陈安瑞

trustseed

# GDPR REGULATION
# IS THE CHALLENGE OF TRUST IN THE DIGITAL AGE

陈安瑞

# 1. GDPR REGULATION SCHEME

trustseed

陈安瑞

trustseed

# WHY GDPR ?

GLOBAL DEMOCRACY THREATENED

1. INDIVIDUALS LOSE IN CLOUD COMPUTING
   **90 %** OF MANAGEMENT CONTROL.

2.CURRENTLY INTERMEDIARIES IN CLOUD DO NOT TAKE THE 90 % RESPONSIBILITY FOR THEM OR ONLY BY OBLIGATION OF MEANS

---

THUS THE EUROPEAN COMMISSION and PARLIAMENT

1. RESOLVED THE RESPONSIBILITIES OF THE **90 %** BY TWO MAIN REGULATIONS **GDPR** and **e.IDAS**
   **APPLIED TO**:

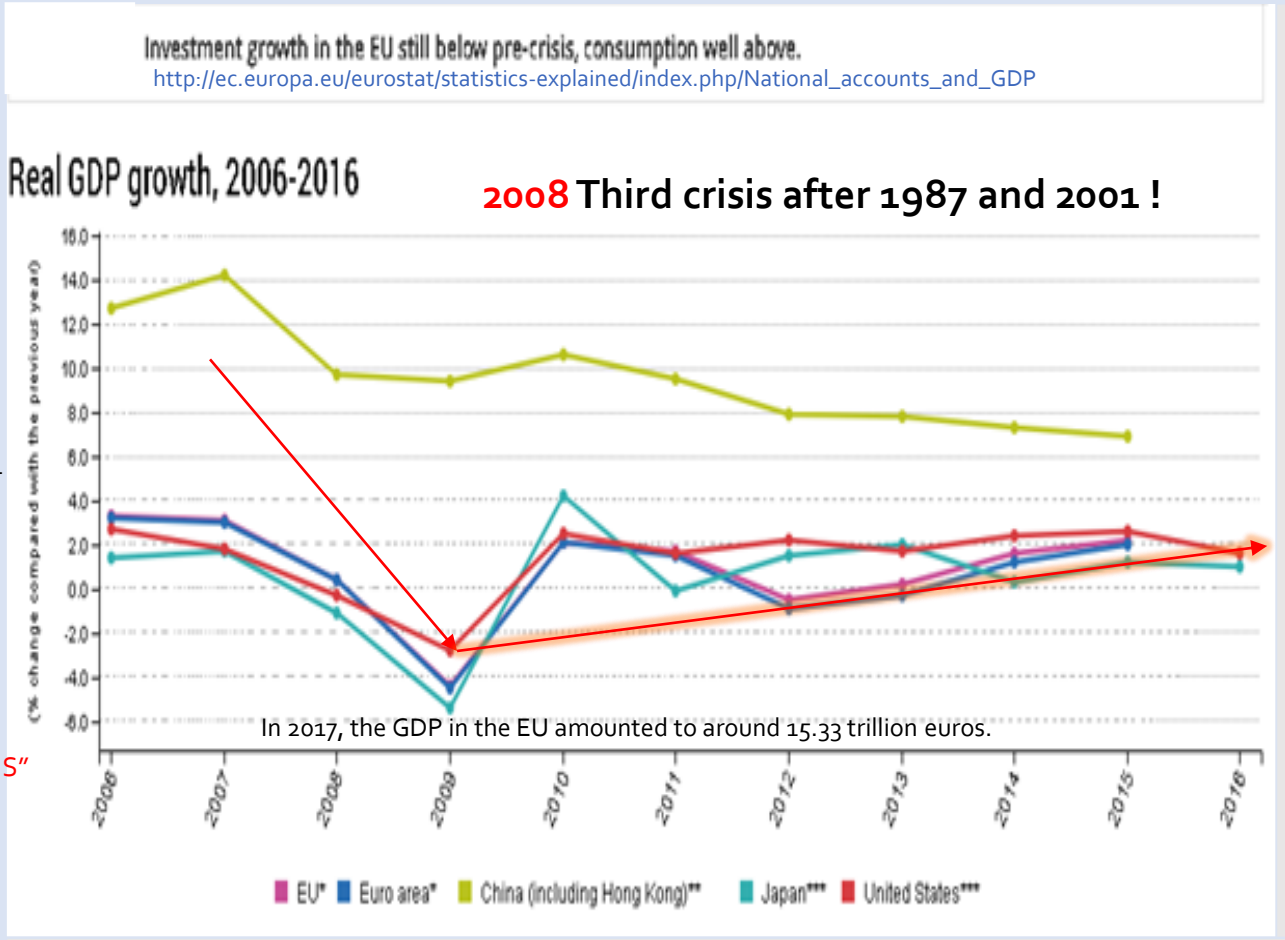
-1.**ENTERPRISES** (CONTROLLERS) GDPR Art. 24 & e.IDAS Art.21
-2. **OPERATORS** (PROCESSORS) GDPR Art.28 & e.IDAS Art.24
-3.**VALIDATION BODIES** GDPR Art.40-41 & e .IDAS Art.33
Including "APPROPRIATE GUARANTEES"
With dedicated obligations of Result.

APPLIED TO:

-**SOFTWARE-HARDWARE EDITORS** GDPR Art.43 & e.IDAS Art.30
Including "APPROPRIATE TECHNICAL & ORGANISATIONAL MEANS"
With dedicated software and hardware certified.

2. THREATENS THE RESPONSIBILITIES OF COMPANIES AND DISQUALIFYING AND PROHIBITING PROVIDERS TO MANAGE A PORTAL OF SERVICES OR A PLATFORM OF OPERATIONS BY MEANS OF SANCTIONS EQUAL TO **4 % OF THE REVENUE**.

Investment growth in the EU still below pre-crisis, consumption well above.
http://ec.europa.eu/eurostat/statistics-explained/index.php/National_accounts_and_GDP




The latest major invention in "Services" is the "financial instruments" creation in 1982 which multiplied by 10,000 outstanding transactions (Derivative Markets) and by 100 losses "termination" because of insufficient controls!

trustseed

# THE BIGGEST CHALLENGE OF HUMAN ORGANIZATION FOR 50 YEARS

In aviation, the challenge of the sound barrier lasted 54 years.

20 years to exceed 200 km / h in 1913, the Wright brothers.

54 years old to overcome the **Sound Barrier** in 1947: Chuck Yeager Bell 1126 km / h

In digital communication, the challenge is even faster: probably 12 years

Current competitors are followers: They have not yet taken up the challenge of the "**Digital Barrier**" to meet the GDPR Regulation.

The economic consequences of this profound IT reform are incalculable and will reverberate around the world:

GDPR

**With GDPR, the « DIGITAL BARRIER » will be overcome in few years !**

The number of "qualified" Operators (Processors), "qualified " Companies (Controllers responsible of Trust Services), "qualified "Chartered Control Bodies" (Marketplaces) including "certified" Management Software Publishers, will decrease by **65%.**

**The segmentation of "Regulatory Processes" in the banking sector has already experienced a reduction in the number of banking licenses in Europe above 65%.**

Documentary digitization will reduce management costs by **€ 700 billion** and the risks by **80%** (European Commission SSEDIC DG Connect 2012)

Data qualification optimizes decision support and certification systems through analysis and artificial intelligence :

PwC in its study "Sizing the prize", estimates that global GDP could grow by 14% by 2030 thanks to artificial intelligence. The **AI** is expected to contribute **$ 15.7 trillion to the global economy in 2030**, more than the current cumulative GDP of China and India.

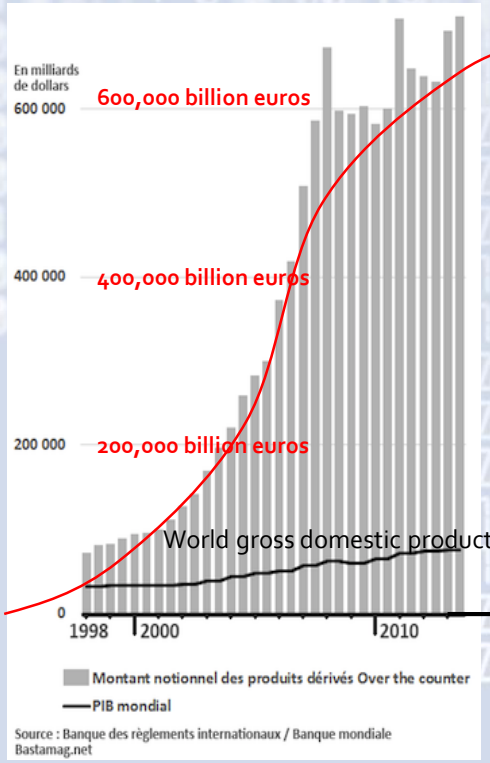
trustseed

# why so much severity?

Operators-Banking networks are also concerned by the GDPR as Operators-Commercial or Documentary networks

GDPR streamlines all international regulations, especially to avoid unbearable banking cracks:

**Bâle 1**,Ratio **Cook** , **Solvency Ratio**, **MIFID II** (Organising Trading Facilities), **EMIR** (European Market Infrastructure Regulation), **FATCA** II-(Foreign Account Tax Compliance Act), **BALE 3** (Liquidity Coverage Ratio, NSFR Net Stable Funding Ratio 2019), **RUBIK** (bank secrecy), SOLVENCY 2 (ratios MCR & SCR), AIMFD (Alternative Investment Fund Managers Directive), **PSD2** Payment, Reference **COBiT 5**: Governance standards including, TOGAF, PMBOK, Prince2, COSO, ISO 20000, ISO 27001, ITIL, PCI DSS, **Sarbanes-Oxley/IFRS**.




## Notional amount of derivatives "over the counter"

## 10 times the real economy

For rotten products, the US Court ordered Goldman Sachs to pay $ 5 billion, JPMorgan $ 13 billion and Bank of America $ 16.6 billion.

Deutsche Bank its balance sheet1600 billion euros, equivalent to half or **50 %** of Germany's GDP, and one-tenth of the GDP of the European Union

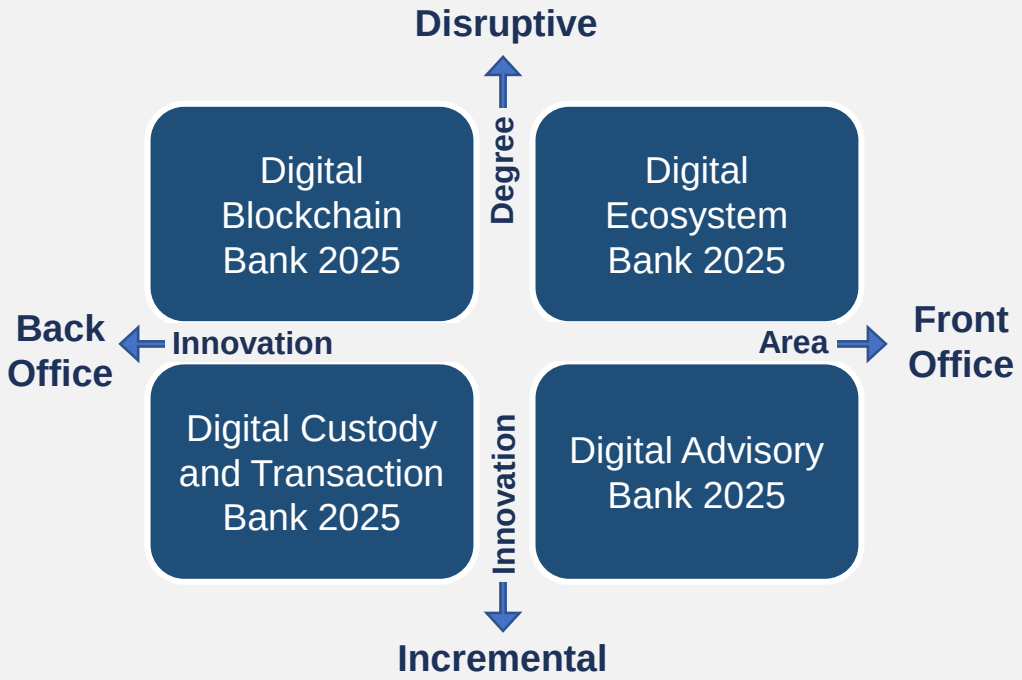
US justice has claimed $ 14 billion from Deutsche Bank (12.5 billion euros) for the 2007 subprime scandal that led to the 2008 financial crisis. currently in 8000 legal proceedings in the world!

Banca Monte dei Paschi di Siena (MPS) 360 billion euros of bad loans (of which 210 billion would be partly irrecoverable), or **20%** of Italy's GDP.

# FUTURE OF FINANCIAL SERVICES
# IMPACT OF DIGITIZATION

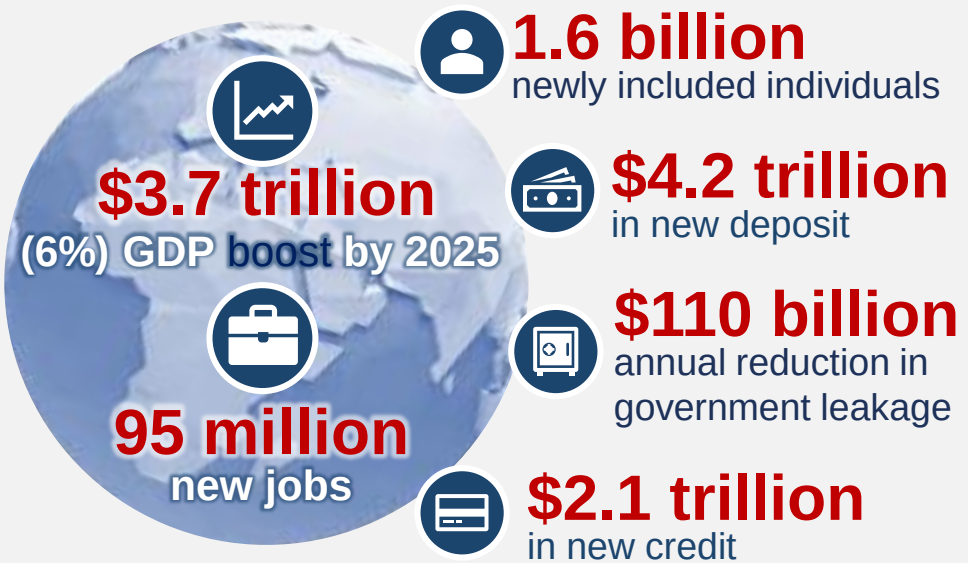
"By 2030, financial services will be completely transformed requiring substantial steps to be taken today by the industry, new entrants and regulators to ensure a positive outcome of the transformation. If unchecked, the impact of these forces on client choice, the range of providers and the level of risk in the system is going to be dramatic, resulting in a financial system dominated by a few large fintech players fuelled by their power of data aggregation relatively unencumbered by the current levels of regulation plus a handful of today's incumbents."

*Source: Global Future Council on Financial and Monetary Systems, The Global Financial and Monetary System in 2030, World Economic Forum, May 2018*




**Digital Bank Model 2025**

*Source: University of St Gallen, Switzerland, April 2017*




**Potential impact of digital finance**

*Source: McKinsey Global Institute Analysis, 2016*

陈安瑞

trustseed

# UNPREDICTABLE HUMANS

## STILL THE WEAKEST LINK IN DATA SECURITY

### INSIDER THREATS

Coming from unintentional or malicious behaviour by employees, former employees, contractors or partners with knowledge of the security practises and credentials.


**78%** of security experts say that the biggest threat is negligent or careless employees who do not follow security policies.

**90%** of organizations experience at least one insider threat each month.


**Internal actors are responsible for data loss 43% of the time.**

The average organisation experiences 9.3 insider threats per month… 1 every 3 days !

In 2003, U.S. companies suffered $40 billion in losses from unauthorized use of computers by employees, and this is growing.

Source: CODE42

trustseed

# Europe wants to reduce the impact of external crises

## WE REMEMBER 2008-2009


Europe wants to eradicate fraud, toxic products and the diversion of industrial property (IP).

