クラウド通貨と Redundant Array of Independent Detection Agents

ショーン H.ワージントン
コンピュータ科学学科ビュートカレッジ
オロヴィル、アメリカ合衆国
Worthington@Butte.edu

要約

暗号通貨よりも優れた特性を持つ、新しい電子通貨を発表いたします。通貨は、人から人へと電子的に交換できる JPEG 画像またはテキストファイルの形式をとります。ユーザーは、RAIDA（Redundant Independent Detection Agents）というクラウドサーバーを使用して、偽造品を即座に検出することができます。 RAIDA は、複数のクラウドを使用しており、少数のクラウドによって検出プロセスを制御または破壊できないようにします。 通貨の価値と安定性は、RAIDA の完全性と信頼性に依存します。

前書き

ビットコイン、その他の暗号通貨の成功により、お金の本質が何であり、完璧な電子通貨とは何なのかという疑問がこの研究の動機になりました。情報システム的アプローチを採用し、クラウドネットワークのグループ内における信頼と完全性に基づく通貨システムが実装されました。 結果として得られるシステムはビットコインよりも優れたパフォーマンスがありました。

仮説

お金とはデータである

最初の仮説は、私たちが保持するお金であるトークン、すなわち紙幣やコイン、請求書、銀行口座の数字は実際にはより大きなシステムの一部であり情報システムだということ。具体的に言えば、人々の間で物理的に実装された分散データベースであり、私たち個々人がデータの小さな部分を保持しているということ。私たち個人は、私たちの頭を使って、自分のお金で提供される情報を処理して有益に利用します。我々は、価格によってお互いに重要な情報を伝えます。お金と私たちの行動の間の相互作用は、効率的な経済を作り出すために、私たちの行動を自発的に組織化することを可能にします。

お金の本質的特徴は偽造通貨でないこと

第二の仮説は、金銭の価値は、それが作られた物質から生じるのではなく、それを模倣するために必要な努力とデータとしての完全性から生じること。金貨、紙幣、ビットコインはすべて異なったものから作られていますが、それらはすべてお金として使われており、そのすべてが価値を持っています。金、紙幣、ビットコインで作られた通貨システムは、偽造することは非常に困難ですが不可能ではありません。金は採掘して鋳造すれば二重のコインにすることができます。紙幣は偽造専門家や財務省自身が印刷することができます。ビットコインはパズルを解くことによって "採掘"することができます。しかし、「完璧な」お金は偽造することはできません。

実験設計

お金の本質的な属性は、偽造品を作ることができないものである、という仮説に基づいて偽造品の検出を提供するプロセスを開発し実装した。仮説 「お金はデータである」が真であると仮定すると、通貨システムは、データベースがそのデータ整合性を与えるように設計されるのと同じ方法で、お金の完全性を与えるように設計されなければならない。データの完全性という一般的な目標を達成するために、独立した多国籍の組織のコンソーシアムによって管理される、冗長で堅固なクラウドが設計されました。このシステムは最終的に、RAIDA と名付けられました。CloudCoin コンソーシアムが組織され、デジタル通貨が発行され、RAIDA に配備されたことは注目に値します。そして、クラウドを元にする認証システムについて特許が申請されています。

この通貨の動作に関する簡単な説明

私は 25 個のランダムな GUID（グローバル UID：グローバルに一意の識別子）が埋め込まれた JPEG イメージを持っています。この JPEG を CloudCoin と呼びます。各 RAIDA クラウドは 25 個の GUID のうちの 1 つを知っています。私は、コンソーシアムが作成した簡単な無料のオープンソースソフトウェアを使用して、RAIDA と並行して GUID を認証することで、私

が所有者であることを証明することができます。私があなたから何かを購入したいのであれば、私はあなたに JPEG 画像を提供します。そして今私たちは両方とも秘密の番号を知っています。 秘密の番号を知っている人は誰でも RAIDA に連絡すれば変更できます。 これであなたの秘密の番号に変更することができます。 そうすれば、あなたは CloudCoin の所有者になり、私はもはや RAIDA に登録された番号を知りえません。

クラウド通貨の構成要素

システムの 3 つの主要コンポーネントは、eMint、CloudCoin、RAIDA です。

eMint：CloudCoin を作成し、初期所有者に分散して RAIDA に登録するもの。ミント（鋳造の意）処理が完了すると、結果データと共に eMint が破棄されます。eMint 後、システム内の金額は増減しません。

CloudCoin：偽造されないようにするコードを含む電子マネーとして使用される JPEG 画像。コードには以下が含まれます：

SN（シリアル番号）：IP アドレスのようなドット小数で表示される 32 ビットの数値（例：1.210.84.52）。SN は、お金の金種を決定し、RAIDA クラウドがそれを格納し保護するのに役立ちます。 SN の最初の 8 桁はネットワークアドレスで、CloudCoin がどの RAIDA に属しているかを示します。所属 RAIDA は 1 つだけです。しかし、CloudCoin があまりにも価値が高くなると、ネットワークは倍増・複製され、すべての所有者は以前の 2 倍の金額になります。この倍増は 8 回発生する可能性があり、毎回システムにフォールトトレラントを追加します。次の 8 桁はサブネットです。これにより、ユーザーとソフトウェアは通貨の種類を特定し、より価値の高い通貨を保護するための措置を講じることができます。最後の 2 桁はアドレスです。アドレスの長さは、システム内の通貨単位の正確な量を固定します。

