Les Blockchains

De la théorie à la pratique, de l'idée à l'implémentation

*Témoignage de **Michel BELLANGER**, Directeur Marketing - Data Strategist*

Dr. Billal CHOULI
Frédéric GOUJON
Yves-Michel LEPORCHER

informatique technique

Fichiers complémentaires à télécharger

Collection EPSILON

Table des matières

Les éléments à télécharger sont disponibles à l'adresse suivante :
http://www.editions-eni.fr
Saisissez la référence de l'ouvrage **EPBLOC** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Chapitre 3
La cryptographie et la Blockchain

Chapitre 4
Les systèmes distribués et le consensus

Chapitre 5
Les Blockchains : leurs types et leur sécurité

Chapitre 6
Les smart contracts ou contrats intelligents

Chapitre 7
Blockchain 2.0 : les applications décentralisées

Chapitre 8
Développement d'une application décentralisée

Chapitre 9
Création d'un portefeuille et d'une Blockchain

Chapitre 10
Lier la Blockchain à d'autres applications

Chapitre 11
L'écosystème de la Blockchain 2.0

Chapitre 12
Initiatives en faveur de la Blockchain

Chapitre 13
La Blockchain et le Big Data

Chapitre 14
Les limites de la technologie

Chapitre 5
Les Blockchains : leurs types et leur sécurité

1. Quelle sécurité pour la Blockchain ?

Pour aborder la sécurité, nous allons parler de deux sujets : les clés publiques/privées et la traçabilité.

1.1 Les clés publiques/privées

Dans la Blockchain, une clé privée vous permet de signer vos transactions, des clés publiques permettent au réseau de vérifier qui sont les détenteurs des comptes. Avec ce système, vous pouvez déposer un document (contrat, brevet…) sur la Blockchain, ce dernier sera crypté aussi longtemps que nécessaire. Il pourra devenir lisible au moment où vous le voudrez simplement en publiant la clé de chiffrement. Toutes les versions hébergées sur la Blockchain deviendront alors lisibles par tous. Le fait que tout soit horodaté permettra de certifier la date de dépôt de votre document sur la Blockchain. Mais attention, la sécurité de la Blockchain est assurée tant que la majorité des mineurs honnêtes contrôlent plus de puissance de calcul qu'un groupe de mineurs ayant des intentions malhonnêtes. Il faut donc que la majorité des intervenants ne soient pas malveillants, plus le réseau est grand, plus le nombre d'ordinateurs nécessaire pour en représenter plus de la moitié du réseau sera élevé, plus il deviendra coûteux d'en prendre le contrôle.

Si une personne ou un groupe de personnes arrive à représenter plus de la moitié des ordinateurs du réseau à des fins malintentionnées, nous parlons d'une attaque à 51 %. Est-ce possible ? Une attaque à 51 % ne peut pas être utilisée pour dérober de la crypto-monnaie qu'on ne possède pas (la clé privée protège toujours), mais elle peut impacter toutes les nouvelles transactions en provoquant en très peu de temps l'engorgement et l'effondrement de la monnaie.

Satoshi Nakamoto, le créateur de Bitcoin, avait envisagé ce type d'attaque, mais il avait imaginé le système conformément à l'idée que cela serait très compliqué d'amasser assez de puissance de calcul. Pour pouvoir lancer une attaque à 51 %, il faudrait disposer de la même puissance que le reste du réseau plus un epsilon infinitésimal, ce qui est très difficile pour une seule personne.

Il est important de mentionner que le basculement arrive vraiment à partir de 50 % plus quelque chose. Une attaque à 50,1 % serait plus dévastatrice qu'une attaque à 49 %. Dès qu'on dépasse le seuil fatidique des 50 %, on a la garantie mathématique de pouvoir altérer la Blockchain. Mais vous l'aurez compris, plus la Blockchain est importante, plus il est compliqué d'en représenter plus de 50 %.

Mais revenons à la sécurité Blockchain basée sur les clés privées et publiques. Quel est le fonctionnement ? Nous pouvons prendre l'image d'une boîte aux lettres. La fente de cette dernière permet à tout le monde de déposer des documents à l'intérieur. Cela correspond à la clé publique. Par contre, pour accéder aux documents, le propriétaire de la boîte aux lettres possède une clé pour l'ouvrir. La clé de la boîte aux lettres correspond à la clé privée. Donc, pour résumer, la clé publique permet de déposer des objets, la clé privée permet de les ouvrir et de les lire. Une clé privée permet de calculer une clé publique, mais l'inverse est impossible. Cette méthode a pour nom la cryptographie asymétrique, car les clés ne sont pas identiques et n'ont pas le même rôle. Dans le cas de Bitcoin, vous possédez également une adresse. Elle est calculée à partie d'un hash de la clé publique, clé publique elle-même calculée à partir de la clé privée. Si nous reprenons l'exemple de la boîte aux lettres, l'adresse Bitcoin correspond à votre adresse postale, permettant à votre facteur ou à un livreur de retrouver votre boîte aux lettres pour y déposer lettres et colis. La clé publique permet donc d'authentifier une adresse. Ce point est extrêmement important dans le fonctionnement de la Blockchain et son mécanisme de traçabilité.

© Editions ENI - All rights reserved

Lorsque votre compte Blockchain effectue une transaction, il inclut la clé publique dans chaque signature, permettant de valider que vous en êtes à l'origine.

Vous aurez compris l'importance de la clé privée, aussi précieuse voire plus que votre code de carte bleue. Certains mettent en place un « cold storage » (stockage à froid) de leur clé privée (donc pas d'enregistrement sur un ordinateur connecté à Internet) en enregistrant cette clé sur un papier placé dans un bon vieux coffre-fort physique.