## Our economy is a pierced basket

| Loss of income | € |
|---|---|
| Tax Fraud | 1,00 |
| Financial Fraud | 0,080 |
| Soils, $CO_2$, Agri. | 0,020 |
| Social Fraud | 0,100 |
| Underground Economy VAT | 0,255 |
| Total | 1,455 |

$$\frac{\text{LOSS}}{\text{GDP}} = \frac{1{,}455}{17{,}278} = 8{,}42\%$$

trustseed

# 2018 Cybercrime Statistics: A closer look at the "Web of Profit"

Cybercrime will generate at least **$1.5 trillion** this year—and that's conservative
https://www.thesslstore.com/blog/2018-cybercrime-statistics/


Acceleration of transactions
FRAUDS
Dysfonction
GANG SCAM
Transfers
Secrecy breach

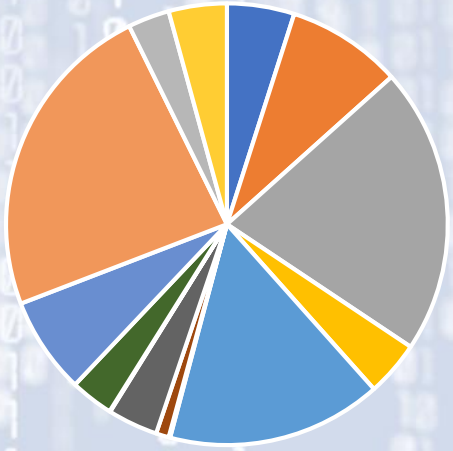
| E.IDAS GDPR | HYPER REGULATED ACTIONS | Main causes of economic disorder Links |
|---|---|---|
| E.IDAS ART. 26 | **FAKE DOCUMENTS ILLEGAL SIGNATURES** | Lehman Brother 2008 Le Monde Journal » Determine the real debts in an incredible entanglement" **SNT University Lux: « in 2012 the Italian police seized $ 6 trillion of fake U.S. bonds hyper Regulated actions** |
| GDPR. Art.40-41 E.IDAS. Art.33 | **TAX EVASION FINANCIAL FRAUD** NON INDEPENDANT CONTROL NON INDEPENDANT VALIDATION | Swap Credit Lyonnais http://www.liberation.fr/futurs/1996/08/21/lyonnais-peyrelevade-a-decouvertil-a-congedie-l-homme-qui-aurait-pu-eviter-la-perte-de-plusieurs-mil_179282 https://fr.myeurop.info/2013/12/04/fraude-fiscale-conseil-constitutionnel-censure-12410 EU 2000 billions € tax evasion |
| GDPR Art.40 | **GROWING MASS VIOLATION OF CODE OF CONDUCT + PROCEDURE** IMPUNITY, LEGAL EVASION JUSTICE SATISFACTION CLASS ACTION | Société Générale France Capital Market, Samsung Electronics. https://fr.wikipedia.org/wiki/Crise_financi%C3%A8re_de_janvier_2008_%C3%A0_la_Soci%C3%A9t%C3%A9_g%C3%A9n%C3%A9rale Class Action TOBACCO, ENRON, WORLD COM, EXXON MOBIL, CENDANT, TIME WARNER, NORTEL. DEUTCH BANK s currently facing 8000 legal proceedings in the world! https://www.bastamag.net/Deutsche-Bank-en-crise-la-plus-grosse-banque-allemande-fait-planer-la-menace-d |
| GDPR Art. 47 GDPR.Art.40.4 | ORGANISED GANG SCAM **CRIMINAL JOINT VENTURES** MASS ABUSE OF TRUST VIOLATION OF TRACEABILITY MECHANISMS | Facebook https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica Volkswagen: https://fr.wikipedia.org/wiki/Affaire_Volkswagen https://fr.wikipedia.org/wiki/Scandale_sanitaire |
| GDPR Art.44 | EXCHANGE CONTROL TRANSFER OF MONEY **VIOLATION OF DATA TRANSFER OBLIGATIONS** | WhatsApp https://www.lesechos.fr/19/12/2017/lesechos.fr/0301042495061_la-cnil-met-en-demeure-whatsapp-pour-transfert-illegal-de-donnees-personnelles.htm Sanofi Aventis Algeria http://www.dzentreprise.net/transfert-illegal-de-capitaux/ 4,700 bitcoins were stolen, the equivalent of $ 60 million. http://www.dailymail.co.uk/news/article-5154737/Bitcoin-miner-NiceHash-reports-hack-theft-wallet.html $1 billion by hacking ATMs. https://cybersecurityventures.com/hack-blotter/ |
| GDPR. Art.90 | ATTACKS, MISUSE OF DATA & INTELLECTUAL PROPERTY **BREACH OF SECRECY** | EQUIFAX , UBER, Swedish Transport Agency, STA. WannaCry/Deloitte/NSA-Petya/NotPetya/DoubleLocker/NCSC/Imgur/NiceHash https://en.wikipedia.org/wiki/Cyberattack NSA : https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html |

陈安瑞

trustseed

# GDPR REGULATION : 4310 TERMS OF LEGAL AND COMPUTER SECURITY USED DIFFERENTLY

## GDPR + e.IDAS +NIS SECURITY



IDENTITY
PROCEDURES
LEGAL BASIS
PENALTIES
SECURITY SECRETY
TRUST
CERTIFICATE
STANDARDS SCHEMES
ORIGINAL DOC
ORIGINAL SIGNATURE
DIGITAL SEAL
STRONG CONSENT
TRANSFER
REAL TIME CONTROL
CODE OD CONDUCT
GUARANTEES

| | MAIN ITEMS OF REGULATIONS | GDPR | e.IDAS | NIS | total |
|---|---|---|---|---|---|
| | I.CONTROLLER (FRONT-OFFICE) | | | | |
| | I.1. CONTROLLER :SERVICES | | | | |
| 1 | IDENTITY | 94 | 211 | 3 | 308 |
| 2 | PROCEDURES | 161 | 40 | 26 | 227 |
| 3 | LEGAL FRAMEWORK EVIDENCE VALUE | 400 | 53 | 27 | 480 |
| 4 | PENALTIES | 77 | 82 | 2 | 161 |
| | I.2. CONTROLLER: PERSO. DATA | | | | 1176 |
| 5 | SECURITY SECRETY | 300 | 17 | 144 | 461 |
| 6 | TRUST | 2 | 232 | 10 | 244 |
| 7 | CERTIFICATE | | 144 | | 144 |
| 8 | STANDARDS, SCHEMES | 18 | 477 | 1 | 496 |
| | | | | | 1345 |
| | II.PROCESSOR (BACK-OFFICE) | | | | |
| 9 | CRYPTO CREATION | 70 | 2 | 17 | 89 |
| 10 | DIGITAL SIGNATURE | 1 | 130 | | 131 |
| 11 | DIGITAL SEAL TIMESTAMP | | 106 | | 106 |
| 12 | STRONG CONSENT (1) | 60 | 59 | | 119 |
| 13 | TRANSFERT | 135 | 7 | | 142 |
| | | | | | 587 |
| | III. VALIDATION BODY | | | | |
| 14 | CONTROL REAL TIME | 449 | 564 | 8 | 1021 |
| 15 | CODE OF CONDUCT | 58 | 3 | 1 | 62 |
| 16 | GUATANTEES | 81 | 35 | 3 | 119 |
| | | | | | 1202 |
| | | **1906** | **2162** | **242** | **4310** |

# PERSONAL DATA?
# IN CLOUD COMPUTING , YOU LOSE 90 % OF YOUR MEANS OF CONTROL !
# CONTROLLER & PROCESSOR TAKE CARE OF YOU !

trustseed

- Name
- Physical Address
- Address IP
- Address email
- Phone number
- Localisation
- Online ID
- Health Information
- Earnings
- Consumption habits
- Travels
- Biometrics
- Social networks, archive mails
- …

YOU-SERVICE PROVIDER-
As a "CONTROLLER"
COLLECT,STORE,USE OF DATA ?

YOU MUST RESPECT
THE INDIVIDUAL RULES (1)

YOU PROCESS DATA, DOCUMENT & SIGNATURE
FOR USERS
As a "PROCESSOR" -
YOU ARE ALSO (2) CONCERNED !

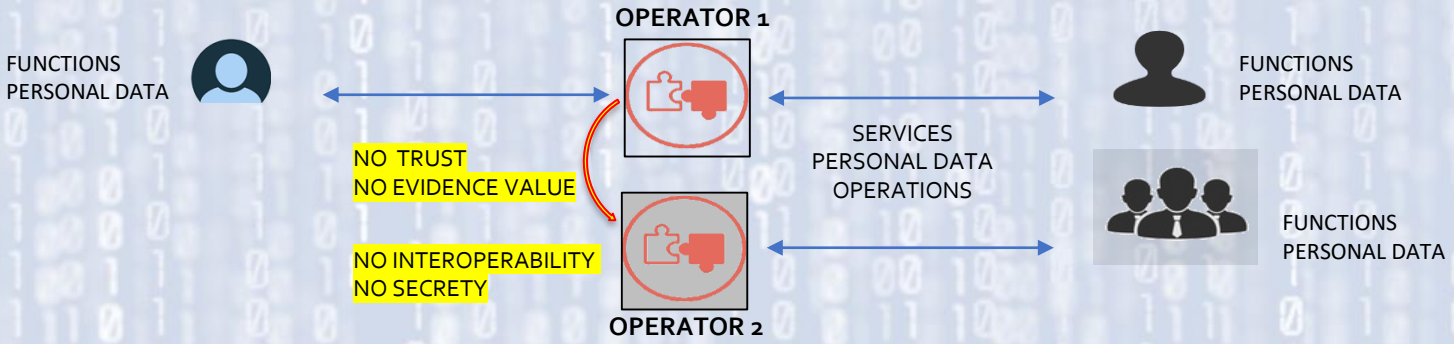
(1) The rights to request from the **Controller** :
**access , rectification , erasure** of personal data, or **restriction of processing** concerning the data subject (**Profiling**). The rights to **revoke,** to **object the data processing** as well as the right to data **portability**, **pseudonymisation** and **confidentiality-secrecy**;

(2)The application of the general data protection principles is mandatory to deliver "**Appropriate Guarantees**" and "**Technical and Organisational Measures**" **specified in each digital "Code of Conduct" and organized with "Control & Certification Mechanisms" designed for** real time **purpose limitation** , for **data minimization**, for **data protection & finalization, for limited storage periods**, for **data quality, for legal basis regarding each categories of personal data**, for **Data Transfer Security** to safeguard counterparties not bound by corporate rules.

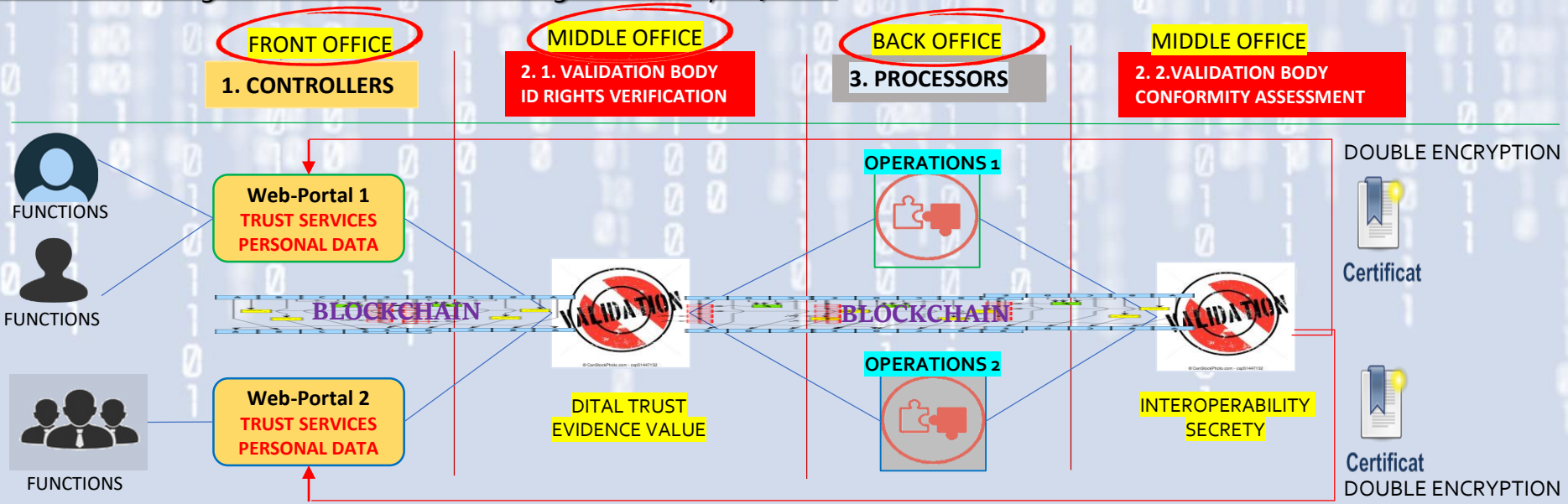
**If you have personal data from anybody else, you are prohibited from operating them by yourself !**

# THE GDPR REGULATION CHANGES COMPLETELY THE INTERNATIONAL ORGANISATION OF COMMUNICATION NETWORKS

Before the GDPR Regulation




After the coming into force of the GDPR Regulation May 28, 2018



陈安瑞

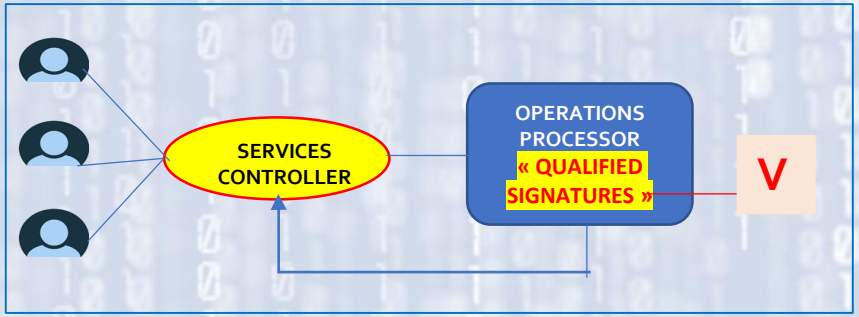
trustseed

# Mandatory Security Leverage Application

The GDPR and e.IDAS Regulations establish a “first level “of IT security (Access, Confidentiality) and legal security (Evidence Value) for exchanges between users of the same operator-processor using a "qualified signature".

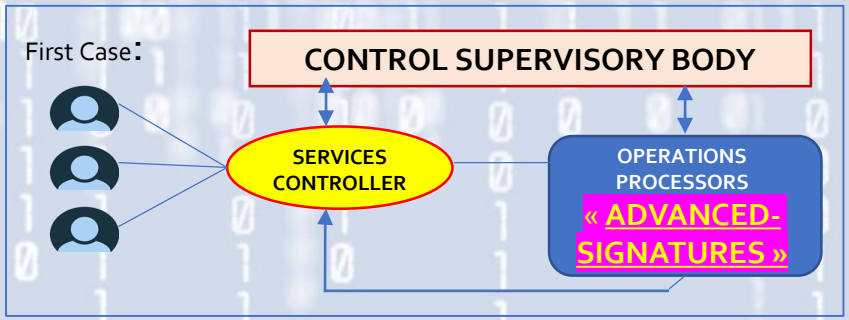
In 4 cases, the security level should be about **5 times** higher by adding:

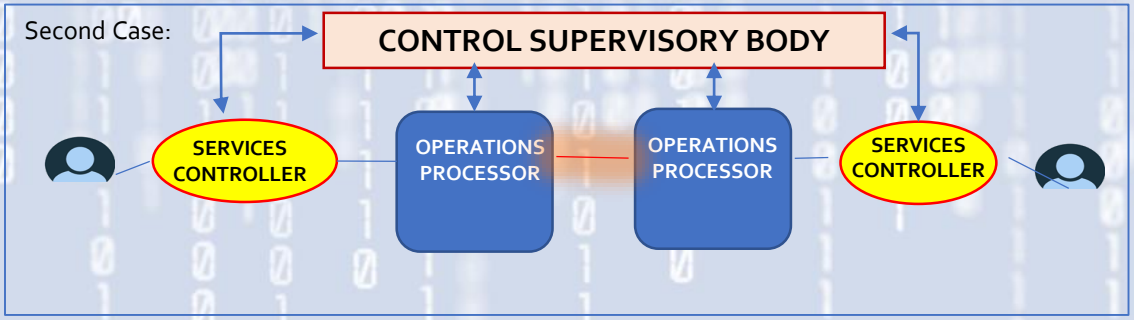
1. A “code of conduct” with “appropriate s guarantees” and “control mechanisms “carried out by an approved and “Independent supervisory body”.
2. “Appropriate technical and organizational means “and certified by an independent “conformity assessment body.”

