

『World Economy Report』 Vol.1 実現可能な電子通貨の設計

川野祐司（東洋大学教授）

1. キャッシュレス化の進展

企業間取引や国際的な決済の分野ではかなり古い時代からキャッシュレスな取引が行われていた。手形や小切手もキャッシュレスな取引だといえる。銀行振り込みや引き落としは個人にも広く普及している。キャッシュレス化自体は新しい現象ではないものの、近年は個人による店頭での支払いやオンラインショッピングなど、より幅広い場面でのキャッシュレス化が進んできている。現金での支払いには匿名性があり、いつ、どこで、誰が、どのような取引をしたのかが分からない。キャッシュレスな支払いではこれらのデータを収集することができ、データを活用したビジネス機会が生まれるとともに、違法な取引の抑制も期待されている。

以前はキャッシュレスな支払いではクレジットカードしか選択肢がなかったが、ICT化の進展や決済を支えるインフラが整備されてきたことで選択肢が広がってきた。特にスマートフォンとQRコードの組み合わせにより、利用者の個人だけでなく小売店側も安価にサービスを利用できるようになってきている。キャッシュレス化は先進国だけでなく途上国でも進んでおり、日本は世界の中でも遅れが目立ちつつある。政府は2027年までにキャッシュレス決済の比率を40%にまで高める数値目標を設定したが、かなり低い目標だと言わざるを得ない。

スマートフォンを使ったモバイルペイメントが普及しつつあるが、決済の仕組みにより2つに分かれる。第1は銀行預金の振り替えを行うもので、スウェーデンのSwish、デンマークのMobilePayやDankortアプリ、ノルウェーのVipps、ベルギーのペイコニック、フィンランドのSiirtoなどが知られている。先進国だけでなくインドのRupayなど途上国での取り組みもある。デビットカードがスマートフォンの中に入っているイメージだ。第2は電子マネーで、日本でもnanaco, Edy, Suica, WAONなどの電子マネーがスマートフォン上で利用可能になっている。日本ではクレジットカードからチャージすることが一般的だが、中国のAlipayやWeChatPayなど銀行口座からチャージするパターンもある。電子マネーはケニアのMpesaなどアフリカにも広がっている。

仮想通貨も支払い手段となる可能性を秘めている。ビットコインとそこから派生して誕生した多くの仮想通貨では、システムを管理する中央集権的な仕組みがなく、システムに参加する人々の信頼度が不明確であっても通貨の取引が安全に行われ、全ての取引データを誰でも作り出したり参照したりできる新しい仕組みを取り入れている。現在は投機の対象になっているものの、わずかながら支払い手段としても使われている。仮想通貨は安価な手数料でリアルタイムに送金できることから、国際送金に適しており、出稼ぎ労働者の本国への送金などに強みを発揮する。実際に、国際的な決済サービスを展開しているSWIFTは、仮想通貨の広がりを受けて事業の改革に追い込まれている。仮想通貨は分散型台帳技術を使っているものが多く、中でもブロックチェーンを利用するものが多い。ビットコインのブロックチェーンはデータの改竄が難しいという特徴があり、様々な分野から注目を集めている。

2. 電子通貨を巡って

銀行、ICT企業、オンラインショッピング事業者など民間事業者がキャッシュレス化を進めているが、現金を発行している中央銀行もキャッシュレス化に興味を持っている。現金は偽札防止技術の開発、デザインの決

定、印刷、保管、輸送、真贋判定、廃棄など様々なコストがかかる上に、紙や金属資源を多く使用する。日々の取引はキャッシュレス化が進んでいるものの金融危機などが発生すると現金の引き出しが増えることが分かっており、現金は不便ではあるものの信頼のおける支払い手段とみなされている。中央銀行が発行する支払い手段は経済における役割が非常に高いが、技術が進歩している現在、紙の形態で発行される現金が最も安全で信頼できるものなのか、という疑問が残る。

