Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

自律分散型組織DAOの匿名環境下における内部告発手法
Whistleblowing Method in Anonymous Environment of Decentralized Autonomous Organization: DAO

津田匠貴 * Shouki Tsuda　荒木俊輔 Shunsuke Araki　正田英樹 Hideki Shoda　安土茂亨 Shigeyuki Azuchi
田中貴規 Takanori Tanaka　中城元臣 Yukishige Nakajo

キーワード Ethereum ブロックチェーン, 秘密分散法, DAO, 内部告発

あらまし

Decentralized Autonomous Organization(DAO) は共通目的を持つ個人からなる非中央集権的組織であり, 独自トークンの発行や分散台帳の機能をもつブロックチェーンを前提としている．この組織による分散的サービス Web 3.0 に対し, 中央集権的な運営の Twitter などの従来のサービスは Web 2.0 と呼ばれる．DAO には匿名で参加できる利点がある．その一方で, 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的に運営することが一般的である．ところが, これに起因する資金の持ち逃げといった問題が数多く発生している．本研究では, DAO の匿名性を維持しつつ, この種の不正防止のために, Ethereum ブロックチェーンにおいて秘密分散法を用いたアカウントリンクと内部告発機能を提案する．Ethereum[1] は汎用性と相互運用性の観点から巨大なエコシステムを持っており, 新しい DAO を構築する例が多いことから, 本研究の対象にした．

問題の本質は, DAO の持つ匿名性が不正を行いやすい状況を作り出していることである．例えば, 資金の持ち逃げが起こっても犯人の特定が困難なうえ, その資金を取り戻すことはほぼ不可能である．その抑止力として, DAO において内部告発機能の提供を考えた．しかしながら, 先にも指摘したとおり, Web 3.0 の匿名性もあり, 犯人の特定は困難である．そこで, 本研究では, Web 3.0 上のアカウントの匿名性を保ちつつ, 実社会により近い Web 2.0 上のアカウントと紐付けることで, 内部告発と, その正しさによって Web 3.0 上のアカウントを Web 2.0 上のアカウントから特定する仕組みを考える．つまり, Web 2.0 のアカウントに対して告発が行われ, それが正しいと認められた場合, Web 3.0 のアカウントが特定される手法を提供する．図 1 は上述の手法を Ethereum 上で実現するために考案したアカウントリンクである．

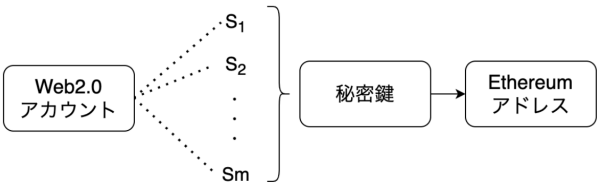

図 1: アカウントリンク

全ての参加者は, 以下のように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秘密分散法に基づいて m 個の share に分割する
2. 1 つの Web 2.0 アカウントにつき, m 個の share を紐付けたペアを作る
3. それぞれのペアを m 人の参加者に配る

秘密分散法により n 個以上のペアが集まれば, 被告発者の秘密鍵が復元され, アドレス上の資産を失うリスクを負う．この唯一の回避法は, 自身が内部告発の対象にならないように Web 2.0 上で誠実な振る舞いを続け, DAO に損害を与える言動を慎むことである．

本研究では, Web 2.0 上での謀議に対する内部告発を有効にするために, 秘密分散法を用いたアカウントリンクを提案した．これにより各参加者は資産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．本提案の課題は, 一般的な秘密分散法はディーラーの存在を仮定しているため, DAO の利点である自律分散性を損なうことである．今後は, DKG を組み込み, 分散環境に適したスキームを提案したい．

参考文献

[1] V. Buterin, “Etherium Whitepaper,” https://ethereum.org/en/whitepaper/, 2013.

* 九州工業大学, 〒 820-8502 福岡県飯塚市川津 680-4, Kyushu Institute of Technologyliation, Kawazu 680-4, Iizuka, Fukuoka, 820-8502 Japan, tuda.syouki484@mail.kyutech.jp