Blockchain as a service

Introduction

Dans ce chapitre nous allons découvrir le monde des blockchains : comprendre le fonctionnement de la blockchain, identifier les différents types de blockchain et approfondir notre connaissance sur la façon sur la sécurité de la technologie blockchain. Nous allons étudier la blockchain as service et approfondir notre connaissance sur la façon dont les BAAS fonctionnent.

III.1 Définitions et notions fondamentales

III.1.1 Qu'est-ce que la blockchain ?

La première blockchain est apparue en 2008 avec la monnaie numérique bitcoin, développée par un inconnu se présentant sous le pseudonyme Satoshi Nakamoto.

Les registres distribués numériques promettent de résoudre ces problèmes grâce à une combinaison unique de réseaux distribués et de cryptographie.

Une blockchain est une structure de données qui permet de créer un livre numérique de données et de le partager dans un réseau d'individus indépendants.

Ce registre a une particularité, il n'est pas stocké sur un serveur central mais il est détenu par plein d'ordinateurs en même temps. D'un point de vue commercial, la blockchain peut être définie comme un réseau d'échange peer-to-peer pour transférer de la valeur, tandis que, d'un point de vue juridique, elle peut être définie comme une technologie permettant de valider les transactions. La compréhension des blockchains est extrêmement complexe, aussi bien au niveau de leur fonctionnement que de leur mise en place.

Pour essayer de comprendre le mieux possible cette nouvelle technologie, nous allons étudier les différentes définitions qui lui sont données par des spécialistes :

« Dans son essence, la blockchain est une technologie qui enregistre des transactions en permanence, d'une manière immutable, mais de sorte à permettre une mise à jour constante. Elle permet une traçabilité illimitée dans le temps. »

« La Blockchain est un registre partagé et distribué destiné à faciliter le processus d'enregistrement des transactions et de suivi des actifs dans un réseau d'entreprises. Un actif peut être un bien tangible (maison, voiture, liquidités, terrain), ou intangible, par exemple des éléments de propriété intellectuelle comme les brevets, les droits d'auteur ou les marques. Un réseau Blockchain permet de suivre et d'échanger pratiquement tout bien possédant une certaine valeur en réduisant les risques et en diminuant les coûts pour tous les interlocuteurs concernés. »

« La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle »

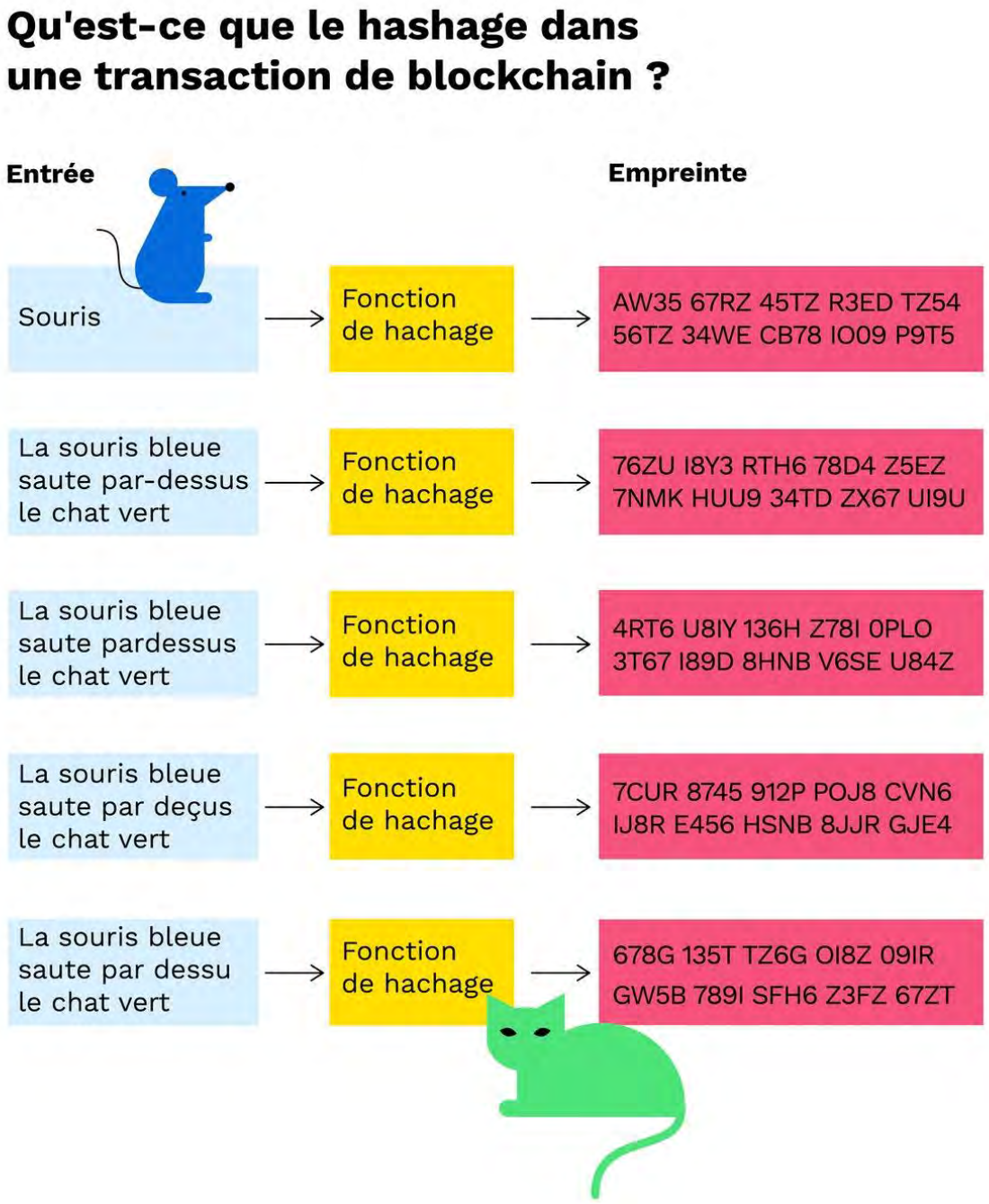


FIGURE 2 : LE HASH

Le Hash est un élément clé de la technologie blockchain, il est le fil conducteur qui permet de lier les blocs entre eux.

La blockchain a deux caractéristiques principales.

- Elle apporte la confiance là où il n'y en a pas. En fait, les systèmes basés sur la blockchain garantissent une plus grande transparence en mettant les informations à la disposition de tous les participants au réseau, mais ils exploitent également la cryptographie et la validation par les pairs des transactions pour garantir l'intégrité des données et l'immuabilité des enregistrements.
- Les systèmes basés sur la blockchain sont entièrement distribués. La vie privée des utilisateurs est protégée par l'utilisation de pseudonymes tandis que la fiabilité du système est assurée par le stockage d'une copie de la base de données dans chaque nœud.

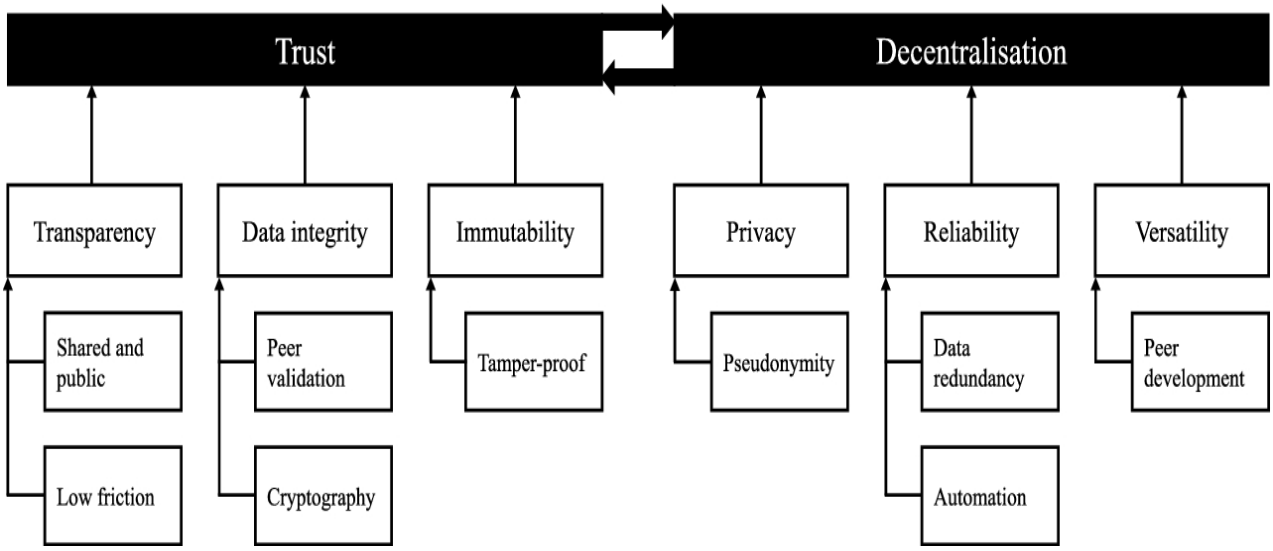


FIGURE 3 : FONCTIONNEMENT DE LA BLOCKCHAIN

Ces deux caractéristiques clés de la blockchain sont finalement interconnectées, car des mécanismes de confiance sont nécessaires pour créer un réseau décentralisé, et la décentralisation fournit aux utilisateurs les moyens de s'impliquer dans le réseau en établissant la base d'un mécanisme de consensus.

