GT 50 改善

VISIONARY INNOVATORS

Cryptography

practice implementations

[EPISODE II]

Sandro Fontana,
CEO GT50 sandro.fontana@gt50.org

in Bruce Schneier we trust ⟶ Applied Cryptography 2nd edition 1996

Who we are

GT50 is a Visionary Innovators Company
We are focused in turning technology into real worth applications

GT50 people has got more than 30 years experience in digital security and data protection

We are engaged in combining different existing and robust technologies
like Sym/Asym Cryptography 2D Timbro Digitale and QR Code
to enhance Security and application of Digital Certification Solutions

Our Mission is turning technology into real Value Added Applications,
keeping the best standards in term of security of the process managed

We give Technical Service and Support to more than 100 Customers - Public and Private Market - provided with "Timbro Digitale" Solutions: 2D-Plus and Lambda

We also provide our customers with Consulting Services

blockchain technology

Since 2016 GT50 deals with distributed register technology (DLT / blockchain)

Since the end of 2018, we have activated a FACTOM blockchain node, which can be used by customers as "as-a-Service"

We have also integrated the FACTOM functions into our cloud service "Digital Stamp λService" for notarization of documents.

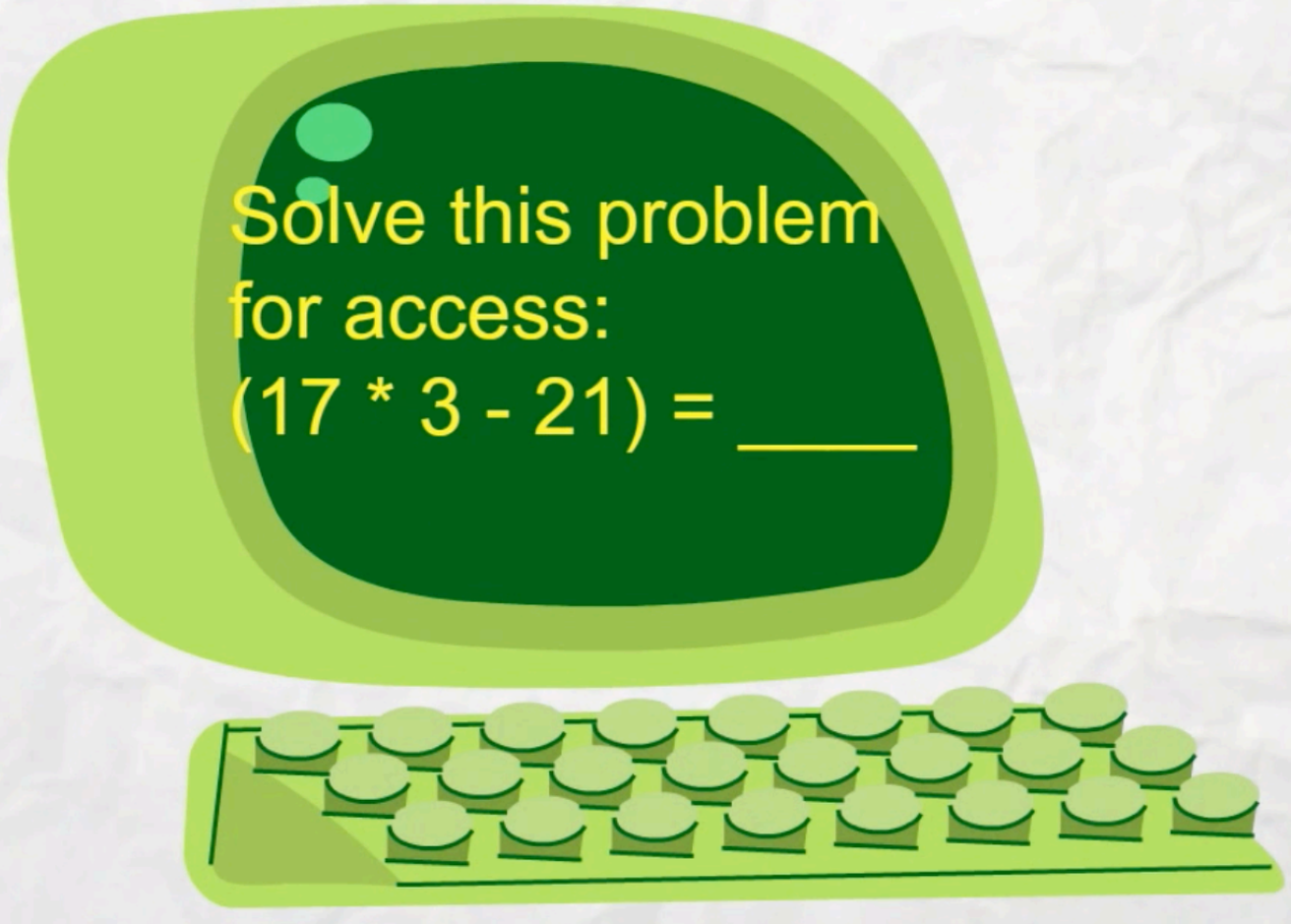
in September 2019 we activated a node of the Quadrans blockchain, a blockchain compatible with the EVM (Ethereum Virtual Machine), but with a very powerful consensus protocol.