中央銀行が発行するデジタル形式の法定通貨については様々な呼称があるが、本稿では電子通貨（e-cash）と呼ぶことにする。中央銀行と市中銀行の間でやり取りされる中央銀行当座預金はすでにデジタル化されているが、電子通貨は個人が使える支払い手段を指す。2017年にかけてカナダやシンガポールでは中央銀行当座預金にブロックチェーンのような新技術が使えるのか研究が行われた。2017年には国際決済銀行の四季報で中央銀行が発行するデジタル通貨の分類が試みられている。スウェーデンの中央銀行であるリクスバンクは、電子通貨e-kronaの発行に関する研究を進めており、2017年に1回目の中間報告を公表し、2018年中にも発行の是非を判断する見通しとなっている。一方、デンマークの中央銀行は2018年に入って電子通貨の発行は金融システムに与える影響が大きいとして発行に否定的な見解を示している。イギリスの中央銀行ではキャッシュレス化の進行がマクロ経済にどのような影響を与えるのか試算が試みられている。南米ではベネズエラのペトロ、ウルグアイのe-pesoなど仮想通貨のICO（イニシャル・コイン・オファリング）を利用した政府発行の仮想通貨が誕生した。ただしこれらの仮想通貨は価値の裏付けのない政府債務だと解釈できる。いずれにせよキャッシュレス化の進展は電子通貨の発行に関する議論にまで発展しており、電子通貨の登場は遠い将来の話ではなくなりつつある。

3. 電子通貨に求められる役割

電子通貨は既存の現金と同じような使い勝手の良さを持つ必要があるが、現金と全く同じ機能を果たすべきとは限らない。例えば、電子通貨にIDを振ることで使用履歴をある程度追跡できるようになり、現金が持つ匿名性は失われる。電子通貨の法的な位置付けによっては、ウォレットと呼ばれる電子通貨管理機に多くの金額、極端なケースでは全財産を移すことができるようになり、多額の現金を持ち運ぶ不便さがなくなる。人によっては銀行口座を解約するかもしれない。電子通貨の仕様によって果たす役割は大きく異なるため、仕様や関連法規についての議論は早くから進める必要がある。

技術面では、電子通貨には数多くの支払いを処理できるスピード、二重支払いを防止する信頼性、データの改竄を防ぐ安全性が求められる。二重支払いとはシステムの遅延やバグを利用して同一の電子通貨の支払いを複数回行うことである。ビットコインでは二重支払いを試みる攻撃が日常的に行われているが、ブロックチェーンの生成ルールを工夫することで二重支払い攻撃を回避している。また、現在のところ、ビットコインのブロックチェーンデータの改竄は技術的にほぼ不可能であり、取引データが過去に遡って書き換えられるリスクは限りなく小さい。仮想通貨の流出事件や詐欺事件は、仮想通貨の管理や関連プログラムの作成ミスによるものであり、仮想通貨の仕組み自体に起因するわけではない。一方で、ブロックチェーンは処理速度が遅いという問題点を抱えている。ビットコインのブロック生成速度は平均10分と非常に遅く設定されており、支払いの遅延がたびたび生じている。イーサリアムという仮想通貨ではブロック生成速度を12秒まで短縮しているものの、2017年末にはクリプトキティーズという猫のアプリが流行ったことでイーサリアムネットワークに遅延が生じた。現在では、電子通貨のプラットフォームにブロックチェーンは使えないというのが一般的な見解になりつつある。しかし、中央集権的なサーバーを用意してデータを集中的に処理する従来の決済プラットフォームでは、サーバーの維持費用の負担やセキュリティ対策が欠かせない。スピードの遅さを克服するための技術としてアイオタという仮想通貨に用いられているDAG（有向非巡回グラフ）が注目されているが、現時点では電子通貨のプラットフォームに関する研究はまだないようだ。既存の技術単体では電子通貨の機能を実現でき

