O-024

CBDC といった価値を有するデータを安全に送受信するためのネットワークについて

乾泰司†、髙橋亘‡
†ISO/TC68 委員会、ISO20022 (Payments SEG, Securities SEG), Citron システムズ，‡大阪経済大学

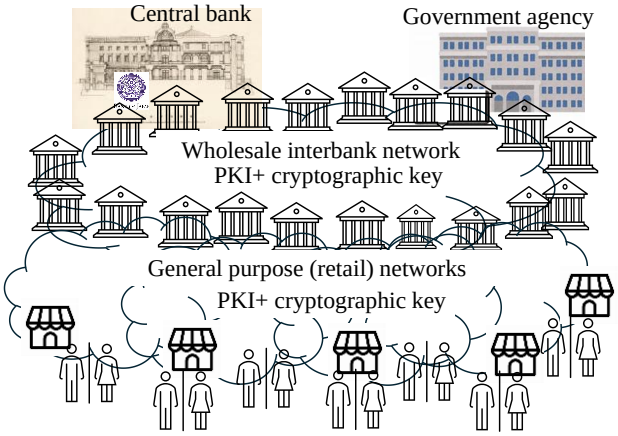
Possible network infrastructure securely transferring data having value themselves such as CBDCs

Taiji Inui† ISO/TC68 Committee., SO20022 (Payments SEG, Securities SEG),& Citron Systems
Wataru Takahashi‡ Professor, Osaka University of Economics

1. はじめに

現在、紙による情報を遠隔地に送る場合に手紙やはがきという手段を利用することが可能である。一方、日本銀行券といった紙幣を遠隔地に送る場合には、現金書留という特殊な封筒を使う必要がある。因みに現在、金額でみれば決済の大半は銀行預金の振替で行われているが、そのシステムを概観すると、ネットワーク上を電送されるのは、振込指図などの決済を指図する指図手段という情報であり、決済手段である「お金」という価値そのものは、堅固なセキュリティで、守られたデータベース内に格納されている。世界的にそのセキュリティの高さで知られている日本銀行金融ネットワークシステム（日銀ネット）も価値となるデータ（日本円）は、物理的にも情報技術的にも確りとしたデータベース内に安全に格納されており、日本銀行券に相当する「お金」がネットワークを通じ外部に出て行くことはない。また、銀行（金融機関）間の支払ネットワークである全銀システムも、ネットワーク上を行き交うのは情報であり、価値そのもの（お金）ではない。一方、最近の決済に関する動向を見ると、多くの国（中央銀行）で、CBDC（Central Bank Digital Currency）の発行を検討している。実際、2023 年 11 月に日本銀行から公表された「中央銀行デジタル通貨に関する日本銀行の取り組み」によると、「今後、中央銀行デジタル通貨（CBDC）に対する社会のニーズが急激に高まる可能性」、「現時点で CBDC を発行する計画はないが、しっかり準備しておくことが重要」、「実証実験と制度設計面の検討を進めていく」、「デジタル社会にふさわしい決済システムのあり方について、幅広い関係者とともに考えていく必要」といった文言に加え、CBDC の発行の必要性に関する各国中銀へのアンケート結果として「半数以上の先が、近い将来リテール CBDC を発行する可能性がある」としている。このような状況を背景として、これまでの決済システムと異なり、CBDC という決済手段＝「お金」そのもののデータが、データベースを飛びだし、ネットワークを介して遠隔地に送られることを想定する必要があると言える。これを、冒頭の現金書留に当てはめると、ネットワーク上（回線内）を価値のあるデータ（お金そのもの）が移動する事となる。従って、現金書留と同様に、電送される CBDC を守るセキュリティ対策が必要となる。本ペーパーでは、PKI (Public Key Infrastructure) に代表される公開鍵暗号化方式を活用し CBDC を安全に遠隔地に送る方法を提案している。なお、現金の発行・流通と同様に、

An image of two-tier network architecture



CBDC の場合も、中央銀行から金融機関（銀行）を経由して店舗・一般家庭へと流通していく二層構造を採用するのが自然と思われる。

2. CBDC を送受信するためのネットワーク

中央銀行が法定通貨として発行する CBDC は、十分なセキュリティおよび匿名性を保証する必要がある。本稿では、CBDC という価値のあるデータを安全に電送するためのネットワークインフラについて以下議論したい。組織としては、CBDC を発行し流通させる中央銀行に加

