシャー州など特定の法域での法的保護と権限を自動的に保証するトランザクションモデルについて考察することができます。

カルダノ・プロジェクトでは、カルダノ財団、**IOHK**および他のエンティティと協力して、スマートコントラクト開発者が使用するマーケットプレイス**DAO**の参照ライブラリを作成するつ

[31] インテル**SGX**商用ライセンス規約を参照

もりです。我々は、これらの**DAO**によって保険市場および規制市場が形成され、その結果に基づいて自ら進化していくことでしょう。

5. 持続性

仮想通貨分野を深く知るにつれ、多くの概念的矛盾が生まれます。仮想通貨は、変更を行うことが難しくなるように設計されていますが、すべての技術と同様に、設計上の欠陥や進歩に対応するために変更を行う必要があります。ブロックチェーンは、中央集権化を防止するために作られましたが、そのシステムの変更、維持には強力なアクターが必要です。

最ももどかしいのは、ほとんどのステークホルダーが欠点とみなし、それを是正する必要があると認識しているにも関わらず、コンセンサスに至らない時でしょう。

ビットコインのブロックサイズに関する議論は、**2**年以上にわたり活発に行われてきました。ネットワークのピーク容量があるため、毎日総額十億ドルを超える取引が保留されています。

一時的な解決のための単純なパラメータの変更でさえ行えないのであれば、そのシステム上にインフラストラクチャを構築するために何十億ドルをも費やす政府や企業は安心して投資することができるでしょうか。また企業は、設計の合理的なアップグレードも行えず、説明責任のないプロトコルに戦略的リスクを負う覚悟があるでしょうか。

歴史を振り返ってみると、インターネットの進化は、**IPv4**から**IPv6**への移行のような単純な変更でさえ数十年もの年月を要しました。現在も同様の状況なのです。しかしブロックチェーン技術とインターネットの間には異なる管理体制に従っているという点で全く対照的です。

インターネットは**DARPA**から開発された軍事プロジェクトであり、それは政府の強力な支援と、定評のある支援団体のおかげで成長してきました。インターネットは、ネットワークを独占しようとする企業の影響を受けることなく、非営利的な条件のもとで発展してきました。実際には、電子商取引は**1992**年に廃止されるまで **NSF AUP** に違反していたのです。

インターネットには企業が商業化を行う前に、すでに確固たる規格、原則、そして強い支持者がいました。しかしこれらは、**AOL**やマイクロソフトのような企業が**ActiveX**のような独自の技術を開発して、ウォールガーデンを構築することを阻止できませんでした。またこの基盤では、**Google**などの次世代アクターが膨大なユーザーと大規模な資金でもって行う独自のアジェンダの推進を止めることはできませんでした。

レントシーキング[32]を求めるマイナーや商人にとって、仮想通貨とは究極の商業的動機に基づいたエコシステムです。この点を考慮すると、仮想通貨の管理体制の進化は、最大限の利益をもたらす結果となりました。

たとえば、マイナーの利益率を向上させるために検証不要のマイニングが頻繁に行われていますが、これはマイニングの目的とその有用性を完全に無視しています。マイニングの集中化は一握りのアクターがビットコインのハッシュパワーの大半を管理することによってすでに起きています。

インターネットのように、仮想通貨を変えるにはコンセンサスが必要です。しかし特定のブローカーへの急速な集中化が発生し、変更が彼らにとって不都合である場合にはどうなるのでしょうか。

インターネットとは異なり、ほとんどの仮想通貨のブートストラップは利他的、または学術的な目的によって行われるのではありません。開発当初から、利益を得ようとするグループもあれば、その利益を確保するために配属された強力なブローカーもいます。

発足者らによる中央集権化は仮想通貨が常にその進化において直面しなければならない現実です。我々は、集中化を回避することはできませんが、少なくとも次第に分散されるように設計するべきです。

カルダノでは、どのような要因によって集中化が促進されるのか、いかなる技術を適用すれば我々のプロトコルが次第に**Web**のような公共インフラストラクチャの奨励に繋がるのかの検討を行いました。

完全なる分散化は実質的に不可能、あるいは非生産的であることは認めざるを得ません。しかし、特定の要因を奨励することによってよりバランスのとれたシステムを形成することはできます。

第一に、クラウドセール資金の集中管理は、早期のプロトコルの迅速な開発を可能にする一方で、調達資金は最終的には多様化され、開発スピードもより体系的かつ慎重なペースに落とす必要があります。また資金調達は文化的、言語的、地理的偏見を避ける必要があります。

