Vers une Auto-protection Collaborative des Systèmes Connectés fondée sur la Blockchain et les Microservices Unikernels

Constant Rohmer*, Mohamed-Aymen Chalouf*, Pierre Alain*, Guillaume Doyen†
*SOTERN - IRISA (UMR CNRS 6074), Rennes University,
†SOTERN - IRISA (UMR CNRS 6074), IMT Atlantique,
*{constant.rohmer, mohamed-aymen.chalouf, pierre.alain}@irisa.fr, †guillaume.doyen@imt-atlantique.fr

***Abstract*—L'augmentation de la surface d'attaque et la complexité croissante des systèmes d'information rendent les réponses humaines inadaptées face aux menaces modernes. L'introduction de concepts comme l'auto-protection et la cybersécurité collaborative permet d'envisager de nouveaux systèmes de défense adaptés aux exigences actuelles. Il se pose alors la question de concevoir une architecture autonome de confiance, qui soit capable d'orchestrer en temps réel des réponses coordonnées et d'appliquer des contre-mesures ciblées et adaptatives. Cette thèse vise à répondre à ce besoin en conciliant fiabilité, robustesse et performance. L'approche proposée s'appuiera sur la blockchain pour garantir l'inaltérabilité et la traçabilité des actions, tout en automatisant les réactions via des contrats intelligents (*smart contracts*). Les microservices *unikernels* viendront compléter cette architecture en assurant l'adaptabilité et la parallélisation des opérations, améliorant ainsi la scalabilité et le temps de réponse. Une fonction d'orchestration multi-objectifs sera également introduite pour coordonner les ressources, prioriser les actions et éviter les conflits. Enfin, une évaluation rigoureuse permettra de valider les performances de la solution et de garantir une réaction collaborative efficace et optimisée.**

***Index Terms*—Auto-protection, Cybersécurité Collaborative, Blockchain, Microservices, Unikernels**

I. Introduction

La diversification et la multiplication des applications, services et utilisateurs de l'Internet entraînent une augmentation significative de la surface d'attaque. Par conséquent, les systèmes d'information sont confrontés à un nombre croissant de menaces, nécessitant des réactions rapides pour en limiter les impacts. Cependant, les systèmes de défense actuels reposent encore sur l'intervention d'opérateurs humains, un processus devenu trop lent face à la vitesse des attaques modernes et la complexité des systèmes à protéger [1]. Cette situation impose de repenser les stratégies de défense, en adoptant des approches capables d'assurer une réponse automatique et coordonnée aux menaces. C'est dans ce contexte qu'a émergé le concept d'auto-protection [2], qui permet donc aux systèmes de gérer leur sécurité de manière autonome et de réagir aux attaques en temps réel.

Aujourd'hui, cette automatisation ouvre la voie à des solutions à plus grande échelle, comme l'auto-protection collaborative. En regroupant les efforts de multiples acteurs, cette approche repose sur le partage d'informations entre des systèmes jusqu'ici indépendants, ce qui permet une détection et une réponse collective plus efficaces aux attaques. Cette collaboration est d'autant plus intéressante que le nombre de participants est élevé. Parmi les applications de l'auto-protection collaborative figurent le partage de renseignements sur les cybermenaces (*Cyber Threat Intelligence*, CTI) et la détection d'attaques par apprentissage fédéré [3].

Cependant, la réaction collaborative soulève des défis supplémentaires. Les systèmes doivent s'appuyer sur une architecture de confiance, capable d'orchestrer une réponse coordonnée et d'appliquer des contre-mesures ciblées et dynamiques, le tout en temps réel. L'objectif de cette thèse est ainsi de concevoir une solution fiable, robuste et performante pour répondre à ces exigences. Nous proposons alors d'explorer l'utilisation combinée de la blockchain et des microservices.

En effet, la blockchain est particulièrement adaptée pour renforcer la confiance dans un environnement collaboratif sans tiers de confiance. Son architecture décentralisée permet d'éliminer le point de défaillance unique (*Single Point of Failure*, SPoF) des systèmes centralisés. Elle offre des garanties essentielles comme l'inaltérabilité des données, la traçabilité des actions et l'automatisation via les contrats intelligents (*smart contracts*). Ces caractéristiques permettent de sécuriser les échanges tout en automatisant la réaction de manière transparente et vérifiable par tous les participants.