1.2 La traçabilité des transactions

Pour qu'une transaction soit validée, il faut que le bloc soit rattaché à la chaîne. Pour ce faire, un utilisateur doit valider son contenu, c'est le rôle des « mineurs ». Un mineur, c'est tout simplement un utilisateur qui a mis son ordinateur en lien avec la Blockchain pour que sa puissance de calcul soit utilisée pour le fonctionnement de la Blockchain. Dans le cas des crypto-monnaies, les mineurs vérifient que l'argent est bien en votre possession et ils retracent l'historique de cet argent en validant les blocs précédents. Une fois que tout est vérifié, la transaction est validée. Tout ceci est théoriquement sans faille car tout l'historique est vérifiable : le bloc contient dans son en-tête les références aux blocs précédents. Pour falsifier un bloc, il faudrait modifier tous les blocs membres de cet historique. Étant donné que les données sont décentralisées et dupliquées, il est impossible de mettre en œuvre cette opération illicite. Tout est donc scruté et vérifié par les mineurs, les transactions validées, les données décentralisées, mais vous restez anonyme.

2. Blockchain publique ou privée ?

La Blockchain "historique", c'est la Blockchain publique. C'est-à-dire une Blockchain que n'importe qui dans le monde peut lire. Chacun peut lui envoyer des transactions et s'attendre à ce qu'elles soient incluses dans le registre, du moins tant que ces transactions respectent les règles de cette Blockchain. C'est le cas de Bitcoin par exemple, pour lequel chacun a libre accès au registre. Chacun participe également librement au processus d'approbation, celui qui permet de décider quel bloc sera ajouté à la chaîne et qui définit l'état actuel du système.

2.1 Les Blockchains de consortium (Blockchains sous contrôle)

Dans les Blockchains « de consortium », un certain nombre de nœuds sont en charge du processus d'approbation, c'est-à-dire que le consensus est contrôlé par un ensemble présélectionné de nœuds. Par exemple, une trentaine d'organisations pourraient se mettre d'accord et mettre en place une Blockchain dans laquelle un bloc devrait être approuvé par au moins quinze d'entre elles pour être valide. Nous voyons donc deux différences importantes par rapport au système originel : non seulement les participants au processus d'approbation sont limités et sélectionnés, mais en plus, ce n'est plus la règle de la majorité qui s'impose. Dans ce cas, la Blockchain est partiellement décentralisée.

Le droit de lire la Blockchain, c'est-à-dire l'accès au registre, peut alors être public, réservé aux participants, ou bien hybride.

2.2 Les Blockchains privées (permissioned)

Dans les Blockchains privées, le processus d'approbation est limité à un unique acteur, bien que les autorisations de lecture par exemple puissent être publiques ou partiellement limitées. La Blockchain est dite centralisée, elle perd donc l'intérêt d'être décentralisée mais garde la particularité d'être cryptée. L'usage d'une Blockchain purement privée est donc limité comparé à l'usage d'une Blockchain contrôlée ou purement publique.

© Editions ENI - All rights reserved

Les Blockchains privées ou de consortium ont néanmoins plusieurs avantages, attractifs pour les institutions financières, qui peuvent expliquer l'intérêt qu'elles leur portent depuis peu : gouvernance simplifiée, acteurs connus, coûts réduits, rapidité, confidentialité. Le tout sans la perte de contrôle qu'implique la version publique issue de Bitcoin. Une évolution à surveiller qui sera sans doute au cœur du futur des Blockchains !

2.3 Les Blockchains publiques (unpermissioned)

Tout le monde peut lire et écrire et participer au processus de consensus, sans limites. Nous sommes dans le cas d'une ouverture totale. Il existe plusieurs Blockchains publiques et chacun est en droit de créer la sienne. En tant que substituts aux réseaux centralisés, ces Blockchains ont un fonctionnement basé sur des principes crypto-economiques définis par Vitalik Buterin : "La combinaison d'incitations économiques et les mécanismes de vérification en utilisant la cryptographie comme une preuve de travail ou preuve de la participation." Autrement dit, chacun est incité à participer à la vérification des transactions par des avantages économiques. La part que chacun peut prendre dans le processus de consensus est définie en fonction des ressources qu'il peut mettre à disposition. Mais le risque avec ce mode de fonctionnement, c'est que le traitement soit au final réalisé sur de gros pools de mineurs extrêmement puissants. Le fonctionnement pourrait alors s'apparenter à une Blockchain publique avec un fonctionnement de Blockchain de consortium. Mais, les Blockchains publiques restent entièrement décentralisées.

2.4 La gouvernance de la Blockchain

Le degré de gouvernance dépend du mode de Blockchain. Plus il est ouvert, moins nous pouvons y mettre de gouvernance. Il nous faut donc faire la distinction entre les Blockchains publiques, de consensus et privées.

Pour une Blockchain publique, c'est aux nœuds du réseau de valider les choix discutés et initiés par les développeurs en décidant de valider ou non les modifications proposées. La seule règle de fonctionnement est définie par la technologie (selon l'expression, « Code is Law » du juriste américain Lawrence Lessing).

En revanche, pour une Blockchain privée ou de consensus, le processus de consensus ne peut être réalisé que par un nombre limité et prédéfini de participants. L'accès en écriture est contrôlé par une organisation ou un groupe d'organisations. L'accès en lecture, quant à lui, peut être restreint ou totalement public.

© Editions ENI - All rights reserved