



HAL
open science

Les technologies blockchain au service du secteur public

Perrine de Coëtlogon, Marc Durand, Maxime Jeantet, Claire Génin, Romuald Ramon, Pierre Boulet

► To cite this version:

Perrine de Coëtlogon, Marc Durand, Maxime Jeantet, Claire Génin, Romuald Ramon, et al.. Les technologies blockchain au service du secteur public. [Rapport de recherche] Université de Lille (2018-..). 2021. hal-03232816v2

HAL Id: hal-03232816

<https://hal.science/hal-03232816v2>

Submitted on 23 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - ShareAlike 4.0 International License



Université
de Lille

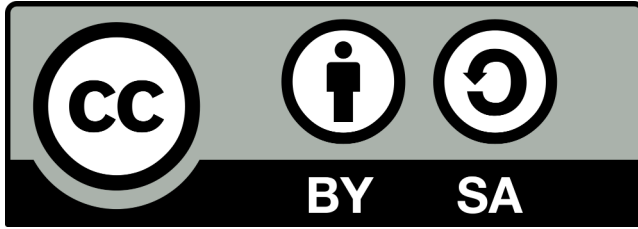
Livre blanc

Les technologies blockchain au service du secteur public

Université de Lille avec KAPALT
v1.0.1, juin 2021



CEF Digital
Connecting Europe



Ce document est mis à disposition selon les termes de la **Licence Creative Commons Attribution - Partage dans les Mêmes Conditions 4.0 International**.

Vous êtes autorisé à :

Partager — copier, distribuer et communiquer le matériel par tous moyens et sous tous formats .

Adapter — remixer, transformer et créer à partir du matériel pour toute utilisation, y compris commerciale.

Selon les conditions suivantes :

Attribution — Vous devez créditer l'Œuvre, intégrer un lien vers la licence et indiquer si des modifications ont été effectuées à l'Œuvre. Vous devez indiquer ces informations par tous les moyens raisonnables, sans toutefois suggérer que l'Offrant vous soutient ou soutient la façon dont vous avez utilisé son Œuvre.

Partage dans les Mêmes Conditions — Dans le cas où vous effectuez un remix, que vous transformez, ou créez à partir du matériel composant l'Œuvre originale, vous devez diffuser l'Œuvre modifiée dans les mêmes conditions, c'est à dire avec la même licence avec laquelle l'Œuvre originale a été diffusée.

Pas de restrictions complémentaires — Vous n'êtes pas autorisé à appliquer des conditions légales ou des mesures techniques qui restreindraient légalement autrui à utiliser l'Œuvre dans les conditions décrites par la licence.

Sommaire

Introduction	4
Méthodologie	5
1. Secteur public : une vision française et européenne de la blockchain	7
1.1. La blockchain : du Bitcoin à une technologie au service des usagers du service public	7
1.2. Comprendre la blockchain d'un point de vue métier	12
1.3. Les apports de la blockchain dans un environnement de transformation digitale de l'État	14
1.4. Mon problème métier peut-il être résolu par les technologies blockchain ?	16
1.5. Pourquoi utiliser une blockchain plutôt qu'une autre technologie ?	18
1.6. En quoi la blockchain peut-elle faciliter la collaboration entre administrations ?	20
2. L'EBSI : infrastructure européenne de service blockchain	21
2.1. Le partenariat Européen de la blockchain	21
2.2. Introduction à l'EBSI - European Blockchain Service Infrastructure	23
2.3. L'EBSI, une blockchain qui se démarque de toutes les autres	24
2.4. Une technologie à utiliser dans un cadre de souveraineté nationale et européenne	25
2.5. La trajectoire de l'EBSI : de la phase pilote (V1) à la feuille de route technologique (V2, V3)	26
2.6. Les bénéfices de l'EBSI	29
2.7. Pourquoi en tant qu'administration, utiliser EBSI plutôt qu'une autre blockchain ?	30
3. Utilisation pratique de la blockchain pour l'amélioration du service public	31
3.1. Éléments fondamentaux de mise en place d'un projet blockchain au sein du secteur public	31
3.2. Les sept cas d'usage présélectionnés par l'EBSI avec des projets en cours	35
4. Fiches descriptives de cas d'utilisation	41
Équipe	56
Remerciements	57
Contact	

Introduction

Les technologies blockchain combinent des innovations à des solutions informatiques existantes sur des systèmes informatiques distribués. Elles modifient de façon décisive la façon dont les organisations, même concurrentes, émettent et transfèrent en confiance des données ou des actifs numériques¹, sans passer par une structure centrale de contrôle.

Il peut sembler paradoxal de réfléchir aux applications de la blockchain dans le secteur public, alors que son origine, au travers de l'apparition du bitcoin, avait un objectif précis : désintermédiaire des institutions étatiques et des tiers de confiance dans les fonctions régaliennes de l'émission de la monnaie et du suivi des transactions financières et de leur enregistrement.

Si cette antinomie est historiquement légitime, les objectifs de ce document sont d'expliquer pourquoi il convient de distinguer la philosophie originelle de la blockchain de sa capacité fonctionnelle, de montrer comment depuis plusieurs années elle a fortement évolué et a su démontrer sa compatibilité avec un environnement réglementé et sa maturité technologique.

D'ailleurs aujourd'hui, vouloir parler de « LA » blockchain² est un exercice vain. Elle se décline désormais sous différentes formes avec des caractéristiques communes (distribution, registre, transparence, traçabilité, immutabilité, sécurité) mais aussi des différences significatives quant aux méthodes de gouvernance, d'authentification des acteurs et de confidentialité des transactions.

L'enjeu de ce document est de montrer que le secteur public peut bénéficier des caractéristiques uniques offertes par les technologies blockchain, tout en respectant ses valeurs et en offrant une meilleure expérience et une confiance renforcée à l'utilisateur du service public français et européen.

Cette réflexion sur leur utilisation dans ce secteur particulier repose sur plusieurs questions de fond :

- Comment peuvent-elles concourir à la mise en place d'une infrastructure interopérable et commune, tout en conservant les architectures et applications existantes dans chaque administration ou société intervenante ?
- Existe-t-il des perspectives particulièrement intéressantes face à des écosystèmes complexes où diverses parties prenantes doivent collaborer autour de procédures et logiques métiers ?
- Comment s'assurer que cette collaboration se réalise tout en garantissant la qualité, la source, la confidentialité et la transparence des données échangées qui sont devenues les seuls gages de confiance pour l'utilisateur final ?

¹ La notion d'actif numérique permet de représenter et modéliser aussi bien des objets intangibles et immatériels via l'agrégation de données provenant de plusieurs systèmes d'information (des diplômes, des brevets, des dossiers administratifs...) que des objets tangibles, matériels (un immeuble, un véhicule, un conteneur, un produit alimentaire, un vaccin...) représentés par son jumeau numérique.

² Ce document de travail utilise le terme « blockchain » par souci de lisibilité : il doit être compris pour désigner les « technologies blockchain » ou « technologies chaînes de bloc » en général.

Méthodologie

L'université de Lille est à l'initiative du présent livre blanc. Porteuse depuis 2018 du groupe de travail Blockchain Education France pour la Direction du Numérique pour l'Éducation du Ministère de l'Éducation Nationale, de la Jeunesse et des Sports, elle est l'opérateur de la Direction Interministérielle du Numérique (Service du Premier Ministre, ci-après DINUM) pour la réponse à l'appel à projets européen CEF-TELECOM-BLOCKCHAIN avec ses partenaires RENATER (Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche) et la société Blockchain Certified Data SAS.

À ce titre, elle testera en 2021 et 2022 les cas d'usage « diplôme », « notariation » et « identité auto-souveraine » sur l'Infrastructure Européenne de Service Blockchain (European Blockchain Service Infrastructure, ci-après EBSI).

Avec ce document, elle porte à la connaissance des administrations des éclairages sur les technologies blockchain en général, les sept premiers cas d'usage en cours de production ou d'étude sur l'EBSI ou sur d'autres blockchains. Forte de l'expertise acquise au sein du Partenariat Européen de la Blockchain, elle souhaite promouvoir ces technologies pour leur potentiel considérable de transformation numérique des services publics, nationaux, européens et internationaux.

Elle s'appuie sur des expérimentations « métier » pour décrire les potentialités sans cacher les obstacles actuels à leur adoption dans différents usages qui intéressent directement des administrations françaises : la certification, les transactions, la troisième génération de l'identité numérique ou encore l'archivage. Ces dernières pourraient améliorer considérablement l'efficacité des services en ligne à l'usage, en adaptant bien entendu la technologie au type de prestation à exécuter.

Les informations fournies ici résultent d'une revue maîtrisée de la littérature sur le domaine de la blockchain et de la documentation à disposition sur le site dédié à l'EBSI à la date de production de ce document. Les auteurs se sont appuyés sur des entretiens avec les responsables métiers d'administrations françaises ou des délégués de service public.

Prochainement en ligne, ce livre blanc a vocation à évoluer, s'enrichir de nouveaux sujets thématiques (santé, transport, recherche) ou technologiques (jumeau numérique, jeton non fongible ou NFT, non fungible token). Il se déploiera en points focus, points contacts, propositions et donnera des pistes de financements.

1. Secteur public : une vision française et européenne de la blockchain

1.1. La blockchain : du Bitcoin à une technologie au service des usagers du service public

Internet a radicalement transformé l'accès à l'information et son échange et il joue un rôle fondamental dans la société et l'économie actuelles. Il était pourtant difficile d'imaginer l'ensemble des services offerts aujourd'hui lors de l'introduction des premiers outils nécessaires à sa démocratisation il y a trente ans.

La blockchain, depuis la publication du livre blanc du bitcoin en tant que premier actif numérique, a considérablement élargi en une dizaine d'années la palette de ses domaines d'application et de ses cas d'usage potentiels ; elle pourrait jouer, sous différentes formes, un rôle comparable à celui d'Internet dans un domaine que celui-ci ne couvre pas : la transaction informatique et juridique de confiance.

En effet, si Internet est le véhicule privilégié de l'échange de toutes les formes numérisées de l'information, il n'est pas le garant, en tant qu'infrastructure réseau, de son unicité ou de son fonctionnement.

Considérons l'exemple d'un service numérique tel qu'un logiciel. Libre, il peut être dupliqué gratuitement à l'infini et Internet va nous permettre d'y accéder très simplement. Mais s'il est soumis à une licence que nous voulons acquérir, la transaction va nécessiter, outre l'intervention d'un tiers de confiance (par exemple le GIE Visa), une « délégation » de notre confiance vis-à-vis du fournisseur (l'éditeur de logiciel qui gère les droits de licence selon ses propres règles techniques auxquelles nous n'avons pas accès). Il nous sera donc impossible d'en céder la propriété ou une licence à un tiers, contrairement à l'exemplaire d'un livre par exemple, acquis une fois pour toutes.

C'est à cette problématique que les technologies blockchain répondent : autoriser les échanges fiables de pair à pair, sans passer par un organe de contrôle unique et centralisé, en assurant le processus vérifiable et permanent d'enregistrement des transactions et de suivi des actifs numériques. Ceci est réalisé sur la base d'une infrastructure décentralisée et en s'appuyant sur un registre partagé et distribué sur les nœuds (terme technique pour définir un ordinateur, un serveur) du réseau, chaque nœud possédant une copie intégrale du registre.

La blockchain est une infrastructure décentralisée enregistrant des transactions horodatées, représentant un changement d'état sur un actif numérique. L'enchaînement de ces transactions constitue le registre partagé.

Le mot transaction doit être pris ici dans son acception large, ne se réduisant pas à l'échange d'un actif numérique (digital asset) mais couvrant aussi ses changements

d'état (événement, fait, acte). Dans l'administration, c'est par exemple un dossier qui va changer de « propriétaire » au sens de responsable, au fur et à mesure de son avancement entre différentes entités impliquées dans son traitement global.

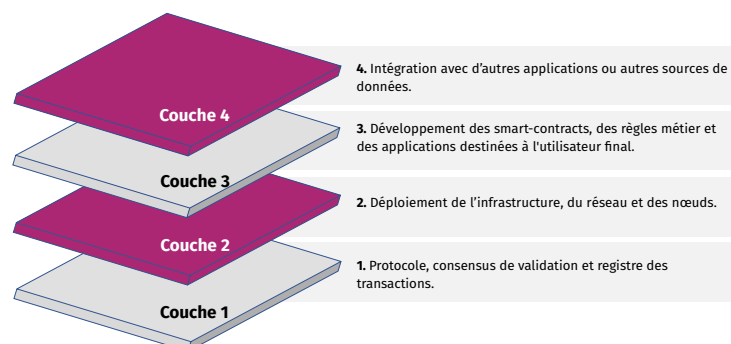
La blockchain, infrastructure centrée autour de la notion d'actif numérique, en assure la traçabilité à partir de sa création et tout au long de son cycle de vie en l'accompagnant dans le temps. Ceci va s'articuler en particulier au travers d'échanges sécurisés que l'on retrouve au cœur des relations et des processus entre les différents acteurs de l'écosystème du secteur public : de l'utilisateur à l'administration en passant par une série d'organismes, de sociétés ou d'intervenants du monde public, semi-public ou privé.

En plus de l'enregistrement d'une transaction sans tiers de confiance, les technologies blockchain ont vu apparaître la capacité, avec la création d'Ethereum en 2015, d'automatiser des processus, là encore sans nécessité d'une intermédiation humaine. Ceci se fait par le biais de contrats dits "intelligents" (smart-contracts), programmes informatiques s'exécutant sur la base de logique métier et s'intègre comme composante supportée par une blockchain.

Schématiquement, l'environnement nécessaire à la mise en place d'une blockchain peut s'apparenter à une structure en 4 couches :

- **La couche 1** représente les protocoles d'échange d'information et de consensus de validation des transactions qui transitent sur la blockchain et qui sont historisées dans le registre partagé. Cette couche s'appuie exclusivement sur des logiciels en open source pour des raisons de sécurité et de confiance dans l'infrastructure.
- **La couche 2** porte le déploiement de l'infrastructure et du réseau qui sous-tend l'ensemble des nœuds, c'est-à-dire des participants actifs de la blockchain.
- **La couche 3** correspond à la couche applicative elle-même constituée des contrats intelligents (smart-contracts) représentant les règles métiers et des applications destinées à l'utilisateur final.
- **La couche 4** symbolise l'intégration de la blockchain dans un existant : les autres applications et les sources de données du système d'information.

► **La mise en place d'une Blockchain d'entreprise va s'appuyer sur 4 couches principales**



Source : KAPALT

La blockchain est donc clairement une infrastructure décentralisée et non pas une application, une plateforme ou un site web « traditionnels » : les couches 1 et 2 déterminent les caractéristiques de l'écosystème et de la gouvernance de la blockchain en tant que telle, tandis que les couches 3 et 4 représentent les spécificités de la réponse aux besoins métier dans l'environnement propre.

Toutes les blockchains vont présenter des caractéristiques communes et uniques :

- **Consensus** : sur les méthodes et donc les inscriptions du registre : l'algorithme correspondant assure que les règles du protocole soient respectées et que toutes les transactions aient lieu de manière fiable, ce qui induit que l'ensemble des acteurs possède en temps réel une vision commune et transparente.
- **Immutabilité** : une transaction ou un événement enregistré dans la blockchain est daté, historisé et ne peut plus être modifié ou supprimé.
- **Irrévocabilité** : une transaction respectant les règles métiers et validée selon les règles du consensus ne peut être annulée.
- **Provenance** : tout actif géré par la blockchain est tracé de manière transparente et son historique est visible pour les acteurs ayant les droits.

