UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À

L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE

APPLIQUÉES

PAR

INES YAHIA

SYSTEME DE BLOCKCHAIN HIERARCHIQUE ET AUTHENTIFICATION LEGERE POUR UN RESEAU V2G SECURISE

DECEMBRE 2022

Résumé :

Les réseaux V2G constituent les infrastructures permettant aux véhicules électriques et aux bornes de charge de communiquer afin de charger et de décharger ces véhicules. La norme ISO 15118 a défini les exigences de communications entre les bornes de charge et les véhicules électriques et a introduit le protocole PnC (Plug and Charge) qui facilite le chargement du véhicule pour l'utilisateur. Ce dernier a seulement à brancher le câble de chargement sur la borne sans aucune autre intervention. La norme ISO 15118 a opté aussi pour l'utilisation de l'infrastructure hiérarchique à clé publique X.509 (PKI) pour la facilité des échanges entre le véhicule et la borne qu'elle apporte et pour la sécurité de la communication qu'elle offre à travers les mécanismes cryptographiques utilisés.

Les véhicules électriques sont considérés comme un moyen de transport futur pour les particuliers, il est donc indispensable d'assurer l'efficacité et la sécurité des échanges établies entre les entités du réseau. C'est pour cette raison que les réseaux V2G sollicitent beaucoup l'intérêt des chercheurs, qui ont proposé de nombreuses solutions, mais dont les lacunes persistent encore, comme : la nécessité d'une entité intermédiaire de confiance, un schéma d'authentification lourd, négligence des ressources limitées des entités, ...

Dans l'objectif de corriger ces inconvénients et de rendre le système plus robuste, nous proposons notre solution, qui respecte les exigences de la norme ISO 15118, tout en intégrant un schéma d'authentification léger et la technologie blockchain. Cette dernière va constituer un moyen de stockage de données, capable de rendre plus sécurisées nos informations en assurant le contrôle d'accès aux données et en gardant une trace de l'historique des événements. Il faut aussi noter que notre système ne repose pas sur l'utilisation d'une seule blockchain, mais sur quatre blockchains dont deux sont publiques et deux sont privées. Pour la sécurité de notre système, nous avons aussi intégré d'autres moyens afin de le protéger contre les différentes attaques.

Notre solution répond aux critères de sécurité, en assurant la confidentialité, l'intégrité des données, l'anonymat, ainsi que la non-répudiation. Notre approche offre une résistance aux multiples attaques récurrentes et allège considérablement les véhicules électriques qui sont limités en ressource de stockage et de calcul. La modélisation a été réalisée en utilisant l'outil Tamarin Prover, et la simulation avec RiseV2G.

Les analyses des résultats de la modélisation ainsi que ceux de la simulation ont prouvé que notre système répond aux attentes, en offrant une communication sécurisée, rapide avec un schéma d'authentification léger, et robuste contre de multiples attaques.

Abstract:

V2G networks constitute the infrastructures allowing electric vehicles and charging stations to communicate in order to charge and unload these vehicles. The ISO 15118 standard defined the requirements for communications between charging stations and electric vehicles and introduced the PnC (Plug and Charge) protocol which facilitates charging the vehicle for the user. The latter only has to plug in the charging cable. Loading on the terminal without further intervention. The ISO 15118 standard has also opted for the use of the X.509 hierarchical public key infrastructure (PKI) for the ease of exchanges which it provides and for the security of the communication which it offers through the cryptographic mechanisms used.

The electric vehicles being considered as a future means of transportation for individuals, it is therefore essential to ensure the efficiency and security of the exchanges established between the entities of the network. For this reason, the V2G networks solicit a lot of interest from the researchers, who have proposed many solutions, but shortcomings persist, such as: the need for a trusted intermediary entity, a cumbersome authentication scheme, neglect of the limited resources of the entities and many others.

To address these shortcomings and make the system more robust, we propose our approach, which is based on the requirements of ISO 15118, integrating a lightweight authentication scheme, and blockchain technology. The latter will provide a means of data storage, a way to make our information more secure by ensuring access control to data and keeping track of the history of events. It should also be noted that our system does not rely on the use of a single blockchain, but on four blockchains, two of which are public and two are private. For the security of our system, we have also integrated solutions to protect it against various attacks.

Our solution meets security criteria, ensuring confidentiality, data integrity, anonymity, and non-repudiation. It resists to multiple recurring attacks and considerably lightens electric vehicles which are limited in storage and computing resources. Modeling and simulation were performed using the Tamarin Prover and RiseV2G tools respectively.

The modeling and simulation results demonstrated that our approach meets expectations, providing secure communication, being fast and lightweight, and being robust against multiple attacks.

Remerciements

Je remercie tout d'abord, Dieu le Miséricordieux, le Tout-Puissant de m'avoir donné la force, la Persévérance et la patience pour achever mon travail.

Je tiens à remercier le Professeur Boucif Amar Bensaber pour son encadrement de qualité, sa disponibilité, ses judicieux conseils, son suivi, ainsi que pour son encouragement qui m'a amené à bien finaliser ce travail.

Je remercie également les membres du jury Mhamed Mesfioui et Ismail Biskri, pour leur lecture et évaluation qui ont permis l'amélioration de ce travail.

Je remercie beaucoup mes amis et mes collègues du laboratoire LAMIA pour leurs soutiens, et encouragements durant mes études.

Un grand merci aussi à tous les membres de ma famille et en particulier à ma mère B.Djemaa et à mon mari K.Mohamed Amir qui m'ont été d'un soutien inestimable.

Table des Matières

Liste des Figures:

Liste des Tableaux :

Liste des Abréviations :

V2G	Vehicle to Grid Communication
PKI	Public Key Infrastructure
EV	Electric vehicle
EVCC	Electric vehicle Communication Controller
SECC	Supply Equipment Communication Controller
EVSE	Electric Vehicle Supply Equipment
LAG	Local Aggregator
CA/RA	Certification/Registration Authority
MO	Mobility Operator
OEM	Original Equipment Manufacturer
PnC	Plug and Charge
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
TLS	Transport Layer Security
DES	Data Encryption Standard
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm
PoW	Proof of Work
PoS	Proof-of-Stake

Chapitre 1 Introduction

Certes de nos jours, plusieurs moyens de transport sont offerts, mais la voiture reste le moyen de transport offrant le plus de liberté et de flexibilité. La grande majorité des voitures utilisées aujourd'hui nécessitent du carburant pour effectuer des déplacements. Le carburant contient une énergie chimique transformée en énergie mécanique et cela grâce à la combustion [1]. L'énergie produite par ce procédé n'est pas sans conséquence, en effet, la pollution atmosphérique est liée à la combustion du carburant qui libère des particules volatiles telles que le benzène, les métaux et le dioxyde de soufre [2], amenant ainsi à la pollution et à la formation de smog. Ce dernier est un mélange toxique de gaz ayant des effets très néfastes sur la santé et l'environnement. [3]

D'autre part, l'extraction d'une ressource de quantité finie comme le pétrole entraîne des enjeux économiques et industriels. Effectivement, le pétrole est une ressource qui ne durera pas éternellement et arrivera un jour à épuisement. On parle alors du pic pétrolier, qui est le moment où la production de pétrole atteint son maximum avant de décliner jusqu'à épuisement. Selon les experts, ce pic sera atteint aux plus tard d'ici 2030. Par conséquent, il est important de trouver un remplaçant pour cette ressource si précieuse.[4]

Afin de répondre aux besoins de l'économie verte et à l'épuisement du carburant, il fut l'avènement des voitures électriques. Le premier prototype de voiture électrique a vu le jour en 1834 suivi par l'invention et l'ajout de batterie rechargeable en 1859, mais en étant en concurrence avec les voitures à essence et en vue de la complexité de l'utilisation des batteries rechargeables, ce type de voiture fut écrasé par la concurrence, à savoir les voitures à essence. En 1973, la sensibilisation écologique et la dépendance au carburant ainsi que l'assèchement des énergies fossiles comme le pétrole ont fait resurgir l'idée des véhicules électriques. Depuis 2013, les constructeurs automobiles travaillent sur l'évolution des voitures électriques et sur leur adaptation à notre quotidien pour une écologie plus verte. [5]