La capacité des utilisateurs à lire et à soumettre des transactions à une blockchain dépend de leur accès aux transactions.

III.1.2 Les types de blockchains

Il existe différents types de blockchains :

- Les blockchains publiques

La blockchain publique est le premier type à avoir été créé à grande échelle. Dans une chaîne publique, tout le monde peut lire son contenu. Chacun peut y rajouter des informations (ou des transactions) et s'attendre à ce qu'elles apparaissent dedans (si tant est qu'elles respectent les règles de cette chaine). Chaque membre du réseau peut aussi participer au processus d'approbation (le consensus), celui qui permet de décider quel bloc sera ajouté à la chaine, et qui définit l'état actuel du système.

La sécurité et la décentralisation des blockchains publiques reposent sur le principe que les différents membres acceptant de mettre à disposition du réseau des ressources – que ce soit de la puissance de calcul dans un consensus de type preuve de travail, ou des actifs dans un consensus de type preuve d'enjeu – pour vérifier les nouveaux blocs seront rémunérés pour les récompenser.

- Les blockchains autorisées

Les blockchains autorisées, telles que Ripple, contrôlent les rôles que les individus peuvent jouer au sein du réseau. Elles sont toujours étendues et possèdent des systèmes distribués qui utilisent un token natif.

- Les blockchains privées

Enfin, dans les blockchains entièrement privées une seule organisation est responsable de l'écriture dans la chaîne et du processus d'approbation. La lecture peut, comme dans le type hybride, être en libre accès ou bien restreint.

Ce type de blockchain est attractif en théorie pour les institutions souhaitant tirer parti des avantages de la technologie sans la perte de contrôle associée à la décentralisation complète, mais n'a en pratique pas beaucoup d'intérêt. Une blockchain totalement privée ne serait qu'une base de données d'entreprise, mais plus lente et plus chère qu'une base de données classique.

	Blockchain publique	Blockchain autorisé	Blockchain privé
Participation dans le consensus	Tous les noeuds	Des nœuds sélectionnés	Un seul nœud
Lecture	Publique	Publique ou privé	Public ou privé
Possibilité d'altération	Presque impossible	Presque impossible	possible
Efficacité	Faible	élevé	élevé
Centralisation	non	partielle	oui
Accès	sans permission	Avec permission	Avec permission

TABLEAU 1 : COMPARAISON ENTRE LES DIFFERENTS TYPES DE BLOCKCHAIN

Source : ZHENG, Z, XIE, S. DAI, H. CHEN, X. 2016, « Blockchain Challenges and Opportunities : à Survey », https://www.henrylab.net/pubs/ijwgs_blockchain_survey.pdf,

Quel que soit le type de blockchain, certaines caractéristiques clés sont communes à toutes :

Réseau distribué : l'adoption d'une blockchain supprime toutes les entités centralisées et distribue l'accès à tous les participants du réseau. En d'autres termes, tous les participants du réseau, et non un particulier, peuvent vérifier les transactions. Les mineurs sont des acteurs clés de ce réseau distribué car ils s'efforcent de résoudre les problèmes de calcul qui permettent de créer, vérifier et stocker en toute sécurité les transactions.

Cryptographie : elle permet aux parties de préserver la confidentialité des informations qu'elles s'envoient. Blockchain utilise des mécanismes d'infrastructure à clé publique (PKI) pour exécuter des transactions. Chaque utilisateur de la blockchain possède une clé publique et une clé privée. Pour terminer une transaction, un expéditeur doit connaître la clé publique du destinataire qui peut déchiffrer le message en utilisant sa propre clé privée. Chaque transaction est stockée dans un bloc, qui a une empreinte digitale unique (c'est-à-dire un hachage) qui garantit l'authentification de la source de la transaction.

Horodatage : chaque transaction qui se produit sur la blockchain est horodatée et personne ne peut la changer une fois qu'elle a été enregistrée.

Les types de blockchains utilisent la cryptographie pour permettre à chaque participant sur un réseau donné de gérer le registre de manière sécurisée sans avoir besoin d'une autorité centrale pour appliquer les règles. L'élimination de l'autorité centrale de la structure de la base de données est l'un des aspects les plus importants et les plus puissants des blockchains. Les blockchains créent des transactions permanentes. La permanence de la transaction est fondée sur la permanence du réseau. Dans le contexte des blockchains, cela signifie qu'une grande partie d'une communauté blockchain doit accepter de modifier l'information et est incitée à ne pas modifier les données.

Une blockchain est un système pair-à-pair sans autorité centrale qui gère le flux des données. L'une des principales façons d'éliminer le contrôle central tout en maintenant l'intégrité des données est d'avoir un réseau large distribuée d'utilisateurs indépendants.