Comme le formule Antony Lewis, directeur de la recherche chez R3, *“Quand les gens disent que les blockchains sont immuables, cela ne veut pas dire que les données ne peuvent pas être modifiées, ils veulent dire qu’il est extrêmement difficile de changer leurs états sans collusion ou action frauduleuse, et si vous essayez, il sera extrêmement facile de détecter la tentative”.*

Catégorisation des blockchains

En simplifiant, deux grands types de blockchain existent. Pour un participant, elles vont se différencier par l'autorisation d'accès (totalement libre ou administré) et le type d'action (écriture et/ou lecture simple) qu'il peut réaliser.

A) Les blockchains sans permission dites « publiques »

Elles sont nées avec le bitcoin. Leur développement est open source, et tout leur contenu (informations et transactions) est public. Elles sont accessibles à tous, ne nécessitent aucune autorisation d'accès et chacun peut y réaliser des transactions. Les participants n'y sont donc pas identifiés et utilisent des pseudonymes. Ces réseaux rémunèrent la participation des entités chargées de la validation des transactions du réseau par un système de jeton (*token*).

Dans les faits, ce type de blockchain s'appuie pour les couches 1 et 2, sur des fondations externes assurant le bon fonctionnement du protocole, le développement de l'écosystème et les modalités de gouvernance. Citons par exemple : Fondation Ethereum, Tezos ...

Les jetons (ou *tokens*) constituent une crypto-monnaie ou un actif numérique, pouvant être acheté ou vendu sur une plateforme d'échanges. Ainsi, le bitcoin est le jeton de la blockchain Bitcoin et l'ether celui de la blockchain Ethereum.

Il faut souligner ici que le qualificatif de « public » n'a aucun lien avec la notion de secteur public, puisqu'au contraire l'essence même de ce type de blockchain repose sur une décentralisation totale et sur l'absence de tout organe de contrôle.

Lors d'une transaction sur le réseau (Bitcoin, Ethereum, Tezos ...) l'échange « monétaire » se réalise en toute sécurité et en toute confiance entre inconnus, sans système bancaire, car la validation de la transaction est liée à un algorithme de consensus, qui dans la majorité des cas est soit la « preuve de travail » soit la « preuve d'enjeu ».

Dans le cas de Bitcoin par exemple, l'algorithme de consensus est la « preuve de travail ». C'est celui-ci qui est à l'origine du coût énergétique engendré sur Bitcoin.

Il est cependant important de rappeler que ce type de mécanisme de validation a été choisi par les premiers réseaux comme Bitcoin ou Ethereum pour son niveau de sécurité, prérequis nécessaire à la construction de la confiance alors que l'accès au réseau est ouvert à tous et sans obligation d'identité. Dans ce contexte, toute connexion doit être considérée comme potentiellement frauduleuse.

Afin de résoudre ce problème de consommation énergétique mais aussi d'augmenter la rapidité de validation et la capacité en nombre de transactions par seconde possible, de nouvelles technologies blockchain ont vu le jour (ARKEcosystem, TEZOS, Tollar hashnet, Polkadot...). En intégrant l'algorithme de « preuve d'enjeu », la consommation énergétique nécessaire à la validation des transactions est réduite en quasi-totalité tout en assurant une augmentation significative de la capacité de transactions et en gardant un niveau de sécurité élevé.

Sur les réseaux dits publics, les parties n'ont pas besoin de se connaître pour réaliser des transactions. Les algorithmes de consensus sont garants de la confiance et du bon déroulement des transactions. Ces infrastructures et ces réseaux sont particulièrement résilients étant donné leur décentralisation sur des milliers de nœuds interconnectés qui enregistrent et mettent à jour le registre.

B) Les blockchains à permission

Ces réseaux émergent en 2016, forts du constat que certains écosystèmes composés d'acteurs régulés et identifiés pourraient bénéficier d'infrastructures réseaux dédiées permettant une meilleure gestion des flux de données et de leurs partages.

À l'inverse des blockchains sans permission qui offrent une infrastructure réseau clé en main, les technologies blockchains à permission apparaissent sous la forme de briques technologiques (framework) open source, déployables à la demande et dont l'architecture dépendra de l'écosystème et de la problématique sous-jacente.

Elles vont être utilisées dans des cas d'usage où l'anonymat ou, plus précisément, le pseudonymat des intervenants n'est pas envisageable ou souhaité. De la même façon, elles s'imposent dans les contextes où une décentralisation complète de la gouvernance ou l'utilisation d'une cryptomonnaie ou d'un jeton ne sont pas nécessaires. Les participants sont parfaitement identifiés. L'accès et les actions en écriture vont être soumis à autorisation, seule la lecture restant potentiellement libre. La source des données est authentifiée. Elles permettent également de gérer à un niveau de granularité extrêmement fin, la nature des données (publiques, partagées ou privées), de les chiffrer et donc d'assurer moins de transfert de données personnelles et une confidentialité des échanges plus forte entre les acteurs du réseau.

Ce type de blockchain existe le plus souvent dans un cadre régulé ou réglementé, ou pour un consortium d'entreprises en B2B (business to business). Citons par exemple pour la couche 1 : Hyperledger Fabric et Besu de la Linux Foundation, Quorum, Corda, Multichain etc. Les participants vont pouvoir y jouer des rôles différents en fonction de la gouvernance adoptée et la notion de confiance apparaît.

À la différence d'une blockchain sans permission (publique), les parties prenantes sont connues. Leur qualité va jouer un rôle dans la validation d'une transaction : c'est la distinction fondamentale dans cette typologie.

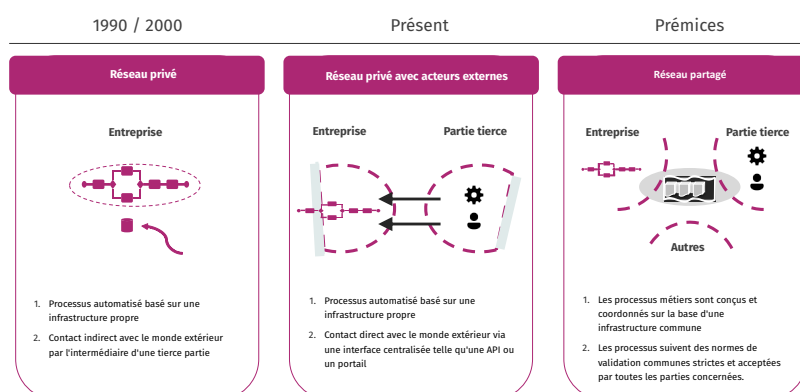
En cohérence avec l'objectif de transparence, toutes les technologies blockchain sont par philosophie open source ; ce qui rapprochent la plupart de leurs promoteurs des mouvements de l'ouverture tels que l'open government, open data, open science, open education...

1.2. Comprendre la blockchain d'un point de vue métier

De manière générale, la blockchain contribue, sans nécessité d'un tiers de confiance (c'est-à-dire d'une structure « extérieure » à l'écosystème vérifiant les transactions et empêchant toute sorte de fraude), à lever simultanément trois incertitudes ou difficultés récurrentes du secteur public :

- **Authentification** : savoir avec qui l'on traite, c'est-à-dire avec confiance quant à la légitimité de l'intervenant, ce qui inclut les compétences ou les certifications dans le cas d'un prestataire de services au sens large. La réputation pour un tiers devient un élément clé qui bénéficie naturellement avec le temps de l'effet « réseau ».
- **Traçabilité** : avoir une connaissance certifiée de l'évolution d'un actif dans le temps via une auditabilité, une traçabilité et une certification de la donnée qui le représente dans le monde digital. Cela permet de posséder une correspondance fiable et permanente entre un actif physique (un véhicule, un bien immobilier, etc.) et son jumeau digital.
- **Unicité** : supprimer entre les différentes parties prenantes les frictions qui actuellement sont la cause d'échanges multiples de mails, de fichiers de différents formats, de discontinuités dans le traitement des informations voire de litiges. La numérisation des workflows entre les acteurs, la fiabilité des transactions ou des échanges réalisés et la transparence du registre vont faire diminuer drastiquement le nombre de ces écarts et vont garantir, sans besoin d'un tiers de confiance extérieur, la complétude et la qualité des échanges.

► Évolution des réseaux professionnels fonction des capacités technologiques du marché



Du point de vue des processus « métier », la blockchain représente *de facto* les prémices d'une évolution profonde du mode de fonctionnement en réseau des organisations au sens large, secteur public inclus, que ce soit entre elles ou avec les acteurs externes.

Bien entendu, d'autres technologies autorisent déjà l'échange d'informations de manière sécurisée mais elles s'appuient sur des processus internes à chaque organisation. La blockchain offre une nouvelle possibilité : ***une entité a la capacité de « partager » une sous-partie d'un processus de manière transparente et sécurisée avec d'autres parties prenantes de son écosystème tout en gardant la maîtrise totale de ses données propres.***

Les technologies blockchain ne doivent donc pas être considérées comme un nouveau support d'envoi et de réception de données, mais bien comme un registre partagé par plusieurs entités. Les blocs d'informations qui composent ce registre contiennent des enregistrements permanents qui dépendent du domaine applicatif.

À titre d'illustrations dans le secteur public, une blockchain a la capacité de créer un enregistrement immuable et décentralisé :

- des changements d'état durant le cycle de vie d'un document (visualisation par le fonctionnaire de l'évolution du document) ;
- des étapes que les produits franchissent le long d'une chaîne d'approvisionnement (traçabilité des mouvements douaniers, etc.) ;
- des transactions financières (suivi des subventions, de flux financiers...).

Et puisque ce registre est dupliqué et distribué en temps réel (ou quasi-réel) à tous ses participants, la blockchain va permettre et faciliter le passage d'une perspective totalement « privée » des processus vers un plus grand partage des données métiers.

Attention : il est important de préciser que, la plupart du temps, le registre partagé entre les parties prenantes ne contient que les attributs de preuve de la donnée et non la donnée elle-même. La donnée reste pour sa part en base de données et, dans ce cas, seule son empreinte numérique est enregistrée dans le registre blockchain.

Cela n'élimine pas pour autant les questions de sécurité et de véracité. En effet, si l'attribut de preuve enregistré sur la blockchain permet la transparence, l'immuabilité et la traçabilité, en cas de perte de la donnée en base, ces attributs de preuve ne permettront pas de la retrouver ou de la reconstruire.

1.3. Les apports de la blockchain dans un environnement de transformation digitale de l'État

La blockchain se pense comme une infrastructure en réseau de type « pair à pair » sur laquelle vont tourner des applications transactionnelles qui peuvent être en mode

- **G2G** – Gouvernement à Gouvernement (par exemple entre différentes administrations ou agences publiques nationales et transnationales) ;
- **G2C** - Gouvernement à Citoyen (entre une administration et un citoyen) ;
- **C2C** - Citoyen à Citoyen (entre citoyens incluant un élément relevant du service public).

Les organismes gouvernementaux sont les intermédiaires essentiels de ces transactions et les garants de leur bon fonctionnement. Les documents qu'ils délivrent ou certifient sont le moyen standard de pouvoir vérifier les informations sur les personnes (cartes d'identité, permis de travail, permis de conduire, etc.) et les biens (origine des conteneurs, sécurité des produits, etc.).

Par rapport aux bases de données centralisées traditionnelles, la blockchain garantit deux spécificités :

- **par construction, l'intégrité et la traçabilité en temps réel des données, pour une collaboration efficace et transparente entre les utilisateurs, sans utilisation d'un tiers de confiance extérieur ;**
- **l'auto-exécution de contrats intelligents pour automatiser et sécuriser des processus, avec à la clé des gains en termes d'efficacité et de qualité.**

Dans le cas des services publics, cela signifie par exemple que la blockchain peut faciliter les contrôles de l'intégrité et de l'origine des documents officiels sans qu'il soit nécessaire de contacter à chaque fois leur entité émettrice. Dans ce cas, le partage des données peut se faire de manière totalement sécurisée entre portefeuilles numériques.

Puisque les blockchains représentent des systèmes distribués avec une forte automatisation potentielle, elles peuvent être utilisées pour concevoir efficacement des plateformes peu coûteuses, conduisant à des économies significatives dans le traitement des données, tout en augmentant la robustesse du système.

Les solutions mises en place dans des applications distribuées (dApp) doivent être conçues comme toutes applications de façon ergonomique.

Les avantages de la blockchain peuvent se décliner en quatre catégories principales :

► Bénéfices liés à l'utilisation d'une Blockchain



Gain de temps

- Réaliser des transactions en temps quasi-réel
- Optimiser la validation des processus



Réduction des coûts

- Mutualiser le coût des infrastructures
- Optimiser les intermédiaires
- Supprimer les tâches redondantes
- Supprimer le papier
- Améliorer la qualité des données



Sécurité renforcée & Gestion d'identité

- Protéger contre la falsification, la fraude et la cybercriminalité
- Créer un réseau membres multi-entités
- Fournir une gestion de l'identité
- Fournir une granularité d'accès à différents niveaux
- Traçabilité de l'historique



Nouveau modèle économique

- Conduire à la création de nouvelles entreprises
- Réinventer le produit existant
- Permettre la création de nouveaux produits / services
- Créer de nouveaux flux de revenus

Source : KAPALT

Pour tout type de structure du secteur public, les possibles améliorations opérationnelles des technologies blockchain visent :

- le coût de vérification des identités ;
- le coût de vérification de l'origine ou de l'historique ;
- la réduction de la fraude ;
- l'audit des événements et des changements d'état ;
- l'automatisation de certains processus : facturation, paiement, etc. ;
- la gestion automatique de l'allocation d'actifs non-financiers ;
- l'accélération des transactions.

1.4. **Mon problème métier peut-il être résolu par les technologies blockchain ?**

C'est bien entendu le cœur du questionnement pour une administration ou une agence du secteur public. Les technologies blockchain n'échappent en rien aux règles habituelles qui devraient précéder toute introduction potentielle d'une technologie : quelles sont les conditions nécessaires, et non pas simplement suffisantes, pour en justifier l'usage ?

Une blockchain, de manière générale, n'est d'aucune utilité pour résoudre un problème purement interne à une organisation. Son intérêt ne se pose donc que dans le cadre d'interactions externes avec son environnement.

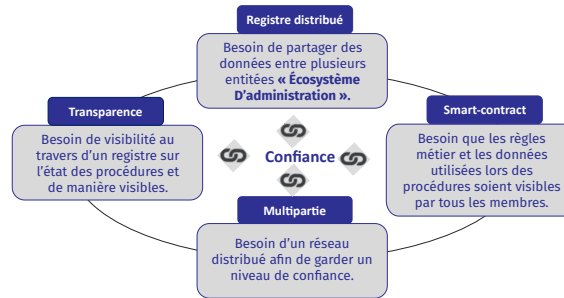
Il est donc important de recourir à une approche holistique en se plaçant au niveau de l'écosystème et de sa dynamique :

- Quels sont mes partenaires de travail actuels ou potentiels afin de résoudre ce problème ou de répondre à ce besoin ?
- Quels sont mes points de frictions sur la chaîne de valeur de ma procédure ? Sont-elles internes à mon organisation ou externes ? Suis-je dépendant de sources de données externes ?
- Quelle est la macrotrajectoire : périmètre fonctionnel et/ou le nombre de parties prenantes (aujourd'hui, dans un an, dans 3 ans...)?

À ce premier niveau, un certain nombre de critères doivent être analysés. Sachant que cette liste n'est naturellement pas exhaustive, on peut citer :

- le nombre d'acteurs impliqués (administrations, agences publiques, délégataires, sociétés privées, destinataires...);
- la volumétrie des échanges et des transactions ;
- le degré de collaboration et de transparence souhaité ;
- la fréquence des dysfonctionnements, des ruptures de traitement, des frictions ou des litiges actuels ;
- le niveau de confidentialité et de sécurité à atteindre ;
- les bénéfices potentiels pour chacune des parties.

