L-021

DID/VC エコシステムにおける Trust Framework 遵守を強制するアーキテクチャの提案

Proposal for an Architecture to Enforce Trust Framework Compliance in the DID/VC Ecosystem

齊藤 健斗† 大月 魁†
Kento Saito Kai Otsuki

1. はじめに

近年、デジタルアイデンティティの管理と流通において、自己主権型アイデンティティ（Self-Sovereign Identity: SSI）の概念が注目されており、それを実現する基盤技術として、分散型識別子（Decentralized Identifier: DID）および検証可能な資格情報（Verifiable Credential: VC）の国際的な標準化が進展している [1] [2]。DID/VC の導入により、ユーザーは自身の識別情報や属性情報を中央集権的な管理主体に依存せず、安全かつプライバシーに配慮した形で提示・共有することが可能となる。

デジタルアイデンティティ及び VC を活用したユースケースは急速に拡大しており、公的証明（例：運転免許証、在留カード）にとどまらず、航空券や会員証、オンラインイベントチケット、企業内認証、さらには趣味嗜好やスキル・実績を表すバッジ型クレデンシャルなど、従来の書面による証明の延長線上にある多様な適用が期待されている [3]。これらのユースケースにおいては、暗号学的な正当性の担保に加え、クレデンシャルが「意図されたとおりに正しく発行・管理されているか」という運用面の信頼性が重要となる。

しかしながら、現行の技術仕様においては、VC の Issuer（発行者）や Verifier（検証者）等の参加者がエコシステムで定められたルールを順守させる技術的な仕組みは存在しない。W3C Verifiable Credentials Data Model 仕様では、VC に `termsOfUse` プロパティを付加することによりポリシーの記述は可能であるが、それが実際に遵守されているかを担保する手段は標準化されていない [4]。そのため、不適切なクレデンシャルの発行や、ホルダーの同意を得ずに提示された情報を検証者が不適切に利用するといったリスクが残存している。

このような課題を補完するため、近年では eIDAS [5] や Pan-Canadian Trust Framework (PCTF) [6]、Trusted Digital Identity Framework (TDIF) [7] など、特定の条件下で信頼できる発行者（Trusted Issuer）や検証者（Trusted Verifier）を中央的に認定し、信頼性を保証するガバナンス・フレームワークの整備が進められている。これらの枠組みは、厳格な審査と認証プロセスによって発行主体の信頼性を担保するものであり、国家間や業界内の相互運用性を実現する上では有効な手段である。

一方で、このような中央認定型の枠組みには、次のような限界も存在する。第一に、新規参入者にとって、認定を受けるためのプロセスが煩雑かつコスト高となり、結果としてエコシステムへの参加障壁が高まるという問題がある。第二に、エコシステム運営主体にとっては、すべての発行者を対象に認定・監視・更新を行うことが人的・制度的に大きな負担となり、ガバナンス運用のスケーラビリティが損なわれる。さらに、ロングテール的な多様なユースケースに対しては、中央的なルール設計が実態と乖離しやすく、柔軟な対応が困難となる。

このように、VC のエコシステムは、「分散性」と「信頼性」の両立に構造的な課題を抱えていると考えられる。本研究では、その解決に向けたアプローチとして、クリプトエコノミクスの概念を応用し、経済的インセンティブによりポリシー遵守を促進する仕組みの構築を試みる。中でも、Ethereum 等の分散型ネットワークにて活用される Proof of Stake（PoS）[8] にて用いられる概念である、ステーキングとスラッシングに着目する。ステーキングとスラッシングの設計では、参加者が一定の資産をステーキングし、誠実な行動に対して報酬を得る一方で、ルール違反にはステークの一部がスラッシュ（没収）されるという、経済的ペナルティを通じた信頼維持の仕組みを提供している [9]。

本稿では、この PoS モデルが持つステーキングとスラッシング の構造を応用し、VC エコシステムにおいて分散性を保ちつつ、信頼を自律的かつ経済的に担保する新たなアーキテクチャの設計と、その実現可能性について検討する。

