Utilisation de blockchains et d'applications Android Automotive pour une gestion sécurisée et fiable des données d'accidents de véhicules

Luc Gerrits, Thomas Mabrut, François Verdier
Université Côte d'Azur - LEAT - CNRS UMR 7248
930 route des Colles, BP 145 06903 Sophia Antipolis cedex, France

1. Introduction

Les accidents de la route constituent un problème majeur de sécurité publique qui touche des millions de personnes dans le monde. Une gestion efficace des données d'accident est essentielle pour la déclaration, l'enquête et la prévention des accidents dans les délais appropriés et avec précision. Dans cet article, nous présentons une nouvelle approche pour la gestion sécurisée et fiable des données d'accidents de véhicules en utilisant la technologie blockchain et une application type Android Automotive. Nous proposons une solution de stockage de données en temps réel qui utilise le système de fichiers InterPlanetary File System (IPFS) et une blockchain privée (basée sur Substrate) pour une gestion décentralisée et infalsifiable des données. Notre système permet le stockage efficace et sécurisé des données d'accident, y compris les informations sur le véhicule, les coordonnées GPS et de nombreux autres capteurs du véhicule, de manière transparente et immuable. En utilisant des contrats intelligents, nos résultats expérimentaux montrent que notre système peut efficacement stocker des données d'accidents de véhicules avec une faible latence (moins de 8 secondes) et avec un débit de la blockchain de 560 transactions par seconde.

Ce travail fait partie du projet Smart IoT for Mobility [1] qui vise à développer une nouvelle économie basée sur la technologie blockchain et les contrats intelligents pour l'Internet des objets (IdO ou IoT en anglais).

2. État de l'art

2.1. Blockchain et contrats intelligents

De nombreuses technologies de blockchain ont vu le jour depuis la création de la crypto-monnaie Bitcoin. La blockchain fournit un enregistrement distribué de données qui est immuable, transparent et permet un consensus entre les nœuds participants. Des algorithmes tels que Proof-of-Work (preuve de travail), Proof-of-Elapsed-Time (preuve de temps écoulé) et Practical-Byzantine-Fault-Tolerance (tolérance pratique à l'égard des défaillances) sont disponibles pour aider à atteindre ce consensus. Dans le même temps, les dispositifs IoT deviennent de plus en plus populaires. Ils permettent aux objets du quotidien d'échanger des données et de mettre en œuvre des applications spécifiques. Toutefois, il est possible d'élargir encore les cas d'utilisation potentiels de la technologie IoT en utilisant la blockchain et les contrats intelligents [2].

Les blockchains publiques offrent confiance et sécurité à toute personne souhaitant participer au réseau. Ce type de blockchain est très décentralisé. Toutefois, elles sont également connues pour leur lenteur à parvenir à un consensus, leur manque de scalabilité et une volatilité de la valeur des crypto-monnaies. Pour remédier à ces problèmes, de nouvelles règles de consensus sont en cours d'élaboration. Malgré ces difficultés, les blockchains publiques sont connues pour leur transparence et peuvent être utilisées pour vérifier l'authenticité des enregistrements.

Les blockchains privées, également appelées blockchains de consortium, nécessitent une autorisation pour participer au réseau. Elles sont généralement utilisées pour créer des blockchains contrôlées par une ou plusieurs organisations. En connaissant les participants de la blockchain, il est également possible de tenir quelqu'un pour responsable (des données, du fonctionnement, etc.). Les règles de consensus des blockchains privées peuvent être plus facilement gérées et mises à jour, et permettent aussi d'accélérer l'ajout de transactions par rapport aux blockchains publiques. Il n'est pas nécessaire de mettre en œuvre une crypto-monnaie native dans ce type de blockchain. Les industries qui sont réglementées par la loi, des tiers de confiance, exigent des solutions techniques toujours plus efficaces et moins coûteuses, ce qui rend ces blockchain bien adaptées. Une blockchain privée est choisie pour la structure de notre cas d'utilisation (Sect.3).

Les contrats intelligents (smart contracts) sont des programmes qui sont exécutés dans la blockchain. Ils permettent l'automatisation de logique dans la blockchain et la création d'applications au-dessus du réseau. Seules les blockchains qui prennent en charge les contrats intelligents peuvent tirer parti de cette fonctionnalité. En fournissant un moyen d'automatiser les transactions et les opérations, les contrats intelligents peuvent réunir les technologies IoT et blockchain. L'utilisation de ces contrats intelligents est décrite dans la Sect.3.

2.2. IoT, Blockchain et le secteur automobile

Les appareils IoT sont des architectures contraintes dont les limites matérielles sont bien connues. Ces limites sont la faible empreinte mémoire, la durée de vie limitée de la batterie et la faible puissance de calcul. La technologie blockchain nécessite une puissance de calcul importante et sa base de données augmente à l'infini. L'intégration de la technologie blockchain dans le domaine de l'IoT est donc un défi pour la recherche et l'industrie. Les auteurs des travaux connexes les plus importants (comme [3]) ont combiné la blockchain et les réseaux IoT. Pendant longtemps,

les véhicules ont été équipés de dispositifs IoT très limités, ce qui rendait l'intégration de la blockchain impossible.