Les microservices apparaissent alors comme un complément essentiel pour améliorer les performances et l'adaptabilité de la solution de réaction. Ils pourraient permettre de paralléliser l'exécution des *smart contracts*, améliorant ainsi à la fois le temps de réponse et la scalabilité de la blockchain. De plus, les microservices pourraient également servir de support à l'application des contre-mesures, car ils facilitent la mise à jour et le redéploiement à la demande de certains composants, sans perturber l'ensemble du système.

Cependant, la mise en œuvre d'une solution fondée sur la blockchain et les microservices soulève plusieurs défis majeurs. Tout d'abord, il est essentiel de définir les rôles des différentes entités du système. Il faut ensuite concevoir les *smart contracts* chargés d'orchestrer l'enchaînement des

Cette étude est soutenue/partiellement financée par l'ANR dans le cadre du projet de l'EUR CyberSchool et du projet CMA Cyberskills4all (respectivement ANR-18-EURE-0004 et ANR-23-CMAS-0026)

réactions aux attaques tout en évitant les conflits entre les actions initiées par diverses entités. Cela nécessitera la conception d'une fonction d'orchestration distribuée sur la blockchain capable de coordonner les réactions en fonction des objectifs définis, tout en optimisant les performances du système. L'implémentation d'un algorithme multi-objectifs permettra ainsi de trouver un compromis entre les priorités opérationnelles, le délai de réponse, et la scalabilité de la plateforme. Finalement, une évaluation rigoureuse sera indispensable pour valider les performances de la solution et garantir son efficacité globale.

Le reste de cet article est organisé comme suit : la partie II présente l'état de l'art associé à l'utilisation de la blockchain et des microservices pour la cybersécurité et l'auto-protection collaborative ; la partie III aborde nos contributions à venir dans ce domaine ; nous concluons finalement cet article dans la partie IV.

II. État de l'art

A. La Blockchain pour la Cybersécurité

La blockchain est déjà exploitée pour améliorer la fiabilité de divers domaines et applications, tels que l'Internet des objets, le stockage des données de santé et la gestion des identités numériques [4]. En plus du stockage inaltérable de données, la blockchain permet également de stocker et exécuter du code avec les *smart contracts*. L'introduction des *smart contracts* a permis l'automatisation et la décentralisation de plusieurs mécanismes de sécurité tels que la gestion des certificats [5], le contrôle d'accès [6] ou la gestion des configurations réseau [7].

Dans ce contexte, son potentiel a également été exploré dans le domaine de la cybersécurité collaborative. L'usage de la blockchain en cybersécurité collaborative est déjà bien établi, comme l'indiquent Miller & Pahl [8]. Elle a notamment été étudiée dans des domaines tels que la détection d'intrusion [9] et la remédiation des attaques par déni de service distribué (*Distributed Denial of Service*, DDoS) [10], [11].

Selon [8], Ethereum est la technologie la plus utilisée pour les solutions de cybersécurité fondées sur la blockchain. Ceci est dû à son accessibilité et à son écosystème établi d'applications décentralisées construites avec les *smart contracts* [11], [12]. Toutefois, la même étude indique un éloignement progressif d'Ethereum au profit de technologies comme la blockchain Hyperledger Fabric (HLF) [10], [13]. La popularité croissante d'HLF peut être attribuée à une confidentialité accrue et à son architecture modulaire. Certains articles ne précisent ni la technologie blockchain ni le consensus employés et se limitent à exploiter le concept de blockchain sans en considérer l'implémentation [14]. De même, la question des performances n'est pas toujours abordée dans sa globalité, c'est-à-dire en prenant en compte divers aspects tels que la latence, le débit, la scalabilité et l'impact sur les ressources système [13], [15], [16]. Or une analyse complète est essentielle pour évaluer et justifier la pertinence de ces solutions, que ce soit pour la détection ou la réaction aux attaques.