2. 関連研究

信頼の担保は技術観点及びガバナンス観点の両面にて実現される。本章では、要素技術とフレームワーク・ガイドラインの動向と課題を紹介する。

2.1 デジタルアイデンティティと DID/VC 技術の位置づけ

近年、行政手続き、金融サービス、教育、医療など多様な領域においてオンライン化が急速に進展しており、デジタル上で個人を識別し、適切に属性情報を証明するための「デジタルアイデンティティ」の重要性が高まっている [10]。デジタルアイデンティティは、本人確認やサービス提供における中核的な役割を担っており、安全性と利便性を両立する基盤技術として注目されている。

しかしながら、現状の多くのデジタル ID 管理は、サービスごとに個別のアカウントや識別子を必要とするため、ID の乱立や情報の分断が生じている。また、ID の発行や管理を特定の事業者が一方的に担う中央集権的な構造では、ユーザーが自身の情報に対して十分な制御権を持てないという課題も指摘されている [2]。加えて、サービス横断的な相互運用性やプライバシー保護の観点でも、従来の ID モデルには限界が存在している。

こうした課題に対応する新たなアプローチとして、自己主権型アイデンティティ（Self-Sovereign Identity: SSI）の概念が登場している [11]。SSI は、個人が自身の識別情報および関連する資格情報を自ら管理・提示すること

† 株式会社 NTT ドコモ および 株式会社 NTT デジタル NTT docomo Inc. & NTT Digital Inc.

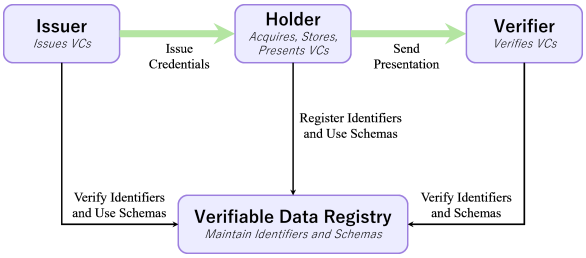

図 1. Verifiable Credential エコシステムの基本構造

を可能にし、情報の真正性とユーザーのコントロール権の両立を目指すモデルである。SSI は「中央を信用する ID 管理」から「ユーザーが主権を持つ ID 管理」への転換を促すものであり、分散型技術の進展とともに国際的な注目を集めている [2]。

この SSI の実現を支える技術基盤として、W3C を中心に標準化が進められているのが、分散型識別子（Decentralized Identifier: DID）および検証可能な資格情報（Verifiable Credential: VC）である。DID は、従来の中央リポジトリに依存せずに識別子を発行・管理できる仕組みを提供し、VC はその識別子に紐づく属性情報の検証可能な提示と確認を可能にする。これらは、分散性と相互運用性を備えた次世代のデジタルアイデンティティ基盤として、各国・各業界における導入が進みつつある [2]。

DID（Decentralized Identifier） DID は、特定の中央管理者に依存せず、個人または組織が自身で生成・管理可能な識別子である。DID に対応する DID ドキュメントには、公開鍵、認証手段、サービスエンドポイント等の情報が格納される。DID の多くは分散型台帳（Distributed Ledger Technology: DLT）上に記録されることで可証性と改ざん耐性を実現するが、すべての DID が DLT を必要とするわけではない。たとえば `did:key` のように、ローカルで自己生成・運用可能な軽量な DID メソッドも存在する [12]。

VC（Verifiable Credential） VC におけるの関連主体間の基本的な相互関係を図 1 に示す。本図は、エコシステム内での各主体の役割と情報の流れを視覚的に整理したものであり、以降の議論の前提として参照されたい。VC は、個人の学歴、資格、属性、権限などの情報をデジタルに証明する枠組みである。発行者（Issuer）が暗号署名によってクレデンシャルを発行し、それを保持者（Holder）が自身で保管・提示し、検証者（Verifier）が真正性を検証するという三者構造で運用される。さらに、VC の基盤には、スキーマや DID ドキュメント、認定された発行者の情報などを保持する Verifiable Data Registry（VDR）が存在し、エコシステムが運用される。

