White Paper of Crypto Cash

一般社団法人情報セキュリティ研究所
代表理事　　中村宇利

＜はじめに＞

人類が物々交換に限界を感じ始めたころ、間接的に価値の交換を行う手段として貨幣が考案され、現金取引が生まれた。取引を行う人の信用で成り立つ信用経済に比べて、信頼できる発行者が発行したエンティティを有する現金を使えば、取引を行う人の信用は必ずしも必要ではないので、少額取引から巨額取引まで、高頻度で行えるため、現代経済学においては不可欠の取引形態とされている。

現代では、貨幣の基本機能は「決済手段」、「価値の保蔵手段」、「価値尺度」の 3 つと言われている。特殊な形の石や貝殻から始まり、金属、紙とその媒体を変えて進化してきたが、偽造、不正使用の問題に終止符を打つことを目的に 20 世紀半ばより開発されてきたのが、究極の貨幣である、「Crypto Cash（暗号貨幣）」である。80 年前後に誕生した最初の Crypto Cash は、暗号化されたデータをプラスチックカード上の情報保存部分に格納する固定額式のもので、プラスチックマネーと呼ばれた。尚、日本国内で広く使われている Suica はこれらプラスチックマネーの後継と考えられるが、再課金可能方式としたことで、偽造、不正使用ができるようになってしまい、当初の Crypto Cash の目的は果たせていない。

その後 1983 年に、米国 David Chaum 博士によって暗号化された貨幣情報だけで Crypto Cash を作成できることが示され、1989 年に DigiCash として事業化された。暗号化された貨幣情報だけで Crypto Cash をつくるということは、「デジタルの現金」を作ることができることを意味し、その後数多くの企業が DigiCash に続いた。

Windows95 が発売され、また、インターネットブラウザーNetscape が利用できるようになった 1995 年頃には、インターネットは専門家のための単なる掲示板から、一般向けの商取引の主戦場に変貌しようとしており、Crypto Cash は、この商取引に必須のツールとして注目を浴び、ときあたかも新通貨のカンブリア紀という様相を呈していた。米国や英国を中心に新しい Crypto Cash のコンセプトが次から次に発表され、実用化され、そして淘汰されていった。今から考えれば、当時の未完成の不完全な暗号技術を用いる故に、本当に安全な Crypto Cash は作れる由もなかったのである。

Crypto Cash の完成には、暗号技術そのものの完成が不可欠であり、更なる 10 年を必要とした。

世界で初めての真の Crypto Cash が完成して 2 年が過ぎたころ、SATOSHI NAKAMOTO の名前で紹介され、実用化されたひとつの試みがあった。ビットコインである。時代考証を行うならば、恐らく DigiCash と同じ頃の論文であり、DigiCash 以前の現金方式ではない「台帳」方式の一試案であり、当時の不完全な暗号技術を用いる。台帳として半世紀以上前から使われているハッシュチェーンを使用する。総じて技術的には見るべきものはないが、全ての参加者に同じ台帳を持たせることによって、膨大なコストをかけて多数決方式で台帳の改竄を防ごうとすることに特長がある。合意形成に一定の時間をかけ、その間に取引内容に意義がないことを全員が確認し（真贋チェック）、既に使われたものでないか確認（二重使用チェック）する。多数決方式なので民主的に見えることが幸いしたのか、単なる投機目的なのか、一部の熱狂的なユーザーを獲得した。ところが、代表的な暗号資産（仮想通貨）のイーサリアム系で昨年初頭、ビットコイン系で本年初頭に 51%

攻撃が行われ、壮大な多数決実験はすでに終焉を迎えようとしている。

＜Crypto Cash＞

新しい暗号貨幣である“Crypto Cash”は、完全暗号技術を使って、発行者情報や価値情報を直接暗号化し、暗号化後の記号列を暗号貨幣とする。さらに、信用情報、使用条件、利息、期限などの条件も合わせて暗号化することで、様々な機能を持つ暗号貨幣を作ることができる。完全な暗号技術を使用することで、偽造、不正使用を防止する。また、記号列であり媒体を問わないので、金属に刻印され硬貨にしたり、紙に印刷して紙幣にしたりして使用される。もちろん「デジタルの現金」としても使用される。さらに、記号列という実体を持つので、実体のある貨幣として保蔵に適することも特徴の一つである。

