DIGITAL BANK BUSINESS MODEL

The future of Banks

Traditional banks are losing their business assets (Services), their market share (Customers) and their financial value (Provision for risk of infringement of digital regulations) because they do not know how to carry out the transformation or digital transmutation in the absence of technology adapted to their operational needs.

In this context of uncertainty, they continue to launch reforms whose costs are prohibitive and the results uncertain (1) Seed article Challenges.

Online banks currently do not earn money because they do not distribute innovative services and their digital exchange networks do not guarantee any legal and IT security to protect their customers and the counterparties of their customers in any business.

In other words, no bank operator and no subcontractor guarantee the legal value of a signed document online.

Now in Cloud Computing, the signatories of a transaction no longer have, among the 20 computer means necessary for the legal certification, only exclusive control of the three legal functions of identification, authentication and consent.

The two Data Protection (GDPR) and e .IDAS Regulations were therefore intended to oblige the “trust services” and the banking operators to assume this obligation of result since in the cloud computing, henceforth no one can administer on their own demonstration of digital evidence without any of the necessary computer facilities and without any authorized access to Data Centers.

The economy in profound change

The economic forecast establishes that within 15 years, the online "Trust Services" will be in contact mainly with Financial Analysis Services, Marketing and Advertising Services (Customer Trust Management) and the Artificial Intelligence Providers. (2) whose turnover in 2030 will be equivalent to the current GDP Gross Domestic Product of Europe (€ 16,500 billion).

The "Trust Services" present in the companies upstream of all these sensitive and outsourced activities, will use subcontractors qualified by industrial, computer and logistical "means" (Signature, Sealed and Encryption) at the same time reliable, agile and " Certified "end-to-end in a blockchain.

The legal and IT security levels of online transactions, the traceability of multilateral and cross-border transactions (Multiple Parties, Services and Operators) and the agility of encryption and adjustment variables (pseudonymisation, rectification, deletion, opposition) will be systematically verified by a validation body under the principle that "***no one can constitute evidence on its own"*** and in accordance with Article 41 of the GDPR Regulation

Prevention against risks, frauds and anomalies, compliance with professional codes of conduct, the interoperability of digital trust networks, and finally the qualitative improvement of finished products, are in this context the 4 main factors of the progress sought in the digital economy by the European Commission with such pioneering regulations (GDPR and e.IDAS).

These factors of progress will finally protect the markets from the catastrophic consequences of several financial crises in cascade (3) whose visible impact still remains today.

Prevention is an obligation

These factors of progress in the digital economy still subject to the many hazards of cloud computing and capital markets, will be protected by the defense and resilience systems imposed in the new regulations of the Trusted Services Networks, as well as by the labeling. (EC) companies and certification of means regarding software applications.

The defense system provides for "disqualification" in the market and heavy fines for infringing companies (4). This deterrence against "organized fraudsters" whose number is increasing rapidly with white-collar crime and migratory waves, should thus put an end to the international phenomenon of digital delinquency that benefits from exponential “mass treatment” to infiltrate operations.

The resilience system consists in subordinating the actions of the "trust services" in the companies (Controllers) and subordinating the operations of the qualified subcontractors (Processors), to the systematic verification in real time of the personal rights (before any commitment : prevention obliges), as well as the control of compliance and legality of the services performed online on behalf of the parties: it looks like “Air Traffic Control” !

These results are conveyed in a blockchain whose validation body carries out the general inspection, issues the certificates of legal value to the signatory parties, and possibly notifies the “trust services” and the “qualified operators” of a change of procedure if an anomaly or a malfunction has been detected.

Deterrence against "organized fraudsters"

The digital economy is much more effective than the real economy in prosecuting mass organized crime and violating professional codes of conduct.

The Data Protection Regulation already demonstrates its effectiveness in the implementation of heavy cross-border sanctions by punishing online market transactions that are unfair (illegal services), illegal (lack of traceability) or infringement vis-à-vis a code of professional conduct (Failure of security or probative value).

Penalties (4% of turnover) and temporary or permanent withdrawals of the right of exploitation (Disqualification) in an organized online market directly challenge managers, shareholders and subcontractors who are jointly and severally liable with company pursued. The collapse of Facebook's share price reveals the effectiveness of the digital regulatory arsenal in force today.

The digital bank arbiter of digital trust

Compared to this historic challenge, the digital bank is finally positioned as the protector of businesses and individuals if it knows how to ensure legal and IT security through its own network of digital trust.

It is neither more nor less a return to the original profession of the bank which originally guaranteed a space of confidence in the relations, the exchanges, the deposit and the secrecy of the data and the signed documents.

The digital bank provider of a reliable and universal digital solution

For companies in Europe, ie 200,000 large companies with more than 250 employees, and 24 million medium or small size, their protection and regulatory compliance (Data Protection 24 May 2018) resolved by the intermediary Qualified Trust Network of a "digital bank", this is a bargain.

This means an economy for companies that exceeds 85% of the expected costs for their digital transformation ($ 30M for a large company, see 5).

