Bienvenue sur Notepad!
Lien vers l'aide : https://wiki.inria.fr/support/Notepad

Sujet du Pad: Séminaire du LIRIMA

Mercredi 13 novembre 2019
Exposé de Patrick Valduriez, Inria : **« Blockchain 2.0: opportunités et risques »**

IMPORTANT
couper les micros et les caméras sur les postes de travail/les terminaux avant que la conférence ne démarre afin d'éviter les interférences
relancer la connexion en cas de perte du son et/ou de la vidéo

Merci de transmettre via ce nodepad vos remarques et questions à propos de cet exposé.
Un modérateur sur le site de diffusion (à Rennes) se chargera d'en faire la synthèse et posera les questions à l'orateur à l'issue de la présentation.

Vous pouvez ajouter vos entrées dans n'importe quel endroit dans le notepad.
Cela vous permet de compléter une question posée préalablement par un(e) autre participant(e) ou y ajouter un commentaire.
Cela vous permet également de regrouper vos questions et commentaires en un même endroit.

Merci de faire précéder vos entrées du nom de votre site de réception (et/ou de votre nom).

IFIC:
Question 1 : Comment la blockchain pourra m'aider à creer un droit d'auteur pour un logiciel que j'ai crée ?

PV: voir la blockchain: https://blockchainyourip.com/proteger-son-logiciel/

Question 2 : Quel impact de la ou des blockchains sur l'environnement et l'ecologie (exemple : consomation electrique)

PV: En général, pour la blockchain pubique, et notamment avec le PoW, l'impact est catastrophique. La consommation électrique annuelle pour Bitcoin est celle d'un pays de la taille du Danemark.
Mais ce n'est pas nécessairement le cas pour la blockchain privée, qui peut s'appuyer sur un protocole de consensus moins gourmant.

Question 3 : faut il repartir les noeuds un peu partout dans le monde pour avoir un consensus international sur une blockchain commune entre les etats?

PV: la blockchain a été conçue justement pour s'affranchir de tout pouvoir central et de tout état. Pas sur qu'une blockchain internationale (pour faire quoi?) ait un sens.

Question 4 : La technologie du blockchain est elle issue du domaine de defense/militaire ?

PV: au contraire, elle a été développée par des cypherpunks (des libertarians pronant la liberté individuelle).

Question de Georges (ENSP Yaoundé): la blockchain ne sert-elle qu'à gerer les bitcoins? n'y a-t-il pas d'autres types d'utilisation?

PV: la blockchain a été conçue initialement pour sécuriser les transactions bitcoin, mais avec la génération actuelle programmable (Blockchain 2.0),
on voit apparaitre toutes sortes d'applications pour échanger des avoirs (contrats, titres de propriété, produits, ...).

un bloc est validé toutes les 10mn (pour eviter l'inflation): et donc, est ce que le nombre de transaction possible/jour est limité par jour ?
PV: absolument, 10mn est une moyenne pour valider un bloc, ce qui résultate d'un choix de conception de la blockcain bitcoin (taille fixée du bloc, et PoW dont la résolution est proportionnée à la taille du réseau).

la libra de facebook : fonctionnera t elle avec sa propre blockchain ou utilisera elle une blockchain existant ?
PV: sa propre blockchain, avec son propre protocole.

AUF Yaoundé : Questions

1) Que pensez-vous du selfish mining ? est-ce que cette technique améliore la sécurité de la block chain ?
PV: pas du tout, le selfish mining est la collusion de miners (coalition) pour mettre en commun leur puissance de calcul, et ainsi avoir plus de chances d'augmenter leur revenus du mining.

2) N'y a t-il pas d'autres structures de blockchain que les séquences de block? la structure de Graphs Acyclic Dirigés ?
PV: non, une blockchain est une chaine de blocs. Mais il y a d'autres structures concurrentes de la blockchain, notamment Tangle pour la cryptomonnaie Iota basée sur un DAG
(conçue pour l'IoT, mais qui ne me parait pas compétitif avec la blockchain en termes de sécurité et décentralisation).
On peut bien sur imaginer toutes sortes de structures concurrentes, mais on ne doit pas les appeler blockchain.

3) N'est-il pas possible de modifier la transaction stockéess dans yne blockchain privée ?
PV: si, c'est ce que j'ai montré dans l'exemple d'attaque des 51%.

4) Est ce que la blockchain peut contribuer au blanchimment d'argent ?
PV: c'est l'une des premières utilisations.

5) Qu'est ce qu'un pays africain peut gagner à utiliser la blockchain ?
PV: comme je l'ai dit dans l'exposé, pour pallier aux carences des services des états.
Par exemple, la blockchain bitland au Ghana permet de gérer le cadastre de façon à éliminer la corruption
(voir https://www.cryptokemet.com/ghana-bitland-cadastre-blockchain/).
Voir aussi https://www.usine-digitale.fr/article/la-blockchain-un-formidable-levier-de-developpement-pour-l-afrique.N710619.

****
Mercredi 11 septembre 2019
Exposé de Ludovic Mé, Inria : « Cyber security: current challenges »

Merci de transmettre via ce nodepad vos remarques et questions à propos de cet exposé.
Un modérateur sur le site de diffusion (à Rennes) se chargera d'en faire la synthèse et posera les questions à l'orateur à l'issue de la présentation.

Vous pouvez ajouter vos entrées dans n'importe quel endroit dans le notepad.
Cela vous permet de compléter une question posée préalablement par un(e) autre participant(e) ou y ajouter un commentaire.
Cela vous permet également de regrouper vos questions et commentaires en un même endroit.

Merci de faire précéder vos entrées du nom de votre site de réception (et/ou de votre nom).

Questions :
1) quels sont les enjeux "nouveaux" de la sécurité dans le contexte du cloud computing ?
= Perte de localisation des données
= Capacité à offrir des traitements sur des données externalisées

2) des exemples /scenarios illustrant des calculs sur des données chiffrées ?

3) la difference entre les termes : Security de SI vs cyber security vs cyberresliance
= juste ancienne et nouvelle appellation pour Security de SI et Cyber Security
= cyberresiliance est un concept différent, selon lequel un système continuera à

offrir les services malgré l'attaque

4) difference entre security 2 privacy by default vs security 2 privacy by design ?

5) Pour concevoir le hardware qui est cyber-securisé , il faut comprendre comment l'attaque peut atteindre le hardware.
Question: est ce que vous pouvez donner quelques exemples sur ce type d'attaque et comment il peut atteindre le hardware

difference entre : resilience vs tolérance aux pannes vs tolérence aux fautes ?
=

Il faudrait que le site de Tunis coupe le son svp.
c'est fait. Merci :-). Il y avait un écho énorme.

Fin du séminaire à 17h35
Merci !