DAEX：分散型デジタル資産決済エコロジー
テクニカルホワイトペーパー

contactus@daex.io

要約

デジタル資産に描かれた明るい曲線は、信頼性と安全の方で常に暗くて光がない。現在のデジタル資産業界には多くの欠陥があり、市場流動性や資産価値、エコロジー秩序などの内在的な訴えは進化する必要がある。本文はDAEX決済コロジーのレイヤー構造や決済チェーン、マルチ資産ウォレット、アイデンティティチェーンを含む製品ソリューションを紹介し、非同期オープンネットワークにおけるASPOSの価値コンセンサスメカニズムを定義し、透明で安全な管理メカニズムの確立を期待し、将来デジタル資産取引の基礎の斬新決済ネットワークを構築し、安全や信頼性及びオープンなエコロジービジョンを実現し、人々がその価値を証言することを促進する。

1 エコロジーの概要

1.1 背景

（1）頻繁なデジタル資産安全事件

今までのデジタル資産の発展におけて、投資家や取引所はハッカーの攻撃を遭遇する事件が珍しくない、特に最近のデジタル取引所 Coincheck はハッカーの攻撃を遭遇した。これは主なデジタル資産価値にそれぞれ程度の幅で下落した。これらのリスク事象により、デジタル資産市場は直面する安全と信頼性問題について急ぎで解決する必要がある。

（2）不完全な業界決済施設

ブロックチェーン 3.0 世代は、ビジネスシーンで駆動されるブロックチェーンの基礎プロトコルを再構成する必要があり、これにより具体的な分野の重量級製品を実現する。現在、ブロックチェーン技術に基づく登録のデジタル資産業界は、明確な責任境界と十分な透明性及び安全性が欠如し、悪質な操作や意外な盗難を遭遇しやすいである。

（3）安全と信頼性インフラの欠如

デジタル資産エコロジーのインフラにおいて、決済メカニズムを変更するのが重要である。一般的なデジタル資産決済メカニズムは、開拓性を欠如し、複数の市場および豊富なデリバティブとインテリジェント資産市場について浸透と統合能力を欠失し、必要なエコロジー決済施設はデジタル資産の各活動に安全と信頼のサービスを提供する。同時に、良質なデジタル資産ウォレットはブロックチェーン技術に基づくその裏の信頼性を示す必要があり、これは市場の苦境を解決するだけでなく、デジタル資産の取引関係を進化させ、本当に安心の資産安全管理者になる。

1.2 エコロジーのデザイン

DAEX が取り込んで構築する分散型デジ

タル資産決済エコロジーは、ブロックチェーンに基づくマルチ資産決済の基礎プロトコルから出発し、資産と取引のデカップリング、トークン及び権限の強化を通じて、デジタル資産取引の基礎構造を再構築し、多くの面で決済エコロジーの安全性と柔軟性を保証する。これにより、デジタル資産接続ノードの取引プラットフォームと一般的なデジタル資産ユーザーを含め、DAEX は全体デジタル資産のエコロジーにサービスを提供することができ、より安全より効率的な分散型資産の登録と決済業務モードを可能になる。

1.2.1 価値チェーン

DAEX エコロジーは、デジタル資産取引の上流と下流の産業構造を最適化及び改善することに向け、身分認証と資産登録から資産精算及び決済の全体チェーン価値のサービスプロセスをカバーする。

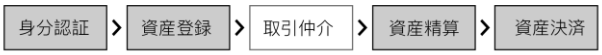

図 1：決済エコロジーの価値チェーン

取引、決済、信託管理を層別化することは、DAEX チームがデジタル資産業界における長年の実践及びインターネット技術専門家とコンピュータ科学者の総合的な知識を集めて、共同で得た最適化のソリューションである。徹底的追求の偏屈な集中化を離脱後に、分散型取引プラットフォームと分散型決済を組み合わせる経験で、人々がその価値を証言できるネットワークを創造する。

1.2.2 エコロジーのコンポーネント

DAEX エコロジーは、マルチ資産ウォレットをリンカーとし、身分認証センターや資産決済センター及び登録決済センターをリンクする。決済センターは分散型決済チェーンがブロックチェーンの安全と信頼のメカニズムを通じてデジタル資産価値移転における信用度を向上させ、また標準化の決済協議に基づくオープン決済エコロジーを支える。

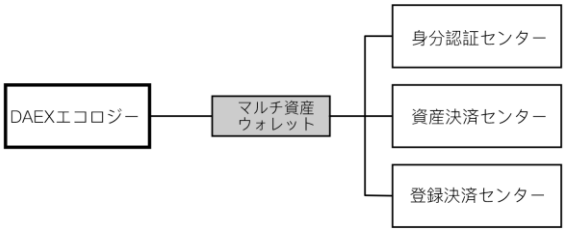

図 2：決済エコロジーのコンポーネント

決済チェーンは従来のパブリックチェーンの各技術特性を備え、そしてコンセンサスメカニズム、取引暗号化、プライバシー保護などの主要技術に最適化とアップグレードさせる。また、決済市場に基づいて、デジタル資産分野の身分認証、登録マッピング、交換支払い及び資産管理などの具体的な需要を細分化し、身分認証センター及び登録決済センターとともに、既存取引モードと完全に互換性がある基礎構造を提供し、且つ将来事業発展のクリアリングサービス（Clearing-as-a-Service）ソリューションをサポートすることができる。さらに、健全な取引エコロジー建設の責任を取るために、DAEX は安定の審査可能なスマート契

約による金融決済シナリオを拡大し、決済チェーンレイヤーに分散型スマートデジタル資産やデジタル資産オプション先物などの金融デリバティブを加え、オープン決済システムに潜在的無限な自己進化空間を持される。

決済チェーンに基づく派生の分散型デジタル資産ウォレットは、ユーザーが自己決済に利用のツールであり、これにより資産の管理を実現且つ交換決済シナリオを充実させる。スレッショルド署名、グローバルアイデンティティ証明書、信頼性コンピューティング環境などの技術と管理メカニズムに基づいて、さまざま種類のユーザーに機能完全なデジタル資産管理サービスを提供する。例えば、取引プラットフォームの企業レベルサービス製品は、権限の分離とリスクの制御を重視する。ユーザー資産のサービス製品は、資産の多様性と秘密鍵の安全性を重視する。

1.3 能力モデル

オープンエコロジー構造は、複数タイプのエンティティがコラボレーションによる情報処理と価値移転を完了することに満足させる可能である。各レイヤーの対象に向け、DAEX はその必要な基本機能を提供する。例えば、決済チェーンに基づくデジタル資産マッピングとクリアリングサービス、マルチ資産ウォレットに基づくセグメント化されたキーと信頼性のライセンスメカニズム及び身分認証センターの証憑ライフサイクル。

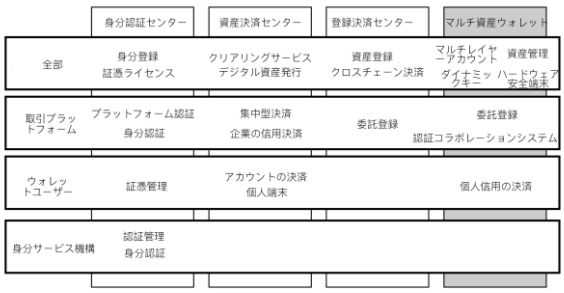

図 3：決済エコロジーの能力モデル

2 エコロジー企画

2.1 エコロジーの構成

清算チェーンは清算エコロジーのコア基礎チェーンであり、その応用レイヤーは複合式のクロスチェーン業務構造をサポートし、身分チェーンと決済チェーンを含む複数の機能チェーンと接続することが可能である。同時に、取引プラットフォームのレイヤー化分枝チェーンにより、高並行性需要の技術指標が満たされる。DAEX マルチ資産ウォレットは、分散型資産管理と分散型の清算及び決済サービスを実現するキャリアであり、標準化されたサービスとしての清算を実現する。そして、清算チェーンのインフランに基づいて、物理的な分離かつロジック独立の身分認証センターと資産登録決済センターを併設し、完全な清算及び決済価値チェーンとエコロジーガバナンスシステムを構築する。「マルチセンター」のレイヤー化エコロジー構造は、ブロックチェーンプロトコル自体の制限を解決するため、そして分散型ネットワークが安全で

