Utilisation de SGX dans la Blockchain pour optimiser la sécurité

Maysa Abou Jamra

March 8, 2018

Sommaire

1 Introduction

1.1 La blockchain et son consensus

La Blockchain est la technologie à la base de Bitcoin et d'autres cryptocurrencies qui a été salué comme une grande innovation disruptive avec le potentiel de transformer la plupart des industries. Le capital total du marché mondial de la blockchain basé sur les jetons et les cryptomonnaies a atteint plus de $200B à partir de 2018 [1], et devrait se développer davantage .Ce qui distingue la blockchain des bases de données distribuées traditionnelles est la capacité d'opérer dans un cadre décentralisé sans compter sur la confiance d'une tierce personne. Pour cela , leur composante technique de base est le consensus pour parvenir à un accord entre un groupe de noeuds et par la suite assurer la sécurité de tout le système. Maintenu par un réseau peer-to-peer de méfiance mutuelle entre participants, ces systèmes utilisent la preuve de travail [2]pour résoudre le principal défi de parvenir à un consensus entre les contributeurs. La preuve de travail(Proof of Work) est l'algoritme de consensus utilisé dans la Blockchain Bitcoin .Cet algorithme est robuste contre les mauvais comportements et les participants malveillants, mais il nécessite que les participants gaspillent de l'energie et du temps . En switchant vers le Proof of Stake[3] , la blockchain Ethereum essaye de résoudre ce problème , mais la sécurité et le non équité reste des défis pour cet algorithme .

Comme plus d'applications sont construites sur la blockchain , différentes approches sont développées pour améliorer la performance de sa construction et donc de son consensus . De nombreux efforts ont été déployés pour concevoir un nouveau backbone de la blockchain pour améliorer la latence, le débit, et la scalabilité (par exemple, [4, 5]). Bien que ces travaux essaient de résoudre le problème de performance à travers des approches purement logicielles (basees sur le software) , "Trusted Computing Technology" offre une autre opportunité d'améliorer la performance d'une blockchain en utilisant les propriétés spéciales du hardware . Le client blockchain peut tourner dans un environnement de confiance avec une certaine assurance de sécurité ; et cet environnemnet assure que les protocols qui vont être intégrés seront bien suivis . Dans cet article , je vais évoquer notamment l'utilisation d'une nouvelle technologie développée par Intel (Intel SGX) qui propose de nouveaux algorithmes de consensus pour la blockchain afin d'améliorer son fonctionnement et sa sécurité .

2 La sécurisation par Intel SGX

2.1 Introduction

La technologie Intel SGX (Intel Software Guard Extension) a été développée par Intel en 2015 depuis l'architecture Skylake [6] .La principale différence entre SGX et une architecture standard est que le modèle de menace de SGX considère que le logiciel système n'est pas fiable. L'idée est de ne pas faire confiance au OS et à l'hyperviseur puisque parfois les attaqueurs les utilisent pour attaquer l'application et prendre les données [7] , mais simplement faire confiance à une zone mémoire (enclave) protégée par le hardware dans laquelle le développeur d'application met le code et les données secrètes . SGX assure aussi le calcul securisé sur une machine distante ce qui n'est pas une nouvelle idée [8], mais son implémentation était par Intel SGX .

2.2 Securité dans SGX

Intel Software Guard Extensions (SGX) est un ensemble de nouvelles instructions disponibles sur les CPU Intel récents qui confèrent des protections matérielles sur le code au niveau de l'utilisateur. SGX permet l'exécution de processus dans un environnement d'exécution sécurisé (TEE), et plus particulièrement dans SGX dans un espace d'adressage protégé connu sous le nom "enclave". Une enclave protège la confidentialité et l'intégrité du processus de certaines formes d'attaques "hardware" et d'autres processus sur le même hôte, y compris les processus privilégiés comme les systèmes d'exploitation. Une enclave peut lire et écrire en dehors de la région de l'enclave mais aucun autre processus ne peut accéder à la mémoire d'enclave. Ainsi l'exécution isolée dans SGX protège les données et le code sensible pour s'exécuter correctement et en toute confidentialité et intégrité, mais repose sur le système d'exploitation (potentiellement malveillant) pour effectuer les appels systèmes tel que E / S, etc.