Des méthodologies spécifiques ont été développées pour évaluer la pertinence de l'utilisation de la blockchain et pour déterminer le type de blockchain le plus adapté aux contraintes du cas d'usage [17], [18]. En effet, les blockchains se distinguent par deux critères : le contrôle d'accès, qui oppose les blockchains publiques (*public*) accessibles à tous aux blockchains privées (*private*) réservées à certains utilisateurs; et la politique de validation de données, qui différencie les blockchains fermées (*permissioned*), où seuls des acteurs approuvés valident les transactions, des blockchains ouvertes (*permissionless*), où tous les participants peuvent prendre part au processus de validation.

Le choix du consensus est également essentiel, car c'est cet algorithme qui permet aux participants d'ajouter de nouveaux blocs à la blockchain et d'en conserver une copie identique et ordonnée [19]. C'est donc le consensus qui détermine la sécurité, la performance et la scalabilité du système final. Les performances des consensus permettent de faire un premier tri en vue de leur utilisation dans notre cadre applicatif. La preuve de travail (*Proof of Work*, PoW) et la preuve d'enjeu (*Proof of Stake*, PoS) utilisées respectivement par les blockchains Bitcoin et Ethereum introduisent des délais minimums importants : 10min pour Bitcoin et 15s pour Ethereum. Ces délais, bien qu'acceptables pour des transactions financières, sont incompatibles avec leur usage dans un contexte de réaction à des attaques. Il faut également veiller à ce que des participants ne puissent pas profiter du système sans y contribuer (*free riding*) ou déclarer de fausses attaques pour le manipuler. De plus, comme le contenu partagé par les participants a pour but de modifier les configurations de tous les systèmes connectés participants à la blockchain, une erreur pourrait entraîner des interruptions de service ou des dysfonctionnements pour les utilisateurs légitimes. De manière similaire, un acteur malveillant ayant compromis un nœud et adoptant un comportement byzantin ne doit pas pouvoir provoquer l'échec du consensus et bloquer le système. Par conséquent, les consensus résistants aux pannes (*Crash Fault Tolerant*, CFT) ne sont plus suffisants et il est nécessaire d'adopter des consensus résistants aux comportement byzantins (*Byzantine Fault Tolerant*, BFT) [19]. Ces derniers permettent au système de continuer de fonctionner tant que le taux d'acteurs byzantins reste strictement inférieur à un tiers du total des noeuds participants [19]. Cependant, un nombre élevé de participants peut dégrader les performances des consensus BFT, qui sont particulièrement sensibles au nombre de nœuds [19], entraînant ainsi des problèmes de scalabilité.

B. Utilisation combinée de la Blockchain et des Microservices

Selon [20], l'intégration des microservices dans les blockchains est une évolution naturelle, alignée sur l'architecture des services et infrastructures réseau de nouvelle génération. Pour optimiser les performances des systèmes blockchain, des études récentes suggèrent d'exécuter les *smart contracts* via des microservices. En effet, l'exécution des *smart contracts* repose sur le consensus du réseau, et l'approbation séquentielle des transactions dans un bloc

limite la scalabilité et les performances de la blockchain [21]. Santos et al. [22] estiment alors que les microservices pourraient pallier cette limitation de la blockchain grâce à leur flexibilité, leur haute disponibilité et leur capacité à s'adapter aux charges variables. La scalabilité et le temps de réponse de la blockchain pourraient être améliorés par la parallélisation de l'exécution des *smart contracts*, mais les gains en performances dépendent fortement des technologies utilisées. Comme ce qui a été souligné par [8] pour l'utilisation de la blockchain en cybersécurité collaborative, les auteurs de [22] soulignent que la plupart des solutions combinant la blockchain et les microservices n'ont pas été évaluées de manière approfondie ou ne présentent que des preuves de concept.

