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

信頼度を用いた実用的な Proof of Personhood プロトコルの提案
A Practical Proof of Personhood Protocol Using Credit Score

兵頭 昇虎 * 尾形 わかは *
Hyodo Shogo Ogata Wakaha

Keywords: proof-of-personhood, proof-of-work, proof-of-stake, blockchain

パーミッションレスのコンセンサスアルゴリズムでは，Sybil 攻撃を防ぐなどの安全性を確保するために，Proof of Work[1] や Proof of Stake が一般的に用いられる．しかし，どちらのアプローチにも多くの資源を持つ一部の参加者によってコントロールされてしまうという不公平さの課題がある．これを解決する方法として Proof of Personhood(PoP)[2] が提案されている．PoP とは匿名性を維持したまま，実在の人間と仮想的な ID を 1 対 1 で結びつけるメカニズムで，これを実現するために多くの資源を必要としないため，平等なコンセンサスを実現できる．

PoP のアプローチとして，Web of Trust や政府発行の ID，生体情報などが考えられるが，定量的な分析が困難であることや，プライバシー保護の問題，パーミッションレスなシステムでは使えないなどの課題がある．そこで本研究では，これらの課題を解決できる Pseudonym Party(PP)[3] という手法に注目する．

PP とは参加者が実際に開催されている現実の集会に参加することで，その参加者と仮想的な ID が 1 対 1 で結びつけることができるものである．これは，実在する人物は 1 つの場所にのみ存在するという特性のみによって実現されるため，参加者の個人情報を用いず，プライバシー保護の観点からも安全な手法である．しかし，PP は次の 2 つの課題がある．1 つ目は，現実に開催されている集会に参加しなければならず，地理的な要因で参加できない可能性があること．2 つ目は，新しい参加者を受け入れるために定期的に PP が開催されるが，毎回出席しなければならないこと．一回でも欠席すると，次の PP に参加するまでシステムから除外されてしまう．PP の開催頻度が少ない場合，長期間システムに参加することができなくなる可能性がある．

そこで本研究では，これらの課題を解決する信頼度型 PoP 方式を構築する．1 つ目の課題は，PP を仮想的に実行する Virtual Pseudonym Party(VPP) を構築することで解決する．また，2 つ目の課題は，ある仮想的な ID の所有者が他に ID を所有していないという信頼の度合いを示す信頼度を導入することで解決する．信頼度を用いることで，PP を欠席したとしても，信頼度は低下するが，システムから除外されることはない．信頼度が低下しても，その後 PP に参加し続ければ元の信頼度まで回復できる可能性がある．また，本研究では信頼度型 PoP の安全性として soundness と fairness を定義し，提案する VPP ベースの信頼度型 PoP 方式が満たす安全性について評価する．

参考文献

[1] A. Back, “Hashcash — A Denial of Service Counter-Measure,” Aug. 2002.

[2] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly and B. Ford, “Proof-of-personhood: Redemocratizing permissionless cryptocurrencies,” Proc. IEEE Eur. Symp. Secur. Privacy Workshops, pp. 23–26, Apr. 2017.

[3] B. Ford and J. Strauss, “An offline foundation for online accountable pseudonyms,” Proc. the 1st Workshop on Social Network Systems, pp. 31–36. ACM, 2008.

* 東京工業大学，〒 152-8550 東京都目黒区大岡山 2-12-1，Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo.