rewarded market certification & decentralized brand's anti-counterfeiting

bCerty whitepaper

www.bcerty.io

draft 26/10/2018

1 SUMMARY

1 Abstract 1
1.1 Concise summary 1
1.2 Scenario 1
1.3 Problem 2
1.4 The solutions 2
2 Platform 4
2.1 Today centralized 4
2.2 Future decentralization 4
3 Operators identification 5
4 Objects management 6
4.1 Production 6
4.2 Verification 7
4.2.1 Verification incentive and verification Bounty 7
4.2.2 Dynamic code updating 9
4.3 Purchase 9
4.4 Exchange an resell of used products 10
4.5 Personal products & “minibrand” 10
4.6 Analytics 10
5 State of the art 11
5.1 The applications 11
5.2 Commercial agreement 12
5.3 The reference market and the competitive advantages over the competition 12
5.4 Research and development 13
6 Migration Plan 14
6.1 Users identification and TAG management 14
6.2 Project phases 14
7 Future vision 15
8 Time line 15
9 The Team 16

1 ABSTRACT

1.1 CONCISE SUMMARY

BCerty will move an anti-counterfeiting patented system, currently used to univocally identify every single object and his property, onto the blockchain technology.

This improving gives to producers the opportunity to use the newest and better technology as well as a great marketing leverage versus his final customers.

The brand protection, for which now billions are spent, will be made directly by end users whom will obtain credits as reward for their fidelity and interaction with the goods.

Furthermore, the marketing and product's information will lead to a fast, easy and secure communication channel between producers and customers.

The goal is to decentralize the investigations on product's originality giving to people the opportunity to be paid to verify product's originality.

1.2 SCENARIO

In the modern time we would like to access all kind of information, especially on objects that we buy and use. During a shopping experience we like to verify the quality of the object. We trust that the object in the shop is not counterfeited, even if there is a big grey market in counterfeited goods. We like to know technical aspect, understanding if the raw material is a high quality one, and retrieve information about the manufacturer. More and more we use internet for fast research and we try to filter out information that are not reliable.

We verify the expiring date or the warranty, that most of the time are not easy to read. We try to understand for how long the product is in the market and we try to read few comments from users that already have it.

After the purchasing we need to remember to store the receipt and fill up the modules, on-line or on paper, for the warranty activation. Then we need to identify all the uses of the object and the maintenance.

In case we decide to resell the object, we would like to do it in a secure way. To obtain a better reliability and selling power, what we need is a system that certifies the originality and the history of it. All of this should take place in a telematic negotiations, that now is more and more prone to fraud.

In case of theft of valuables, it is almost impossible to uniquely identify the object. For this, each of us remembers any peculiarities of his, or her, own object that makes it unique or tries to find tools that allow him to recognize it in the event of loss or theft.

Seen on the part of the manufacturer, it is always of the utmost interest to provide customers with what they want, to reduce waste by producing material that remains uninvited and unused. Therefore it is useful to get anonymous analytics on their customers, who they are, what kind of products they prefer, where, how and when they buy.

At the same level of product quality, it is undeniable that the choice of the user falls on who offers the best service and for sure the user will give their fidelity to brands which will someway recognize him as a part of its story.

Additionally, personal data management is extremely timely to protect privacy and make sure that such data is not manipulated.

1.3 PROBLEM

With the current solutions we are unable to verify the full specifications of a product, we must stick to and content with what is stated on the label.

On average we are not able to determine the quality of a sold item, in the physical store or online. We are not even able to know if the reviews on the internet are genuine or manipulated.

Often, warranty activation procedures are costly and unused by the customer. After a few months, the receipt, printed with thermal printers, is unreadable. You need to make a photocopy and store it in a drawer to consult it periodically to remember its expiration date.

The manufacturer uses tools, never fully effective, to test and track the work of outsiders and sellers. Sell-out data on average are received after periodic expiration and more frequently only after any reorders that must be urgently escaped. This implies nonlinear trends in production loads.

Also, the manufacturer knows that even fake products can be sold in stores, which compromise his earnings and worse still can compromise his image. User feedback is not easy to use, so any product enhancements have very long response times.

An example can be made trying to explain which the result of counterfeiting for producers is:

> *The producer uses a subcontractor to make 6.500.000 glasses for whose it pays 15€/pcs; it sells the product to optical store for 60€/pcs.*
>
> *The subcontractor makes ~7.000.000 pcs (declaring 8% production error) and sells the overproduction to optical stores for 30€/pcs.*
>
> *=>The producer loose ~7.500.000 €*

To identify counterfeited glasses the producer wastes millions of euro per year in investigation.

Furthermore, while on a one-to-one basis, customer relationship becomes data driven, it is necessary that the benefits of using such data can only be exploited if the user's expectations are adequately met and that privacy is guaranteed as well as the veracity of personal data.

1.4 THE SOLUTIONS

The solution consists in creating a system that can guarantee the originality of a product with certainty, and that ensure also the end-user purchasing.

bCerty is a service that provides our customers with the certification of the product’s originality and their after-sales certifications. To obtain it we use our unique markers (tags) applied to the product which leverage a patented algorithm system. This allows an extension of the certifications concept beyond the traditional supply chain, reaching the final consumer.

The system also permits the certification of the ownership of each item or the management of its warranty and thereby collects important market data for all manufacturers. The system value proposition for manufacturers, besides product certification, is the ability to get to know their market deeply, thanks to the use of product's data that are collected through the system.

