巻頭言

デジタル通貨の情報通信基盤技術に関する現状と課題

Current Status and Issues Related to ICT Infrastructure for Digital Currency

櫻井幸一 *Koichi Sakurai*

九州大学 大学院システム情報科学研究院 教授

Professor, Graduate School of Information Science and Electrical Engineering, Kyushu University

三菱UFJ信託銀行が2022年２月に円連動型のデジタル通貨の本格運用を宣言した。中国は2021年９月に仮想通貨の取引を完全に禁止し，2022年に入ってデジタル人民元のスマートフォン向けウォレットアプリの配信を始め，北京2022オリンピックでの利用を開始した。投資対象となっているビットコインに代表される仮想通貨(暗号資産)に対し，デジタル通貨は中央銀行が発行する法定通貨建てである(Central Bank Digital Currency：CBDC)。

インターネットを使って商品売買や契約を行う電子商取引が2000年代に本格化し，現在まで広く普及している。この技術基盤の一つには，SSL(Secure Socket Layer)でクレジットカード番号を安全に送ることを可能にしている公開鍵暗号がある。日本では，公開鍵認証基盤(Public Key Infrastructure：PKI)の普及を目指し，経済産業省主導傘下で，eコマースプロジェクトに，三菱電機も含め多くの国内電機通信メーカーも参加した。この時期には，日本電信電話㈱(NTT)と日本銀行とが共同で，現金同様の匿名性を持つデジタル通貨(当時の呼び名は，電子マネー)を開発した。ここでも，利用者のプライバシーを守りながら，デジタル情報の複製による不正な二重使用の防止という課題解決に，高度な暗号が使われている。

おかげでPKIは普及し現在に至っているが，デジタル通貨自体は実用化にまでは至らなかった。代わりに，JRのICカードであるSuicaが普及し，現在ではスマートフォンに搭載されるお財布携帯にまで進化している。また，スマートフォンにQRコード(注1)を組み合わせたキャッシュレス決済は，日本でもコンビニエンスストアを中心に普及してきた。その中で2019年に独自決済サービスを始めたものの，開始直後から不正利用の被害が確認されたため，一旦はサービスを停止した事例は記憶に新しい。これは，利用者の認証を二段階構造にしていなかった弱点を突かれたサイバー攻撃の一つである。では，二段階認証で十分安全かという議論もあり，こうした技術の安全性の解明も研究課題である。

ビットコインは分散システムと呼ぶことも多いが，私自身は非中央集権型又は分権型システムと呼んでいる。これは，PKIが信頼できるセンターに基盤を置く中央集権型とは正反対である。PKI以前のPGP(Pretty Good Privacy)という暗号化ソフトウェアを思い出そう。ここでの利用者登録は，友達の紹介による信頼の和を広げるもので，中央管理者が存在しない民主型である。ビットコインの基盤も，ある意味ではPKI以前のPGP民主型基盤に戻ったとも言える。

そして今，各国の中央銀行が発行を構想しているCBDCは，仮想通貨から再び中央集権型に戻ることになる。この意味では，NTTと日本銀行とが共同試作した電子マネーも再評価されるべきであるが，現状はそうなっていない。日本銀行も，米国同様にCBDCを発行することの長／短所を検討しているが，いまだ試行プロジェクトの計画宣言にとどまっている。しかしこの20年間で，暗号を始め情報通信技術が大きく進歩した。スマートフォンの性能はいまだに進化しており，さらにアプリケーションのダウンロードサービスも普及した。CBDCもこうした基盤の利活用を前提としているが，中央銀行が利用者全てに共通の利用環境を提供できるかどうか，という課題がある。またビットコインに使われている楕円(だえん)曲線暗号の寿命はあと10年程度が限界であろう，という技術評価にも留意する必要がある。さらに量子計算機が登場すれば，多くの仮想通貨の暗号は解読されることになり，永続運用可能な暗号資産やデジタル通貨の設計自体が未解決問題である。

こうした変化は，分散・分権基盤から再び中央管理基盤に戻るCBDCを手本に，新しいデジタル商取引を生み出す好機会と考えることもできる。解決すべき課題の一つには，オープンアプリをスマートフォンにダウンロードする際の信頼性確保がある。政府はマイナンバー(注2)の利活用を掲げており，技術的にはスマートフォンとの連携に有効な仮想化技術であるTEE(Trusted Execution Environment)も注目されている。暗号技術を始め，三菱電機の情報通信技術と新たなビジネスサービス展開に期待したい。

(注１)　QRコードは，㈱デンソーウェーブの登録商標である。
(注２)　マイナンバーは，デジタル庁会計担当参事官の登録商標である。