Aujourd'hui, les véhicules électriques sont de plus en plus en demande et plusieurs pays prévoient la croissance de la migration vers ces véhicules. Parmi ces pays, on retrouve le Canada, qui exige que d'ici à 2035 tous les véhicules et camions légers vendus soient des véhicules sans émission de gaz [6]. Avec la norme ISO 15118 qui a introduit le protocole Plug and Charge (PnC), l'utilisation et le chargement des véhicules électriques sont rendus plus faciles. Ce dernier permet de recharger la batterie d'une voiture électrique auprès d'une borne de charge juste en branchant le câble de chargement sans autre intervention supplémentaire du conducteur. Ce protocole effectuera toutes les opérations d'identification, de chargement et de facturation.[7,8]

La norme ISO 15118 apporte une certaine sécurité aux réseaux V2G (Vehicle to Grid) en intégrant une infrastructure hiérarchique de certificats X.509 pour gérer l'attribution de certificats aux différentes entités et pour assurer la sécurité des échanges. L'aboutissement à une opération de chargement ou de déchargement passe par une opération d'échange d'informations pour établir une

authentification et dans la norme ISO 15118 des informations sensibles sont échangées lors de cette phase, ce qui représente un risque pour les deux entités communicantes. D'où la nécessité de préserver la sécurité et la confidentialité du véhicule en préservant les informations telles que : l'emplacement du véhicule, le calendrier de charge, le taux de la batterie, les opérations et les activités effectuées.[9]

Les réseaux V2G sont également cibles de plusieurs types d'attaques visant à perturber leurs bons fonctionnements en faisant atteinte à la confidentialité, la disponibilité et l'intégrité des informations. Les échanges effectués au niveau de ces réseaux doivent être allégés en vue des ressources limitées des véhicules en termes de stockage et de puissance de calcul. Par conséquent, il faut alléger les véhicules et attribuer plus de tâches aux entités ayant une plus grande puissance de calcul et de stockage.

Dans la mesure où nous voulons avantager plus les réseaux V2G en améliorant leur sécurité et leur performance, nous proposons notre solution, qui est efficace, sécurisé, rapide et qui consomme moins d'énergie en calcul. Notre solution est basée sur l'utilisation de l'infrastructure PKI (Public Key Infrastructure) de la norme ISO 15118 et la technologie Blockchain. Notre système intègre aussi un schéma d'authentification et de chargement/déchargement, ainsi que des solutions visant à résister aux attaques les plus récurrentes sur ces réseaux.

La suite de ce mémoire est organisée comme suit : le chapitre deux introduit les réseaux V2G en présentant l'infrastructure PKI, la norme ISO 15118, ainsi que la sécurité des réseaux V2G. Le chapitre trois présente la technologie Blockchain, les différents algorithmes de consensus et la sécurité apportée par cette technologie. Le chapitre quatre porte sur une revue de la littérature concernant les réseaux V2G, les Réseaux Vanet, et les Blockchains. Le chapitre cinq présente notre article scientifique intitulé HIERARCHICAL BLOCKCHAIN SYSTEM AND LIGHTWEIGHT AUTHENTICATION FOR A SECURE V2G NETWORK soumis au journal IEEE Transactions on Vehicular Technology. Le chapitre six présente notre modèle et le schéma explicatif associé. Ce chapitre inclut aussi une partie sécurité, où nous présentons les attaques les plus nuisibles aux réseaux V2G en termes de consommation d'énergie et de temps de calcul, ainsi que les solutions proposées. Le septième chapitre met en évidence l'ensemble des outils utilisés et l'analyse des résultats obtenus à travers l'étude de notre solution. Et enfin le dernier chapitre porte sur la conclusion générale et les perspectives.

Chapitre 2 Réseaux V2G et infrastructure PKI

2.1 Introduction :

Les réseaux V2G (Vehicle to Grid) constituent l'infrastructure permettant le transfert de l'énergie renouvelable, précisément l'électricité, entre les entités communicantes afin de charger et/ou décharger les véhicules électriques. Le transfert de l'énergie électrique dans les deux sens contribue à la stabilisation du réseau électrique et à la charge des véhicules électriques dans les moments où l'énergie électrique est en abondance.[10]

Une telle infrastructure nécessite l'établissement des spécifications relatives à la communication des entités intervenantes dans les opérations établies au sein de ce réseau. La Norme ISO 15118-1 a spécifié les exigences de communication de haut niveau concernant les deux couches : physique et liaison de données [10], tandis que la norme ISO15118-2 a décrit les menaces de sécurité contre lesquels des mesures de protection ont été mises en œuvre.

Dans la suite de ce chapitre, nous allons présenter les acteurs participants dans les réseaux V2G, les types de communication énoncée par la norme ISO 15118 suivis par les opérations effectuées au sein du réseau V2G, l'infrastructure à clé publique (PKI) ainsi que son lien avec les réseaux V2G. Ensuite, nous allons discuter des certificats utilisés dans cette infrastructure, et enfin, nous présenterons les piliers et les mécanismes de sécurité dans les réseaux V2G.

2.2 Les acteurs V2G :

La Norme ISO 15118 définit deux groupes distincts d'acteurs participants au réseau V2G :

2.2.1 Les acteurs principaux : ce sont les entités visibles participantes directement au processus de chargement, soit le véhicule électrique et la borne de recharge comme le montre la figure 1.

2.2.1.1 Le véhicule électrique (EV) : est l'entité disposant d'un moteur électrique, alimenté par une batterie électrique rechargeable, et intégrant un contrôleur de communication (EVCC) permettant un échange d'information sécurisé avec la borne de recharge. Un véhicule électrique comporte également une interface homme-machine, un chargeur, et une unité de contrôle pour gérer la capacité de stockage et de traitement des données du véhicule.

2.2.1.2 La borne de charge (EVSE) : est l'entité permettant le chargement d'un ou plusieurs véhicules électriques à la fois. La borne de charge dispose d'un contrôleur de communication (SECC) qui offre une communication sécuritaire avec le véhicule à traves l'EVCC, d'une interface homme-machine, d'un compteur d'énergie électrique et d'une unité permettant le paiement.

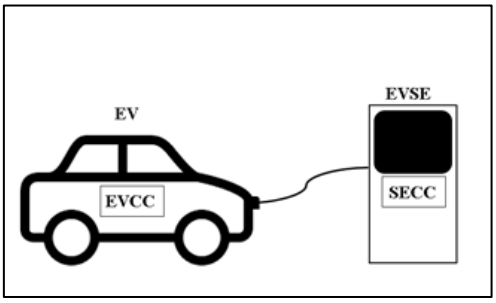


Figure 1 Acteurs principaux V2G

2.2.2 Les acteurs secondaires : ce sont les entités participantes au processus de charge de façon indirecte, soit le fabriquant d'équipement d'origine (OEM), l'opérateur de mobilité et le fournisseur de service.

2.2.2.1 Le fabriquant d'équipement d'origine (OEM): est l'entité détenant une marque de fabrication des véhicules électriques.

2.2.2.2 L'opérateur de mobilité : est une entreprise permettant d'enregistrer et d'attribuer un contrat pour les véhicules électriques, pouvant ainsi avoir accès aux services offerts par les stations de charges.

2.2.2.3 Le Fournisseur de service : est une entité permettant de fournir des services à valeur ajoutée durant les opérations de chargement/déchargement établies entre acteurs principaux.