By the end of October, we will also activate an Algorand(i), blockchain node, which promises to implement the first permissionless blockchain, with immediate and scalable transactions.

(i) founded by Silvio Micali, an Italian computer scientist and professor at MIT; he won Turing award in 2012(the equivalent of the Nobel prize in computer science)

there are two kind of cryptography in this world:

cryptography that will stop your kid sister from reading your files, ...



there are two kind of cryptography in this world:

... and cryptography that will stop major governments from reading your files.

http://bit.ly/GT50-Videos

Cryptographic Suite:
ETSI (EU)
NIST (USA)

other sources:
ISO
RFC

to avoide case like
Kuznyechik block cipher
&
Streebog hash function
http://bit.ly/2E2XL9S

GT 50 改善
VISIONARY INNOVATORS

what we do

Timbro Digitale

RSA2048
SHA256
XML/XSL

CAdES

LAMBDA SERVICE

RSA2048
SHA256
AES256

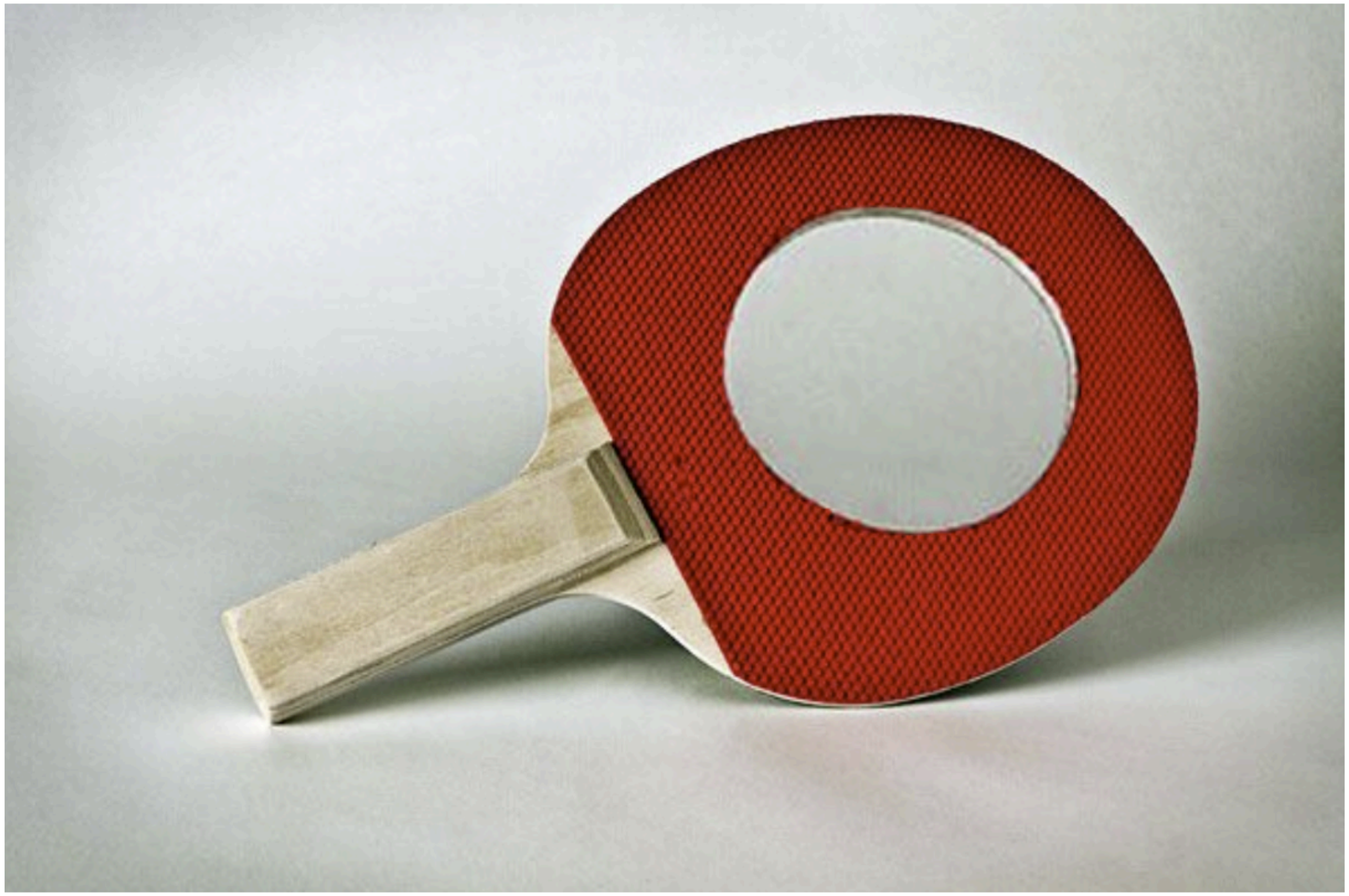
PAdES

Q-ID

A1024/2048
SHA256
BCrypt
AES256
OATH rfc4226 / rfc6238
OCRA rfc6287
QRCode

PhotoShield

RC4
SHA256



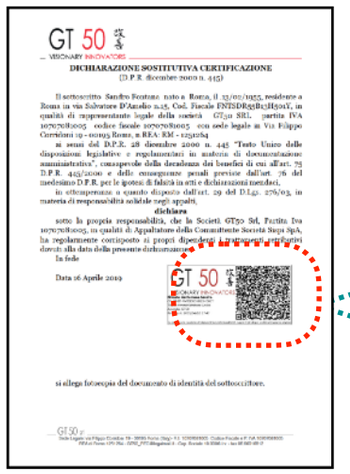
how about the value of
the printing of a digitally signed document?

GT 50 改善
VISIONARY INNOVATORS

what it is

LAMBDA SERVICE

Lambda Service allows you to generate digitally signed PDF (PAdES) documents, customizing the signature area, in which a special secure QRCode (λSeal) is inserted.


GT 50 改善
VISIONARY INNOVATORS

DICHIARAZIONE SOSTITUTIVA CERTIFICAZIONE
(D.P.R. dicembre 2000 n. 445)