It also provides them with a global and indispensable solution for the compulsory certification of digital accounting documents (240 billion digital documents in Europe to be certified in an annual digital balance sheet Source SSEDIC -DG Connect European Commission).

This generic protection and compliance solution adapted to each company contributes to reducing the management and accounting documentary costs by 70% by finally providing qualified employees with the agile means of managing the documentary and monetary secret.

The company thus manages to build its own networks of trust, validation and revocation to manage respectively in real time its counterparties, its transactions (Assets & Liabilities) and its powers or proxies of electronic signatures (Employees).

The official qualification of the "trust services" of the company and the adhesion facilitated to the counterparties in the network of trust of the digital bank, avoids to the company the loss of the Internet traffic caused by the current movement of defiance; and this voluntary membership of counterparties opens up significant prospects for the sustainable acquisition of market shares.

For individuals, it is a restoration of trust vis-à-vis companies that comply officially (Label CE) GDPR Regulations (Data Protection Privacy) and e.IDAS (Signatures).

This trust is based on tangible elements since the companies labeled thanks to the trust network of the digital bank, respect the obligations of results which are imposed on them by the new legislation, and in particular by knowing how to administer at the request of each party "the digital proof "relating to the validity of the rights of each person and relating to the conformity of the operations carried out on his behalf.

Digital Bank Solves Critical Global Social Problem

A digital bank that offers large companies with an Internet portal the benefits of its “Digital Trust Network" will be very successful.

In fact, the "digital bank" enables companies to save most of their digital transformation load, reduce the annual document management budget, maintain long-term compliance with internal procedures and increase their Internet market shares without risk of penalty or temporary or permanent exclusion.

In addition, the official qualification of all commercial and financial data by nature of transactions or letters, allows the company to keep control of the ownership of its data, and to pseudonymize them, in all acts of communication organized with Big Data and Artificial Intelligence services.

The lucrative concession of these data, compulsorily qualified according to each purpose, does not expose the company (especially in intermediation) to the risk of a penalty for which it could be held jointly and severally liable for services designated for their external exploitation.

Each company can dynamically create its own digital networks with business secrecy

The fact that the company belongs to the trusted network of the "digital bank" enables it to create its own private network of digital trust with any counterpart, company or individual, by setting its conditions of exchange and management of the documentary secret.

In the bid of several counterparties, the trading conditions of the qualified company will prevail over the others, in other words, each counterparty must be part of the trusted network of the digital bank to be insured.

The digital bank will anticipate in its digital trust network the organization of a wide range of financial service providers and marketing services whose procedures are already in full compliance with the accounting, legal and monetary regulations as well as with each professional code of conduct (Health, Food Distribution, Transport, Insurance, Retirement, ...).

The technology behind the digital banking project

Digital Banking needs to build its network of digital trust qualified for businesses and for individuals from three IT solutions.

The first solution called "Trusted Services" is installed in the company to connect to an operator who is the only qualified manager in the implementation of letters, transactions or contracts, with its “certified” software means of creation, encryption and communication regarding digital originals of documents and including personal, mutual or reciprocal signatures.

The second so-called "Operator" solution as already indicated uses software means with blockchain traceability mechanisms embedded and controlled by a Validation Body responsible for the application of the digital code of conduct vis-à- vis its National Market Authority.

The third solution ensures in real time for the legal validation of the commitments by signatures, on the one hand, the instantaneous verification of the rights of the signatory parties revocable at any time, and on the other hand, the control of the conformity of the documentary operations subject to the criteria defined for each type or model of exchange, subject to the special conditions between the Parties, and subject to the rules prescribed in the code of professional conduct.

These three technologies are now operating in a generic platform that can be adapted to the digital banking project.

The business model is disruptive

The opening by the company of the documentary and monetary accounts managed in the digital bank is carried out according to a subscription calculated on the average outstanding of documentary and monetary flows secured and certified each year.

The certification of the digital balance sheet and the documentary secret managed in collaborative mode costs around € 1 per document (instead of the current full cost of more than € 3.5). This cost is easily comparable to that of competitors who offer a service at € 2.5 for a degraded service of 60-80% (6). For individuals, only the registered / signed email, the signed contract and the digital registered letter are invoiced.

A model of pervasive growth

The digital bank can already count in Europe on the processing of 240 billion accounting documents to be certified for the digital balance sheet, which the Auditors will henceforth have to enforce the obligations of the GDPR and e.IDAS regulations for online signatures.

To this estimate, we can add all the transactions between Europe and the rest of the world, especially those made with North America and with China, or 25 billion documents.

The digital bank is pervasive because each company by expanding its network of trust to a partner, allows it to take advantage of it by inviting with its address book all its counterparts to join this network agile, qualified and efficient.

The internationalization of digital exchanges between European companies and those of other continents will quickly increase the reputation of this professional network in full compliance with the regulation of digital markets and social networks.

A patent of "Crypto-Asset Issuance"

The Digital Trust Network of the digital bank creates Crypto-Assets, Crypto-Securities and Crypto-Money, "on demand", in compliance with the regulations (Unicity, Sealing, Signature, Encryption, Blockchain, Probative Value Validation) and by applying the authorization procedures obtained by the Issuers (companies) to the National Market Authorities.