This provides the basis for action on which to build the rest of the infrastructure, and to obtain applications that are otherwise unreachable today.

Blockchain-based applications doubtless have the potential to improve the supply chain. They provide an infrastructure that records, certifies and maps a property that is transferred between often distant parts, connected to each other through a distribution chain. In this way, the goods would be pawns that can be transferred over a chain of checks that verifies, in a safe and transparent process, a transaction. The terms of each transaction will remain irrevocable and immutable, open to the control of anyone or only authorized users. Smart contracts can also be used to make payments and other procedures automatically.

Find the way to free up data security from the honesty of an entity/company. We are going to develop an intrinsically secure system that arranges the data control over the same network.

The goal is to gradually decentralize the current service using the chain. We want to get a completely trustless system in the basic functionality, where it will not be our task to guarantee for objects and manufacturers but where everything will happen in a transparent and autonomous way.

With the certified purchase it will be the same item which will remember the date and place of purchase. It is also possible for the user to associate information with the object and attach any other public or private note even in multimedia form.

Additionally, social spaces will be created dedicated to products, where users can discuss in a private and secure environment of their purchase. This is to help brand growth and strength by leveraging and sustaining the natural human need of contacts and social relationships. We can do this thanks to these discussion spaces accessible only to those who actually have a certain object. This will give the opportunity to produce exclusive content and customized offers.

Thanks to this, what is also proposed is a new marketing tool where the product interacts with the final buyer. It may be the same user who, telling his own experiences with the product, offers the opportunity to tell the world his experience with a "user story telling". Larger agencies will no longer be able to propose content to be circulated in advertising, they can be the users themselves to offer their own experiences to increase Brand's value as global testimonials.

This is done accessing statistical or punctual information, in anonymous way to preserve the privacy of users. Each product can be traced not only to the store's shelf but far beyond, after selling each product to its new owner.

This new definition of traceability is a guarantee of ownership and also originality and allows, for example, to identify the places where it is most counterfeited, receiving reports to counter the gray market. By exploiting the potential of blockchain, manufacturers will easily decide how much and how to spend for anticounterfeit. BCerty private token-based system will transform the ultimate consumer into a private investigator for companies, even when he does not buy object, he will may be rewarded simply verifying products.

Relating to the previous scenario in example, the millions currently spent by producer to pay detectives will be distributed between the people:

> *producer places these millions in token into the glasses to reward the distributed investigators. Subcontractors can't distribute fake copies, and everybody is happy to gain tokens, just shopping.*

Thus, we will obtain the distributed investigations on product's originality paying people to verify product's originality.

2 PLATFORM

2.1 TODAY CENTRALIZED

Currently, the platform, offered by the Italian firm DigiCanDo Srl, is based on a classical client-server infrastructure, organized around a cloud service that exposes APIs and a web portal to access the service. To this, a cloud database and various clients are connected. The platform is currently under development, but already operational in basic functionality.

Other features will be implemented in the future for customers and manufacturers.

2.2 FUTURE DECENTRALIZATION

The goal is to gradually decentralize the service, depending on the availability of resources and the implementation convenience. For this purpose, a hybrid structure where part of the data is handled in a traditional way and is part of the chain infrastructure has been studied, winning a research and development call for the province of Bolzano (Italy).

Hybrid architecture has been designed to deliver maximum functionality and efficiency with minimal cost. The decentralized part will be studied, implemented and integrated in a gradual way, absorbing functionality from the previous implementation.

The overall architecture will be defined in layers as follows:

1. **Identity service**
   An operator identification system will define the addresses that can operate on the blockchain, with its roles and permissions. This will be used as a basis for identifying producers, sellers and their delegates.
2. **Item manager**
   This layer will handle tag management, production, purchasing, exchange, and verifications. This layer will be decentralized.
3. **Social application**
   The social and application layer based on certified tags and certified properties. It will allow, among other things, to evaluate and comment on the products, to publish related material in private spaces and to arrange protected sales. This layer will be decentralized at a later time.
4. **Managed services**
   A server application layer will offer the deployment of non-decentralized services and APIs to access the various clients. This layer will run centrally but will provide data access and accessory services rather than basic functionality. It will also offer collection and processing of optional data that you do not want to decentralize for various reasons.

5. **Client**
   The latest layer will be related to applications and the web portal that will provide the entry point for the full user experience. They will interfere with server API and nodes, or natively only with blockchain nodes if needed.