本モデルにおいては、**Issuer** が VC を発行し、**Holder** に対して資格情報を提供する。Holder は受け取った VC を安全に保持し、必要に応じて **Verifier** に提示することで自身の属性や資格を証明する。Verifier は提示された VC の真正性と有効性を検証するにあたり、Issuer やスキーマ情報を含む DID Document の情報を、**VDR** を通じて参照する。

VDR は、DID の解決やスキーマ定義の保管、VC に関わる各主体の識別子の登録など、エコシステムにおける信頼の根拠となる情報を提供する基盤である。各ロールは VDR を通じてスキーマや識別子を登録・参照しながら相互に連携し、VC の発行・提示・検証という一連のプロセスを安全かつ相互運用可能な形で成立させている [13]。

また、VC には選択的開示（Selective Disclosure）[14] やゼロ知識証明（Zero-Knowledge Proof: ZKP）[15] といったプライバシー保護のための技術が導入可能であり、ユーザーは自身の情報を必要最小限で提示できるなど、高い柔軟性と再利用性を有する。

なお、W3C による Verifiable Credential Data Model の仕様では、発行時に `termsOfUse` プロパティを付加することで、当該 VC の利用に関するポリシーや条件を記述することができると定義されている [4]。しかしながら、これらのポリシーが実際に遵守されているかを技術的に強制・検証する手段は標準仕様の中には含まれておらず、VC の利用における運用上の信頼性は各エコシステムの裁量に委ねられている。

以上のように、DID および VC は、自己主権型アイデンティティ（Self-Sovereign Identity: SSI）の実現に向けた中心的な技術であり、分散型エコシステムの信頼構築において重要な役割を果たしている。しかしながら、これらの技術が提供するのは、あくまで VC の発行・提示・検証の技術的正当性に限られており、各参加者がその運用ポリシーに準拠しているかどうかを保証する仕組みは含まれていない。次節では、この点に着目し、エコシステム全体における信頼性維持の課題と対応策について検討を行う。

2.2 フレームワーク・ガイドラインの動向と課題

VC エコシステムの基本構造を用いたデジタルアイデンティティ技術は、さまざまなユースケースへの実装を想定して、各国政府や国際的な標準化団体により、制度的・技術的なフレームワークの整備が進められている。これらは、個人認証、資格証明、デジタルウォレットなどの領域で、実運用を見据えた信頼の担保や相互運用性の確保を目的とした取り組みである。

例えば、EU が推進する eIDAS 2.0 は、加盟国間で相互に認証可能な ID プロバイダーや Issuer の登録枠組みを提供し、デジタルアイデンティティウォレット（EUDI Wallet）の標準化と利用促進を目指す包括的な制度である [5]。また、Pan-Canadian Trust Framework (PCTF) [6]、IDunion Network [16]、Trusted Digital Identity Framework (TDIF) [7]、およびモバイル運転免許（mobile Driving License, mDL）[17] なども、分散型エコシステムの構築を志向しつつ、信頼性確保の手段として「Trusted Issuer」のような中央認定構造を一部に取り入れている。

このような枠組みは、業界や国・地域ごとの法制度との整合性を確保し、制度的信頼を提供する上では有効である。一方で、こうしたガバナンスモデルの多くは、エコシステム参加者が自律的にポリシー遵守を担保するための仕組みを欠いており、ポリシーの遵守を中央的な認定と監督に依存しているという構造的な限界がある。その結果として、以下のような課題が発生し得る：

- 新規事業者が Issuer や Verifier として参加するには、認定取得に関する手続きや審査負荷が大きく、エコシステム参入の障壁となる。

- 認定済みの Issuer が増加し、大量のクレデンシャルが発行されるようになると、中央的な監査や運用のための人的・制度的コストが増大し、持続可能性に課題が生じる。

- 認定制度が包括的である一方、短期的・多様なユースケースへの柔軟な適用が難しく、中央的なルール設計が実態と乖離しやすい。たとえば、イベントチケットやオンライン講座などで発行される一時的な証明に対しては、フレームワークにより設定された発行条件が実態よりも厳しすぎるケースが考えられる。

このように、現行のトラストフレームワークは、信頼性を確保する設計にはなっているものの、スケーラブルかつ自律分散的なエコシステム運営という観点からは改善の余地がある。