Il sottoscritto Sandro Fontana nato a Roma, il 13/02/1955, residente a Roma in via Salvatore D'Amelio n.25, Cod. Fiscale FNTSDR55B13H501Y, in qualità di rappresentante legale della società GT50 SRL partita IVA 10707081003 codice fiscale 10707081005 con sede legale in Via Filippo Cervinara 19 - 00133 Roma, n REA: RM - 1251264

ai sensi del D.P.R. 28 dicembre 2000 n. 445 "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", consapevole della decadenza dei benefici di cui all'art. 75 D.P.R. 445/2000 e delle conseguenze penali previste dall'art. 76 del medesimo D.P.R. per le ipotesi di falsità in atti e dichiarazioni mendaci,

in ottemperanza a quanto disposto dall'art. 29 del D.Lgs. 276/03 in materia di responsabilità solidale negli appalti,

dichiara

sotto la propria responsabilità, che la Società GT50 Srl, Partita Iva 10707081003, in qualità di Appaltatore della Committente Società Sisgi SpA, ha regolarmente corrisposto ai propri dipendenti i trattamenti economici dovuti alla data della presente dichiarazione.

In fede

Data 16 Aprile 2019

si allega fotocopia del documento di identità del sottoscrittore.


GT 50 改善
VISIONARY INNOVATORS
Firmato da: Fontana Sandro
CF: TINIT-FNTSDR55B13H501Y
Titolo: Amministratore Unico
Azienda: GT50
Firmato il: 2019/04/16 17.47

La copia su carta è conforme all'originale firmato in formato PAdES. Leggere il QrCode per accedere al documento originale

λSeal

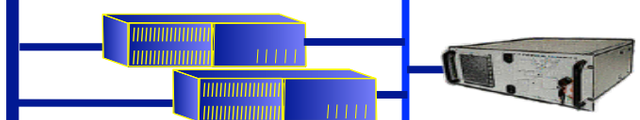
Moreover: A) a crypted copy (AES256) of PAdES file is stored in cloud:
the only instance of the key is contained in Lambda Seal
B) if requested, an "entry" is generated into FACTOM blockchain
as notarization

