30° Anno

EUSTEMA®

Making Innovation

UniAquila - Workshop 14 maggio 2019

Blockchain and Cryptography
In documentary processes

EUSTEMA
Making Innovation

Agenda

1. Eustema overview
2. Blockchain and Cryptography
3. Document notarization
4. Smart Contracts

EUSTEMA
Making Innovation

Stay ahead
WITH OUR TEAM

500+ PEOPLE
DELIVERY MANAGEMENT

Continuous trainig, development paths and career counseling.
More than 350 innovation projects every year.

40+ R&D

Working on avantgarde projects of ICT. Innovation is the driver of Eustema R&D transformation

100 + Clients

PAC and PAL
Utilities
Telco
Trasports
Energy
Finance
Post
Media.

More than the 70% of our clients has been working with us for the last 10 years.

3 headquarters

Strong relationship with our clients thanks to our presence on field.
We build architectures based on innovative technologies.

30 years

Of experience in ICT, a story of innovation, products and succesful projects.
We have been certified Innovative Firm by the Investment Compact decree.

Eustema Traning Lab

640 professional certifications

20.000 training hours

90% trained people per year

Eustema Academy
More than 6 courses per year, 15 students per class, collaboration with universities and research centers.

EUSTEMA
Making Innovation

IT Solutions

IT SERVICES

Data Analytics

Data Governance & Quality
Data Lake & Safe
Big & Fast Data
Self Service BI & Data Analytics

Enterprise Content Mgmt

Systems of documentary repository.
Multimedial and interactive documents.
Unified Enterprise Search

Enterprise Application

Architecture Design
Serverless & Microservices Architecture
Technology Architecture Design
Omnichannel Application Development
System Integration
Application Modernization
Software Quality Assurance

Digital Media

Web Architecture Design
UX Design,
Web & Social Analytics
Web Content Management
Enterprise Social Business
& Collaboration Web, Mobile

GEO/GIS

Cloud Computing

Public & Private Cloud Solution
Cloud Application Migration
IT Transformation
XaaS Management

BPM

Security & Privacy

Security, Privacy & Compliance
Assessment: ISO 27001, GDPR, NIS
GDPR Data Driven
Fraud Management Solution
Ethical Hacking

System Mgmt

Speed up our country growth promoting innovation as a support to our client's businesses.

