CARNET DE BORD : BLOCKCHAIN POST-QUANTIQUE

TEAUDORS Mickaël & VALERI Yoann

19 MARS 2019

UNIVERSITE PIERRE ET MARIE CURIE

Table des matières

1. Introduction

Notre projet semestriel s'intitule « BlockChain Post-Quantique ». Nous nous intéressons dans ce projet à la structure de donnée qu'est la BlockChain. Il s'agit d'une liste chaînée de blocs de données, contenant un ensemble de transactions, et notamment utilisée pour la gestion des crypto-monnaies ou des contrats intelligents. Ce moyen de gestion des données, apparu au grand public en 2008 par son utilisation pour la crypto-monnaie Bitcoin, est aujourd'hui en grande expansion, et représente actuellement plus de 150 milliards d'US dollars. Pour ce projet, il nous a été expliqué comment le modèle de sécurité fonctionne. Celle-ci est basée sur deux algorithmes : l'algorithme dit « Proof-Of-Work », servant à insérer des blocs dans la chaîne, et celui dit « Signature », servant à montrer la validité des transactions effectuées. Il a été prouvé que le premier est résistant aux ordinateurs quantiques, mais le second ne l'est pas, et remplacer celui-ci (dans une plateforme open-source de manipulation de BlockChain nommé Hyperledger) constitue le cœur de notre projet.

2. Mots-clés : Mindmap

3. Descriptif de la recherche documentaire

Pour notre projet, il nous a été fourni dans le sujet le nom d'un article présentant l'intérêt du sujet. Pour pouvoir le lire, nous avons cherché ce nom dans un moteur de recherche, et avons trouvé ledit article sur le site arXiv.org, un des bases de données spécialisées en informatique. Après avoir lu ce document et avoir eu notre premier rendez-vous avec nos encadrants, nous avons pu prendre connaissance des différents outils que nous allons utiliser pour notre projet. Cela nous a permis de voir les algorithmes que nous avons à remplacer, et ce qu'ils utilisaient. Nous avons donc cherché des articles sur ces points, en commençant par les comparer avec les sources données dans l'article de départ, et les avons cherchés sur arXiv.org, Springer Link ou encore Semantic Scholar. De cette manière, nous avons pu comparer les différents sites et les informations données sur chaque document en les ajoutant dans Zotero, et en comparant les champs remplis. Nous avons donc à l'heure actuelle 3 articles de revue, 2 articles de colloque et un rapport. Ce dernier correspond à l'explication du fonctionnement de l'algorithme que l'on doit implémenter pour notre projet.

4. Bibliographie produite

[1] Lov K. Grover. 1996. A fast quantum mechanical algorithm for database search. *arXiv:quant-ph/9605043* (May 1996). Retrieved March 9, 2019 from http://arxiv.org/abs/quant-ph/9605043

[2] C. P. Schnorr. 1990. Efficient Identification and Signatures for Smart Cards. In *Advances in Cryptology — CRYPTO' 89 Proceedings* (Lecture Notes in Computer Science), 239–252. DOI: https://doi.org/10.1007/0-387-34805-0_22

[3] Antoine Casanova, Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. 2017. *GeMSS: A Great Multivariate Short Signature*. UPMC - Paris 6 Sorbonne Universités ; INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France ; LIP6 - Laboratoire d'Informatique de Paris 6. Retrieved March 9, 2019 from https://hal.inria.fr/hal-01662158

[4] Peter W. Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing* 26, 5 (October 1997), 1484–1509. DOI: https://doi.org/10.1137/S0097539795293172

[5] Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel. 2018. Quantum attacks on Bitcoin, and how to protect against them. *Ledger* 3, (October 2018). DOI: https://doi.org/10.5195/ledger.2018.127

[6] Mihir Bellare and Phillip Rogaway. 1993. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security* (CCS '93), 62–73. DOI: https://doi.org/10.1145/168588.168596

5. Evaluation des sources

- Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel, “Quantum attacks on Bitcoin, and how to protect against them”:

Ce document est un article a été publié en 2017 et n’a subit aucune révision ou n’a pas été réfuté depuis lors. Il s’agit de l’article proposé dans notre sujet de projet, explique le fonctionnement d’une BlockChain, et surtout démontre pourquoi l’algorithme de « Proof-Of-Work » est résistant aux ordinateurs quantiques, tandis que celui de « Signature » ne l’est pas. L’article est donc en partie général tant il explique la nécessité de changer un des algorithmes utilisés, mais aussi spécialisé, dans son utilisation de notions avancées d’attaque cryptographiques, de calculs de complexité ou de parallélisation. Les 5 auteurs sont des chercheurs, venant des universités de Singapour, de Paris Diderot et de Sydney. Les calculs et résultats démontrés se font à partir de données publiques. Cet article a été produit dans le but de montrer la nécessité de changer l’algorithme « Signature » utilisé par les BlockChain pour résister aux ordinateurs quantiques et éviter la potentielle réécriture de transactions par des tiers mal intentionnés. Les informations proposées sont donc objectives dans le sens où les auteurs proposent 11 différents algorithmes pour régler les problèmes de sécurité, sans en favoriser un en particulier, mais en donnant les avantages et inconvénients de plusieurs d’entre eux.

- Antoine Casanova, Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem, “GeMSS: A Great Multivariate Short Signature”:

Ce document est un rapport de recherche publié le 18 décembre 2017 et mis à jour le 7 février 2019. C’est un rapport présentant le principal algorithme que nous devons implémenter pour remplacer celui de « Signature » utilisé dans Hyperledger. Les informations données sont donc importantes à notre compréhension des calculs impliqués dans notre projet. C’est un document destiné à un public connaisseur car reposant sur des concepts avancés d’algèbre polynomiale et de cryptographie. Les auteurs sont des membres de l’Inria (Institut national de recherche en informatique et en automatique), un établissement public spécialisé en mathématique et informatique rassemblant des chercheurs et membres du secteur privé. Le sujet abordé constitue donc le cœur de leurs recherches, et elles sont légitimes pour parler du sujet, étant les inventeurs de l’algorithme. Le document a d’abord été publié sur le site de l’Inria. Les calculs et résultats démontrés se font à partir de données publiques, utilisant d’autres propositions d’algorithmes de signature. Ce rapport (et l’algorithme associé) ont été produit à la suite d’un appel d’offre de NIST (National Institute of Standards and Technology, une organisation américaine chargé de la standardisation des technologies) portant sur la création d’algorithmes destinés à devenir des standards dans la cryptographie asymétrique post-quantique. Le document est donc en conséquence biaisé, car il s’agit de la documentation de l’algorithme concerné.

- Claus-Peter Schnorr, “Efficient Identification and Signatures for Smart Cards”:

Ce document est un article publié en 1989, et non mis à jour depuis. Il s’agit d’un article donnant un protocole d’authentification pour la cryptographie asymétrique, caractérisé par le fait qu’il est à divulgation nulle de connaissance (s’authentifier auprès d’une entité extérieure sans révéler aucune

information sur des informations secrètes). Ce protocole est celui est utilisé dans Hyperledger pour permettre d'authentifier une personne sans donner sa clé privée. L'article présente donc l'algorithme et montre sa complexité temporelle ainsi que ses avantages cryptographiques, et est donc destiné à un public spécialisé. L'auteur est Claus-Peter Schnorr, un chercheur de l'université de Frankfort spécialisé en mathématique et cryptographie, donc qualifié pour parler du sujet. L'article présentant un algorithme et évaluant sa complexité, il est aisé de vérifier leur validité. De plus, l'algorithme est encore très utilisé aujourd'hui, malgré le fait qu'il date de 30 ans. Il a cependant été montré non résistant à certaines attaques, mais également amélioré et mêlé à d'autres algorithmes pour en faire un des plus résistant aujourd'hui. Cet article a été produit pour montrer l'intérêt de l'algorithme, et son efficacité dans l'authentification à divulgation nulle de connaissance. L'information est donc biaisée, car parlant exclusivement d'un seul algorithme, et montrant son utilité.