Avec une taille d'image et un temps de démarrage bien inférieurs aux machines virtuelles et conteneurs, les microservices *unikernels* permettent des stratégies de déploiement plus flexibles et dynamiques [23]. Leur utilisation est une réelle opportunité d'optimiser les performances tout en réduisant la surface d'attaques des systèmes [24] ce qui les rend d'autant plus intéressants pour notre cadre applicatif. Alp et al. [25] ont comparé plusieurs stratégies d'exécution des *smart contracts* avec des *unikernels* : un déploiement à l'avance pour réduire le surcoût de création, un déploiement à la demande pour minimiser le gaspillage de ressources, et une approche hybride conciliant les deux. Leurs résultats montrent que, malgré un faible temps de démarrage, l'instanciation dynamique des *unikernels* reste trop lente. À l'inverse, un déploiement statique, associé à un mécanisme de récupération des ressources inactives (*garbage collector*), apparaît comme une solution plus viable.

III. Contributions de la thèse

Cette thèse propose d'explorer l'utilisation combinée de la blockchain et des microservices pour relever les défis inhérents à la mise en œuvre d'une solution de réaction collaborative dans le cadre de l'auto-protection des systèmes connectés.

Une première étude empirique a déjà été réalisée sur un système de partage d'informations dédié à la réponse aux attaques DDoS. Nous avons choisi de nous intéresser au DDoS car ce type d'attaque est très fréquent et peut avoir un impact important sur la disponibilité et les performances des services de l'Internet. De plus, les attaques DDoS constituent un des sujets centraux dans le domaine de la cybersécurité collaborative fondée sur la blockchain, ce qui en fait un cas d'usage pertinent pour illustrer notre approche théorique et pratique, ainsi que pour se positionner par rapport à l'état de l'art. L'analyse des performances a été réalisée via un banc de test qui permet l'émulation d'un réseau étendu (*Wide Area Network*, WAN) à une échelle continentale. Cette analyse a également été l'occasion d'étudier l'impact sur les performances de différents paramètres de la blockchain comme le nombre de nœuds, le délai de communication entre les nœuds, ou le nombre de transactions par blocs.

Nos perspectives de travail s'articulent autour des trois verrous identifiés précédemment : la fiabilité, la robustesse et la performance.

A. Une solution fiable

Le premier verrou technologique à lever concerne la fiabilité du système dans un environnement où plusieurs entités collaborent pour détecter et réagir à des attaques. Un participant malveillant ou compromis ne devra pas être en mesure d'exploiter le système à ses propres fins, ou de compromettre le processus collaboratif. Cela nécessite une architecture capable de garantir la transparence, l'intégrité et la traçabilité des actions menées. Nous étudierons ainsi une architecture fondée sur la blockchain et les microservices, dans laquelle les rôles des différentes entités du système seront précisément définis. Au vu des différents types de blockchains existants, il apparaît essentiel de motiver rigoureusement le choix de la technologie blockchain employée. Dans ce contexte, il sera intéressant d'appliquer les différentes méthodologies de l'état de l'art afin de déterminer si la blockchain est pertinente et quelle technologie de blockchain serait la plus adaptée [17], [18]. Il sera également crucial de se pencher sur le choix de l'algorithme de consensus, qui joue un rôle déterminant dans la sécurité et l'intégrité du processus de validation des transactions ainsi que sur les performances de la blockchain.

Une partie essentielle de cette contribution réside dans la conception et l'implémentation des *smart contracts*. Ces derniers permettront l'enchaînement des actions nécessaires pour répondre aux attaques. Leur stockage dans la blockchain garantira leur exécution sécurisée et un enchaînement ordonné des contre-mesures. En complément, nous étudierons les possibilités de cibler l'application des contre-mesures par le déploiement dynamique de microservices en fonction du contexte spécifique des attaques détectées.

B. Une solution robuste

La robustesse du système est un autre défi clé, notamment face aux conflits entre actions initiées par les entités, ou en présence de contraintes fortes sur les ressources disponibles. En effet, le système d'auto-protection collaborative devra être capable de gérer plusieurs incidents en parallèle, ce qui pourra alors provoquer des conflits entre les réactions respectives (p.ex. conflit de configuration d'un pare-feu, ou ressources insuffisantes pour déployer plusieurs contre-mesures).

