Provisional Patent Application Number 62354022

Electronic Filing System ID	26160325
Application Number	62354022
Confirmation Number	8528
Title of Invention	A Counterfeit Detection Process That Can Be Used as an Electronic Monetary System
Listed Inventors	Sean H. Worthington
Docket Number	TPP30944
Receipt Date	23-JUN-2016
Time Stamp	18:48:05
Application Type	Provisional
Documents Filed	Specification Drawings – only black and white line drawings Micro Entity Status Certification Provisional Cover Sheet Fee Worksheet

A Counterfeit Detection Process That Can Be Used as an Electronic Monetary System

FIELD OF THE INVENTION

The present invention relates generally to a method and apparatus for counterfeit-proof currency. More specifically, the process of the present invention allows one to make electronic or paper money that cannot be counterfeited

BACKGROUND OF THE INVENTION

The process of the present invention allows one to make electronic or paper money that cannot be counterfeited. The process provides a fault tolerant monetary system that is highly available and - like the Internet itself - cannot be taken offline by force, surveilled or tampered with. The process provides the ability for money to change hands over the Internet without intermediate banks thus the process reduces transaction costs and creates privacy. The paper version of the money can also be inserted into - or written directly on to - products (like shoes, handbags and fine art) to stop counterfeiting. This will reduce counterfeiting worldwide and allow for the creation of more perfect monetary systems that work over the Internet without banks.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flow chart diagram detailing the present invention
FIG. 2 is a flow chart diagram detailing the present invention

DETAIL DESCRIPTIONS OF THE INVENTION

All illustrations of the drawings are for the purpose of describing selected versions of the present invention and are not intended to limit the scope of the present invention.

The process of the present invention allows one to make electronic or paper money that cannot be counterfeited. The process provides a fault tolerant monetary system that is highly available and - like the Internet itself - cannot be taken offline by force, surveilled or tampered with. The process provides the ability for money to change hands over the Internet without intermediate banks thus the process reduces transaction costs and creates privacy. The paper version of the money can also be inserted into - or written directly on to - products (like shoes, handbags and fine art) to stop counterfeiting. This will reduce counterfeiting worldwide and allow for the creation of more perfect monetary systems that work over the Internet without banks.

The present invention creates money that is marked with codes which can be checked against gangs of trusted servers on the Internet. The code is updated every time the item is checked for counterfeit. The servers act as an array of independent agents with each one having a small part of the detection job but they themselves cannot use their information to counterfeit. These servers can be spread out over the world so that no one entity can take control of the process. If some of the servers are destroyed or taken offline the system will still work because of the fault-tolerant measures built into the process.

Components:

SN (Serial Number): Binary number whose length in bits determines the maximum number of genuine articles that the process can track.

AN (Authenticity Number): Randomly generated binary number 8 bytes in length.

GA (Genuine Article): Something that is not to be counterfeited such as electronic money, paper money, handbags, shoes or fine art.

Nomenclature: The name of a Genuine Article used by people to distinguish the item from other items.

COA (Certificate of Authenticity): A static (non-changing) Serial Number paired with a dynamic Authenticity Number and a static Nomenclature. The Authenticity Number changes each time the Genuine Article changes ownership. The Certificate of Authenticity must be attached to a Genuine Article.

PAN (Proposed Authenticity Number): A randomly generated binary number 8 bytes in length created by someone who is being offered ownership of a purported Genuine Article.

Counterfeit Detection Agent: A person or computer-server that can verify that at least part of the Authenticity Number is correct and can update the stored Authenticity Numbers with the Proposed Authenticity Number each time the owner of the Genuine Article changes.

Counterfeit Detection System: A group of Counterfeit Detection Agents who together can test the entire Authenticity Number and identify a counterfeit.

RAIDA (Redundant Array of Independent Detection Agents): A distributed storage system that works as a Counterfeit Detection System and also provides fault tolerance, high availability and decentralized management in order to create trust in the Certificate of Authenticity. The simplest form of RAIDA would require three Counterfeit Detection Agents. The more Counterfeit Detection Agents in the RAIDA, the less likely it is to be compromised.