信頼的に外部情報とインタラクティブを行うことを確保する。その内に、身分認証センターと資産登録センターはそれぞれに身分チェーンと決済チェーンにマッチングする。同時に、資産と業務の安全なレベルを高めるために、多段階の多様な認証技術を採用し、そして独立センターの片方信頼度を最小限に抑え、分散型帳簿とエコロジーコンセンサスに基づく中立技術によってエコロジーの信頼性裏書を実現する。

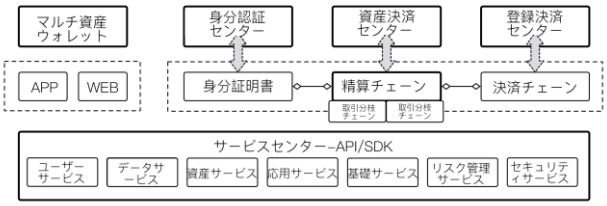

図 4：決済エコロジーの構成

2.2 アカウントシステム

清算エコロジーのアカウントシステムは資産と所有者との間の関係を確立し、これは分散型帳簿のコアの一環である。各参加者にとって、自分の清算アカウントの作成することは分散型清算と決済サービスを利用の第一歩である。DAEX エコロジーに、アカウントシステムは所有者をコアとして、アカウントの各種資産数と取引事件を記録し、拡張可能なアカウント構造は柔軟な業務モードをサポートする。同時に、すべてのアカウントは認証された信頼性の身分であり、デジタル資産の委託管理は制御可能な安全環境で、ユーザーはデジタル資産の所有権を持つ。それではこのアカウントシステムの存在であるため、デジタル資産はプライバシー保護戦略によって非公開の実名身分を持ち、資産の確実性と所有権にサポートを提供する。

清算エコロジーに、利用者の種類に応じて、アカウントは個人アカウントと組織アカウントを区分されることができ、その中に組織アカウントは一般組織アカウントと取引プラットフォームアカウントを含む。一般的に、組織アカウントは高頻度取引または複数レベル許可の企業型アカウントに適用し、例えばマーケットメーカーやファンド。個人アカウントは支払交換の優先的な方法である。取引プラットフォームアカウントは特殊な組織アカウントとして、信頼性清算を実現する重要な部分である。

図 5：清算エコロジーアカウントシステム

デジタル資産の状況により区分する場合は、各アカウントは対応する委託管理アカウントとマッピング口座にも派生されることができる。委託管理アカウントは登録資産の委託管理状態を示され、公開的に監督し、異常な不正流用を避ける。マッピングアカウントは、資産登録後の清算チェーンに記載された実際の有効資産である。委託管理アカウントは頻度に応じて更新と決

され、マッピングアカウントは使用シナリオや業務需要によって様々なサブアカウントに分割されることができ、サブアカウントとの間の資産配置によるさまざまな業務戦略を実現し、例えば資産アカウントや取引アカウントとの間の分離管理。一般組織のマッピングアカウントはレイヤー化役割によって許可審査メカニズムに埋め込まれる。個人ユーザーは取引所に関連のサブアカウントの作成により、同じ身分でのマルチ取引プラットフォームの個別アカウント操作を実現する。取引プラットフォームのマッピングアカウントはプラットフォーム内部のユーザサブアカウント取引の清算と決済の統合でチェーンにリンクすることにサポートし、金融製品のサブアカウントに基づくリスクブロッキングを実現することができる。

清算エコロジーで、アカウントの一般的な構造は全体的な身分ロゴ、カスタマイズ名称、アカウントタイプ、アカウント状況、清算アドレス及び資産リストを含め、その中に資産リストはデジタル資産の種類、委託アドレス、残高などの重要要因の多次元配列である。

全体的身分のロゴ	決済アドレス	アカウント名	アカウント類別	アカウント状況	取引プラットフォームロゴ	資産リスト 資産種類、残高、*信託アドレス

図 6：清算アカウントの構造

アカウントの取引事象は振出先、振入先、資産種類、発生額、事象時間、事象タイプ、取引ルート、取引ハシ、ブロック高さなどの出入情報を含む。

振出先	振入先	資産種類	発生額	事象時間	事象タイプ	ルート	*取引ハシ	*ブロックの高さ

図 7：清算取引事象の構造

2.3 ビジネスモデル

デジタル資産業界は出現したからグローバル化の金融世界であり、様々な区域とリンクの金融製品である。現在、ユーザーのデジタル資産はさまざまタイプと機能特徴のデジタル資産ウォレットまたは取引プラットフォームによって管理且つ記帳し、各ツールはそれぞれに資産の清算と決済のプロセスを完了し、情報の透明性と資産安全の責任は分散型の公的チェーンノードまたは集中化の運営主体による担い、クロスプラットフォームのデジタル資産の清算と決済は同時に業務モデルと技術的ボトルネックによって制限される。DAEX は分散型清算による集中化取引の資産信頼性問題を解決し、集中化と分散型取引のそれぞれの利点を組み合わせて、デジタル資産取引プラットフォームと投資家にデジタル資産業界に適用される完全な安全システムと資産保険ボックスを提供し、公平性やコンプライアンス及び効率性を兼ね備える。

現在の従来的な金融市場は、銀行、登録決済会社、取引所、証券会社、ファンド会社などから共同で構成さる成熟の商業エコロジーであるが、デジタル資産市場の構造的発展過程にも同様のように、さらに複数の専門的な組織に転化し、ではこれらの

組織は分散型的または分散型コミュニティの形である可能性があり、技術によって信頼性を作り出し、そして財務と道徳的リスクを低減且つ分離し、次の通りに実現する。

（1）データの真実と信頼性

デジタル資産の分散型清算と決済はデータの改ざんや偽装のリスクを避け、データの裏の資産所有者のみにデータの「変更」操作を開始する権利を持つ。

（2）資産のリアルタイム登録

デジタル資産取引を譲渡後に、標準の清算と決済プロセスによるデータの変更はすべてのノードに同期可能なことを確保させ、クロスドメイン資産の統一登録を実現する。

（3）プライバシー保護

システムの内部とスマート契約においてプライバシー保護策を追加し、資産関連者の明示的因子とチェーンの身分のコード化に基づいて、個人及び取引プラットフォームのプライバシーデータの保護を強化することができる。

DAEX 清算エコロジーの本質は取引データがデジタル資産から分離したレイヤー化システムを実現し、構造のレイヤー化とデータの断片化により、取引プラットフォームを専門の取引サービス機構になり、すべてのデジタル資産は委託管理機構による登録を完了し、取引の清算は分散型清算チェーンによって保障される。委託管理の基本的業務の流れは図 8 に示される。

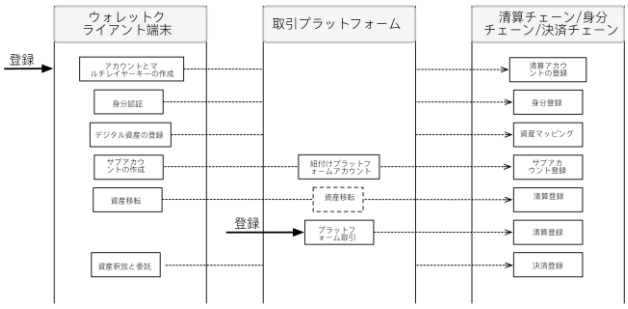

図 8：委託清算の基本ビジネスプロセス

取引プラットフォームの業務継続性を確保するために、分散型清算プロセスは取引に向ける委託清算とサービスに向けるクレジット清算を区分し、徐々に人々の清算にアップグレードする。その内に次のことがある。

