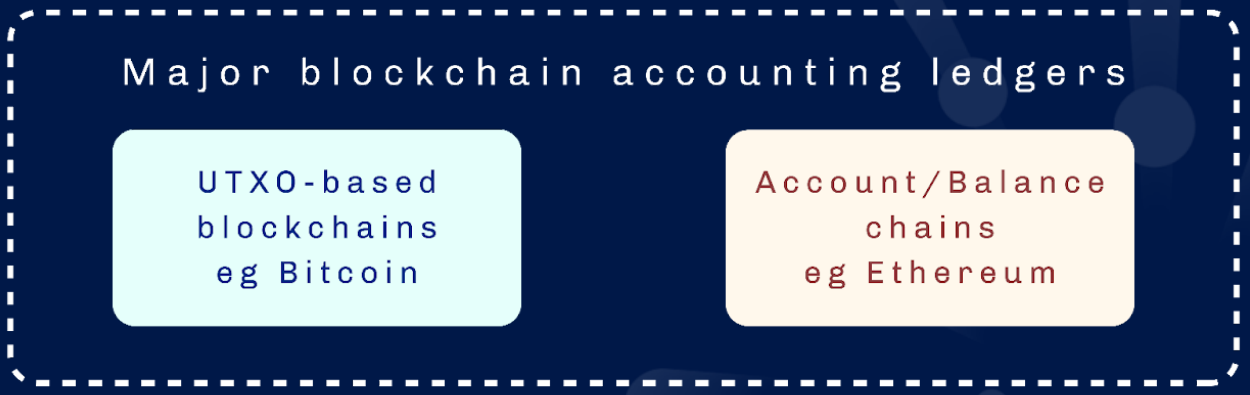
CARDANO

EUTXOハンドブック

はじめに

ブロックチェーンネットワークは複雑なデータの構造物です。トランザクションは継続的にチェーンと交差し、基盤となる台帳の完全性と信頼性を維持するために慎重な追跡と管理を必要とするデジタルフットプリントを作り出します。

ブロックチェーン界には、UTXOベースのブロックチェーン（例えばビットコイン）と、アカウントベースのチェーン（イーサリアムなど）という、2つの主要な会計台帳が存在します。

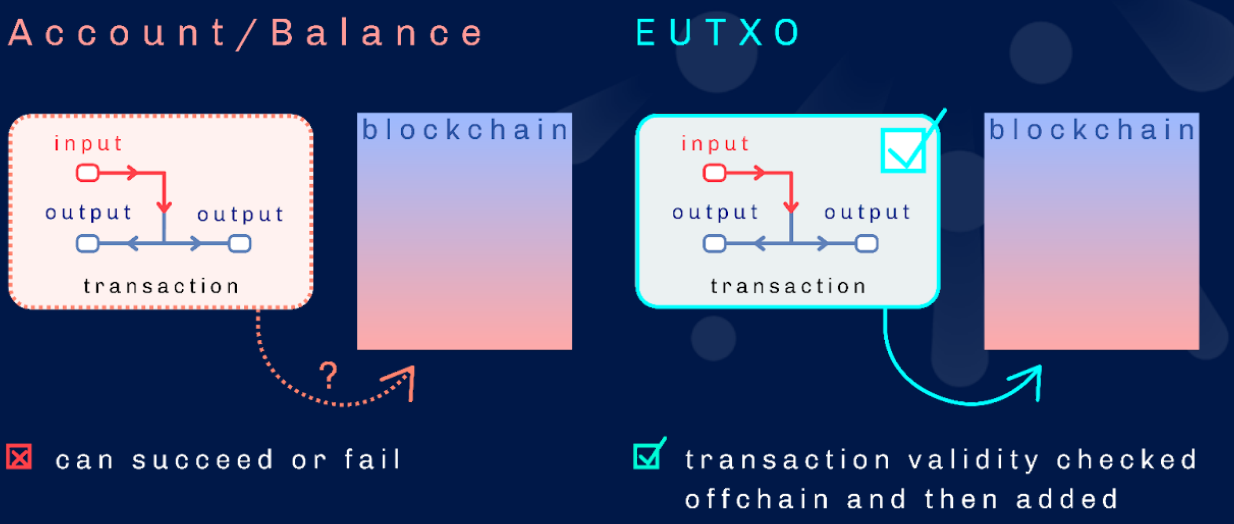


Cardanoは、ビットコインのUTXOモデルとイーサリアムのスマートコントラクト処理能力を組み合わせた、拡張未使用トランザクションアウトプット（Extended UTXO：EUTXO）モデルです。EUTXOの適用により、スマートコントラクトをCardanoチェーンに実装することができます。

EUTXOモデルには他のアカウントモデルにはない利点があります

EUTXOモデルには、他のアカウントモデルにはない利点があります。トランザクション認証の成否はトランザクション自体およびそのインプットにのみ依存し、ブロックチェーンの他の要素は無関係となります。結果として、トランザクションの有効性は、トランザクションがブロックチェーンに送信される前に、オフチェーンで確認することができます。他のトランザクションが、使用を想定しているインプットを同時に消費した場合にはトランザクションが失敗する場合もあり得ますが、すべてのインプットが存在すれば、トランザク

ションは成功することが保証されます。これは、実行中にトランザクションが失敗する可能性のあるイーサリアムとはまったく対照的です。



EUTXOを理解するには、ブロックチェーンの会計モデルとは何か、これが必要とされる理由、その機能、特質を理解することが必要です。

ブロックチェーンの会計モデルとは

すべての企業や営利団体は、利益、損失、キャッシュフロー、その他のパラメーターの正確な記録を維持するために、貸借対照表を必要とします。このすべてのデータの会計管理を慎重に維持することにより、企業はいつでも財務状況を一目で視覚化することができます。企業の会計台帳には別の利点もあります。資金の来歴および所有権の追跡能力です。

ブロックチェーンネットワークもまた、だれが何のコインを（いくつ）所有しているかを特定し、こうしたコインがどこに行くか、どれが使用済みであるか、どれが使用可能であるかを追跡する会計モデルを必要とします。

UTXOモデルとアカウント/残高モデルの概要

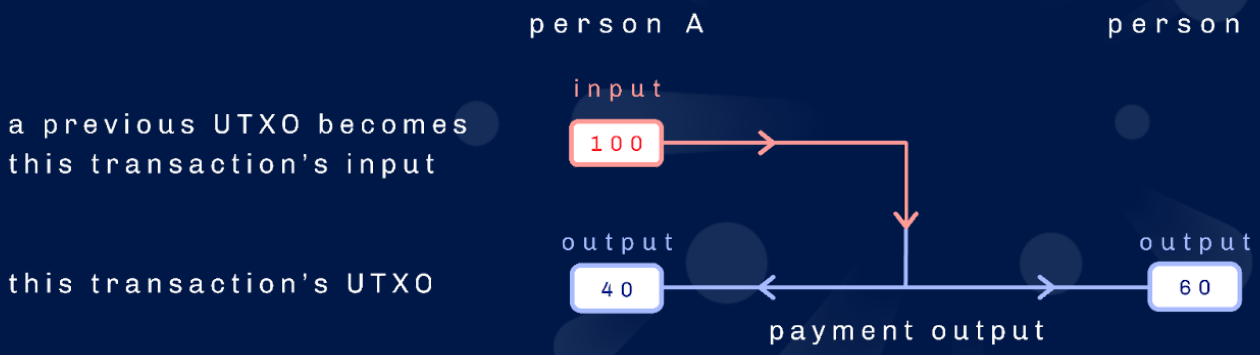
数十年前、会計士は実際の台帳に資金の動きについての記録を手書きで記入していました。今日、企業は同様のことを電子的に行っています。ブロックチェーンは、来歴と所有を追跡するために、トランザクションを記録としています（台帳への記入に非常に似通っています）。これらのトランザクションには多くの情報が内包されています（コインの送金元、送金先、トランザクション後の残高）。

ここでは、UTXOモデルとアカウントベースモデルの概要を紹介します。

UTXO

UTXOモデルでは、資産の動きは有向非巡回グラフの形式で記録されます。ここではノードはトランザクション、エッジはトランザクションアウトプットであり、トランザクションが追加されると一部のUTXOが消費され、新たなUTXOが加えられます。ユーザーのウォレットは、ユーザーに所有されるすべてのアドレスに関連する未使用アウトプットのリストの記録を保管し、残高を計算します。