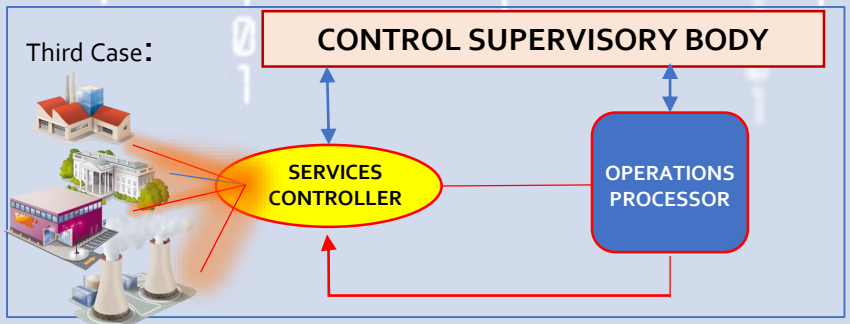


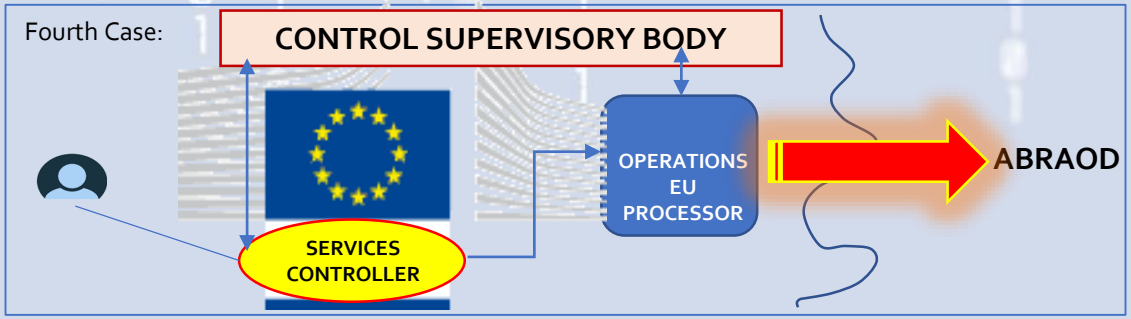

**The 4 cases are:**

1. The processor-operator uses an “**advanced signature** “instead of a “qualified signature “for each signatory.
2. The processor operator communicates (**trusted interoperability**) with another processor operator.
3. The processor-operator processes the “**data of several related companies**.”
4. The processor-operator “transfers “ “**personal data outside Europe**”.



400

20 METHODOLOGY ISSUES

20 TECHNOLOGY APPLICATIONS

| | SIGNATURE CERTIFICATE | COMMITMENT SOFTWARE | MEAN OF AUTHENTICATION | IDENTITY CERTIFICATE | BILATERAL AGREE.SOFT WARE | DATA DISCLOSURE SOFTWARE | CROSS SCHEDULING SOFTWARE | DOC. ISSUANCE SOFTWARE | ADVANVED SIGNA. SOFTWARE | MULTILATERAL ENCRYPTION | DATA SEALED TRANSFER | DOCUMENT ACCOUNT SOFT | LEGAL PROOF ARCHIVING | RECTIFICATION REVOCATION | PSEUDONYMISATION SOFT | ERASURE, PROROGATION | MEAN OF AUTHENTICATION | IT ARCHITECTURE PROCESSING | TRACEABILITY VALIDATION | PROFILING |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PRIVATE LAW | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| PUBLIC LAW | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| REGULATIONS | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| INSURANCE RISK mgt | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| CORRESP. BANKING | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| CORRESP. MAILING | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| CORRESP.MARKETS | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| SOFTWARE APPLICA. | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| ID RIGHTS PROXIES | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| COLLABORATIVE mgt | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| SIGNATURE mgt | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| CRM CUSTOMER RELA | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| DOCUMENT mgt | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| ARCHIVING mgt | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| LIFE CYCLE mgt | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| AUDIT manual Visual | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| CYBER SECURITY policy | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| SUPERVISORY CONTROL | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| NETWORK INTEROPERA | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| STANDARDS | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |

# LIST OF REGULATORY FUNCTIONS GDPR- e.IDAS – NIS

## Part 1 TRINARY SYSTEM

### I. Functions concerning Controllers

1. **Creation and dynamic registration of Identities** and Multi-Community Digital Certificates with signed and timestamped legal support documents.

2. **Management and rating of digital authentication systems** by providing them with multiple identification factors: between 3 and 5 factors for the protection of different accesses.

3. **Management of signature services for all categories** of letters, transactions, payments and financial and banking instruments on a multilateral legal basis and interoperability real time.

4. **Management of the consents of bilateral relations** of civil, commercial, financial, banking, health, transport, company, energy ... and management of the consents of personal signatures on line by two-dimensional code (QR CODE By TRINARY SYSTEM EMBEDDED)

5. **Management of exceptional rights**: rectification, limitation, deletion, pseudonymisation, opposition, revocation, forgetting, withdrawal of consent, portability, claim-reparation.

6. **Management of the prevention against fraud**, the updating of the unambiguous personal rights, the minimization of the disclosed data, the limitation of the treatments and the finalization of the transmissions for each order of a commitment by signature (s) realized on behalf of a user and its counterparties by one or more "Controller (s)" with one or more "Processors" in the same Country or Cross-Border.

7. **Management of the electronic signature certificates associated** with each digital trust services portal, each documentary account, each document signature (Qualified or Advanced Signatures), each document encryption, each sworn employee (digital notary), with each "Controller" communication, each " Processor "communication, and each validation of an independent chartered control body.

8. **Management of Extended Scorecard Templates or Extended Traceability Files** (Marqued data) that are defined by trade categories, and which are embedded in a blockchain specific to each category of mail, transaction, payment or financial and banking instrument, and which are subject to in sequence to the authorized control and validation body.

# LIST OF REGULATORY FUNCTIONS GDPR- e.IDAS – NIS
## Part 2 TRINARY SYSTEM

**II. Functions for Processors**

1. Collecting the data to be processed
2. Creation of accounting and unique documentary originals
3. Creation of originals of qualified or advanced signatures and pairing with individual consents
4. Encryption of originals of documents with the protection of private keys and with public protection clauses for judicial, police and military actions in real time.
5. Transfer of XML Marqued Data by use case: accounting, profiling, statistics, artificial intelligence ...
6. Collaborative En-De-Cryption Information Management Account (Real Time Enabling)
7. Personal Property Retention Account by Categories of Assets and Liabilities
8. Transfer of ownership and simultaneous change of the encryption key
9. Automatic processing of exceptional rights: rectification, limitation, deletion, pseudonymisation, opposition, revocation, forgetting, withdrawal of consent and portability.
10. Renewal of integrity certificates

# LIST OF REGULATORY FUNCTIONS GDPR- e.IDAS – NIS

## Part 3 TRINARY SYSTEM

### III. Functions concerning the approved inspection and validation body (s)

1. Dynamic notation of community identities

2. Dynamic notation of authentication systems

3. Dynamic notation of personal legal signature systems

4. Dynamic notation of strong and informed consent systems

5. Dynamic notation of the legal value of signed exchanges

6. Repository by codes of conduct of the categories of exchanges and blockchains

7. Revocation list: identities, bilateral agreements, powers, mandates, certificates ...

8. List of certified software and hardware features

9. List of qualified "Controllers" and "Processors"

10. List of certification authorities for strong authentication of portals

11. List of Certification Authorities for Individual Strong Authentication

12. List of Certification Authorities for Authentication of Personal Management Accounts (Data and Search Engine)

13. List of Certification Authorities for Authentication of Personal Retention Accounts (Originals-Ownership and Transfer of Personal Property)

14. List of certification authorities for timestamping and sworn notary

15. List of certification authorities for the signatures of "Controllers", "Processors" and "Authorized Inspection Bodies"

16. Sequential validation of the blockchain by category of digital exchanges

17. List of subcontracting mandates, interoperability and portability networks

18. Treatment of processing and transfer anomalies and rectification and alert procedures

19. Cyber security treatment, mandatory or rogatory procedures.

20. Control of profiling data: final destination, management cycle, destruction or restitution

21. IoT data control: final destination, management cycle, destruction cycle or return cycle

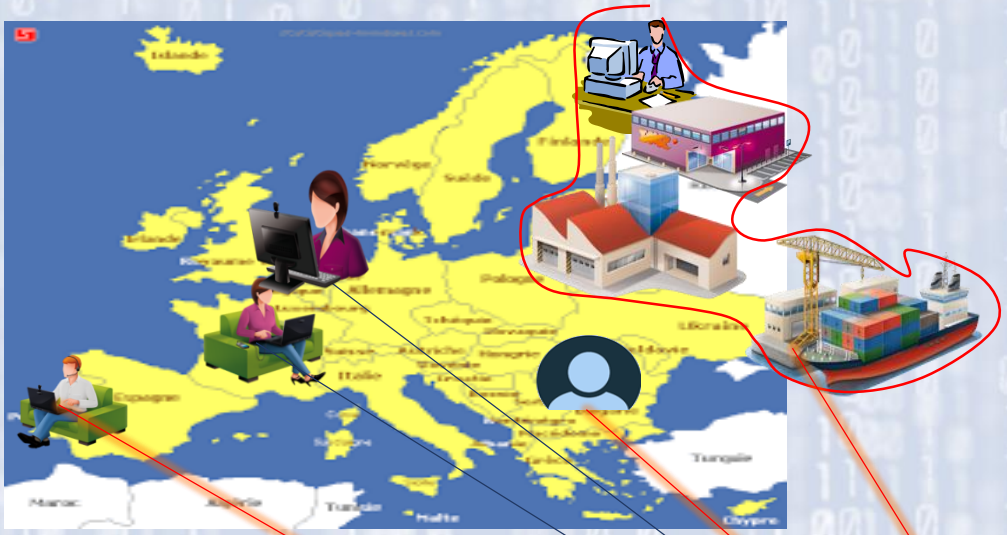
22. Artificial intelligence data control: final destination, management cycle, destruction cycle or restitution cycle

23. Check for Renewal of Digital Signature Certificates regarding documentary integrity long term

24. Digital Prosecution Procedures

陈安瑞

# Strengthening of the guarantees for exchanges involving a Group of Companies or a Relationship outside Europe.




The commitments signed between a "Group of Companies" and a private Individual domiciled in Europe (Art.47)
Or the commitments between a Private Individual domiciled in Europe and a Private Individual domiciled or residing outside Europe (Article 44),
**For both of them,** the use of an Advanced Signature instead of a Qualified Signature between multilateral Signatories, Art.26 e.IDAS.

This situation requires " Appropriate Safeguards and Guarantees " **higher** (Art.45) to others **that the Controller (Service Portal) must obtain.**

These "Appropriate Safeguards" and "Guarantees" require:

1. A **Code of Conduct** (Art.24.3 and 40) with "**control mechanisms"** monitored by an Chartered independent Validation Body.

2. "**Technical and Organizational Measures"** (Art.24.28.1), including tests -impact assessments, and **certification (3 years) mechanisms managed by a "Conformity Assessment Body"** for the software and hardware products used (Art.25).

CONTROLLER

PROCESSOR

VALIDATION & CONTROL BODY

HIGHER CONTROLS — LOWER CONTROLS

trustseed

# THE SANCTIONS BAROMETER

**Fine of**

**20M€**  **or** **4% Turn Over** 

- Non-respect of the principles of the protection of personal data
- Offense against consent rules
- Infringements of data transfers outside the Europe

**Fine of**

**10M€**  **or** **2% Turn Over** 

No data protection at design time and by default
Failure of data security
No notification of data breaches
Absence of a register of treatments
Non-compliance with the DPO designation rules

**1st warning**

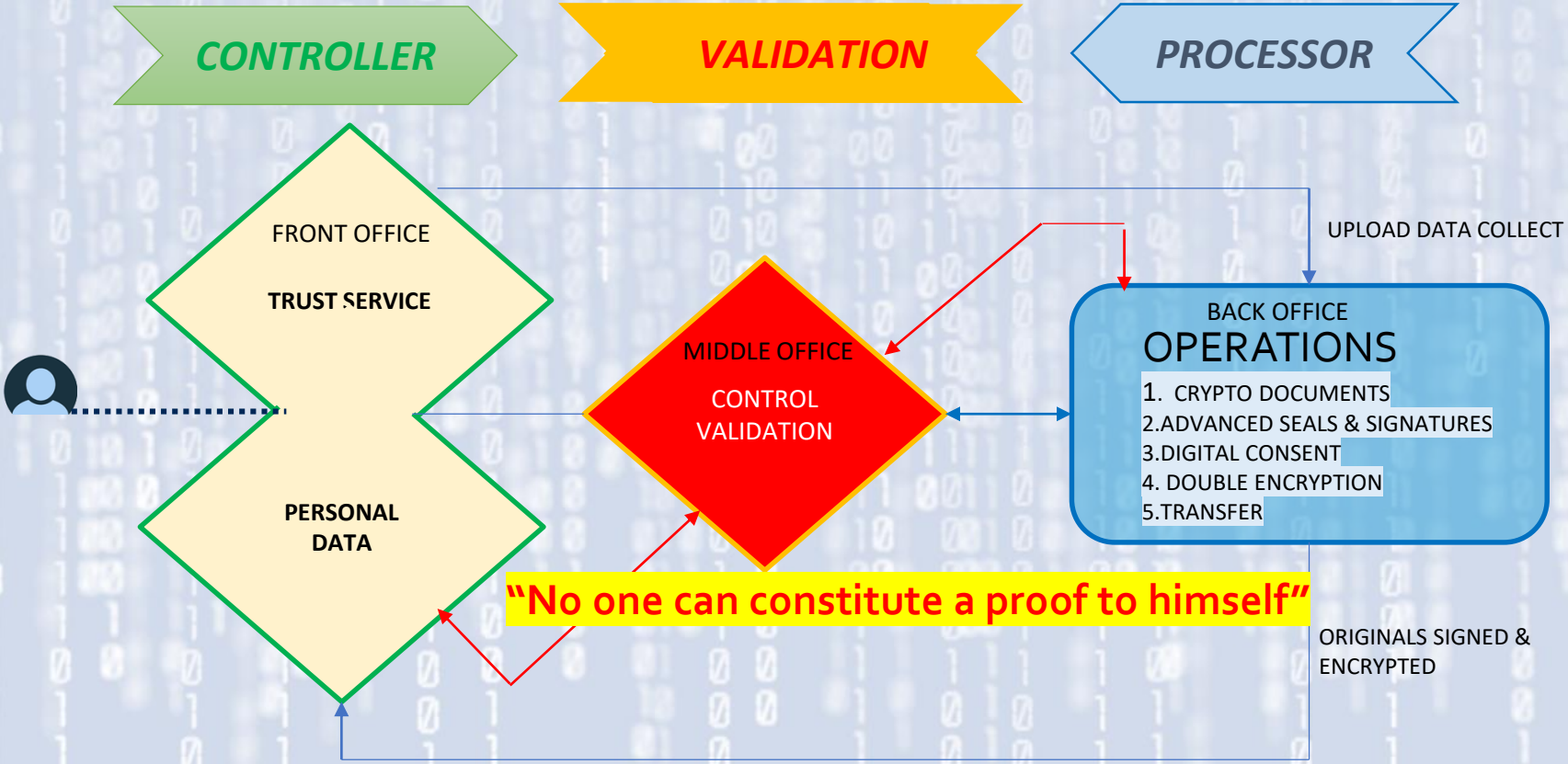
**In writing**

陈安瑞

# 2. MANDATORY TRUSTWORTHY NETWORK

trustseed

# SECURITY & LAWFULNESS LEADS TO FRAGMENTATION



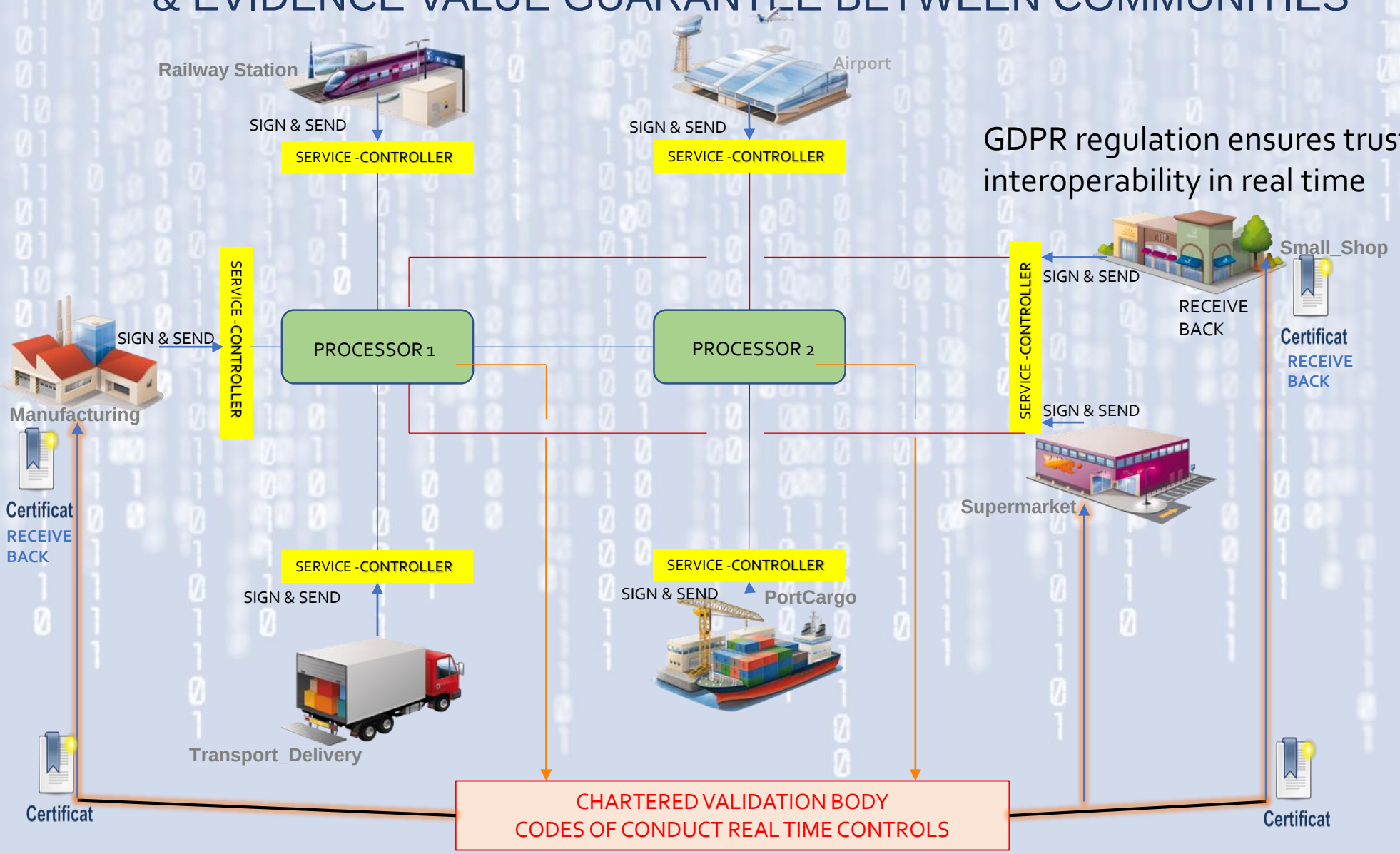

1952 Words to separate 3 independant responsabilities

| WORDS | REGULATIONS | GDPR | e.IDAS | TOTAL |
|---|---|---|---|---|
| 1.1 | SERVICES | 44 | 323 | 367 |
| 1.2 | PERSONAL DATA | 862 | 117 | 979 |
| 2 | OPERATIONS | 59 | 18 | 77 |
| 3 | CONTROL VALIDATION | 100 | 428 | **528** |
| TOTAL | SEGMENTATION | 1065 | 886 | **1952** |