え、CBDC を格納する電子金庫、電子財布といった「デジタルデバイス」についてセキュリティを含め企画・管理を担当する政府機関 を設置することが考えられる。

CBDC およびデジタルデバイスの認証には、各々、中央銀行および当該政府機関を認証局とする PKI を利用する。この際、暗号化鍵（秘密鍵、公開鍵いずれも）が当該ネットワークインフラ（デジタルデバイスを含む）の外部に露出しない仕組みを提供。また、CBDC が偽造、改竄された場合に、そのような不正を速やかに検知できるインフラを提供する。CBDC 発行に際しては、中央銀行において 1 組の CBDC 認証用秘密鍵および公開鍵を生成し、同中銀内にある物理的にも情報セキュリティ的にも守られた安全な場所に CBDC 認証用秘密鍵を保管する。

各 CBDC には、数字及びアルファベットによるユニークな記番号を付与する。これは、現状、日本銀行券に付番されている記番号と同じ機能を持つものであり、すべての CBDC を特定できることになる。ただ、現段階では、CBDC に日本銀行券と同様な金額（券種）による「Denomination」 を付与するかは定かではない。更に、CBDC には、中央銀行の「印章」を中央銀行の秘密鍵で暗号化したものを付与し、中央銀行の公開鍵で復号化することにより、真贋の判定ができるようにする。また、デジタルデバイスには、当該政府機関の秘密鍵で暗号化した同政府機関の「印章」を付与し、同政府機関の公開鍵で復号化することにより、同デジタルデバイスの真贋を判定できるようにする。

CBDC をデジタルデバイス間で送受信する場合、一般的にインターネットのようなセキュアではないネットワークを利用することも想定される。具体的には、各デジタルデバイスの秘密鍵と公開鍵により、相互認証を行うと共に十分なセキュリティ（強度）を持つ共通鍵を生成・共有することにより、ネットワークを介して CBDC を送ることが可能となる。このような仕組みを提供することにより、インターネットといった比較的安全でないネットワークを介し CBDC を送受信できるようにすることが望まれる。詳細は、Google サイトに掲示されている「中央銀行ないしは同等の機能を有する機関が法定通貨として発行することを目的とした電子マネーおよび電子マネーシステム」参考文献 1 を参照願いたい。

3. おわりに

以上、GDCC による金融市場の発展について、議論してきたが、本提案は、まだ法律面をはじめとする課題も多く残っており、異なる分野、立場の方々の精査や更なる検討により、実用化に向けた様々な取組がなされることが期待される。本報告を検討するにあたり、多くの方々のご支援、ご助言を頂いた。ここに深く感謝する次第である。特に、NTT データ社の竹之下誠氏、山本周氏、CITRON システムズの渡辺大修氏に衷心より御礼申し上げる。なお、本報告に記載されている内容や意見は、著者等個人の考えであり、中央銀行あるいは国際機関他いかなる機関の見解を示すものではないことに留意の要。

参考文献

1. Electronic money issued by central bank or institute having equivalent function as legal tender, 2009
https://patents.google.com/patent/JP2009020848A/ja
https://patents.google.com/patent/JP2009020848A/en
2. 甦る永楽銭—貨幣の将来とアジアデジタル共通通貨、髙橋亘、京都銀行、2020
3. アジアデジタル共通通貨についての一考察、乾泰司、髙橋亘、石田護、神戸大学経済経営研究所、2020
4. A proposal for an Asia digital common currency, Taiji Inui, Wataru Takahashi, Mamoru Ishida, VoxEU (CEPR Centre for Economic Policy Research London), 2020
5. 東南アジアにおける資金・証券決済環境の現状と今後の見通し、乾泰司、財務省 2022 年
6. 国際通貨としてのアジアデジタル共通通貨、乾泰司、髙橋亘、ニッセイ基礎研究所、2022
7. アジアデジタル共通通貨の発行方法・手順および検討課題について、乾泰司、髙橋亘、石田護、神戸大学経済経営研究所、2023
8. グローバルデジタル共通通貨の提案、乾泰司、髙橋亘、情報処理学会、2023
9. アジアデジタル共通通貨（ADCC）の価値（為替相場）について、乾泰司、髙橋亘、金融学会、2024
10. グローバルデジタル共通通貨（GDCC）の金融市場発展への貢献、乾泰司（Citron システムズ），髙橋　亘（阪経大）、情報処理学会、2025