RAIDA Level: Configurations of Servers that employ the techniques of striping, mirroring, or parity to create large reliable data stores from multiple Counterfeit Detection Agents (Servers). RAID levels and their associated data formats are standardized by the Storage Networking Industry Association (SNIA) in the Common RAID Disk Drive Format (DDF) standard. See: http://snia.org/tech_activities/standards/curr_standards/ddf

eMint: The entity that creates the Certificate of Authenticity and gives them to the owner and records them in the Authenticity System's RAIDA.

Authenticity System: An anti-counterfeit system consisting of the eMint, Counterfeit Detection Agents, Counterfeit Detection Systems, RAIDA and Certificate of Authenticity that can be used as a monetary system.

Owner: Person who owns the Genuine Articles who may engage in buying and selling.

Candidate Owner: Person who is interested in taking ownership of a purported Genuine Article but would like the item's authenticity tested first.

RAIDA Provisioning Process: The process of registering Certificates of Authenticity with a newly created RAIDA. Once the process is complete, the eMint is destroyed and the RAIDA becomes closed to new serial numbers.

The Counterfeit Detection Process: The process in which a Candidate Owner can test a purported Genuine Article for Authenticity by using the Counterfeit Detection System or RAIDA.

Counterfeit Detection Request: An encrypted message that triggers counterfeit detection and, ownership change. The message includes the Nomenclature, Serial Number, RAID

formatted Authenticity Number data, and RAID formatted Proposed Authenticity Number data.

Counterfeit Detection Response: A encrypted message that indicates whether the Certification of Authenticity is counterfeit.

Steps:

There are two sup-processes: The RAIDA Provisioning Process and the Counterfeit Detecting Process.

The RAIDA Provisioning Process:

Step 1. Creation of the RAIDA

1. A RAIDA Level is specified and an appropriate number of Counterfeit Detection Agents are created based on the RAIDA format standard.

Step 2. eMint makes a Certificate of Authenticity.

1. A fixed amount of Serial Numbers are generated.
2. A matching amount of Authenticity Numbers are randomly generated.
3. The Serial and Authenticity Numbers are paired together to form Certificates of Authenticity.
4. An appropriate Nomenclature is assigned to each Certificate of Authenticity.

Step 3. The eMint sends the Certificates of Authenticity to their Owners and registers the Certificates of Authenticity in the RAIDA.

1. The eMint formats the Authenticity Number using the appropriate RAID data format standard according to the specified RAID Level.

2. The eMint sends the Serial Number, Nomenclature and the RAID formatted Authenticity Number data to the RAIDA.

3. The eMint sends the Certificates of Authenticity to the first Owners.

Step 4. The eMint is destroyed and the RAIDA is Locked.

1. All the data created by the eMint that is outside of the RAIDA is deleted permanently.

2. The RAIDA is locked so that no more Serial Numbers can be added and the serial numbers become read only.

3. A mathematical hash is generated against all the Serial Numbers stored in the RAIDA so that if any are added or deleted from the RAIDA, the RAIDA can be shown to be corrupt mathematically and reverted to a state before the corruption occurred.

The Counterfeit Detection Process:

Step 1. The Owner of Certificate of Authenticity transfers ownership (buys/sells).

1. The purported Genuine Article with its attached Certificate of Authenticity is passed from the current Owner to the Candidate Owner.

2. The Candidate Owner checks the Nomenclature on the Certificate of Authenticity to see if it matches what the Genuine Article is purported to be. If there is a difference, then the transaction ends. e.g. if the Owner identifies the purported Genuine Article to be a diamond but the Candidate Owner reads the Certificate of Authenticity Nomenclature to say the item is a pair of shoes then the diamond seller has taken a Certificate of Authenticity from shoes and put it on the diamond (Which is most likely counterfeit). If the Nomenclature matches the item, then proceed to the next step.

3. The Candidate Owner formats the Authenticity Number using the appropriate RAID data format standard according to the specified RAID Level.

4. The Candidate Owner generates a random Proposed Authenticity Number.

5. The Candidate Owner formats the Proposed Authenticity Number using the appropriate RAID data format standard according to the specified RAID Level of the RAIDA.

