

OVCODE

Blockchain Verification Engine

Digital Seal of Trust

January 15, 2018

Abstract

Verification is proving the truth of existence, ownership, and other related important information. Through verification, proper valuation of assets is defined. ^[1] Processes and techniques for verification have been around since time immemorial, starting with seals and evolving to signatures, holograms, stamps, and other mechanisms. ^[2] With the advent of technological advancements, however, the risk of data manipulation and fraud has increased. On this premise, OVCODE, a Blockchain verification engine for digital, intangible, and physical assets, was developed. It is a platform that establishes the truth, accuracy, and validity of any entity with value using Blockchain technology. To achieve the least risk and establish transparency and trust, OVCODE takes advantage of Blockchain's immutability and decentralized properties along with cryptography techniques. In addition, OVCODE devised a zero-cycle latency authentication algorithm for integrity of data within the network. To proliferate usage, OVCODE APIs will be exposed and free of use to the public. The vision is to be the verification engine that unlocks positive economic value. OVCODE becomes your digital seal of trust.

Introduction

Verification is an auditing process that examines the existence, ownership, and other essential information related to the asset. ^[1] However, the importance of verification goes beyond audit principles. Through verification, proper valuation of assets is defined. A well-verified asset maximizes potential for sale, loan and compensation thus, unlocking the asset's economic positive value. ^[3]

Since time immemorial, physical representation of authenticity has been well known for verification usage. The use of seals, for example, can be traced back to more than 7000 years ago. Royalty and governments would affix their own seal for identification, authentication, and verification. It then evolved to the development of signatures, holograms, stamps, and other mechanisms for authentication. But with the advent of technology, the risk of data manipulation and fraud has increased. Identification, authentication, and verification procedures have to keep up by establishing transparency and trust during the process. This is where OVCODE comes in handy.

OVCODE is a Blockchain verification engine for digital, intangible, and physical assets. This may range from digital media, source codes, and intellectual properties to gold, real estate, corporate bonds, state, local government securities, and other entities with value.

By design, Blockchain is distributed, decentralized, and inherently resistant to modification of data. Once recorded, any given data cannot be altered retroactively without alteration of all subsequent data, which requires collusion of the network majority. This makes data in the Blockchain immutable.

OVCODE is a patented technology that integrates Blockchain to digital signature and cryptography to achieve the least amount of risk and to establish transparency and trust. OVCODE becomes your digital seal of trust. With this verification mechanism, OVCODE unlocks positive economic value using the Blockchain technology.

The remainder of the paper will discuss the following:

- The Verification Market
- The Technology
- Future Work
- Proof of Completeness
- Conclusion

The Verification Market

Digital, intangible, and physical assets require verification to confirm existence, ownership, validity, history, and other vital information.

The verification market fundamentally shadows the current value of existing assets and activities related to those assets. Activities may include, but not limited to, transfer of ownership, asset enhancements, and other changes to the assets.

Verification encompasses the asset itself and the activities related to it with respect to the person verifying and the timeframe of verification.

In this sense, although assets are finite, verification to these assets are infinite over time.

To give a picture of a portion of the market size, discussed below are assets per category:

A. Digital Assets

A digital asset, in essence, is anything that exists in a binary format and comes with the right to use.^[4]

This may include but are not exclusive to: digital pictures, digital drawings, digital documents, audible content, motion picture, websites, blogs, digital books, digital media and other relevant digital data that are currently in circulation or are, or will be stored in digital appliances such as: personal computers, laptops, portable media players, tablets, storage devices, telecommunication device and the likes. ^[4]

The majority of digital assets possess monetary and/or sentimental value. Since digital assets represent the goods sold by a business or they are in themselves among the goods being sold, their value usually increases according to their usage. ^[4]

The Internet is growing to over 12-trillion gigabytes of digital data and doubling in size every two years. ^[5]

B. Intangible Assets

An intangible asset is an asset that is not physical in nature. ^[6]

Corporate intellectual property, including items such as patents, trademarks, copyrights, insurance policies, and business methodologies, are intangible assets, as are goodwill and brand recognition. ^[6]

The market capitalization of all of the world's stock markets is equal to \$73 trillion. The high-end estimate for the value of all derivative contracts, on the other hand, is as high as \$1.2 quadrillion. ^[7]

Like physical assets, total global intangible assets are not quantified. But with just examples cited above, it is evident that market for verification of intangible assets is high.