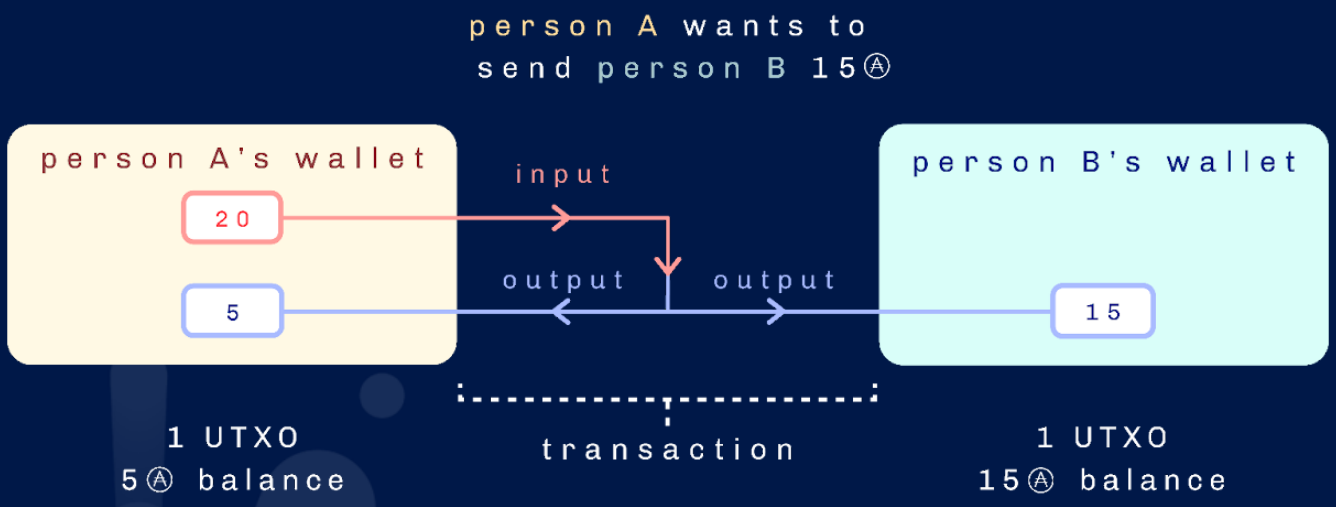
...トランザクションが追加されると一部のUTXOが消費され、新たなUTXOが加えられます



UTXOはさまざまな点で現金に似ています。たとえば、財布に$50入っていると思ってください。この金額は、複数の組み合わせで成り立つと考えられます。例えば、$20紙幣が2枚に$10紙幣1枚、または$10紙幣が4枚に$5紙幣が2枚、ほかにもたくさんあります。しかし、組み合わせがどうであれ、金額（$50）が変わることはありません。UTXOの仕組みも同様です。ブロックチェーンのウォレットにある残高（例えば150コイン）は、それ以前のトランザクションに基づき、多くの異なるUTXOの組み合わせで構成されることが考えられます。ただし、残高は変わりません。言い換えると、所与のウォレットアドレスに保有される残高は、以前のトランザクションで生じた未使用のUTXOの総額となります。

UTXOモデルにおける「釣り銭」の概念

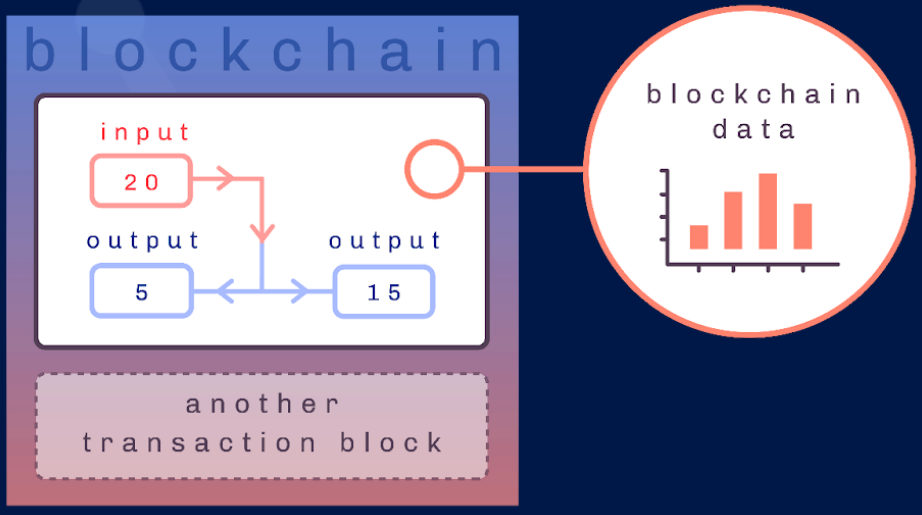
店頭での現金取引のように、UTXOも「釣り銭」を導入しています。例えば財布から$50紙幣を出して$15の支払いをするために、紙幣をバラバラに裂くことはできません。レジで$50紙幣をそのまま渡し、お釣りを受け取ります。UTXOの仕組みも同様です。UTXOを小さく「分割」することはできません。UTXOはそのまま全部が使用され、ユーザーのウォレットアドレスには、お釣りに相当するより少額のUTXOが戻されます。



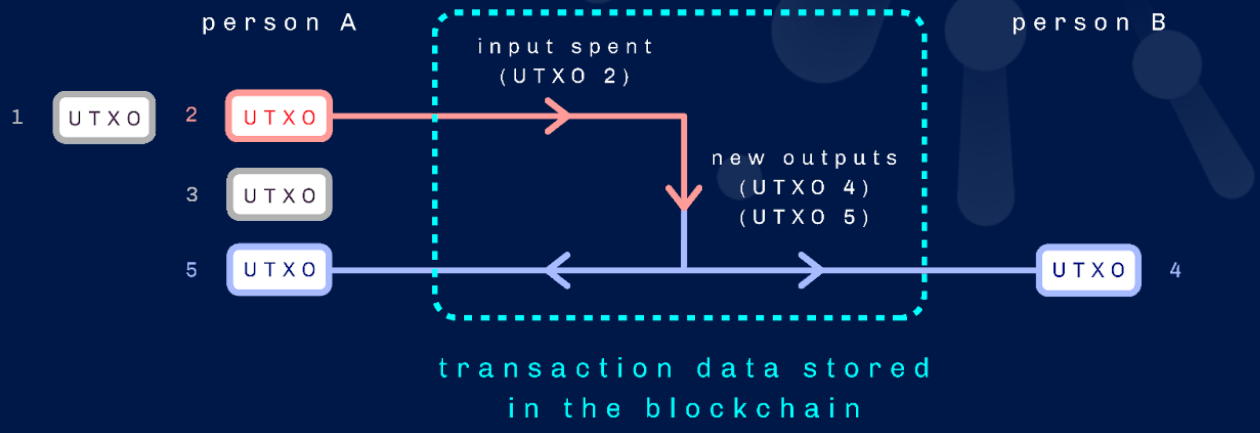
UTXOはそのまま全部が使用され、ユーザーのウォレットアドレスには、お釣りに相当するより少額のUTXOが戻されます

UTXOモデルの利点

送信されるUTXOのサイズ、古さ、金額の確認および追跡によって、ブロックチェーンの使用量およびチェーンの財務活動に関する正確なメトリクスを抽出することができます。



UTXOにはその他の利点もあります。たとえば、スマートコントラクトの並列化とプライバシーにより、スケーラビリティが向上します。また、各UTXOは一度だけ全体として消費されるため、トランザクションの確認が格段にシンプルになり、トランザクションロジックは簡易化されます。



UTXOのまとめ

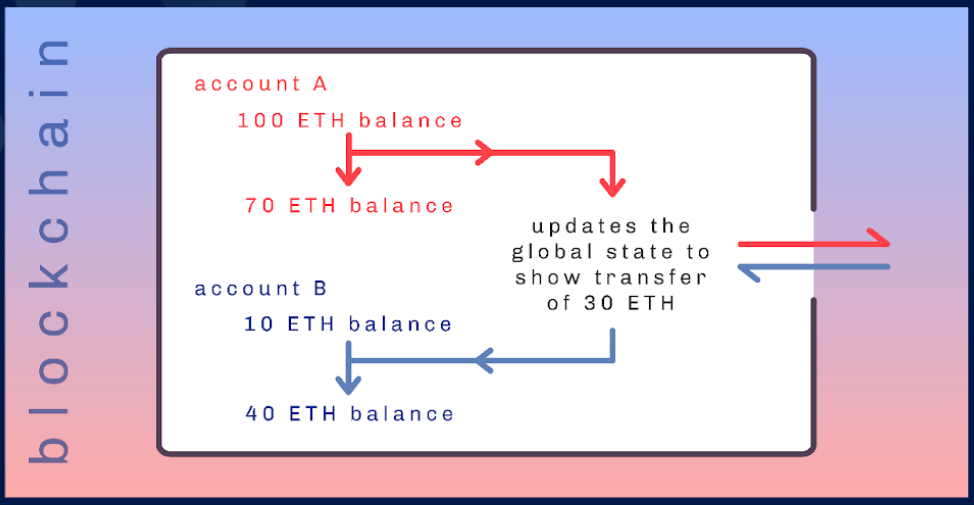
- UTXOは前回のトランザクションのアウトプットであり、将来的に使用することができます。
- UTXOチェーンにはアカウントはありません。代わりに、コインはUTXOのリストとして保管され、トランザクションは既存のUTXOを使用し、新たなUTXOを生成することで作成されます。
- 残高とは、所与のアドレスにより管理されるUTXOの総額です。
- UTXOは、「釣り銭」を使用する、不可分（UTXOは全体として使用される）という点で現金に似ています。