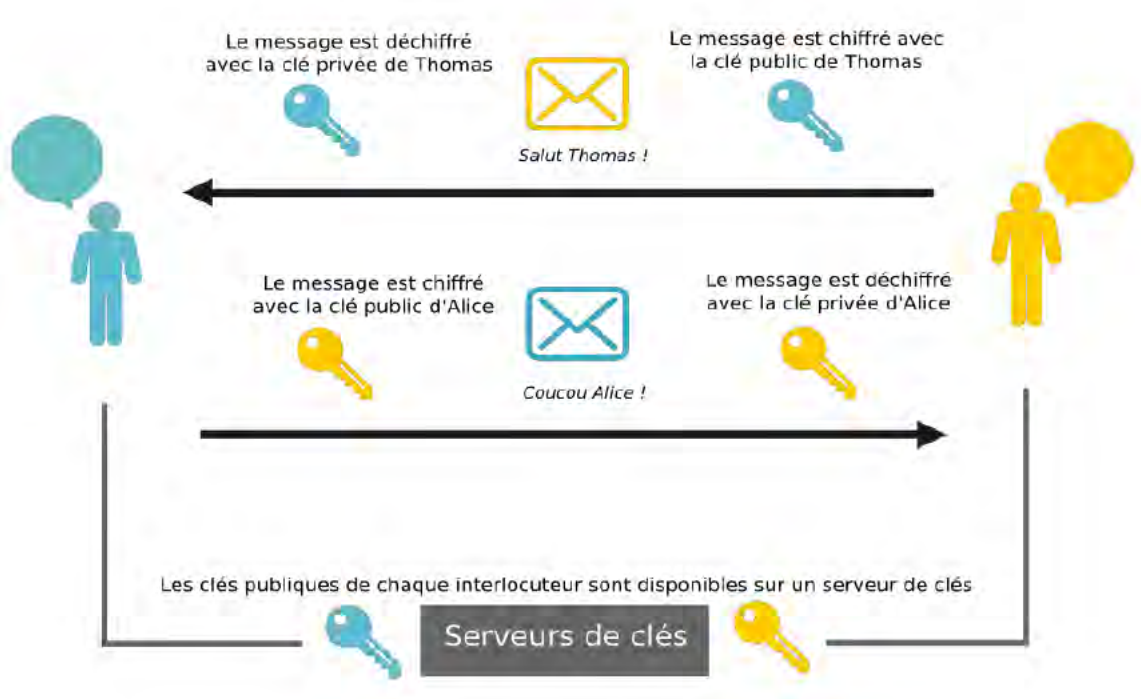
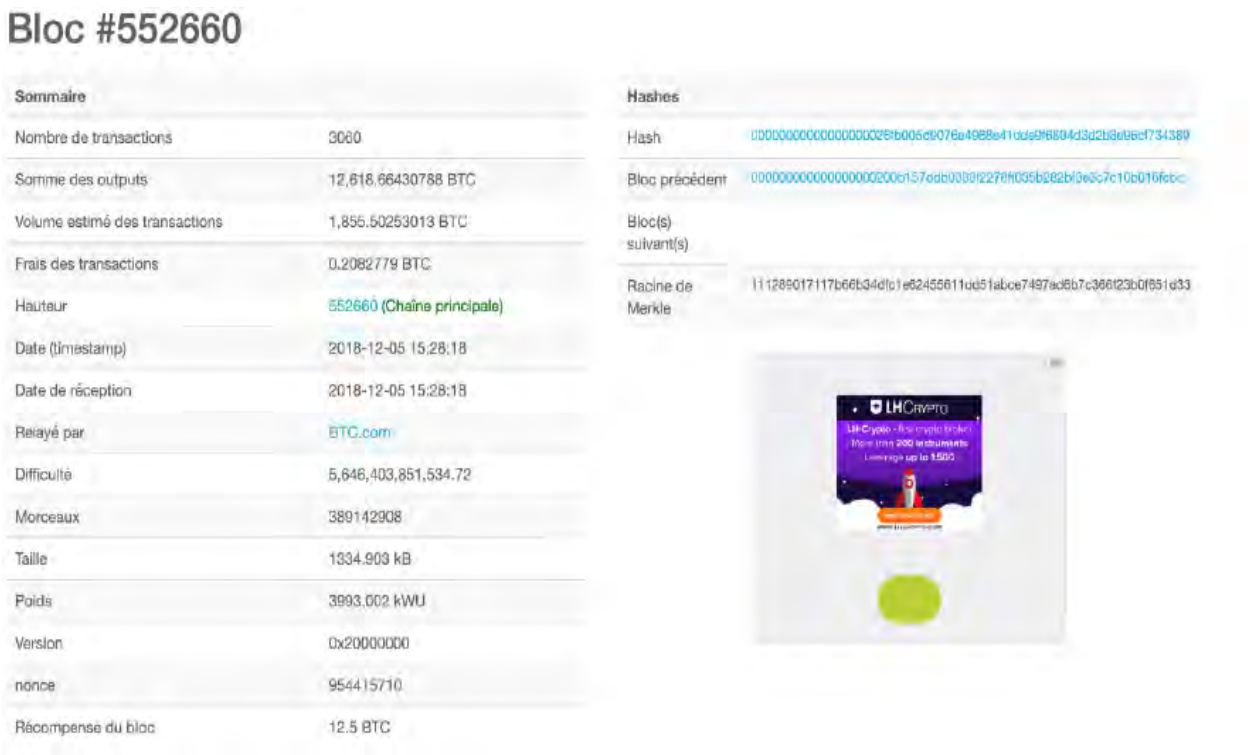


FIGURE 4 : PRINCIPE DE CRYPTOGRAPHIE

Le principe de clé publique et clé privée est un principe cryptographique qui permet uniquement aux intéressés de déchiffrer les messages qu'ils échangent. (11)

III.1.4Structure de la blockchain



Bloc #552660

Sommaire	
Nombre de transactions	3060
Somme des outputs	12,618.66430788 BTC
Volume estimé des transactions	1,855.50253013 BTC
Frais des transactions	0.2082779 BTC
Hauteur	552660 (Chaîne principale)
Date (timestamp)	2018-12-05 15:28:18
Date de réception	2018-12-05 15:28:18
Relayé par	BTC.com
Difficulté	5,646,403,851,534.72
Morceaux	389142908
Taille	1334.903 kB
Poids	3993.002 kWU
Version	0x20000000
nonce	954415710
Récompense du bloc	12.5 BTC

Hashes	
Hash	0000000000000000000026fb005d9076a4988e41dde9f6894d3d2b8e96ef734389
Bloc précédent	0000000000000000000200c157ddb0389f22769f095b282bf3e8c7c10b016fcbc
Bloc(s) suivant(s)	
Racine de Merkle	11128917117b66b34dfc1e62455611dd51abce7497ad6b7c366f23b0f851d33

FIGURE 5 : BLOCK DE LA BLOCKCHAIN BITCOIN

On voit ici un bloc d'une blockchain et toutes les informations qui le concerne.

Elles sont composées de trois parties principales :

Le bloc : une liste de transactions enregistrées dans un livre sur une période donnée. La taille, la période et l'événement déclencheur pour les blocs sont différents pour chaque blockchain.

La chaine : un hash (Fig.1) qui relie un bloc à un autre, les enchainant mathématiquement ensemble. C'est l'un des concepts de la blockchain le plus difficile à comprendre. C'est aussi la magie qui colle des blocs ensemble et leur permet de créer une confiance mathématique. Le hash dans la blockchain est créé à partir des données qui se trouvaient dans le bloc précédent. Le hash est une empreinte digitale de ces données qui verrouille les blocs dans l'ordre et dans le temps.

Le réseau : le réseau est composé de nœuds pleins. C'est un ordinateur qui exécute un algorithme sécurisant le réseau. Chaque nœud contient un enregistrement complet de toutes les transactions qui ont déjà été enregistrée dans cette blockchain.

Les nœuds sont localisés partout dans le monde et peuvent être exploités par n'importe qui.

III.1.5Fonctionnement de la blockchain

Les blockchains peuvent créer la confiance dans les données numériques. Lorsqu'une information a été écrite dans une base de données blockchain, il est presque impossible de la supprimer ou de la modifier.

Le fonctionnement général d'une blockchain sous-jacente à un transfert d'actifs est présenté ci-dessous.

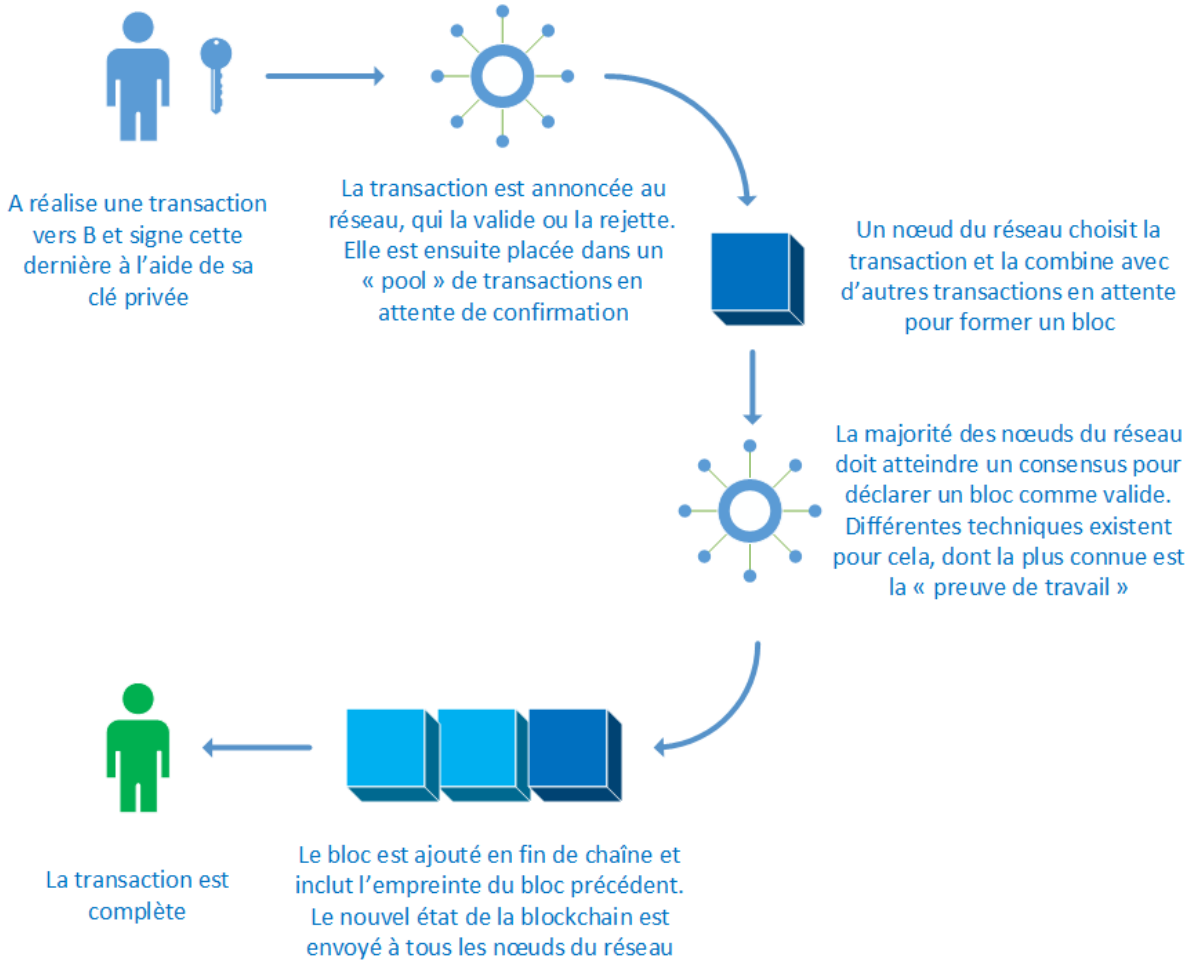


FIGURE 6 : FONCTIONNEMENT DE LA BLOCKCHAIN

Il s'agit effectivement d'une chaîne de blocs. Cependant, les blocs sont ici des informations numériques stockées sur une base de données publique faisant office de chaîne.

