INTRODUCING CLOUD CURRENCIES
And
THE REDUNDANT ARRAY of INDEPENDENT DETECTION AGENTS

Sean H. Worthington
Department of Computer Science
Butte College, Oroville, CA United States of America
WorthingtonSe@Butte.edu

Abstract - A novel electronic currency with superior characteristics to cryptocurrencies is introduced. The money takes the form of JPEG images or text files that can be passed from person to person electronically. Users can instantly detect counterfeits by using a novel grouping of server clouds called RAIDA (Redundant Array of Independent Detection Agents). The RAIDA employs multiple clouds to ensure that the detection process cannot be controlled or destroyed by a minority of cloud entities. The value and stability of the currency depend upon the integrity and trustworthiness of the RAIDA.

Keywords - Electronic money; Economics; Electronic commerce; International trade.

INTRODUCTION

With the success of Bitcoin [1] and other cryptocurrencies, the question of what the essence of money is and what would be a perfect electronic currency drives this research. An information systems approach has been employed and a monetary system based on the trust/integrity of a group of cloud networks have been implemented. The resulting system performs better than Bitcoin.

THE HYPOTHESES

Money is Data - The first hypothesis is that money, the tokens we hold, the coins, bills, and numbers in our bank accounts are part of a bigger system - an information system. Specifically, a distributed database that is physically implemented among people. Each one of us oversees holding a small part of the data. Each one of us uses our minds to process the information provided by our own money to economize. We communicate key information to each other via prices. The interaction between money and our behavior allows us to spontaneously organize our behavior to create an efficient economy.

No Counterfeits **-** The Essential Characteristic of Money. The second hypothesis is that the value of money does not arise from the substance that it is made of but from the effort required to counterfeit it and its integrity as data. Gold coins, paper dollars, electronic Bitcoins are all made of different stuff and yet they are all used as money, and all of them are valuable. Monetary systems made of gold, paper money and Bitcoin are very difficult to counterfeit but IT IS not impossible. Gold can be mined and minted into duplicate coins.

Paper money can be printed by expert counterfeiters and by a treasury itself, Bitcoins can be "mined" by solving puzzles [2]. However, "perfect money" cannot be counterfeited.

EXPERIMENT DESIGN

Building on the hypothesis that the essential attribute of money is that it cannot be counterfeited, a process was developed and implemented to provide for the detection of counterfeits.

Assuming the hypothesis "money is data" is true, a monetary system was designed to give its money integrity in the same way that a database would be designed to give its data integrity. To achieve the general goal of data integrity, a redundant and robust system of clouds governed by a consortium of independent multinational organizations was designed. The end result is called RAIDA. It should be noted that a patent was filed for Cloud-Based authentication systems, a "CloudCoin Consortium" was created and a digital currency was minted and deployed in the RAIDA.

SIMPLE EXPLANATION OF HOW THE CURRENCY WORKS

I have a JPEG image with twenty-five random GUIDs (Globally Unique Identifiers) embedded in it that only I know. We call this JPEG a CloudCoin. Each RAIDA cloud knows one of the twenty-five GUIDs. I can prove to you that I am the owner by authenticating the GUIDs in parallel with the RAIDA using simple free open-source software made by the Consortium.

If I want to buy something from you, I will give you the JPEG image and now we both know the secret numbers. Anyone who knows the secret numbers can change them by contacting the RAIDA. Now you can use the secret numbers to change them to your own secret numbers. Now, you are the owner of the CloudCoin, and I no longer know the numbers registered in the RAIDA.

COMPONENTS OF THE CLOUD CURRENCY

The three major components of the system are the e-Mint, CloudCoin, and the RAIDA.

e-Mint*:* The entity that creates the CloudCoin, disperses it to the initial owners and registers them in the RAIDA. After the minting process is complete, the *eMint* is destroyed along with any resulting data. After minting, the amount of money in the system will not increase nor decrease.