2.3 クリプトエコノミクスにおけるステーキングとスラッシングの設計思想

ブロックチェーン技術の発展により、中央管理者の介在なしに持続的なネットワーク運用を実現するための仕組みとして、経済的インセンティブを活用した合意形成メカニズムが広く採用されてきた。その中核にあるのが、暗号技術と経済的仕組みを組み合わせた「クリプトエコノミクス（Cryptoeconomics）」という設計思想である [18]。

クリプトエコノミクスでは、ノードや参加者が誠実な行動を取ることに対して正の報酬が与えられ、悪意ある行動に対しては経済的損失が発生するような構造が設計される。Proof of Stake（PoS）は、その代表的な合意手法の一つであり、従来の Proof of Work とは異なり、ネットワークへの参加資格と責任を「ステーク（Stake）」という資産のロックによって表現する。

PoS においては、バリデータ（Validator）がネットワークに参加する際に暗号資産をステークとして預け入れ、ブロックの提案や取引の検証に従事する。誠実な行動を取れば報酬を得られる一方で、不正行為やルール違反（たとえば二重提案や不正な署名）が発覚した場合には、預け入れたステークが部分的または全額「スラッシュ（Slash）」として没収される。これにより、「誠実に振る舞うことに経済的な価値があり、不正を行うと損をする」というインセンティブ構造が成立する [9]。

このような設計において、PoS は信頼形成そのものを目的としているわけではなく、むしろ参加者が誠実な行動を経済合理的に選好するように誘導する「抑止構造」の一要素であると解釈できる。言い換えれば、信頼に値する行動を強制せずとも、他の選択肢が損失を伴うために結果的に誠実な行動が促されるという、制度的ガバナンスに代わる手法である。

Ethereum では、こうしたステーキングとスラッシングの構造がプロトコルレベルで実装されており、PoS の導入により、ファイナリティのある分散合意形成が可能となった [19]。また、実運用においては、32 ETH をステークしたバリデータが不正行為を行った場合、他のノードによって違反が報告され、自動的にスラッシュ処理が行われ、報告者への報酬分配までが設計されている [8]。

本研究では、この PoS におけるステーキングとスラッシングの設計思想に着目し、VC エコシステムにおける信頼担保の枠組みとしての応用可能性を検討する。特に、Issuer や Verifier といった参加者が、ポリシー遵守を自己主張的に行うだけでなく、経済的担保を通じてその行動に責任を持つような構造の設計が、本質的なスケーラビリティと信頼性の両立に寄与すると考えられる。

2.4 本研究が着目する課題領域

本章では、DID/VC の基盤技術と、制度的なトラストフレームワークの両面から、分散型デジタルアイデンティティの実現に向けた既存の取り組みを概観した。

DID/VC は、識別子や資格情報の真正性と相互運用性を担保する技術として注目されているが、発行や利用の過程においてポリシーが遵守されているかを技術的に検証・強制する仕組みは備えていない。

一方、eIDAS や PCTF などのフレームワークは、信頼性を担保する制度として有効であるが、中央認定構造に依存することにより、参入障壁や運用コストといったスケーラビリティ上の課題がある。

さらに、VC のユースケースが多様化される中で、こうした中央集権的枠組みのみでは柔軟な対応が困難である。

このような背景のもと、本研究では、PoS におけるステーキングとスラッシングの設計思想に着目し、エコシステム参加者の自律的なポリシー遵守を促す、新たな信頼形成モデルの可能性を検討する。

3. 提案手法

本研究では、VC エコシステムにおけるルール遵守と信頼性を、中央的な認定制度のみに依存しない新たなエコシステム運用の枠組みを提案する。従来のトラストフレームワークに見られるような中央集権的な監査や認定は、信頼性を担保する手段として有効である一方で、参入障壁や運用負荷といったスケーラビリティの課題を伴っていた。

本提案では、ブロックチェーン分野において分散的な行動制御の仕組みとして広く用いられている「ステーキングとスラッシング」の設計思想に着目し、エコシステム参加者が経済的担保を伴って自律的にポリシーを遵守するよう動機づける構造を設計する。具体的には、参加者を以下の 3 つのロールに分類し、それぞれの動機と役割に応じた経済的インセンティブ設計を行う。