2.3 Secret Provisioning

SGX permet à un système distant de vérifier le logiciel fonctionnant dans une enclave pour lui communiquer les données après en toute sécurité. Quand une enclave est créée, le CPU produit un hachage de son état initial connu sous le nom de "measurement"(mesure). Le logiciel de l'enclave peut, à un moment ultérieur, demander un rapport qui inclut une mesure et des données supplémentaires fournies par le processus. Le rapport est signé numériquement à l'aide d'une clé du hardware pour produire une preuve que le logiciel mesuré fonctionne dans une enclave protégée par SGX. Cette preuve, connue sous le nom de "Quote", est une attestation qui peut être vérifiée par un système distant. SGX signe le "Quote " en utilisant une signature de groupe appelée EPID (Enchanced Privacy ID) [9].

Quand l'utilisateur reçoit ce "Quote" signé , il demande une vérification d'un serveur de Intel. Après cette vérification, l'entité distante peut fournir des secrets à cette enclave SGX ce qu'on appelle "Secret Provisioning ". Généralement, l'approvisionnement secret (Secret Provisioning) est effectué via un canal très sécurisé. Le canal sécurisé est établi entre l'entité distante et l'enclave, et la communication entre eux est chiffrée par la clé d'enclenchement SGX générée de manière aléatoire sur la base de la clé du CPU . Cette clé d'enclave n'est jamais exposée en dehors de la portée de l'enclave, et donc personne d'autre n'est capable d'inspecter cette clé pour déchiffrer les secrets pendant les communications.

2.4 TCB dans SGX

Le TCB (Trusted Computing Base) est l'ensemble des mécanismes de protection (matériel, micrologiciel et logiciel) qui fournissent un environnement informatique sécurisé . Concernant SGX , la TCB est constituée de l'ensemble minimal de composants à lequels on va faire confiance en s'appuyant sur le principe qu'une petite TCB minimise la surface d'attaque. Ses composants dans SGX sont :

• Le processeur et tout ce qui est à l'intérieur de ses paquets, y compris la logique matérielle, microcode, registres, mémoire cache.

• Les composants du logiciel utilisés pour l'attestation .

2.5 Usages de Intel SGX

Avec l'avènement et la popularité du Cloud computing, de l'Internet des objets et de la blockchain , l'exigence de confiance pour les terminaux a considérablement augmenté. Un terminal qui s'exécute dans un environnement d'exécution non fiable, peut générer de sérieux problèmes de sécurité . Avec la sortie de Software Guard Extension (SGX), Intel a fourni des garanties de sécurité pour ces technologies , y compris des protections tout au long du cycle de vie des données , au repos , en cours d'utilisation et en vol[10, 11, 12, 13]

3 La technologie Blockchain

3.1 Introduction à la Blockchain

La blockchain est une technologie originale permettant à des utilisateurs de transférer de la valeur entre agents sans besoin d'un intermédiaire . Le fait d'effectuer des transactions sur la blockchain coûte moins cher et elles sont de toutes natures , garanties et auditables par tout le monde, sans avoir besoin d'un tiers de confiance . Ces transactions sont infalsifiables puisque chaque transaction nécessite une clé privée pour la crypter et une autre publique pour désigner le recepteur . Après que la transaction est encryptée et validée par le consensus [14], une nouvelle ligne est inscrite puis verrouillée dans le dernier bloc de la blockchain . Enfin , la blockchain est répliquée dans tous les noeuds du reseau . Les principales blockchains de nos jours sont : Bitcoins , Etherum , Hyperledger .. [15]

3.2 Propriétés de la Blockchain

La blockchain invalide tout pouvoir économique puisqu'elle rend possible le développement d'un service autonome (sans tiers de confiance) à moindre coût . C'est un socle technologique accessible , partagé et sécurisé .

Les trois propriétés de la Blockchain sont :

1. La désintermédiation : Les agents échangent entre eux directement et la validation des transactions est faite par le consensus en évitant d'avoir recours à un tiers de confiance .