- 委託清算は分散型清算の主な会計方法である。
- クレジット清算は将来の支払交換の重要な清算業の形である。
- クレジット清算は資産の登録プロセスに制限されない。取引プロセスのリスク管理、クレジットレベル及びプラットフォーム保証金に対して一定の要求がある。
- 人々の清算はDAEXエコロジーの各ユーザーに複数のルートによってデジタル資産清算のコンセンサス同期過程に参加且つ検証し、清算報酬を得る機会がある。

2.4 エコロジープロトコル

統一の業務プロトコルはサービスとしての清算などのサービスモデルをを実現す

る基礎であり、多様なシナリオに対応する必要があり、リッチな抽象的な業務モデルにより、クロスプラットフォームのチェーンのデータ共有を満たす。そのため、清算エコロジーはデータの記録方法について十分に通用的、標準的かつ構築しやすい。同時に、各構造化情報を有効的に表示することができ、そしてカスタマイズ可能なオープンプロトコルを備え、それによって業務範囲の開拓による必要なプラットフォームとクロスチェーンの要求を実現する。

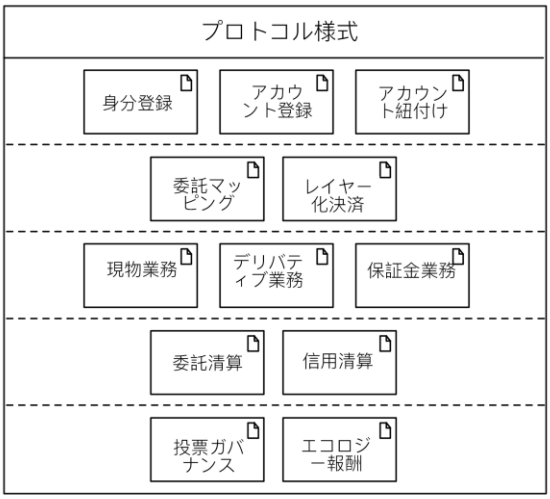

図 9：清算エコロジーの基本プロトコル

エコロジープロトコルは清算と決済帳簿に保存される業務情報ドメインとフォーマット、業務プロセスに発生の業務状況、業務状況変更の触発方法と条件及び関連する更新情報などを規範化する。各参加者は身分アカウントによってスマート契約に基づく実現する業務プロトコルを締結するため、その実行過程はブロックチェーンシステムの客観的な技術裏書を取得し、これはプロトコルが各ノードにおける一致実行することを含め、すなわち業務主体が認められる。プロトコルの実行プロセスは正確に記録され、その最終結果は改竄できない。つまり実行される業務事実は否定できない。

3 エコロジーの構造

ブロックチェーン技術が持つ無仲介化と非改竄の遺伝子は、DAEX エコロジーの価値蓄積と流通に基本的なソリューションを提供し、しかし一つ分散型自律的なコミュニティエコロジーを実現するために、基本プラットフォームの必要な性能を備え、つまり業務の需要に適応なスループットのほか、また全体エコロジーのインフラは優れた相互操作性による完全な「コンセンサス」が必要であり、これは分散型ファイルシステムの利用でデータストレージのパフォーマンスを向上させること、コンセンサスプロトコルによる清算と決済モデルの最適化、マルチ資産ウォレットに基づくデジタル資産ツールの安全性と容易性を向上させること、また業務ガイドを提供するサービス化インターフェースが快速アクセスのサポートなどのソリューショを含む。これにより清算エコロジーの製品の組み合わせが以下の利点を備える。

（1）より強固

ユーザーがプライベートで保管、完全なキーを送信する可能性を回避し、そしてユーザーをコアとし、チェーンの複数コンセンサスに基づいて、分散型元帳で効率的なアカウンティングを完成させる。

（2）より豊富

ブロックチェーンの拡張性を拡大し、マルチ資産の快速取引をサポートする。また、清算チェーンの上位レベルの基本サービスは、既存の取引の深さを保持するだけではなく、デリバティブとスマート資産の豊かなビジネスエコロジーを提供することができる。

（3）より高い信頼性

マルチ資産ウォレットが採用のセグメント化キーメカニズムと信頼性コンピューティング環境は資産の安全性を向上させる。同時に、清算価値ファクタに基づくコンセンサス・メカニズムは公平で共有する価値報酬と詐欺行為の処罰の権威を確保する。

3.1 清算チェーン

清算チェーンはデジタル資産取引プラットフォームなどにインターフェースのサポートを提供し、個人取引先、組織取引先にデジタル資産ウォレットの身分認証情報を利用で支払交換の操作を行うことができ、そしてコアスマート契約の資産清算プロセスを完了する。また、デカップリングと柔軟に配置可能な機能コンポーネント及び清算チェーンのスマート契約エンジンは共同で複数のシナリオの需要に適応し、デジタルスマート資産の様々な行動活動を満たす。

清算と決済の業務については、清算チェーンの必要性がそれのスマート契約を持っていないオリジナルチェーンにアトミック性を与える。両側の協議の結果によって、突進能力を持つ清算と決済の契約を実現し、資産引き渡す決済のアトミック性を確保する。清算チェーンは双方向で委託管理資産とマッピング資産に目指し、ユーザーはデジタル資産の流れのみに確認し、同時に清算エコロジーで共同で建設の取引プラットフォーム連合にメンテナンス且つ各参加者の誠実さを向上させる。清算チェーンの「マイナー」は清算の証人として、清算チェーンの現在のデジタル資産状況について検査と監視を行う。彼らが取引要求を受けると、その結果に対して真実の一致性を達成することを確保するために、清算と決済プロトコルを同期に執行する。正直なマイナーは清算チェーンにおける参加程度が高くければ、システムの全体安全性にも高くなる。

3.1.1 デザイン原則

- スマート契約は清算エコロジーの主要な価値キャリア方式である。
- 清算価値ファクターはノードが報酬を検証する重要な要因である。
- POS コンセンサスメカニズムをアップグレードし、取引パフォーマンスと数学的なランダム性を向上させる。
- デジタル資産取引の指向性暗号化案を提供し、一部シナリオは清算関連側のチェックと取引検証をサポートする。
- 規制支持と監査実現の要求を満たす。
- 清算チェーンのデータの一致性は

コア要件であり、緊急時に効果的なガバナンスメカニズムを使用で分岐を回避することができる。

3.1.2 製品の構造

清算チェーンが実現するブロックチェーンの基本機能についてはキー管理、スマート契約、元帳データなどを含め、そしてノード、ブロック情報の監視を提供する。具体的には、図 10 に示す 3 つレイヤー構造である。

（1）基礎プロトコルとシステムサポートレイヤー

清算チェーンの基本的なインフラとし、ブロックチェーンのブロック構造、ストレージタイプ、帳簿モデル、操作指令などの標準とプロトコルを定義するだけなく、クラウドサービス技術システムとを互換性にもあり、コンテナテクノロジを利用で迅速な展開と配置管理を実現することができる。

図 10：清算チェーンの構造

（2）コアモジュールレイヤー

コアモジュールレイヤーのデータインタラクティブは内部データ交換プロトコルによって実現され、各コンポーネント機能は独立かつデカップリングし、同時にデータとロジックに分離され、それによりモジュールコンポーネントのプラガブルと拡張性を実現する。

コンセンサスコンポーネント：コンセンサスコンポーネントは主に取引のブロードキャスト、並べ替え、実行とコンセンサスなどの内容を完成する。POS 保証金マージンメカニズムに基づいて、清算価値ファクターの報酬と検証可能ランダム関数を統合する。

帳簿とストレージコンポーネント：帳簿情報の持続性は成熟の NoSQL データベースに基づいて実現され、それでは KV データフォーマットは簡潔と快速なストレージモデルを提供し、ストレージ情報は非改竄性を備える。