Chaque bloc contient des informations au sujet d'une ou plusieurs transactions : la date, l'heure, le montant… les participants à cette transaction sont en revanche anonymes, et identifiés par une signature numérique

Ainsi, une fois qu'un bloc est inclus dans la chaîne, et qu'un certain nombre de blocs ont été rajoutés après lui, il devient virtuellement impossible de modifier les transactions de ce bloc car cela impliquerait de recalculer tous les blocs suivants. Les transactions sont considérées comme irréversibles et finales après leur inclusion dans un bloc validé.

Toute blockchain publique fonctionne nécessairement avec une monnaie ou un token (jeton) programmable. Bitcoin est un exemple de monnaie programmable.
Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les nœuds du réseau appelés les "mineurs", selon des techniques qui dépendent du type de blockchain. Dans la blockchain du bitcoin cette technique est appelée le "Proof-of-Work", preuve de travail, et consiste en la résolution de problèmes algorithmiques.

III.1.6 Usage de la blockchain

Le caractère décentralisé de la blockchain, couplé avec sa sécurité et sa transparence, promet des applications bien plus larges que le domaine monétaire.
Ainsi on peut classer l'utilisation de la blockchain en trois catégories :

- Les applications pour le transfert d'actifs (utilisation monétaire, mais pas uniquement : titres, votes, actions, obligations…).
- Les applications de la blockchain en tant que registre : elle assure ainsi une meilleure traçabilité des produits et des actifs.
- Les smart contacts : il s'agit de programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.

  Le smart contract, en français le contrat intelligent, est une sorte d'accord qui permet d'automatiser certaines actions. Dans ces contrats définis en amont, on décide des conditions nécessaires à la réalisation d'une action. Ces conditions sont directement

liées à la blockchain, et dès le moment ou ces conditions sont réunies, le contrat exécutera certaines actions.

Combinée à l'anonymisation des utilisateurs, cette caractéristique rend la blockchain confidentielle et sécurisée. C'est la raison pour laquelle cette technologie est de plus en plus utilisée.

III.2 Qu'est-ce que la BAAS ?

Le secteur de la technologie blockchain se développe et les blockchains ouvertes ne sont pas les seuls types de registres distribués. Malheureusement, la création, la configuration et l'exploitation d'une chaîne de blocs sont des tâches complexes et la plupart se découragent face à cette difficulté. En effet, certaines entreprises et des particuliers projets nécessitent pour leurs projets la mise en place de blockchains privées dont les utilisateurs sont identifiés. Ces blockchains privées permettent notamment une exécution des transactions plus rapide, mais nécessitent des qualités techniques pour être mises en place. Des entreprises proposent donc des services de mise en place de blockchains privées personnalisées, ce que l'on peut appeler le BAAS (blockchain as a service).

Les BaaS ou Blockchain en tant que Services sont des services Cloud permettant aux entreprises d'exploiter la chaîne de blocs sans avoir à développer et gérer leurs propres infrastructures. Il s'agit en fait de l'équivalent dans le grand livre distribué du SAAS, le moyen par lequel les entreprises s'abonnent et accèdent à des logiciels basés sur le cloud. Ces services tiers constituent un développement relativement nouveau dans le domaine en pleine croissance de la technologie blockchain. L'application de la technologie blockchain est allée bien au-delà de son utilisation la plus connue dans les transactions de crypto-monnaie et s'est élargie pour traiter les transactions sécurisées de toutes sortes.

La BaaS ou Blockchain en tant que Service est la création et la gestion par un tiers de réseaux basés sur le Cloud pour les entreprises développant des applications Blockchain.

Ce type de service Cloud permettant aux utilisateurs de créer, d'héberger et d'utiliser leurs propres applications, contrats intelligents (smart contracts) et fonctions de Blockchain. Le fournisseur de services Cloud se charge de gérer les tâches et activités nécessaires pour garder l'infrastructure agile et opérationnelle.

Le BaaS est basé sur le concept de SaaS (logiciel en tant que service) et fonctionne de la même manière. Il s'inscrit dans un contexte où les modèles économiques liés au Cloud Computing sont de plus en plus populaires.

Il s'agit d'une nouveauté dans le domaine en plein essor de la technologie Blockchain. Alors que les cas d'usage de la Blockchain s'étendent désormais largement par-delà les transactions de cryptomonnaies, la demande en services d'hébergement est en forte hausse.

III.2.1 Fonctionnement BAAS

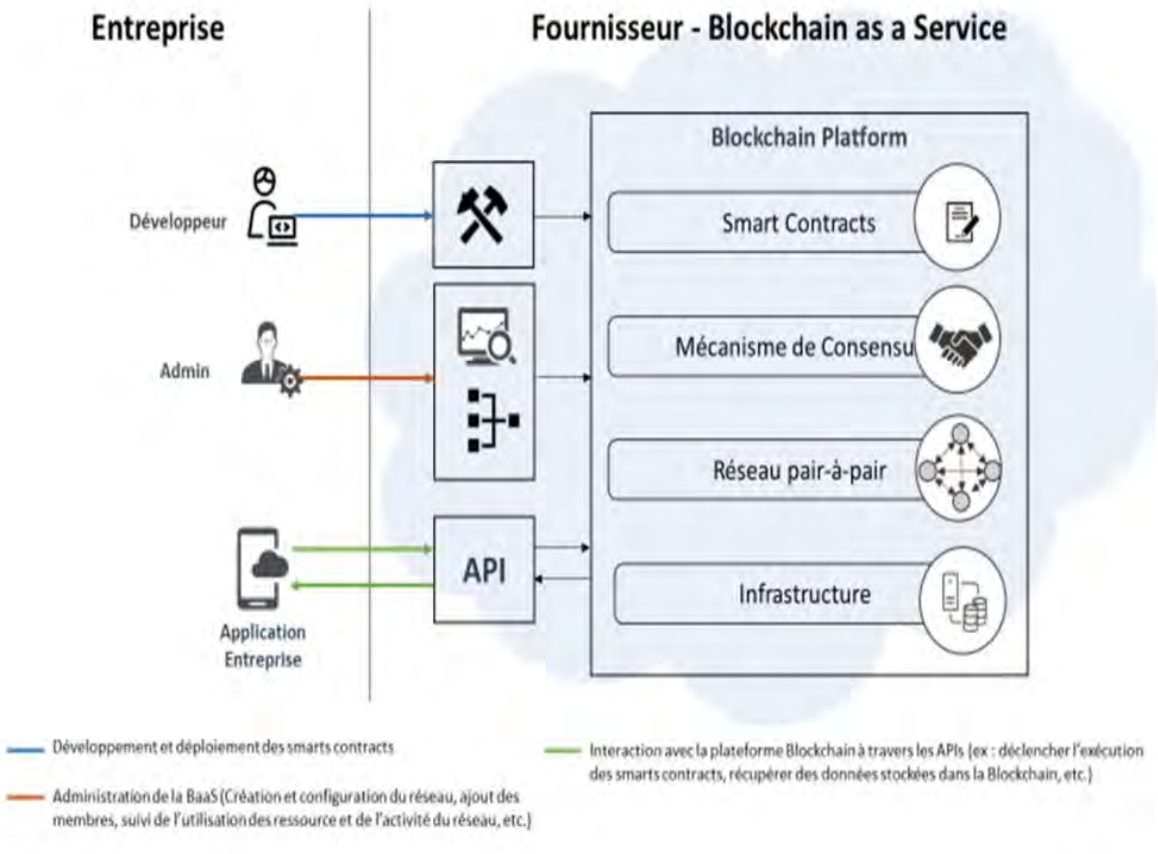


FIGURE 7 : FONCTIONNEMENT BAAS

Il fonctionne comme une sorte d'hôte Web, exécutant l'opération backend pour une application ou une plate-forme basée sur une chaîne de blocs.