2. La sécurité : Elle est garantie dans la blockchain par deux mécanismes :

   - Le procédé cryptographique : Le code de chaque nouveau bloc contient l'identificateur de son prédécesseur (hash) de facon que la modification d'un bloc impliquerait le changement de l'ensemble des blocs de la chaine ce qui est impossible .
   - L'architecture décentralisé : L'ensemble des blocs est répliqué dans les noeuds du réseau et non pas dans un serveur unique ce qui agit comme une défense face au risques de vols de donées .

3. Autonomie : Contrairement aux services en ligne qui demandent leurs besoins d'infrastructure des plateformes , dans la blockchain la puissance de calcul et l'espace d'hébergement sont fournis par les réseaux eux-mêmes (par les mineurs).

3.3 Consensus

La blockchain est un grand registre de compte décentralisé , cela signifie que chaque noeud(full-node [16]) du réseau a une copie de ce registre . Lorsque de nouvelles transactions doivent être ajoutées à la blockchain, cela entraîne un problème. Les noeuds du réseau doivent être d'accord (ou parvenir à un consensus) sur un nouvel état de la blockchain. Le problème se résume à "Quel bloc de transactions allons-nous tous ajouter à notre blockchain prochaine?".Supposons que tous les noeuds vont créer un nouveau bloc de toutes les transactions chaque période de temps (10 minutes en bitcoins) , le résultat sera que différents noeuds auront des blockchains différents . Les transactions ne peuvent pas être propagées instantanément sur l'ensemble du réseau. Ainsi, une transaction donnée peut tomber dans l'intervalle de temps de 10 minutes pour certains noeuds, mais arriver en retard à d'autres noeuds plus éloignés.Les noeuds sont maintenant en désaccord et il n'est pas certain que blockchain soit la véritable blockchain du réseau.Donc, pour éviter cela, un algorithme de consensus est nécessaire, ce qui permet à tous les noeuds du réseau de se mettre d'accord sur le prochain bloc à ajouter, donc il n'y a qu'une seule version de la vérité. Un noeud devra proposer le bloc suivant à ajouter, et les autres noeuds devront pouvoir vérifier facilement que le bloc est valide . Chaque mineur, en générant un bloc, peut choisir le contenu du bloc, en particulier quelles transactions seront inclus et dans quel ordre. Les participants au système sont connectés par un réseau peer-to-peer qui propage des transactions et des blocs. Occasionnellement, deux mineurs ou plus pourraient presque simultanément générer des blocs qui ont le même parent, formant deux branches dans la blockchain et briser sa structure à une seule chaîne. Ainsi un mécanisme est utilisé pour choisir quelle branche étendre et celle choisit est la plus longue chaîne disponible (blockchain détenant le plus fort contenu en calcul).

4 SGX dans la Blockchain

4.1 Problèmes des Algorithmes de consensus existants

La sécurité et la robustesse de la blockchain dépend de son modèle de consensus. Plusieurs algorithmes de consensus existent pour conserver une même blockchain décentralisée notamment "Proof Of Work "(POW) qui est utilisé dans la blockchain Bitcoin .

Le but de POW (ou Proof of Work) est de prévenir les noeuds d'ajouter un nombre arbitraire de blocs dans un temps court pour assurer la sécurité de la blockchain. Par conséquence , afin de valider un bloc et de produire de nouveaux "tokens" , les mineurs doivent résoudre un problème mathématique difficile ce qui conduit a un gaspillage d'énergie et de resources de calcul . L'attaque 51% peut compromiser une blockchain basée sur le POW sachant que c'est délicat [17]. Ethereum[18] a switché du Proof of Work au Proof of Stake(preuve d'enjeu)pour éviter le problème de gaspillage [19, 3, 20]. L'utilisateur dans cet algorithme doit prouver la possession d'une certaine quantité de cybermonnaie pour prétendre valider des blocs supplémentaires dans la chaîne de blocs et de toucher la récompense .

L'implémentation actuelle de proof of stake est vulnérable aux attaques [21, 22] et c'est pas équitable. Il existe de même d'autres méthodes de consensus et chacune

apporte son lot d'avantages et d'inconvénients[23] .

4.2 Algorithmes de consensus proposés par SGX

Cette technologie proposée par Intel a aidé pour développer de nouveaux algorithmes pour le consensus afin d'améliorer le fonctionnement de la Blockchain , des cryptocurrencies et de la sécurité .