► **Les principaux critères de choix pour utiliser une Blockchain / DLT ou pas...**



Source : GARTNER

Si la donnée est uniquement utilisée par un nombre réduit d'entités ou si le degré de collaboration entre les parties tierces n'est pas élevé ou si le ratio entre mises à jour sur lectures pour les transactions est faible alors l'utilisation d'une blockchain est hautement challengable

Ainsi, de manière macroscopique, si la réponse à un (ou plusieurs) de ces critères est peu élevée à terme, il est légitime de considérer que le choix d'utiliser la blockchain n'est pas forcément le meilleur. Cela ne signifie pas que des critères suffisamment forts ne puissent pas à eux seuls justifier une analyse complémentaire, mais ils doivent être pondérés dans une vue globale.

En particulier, des bénéfices clairs pour chacun des participants actifs du réseau doivent être à ce stade identifiés. Ceux-ci peuvent être de nature différente pour deux parties prenantes avec, par exemple, une meilleure excellence opérationnelle pour l'une et une meilleure qualité des données pour l'autre. Mais la croissance du réseau qui est la condition *sine qua non* d'une initiative blockchain ne se réalisera pas sans eux.

Une blockchain ne se construit pas au simple bénéfice d'une partie unique, elle ne se justifiera dans le temps qu'au travers de la conjonction de bénéfices tangibles pour les différents acteurs impliqués dans l'écosystème.

C'est cette caractéristique qui fait que la blockchain peut avoir des apports uniques, mais à la condition d'être pensée dans un environnement pouvant se révéler complexe.

Si le niveau des critères préliminaires apparaît comme suffisamment élevé, et il dépend bien entendu du contexte métier, alors une analyse plus fine des besoins à résoudre pourra être ensuite lancée. Il conviendra de ne pas simplement les confronter aux capacités et aux apports de la technologie elle-même, mais aussi de comprendre en amont quels sont les facteurs clés de succès de la mise en place potentielle d'une blockchain.

1.5. Pourquoi utiliser une blockchain plutôt qu'une autre technologie ?

Les technologies blockchain sont des technologies récentes qui évoluent constamment, mais qui n'ont pas vocation à se substituer, en tant que telles, à une technologie déjà en exploitation et qui a fait, parfois depuis de très nombreuses années, la preuve de sa robustesse. En comparaison directe, une technologie plus mature (par exemple une base de données centralisée ou distribuée, l'EDI, etc.) va offrir une meilleure maîtrise de la mise en place et des coûts associés (conception, design, développement, mise en production, maintenance, etc.).

Pour faire de la traçabilité dans une chaîne d'approvisionnement, du partage sécurisé d'informations ou encore de la réconciliation de données entre partenaires dans tous les secteurs d'activité, nul n'a attendu la mise en place des couches 1 à 3 des technologies blockchain.

Considérons maintenant, par exemple, le cas fréquent du rapprochement de données transitant d'une organisation à une autre. Il y a potentiellement des différences de format, des incohérences, des problèmes de qualité et de complétude des données, etc. Cette situation est génératrice d'un surcroît de travail parfois très lourd de contrôles manuels voire de ressaisies n'apportant aucune valeur ajoutée au destinataire.

La question que l'on peut alors se poser semble naturelle : pourquoi les autres technologies et outils existants n'ont pas permis de résoudre certains de ces problèmes ?

Les considérations à prendre en compte ici sont loin d'être *stricto sensu* techniques.

On peut citer :

- Qui est le propriétaire de la donnée à un instant spécifique du processus ?
- Quelles sont les limites de responsabilité de chacun ?
- Quel est le niveau de confiance entre les acteurs ?
- Existe-t-il le besoin d'une intermédiation ou pas ?

Une autre technologie ou la combinaison d'autres technologies pourrait (ou aurait pu), dans de nombreux cas de figure, répondre aux besoins fonctionnels, mais ce sont les conditions relatives à l'écosystème ou à la gouvernance qui peuvent ici favoriser le choix d'une technologie blockchain. C'était techniquement possible mais *de facto* irréalisable opérationnellement parlant.

C'est pourquoi, dans les réalisations opérationnelles du marché, la grande majorité des usages de la blockchain offre non pas une substitution « améliorée » à une fonction existante mais bien plutôt un complément ou un nouveau service à valeur ajoutée qui ne pouvait pas être proposé auparavant de manière réaliste sans cette technologie.

Certaines réussites tout à fait significatives, comme TradeLens³, un registre permettant la traçabilité des containers dans le transport maritime mondial, passent d'ailleurs par la « simple » numérisation d'un document « papier ». Leurs versions numériques circulent entre un nombre significatif de structures (publiques et privées) et nécessitent la transformation digitale de l'ensemble des processus associés.

³ TradeLens : <https://www.tradelens.com>

1.6. En quoi la blockchain peut-elle faciliter la collaboration entre administrations ?

Pour éviter, dans le cadre du secteur public, le travers de nombreux projets préliminaires (PoC : Proof-of-Concept) blockchain lancés ces dernières années dans tous les secteurs, il semble important de mener une double investigation préalable à un début de projet :

1. S'assurer que la technologie est capable de répondre aux exigences nécessaires à l'application (volumétrie, performance, sécurité, respect de la conformité...) en production réelle.
2. Comprendre en quoi l'une (*a minima*) des propriétés spécifiques de la blockchain (consensus, immutabilité, irrévocabilité, provenance) est réellement nécessaire au processus.

En vérifiant seulement le premier point, on est conduit à un projet peut-être techniquement réalisable, mais où l'utilisation d'une blockchain en tant qu'apport métier ne se justifie pas. Comme vu précédemment, pourquoi faire dans ces conditions le choix de cette technologie plutôt que celui d'une autre plus mature et mieux maîtrisée ?

En se focalisant sur le second point, on arrive à un projet qui, au-delà du pilote, va se révéler tout simplement impossible à mettre à l'échelle ou en production ; ceci pour des raisons de gouvernance, de coût, de complexité technique ou de conformité. Un nombre très significatif de projets préliminaires blockchain se retrouvent dans ce cas de figure.

Respecter cette approche duale doit permettre de s'assurer que le projet envisagé a la capacité de fournir de façon opérationnelle un ou plusieurs avantages tangibles de la blockchain pour le secteur public par rapport à d'autres solutions technologiques entre administrations, nationales, européennes ou internationales :

- Supprimer les tâches redondantes de vérification de données et de duplication des processus grâce aux partages d'une source commune validée et acceptée comme telle par l'ensemble des parties.
- Fournir une transparence et une confiance puisqu'il n'y a pas de propriétaire « unique » des données du registre partagé.
- Identifier et quantifier plus facilement les bénéfices pour chacune des parties puisque l'intérêt commun et le service de l'utilisateur constituent la valeur cardinale et partagée par les acteurs.

2. L'EBSI : infrastructure européenne de service blockchain

L'EBSI représente une illustration concrète d'une blockchain pour le secteur public.

2.1. Le Partenariat Européen de la Blockchain

Le Partenariat européen de la blockchain (EBP)⁵ est une initiative conjointe de la Commission européenne, des 27 États membres de l'Union Européenne, de la Norvège et du Lichtenstein (membres de l'Association Européenne de Libre-Échange) signé le 10 avril 2018. Cet accord prévoit notamment :

- le développement de visions et d'initiatives conjointes par le biais du partenariat dans une approche paneuropéenne ;
- la mise en place pour le secteur public européen et transfrontalier de l'Infrastructure Européenne de Service Blockchain (EBSI) ;
- la promotion de la sécurité juridique avec un cadre juridique global favorable à l'innovation (actifs numériques, contrats intelligents) ;
- l'accroissement des financements pour l'innovation blockchain (subventions et soutien aux investissements) ;
- le soutien à l'interopérabilité et aux normes ;
- le soutien aux formations pour le développement des compétences blockchain ;
- l'interaction avec la communauté blockchain (dont INATBA, l'association européenne des parties prenantes de la blockchain et le Forum-Observatoire de la Blockchain au niveau européen, mais aussi les réseaux internationaux).

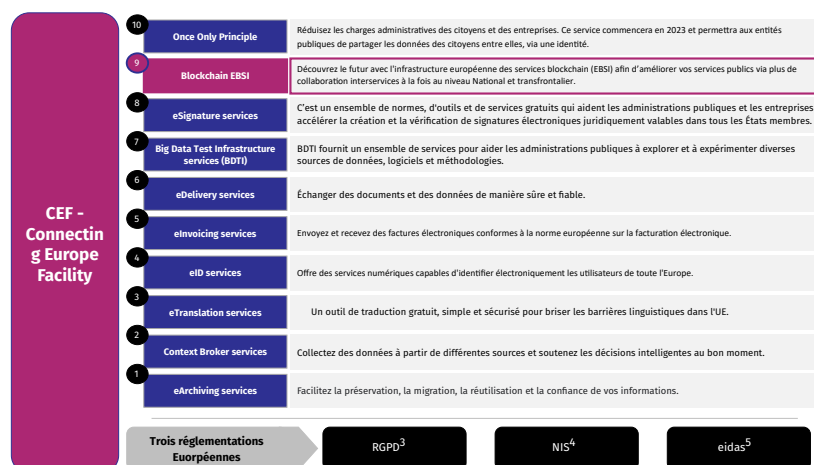
Le groupe politique du Partenariat Européen de la Blockchain a confié à sa direction du numérique, la DGCNECT, le soin de créer, avec sa Direction des Systèmes d'Information, la DIGIT, l'infrastructure Blockchain Européen (EBSI – European Blockchain Service Infrastructure) dans le respect des « acquis » européens. L'infrastructure déployée est « durable » (excluant par exemple l'algorithme de preuve de travail et intégrant des technologies utilisant des algorithmes tels que « la preuve d'enjeu », « la preuve d'autorité », etc.). Elle participe à la création des standards internationaux et respecte la réglementation sur les données personnelles.

⁴ <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership>

L'objectif est d'offrir aux États membres du partenariat un environnement et une infrastructure clé en main, permettant un haut niveau de collaboration et une gouvernance inédite afin d'améliorer et d'innover en matière de services publics nationaux et transnationaux.

L'EBSI est une composante de base du Connecting Europe Facility (CEF), l'infrastructure informatique européenne de connexion, avec ses « blocs de construction » (building blocks), destinés à s'interfacer (schéma ci-dessous). Il fournit des logiciels, des spécifications et des services interopérables et réutilisables permettant son adoption par les institutions européennes, les administrations publiques européennes et à terme également les entreprises.

Au terme d'un processus de consultation des Etats membres alliant construction technologique et réglementaire, certaines parties du CEF font d'ailleurs l'objet de réglementation directement applicable dans les Etats membres (par exemple la réglementation sur l'identité numérique eIDAS).



Source : KAPALT

Sources :

- CE / traduction Kapalt - Blockchain pour Entreprise
- Connecting Europe Facility ⁵
- RGPD (protection des données) ⁶
- NIS: sécurité informatique ⁷
- eidas: services de confiance ⁸

⁵ <https://ec.europa.eu/cefdigital/wiki/display/cefdigital/cef+digital+home>

⁶ https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

⁷ <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

⁸ <https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification>

2.2. Introduction à l'EBSI - European Blockchain Service Infrastructure

L'EBSI offre une infrastructure clé en main, intégrant de nombreuses briques technologiques. Dans ce contexte, les administrations peuvent l'intégrer au coeur de leur propre stratégie de transformation digitale et profiter de nombreux outils proposés en surcouverte.

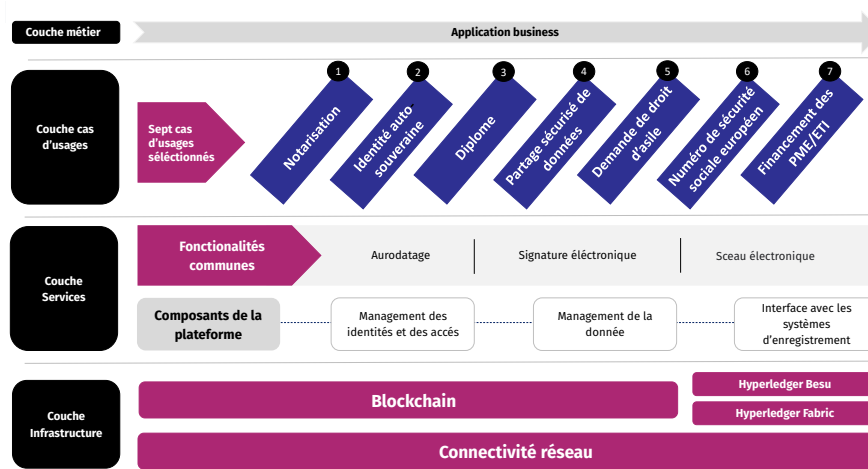
L'idée est d'apporter la confiance par une infrastructure européenne unique gérée conjointement par des institutions publiques. EBSI n'est pas axée sur la création d'une technologie mais plutôt sur la création d'un réseau utilisant des technologies disponibles et éprouvées, en les complétant si elles ne suffisent pas.

L'EBSI s'organise autour d'une architecture en plusieurs couches (voir le schéma ci-dessous), regroupant différentes briques technologiques et déployables "as-a-service" et sur la base des cas d'usage présélectionnés par les États membres (schéma ci-dessous). Les 4 premiers cas d'usages (numérotés de 1 à 4) sont actifs et bénéficient d'une antériorité par rapport aux 3 derniers (numérotés de 5 à 7), qui débute à la date du présent rapport.

Dans le domaine du secteur public, la blockchain européenne EBSI joue un rôle fondamental. Elle offre un cadre flexible pour les couches 1 et 2 tout en assurant le strict respect des règles de confidentialité, de sécurité des données et de conformité. Tout usager ou intervenant du service public en tirera les bénéfices en termes de confiance, transparence et efficacité opérationnelle, au travers des applications mises à disposition dans la couche 3 tandis que l'intégration avec le patrimoine applicatif existant de la couche 4 sera simplifiée.

Les aspects techniques sont détaillés dans la documentation du site :

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI>



Source : KAPALT

2.3. L'EBSI, une blockchain qui se démarque de toutes les autres

Comme mentionné au début de ce rapport, une blockchain est un registre distribué accessible au sein d'un réseau de pair à pair et dont les écritures (transactions) sont émises et validées par consensus entre les membres du réseau.

Ainsi, la blockchain du fait de son architecture (différente d'un réseau à un autre) permet la création d'une infrastructure propre à un écosystème donné. Cette infrastructure blockchain permet à chacun des membres de travailler et de collaborer dans un environnement de confiance tout en gardant le contrôle sur ses procédures métier et ses données propres.

Le déploiement d'une blockchain entre acteurs d'un même écosystème nécessite donc la mise en place de règles de gouvernance.

Dans ce sens, il est important de comprendre comment l'EBSI s'articule au niveau de son architecture, lui permettant de créer cet environnement de confiance à la fois pour les administrations et son utilisateur final, le citoyen.

Contrairement à d'autres réseaux blockchain comme Bitcoin ou Tezos où la confiance dans la bonne exécution des transactions réside exclusivement dans les algorithmes de consensus / validation (preuve de travail et preuve d'enjeu, respectivement), la blockchain EBSI, dans sa version 1, intègre un algorithme de validation beaucoup plus régalien dans tous les sens du terme, : la preuve d'autorité (Proof-of-Authority).

Cette notion de preuve d'autorité est fondamentale car elle permet à l'État, et par extension à ses administrations et délégations de service public ou autres acteurs, le droit de devenir nœuds validateurs de données et d'écrire sur le registre de manière immuable et irrévocable des événements (transactions), traduisant un changement d'état sur des données du service public.

L'EBSI par son design, ne désintermédie pas la confiance dans la fonction régaliennne de l'État et s'inscrit dans une perspective de fluidification, de conservation, de transportabilité et de pérennité des services publics et des données du citoyen.

Cette architecture initiale permet donc de proposer un premier niveau de valeurs probantes des données sous format numérique, nécessaire à la création d'un environnement de confiance pour une meilleure collaboration entre les administrations dans leur mission aux citoyens.