AN（認証番号）：通貨の所有者と異種の RAIDA クラウドにのみ知られている 16 バイト長のランダムに生成された 2 進数。プライマリ RAIDA クラウドごとに 1 つずつ、２５個の AN があります。 パリティ情報クラウドは、これらの AN に基づいて計算され、RAIDA パリティクラウドによって格納されます。

金種：例えば、サブネットの値が 96 と 255 の間の通貨はすべて金種 250 の CloudCoin です。金種は、1、5、25、100、250 の 5 種類があります。（システム上で個々の金種の量は固定されています。金種は SN のサブネット部分と対応しています）

RAIDA（Redundant Array of Independent Detection Agent=独立エージェントの冗長アレイ）：
偽造通貨検出システムとして機能する分散ストレージシステム検出システム。フォールトトレランス、高可用性。CloudCoin の信頼性を高めるための分散型管理システム。 RAIDA には 25 のクラウドがあります。RAIDA はクラウドがオフラインになると、新しいクラウドが素早くそのクラウドに置き換わります。各クラウドは「センチネル（見張り）」クラスターであり、その後ろに 32 個の「検知エージェント」が隠れています。少なくとも 9 つのクラウドオペレータが検知されずに結託して作業しなければ、システムを破壊することはできません。RAIDA は他の認証システムとは異なり、25 個のユニークな CloudCoin スライスが平行して認証します。ただしコインは、それらのすべてで認証する必要はありません。

RAIDA の構成部品は次のとおりです。

PAN（Proposed Authenticity Number）：純正の CloudCoin の所有者が作成したランダムに生成された長さ 16 バイトの 2 進数。

RAIDA クラウド（偽造検出エージェント）：
CloudCoin の真正性番号を検証し、CloudCoin のトレード中に提案された真正性番号で置き換えることができるクラウドベースのサービス。取引プロセスは「パスワード所有」と呼ばれ、単語「pown」がそれを記述するために発明されました。RAIDA は、「トリプルケルベロス（Triple Kerberos）」システムを利用して、自己修復のために論理的に配置されています。これは、破砕された RAIDA クラウドが自己の真正性番号を、他の 3 つの RAIDA クラウドを信頼することで可能になっています。この目的は、RAIDA クラウドが破壊されたか、または使用できなくてもデータが失われないようにすることです。"破砕された"という語は、他のすべての RAIDA クラウ

ドが認証しているのに、ある RAIDA クラウドが認証しないことを意味します。

偽造検知要求：偽造の検出と所有権の変更を要求する暗号化されたメッセージ。このメッセージには、名称、シリアル番号、認証番号、提案された認証番号が含まれています。

偽造検出応答：CloudCoin が偽造品であるかどうかをクライアントに伝える暗号化されたメッセージ。

取引のプロセス（powning）

CloudCoin は現在のオーナーから別のオーナーへ電子的に渡されます。所有候補者は、信頼できるソフトウェアで CloudCoin JPEG ファイルを開き、CloudCoin の金種が意図される金種と一致するかどうかを確認します。これは、小さい金種を高い金種に変換することを阻止します。 CloudCoin の名称は、シリアル番号のサブネット部分を調べることで判断できます。差異がある場合、取引は終了します。金種が品目と一致する場合には、プロセスを続行します。所有候補者は、２５の RAIDA クラウドに偽造検知要求をを送信します。

偽造検知要求には、金種、シリアル番号、および対応する認証番号が埋め込まれます。クラウドは、送信された真偽番号データが、保管中の金種とシリアル番号と一致するかどうかを確認します。 数字が一致しない場合、偽造品として反応し、そうでなければ真正 CloudCoin として応答します。こうして所有候補者は、CloudCoin が偽造品でないことをチェックし、所有権を得ます。所有候補者のソフトウェアは、AN を置き換えるために 25 個のランダム PAN（Proposed Authenticity Number）を生成します。所有候補者は、25 個の RAIDA クラウドに所有権移動要求を送信します。各要求には、金種、シリアル番号、対応する AN（真正性番号）および PAN（提案された真正性番号）またはそれらの対応するパリティデータが埋め込まれています。

RAIDA 内の２５の検出エージェントは、認証番号データが、そのストレージ内にある名前とシリアル番号と一致するかどうかを確認します。番号が一致すると、格納されている認証番号が PAN に置き換えられます。この時点で、所有候補者だけがこれらの番号をすべて知っているので、所有候補者は新しい所有者になりります。次に、新しい所有者は新しい秘密の真正性番号を反映する変更されたバージョンで元の JPEG を上書きします。