本節では、まず各ロールの定義とその動機を示した上で、相互作用によって形成される行動モデルを説明する。続いて、ステークのライフサイクルについて概説し、提案手法の全体像を明らかにする。

3.1 ロールの定義とエコシステムへの参画動機

本提案では、参加者が自律的にルールを遵守しながら行動できるインセンティブ構造を構築するため、エコシステム内の役割を以下の 3 つのロールに分類する。それぞれのロールは、異なる立場から信頼の維持に貢献しつつ、経済的・社会的な見返りを得ることを目的として行動する。

- **Trust Declarant**：信頼宣言者。自身の誠実性を示し、他の参加者からの信頼を獲得・維持したいという動機を持つロールである。行動の対価として、継続的に VC を発行・検証し続けられることが期待される。このロールは、具体的には **Issuer** や **Verifier**

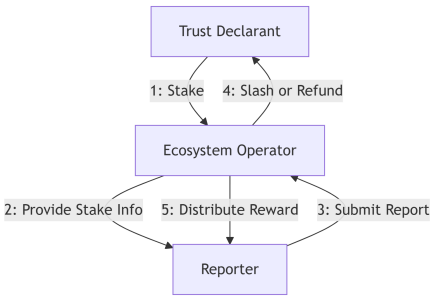

図 2. 各ロールの関係図

が想定される。彼らは、**Ecosystem Operator** へと一定額のステークを預託し、その行動に対して責任を持つ。

- **Reporter**：報告者。不正やポリシー違反を発見し、それを報告することで報酬を得たいという動機を持つロールである。正当な報告が受け入れられることで、自身が被害を受けるリスクを下げると同時に、エコシステム全体の健全性維持にも貢献する。Reporter は、エコシステム内の参加者である必要はなく、外部の観察者や第三者も含まれ得る。

- **Ecosystem Operator**：このロールは、報告内容の審査、違反認定、スラッシング実行、報酬分配といった機能を担う。報告が有効と判断された場合、Trust Declarant のステークの一部がスラッシュされ、報告者に報酬として分配される。残余はトラスト保全のためのプールに蓄積される。さらに、違反の履歴は公開ログとして記録・管理され、今後の信頼判断の参照情報として活用可能とすることも拡張の余地として考えられる。

3.2 各ロールの行動モデル

図 2 に、本提案における 3 つの主要ロールの相互作用を通じた信頼形成の関係図を示す。本モデルは、Trust Declarant、Reporter、Ecosystem Operator の 3 者がそれぞれの役割と動機に基づいて行動し、経済的インセンティブを介してエコシステムの信頼性を維持する構造である。

以下に、各ロールの行動とその前提となる設計思想を示す。

- **Trust Declarant**：このロールに該当する主体（例：Issuer や Verifier）は、VC の発行や検証などの信頼形成行動を行う前に、あらかじめ一定額のステーク（担保）を預託する。預託のタイミングはエコシステムの設計に応じて柔軟に設計可能であり、参加時の入場料的ステークや、各トランザクションに紐づけた都度ステークといった方式が考えられる。ステークはロック期間中に拘束され、違反報告がなければ返金されるが、有効な報告が認定された場合にはスラッシング（没収）対象となる。

- **Reporter**:エコシステム内外の誰もがこのロールを担うことができる。Trust Declarant の行動においてポリシー違反を発見した際、証拠とともに Ecosystem Operator へ報告を提出する。報告が受理・認定された場合、報酬が支払われるため、経済的なインセンティブがレポートの動機付けとなる。この設計により、中央集権的な監視機構を持たずとも、エコシステム参加者による自律的な監視が機能する。