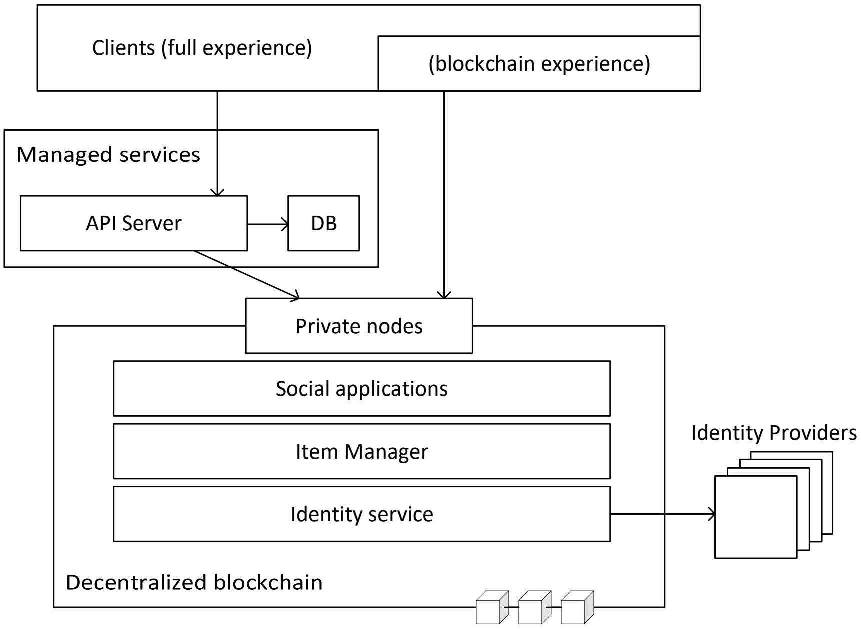


Figure 1 architectural scheme

To offer the best privacy protection, some service data, such as application usage analytics, tags readings and verifications, or objects that do not have bCerty certification, will in case be privately collected by DigiCanDo and will not be published on blockchains. However, blockchain functionality will not require the intervention or consent of DigiCanDo to be executed.

All code published on blockchain will be open source, this to embrace the idea of providing as transparent a service as possible and provide security to service users.

3 Operators identification

The operators, or those who can perform actions on the service, will be identified by an Identity Service that will be concerned with issuing non-transferable certificates. BCerty will have the root certificate, and together with each certificate will issue permissions to operate on the platform, and possibly issue other certificates. It will then be possible to appoint other independent certifiers who can operate without the intervention of BCerty or will be possible for brands to auto certificate themselves. These certificates may be timely and may be renewed or revoked by the petitioner as further detailed below.

While the root certificate will remain encrypted, protected by a multiple signing key, some examples of underlying certification entities may be BCerty itself, issuing an SSL Extended Validation Certificate, signing up to an accredited business log. The ability to have more certification entities also decentralizes the authorization to access the use of service for business purposes.

The cascading structure of issued certificates will be like the SSL certificate release system. Each certificate will contain all the public information of the certification body, accessible by anyone, and attesting the ability to operate from certain addresses. Any private information may be collected and kept secret by the BCerty servers or encrypted within the certificate.

Each certificate will contain the user-granted permissions, that is, a list of actions that the user will be able to accomplish, otherwise normally unauthorized. For example, we can manage a company's production, or create other sub-certifications. The undersigned may enjoy most of his father's certificates, but other specific rules will have to be defined. A certificate is valid only if all parent certificates, up to the root certificate, are valid. Removal of a father certificate in fact cascades with the removal of all child certificates.

Certain categories that will need identification to operate are certified manufacturers and resellers.

4 Objects management

Tags represent a physical or virtual object of which you can own the property. They can be associated with a certificate issued to the manufacturer by identification and will enjoy different cases of different features. Each tag has a unique identifier that can instantly identify the object.

4.1 Production

Production will take place via a contract that will issue the tags as non-fungible tokens, and it can be of two types:

- **personal tag**
  the simplest, they directly contain object information. They are dedicated to the cataloging of personal assets for private use. They can be produced by any user without special requirements and can be guaranteed by the user himself through independent means. Object information can be encrypted.
- **production tag**
  they are dedicated to mass productions, which involve different units by type of goods. They are linked to a manufacturer and can be identified as genuine if the manufacturer has a valid certificate.
  Tag are associate each with an object profile, shared information collectors, related to the objects produced. The object profiles can only be modified by the manufacturer or his delegates.
  Production tags can be enabled to be purchased and verified, they can contain a verification bounty (see paragraph Verification)

Tags can be created already enabled or can be subsequently enabled by the manufacturer or authorized vendor. A tag that is not enabled is a tag that is no longer recognized by the manufacturer and therefore will not be affordable or verifiable. Each tag, if enabled, can be purchased autonomously by a final user.

To create a tag, you need to spend ethers in the contract. This will be the main gaining method of BCerty. The price for creating a tag will be arbitrarily defined by BCerty, observing the value of tokens in the market and periodically updating the relative cost.

Each tag maker can optionally sign, directly or through appointment, the various stages of the work. A signature sets a guarantee seal on when and where the various processing phases are performed. You will also be able to associate more information for the buyer or for logistic traceability at this stage.

Whenever an owner decides to resell a tag, he or she may do so unless the specific rules imposed by the manufacturer.

4.2 Verification

Each verifiable tag will be equipped with an NFC read / write tag, where a dynamic code will be stored inside it. This code will be a private elliptical encryption key, while blockchain associated with the same tag will find the corresponding public key. If the keys match, the tag is original.

Our Anti-Counterfeiting Patent (PCT / IB2015 / 056637) expects the dynamic code to be updated to prevent identical clones from the same tag. You will then need to provide an end user incentive to participate in this verification process, then rewrite the code on the physical tag.

Dynamic code update will not be mandatory, but the manufacturer can set policies to reward who decides to update it. For example, the introduction of the verification bounty (as explained below) may be an incentive for product verification by not only buyers, but also all the customers of the various retail outlets. This will potentially transform any user into a private investigator.