陈安瑞

trustseed

# GDPR REGULATION ENSURES IN REAL TIME TRUST INTEROPERABILITY & EVIDENCE VALUE GUARANTEE BETWEEN COMMUNITIES



trustseed

# CONTROL OF PERSONAL DATA: THE GAFA FOOTPRINT

**How can these Large Communities converge into GDPR regulation?**

**90%**
Internet search

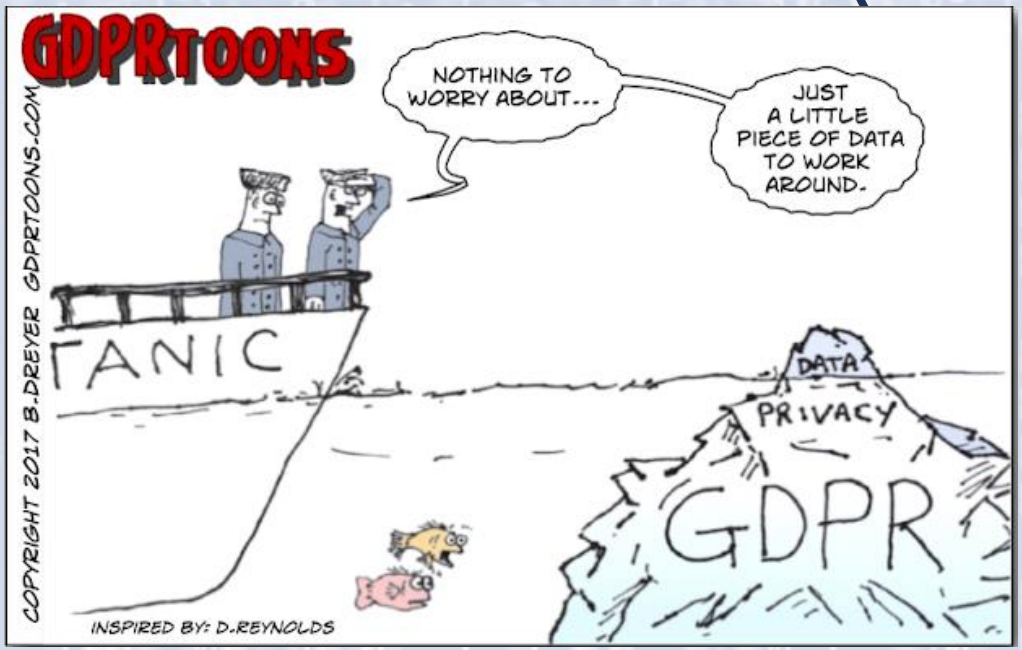
**45%**
smartphone traffic

**75%**
social media traffic.

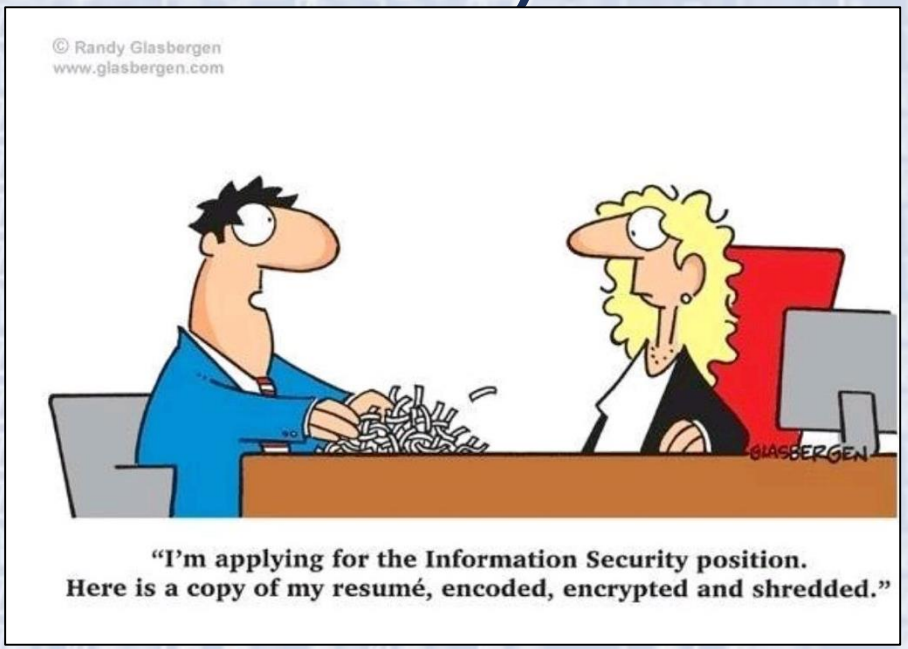
**6%**
retail transactions

trustseed

# A REGULATED LANDSCAPE (AT LEAST IN EUROPE)




UNDERSTANDING AND AWARENESS




ENFORCEMENT

**GARTNER SAYS ORGANIZATIONS ARE UNPREPARED FOR THE 2018 EUROPEAN DATA PROTECTION REGULATION**, May 3, 2017

Gartner Inc. predicts that by the end of 2018, more than 50% of companies affected by the GDPR will not be in full compliance with its requirements. http://www.gartner.com/newsroom/id/3701117

**90% OF BUSINESSES ARE NOT READY FOR GDPR SURVEY REVEALS**, September 20, 2017

https://www.businessleader.co.uk/90-businesses-not-ready-gdpr/35818/

**TREND MICRO RESEARCH REVEALS C-LEVEL EXECUTIVES Including "Packaged Software Publishers" " in the middle" ARE NOT PREPARED FOR GDPR IMPLEMENTATION**, September 5, 2017.

trustseed

# EVERYBODY IS CONCERNED... AND NOT ONLY IN EU…


Associations

Public Administrations

EU Enterprises

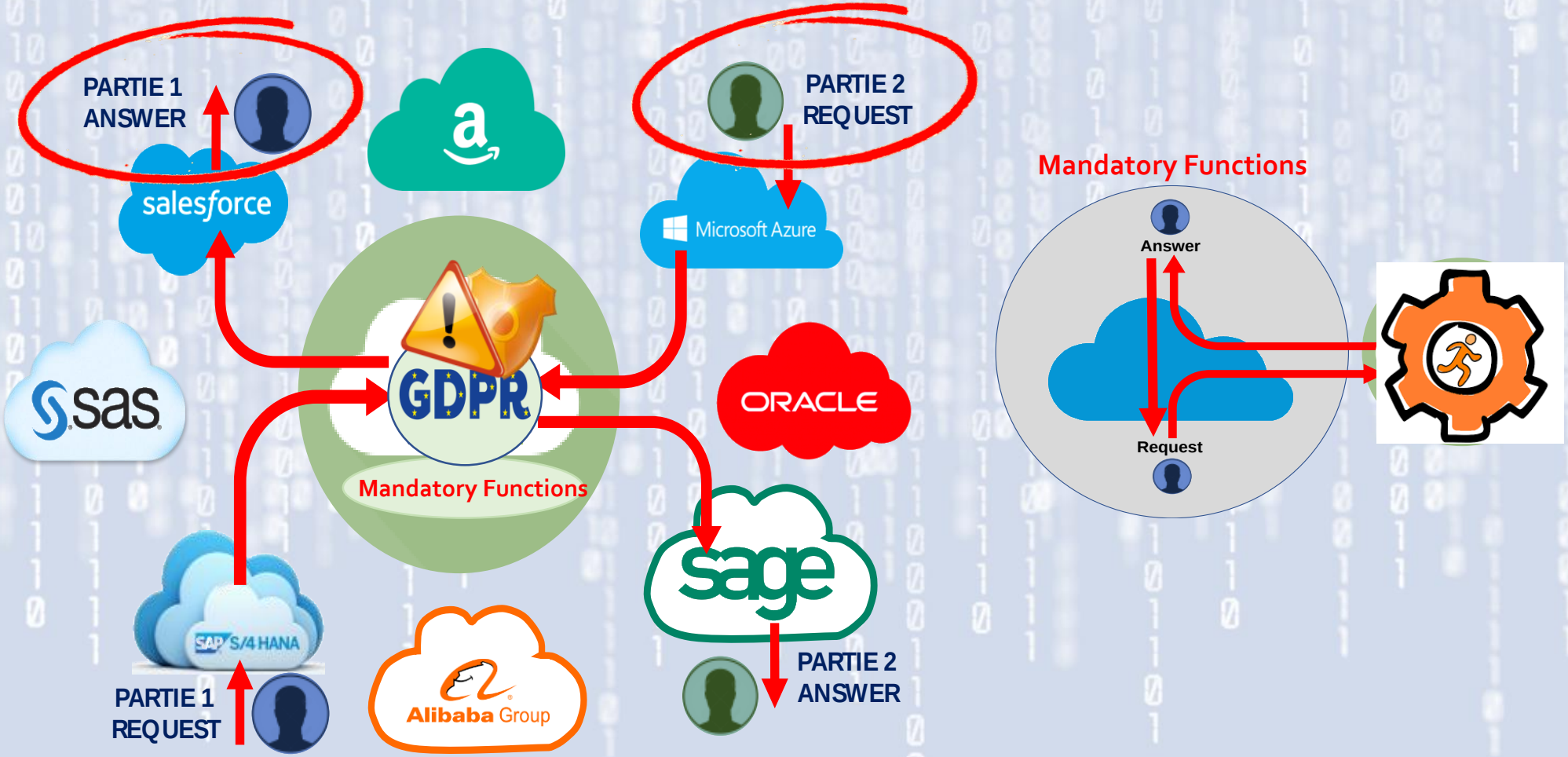
Sub-contractors

&

Non-EU Enterprises dealing with EU personal data

trustseed

# THE ANSWER IS
## AN AGNOSTIC SOLUTION FOR MANAGING MANDATORY FUNCTIONS



陈安瑞


# 3. MAIN BARRIERS TO OVERCOME

trustseed

# THE MAIN TECHNOLOGICAL BARRIERS

## 1. DOCUMENT « ORIGINATION/ISSUANCE » INCLUDING CONDENSATE SEAL & NOTARY SIGNATURE

**In the physical world: What do you need to guarantee an original?**

DEMATERIALIZATION

Physical Signatures of all the Parties

Certifies that the original is kept in his locker and that a physical copy is equivalent to the original.

A Notary

**In the digital world: What do you need to guarantee an original?**


Principle of Uniqueness

UNIQUENESS: UNIQUE ORIGINAL FILES


Digital Signatures of all the Parties

A UNIQUE WAY to seal & certify the existence of an original and the conformity of the various copies to the original.

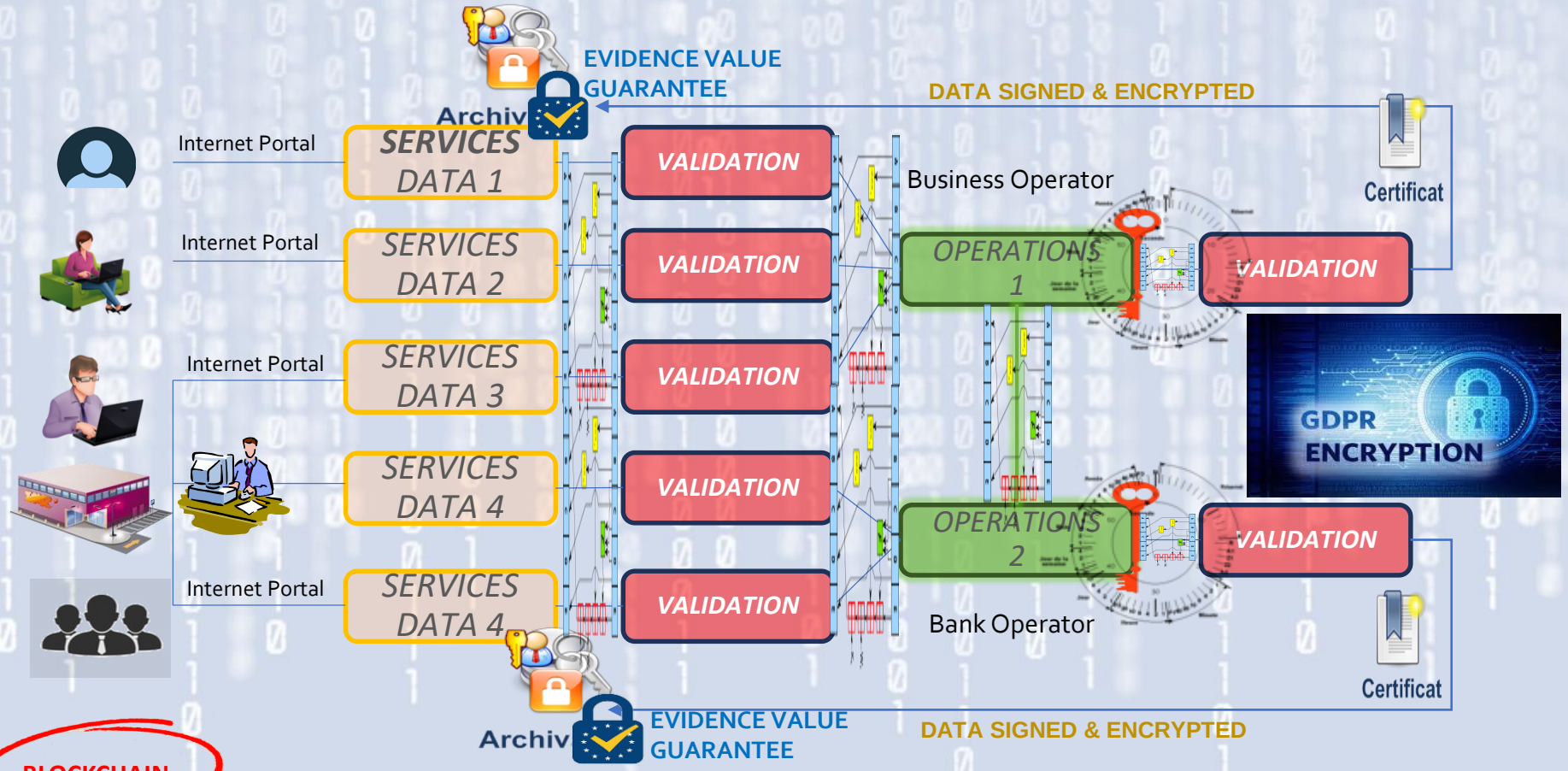

https://www.international-due-diligence.org/fake-financial-documents/
SNT University Luxemburg: "Italian police seized $6 trillion of fake U.S. bonds, which is an indicator of the existing shortcomings in this area.

trustseed

# THE MAIN TECHNOLOGICAL BARRIERS

## 2. COLLABORATIVE MANAGEMENT FOR MULTILATERAL – CROSS BORDER

« ADVANCED SIGNATURES » & « DOUBLE KEYS ENCRYPTION »