Le secteur automobile connaît actuellement une transformation dans le domaine de l'infotainment embarqué (IVI) et de la connectivité, accélérée par le besoin croissant d'appareils intelligents, d'une expérience utilisateur améliorée, de fonctions connectées supplémentaires et, plus généralement, de capacités de conduite améliorées. Cette évolution permet de mettre en œuvre des applications plus complexes dans le véhicule. Dans le domaine de l'IoT automobile, les défis présentent des risques importants pour les individus, y compris la possibilité de dommages graves, voire de décès. La littérature montre un grand intérêt pour la technologie blockchain en tant que solution à certains des problèmes de l'IoT, y compris pour les cas d'utilisation de l'IoT dans les véhicules [4][5][6].

3. Mise en œuvre et cas d'utilisation

Dans notre travail, nous avons créé une application Android Automotive qui récupère les informations sur le véhicule et les transmet à une blockchain privée (créée par le fabricant du véhicule) lorsqu'un accident est détecté (Figure 1). Les données brutes sont envoyées à un nœud IPFS et un hachage cryptographique unique des données (CID) est envoyé à la blockchain. Les CID des données des véhicules sont gérés par des contrats intelligents, ce qui permet seulement aux véhicules autorisés de stocker des informations et d'identifier les conducteurs. Les applications décentralisées (dApp) peuvent ultérieurement tirer parti de ces contrats intelligents.

Android Automotive est un système d'exploitation entièrement intégré pour l'IVI. Il a donc accès à diverses informations précieuses sur le véhicule, telles que la vitesse, l'accélération, la position GPS, la capacité de la batterie et 136 autres capteurs. Toutefois, l'accès aux capteurs du véhicule est contrôlé par le framework Android Automotive et à la mise en œuvre de la plateforme spécifique à chaque constructeur pour des raisons de sécurité ou de sûreté. Dans notre travail, nous considérons que nous pouvons accéder à tous les capteurs.

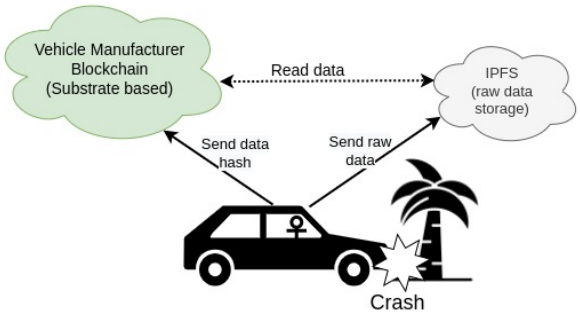

Figure 1: Cas de l'accident, une application Android Automotive connectée à une blockchain et à l'IPFS

Nous avons évalué la solution de l'application en fournissant des détails sur la taille des données et la latence. La blockchain privée est évaluée en fournissant le nombre de transactions par seconde, le blocktime et le temps de test.

L'application envoie en moyenne 128 kbits (données brutes + formatage de la sérialisation). L'ajout d'images ou de données de caméras vidéo augmenterait considérablement les besoins de stockage, qui atteindraient plusieurs gigaoctets. Naturellement, avec la vitesse actuelle de la bande passante, l'envoi de 128 kbits (sur internet) est relativement rapide, mais l'augmentation des données se traduira toujours par une plus grande latence. Globalement, l'application prend 1,088 seconde pour traiter et envoyer les données après la détection d'un accident en utilisant une configuration locale de la blockchain. Dans une configuration en cloud (c'est-à-dire plus proche d'un scénario cas réel), l'application prend 7,105 secondes.

Nous avons testé les performances de la blockchain en envoyant 10k transactions à un taux de 100 à 2000 transactions par seconde. Ce benchmark permet d'explorer les limites de traitement des transactions de la blockchain. Le débit maximum de la blockchain est en moyenne limité par un maximum de 560 transactions par seconde. Le temps de creation d'un bloc est de 6 secondes et le temps de test du benchmark est au minimum 12 secondes. Théoriquement, le temps de test prévu devrait diminuer à mesure que le nombre de transactions envoyées à la blockchain augmente (i.e. 12 secondes est le temps minimum pour traiter 10k transactions).

4. Conclusion

Notre mise en œuvre pratique a permis d'établir avec succès la communication entre le véhicule et la blockchain et l'IPFS. La blockchain inclut un contrat intelligent qui facilite les contrôles d'autorisation de base. Nous n'abordons pas tous les défis, tels que la protection de la vie privée et la confidentialité, qui sont des sujets étudiés dans la littérature. Cependant, nous évaluons notre travail, exprimons ses limites et discutons des travaux connexes.

Dans les travaux futurs, nous avons l'intention d'étendre le cas d'utilisation en incluant plusieurs constructeurs automobiles (ou services), créant ainsi un écosystème plus complexe qui nécessiterait l'interconnexion de plusieurs blockchains.

References

[1] F. Verdier *et al.*, "Smart IoT for Mobility: Automating of Mobility Value Chain through the Adoption of Smart Contracts within IoT Platforms," in *17th Driving Simulation & Virtual Reality Conference (DSC)*, 2018.

[2] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the iot and industrial iot: A review," *Internet of Things*, vol. 10, p. 100081, 2020, special Issue of the Elsevier IoT Journal on Blockchain Applications in IoT Environments.

[3] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126 – 142, 2018.

[4] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "Blockchain for the internet of vehicles: A decentralized iot solution for vehicles communication using ethereum," *Sensors*, vol. 20, no. 14, 2020.

[5] R. Jabbar, N. Fetais, M. Kharbeche, M. Krichen, K. Barkaoui, and M. Shinoy, "Blockchain for the internet of vehicles: How to use blockchain to secure vehicle-to-everything (v2x) communication and payment?" *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15 807–15 823, 2021.

[6] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Communications Magazine*, vol. 56, no. 10, 2018.