La figure 2 ci-dessous résume l'ensemble des acteurs participant au réseau V2G:

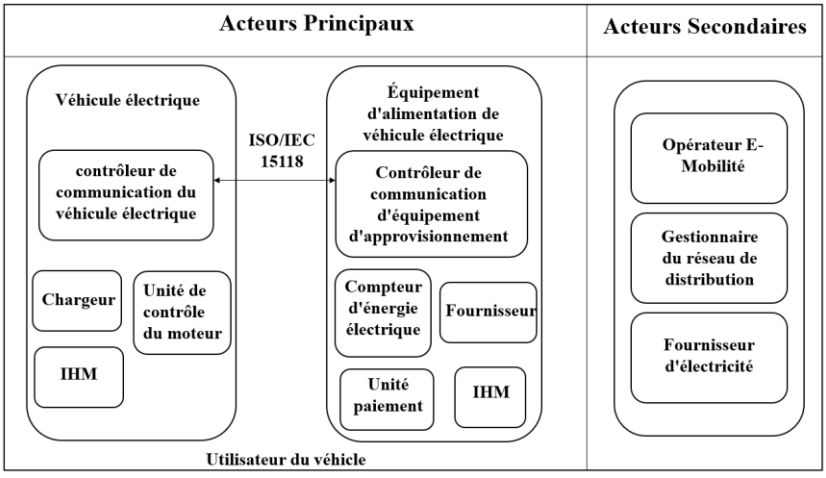


Figure 2 Acteurs participants au réseau V2G [11]

2.3 Type de communication dans les réseaux V2G:

Selon la norme ISO 15118, une communication au sein d'un réseau V2G est divisée en deux types : une communication basée sur la signalisation de base et une communication de haut niveau. Le type de communication à utiliser est dépendant du type de communication supporté par les deux entités communicantes et du cas d'utilisation nécessaire.

Une communication basée sur la signalisation de base est utilisée dans les cas suivant : la gestion des états du véhicule, la gestion du pilote de contrôle pour la sécurité et l'initialisation du processus de charge. Tandis que la communication de haut niveau est utilisée pour activer des fonctionnalités telles que l'identification, le paiement, le nivellement de charge et les services à valeur ajoutée.[10]

Une communication de type haut niveau est possible seulement si les deux entités communicantes sont équipées du dispositif de communication de haut niveau.

2.4 Opérations effectuées dans les réseaux V2G :

Les principales opérations effectuées dans les réseaux V2G sont :

2.4.1 Identification : est une fonction permettant au véhicule de s'identifier à la borne de charge, afin de recevoir une autorisation pour pouvoir accéder aux services offerts. Une identification peut être effectuée à travers un identifiant du certificat de contrat ou une carte de paiement.

2.4.2 Authentification : est une procédure dont le but est de vérifier la validité des informations présentées lors de l'identification.

2.4.3 Autorisation : après l'opération de l'authentification vient l'opération de l'autorisation, où le propriétaire doit présenter un mode de paiement, donnant ainsi à une approbation ou un refus à la demande de chargement du véhicule.

2.4.4 Paiement : après avoir obtenu une autorisation, l'unité ou le mode de paiement sera sélectionné par le propriétaire du véhicule qui peut être à travers son certificat de contrat ou une carte de crédit/débit. Les prix de l'opération effectuées se font selon un tableau de tarifs de vente.

2.4.5 Service à valeur ajoutée : présentant d'autres services offerts à part le service de charge, on retrouve dans la norme ISO 15118 des exemples de service à valeurs ajoutées, tel que : la pré-réservation d'une borne de charge publique, la disponibilité des bornes le long du trajet, ainsi que l'énergie disponible et nécessaire jusqu'au prochain chargement, etc.

2.4.6 Charge : est l'opération permettant d'augmenter le niveau de la charge du véhicule tout en respectant le calendrier de charge. Ce dernier indique les limites de charge d'un véhicule électrique par rapport à un temps spécifique.

2.4.7 Plug and charge : est un mode d'identification permettant une identification automatique après le branchement du véhicule sur l'EVSE, enclenchant ainsi son chargement.

2.5 Infrastructure à clé publique (PKI) :

La norme ISO 15118 est basé sur l'infrastructure à clés publiques PKI. Cette dernière est définie comme suit :

2.5.1 Définition : PKI (Public Key Infrastructure) est l'abréviation d'infrastructure de gestion de clés, intégrant un ensemble de techniques et de solutions de chiffrement à clé asymétrique (chiffrement à clés publiques), dont le but est de délivrer et gérer des certificats numériques. Un certificat numérique se définit en un document électronique qui permet d'identifier et authentifier chaque entité de façon unique, et à sécuriser les échanges entre les entités communicantes. Un certificat numérique est généré et signé par une autorité de certification et la signature va servir à lier la clé publique à cette identité.

Une PKI est composée de cinq entités, dont chacune a un rôle précis à jouer. L'autorité de certification ou de confiance (AC) est l'entité qui a le plus de poids dans l'infrastructure et qui signe son propre certificat. Elle a pour devoir de générer et signer les certificats des autorités sous-jacentes, ainsi que de contrôler leurs durées de vie. L'autorité de certification doit aussi participer à la vérification et à la validation de ces certificats lors de l'authentification des entités. Si le certificat correspondant n'est pas valide, il sera mis dans une liste de révocation détenue par l'autorité de certification.

2.5.2 L'autorité d'enregistrement (AE) : est une entité intermédiaire entre l'autorité de certification et l'interface de l'utilisateur. Elle a pour rôle de recevoir, vérifier et enregistrer les nouvelles demandes d'enregistrement des certificats des nouveaux utilisateurs dans l'infrastructure PKI.

2.5.3 L'Autorité de dépôt (Annuaires de certificats) : cette dernière a pour charge de détenir et gérer l'archivage des certificats numériques et des certificats expirés ou révoqués.

2.5.4 L'autorité de séquestre : est une entité ayant pour rôle de stocker et de mettre à jour les clés de chiffrement générées par l'autorité d'enregistrement.

2.5.5 L'entité finale (End Entity) : est l'entité qui va bénéficier et utiliser des certificats émis (il peut s'agir d'une entité émettrice comme le véhicule ou une entité réceptrice comme la borne de charge).

La figure 3 illustre les principales entités d'une infrastructure à clé publique.

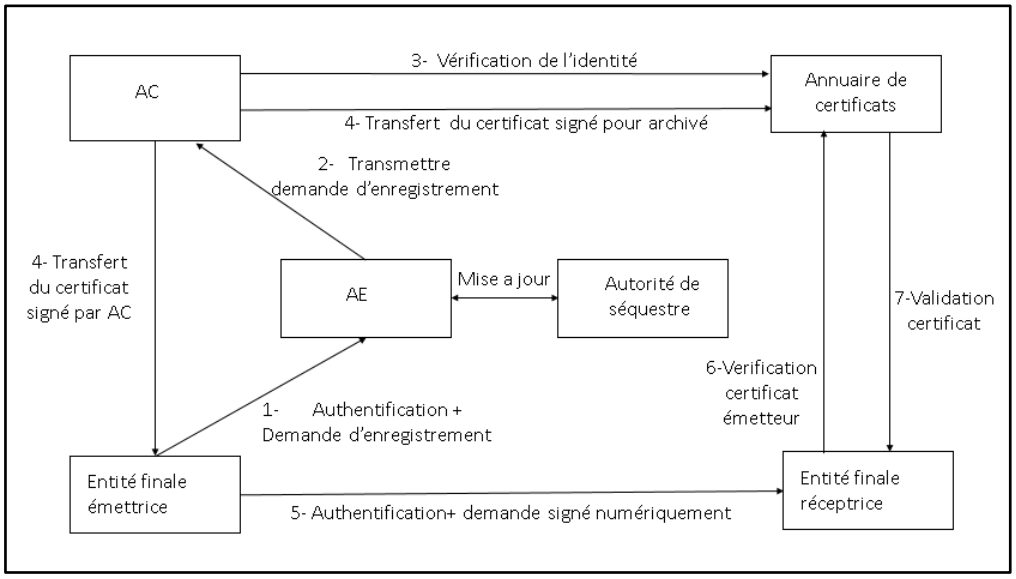


Figure 3 les principales entités d'une infrastructure à clé publique [12]

2.6 L'infrastructure (PKI) et la norme ISO 15118 :

L'infrastructure à clés publiques permet de générer les certificats, gérer leur cycle de vie, établir une identification et une authentification des entités communicantes. Elle assure une certaine sécurité entre les échanges, et offre d'autres services tels que la révocation et l'archivage de ces certificats.