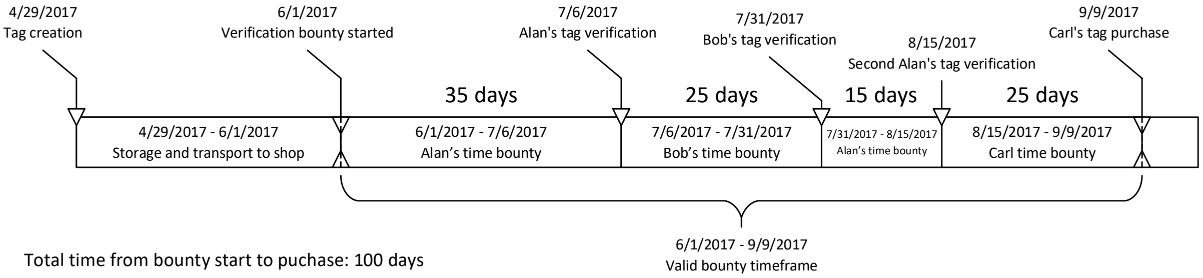
Each verification operation is tracked on blockchains, except for any negative verifications that will trigger an optional reporting to our service with the necessary data. However, each reading and verification, unless otherwise expressed by the user, will be detected by our service to provide useful information to the user and for analysis purposes.

4.2.1 Verification incentive and verification Bounty

Each product tag will contain a verification bounty, expressed in ether, set by the manufacturer. The bounty will be released at time of purchase to anyone who has verified the originality of the product and will have contributed correctly to the code update. The bounty will be distributed proportionally to the time lapse of the previous verification. This prevents phenomena of continuous updates from the same person from different addresses. The purchase is a final check. Different proportionality policies will allow manufacturers to stimulate verifications or purchases.

You can start a bounty at a predetermined time so that if the manufacturer knows that a particular product will arrive at a store on a specific date, you can prevent brokers from getting the bounty, or the first verifier to take all the stock and transport time. Alternatively, you can ask the seller to check out the products and activate the tags they receive.

Verification bounty: 100 finney



Total time from bounty start to puchase: 100 days

Total bounty time:

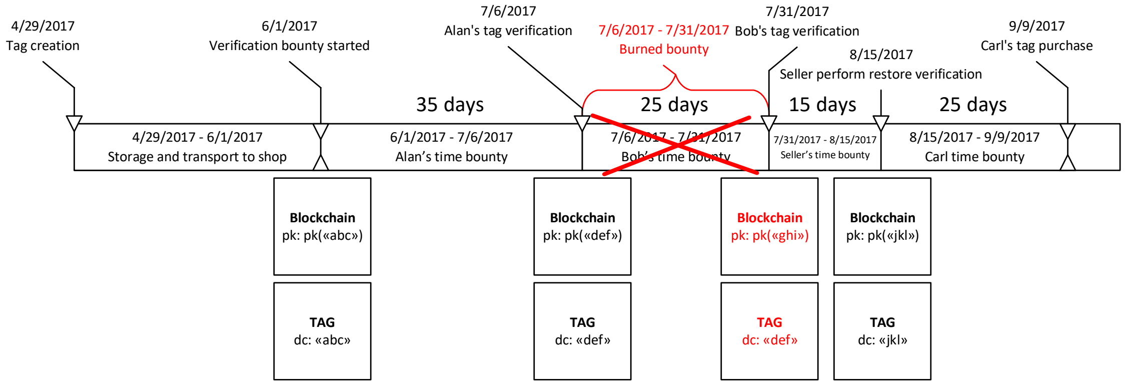
- Alan: 35 + 15 = 50 days
- Bob: 25 days
- Carl: 25 days

Received bounty:

- Alan: 50 finney
- Bob: 25 finney
- Carl: 25 finney

Figure 2 example of deployment of the verification bounty

A malicious user may try to update blockchain verification status and not update the code within the NFC tag, causing the status of the object to be recognized as "not original" for subsequent verifications. The seller will then have the power to repair this wrong state. If you need to reset the dynamic code from the vendor, the bounty that has passed since the last valid verification check will be burned, and the seller may receive a percentage of that bounty. However, you will not be able to abuse this power because the task you are performing will be traced and associated with an identified and public account attributable to the seller.



Legend:

Blockchain Tag's values on blockchain

TAG Tag's values on NFC

* **dc**: dynamic code (private key)
* **pk**: public key
* **pk(dc)**: public key related to a dynamic code

Actions:

6/1/2017) Verification bounty started
7/6/2017) Alan perform a valid verification. New dc become «def»
7/31/2017) Bob read «def» from tag, perform a verification on blockchain, but doesn't write new dc «ghi» on NFC
8/15/2017) Seller read «def» on tag, and discover a «not original» object into its store. He performs a restore verification, with «def» as last valid verification. This burns all bounties between 7/6/2017 (when «def» has been written) and 7/31/2017 (last verification reported on blockchain)
9/9/2017) Carl buy the object

Verification bounty: 100 finney
Burn incentive percentage: 5%

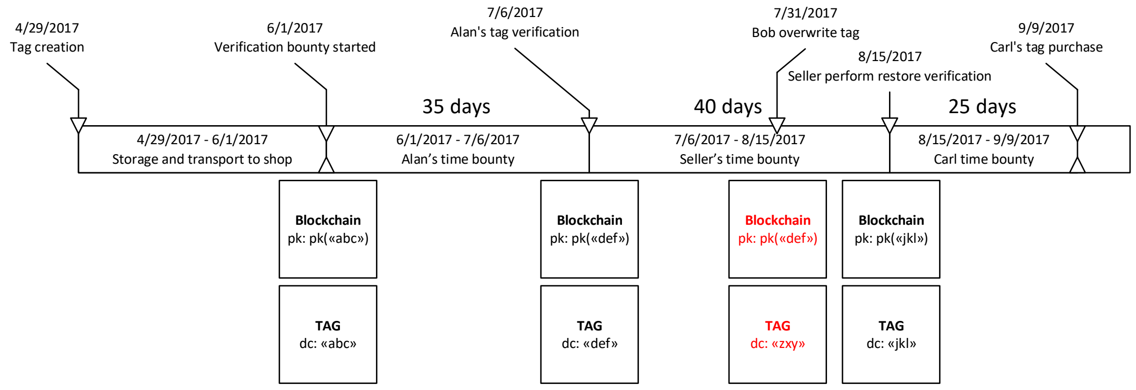
Received bounty:

- Alan: 35 finney
- Bob: ~~25 finney~~ 0 finney (burned)
- Seller: 15 finney + (25 finney * 5%) = 16.25 finney
- Carl: 25 finney

Figure 3 restoring originality with a "burnt" bounty

Restoring the originality of an object can generally be performed by the tag owner, an authorized and identified vendor profile or the authorized and identified manufacturer.

Although NFC tags are protected from accidental writing, the dynamic code might be altered by some malicious intent. If, during restoration, the seller cannot indicate a valid previous code, then the seller will simply perform a normal verification by restoring originality without burning any bounty. Verification of the seller will still receive 100% of the expected bounty as a regular validation.



Legend:

Blockchain	Tag's values on blockchain
TAG	Tag's values on NFC

* **dc**: dynamic code (private key)
* **pk**: public key
* **pk(dc)**: public key related to a dynamic code

Actions:

6/1/2017) Verification bounty started
7/6/2017) Alan perform a valid verification. New dc become «def»
7/31/2017) Bob overwrity tag with an altered code «zxy»
8/15/2017) Seller read «zxy» on tag, and discover a «not original» object into its store. He performs a restore verification without any previous valid code.
9/9/2017) Carl buy the object

Verification bounty: 100 finney
Burn incentive percentage: 5%

Received bounty:

- Alan: 35 finney
- Bob: 0 finney
- Seller: 40 finney
- Carl: 25 finney

Figure 4 restoring originality without a "burnt" bounty

This means that the oldest unsold objects will have on average higher values to be collected, encouraging "hacking the hired" and consequently stock recycling. It will also be possible to create special objects linked, for example, to hunting campaigns at the prize where it is made public that one of the pieces issued contains a greater bounty verification than the others, but without saying which one.

4.2.2 Dynamic code updating

The code upgrade will be by encrypting its Ethereum address with the dynamic code on the tag, which is a private 128bit (UUID) or 256bit elliptical encrypted key, and enclosing the public key of a new encryption randomly selected by the client. Instead, the contract will decipher the posted address with the current public key and then verify that the verifier author corresponds to the transaction's author, so the private key read is correct.

128bit elliptical key encryption is considered to be on average secure, equally safe for a 64-bit AES key and would take about half an hour of brute force attack from the current Bitcoin mining power to be broken.

Bitcoin currently only produces, consumes and consumes around $ 75,000 every half hour, all to get only one portion of the bounty of an item, which can also be canceled by a seller. However, to protect really important figures may not be enough, and in that case, you will need to use 256bit encryption.

This would equate to a 128bit AES, which with the current Bitcoin computing power would take 10^{12} years to be broken (it is the same protection used by Ethereum)

4.3 Purchase

The purchase will be executed through a secret key printed with a code (QR o other) on the tag, this code can be discovered only with an irreversible mechanical action on the TAG. It is needed to perform a transaction that will sign your address with the key found. On chain a contract will verify signs with the public key and verifies that the address shown corresponds to the buyer's name. This way the purchase will be authorized.

4.4 Exchange an resell of used products

It will be possible to resell the objects owned by a contract that will certify the seller's actual possession of the object and collect the buyer's payment. Only when both parties have successfully completed the transaction will the contract release the credit to the seller and will automatically transfer ownership to the buyer.

Payment can be made in ether, as well as in other currencies possibly regulated by a certification oracle. The exchange currency and the desired quantity must be pre-set before the transaction.

It will also be possible to transfer the property of a tag without a money counterparty transfer, but the operation must still be authorized by both parties.