P2P 通信コンポーネント:ブロックチェーンノードの間に P 2 P 通信を確立し、ダイナミック新規追加ノードを見出すことができ、そしてブロック情報を同期させる。

スマート契約ブラウザ：バーチャルマシン完全なチューリングの実行エンジンに基づいて、スマート契約にカプセル化と互換性することができる。各ノードは実行状況と結果のコンセンサスを確保する必要がある。それぞれ業務シナリオに適用する契約ロジックの作成により、清算チェーンのプログラミング性を実現する。

プライバシー保護コンポーネント：取引関係者だけで見られる取引レベルの暗号化をサポートし、取引無関係の非参加者は既存取引内容の暗号化後のハシ値のみを取得、検証する。

ノード管理コンポーネント：ノード権限のダイナミック配置と検証をサポートする。ノードは検証ノードと普通ノードを区分され、前者はコンセンサスプロセスに参加する。

エコロジーガバナンスコンポーネント：エコロジーガバナンスメカニズムを改善する技術ソリューションとして、ブロックチェーン技術が初期段階に起因する未知のエラーによるエコロジー破壊を回避する。清算エコロジーは長期的安定の持続可能なエコロジーであり、エコロジーコミュニティに設定のある特殊役割の機能に基づいて、分散型ガバナンス構造と合わせ、チェーンの外部で協議一致の状況で清算チェーンに応急処理能力を備え、悪意の破壊やソフトウェアバグ、ハード分岐などの突発状況を解決する。これは、運行とメンテナンスの可能性がブロックチェーンエコロジーとコミュニティ自律性のプロセスで実行できるようになる。つまりパラメトリックなデザインによるエコロジーは自己修復の能力を備える。

クロスチェーンコンポーネント：マルチチェーンおよび分岐チェーンの帳簿との間の情報インタラクティブをサポートし、データと業務ロジックは分離され、これは取引清算サブチェーン、身分チェーンおよび決済チェーンを含む。

(3) エコロジーサービスレイヤー

エコロジーサービスレイヤーはブロックチェーンの基本的プロトコルとコアモジュールの間の具体的な実現とシナリオのインターフェースに基づいて、API、SDK などの完全なツールセットを提供する。

RPC コンポーネント：ノードに送信された RPC の要求を処理し、ノードデータインタラクティブのエントリポイントである。ルールチェックによる無効なメッセージをフィルタリングすることができ、コンセンサス負荷が軽減させる。同時に、RPC サービスを柔軟に配置することにより、負荷バランスを実現することができ、そして各伝送プロトコルルールとシナリオのインターフェースをカスタマイズすることができ、さまざまな清算及びデリバティブサービスを満たす。

ブラウザコンポーネント：清算チェーンブロックブラウザを実現する基本である。ブロック情報、取引情報、ノード状況、ネットワーク状況などの情報及び統計結果の直接照会を提供する。

契約管理コンポーネント：スマート契約のモジュール化管理を提供し、これは契約の作成、テスト、配置、アップグレード及びテンプレート編集を含む。

エコロジー応用コンポーネント：清算チェーンは業務プロセスに向けるブロック

チェーン製品であり、エコロジー応用コンポーネントによる効率的身分、清算と決済、資産マッピングと発行などの応用機能を実現する。

3.2 マルチ資産ウォレット

清算エコロジーのマルチ資産ウォレット（DAEX ウォレット）は、それぞれに企業と個人ユーザーがデジタル資産を管理する要求に満たす。同時に、該当ウォレットもデジタル資産の身分証明書であり、身分認可により、それぞれに DAEX エコロジーの各取引プラットフォームにアクセスすることができる。

現在のデジタル資産ウォレットは、ユーザーが APP をアンインストールまたは再インストール、App Store 製品規則の変更、ユーザーがキーワードを忘れ、keystore ファイルを紛失などの原因で、ユーザーの資産が失われた事件が頻繁に発生した。DAEX ウォレットは複数レイヤー安全防御システムを提供し、ユーザーの行動安全、モバイル安全防御、キー安全管理、複数ファクターの検証などの多次元でデジタル資産の安全を保障し、資産の盗難を防止する。同時に、セグメント化キーメカニズムで条件付きによるキー紛失の原因で資産損失の問題を解決した。

使いやすさは DAEX ウォレットの一つハイライトであり、まずはこのハイライトが顧客のレイヤー化に表現し、組織と個人ユーザーにそれぞれに製品機能とクライアント端末を作り出し、それを異なる役割の資産マネージャーになる。また、先進的清算チェーン資産マッピングに基づいて、それはデジタル資産の管理と送受信にショートカットチャネルを提供する。同時に、ウォレットは身分であるこたで取引プラットフォームを埋め込み、取引コストの低減及び資産移転の確認時間を短縮することに役立つ。さらに、DAEX ウォレットはハードウォレットエントリを提供し、そのデリバティブソフトキーはエンドツーエンドの安全基盤を持ち、非否認シグネチャによるデジタル世界で高い信頼性を確立することができる。

3.2.1 デザイン原則

- マルチ資産マネージャーにポジショニングし、各主流派のデジタル資産をサポートする。
- 統一身分ロゴによる統合でアカウントの資産を管理し、それぞれのブロックチェーンがそれぞれのアカウントシステムと技術構造を持つ集合難問を解決する。
- 複数セグメントキーは分散でユーザーの資産を保護し、ユーザーは資産に絶対的な取引権を保有する。その他のキーの一部を委託で管理する組織はすべて単独でキーを回復または資産の取引を開始することができない。
- 独立性がある且つ取引プラットフ

ォームに適用の専門資産管理プラットフォームであり、企業レベルの機能性を埋め込み、例えば複数レベル認証と業務コラボレーション。

- ワンストップデジタル資産管理ツールである。ストレージ、支払い、交換、第三者サービスなどのシナリオのニーズに満たし、同時にデジタル資産の付加価値機能を拡張する。

3.2.2 製品の構造

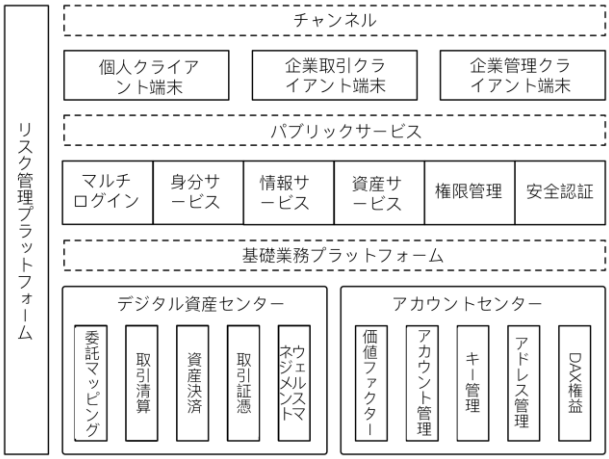

図 11：マルチアセットウォレット製品の構造

（1）基本機能

ウォレット資産のアドレスはランダムで生成され、ユーザーは各マッピング資産の管理をカスタマイズすることができる。エコロジーの資産移転プロセスは、清算チェーンのマッピング資産クレジット会計による完了し、且つユーザーカスタマイズ ID に基づく資産移転をサポートする。セッションごとでの決済プロセスはリスクレベルに応じて相応なレイヤー化対策に適合し、動的なパスワード、生体情報及び物理情報を含む複数組み合わせる相互検証をサポートする。決済を検証するたびに、清算と決済のリストによる双方向で残高を照合し、清算チェーンデータとウォレット資産アカウントとの一致性を確保する。リスク管理プラットフォームはデジタル資産の事前、進行中のリスク管理システムを提供し、身分とデバイスの識別、リスクモニタリング、ダイナミック戦略などの多次元でユーザーの資産を保障し、プロセスの監督を支える。