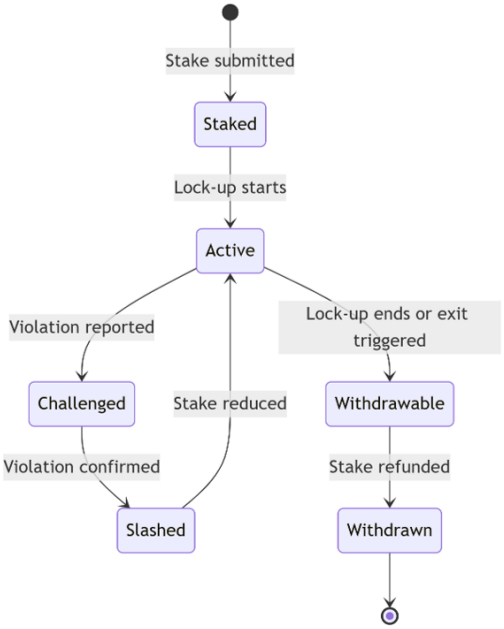

図 3. ステークのライフサイクルを表す状態遷移図

- **Ecosystem Operator**：このロールは、報告内容の審査、違反認定、スラッシング実行、報酬分配といった機能を担う。報告が有効と判断された場合、Trust Declarant のステークの一部がスラッシュされ、報告者に報酬として分配される。残余はトラスト保全のためのプールに蓄積される。さらに、違反の履歴は公開ログとして記録・管理され、今後の信頼判断の参照情報として活用可能とすることも拡張の余地として考えられる。

3.3 ステークのライフサイクル

本提案における信頼担保の中核は、Trust Declarant によって預託されるステーク（担保資産）である。このステークは、ルール遵守の経済的保証として機能し、不正があった場合にはスラッシュ（没収）される。一方で、誠実な行動が継続された場合には、ロック期間終了後に返金される。

図 3 に示すとおり、ステークは以下のような状態遷移に従って管理される。

- **Staked**：Trust Declarant がステークを預託した直後の状態。以降のロック期間が開始される。

- **Active**：ステークがロックされている期間中の状態。この期間中は、ポリシー違反の報告を受け付ける。違反が報告されなければ、ロック期間終了後に返金可能な状態へと遷移する。

- **Challenged**：有効な違反報告が提出された状態。報告は Ecosystem Operator によって評価される。

- **Slashed**：違反が認定され、ステークの一部または

全額が没収された状態。スラッシュ後、残額はロック状態に戻り、再び返金対象となる。

- **Withdrawable**：ロック期間が終了し、ステークの残余が返却可能となった状態。またはステークの残余が 0 になった等のトリガーにより明示的にロックされている期間が終了した状態。
- **Withdrawn**：返金処理が完了し、ステークの残余が Trust Declarant に返却された最終状態。

このように、ステークのライフサイクルは、誠実な行動に対しては資産の返却を、不正行為に対しては資産の没収と報告者への報酬という形で明確な経済的結果をもたらす。これにより、エコシステム参加者に対して自律的な行動制御が働く構造が実現される。

4. 提案手法の導入による期待効果

本節では、本研究で提案するステーキングおよびスラッシングに基づく信頼維持メカニズムを VC エコシステムに導入した場合に期待される効果について論じる。本提案は設計方針として抽象度を保っており、ステークの預託方法や違反情報の公開手法、ガバナンス機構の構成など、さまざまな実装パターンに柔軟に適用可能である。

たとえば、Trust Declarant がステークを預けるタイミングは、初期参加時に一括で預託する方式（入場料モデル）や、発行・検証の各トランザクションに応じて逐次預ける方式（トランザクション課金モデル）などが考えられる。また、ステークの状態や違反履歴をパブリックブロックチェーン上で公開することで、高い透明性と改ざん耐性を両立できる。スラッシュの比率や報酬分配の設計も、固定パラメータとして定義するほか、分散型自律組織（Decentralized Autonomous Organization: DAO）[20] の投票等を通じて柔軟に運用することも可能である。

新規参入者に対する障壁の緩和　従来のトラストフレームワークでは、Trusted Issuer として認定されるまでに高い審査基準や手続きが求められ、これが新規事業者の参入障壁となっていた。提案手法では、明示的なステーキングによって初期から「経済的な責任」を果たすことができるため、認定制度に代わる自己担保型の信頼獲得メカニズムとして機能する可能性がある。これにより、ロングテールの多様なユースケースにおいても、参加のハードルを抑えつつ一定の信頼性を担保する仕組みが実現できる。