On parle de Baas (Blockchain en tant que Service) lorsqu'un fournisseur externe de service Cloud se charge de mettre en place, de configurer et de gérer une infrastructure de technologie Blockchain. En payant pour un service Baas, le client charge le fournisseur de mettre en place et de maintenir les nœuds connectés de la chaîne de blocs.

Le fournisseur prend en charge la maintenance de l'infrastructure et de tous les éléments liés à la chaîne de blocs. D'autres activités connexes font également partie du service : gestion de la bande passante, allocation des ressources, hébergement, fonctionnalités de sécurité et de protection contre les cyberattaques…

Ainsi, le modèle Baas permet aux clients de se focaliser uniquement sur les fonctionnalités de leurs chaînes de blocs plutôt que de devoir se préoccuper en même temps des questions liées aux performances et à l'infrastructure.

Le fonctionnement d'un service Baas peut être comparé à celui d'un service d'hébergement web, où le client paye un fournisseur comme AZURE Web Services pour héberger son site sur ses serveurs plutôt que de devoir l'héberger sur son propre ordinateur et gérer les questions de maintenance et d'infrastructure.

En ce sens, le modèle Baas pourrait permettre une pénétration plus large et plus profonde de la technologie blockchain dans les entreprises de toutes les industries. Quels que soient sa taille et son secteur d'activité, une entreprise peut désormais externaliser toute la prise en charge technique de la chaîne de blocs et se concentrer sur ses objectifs.

Les Baas sont en effet des services cloud, tout comme les SaaS (Software as a Service) et les PaaS (Platform as a Service), qui permettent aux entreprises de déployer facilement des applications blockchain basées sur une plateforme développée et maintenue par le fournisseur. Celle-ci peut être configurée selon différentes technologies (Ethereum, Hyperledger, Corda, etc.) et comprend notamment :

- Tous les composants d'infrastructure (réseaux, stockage, serveurs, virtualisation, etc.) ;
- Un réseau pair-à-pair constitué d'un ensemble de nœuds interconnectés permettant la gestion d'une copie de la blockchain et l'exécution des transactions et des smart contracts ;

- Un mécanisme de consensus permettant de mettre à jour de façon sécurisée la blockchain par les nœuds ;
- Un service de gestion des droits d'accès et d'adhésion au réseau pour les blockchains privées ;
- Des fonctionnalités de sécurité pour contrer les cyberattaques.
- Afin de permettre l'interaction avec la plateforme, le fournisseur de BaaS met également à disposition de l'entreprise :
- Une console pour administrer la plateforme ;
- Des outils pour programmer et déployer des smart contracts implémentant la logique business de l'application ;
- Des interfaces de programmation d'applications (API) et des kits de développement logiciel (SDK) pour déclencher des transactions dans la blockchain à partir des applications appelantes.

III.3 La sécurité de la blockchain

III.3.1 Sécurité de base de la blockchain

La sécurité de la blockchain est la gestion complète des risques pour un réseau de blockchain, utilisant dans le cadre cybersécurité, des services d'assurance et les meilleures pratiques pour réduire les risques d'attaques et de fraudes.

La technologie Blockchain produit une structure de données avec des qualités de sécurité inhérentes. Il est basé sur des principes de cryptographie, de décentralisation et de consensus, qui garantissent la confiance dans les transactions. Dans la plupart des blockchains ou technologies de registre distribué, les données sont structurées en blocs et chaque bloc contient une transaction ou un ensemble de transactions. Chaque nouveau bloc se connecte à tous les blocs qui le précèdent dans une chaîne cryptographique de telle sorte qu'il est presque impossible de falsifier.

Toutes les transactions au sein des blocs sont validées et acceptées par un mécanisme de consensus, garantissant que chaque transaction est vraie et correcte.

La technologie blockchain est basé sur la décentralisation, avec la participation des membres à travers un réseau distribué. Cela signifie qu'il n'y a pas de point de défaillance unique et qu'un seul utilisateur ne peut pas modifier l'enregistrement des transactions. Cependant, les technologies blockchain diffèrent sur certains aspects de sécurité critiques. Les réseaux blockchain peuvent différer quant à savoir qui peut participer et qui a accès aux données. Les réseaux sont généralement décrits comme publics ou privés, selon qui est autorisé à participer, et avec ou sans autorisation, selon la manière dont les participants accèdent au réseau.

Les réseaux publics de blockchain permettent généralement à quiconque de se joindre et aux participants de rester anonymes. Une blockchain publique utilise des ordinateurs connectés à Internet pour valider les transactions et parvenir à un consensus. Si on prend le Bitcoin qui est probablement l'exemple le plus connu de blockchain publique, et il parvient à un consensus grâce au « minage de bitcoins ». Les ordinateurs du réseau bitcoin, ou « mineurs », tentent de résoudre un problème cryptographique complexe pour créer une preuve de travail et ainsi valider la transaction. En dehors des clés publiques, il existe peu de contrôles d'identité et d'accès dans ce type de réseau.

Les blockchains privées utilisent l'identité pour confirmer l'adhésion et les privilèges d'accès et ne permettent généralement qu'aux organisations connues de se joindre. Ensemble, les organisations forment un « réseau d'affaires » privé et réservé aux membres. Une blockchain privée dans un réseau autorisé parvient à un consensus grâce à un processus appelé « approbation sélective », où des utilisateurs connus vérifient les transactions. Seuls les membres disposant d'un accès et d'autorisations spéciaux peuvent gérer le registre des transactions. Ce type de réseau nécessite davantage de contrôles d'identité et d'accès.

La technologie blockchain produit un registre de transactions infalsifiable, cependant les réseaux blockchain ne sont pas à l'abri des cyberattaques et de la fraude.

Les personnes mal intentionnées peuvent manipuler les vulnérabilités connues de l'infrastructure de la blockchain et ainsi divers piratages et fraudes ont été réussi au fil des ans. On peut citer certaines attaques : exploitation du code, clés volées, ordinateur d'un employé piraté. Les pirates informatiques et les fraudeurs menacent les blockchains de quatre manières principales : le phishing, le routage, les attaques Sybil.

Lors de la création d'une application de blockchain d'entreprise, il est important de prendre en compte la sécurité à toutes les couches de la pile technologique, et comment gérer la

gouvernance et les autorisations pour le réseau. Une stratégie de sécurité complète pour une solution de blockchain comprend l'utilisation de contrôles de sécurité traditionnels et de contrôles technologiques uniques.

Certains des contrôles de sécurité spécifiques aux solutions de blockchain d'entreprise incluent

- Gestion des identités et des accès
- Gestion des clés
- La confidentialité des données
- Communication sécurisée
- Sécurité des contrats intelligents
- Avenant de transaction

Il existe un certain nombre d'autres risques avec les solutions blockchain, et ils peuvent être classés en trois grandes catégories :

Affaires et gouvernance : les risques commerciaux comprennent les implications financières, les facteurs de réputation et les risques de conformité. Les risques de gouvernance émanent principalement de la nature décentralisée des solutions blockchain et nécessitent des contrôles stricts sur les critères de décision, les politiques de gouvernance, l'identité et la gestion des accès.

Processus : Ces risques sont associés aux différents processus qu'une solution blockchain requiert dans son architecture et ses opérations.

Technologie : la technologie sous-jacente utilisée pour mettre en œuvre divers processus et besoins commerciaux peut ne pas toujours être le meilleur choix, ce qui peut entraîner des risques de sécurité.

Certains de ces risques sont présentés dans le tableau 2.