単独の個人と企業レベルのウォレットは、便利的シングルオペレーションとフロー化制御のマルチオペレーションニーズに満たすことができる。同時に、それぞれレベルのサブアカウントの作成により、迅速なクロスプラットフォーム及びクロス業務の資産財務管理を実現する。DAEX はワンストップのデジタル資産ウェルスマーケットを構築することに取り込み、これはデリバティブサービス、高品質資産管理、デジタル資産投資のコンサルティング、資金調達などの金融商品を含む。また、ウォレットは多彩のデジタル資産応用エコロジーにも提供し、例えばマーケット情報や第三者 DAP などのサービス。

該当ウォレットは DAX トークンの各な権益にも集中し、信頼性投票と清算証言報酬の獲得を含め、DAX を持つユーザーに清算エコロジーの建設に完全に参加することができる。

（2）セグメントキー

ユーザーの清算と決済アカウントは 3 段階キーメカニズム（ユーザー端末、ユーザー端末、委託管理端末）を採用でデジタル資産の安全制御を実現し、その中に秘密キーはセグメントによる暗号文で格納され、且つキーフラグメントは複数のメディアに格納される。信頼性のコンピューティングと通信環境に基づいて、キーメカニズムはキー作成、秘密キー切り分け、秘密キーフラグメントの暗号化格納、キー安全伝送、キーローカル回復と署名を含む全プロセスをカバーする。そのため、権限管理戦略に合わせ、それぞれシナリオの安全要件を実現することができる。

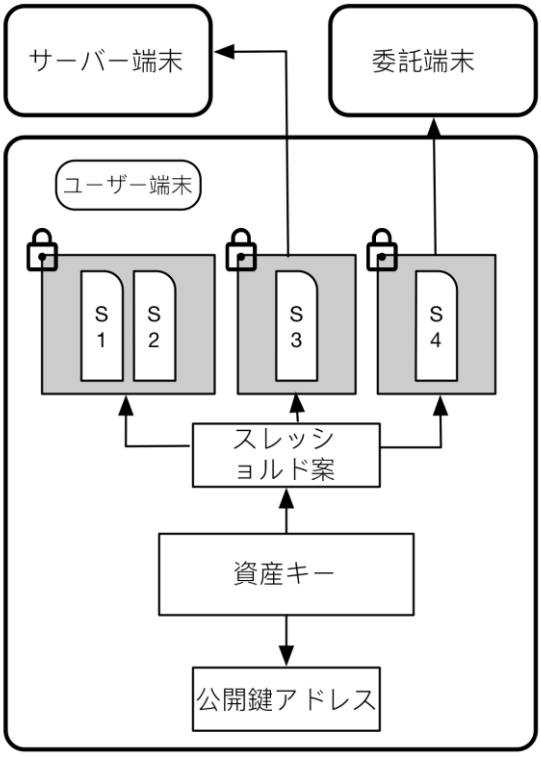

図 12：公開鍵アドレスセグメントキーのメカニズム

3.3 身分チェーン

デジタル資産取引プロセスに完全的、規則的、信頼的な身分サービスを提供するために、身分認可チェーンに基づく分散型身分認証センター（Distributed ID Center）は全体的視点の身分管理を実現した。これは身分登録、認証登録、身分証明書の管理、身分識別及び認可などのプロトコルと規範を含む。DIDC は各ユーザーに清算チェーンの身分ロゴを作成し、身分情報の記号化により、チェーンでの流通について信頼性の匿名を実現し、クロス取引プラットフォーム価値流通の身分基盤である。

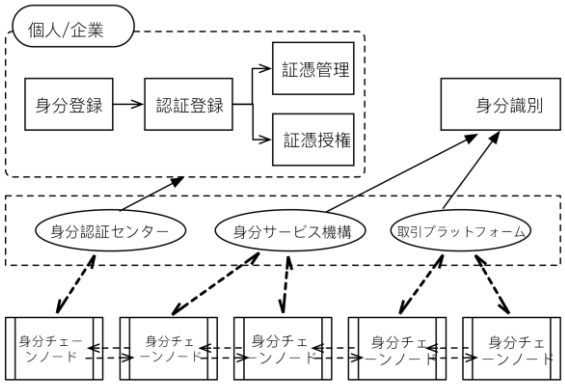

図 13：身分チェーンの全体構造

3.3.1 デザイン原則

- 複数の参加主体、複数の認証方法、複数の情報収集ルート。
- 強弱認証を含むレベル別確認認証レベルをサポートする。
- 身分認証の信頼性環境を提供し、身分証明書の発見、更新、抹消などのプロセスにおける安全の脅威を防ぐことができる。

- デジタル資産取引所、DAP P 及び第三者身分機構とともに全体ネットワーク身分連合を構築する。

3.3.2 主要機能

身分認証センターは身分チェーンに協力で身分管理プロセスを完成する。それは信頼性の環境に実行され、ユーザーが安全且つ正確に身分証明書の情報を提供することにサポート可能になる。同時に、身分認証プロセスにおける攻撃者からそれぞれの攻撃手段による発生の安全の脅威に直面し、従って、必要な安全技術を配備で認証通信プロセスにおけるオンライン推測、偽装サービス提供者の攻撃、盗聴攻撃、再生攻撃、セッションハイジャック、中間者攻撃、サービス拒否攻撃及び悪意コードインジェクション攻撃を防止する。

身分認証プロセスにおける各部分の認証強度に基づいて、それぞれレベルの身分認証を定義し、すなわちユーザー登録時にそれぞれの登録信頼性レベルを申請し、関連するユーザーの身分証明書に対応した後に、それぞれの証憑信頼性レベルを得ることができる。信頼性レベルが高ければ高いとほど、より多くデジタル資産サービスを利用することができる。身分管理プロセスは主に以下の 5 つ部分を含む。

（1）身分登録

全体共有する身分登録サービスであり、利用者は必要な身分証明情報を記入し、同時に関連する証憑材料を提供しなければならない。プロセスを簡素化するために、第三者身分サービス機構のアクセス登録をサポートする。

（2）認証登録

認証登録は登録された身分の検証であり、且つ身分データの暗号化とフラグメント持続化を完成し。認証が通った後に、身分チェーンは暗号化された身分情報のみに登録し、つまり身分の指紋である。

（3）証憑管理

身元認証の登録を完了した後に、身分証明書のマッピングは直ちに実行される。すなわち清算チェーンアドレスと身分証明書の同期紐付けを完了する。また、このプロセスは証明書の追加、更新、抹消などの身分ライフサイクルの管理サービスも提供する。

（4）証憑授権

身分チェーンに基づく信頼性認証であり、エコロジーシステムの内部と外部のクロスチェーンとクロス応用の身分共有サービスを実現する。

（5）身分識別

取引プラットフォームと身分サービス機構は許可を経て身分の識別サービスを利用することができ、ユーザーの身分認証情報に対するクロス検証および認証フィードバックを完成する。

3.4 決済チェーン

デジタル資産登録センター（Digital

Assets Registration Center）は決済チェーンデジタル資産の登録委託管理と清算チェーンにおける資産マッピングを実現する。資産マッピングはクロスチェーンによるロックし、様々なデジタル資産の自由発行と流通をサポートする。同時に、複数認証技術と戦略による「登録者」の真実性を検証し、分散型構造とダイナミックアカウントで価値管理の安全性を向上させ、単一ポイントの障害による発生する資産の「凍結」を回避する。

資産登録センターのデジタル資産の委託管理ウォレットはクールウォレットであり、オフラインの安全ルームに保管する。各デジタル資産は分離ネットワークを採用による異種サーバーで独立運行及び監視される。チェーンにおけるデータは、複数ポイントの同期による適時性と正確性を確保し、リアルタイムで第三者のブロックブラウザと双方向による検証する。DARC の主な役割は次のことを含む。

