Lettre des "Lundi de la cybersécurité" no 55

Lutte des cryptomonnaies travail ou enjeu

Preuve de travail ? Preuve d'enjeu ? Quel protocole de consensus ?

Ce 15 septembre 2022, un évènement est intervenu qui pourrait changer la face des cryptomonnaies : Ethereum prenait la résolution de passer de la preuve de travail à la preuve d'enjeu. Qu'est-ce que cela signifiait ? Le monde des cryptoactifs allait-il changer de base ?

Dans le même temps, je recevais un bouquin que m'envoyait son auteur, le professeur Jean-Paul Delahaye, livre préfacé par le professeur Jean-Jacques Quisquater « **Au-delà du Bitcoin** », Par ce livre clair et très pédagogique, j'ai beaucoup appris sur les cryptomonnaies et sur leurs bases, les blockchains.

L’idée m’est venue de vous faire profiter de leur compétence et de leur pédagogie dans un Lundi de la cybersécurité.

Les transactions en attente, que ce soit pour acheter ou vendre des crypto monnaies ou pour enregistrer un contrat intelligent comme avec Ethereum qui ne gère pas que des cryptomonnaies, sont regroupées sans un bloc de données. Ce bloc est horodaté, signé, validé par consensus et ajouté à un serveur de la blockchain et transmis automatiquement à tous les autres serveurs qui constituent cette blockchain. Le problème est : **Qui est mandaté**, avec consensus de tous les validateurs, pour ajouter ce bloc dans ceux qui existent déjà dans la blockchain ? Tout est là, **c’est le protocole de consensus**.

Dans la stratégie du Bitcoin, basé sur la preuve de travail PoW, c’est le « mineur » qui a trouvé le premier la solution à un problème mathématique très coûteux en ressources de calculs, solution basée sur la constitution du bloc de données avec ajout d’un nonce (partie aléatoire) qui doit donner, en passant par un algorithme de calcul de condensat, le SHA256, une valeur inférieure à un seuil (avec un certain nombre de 0 en tête du condensat). Il faut pour cela que les mineurs exercent une multitude d’essais de calculs de condensats et celui qui gagne, par un coup de chance a forcément utilisé, beaucoup de ressources en calculs et beaucoup d’énergie électrique. A quoi sert le résultat ? A rien d’autre que permettre au mineur d’ajouter son bloc et d’être rémunéré en fractions de Bitcoins pour avoir le premier réussi à trouver une solution, et cela toutes les 10 minutes actuellement.

Dans la stratégie d’Ethereum, passé maintenant à la preuve d’enjeu, chaque validateur place une somme en séquestre, par exemple en fractions d’ethers, la monnaie d’Ethereum. Plus la mise d’un validateur est importante, plus il a de chances d’être celui qui pourra ajouter un cloc. Mais attention ! S’il triche, il perd sa mise.

Wallet, Halving, Nonce, SHA256, Fork, attaque 51%, attaque Sybil, et bien sûr importance du Merge d'Ethereum qui adopte la POS après avoir fonctionné avec la POW, je laisse les deux sommités internationales que nous invitons pour nous parler de tout ça au Lundi de la cybersécurité de janvier. Ces deux professeurs sont ainsi de grands pédagogues qui savent faire comprendre même les notions les plus complexes.

Je donne la plume au Professeur Jean-Jacques Quisquater

En introduisant rapidement les blockchains, je parlerai des preuves dans le contexte de ces blockchains, et leur histoire, en partant de la première (Haber-Stornetta, 1990) qui voulait résoudre une question d'estampillage ("le cachet de la poste"), d'une part, jusqu'à aujourd'hui où cela dépasse de beaucoup les questions de cryptomonnaies. Il y aura un peu de cryptographie. Il faudra aussi parler des monnaies électroniques, plus large que les cryptomonnaies, en partant du problème de la double dépense que veut résoudre bitcoin : cela le dépasse aussi, regardons les billets électroniques de train, de spectacles, etc. Et, enfin, les problèmes de la décentralisation (généraux byzantins, etc) dans les réseaux, et ses solutions : un problème central en ce moment :-). Je parlerai en termes simples des propriétés des diverses solutions. L'accent sera mis sur deux propriétés : la cybersécurité et la consommation des ressources. Ceci est souvent vu comme antagoniste : comment concilier cela ?