4.5 Personal products & "minibrand"

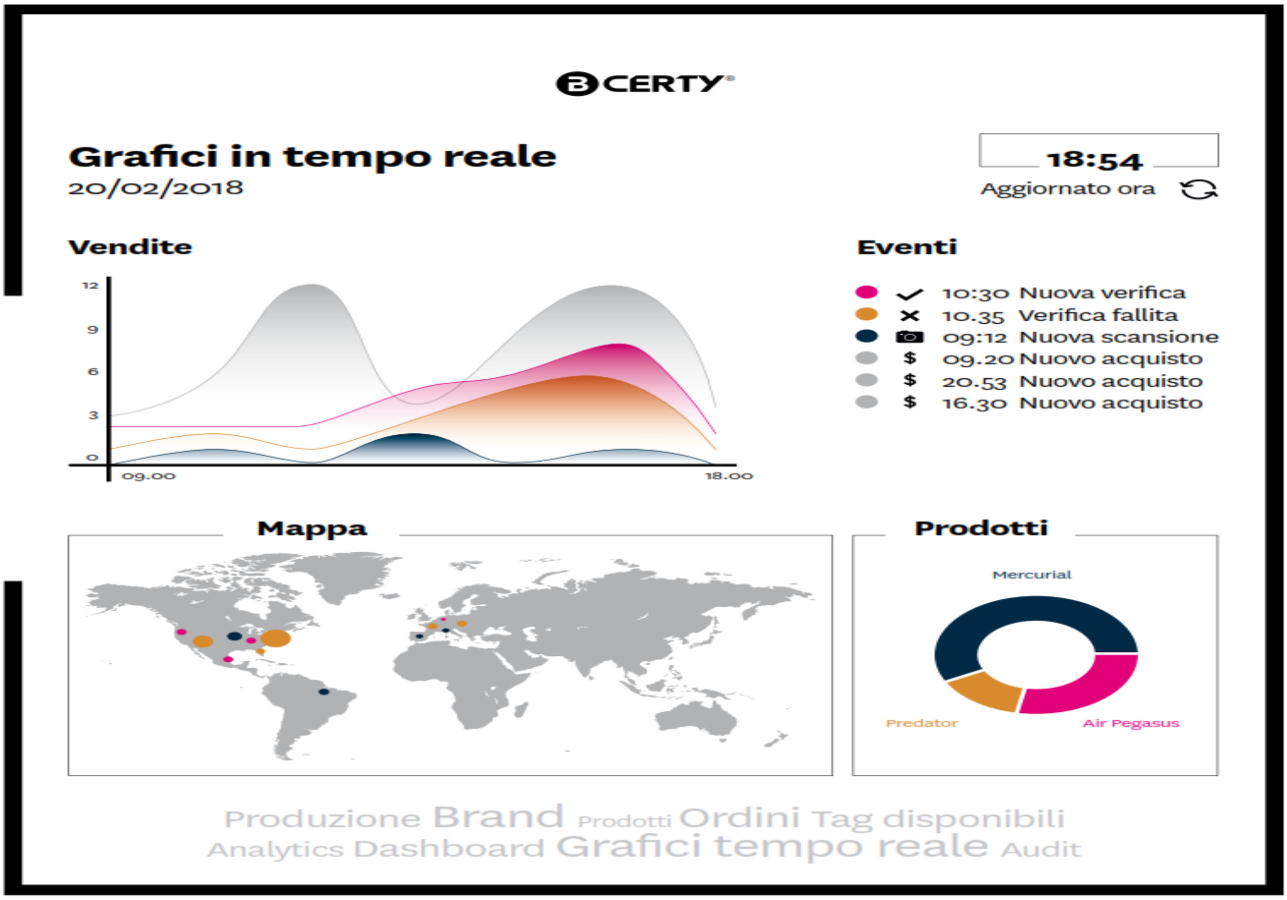
In parallel with the development of the blockchain service, BCerty intends to further develop the service offered, allowing each individual user to create tags and correlate them to their products. This project, called "minibrand", aims to make the bCerty service known as much as possible. By doing so, increasing the knowledge of the name of the service within users, it will be easier to market it to major manufacturers.

Each user can then become a small producer, offering a free service for producing and managing some ten TAG content. The token value of a larger number of managed tags will, however, remain at a level slightly higher than that of the tags offered in larger volumes for small producers. This is to offer even small realities who want to try to create a personal brand, the ability to propose unique and globally recognizable products

4.6 Analytics

User data analytics will be available to everyone regarding blockchain public data. They will then be able to supply the producers themselves with report extraction. Howerver, analytics may eventually be disabled on the application even if data are anonymous and consciously given.

We will only offer exclusive access to anonymized data collected from our applications analytics, such as the GPS location where verifications and purchases are being made, or readings and verifications (also failures) that will be communicated to our service. We will also have access to counterfeit product reporting data, i.e. products covered by counterfeit bCerty technology and therefore with buyers/inspectors failed checks.



CERTY

Grafici in tempo reale
20/02/2018

18:54
Aggiornato ora

Vendite

Eventi

- ● ✓ 10:30 Nuova verifica
- ● ✕ 10.35 Verifica fallita
- ● 📷 09:12 Nuova scansione
- ● $ 09.20 Nuovo acquisto
- ● $ 20.53 Nuovo acquisto
- ● $ 16.30 Nuovo acquisto

Mappa

Prodotti

Produzione Brand Prodotti Ordini Tag disponibili
Analytics Dashboard Grafici tempo reale Audit

5 State of the Art

Business and service development has already begun, the company currently offering the service is an Italian s.r.l. company named DigiCanDo. We have already achieved the first concrete results. Next are summarized the main points.

5.1 The Applications

The service is currently able to administer the production of tags for different brands and products, purchasing and verifying them. It manages user profiles, allows you to leave certified comments on purchased products, and personalize them with private notes and images attached.

The core of the infrastructure is a server application built with Asp.Net Core and based on the MongoDB document database, all of which is hosted on a cloud network. The web portal consists of a consumer part dedicated to the end user, and a production panel dedicated to Brand Operators, where they can administer items and tags for their products. Everything is designed to be mobile-compatible.

We have developed a consumer-compliant client application for the most popular platforms: Android, iOS, and Windows. We use the Xamarin framework for synchronous development of the three applications. The application reproduces the consumer portal aspect of the web portal and adds features that require physical access to hardware devices, such as originality verification with NFC.

We have also implemented a desktop production application for Windows environment, dedicated to companies that want to certify their brand with our service. With this application you can scan the in-line production tags, activate them, and print their labels if necessary. In the future, we intend to make the application compatible with both Linux and Mac OSX environments.