Pour répondre à ce défi, nous proposerons l'intégration d'une fonction d'orchestration capable de coordonner les réactions aux différents incidents. Cette fonction jouera un rôle central dans la gestion des ressources en priorisant les actions à entreprendre selon leur criticité et leur impact sur les objectifs globaux. La fonction d'orchestration sera également munie d'un garbage collector, analogue à celui de Alp et al. [25], qui permettra d'optimiser l'utilisation des ressources et de garantir la continuité et la fluidité du système même en cas de forte charge. Finalement, il sera intéressant d'évaluer la tolérance aux pannes des microservices et leur capacité à isoler les erreurs sans affecter l'ensemble du système.

C. Une solution performante

Les performances de la solution sont essentielles pour respecter les contraintes de réactivité imposées par notre cadre applicatif. Pour ce faire, la thèse explorera la parallélisation de l'exécution des *smart contracts* en s'appuyant sur une architecture microservices et plus particulièrement les *unikernels*. Cet ajout devra être réalisé en suivant la même méthodologie que pour l'utilisation de la blockchain évoquée dans la section III-A : Nous commencerons par analyser la pertinence théorique avant de choisir les technologies et enfin d'en évaluer les performances. L'objectif sera ensuite d'évaluer dans quelle mesure les microservices, et plus particulièrement les *unikernels*, peuvent améliorer la scalabilité et le temps de réponse des *smart contracts* tout en maintenant un niveau de sécurité adapté aux contraintes de l'auto-protection collaborative. Nous examinerons les différents modèles d'exécution possibles, notamment les trois approches proposées par Alp et al. [25] et comparerons leurs impacts sur la gestion des ressources et la résilience du système.

Par ailleurs, le banc de test développé pour notre première étude sur le DDoS mentionnée précédemment sera réutilisé et étendu pour permettre une évaluation rigoureuse des performances. Cette évaluation reposera sur des expérimentations les plus réalistes possibles, afin de mesurer précisément les délais de réponse, la capacité de traitement et la scalabilité de la plateforme. Ces analyses permettront de valider la pertinence des choix technologiques effectués et d'identifier les éventuelles limitations de la solution proposée.

IV. Conclusion

Face à la complexité croissante des systèmes d'information et à l'évolution des menaces, l'auto-protection collaborative représente une approche prometteuse pour renforcer la cybersécurité des systèmes. Cette thèse s'inscrit dans cet objectif en proposant une solution combinant blockchain et microservices afin de répondre aux exigences de fiabilité, de robustesse et de performance nécessaires à une réaction coordonnée et dynamique contre les attaques. En perspective, notre approche pourra être généralisée à différents types d'attaques afin d'évaluer sa flexibilité face à différentes menaces. De plus, au-delà de la réaction aux incidents, l'application de notre solution à la détection des attaques pourrait ouvrir de nouvelles opportunités pour renforcer la cybersécurité collaborative.

References

[1] N. Zuk, "Welcome to the Era of Autonomous Security," Feb. 2022. [Online]. Available: https://www.paloaltonetworks.com/blog/2022/02/extended-security-intelligence-and-automation-management/

[2] J. Kephart and D. Chess, "The vision of autonomic computing," *Computer*, Jan. 2003, conference Name: Computer.

[3] L. Lavaur, M.-O. Pahl, Y. Busnel, and F. Autrel, "The Evolution of Federated Learning-Based Intrusion Detection and Mitigation: A Survey," *IEEE Transactions on Network and Service Management*, Sep. 2022.

[4] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustainable Energy Technologies and Assessments*, Aug. 2022.

[5] L. Mendiboure, M. A. Chalouf, and F. Krief, "A Scalable Blockchain-based Approach for Authentication and Access Control in Software Defined Vehicular Networks," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*. Honolulu, HI, USA: IEEE, Aug. 2020.

[6] T. Sylla, L. Mendiboure, M. A. Chalouf, and F. Krief, "Blockchain-Based Context-Aware Authorization Management as a Service in IoT," *Sensors (Basel, Switzerland)*, Nov. 2021.

[7] I. D. Alvarenga, G. A. F. Rebello, and O. C. M. B. Duarte, "Securing configuration management and migration of virtual network functions using blockchain," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2018, iSSN: 2374-9709.