第二に、コミュニティが仮想通貨に関する技術の根底ある性質についてより多くの情報を取得していくにつれて、ロードマップに関する決定はコア開発者や財団によって集中化されてはいけません。プロトコルの変更を提案、検証、および制定するには、ブロックチェーンに基づいた方法が必要となります。

[32]この用語の詳細については、リンクを参照

第三に、カルダノ**SL**ブロックチェーンを維持するためのインセンティブは、すべてのユーザーの集約的な要望に直接対応しなければなりません。我々は、コミュニティの意志とは独立している特定のアクターが出現することを許してはいけません。

一点目に関して言えば、カルダノは財務システムの統合を行わなければなりません。二点目に関しては、**CSL**によって調整されたシステムを通じて、カルダノ改善案を提案できるような正式なプロセスを導入する予定です。三点目に関しては、ウロボロスがエレガントな解決策を提供してくれると考えています。

上記のトピックに関してより詳しい情報を提供することができますが、ここでの議論の範疇を超えています。このメカニズムの設計は、不完全な理論と確固たる標準モデルが存在しない、最も複雑で相互依存する学問分野の**1**つです。

ここで第二章において解説した科学主導型のアプローチがうまく機能します。**IOHK**の**Veritas**チームはカルダノの参照財務モデルを開発するために、ランカスター大学の**Bingsheng Zhang**教授率いるグループと協力して研究を行なっています。参照モデルは**2018**年の統合を目指しており、我々は**2017**年末までに論文審査のある専門誌にて公開されることを期待しております。

仮想通貨に関するプロトコル変更の正式な説明と検証方法に関してですが、このトピックは存在論的概論と多数のユーザーが参加するためのインセンティブメカニズムの両方を必要とするため、ほとんど理解されません。おそらくなんらかの代表民主主義的なプロセスが登場するか、**Liquid Feedback**を使用することによって、より合理的な投票システムを提供できます。

この方向での研究においては、**IOHK**の正式な関与がカルダノの発展に少なからず貢献すると我々は考えています[33]。出発点として我々は、参照財務モデルと共に、同意を得るためのいくつかの仕組みを導入します。決定的な解決策を検討するにはさらなる研究が必要です。

最後に、ウロボロスのインセンティブを向上させるための研究は、オックスフォード大学の**Elias Koutsoupias**教授の監督下で行われています。ウロボロスの暗号基盤は拡張性に必要な技術とともに確立された後、債券、ペナルティ、エキゾチックなインセンティブの幅広い考察が参照プロトコルに追加されることでしょう。

[33]**IOHK**は**2020**年末までカルダノの継続的な構築を行います。

6. 結論

仮想通貨は、プロトコル、ソースコード、及びその実用性を単に足し合わせたものではありません。これは究極的には人々を刺激し、活発にし、相互に繋ぐ社会システムです。過去のプロトコルの中途半端な解決策や、失敗、及び不測の結果による失望から、我々はより良いものを構築するために出発しました。

このプロセスは単純でありませんし、我々は全てを成し遂げられるとも思っていません。人々と社会の変化に伴い、社会的なプロトコルも不規則で継続的に変化します。有用であるためには、カルダノは進化し続けなければなりません。

進化は片手間または壮大な設計によって導かれたものではありません。それは無数の過ちや問題から触発されたセレンディピティのプロセスです。カルダノではデジタルにおいてそのプロセスを体現することを目指しており、それによって今日の市場で生き残り、将来のニーズを満たすための進化に十分適応できるものを構築します。

これまでのセクションではこの目標をいかに達成するかについて論じてきました。我々は、認知上のバイアスを認識し、歴史から学び、厳格なプロセスに従うことを徹底しました。さらに、急速な開発の必要性と、伝統的に受け継がれた形式手法との間にバランスを取ろうとしました。

このプロジェクトを立ち上げられたことを大変光栄に思います。過去**2**年間で、我々は既に証明可能安全なプルーフオブステークプロトコルを開発し、小隊規模の**Haskell**開発者チームを編成し、カルダノの開発を多くの才能ある科学者の注目の的とすることに成功しました。

実験室から現実社会にこのシステムを解き放つことは、ときに痛みを伴いますが、我々の望みはカルダノが単一の論理構築された文章にまとめあげられることです。カルダノはその先人から知恵を授かり、自らのコミュニティにおいて良い市民であり、常に解決策を見出していく実践的な開拓者です。

我々は未来を予知することはできませんが、人々にとってより良いものを作ろうとしていることをうれしく思います。最後まで精読して頂き、ありがとうございました。