The best profitability in the field of Cyber Security

The distributed profit (EBITDA) of this activity protected by a barrier of 180 patents is greater than 40% of the turnover in the first years, a rate of return much higher than the Euronext margins of which we were founder in 1992 with André Serre (Sicovam).

The European Commission has estimated that the activity of qualified digital trust networks, ie compliant with the GDPR and e.IDAS Regulations, would save Europe € 700 billion a year. The digital bank thus defined has every chance of succeeding.

On an average PER of 20 with an EBITDA equal to 38% of the turnover, the incoming shareholders will still be the customers of the digital bank because they know their strengths.

In the end, the digital bank thanks to its network of qualified trust and the interoperability that it provides to individuals and companies, between all sectors of digital markets, perfectly masters all internal and external operating constraints relating to personal data and their purpose.

Agile digital bank in the intermediation of qualified personal data

For this reason, the external exploitation of personal data being subject to very strong regulations, the digital bank will pioneer in the preparation of data intended for external treatments (Marketing, Public Relations, Artificial Intelligence, Statistics, Elections, Rating -Scoring).

Indeed, thanks to the qualities of its Qualified Trust Network, the digital bank is the only one able to control in real time in its digital trust network all the functions of minimizing data, limiting operations, finalizing services, transfer of ownership, portability of outstanding, secure double encryption, as well as all the adjustment variables for the pseudonymisation-the rectification -the erasure- and opposition, from which the externalization of personal data, with the " "strong and informed consent" of the holder, is actually possible ***if taking into account each specific final destination*** agreed with listed beneficiaries, that is to say the "qualified" providers in Marketing, Big Data or Artificial Intelligence.

The "digital bank" will therefore be in a privileged position to administer the targeted management of this personal data by preparing its customers lawful contracts with the best specialists in Big Data, Marketing and Artificial Intelligence.

As a qualified administrator of these personal data to ensure the long-term protection and to preserve all the finalities, vis-à-vis their customers, the digital bank will have a particular responsibility and for this activity a second source considerable income.

The digital bank at the heart of the digital economy

The digital bank in this context of real-time control of the personal data possibly accessible by rogatory commission (Public Law) or by judicial warrant (Ministry of Justice) will also interest the administrations responsible for cyber security of the national territory (Cyber Crime, Defense National) who must, as such, arbitrate between Private Law and Public Law, while respecting human rights (digital version). To say otherwise is to invalidate the digital banking project.

In this respect, the indicated blockchain which articulates the "trust services" and the "service operators" with the "validation authorities" has a very fine granulometry in the blocks and an infallible security system (Signature, Sealing, Double Encryption, Random Key Sets) that provide a very fine-grained control over the information disclosure process by giving the Judge or Decision-maker some latitude in the spectrum of investigation of the data so as to avoid any excess or abuse of uncontrollable disclosure, which is not the case of the public blockchain that reveals everything without any precaution or intelligence. There are about 350 pieces of information and 50 protected blocks in the blockchain for each digital transaction, which ensures a very high level of exclusive control of trust attributes, identity privacy and intellectual property.

The digital bank at the heart of developments in the blockchain

The digital bank chooses a blockchain, a strategic option, achieving three types of interoperability to avoid any financial or criminal risk.

1. Legal interoperability which consists in respecting the separation between the holders of the identities and attributes of trust (Services), the qualified service providers for the operations (originals, signatures, encryption), and the validation bodies (validation of the rights / Lists of revocation -Conformity / Codes of Conduct) following the principle of "no one can constitute evidence on its own" and following article 41 GDPR.

2. Community interoperability, which consists in respecting between the sectors of activity their codes of conduct with their mutual conventions.

3. Cross-border interoperability which consists in applying to the nationals of each country the national regimes of tax residence, signatures, encryption and documentary secrecy.

The digital bank takes into account in the definition of its blockchain three key factors of security, legality and control of the risks, essential for the States and the resilience of their marketplaces.

1. The first factor is to protect the "trust service" of the enterprise, which is jointly responsible for the fault of its subcontractors. The trust service established in the company whose digital bank provides the IT solution in its Qualified Network, takes responsibility for the SLA Service Leverage Agreement with respect to its counterparties, and as such, it defines strictly the obligations and responsibilities of the operators and the validation bodies in such a way that there is no ambiguity in the traceability mechanisms and in the investigation of a fault for which they would be held jointly and severally liable vis-à-vis the national market authority.

2. The second factor is to organize the millions of signature, seal and encryption keys that must absolutely and permanently (N years) remain under the exclusive control of users, which presupposes a restrictive constituency and manipulation of the keys inspected at all moment to verify their protection and exclusive possession.

3. The third factor :the manifestation of strong and informed consent is another requirement that assumes that each signatory can obtain disclosure of a document (PDF image) and proof of the integrity of its signature and those of others, without any of the providers is not aware of this information or the control of these private or secret means. The mechanisms of the blockchain must provide the permanent demonstration for the validity of the commitments by signatures that all these processes of disclosure reserved to the signatories are circumscribed in secure spaces under the responsibility of the subcontractor operators, under the supervision of the validation bodies, and for the exclusive use of the company (SLA) and its counterparties.