Crypto Cash は、金属や紙の貨幣をベースとした通貨と同様、国家の信用をベースにした法定通貨としても、他の法定通貨との兌換券としても発行され得るが、香港の法定紙幣のように、銀行やグローバル企業などの発行者または発行グループの信用で発行されてもよい。また信用の保証として、金銀などの貴金属のほか、資源価値を担保として、その兌換性による信用を利用して発行されることも考えられる。

現在の通貨のほとんどは、予め発行量を決めて発行し、一般には国或いは中央銀行が、貨幣を保管・管理しながら市場に流通させる。

Crypto Cash は、発行者及び価値を確認のうえ、完全暗号技術を用いて暗号化し暗号貨幣情報（記号列）を発行する。Crypto Cash を使用する際には必ず真正性、未使用を確認し、受領者は保蔵または決済する。その都度新たな暗号貨幣情報（記号列）に更新することでより高い安全性を確保できる。

改めて整理すると、Crypto Cash は以下の 4 つのコア機能によって構成され、目的に合わせて応用システムと組み合わせて使用される。

a. 信用（担保）確認機能
   法定貨幣との兌換、または担保を確認する。法定通貨との兌換の場合は紙幣番号、また例えば資源担保の場合はその資源鉱区にナンバーリングしてその鉱区を貨幣情報に加える。
b. Crypto Cash 発行機能
   発行者情報や価値情報を完全暗号化して Crypto Cash を発行する。
c. Crypto Cash 保管・管理機能
   発行済 Crypto Cash を保管・管理し、市場流通量を調整する。
d. Crypto Cash 真正確認機能
   Crypto Cash を使用する際、本物かどうか、すでに使われたものでないか、確認する。

Crypto Cash は、もともと法定通貨の偽造、不正使用防止を目的として開発されたが、崩壊しつつある従来の暗号資産の救済や、暗号証券／債券の発行・管理、暗号保険の発行・管理などの応用が準備されている。

<Example>

〈ユーザー発行型 Crypto Cash〉

Crypto Cash では、予め発行する「サーバ発行型」に加えて、Crypto Cash の使用者が使用の度に発行する「ユーザー発行型」も実現できる。つまり、中央集権的な存在だけでなく、誰でもが貨幣としての Crypto Cash を発行できるようなシステムを構築することが可能である。その際、従来のパーソナルチェック同様、個人の預金、プリペイド残高や信用を担保として発行される。尚、世界で 1 兆ドルを超えるとされる盗難や偽使用の心配なしに、それぞれ従来のデビットカード、プリペイドカード、クレジットカード同様の使用ができる。専用のカードリーダーや専用線が必要ないので、導入は容易である。

ここで、ユーザー発行型の実用例として、近年急増するカード詐欺（例えば、カード番号を不正取得して不正使用する）を防止できる、デビットカード型 Crypto Cash（DC-CC）を、図を用いて説明する。

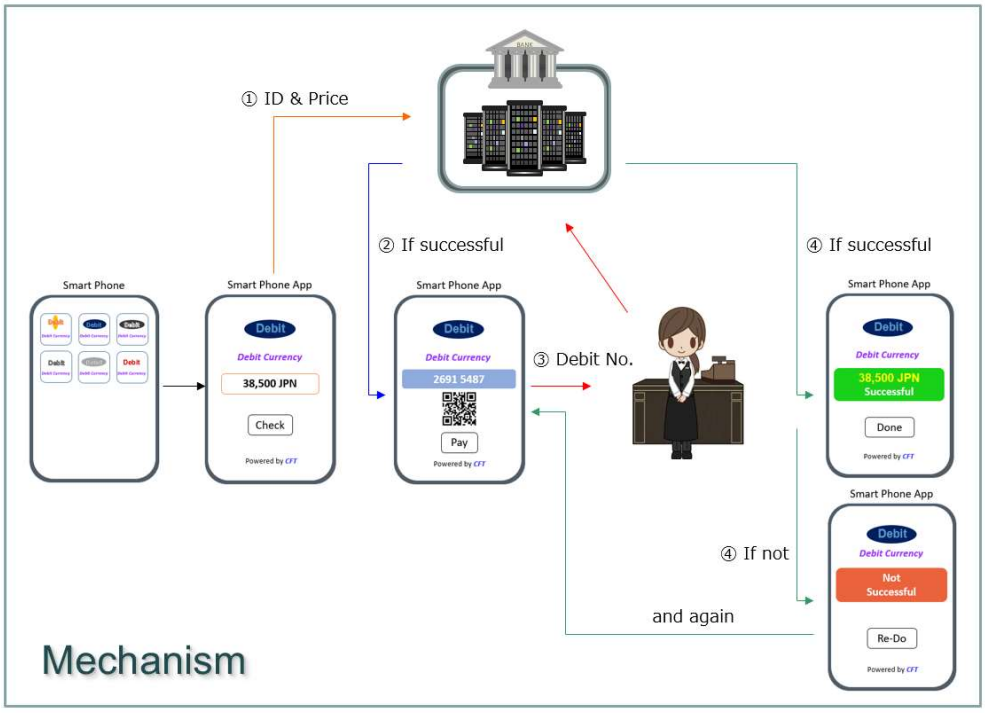
ユーザーは、DC-CC を使用するために、銀行に普通口座を開設し、DC-CC 専用アプリを例えば自らのスマートフォンにインストールし、銀行より秘密裏に与えられたパスコードでアクティベートして準備した上で DC-CC を以下の手順で使用する。