Catégorie	Risque	Description des risques

Entreprise et gouvernance	La prise de décision	Une solution blockchain a un processus de gouvernance décentralisé qui crée des risques liés au manque de contrôle sur la conformité aux politiques et la prise de décision.
	Contrôles d'accès	Le manque de gouvernance centralisée peut également réduire le contrôle sur qui peut accéder à la plate-forme et le niveau d'accès fourni à chaque utilisateur.
	Financier	Les risques financiers dans une solution blockchain proviennent principalement du risque de transactions frauduleuses et de pertes de données critiques dues à des failles de sécurité potentielles.
	Risques d'audit, juridiques et de conformité	Certaines opérations sur la plateforme peuvent s'appuyer sur des données stockées en chaîne ou validées par des données en chaîne. Cela peut entraîner des problèmes avec les réglementations de conformité et la conformité aux audits des systèmes et des applications. Elle peut également introduire des risques juridiques qui définissent la responsabilité des données en question.
Processus	Gestion des identités et des accès (IAM)	Un accès non autorisé à la plate-forme peut avoir des conséquences désastreuses pour les membres avec une perte de données critiques, la suspension des opérations et un accès refusé. L'absence d'IAM peut également entraîner une invocation incorrecte de certaines fonctions de contrat intelligent.
	Communications sécurisées	Des communications non sécurisées entre différents nœuds au sein de la solution ou entre la solution et des composants externes peuvent entraîner une mauvaise direction, qui à son tour peut entraîner des problèmes de sécurité au niveau du transport. Cela peut également soulever des défis liés aux autorisations d'accès et aux menaces d'attaques internes.
	Solution vulnérable (codes non testés)	Les codes ou solutions non testés qui proviennent de processus ou de méthodologies non certifiés DLT peuvent être vulnérables au piratage et peuvent avoir un impact sur l'activité globale et l'opérabilité de la solution.
	Clés d'identité Blockchain sur le module de sécurité matérielle (HSM)	Lors de l'utilisation d'un HSM partagé pour stocker les clés d'identité de la blockchain, un ensemble de clés pour une organisation peut potentiellement être mélangé avec ceux d'une autre organisation.
	Sécurité des infrastructures	L'infrastructure sous-jacente qui est déployée pour l'architecture d'une solution blockchain peut avoir de nombreux problèmes, y compris un accès inutile et des paquets indésirables essayant d'entrer dans le réseau.

La technologie	Stockage, expiration et dysfonctionnement des clés	Les clés d'identité et les jetons de transaction de la blockchain sont un composant important de la solution. Les défis liés à l'expiration, au renouvellement, à l'archivage et à la révocation des certificats et des clés peuvent entraîner d'énormes risques pour le fonctionnement de la plate-forme.
	Sécurité des applications	La blockchain elle-même est immuable et infalsifiable, mais les applications qui exploitent le réseau posent des défis à tous les niveaux.
	Validation et authentification du grand livre partagé	Il est important de comprendre la validité et l'authenticité du grand livre partagé. Il s'agit également d'une technologie émergente et les risques associés sont parfois inconnus.
	Risques dans les contrats intelligents	Les contrats intelligents sont un élément important d'une solution blockchain, et toute faille logique dans la mise en œuvre de ces contrats ou de leurs transactions peut entraîner la validation de contrats ou de transactions incorrects.
	Risques liés à la suppression, à l'audibilité et au consensus	Il est important de prendre en compte les risques de suppression de parties lorsqu'une partie quitte le consortium et d'appliquer les procédures appropriées. La configuration du réseau distribué dans la blockchain est sujette à des risques d'audibilité et de consensus.

TABLEAU 2 : CATEGORIE DE RISQUE ET RISQUES ASSOCIES AVEC DESCRIPTION (W [9])

La sécurité d'une solution doit également être évaluée dans le contexte de son modèle de menace. La blockchain, par nature, offre de solides garanties d'intégrité des enregistrements, mais un certain nombre de choses peuvent mal tourner dans d'autres parties d'une application basée sur la blockchain, ce qui peut entraîner des compromis et des pertes. La clé pour sécuriser correctement une telle application est de développer un modèle de menace complet pour elle et d'atténuer les faiblesses identifiées.

Les modèles les plus connu sont les modèles d'usurpation d'identité, de falsification, de répudiation, de divulgation d'informations, d'attaques par déni de service et d'élévation de privilèges qui est utilisé pour étudier les relations entre les acteurs et les actifs, examiner les menaces et les faiblesses liées à ces relations, et proposer des atténuations appropriées.

Les applications blockchain intègrent souvent des composants externes - systèmes de gestion des identités et des accès (IAM), authentification multi facteur (MFA), infrastructure à clé

publique (PKI) et systèmes de réglementation et d'audit - qui sont détenus et gérés par des acteurs. Ces systèmes doivent être soigneusement examinés avant de pouvoir faire partie de la solution globale au fur et à mesure qu'ils sont développés ou contrôlés par des tiers.

La figure 1 prend en compte les différents facteurs et dérive un modèle de menace qui peut être appliqué dans une implémentation basée sur la blockchain.

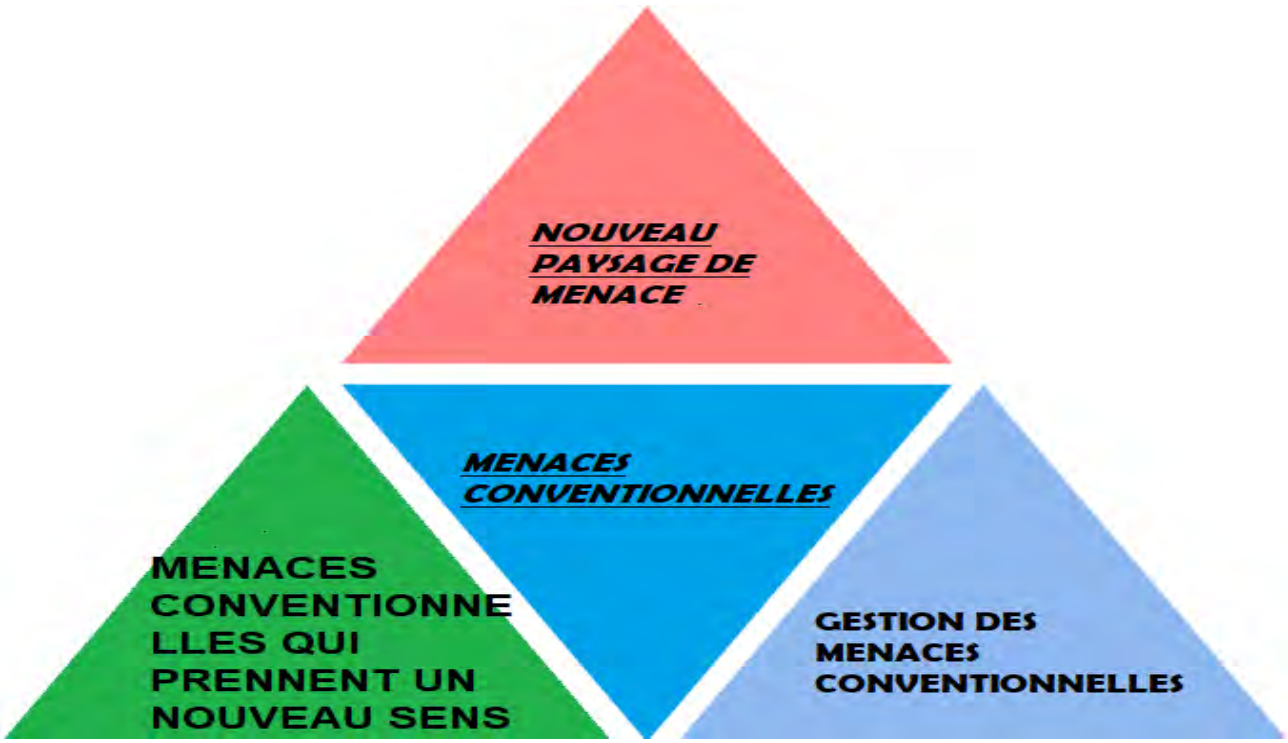


FIGURE 8 : MODELE DE MENACE DANS UNE SOLUTION BLOCKCHAIN

Les menaces illustrées dans la figure 1 peuvent être classées en trois catégories principales :

- Nouveau paysage de menaces - ce sont des menaces spécifiques à la blockchain.
- Les menaces conventionnelles qui prennent un nouveau sens - avec l'ajout de la blockchain, les menaces conventionnelles apportent un nouveau sens en ajoutant de nouvelles menaces.
- Gestion des menaces conventionnelles - ce sont les menaces globales qui doivent être traitées pour toute solution.