5.2 Commercial agreement

DigiCanDo has signed a partnership agreement with *Visottica-Comotec*, the leading manufacturer of metal components for glasses and with it wants to penetrate this sector.

Similarly, other companies supplying important components in the various sectors have been approached for the purpose of signing similar agreements. We quote as an explanatory example but not exhaustive the *Okinawa* leather label maker with which we want to propose the bCerty service by inserting an NFC chip inside the labels.

A first field test was carried out by applying the service to 8000 bottles of wine from the *Laimburg* wine cellar of Bolzano.

The company's real business activity began in the spring of 2017; Previously, from October 2016, we presented the product to companies in different product sectors to get feedback and improve when we received objections to the status of the service. At present, a dozen negotiations with small, medium-sized footwear and clothing companies are active, with which negotiations are heavily influenced by design timeframe in the fashion industry.

5.3 The reference market and the competitive advantages over the competition

The service currently offered by DigiCanDo competes with companies from different sectors. Mainly the competition takes place with startups that offer anti-counterfeit services, among them in the current market there are competitors who propose service with smart NFC tags. We will not go on to analyze the robustness of the systems used, while knowing the other weaknesses, but only what is perceived by the market, the offer of services that can offer added value to competitiveness.

Additionally, the service can compete with agencies dealing with market profiling and direct marketing analysis.

A hybrid system like the one presented, it offers several advantages. By concretizing the development on Ethereum currently we can highlight the following advantages:

- all the features that are migrated to smart-contract are in fact completely decentralized and unstoppable. There can be no one (who does not have the private key of BCerty) that can stop the execution of the contract or block access individually. This also includes DDOS-type invulnerability.
- Blockchain content is permanent and unalterable. This implies that it is impossible for any attacker (or for BCerty himself) to alter the past history of the data.
- This implies that any value is distributed on blockchain, whether it is economical or commensurate with a generic asset (such as the property of a tag), is highly reliable and certified. On blockchain the value of a virtual property is real, and comparable to something physical.

- The property of an asset on blockchain is incontrovertible, since anyone can demonstrate transparently that he is the owner of a value he owns.
- Users will be able to fully use the service published on smart-contract, but subject to our rules. This implies that:
  - we can reach with our system even users who would normally refuse to use our service, for example, for data processing issues;
  - we can continue to analyze the usage that is being made, what properties are exchanged and what actions are generally executed, but accounts potentially anonymous;
  - we can determine the degree of autonomy and freedom to give users. For example, we can decide to produce only the token to deploy to represent the property of the objects, or we can give users the ability to create their own. We can define precise rules for exchanges, or decide not to define it at all, and so on;
- Blockchain also allows you to set up a transparent review system, which makes it clear to everyone that the reviews posted really come from people who bought the original product: one purchase, one review. Such reviews will be unmistakable, unalterable (if not the author), and will therefore gain a remarkable value over any review deposited on a central server, where it is easily manipulated.
- We can publish the open source contract solution. The contract itself is compiled in machine code, and is therefore difficult to interpret, except through reverse engineering. However, by deciding to publish the source code, the community can compile it and verify that the published contract corresponds to what has been stated. This would eliminate the need for the user to trust BCerty's work, effectively increasing the trust of the service.
- Blockchain is currently one of the major innovation frontiers. Adopting it now would mean projecting into the cutting edge of web services. This would benefit the company's image and could be used as a marketing tool. This would also lead us to a situation of advantage in comparison to the competitors, who would be forced to pursue innovation.
- With a sufficiently versatile implementation, we could impart ourselves as a de facto standard for the certification of non-economic property ownership over blockchains. Currently there is no service yet doing so.

5.4 Research and development

In addition to the main theme of this document, namely blockchain and decentralization, the team, which is the DigiCanDo’s team, has already done in the past, and is still pursuing technology research. It is in fact an innovative startup, and already won a call in the province of Bolzano for this research.

Two original research projects have been developed in the software field:

- ODM (Object-Document Mapper) for MongoDB in .Net environment
  Document databases are getting more and more popular, but there is no effective solution for interaction with them that is comparable to an ORM for relational databases. An original solution for MongoDB has been developed that implements some key functions such as interconnection between different documents, lazy loading and optimization on preventive uploading of some information from linked documents to reduce disk operations. At present, bCerty service is based on this technology implemented and currently in development. It is like to release the open source code in the next future.
- Data filter and operations on application domain

By increasing the complexity of applications, it is often more and more difficult to control effective access to data and actions by various users, who will necessarily have different roles and accesses. Also, when a domain provides a data in response to a query, this may consist of information normally unavailable to the user and should be filtered. This usually leads to duplication of access information on multiple points of the application.
We must also make sure that this information is really secure, and cannot be claimed, for example, through the application layer bumps, or through particular data copying or data strikers.
Our de facto solution places a central layer of permissions that filter access directly to the application domain, preventing user access to the application logic itself, where the user does not have the permissions required to request access.

By hardware point of view we develop multiple custom prototype of NFC tags for different applications and size.

6 Migration Plan

The ultimate goal of the project is to create a decentralized platform for tracking and managing products from production (correlating a tag to an object with all the properties and related information) to after sell, certifying the originality and property of physical or virtual objects.

Planned migration will ensure the continuity of service in its entirety. The blockchain components will be implemented incrementally and the data will be gradually transferred to the new platform. All the data we manage on blockchain will always be accessible by the API of our service.

The achievement of this is preceded by some intermediate milestones as it is intended to divide this part of the project into different phases.