À l'image de sa technologie sous-jacente, l'EBSI permettra de créer une nouvelle génération d'applications ouvertes et collaboratives sur la base de procédures administratives multipartites. Elle contribuera à l'établissement d'une vision unique

des procédures pour l'ensemble des parties prenantes fondées sur la responsabilité et la transparence, et au bénéfice de l'utilisateur.

2.4. Une technologie à utiliser dans un cadre de souveraineté nationale et européenne

À l'heure où l'Europe accuse un important retard technologique comparativement aux géants de la technologie américains et chinois, des questions de souveraineté numérique se posent quant à la dépendance européenne tant dans le secteur public que privé.

Dans un contexte de transformation numérique accélérée du fait de la pandémie, le choix des technologies et des infrastructures sur lesquelles les États européens construiront leurs services publics de demain est crucial. Tout particulièrement en ce qui concerne les infrastructures de stockage et de gestion des données du citoyen.

Dans ce sens, “si la numérisation des documents officiels accélère le flux d’informations et facilite la vie des citoyens, elle laisse également place à des activités frauduleuses, car sans les outils numériques appropriés, les documents numériques restent relativement faciles à falsifier. Cela reste l’une des principales raisons pour lesquelles le manque de confiance dans le monde numérique constitue toujours un défi majeur pour les gouvernements. En bref, le problème est bien plus important que le partage de documents et d’informations sensibles sur Internet. Aujourd’hui, le principal défi consiste à trouver un moyen de rendre les interactions en ligne quotidiennes, sûres et dignes de confiance pour toutes les parties concernées.”⁹

Dans ce contexte, les technologies blockchain, et en particulier l'EBSI, offrent une opportunité rare de chiffrer nos données, les rendant sécurisées, vérifiables, traçables (unicité), transportables, ceci grâce à une technologie durable et sur la base d'un référentiel commun au niveau de l'Union Européenne et interopérable au niveau mondial. Le contrôle et la sécurité de nos données via l'EBSI au travers de son architecture et de sa gouvernance assureront une souveraineté renouvelée aux États membres, permettant des collaborations inédites tout en conservant un contrôle adéquat.

En effet, la gouvernance de l'EBSI englobe dans son périmètre à la fois le stockage de données et la mise en place des critères nécessaires pour fournir des services qui touchent à l'identité du citoyen (par exemple RENATER pour la France est à la fois fournisseur de stockage et opérateur de fédération d'identité pour l'enseignement supérieur et la recherche).

⁹ <https://ec.europa.eu/cefdigital/wiki/display/cefdigital/the+challenge+for+digital+transformation+in+public+administration>

2.5. La trajectoire de l'EBSI : de la phase pilote (V1) à la feuille de route technologique (V2, V3)

L'objectif ultime du Partenariat Européen de la Blockchain est de réussir à créer à la fois une infrastructure blockchain européenne mais également un environnement technologique et juridique permettant une transformation harmonieuse des services publics vers le numérique. Le défi le plus ambitieux est de construire et mettre à disposition des services publics, de manière incrémentale, cette infrastructure de l'EBSI. De plus, au niveau des cas d'usages et des parties prenantes un travail important, mais salvateur sur les données concernées sera nécessaire. Cette mise en commun permettra d'innover au cœur des services publics européens ou transfrontaliers et constituera l'un des blocs technologiques majeurs dans la construction de solutions informatiques européennes interconnectées, de nature à instaurer la confiance du citoyen européen.

Dans les deux prochaines années, l'objectif du partenariat européen de la blockchain et de l'EBSI dans sa version 1 et bientôt 2 sera de tester, sous le pilotage du groupe « Politique » et avec l'aide d'un groupe « Technique », les sept cas d'usages :

1. Identité auto-souveraine (avec un pont vers la technologie mise en place par la réglementation eIDAS) ;
2. Diplômes et certificats vérifiables ;
3. Notarisation ;
4. Partage de données sécurisé ;
5. Demande de droit d'asile ;
6. Émission d'obligations pour la reprise post-CoVid19 ;
7. Numéro de sécurité sociale européen.

À plus long terme, les autres objectifs stratégiques de l'EBSI sont d'améliorer les services gouvernementaux transfrontaliers et de réduire l'impact environnemental de l'Europe, de permettre le développement de pôles et de projets technologiques européens et d'améliorer la mobilité transfrontalière des citoyens et des entreprises tout en respectant les réglementations applicables, notamment le RGPD et l'eIDAS.

La première version de l'EBSI est sortie au mois de juillet 2020 dans une phase pilote. Elle est basée sur deux protocoles open source à permission utilisables par tous : Hyperledger Fabric et Hyperledger Besu, qui intègrent un algorithme de validation de preuve d'autorité (Proof-of-Authority). Des nœuds sont installés et testés dans tous les États membres par les organisations autorisées. RENATER (Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche) porte pour la France les premiers nœuds EBSI.

En effet, la gouvernance de l'EBSI englobe dans son périmètre à la fois le stockage de données et la mise en place des critères nécessaires pour fournir des services qui touchent à l'identité du citoyen (par exemple RENATER pour la France est à la fois fournisseur de stockage et opérateur de fédération d'identité pour l'enseignement supérieur et la recherche).

Une suite d'APIs a été développée sur quatre cas d'usages sélectionnés pour leur facilité de mise en test par des administrations et parties prenantes avec le soutien et l'accompagnement des équipes techniques de la commission Européenne ¹⁰.

La version 2 est attendue pour le début de 2021. Elle permettra le déploiement de nouveaux nœuds, une mise en production des 4 cas d'usages de la version 1 ainsi que les tests et mise en production de 3 cas d'usages supplémentaires sélectionnés par les États membres. Cette version 2 se verra ajouter un nouveau protocole intégrant une implémentation de l'algorithme de validation de la preuve d'enjeu (Proof of Stake), qui permettra de travailler sur l'interopérabilité d'au moins deux modèles de blockchain.

De manière plus générale, cette stratégie a pour but d'intégrer au sein de l'EBSI et au fil des versions d'autres réseaux et protocoles. Cette approche très ouverte permettra à l'Union européenne de profiter pleinement des technologies construites autour de l'open source et leurs communautés à travers le monde. En d'autres termes, l'EBSI intégrera dans son architecture modulaire au fil de l'eau toute technologie qui respectera les critères, les standards et la compatibilité des réglementations en place. C'est une caractéristique essentielle pour assurer la pérennité de l'infrastructure.

Dans cet esprit, il n'est pas exclu que des blockchains sans permission (dites publiques) soient à l'avenir proposées au sein de la boîte à outils EBSI. Ces ajouts de briques technologiques permettront également de répondre à un plus grand nombre de cas d'usage. La construction du réseau sous-jacent devra répondre à des spécificités à la fois métier (procédure et réglementation) mais aussi d'écosystème et de gouvernance propre à chaque pays et administration.

¹⁰ <https://ec.europa.eu/cefdigital/wiki/display/cefdigital/get+started+ebs>

Sur des versions ultérieures (horizon 2023/2024 pour la Version 3), un accès à l'EBSI sera proposé aux entreprises dans une optique de cocréation et sur une base commune : l'économie circulaire de demain. Les cas d'usage retenus dans le cadre de cette version font actuellement l'objet d'appels d'offres¹² ayant pour but d'accélérer la recherche et le développement de solutions. Ces cas d'usages sont définis comme étant à haut volume et haute vélocité (V&V) et sont en grande partie inspirés du Circular Action Plan Report et du passeport produit digital¹³ (liste non exhaustive) :

1. Soutien au développement d'une économie circulaire et à l'exploitation du passeport de produits numériques améliorant la traçabilité et la circularité de tous les produits et composants sur le marché de l'UE10. Cela concerne potentiellement le suivi des matières premières dans les produits physiques qui sont commercialisés et utilisés dans l'UE ou des données qui devraient être suivies à travers différents cycles de vie des produits (par exemple les batteries).
2. Traçabilité des données et documents concernant l'ensemble des bâtiments, équipements et matériaux.
3. Traçabilité des produits pour limiter la contrefaçon.
4. Preuve de l'origine et du conditionnement du produit dans les chaînes alimentaires et agroalimentaires.
5. Suivi des articles douaniers compatibles avec l'internet des objets (IoT : Internet of Things) à autres applications telles que le suivi en temps réel du géopositionnement et de l'état du système d'objets en mouvement rapide à travers les frontières.
6. Suivi des transactions ou des factures à des fins de TVA (limitation de la fraude à la TVA).
7. Gestion à l'échelle de l'UE des droits de propriété intellectuelle (comme les brevets, les marques, les droits d'auteur), y compris la gestion des droits d'auteur qui peuvent être directement associés au contenu numérique en temps quasi-réel.

¹¹ <https://ec.europa.eu/cefdigital/wiki/display/cefdigital/2020/12/03/eu+blockchain+call+for+tenders+launched>

¹² https://eur-lex.europa.eu/resource.html?uri=cellar:9903b325-6388-11ea-b735-01aa75ed71a1.0017.02/doc_1&format=pdf

2.6. Les bénéfices de l'EBSI

En participant au réseau EBSI, l'administration nationale pourra utiliser l'infrastructure et les solutions disponibles pour :

- Offrir des services intégrés améliorés aux usagers et aux entreprises, à la fois dans son propre pays et au sein de l'Union européenne
- Améliorer la transparence et la confiance dans les services publics
- Simplifier les processus administratifs et en augmenter l'efficacité
- Augmenter la sécurité et la confidentialité des données
- Assurer la durabilité, la portabilité et la viabilité des données

Les nœuds validateurs seront localisés dans les États membres et chez les partenaires commerciaux en dehors de l' Espace Economique Européen.

L'architecture modulaire de l'EBSI fournit :

- Une résilience accrue d'un réseau de systèmes et de données pouvant prendre le relais sur des nœuds défaillants et distribuer les preuves géographiquement
- Une confiance accrue grâce à l'utilisation de protocoles blockchain robustes, capables de passer à l'échelle et permettant le déploiement de contrats intelligents (smart-contracts)
- Une cyber sécurité améliorée grâce à l'application des pratiques de chiffrement
- Une amélioration des performances des systèmes transfrontaliers grâce à l'utilisation de système de stockage de données distribuées
- Des capacités à géométrie variable pouvant convenir à des États membres de taille différente ainsi que des applications locales ou transfrontalières.

En d'autres termes, l'EBSI est une infrastructure blockchain regroupant une véritable boîte à outils déployable à la demande.

Ce panel d'outils est d'ores et déjà disponible en version de test et à la disposition des administrations et du secteur public dans leurs projets de transformation digitale avec le but d'améliorer les services publics et la vie du citoyen.

2.7. Pourquoi en tant qu'administration, utiliser EBSI plutôt qu'une autre blockchain ?

Pour une entité du secteur public, il est légitime, dans le cas de figure où une opportunité blockchain est susceptible d'exister, quel que soit son niveau de maturité, de s'interroger sur la pertinence du choix de la blockchain EBSI. En quoi possède-t-elle la capacité de faciliter, accélérer un projet et d'en assurer la pérennité en tant qu'administration au service du citoyen ?

Ici, il convient d'évaluer, par rapport aux autres offres du marché, les caractéristiques de l'EBSI susceptibles d'offrir des avantages dans les différentes étapes de l'initiative Blockchain, de la réflexion initiale au déploiement :

- la mise à disposition d'une boîte à outils pour accélérer le développement et la mise en place d'une initiative blockchain ;
- l'interopérabilité progressive avec d'autres types de blockchain, qui viendra en soutien à la massification des transactions réalisées ;
- l'aide quant au choix des différents composants d'une blockchain, en particulier pour les couches 1 et 2 ; cette sélection étant de manière générale extrêmement chronophage et complexe pour un projet pris individuellement (benchmarks, compétences techniques nécessaires, etc.) ;
- la pérennité puisque les choix technologiques sont supportés par l'ensemble de la communauté et que celle-ci est le garant de la continuité et de la compatibilité dans le temps des différentes versions ;
- la gouvernance qui, comme l'écosystème, est au cœur de toute initiative blockchain et qui va pouvoir directement bénéficier de l'offre l'ESBI en particulier pour les couches 1 et 2 ;
- l'offre clé en main pour l'infrastructure de réseau (couche 2) puisque chaque projet blockchain se heurte ici à un choix difficile : soit dépendre étroitement des choix des fournisseurs/opérateurs de l'infrastructure (sécurité, réseau, etc.) soit avoir la responsabilité de gérer ces problèmes complexes et nécessitant des compétences encore rares.

Sur tous ces points, l'EBSI fournit une réponse simple et flexible et répondant directement, par construction, aux exigences du secteur public en termes d'ouverture, de pérennité et d'indépendance.

3. Utilisation pratique de la blockchain pour l'amélioration du service public

La blockchain a pu être perçue comme une technologie innovante avec un fort potentiel de transformation, voire à vocation disruptive, qu'une organisation se devrait absolument de tester au risque de rater le dernier phénomène à la mode. Ce qui explique que de nombreux projets pilotes, jusqu'à ces toutes dernières années, ont été lancés alors que l'utilisation de cette technologie ne se révélait ni indispensable ni même justifiée.

En appliquant cette approche, la blockchain est une solution qui rechercherait un problème à résoudre. Or, partir de la technologie et non pas du problème métier est un exercice particulièrement inefficace d'un point de vue utilisateur. C'est aussi une cause classique d'échec de projet de transformation numérique des organisations.

**Nous proposons ici d'appliquer une démarche inverse :
"J'ai identifié un problème existant ou un besoin
nouveau, je recherche quelles technologies sont les plus
à même de les satisfaire".**

3.1. Éléments fondamentaux de mise en place d'un projet blockchain au sein du secteur public

La blockchain, comme toute autre technologie, n'échappe pas aux fondamentaux de gestion d'un projet de transformation numérique.

Cependant, à l'inverse d'un projet traditionnel le plus souvent centré sur une vision "interne à une organisation", la blockchain nécessite systématiquement une approche très collaborative, tenant compte des parties prenantes et des différents systèmes d'information entrant en jeu.

En d'autres termes, la technologie blockchain, c'est faire le choix d'un sport d'équipe.

- le sport c'est la « blockchain ».
- l'équipe, ce sont les parties prenantes qui constitueront l'écosystème.

Le but du jeu, c'est de créer de la valeur ajoutée en dynamisant une problématique commune et en tirant à travers ces synergies des bénéfices clairs pour chacune des parties prenantes.

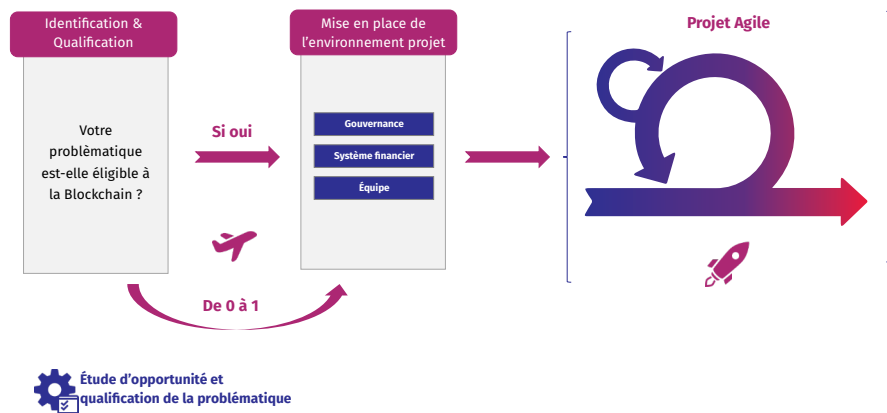
Ce « but du jeu » va prendre différentes formes en fonction de la problématique.

Il peut se traduire par de l'amélioration de service public existant comme le passage d'une procédure papier s'appuyant sur un écosystème complexe (par exemple : la procédure de droit d'asile ou l'e-apostille) à de nouveaux services aux usagers comme la mise en place actuelle d'un véritable service public du C.V. , moteur de l'engagement de Blockchain Education France au sein de l'EBSI.

