

ビットコインの計算量問題・脆弱性を抜本解決する新合意形成技術

小川 猛志 (東京電機大学 システムデザイン工学部 情報システム工学科 教授)

研究目的・背景

改竄が極めて困難な分散台帳技術である**ブロックチェーン**が、電子マネー、電子投票、IoTリソース管理、スマート契約など、様々なサービスのプラットフォームとして期待されている。主要なブロックチェーン技術の**(PoW)**は**計算量問題と脆弱性の課題**がある。それらを抜本的に解決する**新技術(PoL)**を開発したので紹介する。当該技術は、**安価なIoTマシン**であっても、様々な用途で使用可能な分散台帳を**低消費電力で安全**に利用可能となる。

技術の概要

■ 既存のブロックチェーン

【取引が発生し承認作業を実施する流れ】

- 1) 複数の取引のデータをまとめたブロックを作成
- 2) 全ノードでNonceと呼ばれる値を計算
- 3) いち早くNonceを算出した計算者は、他の計算者へあっているか確認
- 4) 承認後、計算者がブロックチェーンに接続
- 5) 計算者は報酬を受取る

マイニング作業

【ブロックチェーンの考え方】

- 計算者によるマイニング作業にて、データが正しいという合意を得る仕組み。=**Proof of Work [Pow]** と言う
- マイニング作業の仕組み (前提条件)

マイニング作業の報酬 > データ改竄で得る報酬

【課題】

- 1) マイニング作業時の消費電力は、オーストリア1国の消費電力を既に超過
- 2) 専用ハードを実装した端末以外はいくじに参加できない。
- 3) また高性能な端末グループにより当選率を不正に操作する51%攻撃やセルフフィッシュマイニング攻撃が頻発。

■ 研究・開発した技術

- ノードのIDとブロック番号のデジタル署名 (E-IDと略す)と前回当選したノードのE-IDであるLucky_IDを入力した「おみくじ」で当選者を決定。 **当選者抽出の不正防止をする。**

$\text{Hash}[E\text{-ID} + \text{Lucky_ID}1 + \text{Lucky_ID}2 + \dots + \text{Lucky_ID}m + \text{TS}] < \text{閾値}$

想定される用途

- ◆ パブリックブロックチェーンで期待されている全用途
- ◆ 特にIoT等低消費電力で安全性が必要なサービス

従来技術(PoW)より優れている点

- ◆ 現時点で不正が出来ない「くじ」はPoWとPoLのみ
- ◆ PoWに比べ極少の計算量で分散合意形成が可能
- ◆ 計算能力に基づく51%攻撃やセルフフィッシュマイニング攻撃などの攻撃が不可能
- ◆ ノード間の多数決で有効と合意したIDやIdPが保証するIDに基づく公平性の担保が可能(マネーロンダリングや人工知能による取引排除、電子投票等の応用も可能)

既存技術(Proof of Work:PoW)

計算量が事前に予測できない数学問題を最初に解いたノードが当選
⇒ 計算量の予測不能性を「くじ」に利用



10¹⁹ 回以上の計算、72 TWh/年以上の消費電力が必要

強大な計算能力があれば容易にトランザクション取消攻撃(2重支払攻撃)が可能 (Bitcoin Gold, 2018.5, 推定1800万\$被害等)

本発明(Proof of Lucky ID:PoL)

誰も入力値を制御出来ず出力予測も不可能だが、公正性の検証が可能なくじ「おみくじ」を発明
⇒ 「デジタル署名」秘密鍵の逆計算不能性を利用

くじの当事者でも全入力値の制御は不可

くじの当事者でも出力値の予測不可

「おみくじ」

出力 当たり!

- 1回の「おみくじ」で当選者を決定
- 計算能力に基づく攻撃が不可能

企業への期待

◆ 既知の主要攻撃への耐力は机上で確認済みだが、その他の攻撃の可能性評価や、トランザクション性能の向上策など、プロトタイプの開発とフィールド実験を予定しており、共同研究や支援を希望します。

特許・論文情報

- ◆ 出願名称: ノード、合意形成システム 及び当選者決定方法
- ◆ 出願番号: 特願2018-114659
- ◆ 論文: "Proposal of Proof-of-Lucky-ID (PoL) to Solve the Problems of PoW and PoS," IEEE International Conference on Bitcoin 2018, pp. 1212-1218, Jul.2018.