アカウント/残高モデル

名前が示唆するように、アカウント/残高会計モデルを使用しているブロックチェーンモデルは、コイン残高の管理にアカウント（秘密鍵またはスマートコントラクトで管理される）を使用します。このモデルでは、資産はユーザーのアカウント内の残高として示され、残高はアカウントのグローバルステートとして保管され、各ノードに保持されてトランザクションのたびに更新されます。

アカウント/残高チェーン（イーサリアムなど）の運営は多くの点で伝統的な銀行口座と似ています。ウォレットの残高はコインが入金されると増え、どこかに送金されると減ります。ここでの重要な違いは、UTXOとは異なり、ユーザーは自分の残高の一部を使用できることです。例えば、アカウントに100ETHを保有している場合、その一部（例えば30ETH）を誰かに送金することができます。その結果としてアカウントの残高は70ETHとなり、コインの送金先アドレスの残高は30ETH増加します。アカウント/残高会計モデルにはUTXOモデルのような釣り銭の概念は適用されません。

アカウント/残高チェーンの運営は伝統的な銀行口座と似ています



アカウント/残高モデルのまとめ

- 銀行の運用モデルと似ています。
- ユーザーはコイン残高を保有するアカウントを持ちます。
- 残高の一部を使用することが可能です。
- 釣り銭の概念は適用されません。

EUTXOモデル

EUTXOを理解するには、Cardanoでトランザクションがいかに機能するか、特に、トランザクションアウトプットとインプットの役割を理解することが重要です。

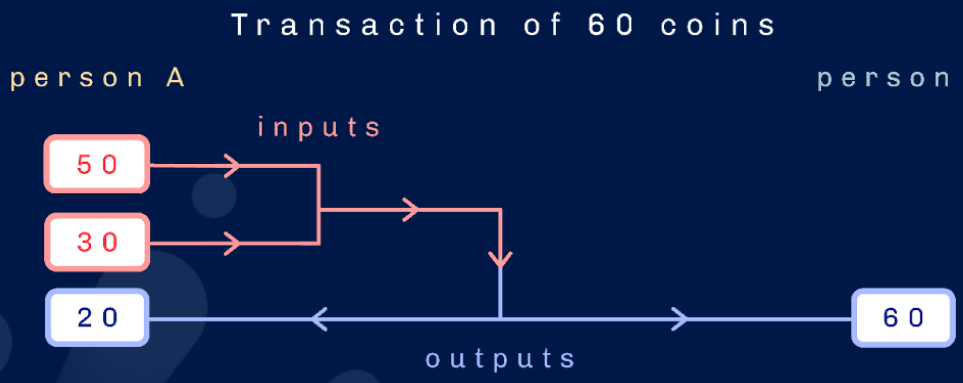
トランザクションの要点：アウトプットとインプット

トランザクションは以前のアウトプットをロック解除し、新しいアウトプットを作るアクションであると考えられます

*トランザクション*という用語は、通常金融関連をイメージします。これはビットコインには当てはまりますが（ビットコインのブロックチェーンはピア間の資金移転に使用されるため）、より幅広い用途を持つブロックチェーンも多数存在します（Cardanoを含む）。この場合、トランザクションという用語のニュアンスは広がり、価値の移譲を示す場合もあります。

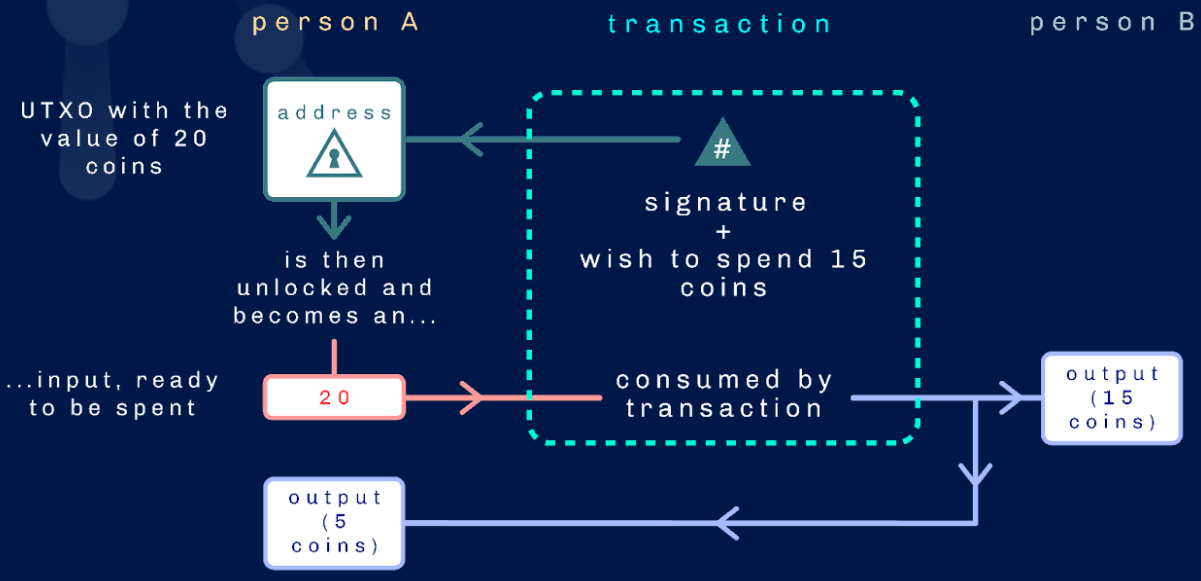
ブロックチェーン環境では、各トランザクションには1つ以上のインプット、そして、1つ以上のアウトプット

を含むことができます。トランザクションの仕組み、そして、それがUTXOといかに関連するかを理解したければ、インプットおよびアウトプットというコンセプトを理解する必要があります。抽象的に言えば、トランザクションは以前のアウトプットをロック解除し、新しいアウトプットを作るアクションであると考えられます。



トランザクションアウトプット

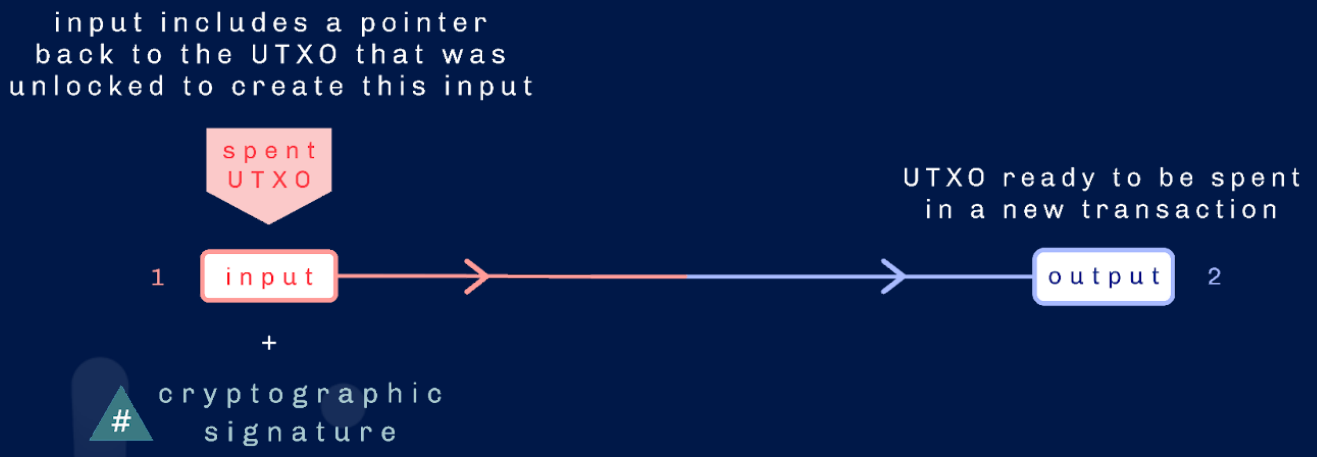
トランザクションアウトプットには、1つのアドレス（ロック）と値が含まれます。アドレスに紐づいた署名は、アウトプットをロック解除するための鍵にあたります。ロック解除されると、アウトプットはインプットとして使用することができます。新しいトランザクションは以前のトランザクションのアウトプットを使用し、将来消費することのできる新たなアウトプットを生成します。各UTXOは1回だけ、全体としてのみ使用できます。各アウトプットは1つのインプットとしてのみ使用できます。



トランザクションインプット

トランザクションインプットは以前のトランザクションのアウトプットです。トランザクションインプットにはポインターと、ロック解除用の鍵として機能する暗号化署名が含まれます。ポインターは以前のトランザクションアウトプットを指定し、鍵がこのアウトプットをロック解除します。インプットによりアウトプットがロック解除されると、ブロックチェーンはこのロック解除されたアウトプットを「使用済み」とマークします。所与のトランザクションにより作成された新たなアウトプットは、次に新たなインプットにより指定され、そうしてチェーンは続いていきます。これらの新たなアウトプット（ロック解除されていない、すなわち*使用*されていないもの）がUTXOです。未使用アウトプットとは単純に、いまだに使用されていないアウトプットのことです。