La norme ISO 15118 est basée sur l'utilisation de l'infrastructure PKI hiérarchique X.509[13]. La norme X.509 désigne un sous-ensemble de la norme X.500, qui est une spécification établie par L'ITU (Union Internationale des Télécommunications). La norme X.509 traite les Certificats et les clés publiques et elle fournit une structure et une syntaxe en utilisant la notation ASN.1 (Abstract Syntax Notation One) recommandée par des documents officiels dit RFC (Requests for Comments), ce qui permet d'enregistrer les informations du certificat et les listes de révocation des certificats. [14]

Une infrastructure hiérarchique désigne une architecture en pyramide, où le sommet dit (CA-ROOT) représente l'entité racine qui est l'autorité de certification. Au niveau deux, on retrouve les autorités intermédiaires (CA1 et CA2) qui délivrent des certifications à d'autres CA intermédiaires et aux CA opérationnelles. Ensuite, on retrouve les CA opérationnelles qui délivrent des certificats aux entités finaux.

La figure 4 illustre une PKI hiérarchique [15].

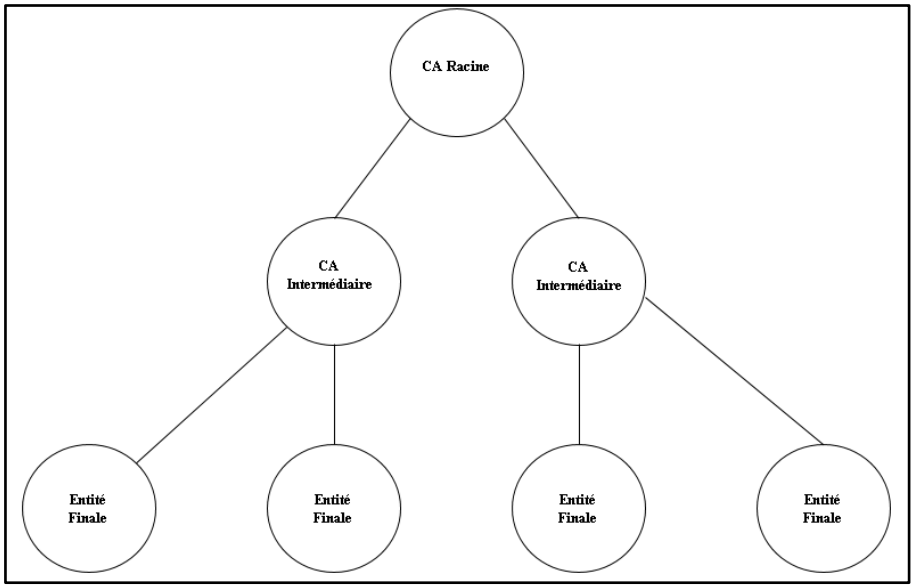


Figure 4 PKI hiérarchique

Plusieurs autres architectures PKI existent telles que le « Peer-to-Peer » (également appelée Mesh PKI) largement utilisé dans les réseaux (MANET), où les entités CAs sont égales et au même niveau, et ces dernières signent les certificats des unes et des autres après avoir effectué une authentification mutuellement. L'architecture représente plusieurs lacunes tel que la complexité de la vérification du chemin du certificat dû à la pluralité des chemins entre les entités, aussi il faut prendre en compte que la création d'un chemin de certification depuis le certificat d'une entité jusqu'à l'entité de confiance est non déterministe. L'architecture représente aussi un risque de formation de boucles lors de la construction du chemin de certification. [16]

La figure 5 illustre une infrastructure PKI en Peer-to-Peer:

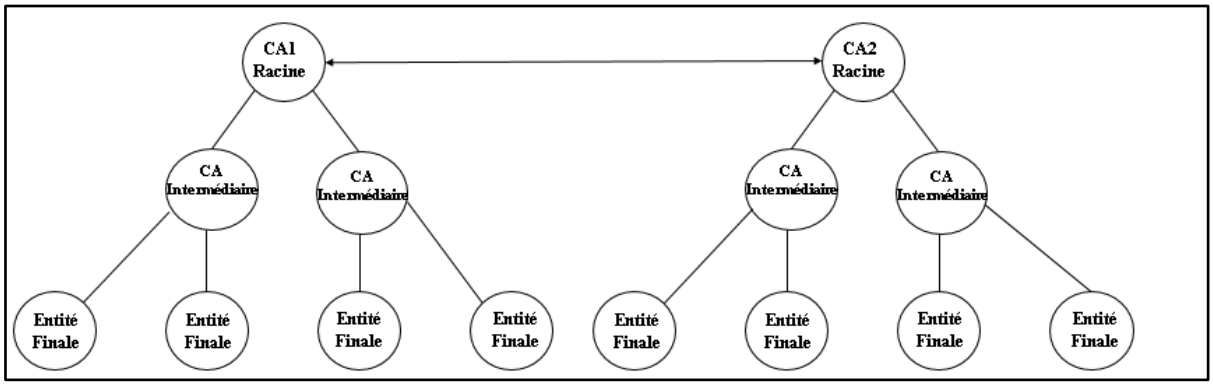


Figure 5 PKI Peer-to-Peer

L'architecture en Pont CA (Bridge CA), quant à elle est utilisée pour lier des systèmes PKI séparés et distincts, en créant entre-eux une relation de confiance via un processus de certification croisée entre les différentes CA (CA délivrant un certificat à une autre CA) [17]. La présence « d'une autorité de certification Pont » ne permet pas seulement d'établir un lien de confiance, mais également de minimiser les échanges entre les autorités de certifications, car ces dernières n'ont plus besoin de partager leurs clés publiques.

La figure 6 illustre une infrastructure PKI en Pont : [15].

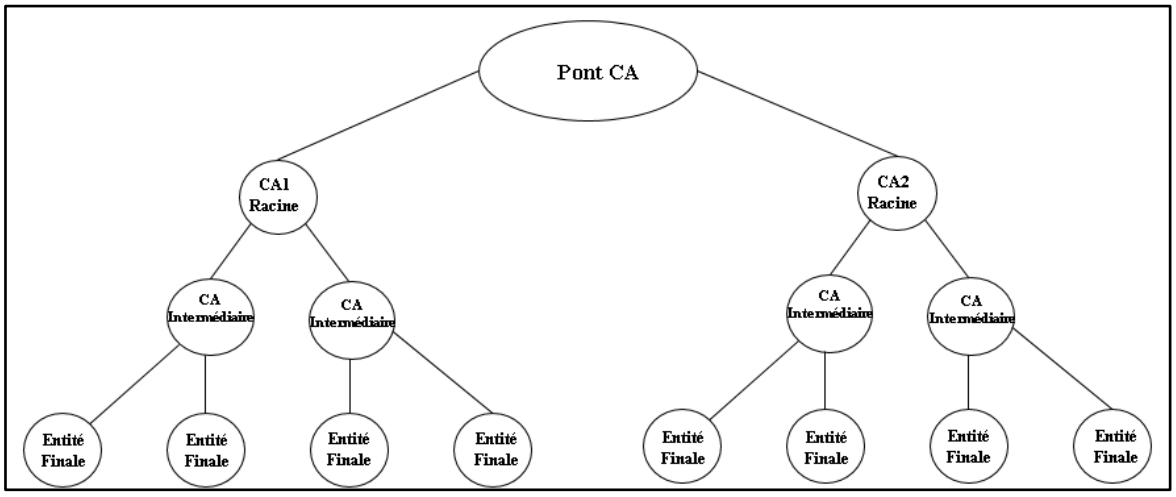


Figure 6 PKI Pont

Le choix de la norme ISO 15118 s'est posé sur l'utilisation de l'architecture hiérarchique X.509 pour la sécurité et la facilité des échanges qu'elle apporte, que ce soit pour des échanges entre les autorités de même niveau ou de niveaux différents. La figure 7 illustre la structure de certificat résultante établie par la norme ISO 15118-2.[13]

