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:自立分散型組織) は経済的な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.

多くの DAO では自立分散的に機能するまで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いるが, 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. 不正を防止し, コミュニティによる分散的統治を実現するために, 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 シャミアの秘密分散法

ある秘密を分散情報として管理し, 事前に定めた閾値以上の分散情報が集まった場合にのみ復元できるという仕組みである. 各メンバーを $U_1, ..., U_n$ とし, 素数 $p(n < p)$, 秘密 $s(s \in Z_p)$ としたとき, 各 U_i には $d_i \in Z_p$ が割り当てられる. また, 秘密を分散し, 配布する役割を担うディーラー $D \notin U_1, ..., U_n$ としたとき, シャミアの秘密分散法における流れは以下のようになる.

1. D は各 $1 \leqq j \leqq t-1$ について, 秘密かつ無作為に $a_j \in Z_p$ を選び, 式 (1) のような多項式を定める.

$$f(x) = s + a_1 x + a_2 x^2 + ... + a_{t-1} x^{t-1} \quad (1)$$

   このとき, 秘密 s について,$s = f(0)$ である.

2. D は U_i に $s_i = f(d_i)$ を送る.
3. 任意の t 人のメンバー $U_{i1}, ..., U_{it}$ は式 (2) のラグランジュ補間公式を用いることで秘密を復号することができる.

$$s = \sum_{k=1}^{t} s_{i_k} \prod_{1 \leqq \ell \leqq t, \ell \neq k} \frac{d_{i_\ell}}{d_{i_\ell} - d_{i_k}} \bmod \mathrm{p} \quad (2)$$

3 メンバーシップの提案

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は, 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 上から事前に察知するのは困難だが,Web2 上のコミュニケーションツールのチャット内容などから推測できるので, 予め Web2 上のアカウントと Web3 上のアカウントを紐付け,Web2 上のアカウントが公開された場合にのみ Web3 上のアカウントを特定でき, 罰則を与える構図を考えた.

このようなスキームであれば, 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.

図 1: アカウント管理モデル

図 1 は上述のスキームを実現するために考案したアカウント管理モデルであり, 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. Ethereum Address を作成する際に使った秘密鍵を m 個の secret share に分割する
2. 1 つの Web2 account につき,m 個の secret share を紐付けたペアを作る
3. それぞれのペアは m 人のメンバーに配られる

これにより, 閾値 n 個以上のペアが集まればラグランジュ補間公式より, 被告発者自身の秘密鍵が復元され,Ethereum Address 上の資産を失うなどのリスクを追うことになる. 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 上で誠実な振る舞いを続け,DAO にとって危害を与えるような言動を慎むことである.

4 まとめ・今後の展望

本研究では,DAO におけるコアメンバーへの牽制を意図した内部告発スキームの準備としてアカウント管理モデルを提案した. 現在の段階では, ペアの増減に対応できないうえ、中央集権的なディーラの存在を仮定しているなどの課題がある. そこで, 今後はこのような課題を解決できるプロアクティブ秘密分散法を使った改良を行う.