DAO における内部告発の提案

情報・通信工学科 荒木研究室所属 182C1117 津田匠貴

1 はじめに

DAO(Decentralized Autonomous Organization:自律分散型組織) は共通目的を持った匿名個人らが中央集権的な管理主体を持たずに経済活動を行う組織であり, 独自トークンの発行や分散台帳としての記録機能をもつブロックチェーン技術の使用を前提に成り立っている. このような組織が運営する分散的サービスは Web3.0 と呼ばれる. これに対し, 特定の企業が中央集権的に運営する Twitter などの従来のサービスは Web2.0 と呼ばれる. Web3.0 上の組織である DAO には検閲耐性があり誰でも匿名で参加できるといったメリットがある一方, 自律分散型的に機能するまでは株式会社などの中央集権的組織が主体となって運営しており, 彼らによる資金の持ち逃げといった問題が数多く発生している. このような不正を防止し, コミュニティによる分散的統治を補助するために, 本研究では Ethereum ブロックチェーンにおいて秘密分散法を用いたメンバーシップの導入と内部告発機能を提案する. これは不正を行う兆候があるユーザーを検知した場合に内部告発を行い, メンバーの投票による審議を行うことで, 不正を防止するスキームを目指している.

2 Ethereum

Ethereum は暗号資産の移転・管理を誰でもプログラム可能にするスマートコントラクトを実装している. すでに多くのアプリケーションがこの上に構築されており, これらはいずれも同じプロトコル上で動くため, 相互に連携させることも容易である. このような汎用性と相互運用性の観点から他のブロックチェーンと比べても巨大なエコシステムを持っている. そのため新しい DAO を Ethereum 上に組織するプロジェクトが多い. 本研究でも, このような背景から Ethereum 上の DAO を対象とする.

3 秘密分散法

秘密分散法とはある秘密を share と呼ばれる欠片に分割し複数のメンバーで管理する方式である. 本研究では事前に定めた閾値以上の share が集まった場合にのみ復元できる閾値型秘密分散法を用いたメンバーシップを提案する. この手法では, ある多項式上の点を share とし, それを各メンバーに配布するディーラーの存在を仮定している. 閾値以上の share が集まった場合に多項式を復元することができ, 秘密を復号することができる.

4 DAO における内部告発の矛盾点とその解決方法

DAO において内部告発を実現する場合, 不正の疑いがあるメンバーを特定する行為は, 匿名環境下での活動と矛盾する. また, 内部告発の対象となる資金の持ち逃げをされた場合, 資金を取り戻すことはほぼ不可能であるため, インシデントが起きる前に不正を防ぐ必要がある. そのような不正を Web3.0 上の取引から事前に察知するのは困難だが, Web2.0 上のチャット内容などから推測できる. そこで本研究では, 予めこれらの Web2.0 上のアカウントと Web3.0 上のアカウントを紐付けるメンバーシップを考案した. これにより, 告発によって Web2.0 上のアカウントが公開され, メンバーによる判決結果から有害と認められた場合にのみ, 被告発者の Web3.0 上のアカウントを特定し罰則を与えることができる. このスキームでは, 不正を行おうとすればリスクを負うため, そのような行いを起こそうとするメンバーに対する牽制や, 上述の矛盾を緩和することができる.

5 閾値型秘密分散法を用いたメンバーシップ

図 1 は上述のスキームを Ethereum 上で実現するために考案したアカウント管理モデルである.

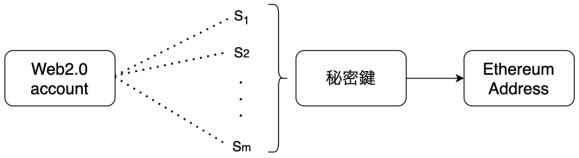

図 1: アカウント管理モデル

全てのメンバーは以下の流れに従いアカウントを登録する.

1. アドレスを作成する際に使った秘密鍵を閾値型秘密分散法に基づいて m 個の share に分割する
2. 1 つの Web2.0 account につき, m 個の share を紐付けたペアを作る
3. それぞれのペアを m 人のメンバーに配る

閾値型秘密分散法により n 個以上のペアが集まれば, 被告発者自身の秘密鍵が復元され, アドレス上の資産を失うなどのリスクを負うことになる. このようなリスクを回避する唯一の方法は, 自身が内部告発の対象にならないことであり Web2.0 上で誠実な振る舞いを続け, DAO に危害を与えるような言動を慎むことである. また, 内部告発とメンバーによる審議および制裁のコントロールはスマートコントラクトを用いて行う.

6 まとめ・今後の展望

本研究では, DAO のコアメンバーによる資金の持ち逃げといった不正を防止する内部告発の準備として閾値型秘密分散法を用いたアカウント管理モデルを提案した. これにより各メンバーは資産の損失リスクを負った状態で活動するため, 言動に責任を持たせることができる. しかし, 利用を想定している一般的な閾値型秘密分散法では, ディーラーの存在を仮定しているため, DAO のメリットである自立分散性を損なう形になっている. そこでまずは, DKG を組み込むことで分散環境に適したスキームを再設計する. また, ペアの増減や, 結託攻撃に対応するために, 今後はプロアクティブ秘密分散法や属性ベース暗号による改良も試みる.