6. The Candidate Owner sends a Counterfeit Detection Request to the RAIDA. Embedded in the request are the Nomenclature, Serial Number, the RAID formatted Authenticity Number data, and the RAID formatted Proposed Authenticity Number data.

7. Each detection agent in the RAIDA will see if the Authorization Number data matches the Nomenclature and Serial Number that it has in its storage. If the numbers match, then the data will be replaced with the new data (from the PAN) and the Detection Agent will respond back with “Genuine!" where the blank will

be filled in with the Nomenclature. If two or more detection agents respond with matching “Genuine!” responses, then the Certificate of Authenticity is not counterfeit. Otherwise the Certificate of Authenticity is counterfeit and the Candidate Owner is informed.

8. If the Certificate of Authenticity is authentic, then the Candidate Owner becomes the Owner and must modify their Certificate of Authenticity so that Proposed Authenticity Number replaces the Authenticity Number.

How the components will be arranged and how they will work together:

- The eMint is a computer program and will talk to the RAIDA when it needs to register new money (Certificate of Authenticities). Once the eMint has done its job it can be destroyed and will no longer be part of the process.

- The RAIDA is a storage system employing many servers. Servers should be spread out all over the world in order to keep one entity from seizing control of the entire process. Serial Numbers are added to the RAIDA before it goes into service. No new Serial Numbers can be added once the RAIDA goes into service.

- The RAIDA will respond to Counterfeit Detection Requests posed by Candidate Owners of purported Genuine Articles and update Authenticity Number data in the RAIDA's internal storage. The RAIDA uses RAID Levels that have already been standardized.

- Candidate Owners have to look at the Nomenclatures on the Certificate of Authenticity first to see if it matches the item they want ownership of. Then they can send Counterfeit Detection Requests to the appropriate RAIDA to verify authenticity. If the item is good, the Candidate Owner becomes the Owner and it is their duty to update the Authentication Number to the Proposed Authentication Number.

Although the invention has been explained in relation to its preferred embodiment, it is to be understood that many other possible modifications and variations can be made without departing from the spirit and scope of the invention.