Such constraints give the blockchain a very special configuration that is neither a "Public Permisionless Blockchain" nor a "Private Permissioned Blockchain" (Proof of Stake) but rather a Meta Private BlockChain (Proof of Trust).

In any case, it is hard to imagine in these conditions to entrust (in an SLA) the complexity of digital trust tasks (or coverage of security risks, legality and interoperability) to "Minors", to index the management price on the price of their currency (volatility) and take the "risk of good end" on a minor, or the "systemic risk" on several minors for many reasons in violation of GDPR Regulations, E. IDAS and NIS.

The digital bank arises as an alternative to all organizational schemes that do not cover the systemic risk of digital transactions, nor the monetary risk of their processing (€ 240 billion in Europe) in order to simplify once and for all, as demanded States, and transparently, exchanges between individuals and businesses: new digital social networks.

Eric Blot-Lefevre

TRUSTCORP Lux.

(1) (1) https://www.challenges.fr/entreprise/rgpd-le-cout-faramineux-de-protection-des-donnees-personnelles-pour-les-entreprises_580413.

(2) PWC estimates that the turnover of artificial intelligence will exceed 16,000 billion € in 2030, a figure that we compare to the European Gross Domestic Product which is currently 16,500 billion €.

(3) The last crisis of 2008 which caused the collapse of GDP reaching 18.000 billion euros in 2007, is still not absorbed since the level was at 12.000 billion euros in 2008 and it caps at 16.000 billion in 2017.

(4) Penalties paid by banks, social networks, integrators, software companies increased by more than 100% in 2017 totaling more than 50 billion dollars. With the GDPR regulation put into effect on May 24, 2018, experts estimate that the penalties will exceed 200 billion in 2020 and that the financial consequences of disqualification will affect the stock market price or the market capitalization of several hundred billion dollars.

The latest sanctions were in 2017: Bank ($ 15bn), Automotive ($ 35bn), Computer Networks ($ 20bn) in net growth.

Banque Digitale : Business Model

L'Avenir des banques

Les banques traditionnelles perdent actuellement leur fonds de commerce (Services), leur part de marché (Clients) et leur valeur financière (Défaut de qualification règlementaire pénalisant dans le domaine digital) parce qu'elles ne savent pas comment réaliser la transformation ou la transmutation digitale en absence de technologie adaptée à leurs besoins opérationnels ; et dans ce contexte d'incertitude, elles continuent de lancer des réformes dont les coûts sont prohibitifs et les résultats incertains (1).Coût faramineux selon l'article Challenges .

Les banques en ligne actuellement ne gagnent pas d'argent car elles ne distribuent pas de services innovants et leurs réseaux d'échanges numériques ne sont garants d'aucune sécurité juridique et informatique pour protéger leurs clients et les contreparties de leurs clients !

En d'autres termes, aucune banque et aucun opérateur sous-traitant ne garantissent la valeur juridique d'un document signé en cloud computing alors que les signataires ne disposent plus parmi les 20 moyens informatiques nécessaires pour la mise en œuvre que du seul contrôle exclusif de leurs trois fonctions d'identification/authentification et consentement. Les deux règlements Data Protection (GDPR) et e .IDAS avaient donc pour but d'obliger les services de confiance et les opérateurs bancaires à assumer cette obligation de résultat puisqu'en cloud computing, dorénavant plus personne ne peut administrer par soi-même cette démonstration de la preuve numérique sans aucun des moyens informatiques nécessaires et sans aucun accès autorisé aux Data Centers.

L'économie en profonde mutation

La prospective économique établit que d'ici 15 ans, les «Services de Confiance » en ligne seront en relation principalement avec les services d'Analyse Financière, les Services de Marketing et de Publicité (Customer Trust Management) et les Prestataires d'Intelligence artificielle (2) dont le chiffre d'affaires en 2030 sera équivalent au Produit Intérieur Brut actuel de l'Europe (16.500 Milliards €).

Les "Trust Services" présents dans les entreprises en amont de toutes ces activités sensibles et externalisées, utiliseront des sous-traitants qualifiés par des "moyens" industriels, informatiques et logistiques (Signature, Scellé et Chiffrement) à la fois fiables, agiles et "certifiés" de bout en bout dans une blockchain. Les niveaux de sécurité juridique et informatique des transactions en ligne, la traçabilité des opérations multilatérales et transfrontalières (Multiples Parties, Services et Opérateurs) et l'agilité du cryptage et des variables d'ajustement (pseudonymisation, rectification, effacement, opposition) seront systématiquement vérifiés par un organe de validation en vertu du principe que "Nul ne peut se constituer une preuve à lui-même" et en conformité avec l' article 41 du Règlement GDPR.