Je donne la plume au Professeur Jean-Paul Delahaye

Aujourd'hui que fonctionnent plusieurs blockchains de cryptomonnaies très importantes en capitalisation (plusieurs centaines de milliards de dollars pour les premières) il est possible de faire une sorte de bilan de leur robustesse aux attaques, et des conséquences concrètes de leur fonctionnement. Ce bilan concernera bien sûr la consommation électrique du réseau des validateurs et de leurs associés (les « mineurs » dans le cas du Bitcoin), mais concernera aussi la consommation de composants électroniques, l'incitation au vol d'électricité, etc. Je défendrai le point de vue qu'il ne fait plus aucun doute que la « Preuve d'enjeu » doit être préférée à la « Preuve de travail », cette dernière s'étant révélée être une sorte de piège logique et économique dont malheureusement il est difficile de sortir, comme le montre le cas d'Ethereum qui a mis plus de quatre années à se libérer de la « Preuve de travail », chose faite depuis le 15 septembre 2022.

Je reprends la plume

Jean-Paul Delahaye donne clairement sa préférence à la Preuve d'enjeu. Il nous livrera ses arguments.

Qui est le professeur Jean-Jacques Quisquater ?

Jean-Jacques Quisquater est un cryptologue belge, professeur à l'université catholique de Louvain en Belgique, et membre de l'ARCSI. Docteur d'État en science informatique obtenu au Laboratoire de recherche en informatique de l'université d'Orsay, il est membre de l'IEEE

Qui est le professeur Jean-Paul Delahaye ?

Jean-Paul Delahaye est docteur d'Etat en mathématiques sur la théorie des transformations de suites. Informaticien, professeur émérite à l'université de Lille, Campus Scientifique CRISTAL, Centre de recherche en informatique signal et automatique de Lille. Il écrit des articles dans la chronique « Logique et calcul » de la revue Pour la Science.

Demande d'inscription pour le Lundi de la cybersécurité de janvier

Lundi 16 janvier à partir de 18 h 00, en ligne par visio conférence Zoom et sur place à l'université de Paris, 45 rue des Saints-Pères, Paris 6e

Nos « Lundi de la cybersécurité » **sont gratuits** et veulent vous offrir une fête technologique qui marque les esprits, nous nous y employons. **Demandez votre inscription, par courriel** et vous recevrez un hyperlien personnel vers la visioconférence un peu avant le jour de l'événement, ou si vous demandez de venir sur place, les coordonnées de l'amphi.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Dans le message d'inscription, nous apprécierions que vous écriviez quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité. Evitez le style télégraphique, nous sommes toujours heureux de vous lire et de connaître votre intérêt pour nos événements.

Et n'oubliez pas de préciser si vous souhaitez être en présentiel 45 rue de Saints-Pères Paris 6e ou à distance par Zoom.

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués à l'intervenant.

Un quart d'heure avec Arnaud Coustillière, président du Pôle Excellence Cyber

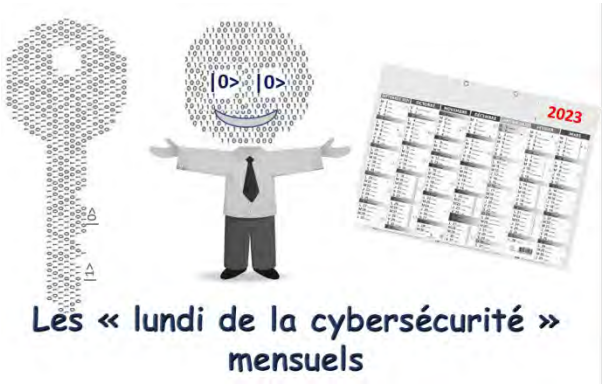
PÔLE D'EXCELLENCE CYBER

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses, autour de 19h15, nous donnons pour quinze minutes la parole à une organisation, qui opère dans l'écosystème du numérique et dans la sécurité de l'Information.
Le discours de 60 mn des intervenants sera suivi, pour le quart d'heure des initiatives, par l'intervention du **vice-amiral d'escadre (2S) Arnaud Coustillière, président du Pôle Excellence Cyber (Rennes & Paris)**.

Retour sur les Lundi de la cybersécurité précédents.

Vous trouverez tous les détails, slides, enregistrements sur le web de l'ARCSI, en https://www.arcsi.fr/ pour les plus récents et en https://www.arcsi.fr/evt_passes.php pour les évènements plus anciens. Les quarts d'heures accordés aux initiatives se trouvent en première page du site de l'ARCSI, là où sont les logos des organisations qui se sont déjà exprimées dans nos Lundi précédents.

Gérard



Lundi de la cybersécurité de février

lundi 6 fév. 18h-20h

Avec Cédric Cartau, RSSI CHU de Nantes

La cyber en santé et ses spécificités