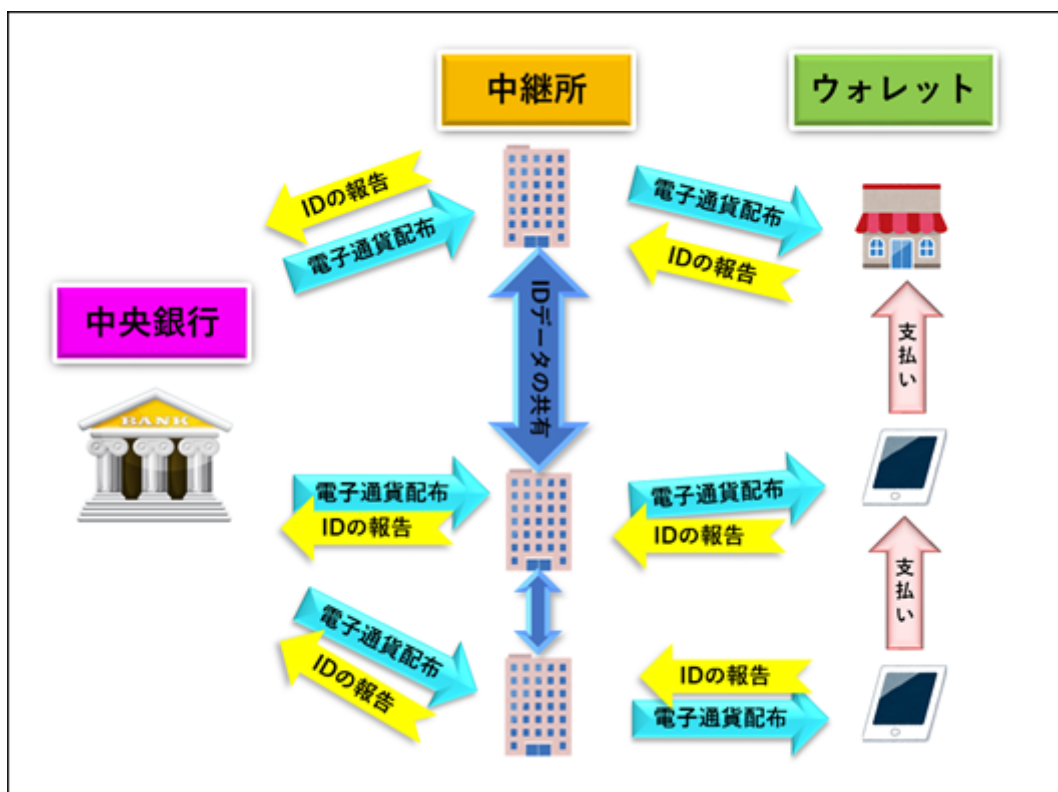
ない。ビットコインも既存の技術を組み合わせることで通貨の支払いを実現させたが、電子通貨でもいくつかの技術を組み合わせる設計するのが現実的な解決策となる。

普及は電子通貨の大きな問題点となる。日本は、高齢者でもAlipayなどを使いこなす中国やモバイルペイメントを使うヨーロッパとは大きく状況が異なる。地方部や高齢者層へのウォレットの配布と普及は他の国よりも苦戦すると予想される。日本で電子通貨を発行する場合は現金との併用期間をやや長めに設定する必要があるだろう。場合によっては世代交代を待つ必要もあるかもしれない。ウォレットの形態はスマートフォンのアプリの他に、太陽電池や液晶画面の付いたカードもあり得る。いずれもPINコード（暗証番号）や指紋認証機能などと併用して利便性と安全性のバランスを取ることができる。現金の場合は財布を盗まれたら制約なく使われてしまうが、電子通貨のウォレットは盗難者にとって現金入りの財布よりも不正利用のハードルが一段階高い。外国人観光客が利用できる一時的なウォレットも整備する必要がある。

4. 電子通貨の設計

スウェーデンのリクスバンクのレポートでは、e-kronaは電子マネーのようにウォレットやカードが管理する仕様とリクスバンクのサーバーで集中的に管理する仕様が併記されている。電子マネー方式では個人間の現金の受け渡しのような取引も簡単に行うことができ、膨大な数の取引をリクスバンクのサーバーで記録する必要はないが、電子通貨に追跡機能を付けることができず、現行の法制度ではマネーロンダリング規制がネックとなってウォレットに多額の電子通貨をチャージできない（EUでは250ユーロ相当に制限される）。一方でリクスバンクのサーバーですべての取引を記録する方式では莫大なデータの迅速な処理が問題となる。通信トラフィックの集中や自然災害などでサーバーがダウンしたら電子通貨の取引がストップしてしまう。電子通貨のシステムには、市中で膨大な数の取引が行われているにもかかわらず中央銀行のシステムで処理する件数は少なく済むという工夫が欠かせない。そこで、本稿では図のように中央銀行、中継所、ウォレットの3層からなる電子通貨のシステムを提案したい。なお、本稿で提案するシステムでは電子通貨に金利は付かない。