La principale critique à émerger est que les participants auraient besoin d'utiliser un hardware Intel SGX pour exécuter du code dans une zone protégée qui ne peut pas être inspectée ou falsifiée.

C'est ainsi qu'on sache - en théorie - que les transactions dans les blocs sont correctes et qu'il ne peuvent pas être altérés à cause de la cryptographie impliquée.

4.2.1 Proof Of Elapsed Time

POW consomme de l'énergie et demande du hardware puissant pour résoudre les problèmes mathématiques . Intel a proposé , en se basant sur la techno SGX ,le concept POET (Proof Of Elapsed Time) d'où le client blockchain peut s'exécuter dans un environnement sécurisé qui est l'enclave . Chaque noeud génère un nombre aléatoire selon une fonction de distribution afin de déterminer le temps d'attente (waiting time) avant d'avoir l'autorisation de générer un bloc (le bloc se produit dans une loterie aléatoire) et chaque noeud génère une paire de clés . La formule que le noeud utilise pour générer le temps d'attente réduit la probabilité de collision (que plusieurs noeuds auront même waiting time) . Ce temps d'attente est utilisé pour un bloc ou plusieurs et c'est le rôle de SGX de vérifier l'exécution correcte du processus de "timer" pour garantir la sécurité du système .Ce temps augmente avec le nombre de noeuds actifs . Quand le bloc est généré , SGX fournit au noeud qui a créé ce bloc une preuve de ce temps attendu "proof of waiting time" qui sera vérifié par les autres noeuds. Cette preuve est une attestation qui prouve à d'autres dans le système que le client a attendu comme il aurait dû . Des tests statistiques sont utilisés pour déterminer si un noeud a généré plus qu'un certain nombre de blocs dans un certain temps afin de rejeter ses blocs .[24, 25].

On peut citer deux remarquables avantages de cet algorithme qui sont :

1. L'efficacité : cet algorithme est plus respectueux de l'environnement que la preuve de travail puisqu'il ne demande pas que les noeuds participants effectuent une charge de travail de calcul coûteuse .

2. L'equité : Il atteind le but de "one CPU one vote" dans le sens que tous les CPU ont les mêmes chances de gagner à cette loterie .[26].

D'ailleurs , POET présente deux défis [27] :

1. broken chip problem : La sécurité de SGX n'est pas parfaite[28, 29] et comme pour tout hardware à lequel on fait confiance, il faut s'attendre à ce qu'un adversaire disposant de ressources suffisantes puisse le casser. Ainsi, il faut s'attendre à ce que certains processeurs SGX soient cassés. Dans le schéma basique de PoET , "broken ship" a un effet dévastateur, car elle permet à un mineur de simuler un temps de minage nul et de gagner tous les tours de consensus, c'est-à-dire de publier tous les blocs. Intel a proposé un test

statistique pour détecter les ruptures, mais les détails ne sont pas publiés . Le résultat est catastrophique parce qu'avec PoET, un seul noeud brisé est capable de performer des attaques majoritaires sur la blockchain .

2. stale chip problem : Dans de nombreux contextes pratiques dans les systèmes PoET et les systèmes semblables , un mineur préfere acheter de vieux processeurs SGX ("stale") , les assembler en "fermes" et les utiliser pour miner à peu de frais .De cette façon ,les processeurs tournent au ralenti et de telles fermes rétablissent une partie du gaspillage (waste en hardware) que le POET essaie d'éviter.

4.2.2 Proof Of Luck

Les conceptions actuelles de blockchains sont lents, en utilisant beaucoup de temps (POET) et d'énergie(POW) dans le mécanisme de consensus pour cela ce nouveau algorithme a apparu . POL (Proof Of Luck) est construit sur la base de TEE (Trusted Execution Environment) notamment SGX [30]. L'idée est que chaque noeud génère un nombre aléatoire qui est la valeur de chance "luck " et celui qui aura le plus grand nombre ajoute un nouveau bloc . Cette valeur aléatoire qu'on va nommer "l" est généré par un service donné par Intel dans l'enclave . De cette façon ,on aura peut être le même noeud qui génère tout le temps le plus grand nombre . L'algorithme a besoin donc de plus d'un "wait Round-Time " qui est un temps fixe que les participants doivent attendre avant de générer la valeur de chance pour éviter la dernière situation . Un autre souci est la possibilité que les horloges ne soient pas synchronisés , si par exemple le réseau n'est pas bon ce qui conduit a une génération de plusieurs blocs des noeuds qui croient que chacun a la chance la plus élevée . Pour résoudre ce problème , deux fonctions ont été integres : "PoLRound" et "PoLMine".

