The vulnerability of current blockchains Blockchain disconnected from qualified Trust Networks Blockchain and GDPR-e.IDAS Regulations: the convergence to be made

THE CRAZY GUARDS OF THE BLOCKCHAIN

Nom BLOT-LEFEVRE Eric- SURVEY August 2018-TrustSeed R&D I

TITLE 1. BLOCKCHAIN CONSTRAINTS FOR SIGNATURE ENGAGEMENTS IN E.IDAS, GDPR AND NIS (SECURITY, INTEROPERABILITY AND RESILIENCE) REGULATIONS.

Separation of digital powers

The GDPR regulation in Article 4 establishes a **separation of powers** between the "trust services" guaranteeing the protection of personal data and which are qualified as Controllers (Art.4.7), the "service operators" provided with certified means to achieve transactions and which are qualified as "Processors" (Art.4.8.) and the supervisory authorities delegating their control and validation functions to independent bodies (Art.4.21 / Art.41) under the principle of " no one can constitute evidence on its own ".

Trust Services sign SLA Service Leverage Agreement

Strong commitment with results obligations

"Trust services" are usually organized in companies with an Internet portal. These services, which sign the SLA with their counterparties, are jointly and severally liable with their qualified service providers for performance obligations with respect to these counterparties: data confidentiality , exclusive control of the means of authentication, consent and signature, traceability and legality of digital transactions . To these primary obligations are attached individual rights: revocation, rectification, erasure (forgetting), and opposition.

The Trusted Service in SLA also undertakes to ensure that the Qualified Provider (Processor) and its potential suppliers comply with the following obligations:

1. The minimization of data Art. 25-47 GDPR : in other words, only the strictest necessary for the establishment of the document and the signatures must be disclosed in the matter of personal data.

2. Restriction or limitation of operations Art.18-19 GDPR: this means that the number of original documents and signatures is pre-established to ensure their "Uniqueness" with a distinctive registration, and to block or prohibit production beyond that limit.

3. Finalization of processing Art.5-13-28-32 GDPR: this means that the limited number of specific operations must be executed and controlled in such a way that there are no omissions liable to impair the quality of the service, the safety of the parties and the value probative of their signature commitments.

Chapter III Section 1 The General Provisions on Liability and the Burden of Proof states that the "Providers" (Processors) of the "Trust Services" are liable for damages caused by

a breach of their settlement obligations. It is up to the Provider to prove that the damage was caused without fault or negligence (Art.13).

By possibly limiting his liability in the SLA, the provider runs the risk of being punished for wrongfulness and disloyalty: in other words, none of his services can be done with impunity (Art.13.2).

Here is a summary of the obligations between Controllers and Processors under the control of a validation instance.

Particular and joint responsibility of the validation body

For its part, the Control and Validation Body, to exercise its obligations must manage in real time a number of databases from which are assessed the legal value, or the level of security required for each type of mail or transaction versus a rating scale used for all codes of conduct.

The independence of the validation authority with respect to trusted communities and services makes it possible to manage a rating calculated according to the Supporting Documents signed necessary for each community and validated by it.

The independence of the validation body is also used to keep the revocation lists, on the one hand those relating to users for the means (Authentication / Signature / Consent) and the powers they grant each other, ensuring the interoperability of the updated lists of all the changes which have occurred intraday, and secondly, the lists relating to users with regard to *mandated trust services* which cannot be revoked by themselves.

The independence of the validation body is also used to model for each community, business and code of conduct the traceability mechanisms specific to each type of transaction, to follow the traceability of the choice and order of service, transaction and counterparties, and serves finally, to verify the traceability of the programmed operations between several services and operators mandated by the signatory and counterparties.

The independence of the validation body is also used to maintain the list of qualified Controllers (Trust Services) and Processors (Service Providers) and possibly to detect faults, anomalies or frauds that may result in a penalty, a disqualification or a correction of procedure (Operation) or traceability mechanism (validation) to maintain resilience.