LAMBDA SERVICE

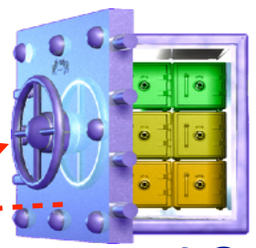
sending PDF file

return signed PDF files

λPeS / αPeS



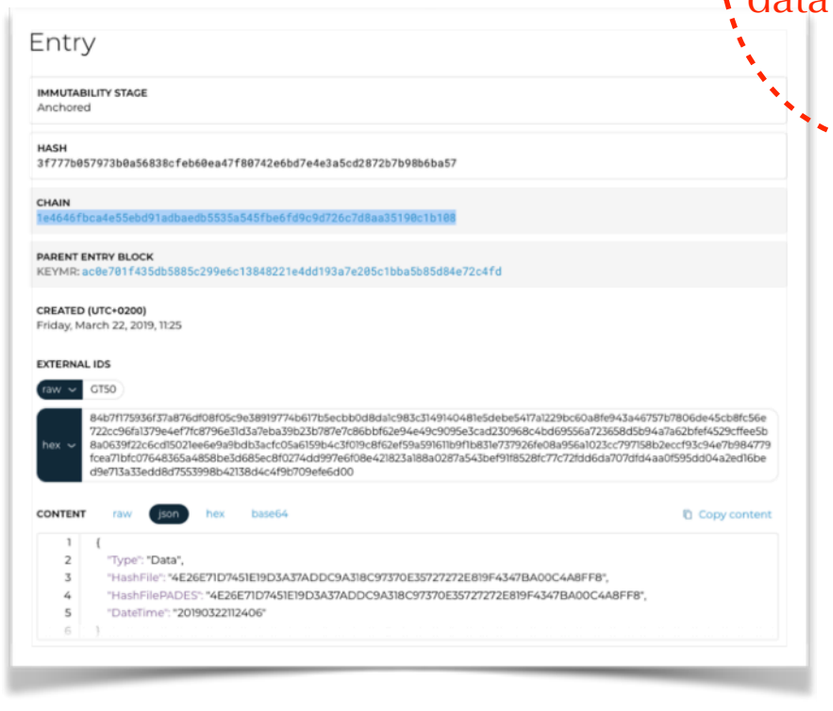
encrypted copy of
signed PDF files (PAdES)

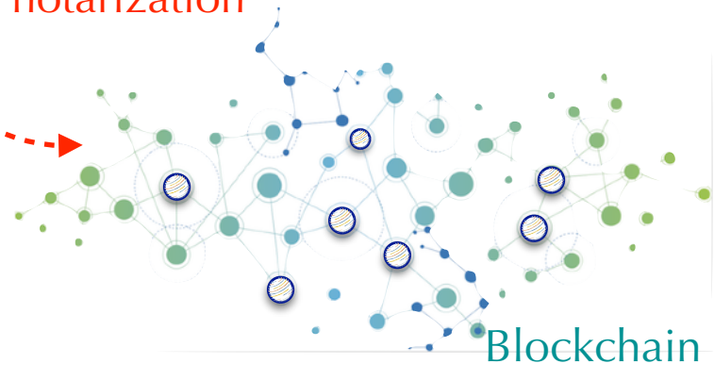


λStore
Data Base on-line

Universal
QReader™

data notarization





Blockchain

contents

λSeal

contains metadata needed to retrieve the (encrypted) PAdES file from the cloud and the unique key to decrypt it

The contents could be sealed using RSA 2048
(not standard format seal)

Universal QReader™ a free App for smartphones and tablets, downloadable from PlayStore(Android) and AppStore(IOS)

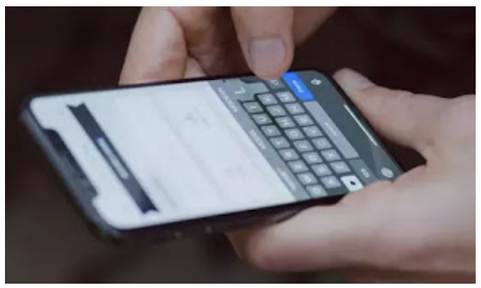
TR

True Reporter

news source origin verification

True Reporter: operating environment

In today's world, information - photos, videos, recordings, text - is increasingly being created by simple citizens/readers (with the desire to publish) or freelancers; in this context - and often also in the professional world of reporters - smartphones have replaced cameras and workstations.