Our development and research center

Innovation for tradition

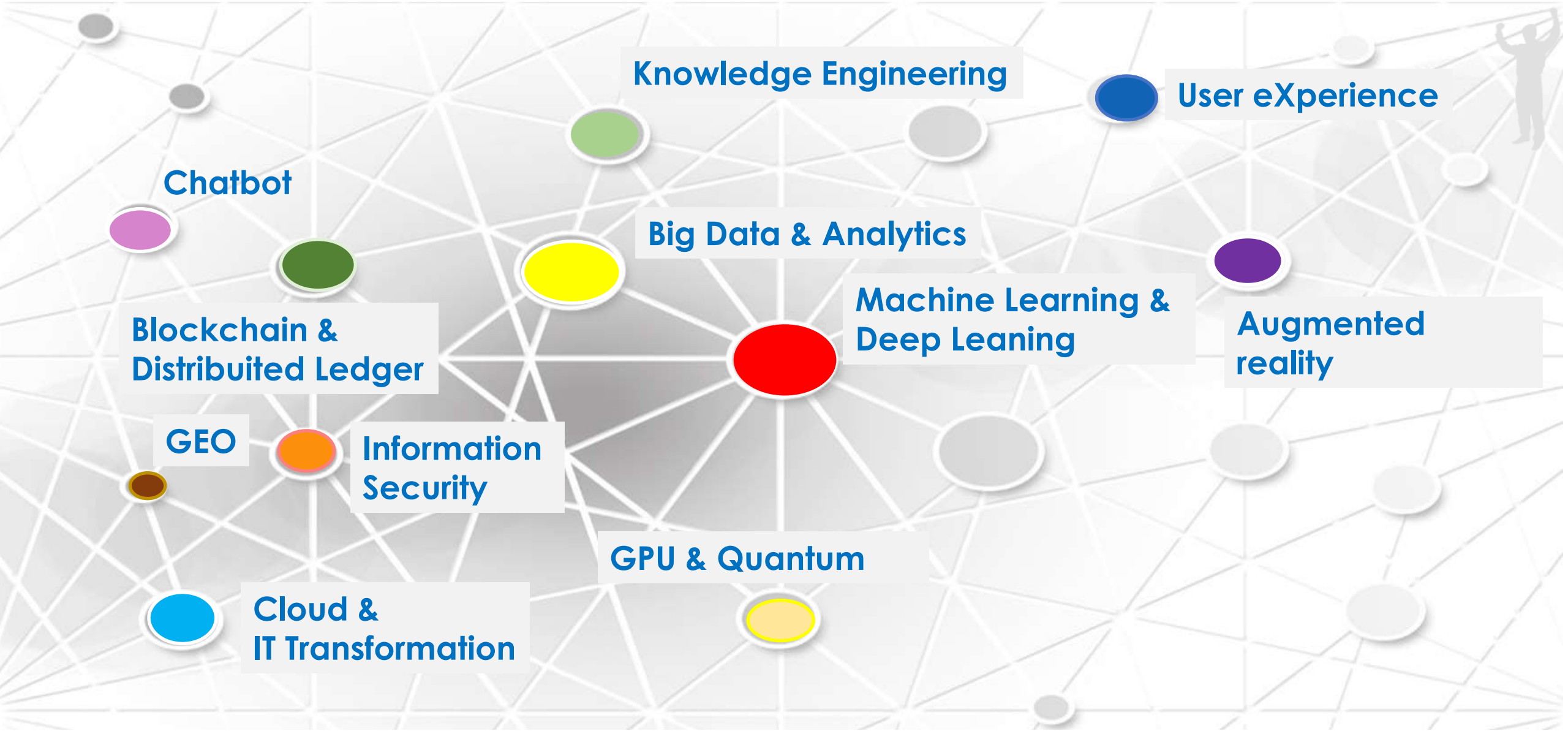
Eustema R&D

What we do

- ✓ Participation to National (MISE, MIUR, POR) and European (Horizon2020) Research Calls.
- ✓ Realization of projects of Industrial Research, Experimental Development and POC
- ✓ Partners of Centro di Competenza ad Alta Specializzazione Industria4.0/MedITec.
- ✓ Partnership with Research Centers and Universities.
- ✓ Participation to Open Innovation Tables.
- ✓ Partnership with Startups.
- ✓ Pre-sale help to innovate our business.

Development and Research center

Technologies



Blockchain for Business

Possible Use Cases

NOTARIZATION: ability to certify informations exchanged in a transaction between two sides, e.g. implements the process of certifying a document. It enables a business to certify the content and timestamp of a document.

TOKENIZATION: process of digitalization of a real asset (e.g. creation of financial assets). It can be used to create new coins on a network.

SMART CONTRACT: way to digitalize a real contract in the form of software code. It allows you to automate actions associated with its clauses, as well as any related payment actions.

Blockchain for data integrity

Security and Privacy

1. **Confidenciality (C):** ability to ensure that shared information can only be viewed by those who are authorized to access them.
2. **Integrity (I)**: ability to guarantee the integrity of informations or impossibility of manipulation without this being detected.
3. **Availability(A)**: ability to guarantee continuous availability of informations.

The use of permissioned blockchains with authentication mechanisms, block encryption and end-to-end cryptography, can guaranteed the CIA trade and be compliant with data privacy requirements.