トランザクションインプットにはポインターと、ロック解除用の鍵として機能する暗号化署名が含まれます

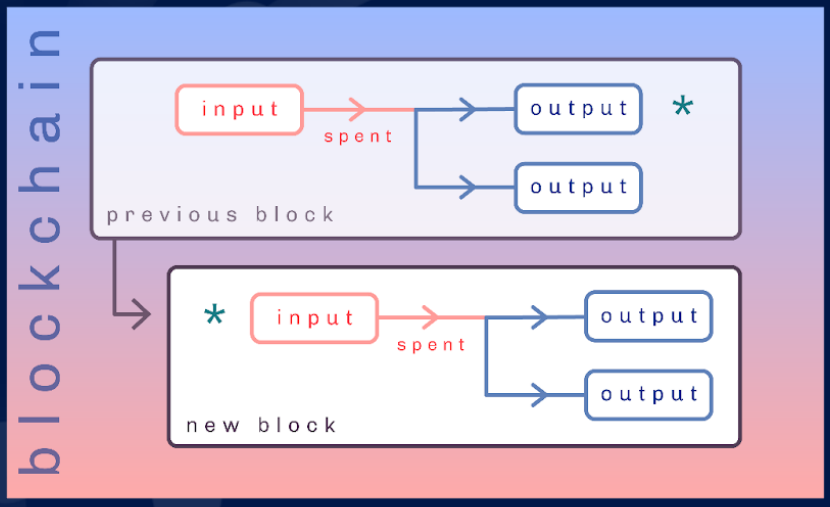


UTXOの仕組みのまとめ

UTXO会計モデルでは、トランザクションは以前のトランザクションからの未使用アウトプットを消費し、将来のトランザクションでインプットとして使用できる新しいアウトプットを生成します。

各ブロックチェーンノードは全UTXOのサブセットの記録を常時保管しています

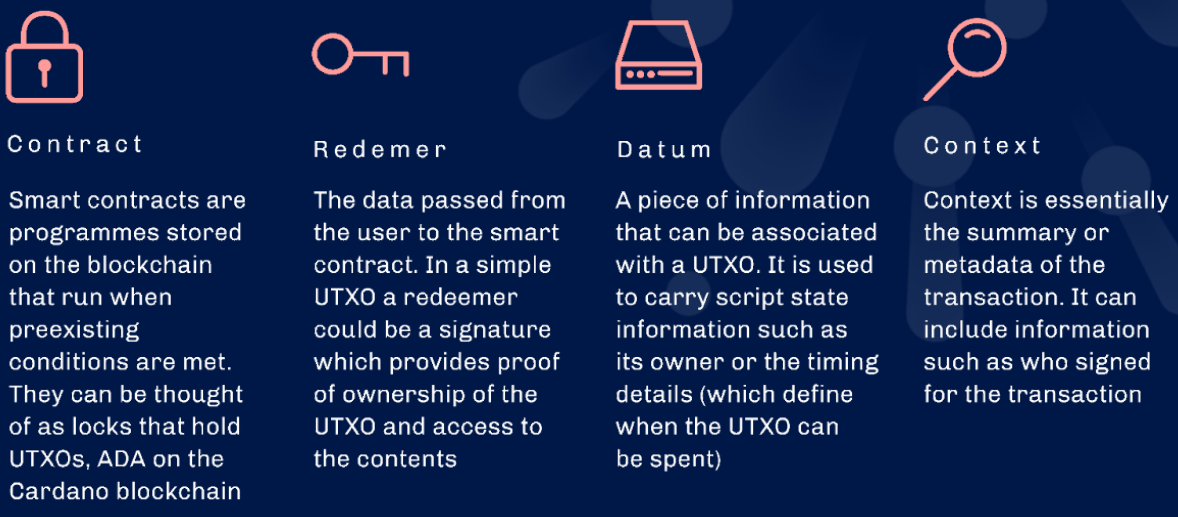
ユーザーのウォレットはこれらのUTXOを管理し、ユーザーが所有しているUTXOを使用したトランザクションを開始します。各ブロックチェーンノードは全UTXOのサブセットの記録を常時保管しています。これをUTXOセットと呼びます。技術用語で言うところのchainstateであり、各ノードのデータディレクトリーに格納されます。新しいブロックがチェーンに追加されると、chainstateは自動的に更新されます。この新ブロックには最新のトランザクションリスト（もちろん使用されたUTXOやchainstateの最終更新時以降に作成された新UTXOも）が含まれます。各ノードはchainstateの完全なコピーを維持します。



EUTXOは、以下を組み合わせたトランザクションメカニズムです。

- スマートコントラクト：UTXO、ADA、ネイティブ資産、NFTをロックする
- リディーマー：資産のロックを解除して使用可能にするために、ユーザーから提供されるデータ
- データム：ハイスコア、ユーザー情報、アプリ関連情報などのデータ

- コンテクスト：検証中のトランザクションについてのメタデータなどの情報



EUTXO：Cardanoの選択を支える原理

ビットコインの「vanilla」UTXO会計モデルはCardanoには適しません。Cardanoは支払い処理よりも多くを実行するために設計されています。とくに、スマートコントラクト機能のためのプログラミング表現力向上の必要性は、新たな（「拡張型の」）ソリューションを要求しています。

「基本的」なUTXOモデルは、プログラム可能な表現力において限界があります。イーサリアムのアカウント/残高会計モデルはこの問題にアカウント/残高台帳および関連するコントラクトアカウントで対処しています。しかしそうすることにより、コントラクトコードのセマンティクスはかなり複雑になります。そこで、非常に高くつきかねないコードの脆弱性を避けるために、コントラクトの作成者がセマンティクスのニュアンスを完全に習得せざるを得ないという好ましからざる状況を招いています。

「拡張」UTXOソリューションは、既存のUTXOモデルが提供できない2つの追加的機能を必要とします。

1 – コントラクトステータスの維持を可能にすること

2 – 同じコントラクトコードをトランザクション全体のシークエンスで使用できるようにすること。これを*継続性*と呼ぶ

EUTXOモデルが持つ強みは、有効なトランザクションに必要な手数料を送信前に正確に予測できることです

EUTXOモデルが持つ強味は、有効なトランザクションに必要な手数料を送信前に正確に予測できることです。これは、アカウント/残高モデルには見られない、ユニークな特徴です。

Plutus Core

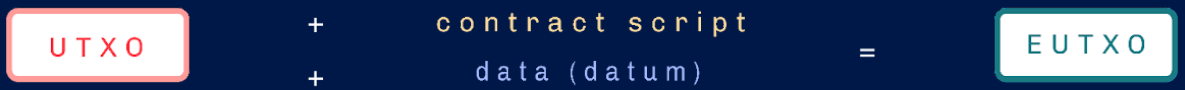
EUTXOの実装には、スクリプトとデータという、アカウント/残高モデルとは異なる2つの重要な要素が含まれます。スクリプトには、明確に指定されたスクリプト言語が必要です。また、アウトプットに添付してリディーマーとして使用されるデータ型を定義することも重要です。リディーマーデータはシンプルな（代数的）データ型で、Hasukellで簡単に定義できます。

Cardanoのスクリプト言語であるPlutus Coreはこれら2つの要素を提供します。これはHaskellに似た、シンプルな関数型言語です。実際、Haskellの大部分のサブセットを使用して、Plutus Coreのスクリプトを作成することができます。開発者がPlutus Coreのコードを書くことはありません。Haskellコンパイラープラグインが、すべてのPlutus Coreスクリプトを生成します。

ノードは、オンチェーンで「ライブ」でトランザクションが検証されている間にこれらのスクリプトを実行します。スクリプトは、バリデータースクリプトの形式でUTXOをロックするか、ミントポリシーとしてネイティブトークンのミント（鋳造）やバーン（廃棄）を管理します。

EUTXOの実装には、スクリプトとデータという、アカウント/残高モデルとは異なる2つの重要な要素が含まれます

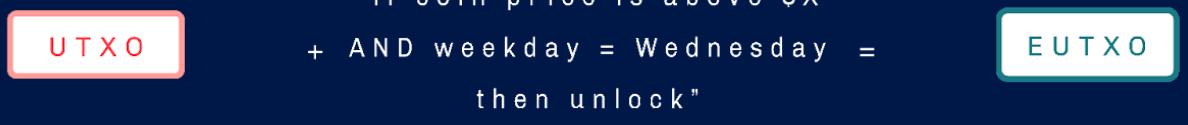
適切なHaskellライブラリーは、検証中にトランザクションを検査するためのコアデータ型、そして多くのヘルパー関数とより高いレベルの抽象化を提供することによって、このような検証ロジックの作成を単純化します。これにより、コントラクトの作成者はビジネスロジックに集中でき、低レベルの雑事に煩わされる必要がなくなります。



