

Lettre des "Lundi de la cybersécurité" no 46

Blockchains dans la cybersécurité et cybersécurité des blockchains



Lundi 14 mars
18h00-20h00

En visioconférence



Blockchains dans la cybersécurité et cybersécurité des blockchains



Intervenant **Renaud Lifchitz**
Directeur scientifique - Holiseum



Organisateurs



Ahmed Mehaoua
Professeur chercheur
Université de Paris



Béatrice Laurent



Gérard Peliks

La blockchain une base pour la cybersécurité ? mais quelle cybersécurité pour la blockchain ?

Renaud Lifchitz, certains d'entre vous l'ont vu se produire à notre Lundi de la cybersécurité de janvier 2021 sur le sujet *Génomique et cybersécurité* ? Quel spectacle ce fut ! ARN messenger, séquençage du génome, prédiction sur l'avenir de sa santé, Renaud a déployé toute la mesure de ses connaissances et de son talent.

Renaud revient sur scène pour nous présenter, dans notre **Lundi de la cybersécurité du mois de mars 2022**, le lundi 14 mars, un autre sujet d'actualité autour de la **blockchain**. Je précise, ce ne sera pas un événement centré sur le Bitcoin, son minage et son économie, Renaud insistera sur les nombreuses autres applications de la blockchain dans la cybersécurité et sur la cybersécurité de la blockchain. Annuaire ouvert à tous en lecture, mais en écriture seulement à quelques-uns, annuaire pouvant être dupliqué sur de multiples plateformes réparties autour du monde (voilà pour la disponibilité) ; constitué de blocs d'information,

chaque bloc étant lié par la signature du précédent (voilà pour l'intégrité), la blockchain deviendra une technologie incontournable dans une architecture globale de cybersécurité.

Mais que ces blocs hébergent des cryptomonnaies, des contrats intelligents, ou des données de toute autre nature, qu'en est-il de leur cybersécurité ? Renaud nous présentera son sujet en deux parties : La blockchain pour la cybersécurité et la cybersécurité de la blockchain.

Et la technologie de la blockchain pourrait être à la base d'un Internet du futur, car le « web3 » basé sur la blockchain et sur les contrats intelligents pourrait bien rendre l'Internet beaucoup moins centralisé, beaucoup moins dépendant des USA que celui que nous connaissons aujourd'hui. C'est dire l'importance de la cybersécurité de la blockchain, dont Renaud nous parlera.

Que Renaud nous parle, comme dans des « Lundi de la cybersécurité » précédents, de protocoles réseaux des couches basses pour lier les objets connectés ou des portes électroniques des ordinateurs quantiques, assister à ses discours est toujours une fête, et on apprend beaucoup et avec enthousiasme ! Il sait s'adapter à tous les niveaux.

Bravo Renaud et merci d'avoir accepté de permuter ton intervention avec celle prévue d'un autre intervenant qui a craint de ne pas être disponible en mars et dont nous avons donc reporté l'intervention au dernier trimestre 2022.

Je donne la plume à l'intervenant, Renaud Lifchitz



"Les blockchains sont connues pour leurs applications financières, ce qui éclipse malheureusement bien souvent leurs nombreux autres intérêts. Nous nous focaliserons ici sur les principes, techniques et projets blockchain concrets qui apportent un réel intérêt d'un point de vue confidentialité, intégrité, disponibilité ou authentification.

Ainsi, les blockchains correctement utilisées permettent de drastiquement réduire les points de défaillance unique ("SPOF"), diminuer notre dépendance au cloud ou encore réduire nos coûts d'infrastructures, en s'appuyant sur des réseaux décentralisés existants où les coûts sont partagés. De nombreuses techniques démocratisées par les blockchains sont aussi sous-exploitées en cybersécurité (preuves de sécurité, preuves protocolaires, preuves "zero-knowledge", ...) et pourraient connaître un essor dans nos prochains développements logiciels.

Les blockchains peuvent aussi être un formidable outil de souveraineté numérique en permettant de s'abstraire d'acteurs étrangers centralisés auxquels nous faisons confiance en permanence (autorités de certifications, serveurs DNS racines, ICANN, RIPE ...)

Les blockchains introduisent de nouveaux concepts et de nouvelles opportunités, mais aussi des spécificités dans l'approche de la sécurité. Quels sont ces nouveaux risques ? Comment les traiter et les intégrer dans le choix d'une architecture blockchain, dans le choix d'une technologie, dans la conception d'un projet et dans son implémentation pratique ?"

Je reprends la plume

Qui est cet intervenant ?

Renaud Lifchitz, directeur scientifique de Holiseum, et membre de l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information) est un expert français reconnu en sécurité informatique ayant une longue expérience d'auditeur et de formateur, principalement dans le secteur bancaire et le secteur télécom. Il s'intéresse tout particulièrement au développement sécurisé, aux protocoles de communication sans fil et à la cryptographie.



Il a été intervenant dans de nombreuses conférences internationales et a formé directement plus de 2000 personnes. Ses travaux de sécurité les plus significatifs portent sur les thèmes : cartes bancaires sans contact, géolocalisation GSM, blockchain, signatures RSA, ZigBee, Sigfox, LoRaWAN, Vigik et calcul quantique.