C. Physical Assets

A physical asset is an item of economic, commercial or exchange value that has a tangible or material existence. ^[8]

There has not been a study defining the value of the overall global physical assets because of its subjective nature. But to give an idea, below are prevalent physical assets presented with their equivalent global value:

The global real estate market has an estimated value of *\$217 trillion*. ^[7] This covers residential property, offices, retail space, hotels, industrial land, agricultural land, as well as other commercial uses. While the world's total aboveground gold reserves are estimated to be worth \$7.7 trillion. ^[7]

Though not defined, with these two physical assets alone, market size already reached \$224 trillion.^[7]

The Technology

OVCODE is a platform that establishes the truth, accuracy, and validity of any entity with value using a decentralized and distributed computational network over a heterogeneous communications environment.

OVCODE integrates Blockchain to digital signature and cryptography technologies for its verification technology. It transforms an original entity into a verifiably authenticable entity using the Blockchain technology over a communications network such as the Internet.

'Entity' may refer to, by way of examples and not by way of limitation, a tangible asset such as a car, a physical characterization of a tangible asset such as a Transfer Certificate or Title or a Condominium Certificate of Title, a physical characterization of an intangible asset such as a Certificate of Letters Patent or Certificate of Trademark Registration, and a celestial body such as a satellite or a spacecraft. It is to be understood and appreciated that anything in the universe whose authenticity is feasibly verifiable, and/or worth verifying, mostly due to its economic, social and/or moral related values, or otherwise, may be referred to as the "entity" in this paper.^{[9][10]}

Digital transformation brings huge, problematic gaps especially in authenticity of assets. The gap happens after creation of the database entry, to printing until storage. Tampering and data manipulation can happen in any of these gaps. To prevent this, OVCODE is designed for zero-cycle latency authentication at source.

An electronic record of the original entity is created and associated to a set of securely encrypted unique identifier called the cryptographic hash. The publisher of the original entity initiates publishing of the cryptographic hash to the OVCODE Blockchain network by digitally signing the transaction.

Hash-based transformation, being a multi-step procedure, means that any digitally signed serial number generated by way of using a hash-based transformation may be altered before it gets imprinted on an object as a textual component. With OVCODE's zero-cycle latency authentication, integrity of data associated with encrypted messages in implementing transformation of an original entity into a verifiable entity is uncompromised even in cases where attackers have already gained control of the encrypted messages, for providing a secure, traceable and verifiably authenticable chain of evidence in such implementation, and for ensuring security of data associated with the process of generating digitally signed serial numbers.

Multiple connected OVCODEs can be represented by a single OVCODE. The identity of the single code depends on how the multiple connected codes are defined. Definitions

of the sequence vary from one entity to another. Furthermore, to unlock the single OVCODE, multiple OVCODEs must be well verified according to the requirements set by entity. E.g. a well-verified asset assigned with a single code may consist of multiple verified codes such as: an electronic representation of the land title, tax declarations, and other documentations from the registering body.

Verification of the entity published includes identification and matching of the publisher's digital signature and cryptographic hash previously published to the Blockchain network. Other information relative to the entity published may also be verified, e.g. (1) Verification of Ownership (2) Verification of Authenticity (3) Verification of Origin (4) Verification of Entity's History (5) Verification of Date and Time Published.