冗長性の修正

RAIDA クラウドは必ずしも 100％利用できない可能性がありますが、RAIDA クラウドの 10 台だけが認証に必要であるため、これは問題ではありません。RAIDA クラウドの一部が CloudCoin が偽造品であると応答すると、これらのサーバーはクライアントが冗長性修正要求を発行することによって訂正できます 冗長性修正要求は、ケルベロスのフォーマット形式を使用して、RAIDA クラウドが CloudCoin 所有者を介して暗号化されたデータを送信できるようにします 暗号の鍵は RAIDA クラウドの冗長パートナーに知られています。CloudCoins の認証データは、CloudCoin ファイル自体に格納されます。CloudCoin の冗長性は、ユーザによって制御されます。

実験

オーストラリア、マケドニア、フィリピン、セルビア、ブルガリア、フランス、スイス、英国、インド、アメリカ、スウェーデン、カナダ、ルーマニア、台湾、ロシア、コロンビア、シンガポール、ドイツ、ベネズエラ、ウクライナ、ルクセンブルクにおいて、異なる国籍の 20 人の RAIDA 管理者が募集され、25 のクラスタが設定されました。このプロセスは完了するのに 3 ヶ月を要しました。

オペレーティングシステムは、Microsoft Windows や、さまざまなバージョンの Linux で構成されていました。RAIDA プロトコルは aspx と php で実装されました。CloudCoin コンソーシアムポケットバンクという Android アプリケーションを含むクライアント側のソフトウェアが作成されました。 CloudCoins は、アプリケーションを使用して 5 人の異なるユーザーに電子メールで渡されました。 各人は CloudCoins の所有権を取得しました。実験中、RAIDA5 番サーバーの管理者が自分のコンピュータの付近で亡くなっているのが発見されるという事件がありました。このため、RAID5 のデータは管理不能になりました。RAIDA から RAIDA5 を取り出し、新しい RAIDA5 を実装しました。 テスト中の CloudCoins が破損していました（破損しているということは、すべての認証番号が認

証されていないことを意味する）。しかし、数秒でシステム設計通り各 CloudCoin は自己修正することができました。実験は 2017 年 2 月 4 日に終了しました。

このように、CloudCoin は電子通貨として有用であることが証明されました。そして、RAIDA の発明は新しいフォールトトレラントな認証システムとして動作することが証明されました。RAIDA は、Bitcoin が使用するブロックチェーンよりも優れた性能を発揮しました。なぜなら、RAIDA はトランザクションを実行するのに 2 秒以下しかかからなかったからです。RAIDA にはユーザーアカウントやソフトウェアのダウンロードが必要ありません。取引は、Bitcoins のような半秘密取引ではなく、100％のプライベート取引でした。 RAIDA 技術については、すでに USPTO に特許が提出されています。
"CloudCoin"と言う名前は、登録商標の手続きがされています。CloudCoin コンソーシアムは現在、CloudCoin をグローバル通貨として提供する準備を進めています。RAIDA は紛失した CloudCoin のクリーンアップによって資金提供されますので、取引は無料で提供されます。

結論

CloudCoin クラウドベースの通貨が実際の通貨として受け入れられるようになるかどうかはまだ分かりません。しかし、クラウド通貨という概念には、暗号通貨よりも優れていると思われる機能があります。 CloudCoin などのクラウド通貨はユーザーアカウントを必要とせず、CloudCoin の最後の取引の月を除くすべてのユーザーデータを収集または追跡しないため、CloudCoin は Bitcoin よりも秘密保持機能が高い可能性があります。CloudCoin は暗号化に依存しないため、CloudCoin の方がはるかに高速であり、二重の使用は不可能と思われます。また、CloudCoin は近い将来に問題になる可能性のある「量子コンピュータ解読」からも安全であると思われます。また、CloudCoin のインフラは、RAIDA プロバイダが、紛失した CloudCoin（CloudCoin を使用したり、何年もチェックしていない CloudCoin）を掃除して、その管理に費用を支払うことができるようにすることで、自己資金提供が可能です。
CloudCoin のようなクラウド通貨は特別なソフトウェア、財布、データを必要としないので、非常に使いやすくなっています。JavaScript を実行する単純な Web ページは、交換を可能にするために必要なすべてのクライアント側のソフトウェアを提供できます

RAIDA の存在の証拠は、オンラインテスター http://CloudCoin.co/detect.html または RAIDA の機能をテストするために使う、ダウンロード可能なプログラムを調べることで理解することができます。 このようなプログラムは、github.com から「RAIDA Tester」を検索してダウンロードできます。CloudCoin のガバナンスについては、http://CloudCoinConsortium.org にあります。その他の有用なウェブサイトには http://CloudCoinConsortium.com が含まれています。CloudCoins を交換するためのオープンソフトウェアは github からダウンロードできます。RAIDA は、いかなる組織体によっても所有または管理されておらず、理論上は破壊することができません。

参考資料：

1. Nakamoto. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System.[Online]. Available: http://www.cryptovest.co.uk

2. Eyal and E Gun Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable", in Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, pp. 436-454