BLOCKCHAIN

SERVICE-DATA / VALIDATION / OPERATION / VALIDATION. DATA SIGNED & ENCRYPTED

陈安瑞

trustseed

3. ORIGINAL DOCUMENT ISSUANCE

4. ORIGINAL SIGNATURES & CONSENTS

5. MULTILATERAL COLLABORATIVE ENCRYPTION

2.MULTILATERAL COMMITMENT S BY SIGNATURES

1.MULTILATERAL AUTHENTICATION

6. INDEPENDENT CHARTERED CONTROL BODY

7. ACCOUNT FOLLOW-UP & LEGAL PROOF ARCHIVING


PORTAL SERVICES
QUALIFIED CONTROLLER

OPERATIONS
QUALIFIED PROCESSORS

| | CROSS BORDER EXCHANGE BY SIGNATURES |
|---|---|
| 1 | MULTILATERAL IDENTITY REGISTRATION & RATING |
| 2 | MULTILATERAL AUTHENTICATION MEANS |
| 3 | MULTILATERAL COMMITMENT BY SIGNATURES |
| 4 | SIGNATORIES POWER OF ATTORNEY BY COMMITMENT CATEGORIES |
| 5 | CHECKING & SCHEDULING MULTILATERAL COUNTERPARTIES RIGHTS |
| 6 | ORDER BY MINIMIZATION, LIMITATION AND FINALIZATION |
| 7 | COMPULSORY ADDITIONAL SERVICE OPTIONS |


PACKAGED SOFTWARE EDITORS ERP's
Enterprise Resource Planning

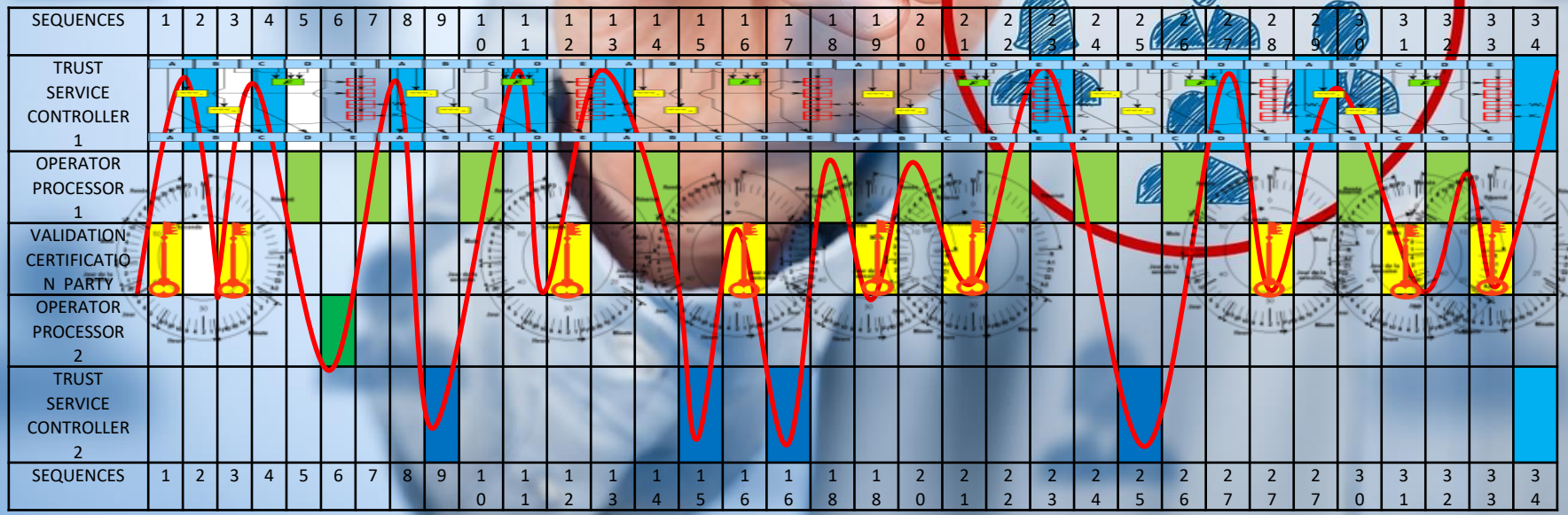
| | CROSS BORDER DOCUMENTS-SIGNATURES-CREATION-ENCRYTION |
|---|---|
| 1 | DATA FILE COLLECTION & MULTILATERAL ORIGINAL ISSUANCE |
| 2 | MULTILATERAL ORIGINAL ADVANCED SIGNATURES CREATION |
| 3 | MULTILATERAL AND CROSS-BORDER CONSENT OF SIGNATORIES |
| 4 | MULTILATERAL ENCRYPTION BY ACCOUNT AND DOCUMENT |
| 5 | CHECKING CONFORMITY & PROBATIVE VALUE CERTIFICATION |
| 6 | ACCOUNTS COMMUTING, XML TRANSFERT LEGAL PROOF ARCHIVING |
| 7 | KEY VAULT, REPROCESSING RECTIFICATION OR RENEWAL |

IDENTITY RIGHTS:& MEANS RATING –REVOCATION LISTS/ *CODES OF CONDUCT –CONTROL MECHANISMS-*CERTIFIED MEANS LIST- QUALIFIED PARTIES LIST

CHARTRED CONTROL
SUPERVISORY BODY

# THE MAIN TECHNOLOGICAL BARRIERS

## 3. « BLOCKCHAIN » INCLUDIND CONTROLLERS, PROCESSORS, CHARTERED VALIDATION BODY.



陈安瑞

trustseed

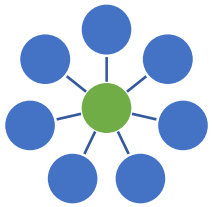
# 4. PUBLIC BLOCKCHAIN? YES BUT…

陈安瑞

trustseed

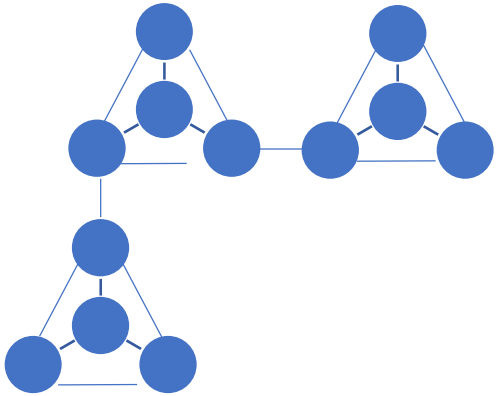
# LEDGER BASED ARCHITECTURES

**Internal Transaction**



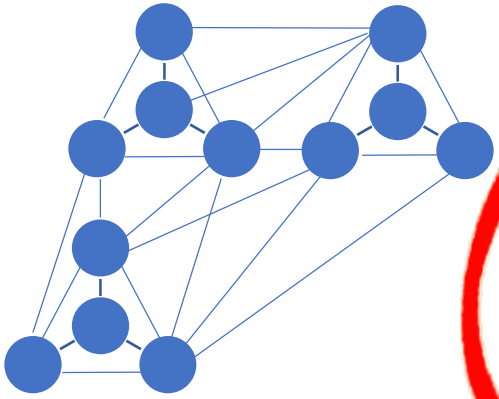
**Centralized**

**Middleware/Messaging Clearing Houses**



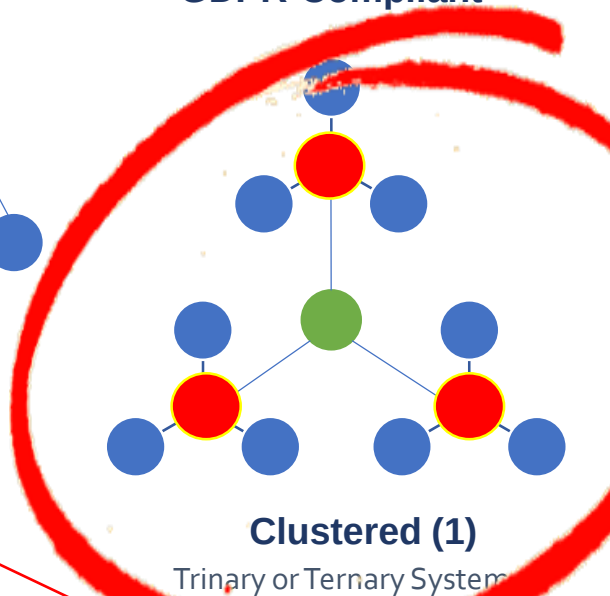
**Distributed**

**Blockchain**



**Decentralized**

**Blockchain GDPR-Compliant**



**Clustered (1)**

Trinary or Ternary System

'Current offers and sales of ether are not securities transactions.'
**William Hinman, SEC**

The **Securities and Exchange Commission SEC**. William Hinman, the agency's director of the division of corporate finance, said

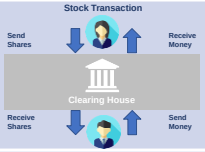
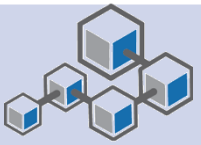
"Based on my understanding of the present state of ether, the Ethereum network, and its decentralized structure, current offers and sales of ether are not securities transactions," Hinman said at Yahoo's All Market Summit: Crypto in San Francisco.

Joe Lubin, a cofounder of Ethereum and the founder of CosenSys, a major Ethereum application company, says he is grateful for the SEC's decision. "We applaud the clarity provided by Director Hinman and the SEC today,"

**(1)** « Clustered » means Trinary System between « Front Office » Controllers, « Back Office » Processors and « Middle Office » Chartered Validation & Control Bodies.

trustseed

# TRINARY SYSTEM VS. EXISTING ARCHITECTURES

| | Internal Transaction | Middleware/ Messaging | Clearing Houses | Public Blockchain | TRINARY SYSTEM Private Blockchain |
|---|---|---|---|---|---|
| |  |   |   |  |  |
| **Architecture** | Centralized internal database (e.g., IBM, Oracle). | Secure inter-party messaging/queue-based middleware. | Third party agent-in-possession. | Distributed ledger with cryptographic integrity. | Original trinary architecture, clustered distributed ledger, trustworthy community management cryptographic integrity. |
| **Settlement Process** | Internal. | Independent (but enabled by messaging). | Via clearing house. | **Consensus (Proof of stake or proof of work).** | Trusted relations and credentials management to establish consensus. **PROOF OF TRUST** |
| **Speed** | Real-time. | Up to 3-5 days. | Days, transaction dependent. | **Near real-time to minutes.** | **Real-time.** |
| **Transaction cost** | Internal IT. | External provider + settlement cost. | Third-party service. | Similar to internal database. | Marginal with respect to current operational cost. |
| **Benefits** | Speed, cost and (relative) simplicity. | Secure transaction between external parties, standardized data format. | Reduced settlement risk/DVP. | Enables third-party transaction to be as simple and efficient as internal transactions. | By design compliance with GDPR, eIDAS and NIS regulations. Signature integrity, signature consent, electronic seal. Seamless integration with existing systems/workflows. Modularity and full interoperability. Real-time management of revocation lists and traceability. |
| **Limitations** | Committing transactions with third parties/across network. | Data errors slow transactions, flexibility. | Complex and cumbersome, expensive. | Technology maturity, integration with existing systems/workflows, consensus not controlled by independent body, difficult to manage revocation, relies on the absence of trust between parties. | Need for strong enrolment to enable multi-factor authentication. |

trustseed

# GDPR vs. Blockchain

| | BLOCKCHAIN PROOF OF WORK/STAKE | | PROOF OF TRUST |
|---|---|---|---|
| In the context of GDPR compliance (from May 25, 2018) | Permisionless Blockchain (public) | Permissioned Blockchain (private or consortium) | Private blockchain (supervised and trusted) TRINARY SYSTEM |
| 1. Offline access (Art.13.2.b-Art.15) | No | No | Yes |
| 2. Validation independent from the infrastructure (Art.40.4-41.2.b) | No | No | Yes |
| 3. Total transaction privacy (Art.90.1) Data minimization disclosure (Art.5-47.2;d), pseudonymisation (Art. 32.1.a) | No | No | Yes |
| 4. Infrastructure shared (Art.29) by Controllers (Art.24) and Processors (Art.28) separately | No | Yes (Possible) | Yes |
| 5. Inexpensive (low transaction cost Including mandatory “appropriate means & guarantees”(Art.32-40-41-42) | No | Yes | Yes |
| 6. Fast (quick transaction validation) Art.5.1.d –Art.28.3. | No | Yes | Yes |
| 7. Proof of Identity, Rights, Proxies, Consent (Interchange, Signature) Art.6.3.b-Art.13.1.c | No | Yes (Possible) | Yes (Advanced Signature) |
| 8. Possibility to pseudonymiseerase, modify or update an information or a mean (e.g., right to be forgotten, key/certificate renewal). Art.16-17-18-19-20-22. | No | No | Yes |
| 9. Full compliance control against public or private regulations e.IDAS Art.26.33.45. | No | No | Yes |

陈安瑞

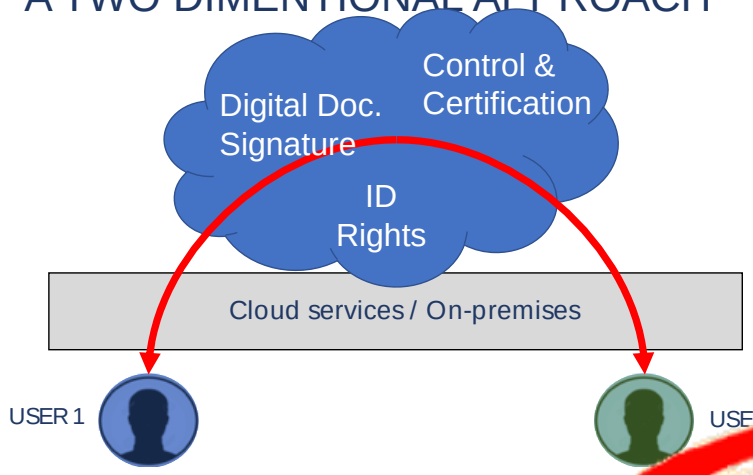
trustseed

# A SCALABLE PLATFORM

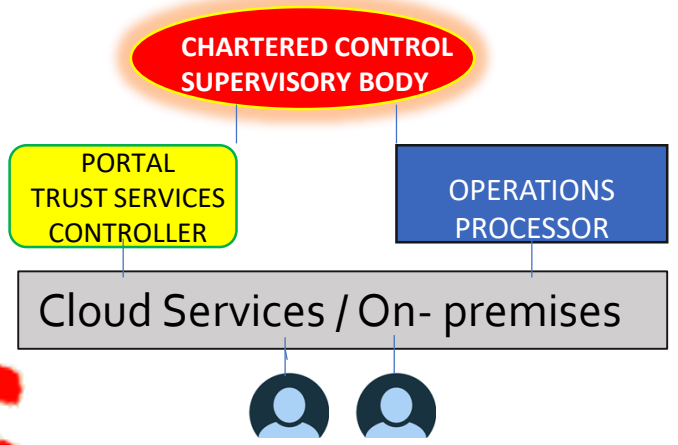
THE MUST :

**Complexity reduced to its simplest expression**
**Regulatory Assurance by the appropriate level of guarantee**
**Execution in “Real Time" and in "Present Value" or "Value Date"**

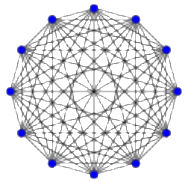
## TODAY
## A TWO DIMENTIONAL APPROACH



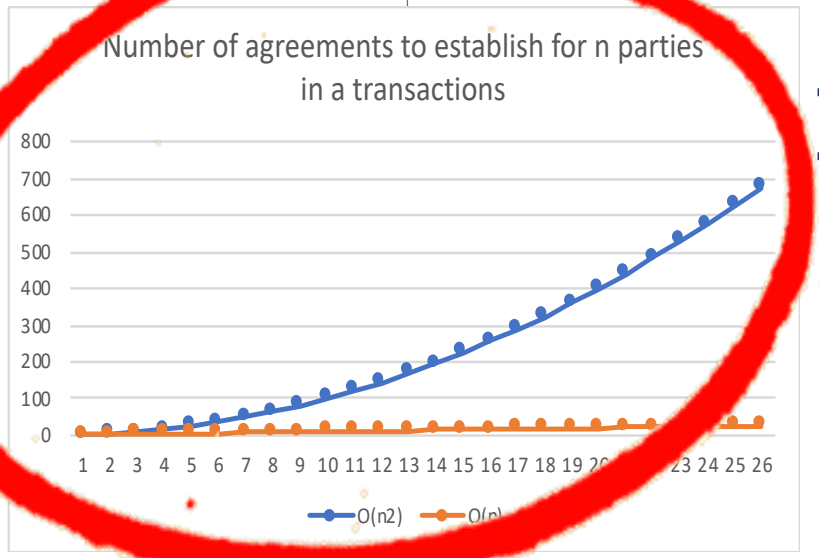

## TOMORROW (WITH VALESIGN)
## A THREE DIMENTIONAL APPROACH



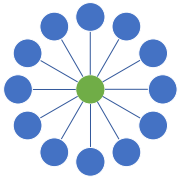

- Parties of the transaction are responsible for their own trust (= Security + Conformity) controls.
- Breaches are detected after the transaction ends (during the execution).
- Resolution of breaches are made through legal litigations between parties. No control on time.
- Complexity of multi-parties transaction is $O(n^2)$:



*n* parties in a transaction means $\frac{n \times (n-1)}{2} = O(n^2)$, bi-lateral negotiations.