The use of this model, involves a series of risk:

- the ease with which this information is produced and shared, makes it difficult for the owner to protect it from misuse and to claim own intellectual property right;
- those who have to use/publish the information, need to verify with certainty at least the provenance of the news and need a kind of non-repudiation by the reporter;
- without any provenance certainty, for all of us there is a great difficulty in extracting real news from the sea of misinformation;

True Reporter: operating environment

It is therefore necessary to have:

a system that is easy to access and that allows - on the one hand- to certify where, when and by whom a piece of information has been produced

at the same time, to provide the producer (reporter) with a record of the event and its content that allows him/her to prove forever the ownership of the information itself.

a place where is possible store any kind of information, in fully compliance with GDPR(*)

with these boundary conditions, the integration of an App on our smartphone, cloud computing and blockchain technology create a suitable tool for the purpose.

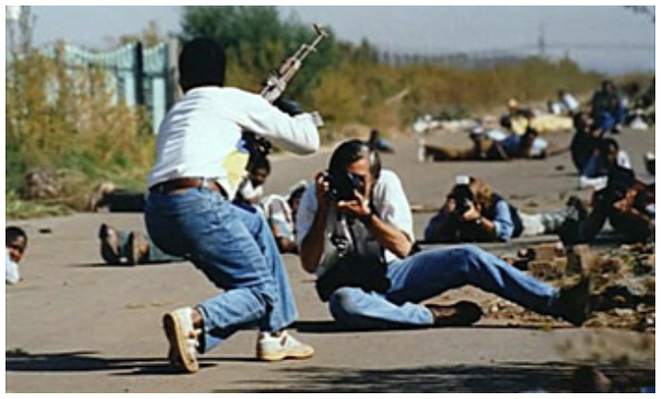
(*) General Data Protection Regulation (EU) 2016/679

True Reporter: available technology

It is not necessary to remember that we currently no longer own smart phones.

What we always carry with us is an extremely powerful computer, always connected to the Internet.

With its various functions, this computer allows us to photograph, shoot videos, record voice, write texts ... and of course even make phone calls.



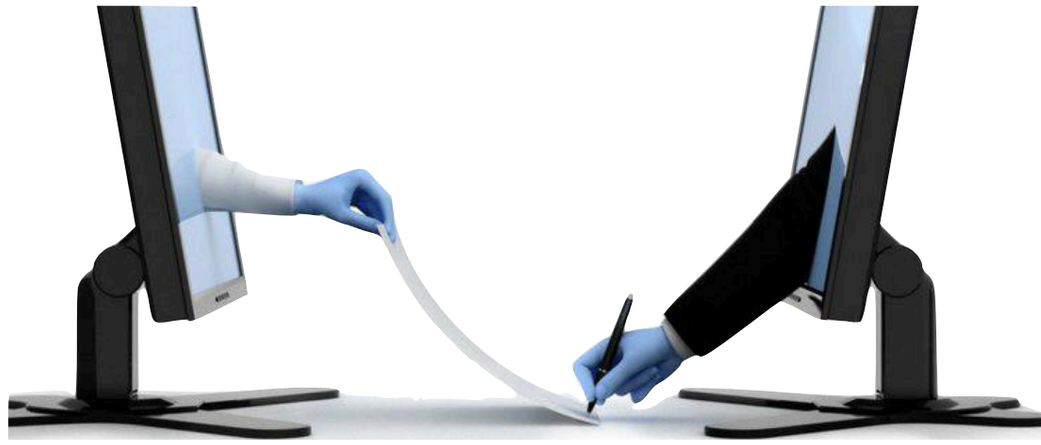
The operational context and the need for immediacy do not allow the availability of a trusted third party to operates the process of certification of the data.

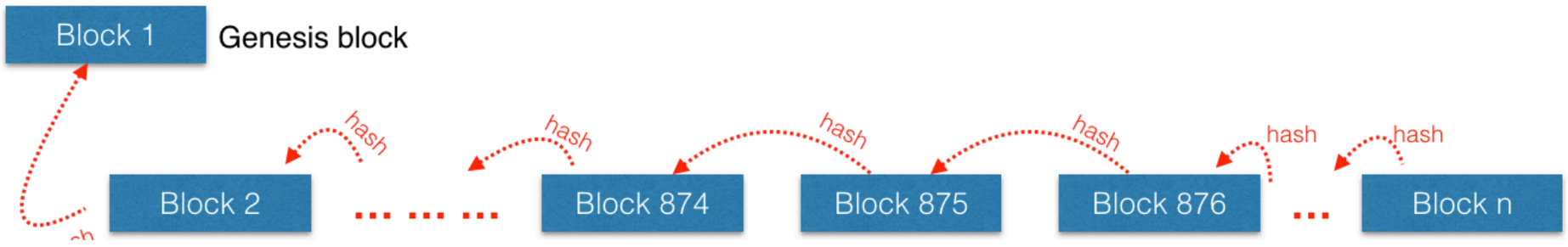
Nevertheless an information certification process - created by our mobile phone - perhaps in the face of a sudden event and in unpredictable places, is a challenge that can be met.