Au début de chaque tour, le participant prépare l'environnement sécurisé qui est l'enclave pour miner sur une chaîne particulière en appelant "PoLRound" et en passant le dernier bloc actuellement connu. Il attend un temps de tour "Round-Time" , cela garantit qu'un participant attend le "ROUND TIME" en recevant les blocs minés ce qui leur permet de passer au plus chanceux (déterminé par POLMIne). Après que "ROUND TIME" passe, le participant appelle "PoLMine" pour miner un nouveau bloc. Le participant passe l'en-tête du nouveau bloc et le bloc qu'il va étendre (comme "PreviousBlock"). "PreviousBlock" peut être différent du "roundBlock" qui a été passé à PoLRound, mais nous exigeons que "roundBlock" et "PreviousBlock" ont le même parent. La fonction "POLMINE" détermine le bloc gagnant de tous les blocs minés des participants dans un tour. Pour optimiser la communication de protocole, l'algorithme retarde par un "sleep" d'un temps qui est en fonction de "l" (la chance) , qui prescrit un délai plus court pour les plus grands nombres (plus chanceux) et une plus longue période d'attente pour les numéros malchanceux. Si un participant reçoit un bloc plus chanceux avant la fin de son propre minage, il n'aura pas besoin de diffuser son propre bloc. Un compteur monotone est utilisé pour interdire les invocations concurrentes du SGX .

Avantages :

1. Validation des transactions à faible latence

2. Minimiser l'utilisation de l' énergie et la puissance de calcul

3. Scalabilité pour un plus grand nombre de participants

4. Arreter le débat entre ASIC et non ASIC [31] pour le minage , tous les CPU Intel SGX peuvent miner

4.2.3 Proof Of Useful Work

POUW (Proof Of Useful Work) est un algorithme de consensus qui donne une approche très différente de la minimisation du gaspillage brodée par le projet "REM " [32] . Plutôt que de compter sur le hachage de POW , elle utilise un autre type de PoW, dans lequel le travail est utile. Ce concept est appelé la Preuve de Travail Utile (Proof Of Useful Work). Pour permettre la vérification du travail sur des charges de travail utiles arbitraires, REM repose sur la technologie: Intel SGX. Cet algorithme trouve des solutions pour les deux problèmes rencontrées avec POET.

Tout d'abord, le problème "broken chip ". La sécurité SGX est imparfaite et donc il est à prévoir qu'un adversaire ayant des ressources suffisantes peut la casser . Donc, il faut s'attendre à ce que certains processeurs SGX soient cassés. Dans le schéma de base Poet, "broken chip " a un effet dévastateur, car elle permet à un mineur de simuler un zéro temps d'extraction et de gagner tous les tours de consensus , et par la suite publier tous les blocs. Intel a proposé un test statistique pour détecter les ruptures, mais les détails ne sont pas publiés .

Pour faire face à ce défi , REM propose d'utiliser un test statistique rigoureux avec des fondations formelles dont l'efficacité est montré analytiquement . Il peut limiter strictement les gains des adversaires qui ont le "broken chip" tout en minimisant le rejet de blocs incorrect de mineurs honnêtes.

Un autre problème de POET était le "stale chip ". C'est là qu'intervient l'approche de preuve de travail utile de REM (PoUW). Les mineurs avec cet algorithme effectuent n'importe quelle charge de travail qu'ils considèrent utile te que "protein-folding computations" ou "ML classification algorithms"... Les mineurs peuvent prouver qu'ils ont travaillé sur ces problèmes en utilisant SGX. La probabilité qu'un mineur extrait un bloc est proportionnelle à la quantité de travail qu'il effectue. Ainsi, REM transforme le travail utile en effort de minage. C'est techniquement difficile de rendre POUW fonctionner . Il exige que les charges de travail eux-mêmes soient compilés et instrumentés en utilisant SGX pour prouver l'exactitude . La critique qui reste commune entre POET et POUW et POL est que avec tous ces algorithmes Intel est impliquée , ce qui rend la blockchain partiellement décentralisé .