Renaud Lifchitz et les blockchains



JANVIER 2018

BLOCKCHAIN : ETAT DES LIEUX ET PERSPECTIVES

Michel Benedittini
Amélie Rives

D'après une étude réalisée pour la DGRIS du Ministère des Armées avec la participation de Henri d'Again, Pierre Gérard, Eric Larchevêque, Renaud Lifchitz.

Utilisateur précoce de bitcoin depuis l'été 2010, **Renaud Lifchitz** réalise la première présentation publique en France sur le bitcoin au printemps 2011, participe à la conception de la preuve de travail de DataCoin et PrimeCoin (1) qui a battu plusieurs dizaines de record du monde en théorie des nombres.

Depuis, il développe sur les blockchains, et a été auditeur, conseiller et investisseur dans une cinquantaine de projets blockchain.

En 2018, il est contributeur au rapport parlementaire de l'OPECTST du Sénat sur les enjeux technologiques de la blockchain (2) ainsi qu'au rapport de CEIS "Blockchain : état des lieux et perspectives" pour le Ministère des Armées (3)

Il participe régulièrement à de nombreuses interviews médias, podcasts, et livres sur la blockchain.

- (1) <https://bitcoinmagazine.com/articles/primecoin-the-cryptocurrency-whose-mining-is-actually-useful-1373298534>
- (2) <http://www.senat.fr/notice-rapport/2017/r17-584-notice.html>
- (3) https://www.avis-partners.com/wp-content/uploads/2019/11/NoteStrat_Blockchain_Web.pdf

Demande d'inscription au Lundi de la cybersécurité de mars 14 mars à partir de 18 h 00, par visio conférence



Nos « Lundi de la cybersécurité » **sont gratuits** et veulent vous offrir une véritable fête technologique dont on se souvient longtemps, nous nous y employons. **Le prochain** ne se fera encore que par **visioconférence Zoom**. Nous espérons reprendre bientôt, en parallèle, nos « Lundi de la cybersécurité » en présentiel dans un amphi de l'université de Paris, en avril peut-être si la situation sanitaire nous le permettra. Pour la logistique de ce webinaire, et l'accueil chaleureux quand c'est possible à l'université de Paris, 45 rue des Saints-Pères Paris 6^e, nous adressons nos vifs remerciements au professeur Ahmed

Mehaoua de cette université.

Demandez votre inscription, par courriel, et vous recevrez un hyperlien personnel vers la visioconférence Zoom un peu avant le jour de l'évènement. Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

avec « **Inscription 14/03** » dans l'objet **ET** dans le corps du message 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 évènements.

Quelques minutes avec le général de division Marc Boget, commandant de la gendarmerie dans le cyberspace.

Suivant la tradition, dans nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19h15, nous donnons pour quelques minutes la parole à une organisation à but non lucratif, qui opère dans l'écosystème du numérique et dans la sécurité des biens et des personnes. Ce mois-ci, **honneur à la gendarmerie nationale**, en particulier au **ComCyberGend** et à son commandant le **général de division Marc Boget**.

Notez que l'effectif de la gendarmerie dans le cyberspace va rapidement monter en nombre dans les prochains mois en intégrant des réservistes opérationnels et citoyens.
Vous peut-être ?



Le commandement de la gendarmerie dans le cyberspace (ComCyberGend) est un organisme du ministère de l'Intérieur, opérationnel depuis août 2021. Il est chargé de fédérer l'action de ses services spécialisés, dont le Centre de lutte contre les criminalités numériques (C3N) et le réseau CyberGEND des enquêteurs numériques de la gendarmerie.



Il intègre également la brigade numérique de la gendarmerie et la plateforme Perceval en charge des signalements de fraude à la carte bancaire.

Son objectif est d'animer, de coordonner, de mettre en cohérence, de renforcer et de rendre plus visibles et lisibles les capacités de la gendarmerie dans le domaine cyber, qu'il s'agisse de prévention, de formation ou d'investigations.

Comme nous serons en période de réserve, aucun enregistrement de l'intervention sur le ComCyberGend ne sera fait. C'est dire qu'il vaut mieux être présent.

Retour sur le Lundi de la cybersécurité précédents

Francis Bruckmann, webmestre de l'ARCSI, a mis sur le web de l'organisation divers documents, replay, slides, sur les "Lundi de la cybersécurité" précédents. Voir en https://www.arcsi.fr/evt_passes.php

Consultez l'ensemble du web : <https://www.arcsi.fr/> on y trouve des éléments très intéressants, et revenez-y un peu plus tard car, au détour d'une page, vous y trouverez des éléments sur le Lundi de la cybersécurité de février que Francis aura pris le temps d'ajouter.

Les enregistrements des conférences sont disponibles sur la chaîne DailyMotion de l'ARCSI, à l'adresse <https://www.dailymotion.com/arcsi>

Lundi de la cybersécurité d'avril

4 avril



La cybersécurité, un métier de femme !

avec Anne Souvira

Chef de la mission "Cyber" de la préfecture de Police de Paris



Tous cyber sécurisés dans un monde décovidé

Gérard