# BLOCKCHAINS : QUELLES COMPÉTENCES POUR RÉPONDRE AUX ENJEUX DE LA TRANSFORMATION NUMÉRIQUE ?

***Pasc@line*** *(www.assopascaline.fr) qui associe les établissements d'enseignement supérieurs et les entreprises du Numérique, a réalisé un travail important sur le développement des compétences des ingénieurs dans le secteur du Numérique.*

***La commission e-compétences*** *de Pasc@line a pour objectif de préparer l'avenir des entreprises et des établissements de formation afin de répondre aux besoins du marché en termes de compétences.*
*http://www.assopascaline.fr/650_p_33349/e-competences.html*

Depuis plus d'un an et demi, le phénomène « blockchain » est apparu sur la scène médiatique avec la promesse de changements considérables dans les rapports entre particuliers, États et organisations, à l'instar de ce qu'a pu représenter pour le monde l'arrivée d'Internet. Bien évidemment, ces nouvelles technologies ne sont pas exemptes de défis qu'ils soient économiques, socio-anthropologiques et juridiques en lien avec la gouvernance et le déploiement qu'elles nécessitent.
Ces challenges sont aussi d'incroyables opportunités à saisir pour tous ceux qui souhaitent participer à cet avènement qui pourrait remodeler le monde tel que nous le connaissons.

## DANS QUEL CONTEXTE PARLE-T-ON DE « BLOCKCHAINS » ?

Une blockchain est une structure de données chainées produites chronologiquement selon des amplitudes de temps et des règles de consensus définies dans un protocole. Les « blockchains » peuvent s'assimiler à des livres de comptes ou des registres numériques publics, répliqués et partagés entre utilisateurs et validateurs. Les informations qui transitent sur un réseau sont regroupées dans des « blocs » représentant chacun une page du livre. Les blocs sont automatiquement empilés de façon chronologique afin d'horodater les données dans leur ordre d'arrivée. Lors de la création d'un nouveau bloc, des validateurs sécurisent et verrouillent cryptographiquement les informations qu'il contient en incluant également la référence au bloc précédent. Ainsi, il devient quasiment impossible de falsifier un bloc sans modifier tous les autres blocs arrimés à la « chaîne ».

La blockchain est un support qui permet, si plusieurs critères se trouvent réunis, de créer une légitimité et donc de la confiance. Cette légitimité est intrinsèquement liée aux règles de son protocole, de son architecture, ainsi qu'à l'écosystème des acteurs. **Les « blockchains[1] » ne sont donc pas qu'une affaire de technologie, mais aussi de gouvernance, de psychologie et de sociologie**.

Chaque transaction, poussée et traitée au sein du réseau d'un protocole de registre distribué, se présente sous la forme d'un script appelé « Smart Contract ». Ce script est aussi appelé « Application Décentralisée » ou plus familièrement « Dapps » pour « Decentralized Applications ». Une « Dapp », sous sa forme la plus simple, permet l'échange d'unités de comptes, c'est-à-dire un transfert de valeur entre deux comptes. Il peut s'agir d'une cryptodevise comme par exemple le bitcoin.

[1] La « blockchain » est une métonymie. Dans le langage courant, le mot « blockchain » remplace le concept de protocole informatique par celui d'une de ses composantes (c'est à dire la technologie « blockchain »). Afin d'éviter tout amalgame, il est donc plus juste d'utiliser le terme de « Protocole de Registre Distribué » plutôt que celui de « blockchain ».

L'ajout de conditions permet de transformer une simple transaction en de nouvelles applications aussi appelées « Smart Contract ». Ces « smarts contracts » peuvent avoir une valeur légale et s'appliquer dans le cadre d'exécution de contrats commerciaux. Le « Smart Contract » complète l'utilisation première de la blockchain pour en faire de la certification, de la notarisation, du vote, de l'échange de titres, de parts sociales, d'obligations ou des agents autonomes.