Dans ce contexte, il est important que la mise en place d'un projet blockchain, dès lors que la problématique a été identifiée et qualifiée, puisse se réaliser au sein d'un environnement de projet permettant l'intégration des parties prenantes.

De plus, un projet blockchain s'accompagne de la mise en place d'une gouvernance bien précise. Cela permettra le bon déroulement de celui-ci tant dans la définition des rôles de chaque partie prenante (qui fait quoi et apporte quoi ?) que dans le maintien de l'infrastructure globale (qui paye quoi ?) sur le long terme.

La mise en place d'un environnement projet adéquat est fondamentale à la bonne communication et collaboration entre toutes les parties prenantes amenées à travailler ensemble sur le réseau distribué.



Source : KAPALT

La phase de 0 à 1 illustrée ci-dessus est particulièrement importante afin de bien comprendre pourquoi la blockchain présente un intérêt (ou non). Cette phase permettra également de tester et présenter le projet aux parties prenantes qui sont indispensables à la réalisation du projet.

Trois types de projets blockchain sont imaginables :

A) La problématique relève à 100% du service public et est gérée par un écosystème d'administrations

Il s'agit d'ouvrir les silos d'informations afin de permettre une meilleure réconciliation et collaboration des différentes procédures au sein des administrations.

Bien entendu, la confiance au sein de l'écosystème est implicite, forte du fait de la connaissance des parties prenantes entre elles et leur appartenance commune au secteur public. Dans ce cas, une infrastructure blockchain contribuera à atteindre une excellence opérationnelle de bout en bout.

Dans ce cas de figure, la complexité de l'écosystème devra être examinée avec soin afin de justifier l'utilisation de ce type de technologie. Il est tout à fait possible, puisque la confiance entre les parties est assurée de fait, que d'autres technologies répondent également à la problématique.

B) La problématique touche un service public dont la responsabilité relève de l'État contractuant avec une structure privée

La structure privée peut être à but lucratif ou non (exemple : le système de santé, l'éducation, etc.).

Dans ce cas de figure, l'État propose une infrastructure et un environnement de projet qui permet de créer un niveau de confiance tout en améliorant la collaboration et la traçabilité.

La confiance étant moindre que dans le cas précédant étant donné un écosystème plus complexe, une infrastructure blockchain est vraisemblablement plus légitime comparativement à une autre technologie.

Ici, les administrations jouent un rôle majeur dans l'écosystème et permettent le déploiement d'une infrastructure et d'outils à destination des autres parties prenantes.

C) La demande est étatique mais l'information provient en tout ou partie du secteur privé

Il s'agit ici des cas où l'État souhaite améliorer la traçabilité et l'efficacité de ses services en collaborant mieux avec le secteur privé tout en préservant le degré de liberté et de responsabilité de l'écosystème privé.

Exemples : le suivi des transactions ou des factures à des fins de TVA (avec à la clé la limitation de la fraude à la TVA), le suivi des procédures de remboursement par la sécurité sociale (réduction de la fraude également).

Dans ces contextes, la blockchain (le registre distribué) se verra jouer un rôle fédérateur autour d'une infrastructure commune et partagée, permettant la standardisation des procédures en représentant une complémentarité aux plateformes de l'État.

De plus, il est important de rappeler que la blockchain s'inscrit dans une logique de partage de l'infrastructure, permettant à chaque partie prenante de garder ces responsabilités et ces règles, tout en donnant un niveau de transparence et d'accessibilité (sur un principe équivalent à celui du « besoin d'en savoir ») sur la procédure en question aux autres parties prenantes.

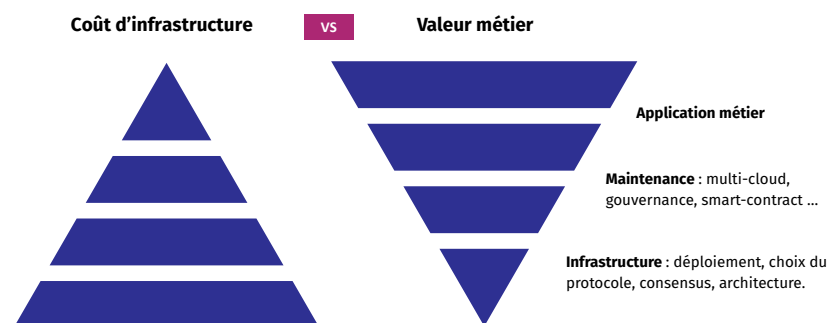
Dans cette logique d'écosystème, de maintien de l'infrastructure blockchain et de décentralisation minimum, il est très probable que les administrations devront s'appuyer et s'associer à des entreprises françaises dont l'État est aujourd'hui actionnaire (par exemple : IN Groupe, Orange, La Poste, EDF, Thalès, Engie...). Cette collaboration est nécessaire afin de permettre de rassembler les compétences pour le déploiement des infrastructures blockchain.

En effet, alors que la valeur est portée par l'application métier, la majorité des coûts réside dans l'infrastructure blockchain elle-même. Cela explique, dans une certaine mesure, les freins ou les réticences rencontrées actuellement pour l'adoption de ces technologies blockchain. Répondre à cette problématique est bien l'objectif même du projet EBSI.

Une des clés de la réussite de la mise en œuvre de l'EBSI ou de toute infrastructure blockchain réside dans la capacité à s'appuyer sur une filière blockchain française et européenne forte rassemblant un grand nombre d'entreprises et de compétences prêtes à soutenir et accompagner les administrations dans cette transformation et également l'EBSI elle-même dans son passage en production.

► **La valeur réside dans l'application métier...et la majorité des coûts dans l'infrastructure**

Cela explique dans une certaine mesure les freins actuels à l'adoption de la technologie blockchain



Source : KAPALT

3.2. Les sept cas d'usage présélectionnés par l'EBSI avec des projets en cours

1) Identité auto-souveraine

Elle représente un pont vers la technologie mise en place par la réglementation eIDAS au sein de l'infrastructure européenne connectée CFE.

Ce cas d'usage est particulièrement transverse à l'ensemble des autres cas d'usage. Il est d'autant plus stratégique pour les États puisqu'il s'agit de préserver la souveraineté des individus via leurs identités et donc l'accessibilité à une identité sécurisée et de qualité. L'Identité auto-souveraine est une nouvelle approche pour stocker, gérer, contrôler et partager des données en rapport avec des individus, des organisations ou des objets.

Cette approche, qui se situe aujourd'hui entre la recherche, le développement et quelques mises en production à venir prochainement, a le potentiel de créer une valeur significative dans différents secteurs de l'économie.

Les possibilités d'utilisation dans le secteur public sont très nombreuses. Les cas suivants ont été identifiés comme étant susceptibles de couvrir le plus grand nombre d'États membres :

- la facilitation de l'accès aux services d'administration en ligne ;
- la demande d'asile ;
- la numérisation des diplômes ;
- la numérisation des papiers d'identité (Passeport, carte d'identité ...) ;
- les prescriptions de médicaments en lien avec les systèmes de sécurité sociale existants ;
- les licences publiques et autres documents publics (permis de conduire, carte grise ...) ;
- les transports publics et transferts sociaux (retraite, invalidité, maternité...).

Au-delà de ces cas d'utilisation ambitieux, c'est bien une opportunité formidable pour nos démocraties européennes de replacer le citoyen au centre de la perspective en lui redonnant le contrôle sur ses données.

Dans ce contexte, plusieurs projets d'implémentation d'identité auto-souveraine ont émergé. Ces projets sont en grande majorité open source permettant un développement à la fois de haute qualité et s'appuyant sur un écosystème riche.

En Europe, des initiatives similaires à Alastria en Espagne, dont l'une des briques cœur du projet est l'identité auto-souveraine, devraient voir le jour en 2021. On peut citer aussi les travaux d'AgdataHub en France pour des identités auto-souveraines à destination du monde agricole (individus, entreprises, objets) qui nécessitent une interconnexion avec le régalien en matière d'identité civile.

Agdatahub : <https://agdatahub.eu>

ESSIF :

La Commission Européenne travaille également à l'élaboration d'une solution de Référentiel de l'Identité Auto-Souveraine Européen, le projet ESSIF (European Self-Sovereign Identity Framework ¹⁴). L'objectif est de déployer l'ESSIF en l'alignant avec l'EBSI de sorte qu'il existe une identification utilisable, soutenue par une plateforme (un hub) d'identifiants personnels stockés en conformité avec le Règlement Général sur la Protection des Données Personnelles ¹⁵.

Il est fondamental de rappeler que le projet ESSIF ne prend en aucun cas le contrôle sur les identités des citoyens au niveau européen, mais propose un cadre et une implémentation via une boîte à outils paramétrable en fonction du contexte d'utilisation dans le pays concerné.

La norme et les fonctionnalités proposées via l'ESSIF et l'EBSI permettent aux administrations, si elles le souhaitent, de tirer parti d'une véritable brique technologique des identités numériques fortes à destination du citoyen.

¹⁴ <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505734>

¹⁵ <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=262505360>

2) Notarisation

Ce cas d'usage décrit en réalité l'une des technologies de base utilisées au sein d'une solution blockchain. Cette technologie, ou devrions-nous dire ce concept, qui ne date pas de la blockchain, réside dans l'utilisation des « fonctions de hash » en cryptographie.

Un « hash » en informatique permet de générer une empreinte cryptographique unique à une donnée numérique (un pdf, un livre, un nom, une adresse, un contrat, etc.). Cette méthode informatique est plus communément appelée, notarisation.

Dans ce sens, le cas d'usage « Notarisation » vise à démontrer que dans bien des cas, cette seule fonctionnalité, nativement incluse dans le design d'une infrastructure de registre distribué permettrait de résoudre de nombreux problèmes liés aux erreurs relatives à l'état et la véracité probante d'une procédure multipartite.

Une infrastructure blockchain (par exemple l'EBSI) permettrait donc, via cette méthode de notarisation, l'enregistrement de l'identité numérique des documents ou de l'état de la procédure à l'instant T au sein du registre distribué, créant mécaniquement une liaison entre les données et une historisation de celle-ci.

Cette notarisation serait, dans le cas de la blockchain EBSI, liée à une délégation de pouvoir d'écriture sur ce registre à l'administration ou à l'entité concernée. Elle permettrait donc de réconcilier des procédures entières sur une même infrastructure permettant les actions suivantes :

- Enregistrer des documents numériques ;
- Vérifier leur authenticité ;
- Créer un historique sécurisé et horodaté des données ;
- Relier les empreintes numériques de fichiers et leurs métadonnées ;
- Échanger des empreintes numériques de données avec des tiers de manière conforme au RGPD.

Cette fonctionnalité de la blockchain est ici mise à profit pour créer des pistes d'audit numériques fiables et probantes, permettant d'automatiser les contrôles de conformité et prouver l'intégrité des données.

3) Diplômes et certificats vérifiables

Le cas d'usage des diplômes numériques, sélectionné dans le cadre de l'EBSI, vise à poser les bases d'une plateforme européenne de gestion des "digital credentials" : attestation de réussite au diplôme, open badges et autres titres de compétences, infalsifiables, vérifiables et consultables en ligne.

L'utilisation d'une technologie de registre distribué et de règles transparentes a pour but de créer de la confiance dans l'authenticité des diplômes (lutte contre la fraude), mais également de réduire le temps et les coûts de vérification, la gestion et l'archivage de ces documents. La technologie d'identité auto-souveraine permettra de placer le citoyen, le diplômé, au cœur du dispositif, en le rendant propriétaire et responsable de l'utilisation de son titre numérique.

La feuille de route du cas d'usage « Diplôme » d'EBSI vise à rendre disponible un ensemble cohérent de services pour les personnes, les institutions d'enseignement, les entreprises et les recruteurs.

Le modèle de données permettant aux universités, organismes de formation et entreprises d'émettre des diplômes et attestations est basé sur les standards internationaux tels qu'implémentés dans Europass, mis en place par le projet d'infrastructure des identifiants numériques (EDCI) de la Commission européenne. Il s'agit d'un ensemble de services centralisés permettant la délivrance de justificatifs numériques et leur utilisation via un système de portfolio ou CV en ligne dans 29 langues. Europass et l'EBSI ont vocation à pouvoir être utilisés simultanément pour créer un écosystème complet.

4) Partage sécurisé de données

Afin de promouvoir la coopération transfrontalière et de fournir un accès facile aux informations réglementées des institutions publiques / privées sur les marchés réglementés de l'Union européenne, l'EBSI propose une plateforme qui offre la possibilité d'accéder à une vue unique des informations actuellement stockées dans différentes administrations des États membres. Ces informations sont accessibles sur autorisation basée sur le concept du « besoin d'en connaître ».

La plateforme de partage de donnée sécurisée « Trusted data shared » (TDS) se fonde sur une nouvelle approche pour construire un système distribué et décentralisé en interconnectant les entités publiques / privées de tous les États membres dans une plateforme dédiée. Cela évite d'échanger ces données et offre à la fois une traçabilité complète et une gestion de la propriété tout au long du cycle de vie des données.

L'objectif de TDS consiste à développer une infrastructure de type blockchain, permettant techniquement aux entités des États membres de partager des données de manière publique ou privée et d'en vérifier la validité, la propriété et /ou l'authenticité.

Cette infrastructure de partage de données de confiance (TDS) cible des groupes spécifiques d'entités des États membres ayant besoin de partager des données sur une plateforme sécurisée et fiable, conforme au RGPD, sans utiliser d'intermédiaire.

L'EBSI permet une mise en œuvre de ce cas d'usage grâce à une infrastructure modulable.

5) Émission d'obligations pour les PME pour la reprise post-CoVid19

Au travers de ce cas d'usage, l'EBSI veut permettre l'émergence de plateformes à l'échelle de l'Union Européenne pour le financement des petites et moyennes entreprises, soit par emprunt ou pour le capital. L'objectif est de libérer et cibler l'épargne et les politiques d'investissement vers du co-financement dans le domaine de l'économie durable, de l'innovation et de la modernisation des PME/ETI. La (ou les) plateforme(s) publique(s) déployée(s) au niveau des États membres, dont la colonne vertébrale sera l'EBSI, permettra (ont) d'offrir des services fournis, non pas par une administration, mais directement par un ensemble d'entités privées et publiques fédérées autour de cette infrastructure.

Ce cas d'usage a pour objectif de faciliter le flux de financements privés des propriétaires de capitaux vers les PME ou les projets verts.

6) Numéro de sécurité sociale européen (ESSIN)

Ce cas d'usage ambitieux devrait permettre à terme la portabilité des droits d'un citoyen européen entre les différents États membres.

Il vise à homogénéiser le partage de données afin de prévenir la fraude, les erreurs et les duplications d'identité complexes à gérer. Ce type de solution permettra d'assurer une communication, un échange de données plus facile et plus sécurisé et fluides entre les pays européens et leurs administrations.

L'ESSIN sera un processus mis en œuvre par les autorités publiques fournissant des services de protection sociale pour analyser en toute sécurité les données des citoyens de l'UE et garantir un niveau de service uniforme.

Sur ce sujet, certains pays sont plus avancés que d'autres. Il sera donc intéressant de comparer les approches faites dans chaque pays sur le thème. Au-delà de la vision à long terme, de nombreuses implémentations entre administrations au sein d'un même pays afin de tester la solution EBSI sont envisageables.

Ce cas d'utilisation est en lien étroit avec les cas d'usage identité auto-souveraine et le partage sécurisé de données.

7) Demande de droit d'asile

Ce cas d'utilisation visera à étendre la portée de l'EBSI à un large éventail de processus du secteur public. Il facilitera la gestion des processus transfrontaliers et inter-autorités. Avec pour première problématique, la procédure de traitement des demandeurs d'asile.

