qBitcoin: A Peer-to-Peer Quantum Cash System

目で見る
海外論文発表

池　田　一　毅*

qBitcoin: A Peer-to-Peer Quantum Cash System

Key Words：Quantum Information Blockchain Cryptocurrency Peer to Peer System

＜参加会議名＞ Computing Conference 2018
＜開催場所＞イギリス　ロンドン
＜渡航期間＞ 7/9 ～ 7/24
＜発表タイトル＞
qBitcoin: A Peer-to-Peer Quantum Cash System

私の発表内容について簡単に紹介します。貨幣は登場以来、様々な形あるいはシステムの中で広く使われています。現代はキャッシュレス化が各地で進むと共に、ユーロ危機以降は暗号通貨が多くの注目を集めています。従来の通貨と暗号通貨の大きな違いは、それらの管理方法にあります。造幣局や中央銀行などが貨幣を発行し、管理していたのとは異なり、暗号通貨は所有者全員で管理するという分散型ネットワークの考えに基づいています。最大の特徴は、ネットワークに繋がっている全ての人々があるプロジェクトにリモートで参加可能になり、単独の組織で実現可能な事柄をはるかに超える規模のプロジェクトを実現可能になることです。しかし、データが分散されているために暗号通貨にはセキュリティ上の弱点がいくつかあります。例えば、送金時間を短縮することや、データの乱用を防ぐことなどは暗号通貨を設計する上で最も重要な事柄です。これらの問題は全て暗号技術に起因しています。本研究の目的は、従来のシステムをより安全な量子暗号理論に基づいて設計し直すことでした。

私たちが普段使用している本や web 上の情報は全て古典情報と呼ばれます。一方、ミクロな現象を扱う量子物理学に基づいた情報は量子情報と呼ばれます。近年の量子コンピュータの開発に注目されるように、量子情報理論・技術も徐々に実用され始め、近い将来に量子情報が飛び交うネットワークの実現が期待されています。私は従来の暗号通貨を参考に、分散型の量子ネットワークで使用可能な量子暗号通貨のシステムを設計しました。本研究の提案事項が実現されれば、従来の暗号通貨で問題であった、送金時間の短縮が容易に可能になり、データが物理法則によって安全に守られることが期待できます。

今回の国際会議には、ヨーロッパ数学協会賞を受賞したパリ第７大学の数学者で暗号通貨の研究も行なっている Marco 博士らも参加しており、会議時間終了後も多くの参加者らと本研究内容に関して有意義な交流を深めることができました。

会場

発表風景

* Kazuki IKEDA
1991年9月生まれ
現在、大阪大学大学院　理学研究科
物理学専攻素粒子理論研究室
博士後期課程２年
修士（理学）　理論物理学
TEL：09036147131
E-mail：kikeda@het.phys.sci.osaka-u.ac.jp