5 Limitations et performance

5.1 Performance de Intel SGX

- La taille de l'enclave est limitée uniquement 128MB dont 96MB pour les utilisateurs, le reste pour les metadata

- Les instructions privilegiés ne peuvent pas être executées dans l'enclave puisqu'on ne fait pas confiance au système d'exploitation , donc les "threads" vont sortir de l'enclave et l'appel système s'exécute par le OS . Les entrées et sorties de l'enclave ont un impact sur les performances

- La gestion de l'enclave (pagination) est très coûteuse en performance
- Intel détient le monopole donc il faut la faire confiance

Pour déployer les applications SGX d'une facon plus simple et plus performante , SCONE est un conteneur sécurisée par cette technologie pour exécuter les applications LINUX [33].

5.2 Status de SGX

Les chercheurs ont annoncé, le 3 janvier 2018, avoir mis au point deux cyberattaques "Meltdown et Spectre " [34, 35] permettant la captation de données efficaces contre un très grand nombre de modèles de processeurs, en particulier ceux fabriqués par Intel[36]. Et comme Intel SGX est une technologie Intel destinée aux développeurs d'applications cherchant à protéger le code et les données sélectionnés contre la divulgation ou la modification , la question qui se pose est si cette tehnologie est affectée par ces deux dernières attaques.

Comme les chercheurs de l'Ohio State University expliquent dans un document détaillant SgxPectre [37],aucune attaque de Meltdown n'est démontrée contre des enclaves SGX mais l'attaque Spectre peut compromettre la confidentialité des enclaves SGX et savoir le contenu de la mémoire de l'enclave mais sans toucher l'intégrité [38] .

Intel a récemment publié des directives qui peuvent aider à durcir le code en cours d'exécution dans les enclaves contre Spectre [39]. De même , Intel a déclaré qu'elle va mettre à jour le " software development toolkit " pour les fournisseurs des applications SGX qu'ils prévoient d'être disponible le 16 Mars 2018 et qui seront efficaces contre cette attaque .

6 Travaux connexes

Ce rapport était une simple étude sur l'intégration de Intel SGX à la blockchain publique pour améliorer son consensus et sa sécurité . Dans cette section , j'examine brièvement les travaux connexes sur la sécurité de la blockchain, l'amélioration de son consensus ainsi que l'utilisation de Software Guard Extensions dans la blockchain privée et les smart contracts .

Nakamoto dans le document initial de Bitcoin a montré que lorsque la majorité des utilisateurs sont honnêtes, la probabilité qu'un attaquant réussisse à compromettre la blockchain est très faible à cause de l'algorithme de consensus POW [26] . Plusieurs études étaient concentrées sur l'étude de la sécurité de la blockchain assurée par ce mécanisme [40, 41] . Des cadres formels sont également développés pour étudier la relation entre la performance d'une blockchain basée sur le PoW et son niveau de sécurité [42, 43]. Ces résultats ne peuvent pas être appliqués aux algorithmes de consensus proposés par Intel SGX en raison de leur différence fondamentale de PoW. Une approche similaire à PoET [45], éventuellement originaire avec Dryja [44], est de limiter le gaspillage d'énergie par le "proof of idle" . Les mineurs achètent du matériel pour miner et seront payés en prouvant que leurs équipement restent inactifs(idle). Comme dans PoET, un opérateur avec un budget fixe pourrait rediriger les économies d'énergie à acheter plus de machines à vide, produisant un gaspillage de capitaux .

L'utilisation de Intel SGX qu'on a évoqué dans ce rapport était dans le contexte des blockchains pour améliorer le consensus . SGX peut améliorer aussi le fonctionnement des smart contracts ce qui est proposée par Zhang et al. [45] JUels et al. [46] . De même , Intel peut être utile pour renforcer la blockchain privée en terme de sécurité , confidentialité et scalabilité [47].