En 2009, apparaît le protocole Bitcoin, hiérarchiquement dépendant d'Internet. C'est après quelques années et grâce à un effet de réseau inédit, qu'en 2011 le protocole Bitcoin permet, pour la première fois, la confiance dans le cyber-espace. Bitcoin marie des technologies existant pour la plupart depuis les années 70, comme la cryptographie à clé publique, les algorithmes de consensus, les modes d'opération cryptographique, l'architecture de réseau distribué en pair-à-pair, ainsi que la « blockchain». Ce qui différencie Bitcoin des autres protocoles de registres permissifs (qui existent depuis les années 60) est l'apparition du concept d'unité de compte numérique et programmable ! Depuis la création du Bitcoin, près de 6 600 blockchains ont été créées.
Réputées infalsifiables, toutes les « blockchains » - qui doivent être en mesure de remplacer un tiers de confiance - n'assurent pas cependant le même degré de sécurité.

## DES CHAMPS D'APPLICATION ÉTENDUS DES PROTOCOLES DE REGISTRES DISTRIBUÉS

Les caractéristiques des « blockchains » sont :

- La sécurité
- La transparence et la traçabilité
- La résilience
- La désintermédiation

Les champs des applications sont donc immenses : banques, assurance, immobilier, santé, énergie, transports, divertissement... Les protocoles utilisant une « blockchain » pourraient à terme simplifier, moderniser et automatiser la plupart des services opérés par des « tiers de confiance » centralisés (métiers de banques, notaires, cadastre, ...). De même, les « Smart Contracts » pourraient redéfinir de façon universelle les modes de gouvernance et de gestion du monopole de la monnaie et des transactions financières, impactant les institutions, les entreprises et leurs business models, les organisations, les corporations, les sociétés et les États impliqués, mais aussi les banques et l'économie tout entière.

*Quelques exemples :*

- **Notariat**
  En théorie, la technologie pourrait se substituer à l'intervention humaine.
  En pratique, le notaire va mettre à profit la technologie et l'utiliser pour renforcer le service qu'il propose

- **Logistique et supply chain,** en lien avec la traçabilité :
  - Normalisation
  - Authentification / certification
  - Automatisation

**=>** Impact : Baisse des besoins en compétences dans les domaines liés à la traçabilité, Sécurisation des process, Gains de productivité

- **Finance**
  - Certification des échanges (Court terme - CT)
  - Décentralisation des échanges d'actifs (Moyen terme - MT)

=> Impact sur les métiers de back office, voire sur l'ensemble du système

- **Banque assurance**
  - Communication Client (CT)
  - Gestion d'actifs crypto (MT)
  - Transferts de fonds (MT)
  - Processus Réglementaire – ex : PRIIPs (MT)

=> Impact sur les métiers de back office, voire sur l'ensemble du système

- **Comptabilité-Audit**
  - Dématérialisation des factures, automatisation de la saisie comptable
  - Authentification des transactions
  - Automatisation de l'audit comptable

=> Impact sur les métiers de l'audit et de la comptabilité de faible valeur ajoutée

- **Média/publicité**
  - Décentralisation des données et achat/vente en direct
  - Disparition d'intermédiaires au profit de systèmes communautaires autogérés

- **Santé**
  - Certification des médicaments
  - Partage des données de santé

=> Amélioration de la recherche médicale

## LA DEMANDE PROGRESSE AUTOUR DES COMPÉTENCES LIÉES AUX PROTOCOLES DE REGISTRES DISTRIBUÉS

Les initiatives se multiplient pour tester le potentiel des protocoles de registres distribués : création de projets pilotes et lancement de prototypes. Les secteurs de la finance et de l'assurance sont les principaux recruteurs, des start-ups aux grandes entreprises. Les profils concernés sont expérimentés et pointus : connaissance préalable des architectures ou des langages.

Certains acteurs sont plus en avance que d'autres dans leur stratégie « blockchain ». Des groupes bancaires étudient la technologie depuis quelques temps déjà, tandis que d'autres observent et veulent valider le concept. De façon générale, tous les acteurs de la finance s'y intéressent de près ou de loin. Toutes les grandes sociétés de conseil sont en cours de constitution d'équipes.