- 委託管理キーの動的作成と配布。
- キーフラグメント暗号化ストレージ。
- 資産受入の検証。
- 資産登録とマッピング。
- 資産のクロスチェーン交換。

DAEX 清算エコロジーはブロックチェーンプロトコルレイヤーにおけて、クロスチェーンの価値移転を実現し、ある程度で 1 つ分岐チェーンのソリューションとして理解することができる。具体的には、デジタル資産が第 1 ブロックチェーンから第 2 ブロックチェーンに転移することができ、その後のある時刻に第 2 ブロックチェーンから安全に第 1 ブロックチェーンに戻り、ここの第 1 ブロックチェーンはビットコインやエテリアムなどの決済メンチェーンであり、第 2 ブロックチェーンは清算チェーンという「分岐チェーン」である。それはまさに清算エコロジーの存在により、各デジタル資産はメンネットワークの外でもっとビジネスシナリオとコンプライアンス監督資に沿える資産産取引及び清算と決済を行うことができる。

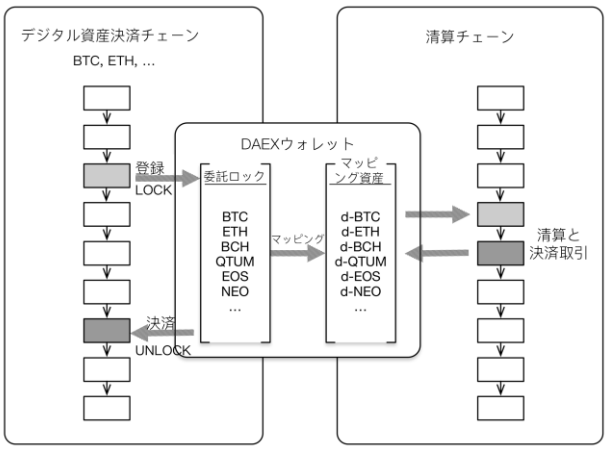

図 14：登録と決済の例示図

4 エコロジーコンセンサス

コンセンサスメカニズムは非信頼性環境で信頼性結論の達成を利用するメカニズムである。現在の公共チェーンにおける様々なコンセンサスメカニズムは、さまざ

まの問題がある。我々が提案の ASPOS（Accumulative Signature for POS）メカニズムは効率的、低エネルギー消費、安全なコンセンサスメカニズムである。ASPOS にブロックはブロードキャストプロセスに各検証ノードが順次に蓄積シグネチャし、シグネチャが一定比率を蓄積または一定確認数があった場合は、チェーンに受けられる。アルゴリズムでは、VRF の抽選関数を使用し、ブロックノードを作成するランダム性が確保し、同時に保証金制度を利用で無利害関係の問題を解決する。ASPOS は自分の視点から非同期パブリックネットワークで高い可用性を持つアルゴリズムである。

4.1 基本コンセンサス

ブロックチェーン技術の先例として、ビットコインはプルーフオブワーク（POW）コンセンサスを利用し、このコンセンサスメカニズムのコアアイデアは経済的報酬とノードコンピューティング競争による帳簿の一致性を維持する。コンセンサスの結果は最大ブワーク負荷付加のブロックがコンセンサスプロセスで勝ち、勝つブロック作り出すノードは経済的報酬を得る。このようなコンセンサスメカニズムの安全性は特別設計の経済的報酬に依存し、そしてオープンネットワーク環境できわめて高い利用性がある。同時にオープンネットワークの複雑性はチェーンに一時的分岐を招くことができ、このような一時的な分岐はシステムの安全性に低下され、且つコンセンサスプロセスに延長されることが生じる。利用性と安全性のバランスを取るために、ビットコインはより長いアウト時間（10 分）を選択し、これによりコンセンサスの効率は低下される（1 秒あたり僅か 7 取引のみを処理する）。また、ビットコインのコンセンサスプロセスに高エネルギー消費は、常に批判される理由の 1 つとなる。

POW のエネルギー消費問題を解決するために、POS システムコンセンサス（POS3.0、DPOS、Casper など）が提案されました。POS においてノードがブロック作成権を獲得する確率はその持つ権益（コイン数、コイン期間、保証金など）の割合に依存する。POS には無利害関係（Nothing at stake）と長距離攻撃（Long range attack）が現れやすく、これはシステムの安全性を深刻に脅かす。Casper は保証金と slasher による無利害関係問題を解決し、弱い主観的是正と検査点制度による長距離攻撃問題を処理する。しかし、Casper アルゴリズムはノードを予測することができ、これは潜在的な DDOS 攻撃を引き起こすことができ、従って、システムの安全性を低下させる。Algorand アルゴリズムはランダム抽選による新規ブロックの発生ノードを決定し、このランダム性は Casper が直面の DDOS の攻撃問題を解決に利用できる。

Casper におけるベッティングベースコンセンサスはコンバージェンスプロセスに他のノードのベッティング状況に基づく自分のベッティングを決定する。このコンバージェンスプロセスは全体のベッティング

情報（すなわち、神様の視点）について強く依存し、システム実行の難しさを増やし、利用性を制限する。POW におけるノードはブロックの選択にも実際の一種ベッティングであり、完全にそのブロックの既知情報に基づく（すなわち自分の視点）。この自分の視点に基づくブロックの選択メカニズムはシステム実行の難しさを低減し、システムの利用性を向上させる。

以上をまとめ、我々は ASPOS コンセンサスメカニズムを提案する。これは Casper の保証金システム、Algorand の抽選システムと POW の自分視点選択メカニズムのコンセンサスが融合された。

4.2 ASPOS コンセンサス

ASPOS はPOSアルゴリズムの変形として、より小さい抽選で選ぶ値とより多く検証署名累計割合のブロックを含む選択することによるブロックをブロードキャストプロセスに分岐のコンバージェンスを実現した。システムの正常な運行を保証するために、プロトコルで相応な収益配分と処罰規則を設計した。

4.2.1 権益の構成

それぞれの POS メカニズムにおける権益の内包はそれぞれ違い、既存の POS メカニズムはコイン価値、コインの発行期間及び保証金額などに基づく異なる形がある。ASPOS の権益は保証金額、ノードの活発度及び清算価値ファクターと有機的に組み合わせた。

ノード価値ファクターはノードを検証でユーザーの清算信頼を獲得する数学的統計であり、総合的権益はユーザーの清算価値ファクターの信頼に基づいて、その高低はノードの最終収益に影響する。そのため、ASPOS は CVF－POS とも呼ばれるが、各ユーザーの積極的な清算価値ファクターによる全体エコロジーシステムの健全な発展を促進することがでる。

$$S = C\sum_{i=1}^{n} F(e_i)$$

S は検証ノードの権益または割合であり、C は検証ノードの保証金限度額であり、F は価値信頼関数であり、e_i は第 i ユーザーの清算価値ファクターであり、n は信頼性ユーザーの総数である。

4.2.2 新規ブロックの作成

システムには、4 つタイプノードを含む：通常ノード、検証ノード、送信前ブロックノード、送信ブロックノード。通常ノードはロック保証金の納付による検証ノードになる。活発度が上位の検証ノードは送信前ブロックノードになる。送信前ブロックノードは抽選関数の抽選でブロックノードになり、抽選されなかった送信前ブロックノードは検証ノードに戻される。

送信ブロックノードは新規ブロックを作成し、そしてブロードキャストする。検証ノード（発信ブロックノードも検証ノードである）は、受信した新しいブロックを検証することができる。検証を通過する場