7 Conclusion

La blockchain possède des propriétés intéressantes dont les potentialités méritent d'être explorées. Et comme toute technologie innovante , des défis existent tojours. Dans cet article , on a évoqué la technologie SGX qui est sensée assurer la confidentialité et l'integrité des données en cours d'exécution même sur une machine distante. Cette dernière peut être utilisée dans la Blockchain pour améliorer son consensus et par la suite sa performance. La seule critique qui reste est que le concept de décentralisation de la blockchain devient partiel avec SGX et impose de faire confiance à Intel .

References

[1] Market Capitalization . `https://blockchain.info/charts/market-cap`.

[2] Preuve de travail ,Récupéré sur Bitcoin.it . `https://fr.bitcoin.it/wiki/Preuve_de_travail`.

[3] Ethereum's Switch to Proof of Stake – Better Than Proof of Work? . `https://usethebitcoin.com/ethereums-switch-proof-work-proof-stake/`.

[4] Nicolas T Courtois, Pinar Emirdag, and Daniel A Nagy. Could bitcoin transactions be 100x faster? In *Security and Cryptography (SECRYPT), 2014 11th International Conference on*, pages 1–6. IEEE, 2014.

[5] Loi Luu, Viswesh Narayanan, Kunal Baweja, Chaodong Zheng, Seth Gilbert, and Prateek Saxena. Scp: A computationally-scalable byzantine consensus protocol for blockchains. *IACR Cryptology ePrint Archive*, 2015:1168, 2015.

[6] Victor Costan and Srinivas Devadas. Intel sgx explained. *IACR Cryptology ePrint Archive*, 2016:86, 2016.

[7] John Criswell, Nathan Dautenhahn, and Vikram Adve. Virtual ghost: Protecting applications from hostile operating systems. *ACM SIGARCH Computer Architecture News*, 42(1):81–96, 2014.

[8] US DoD. Department of defense trusted computer system evaluation criteria (orange book). Technical report, Technical Report DoD 5200.28-STD, National Computer Security Center, 1985.

[9] Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen. Intel® software guard extensions: Epid provisioning and attestation services. *White Paper*, 1:1–10, 2016.

[10] Juan Wang, Zhi Hong, Yuhan Zhang, and Yier Jin. Enabling security-enhanced attestation with intel sgx for remote terminal and iot. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(1):88–96, 2018.

[11] Jake Smith. A More Protected Cloud Environment: IBM Announces Cloud Data Guard Featuring Intel SGX . `https://itpeernetwork.intel.com/ibm-cloud-data-guard-intel-sgx/`, 2017. [Online; accessed 20 December 2017].

[12] ERICA PORTNOY. Azure Confidential Computing Heralds the Next Generation of Encryption in the Cloud . `https://www.eff.org/deeplinks/2017/09/azure-confidential-computing-heralds-next-generation-encryption-cloud`, 2017. [Online; accessed 18-September-2017].

[13] Mike Hearn. Corda: A distributed ledger. *Corda Technical White Paper*, 2016.

[14] SÉBASTIEN BOURGUIGNON. Quelle utilité au consensus dans la blockchain ? `https://siecledigital.fr/2016/11/07/utilite-consensus-blockchain/`, 2017. [Online; accessed 7 November 2016].

[15] Deloitte. La Blockchain Panorama des technologies existantes. `https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/services-financiers/blockchain_panorama-des-technos-existantes.pdf`, 2017.

[16] Full node . Récupéré sur Bitcoin.it . `https://fr.bitcoin.it/wiki/Full_node`.

[17] Jean-Luc , « Qu'est-ce qu'une attaque des 51% ? » . `https://bitcoin.fr/quest-ce-quune-attaque-des-51/`.

[18] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 2014.

[19] USER "QUANTUMMECHANIC" , Proof of stake instead of proof of work . `https://web.archive.org/web/20160320104715/https://bitcointalk.org/index.php?topic=27787.0`.

[20] Aggelos Kiayias, Ioannis Konstantinou, Alexander Russell, Bernardo David, and Roman Oliynykov. A provably secure proof-of-stake blockchain protocol. *IACR Cryptology ePrint Archive*, 2016:889, 2016.