La prévention vis-à-vis des risques, des fraudes et des anomalies, l'obéissance aux codes de conduite professionnels, l'interopérabilité des réseaux de confiance numérique, et enfin l'amélioration qualitative des produits finis, sont dans ce contexte les 4 principaux facteurs du progrès recherché dans l'économie digitale par la Commission Européenne avec des Règlements aussi précurseurs (GDPR et e.IDAS). Ces facteurs de progrès protègeront enfin les marchés des conséquences catastrophiques de plusieurs crises financières en cascade (3) dont l'impact visible subsiste encore de nos jours.

La prévention est une obligation

Ces facteurs de progrès dans l'économie digitale encore soumise aux nombreux aléas du cloud computing et des marchés de capitaux, seront protégés par les systèmes de défense et de résilience imposés dans la nouvelle règlementation des Réseaux de Services de Confiance, ainsi que par la labellisation (CE) des entreprises et la certification des moyens d'évaluation des logiciels nécessaires.

Le système de défense prévoit la «disqualification» dans le marché et de lourdes amendes à l'encontre des entreprises contrevenantes (4). Cette dissuasion contre les «fraudeurs organisés» dont le nombre augmente rapidement avec la criminalité en col blanc et les vagues migratoires, devrait ainsi mettre fin au phénomène international de la délinquance numérique qui profite des traitements de masse exponentiel pour s'infiltrer dans les opérations.

Le système de résilience consiste à subordonner les actions des « services de confiance » dans les entreprises (Controllers), et à subordonner les opérations des sous-traitants qualifiés (Processors), à la vérification systématique en temps réel des droits personnels (avant tout engagement : prévention oblige), ainsi qu'au contrôle de conformité et de légalité des prestations réalisées en ligne pour le compte des parties. Cela ressemble à la sécurité du système « Air Traffic Control » !

Ces résultats sont véhiculés dans une blockchain dont l'instance de validation fait l'inspection générale , délivre les certificats de valeur juridique aux parties signataires, et notifie éventuellement aux services de confiance et aux opérateurs qualifiés un changement de procédure si une anomalie ou un dysfonctionnement a été détecté.

La dissuasion à l'encontre des « fraudeurs organisés »

L'économie digitale se révèle beaucoup plus efficace que l'économie réelle dans la poursuite des infractions organisées en masse et en violation des codes de conduite professionnels. Le Règlement de la Data Protection démontre déjà son efficacité dans la mise en œuvre de lourdes sanctions transfrontalières en punissant les opérations de marché réalisées en ligne qui sont déloyales (services illicites), illégales (défaut de traçabilité) ou en infraction vis-à-vis d'un code de conduite professionnel (Défaut de sécurité ou de valeur probante).

Les pénalités (4% du Chiffre d'affaires) et les retraits temporaires ou définitifs du droit d'exploitation (Disqualification) sur un marché organisé en ligne interpellent directement les dirigeants, les actionnaires et les prestataires sous-traitants qui sont solidairement responsables avec l'entreprise poursuivie. L'effondrement du cours boursier de Facebook révèle l'efficacité de l'arsenal règlementaire digital en vigueur de nos jours.

La banque digitale arbitre de la confiance numérique

Par rapport à ce défi historique, la banque digitale se positionne enfin comme le protecteur des entreprises et des particuliers si elle sait garantir la sécurité juridique et informatique par l'intermédiaire de son propre réseau de confiance numérique.

C'est ni plus ni moins un retour au métier d'origine de la banque qui garantissait à l'origine un espace de confiance dans les relations, les échanges, le dépôt et le secret des données et des documents signés.

La banque digitale apporteur d'une solution digitale fiable et universelle

Pour les entreprises en Europe, c'est-à-dire 200.000 grandes sociétés ayant plus de 250 employés, et 24 millions de taille moyenne ou petite, leur protection et leur mise en conformité règlementaire (Data Protection 24 Mai 2018) résolues par l'intermédiaire du Réseau de Confiance Qualifié d'une « banque digitale », c'est une aubaine.

Cela signifie une économie pour les entreprises supérieure à 85% des charges prévues pour leur transformation digitale (30M $ pour une grande entreprise, cf. 5).

Cela leur apporte en plus une solution globale et indispensable pour la certification obligatoire des documents comptables digitaux (240 milliards de documents digitaux en Europe à certifier dans un bilan digital annuel. Source SSEDIC -DG Connect Commission Européenne).

Cette solution générique de protection et de mise en conformité adaptée à chaque entreprise contribue à faire baisser de 70% le coût documentaire de gestion et de comptabilité en procurant enfin aux employés qualifiés les moyens agiles de gestion du secret documentaire et monétaire.

L'entreprise parvient ainsi à construire ses propres réseaux de confiance, de validation et de révocation pour gérer respectivement en temps réel ses contreparties, ses transactions et ses pouvoirs ou procurations de signatures électroniques (Employés).

La qualification officielle des « services de confiance » de l'entreprise et l'adhésion facilitée aux contreparties dans le réseau de confiance de la banque digitale, évite à l'entreprise la perte du trafic Internet causée par le mouvement actuel de défiance ; et cette adhésion volontaire des contreparties ouvre des perspectives importantes d'acquisition durable de parts de marché.