EUSTEMA
Making Innovation

Use case: Notarization

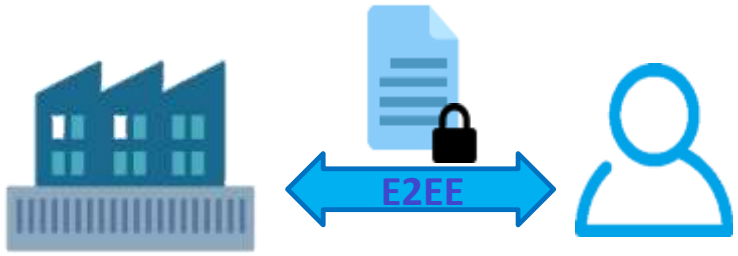
Blockchain4doc

Blockchain4doc is a protection system than can be applied on a documental repository and it is intended to be used within a business network. (Proof of existence).

Security lies in the use of a permissioned blockchain, and end-to-end encryption (E2EE), a lock time that ensures the application Integrity and Confidentiality of the contents, in addition to the guarantee of a correct versioning.

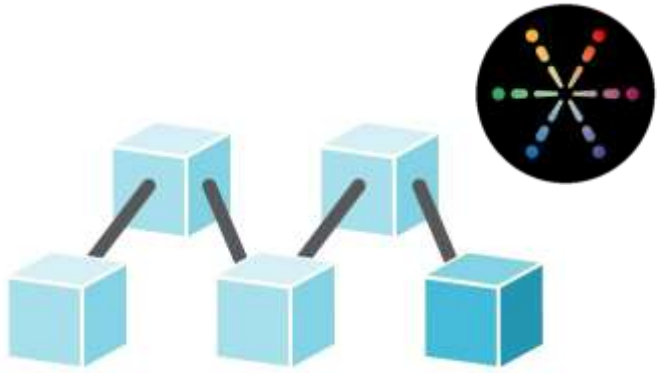
EUSTEMA
Making Innovation

Blockchain4Doc



1. Confidentiality: Protection of documents during transfer from company server to user machine. (End-to-end encryption).

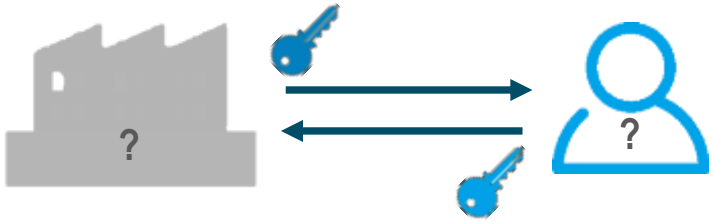
2. CIA: Widespread control by users on the versioning, integrity and authentication of each file(**Blockchain**)



3. LockTime: SmartContract which implements a time capsule to access the document only when certain temporal conditions occur(**Blockchain**)

Blockchain4Doc

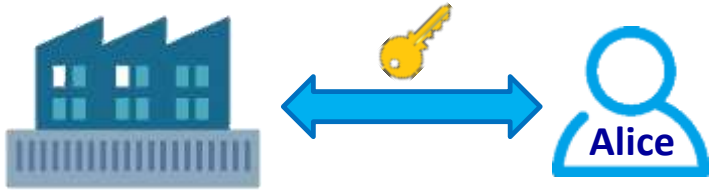
end-to-end encryption (E2EE)



1 Each user has a pair of asymmetric keys that uniquely identify him. These are used during the handshake.

Thanks to the public key – user link, company and employee are mutually authenticated.