ガバナンス運用コストの低減　中央認定型のガバナンスにおいては、参加者の審査・更新・監視に係るコストや人的リソースが制度の拡張性を阻害する要因となっていた。提案手法では、ステーキングおよびスラッシングを通じて参加者自身にインセンティブを与えることで、中央による審査や強制的な監査を不要とし、自律的かつ分散的な信頼形成が可能となる。これにより、運用負荷の軽減とともに、より持続可能なガバナンス設計が期待できる。

中央認定型との補完的な運用　本提案は、既存の中央認定型トラストフレームワークと対立するものではなく、むしろ補完的に運用可能な構造を想定している。たとえば、法的効力や高い真正性が求められる公的な VC（例：運転免許証、在留カードなど）については、従来通り、中央認定組織によって厳格に認定された Issuer や Verifier による発行・検証が適している。一方、イベント参加証やオンライン講座の修了証といった、一定の信頼は必要であるものの法的な厳格性までは求められない VC に対しては、本提案によるステーキング・スラッシングを用いた経済的インセンティブモデルが有効に機能する可能性がある。

このように、VC の性質や用途に応じて中央認定型と提案手法を使い分けることで、エコシステム全体としては、厳密性とスケーラビリティの両立が可能となる。これは、ロングテール的な多様なユースケースに柔軟に対応しつつ、制度的信頼を損なわないガバナンス設計の実現にも寄与すると期待される。

信頼確保の分散性と持続性の向上　従来のフレームワークでは、信頼性の確保は中央組織による認定や監査に強く依存しており、制度疲労やボトルネックの原因となっていた。提案手法では、各参加者が自らステークを担保として信頼を「宣言」する構造であるため、中央的な介入なしに信頼が維持される。さらに、違反検出も任意の参加者による通報に委ねることで、検出能力の分散化とエコシステムの自律性が高まる。

5. 結論と今後の検討課題

本研究では、VC エコシステムにおける信頼担保のあり方に着目し、従来の中央認定型モデルと補完的な運用が可能な分散的な仕組みとして、ステーキングおよびスラッシングに基づくインセンティブ設計を提案した。我々は、Ethereum などに代表される PoS に見られるステーキングとスラッシングの構造を参考にしつつ、エコシステム参加者が経済的責任を伴って自律的に行動することで、信頼形成とスケーラビリティの両立を図る新たなアーキテクチャを示した。

こうした提案を現実のエコシステムに実装していく上では、以下のような論点をさらに検討する必要がある。

- **誤検知リスクと通報の信頼性向上**：Reporter による報告が制度の中核を担う以上、虚偽報告や過剰な通報のリスクに備える必要がある。我々は、報告者自身にも一定のステークを課す仕組みを導入することで、報告の信頼性を担保する設計が有効と考える。また、報告履歴に基づく Reporter 評価制度も将来的な補完策として検討の余地がある。
- **運用の透明性と信頼性の確保**：Ecosystem Operator が実施するスラッシュや返金判断の基準が不透明なままでは、特定の参加者に対して恣意的な運用がなされているとの疑念を招き、エコシステム全体の信頼性を損なうおそれがある。参加者が制度に対して「公平に扱われている」という安心感を持つためには、スラッシュ執行や判定の記録が誰でも検証可能であることが重要である。本提案では、これらのログや意思決定の根拠をブロックチェーンや IPFS などの分散ストレージ上に公開することで、改ざん耐性と透明性の両立を図り、外部からの監査やコミュニティ主導のガバナンスも実現可能とする。

- **仕組み設計における公正性の担保**：スラッシングは経済的ペナルティを伴うため、手続きの正当性と反論機会の確保が不可欠である。例えば、違反が報告された時点（Challenged 状態）で Trust Declarant が反論証拠を提出できる設計や、スラッシュ率などの制裁パラメータを DAO 型ガバナンスで動的に調整可能とする構成が考えられる。

今後は、これらの論点に対してプロトタイピングや実証実験を通じた実装検証を行い、制度的・技術的両面から持続可能な分散型信頼メカニズムの確立を目指していく。

6. 参考文献

[1] Shigeya Suzuki. Decentralized identifiers (did) と verifiable credentials (vc) の現況. **電子情報通信学会誌**, 18(1):42–55, 2024.