6.1 Users identification and TAG management

Initially, a fully functional infrastructure based on traditional cloud-client technologies is expected to be implemented, in which all data is maintained on our servers and databases. This installation can evolve in functionality almost independently of the rest.

The parallel development of the core of the blockchain-based application will take place. We will start producing the first decentralized tags, once we will be able to provide an infrastructure that meets Layers 1 and 2 (basic identification, tagging, and verification).

6.2 Project phases

Subsequently, blockchain integration of the application layer will be made available, such as content production and product blockchain evaluation. However, development of this point requires the development of the Ethereum infrastructure, and specifically of Swarm.

The second phase will consist in the creation of the production environment, i.e.: in the software development of an architecture for a system that allows the correlation of a bCerty tag (each marker) to each product object. This correlation will bring with it all the information about the product and will enable the certification of the supply chain as well as the originality of the product. All product data will then be managed in a transparent and decentralized way through the blockchain.

In the third phase, the instrument that allows the transaction of ownership of the product to be certified must be realized; this is one of the phases that can probably be conceptually simpler, given the intrinsic ability of the blockchain to handle transactions.

The next project goal is to create a platform that allows control and verification of objects. It will be a web based or even native application for different operating systems, which will use the information on the tag and compare it with what is stored in the blockchain to provide anyone with a transparent certainty of the authenticity of production data that, without the need for any external or superior body, certifies the ownership and originality of the products.

The ultimate goal is therefore to integrate the above-mentioned outcomes to implement the service contract ecosystem, that is, the set of software modules that interact with each other, providing the basic functions for managing objects at the baseline level: creation, purchase, exchange and verification of originality and property.

In this way, you will get a decentralized platform that can guarantee the originality of a product with certainty and that it will continue to ensure that a certain user purchases the product. Additionally, the data is transparent and constantly accessible to everyone while maintaining the privacy of each user.

Schematically the intermediate objectives that lead to the project's ultimate goal:

- the development of an IT infrastructure based on blockchains, which allows the recognition of operators of various levels of service;
- development of a software environment that allows certified correlation of bCerty tags to each single "real" product.

7 FUTURE VISION

In the future, it will be possible to transform the physical tags into smart tags that can be associated with specific contracts for certain functions defined by the manufacturer. You can make programmable objects of any kind, to associate information, roles, and behaviors. All of this is managed by a framework that will guarantee the authenticity of the object, ownership by a user and possibly transferability of the object. For example, we can handle shipping subscriptions, event tickets, loyalty cards, energy utilities, and so on.

8 TIME LINE

Following is a road map of the main points for project development. In each case we consider that as this is a state-of-the-art development environment and where research is very active, actual implementation times may vary from forecasts:

- **November 2018 – Identity service**
  Design and implementation of the infrastructure for managing the entities involved in the service. It must be able to handle certificates to the operators, and to guarantee the privileges of action based on the roles covered.
- **February 2019– Production Manager**
  Design and implementation of the tag production and management system. For these it must provide the basic functions of production, purchasing, verifying originality and exchanging between users.
- **June 2019 – Integration with actual platform**

The use of blockchains differs substantially from the use of a central infrastructure service. Therefore, integration between the two worlds must be studied and implemented, both from the point of view of user experience and from a technical point of view, in order to progressively move from architecture to architecture.

- **2020 Migration and development of other decentralized features**
  The bCerty system will migrate into its capabilities more and more on blockchain infrastructure.

9 THE TEAM

People currently involved in this project are:

- Sergio Marchese, co-founder and CEO
  Graduated in Electronic Engineering at the University of Padua. He has experience in manufacturing and commercial organization of companies. He deals with the general administration of DigiCanDo.
- Mirko Da Corte, Co-Founder and CTO
  Graduated in Computer Science at the University of Udine, he has the role of administering the technical development of the project, and in particular aspects of IT.
- Andrea Stona, Co-Founder and Hardware Manager
  Graduated in Physics at the University of Padua, he is responsible for DigiCanDo's hardware development. He also owns the company Kerr Srl, of which he is founder, in which he designs electronic components and ASICs for the consumer and industrial sector.
- Mattia Dalzocchio, developer
  Graduated in Communications Interfaces and Technologies at the University of Trento, he deals with the development of aspects of user experience and front-end projects.
- Nicolò Decet: sales
  Always passionate about high-tech he graduated as an IT expert and then stay updated on the latest technologies. He is a curious and enterprising person with an entrepreneurial spirit that developed as a commercial agent. Love dealing with people and discussing new projects.
- Nicola De Castello: advisor
  Graduated in Economics and Business at the University of Verona co-founded the company DigiCanDo and collaborates in following the business and financial aspects.
- Leonardo Pedretti: advisor
  Leonardo is an attorney and he is focused, since its graduation in Law in 2010, in interaction and effects between financial law and computer science. He has co-founded the first Bitcoin meetup in Italy and he manages a community with thousands of followers on facebook and telegram. He is the founder and administrator of Ethereum Italy, he is the author of the first Ethereum White Paper Italian translation and the first and only Italian who interviewed Vitalik Buterin. He is the cofounder of Inspheer and he built one of the first Italian mining farm of Bitcoin and Litecoin. He does consulting for Holytransaction.com (a cryptocurrencies wallet service).
- Jacopo N. Pedretti: advisor
  Lawyer specialized in financial intermediation. From the very beginning follows all the issues concerning the Blockchain and in particular regulatory aspects. He co-founded the community Italian by Ethereum and Inspheer.