図1 電子通貨のシステム



中央銀行は現金と同じように電子通貨を創り出して供給する。電子通貨1円につき1つのIDが付けられており、中央銀行のサーバーは電子通貨がどこに存在しているのかデータを保管している。また、中央銀行は中継所やウォレットの認証を行っており、中継所IDやウォレットIDも保管している。電子通貨IDと中継所IDはペアで保管されているため、中央銀行はそれぞれの中継所が何円分の電子通貨を保有しているのか把握している。

中継所は中央銀行から一時的に電子通貨を預かり、ウォレットに配布する役割を担っている。現金の世界では、銀行が中央銀行から現金を預かって民間に配布している。中継所は銀行と同じような役割を果たすが、銀行だけでなく幅広い事業者が中継所になる可能性がある。中央銀行から中継所に電子通貨が移動したことは中央銀行のサーバーに記録される。中継所も中央銀行から受け取った電子通貨IDを保存する。中継所同士で電子通貨の融通をすることもできる。中継所はウォレットに電子通貨を配布する際に、電子通貨IDとウォレットIDを紐づける。つまり中継所は誰がいくら持っているのかを把握している。中継所同士は定期的にデータの共有を図る。自分のデータだけでなく、他の中継所のデータもバックアップとして保管する。

ウォレットは中継所から受け取った電子通貨IDを保管する。ウォレットは個人が保有するだけでなく、企業や商店も保有できる。個人間で電子通貨を受け渡したり、買い物で電子通貨を支払ったりすると、ウォレット間で電子通貨が行き来する。支払い側のウォレットが受け取り側のウォレットに電子通貨IDを伝達することで支払いが完了する。ウォレットは一定期間（例えば24時間）ごとに中継所に保有する電子通貨のIDを報告する。中継所はこの報告を受けて自分のデータベースを更新する。支払い側のウォレットと受け取り側のウォレットが異なる中継所に紐づけられている場合、中継所は自分が把握していない電子通貨IDを受け取ることになる。その際には中継所同士で電子通貨IDを確認し合って互いに正しいデータを保管する。中継所も一定期間ごとに中央銀行に自らが保有する電子通貨IDを報告し、中央銀行のサーバーは電子通貨IDと中継所IDのペアデータを更新する。

このシステムは、中央銀行は中央集権的なデータベースを運用し、中継所は分散型台帳技術を利用するハイブリッドシステムになっている。このシステムでは、中央銀行はウォレットを認証してIDを与えるが、電子通貨がどのウォレットに入っているのかを知ることはできない。中継所も一定期間ごとに電子通貨がどのウォレットに入っているのか知ることができるが、リアルタイムの動きは分からない。リアルタイムの把握を犠牲にする代わりにやり取りするデータ量を削減している。中央銀行は電子通貨IDとウォレットIDを紐づけないことにしたが、紐づけも可能である。通信技術などの向上により、ウォレットにより頻繁に電子通貨IDを報告させて把握率を高めることもできるが、その必要性について議論の余地がある。

日本では現金流通額のGDP比率が国際的に見て高いが、多くの現金が退蔵されていることも原因の一つだと考えられる。日本では紙幣のデザインが変わっても旧紙幣が有効なままにされている。どこに退蔵されたのか分からない現金もかなりあるだろう。この問題に対処するために、ウォレットが一定期間（例えば1年間）中継所への報告を怠るとウォレットがロックされる機能を付加することができる。ウォレットの保有者が死亡して相続人がいない場合などに該当する。一定期間（例えば5年間）ロックされた電子通貨を廃棄処分にすることもできる。電子通貨のメリットの一つとして、経済に投入されて使用されている金額をかなり正確に把握できることが挙げられる。様々な経済統計に利用できるだろう。

電子通貨の設計次第では金融システムに大きな影響が出るが、本稿が提案するシステムでは銀行が中継所に参入することでこれまでと似たような役割を果たすことができる。所得や預金の少ない人は口座を解約するかもしれないが、企業や大口預金者が残るだろう。電子通貨に金利が付かないため、ウォレットには一定金額を入れておき、それを超える部分は銀行口座に預金することが予想されるためである。金融政策に与える影響も

最小限で済むだろう。

※本レポートは、平成29年度日本国際問題研究所プロジェクト「反グローバリズム再考：国際経済秩序を揺るがす危機要因の分析」における「世界経済研究会」の研究活動の一環である。

(2018-04-03)