Vulnerability and feasibility of outsourcing for a validation instance

In the same way that the subcontracting or outsourcing of the tasks of a provider-processor operator is dangerous and complicated, that of the validation instance is also dangerous.

The qualification of subcontractors sharing the responsibility of the Validation Body approved to perform the control of traceability mechanisms, or certain traceability mechanisms seems difficult.

Unlike the previous outsourcing which posed a large security problem to preserve the secrecy and the exclusive control of the keys at the level of the users, in the case of the validation instance, the question is to know if a qualified subcontractor for a traceability mechanism (Sequences) can do so knowingly, ie by having in real time the necessary notations and lists.

Is it permissible for a validation subcontractor to know what is the content of the revocation lists or qualification lists?

The precautionary principle prevails in terms of outsourcing

The feasibility of safe sub-contracting under GDPR regulations is low

For signed and encrypted commitments, the risk is high

The dismissal of an employee, the dismissal of an agent or, on the contrary, the full powers and relationships identified constitute personal data whose confidentiality prevents any dissemination otherwise by means of encryption that complicate the exchanges between the authority Validation and its subcontractor.

Likewise, the knowledge of a person's numerical identity notations, and their variation over time, is an indiscretion and a prejudicial fault insofar as this information can be used without the knowledge of that person in policies of credit, segregation, espionage ... and without we have control of the leakage.

Some information in the traceability sheets normally completed by the Operator to activate the key signature or encryption, to prepare the session of consent, to manage an account or to archive originals, are very confidential and cannot be entrusted by the validation body to a third party subsidiary validation without basing the problem of substance on the identification of the leak of information occurred later and in a context where the data is known by two thirds of confidence at a time!

How to outsource when the principle of confidentiality is not to share information?

How to subcontract when the principle of having means of authentication, signature or encryption by a key, in exclusivity, is based on the non-dissemination of keys by the custodian (Processor) to avoid an uncontrollable breach of trust, c that is to say not allowing to reveal between two thirds of confidence holders of the information which made the fault?

We can only be reserved in practice on the use of a blockchain associating a large number of subcontractors or minors as far as it goes against the optimum security and necessary to identify responsibilities.

Qualified Services and Providers have two strong obligations of results which are the secret of business, personal secrecy, and the absolute certainty that the original files and keys remain under the exclusive control of the owners.

In any case, in an all-out outsourcing scheme, particularly in the banks, it will be considered that the systemic risk and good-end risk is too great, and that the bank's responsibility can be engaged on the basis of an error or breach of trust of a minor. or a subcontractor among others.

Nevertheless, this reservation against all-out sub-contracting does not prevent us from looking in a blockchain if there are sequences in which operations or controls do not raise this problem of confidentiality or exclusive possession and allow to reduce treatment costs.

So why so much communication on the public blockchain if such risks exist.

Blockchain disconnected from GDPR and e.IDAS regulations

The answer is partly because of the ignorance of the founders of these different types of blockchain concerning the GDPR Regulations, e, IDAS and NIS.

If we take into account the 93 rules or constraints of these three regulations and that we associate them intelligently to implement them in commercial, financial or industrial management applications, we will see that none of these blockchains are legal and in fact compliance with professional codes of conduct.

In addition, knowledge of advanced online signatures and collaborative, cross-border and multilateral encryption of these people is probably low: they have no experience of the essential workflows to ensure the dematerialization, legal value, security levels in cloud computing, and instant interoperability in digital trust.

Blockchains do away with the separation of responsibilities: controllers, processors and validation bodies by creating a segregation of information and a joint responsibility!

The delegation of treatment in qualified digital trust networks is subject to the possession by the subcontractor of a certificate of personal signature (informed consent) for his sworn employee and of an electronic seal certificate (integrity seal) for its processing server. No minutes of delegated operation or remote delegated validation cannot have a probative legal value without the qualified certificates of this personal signature and this electronic seal, both appearing on a national revocation list.

Another constraint of e.IDAS and GDPR regulations is that qualified certificates for authentication, integrity and timestamps, as well as personal signature certificates used for legal consent, must be domiciled in a "Key Vault". to meet interoperability and judicial mandate requirements in accordance with each national law.