EUTXOモデルがUTXOを拡張する仕組み

EUTXOは「基礎的」なUTXOモデルを2方向に拡大します。

1. 「アドレス」のコンセプトを「錠と鍵」のアナロジーを使用して一般化します。EUTXOモデルでは、錠を公開鍵と署名鍵に限定する代わりに、スクリプト形式で任意のロジックを含めることができます。たとえば、ノードがトランザクションを検証するとき、ノードはそのトランザクションが特定のアウトプットをインプットとして使用することを許可するか否かを判断します。トランザクションはアウトプットのアドレスが提供するスクリプトを参照し、トランザクションがアウトプットをインプットとして使用できる場合にはスクリプトを実行します。



2. UTXOとEUTXOの違いの2点目は、アウトプットがアドレスと値に加えて（ほぼ）任意のデータを運ぶことができる点です。これにより、ステート（状態）を含むことができるようになるため、スクリプトはさらに強化されます。

ここには、EUTXOを唯一無二なものにしているもの、そして、この会計モデルが「vanilla」UTXOよりも優れている理由をまとめています。

EUTXOの特徴	重要である理由
各UTXOにはアドレス、値、*そして*、コントラクト固有データの一部であるデータムが含まれています。データムは、*データムオブジェクト*とも呼ばれます。 データムは検証中の追加的引数として送られます。	これで、コントラクトはコードを変更することなく、あるステート（データム）を運ぶことができます。
検証者は、検証中のトランザクションについての情報であるコンテクストを受け取ります。 この情報は、Context型の追加的な引数として送られます。	コンテクストで提供される情報により、検証者は「単なる」UTXOモデルよりもはるかに強力な条件を適用できます。とくに、現在のトランザクションのアウトプットの検査が可能になります。これは、コントラクトの継続性を確保するために不可欠です。
EUTXOは、トランザクションに有効期間を追加することによって、時間にある程度のアクセスを提供します。 これは*ティック*のインターバルです	このインターバルにより、検証中に実行されるスクリプトが、現在のティックがインターバル内にあると想定できますが、ス

（台帳システムで単調に増加する進行単位として定義されます。これは通常ブロック番号またはブロック高に対応します）。この間にトランザクションを処理することができます。	クリプトは現在のティックの正確な値を知りません。

EUTXOがUTXOよりも優れている理由

- Cardanoの分散性とセキュリティは、ビットコインのそれを上回っているうえ、アカウント/残高チェーンよりも優れたスマートコントラクト機能を提供
- マルチ資産とスマートコントラクトをサポート
- より優れた柔軟性、セキュリティ、安定性、スケーラビリティ
- プルーフオブワーク型ブロックチェーンが必要とするエネルギーのほんの一部しか使用せずに、プルーフオブステーク型システム上でより多量なトランザクションを並行処理
- IOGはUTXO Allianceのもとで他の7つのUTXO型ブロックチェーンと協力し、イノベーションと相互運用性の境界を押し広げ、共にさらなる改良に取り組んでいる

2022年Cardanoをスケーリングするスプリングボードとしての EUTXO

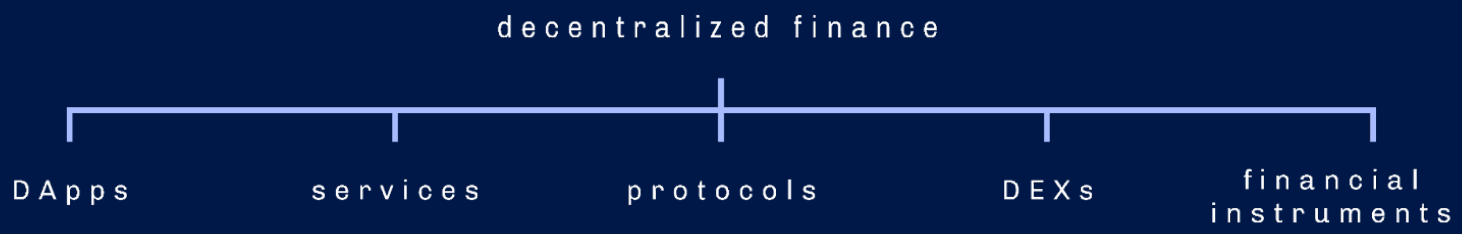
新たなパラダイムと考え方を提示する一方で、EUTXOはスマートコントラクト開発者にアプリケーションを構築してデプロイするための、強力で多用性のあるプラットフォームを提供します。

今年、Input Output Global Inc.はEUTXOの力を活用し、3つの方法でCardanoでのスマートコントラクト構築を最適化します。

- **参照インプット**（CIP-0031）– Plutusスクリプトはトランザクションインプットを使用せずに検査できます。すなわち、インプットに格納された情報を検査するためだけにUTXOを作成する必要はありません。
- **Plutusデータム**（CIP-0032）– データムは、データムハッシュの代わりに直接アウトプットに添付することができます。これにより、ユーザーは所与のハッシュと一致するデータムを指定する必要なく実際のデータムを確認できるため、データムの使用方法が簡素化されます。
- **スクリプト共有**（CIP-0033）– Plutusスクリプトリファレンスは、トランザクションアウトプットに関連付けることができます。すなわち、オンチェーンで記録し、あとで再利用することができます。トランザクションごとにスクリプトのコピーを提供する必要がなくなります。
- 開発者の負担が大幅に軽減されます。複数のトランザクションでスクリプトを再利用することで、トランザクションサイズが大幅に縮小され、スループットの向上とスクリプト実行コストの削減につながります。

変動損失について知りたかったこと、訊きづらかったことのすべて

分散型金融（DeFi）は、ブロックチェーンに構築された分散型のアプリケーション（DApp）、サービス、プロトコル、金融商品の総称です。これは、システムを一元管理する単一の機関を持たない分散型台帳技術によって可能となった、比較的新しい産業分野です。DeFi環境に詳しい人なら、変動損失についても耳にしたことがあるでしょう。これは、誤解しやすい名称（訳者注：言語はimpermanent loss、一時的損失。日本ではよりコンセプトに近い「変動損失」の用語が用いられている）ですが、単純なコンセプトです。



Cardanoは第三世代ブロックチェーンであり、その包括的なDeFi界には多くのDApp、とりわけ分散型取引所（DEX）が存在します。これは、暗号資産取引プロトコルであり、ピアが互いに暗号資産を取引することを可能にします。DEXは、主にAMM（自動マーケットメーカー）とオーダーブックという2種類の設計アーキテクチャを使用します。AMMの実装は比較的単純で、イーサリアムを含むアカウント/残高チェーンの実質的選択肢となっています。しかし、この設計には本質的な欠陥があります。たとえば、変動損失を生みやすいことです。

分散型取引所（DEX）は、暗号資産取引プロトコルであり、ピアが互いに暗号資産を取引することを可能にします

CardanoはEUTXO会計モデルを使用して、チェーン全体の資産の動きを追跡します。EUTXOは決定性を持つため、変動損失の予測可能性が高まります。

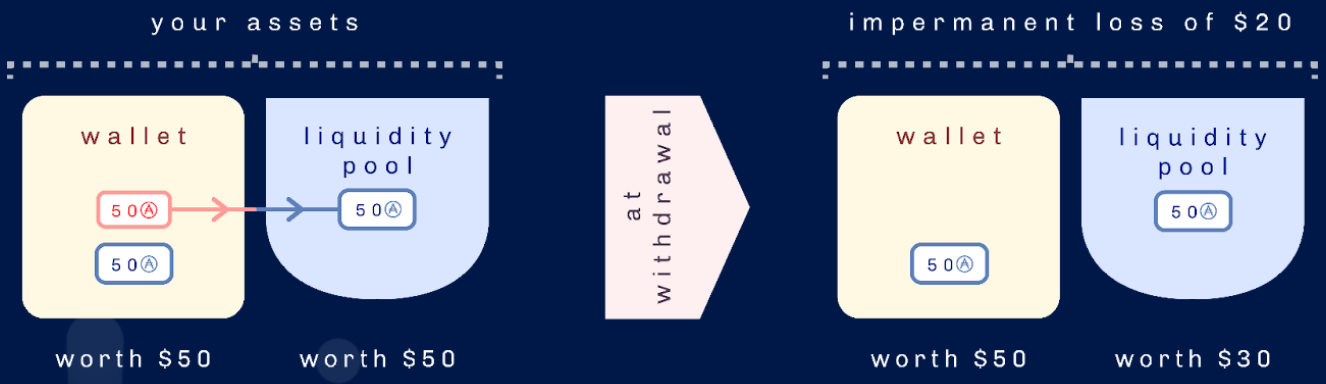
この一見関係のない概念は、ブロックチェーン上で非常に興味深い相互作用を果たします。本稿では、DEXの設計を検討するとともに、EUTXOが、アカウント/残高会計モデルよりも変動損失の予測可能性に優れている理由を説明します。