Pour les particuliers, c'est une restauration de la confiance vis-à-vis des seules entreprises qui se conforment officiellement (Label CE) aux Règlements GDPR (Data Protection Privacy) et e.IDAS (Signatures). Cette confiance repose sur des éléments tangibles puisque les entreprises labellisées grâce au réseau de confiance de la banque digitale, respectent les obligations de résultats imposées par la nouvelle législation , en sachant administrer à la demande de chaque partie « la preuve numérique » relative aux droits personnels et relative à la conformité des opérations réalisées pour son compte.

La Banque digitale résout un problème crucial de société sur le plan mondial

Une banque digitale qui offre aux grandes entreprises équipées d'un portail Internet les bénéfices de « son Réseau de Confiance Digital » aura beaucoup de succès.

En effet la « banque digitale » permet aux entreprises d'économiser la majeure partie de leur charge de transformation digitale, de diminuer le budget annuel de gestion documentaire, de maintenir durablement la conformité des procédures internes et d'agrandir leurs parts de marché Internet sans risque de pénalité ou d'exclusion temporaire ou définitive.

Par ailleurs, la qualification officielle de toutes les données commerciales et financières par natures de transactions ou de courriers, permet à l'entreprise de garder le contrôle de la propriété de ses données, et de les pseudonymiser, dans tous les actes de communication organisés avec des services de Big Data et d'Intelligence artificielle.

La concession lucrative de ces données obligatoirement qualifiées en fonction de chaque finalité, n'expose pas l'entreprise au risque de pénalité dont elle pourrait être tenue solidairement responsable à côté de services désignés pour leur exploitation externe .

Chaque Entreprise peut créer dynamiquement ses propres réseaux digitaux avec le secret des affaires

L'appartenance de l'entreprise au réseau de confiance de la « banque digitale » lui permet de créer son propre réseau privé de confiance numérique avec toute contrepartie, entreprise ou particulier, en fixant ses conditions d'échanges et de gestion du secret documentaire.

Dans la mise en concurrence des offres de plusieurs contreparties, les conditions d'échanges de l'entreprise qualifiée prévaudront sur les autres, autrement dit, chaque contrepartie devra s'inscrire dans le réseau de confiance de la banque digitale pour être assurée.

La banque digitale anticipera dans son réseau de confiance digitale l'organisation d'un vaste éventail de fournisseurs de services financiers et de services marketing dont les procédures sont déjà en parfaite conformité avec la règlementation comptable, juridique et monétaire ainsi qu'avec chaque code de conduite professionnel en vigueur (Santé, Distribution Alimentaire, Transport, Assurances, Retraites, …).

La technologie sous-jacente au projet de banque digitale

La Banque digitale a besoin pour constituer son réseau de confiance numérique qualifié pour les entreprises et pour les particuliers de trois solutions informatiques.

La première solution qualifiée de « Services de confiance » est installée dans l'entreprise pour se connecter à un opérateur qui est le seul responsable qualifié dans la mise en œuvre des courriers, transactions ou contrats, avec ses moyens certifiés de création, cryptage et communication des originaux digitaux de documents et de signatures personnelles, mutuelles ou réciproques.

La seconde solution qualifiée d' « Opérateur » dispose des moyens logiciels déjà indiqués avec des mécanismes de traçabilité fonctionnant dans une blockchain privée qui est sous le contrôle d'une Instance de validation responsable de l'application du code de conduite digital vis-à-vis de son Autorité Nationale de Marché.

La troisième solution assure en temps réel pour la validation juridique des engagements par signatures, d'une part, la vérification instantanée des droits des parties signataires révocables à tout moment, et d'autre part, le contrôle de la conformité des opérations documentaires assujetties aux critères définis pour chaque type ou modèle d'échange, assujetties aux conditions particulières entre les Parties, et assujetties aux règles prescrites dans le code de conduite professionnel.

Ces trois technologies fonctionnent aujourd'hui dans une plateforme générique qu'il suffit d'adapter au projet de banque digitale.

Le business model est disruptif

L'ouverture par l'entreprise des comptes documentaire et monétaire gérés dans la banque digitale est effectuée en fonction d'un abonnement calculé sur l'encours moyen des flux documentaires et monétaires sécurisés et certifiés chaque année. La certification du bilan digital et le secret documentaire géré en mode collaboratif coûte environ 1€ par document (au lieu du coût complet actuel supérieur à 3,5 €). Ce coût se compare facilement à celui des concurrents qui proposent un service à 2,5 € pour une prestation dégradée de 60-80% (6). Pour les particuliers, seuls l'email enregistré /signé, le contrat signé et la lettre recommandée digitale sont facturés.

Un modèle de croissance pervasif

La banque digitale peut déjà tabler en Europe sur le traitement de 240 Milliards de documents comptables à certifier pour le bilan digital dont les Auditeurs devront dorénavant faire respecter les obligations des règlements GDPR et e.IDAS pour les signatures en ligne.

A cette estimation, on peut rajouter toutes les transactions entre l'Europe et le reste du monde, notamment celles réalisées avec l'Amérique du Nord et avec la Chine, soit 25 milliards de documents.

