



## **PROJET**

### **La technologie 'chaîne de blocs'**

Code du Projet **PEM 022017**

#### ***Description du projet***

##### ***Résumé du projet***

Cette initiative vise à créer un groupe de travail mixte entre Cevital/Brandt et les institutions universitaires et de recherche scientifiques Algériennes, autour de la thématique Blockchain.

Blockchain est un concept émergent qui risque de refaçonner le paysage du marché et de révolutionner les pratiques des sociétés à plusieurs égards. En effet, une blockchain ou chaîne de blocs est une base de données distribuée transparente, sécurisée, et fonctionnant sans organe central de contrôle.

Elle tire sa sécurité principalement de la distribution transparente des données et peut fonctionner sans autorité centrale, mais de manière décentralisée grâce au consensus de l'ensemble des nœuds du réseau.

A la lumière de ces données, rester à l'écart des développements qui arrivent chaque jour, n'est définitivement pas un choix pour l'Algérie.

## ***Problématiques***

**But** : Transiger entre pairs sans passer par une autorité centrale pour établir la confiance.

**Principes** : Consensus, Sécurisé, Transparent, Distribué, Ouvert, sans 'double spent', faible coût, à volonté

Les systèmes et solutions informatiques mondialement utilisés dans les différents secteurs d'activités présentent des lacunes parfois très couteuses tel que :

1. Centralisation des données et des traitements,
2. Déficience des mécanismes d'éradication de la fraude, la contrefaçon et la falsification,
3. Fragilité des systèmes de protection des données personnelles et institutionnelles,
4. Lourdeur dans l'exécution des transactions de contrats,
5. Faiblesse des systèmes de paiement électroniques.

Le Blockchain s'est donc récemment imposé comme alternative incontournable pour palier à toutes ces déficiences de par ses fondements basés sur la décentralisation des données et leur ultra sécurisation.

## ***Objectifs***

A titre indicatif, on pourra citer la liste d'objectifs non exhaustive suivante :

1. Développer les compétences nationales (comptabilities building),
2. Anticiper l'impact de la généralisation de Blockchains sur les différents aspects de la société,
3. Concilier le partage des données personnelles et nationales avec leur confidentialité,
4. Sécuriser tous types de contrats et optimiser l'exécution de leurs transactions (exp : banque, eGouv),
5. Proposer de nouvelles applications en IoT (Internet of Things) ou SupplyChain ou Finance, ... etc

## ***Etat de l'art***

Décrivez les principales idées, modèles ou hypothèses déjà considérés pour la résolution de la problématique. Citer les travaux y afférent.

Les principales idées :

1. **IOT décentralisé** : Enregistrement et échange de données sécurisé (messages échangés entre les périphériques intelligents dans une topologie IOT).
2. **Signature sans clé** : Utiliser une infrastructure de sécurité sans clé (KSI) pour alimenter les signatures de données, les marquer et les valider.
3. **Preuve juridique de possession** : Conserver la signature, l'horodatage (timestamp) associé à un document et la valider dans n'importe quel point de la chaîne de blocs.

4. **Règlement du commerce de sécurité** : Autoriser le règlement des transactions en quelques minutes et à une fraction du coût par rapport aux solutions actuelles telles que les dépôts de sécurité centraux (CSD).

5. **Anti-contrefaçon** : les marques, les commerçants et les marchés s'appuient sur la sécurité et les modèles de confiance décentralisés de la chaîne de blocs pour faire respecter les informations d'authenticité du produit.

NB: Toutes ces idées sont développées dans un modèle décentralisé et sécurisé.

**Travaux y afférent :**

**Bitcoin : Monnaie** : La plus importante monnaie cryptographique décentralisée (71 milliards \$, 08/2017).

**FollowMyVote** : Vote électronique

**Moneytis** : Transfert d'argent

**Wekeep** : Assurance : Stocker de l'argent numériquement dans des « séquestres en smart contract »

**Synereo** : Réseau social vraiment en réseau (à l'opposé de FaceBook 100% centralisé)

**Bitproof** : Certification de documents officiels dématérialisés.

**KeeX** : Travail collaboratif : Messagerie d'entreprise sécurisée et gestion de fichiers.

## ***Methodologie***

1. Maîtriser les concepts de base de la technologie Blockchain : Echange d'information, cryptographie, data mining, validation de blocks, ... etc
2. Analyser les architectures software et hardware pour l'implémentation de la Blockchain : Blocs, Pièces, Partage de données, Tolérance aux pannes, Preuve de, Modèles de données, Programmation
3. Maîtriser des plateformes génériques Blockchain réalisées à ce jour : Hyperledger, MultiChain, Ethereum,
4. Maîtriser les interactions entre les plateformes génériques (point 3) et les plateformes applicatives : Finances (R3), Régulation (ISITC Europe), santé (Hashed), ... etc
5. Proposer des nouvelles solutions Blockchain : générique, spécifique, ...

## ***Interdisciplinarité***

Les disciplines nécessaires à la mise en place de la méthodologie telle définie ci-haut sont :

**TECHNIQUE** : Développeurs et architectes technologiques

- Conception et déploiement des systèmes de sécurité et de cryptographie,

- Expérience en développement software à grande échelle sur clouds, containers et CI/CD
- Analyses de menaces, détection d'anomalie et gestion de performance,
- Algorithmes, structures de données, et des technologies décentralisées,
- Cryptographie et sécurité des données,
- Compétences en codage avec au moins un des langues : C, C ++, JAVA, Python, Flash/ActionScript, PHP
- Une bonne compréhension du stockage distribué, comme RDBMS et NoSQL,
- Connaissance en architecture Web (HTTP, sessions, stateless, REST APIs, JSON, etc.),
- Expérience en développement sur les plateformes mobiles,
- Expérience en JavaScript orienté objet et les bibliothèques JavaScript modernes (Closure, jQuery, Node, ...)
- Expérience en SVG, Canvas HTML5 et l'animation via JavaScript et CSS,
- Expérience en intégration de patrons (middleware, message broker, service bus, etc.)
- Excellent en leadership, gestion de projet et compétences organisationnelles
- 

#### **NON TECHNIQUES : Gestionnaires et Analystes.**

- Spécialistes de la stratégie de produit, analystes d'affaires, chercheurs et spécialistes en marketing
- Spécialistes en gestion des risques, sécurité, cryptographie et des processus métier.

#### ***Équipement nécessaire au projet***

Les équipements technique, scientifique, logistique ou autre nécessaires au projet :

1. Laptops de travail et Serveurs (Dev, Pre-Prod, Prod) ;
2. Imprimante scanner multitâches (couleur et noir) ;
3. Onduleurs ;
4. Bureaux et fournitures de bureaux ;
5. Locaux avec téléphone et bonne connexion internet (équipés de plusieurs prises).

#### ***Impacts attendus***

1. Mettre l'Algérie en course pour s'approprier les technologies reliées à Blockchain ;
2. Créer des compétences qui permettraient à l'Algérie de se préparer à tout nouveau défi qui découlerait de la généralisation de Blockchain ;
3. Stimuler l'écosystème des hautes technologies en mettant en lien les industriels avec les chercheurs ;
4. Développer de nouvelles solutions innovantes qui permettraient de créer de nouvelles entreprises.