変動損失の定義

流動性を提供された資産の合計値が、単にそれらを保持した場合に発生したであろう値よりも低い場合。

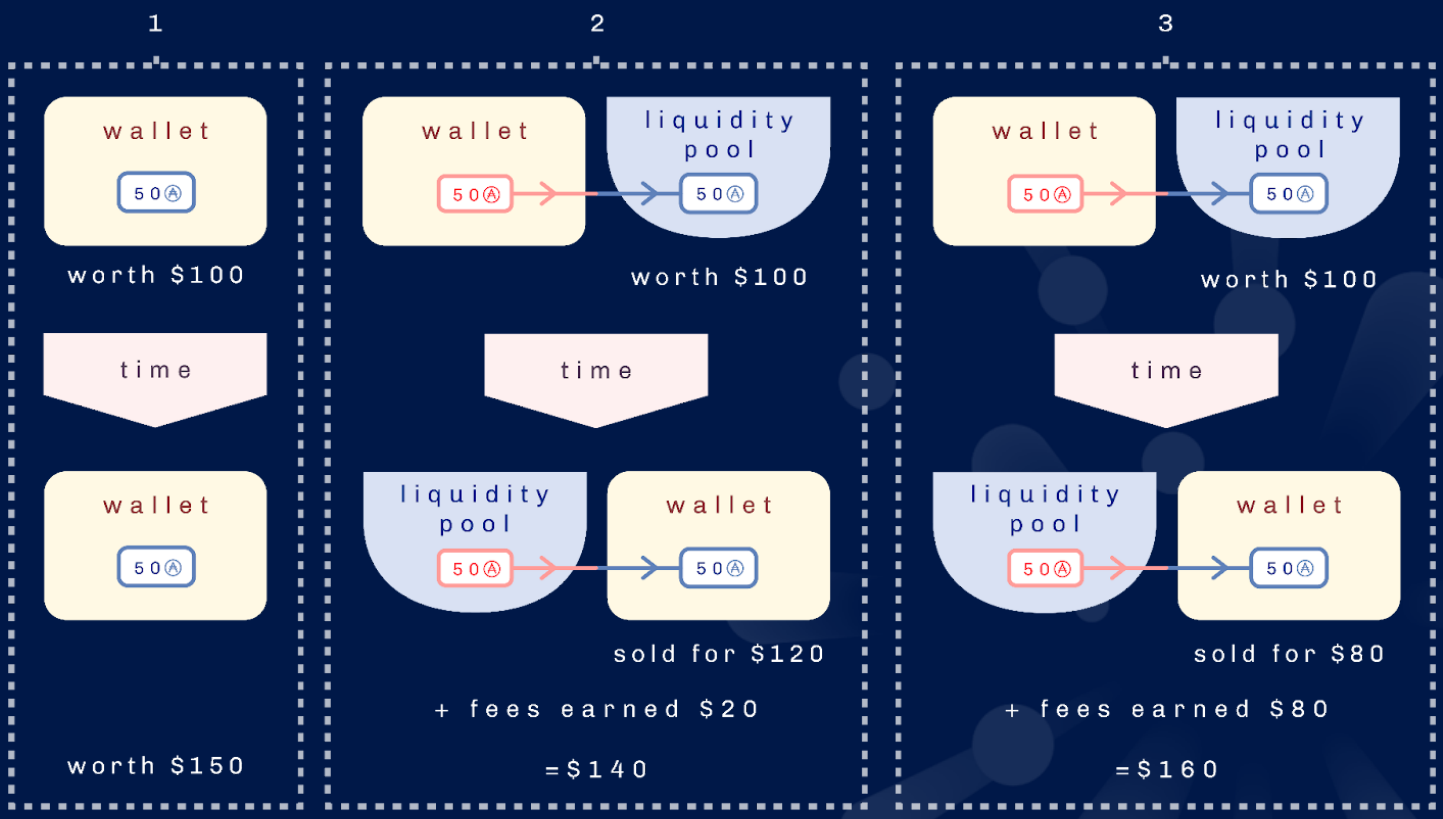
これが、流動性プロバイダーを恐れさせる変動損失の最も単純な定義です。

変動損失は、流動性プールに預け入れた資金の価格が、預金した時点に比べて変動（上下）するときに生じます。言い換えれば、流動性プールからの出金時の資産価値が入金時と異なることです。



「impermanent（一時的）」という名称は誤解を招く恐れがあります。たしかに、トークン価格の低下は一時的で、市場や取引条件に応じて再び上昇することもあります。この場合、価格は上方修正されるため、損失は一時的（impermanent）であると言えます。変動は、出金時のトークンのドル価格が入金時よりも少ないときに限り永続的となります。

変動損失は、流動性プロバイダーが、流動性プールで暗号資産ペアを取引きすることによって稼ぐ手数料の代わりに得るリスクであると言えます。損失が稼ぐ手数料より大きくなれば、流動性プロバイダーは損失を実現します。ただし、トークンを保持したままにしていれば損失は実現しません。実際の金銭的損失はない場合でも、トークンを保持したままの場合よりも利益が少なくなる可能性があることに注意が必要です。



AMMとオーダーブック

変動損失を理解するためには、DEXの基本的な仕組みを理解することが必要です。現在、DEXにはAMMとオーダーブックの2つの設計モデルがあります。変動損失に関してはどちらも以下の如く一長一短あります。

AMM

AMM（自動マーケットメーカー）DEXモードは、スマートコントラクトを使用した暗号通貨ペアの自動取引を可能にします。これらのペアは通常（ただし必ずではなく）イーサリアム系のトークンおよびステーブルコインです。

AMMは流動性プールに依存します。これは、ユーザーが自分の資産をスマートコントラクトにプールしやすくするメカニズムです。プールに流動性があればあるほど、そのプールが関連するDEXでの取引が簡単になり、流動性プロバイダーが得られる手数料や報酬が高くなります。流動性プールは、投資家によって提供された流動性を取引ペアの双方に集約します。プールは、現在の流動性を調べるアルゴリズムを使って、その時点におけるペアの市場価格を計算します。言い換えれば、アルゴリズムはプールの特定の資産の利用可能度を考慮して、その価格を判断します。

AMMは、ユーザーが自分の資産をスマートコントラクトにプールしやすくするメカニズムである、流動性プールに依存します

AMMは、流動性を提供してプールサイズを拡張するためにほぼ完全に流動性プロバイダーに依存して、資産が公正価格で取引されることを保証します。この設計特性は実質的に、流動性プロバイダーがマーケットメーカーであることを意味します。

流動性プロバイダーはもちろん投資にインセンティブを必要とします。これはイールドファーミング、基本的には、デジタル資産の貸出またはステーキングを通じて得たトークン報酬として提供されます。

オーダーブック

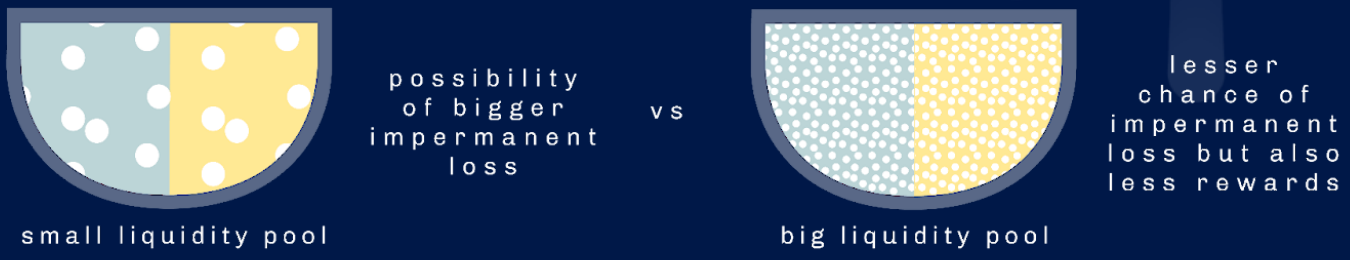
オーダーブック設計を支えるメカニズムは経済分野で長らく存在してきました。これは非常に単純なモデルです。オーダーブックは単純にすべての買い/売り（この文脈ではアスク/ビッド）注文のリストです。したがって、トレーダーが注文を出すと、オーダーブックは資産の価格に応じてそれらをソートします。需要と供給があれば、その資産は取引できます。

CardanoのようなUTXOベースの台帳には、オーダーブックアーキテクチャがはるかに適しています。この設計は、CardanoのEUTXOと組み合わせることで、変動損失の影響を軽減できるためです。

CardanoのようなUTXOベースの台帳には、オーダーブックアーキテクチャがはるかに適しています

変動損失の予測（不）可能性

ユーザーは財政的リターンのためにプールに流動性を提供しますが、これにはリスクも伴います。プールのトークン量とそれに寄与する流動性プロバイダーの数は、変動損失が発生する可能性の主要因であり、こうした考えは潜在的流動性プロバイダーにとって重要です。頻繁な変動損失はプールの枯渇と流動性プロバイダー離れを引き起こします。



変動損失には厄介な問題があります。発生するか否か、どの程度の規模かを予測することが極めて難しいのです。

UTXOベースのチェーンとアカウント/残高ベースのチェーンにおける変動損失

概要

- UTXOベースのチェーンは残高を維持するアカウントを持たない。代わりに、ユーザーのウォレットは、ユーザーに所有されるすべてのアドレスに関連する未使用アウトプットのリストの記録を保管し、残高を計算する。UTXOは多くの点で現金取引に類似している。CardanoのEUTXOモデルは、コントラクト固有のデータであるデータムを追加する。これはCardanoにマルチ資産とスマートコントラクトのサポート機能を付与するため重要である。