True Reporter: available technology

However, the current technology allows to overcome the many doubts and the real problems of this kind of certification

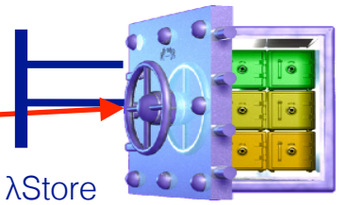
The electronic signature and the blockchain or more generally the DLT (Distributed Ledger Technology), can be one of the tools to support this need.





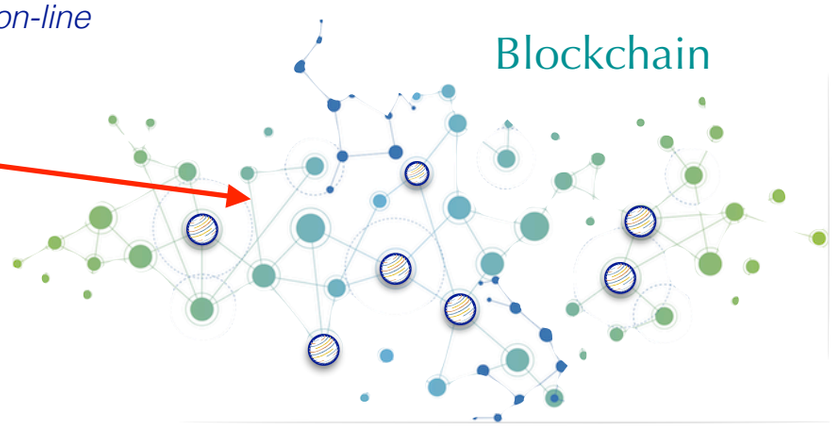
Using True Reporter Platform/1

sending photo/video/audio/text
signed and encrypted



λStore
Data Base on-line

Blockchain



It allows a reporter to film and photograph and record and write a text, then create a Lambda transaction that includes all these elements.

The transaction is inserted into the blockchain and signed with its access keys.

The data are stored online in encrypted form in λStore, which does not know the encryption keys.

Using True Reporter Platform/2

The transaction includes a PAdES receipt that summarizes the time, geographical coordinates and all the elements of the event: photo, film, text, voice recording.


TR
Activity/Event Receipt
24 June 2019, UTC 14:02:44 geographic coordinate : 41°54'39"24 N; 12°28'54"48 E
TEXT:
lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
VIDEO RECORDING:
File immagine documento identità: 20190624 SFN CIE.jpg
VOICE RECORDING:
File immagine Tessera Sanitaria: 20190624 SFN Codice Fiscale.jpg
PHOTOS
-File Contratto Assicurativo: 20190624 SFN contratto A-6987654.pdf
-File video accettazione ed attivazione Polizza: 20190624 attiva polizza.mp4
DIGITALLY SIGNED

Each of these elements is indicated with its hash;
in this way the PAdES receipt implicitly signs all the data.

In the graphic area of the PAdES signature there is a Lambda Seal, in which the data decryption key is present together with the metadata that allow access to the information stored in λStore.

This mechanism allows the reporter to demonstrate ownership of his work, while providing users, newspapers or news distributors, with a certain means to identify the source of what is presented.

At the same time, online data is protected by strong encryption: AES256

Using Smart Contracts (Quadrans)

the evolution of the platform will allow the creation of tokens connected to the intellectual property of the Reporter.

In this way, it will be possible to sell temporary or definitive rights of commercial exploitation (publication) of the information.

In this case the reference blockchain will be Quadrans, because it promises to make an EVM available without Ethereum's performance constraints

quadrans FOUNDATION

Thank you for your attention

Sandro Fontana, sandro.fontana@gt50.org
CISSP, ISO27001 L.A., CISM, CISA
skype/twitter: sinetqnlap
http://sandrofontana.com