Les postes ouverts par les entreprises sont de natures diverses. Sont notamment recherchés des experts ayant une expérience dans la création et l'exploitation de systèmes de grands livres distribués. Le but est de faire de la recherche pour créer un protocole de registres distribués permissifs, des « sidechains » (chaînes filles rattachées à une chaine mère principale) ou méta-protocoles adossés sur un protocole de registres distribués non permissifs (dit publics).

Les grandes entreprises vont plus souvent chercher à travailler avec des startups reconnues dans le milieu pour faire de la R&D. Mais elles devraient aussi s'associer avec les communautés de développeurs. La majorité d'entre-elles n'a pas d'équipe ou de projet « blockchain » en interne, mais fait le choix de travailler avec des experts par le biais de consortium comme R3 CEV.

## DES COMPÉTENCES ISSUES DES SCIENCES ET DES TECHNOLOGIES PLUS TRADITIONNELLES

Les « blockchains » ne sont que l'une des composantes d'une pile de technologies existant depuis plus de 20 ans. Ce sont de simples structures de données chainées. En ce sens, travailler dans ce domaine implique de bonnes compétences en mathématiques concernant le logarithme discret. Ce dernier est un objet mathématique utilisé en cryptologie et appliqué aux fonctions à sens unique. Il permet d'introduire les fonctions de hachages cryptographiques ou encore les courbes elliptiques sur corps fini.

La maîtrise des modèles de calculs complexes sont essentielles comme l'outil du Lambda calcul à 2 opérations (comprenant « l'application » et « l'abstraction ») ou celui du Turing machine, un autre outil indispensable utilisé en théorie de la calculabilité, en théorie de la complexité ou en théorie de l'approximation.

En effet, le Lambda calcul amène au paradigme de la programmation fonctionnelle utilisée au sein du protocole Bitcoin avec « Bitcoin Script », un langage à pile dérivé du Forth. L'outil de Turing machine est, quant à lui, lié au paradigme de la programmation impérative nécessaire pour bien commencer l'apprentissage d'un langage de haut niveau tel que Solidity, un dérivé de Javascript utilisé sur Ethereum. Le protocole Ethereum dispose par ailleurs de plusieurs langages de haut niveau comme Python, Serpent ou encore Viper.

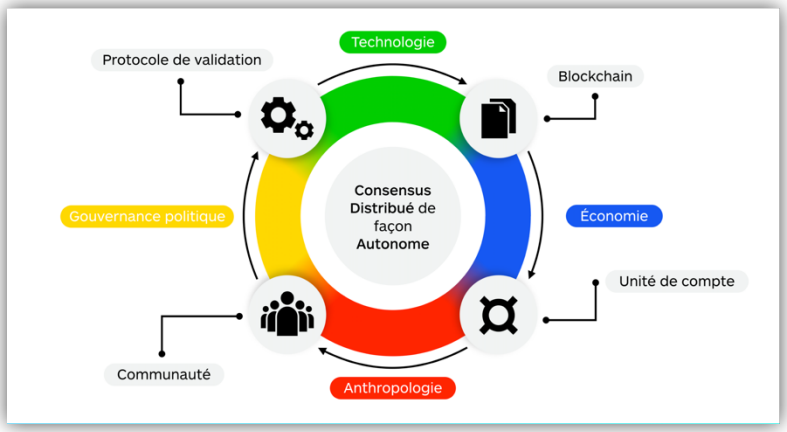
Enfin, les protocoles de registres distribués sont fondamentalement basés sur les fonctions de hachages cryptographiques qui englobent plusieurs dimensions connexes comme :

