5Y-01

Ethereumを用いた信頼推論システムの実装

大森 涼 † 岸上 順一 † 小林 洋介 †
室蘭工業大学 †

1 はじめに

1.1 情報の信頼性

昨今, インターネット上ではフェイクニュースや EC サイトにおける不正レビューなど情報の改竄や偽造が多発し, 情報についての信頼がゆらいでいる. 評判システムはこの問題への対策の一つである.eBay やヤフオク!などの P2P アプリケーションでも評判システムが導入されており, 買い手が取引の後にフィードバックを送信し, 売り手に評価を割り当て公開することで信頼を築くことができる. しかし, 多くのシステムでは複数 ID を発行して評判を操作する Sybil 攻撃 [1] に対して脆弱であり, 代金の保証などの運営による介入が必要な場合が多々ある. また, 中央機関の存在しない分散型アプリケーションでは, 新規 ID を取得するコストが低いことや不正なユーザを罰することができる中央機関が存在しないなどの理由から,Sybil 攻撃に耐性を持つ信頼システムを構築することはさらに困難である.

1.2 先行研究

TrustDavis[2] は経済的インセンティブにより分散ネットワーク上でユーザ同士の信頼度ネットワークを構築するシステムである. ノードを頂点とし辺の重みを信頼度の裏付けとすることで, 重み付き有向グラフを構築する. ここでの裏付けとは任意の金額であり, 裏付けを与えたノードが責務不履行に陥った際に, 自分がいくらまで保証することができるかを表す. 最大フローの導出により未知のノードとの信頼度の上限を求めることができ,Sybil 攻撃への耐性がある.

TrustDavis において, 信頼はプロパティ毎に固有の物である [2]. たとえば, オークション出品者の目利き能力は信頼していなくても, クレーム対応の誠実さは信頼している場合などが考えられる。このため、P2P 取引市場へ実装する場合, 複数の信頼プロパティに対応することが不可欠である.

1.3 目的

そこで本研究では,TrustDavis を拡張し, 分散型オークション市場に対し, 複数の信頼プロパティの取り扱いに対応した信頼システムの開発を目指す.

2 分散型オークション市場

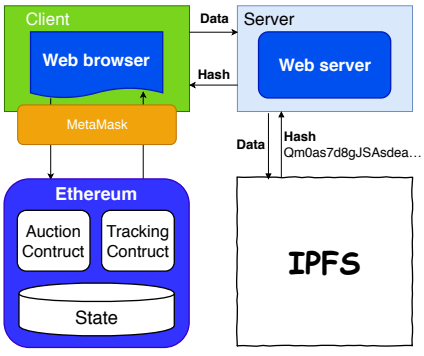

図 1 分散型オークションシステム

本稿では, 新たな信頼システムを導入するモデルとして, 図 1 に示す Ethereum[3] を用いた分散型オークションシステムを用いる [4]. ブロックチェーン技術を用いることで, 特定管理

Development of Ethereum for trust management inference system
Ryo Omori†, Jay Kishigami†, Yosuke Kobayashi†
† Muroran Institute of Technology

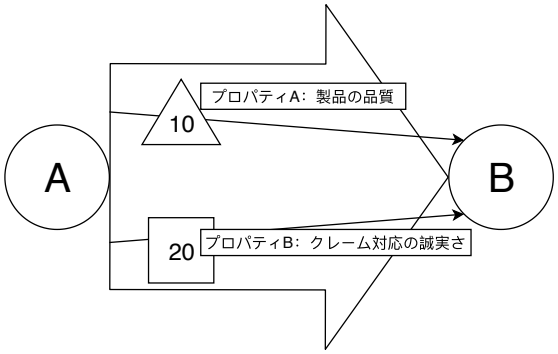

図 2　複数の信頼プロパティ

者が存在しなくとも製品のトラッキングと取引履歴の真正性を保証可能である.

また, 参加者間の信頼プロパティとして以下の二つを定義する. (1) 売り手の提示する製品情報の信頼度:取引後, 売り手が提示した情報通りの製品が買い手の手元に届くかどうかを示す要素. (2) 売り手のクレーム対応の誠実さ:売り手は取引後の返金対応などのクレーム対応を誠実に行う人物であるかを示す要素.

3　要件定義

本稿では信頼システムの要件として, 以下の 3 つを定義した. (a) 特定のシステム管理者が存在せず, 分散システムとして運用可能である.(b) 意図的に複数の ID を変更または発行することによる利益を最小にする必要がある. (c) 参加者が互いの正確な評価を提供し合うインセンティブが必要である.

4　複数プロパティ対応の信頼システム

図 2 は提案システムにおける参加者 A から参加者 B への信頼を表す. 図に示すように,A から B への信頼の裏付けを複数の信頼プロパティ (要素) に対して ETH を信頼の裏付けとすることで行い, 参加者の信頼を重み付き有向グラフで表現する. たとえば, ある出品者の信頼プロパティとして,「プロパティ A:製品の品質」と「プロパティ B:クレーム対応の誠実さ」という 2 つが定義されていた場合, 取引後, 製品の品質が買い手を満足させるものでなかったとしても, 買い手からのクレームに誠実に対応することで, 自身の評判の一部を守ることができる.

5　議論

ここでは,4 で提示したシステムが 3 の要件を満たしているか議論する.(1) の解決は,Ethereum を用いて実装することで特定管理者を必要とせずプログラムを自動実行することによりなされる.(2) について, 参加者間の信頼はグラフの最大フローを求めることで信頼値を求めることができる. よって, アカウントを複製し多くのノードから信頼を集めたとしても, 任意の参加者からの信頼に影響を与えることはできないため, この課題は解決される.(3) について, 本システムでは参加者自身が他の参加者に与える評価に責任を負う必要があることから解決される.

6　おわりに

本稿では, 分散型オークションシステムへ複数の信頼プロパティを取り扱うことのできる信頼システムの実装を提案した. 今後は提案システムを実装する活動を行っていく.

参考文献

[1] Douceur and John R. The sybil attack. pp. 251–260, 2002.

[2] D. B. DeFigueiredo and E. T. Barr. Trustdavis: a non-exploitable online reputation system. 2005.

[3] Gavin Wood, et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, Vol. 151, No. 2014, pp. 1–32, 2014.

[4] 大森涼, 岸上順一. オークションを用いた水産物流通へのブロックチェーンの応用. 第 81 回全国大会講演論文集.