La banque digitale est pervasive car chaque entreprise en élargissant son réseau de confiance à un partenaire, permet à celui-ci d'en profiter en invitant avec son carnet d'adresses toutes ses contreparties à rejoindre ce réseau agile, qualifié et performant.

L'internationalisation des échanges digitaux entre les entreprises européennes et celles des autres Continents va rapidement élargir la notoriété de ce réseau professionnel en parfaite conformité avec la règlementation des marchés digitaux et des réseaux socio-professionnels.

Un brevet de « Crypto-Asset Issuance »

Le Réseau de Confiance Numérique de la banque digitale crée dans ces conditions sans aucune difficulté des crypto-Assets, crypto-Securities et crypto-Money, « on demand », en se conformant à la règlementation (Unicité, Scellement, Signature, Cryptage, Blockchain et Validation) et en appliquant les modalités des autorisations obtenues par les Emetteurs (entreprises) auprès des Autorités Nationales de Marchés .

La meilleure rentabilité dans le domaine de la Cyber Sécurité

Le résultat distribué (EBITDA) de cette activité protégée par une barrière de 180 brevets est supérieure à 40% du chiffre d'affaires dans les premières années, taux de rendement nettement supérieur aux marges d'Euronext dont nous étions fondateurs en 1992 avec André Serre (Sicovam).

La Commission Européenne a estimé que l'activité des réseaux de confiance numérique qualifiés, c'est-à-dire conformes aux Règlements GDPR et e.IDAS, ferait économiser à l'Europe 700 Milliards € par an. La Banque digitale ainsi définie a donc toutes les chances de réussir.

Sur un PER moyen de 20 avec un EBITDA égal à 38% du chiffre d'affaires, les actionnaires entrants seront encore les clients de la banque digitale car ils en connaissent les forces.

En fin de compte, la banque digitale grâce à son réseau de confiance qualifié et grâce à l'interopérabilité qu'elle procure aux particuliers et aux entreprises, entre tous les secteurs de marchés digitaux, maîtrise parfaitement toutes les contraintes d'exploitation internes et externes relatives aux données personnelles et relatives à leur finalité.

Banque digitale agile dans l'intermédiation des données personnelles qualifiées

Pour cette raison, l'exploitation externe des données personnelles étant soumise à une réglementation très forte, la banque digitale sera pionnière dans la préparation des données destinées à des traitements extérieurs (Marketing, Relations Publiques, Intelligence artificielle, Statistiques, Elections, Notations, Rating-Scoring).

En effet, grâce aux qualités de son Réseau de Confiance Qualifié, la banque digitale est la seule à savoir contrôler en temps réel dans son réseau de confiance digital toutes les fonctions de minimisation des données ,de limitation des opérations, de finalisation des services, de transfert de propriété, de portabilité des encours, de double cryptage sécurisé, ainsi que toutes les variables d'ajustement pour la pseudonymisation-la rectification -l'effacement- et l'opposition, à partir desquelles la transmission des données personnelles, avec le « consentement fort et éclairé » du titulaire, est réellement possible et préparée en tenant compte uniquement de la destination finale prescrite par les bénéficiaires, c'est-à-dire les prestataires « qualifiés » en matière de Marketing, Big Data ou Intelligence artificielle.

La « banque digitale » sera donc dans une situation privilégiée pour administrer la gestion ciblée de ces données personnelles en préparant à ses clients des contrats licites avec les meilleurs Spécialistes de Big data, de Marketing et d'Intelligence artificielle.

En tant qu'administrateur qualifié de ces données personnelles pour en assurer la protection durable et pour en préserver toutes les finalités, vis-à-vis de leurs clients -titulaires, la banque digitale aura donc une responsabilité particulière et pour cette activité une seconde source de revenu considérable.

La banque digitale au cœur de l'économie digitale

La banque digitale dans ce contexte de maitrise en temps réel des données personnelles éventuellement accessibles par commission rogatoire (Droit Public) ou par mandat judiciaire (Ministère de la Justice) intéressera également les administrations responsables de la cyber sécurité du territoire national (Cyber Criminalité, Défense Nationale) qui doivent, à ce titre, arbitrer entre le droit privé et le droit public en respectant les Droits de l'Homme (version digitale).

A cet égard, la blockchain indiquée qui articule les « services de confiance » et les « opérateurs de services » avec les « instances de validation » dispose d'une granulométrie très fine dans les blocs et d'un système de sécurité infaillible (Signature, Scellement, Double cryptage, Jeux de Clés) qui permettent de contrôler très finement le processus de divulgation de l'information en donnant une certaine latitude au Juge ou au décideurs dans le spectre d'investigation de manière à éviter tout excès ou tout abus de divulgation non contrôlable , ce qui n'est pas le cas de la blockchain publique qui dévoile tout sans aucune précaution ni intelligence.

La blockchain de la banque digitale comprend en moyenne 50 blocs et 350 informations réparties qui peuvent être décryptées par séquence dans chaque bloc.

La banque digitale au cœur de la définition de la nouvelle blockchain des marchés

La banque digitale choisit une blockchain, une option stratégique, réalisant trois types d'interopérabilité pour éviter tout risque financier ou pénal.