- Trust (= Security + Conformity) controls are guaranteed by independent control body.
- Breaches are detected ahead of transaction execution.
- Resolution of breaches are made during transaction commitment.
- Complexity of multi-parties transaction is linear:



*n* parties in a transaction means *n*, i.e., $O(n)$ controls

陈安瑞

trustseed

# CHARTERED VALIDATION & CONTROL BLOCKCHAIN (GDPR): 3 MAIN CHALLENGES

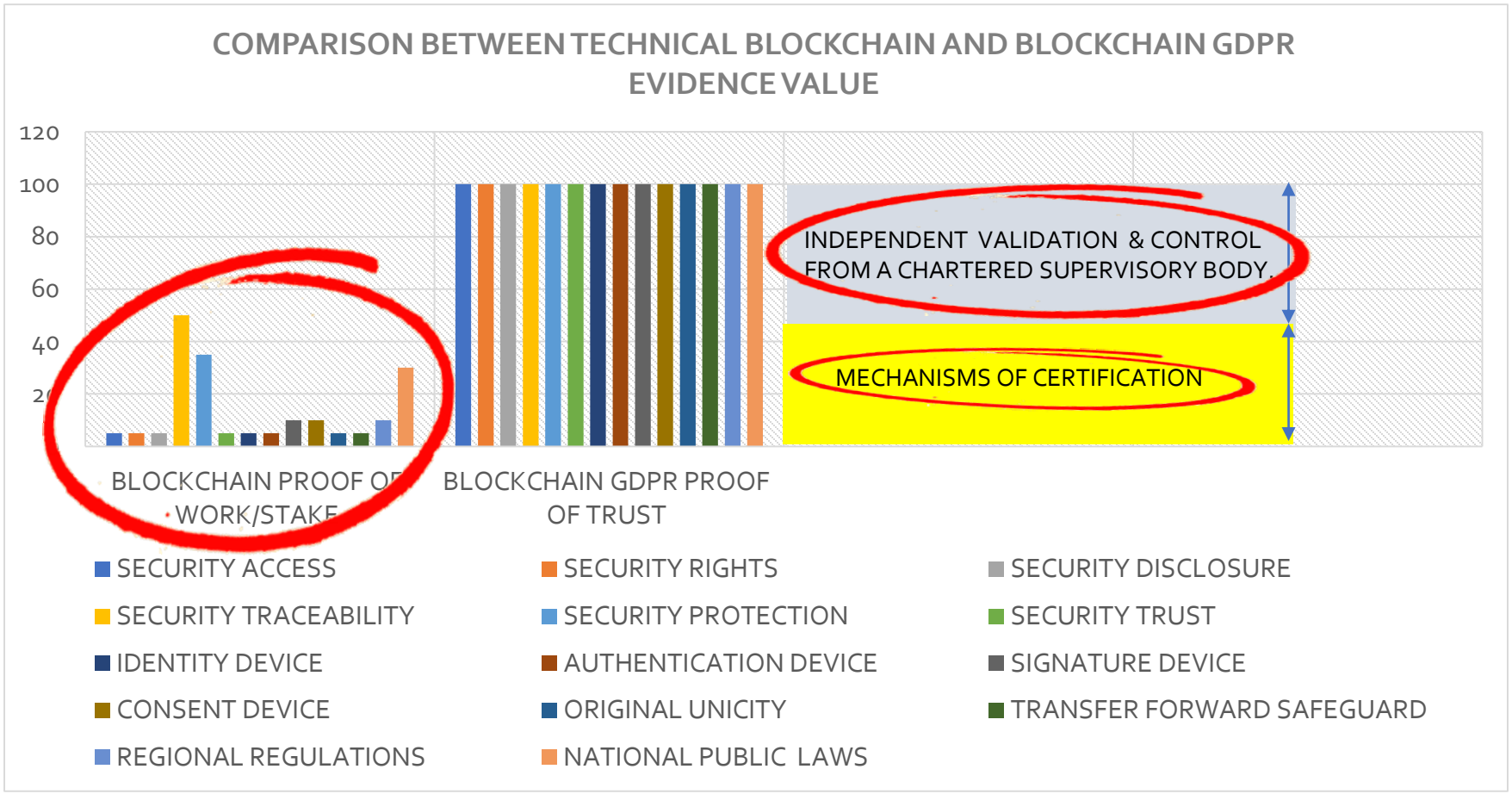
| CHARTERED CONTROL & VALIDATION BLOCKCHAIN | MANDATORY OBLIGATIONS | RULES OF THE GAME | GDPR SHARES RESPONSABILITIES CONTROLLER S/ PROCESSORS/ FRONT OFFICE BACK OFFICE | REAL TIME CONTROL MECHANISMS VALIDITY CONFORMITY | PERIODIC CERTIFICATION MECHANISMS VALIDITY CONFORMITY | SERVICE LEVERAGE AGREEMENT APPROPRIATE GUARANTEES |
|---|---|---|---|---|---|---|
| SECURITY | APPROPRIATE **ORGANISATIONAL MEANS** CERTIFIED PROCEDURES | PRINCIPLES | | | | |
| | 1. TO ACCESS Portal and Account | Qualified Certificates | CONTROLLERS / FRONT OFFICE | VALIDITY | CONFORMITY | GUARANTY |
| | 2.TO MANAGE | Mandatory Rights | CONTROLLERS / FRONT OFFICE | VALIDITY | CONFORMITY | GUARANTY |
| | 3.TO DISCLOSURE | Marking Minimisation | CONTROLLERS / FRONT OFFICE | CONFORMITY | CONFORMITY | GUARANTY |
| | 4.TO SAFE –FOLLOW-UP | Integrity HASH Traceability | PROCESSORS/BACK OFFICE | CONFORMITY | CONFORMITY | GUARANTY |
| | 5.TO PROTECT, TO LIMITE | Finalisation Encryption | PROCESSORS/BACK OFFICE | CONFORMITY | CONFORMITY | GUARANTY |
| | 6. To TRUST MULTILATERAL QUALIFIED | Interoperability Qualification | CONTROLLERS / FRONT OFFICE | VALIDITY | CONFORMITY | GUARANTY |
| DIGITIZING | APPROPRIATE TECHNICAL MEANS CERTIFIED HARD –SOFT WARES | EVIDENCE VALUE MEASUREMENT | | | | |
| | 1.DENTITY REGISTRY CERTIFICATE | EVIDENCE VALUE METRICS | CONTROLLERS / FRONT OFFICE | VALIDITY | VALIDITY | GUARANTY |
| | 2.AUTHENTICATION DEVICE CERTIFICATE | EVIDENCE VALUE METRICS | CONTROLLERS / FRONT OFFICE | VALIDITY | VALIDITY | GUARANTY |
| | SIGNATURE DEVICE CERTIFICATE | EVIDENCE VALUE METRICS | PROCESSORS/BACK OFFICE | CONFORMITY | VALIDITY | GUARANTY |
| | 3.CONSENT DEVICE CERTIFICATE | EVIDENCE VALUE METRICS | PROCESSORS/BACK OFFICE | CONFORMITY | VALIDITY | GUARANTY |
| | 4.FILE DOCUMENT ORIGINAL | EVIDENCE VALUE METRICS | PROCESSORS/BACK OFFICE | CONFORMITY | VALIDITY | GUARANTY |
| | 5.CORRESPONDENCEMAILING TRANSFER | EVIDENCE VALUE METRICS | PROCESSORS/BACK OFFICE | CONFORMITY | VALIDITY | GUARANTY |
| LAWFULNESS | LEGAL & CROSS BORDER FRAMEWORK | SUPERVOSORY BODY | | | | |
| | 1.REGIONAL REGULATIONS | GDPR- e.IDAS | CONTROLLERS / PROCESSORS | CONFORMITY | | LEGAL |
| | 2.NATIONAL LAWS | ROGATORY/JUDICIAL MANDATES | CONTROLLERS / PROCESSORS | CONFORMITY | | LEGAL |
| | 3.PRIVATE LAWS | INTERCHHANGE AGREEMENT | END USERS | CONFORMITY | VALIDITY | LEGAL |
| | 4.CODES OF CONDUCT (MARKET-PLACES) | NATIONAL AUTHORITY of MARKET | CONTROLLERS / PROCESSORS | CONFORMITY | | LEGAL |

陈安瑞

trustseed

# CHARTERED VALIDATION & CONTROL BLOCKCHAIN VIA PROOF OF WORK or STAKE

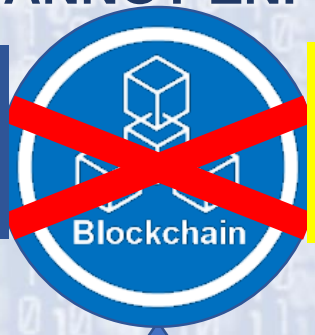
| CHARTERED CONTROL & VALIDATION BLOCKCHAIN | GDPR MANDATORY OBLIGATIONS = WEAK ! | GDPR REGULATION RULES OF THE GAME | GDPR SHARES RESPONSABILITIES CONTROLLER S/ PROCESSORS/ FRONT OFFICE BACK OFFICE | REAL TIME CONTROL MECHANISMS VALIDITY CONFORMITY | PERIODIC CERTIFICATION MECHANISMS VALIDITY CONFORMITY | SERVICE LEVERAGE AGREEMENT APPROPRIATE GUARANTEES |
|---|---|---|---|---|---|---|
| SECURITY | APPROPRIATE ORGANISATIONAL MEANS CERTIFIED PROCEDURES | PRINCIPLES | | | | |
| | 1. TO ACCESS Portal and Account | Qualified Certificates | CONTROLLERS / FRONT OFFICE | VALIDITY | CONFORMITY | |
| | 2.TO MANAGE | Mandatory Rights | CONTROLLERS / FRONT OFFICE | VALIDITY | CONFORMITY | |
| | 3.TO DISCLOSURE | Marking Minimisation | CONTROLLERS / FRONT OFFICE | CONFORMITY | CONFORMITY | |
| | 4.TO SAFE – FOLLOW-UP | Integrity Hash /Traceability | PROCESSORS/BACK OFFICE | CONFORMITY | CONFORMITY | |
| | 5.TO PROTECT, TO LIMITE | Finalisation Encryption | PROCESSORS/BACK OFFICE | CONFORMITY | CONFORMITY | |
| | 6. To TRUST MULTILATERAL | Interoperability Qualification | CONTROLLERS / FRONT OFFICE | VALIDITY | CONFORMITY | |
| DIGITIZING | APPROPRIATE TECHNICAL MEANS CERTIFIED HARD –SOFT WARES | EVIDENCE VALUE MEASUREMENT | TRINARY ARCHITECTURE | | | |
| | IDENTITY REGISTRY CERTIFICATE | EVIDENCE VALUE METRICS | CONTROLLERS / FRONT OFFICE | VALIDITY | VALIDITY | |
| | 1.AUTHENTICATION DEVICE CERTIFICATE | EVIDENCE VALUE METRICS | CONTROLLERS / FRONT OFFICE | VALIDITY | VALIDITY | |
| | 2.SIGNATURE DEVICE CERTIFICATE | EVIDENCE VALUE METRICS | PROCESSORS/BACK OFFICE | CONFORMITY | VALIDITY | |
| | 3.CONSENT DEVICE CERTIFICATE | EVIDENCE VALUE METRICS | PROCESSORS/BACK OFFICE | CONFORMITY | VALIDITY | |
| | 4.FILE DOCUMENT ORIGINAL | EVIDENCE VALUE METRICS | PROCESSORS/BACK OFFICE | CONFORMITY | VALIDITY | |
| | 5.CORRESPONDENCEMAILING TRANSFER | EVIDENCE VALUE METRICS | PROCESSORS/BACK OFFICE | CONFORMITY | VALIDITY | |
| LAWFULNESS | LEGAL FRAMEWORK | SUPERVISORY BODY | | | | |
| | 1.REGIONAL REGULATIONS | GDPR- e.IDAS | CONTROLLERS / PROCESSORS | CONFORMITY | | |
| | 2.NATIONAL LAWS | ROGATORY/JUDICIAL MANDATES | CONTROLLERS / PROCESSORS | CONFORMITY | | LEGAL |
| | 3.PRIVATE LAWS | INTERCHHANGE AGREEMENT | END USERS | CONFORMITY | VALIDITY | |
| | 4.CODES OF CONDUCT (MARKET-PLACES) | NATIONAL AUTHORITY of MARKET | CONTROLLERS / PROCESSORS | CONFORMITY | | |


COMPARISON BETWEEN TECHNICAL BLOCKCHAIN AND BLOCKCHAIN GDPR EVIDENCE VALUE
120
100
80
60
40
INDEPENDENT VALIDATION & CONTROL FROM A CHARTERED SUPERVISORY BODY.
MECHANISMS OF CERTIFICATION
BLOCKCHAIN PROOF OF WORK/STAKE
BLOCKCHAIN GDPR PROOF OF TRUST
SECURITY ACCESS
SECURITY RIGHTS
SECURITY DISCLOSURE
SECURITY TRACEABILITY
SECURITY PROTECTION
SECURITY TRUST
IDENTITY DEVICE
AUTHENTICATION DEVICE
SIGNATURE DEVICE
CONSENT DEVICE
ORIGINAL UNICITY
TRANSFER FORWARD SAFEGUARD
REGIONAL REGULATIONS
NATIONAL PUBLIC LAWS

trustseed

# AND... PUBLIC BLOCKCHAIN CANNOT ENFORCE GDPR

**Total transaction privacy?**




- Data are visible to anyone.
- Blocks are public.
- Even if it is encrypted.

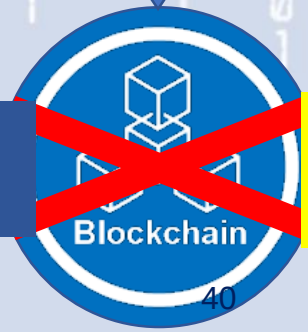
**Right to be forgotten?**


- Blocks are immutable.
- Impossible go back in the past.


**Infrastructure maintained by known/trusted entities?**


- By construction, there is no “a priori” trust established in the public blockchain.
- A consensus must be established.

**Proof of identity?**




- There is no identity check in the public blockchain.

