DAO の機能改善提案 (abstract)

九州工業大学 情報工学部 荒木研究室 津田 匠貴

2021 年 11 月 29 日

1　はじめに

DAO(Decentralized Autonomous Organization:自立分散型組織) は経済的な共通目的を持った匿名の個人らが中央集権的な管理主体を持たず、特定の国や法定通貨に依存せずに活動を行う組織である。このような組織形態を可能にしているのがブロックチェーン技術によって可能になった独自トークンの発行や分散台帳としての記録機能である。

自立分散的に機能するまでは株式会社や NPO などの中央集権的組織が主体となって運営する。彼らによる不正を防止し、その活動を早期にコミュニティへ移管することが求められるため、本研究では現在の一般的な DAO をいかにして理想形に改善できるのか考える。具体的には、メンバーシップの導入とゼロ知識証明をを用いた投票、内部告発機能を提案する。

2　メンバーシップの導入

DAO のメンバーとその他の線引きをするために以下のメンバーシップを導入する。

図 1: アカウント管理モデル

内部告発において、コミュニティ全体で判決を決定し被告へ制裁を行うために以下のような設計となっている。

- 1 つの Secret key を m 個の secret share に分割
- 1 つの Web2 account(Twitter や Telegram のアカウント) につき、m 個の secret share を紐付ける
- それぞれの Web2 account と secret share のペアは m 人のメンバーに配られる
- n 個の secret share が集まればシャミアの秘密分散法により、被告発者の秘密鍵が再現できる
- (n,m) の値は自由に変更できる (n ≦ m ≦総メンバー数)
- Ethereum Address から Web2 account を特定することはできない

3　DAO における投票

プログラムの改善提案や助成金の決定など、DAO の方向性を自分たちで決める民主的な手段として投票は DAO に欠かせない機能であり、多くの DAO ではこの機能を提供している。投票にはガバナンストークン

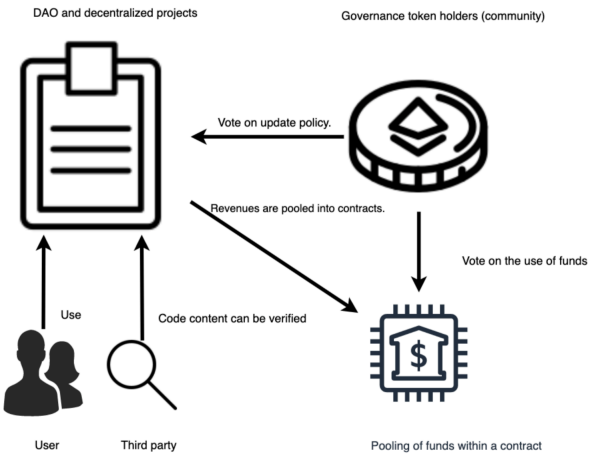

図 2: DAO における投票の仕組み

を使う例がほとんどあり、その取引履歴は分散台帳に記録されているため誰でも確認できる。そのため、個人の資産の流れや投票傾向を他者が把握でき、プライバシーの懸念がある。これを解決する手段としては投票にガバナンストークンを使用せず、純粋な投票機能のみを提供することが挙げられる。「ガバナンストークンを持っていること」=「DAO のメンバーであること」というようにクレデンシャルとして扱われているため、「投票機能」「メンバーシップの識別」に機能を分ける。

4 DAO における内部告発

DAO の内部告発におけるフローチャートは以下のようになる。

1. 告発者を報復から守るために、匿名性を担保する
2. 告発内容に対する判決は、メンバーの投票によって決定される
3. Web3 で起きるインシデントは事後の解決や制裁が難しいうえ、Web3 上の情報のみで事前に察知することは困難である。
4. そのため、Web2 でのチャット内容などから起きうるインシデントを Web3 上のコミュニティの判断で予見し、裁きたい

5 用語解説

- トークン:ブロックチェーンによって発行、管理される資産や権利のことを指す。
- ガバナンストークン:DAO が発行するトークンのことを指す。これは、純粋な資産としての利用のほかに方向性を決める投票権としても利用される。
ï
- スマートコントラクト:ブロックチェーン上で実行されるプログラムであり、トークンの移動や売買の契約を自動で執行できる。
- Web3:ブロックチェーンの登場により唱えられた分散型の web サービスを総称した概念であり、中央

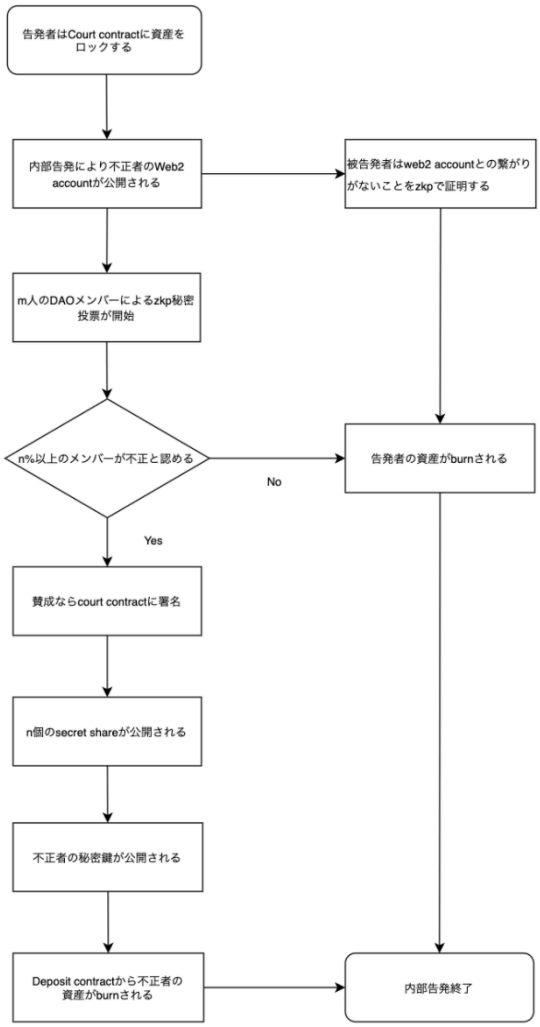

図 3: 内部告発の流れ

集権的なプラットーフォームに依存しているサービスは Web2 と呼ぶ。

- シャミアの秘密分散法:秘密の値を m 個の secret share に分散しユーザに配布する。閾値以上の secret share が再び集まれば秘密の値を復元できる。
- ゼロ知識証明:ある命題の答えを知っていることを、その答え自体を示さずに証明する方法

参考文献

[1] 太宰治、『走れメロス』、新潮（1940 年 5 月号）

[2] 太宰治、太宰治全集 3（ちくま文庫）、筑摩書房 (1988).

[3] Friedrich von Schiller, バラード￥textitde:Die B ￥”urgschaft, 1815.