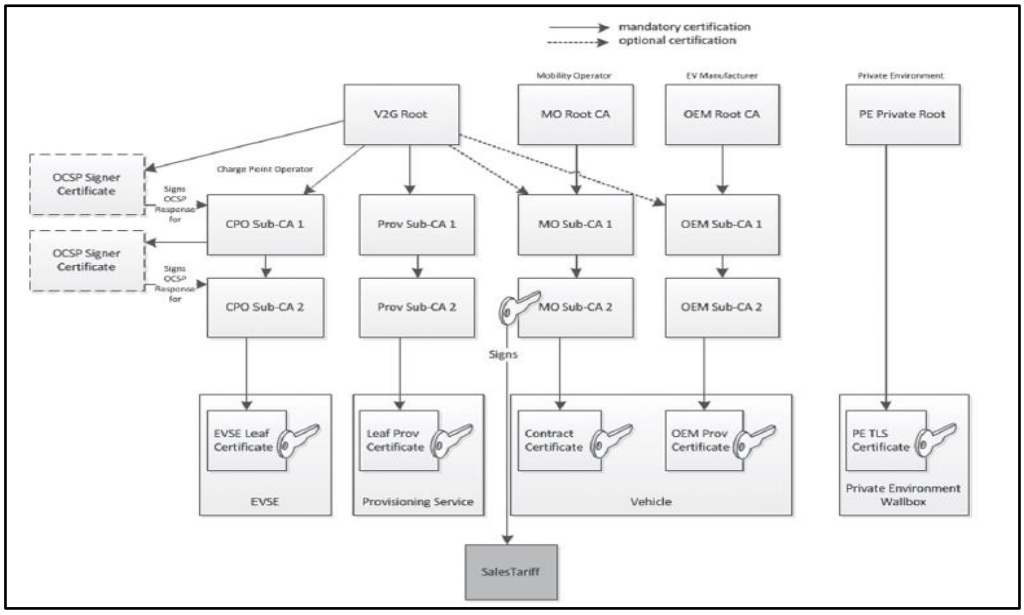


Figure 7 Structure PKI de norme ISO 15118-2.

Certes l'utilisation de cette infrastructure a permis de sécuriser la communication, mais quelques lacunes persistent, comme; la complexité de l'infrastructure qui exige de multiples entités intermédiaires.[18]

2.7 Type de certificats dans l'infrastructure PKI:

Les certificats générés et utilisés dans la norme ISO 15118 sont [13] :

2.7.1 Certificat Racine V2G : est un certificat délivré par une autorité de certification racine, qui détient également les clés privées des entités ayant reçu ce certificat. Les certificats racines sont utilisés par les autorités sous-jacentes pour vérifier l'authenticité des certificats.

2.7.2 Certificat racine de l'opérateur de mobilité : ce certificat sert à signer les certificats de contrat.

2.7.3 Certificat de contrat : ce contrat est délivré par un certificat racine d'opérateur de mobilité, il sert à authentifier un véhicule et un acteur secondaire lors d'une opération de chargement PnC (Plug and Charge).

2.7.4 Certificat SECC : ce certificat est dérivé par une autorité de certification « Racine V2G », il sert à authentifier l'entité SECC auprès de l'entité EVCC.

2.7.5 Certificat d'approvisionnement OEM (Original Equipment Manufacturer) : ce certificat désigne un véhicule de façon unique, il sert à identifier un véhicule électrique au commencement du processus d'approvisionnement.

2.7.6 Certificat racine OEM : ce dernier sert à signer les certificats d'approvisionnement OEM. Chaque OEM peut être propriétaire d'un certificat racine OEM non signé par un certificat racine V2G. Les différents champs d'un certificat tel que défini par la norme X.509 sont [19]:

- **Version** : indique la version X.509 du certificat.
- **Serial number** : numéro de série correspondant à l'autorité de certification.
- **Issuer Name** : nom de l'autorité de certification émettrice du certificat.
- **Validity period** : champ désignant la période de validité de ce certificat.
- **Subject Name** : nom du certificat.
- **Subject pub. Key**: la clé publique du certificat.
- **Extensions** : extensions comprenant des informations supplémentaires tel le chiffrement, l'horodatage.
- **Issuer Unique ID** : identifiant unique désignant le générateur du certificat.
- **Subject Unique ID :** identifiant unique du propriétaire de la clé publique.
- **Signature Algo ID** : identifiant de l'algorithme utilisé pour le chiffrement.
- **Signature** : signature du certificat.

2.8 Sécurité des Réseaux V2G:

Afin d'assurer la sécurité au niveau du réseau V2G, il est impératif de garantir les piliers essentiels de la sécurité informatique, à savoir :

2.8.1 L'authentification : est un processus permettant d'établir une vérification de l'identité électronique et la légitimité entre le véhicule électrique et la borne de recharge.

2.8.2 La confidentialité : est le fait d'assurer qu'au sein du réseau V2G, l'accès à l'information est destiné seulement aux entités légitimes autorisées.

2.8.3 La disponibilité : est la capacité du système informatique à rester opérationnelle pendant une période donnée et ainsi répondre aux requêtes des véhicules électriques.

2.8.4 L'intégrité : désigne la protection des informations transmises dans le réseau V2G contre la falsification et l'altération.

2.8.5 La non-répudiation : est le fait de s'assurer que dans le réseau V2G, aucune entité ne peut en aucun nier l'exécution d'une certaine tâche ou action.

Ces piliers de sécurité peuvent être assurés en appliquant des mécanismes de sécurité, à savoir :

2.8.6 Cryptage (chiffrement) : opération permettant de passer d'une information lisible et claire, a une information incompréhensible et cela dans le but de garantir la confidentialité dans le réseau V2G ; il existe deux méthodes de chiffrement :

2.8.6.1 Le chiffrement symétrique (chiffrement à clé secrète): cette méthode repose sur le partage d'une clé secrète entre le véhicule électrique et la borne de recharge. La même clé est utilisée pour le chiffrement et le déchiffrement du message. Le chiffrement symétrique est facile à mettre en œuvre, mais il nécessite une communication au préalable pour le partage de la clé secrète, ce qui représente un risque pour la compromission de cette dernière. Plusieurs algorithmes de chiffrement symétrique existent tel que: le DES, le Triple DES et l'AES.

2.8.6.2 Le chiffrement asymétrique (chiffrement à clé publique): cette méthode est basée sur l'utilisation d'une paire de clés pour chaque entité du réseau V2G. Une clé publique qui peut être connue par toutes les entités et une clé privée qui n'est connue que par l'entité propriétaire, les deux clés sont mathématiquement liées. Le chiffrement se fait en utilisant la clé publique du destinataire, et le déchiffrement est effectué par le récepteur en utilisant sa propre clé privée. Cette méthode garantit que seulement le destinataire peut déchiffrer le message. Les algorithmes de chiffrement asymétriques les plus connus sont RSA (Rivest–Shamir–Adleman) et ECC (Elliptic Curve Cryptography).

2.8.7 Hachage : est une fonction permettant d'assurer l'intégrité du message au sein du réseau V2G. Un message passe comme valeur d'entrée à travers la fonction de hachage, donnant comme résultat un condensat de message. La valeur d'entrée et la valeur de sortie de la fonction de hachage seront transmises à la destination, qui va appliquer la même fonction de hachage sur la valeur d'entrée, puis comparer le résultat obtenu avec le condensat du message reçu. Si les résultats sont identiques, l'intégrité est validée. La fonction de hachage permet aussi un transfert de données de taille fixe.

2.8.8 La signature numérique : est un mécanisme permettant de garantir l'authentification et la non- répudiation. L'émetteur utilise le résultat du hachage dit condensat ou empreinte pour le chiffrer avec sa clé privée obtenant ainsi une signature. Puis le message d'entrée et la signature sont envoyés au destinataire, qui a son tour, va reproduire une empreinte via la fonction de hachage et déchiffrer la signature avec la clé publique de l'émetteur, si ces derniers sont identiques, l'authenticité de l'émetteur est validée.

2.9 Conclusion:

Dans ce chapitre nous avons présenté les principaux éléments de la norme ISO 15118 et des réseaux V2G, en présentant les entités participantes et les types d'échanges établis entre celles-ci. Ce chapitre introduit également les avantages et inconvénients des différentes infrastructures PKI ainsi que la structure de certificat résultant utilisée dans les réseaux V2G. Enfin, nous avons vu les exigences de sécurité à satisfaire et les mécanismes de sécurité appliqués dans l'infrastructure PKI.