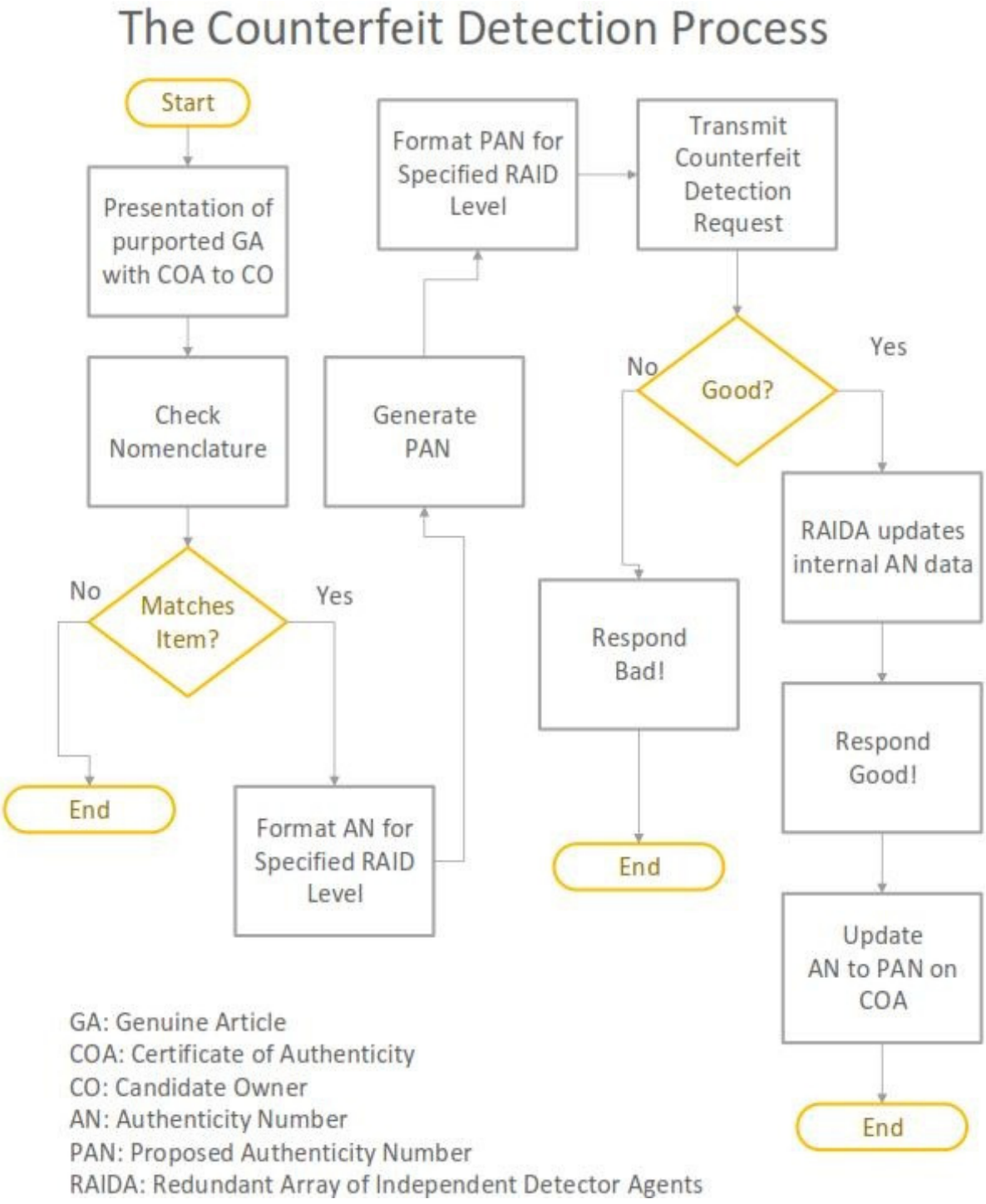
The Counterfeit Detection Process
Start
Presentation of purported GA with COA to CO
Check Nomenclature
Matches Item?
No
Yes
End
Format AN for Specified RAID Level
Generate PAN
Format PAN for Specified RAID Level
Transmit Counterfeit Detection Request
Good?
No
Yes
Respond Bad!
End
RAIDA updates internal AN data
Respond Good!
Update AN to PAN on COA
End
GA: Genuine Article
COA: Certificate of Authenticity
CO: Candidate Owner
AN: Authenticity Number
PAN: Proposed Authenticity Number
RAIDA: Redundant Array of Independent Detector Agents

