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

プライバシーを考慮したブロックチェーンを用いた柔軟なコンタクトトレーシング手法

A blockchain-based flexible contact tracing considering privacy

福田 竜央 * 面 和成 * †
Tatsuhiro FUKUDA Kazumasa OMOTE

キーワード ブロックチェーン, IoT, コンタクトトレーシング, スマートコントラクト

あらまし

近年活用が広まっている IoT 機器の活用事例の 1 つとして、スマートフォン等を用いて、デバイス所有者の接触者や訪れた場所等を追跡するコンタクトトレーシングが存在する。コンタクトトレーシングは、主に感染症対策に用いられているが、人の動きを追跡できることから警察の捜査の補助や目撃証言の補強など犯罪対策への活用が可能であると考えられ、実際シンガポールではコンタクトトレーシング用のアプリを犯罪捜査に利用可能としている [1]。一方で、コンタクトトレーシングでは接触者の情報や位置情報など個人の情報を集めるため、プライバシーの問題があり、特に中央集権的な仕組みの場合、どのようなデータが収集され、収集されたデータが正しく使われているのかなどの懸念が存在する。

このような背景から、分散管理可能なブロックチェーンを組み合わせて、プライバシーの保護及びデータの透明性を確保したコンタクトトレーシングの研究が行われている。しかし、多くの研究はユーザーのプライバシーにのみ注目しており、ユーザーによるデータの偽造を考慮しておらず、また、接触者と訪れた場所の両方の追跡を扱っているものも少ない。ユーザーによるデータの偽造を考慮し、接触者及び訪れた場所の両方の追跡を行なっている研究として Lv らの研究 [2] がある。この手法では、ユーザーは周囲の他のユーザーにチャレンジとして公開鍵をブロードキャストし、レスポンスとして位置情報等の記録する情報を受け取る事で、ユーザーが記録する情報の正当性を他のユーザーに保証してもらっている。しかし、この手法ではデータを記録する毎に異なる公開鍵を必要とするため、ユーザーが多くの鍵を管理する必要がある。

本稿では、ユーザーによるデータの偽造及びプライバシーを考慮したコンソーシアム型ブロックチェーンを用いたコンタクトトレーシング手法を提案し、スマートフォンを用いて実装を行い、提案手法の実現可能性を示す。チャレンジレスポンスとスマートコントラクトによる検証を組み合わせることで、ユーザーによるデータの偽造を検知可能にし、位置情報を暗号化することでプライバシーを保護する。提案手法を用いる事で、通常時はユーザーのプライバシーを保護し、必要に応じてユーザーの同意を得る事で、詳細な行動履歴の追跡ができる柔軟なコンタクトトレーシングを実現する。また、提案手法はブロックチェーンを用いて暗号鍵を管理することで、既存手法より鍵管理コストを削減した。

参考文献

[1] BBC News, “Singapore reveals Covid privacy data available to police,”
https://www.bbc.com/news/world-asia-55541001 , January 5, 2021

[2] Wenzhe Lv, Sheng Wu, Chunxiao Jiang, Yuanhao Cui, Xuesong Qiu, Yan Zhang, “Decentralized Blockchain for Privacy-Preserving Large-Scale Contact Tracing,” arXiv:2007.00894, 2020

* 筑波大学, 〒 305–8573 茨城県つくば市天王台 1–1–1, University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki 305–8573 Japan
† 情報通信研究機構, 〒 184-0015 東京都小金井市貫井北町 4–2–1, National Institute of Information and Communications Technology, 4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-0015, Japan