[8] L. Miller and M.-O. Pahl, "Collaborative Cybersecurity Using Blockchain: A Survey," Mar. 2024, arXiv:2403.04410 [cs].

[9] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," *IEEE Access*, 2018, conference Name: IEEE Access.

[10] M. Hajizadeh, N. Afraz, M. Ruffini, and T. Bauschert, "Collaborative Cyber Attack Defense in SDN Networks using Blockchain Technology," in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. Ghent, Belgium: IEEE, Jun. 2020.

[11] S. Alharbi, D. Alghazzawi, A. Hakeem, L. Mohaisen, L. Cheng, and A. Attiah, "A Blockchain-Based Collaborative Intrusion Detection Systems Framework," *IEEE Internet of Things Journal*, 2023.

[12] Z. El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract," *IEEE Access*, 2019.

[13] W. Guo, J. Xu, Y. Pei, L. Yin, and C. Jiang, "LDBT: A Lightweight DDoS Attack Tracing Scheme Based on Blockchain," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. Montreal, QC, Canada: IEEE, Jun. 2021.

[14] Z. A. El Houda, L. Khoukhi, and A. Hafid, "ChainSecure - A Scalable and Proactive Solution for Protecting Blockchain Applications Using SDN," in *2018 IEEE Global Communications Conference (GLOBECOM)*. Abu Dhabi, United Arab Emirates: IEEE, Dec. 2018.

[15] A. Pavlidis, M. Dimolianis, K. Giotis, L. Anagnostou, N. Kostopoulos, T. Tsigkritis, I. Kotinas, D. Kalogeras, and V. Maglaris, "Orchestrating DDoS mitigation via blockchain-based network provider collaborations," *The Knowledge Engineering Review*, 2020.

[16] S. M. Sajjad, M. R. Mufti, M. Yousaf, W. Aslam, R. Alshahrani, N. Nemri, H. Afzal, M. A. Khan, and C.-M. Chen, "Detection and Blockchain-Based Collaborative Mitigation of Internet of Things Botnets," *Wireless Communications and Mobile Computing*, Apr. 2022.

[17] K. Wust and A. Gervais, "Do you Need a Blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. Zug: IEEE, Jun. 2018.

[18] N. El Madhoun, J. Hatin, and E. Bertin, "Going Beyond the Blockchain Hype: In Which Cases are Blockchains Useful for IT Applications?" in *2019 3rd Cyber Security in Networking Conference (CSNet)*. Quito, Ecuador: IEEE, Oct. 2019.

[19] J. Xu, C. Wang, and X. Jia, "A Survey of Blockchain Consensus Protocols," *ACM Computing Surveys*, Dec. 2023.

[20] D. Krishnaswamy, A. Bhatnagar, K. Chauhan, D. Bhamrah, S. Srivastava, S. Thakur, S. Bisht, S. Narula, K. Jangid, and P. Jundre, "A Microservices-Based Virtualized Blockchain Framework for Emerging 5G Data Networks," in *2019 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019.

[21] S. Wang, X. Zhang, W. Yu, K. Hu, and J. Zhu, "Smart Contract Microservitization," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, Jul. 2020, iSSN: 0730-3157.

[22] R. Santos, P. Soares, E. Rodrigues, P. H. M. Maia, and A. Silveira, "How blockchain and microservices are being used together: a systematic mapping study," in *Proceedings of the 5th International Workshop on Emerging Trends in Software Engineering for Blockchain*. Pittsburgh Pennsylvania: ACM, May 2022.

[23] T. Goethals, M. Sebrechts, A. Atrey, B. Volckaert, and F. De Turck, "Unikernels vs Containers: An In-Depth Benchmarking Study in the Context of Microservice Applications," in *2018 IEEE 8th International Symposium on Cloud and Service Computing (SC2)*, Nov. 2018.

[24] A. Madhavapeddy and D. J. Scott, "Unikernels: the rise of the virtual library operating system," *Communications of the ACM*, Jan. 2014.

[25] E. C. Alp, C. Băsescu, P. Tennage, N. Kocher, and B. Ford, "Efficient Deterministic Execution of Smart Contracts."