- La **cryptographie asymétrique,** qui permet de produire une signature numérique et de s'identifier sur les réseaux afin de réaliser sa transaction. Apprendre la cryptographie par « Transposition » et « Substitution » avec mot-clé est essentiel pour introduire la cryptographie asymétrique
- Les **notions de cryptanalyse** comme l'analyse fréquentielle ou de cryptanalyse moderne comme les attaques sur les modes opératoires.
- Le **mode d'opération cryptographique**
- Les **arbres de Merkle**
- Les différents **protocoles de consensus**
- Les **bases de données utilisant les UTXOs**
- Les **systèmes de compte protégé par un nonce**

## DE L'IMPORTANCE DES SCIENCES SOCIALES ET HUMAINES

Comme la monnaie traditionnelle, les protocoles de registres distribués utilisant une « blockchain » comme support se caractérisent par la confiance qu'ont ses utilisateurs dans la persistance de sa valeur et de sa capacité à servir de moyen d'échange. C'est aussi un lien social dans le sens où son utilisation renforce le sentiment d'appartenance. Ainsi, une communauté se crée autour d'un projet, i.e dans le sens courant, un ensemble de personnes vivant ensemble pour le bien commun et le bien de chacun.

Les protocoles de registres distribués ont donc des dimensions sociales, politiques, psychologiques, juridiques et économiques. Avoir été sensibilisé à cet aspect de la technologie et disposer de notions dans l'ensemble des matières constitutives des sciences sociales et humaines semble donc un prérequis indispensable.




## ÉMERGENCE D'UN NOUVEAU MÉTIER : ARCHITECTE DE REGISTRE DISTRIBUÉ

L'ensemble de ces compétences permet d'exercer le métier, prometteur, d'Architecte de Registre Distribué, qui requiert, comme nous venons de le voir, des compétences dans des domaines plus larges que le seul aspect technologique.
À terme, ce spécialiste « blockchain » doit être en mesure de :

- **Auditer les différents protocoles de confiance** (avantages et inconvénients)
- **Écrire, tester et déployer une application** décentralisée
  *Ex : un actif numérique distribué ou un contrat intelligent*
- **Sécuriser un portefeuille d'actifs** numérique programmable
- **Initialiser, gérer et protéger ces actifs** avec un hardware wallet
- Faire de **l'analyse de données de blockchains**

Il s'agit bien d'un métier, nécessitant des compétences spécifiques et susceptible d'avoir des spécialisations propres :

- **Architecte spécialisé** dans la **création de sidechains**
- **Architecte spécialisé** dans les **propriétés des réseaux, la structure des blocs ou la sécurité**
- **Architecte développeur** avec **audit de l'écosystème des protocoles**
- **Architecte spécialisé** dans la **création d'algorithmes de consensus**
- **Architecte spécialisé** dans la fonction de **test, de déploiement et de maintenance.**
- (...)

L'architecte de registre distribué devra être en capacité à s'adapter à de nouvelles technologies, dans un contexte d'évolution très rapide. Citons notamment des technologies pouvant avoir un impact à court-terme :

- Les **signatures Schnorr**
- Les **signatures Lamport**
- Les **signatures Rings**
- **Covenant**
- **Confidential transactions**
- **MAST**
- **Migration d'UXTO vers MimbleWimble**
- Le **blockchain sharding**

## DE LA MENÉE DE PROJETS « BLOCKCHAINS » ET « SIDECHAINS »

Il est clair que les projets de « blockchains » (et de « sidechains ») ne pourront jamais être l'affaire d'une seule personne, même la plus polyvalente, regroupant toutes les compétences citées ci-dessus. Aussi, la réussite de ce type de projets dépendra de la capacité qu'auront leurs promoteurs à réunir une équipe associant toutes les compétences attendues. Le développement de projets autour de ces protocoles (et méta-protocoles) est reconnu d'une mise en œuvre très complexe nécessitant des compétences hybrides de **savoir**, de **savoir-faire** mais aussi de **savoir-être** eu égard à la diversité des acteurs engagés. Le besoin en compétences techniques et scientifiques du numérique pour participer à cette nouvelle industrie est évident, mais celles-ci ne suffisent pas forcément. Il sera nécessaire de leur associer des compétences en sciences sociales : psychologie, sociologie et économie pour constituer une équipe hétérogène mobilisant une forte intelligence collective (interculturelle et intergénérationnelle).