A. OVCODE Drawings:

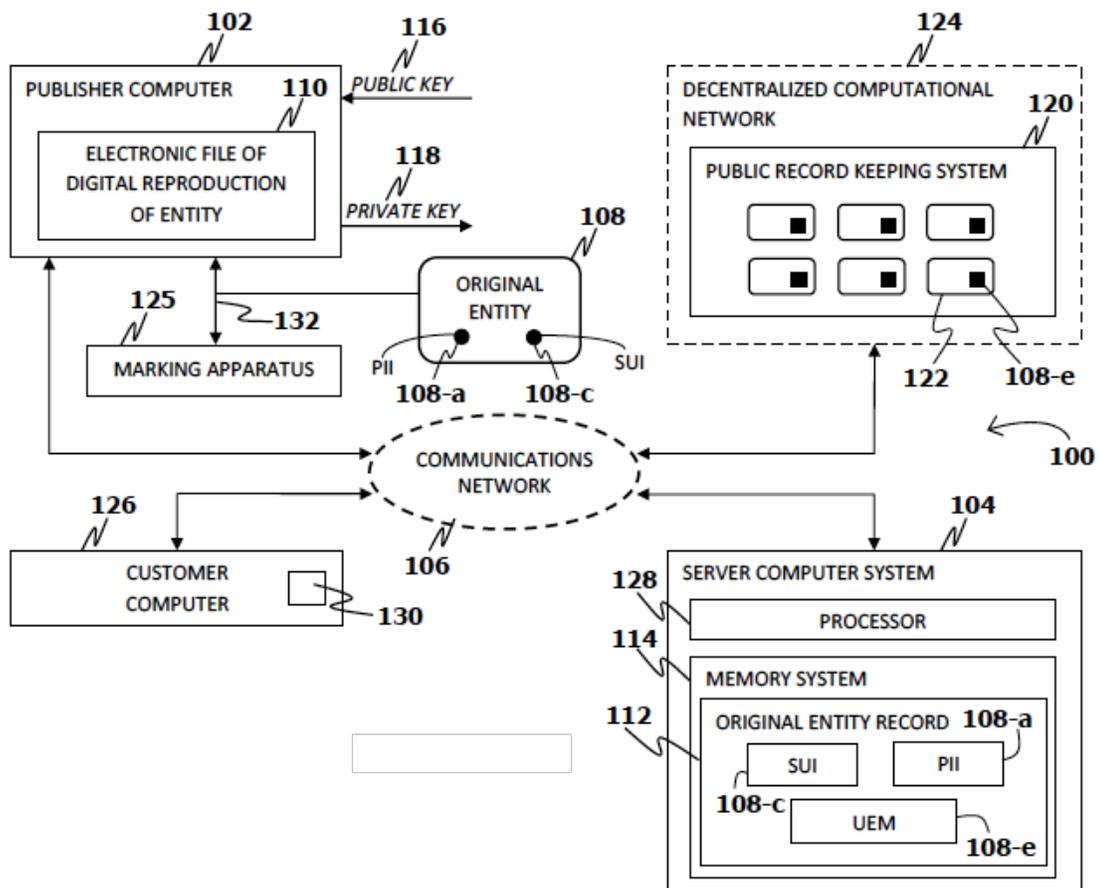


Figure above illustrates a system for implementing transformation of an original entity into a verifiably authenticable entity in a heterogeneous communications network environment of OVCODE. The system aspect of OVCODE is generally designated by reference numeral 100 throughout the ensuing description and/or illustration. The

system **100** mainly includes a publisher computer **102** in operative communication with a server computer system **104** over a communications network **106** such as the Internet.

The publisher computer **102** is preferably arranged to: (i) obtain a digital reproduction of at least one portion of the original entity **108** on which at least one physical indicia identifier or “PII” **108-a** may be appearing; (ii) create an electronic file **110** of the digital reproduction of the at least one portion of the original entity **108**; and (iii) deliver, over the communications network **106**, to the server computer system **104** the electronic file **110**.

The server computer system **104** is preferably arranged and/or configured to: (i) extract the at least one physical indicia identifier **108-a** from the electronic file **110**; (ii) associate a set of unique identifiers or “SUI” **108-c** to the extracted at least one physical indicia identifier **108-a** to create an electronic record **112** of the original entity **108**; and (iii) store in a memory system **114** of the server computer system **104** the electronic record **112** of the original entity **108** having the associated set of unique identifiers **108-c** and at least one physical indicia identifier **108-a**.