Cette problématique dont l'écosystème de parties prenantes est complexe et humainement sensible, pourrait trouver au travers de l'EBSI une solution d'infrastructure fédératrice pour propager en toute sécurité les mises à jour des procédures entre les autorités compétentes en matière d'asile.

Ce cas d'utilisation est en lien étroit avec les cas d'usage identité auto-souveraine et le partage sécurisé de données.

4. Fiches descriptives de cas d'utilisation

>>> Le Projet FR-EBSI

Point de contacts :

DINUM & Université de Lille :

*Perrine de Coëtlogon
Responsable EBP - EBSI
France*

Email: perrine.de-coetlogon@univ-lille.fr

Renater : Anthony Fisson
Responsable Infrastructure
et systèmes chez RENATER

BCdiploma :
*Luc Jarry-Lacombe
Co-founder & CEO
Email: luc.jarry-lacombe@bcdiploma.com*

Maturité du projet: Pilot



Le contexte:

Le projet Fr.EBSI vise à mettre en œuvre, dans le cadre du partenariat européen Blockchain (EBP) signé par la France le 10 avril 2018, une première expérimentation du cas d'usage «Diplôme» sur le service européen de la blockchain Infrastructure (EBSI). Ce projet est à ce jour soutenu par le Ministère de l'Éducation Nationale, de la Jeunesse et des Sports.

L'objectif de Fr.EBSI est d'expérimenter, au sein des institutions partenaires du projet (Université de Lille, France Education International, CRI Paris, emlyon business school, Réseau Canopé), un service d'émission et de gestion de certificats numériques émis sur l'infrastructure EBSI à l'aide de la plateforme BCdiploma :

- délivrance de certificats numériques vérifiables au format « Verifiable Credential » W3C/EDCI,
- mise en place d'identifiants d'identité décentralisés liés aux *credentials*,
- étude des implications juridiques, réglementaires et organisationnelles découlant de l'usage de ces briques technologiques.

L'écosystème (à date):

Le projet Fr.EBSI s'articule autour d'un écosystème de partenaires accrédités par la France et dont l'exécution est confiée à ce consortium de 3 partenaires :



RENATER étant le Réseau National de la Recherche et de l'Éducation qui assurera la maintenance et le test des nœuds EBSI dans le cadre de sa mission d'innovation et avec ses partenaires européens, GRnet, Belnet et Redriss, tous membres du réseau paneuropéen GEANT.



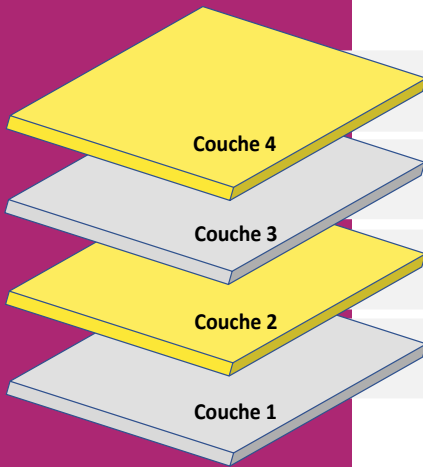
BCdiploma, société française spécialiste des blockchain digital credentials, fournit une plateforme clé en main permettant aux institutions d'émettre des certificats numériques infalsifiables, pérennes et vérifiables, en utilisant une technologie blockchain brevetée, dont la mise en œuvre permet aux Institutions de respecter le règlement général sur la protection des données (RGPD). Le projet Fr.EBSI permettra de déployer la solution BCdiploma sur le Blockchain Services Infrastructure (EBSI) pour un certain nombre de cas d'utilisation, dont celui des diplômes numériques et les certificats, mais aussi sur le cas d'utilisation de l'identité auto-souveraine et de la notarisation. Grâce à son expérience dans l'usage de différents protocoles et infrastructures distribuées, BCdiploma a également été choisi afin de déployer un nœud EBSI.



L'Université de Lille (ULille) coordonnera le projet et sa diffusion, avec un fort soutien de l'AMUE (en charge du développement du logiciel scolaire partagé à l'échelle nationale), RENATER et le Crous, titulaire du projet European Student Card et My Academic ID. L'Université de Lille va documenter de manière indépendante toutes les expériences grâce au financement d'un coordinateur scientifique.

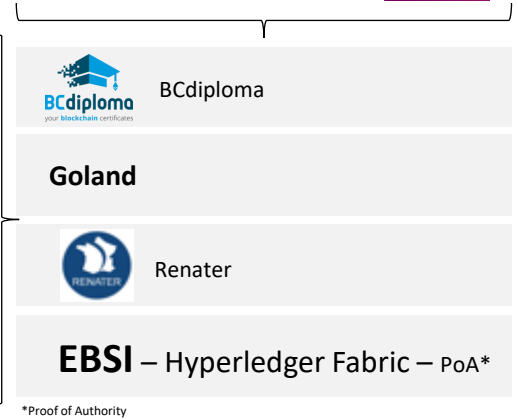
>>> Le Projet FR-EBSI

Une vue aérienne de la solution par couches:



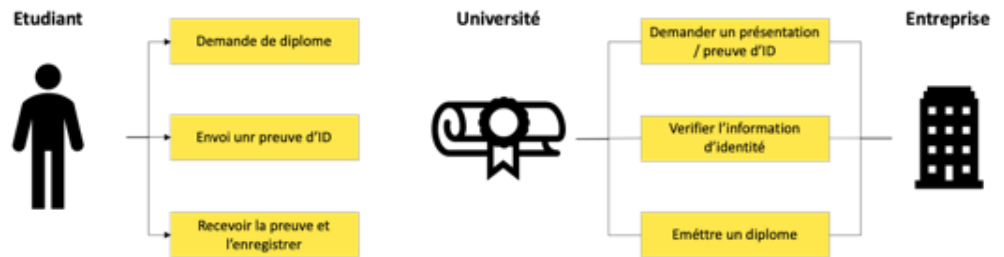
4. Intégration avec d'autres applications ou autres sources de données
3. Développement des smart contracts, des règles métier et des applications destinées à l'utilisateur final
2. Déploiement de l'infrastructure, du réseau et des nœuds
1. Protocole, consensus de validation et registre des transactions

FR-EBSI



Attention, il est important de comprendre sur ce schéma d'architecture ci-dessus que les couches 1 à 3 représentent l'infrastructure. Celle-ci sera à terme disponible à d'autres applications métiers et d'autres opérateurs de services, dès lors qu'ils respecteront les réglementations Européennes et la gouvernance de l'infrastructure EBSI sous-jacente.

Cela permettra aux étudiants, universités et entreprises de réaliser les actions suivantes:



Les trois partenaires présenteront une plateforme opérationnelle connectée à EBSI qui pourra être testée par toute institution émettant des diplômes, titres de compétences ou attestations officielles. L'enjeu de Fr.EBSI est de promouvoir un modèle distribué permettant une bonne fluidité des échanges entre les systèmes d'information centralisés des ministères et ceux des établissements d'enseignement supérieur. Cela permettra aux établissements de garder un certain niveau d'autonomie dans leurs procédures, tout en les harmonisant au niveau national et européen.

Grâce à l'utilisation d'EBSI et du standard international W3C Verifiable Credential, Fr.EBSI créera un lien concret entre les partenaires européens, le projet EDCI et les partenaires internationaux membres du Digital Credentials Consortium et du W3C (MIT Media Lab, Harvard, Toronto, Monterrey, TU Munich, TU Delft ...).

>>> Le Projet d'identité des exploitations agricoles

Point de contacts:

Orange Business Services:
Antoine Maisonneuve

Agdatahub:
Sébastien Picardat

Maturité du projet: Proof of Concept

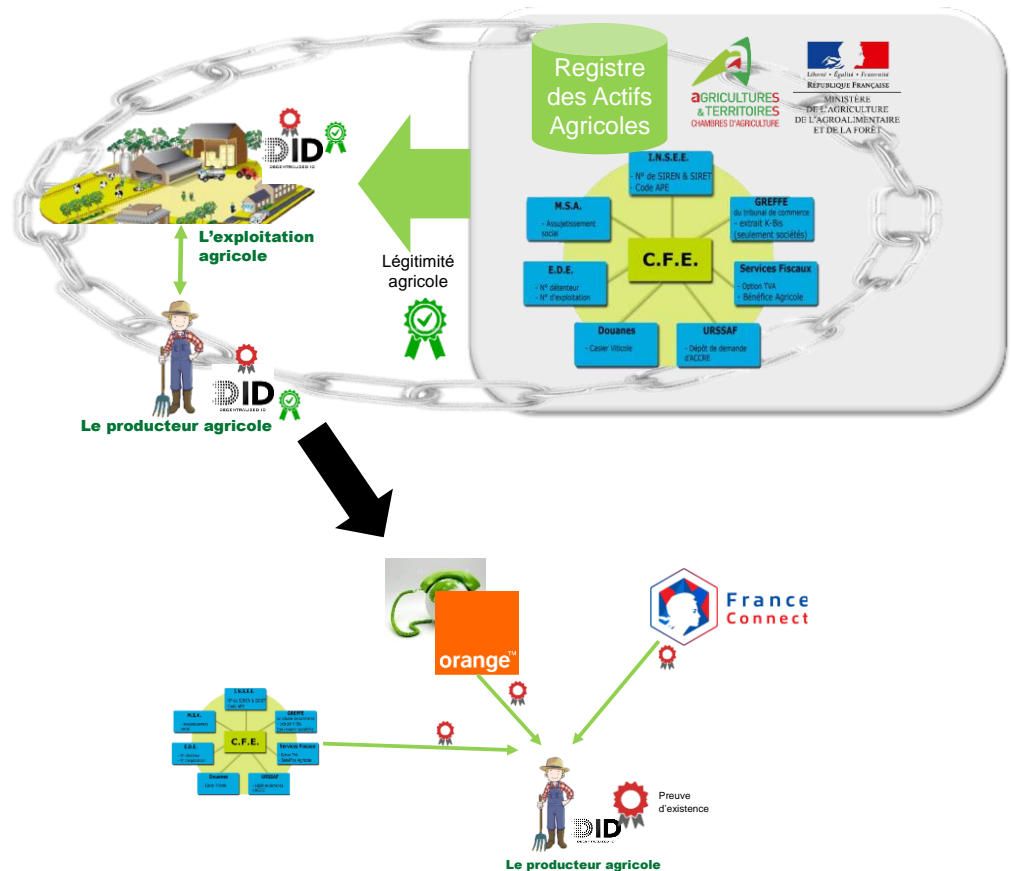


Le contexte:

API-Agro, une SAS créée fin 2017 par 30 associés publics et privés pour rassembler une communauté ouverte d'utilisateurs afin d'opérer une plateforme d'échanges de données agricoles, avec le soutien initial du Ministère de l'Agriculture et de l'Alimentation. API-Agro est depuis 2020 la holding agricole de la société Agdatahub, dont la Banque des Territoires est également actionnaire.

La raison d'être de ce projet: « Doter l'agriculture française et européenne d'une infrastructure souveraine et mutualisée de consentement, d'hébergement, de standardisation et d'échanges de données issues des exploitations agricoles et des opérateurs de l'amont agricole visant à alimenter les modèles d'Intelligence Artificielle et les nouveaux services utiles aux producteurs agricoles et aux consommateurs français. »

En 2020, la société Agdatahub, en partenariat avec Orange Business Services, décide de lancer un projet de co-innovation sur la thématique de l'identité auto-souveraine. Ce projet a pour ambition de proposer une identité auto-souveraine aux 450 000 exploitations agricoles françaises. L'objectif du projet est d'associer cette identité des agriculteurs (personnes physiques) avec les exploitations (personnes morales) afin de répondre aux besoins de protection et d'échange des données au sein des filières agricoles et agroalimentaires.



Source: <http://www.justice.gouv.fr/europe-et-international-10045/cinquantenaire-de-la-convention-de-la-haye-du-5-octobre-1961-22935.html>

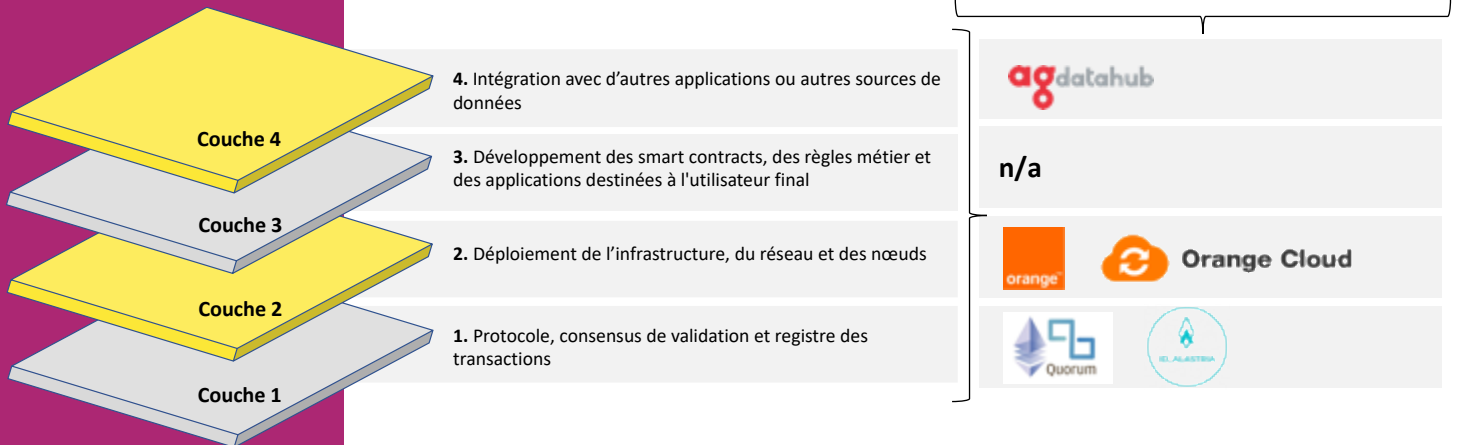
>>> Le Projet d'identité des exploitations agricoles

L'écosystème (à date):

Le projet rassemble actuellement une grande partie de l'écosystème agricole



Une vue aérienne de la solution par couches à date:



Attention, il est important de comprendre sur le schéma d'architecture ci-dessus que les couches 1 à 3 représentent l'infrastructure. Celle-ci n'utilise pas à date l'infrastructure EBSI mais s'oriente vers une interopérabilité avec l'EBSI.

La couche 2 n'est pas l'exclusivité d'Orange Business Service et d'autres fournisseurs de Cloud seront à terme du projet inviter à proposer d'héberger des nœuds et permettre une décentralisation plus complète de l'architecture.

>>> Le Projet de l'e-apostille

Point de contacts:

DINUM & Université de Lille :

Perrine de Coëtlogon
Responsable EBP - EBSI
France
perrine.de-coetlogon@univ-lille.fr

Davron Digital:

Anne-Cécile Bourget-Davron
Directrice Générale
ac@davrontranslations.com

Maturité du projet: Proof of Concept



Le contexte:

En lien avec le cas d'utilisation notarisation, la procédure juridique de l'e-apostille est particulièrement intéressante et pertinente à l'application de la technologie Blockchain. L'e-apostille est une procédure juridique ayant pour objectif l'authentification, la portabilité et la reconnaissance d'actes publics ou privés au sein de différents systèmes administratifs.

Entrée en vigueur le 24 janvier 1965 suite à la ratification de la France, du Royaume-Uni et de l'ex-Yougoslavie, la Convention Apostille est, parmi toutes les conventions de Conférence de La Haye de droit international privé, celle qui compte le plus d'États contractants, au nombre de 120 actuellement. Avec plusieurs millions d'apostilles émises chaque année à travers le monde, c'est aussi la plus utilisée des conventions de La Haye⁽¹⁾.