① スマートフォンのデビットカード型 Crypto Cash アプリを起動して、例えば決済する金額 38,500 円（例）を入力し、ID と共に銀行サーバーへ送信する。

② もし残高が十分あれば銀行サーバーはスマートフォンのアプリに発行許可を与え、スマホ上のアプリは 5 分だけ有効で 38,500 円丁度の金額を決済できる 1 回きり使用可の 8 桁のデビット番号を発行する。このデビット番号は、例えば、38,500 円という価値を特定する情報を暗号化したものである。

③ この番号をお店に伝え、お店はこの番号をそのまま銀行サーバーに送信する。

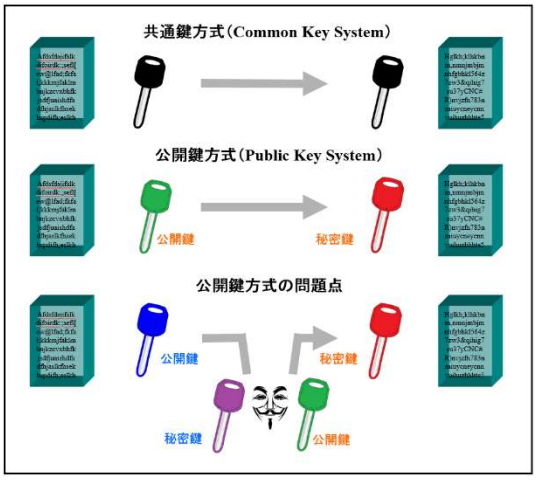
④ 決済が成功裏に終われば、ユーザーとお店の双方に決済終了のシグナルが送られそこで終了するが、失敗したらデビット番号を再発行してやり直す。



参考 1：公開鍵暗号方式とその欠陥

公開鍵暗号は、現在インターネットセキュリティを中心に、最も広く使用されている暗号方式である。暗号者と復号者の間で暗号鍵を事前に共有しなければならない共通鍵方式の最大の問題点である「暗号鍵の配送問題」を克服するため、1970 年代に、英国においてはジェームス・エリス（James Henry Ellis、1924 - 1997）とクリフォード・コックス（Clifford Christopher Cocks、1950 - ）及びマルコム・ウイリアムソン（Malcolm John Williamson、1950 - ）によって、米国においてはスタンフォード大学のホイットフィールド・ディフィー（Bailey Whitfield Diffie、1944 - ）とマーティン・エドワード・ヘルマン（Martin Edward Hellman、1945 - ）によって考案された。公開鍵方式では暗号化する暗号鍵と復号化する暗号鍵が異なるペアによって構成される。公開鍵で暗号化した暗号文はこれと一対をなす秘密鍵によってしか復号化できない。もしこのような一対の鍵が存在するならば、秘密鍵を持つ側に送信される情報はすべて公開鍵によって暗号化されれば、唯一秘密鍵を持つ者だけしか復号化できない。万一ハッカーが公開鍵を手に入れたとしても復号化はできないのである。その結果、公開鍵は誰にでも公開しておきいつでも使えるようにしておくことができるので、公開鍵方式（PKS）と呼ばれるようになった。

