trustseed

The Challenge of the Digital Economy

Change of architecture of communication networks

THE DIGITAL BANKING SYSTEM

Dc. Eric Blot-Lefevre TrustSeed SAS Ceo.

2019

trustseed

The Challenge of the Digital Economy

Change of architecture of communication networks

An Authority and Digital Market Place legally includes:

1. One or more **"Issuer and Operator"** of Digital Assets:
   Commercial & Financial Instruments including Currencies:
2. One or more "**Depositaries and Intermediaries**" of Digital Assets
3. One or more "**Control and Validation Body**" of Digital Asset".

I. **Digital security provided by a Trinary Architecture**

These three distinct responsibilities together constitute what is called a "Trinary Communication Network" designed in accordance with the GDPR Regulation protecting the security of exchanges between individuals and businesses on line.

This GDPR Regulation institutionalizes:

Art. 24 GDPR **The Processing Manager responsible** for exchanges (Intermediation) and documentary archives (Conservation): Administration of rights and personal management functions (Traceability, Double Part, Matching, Pairing, Hash, Encryption).

Art. 27 GDPR. **The Head of the Emission responsible** for the creation of the Unique and Secret Originals of Financial Instruments and Monetary Currencies, and their combination with advanced digital signatures in cloud computing and qualified by Official Certification Bodies.

Art. 40-41 GDPR **The Validation Manager** responsible for monitoring in real time the Personal Revocation / Rectification Lists to update the individual rights managed by each *Treatment Manager*, and responsible for controlling the Traceability, Interoperability and Compliance Mechanisms (Blockchain) applied by each *Emission Manager* according to the professional codes of conduct applied for each type of transaction (Commerce, Banking, Transport, Health, Food, Energy, Insurance, Administration, Leisure, Education, ...).

II. **Investment in digital knowledge**

To create a "Digital Market Place" qualified by a "National Market Authority" for the digital issuance, intermediation and preservation of dematerialized securities and currencies, it is necessary to make the following investments:

1. Learning the organization of digital markets

2. Adaptation of laws and implementing decrees specifying procedures (users) and sanctions (Court of Justice)

3. Familiarity with international regulations, especially in Europe, where there is clear legal progress for data protection, online signing, network security and resilience.

4. Knowledge of International Treaties regarding Transfer Security with "Control Mechanisms" and "Appropriate Warranties".

5. Knowledge of the evolution of ISO, CEN, ETSI Standards ... and new digital standards such as FIDO, 3DSA, 3DTC ... which are built on the Trinary system (Art. 24, Art.27, Art.40 GDPR).

6. International knowledge of Certified and Trinary-compatible software solutions

7. International knowledge of the Processing Managers, the Subcontracting Managers such as the issuance of digital securities or monetary, and the Validation Managers, able to succeed in their digital transformation to be finally “qualified” by the National Authorities or International Markets, and to be “interoperable” between them (for example: Electronic Certification Service Providers or National Authorities qualified in Signatures, Certification and Validation).

III. The challenge of the digital economy, a global and serious solution

The current regulatory context in the digital transformation will make it possible to ensure a very competitive digital economy that is perfectly suited to the development of artificial intelligence, and more efficient to fight systematically against all forms of corruption.

Double-entry accounting between the documentary accounts and the digital money accounts will be certified "intra-day", that is to say instantly, so as to reconcile commercial and financial flows, offset the transfers (Netting), and improve the control of operational risks (Industry, Commerce, Innovation, Banks, Financial Institutions, State Tax Perception).

The malfunctions will be corrected and sanctioned at the same speed ("Intra Day") in order to reduce the cost and the amount of litigation handled by the Courts.

From this point of view, digital processing is the only way to stop the explosive or exponential rise of offenses and disputes facilitated by the "massification of transactions" and the "mobility of individuals" in the world.

With the strengthening of identification / authentication systems protecting access using three or four verification factors, the internal and external violation rates of data protection and their management functions will be reversed: Instead of 65 % of external aggression, there will be only 35%; on the other hand, the rate of internal aggression, particularly in companies (including Trusted Third Parties), with employee corruption, will reach 65% if the networks maintain their current level of vulnerability (without transfer to a trinary system).

Conclusion

Computer and legal security will be strengthened by States to protect their sovereignty and to develop "international organized markets" that are more protective of the individual, the national or community economy, and the environment.