III.3.2 Nouveau paysage des menaces

- Dans cette infrastructure informatique unique, la blockchain introduit de nouveaux paradigmes qui peuvent ne pas être entièrement compris. La plupart des vulnérabilités résident dans les différents composants individuels et la façon dont ils sont assemblés.
- Le système comprend une multitude d'acteurs, chacun d'entre eux pouvant être doté de ses propres mécanismes de gestion de l'identité, il peut donc être difficile d'établir les mécanismes de confiance mutuelle nécessaires à une bonne gestion du consensus.
- Il est important de trouver un équilibre entre le détail des informations collectées afin d'identifier correctement les acteurs du système et la nécessité de gérer et d'éliminer en toute sécurité ces informations pour satisfaire à la législation sur la protection de la vie privée.
- Les attaques doivent être identifiées dans un paysage distribué d'actifs.
- La coordination de la détection, de la réponse et de la récupération entre tous les participants au réseau est indispensable.
- Les attaques structurées ne peuvent être identifiées que par des analyses sur plusieurs participants au réseau. Les attaques contre une blockchain sont plus susceptibles de réussir lorsqu'elles sont dirigées vers l'application et l'infrastructure de support. Les relations entre les participants et les différentes parties du système doivent être soigneusement orchestrées. Les attaquants peuvent essayer d'exploiter les complexités du système et mener des attaques qui exploitent ces relations de manière subtile.

III.3.2.1 Menaces conventionnelles qui prennent un nouveau sens

- De nouvelles vulnérabilités dans l'infrastructure de la blockchain et la falsification des contrats intelligents peuvent entraîner de nouvelles menaces.
- Dans une solution de blockchain décentralisée, l'usurpation d'identité de l'utilisateur et l'élévation incorrecte des privilèges peuvent entraîner de nouvelles menaces.
- Les données externes d'une solution blockchain peuvent être falsifiées ou volées, ce qui peut à son tour conduire à une menace dans une solution blockchain globale.
- Les clés et certificats compromis ou altérés peuvent conduire à une menace dans une solution blockchain

- La perturbation des services peut également constituer une menace.
- Les transactions malveillantes ou la répudiation peuvent donner lieu à des menaces supplémentaires.

III.3.2.2 Gestion conventionnelle des menaces

- Les tests de pénétration sont essentiels dans toute solution et s'appliquent également à une solution blockchain.
- L'analyse des vulnérabilités de l'ensemble de la solution atténue les menaces connues considérables.
- Des procédures d'analyse, de détection et de correction des menaces doivent être mises en place.
- Des plans d'intervention et de récupération en cas d'incident doivent être mis en place.
- Les meilleurs mécanismes de gestion des identités doivent être mis en place.
- La planification de la continuité des activités / la reprise après sinistre est la clé de toute solution blockchain.

III.3.3 Sécurité et bonnes pratiques de la blockchain

Pour la création d'une solution basée sur la technologie blockchain nous devons prendre les considérations suivantes :

- Le modèle de gouvernance des organisations participantes ou des membres
- Les fonctionnalités spécifiques propres à la blockchain
- Les données capturées dans chaque bloc
- Les exigences réglementaires pertinentes et comment les respecter
- Comment les détails de l'identité sont-ils gérés
- Les charges utiles de bloc sont-elles chiffrées
- Les clés sont-elles gérées et révoquées
- Le plan de reprise après sinistre pour les participants à la blockchain
- La posture de sécurité minimale pour les clients blockchain pour la participation
- La logique de résolution des collisions de blocs blockchain

Lors de la création d'une blockchain privée, assurez-vous qu'elle est déployée dans une infrastructure sécurisée et résiliente. De mauvais choix technologiques sous-jacents pour les

besoins et les processus métier peuvent entraîner des risques de sécurité des données en raison de leurs vulnérabilités. Pour la mise en place d'un bon politique de sécurité il faut tenir compte des risques commerciaux et de gouvernance.

Les risques commerciaux comprennent les implications financières, les facteurs de réputation et les risques de conformité. Les risques de gouvernance émanent principalement de la nature décentralisée des solutions blockchain et nécessitent des contrôles solides sur les critères de décision, les politiques de gouvernance, la gestion des identités et des accès.

La sécurité de la blockchain consiste à comprendre les risques du réseau blockchain et à les gérer. Le plan de mise en œuvre de la sécurité pour ces contrôles constitue un modèle de sécurité blockchain. Créez un modèle de sécurité blockchain pour vous assurer que toutes les mesures sont en place pour sécuriser adéquatement vos solutions blockchain.

Pour la mise en œuvre d'un modèle de sécurité de solution blockchain, les administrateurs doivent développer un modèle de risque capable de traiter tous les risques commerciaux, de gouvernance, de technologie et de processus. Ensuite, ils doivent évaluer les menaces pesant sur la solution blockchain et créer un modèle de menace. Ensuite, les administrateurs doivent définir les contrôles de sécurité qui atténuent les risques et les menaces en fonction des trois catégories suivantes :

- Appliquer des contrôles de sécurité propres à la blockchain
- Appliquer les contrôles de sécurité conventionnels
- Appliquer les contrôles métier pour la blockchain

III .3.3.1 Contrôles de sécurité propres à la blockchain

- Traitez l'infrastructure sous-jacente de la solution blockchain comme une infrastructure critique.

Pour garantir que toutes les pratiques de sécurité requises sont en place. Adoptez et appliquez une certification aux normes de l'industrie.

- Partitionnez et adoptez les meilleures pratiques d'espacement des noms afin de réguler l'accès.

La solution doit être partitionnée au moyen de canaux et d'espacement de noms afin de pouvoir héberger des actifs numériques pour tous les membres de la plate-forme. L'espacement de noms lui permet de réguler l'accès aux actifs numériques hébergés sur la plateforme. Compléter cela dès le départ permet également de réaliser des économies, car des modifications ultérieures peuvent nécessiter des retouches.

- Définir et appliquer les politiques d'approbation appropriées en fonction des contrats commerciaux.

La solution blockchain utilise des politiques d'approbation pour définir les critères qui doivent être remplis afin de confirmer qu'une transaction soumise est valide. Les exemples incluent le nombre de signatures requises et de quelles organisations. Ces politiques doivent être liées à un contrat intelligent pour prendre en compte la sécurité du réseau d'entreprise et de tous les actifs et données numérisés associés à ce contrat. En tant que meilleure pratique, ces stratégies doivent être définies et spécifiées au niveau de l'espace de noms (pour l'ensemble du contrat intelligent) ainsi qu'au niveau de la clé du grand livre (pour les entrées uniques dans la base de données d'état mondiale).

- Appliquez les contrôles d'identité et d'accès pour accéder à la solution et aux données de la blockchain.

Définissez des politiques qui garantissent le bon niveau d'accès à la bonne personne pour la bonne utilisation. Les nouveaux membres doivent être intégrés à la plate-forme blockchain via des mécanismes d'identité et d'accès appropriés. Le processus de débarquement doit également être défini pour arrêter toute exfiltration d'informations. Les journaux d'audit et les processus d'accès doivent être mis en place pour alerter l'équipe d'exploitation de toute activité malveillante afin qu'elle puisse être atténuée.

Si l'organisation utilise le système IAM interne et joue le rôle de fournisseur d'identité (IDP), des jetons appropriés tels que OAUTH, OIDC et SAML2 doivent être utilisés pour effectuer l'authentification, la vérification et l'autorisation. Cela s'applique également aux autres membres du consortium. Les décisions clés quant à savoir si les membres du consortium sont des PDI ou des prestataires de services (PS) doivent être prises à l'avance.

- Appliquez le module de sécurité matériel (HSM).

Il est essentiel d'utiliser un HSM pour sécuriser les clés d'identité de la blockchain. Il est également important de s'assurer que chaque organisation dispose de sa propre partition dans le HSM où les clés sont stockées. L'utilisation du HSM pour stocker les clés d'identité de la blockchain garantit la sécurité des clés. Le processus de partition HSM garantit que chaque organisation dispose d'une partition distincte avec des droits et des rôles d'administrateur distincts : responsable du chiffrement, utilisateur de chiffrement, super administrateur, etc.

- Utilisez une solution de gestion des accès privilégiés (PAM) pour les actions escaladées.

Utilisez une solution PAM pour vous assurer que les utilisateurs appropriés disposant des privilèges appropriés accèdent aux composants à des fins d'administration ou de gestion des modifications. Ceci est d'autant plus important que la plateforme peut avoir des informations confidentielles, y compris des données de transaction de paiement pour les utilisateurs et les membres.