The server computer system **104** may be further arranged and/or configured to: (iv) encrypt the electronic record **112** of the original entity **108** using a public key **116** associated with the publisher computer **102** and a digital signature including a private key **118** associated with the publisher computer **102** to generate a uniquely encrypted message or “UEM” **108-e** carrying the associated set of unique identifiers **108-c** and at least one physical indicia identifier **108-a**; (v) publish, over the communications network **106**, the uniquely encrypted message **108-e** to a chain of data on a public record keeping system **120** residing in one or more nodes **122** in a decentralized computational network **124** using at least one decentralized computational network protocol; and (vi) subsequently send, over the communications network **106**, to the publisher computer **102** the set of unique identifiers **108-c**.

The system **100** may also include a marking apparatus **125** operatively coupled to the publisher computer **102** through any appropriate communication bus and/or circuitries **132**. The marking apparatus **125** is preferably arranged to form the set of unique identifiers **108-c** on any portion of the original entity **108**.

The system **100** may also include a customer computer **126** accessing the server computer system **104** over the communications network **106**. By means of which, a customer who is operating the customer computer **126** is enabled to verify whether an entity of interest is authentic relative to the original entity **108** as a point of reference or reference point.

The server computer system **104** may be further arranged and/or configured to: (i) accept from the customer computer **126** a set of unique identifiers of interest formed on the entity of interest having at least one physical indicia identifier of interest; and (ii) determine whether the set of unique identifiers of interest and the at least one physical

indicia identifier of interest are associated with one another and exist in the memory system **114** of the server computer system **104**.

Consequently, the server computer system **104** can be further arranged and/or configured to: (iii) if the set of unique identifiers of interest and the at least one physical indicia identifier of interest are associated with one another and exist in the memory system **114** of the server computer system **104**, fetch from the memory system **114** of the server computer system **104** the electronic record of **112** the original entity **108** corresponding to the associated set of unique identifiers of interest and at least one physical indicia identifier of interest existing in the memory system **114** of the server computer system **104**. Any one or more of the tasks in the server computer system **104**, including the fetching step for example, may be executed by a processor **128** from the memory system **114** of the server computer system **104**.

Accordingly, the server computer system **104** can be further arranged and/or configured to: (iv) communicate, over the communications network **106**, with the decentralized computational network **124** using the at least one decentralized computational network protocol; and (v) identify, as one of the one or more nodes **122** in the decentralized computational network **124**, whether the set of unique identifiers of interest carried by the uniquely encrypted message **108-e** is published to the chain of data on the public record keeping system **120** by decrypting the uniquely encrypted message **108-e** associated with the fetched electronic record **112** of the original entity **108** using the public key **116** associated with the publisher computer **102** which causes creation of the fetched electronic record **112** of the original entity **108** in the memory system **114** of the computer server system **104** of the one or more aspects of OVCODE.

Accordingly, the server computer system **104** can be further arranged and/or configured to: (vi) if the at least set of unique identifiers of interest is recorded in the chain of data, acquire from the memory system **114** of the server computer system **104** in whole or in part the electronic file **110** of the digital reproduction of the at least one portion of the original entity **108** based on the associated set of the unique identifiers of interest and physical indicia identifier of interest; and (vii) transmit, over the communications network **106**, to the customer computer **126** the acquired electronic file **110** of the digital reproduction of the at least one portion of the original entity **108**.

The customer computer **126** which may be operated by a human user may be arranged and/or configured to: (i) receive, over the communications network **106**, the transmitted digital reproduction of the at least one portion of the original entity **108** associated with acquired electronic file **110** from the server computer system **104**; and (ii) output on an output unit **130** of the customer computer **126** the received digital reproduction of the at least one portion of the original entity **108**.^[10]

B. OVCODE Functions:

1. Account Management with Digital Signature

OVCODE code provides management consoles for accounts mapped to its corresponding digital signature. Apart from individual users, OVCODE offers Organization category that has the ability to create sub-admins and users. Each active account is also created a wallet to be used to pay for OVCODE transactions.

2. Cryptographic Hashing

OVCODE uses cryptographic hashing techniques like SHA-256 to generate one-way hashes for entity input. With its service centered approach, OVCODE '*Generate Hash*' function can be integrated to any existing front-end or backend systems.