Malgré une convention et un écosystème fort, l'apostille reste aujourd'hui très complexe et longue. En effet la réconciliation des procédures et les degrés de contrôle entre les administrations ne facilitent pas l'expérience au citoyen. De plus ces procédures sont aujourd'hui encore papier pour la plupart.

Dans ce contexte, la technologie blockchain permettrait de fluidifier la collaboration et améliorer la confiance / la traçabilité dans les documents contractuels, judiciaires ou administratifs (ex: jugement, Kbis, PV d'Ag d'entreprise etc) et en particulier dans le cas de l'e-apostille les données et documents d'état civil manipulés tout au long du cycle de vie de la procédure.

À date, Davron Digital, la filiale numérique de Davron Translations, a été à l'initiative d'une application métier inédite appelée popcorn permettant un processus d'e-apostille et d'e-légalisation de bout en bout avec toutes les chaînes des intervenants, grâce à la traçabilité blockchain. La première version de cette application est construite sur la blockchain Tezos.

Une deuxième approche serait d'intégrer l'application développée par Davron translations à l'infrastructure EBSI tout en développant un écosystème fort.

L'écosystème (à date):

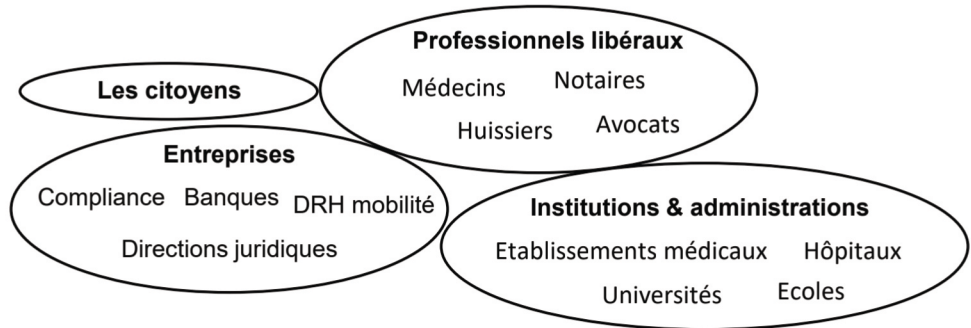
Le projet s'articule principalement autour de l'application développée par Davron Digital.

Afin d'améliorer l'e-apostille, Davron Translations cherche des partenaires au sein des administrations Françaises et Européennes afin de porter le sujet au niveau de l'infrastructure EBSI et légitimer le projet.

Un écosystème fort qui réunira notaires, traducteurs, ministères et consulats est à imaginer pour construire l'infrastructure de notarisation de demain.

Source: <http://www.justice.gouv.fr/europe-et-international-10045/cinquanteenaire-de-la-convention-de-la-haye-du-5-octobre-1961-22935.html>

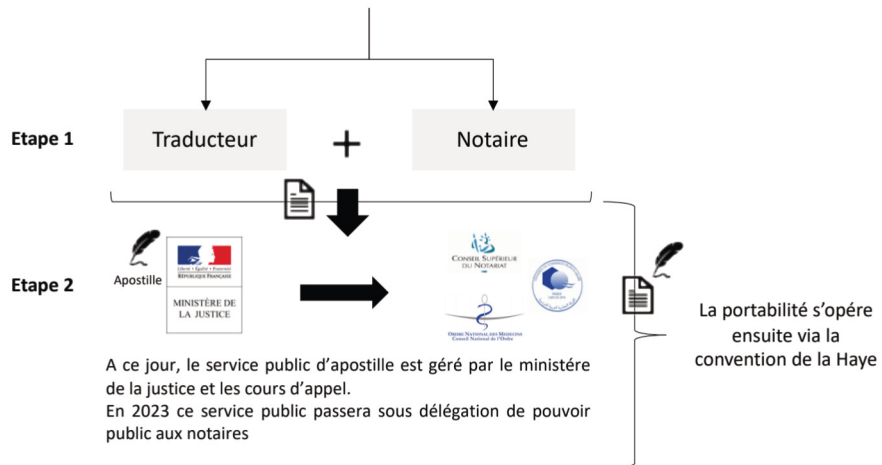
Utilisateurs des procédures E-apostille et E-légalisation (liste non exhaustive)



Identification des parties prenantes aux procédures d'e-apostille et e-légalisation

E-apostille

Une personne souhaite faire une e-apostille sur un certain nombre de documents (comme: passeport, carte d'identité, Kbis, Contrat de mariage, acte de naissance) afin d'assurer la portabilité de ces documents d'un pays à un autre.



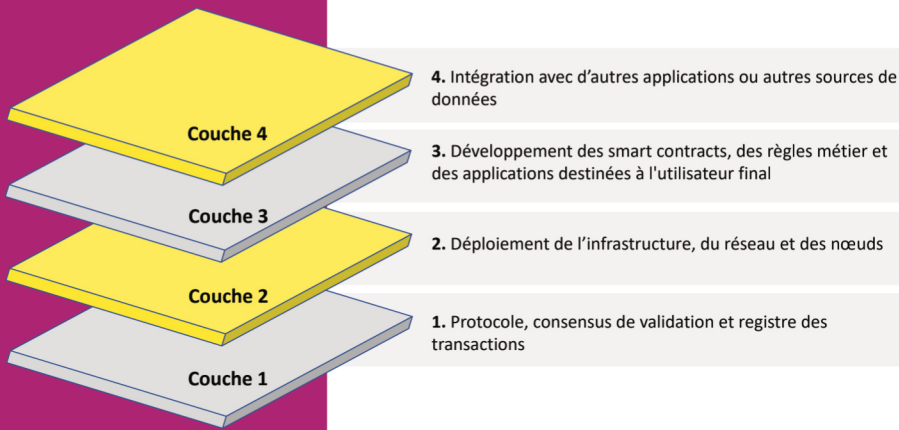
E-légalisation

Dans le cas où la portabilité vers un pays qui n'est pas signataire de la convention de la Haye. Une autre procédure dite de légalisation s'applique via le Ministère des affaires étrangères et les consulats.



Source: <http://www.justice.gouv.fr/europe-et-international-10045/cinquante-ans-de-la-convention-de-la-haye-du-5-octobre-1961-22935.html>

Une vue aérienne de la solution par couches à date:



Porteur du projet

Davron Digital	?
Davron Digital	Davron Digital
n/a	n/a
Installation d'un nœud Tezos	?
Tezos	EBSI

Attention, il est important de comprendre sur le schéma d'architecture ci-dessus que les couches 1 à 3 représentent l'infrastructure. Celle-ci sera à terme disponible à d'autres applications métiers dès lors qu'elles respecteront les réglementations Européennes et la gouvernance de l'infrastructure EBSI sous jacente.

Le porteur de projet est ici l'administration qui a la légitimité à valider et donner une valeur probante aux données provenant de ces procédures d'e-apostille et e-legalisation.

>>> Le Projet DID4ALL

Point de contacts :

IN Groupe

Olivier Dussutour

Jean-François Demeestere

Thomas Foutrein

Thibault Langlois-Berthelot

Maturité du projet :

Pilot



Le contexte :

Le projet DID4ALL vise à mettre en œuvre puis à garantir un système d'enregistrement, global, accessible, fiable et pérenne, du parcours de vie des enfants qui ne bénéficient pas d'une existence juridique dans leur pays. Selon UNICEF, cette inexistence légale concernerait 166 millions d'enfants dans le monde. Plus généralement et selon la Banque Mondiale, ce serait près d'un milliard de personnes dans le monde qui ne pourraient pas justifier d'une reconnaissance ou d'une identité légale.

L'objectif de DID4ALL est d'expérimenter, dans des pays en voie de développement, une solution digitale simple et efficace qui utilise trois technologies combinées – la reconnaissance vocale, la blockchain et les systèmes de télécommunication – afin de proposer à chaque enfant une preuve d'existence cryptographique, dématérialisée et légale tout au long de son enfance. Cette preuve d'existence peut ainsi être déployée facilement par UNICEF : elle ne dépend pas d'un accès à internet, elle est accessible par tous, même les personnes qui ne savent pas lire ou écrire, elle est fiable, car elle repose sur l'identification par la voix qui est un facteur d'authentification unique et, enfin, elle est sécurisée puisque les données sont stockées de façon distribuée puis horodatée sur une blockchain.

L'écosystème (à date) :

Le projet DID4ALL s'articule autour de deux partenaires reconnus et de confiance, respectivement, sur l'identité numérique et la sauvegarde des droits fondamentaux des personnes :



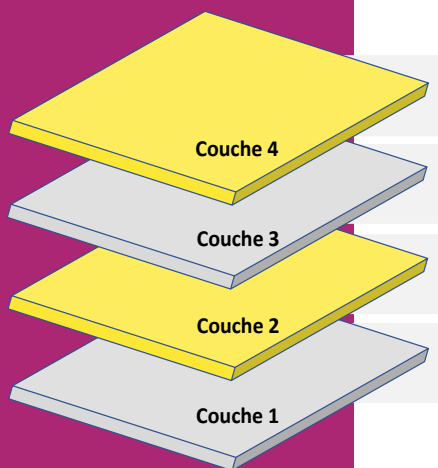
Partenaire de l'État français depuis près de 500 ans, **IN Groupe** (ex **Imprimerie Nationale**) propose des solutions d'identité et des services numériques sécurisés à la pointe de la technologie, intégrant électronique, optique et biométrie. Des composants aux services, en passant par les titres et les systèmes interopérables, en tant que spécialiste mondial de l'identité et des services numériques sécurisés, IN Groupe est présent au quotidien pour faciliter la vie de chacun. Accompagner les États dans l'exercice de leur souveraineté. Protéger l'identité des citoyens. Préserver l'intégrité des entreprises. Quel que soit l'enjeu, IN Groupe, entreprise de souveraineté numérique, contribue à faire valoir pour chacun un droit fondamental : le Droit d'être Soi. IN Groupe est la nouvelle marque du Groupe Imprimerie Nationale et anime la marque affiliée Nexus, experte en solutions d'identité numérique corporate et IoT.



UNICEF est une agence des Nations unies, créée en 1946. Elle est chargée, dans le monde entier, de défendre les droits des enfants, de répondre à leurs besoins essentiels et de favoriser leur plein épanouissement. UNICEF travaille dans les endroits les plus inhospitaliers du monde pour atteindre les enfants et les adolescents les plus défavorisés afin de défendre les droits de chaque enfant, où qu'il soit. Dans 190 pays et territoires, UNICEF met tout en œuvre pour aider les enfants à vivre, à s'épanouir et à réaliser leur potentiel, de la petite enfance à l'adolescence. UNICEF intervient également en cas d'urgence en coordination avec les organismes des Nations unies, les principales organisations humanitaires, et les gouvernements nationaux. Avant, pendant et après les urgences humanitaires, UNICEF est présent sur le terrain pour apporter une aide vitale et de l'espoir aux enfants et à leurs familles.

>>> Le Projet DID4ALL

Une vue aérienne de la solution par couches :



- **Application** utilisateur pour émettre et/ou gérer souverainement les justificatifs numériques de preuve d'existence
- **Utilisation** des standards du W3C (DID & VC)
- **Stockage** sur des serveurs distribués
- **Récolte** des attributs d'identité uniques de l'enfant/parents par reconnaissance vocale



DID4ALL permet de garantir à l'enfant une *preuve d'existence*, en lui offrant *in fine*, le droit d'être soi.

En s'appuyant sur des standards internationaux (*OSIA*, *W3C*), **IN Groupe** et **UNICEF France** ont répondu à une problématique jusque-là inexplorée : une identité numérique dans un contexte de faible connectivité, d'équipement technologiquement limité («*feature-phone*»), d'illettrisme et d'illectronisme. Ces travaux nous ont permis de mettre en œuvre ces standards en s'appuyant sur la blockchain, la biométrie vocale, la décentralisation des données et autres technologies de rupture.

Par conséquent, la réponse de DID4ALL est articulée autour de 4 piliers :

✓ **Accessibilité :**

- *fonctionnel en 100 % vocal (avec possibilité de modes dégradés) ;*
- *accent mis sur l'aisance de manipulation des identifiants ;*
- *flexibilité dans la gestion de l'identifiant.*

✓ **Interopérabilité :**

- *utilisation de standards open source ;*
- *standard OSIA ;*
- *standards W3C (DID & VC) ;*
- *utilisable par tous les services & pays compatibles.*

✓ **Résilience :**

- *stockage décentralisé sur IPFS ;*
- *gestion d'un registre d'état civil ;*
- *application décentralisée ;*
- *notarisation DLT sur Ethereum.*

✓ **GSM conforme :**

- *n'utilisant que le réseau téléphonique (GSM) ;*
- *« feature » phone ;*
- *interactions par appel et/ou SMS uniquement.*

>>> Le projet Blockchain des fréquences PMSE Audio

Point de contacts :

ANFR :
Cédric NOZET



Maturité du projet:

En production



Le contexte:

En capitalisant sur les résultats d'un PoC « Proof of Concept » réalisé dans le cadre d'un projet financé par la Programme des Investissements d'Avenir (PIA) en 2018, l'Agence Nationale de Fréquences (ANFR), accompagnée par un partenaire technique, a développé une solution permettant de coordonner l'utilisation de fréquences audio libres lors de grands évènements (tournois sportifs, salons professionnels, etc.) afin d'y éviter les brouillages.

Cette solution s'appuie sur une blockchain privée Ethereum stockant un registre des fréquences libres de droit utilisables en fonction de la localisation des évènements, un registre des évènements créés et un registre des fréquences déclarées utilisées pour chaque évènement.

Le recours à une blockchain répond au contexte d'autorégulation des bandes de fréquences libres et assure l'intégrité, l'auditabilité et la traçabilité des actions réalisées par les utilisateurs du service « Blockchain des fréquences ».

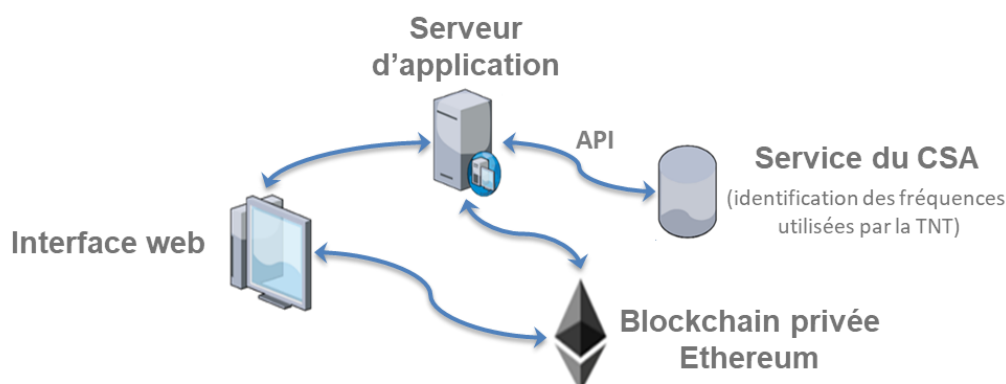
La maturité:

Des tests « grandeur nature » ont été réalisés en 2019 lors de plusieurs grands évènements sur lesquels l'ANFR intervient. Le lancement opérationnel du service était prévu en 2020 et a été reporté du fait de la situation sanitaire. Si le contexte y est plus favorable, la solution sera présentée courant 2021 aux principaux organisateurs de grands évènements avec lesquels l'ANFR interagit ainsi qu'aux principaux diffuseurs intervenant lors de ces grands évènements.

Le fonctionnement:

Un organisateur d'évènement enregistre la localisation et les dates d'un évènement via l'interface web mise à disposition par l'ANFR. Tout utilisateur de fréquences audio libres pendant cet évènement peut, au travers de la même interface web, identifier les fréquences libres et occupées (notamment celles de la TNT via un interfaçage avec un service du CSA), puis déclarer l'utilisation des fréquences dont il aura besoin.