TITLE 1. ANALYSIS OF THE TRACEABILITY AND CERTIFICATION MECHANISMS IN ACCORDANCE WITH THE GDPR REGULATION. ANALYSIS OF ADVANCED ELECTRONIC CACHET AND SIGNATURE CONSTRAINTS IN CLOUD OR USED BY QUALIFIED THIRD PARTIES. CONSEQUENCE ON THE LEGAL MANAGEMENT OF THE BLOCKCHAIN.

Here is a summary example of the sequence of tasks and operations required for the dematerialization, legality and security of a commitment by signature (s) such as the smart contract or the signed payment order by applying the main regulations required:

1. e.IDAS to service trust, signatures, stamps and identification

2. GDPR for Services, Operators, and Supervisory and Validation Bodies

3. EMIR (European Market Infrastructure Regulation)

4. MIFID II (Organising Trading Facilities)

5. FATCA II (Foreign Account Tax Compliance Act)

6. BALE 3 (Liquidity Coverage Ratio, NSFR Net Stable Funding Ratio 2019)

7. RUBIK (bank secrecy)

8. SOLVENCY 2 (ratios MCR & SCR)

9. AIMFD (Alternative Investment Fund Managers Directive)

10. PSD2 Payment

In the example of the treatment of a smart contract or a signed payment order there are 372 tasks in detail that meet regulatory obligations. The traceability mechanisms and the traceability records conveyed in the documentary value chain concern the issuer's trusted service, the recipient's trusted service, the issuer's operator, the recipient's operator, and the service. independent validation. Here in this case, the distribution of tasks in number and percentage.

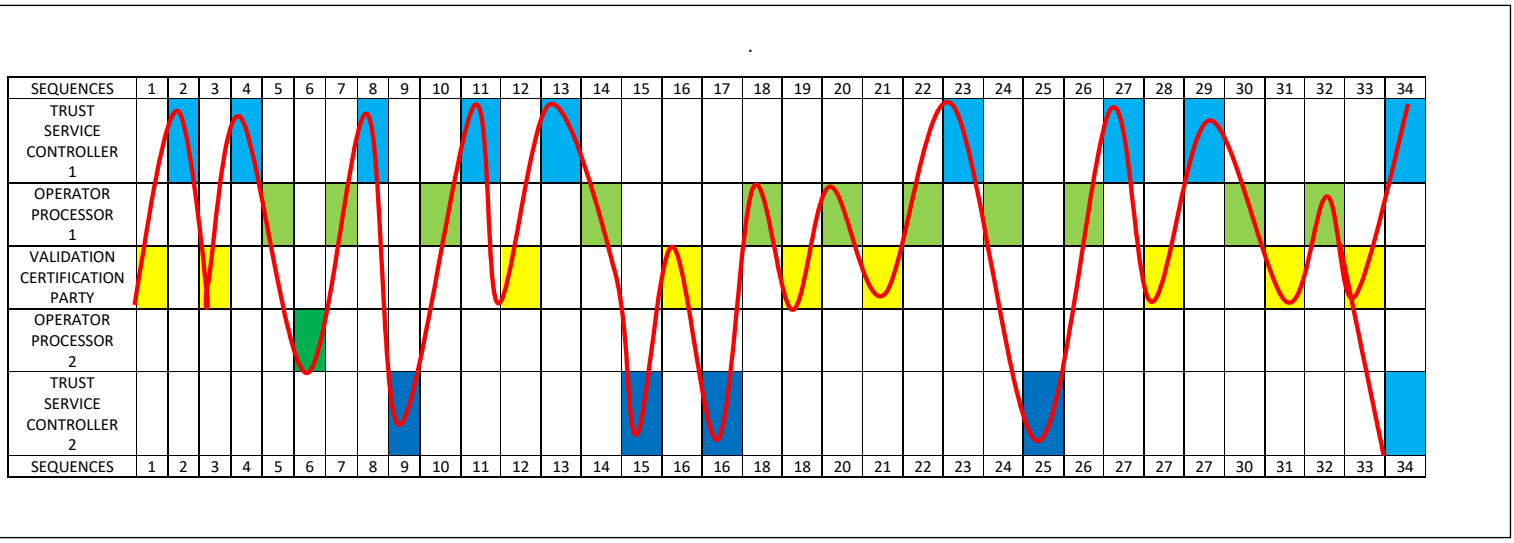
If both parties have the same trust service and the same operator, we will have the second distribution of tasks in number and percentage.