3. Blockchain Publishing

After hash generation, OVCODE publishes the hash to the OVCODE Blockchain network, along with other related information such as: Publisher/Owner (wallet address), DateTime, hash, Transaction code, and other defined parameters.

4. Blockchain Verification

Provided the original entity published, OVCODE matches that given entity to the published data in the OVCODE Blockchain network. You can either scan or enter entity representations, such as: a barcode, an alphanumeric code or a QR, or upload the original entity itself.

5. Developer Console

OVCODE open its APIs and documentation so other developers can build on top of OVCODE. Developers can easily sign up with OVCODE and have access to the APIs and documentation.

6. Payment

Each account is mapped to a wallet. Wallet functions are available for all OVCODE users. You can either load or spend for paid OVCODE transactions.

The Token

OVCoin will be the only medium of payment for OVCODE transactions. OVCoin will be used for the following:

1. Asset Registration
2. OVCODE Blockchain Publishing
3. OVCODE Verification
4. Advertisement Sponsored Features

OVCoin is an ERC20 token and will have a finite supply.

During registration to OVCODE, the user is created a loadable OVCoin wallet. Upon completion of function processes, users will be redirected to the payment page and will be prompted to pay via OVCoin. OVCODE will deduct the payment amount to the user's OVCoin wallet.

Verification costs are fixed for every publishing institution. OVCoin payment will be converted to the fixed payment depending on the current OVCoin market value.

Institutions can project possible usage and buy OVCoin in bulk. Users now have the option to buy from the publishing organization or buy directly from OVCODE.

Future Work

OVCODE's future work will focus on four main elements:

1. Easy Publishing

OVCODE will make it easy for individual users, institutions, corporations and governments to publish their assets in the OVCODE Blockchain. OVCODE will develop the following:

- Developer Console Enhancements and Software Development Kits (SDKs)

The current developer console offers Login and Publishing APIs. For now, registration is manually done on the administration panel. The plan is to open the APIs to everyone. We will be developing a strong Know-Your-Customer (KYC) workflow to check integrity of API users as well as to map OVC wallets to these users. OVCODE will

be adding APIs such as Registration, Verification, Storage Integration, Dashboard, and Reporting.

OVCODE will also develop SDKs for 3rd party hardware and software systems such as printers, document management systems and other systems that need authentication.

- Online Vault Development

For users to have easy access to their asset for publishing, OVCODE will devise an Online Vault system. This will vary according to the users' or institutions' choice of storage, e.g. OneDrive, MS Blob, Dropbox, AWS S3, on-premise file server, etc. OVCODE will connect to these storage mechanisms and tag them accordingly. OVCODE will also track versioning of the assets stored in the Online Vault.

- Mobile Publishing

OVCODE will have a mobile publishing version to make it easier and more convenient for users. The Online Vault will also be integrated to the mobile version. From the Online Vault, users will have access to their asset and will be able to publish it to the OVCODE Blockchain.

2. Fast Verification

OVCODE will make asset verification fast and easy. OVCODE will develop the following:

- SuperHash

The SuperHash will hash multiple hashes to one single representation hash for single assets supported by multiple entities. This way, verification trigger is faster as it is pre-verified upon publishing. The criteria for pre-verification are variable to the workflow set by an individual or an institution.

- Verification Plug-ins

OVCODE will develop plug-ins to streamline verification especially on digital assets and contents. Plug-ins maybe integrated to web browsers, 3rd party systems, or even scanning machines.

- Mobile Verification

OVCODE will have a mobile verification build where users can just scan or input entities to verify. It will also have integration to the Online Vault where users can store verified assets for future reference.

- Infrastructure Upgrade

OVCODE will expand transaction nodes and mining to process publishing and verification commands faster.

3. Community Development Tools

OVCODE will develop and package complete set of tools and knowledge base for individuals, companies, institutions and governments to establish the OVCODE Blockchain infrastructure. OVCODE allows them to set up their own Blockchain registration, publishing, and verification platform.

4. Infrastructure Growth

OVCODE will offer the least possible cost for its transactions. OVCODE will develop the following:

- Ads Integration Revenue

OVCODE will develop an engine that will integrate to advertising companies. This will significantly lower the cost of OVCODE publishing and verification and would increase bounty for the OVCODE network.