CloudCoin: JPEG images used as electronic money that contain codes that prevent them from being counterfeited. The codes include:

- ***SN (Serial Number):*** A 32-bit number displayed in dot-decimal like an IP address (e.g. 1.210.84.52). the SN is used to determine the denomination of the money and help the RAIDA clouds store and protect it. The first octet of the SN is the network address and shows which RAIDA the CloudCoin belongs to. There is now only one RAIDA. However, should CloudCoin become too valuable, the networks are to be doubled/replicated so that all owners will have twice the money they had before. This doubling can occur as many as eight times, each time adding more fault tolerance to the system. The second octet is the subnet. This allows users and software to identify the denomination of the currency and take measures to protect more valuable currencies. The last two octets are the address. The length of the address fixes the exact number of monetary units in the system.

- ***ANs (Authenticity Number***): Randomly generated binary numbers 16 bytes in length only known to the owner of the currency and the disparate RAIDA Clouds. There are 25 ANs, one for each primary RAIDA Cloud. Parity information is calculated based on these ANs to be stored by the RAIDA Parity Clouds.

- ***Denomination***: There is a fixed amount of each denomination of currency in the system.
  These denominations correspond to the subnet portion of the SN. For example, any currency with a subnet between 96 and 255 is a 250 CloudCoin unit.
  Denominations come in 1's, 5's, 25's, 100's and 250's.

RAIDA (Redundant Array of Independent Agents):

A distributed storage system that works as a Counterfeit Detection System and provides fault tolerance, high availability, and decentralized management in order to create trust in the CloudCoin. The RAIDA has 25 Clouds. The RAIDA is designed so that if clouds go offline, new clouds can quickly be brought in to replace them. Each Cloud has a "sentinel" cluster that hides 32 "Detective Agents" behind it. At least nine of an exact arrangement of cloud operators would need to collude undetected to corrupt the system. The RAIDA is unique because unlike other authentication systems, there are twenty-five unique CloudCoin slices that authenticate in parallel. The coin need not authenticate with all of them. The components of the RAIDA include:

- ***PAN (Proposed Authenticity Number):*** A randomly generated binary number 16 bytes in length created by the person who is taking ownership of the purported genuine CloudCoin.

- ***RAIDA Cloud (Counterfeit Detection Agent):*** A cloud-based service that verifies a CloudCoin's Authenticity Number and can replace it with the Proposed Authenticity Number during CloudCoin exchanges. The exchange process is called "Password Owing" and the word "pown" was invented to describe it. The RAIDA is logically arranged for self-repair by adding a system of "Triple Kerberos" that allows fracked RAIDA Clouds to change their stored authenticity numbers by trusting three other RAIDA Clouds that do authenticate. The purpose is to ensure that data is not lost even if a RAIDA cloud is destroyed or unavailable. The word "fracked" was invented to mean a RAIDA cloud that does not authenticate a coin while all the other RAIDA clouds do.

- ***Counterfeit Detection Request*:** An encrypted message that triggers counterfeit detection and ownership change. The message includes the Denomination, Serial Number, Authenticity Number, and Proposed Authenticity Number.

THE PROCESS OF EXCHANGE (POWNING)

The CloudCoin is passed electronically from the Current Owner to the Candidate Owner.

The Candidate Owner opens the CloudCoin JPEG file in software that they trust and checks the denomination on the CloudCoin to see if it matches what the CloudCoin is purported to be. This thwarts any attempts to pass smaller denominations as higher denominations. The denomination of a CloudCoin can be determined by examining the subnet part of its serial number. If there is a difference, then the transaction ends. If the denomination matches the item, then process proceeds.

The Candidate Owner sends a Counterfeit Detection Request to twenty-five data holding RAIDA clouds. Embedded in the request are the denomination, serial number, and corresponding authenticity number. The clouds will see if the authenticity number data sent to them agree with the denomination and serial number that they have in their storage. If the numbers do not match, then they respond as Counterfeit otherwise they respond as Authentic. Now the

Candidate Owner knows the currency is authentic and they can take ownership. The Candidate Owner's software generates twenty-five random PANs (Proposed Authenticity Numbers) to replace the ANs. The Candidate Owner sends a Take-Ownership-Request to the twenty-five RAIDA clouds. Embedded in each request are the denomination, serial number, the corresponding AN (Authenticity Number) and the PAN (Proposed Authenticity Number) or their corresponding parity data.