Au chapitre suivant, nous allons présenter une vue globale sur la technologie blockchain, les améliorations sécuritaires qu'elle peut nous apporter et les lacunes qui peuvent survenir à son utilisation.

Chapitre 3 Chaine de blocs

3.1 Introduction :

La chaine de blocs ou blockchain est une base de données distribuée, définie également comme un grand livre ouvert sans autorité de contrôle centrale. C'est une base de données sous forme de blocs où le premier bloc est dit « bloc genesis » (dans la blockchain Bitcoin). Chaque bloc est relié au bloc précédant à travers une fonction de hachage. Les blockchains servent à stocker les données sous forme de blocs de transaction et à garantir la transparence et la sécurité des données.

La figure 8 suivante illustre un exemple de la structure de la blockchain :

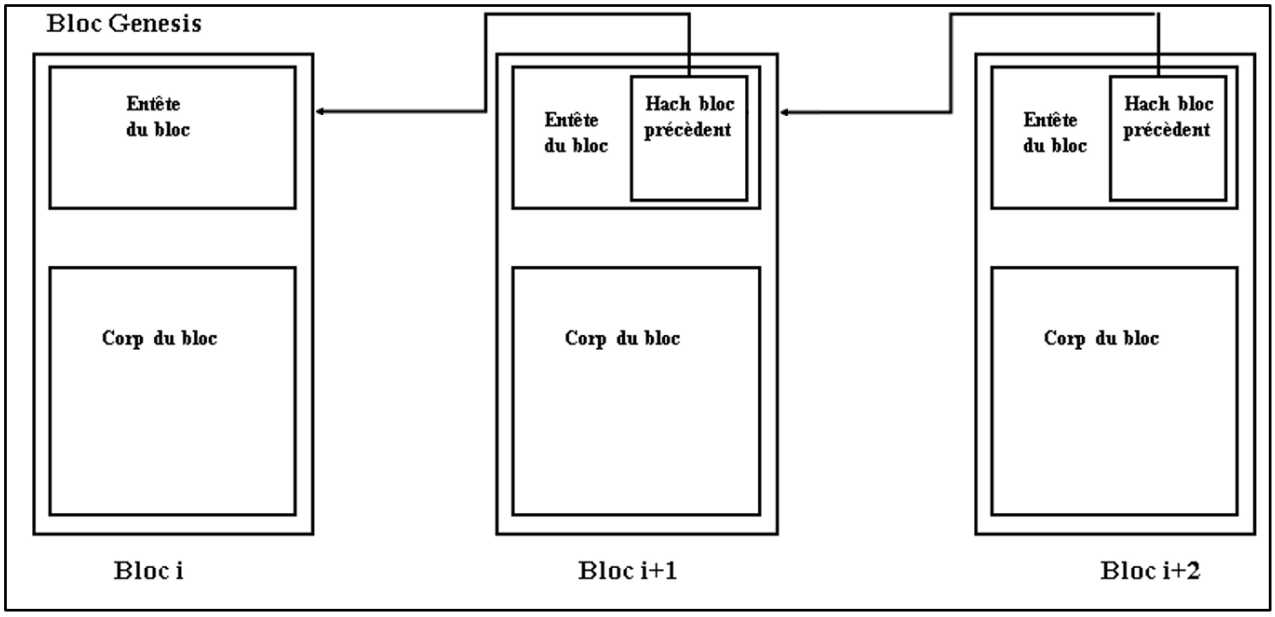


Figure 8 Structure de la blockchain [20]

3.2 Composant d'un bloc de blockchain :

Un bloc d'une blockchain contient un certain nombre de champs définis, toute fois des blocs de blockchains différentes peuvent contenir un à deux champs différents. Ci-dessous, on peut voir la structure d'un bloc qui est présentée en deux parties ; l'entête et le corps du bloc.

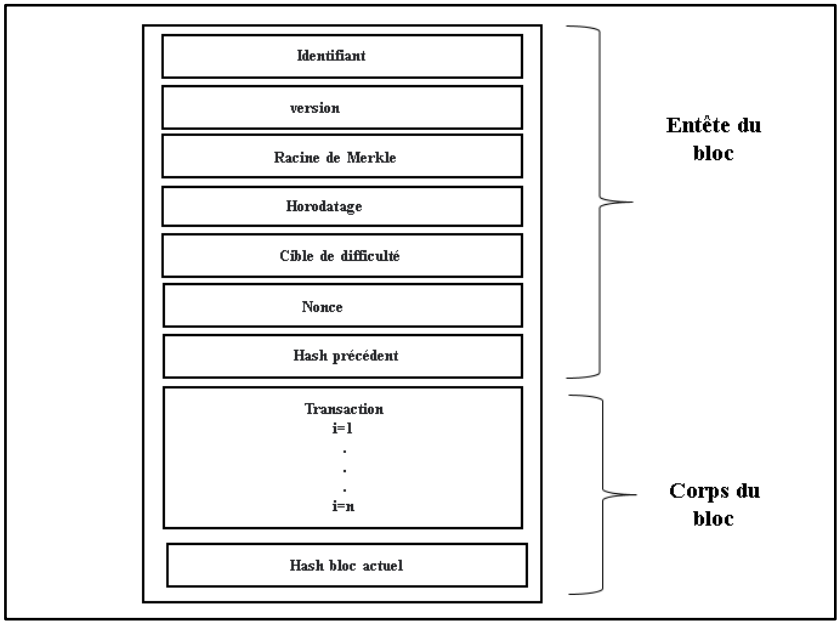


Figure 9 Entête et corps d'un bloc de blockchain

3.2.1 L'entête [21] :

L'entête contient les champs suivants :

3.2.1.1 L'identifiant : est un champ qui permet de pointer de façon unique un bloc dans une blockchain. Dans certaines blockchains, il peut s'agir de la preuve de travail du nœud (validateur ou mineur dépendamment de la blockchain) ayant préparé le bloc à insérer pour des fins de sécurité.

3.2.1.2 Version : ce champ indique la version de la blockchain utilisée. Il existe plusieurs versions de blockchain, ainsi par exemple, la version (01) indique la blockchain cryptomonnaie telle que Bitcoins et la version (04) indique la blockchain pour l'industrie.

3.2.1.3 Horodatage : c'est un champ qui permet de connaitre l'heure et la date où le bloc a été créé. Il apporte également une sécurité au bloc en assurant l'authenticité et l'intégrité.

3.2.1.4 Racine de Merkle : Cette dernière est basée sur une fonction de hachage à sens unique. Ce champ permet de lier les blocs, ordonner et répertorier un ensemble de transactions. À chaque création d'un nouveau bloc, les transactions choisies à partir de la file d'attente sont organisées puis hachées et les haches résultantes vont être combinées puis re-hachées jusqu'à l'obtention d'un seul hach appelé **racine**. Ce dernier va être ajouté à l'entête du bloc. [22]

3.2.1.5 Nonce : ce champ indique un nombre aléatoire que les mineurs doivent modifier à plusieurs reprises jusqu'à la validation du bloc et l'obtention d'une récompense.

3.2.1.6 Cible de difficulté : ce champ indique la puissance de calcul nécessaire pour participer aux opérations effectuées au sein du réseau.

3.2.1.7 Hach précédant : champ indiquant le résultat du hach du bloc précédant, ce qui permet de lier chaque bloc à son prédécesseur formant ainsi une chaine de plusieurs blocs.

3.2.2 Le corps d'un bloc de blockchain contient :

3.2.2.1 Hach du bloc actuel : champ comportant la valeur résultante d'une opération de hachage du bloc actuel.

3.2.2.2 Transactions : champ comportant l'ensemble des transactions pour lesquelles le bloc a été créé. La première transaction représente la transaction récompense qui inclue également les frais de transactions.