合は、署名した後にこのブロックをブロードキャストし、さもなくばこのブロック放棄する。普通ノードはブロックに署名できないほか、他の機能は検証ノードと同じである。

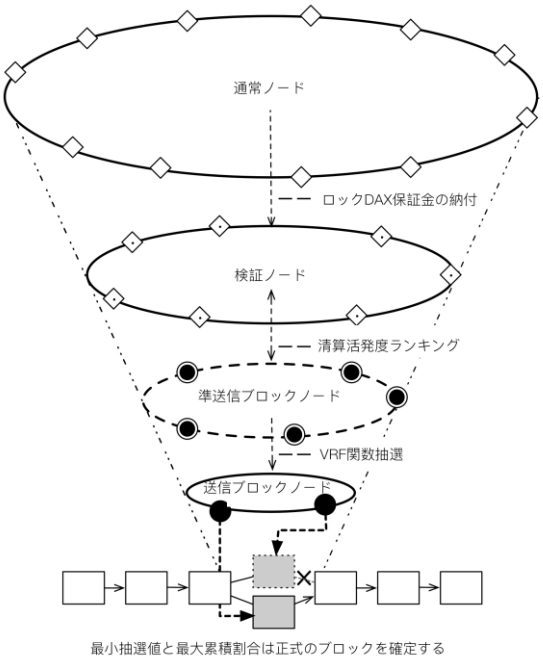

図 15：ASPOS のブロック作成プロセス

特定のアドレスに検証集合契約が存在し、検証者集合の変化を追跡することを使用される。通常ノードはこの契約による保証金を送信することで検証ノードになる。検証ノードは契約にメッセージを送信することによる検証者集合を脱退することに申請することもでき、脱退申請は有効になった後に一定時間の解凍期間を経って、保証金は指定されたアドレスに戻すことができる。

チェーンにおける最高の高さを持つ N 個ブロックでの取引を統計し、すべての取引の提出者から提出した取引総数を統計し、取引総数をランキングし、そのランキングを各取引の提出者の活発度のランキングとし、活発度ランキングの上位 K を持つノードは送信前ブロックノードになる

ASPOS はVRF の抽選関数を採用で次高さブロックのブロックノードを選択する。抽選でもたらすランダム性はノードの賄賂や DDOS 攻撃などの問題を避けることができる。抽選関数は前の高さブロックの hash、現在の高さ、抽選回数とノードの権益による構築され、送信前のブロックノードは自分のキーを VRF 関数に持ち込んで自分の選択値を計算する。もし、送信前のブロックノードの選択値が現在の選択値の閾値により小さい場合は、送信前ブロックノードは送信ブロックノードと見なすことができる。全体的な視点から見ると、VRF のランダム性のため、選択値を満たす送信前ブロックノードは複数存在可能性があり、そして存在しない可能性にある。複数存在する場合は、それぞれに選択値を満たす条件の送信前ブロックノードはそれぞれにブロックを生成し、且つ VRF 関数値を自分によって生成のブロックに含まれ、ブロックを署名且つブロードキャストする。その他のノードは複数のブロックを受信した後に、最小値のブロックを選択して検証を行う。すべての送信前ブロックノードが条件を満されない場合は、改めて同一高さに次の抽選を行い、且つ選択のしきい値を修正する。

$$VRF(Hash(Block(R)), H, N, S, SK) < P$$

抽選関数 VRF の例示は上記の通りであ

り、H は現在の高さ、N は抽選回数、S はノードに対応する権益、R は前ブロックの作成ノードが作成されたブロックに追加するローカル物理ランダム因子、Block(R) は前高さのブロック、SK はノードの秘密鍵、P は選択するしきい値。

より高い権益を持つ検証ノードは大きな確率で抽選される。抽選プロセスのランダム数を増やすために、各送信ブロックノードは新規ブロックを作成する際にノードローカルから取得したランダム因子 S と SK を追加する。複数のノードが抽選されたときに、最小選択値を持つ送信ブロックノードから作成したブロックは、後の宣伝で選択され、各ノードのローカルチェーンに記入され、最終的にすべてのノードはコンセンサスを達成する。システムからアウトの平滑性を確保するために、一定時間ごとで、システムは適応的に調整し、しきい値 P を選択する。

4.2.3 コンセンサスプロセスの説明

すべての検証ノードは自分が受け取った最小選択値を持つ合法的ブロック hash に、累積署名且つブロードキャストし、普通ノードである場合はブロックの選択とブロードキャストのみに行う。検証ノードはブロックハシ蓄積署名にブロック分けでブロードキャストする。署名のサイズが小さいであり、従ってシステムは累積署名の存在による多い通信圧力を増加させない。ノードは同一ブロックの異なる累積署名の順序を受け取った時に、新しいシリアルの累積署名割合は地元より大きい場合、新しいシリアルをローカルシリアルをカバーし、さもなくば新しいシーケンスを放棄する。累積署名の例示図 16 に示す。

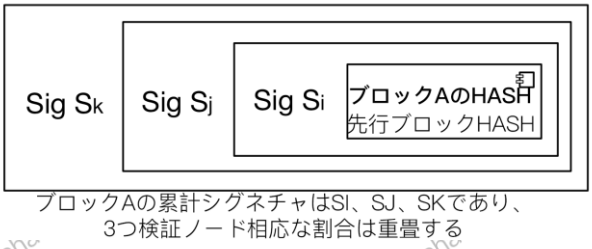

図 16：ASPOS 累計シグネチャ

新規ブロックの累積割合を一定の比率に達するか、または現在の最新ブロックの作成時間を T に達すると、再度活発性ランキングを運行し、且つ抽選で次高さのブロックを作成する。作成した新規ブロックに前ブロックに署名した検証ノードリスト（シーケンスがある）を追加し、これらの情報は署名ノードの収益証明をとする。

一つある高さで複数のブロックを発行した送信ブロックノードはダークノードと呼ばれる。ダークノードによって作成されたブロックはダークブロックである。現在選択値の最小のブロックがダークブロックである場合は、その高さのブロックを再作成する。ダーク根拠は検証集合契約に発送される。検証集合契約はダーク根拠を検証した後に合法的な根拠によってダークノードに処罰する。ダーク根拠は処罰根拠を集められ、処罰根拠は次高さの新規ブロックに記入される。

各ノードは直接にタイムスタンプとロ

ーカル時間との差が一定サイクルを超えるブロックに無視し、且つ前回高さブロックの作成時間との差がシステムサイクルを超える新規ブロックに無視する。

4.2.4 分岐処理

前文で同一高さの異なるブロックをある場合は、より小さい選択値のブロックを選ぶ。あるノードが選択値同一のブロックをある場合は、累積署名の割合大きいブロックを選ばれ、その他は放棄される。選択値は同じ高さと同じ回数の間で比較される。ローカルキャッシュブロックの高さと同じである回数もっと多い合法的新規ブロックがある場合、新規ブロックに該当高さのダークデータ集合にローカルブロックの作成ノードが含まれる場合、ローカルキャッシュのブロックが新規ブロックを置き換えられ、且つ署名（検証ノードの場合）で新規ブロックをブロードキャストする。

4.2.5 報酬と処罰

ノードの収益は 5 種類を含め：ブロックの作成で獲得収益、処罰根拠追加の報酬、収益根拠追加の報酬、怠惰根拠追加の報酬、ブロック検証参加の収益。あるブロックが N 回確認された場合は、該当ブロック収益根拠の収益が相応な検証ノード及び送信ブロックノードによって使用されることができる。検証ノードが検証ノード集合から脱退する場合は、検証ノードの賞罰に対して決済も行う。

処罰根拠をブロックに記入されるノードは報酬を獲得し、収益根拠をブロックに記入するノードは相応な累積割合の収益を得る。検証ノードが受信したブロックにタイムリーな検証署名を行うことに励ますために、検証ノードの収益は収益証憑の順序に従ってべき級数減衰を行う。検証ノードサボタージュ（オフラインまたは無視ブロック伝播）を防止するために、確認数が一定の高さに達するが、検証累計割合が最低限度に達しない場合は、未署名の検証ノードに処罰を行い、処罰根拠は怠惰根拠に記入される。