FIG. 1

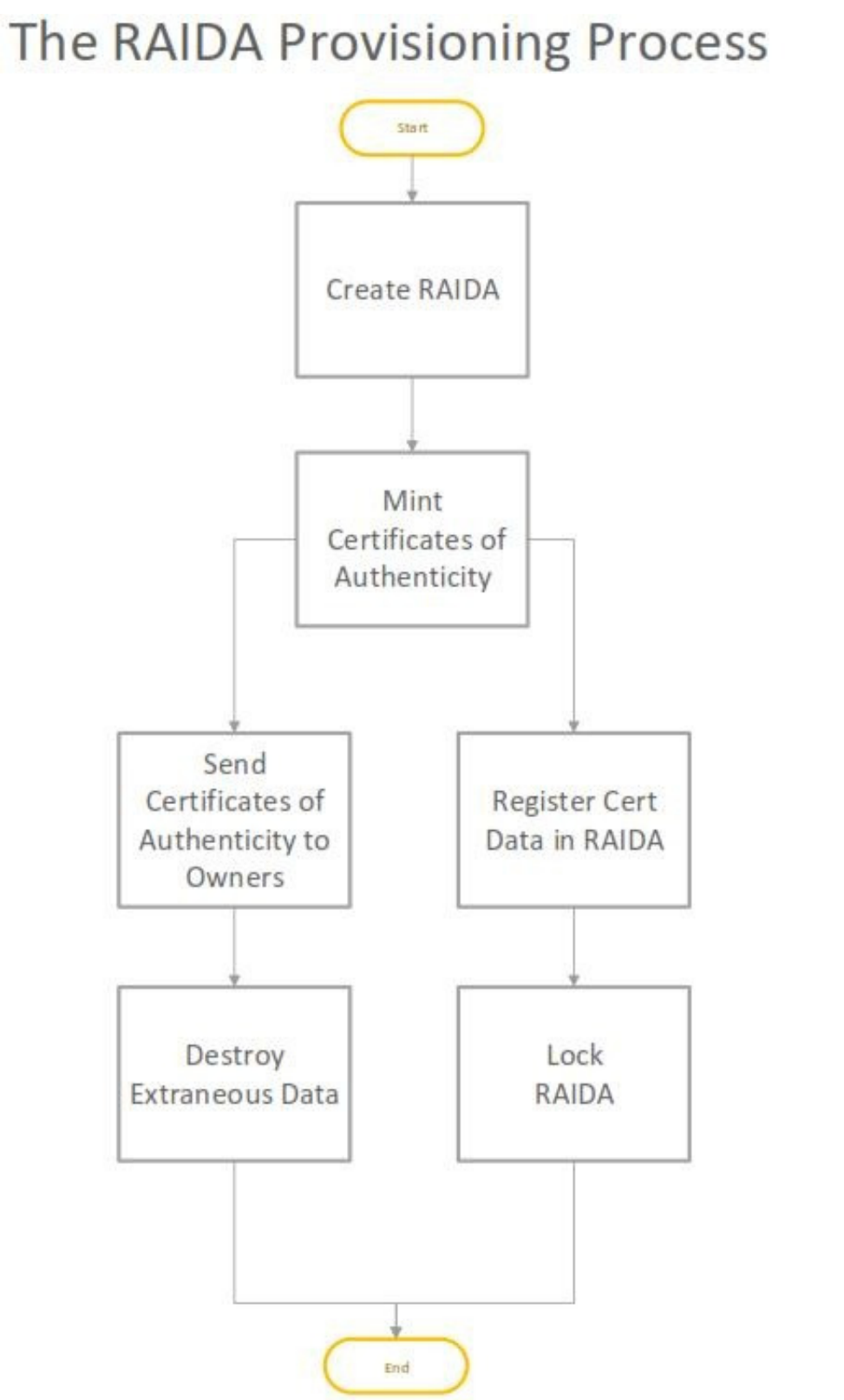
The RAIDA Provisioning Process
Start
Create RAIDA
Mint Certificates of Authenticity
Send Certificates of Authenticity to Owners
Register Cert Data in RAIDA
Destroy Extraneous Data
Lock RAIDA
End

FIG. 2

Electronic Acknowledgement Receipt

EFS ID:	26160325
Application Number:	62354022
International Application Number:	
Confirmation Number:	8528
Title of Invention:	A Counterfeit Detection Process That Can Be Used as an Electronic Monetary System
First Named Inventor/Applicant Name:	Sean H. Worthington
Correspondence Address:	Sean H. Worthington - 1445 Heritage Oak - Chico CA 95928 US - -
Filer:	Sean H. Worthington
Filer Authorized By:	
Attorney Docket Number:	TPP30944
Receipt Date:	23-JUN-2016
Filing Date:	
Time Stamp:	18:48:05
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$65

RAM confirmation Number	5343
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Provisional Cover Sheet (SB16)	ProvisionalSb_TPP30944.pdf	3603079 b1037e37f4763276b1bf8bac66a6ce7b755b933d	no	3
Warnings:					
This is not a USPTO supplied Provisional Cover Sheet SB16 form.					
Information:					
2	Specification	Specs_TPP30944.pdf	39626 e83298c1121071b7666bebc891ad9e55c3ec2617	no	9
Warnings:					
Information:					
3	Drawings-only black and white line drawings	Figures_TPP30944_EMBED.pdf	125800 17d402a59950d1d2a4576bbad759c481e418ce98	no	2
Warnings:					
Information:					
4	Certification of Micro Entity (Gross Income Basis)	PTO15_TPP30944.pdf	3232404 8adf66aa6ba0c69107ba9d786f4e1de0e51faf67	no	2
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	29660 d923ca7396f53e785d57dc981b30ef32f0e6b4a6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	7030569		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.