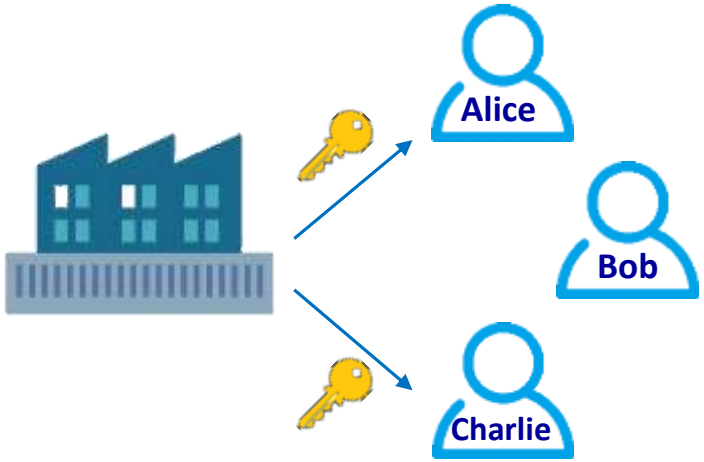
2



3 The material thus exchanged is used to create a secret symmetric key (using RSA, Diffie Hellman).

Blockchain4Doc

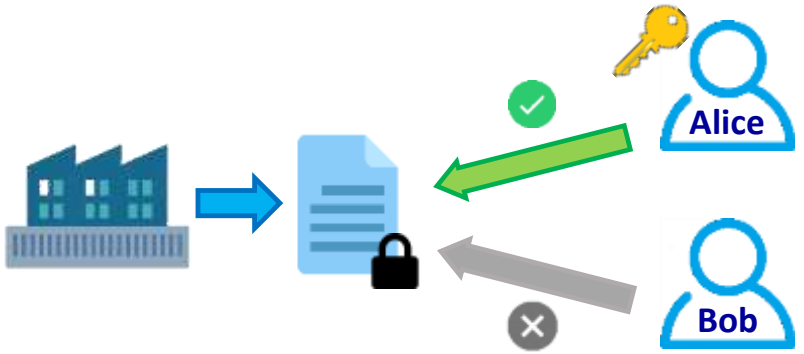
Confidentiality and Privacy



1 The company decides who among the employees can access a given document, and with them creates the relative symmetric key.

Only authorized users (in possesion of a key) can therefore decrypt and read the document.

2



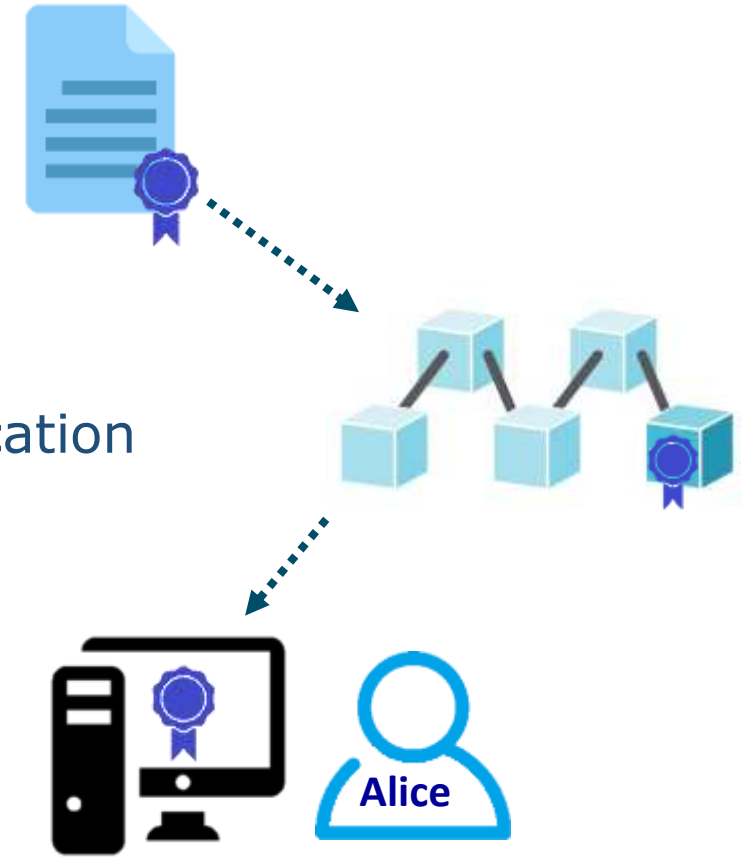
Blockchain4Doc

Flow (1/3)