Progress in security concerns in particular all the deficiencies of identification and authentication, the breach of trust committed by trusted third parties in the disclosure of personal data, the intrusion and the discreet diversion of Industrial Property data, the falsification of original documents, the occult erasure of digital legal evidence, the lack of consent and signature, the lack of encryption and documentary secrecy in collaborative mode, the lack of real-time processing, updating of rights and personal data, as well as the lack of multilateral interoperability.

Unlike traditional material corruption that affects a limited number of operations, corruption in the digital environment can, with a single attacker, generate millions of damages for an astronomical monetary value.

Progress in digital security will also avoid the violation of the Personal Law rules of rectification, erasure, portability and data transfer, and such progress will protect the rights of opposition, revocation, amendment, and the fundamental right to be forgotten.

Without all these security measures, faced with the increasing massification of operations, the investment and control mechanisms in the National Economy are no longer reliable, and the guarantees provided by the Third Party and the State itself are no longer safe, less credible, and more and more expensive.

Central banks are aware of the difficulty and vulnerability of Western economies, where the dynamics of the Couple Investment / Innovations, and the measures of the Quality /Services ratio are poorly controlled, due to lack of knowledge of the prevention, regulation and resilience modes that are essential.

On the other hand, the digitalization of financial instruments and currencies significantly improves their liquidity and their convertibility on the marketplaces on line.

Under these conditions, with mobility of people and capital, individuals and businesses will pay the price to take refuge in States where security is credible for their Digital Assets and Currencies in the medium term.

Le Défi de l'Economie Digitale

Changement d'architecture des réseaux de communication

Le SYSTEME BANCAIRE DIGITAL

Une Autorité et Place de Marché digital comprend légalement :

1. Un ou plusieurs "Émetteurs et Opérateurs" d'Actifs Numériques : Instruments Financiers et Devises/Stocks Monétaires ,
2. Un ou plusieurs "Dépositaires et Intermédiaires d'Actifs Numériques"
3. Une ou plusieurs "Instances de Contrôle et de Validation des Actifs Numériques".

I. La sécurité digitale assurée par une architecture trinaire

Ces trois responsabilités distinctes constituent ensemble ce qu'on appelle un Réseau de Communication Trinaire conçu en conformité avec la Règlementation GDPR protégeant la sécurité des échanges entre les Particuliers et les Entreprises.

Ce Règlement GDPR institutionnalise :

Art. 24 GDPR **Le Responsable du Traitement** chargé des d'échanges (Intermédiation) et des archives documentaires (Conservation) : Administration des droits et des fonctions de gestion personnelles (Traçabilité, Partie Double, Appariement, Adossement, Hash, Cryptage...).

Art. 27 GDPR. **Le Responsable de l'Emission** chargé de la création des Originaux Uniques et Secrets d'Instruments Financiers et de Devises Monétaires, et de leur combinaison avec les signatures digitales avancées en cloud computing et qualifiées par des Organes Officiels de Certification.

Art. 40-41 GDPR **Le Responsable de la Validation** chargé de suivre en temps réel les Listes personnelles de Révocation/Rectification pour actualiser les droits individuels gérés par chaque *Responsable du Traitement*, et chargé de contrôler les Mécanismes de Traçabilité, d'Interopérabilité et de Conformité (Blockchain) appliqués par chaque *Responsable de l'Emission* en fonction des codes de conduite professionnels appliqués pour chaque type de transaction (Commerce, Banque, Transport, Santé, Alimentaire, Energie, Assurances, Administrations, Loisirs, Education, …).

II. L'investissement dans la connaissance digitale

Pour créer une « Place de Marché Digitale » qualifiée par une « Autorité Nationale de Marché » pour l'Emission, l'Intermédiation et la Conservation digitales de valeurs mobilières et monétaires dématérialisées, il est nécessaire de prévoir les investissements suivants :