陈安瑞

TABLE OF COMPETENCE OF TRUSTED SERVICES (GDPR) via **BLOCKCHAIN PROOF OF WORK / STAKE** :NOT GDPR COMPLIANT

trustseed

| | | | DISTRIBUTION OF 70 OBLIGATIONS BETWEEN QUALIFIED THIRD PARTIES | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | FUNCTIONS (20) | PRINCIPLES (12) Value 5 /5 | SECURITY | EVIDENCE VALUE PROBATIVE VALUE | MULTILATERAL NOTATION STATUS CONFORMITY | CONTROL VALIDITY PROOF OF TRUST | REAL TIME INTEROPERABILITY UPDATE A PRIORI | COST REDUCTION COLLABORATIVE EFFICIENCY SIMPLICITY | LIBERTY ABILITIES | APPROPRIATE GUARANTEES EXTERNALITIES | SUB TOTAL |
| 1 | ACCESS IDENTIFICATION AUTHENTICATION | SECURITY PRINCIPLE | 3 | | | 3 | 3 | | | | 9 |
| 2 | SERVICES -CONTROL MECHANISMS MULTIPARTIES | OBLIGATION OF RESULT | | 2 | | 0 | 0 | 1 | | | 3 |
| 3 | AUTHENTICATION MULTILATERAL ADEQUACY | LEGAL BASIS PRINCIPLE | | | 2 | 0 | 0 | 1 | | | 3 |
| 4 | RIGHTS -VALUE MULTILATERAL ADEQUACY | LEGAL BASIS PRINCIPLE | | | 2 | 0 | 0 | | | | 2 |
| 5 | RELATIONSHIP BILATERAL AGREEMENT | CONSENT PRINCIPLE | | | 2 | 0 | 0 | | | | 2 |
| 6 | SIGNATURES (1) MULTILATERAL ADEQUACY | CONSENT PRINCIPLE | | | 3 | 3 | 3 | | | | 9 |
| 7 | DATACATEGORIES MARKING DISCLOSURE REGISTER | SECURITY PRINCIPLE | 0 | 0 | 0 | 0 | 0 | 0 | | | 0 |
| 8 | KEYS EXCLUSIVE OWNERSHIP & ENCRYPTION | Separation of Powers Principle | 0 | | | | 0 | | | | 0 |
| 9 | LIMITED OPERATIONS TREATMENT ASSIGMENT | SECURITY PRINCIPLE | 2 | | | 0 | 0 | | | | 2 |
| 10 | SCHEDULING Certification Mechanisms Multilateral | Separation of Powers Principle | | | 0 | | 0 | 0 | | | 0 |
| 11 | DOCU.+SIGN. ORIGINAL CREATION | Uniqueness Principle | | 2 | | 0 | 0 | 1 | | 0 | 3 |
| 12 | DOCUMENTARY ENCRYPTION | Confidentiality Principle | 2 | | | 0 | 0 | 0 | | 0 | 2 |
| 13 | DATA EXTERNALISATIONTRANSFER ABROAD | Finalisation Principle | | | 0 | 0 | | 0 | | | 0 |
| 14 | OPTION : OPPOSITION REVOCATION CAPACITY | Protection Principle | | | | | 0 | 0 | 0 | 0 | 0 |
| 15 | OPTION : ERASURE CAPACITY | Protection Principle | | | | | 0 | O | 0 | 0 | 0 |
| 16 | OPTION : RECTIFICATION CAPACITY | Protection Principle | | | | | 0 | 0 | 0 | 0 | 0 |
| 17 | OPTION : PSEUDONYMISATION CAPACITY | Protection Principle | | | | | 0 | 0 | 0 | 0 | 0 |
| 18 | OPTION :PORTABILITY CAPACITY | Protection Principle | | | | | 0 | 0 | 0 | 0 | 0 |
| 19 | OPTION : PROROGATION CAPACITY | Protection Principle | | | | | 0 | 0 | 0 | 0 | 0 |
| 20 | OPTION : PROPERTY SWITCHING CAPACITY | Accountability Principle | | | | | 0 | 0 | 0 | 0 | 0 |
| | 3 QUALIFIED TRUSTED THIRD PARTIES | 12 PRINCIPLES | 7/25 | 4/15 | 9/30 | 6/50 | 6/95 | 3/55 | 0/35 | 0/45 | 35 /350 |

**23/70= 33%** SECURE EVIDENCE VALUE

INDEPENDANT VALIDATION

6/95= 6% Real Time PRESENT VALUE

0 MULTILATERAL DIGITAL POLICY

QUALIFIED CONTROLLER : SERVICES

QUALIFIED PROCESSOR : OPERATIONS

CHARTERED VALIDATION BODY

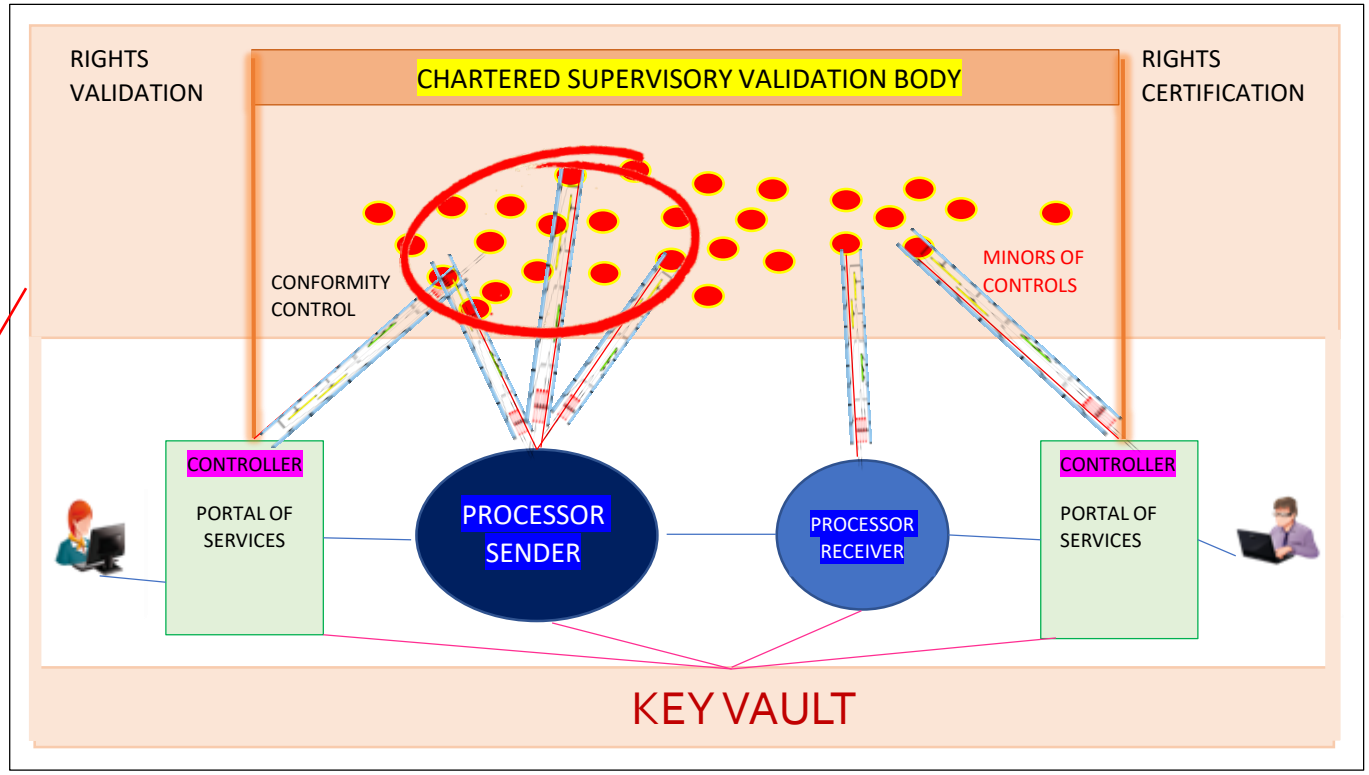
- SIGNATURE OF IDENTITY AUTHENTICATION, OF DOCUMENTARY SIGNATURE, OF TRACEABILITY SEALING
- Notation of the "CURRENT BLOCKCHAIN" Application : 35 / 350 equal 10 %

-

trustseed

# BLOCKCHAIN PROOF OF TRUST IN TRINARY SYSTEM EMBEDDED

| | TRUSTWORTHY MESSAGING GDPR | **Number of Blocks** | % TOTAL 372 BLOCK |
|---|---|---|---|
| 1 | CONTROLLER SENDER/BUYER | **57** | 15% |
| 2 | CONTROLLER RECEIVER/SELLER | **14** | 4% |
| | SUB TOTAL CONTROLLERS | **71** | **19%** |
| 3 | PROCESSOR SENDER/BUYER | **230** | 62% |
| 4 | PROCESSOR RECEIVER/SELLER | **7** | 2% |
| | SUB TOTAL PROCESSORS | **237** | **64%** |
| 5 | CHARTERED SUPERVISORY BODY | **24** | 6% |
| 6 | THIRD PARTIES OF CONTROL | **40** | 11% |
| | **VALIDATION & CONTROL INDEPEDENTLY** | **64** | **17%** |
| | GENERAL TOTAL | **372** | 100 % |



陈安瑞

trustseed

# BLOCKCHAIN PROOF OF TRUST : CONTROL MECHANISMS (Art.41)

| | TRUSTWORTHY MESSAGING GDPR | **Number of Block s** | % TOTAL 372 BLOCKS |
|---|---|---|---|
| 1 | CONTROLLER SENDER/BUYER | 57 | 15% |
| 2 | CONTROLLER RECEIVER/SELLER | 14 | 4% |
| | SUB TOTAL CONTROLLERS | 71 | **19%** |
| 3 | PROCESSOR SENDER/BUYER | 230 | 62% |
| 4 | PROCESSOR RECEIVER/SELLER | 7 | 2% |
| | SUB TOTAL PROCESSORS | 237 | **64%** |
| 5 | CHARTERED SUPERVISORY BODY | 24 | 6% |
| 6 | THIRD PARTIES OF CONTROL | 40 | 11% |
| | VALIDATION & CONTROL INDEPEDENTLY | 64 | **17%** |
| | GENERAL TOTAL | 372 | 100 % |

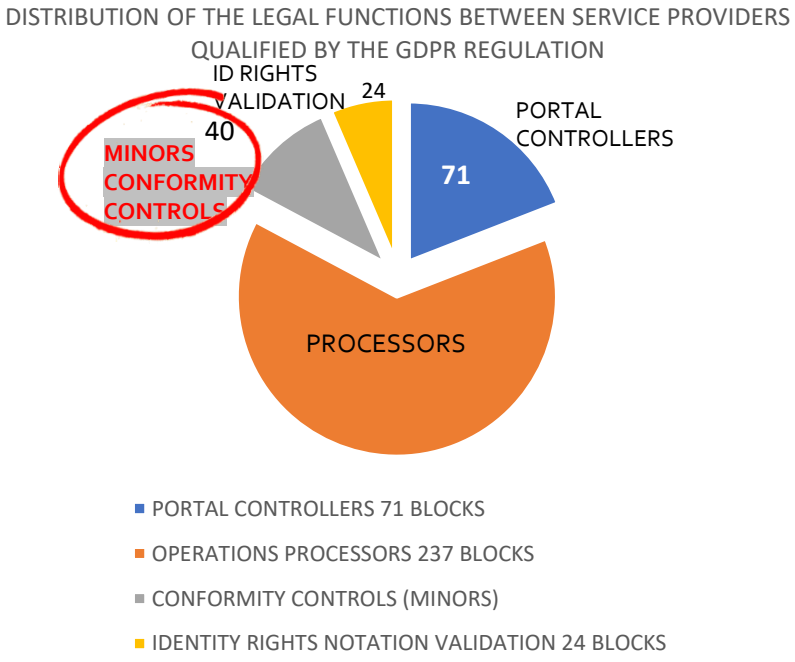
t

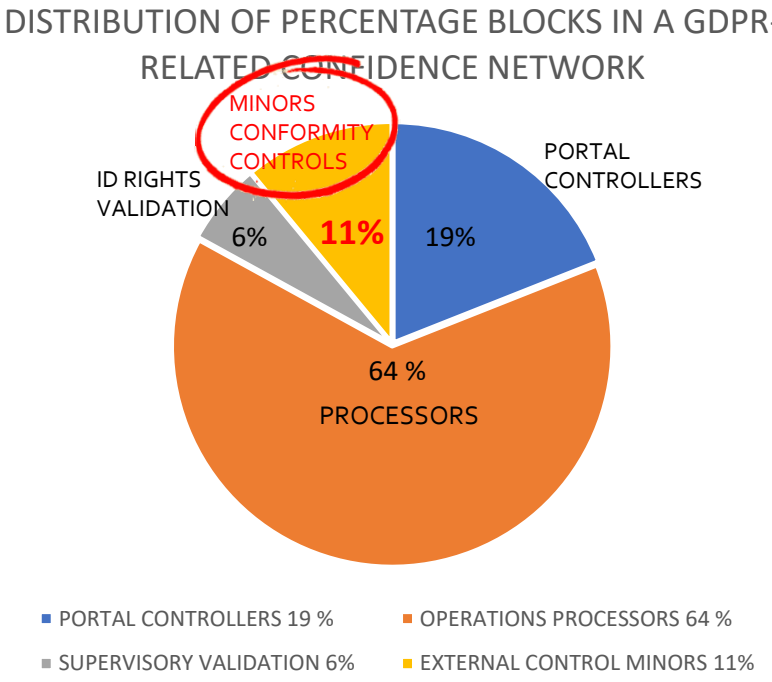
| SEQUENCES | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 28 | 30 | 31 | 32 | 33 | 34 | T | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CONTROLLER** SENDER | | 33 | | 5 | | | | 4 | | | 4 | | 2 | | | | | | | | | | 1 | | | | 4 | | 4 | | | | | | 57 | 15 % |
| SUPERVISORY VALIDATION | 23 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 1 | | 24 | 6 % |
| THIRD PARTY CONTROL | | | 8 | | | | | | | | | 6 | | | | 6 | | | 4 | | 7 | | | | | | 5 | | | 4 | | | | 40 | 11 % |
| PROCESSOR SENDER | | | | | 71 | | 25 | | | 1 | | | | 2 | | | | 45 | | 13 | | 11 | | 3 | | 1 | | | 28 | | 24 | | 6 | 230 | 62 % |
| **CONTROLLER** RECEIVER | | | | | | | | | 4 | | | | | | 3 | | 6 | | | | | | | | 1 | | | | | | | | | | 14 | 4 % |
| PROCESSOR RECEIVER | | | | | | 7 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 7 | 2 % |
| SEQUENCES | 23 | 33 | 8 | 5 | 71 | 7 | 25 | 4 | 4 | 1 | 4 | 6 | 2 | 2 | 3 | 6 | 6 | 45 | 4 | 13 | 7 | 11 | 1 | 3 | 1 | 1 | 4 | 5 | 4 | 28 | 4 | 24 | 1 | 6 | 372 | 100% |
| CUMULATIVE | 23 | 56 | 64 | 69 | 140 | 147 | 172 | 176 | 180 | 181 | 185 | 191 | 193 | 195 | 198 | 204 | 210 | 255 | 259 | 272 | 279 | 290 | 291 | 294 | 295 | 296 | 300 | | | | | | | | 372 | 100% |

305 309 337 341 365 366 372

trustseed

# 372 MICRO CONTROLS - 34 BLOCKS
# INCLUDING SWORN NOTARY EMPLOYEE ADVANCED SIGNATURE




Ethereum network has nearly 25,000 reachable nodes

Bitcoin around 7,000 nodes

陈安瑞

trustseed

# PUBLIC BLOCKCHAIN – POINTS OF ATTENTION

Someone requests a transaction

The requested transaction is broadcasted to a P2P network of computers (the nodes)

Where is going the treatment, which Country

WHO IS HE ?

How to process quickly if 200 tags to be verified in a smart contract

Ethereum network has nearly 25,000 reachable nodes

Bitcoin around 7,000 nodes

VALIDATION

The network of nodes validates the transaction and the user's status using known algorithm

The nodes of validation are anonymous persons

A verified transaction can involve crypto currency, contract, records or other information

The transaction is completed

The new block is then added to the existing blockchain, in a way that is permanent and unalterable

How to manage the right to forget, rectify or renew expired certificates

## CRYPTOCURRENCY

Has no intrinsic value in that it is not redeemable for another commodity such as gold

Has no physical form and exists only in the network

Its supply is not determined by a central bank and the network is completely decentralized

Volatility, Liquidity… no one Corporate Treasurer will accept the deal

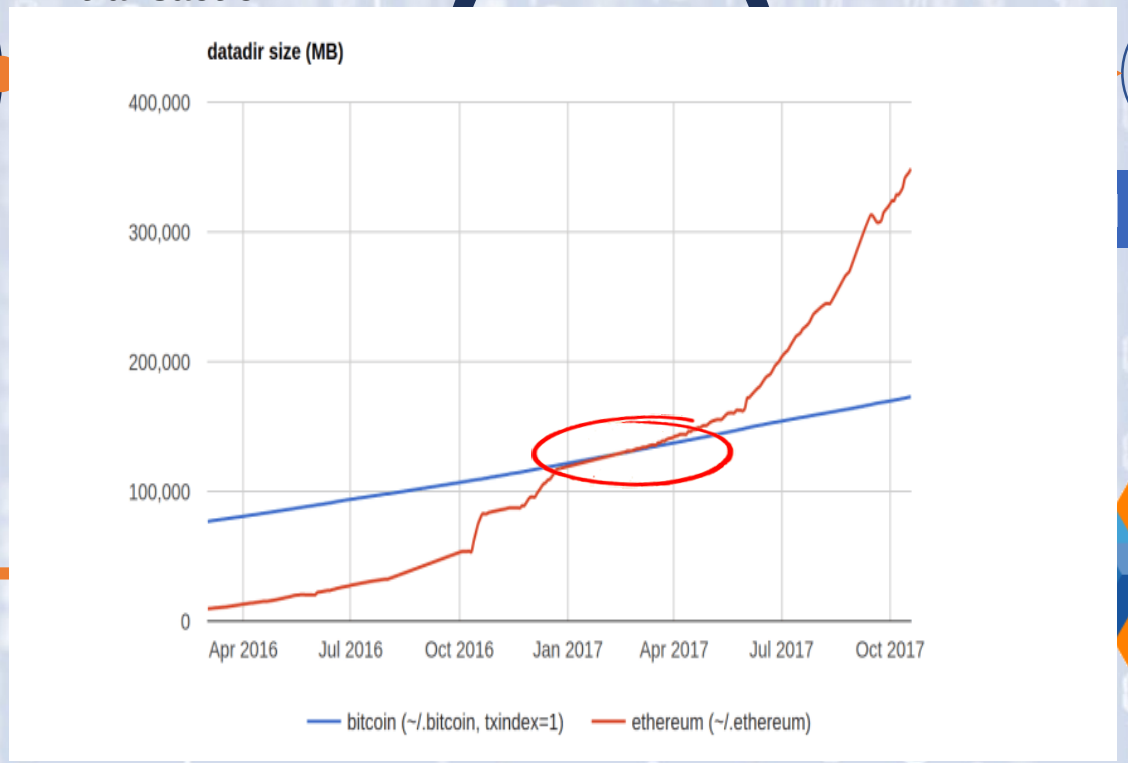
Exchange Risk !! IFRS –Bale 3

trustseed

# PUBLIC BLOCKCHAIN –VERY ENERGY COMSUMING

Someone requests a transaction

The requested transaction




A verified transaction can involve crypto currency, contract, records or other information