L'interopérabilité légale qui consiste à respecter la séparation entre les détenteurs des identités et attributs de confiance (Services), les prestataires qualifiés pour les opérations (originaux, signatures, cryptage), et les organes de validation (validation des droits/Listes de révocation-Conformité/Codes de conduite) suivant ainsi le principe "no one can constitute evidence on its own" et suivant l'article 41 GDPR.

L'interopérabilité communautaire qui consiste à respecter entre les secteurs d'activité leurs codes de conduite avec leurs conventions mutuelles.

L'interopérabilité transfrontalière qui consiste à appliquer aux ressortissants de chaque pays les régimes nationaux de domiciliation fiscale, de signatures, de cryptage et de secret documentaire. Cette qualité permettra de faire fonctionner tous les systèmes de cash management.

La banque digitale prend en compte dans la définition de sa blockchain trois facteurs clés de sécurité, de légalité et de contrôle des risques, mesures indispensables pour les Etats et pour la résilience de leurs places de marchés.

Le premier facteur consiste à protéger le "service de confiance" de l'entreprise qui est solidairement responsable de la faute de ses 'sous-traitants.

Le service de confiance établi dans l'entreprise dont la banque digitale assure la solution informatique dans son Réseau Qualifié, prend la responsabilité du contrat de service (SLA Service Leverage Agreement) vis à vis de ses contreparties, et à ce titre, il définit strictement les obligations et les responsabilités des opérateurs et des organes de validation de manière à ce qu'il n'y ait aucune ambigüité dans les mécanismes de traçabilité et dans les recherches d'une faute pour laquelle ils seraient tenus solidairement responsables vis à vis de l'autorité nationale de marché.

Le second facteur consiste à organiser les millions de clés de signatures, de scellement et de cryptage qui doivent absolument et durablement (N années) rester sous le contrôle exclusif des utilisateurs, ce qui suppose une circonscription et une manipulation restrictives des clés inspectées à tout moment pour vérifier leur protection et leur détention exclusive.

Le troisième facteur : la manifestation du consentement fort et éclairé est une autre obligation qui suppose que chaque signataire puisse obtenir la divulgation d'un document (image PDF) et la preuve de l'intégrité de sa signature et de celles des autres, sans qu'aucun des prestataires n'ait connaissance de ces informations ni le contrôle de ces moyens privés ou secrets.

Les mécanismes de la blockchain doivent apporter la démonstration permanente pour la validité des engagements par signatures que tous ces processus de divulgation réservés aux signataires sont circonscrits dans des espaces sécurisés sous la responsabilité des opérateurs sous-traitants, sous la surveillance des organes de validation, et pour l'usage exclusif de l'entreprise (SLA) et de ses contreparties.

De telles contraintes donnent à la blockchain une configuration très particulière qui n'est ni une "Public Permisionless Blockchain", ni une " Private Permissioned Blockchain" (Proof of Stake) mais plutôt une Meta Private BlockChain (Proof of Trust).

En tout état de cause, on imagine mal dans ces conditions de confier (dans un SLA) la complexité des taches de confiance numérique (ou la couverture des risques de sécurité, de légalité et d'interopérabilité) à des "Mineurs", d'indexer le prix de gestion sur le cours de leur devise (volatilité), et de prendre le "risque de bonne fin" sur un mineur ou le "risque systémique" sur plusieurs mineurs pour de nombreuses raisons en infraction avec les Règlements GDPR, E.IDAS et NIS.

La banque digitale se pose en alternative à tous les schémas d'organisation qui ne couvrent pas le risque systémique des opérations digitales, ni le risque monétaire de leur traitement (240 Milliards € en Europe) afin de simplifier une fois pour toutes, comme le demandent les Etats, et en toute transparence, les échanges entre les particuliers et les entreprises.

Eric Blot-Lefevre

TRUSTCORP Lux.

(1) (1) https://www.challenges.fr/entreprise/rgpd-le-cout-faramineux-de-la-protection-des-donnees-personnelles-pour-les-entreprises_580413.

(2) PWC estime que le CA de l'intelligence artificielle dépassera les 16.000 milliards de € en 2030, chiffre que nous comparons au Produit intérieur brut européen qui est actuellement de 16.500 Milliards €.

(3) La dernière crise de 2008 qui a provoqué l'effondrement du GDP atteignant 18.000 Mds € en 2007, n'est toujours pas résorbée puisque le niveau était à 12.000 Mds € en 2008 et il plafonne à 16.000 Mds en 2017.

(4) Les pénalités payées par les banques, les réseaux sociaux, les intégrateurs, les éditeurs de logiciels ont augmenté de plus de 100% en 2017 totalisant plus de 50 Mds de dollars. Avec le règlement GDPR mis en vigueur le 24 Mai 2018, les experts estiment que les pénalités dépasseront 200 milliards en 2020 et que les conséquences financières de la disqualification affecteront le cours de bourse ou la capitalisation boursière de plusieurs centaines de milliards $.

Les dernières sanctions étaient en 2017 : Banque (15Md$), Automobile (35 Mds$), Informatique Réseaux (20 Mds$) en très nette croissance.