	TASKS	Tags	QTS 1	IVA	OPE1 ISSUER	OPE2 AUXI.	IVA	QTS 2
1	**Mean 1 of Preliminary Session**	10 Tags						
2	**Mean 2 of Portal Selection**	13 tags						
3	**Mean 3 of Initial Authentication in this Portal**	11 tags						
4	**Mean 4 of Selection of a Service**	6 Tags						
5	**Mean 5 Signatory Sender Service Commitment**	4 Tags						
6	**Mean 6 Choice of counterparties**	12 Tags						
7	**Mean 7 Sender & Trust Service TS1 Submission to IVA**	8 Tags						
8	**Mean 8 Documentary Correspondence Disclosure**	5 Tag						
9	**Mean 9 Documentary Files Upload**	10 Tags						
10	**Mean 10 Document PDF & XML Origination**	53 Tags						
11	**Mean 11 BlockChain Multi Operator Processors**	2 Tags						
12	**Mean 12 OPE1 Issuer Advanced Signature creation and prescription**	6 Tags						
13	**Mean 13 Auxiliary Operator Advanced Signature Creation**	7 Tags						
14	**Mean 14 Auxiliary Operator Restitution and OPE1 Administration**	17 Tags						
15	**Mean 15 Multilateral Signatory Notifications**	8 tags						
16	**Mean 16TSP 1 Sender Notification Verification**	4 Tags						
17	**Mean 17TSP 2 Receiver Notification Verification**	4 Tags						
18	**Mean 18 Mechanisms of Traceability Segmentation.**	1 Tags						
19	**Mean 19 Signatory Strong Authentication Sender Signatory**	4 Tags						
20	**Mean 20 IVA ID SIGNATORY SENDER AUTHENTICATION CERTIFICATION**	6 Tags						
21	**Mean 21 SIGNATORY SENDER DISCLOSURE & SCHEDULING (MS)**	2 Tags						
22	**Mean 22 Operator Issuer Sender Signatory Access Authorization Consent Interface**	2 Tags						
23	**Mean 23 Signatory Strong Authentication Receiver Signatory**	3 Tags						
24	**Mean 24 IVA ID SIGNATORY RECEIVER AUTHENTICATION**	6 Tags						
25	**Mean 25 SIGNATORY RECEIVER DISCLOSURE & SCHEDULING (MS)**	6 Tags						
26	**Mean 26 Operator Issuer Receiver Signatory Access Authorization consent Interface**	2 Tags						
27	**Mean 27 Private Keys Controlling Management Sender**	17 Tags						
28	**Mean 28 Private Keys Controlling Management Receiver**	12 Tags						
29	**Mean 29 CONFIDENTIALITY ORIGINEL OF PDF and OF XML**	2 Tags						
30	**Mean 30 Consent of the Signatory Sender**	12 Tags						
31	**Mean 31 IVA Validation Signatory Consent SENDER**	4 Tags						
32	**Mean 32 Consent Receiver Signatory**	13 Tags						