L'architecture simplifiée:



Point de contacts :

CEA:
Sara TUCCI
Coordinatrice blockchain
du CEA List
Email:
Email: sara.tucci@cea.fr

Maturité du projet: Pilot



Le contexte

En 2018, le CEA-List crée un nouveau laboratoire entièrement dédié aux technologies distribuées pour la confiance, dont les *blockchains* ou registres distribués.

Ses équipes évaluent et proposent des algorithmes mis en œuvre au cœur des *blockchains*, qui garantissent la cohérence des données et leur inviolabilité ; étudient leurs propriétés, les problématiques de passage à l'échelle, d'« interopérabilité » (c'est-à-dire de compatibilité entre différentes *blockchains* associées), l'analyse et le contrôle des menaces; et accompagnent les acteurs industriels dans la mise en œuvre de solutions à base de *blockchain*, par exemple *via* la formalisation de *smart-contracts* dédiés et vérifiables.

Dès le premier jour, le laboratoire s'est immédiatement attaché à évaluer si les technologies *blockchain* pouvaient être moins gourmandes en énergie¹. Le « verdissement » des algorithmes de consensus, en particulier pour les *blockchain publiques*, est en effet une étape obligatoire dans le contexte actuel de la transition énergétique. Des *blockchains* efficaces sur le plan énergétique pourraient constituer un véritable tournant pour les applications futures.

La classe des *blockchains* basées sur la preuve d'enjeu (PoS l'acronyme en anglais) semble très prometteuse de ce point de vue. Bien que des études quantitatives sur la consommation globale d'une *blockchain* fonctionnant avec la PoS n'aient pas encore été réalisées, leur fonctionnement ne repose pas sur une course à la vitesse de calcul, mais sur des méthodes d'élection basées sur des crypto-actifs investis par les validateurs.

L'amélioration de ces classes d'algorithmes est donc un objectif majeur. Dans ce domaine, le laboratoire a déjà développé une évolution de l'algorithme de consensus de la *blockchain* Tezos, en collaboration avec Nomadic Labs. Cet algorithme appelé Tenderbake², est basé sur la PoS pour la sélection d'un comité de taille fixe, qui produit un bloc grâce à un algorithme collaboratif robuste aux attaques malveillantes. Tenderbake, par rapport à l'algorithme précédent, garantit que les transactions bénéficient d'un caractère définitif immédiat, qu'elles sont donc irrévocables. Avant ces travaux, le laboratoire avait déjà analysé l'algorithme Tendermint³, au cœur de la *blockchain* publique Cosmos. L'étude avait mis en évidence les principales vulnérabilités et proposé des correctifs, qui ont ensuite été intégrés dans le protocole public.

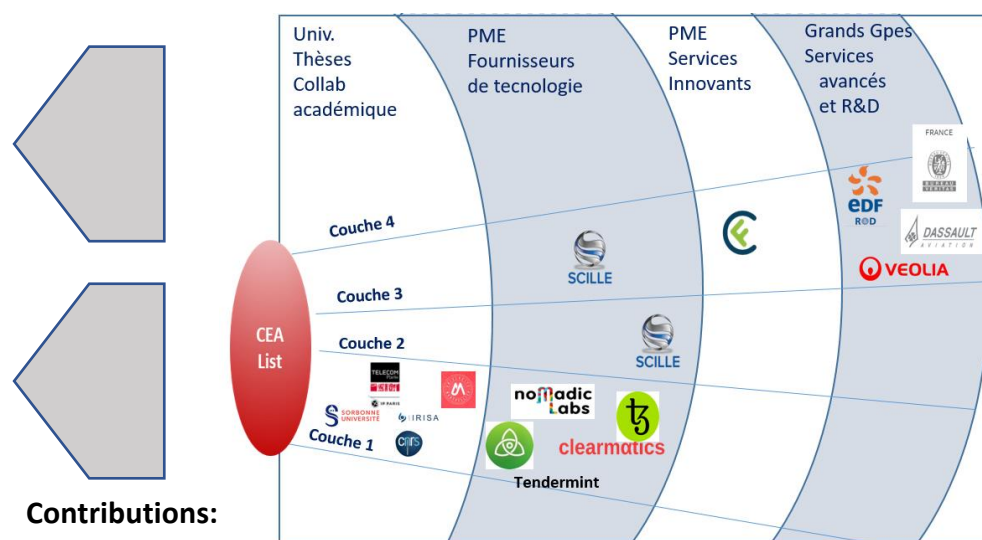
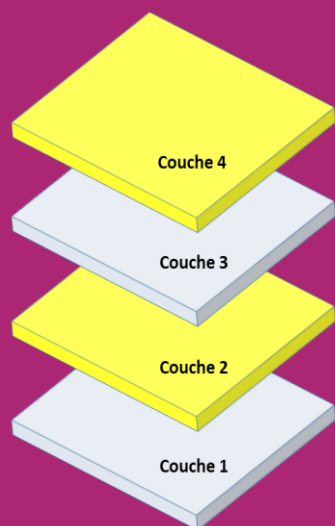
Bien que certains progrès aient été réalisés, il reste encore de nombreux défis à relever pour exploiter pleinement les propriétés de transparence et de certification que la *blockchain* peut apporter.

Le rapport de la mission numérique sur les verrous technologiques de la *blockchain*⁴, préparé par le CEA LIST en collaboration avec INRIA et IMT, met en lumière un grand nombre de ces défis, y compris le passage à l'échelle (des algorithmes et de l'exécution de *smart-contracts*), l'interopérabilité, la question de savoir comment créer des incitations efficaces pour garantir le bon fonctionnement de la *blockchain* dans la durée, et enfin la question de savoir comment assurer la confidentialité sans sacrifier la vérifiabilité des transactions et/ou des contrats intelligents. Des études comparatives sur la consommation d'énergie des blockchains à PoS devraient également être lancées.

Ces défis, toutefois, ne doivent pas nous effrayer, d'autant plus qu'il est déjà possible de faire beaucoup avec la technologie actuelle. A cet égard, nous pouvons mentionner l'application Live Audit de Connecting Food dédiée à la certification de produits dans le secteur alimentaire, dont le premier prototype a été conçu par le CEA LIST en 2017. Cette application est aujourd'hui commercialisée par Connecting Food. Fort de cette expérience, le CEA LIST travaille aujourd'hui à des services de traçabilité et audit dans des multiples domaines. Dans le secteur de l'énergie nous pouvons mentionner le service de transparence pour les contrats de performance énergétique avec Veolia⁵, ou encore la vérification des *smart contract* de certification de l'énergie verte, développées par la start-up TEO⁶.

Ces succès nous propulsent aujourd'hui vers des projets encore plus ambitieux, comme le passeport produit et la certification de l'empreinte carbone ou les places de marché des crédits carbone. Pour ces projets l'intégration entre l'IoT, la *blockchain* et l'IA sera clairement la clé de voute pour réussir.

Ecosystème du CEA List autour de la thématique « blockchains ».



Contributions:

Couche 1:

- Nouveaux protocoles pour des algorithmes de consensus non énergivores
- Evaluation énergétique de solutions blockchains

Couche 3:

- Conception d'une solution de passeport produit modélisation, métriques, simulation expérimentale.

1. <https://digiconomist.net/bitcoin-energy-consumption/>
2. Aştefanoaei, L., Chambart, P., Del Pozzo, A., Rieutord, T., Tate, E., Tucci, S., & Zălinescu, E. (2020). Tenderbake--A Solution to Dynamic Repeated Consensus for Blockchains. arXiv preprint arXiv:2001.11965
3. Amoussou-Guenou, Y., Del Pozzo, A., Potop-Butucaru, M., & Tucci-Piergiovanni, S. (2018). Correctness and fairness of tendermint-core blockchains. OPODIS 2018.
4. https://www.entreprises.gouv.fr/files/files/01-nouveau-portail/Evenements/numerique/presentation-bercy-mission-verrousbc-200210-fr_finale_3.pdf
5. Önder Gürcan, Marc Agenis-Nevers, Yves-Marie Batany, Mohamed Elmtiri, François Le Fèvre, Sara Tucci Piergiovanni: *An Industrial Prototype of Trusted Energy Performance Contracts Using Blockchain Technologies*. HPCC/SmartCity/DSS 2018: 1336-1343
6. <https://group.bureauveritas.com/newsroom/bureau-veritas-engie-and-cea-assure-traceability-green-energy-thanks-blockchain>
7. Sara Tucci Piergiovanni: - *Invited Paper: On the Characterization of Blockchain Consensus Under Incentives*. SSS 2019: 1-15

5. Synthèse

Une blockchain doit être considérée non pas comme une « simple » application mais bien comme une infrastructure visant à résoudre dans un écosystème de nombreuses problématiques métiers, notamment dans les domaines du partage de l'information et de la collaboration.

En utilisant un modèle de données partagé cohérent et un langage offrant la possibilité de modéliser des logiques métiers automatisés, elle autorise le déploiement d'un réseau intégrant un flux de travail multipartite qui valide et stocke les transactions (exemple : des événements sur une procédure administrative) de manière partagée. Elle permet la valorisation de ces données partagées, y compris des jeux de données ouverts par l'administration.

Elle apporte la capacité unique d'éliminer les différences ou écarts entre les structures de données et les interprétations de ces changements d'état. Ainsi, les technologies blockchain dont l'EBSI permettent de réduire voire d'éliminer à terme les « silos de données » traditionnels qui persistent depuis des décennies entre deux entités, ceci en toute transparence et sans besoin d'intermédiation.

Dans un contexte de transformation numérique encore trop souvent considérée dans une perspective purement interne à une organisation, une blockchain offre l'opportunité unique de construire un réseau homogène dont les buts sont de permettre le partage des données et des informations en toute confiance et d'offrir des améliorations significatives en termes d'excellence opérationnelle pour toutes les parties prenantes au service de l'utilisateur du service public.

À l'image de toute implémentation ou introduction d'une nouvelle technologie, la mise en place d'une blockchain est un exercice délicat qui nécessite la rencontre de différents impératifs, seule capable de conduire à une mise en œuvre réussie.

La recommandation méthodologique est de veiller à adopter une approche holistique en intégrant, le plus en amont possible, une vue d'ensemble de la problématique et d'éviter ainsi de ne considérer la blockchain que sous son angle technique.

Cet équilibre s'articule autour de 4 grandes thématiques toutes nécessaires au bon achèvement à terme d'un projet blockchain :

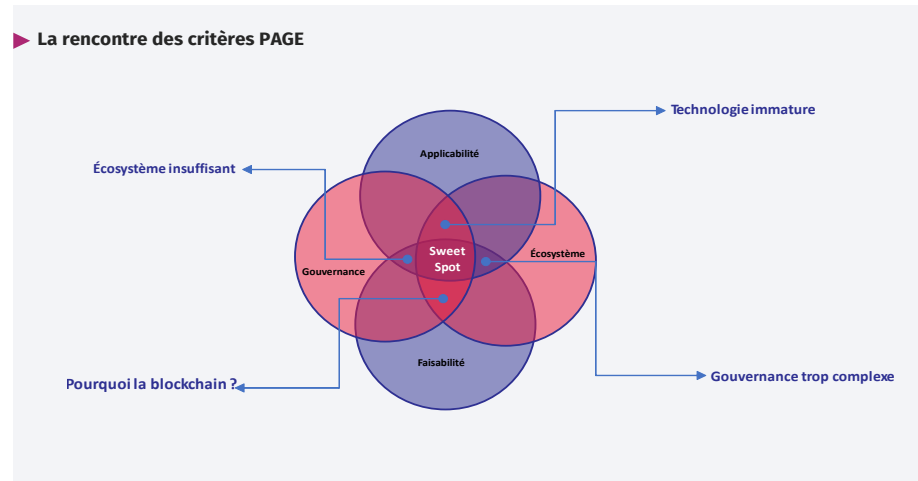
1/ L'applicabilité : Pourquoi utilise-t-on cette technologie ? Quels bénéfices précis en attendre ? Quelles caractéristiques sont nécessaires ?

2/ L'écosystème : Quels sont les environnements, les acteurs et leurs interactions nécessitant le déploiement d'une infrastructure partagée / décentralisée ?

3/ La gouvernance : Qui supporte quoi ? Qui a accès à quelle information ? Qui valide quoi ? Qui paye quoi ? Qui bénéficie de quoi ?

4/ La faisabilité : Quel protocole et quelle technologie utiliser ? Quels sont les niveaux de performance, sécurité, confidentialité à atteindre ? Quelle intégration avec l'existant ?

Quand ces quatre domaines trouvent un périmètre de convergence, alors les conditions nécessaires à la réussite d'une initiative blockchain sont vraisemblablement réunies.



Équipe

Perrine DE COETLOGON

Cheffe de projet blockchain & open education à la Direction de l'Innovation Pédagogique (Université de Lille), Perrine de Coëtlogon est le point contact français du Partenariat Européen de la Blockchain pour la Direction Interministérielle du Numérique. Elle est membre du board d'Open Education Global.

E-mail : perrine.de-coetlogon@univ-lille.fr

LinkedIn : <https://www.linkedin.com/in/perrine-de-coetlogon/>

Marc DURAND

Co-fondateur et responsable de la société Kapalt dédiée aux technologies blockchain, Marc Durand est spécialisé dans l'évaluation et la mise en œuvre opérationnelle des technologies innovantes.

E-mail : marc@kapalt.com

LinkedIn : <https://www.linkedin.com/in/marc--durand/>

Maxime JEANTET

Co-fondateur et consultant blockchain chez Kapalt, Maxime Jeantet accompagne les entreprises et organisations dans leurs réflexions blockchain (formation, étude d'écosystème, étude de faisabilité, gouvernance...).

E-mail : maxime@kapalt.com

LinkedIn : <https://www.linkedin.com/in/maxime-jeantet/>

Claire GÉNIN

Ingénieure-projets européens, Claire GÉNIN est spécialisée dans l'accompagnement des établissements supérieurs et de recherche à la mise en œuvre d'actions des programmes ERASMUS+ et HORIZON-EUROPE.

E-mail : claire.genin.pro@gmail.com

LinkedIn : <https://www.linkedin.com/in/clairegnin/>

Romuald RAMON

Spécialiste en design, communication et marketing (stratégie, création web, graphisme et réseaux sociaux), Il est également le co-fondateur du club de réseautage Rigolatis Commons.

E-mail : contact@romualdramon.com

LinkedIn : <https://www.linkedin.com/in/romualdramon/>

Pierre BOULET

Professeur d'informatique à l'Université de Lille, Pierre Boulet en est le vice-président à la transformation numérique. Il enseigne les systèmes distribués depuis plus de 20 ans et mène des recherches en parallélisme, architecture des ordinateurs génie logiciel et systèmes embarqués. Il fait partie du groupe technique du Partenariat Européen pour la Blockchain.

E-mail : pierre.boulet@univ-lille.fr

LinkedIn : <https://www.linkedin.com/in/pierreboulet/>

Remerciements

Claudio CIMELLI

Ministère de l'Éducation Nationale, de la Jeunesse et des Sports

Philippe CLÉMENT

Orange

Anne-Cécile DAVRON

Davron Translations

Olivier DUSSUTOUR

IN Groupe

Roland FAURE

Aérosureté

Luc JARRY-LACOMBE

BCdiploma

Laurent JOUBERT

Agence du Numérique en Santé

Thibault LANGLOIS-BERTHELOT

IN Groupe

Antoine MAISONNEUVE

Orange Business Services

Stéphane MOUY

SGM Consulting Services

Cédric NOZET

ANFR

Agnès LANUSSE

CEA List

Sara TUCCI-PIERGIOVANNI

CEA List

Franceline FORTERRE-CHAPARD

Ministère de l'Intérieur

Béatrice BERJON-SZATANIK

Ministère de l'Intérieur

Contact

Direction de l'Innovation Pédagogique
Campus cité scientifique
Avenue Paul Langevin
59655 Villeneuve-d'Ascq
FRANCE

