Faut-il adapter la blockchain à la cybersécurité ?

	Faut-il adapter la blockchain à la cybersécurité ?

En suivant l'actualité des nouvelles technologies, il est difficile de passer à côté d'un nouveau « buzz world » qui enflamme les débats : Blockchain ou chaîne de blocs en français. Initialement inventée pour les crypto-monnaies (comme Bitcoin par exemple), la technologie blockchain connait un développement rapide (même la banque de France lance une étude sur l'architecture blockchain) et certains prédisent même une révolution comparable à l'invention du protocole TCP-IP. Il nous a semblé utile de creuser un peu cette technologie afin d'imaginer son impact potentiel dans le domaine de la cybersécurité.

La blockchain Késako ?

Le concept de la chaine de blocs repose sur la décentralisation par opposition à un système pyramidal et hiérarchisé. La chaine permet de regrouper l'ensemble des transactions effectuées par ses membres depuis sa création. Il s'agit en quelque sorte d'un grand livre de compte, anonyme et infalsifiable (certaines chaines sont publiques et d'autres privées).

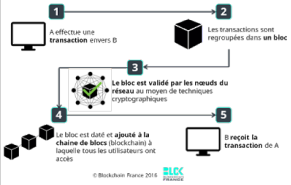
(Image issue du site: blockchainfrance.net)

Le site présente alors le système comme suit:

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 noeuds 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 constitue en la résolution de problèmes algorithmiques..

Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau.



*Plusieurs techniques existent pour « valider » un bloc. Bitcoin utilise la « **proof of work** » – PoW- (preuve de travail) où chaque noeud (mineur) doit effectuer un calcul cryptographique, mais d'autres utilisent la « proof of stake« (PoS) où l'utilisateur doit faire la preuve qu'il détient une certaine quantité de monnaie partagée. Le projet **Ethereum** tente de faire basculer le PoW vers une forme de PoS. **La question de la validation par la communauté est essentielle dans le concept de blockchain, il en est l'essence mais également la fragilité**. En effet, cette étape engendre un temps de latence (jusqu'à 15 min pour Bitcoin) qui rend difficile l'implémentation généralisée de ces techniques. En outre, les « mineurs » consomment de l'énergie à effectuer des calculs cryptographiques inutiles, en clair le PoW ne produit rien (à part de la chaleur et une bonne facture d'électricité).*

Pourquoi faut-il adapter la blockchain à la cybersécurité ?

Que peut-on retenir de cette présentation rapide? En premier lieu la technologie Blockchain permet de supprimer les intermédiaires et les autorités centrales en favorisant un système totalement distribué. En matière de sécurité des systèmes d'information de nombreuses applications reposent sur une « autorité de certification » (signature électronique, certificats etc…). Cette dernière est garante de la confiance entre tiers lors des échanges (messagerie, commerce, déclarations en ligne, vote…), dans ce contexte, blockchain pourrait largement modifier notre environnement. Au sein d'une structure (entreprise ou administration) la sécurité des échanges pourrait ainsi être garantie par la mise en place d'une chaine locale (qui a en outre l'excellente idée d'être auditable).

*Un des développement récent de la blockchain réside dans la notion de « **smart contracts**« :*

les smart contracts sont des programmes, accessibles et auditables par toutes les parties autorisées, dont l'exécution est donc contrôlée et vérifiable ; conçus pour exécuter les termes d'un contrat de façon automatique lorsque certaines conditions sont réunies. Les règles qui régissent le programme peuvent notamment recouvrir tout événement vérifiable de façon informatique

*On peut donc imaginer un développement permettant d'améliorer la détection d'intrusion en implémentant la technologie blockchain au sein même d'un réseau d'entreprise. La confiance entre machines reposerait alors sur des « **smart contracts** » qui, lorsqu'ils sont rompus (machine compromise) déclencheraient des mécanismes d'alerte.*

*Outre la détection d'intrusion au sein d'un réseau de confiance « monitoré » par une blockchain, les applications les plus triviales devraient voir le jour dans les échanges entre systèmes connectés. Là encore, le double intérêt de la technologie repose sur la notion de **confiance décentralisée** et de**traçabilité** deux aspects essentiels pour la cybersécurité.*

La route est encore longue…

En dépit de nombreux avantages et de promesses alléchantes, la technologie blockchain est encore en phase d'expérimentation dans bien des domaines et ne semble pas (à ce jour) en mesure de « passer à l'échelle » pour des applications immédiates en matière de cybersécurité (détection d'intrusion, prévention des attaques etc.). Les limites juridiques ne manqueront pas d'émerger, les tentatives de détournements et de contrôle pour revenir à un état ante en « étoile » et contrôlé sont autant d'obstacles sur le chemin.

Enfin, les expérimentations devront chercher à valoriser l'étape de validation afin de limiter l'empreinte énergétique de cette technologie. Si sous bien des aspects la comparaison avec l'arrivée de TCP-IP est valable, le « modèle blockchain » semble toutefois porteur de changements plus profonds. Le monde de la cybersécurité devrait sans nul doute se lancer rapidement dans la course et expérimenter de nouvelles techniques de défense… [Lire la suite]

Pour aller plus loin:

https://blockchainfrance.net/

https://www.ethereum.org/

https://fr.wikipedia.org/wiki/Cha%C3%AEne_de_blocs

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, arnaques Internet…) et judiciaires (contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Suivez-nous sur

Réagissez à cet article

Source : *Cybertactique: BlockChain et cybersécurité, en route vers une révolution ?*