CRYPTOCURRENCY

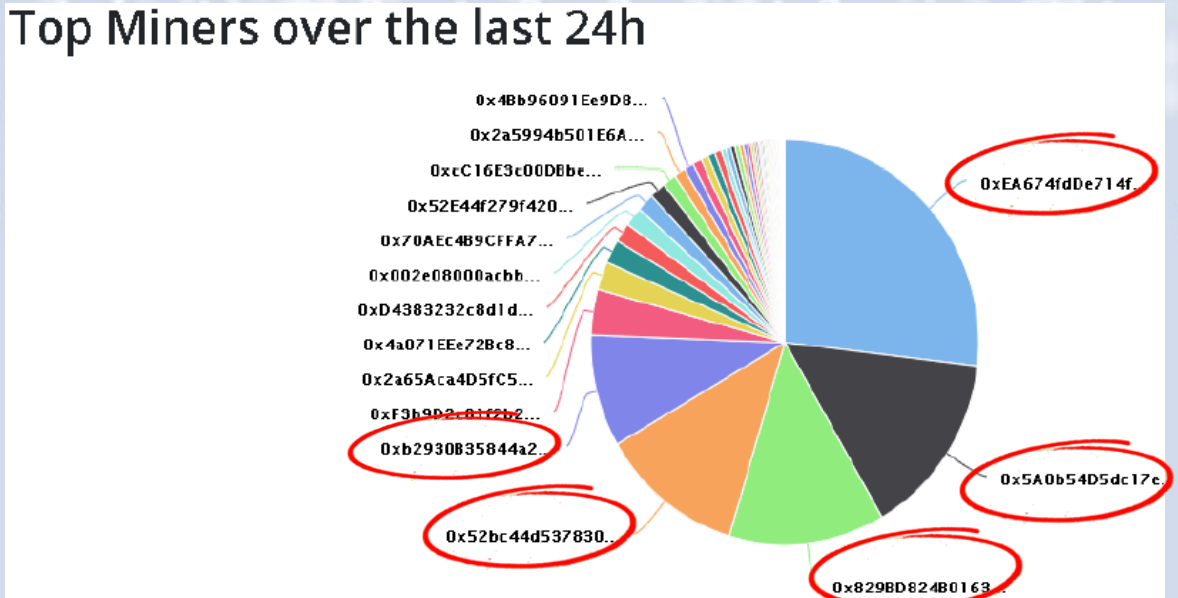
陈安瑞

# A QUESTION OF INDEPENDENCE

Source: https://www.etherchain.org/charts/topMiners (on August 1, 2018 at 15:09 CET)

| Miner | Hashrate | % |
|---|---|---|
| All 75,70% | 281.62 TH/s | 100 % |
| 0xEA674fdDe714f... | 75.68 TH/s | 26.9 % |
| 0x5A0b54D5dc17e... | 41.55 TH/s | 14.8 % |
| 0x829BD824B0163... | 36.60 TH/s | 13.0 % |
| 0x52bc44d537830... | 33.81 TH/s | 12.0 % |
| 0xb2930B35844a2... | 25.26 TH/s | 9.0 % |

No strategic independence





**+72% of the blocks under the control of 4 miners**

trustseed

trustseed

## THE REALITY ON DECENTRALIZATION

**“The entire blockchain for both systems (*Bitcoin and Ethereum*) is determined by fewer than 20 mining entities.”**

Source: Decentralization in Bitcoin and Ethereum Networks, Financial Cryptography and Data Security 2018 (https://arxiv.org/abs/1801.03998)


Lie and vulnerability


**58%**

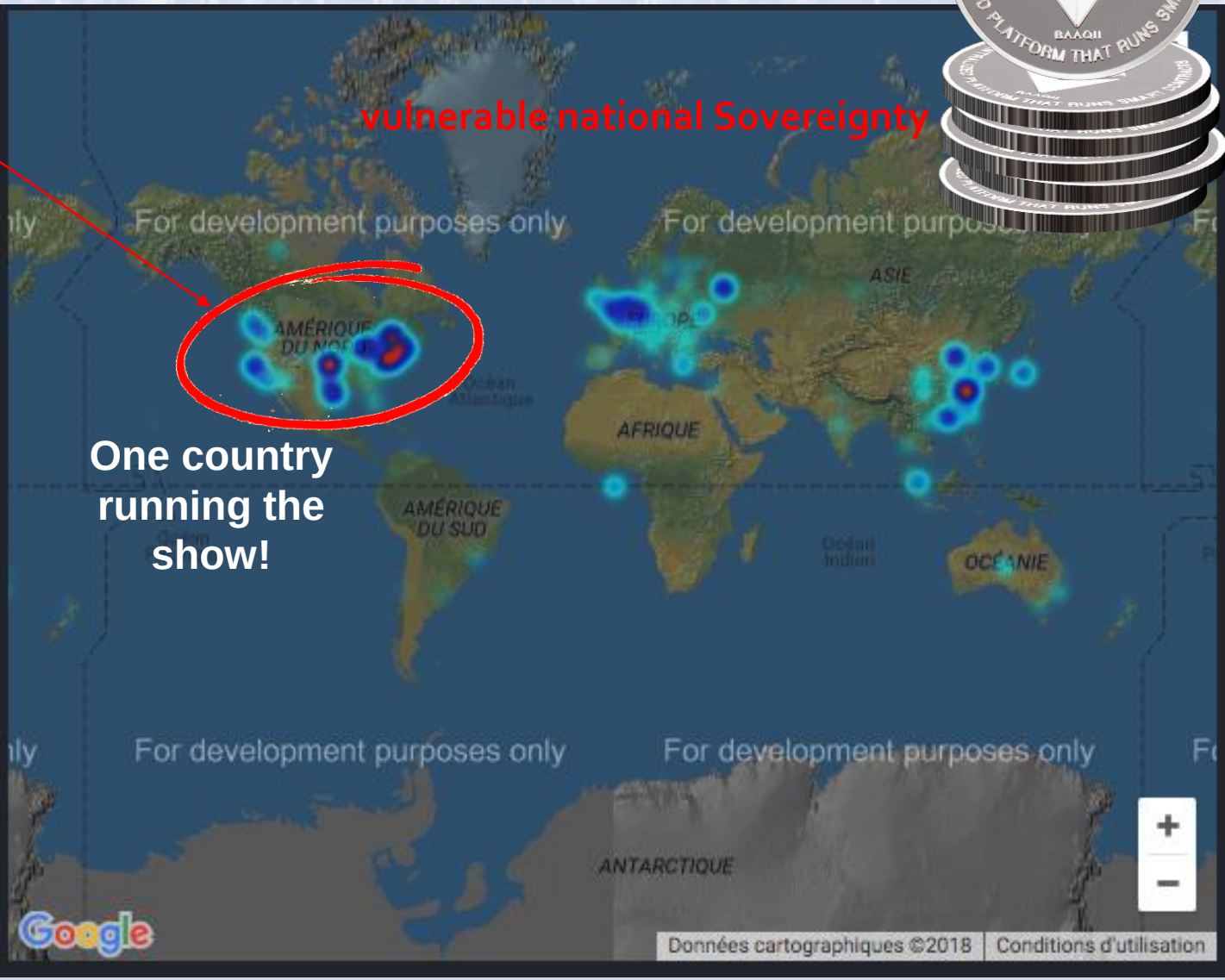

**28%**

陈安瑞

# A QUESTION OF NATIONAL SOVEREIGNTY

Source: https://www.ethernodes.org/ (on August 1, 2018 at 15:09 CET)

| | |
|---|---|
| Total | 14634 (100%) |
| United States | 6007 (41.05%) |
| China | 2026 (13.84%) |
| Canada | 1101 (7.52%) |
| Germany | 625 (4.27%) |
| Russian Federation | 617 (4.22%) |
| United Kingdom | 439 (3.00%) |
| Korea, Republic of | 333 (2.28%) |
| Netherlands | 315 (2.15%) |
| France | 274 (1.87%) |
| Japan | 240 (1.64%) |






trustseed

# THE REALITY ON SECURITY


**"The cost of the deanonymisation attack on the full Bitcoin network is under 1500 €"**

Source: Deanonymisation of clients in Bitcoin P2P network, ACM Conference on Computer and Communications Security, 2014 (*https://arxiv.org/pdf/1405.7418*)

**An no progress to guarantee long term multilateral secrety by « account owner » and by « document proxy » with real time entitlement supervision and the capability to transfer document asset by switching the encryption parameter in favour of the beneficiary instantaneously.**


## Miners' have strong influence on transaction management as they can:

**Lack of Transparency**

1. **Censor transactions (→ DoS) Deny of Service**
2. **Re-order transactions (→ front-running)** **Discretionary right**

Source: Security challenges in Ethereum smart contract programming
Sergei Tikhomirov, CLUSIL Blockchain series – Installment #4 Luxembourg, 7/9/2017
(*https://www.slideshare.net/SergeiTikhomirov/security-challenges-in-ethereum-smart-contract-programming*)

trustseed

# BUILDING A PROFITABLE BUSINESS MODEL?


speculative solution unacceptable by industry

Strategy led by banks favorable to speculation and spread trading !!!!

Source : https://markets.businessinsider.com/currencies/eth-usd, on August 1, 2018 at 16:47 CET

## PRICING BASIC PRINCIPLE

Ethereum transaction fees based on ETH rate.

Highly fluctuating and not regulated.

Bill of Material Cost

+

Development Cost

+

Overhead

+

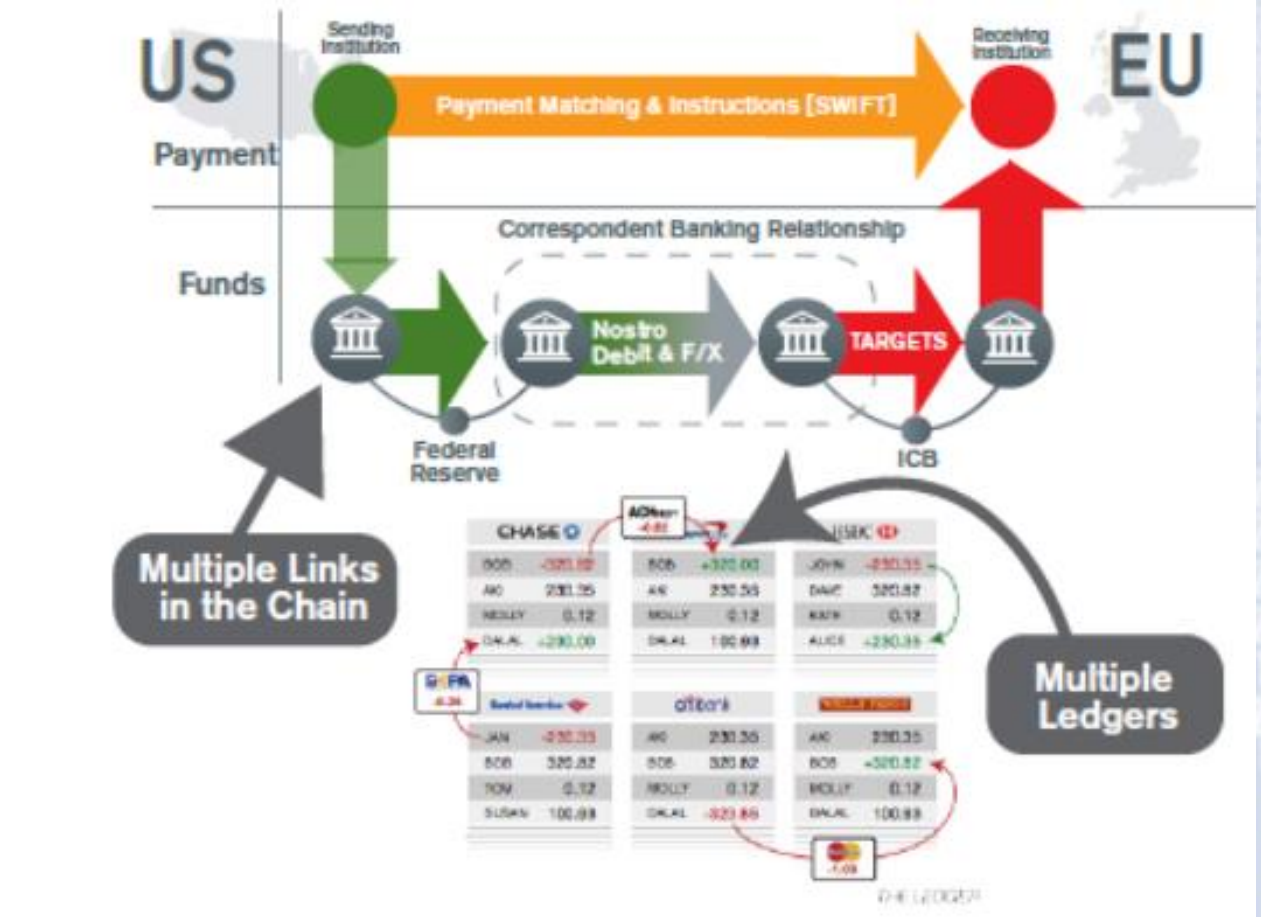
Service/ Product Price

Price of a service/product is negotiated up-front with the customer and cannot handle the fluctuations of ETH.

trustseed

# A CLEAR NEED FOR INTEROPERABILITY

## A PAYMENT TRANSACTION ACROSS MULTIPLE "LEDGERS »




| ISSUES | |
|---|---|
| ▪ **Unpredictable** (slow) delivery | ▪ Manual customer service |
| ▪ **Unpredictable** (high) cost | ▪ High exception rate |

**2 WAYS TO ADDRESS THE PROBLEM:**

**(1) Homogeneization**

- **Hard to achieve**

**(2) Interoperability**

- **Hard to implement and maintain inside each blockchain architecture**
- **Easier to implement and maintain via a third party solution versus Trinary System**

Source: *https://www.finastra.com/viewpoints/product-insights/five-things-blockchain-must-get-right-to-realize-its-full-transformative-potential*

# CONCLUSION: DIGITAL MARKET PLACE REGULATION

trustseed

# CONCLUSION: FROM FEAR TO TRUST

## 3 POSSIBLE SCENARII FOR CYBERSECURITY FUTURE

### Cyberdigital Prehistory

- no anticipation of cyber risk
- little or no collaboration between economic actors

=

- cyber criminal domination
- impact on growth and trust

### Cyberdigital Middle Age

- knowledge of a cyber threat, investments
- few collective rules in force, few alliances
- a shy defense culture

=

- risk of cyber disaster restraint but not null
- risk amplified in a future "everything and all connected"

### Cyberdigital Renaissance

- massive collaboration of private and public actors
- “White net”: more agile defense and prospective vision
- common doctrines

=

- beneficial impact on the economic environment (lower costs of cybersecurity)
- mastering cyber risk
- cybersecurity becomes a “utility”

Loss of trust → Trust

陈安瑞

trustseed

# STATE

NATIONAL SOVEREIGNTY

DIGITAL ECONOMY

CODES OF CONDUCT & SCHEMES

NATIONAL AUTHORITIES OF MARKETS

..Two-dimensional code..

HUMAN RESSOURCES

TRUST SERVICES
CONTROLLERS
PORTALS

Certificat

RETAILS BANKING SERVICES
CONTROLLERS

R&D INNOVATION LABS
Data Protection Impact Assessment,
Tests/Standards

CHARTERED
CONTROL
BODIES

MARKET PLACES
QUALIFIED DATA
PROFILING, SCORING
Artificial Intelligence

CAPITAL MARKETS
QUALIFIED DATA
FINANCIAL RATING /ACCOUNTING
Artificial Intelligence

IP MARMET
QUALIFIED DATA
ANALYSIS, STANDARDS
Artificial Intelligence

CONFORMITY
ASSESSMENT
BODIES

PROCESSORS
CRYPTO ASSETS & SECURITIES

PROCESSORS
CRYPTO-TRANSACTIONS

INDUSTRY SECTORS
CERTIFIED HARD-SOFTWARES
ISO DEVICES

Certificat

RAW MATERIALS
Logistics

CONTROL MECHANISMS → QUALIFIED DATA →

Certificat

EVIDENCE VALUE
APPROPRIATE GUARANTEES
ARTIFICIAL INTELLIGENCE


Thank you for your attention
谢谢你的关注
陈安瑞