[21] Iddo Bentov, Ariel Gabizon, and Alex Mizrahi. Cryptocurrencies without proof of work. In *International Conference on Financial Cryptography and Data Security*, pages 142–157. Springer, 2016.

[22] Proof of Stake versus Proof of Work . `http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf`.

[23] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *Big Data (BigData Congress), 2017 IEEE International Congress on*, pages 557–564. IEEE, 2017.

[24] Sawtooth . https://sawtooth.hyperledger.org/docs/core/releases/latest/introduction.html, 2017.

[25] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. Consensus in the age of blockchains. *arXiv preprint arXiv:1711.03936*, 2017.

[26] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[27] Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. On security analysis of proof-of-elapsed-time (poet). In *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, pages 282–297. Springer, 2017.

[28] Johannes Götzfried, Moritz Eckert, Sebastian Schinzel, and Tilo Müller. Cache attacks on intel sgx. In *Proceedings of the 10th European Workshop on Systems Security*, page 2. ACM, 2017.

[29] Nico Weichbrodt, Anil Kurmus, Peter Pietzuch, and Rüdiger Kapitza. Asyncshock: Exploiting synchronisation bugs in intel sgx enclaves. In *European Symposium on Research in Computer Security*, pages 440–457. Springer, 2016.

[30] Mitar Milutinovic, Warren He, Howard Wu, and Maxinder Kanwal. Proof of luck: an efficient blockchain consensus protocol. In *Proceedings of the 1st Workshop on System Software for Trusted Execution*, page 2. ACM, 2016.

[31] Why We Use GPU vs ASIC . https://www.trymining.com/pages/asic-vs-gpu.

[32] Fan Zhang, Ittay Eyal, Robert Escriva, Ari Juels, and Robbert Van Renesse. Rem: Resource-efficient mining for blockchains. *IACR Cryptology ePrint Archive*, 2017:179, 2017.

[33] Sergei Arnautov, Bohdan Trach, Franz Gregor, Thomas Knauth, Andre Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Dan O'Keeffe, Mark Stillwell, et al. Scone: Secure linux containers with intel sgx. In *OSDI*, volume 16, pages 689–703, 2016.

[34] Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution. *arXiv preprint arXiv:1801.01203*, 2018.

[35] Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. Moritz lipp1, michael schwarz, daniel gruss, thomas prescher 2, werner haas 2.

[36] Today's CPU vulnerability: what you need to know . https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html.

[37] Guoxing Chen, Sanchuan Chen, Yuan Xiao, Yinqian Zhang, Zhiqiang Lin, and Ten H Lai. Sgxpectre attacks: Leaking enclave secrets via speculative execution. *arXiv preprint arXiv:1802.09085*, 2018.

[38] Dr. Greg Wettstein Worker IDfusion LLC. SGX After Spectre and Meltdown Status, Analysis and Remediations . `ftp://ftp.idfusion.net/pub/sgx/sgx-spectre-meltdown.pdf`, 25/01/2018 – Version 1.

[39] Intel® Software Guard Extensions (SGX) SW Development Guidance for Potential Bounds Check Bypass (CVE-2017-5753) Side Channel Exploits . `https://software.intel.com/sites/default/files/180204_SGX_SDK_Developer_Guidance_v1.0.pdf`, February 2018.

[40] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281–310. Springer, 2015.

[41] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer, 2017.

[42] Lin Chen, Lei Xu, Nolan Shah, Nour Diallo, Zhimin Gao, Yang Lu, and Weidong Shi. Unraveling blockchain based crypto-currency system supporting oblivious transactions: a formalized approach. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pages 23–28. ACM, 2017.

[43] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 3–16. ACM, 2016.

[44] DRYJA. T. Optimal mining strategiesSF Bitcoin-Devs presentation . `https://www.youtube.com/watch?v=QN2TPeQ9mnA`, 2014.

[45] Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. Town crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 aCM sIGSAC conference on computer and communications security*, pages 270–282. ACM, 2016.

[46] Ari Juels, Ahmed Kosba, and Elaine Shi. The ring of gyges: Investigating the future of criminal smart contracts. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 283–295. ACM, 2016.

[47] INTEL® TECHNOLOGY SECURING ENTERPRISE BLOCKCHAINS . `https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/08/blockchain-infographic.pdf`, 18 January 2017.