25 detection agents in the RAIDA will see if the Authorization Number data matches the Denomination and Serial Number that it has in its storage.

If the numbers match, then the stored Authenticity Numbers will be replaced with the Proposed Authenticity Numbers. Now, only the Candidate Owner knows all these numbers, hence the Candidate Owner becomes the new Owner. The new Owner then writes over the original JPEG with a modified version that reflects the new secret Authenticity Numbers.

FIXING REDUNDANCY

It is likely that the RAIDA clouds will not be available 100% of the time. This is not a problem as only 10 of the RAIDA clouds are necessary for authentication.

If some of the RAIDA clouds respond that the CloudCoin is counterfeit, these servers can be corrected by the client issuing Fix Redundancy Requests. The Fix Redundancy Requests use a form of Kerberos to allow RAIDA clouds to send encrypted data through the CloudCoin owners. The keys for the encryption are known to the RAIDA cloud's redundancy partners. The authentication for the CloudCoin is stored in the CloudCoin files themselves. The redundancy of the CloudCoin is controlled by the user.

THE EXPERIMENT

Twenty RAIDA Administrators of different nationalities were recruited and Twenty-five clusters were set up in the following countries: *Australia, Macedonia, Philippines, Serbia, Bulgaria, France, Switzerland, United Kingdom, India, USA, Sweden, Canada, Romania, Taiwan, Russia, Columbia, Singapore, Germany, Venezuela, Ukraine and Luxembourg.* This process required three months to complete.

Figure 1: CloudCoin with embedded Authenticity codes.

The operating systems consisted of Microsoft Windows and variations of Linux. The RAIDA protocol was implemented is ASPX and PHP. Client-side software was created including an Android application called CloudCoin Consortium Pocket Bank. CloudCoins were passed by email through five different people using the applications. Each person took ownership of the CloudCoins. During the experiment, unfortunately, the administrator for RAIDA #5 was found dead at his computer. Because of this, RAIDA #5's data became unmanageable. RAIDA #5 was taken out of the network and a new RAIDA # 5 was implemented. The CloudCoins in the test became fracked (fractured meaning that not all the Authenticity Numbers authenticated). However, within seconds, each CloudCoin was able to fix itself as the system was designed. The experiment concluded on February 4th, 2017.

In this way, CloudCoin has been shown to be useful as an electronic currency and that the RAIDA invention works as a new fault-tolerant authentication system. The RAIDA performed much better than the block-chain used by Bitcoin because the RAIDA required less than two seconds to perform a transaction. The RAIDA required no user accounts or large software as opposed to semi-private with Bitcoins. A patent has been filed for the RAIDA technology with the USPTO. A Trademark claim has been filed for "CloudCoin" The CloudCoin Consortium is now preparing to provide CloudCoins as a global currency and transactions will be offered for free as the RAIDA will be funded by the scavenging of lost CloudCoins.

CONCLUDING REMARKS

It has yet to be seen whether the CloudCoin cloud-based currency will become accepted as real currency. However, the concept of a cloud currency has features that would make it superior to cryptocurrencies. Because cloud currencies such as CloudCoin do not require any user accounts and do not collect or track any user data (except the month of a CloudCoin's last transaction), CloudCoin is more private than Bitcoin [3]. Because CloudCoin does not depend on encryption and it is impossible to double spend.
CloudCoin is safe from quantum computer decryption which may become an issue soon. Also, the infrastructure of CloudCoin can be self-funded by allowing RAIDA providers to scavenge lost *CloudCoins (CloudCoins that have not been spent or checked in years*) to pay for their operations. Cloud Currencies like CloudCoin do not require special software, wallets or data and thus are much easier to use.
Simple web pages running JavaScript can provide all the necessary client-side software to make exchanges possible.

Proof of the existence of the RAIDA can be found by looking at an online tester: http://CloudCoin.co/detect.html or a downloadable program used to test the functioning of the

RAIDA Programs like this can be downloaded by searching for "RAIDA Tester". https://github.com/CloudCoinConsortium

The RAIDA is not owned or controlled by any entity and cannot be destroyed. http://raidatech.com/

Open Source software for exchanging CloudCoins can be found at: https://github.com/CloudCoinConsortium

Governance of CloudCoin can be found at: http://CloudCoinConsortium.org.