La direction de projet devra ainsi s'appuyer sur les acteurs clefs que sont les experts en architecture de registre distribué, tout en intégrant notamment des compétences :

- de **prise en compte des nouveaux comportements** des utilisateurs
- de **gestion et d'animation de communauté** et/ou d'écosystème : community manager (...) afin de produire des prototypes de protocoles ou de nouveaux modèles qui pourront être testés en toute sécurité et en toute confiance pour être implémentés avec succès. Le tiers de confiance est la communauté, il convient d'accorder une attention particulière à son écosystème
- (...)

## CONCLUSION - RECOMMANDATIONS

Les formations, écoles et entreprises membres de l'association Pasc@line sont convaincues de l'intérêt des protocoles de registres distribués dotés de « méta-protocoles », de « blockchains » et de « sidechains ». Cependant, le marché de l'emploi sur cette nouvelle thématique doit encore se constituer de façon pérenne et avec des volumes significatifs. Ces protocoles d'un type nouveau souffrent encore d'incertitudes, en matière d'évolution, de business model et de scalabilité, mais aussi en matière de sécurité, de confiance et de technologie. Le positionnement du régulateur est aussi très attendu. **La question de la maturité de l'ensemble est posée.**

Toutefois, il convient que nos entreprises du numérique et écoles sachent anticiper les changements en cours pour former de futurs professionnels en capacité de répondre aux attentes et aux révolutions à venir, au-delà des pionniers et premiers early-adopters, déjà à l'œuvre. Les technologies blockchains sont déjà enseignées dans certains de nos établissements, trop souvent de façon partielle et dispersée dans des cours de sécurité, de cryptologie, d'informatique distribuée ou théorique (...).

Notre commission recommande donc d'intégrer le sujet de la « blockchain » et des protocoles de registre distribués dans le cursus des étudiants ingénieurs comme un élément de spécialisation de 2$^{e}$ ou 3$^{e}$ année, ou de l'imaginer comme un élément de certification spécifique. L'approche n'est pas suffisamment mûre pour en faire une formation en tant que telle.
Cette spécialisation doit intégrer des travaux pratiques sur les usages particuliers que cette technologie permet. Au-delà des fondamentaux techniques déjà assimilés auparavant, nous préconisons, dans le cadre de cette spécialisation en un an, de **dédier un trimestre à la théorie et deux trimestres à des travaux pratiques en fonction de la culture et du domaine d'application de l'école.**
Un des freins essentiels devrait être le niveau en mathématiques exigé pour se mouvoir dans cette technologie. Les candidats ayant ce profil, cette appétence et ces capacités sont peu nombreux. Il est donc particulièrement difficile de les identifier.

Compte tenu du niveau d'exigence scientifique et des concepts utilisés par les « Blockchains », nous ne pouvons que réitérer **l'importance des softskills** dans la formation générale de nos ingénieurs. En effet, ce sujet nécessite explication et promotion, notamment auprès des Directions métiers impactées. Pédagogie et communication seront les bienvenues pour convaincre de manière proactive les différents acteurs de l'entreprise du potentiel disruptif de cette technologie, à anticiper. Pour les mêmes raisons, nous incitons fortement les établissements de formation des futurs utilisateurs (Avocats, Notaires, Banque, Assurance...) à intégrer dans leurs cursus des cours de sensibilisation à ces nouvelles technologies, pour les démystifier et les appréhender de façon plus sereine.
**Les professionnels du numérique doivent se rapprocher des Directions métiers, et réciproquement.**

**La prochaine publication de Pasc@line concernera l'évolution des compétences en lien avec l'émergence de l'IA (Intelligence artificielle).**

**Pour toute information : Association Pasc@line**
**www.assopascaline.fr** - remi.ferrand@assopascaline.fr