- Bounty Programs

OVCODE will devise bounty programs to proliferate usage and increase OVC value. Bounty programs will support the platform to achieve least cost in OVCODE transactions.

5. Artificial Intelligence Integration

OVCODE will integrate with big data management and machine learning algorithms to track patterns and irregularities of all transactions and data collected by the application. The integration will automate verification and fraud detection. Users will have accessible insight on fraud that will serve as guidance in decision making for sustainability

and growth. OVCODE users may create endless models to make sense of the data depending on the type of their business and requirements.

Proof of Completeness

A. OVCODE Developer Console

OVCODE Developer Console allows 3rd party systems to integrate to the OVCODE Blockchain functions. The console opens its Login and Publishing APIs for the developers to build on top of OVCODE easily. A web platform with APIs and complete documentation is provided for developer reference.

B. OVCODE used for Police Security Background Check

Cebu City Police Clearance is an official document issued as a background check by the local police agency to enumerate any criminal records the applicant may have.

Police clearance is one of the documents employers require in the hiring process. It can also be a requirement for passports and other government IDs.

OVCODE integrates to the Cebu City Police Clearance system. Upon production of a police clearance document, OVCODE transforms that document into a cryptographic hash. The cryptographic hash is then published to the OVCODE Blockchain network with the publisher's digital signature. The police clearance published is then assigned an OVCODE to be used for verification. The Cebu City police clearance integration has been operational since May 2016.

C. OVCODE used for the Roman Catholic Church Sacrament Certification

The Archdiocese of Lipa Batangas issues certificates as baptismal, confirmation, marriage, and death certificates, by parish in recognition of those who receive the Sacraments.

It has adopted a computerized system to manage issuance of these certificates OVCODE integrates with certificate issuance system. OVCODE transforms the document into a verifiable entity that is accessible anywhere through the Internet. The system has been operational since June 2016.

D. OVCODE Integration with Cloud-based Productivity Softwares for Authentication and Verification

OVCODE integrates directly to productivity software document processor. The Microsoft Office 365 user has the option to add OVCODE as an Add-in. Once

added, the user can now easily publish his/her documents to the OVCODE Blockchain network. The published documents are converted to a verifiable entity that can be confirmed through parameters given by the users. The document can be verified in the OVCODE platform in web or mobile.

E. OVCODE Website Content Integration for Authentication and Verification

OVCODE provides website owners a tool to secure their content, as well as protect readers from fake news or contents. By installing the OVCODE plug-in in Chrome, owners can now capture verified contents and publish it to the OVCODE Blockchain network. Readers can verify if a website's content is authentic by logging into the OVCODE program.

Conclusion

With the increased verification demand of digital, intangible and physical assets, there is a need to create a global verification engine with a foundation of trust and immutability. OVCODE is a platform that establishes the truth, accuracy and validity of assets using Blockchain technology. OVCODE as a verification engine aims to unlock positive economic value of well-verified assets. The intention of OVCODE is to create a universal digital seal of trust.

References:

- [1] Verification Definition. Wikipedia. Site
[[https://en.wikipedia.org/wiki/Verification_\(audit\)](https://en.wikipedia.org/wiki/Verification_(audit))]
- [2] 7000 Years of Seals. Dominique Collon; JH Betts. 1997
- [3] Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else. Hernando de Soto. 2003
- [4] Digital Asset Definition. Wikipedia. Site
[https://en.wikipedia.org/wiki/Digital_asset]
- [5] Defining Property in the Digital Environment. Bitmark Inc. 2016
- [6] Intangible Asset Definition. Investopedia. Site
<https://www.investopedia.com/terms/i/intangibleasset.asp>
- [7] The Money Project. Jeff Desjardins. 2017
- [8] Physical Asset Definition. Investopedia. Site
[<https://www.investopedia.com/terms/p/physicalasset.asp>]
- [9] Entity Definition. Wikipedia. Site [<https://en.wikipedia.org/wiki/Entity>]
- [10] Patent Publication. OVCODE. 2017