1. The file / document is uploaded to the document repository.

2. The application receives the upload notification and publishes the document hash and its metadata on the blockchain.

3. Client applications that listen on the blockchain see the transaction and read the hash.



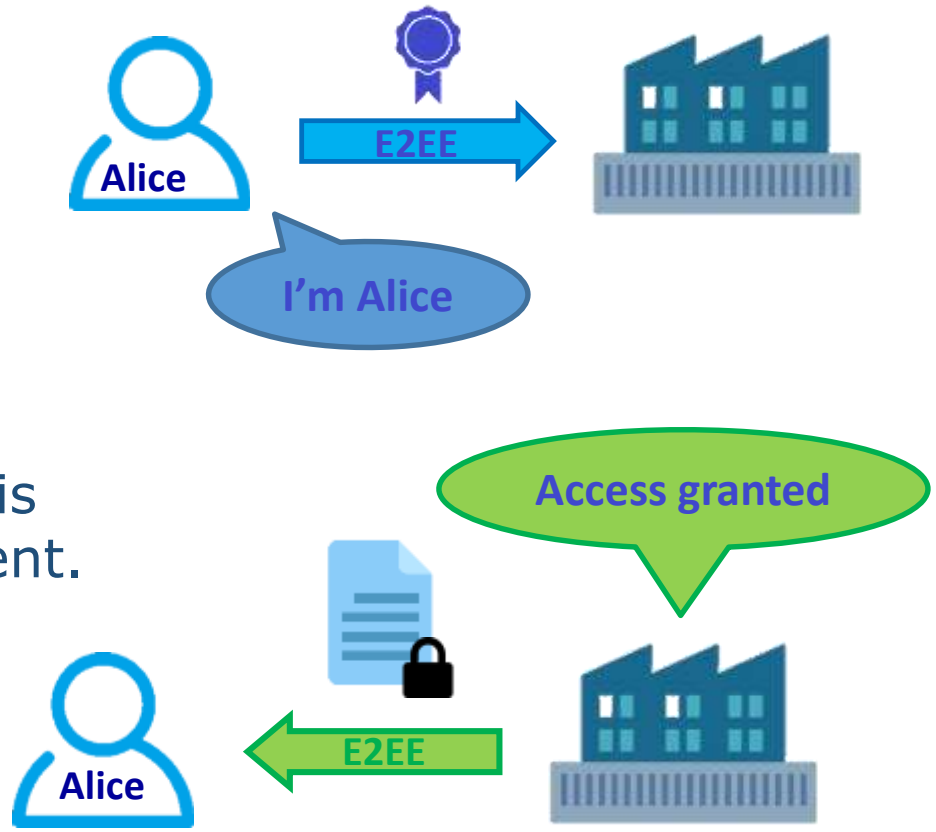
Blockchain4Doc

Flow(2/3)

4. Clients send a request to the company server via E2EE containing the hash read on the blockchain.

5. The server checks that the user is authorized to access the document.

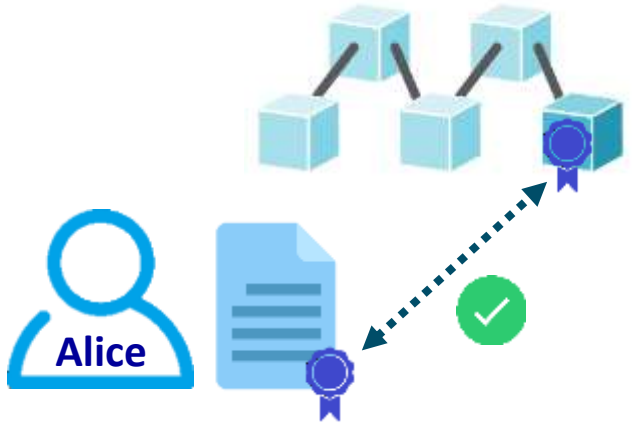
6. Document is sent via E2EE.



Blockchain4Doc

Flow (3/3)

7 Once the document is received, the user calculates the hash and checks that it matches the one read on the blockchain.



8 The client application also acts as a reader, displaying the documents inside it. In this way it is possible to set the revocation of the encryption key if the user no longer has access to the document.