- アカウント/残高会計モデルは、コイン残高の管理にアカウント（秘密鍵またはスマートコントラクトで制御される）を使用する。このモデルでは、資産はユーザーのアカウント内の残高として示され、残高はアカウントのグローバルステートとして保管される。このステートは各ノードに保持され、トランザクションごとに更新される。

2つのモデルにはいくつかの基本的な違いがありますが、AMMと変動損失に限って言えば、1つ重要な特徴があります。アカウント/残高チェーン（イーサリアムなど）で稼働するAMMは、AMM用アルゴリズムとしてより一般的に使用されているCFMM（コンスタントファンクションマーケットメーカー）価格設定式を使用する傾向があります。この式は非効率性をはらんでいます。たとえば、TVL（Total Value Locked/預かり資産：ステーキングで報酬、利子等を稼いでいる暗号資産の総額）は価格範囲全体に分散されます。これは、資産の価格が1ドルまたは1万ドルになる確率が同じであることを意味します。この仮定の下では、CFMMの価格は非現実的であり、実際の市況を反映しない傾向があります。また、少量のトークンの取引は、スリッページ（注文の予想価格と、実際に注文が実行された時の価格の差）が大きくなる傾向があります。CFMMがAMMにとって一般的な選択肢である一方で、このような非効率性は流動性プロバイダーの収益の希薄化につながる可能性があります。より重要なことに、この流動性は変動損失の影響を受けます。

CFMMがAMMにとって一般的な選択肢である一方で、このような非効率性は流動性プロバイダーの収益の希薄化につながる可能性があります

変動損失に対する防壁としてのEUTXOオーダーブックDEX設計

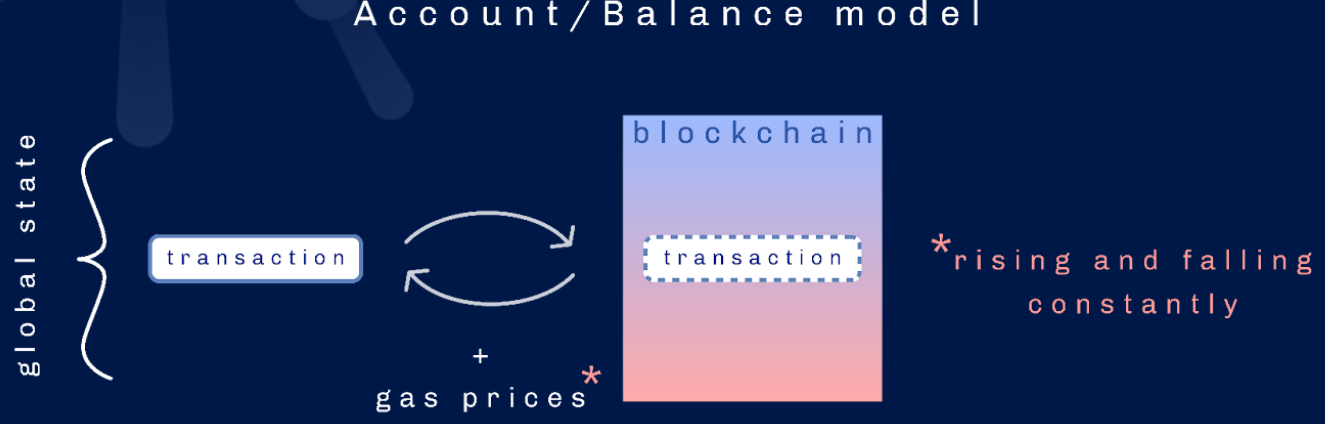
EUTXOアーキテクチャが備える安全性、決定性、並列性、スケーラビリティという利点は、変動損失に対するより強力な回復力を提供するため、オーダーブック設計を使用するDEXに理想的な環境を提供します。この設計の重要な利点の1つは、集中流動性（カスタム価格範囲内で割り当てられる流動性）です。この特性により、流動性の効率は最大化し、変動損失は最小化されます。

EUTXOベースのチェーンにおいてグローバルステートが問題とならない理由

あらゆるトランザクションの結果がグローバルステートに影響するアカウント/残高ブロックチェーンとは異なり、UTXOベースのブロックチェーンではトランザクションの検証はトランザクションレベルで査定され、残高は残りのUTXOの合計になる、すなわちローカルステートで実行されます。

トランザクション手数料はトランザクションが送信されてから検証されるまでの間に大幅に急騰する可能性があります

これはアカウント/残高チェーンの場合即座に問題となります。多数のスマートコントラクトや他のアクターが恒常的にやり取りしてグローバルステートに影響を与える、すなわち資産やリソースが消費され、手数料は常に上下動します。この副作用が、トランザクション手数料の変動の可能性です。実質的に、これはトランザクション手数料がトランザクションの送信から検証までの間に大幅に急騰する可能性を意味します。結果として、このようなトランザクションがチェーンに承認されなくとも、手数料はとにかく徴収されるため、ユーザーに財政的損失を招く怖れがあります。これが、イーサリアムチェーンの設計上の主な欠陥の1つです。



CardanoのEUTXOモデルでは、トランザクションはローカルステートで処理、検証されるため、手数料の浪費が起こる可能性はありません。これは、トランザクションにデータム（追加データ）を加えることで実現します。データムはコントラクト固有の情報を含み、これをトランザクションの検証ロジックにパスすることで、EUTXOの決定性コンテクストを維持します。これは実質的に、トランザクション手数用を事前に知ることができ、変更もしないことを意味します。EUTXOと決定性の歓迎すべき副作用は、悪質なアクターによるトランザクションの再配置が不可能なことです。これは、アカウント/残高モデルのもう1つのリスクです。

CardanoのEUTXOモデルでは、トランザクションはローカルステートで処理、検証されるため、手数料の浪費が起こる可能性はありません

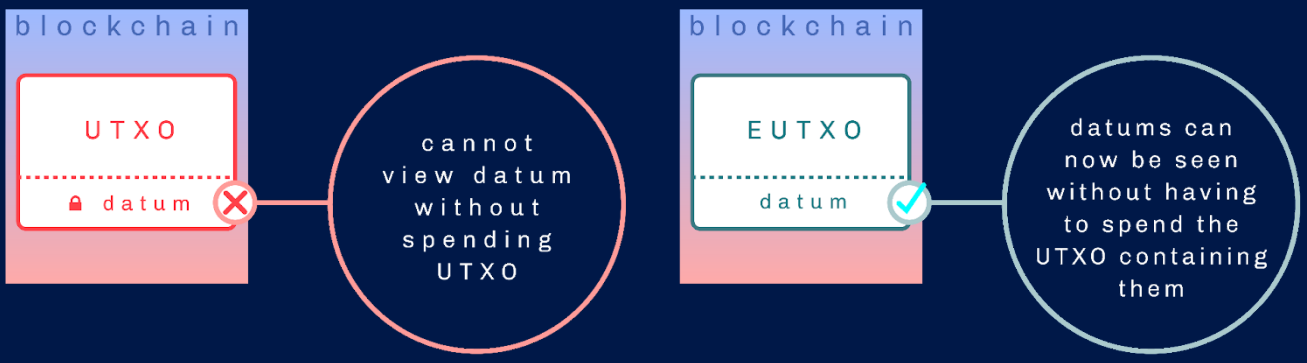
トランザクションの検証をローカルで行うことで、高い並列性というもう1つの重要な利点も提供されます。ノードは、トランザクションが同じインプットを消費しようとしない限り、トランザクションを並行して検証できます。これは、トランザクションを順番に処理するようにデザインされているアカウント/残高チェーンでは不可能です。

更なる強化

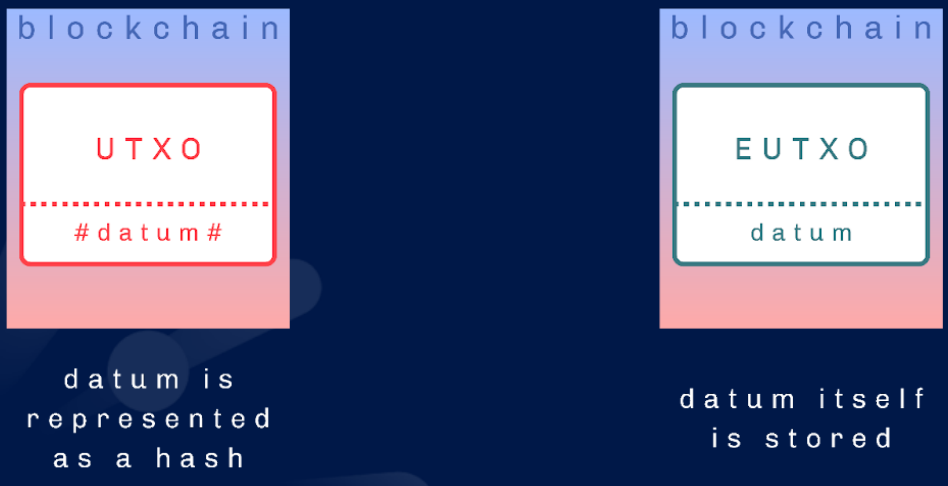
PlutusプラットフォームはCardanoブロックチェーンにネイティブなスマートコントラクト言語を提供します。