Une solution PAM devrait être mise en place avec une rotation des mots de passe et une séparation efficace des tâches. Il est également important de configurer la journalisation de bout en bout pour capturer les flux de l'entrée à la sortie. L'accès aux secrets doit être lié à un système de billetterie, et chaque publication secrète doit avoir un réviseur. Chaque instance d'accès administratif doit être attribuée à un ticket approuvé ou à une modification.

- Utilisez les meilleures pratiques de sécurité des API pour protéger les transactions basées sur les API.

Les API sont la principale forme de communication entre les différentes parties d'une solution blockchain. Les API doivent être protégées de toute utilisation inappropriée et limitées à la portée de la transaction. Bien que la sécurité des API englobe un certain nombre de choses, trois contrôles clés doivent être appliqués pour toutes les API : identification, authentification et autorisation. Il est important de tirer parti d'une norme de l'industrie comme OAUTH, non seulement pour normaliser les interactions, mais également pour sécuriser les API.

- Tirez parti d'un magasin de secrets pour les applications et l'accès privilégié.

La solution blockchain comporte un certain nombre de composants qui interagissent les uns avec les autres avec des transactions basées sur les utilisateurs et les API. Certaines de ces transactions sont basées sur des clés statiques telles que des mots de passe, des jetons ou des certificats. Ces clés doivent être stockées dans un magasin de secrets (où les clés sont chiffrées), et l'accès au moment de l'exécution doit être limité en fonction de l'utilisation. Le magasin de secrets doit prendre en charge un audit granulaire pour la conformité et la gestion des menaces.

- Adopter une approche de classification des données pour protéger les données / informations.

Identifier et classer les données liées aux problèmes commerciaux, juridiques et techniques afin que les contrôles de sécurité des informations appropriés puissent être appliqués pour protéger les données et la confidentialité. La classification des données doit être appliquée en permanence pour tous les membres de la solution blockchain.

- Utilisez des technologies de protection de la vie privée pour les informations sensibles.

Tirez parti de la technologie du grand livre autorisé où la confidentialité est un principe de conception et fournissez des contrôles pour protéger les informations de confidentialité des membres. En outre, appliquez des contrôles de sécurité préservant la confidentialité pour masquer les informations de transaction, telles que l'identité du créateur de la transaction et les détails de la transaction.

- Protégez les applications des vulnérabilités et protégez les données.

Tirez parti de DevOps pour automatiser l'analyse des vulnérabilités des applications pendant le cycle de vie du développement. Il est également essentiel de mettre en œuvre la sécurité des données à différents niveaux (tels que l'application et la base de données) conformément à l'analyse de classification des données.

- Appliquez le contrôle d'accès dans les contrats intelligents.

Les contrats intelligents sont un élément clé d'une solution blockchain et ils appliquent des politiques alignées sur les objectifs commerciaux. Par conséquent, tous les aspects des contrats intelligents doivent être sécurisés. Une attention particulière doit être accordée au contrôle d'accès à la gestion intelligente du cycle de vie des contrats, à l'accès fin au sein du contrat intelligent et aux processus ou applications avec lesquels le contrat intelligent collaborera.

- Tirez parti des modules de plateforme sécurisée (TPM) pour l'exécution de code sensible.

Certains composants de la solution sont plus critiques que d'autres, et ces composants critiques doivent utiliser des modules de plateforme fiables. Cela facilite le stockage du matériel cryptographique - activé par les HSM. Ils permettent également l'exécution de code de chaîne préservant la confidentialité de sorte que l'administrateur du nœud ne puisse pas altérer l'exécution sans être détecté.

- Communications sécurisées à la fois en interne et en externe.

Assurez-vous que toutes les communications sur la plate-forme entre les composants qui interagissent en interne et en externe passent par un canal hautement sécurisé. Cela peut être fait à l'aide de solutions TLS (Transport Layer Security) mutuelles ou standard. Des niveaux de sécurité supplémentaires peuvent être utilisés, y compris la liste d'autorisation IP et la rotation fréquente des clés.

III .3.3.1 Contrôles de sécurité conventionnels

- Utilisez les normes et systèmes de sécurité d'entreprise pour garantir un cycle de vie de développement logiciel sécurisé, une analyse des applications et des politiques de sécurité appropriées.

  Toutes les politiques d'entreprise, normes et plates-formes de sécurité communes doivent être utilisées. Cela offre cohérence, fiabilité, familiarité et efficacité opérationnelle.

- Mettez en place des capacités de gestion des identités et des accès pour l'intégration des utilisateurs.

Utilisez les outils standard de gestion des identités et des accès (IAM) pour l'authentification, le contrôle d'accès et le stockage des données d'identité.

- Mandater l'authentification multi facteur.

Mandate l'authentification multi facteur (MFA) pour l'accès à la blockchain, ainsi que les outils IAM standard. Les utilisateurs et les administrateurs doivent utiliser MFA sans exception.

- Utilisez une gestion solide des clés cryptographiques / certificats.

Utilisez une solution de gestion de clés solide et fiable pour gérer le nombre de clés utilisées dans la solution blockchain, y compris les clés d'identité blockchain, les certificats TLS internes, les certificats TLS externes et les certificats de domaine.

Utilisez une solution PKI interne efficace pour gérer les certificats TLS internes.

Prenez les décisions appropriées de l'autorité de certification pour les certificats TLS externes.

- Tirez parti de la gestion des incidents et des événements de sécurité.

Les organisations doivent établir des flux d'événements de sécurité de la plate-forme vers les membres, et pour les informations d'événements sélectionnées entre les membres. La gestion des incidents et événements de sécurité (SIEM) dans tous les composants de l'architecture est essentielle.

- Tirez parti de la sécurité matérielle.

Tirez parti d'un module de sécurité matériel (HSM) pour stocker les données clés critiques. Étant donné que la plate-forme proposée compte plusieurs membres, l'architecture proposée doit évaluer HSM et son impact. Un protocole ouvert commun pour utiliser HSM est nécessaire pour continuer sur la plate-forme.

Stockez les clés dans des partitions appropriées avec un accès contrôlé pour les membres.

Appliquer la sécurité des applications.

L'application de mesures de sécurité pour les composants individuels garantit que la solution globale ne présente aucune faille de sécurité.

- Appliquer la sécurité de l'infrastructure.

La sécurité de l'infrastructure du réseau et des données stockées sur la plate-forme est essentielle. L'infrastructure sous-jacente (y compris tous les composants logiciels et matériels) sur laquelle la solution blockchain est déployée doit être sécurisée.

- Effectuez des tests de pénétration complets et une évaluation des vulnérabilités.

Assurez-vous d'effectuer des tests de pénétration complets à chaque phase du déploiement de la solution. Il est important d'effectuer des évaluations de vulnérabilité au niveau des

composants de l'organisation individuelle et pour le système global afin de s'assurer que tous les problèmes sont résolus.

III .3.3.1 Contrôles commerciaux

- Définir et mettre en œuvre la gouvernance de la sécurité.

Assurez-vous de mettre en place une gouvernance de la sécurité via diverses politiques, mécanismes de contrôle d'accès et rapports.

Définissez une loi applicable exclusive pour la plate-forme, quel que soit l'emplacement du nœud, afin de garantir que le client bénéficie de la sécurité et de la certitude des lois régissant les litiges et les réclamations juridiques.

- Assurez-vous que la conformité et les contrôles juridiques sont en place.

La responsabilité est un élément important, et chaque organisation est susceptible d'avoir ses propres exigences qui sont dictées par ses services juridiques. Pour cette raison, il est essentiel de définir explicitement la responsabilité de chaque membre et du vendeur en cas de violation ou de violation de la sécurité. Confirmez la conformité avec les audits du système et des applications pour vous assurer que ce risque est atténué.

- Définir, définir et mettre en œuvre des contrôles opérationnels.

Une solution blockchain nécessite une liste complète des processus de sécurité, qui doivent être compilés et suivis une fois que les phases de conception et de construction sont terminées et que la solution est déployée. Chaque acteur, chaque processus opérationnel et toutes les instructions de travail doivent être mis en place pour garantir que le projet fonctionne sans aucune faille de sécurité.

Conclusion

Dans cette partie nous avons défini la blockchain et expliqué les composants essentiels nécessaires pour sécuriser une solution blockchain. L'externalisation de l'infrastructure et des ressources informatiques étant souvent l'orientation privilégiée par les entreprises, plusieurs offres de BaaS sont aujourd'hui proposées par les géants du cloud et permettent de rendre l'adoption de la blockchain plus simple, moins coûteuse et moins risquée.