一般に、公開鍵から秘密鍵を導き出すのに、現実的には不可能なくらいのコンピューティングパワーと時間が必要とされ、よって実質上解読できないとされてきた。RSA 暗号においては、「素因数分解問題」、楕円曲線暗号においては「楕円曲線離散対数問題」と呼ばれる数学的問題を利用している。ところが、共通鍵方式に比べて長大な暗号鍵を用いるため計算時間が膨大に必要で、共通鍵方式の暗号鍵の配送に用いられることが多くなり、現在では「暗号鍵の配送問題」を解決した暗号方式と考えられるようになっている。公開鍵方式では公開鍵を予め公開しておけるので、インターネット時代に最適で、電子入札や SSL、ブロックチェーンなど、広く使われている。そのため、コンピューティングパワーが向上するにつれて解読の可能性が高まるため、その都度脆弱性を克服するために鍵長を長くする試みが行われてきた。しかし、いよいよ量子コンピュータ時代を迎えるにあたり、鍵長を長くするだけでは解決できなくなり、前述の通り、米国 NIST などが、量子コンピュータ時代以後にも使える耐量子コンピュータ暗号の新しい標準アルゴリズムに取り組み始め、新たなアルゴリズムの募集を行っているのである。



しかしながら、さらに根本的な問題として、公開鍵の真正性の保証が容易ではないという問題が露見し、現在では、信頼できる第三者機関（Trusted Third Party、TTP）が発行する公開鍵証明書※4 を用いる公開鍵基盤（PKI）と呼ばれる方法が考案され広く使われている。ところが、証明書をいくらつけても、さらに証明書の証明書であるルート証明書を用いても、偽造が防げないことが明らかとなっており、当初期待された「暗号鍵の配送問題」さえも、決して解決されないことが判明している。

参考 2：完全暗号技術

暗号技術は古来、暗号アルゴリズムと暗号鍵から構成される。暗号を強化するためには、①暗号アルゴリズムをもっと複雑にするか、②暗号鍵の場合の数を増やすことが考えられる。ところが、①、②のどちらの方法を極めても、解読不可能な暗号は作れない。現在の暗号技術のほとんどは、解読困難性を解読に膨大な計算量が必要であることを拠り所としており、決して解読不可能とは言えない。それゆえ、コンピュータの性能が向上すると、解読される可能性が高まるので、より難解な暗号アルゴリズムを用いたり、暗号鍵長を長くして場合の数を増やすように変更したりする必要があり、その都度対応してきた。近未来の量子コンピュータ時代においては、やがて理論的に解読不可能な暗号技術が求められる。

この人類史上の難問に答えを出したとされるのが、AT&T に勤務していたギルバート・ヴァーナム（Gilbert Sandford Vernam、1890 - 1960）によって 1918 年に考案されたる暗号方式であり、1949 年にクロード・シャノン（Claude Elwood Shannon、1916 - 2001）によって、ある条件下において解読不可能であることが証明され、ヴァーナム暗号またはワンタイムパッドと呼ばれる。事前に暗号者と復号者の間で共有する暗号鍵が、ランダムで、かつ、その鍵の長さが送信される平文と同じかそれ以上の長さを持つ場合に、解読不可能となる。ところが、これほどの長さの暗号鍵を共有することは、これまで実用的でないとされてきた。平文と同じ長さの暗号鍵が共有できるのなら、平文自体を共有すればよいからである。

このように、現在、究極の暗号技術を開発する上での最終課題となっているのが、「解読不可能な暗号技術問題」と「暗号鍵の配送問題」の 2 つである。「暗号鍵の配送問題」が解決すれば、ヴァーナム暗号などの「解読不可能な暗号技術問題」を解決した暗号技術を用いることができ完全秘匿通信が可能になる。

この「暗号鍵の配送問題」を解決したとされるのが、「公開鍵方式」であったが、その後致命的な欠陥が発見された。さらにその究極のソリューションとされているのが、量子暗号を用いる量子鍵配送（QKD）であったが、量子暗号を使ってさえも、必ずしも真正な相手と通信できないという、送受信者同士の認証問題はまだ解決されていない。盗聴者が正しい受信者になりすましてしまえば、送信者と直接量子暗号を用いた通信を行い、すべての情報を手に入れたうえで、正しい情報、または虚偽の情報を正しい受信者に再送することができる。

現在、「解読不可能な暗号技術問題」と「暗号鍵の配送問題」の 2 つを解決したと証明されている完全暗号方式が存在し、”完全暗号”と呼ばれ、Crypto Cash に使われている。