La figure 10 montre un exemple d'un bloc de la blockchain Bitcoin où on peut voir les différents champs de l'entête et une transaction parmi les transactions incluses dans le corps du bloc :

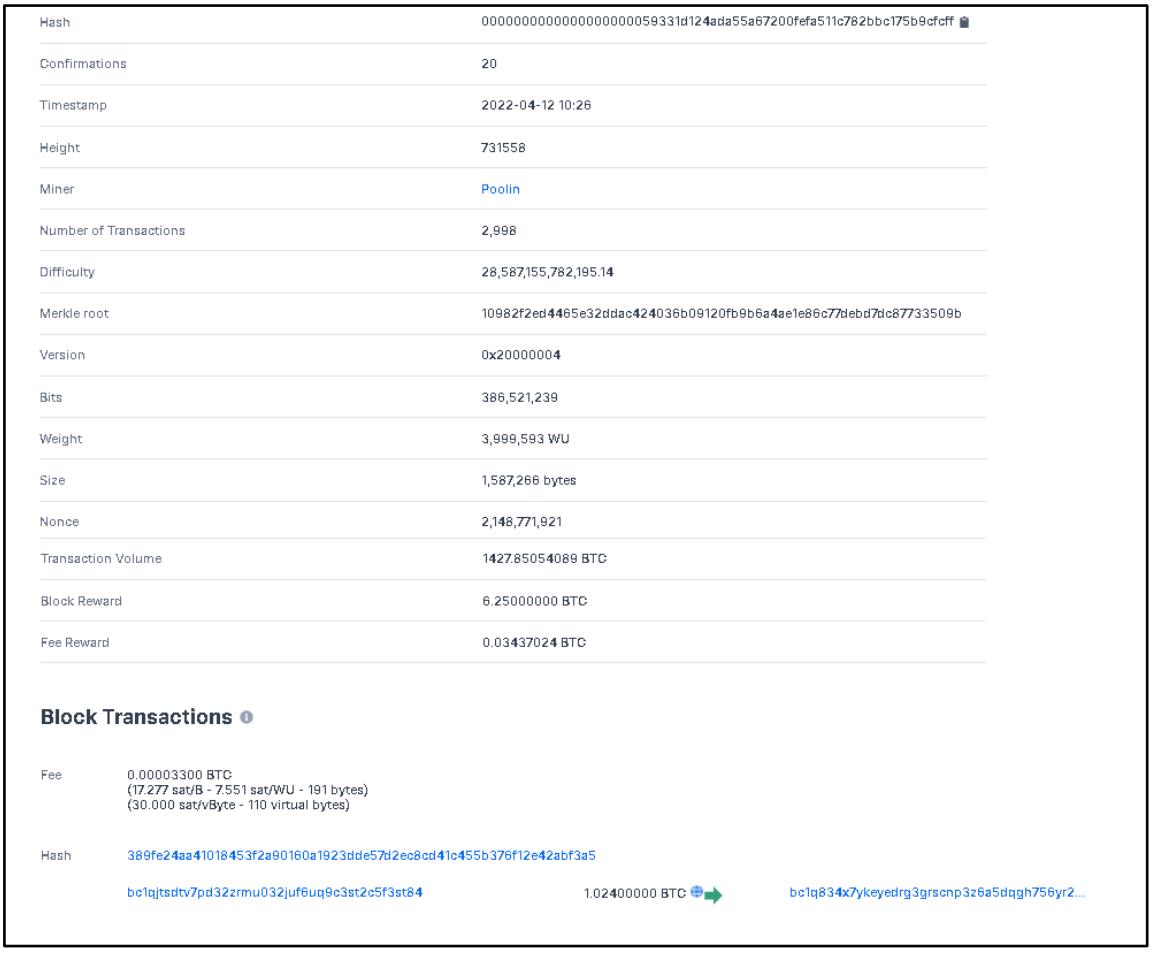


Figure 10 Exemple de bloc de la blockchain Bitcoin]23[

3.3 Les composants d'une blockchain :

3.3.1 Les nœuds : Sont les entités participantes à la création et à la validation de nouveaux blocs dans une blockchain. Chaque nœud détient une copie de cette dernière, ce qui fait qu'il doit nécessairement disposer d'une capacité de stockage mémoire suffisante et d'une puissance de calcul élevé.[24]

3.3.2 Le contrat intelligent: Est un programme auto-exécutable ayant pour devoir de vérifier et d'imposer le respect des négociations établies entre les entités du réseau, tout en décentralisant et sécurisant les transactions.

3.3.3 Portefeuille de cryptomonnaie : C'est un dispositif virtuel ou physique spécifique à chaque nœud et il est stocké dans la blockchain, permettant ainsi le stockage de la cryptomonnaie. Il contient une clé privée et une clé publique. La clé privée permet au nœud de déclencher des transactions et de dépenser de la cryptomonnaie. La clé publique lui permet de recevoir des récompenses (des cryptomonnaies) à la suite d'une validation d'un nouveau bloc ou de recevoir des paiements.[24,25]

3.3.4 Algorithme (protocole) de consensus : C'est un accord permettant une gestion décentralisée, la validation et l'ajout de nouveaux blocs dans la blockchain assurant ainsi la sécurité de cette dernière. Le consensus d'une blockchain est défini à sa création par les fondateurs de celle-ci. Plusieurs algorithmes de consensus existent tels que la preuve de travail et la preuve d'enjeu.[26]

3.4 Les types de blockchain :

3.4.1 Public (sans autorisation) : Les informations contenues dans les blocs d'une blockchain publique sont visibles pour tous les nœuds et chaque nœud peut modifier et valider les blocs. Cependant, pour ajouter un nouveau bloc à la blockchain, il doit être validé par au moins 51% des nœuds participants. Les blockchains publics sont également munis d'un mécanisme de défense (Byzantine Fault Tolerance) contre les nœuds malveillants [27]. Comme blockchain publique, on peut citer : Bitcoin, Ethereum, Litecoin.

3.4.2 Privé (avec autorisation) : Cette dernière est spécifique à un certain nombre de nœuds autorisés à participer à la blockchain. Gérer par une autorité centrale, les blockchains privées sont plus rapides pour la validation de nouveaux blocs et le passage d'un algorithme de consensus à un autre se fait plus facilement comparée à une blockchain publique. Cependant, ce type de blockchain nécessite une confiance interne entre les nœuds pour la validation des nouveaux blocs et une confiance externe entre les nœuds externes de la blockchain [28]. Comme blockchain privée, on peut citer : Hyperledger Fabric.[29]

3.4.3 Hybride : Une blockchain hybride combine à la fois la blockchain publique et la blockchain privée. Elle est gérée par une organisation. Ces transactions et ces blocs peuvent être définis au choix pour être visibles par tout le monde ou seulement par un groupe spécifique. La

blockchain hybride offre une force de sécurité comme la blockchain publique [30]. Comme blockchain hybride, on peut citer : Quorum.[31]

3.5 Le Minage :

C'est une opération permettant de valider et de rajouter un nouveau bloc à la blockchain existante, cette opération est effectuée par des nœuds dits mineurs, les étapes ci-dessous décrivent le déroulement de cette opération : [24]

- Un nœud disposant d'un portefeuille déclenche une transaction en utilisant sa clé privée, dépensant ainsi de la cryptomonnaie.
- La transaction effectuée est déposée par la suite dans un pool de transactions non confirmées, en attendant la création d'un bloc de plusieurs transactions par un mineur.
- Chaque mineur rassemble alors un ensemble de transactions à partir de ce pool de transactions, pour pouvoir créer un bloc et rajouter les métadonnées correspondantes tout en respectant la taille du bloc. (Les blocs créés par les mineurs peuvent contenir différentes transactions)
- Suite à la création du bloc, le processus de minage commence. Pour pouvoir ajouter ce bloc à la blockchain, chaque nœud effectue une opération de minage afin de résoudre un problème mathématique complexe (appelé l'algorithme de consensus) aboutissant ainsi à une signature.
- Après la signature du bloc, le mineur propage ce bloc aux autres mineurs pour sa vérification et sa validation.
- Les autres mineurs vérifient le bloc à travers les données de ce bloc, le hach et la signature. Si le bloc est validé, il sera ajouté à la blockchain et le nœud ayant résolu le bloc reçoit une récompense.
- À la suite de l'ajout du nouveau bloc, les blocs suivants ce dernier rajoute une confirmation dans l'historique des transactions et plus le nombre de blocs le succédant augmente, plus le nombre de confirmations augmente et ainsi la sécurité de ce bloc augmente aussi.