[2] Carlo Mazzocca. A survey on decentralized identifiers and verifiable credentials. *arXiv preprint arXiv:2402.02455*, 2024.

[3] Brian Sletten Daniel Burnett Manu Sporny Ken Ebert Nate Otto, Sunny Lee. Verifiable credentials use cases. https://www.w3.org/TR/vc-use-cases/, 2021. W3C Working Group Note, URL accessed on 2025-06-05.

[4] Verifiable Credentials Working Group. Verifiable credentials data model v2.0. W3c recommendation, World Wide Web Consortium (W3C), 2025.

[5] Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market. https://eur-lex.europa.eu/eli/reg/2014/910/oj, 2014. Accessed: 2025-06-08.

[6] Pan-canadian trust framework (pctf) model final recommendation v1.0. https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf, 2020. Accessed: 2025-06-08.

[7] Trusted digital identity framework (tdif). https://www.digitalidsystem.gov.au/sites/default/files/2023-07/tdif_02_overview_-_release_4.8_-_finance_1.pdf, 2023. Accessed: 2025-06-08.

[8] Ethereum Foundation. Slashing in proof-of-stake, 2024. Accessed: 2025-06-08.

[9] Sheng-Nan Li, Jiahua Xu, Paolo Tasca, and Claudio J Tessone. Proof-of-stake cryptoeconomics design: A general framework of modeling and evaluation. *Available at SSRN 5072963*, 2024.

[10] Strategy&. Digital identity: Opportunities and challenges. 2021. Accessed: 2025-06-08.

[11] Md Sadek Ferdous, Farida Chowdhury, and Madini O Alassafi. In search of self-sovereign identity leveraging blockchain technology. *IEEE access*, 7:103059–103079, 2019.

[12] Walid Fdhila, Nicholas Stifter, Kristian Kostal, Cihan Saglam, and Markus Sabadello. Methods for decentralized identities: Evaluation and insights. In *Business Process Management: Blockchain and Robotic Process Automation Forum: BPM 2021 Blockchain and RPA Forum, Rome, Italy, September 6–10, 2021, Proceedings 19*, pages 119–135. Springer, 2021.

[13] Morteza Alizadeh, Karl Andersson, and Olov Schelén. Performance analysis of verifiable data registry solutions for decentralized identifiers. In *2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, pages 1–8. IEEE, 2022.

[14] Daniel Fett, Kristina Yasuda, and Brian Campbell. Selective disclosure for jwts (sd-jwt). *Internet Engineering Task Force, Internet Draft draft-ietf-oauth-selective-disclosure-jwt-05*, 2023.

[15] Nikos Fotiou, Iakovos Pittaras, Spiros Chadoulos, Vasilios A Siris, George C Polyzos, Nikolaos Ipiotis, and Stratos Keranidis. Authentication, authorization, and selective disclosure for iot data sharing using verifiable credentials and zero-knowledge proofs. In *International Workshop on Emerging Technologies for Authorization and Authentication*, pages 88–101. Springer, 2022.

[16] Berlin Partner for Business and Technology. Idunion: All identity power to the user. Accessed: 2025-06-08.

[17] International Organization for Standardization. Iso/iec 18013-5:2021 personal identification – iso-compliant driving licence – part 5: Mobile driving licence (mdl) application. Technical report, ISO, 2021.

[18] Jaya Klara Brekke. Hacker-engineers and their economies: The political economy of decentralised networks and ‘cryptoeconomics’. *New Political Economy*, 26(4):646–659, 2021.

[19] Danny Ryan, Vitalik Buterin, and Justin Drake. Eip-2982: Serenity phase 0. https://eips.ethereum.org/EIPS/eip-2982, 2020. Defines the slashing and staking mechanism in Ethereum 2.0.

[20] Shuai Wang, Wenwen Ding, Juanjuan Li, Yong Yuan, Liwei Ouyang, and Fei-Yue Wang. Decentralized autonomous organizations: Concept, model, and applications. *IEEE Transactions on Computational Social Systems*, 6(5):870–878, 2019.