予定されているPlutusのCIP（Cardano改善提案）には、以下が含まれます。

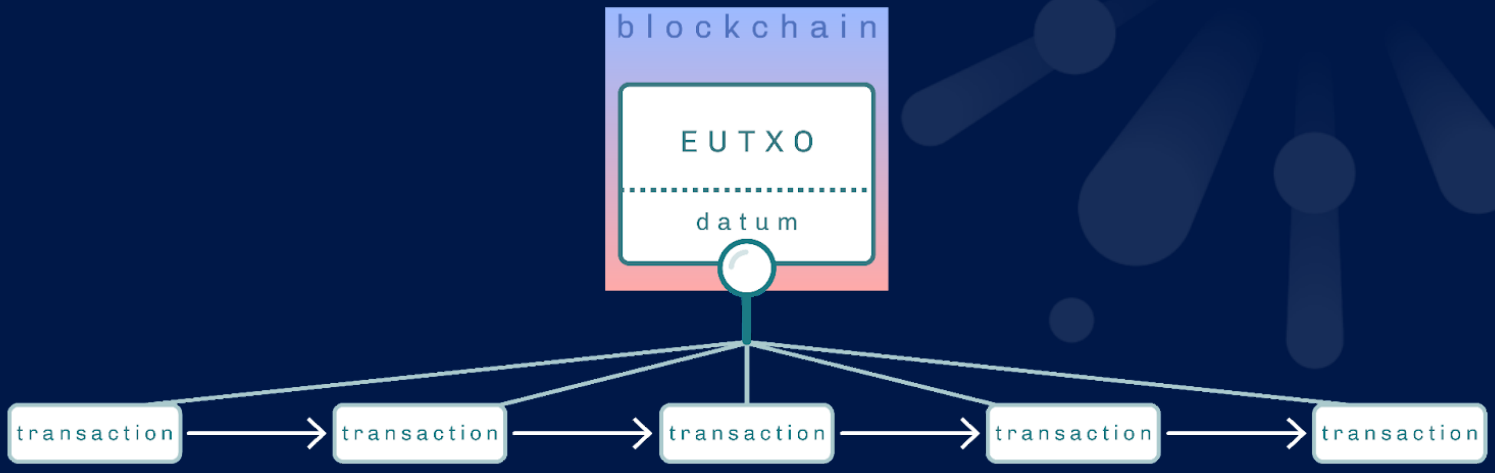
- CIP-31: 参照インプット



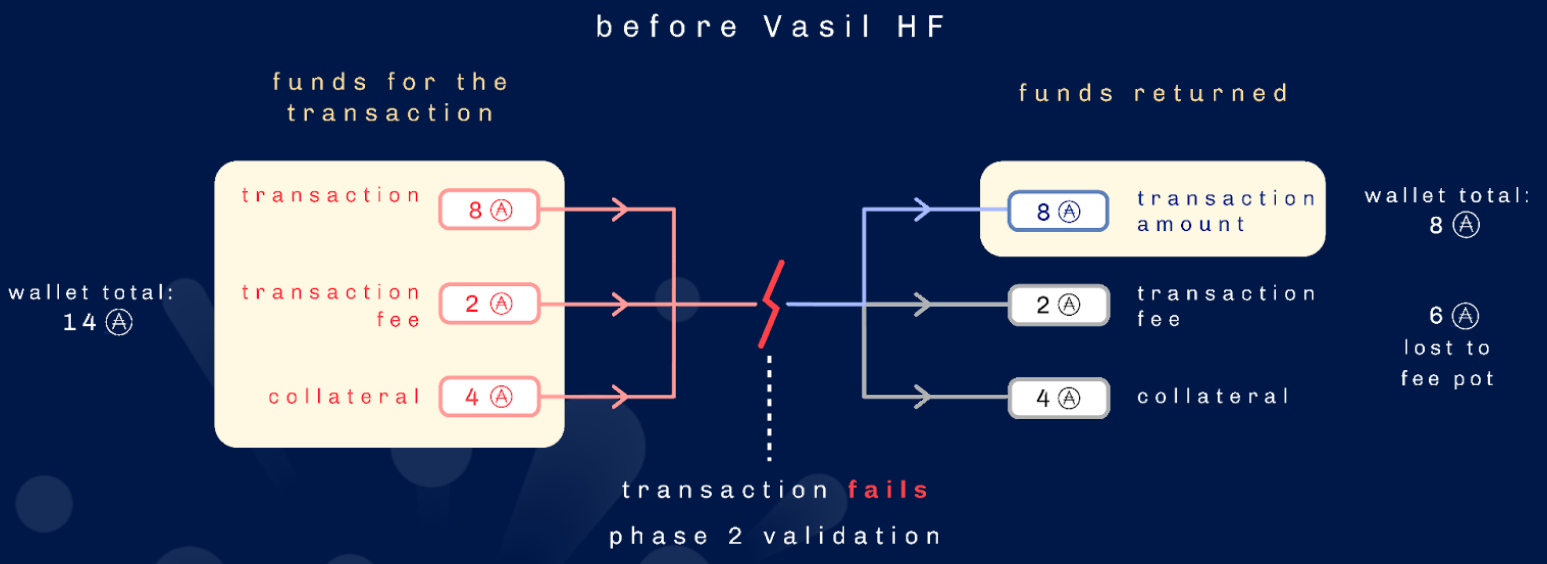
- CIP-32: インラインデータム

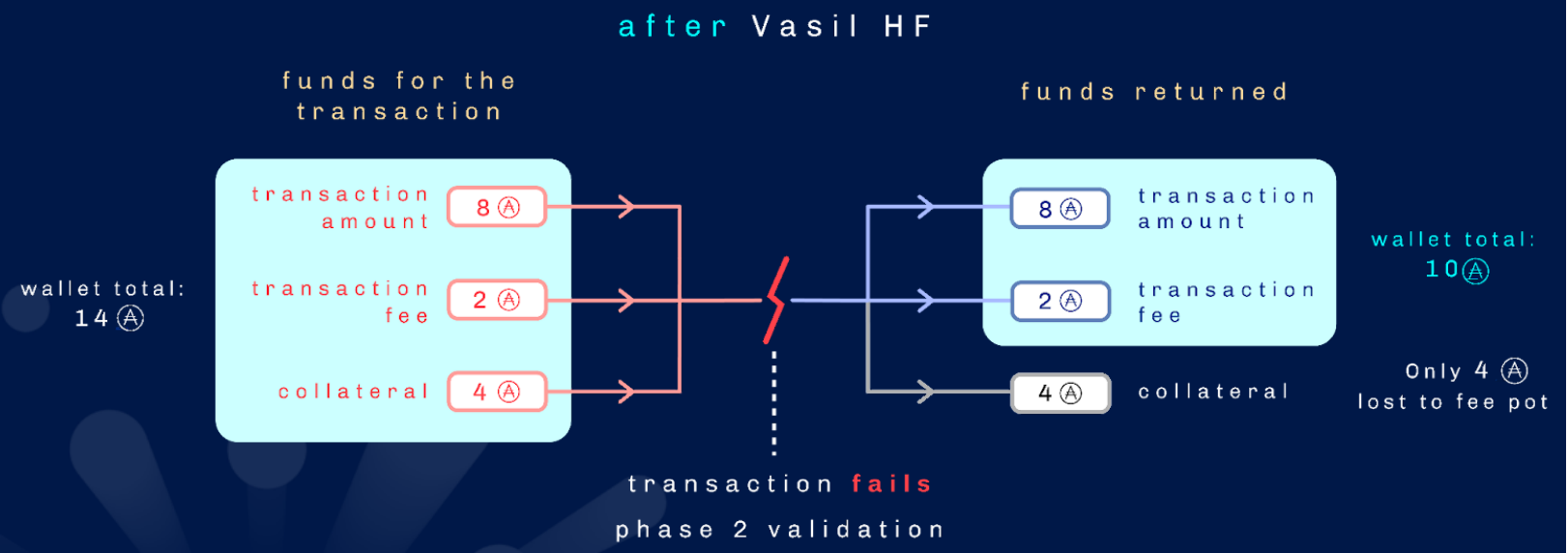


- CIP-33: 参照スクリプト



- CIP-40: 担保アウトプット





結論：EUTXOモデルを革新的で実践的にしているものとは?

Cardanoの台帳モデルはUTXOモデルを拡張し、その主要な利点を損なうことなくマルチ資産およびスマートコントラクトをサポートできるようにします。その革新的な研究は、他のUTXO台帳でサポートされている以上の機能性を可能とし、Cardanoを次世代ブロックチェーン界において他に類を見ないコンペティターとしています。

参考文献

CardanoのEUTXOモデルの詳細は、以下を参照してください。

EUTXO whitepaper

Cardanoの拡張UTXO - マルチ資産とスマートコントラクトをサポートするために構築された会計モデル