Blockchain4Doc (R)Evolution

Time Capsule (1/2)

1. The user uploads a file to the repository. The file is encrypted with a random key (or chosen by the user).

2. The encryption key is recorded on a block of the blockchain that denies reading until a certain date, through the use of a smart contract (LockTime).

3. The document is protected by a key, saved on the blockchain and inaccessible until the default date.

Blockchain4Doc (R)Evolution

Time Capsule(2/2)

3 When the date is reached the key becomes available. It is possible to make a transaction on the blockchain and access the lock with the key.

4 Each authorized user can then access the key to decrypt and read the document.

EUSTEMA
Making Innovation

Some Blockchain Platforms

- ✓ **Hyperledger:** Private blockchain, open source, has been designed for Enterprise use. Main projects: Indy, Fabric and Composer.
- ✓ **Ethereum:** Public Blockchain, was the first to implement smart contracts and define a new language for blockchain (Solidity).
- ✓ **Corda by R3**: Private Blockchain, the result of agreements between hundreds of banks, was designed to favor the standardization of banking services.
- ✓ **Multichain**: Private but open source blockchain, was born as an extension of the Bitcoin core libraries, with which it maintains compatibility.

ethereum

ripple

HYPERLEDGER

MultiChain

corda

Why do we need smart contracts?

- The key thing to observe here is that traditionally, every modification to a chain of ownership has to be done by some kind of trusted third party. This involved government, lawyers etc who usually charge big fees to make such a change.
- With smart contracts we only need to secure the beginning of the chain to the real world. All ownership transactions after that, can be done entirely electronic. Or rather the work usually done by the trusted third party can be done electronically.

Eustema

NETWORKING

Networking to think to new products, services and innovative solutions.

Companies to realize projects of co-innovation

Partnerships for R&D projects co-financed on National and European calls

End-user for experimentation and validation of innovative projects

Technological Partners and Start up

Proof of Concept

EUSTEMA
Making Innovation

IT Solutions

Products

Enterprise Legal Suite

TELEFORUM FOR
Legal Tech Platform per Imprese e Industrie

CERTO
ProcessoTelematico
Giustizia digitale e Processo Telematico

Knowledge Management

EULERO
Customer Satisfaction & Employee Engagement Survey platform

Radioso!
Machine Learning for Business Processes

PLACITO
Record Management with Geolocalization and space optimization process

Geo & Mobile Suite

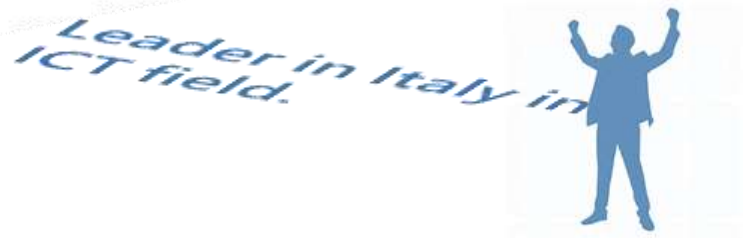
VisitAre
Smart Mobile inspection Systems

GeoTEMA
GIS Mapping & Data Management/Visualization for Weather and early warning

EUTURING
Indoor Positioning & Cognitive Proximity Customer Engagement Solution

Design Tools

ModH
Collaboration & Governance platform for User eXperience Interface



EUSTEMA
Making Innovation

Professional asset

CERTIFICATIONS

- ISO 9001:2015: Quality management systems
- ISO/IEC 20000-1:2011: Information Technology - Service management
- SA 8000:2014: Social Responsability
- ISO/IEC 27001:2013: Information Security

★ ★ ★

Rating legalità
Autorità Garante della concorrenza e del Mercato

EUSTEMA
Making Innovation

EUSTEMA®

Making Innovation

Thank you for your attention!

Donato Cappetta

Responsabile Ricerca e Sviluppo

Email: d.cappetta@eustema.it

Cel. +39 3351409840

Linkedin: www.linkedin.com/in/dcappetta/