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 序論

1.1 本研究背景と目的

AO(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.

1.1.1 論文の構成

2 予備知識

2.1 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.

2.2 DAO

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.

2.3 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.

3 内部告提案

3.1 内部告発の提案