33	**Mean 33 IVA Validation Signatory Consent RECEIVER**	7 Tags						
34	**Mean 34 BLOCKCHAIN CONSO COMPLETENESS CHECK OF LEGAL SIGNATURE CONSENT**	1 Tags						
35	**Mean 35 XML APPLICATION TRANSFER**	4 tag						
36	**Mean 36 Mean of XML Private Data Management Creation SENDER**	2 tag						
37	**Mean 37 DELIVERY SENDER DUPLICATA DOCUMENTARY ACCOUNT ENCRYPTED**	4 Tag						
38	**Mean 38 QTS 1 SENDER Correspondence Account Receipt**	1 tags						
36'	**Mean 36 ' Mean of XML Private Data Management Creation RECEIVER**	1 tag						
37'	**Mean 37 ' DELIVERY RECEIVER DUPLICATA DOCUMENTARY ACCOUNT ENCRYPTED**	2 tag						
38'	**Mean 38 'QTS 2 RECEIVER Correspondence Account Receipt**	1 Tag						
39	**Mean 39 NOTARY BATCH REPORTING**	1 tag						
40	**Mean 40 Sworn Employee Notary Authentication**	4 Tags						
41	**Mean 41 IVA Sworn Employee Notary Strong Authentication Certification**	5 Tags						
42	**Mean 42 QTS Sworn Employee Notary Data Disclosure (MS)**	4 tags						
43	**Mean 43 BATCH REPORTING SEN Sworn Employee Notary SIGNATURE APPROVAL**	28 tags						
44	**Mean 44 IVA SEN Signature Validation**	4 Tags						
45	**Mean 45 SEN Minutes Signature Communication to Correspondence Parties**	8 tag						
46	**Mean 46 Encryption ORA PDF by Adv. Keys protected**	16 tags						
47	**Mean 47 IVA Commitment By Signatures Certification**	1 tag						
48	**Mean 48 TRANSFER ARCHIVING both sides sender and receiver**	6 tags						
		372	57	58	230	7	6	14

In the first table, the division of tasks recorded in the traceability and certification mechanisms considers that each party has its own services and trusted operator.

Qualified Trust Network	Tags Tasks	%
Qualified Trust Service Sender	57	15 %
Qualified Trust Service Receiver	14	4%
OPERATOR Sender Issuer	230	62%
Operator Receiver Auxiliary	7	2%
Validation Party	64	17%



In the second table, the distribution of the tasks recorded in the traceability and certification mechanisms considers that the two signatory parties have the same services and the same trusted operator all qualified by the market authority.

Qualified Trust Network	Tags Tasks	%
Qualified Trust Service only One	71	19 %
OPERATOR Issuer Alone	237	64%
Validation Party	64	17%
Total	372	100%

Processors are effectively bound to secrecy and uniqueness constraints on originals, to constraints of indirect control over the exclusivity of authentication and signature means available to signatories, and to constraints on real-time lists of revocation corresponding to these personal rights.

Processors are also bound by the territoriality rules cited 43 times in the GDPR (Article 4.22) and the very strict transfer rules (15 times cited).

Such a large number of constraints severely limits the possibility of delegating to any subcontractors, and of course this constraint is even more prevalent when subcontractors are domiciled abroad (Main establishment means Article 4.16).

The powers of controllers using foreign outsourcing are very limited (Powers Territoriality Art.58).

In spite of these important reservations, it is conceivable in accordance with the aforementioned articles to use qualified subcontractors or minors with an electronic signature and an electronic seal to deal with the tasks of conformity signatures which are sometimes obligatory for masses considerable amount of transactions.

This is a way to use the blockchain in the overall validation process.

This amounts to decentralizing the function of notary for the application of certain codes of conduct. These are operations that can be done in "batch" after the execution and validation of the parties' signatures, after the transmission of documentary management reports for their immediate information, and before the delivery of the originals in legal archiving.

*This processing phase represents 57 tasks that a total of 372 is **15%** of overall processing that can be allowed in deferred time.*

In conclusion, Governance and Territoriality are two essential parameters of the GDPR and the e.IDAS that limit the scope of the blockchain when it becomes operational and that for companies, the legality and the legal value of their transactions must be insured for their certified "digital balance sheet" and for their tranquility (Penalties of 4% , solidarity).

Governance and Territoriality advocate that the data be domiciled in the national territory and that the keys, many and operationally varied, reside in "Key Vault", absolutely national key supervisors.

In the opposite case, the Nation loses its sovereignty in the digital economy at all levels: execution, protection, jurisdiction, preservation, modification of market operations.