1. Apprentissage de l'organisation des marchés digitaux
2. Adaptation des lois et décrets d'application précisant les procédures (usagers) et les sanctions (Cour de Justice)
3. Connaissance des Règlementations en vigueur sur le plan international, notamment en Europe où l'avancée juridique est manifeste pour la protection des données, la signature en ligne, la sécurité et la résilience des réseaux.
4. Connaissance des Traitées Internationaux concernant la Sécurité des Transferts avec les « Mécanismes de contrôle » et les « Garanties appropriées ».
5. Connaissance des évolutions de Standards ISO, CEN, ETSI… et des nouveaux standards digitaux tels que FIDO, 3DSA, 3DTC… qui sont bâtis sur le système trinaire (Art. 24,27, 40 GDPR).
6. Connaissance internationale des solutions logicielles certifiées et compatibles avec le système trinaire
7. Connaissance internationale des Responsables du Traitement, des Responsables de la Sous-Traitance telle que l'Emission de valeurs mobilières ou monétaires digitales, et des Responsables de la Validation, capables de réussir leur transformation numérique pour être finalement qualifiés par les Autorités Nationales ou Internationales de Marchés, et pour être interopérable entre eux (Par exemple : les Prestataires de services de certification électronique ou les autorités nationales qualifiées en Signatures, Certification et Validation).

III. L'enjeu de l'économie digitale, une solution globale et sérieuse

Le contexte réglementaire actuel dans la transformation digitale va permettre d'assurer une économie digitale très compétitive et parfaitement appropriée au développement de l'intelligence artificielle, et plus efficace pour lutter systématiquement contre toutes les formes de corruptions.

La comptabilité en partie double entre les comptes documentaires et les comptes monétaires digitaux sera certifiée « intra-day », c'est-à-dire instantanément, de manière à réconcilier les flux commerciaux et financiers, compenser les règlements, et améliorer le contrôle des risques opérationnels (Industrie, Commerce, Innovation, Banques, Etablissements Financiers, Etat Perception Fiscale).

Les disfonctionnements seront corrigés et sanctionnés à la même vitesse (« Dans La Journée ») de manière à réduire le coût et l'encours des litiges traités par les Tribunaux.

De ce point de vue, le traitement digitale est la seule manière d'enrailler la montée fulgurante ou exponentielle des infractions et des litiges facilités par la « massification des transactions » et par la « mobilité des individus » dans le monde.

Avec le renforcement des systèmes d'identification/authentification protégeant les accès en utilisant trois ou quatre facteurs de vérification, les taux de violation interne et externe de la protection des données et de leurs fonctions de gestion, vont s'inverser : Au lieu de 65% d'agression externe, il n'y en aura plus que 35 % ; par contre, le taux d'agression interne, notamment dans les entreprises, avec la corruption des employés, atteindra 65% si les réseaux conservent leur niveau de vulnérabilité actuelle (sans mutation en système trinaire).

Conclusion

La sécurité informatique et juridique sera renforcée par les Etats pour protéger leur Souveraineté et pour développer des « Marchés Organisés Internationaux » davantage protecteurs de l'individu, de l'économie nationale ou communautaire, et de l'environnement.

Les progrès en sécurité concernent notamment toutes les carences d'identification et d'authentification, l'abus de confiance commis par des Tiers de confiance en matière de divulgation des données personnelles, l'intrusion et le détournement discret des données de Propriété Industrielle, la falsification des originaux de documents, l'effacement occulte des preuves légales numériques, le défaut de consentement et de signature, l'absence de cryptage et de secret documentaire en mode collaboratif, l'absence de traitement en temps réel, d'actualisation des droits et des données personnelles, ainsi que l'absence d'interopérabilité multilatérale.

Les progrès procurés par la sécurité digitale éviteront aussi la violation des règles de Droit personnel en matière de rectification, d'effacement, de portabilité et de transfert de données, et ces progrès protégeront les droits d'opposition, de révocation, de modification, et le droit fondamental à l'oubli.

Sans tous ces dispositifs de sécurité, face à la massification croissante des opérations, les mécanismes d'investissement et de contrôle dans l'Economie nationale ne sont plus fiables, et les garanties apportées par les Tiers de Confiance et l'Etat lui-même sont de moins en moins crédibles, et de plus en plus onéreuses.

Les Banques Centrales connaissent la difficulté et la vulnérabilité des économies occidentales dont les ressorts du Couple Investissement/ Innovations, et les mesures du Rapport Qualité/Services sont mal maîtrisés, par méconnaissance des modes de prévention, de régulation et de résilience indispensables.

Dans ces conditions, avec la mobilité les personnes et des capitaux, les particuliers et les entreprises paieront le prix pour se réfugier dans les Etats où la sécurité est crédible à moyen terme.