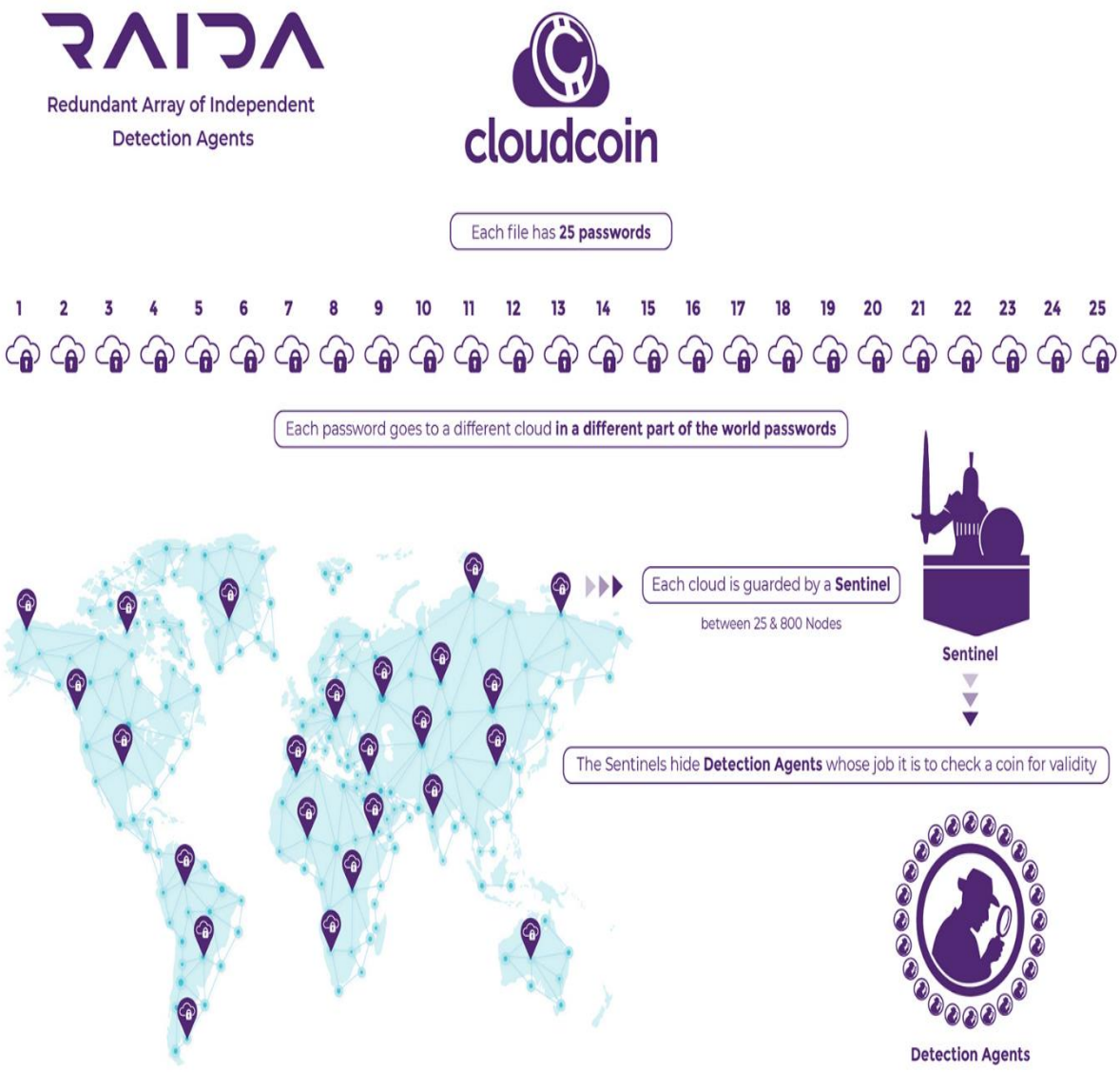
Other helpful websites include:
http://CloudCoinConsortium.com.
https://cloudcoin.global

REFERENCES

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

RAIDA Example One.



RAIDA Example Two.