システムは一定数のブロックに収益を半減する。DAX トークンの総マイニング量は 13.9 億である。

4.3 不正行為の分析

4.3.1 ダブル支払攻撃

一つノードはダブル消費攻撃を実行したい場合は先に発信ノードを選択される必要があり、その後に同時で複数のブロックを作成する。しかし、ブロック伝播のプロセスに、このノードの複数の新規ブロックが同時に検出された場合は、それはダークノードとして告発され、すべての保証金を失う。

4.3.2 51%攻撃

抽選関数で使用される VRF 関数の偽ランダム性及びその関数入力分枝数量に 1 つブロックのランダム性があり、51 %のノードを集中しても、送信ブロックノードに選

ばれない場合は、攻撃を開始することが難しいである。51%のノードと連携で新規ブロックの認証署名を拒否する場合は、最終的に保証金が没収される。

4.3.3 リモート分岐攻撃

各ブロックの間には時効期間の制限があり、すなわち一定期間を超えるで作成のブロックは無効ブロックと見なされ、そしてシステムに伝播できない。これで長距離分岐を避けることはシステムに受け入れられる。長距離分岐は作成できないが、同時に最小選択値を持つブロックは選択される、従ってシステムに新たに入るクライアントは最初ブロックを知るだけでの前提でどの分岐が合法であるかを判断することができる。

4.3.4 孤立攻撃

一部のノードがシステムに長期的に分離される場合は、抽選規則によって、この部分のノードは単独の分岐を作成する。システムが確認数に一定量に達するが、累積署名に対応する権益の割合が p%に達しない検証ノードを処罰し、分離攻撃を実現したい場合は、少なくとも総検証権益 p%を占める検証ノードと連携しなければならない。同時に分離された分枝とメン分枝のブロックにそれぞれで検証し、それで分離伝播を実現することができる。さもなければ、一部検証ノードに分離攻撃による署名の欠如で罰せられた場合は、この分離攻撃はシステムに発見される。

5 エコロジーガバナンス

技術的ソリューション、エコロジー構造及びガバナンスモデルは 1 つブロックチェーンプロジェクトが成功するかどうかの 3 つ重要な次元である。1 つ合理的なエコロジーガバナンスモデルはチェーンにおけるガバナンスプロトコルとオフチェーンの連携コンセンサスの融合である。

チェーンにおけるガバナンスプロトコルの目的はエコロジーシステムのすべてのユーザーが彼らの関心を持つエコロジー事項に参加する権利を有し、投票によって決定を行う。しかし、現在でトークン量やトークン所有者に標準とする投票は、純粋な民主や投票が無関心でエコロジー全体の崩壊につながる可能性がある。同様に、投票プロセスに唯一の決定側の出現を避けるべきである。複数のトークンや創業チームまたはマイナーにもかかわらず、すでに支持されている利益相反が存在する可能性がある。したい、DAEX はトークンの時間価値、ガバナンス価値の順次とタイミングガバナンス席の 3 つ方面から自律性の柔軟性と公平性を向上させ、ガバナンス契約の方式でエコロジーコンセンサスを達成する。

オフチェーンの連携コンセンサスはオフチェーン世界が価値マッピングに基づくガバナンスモードである。このようなコンセンサスはネットワーク監視、リスク追跡、コード審査などの技術的手段を含むだけでなく、エコロジーシステムの融合、リスク

ファンドなどの共同メカニズムが含まれる。DAEX エコロジーでは、清算検証者は取引の合法性を検証することで一定価値を維持し、アプリケーションとの間の管理は重複を存在しない。あるアプリケーションは問題が存在する場合、オフラインの管理メカニズムは直ちに修復することができ、その他のエコロジー応用の正常な動作に影響しない。

ガバナンスモデルのもう一つ重要な側面はコンプライアンスである。コンプライアンスは規制の不確実性を回避し、主流の組織が合法的に当該分野に参加するための基礎的な技術的枠組みを満たすことができるべきである。DAEX エコロジーブループリントはデータと資産の構造的な層別化に基づいて、取引と清算の分離の規制スペースを作り出す。

ブロックチェーン自体の堅牢性はテストされるが、安全は全体的なものである。同時に一つ有効なメカニズムであり、エコロジービルダー、ユーザーと規制当局の注意を必要とする。 ただし、ユーザーにとってセキュリティのしきい値が高すぎることもありますが、多数の攻撃を繁殖させる方が簡単です。 したがって、清算エコロジーはガバナンス介入の頻度を減らすために、次のセキュリティの観点の最適化により、エコロジーシステムのリスク回復力を向上させる。

- **アルゴリズムの安全性**：しきい値シグネチャ、疑似ランダム生成アルゴリズム、VRF などを含め、さまざまな暗号アルゴリズムを最適化する。
- **プロトコルの安全性**:ASPOS はより安全的、効率的コンセンサスメカニズムであり、清算と決済プロトコルは一般的なクロスチェーン技術より安全的、効率的、安価的である。
- **安全性の実現**：スマート契約のマルチパーティー検証、形式化検証と包括的なテスト。
- **管理の安全性**：カスタマイズでブロックチェーンモデルに基づくリスク管理システムを開発し、オフチェーンデータの物理的分離またスライスデータストレージ、企業ウォレット権限のレベル別で管理。

6 リリース計画

2018.Q2　清算エコロジーの全体的デザインとコンセンサスメカニズム

2018.Q3　清算価値ファクターとトークン計画

2018.Q4　エコロジーの配置とノードガバナンス、ハードウェアウォレットソリューション

7 コアチーム

谷燕西：首席戦略官兼ファウンデーション会長。中国とアメリカの有名な金融会社、企業ソフトウェア会社及びインターネット

金融会社の豊富な専門と管理の経験を持っている。華泰連合証券情報技術ドープディレクターと数社金融サービス会社 COO の職務を担当したことがある。アメリカのオプション決済会社で勤務期間に、直接にアメリカのオプション取引市場の唯一決済システム ENCORE の開発と運営に参加した。アメリカのテキサス大学（オースティン）の MBA 学位、ノートルダム大学の修士学位、中国科学技術大学の修士学位及び山東大学の学士を取得した。

唐瑞琮：共同創設者兼チーフアーキテクト。金融科学技術の製品設計と応用研究に専念し、ブロックチェーン、人工知能などの分野で開発した製品がある。中国国内商業銀行の最初のコアシステムに応用されたブロックチェーンプロジェクトおよび業界の初ブロックチェーン技術に基づく企業の売掛金チェーンプラットフォームの業務を担当した。2 つブロックチェーンの特許を持っている。浙江大学ソフトウェアエンジニアリングの修士を取得した。

張華：共同創設者。複数デジタル資産取引プラットフォームの投資家であり、IDEL 国際デジタル経済連盟のメンバーである。世界的に有名な金融機関に務め、長年に携わって世界トップ 500 企業の業界分析と戦略コンサルティングの仕事を従事している。2014 年からブロックチェーンやデジタル資産の分野で創業し、支払いやウォレットなどの分野にブロックチェーンを利用することに取り込んでいる。ブロックチェーン業界のオピニオンリーダーであり、2016 年金融技術・介甫賞年次女性 CIO であり、Qtum や Vechain など数十ブロックチャインプロジェクトの初期投資家である。上海交通大学から卒業した。

周岩：ウォレットアーキテクチャ科学者。10 年以上のシニアインターネットプロジェクト管理と開発経験があり、オールスターズエンジニアを務め、各種データベースクラスターの構築に精通している。すべてのメインブロックチェーンとデジタル資産ウォレットの構造にも精通している。

沈冰流：ブランドマーケットパートナー。インターネット金融と企業サービス分野に務めた長年の経験がある。テンセント高級ビジネスマネージャーを担当し、テンセン

トの優秀従業員を獲得し、ウィーチャット支払いと金融技術及び020業界の戦略協力の業務を担当し、多くの顧客にAPP　Storeランキングトップ10に成功入るのを応援した。華東政法大学の経済法専門で卒業した。