3.6 Les Algorithmes de consensus :

3.6.1 La preuve de travail (PoW) : Cet algorithme de consensus est utilisé par de nombreuses blockchain telles que le bitcoin, le litecoin et l'Ethereum.

La preuve de travail est basée sur la fonction de minage pour l'ajout de nouveaux blocs à la blockchain. Chaque bloc contient une signature qui est issue de l'exécution d'une fonction de hachage sur ce bloc. Ce dernier ne peut être ajouté à la blockchain si sa signature ne commence pas par certains caractères prédéfinit, pour cela les mineurs doivent changer plusieurs fois une chaine de caractère inclus dans le bloc dit « le nonce » jusqu'à l'obtention d'une signature répondant au critère prédéfinit (la suite de caractère nécessaire). Le mineur ayant résolu le problème reçoit une récompense et des frais de transaction. [24,32]

La preuve de travail offre une résistance contre plusieurs attaques, mais consomme énormément d'énergie de calcul. Comme on peut le voir sur la figure 11 qui illustre la consommation d'énergie électrique par la blockchain Bitcoin (utilisant PoW) à travers les années, la ligne continue rouge indique l'estimation de l'énergie électrique consommée et la ligne discontinue orange indique le minimum d'énergie électrique consommée.

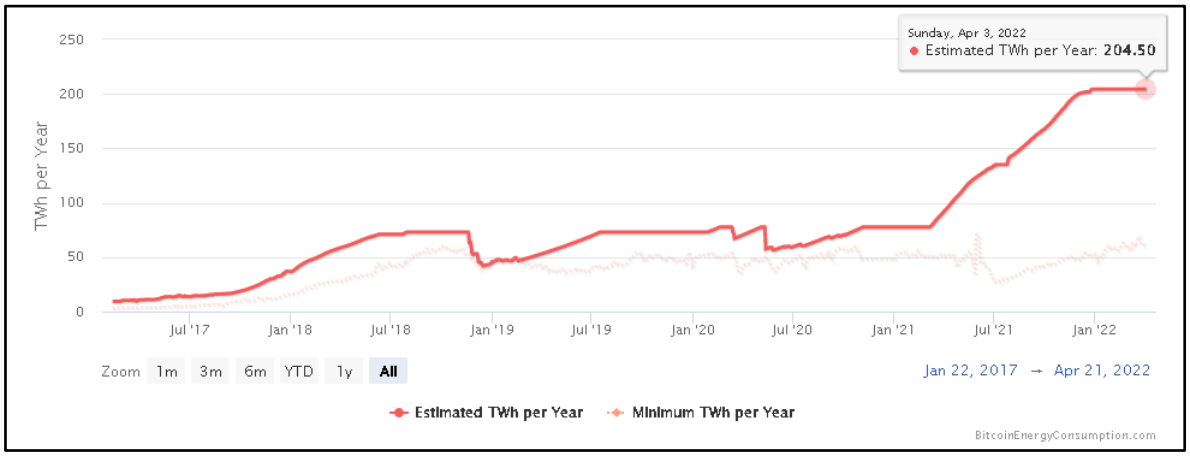


Figure 11 Consommation d'énergie dans le bitcoin **[32]**

La consommation d'électricité au Québec pour l'année 2018 s'élève à 197,3 milliards de kWh ce qui vaut 197 Térawatts, dont 35% représentent la consommation résidentielle soit 68 Térawatts [33], en comparant cette dernière avec la consommation minimale d'énergie électrique par la blockchain Bitcoin seulement, qui s'élève à 60 Térawatts en cette même année, on peut voir que la quantité d'énergie consommée par cette blockchain est considérablement très proche de la consommation résidentielle d'un état de la taille du Québec.

3.6.2 La preuve d'enjeu (PoS) : Contrairement à la preuve de travail, la preuve d'enjeu consomme moins d'énergie de calcul. Les différents nœuds du réseau appelés « minters » déposent une partie de leurs cryptomonnaies pour pouvoir ajouter un nouveau bloc à la blockchain et l'algorithme sélectionne aléatoirement un minter parmi les minters pour créer le bloc durant un intervalle de temps limité.

Dans la preuve d'enjeu, les nœuds ayant le plus de cryptomonnaies sont considérés comme des nœuds ayant intérêt à sécuriser la blockchain. Certes la preuve d'enjeu évite les cas de centralisation qui peuvent survenir au niveau de la preuve de travail si des mineurs disposent de plus forts équipements de calcul tels ASIC (Application Specific Integrated Circuit), et consomme moins en énergie, mais elle est considérée comme étant moins sécurisée que la preuve de travail.[34,35]

La figure 12 illustre la consommation de l'énergie électrique par les deux blockchains : Bitcoin et Ethereum. On remarque sur les deux diagrammes que la blockchain Bitcoin utilisant PoW est largement plus gourmande en énergie que la blockchain Ethereum utilisant PoS.

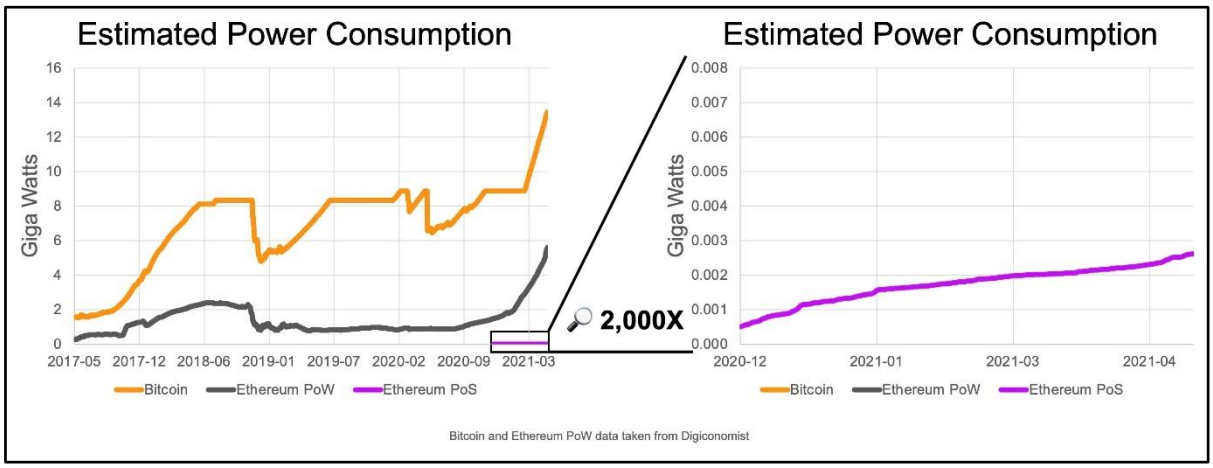


Figure 12 Consommation de l'énergie électrique par les blockchains Bitcoin et Ethereum [36]

D'autres algorithmes de consensus existent tel que : La preuve de temps écoulé (PoET), La preuve d'importance (PoI) … etc.

3.7 Sécurité blockchain :

La technologie blockchain assure la sécurité, la transparence, l'intégrité des données, et la confidentialité dans le cas d'une blockchain privée.

Les algorithmes de hachage utilisés dans les blockchains varient d'une blockchain à une autre. La blockchain Bitcoin utilise le protocole SHA256 alors que la blockchain Ethereum utilise la variante SHA-3 (KECCAK256).[37,38]

Les algorithmes de cryptage varient également. La blockchain Bitcoin utilise l'algorithme ECDSA pour la génération des paires de clés privées et publiques ainsi que la signature et la vérification des transactions. [39]

Les smart contrats sont catégoriques pour assurer non seulement le bon fonctionnement de la blockchain, mais également pour assurer la sécurité de cette dernière. [40,41]

Les blockchains sont ciblées par plusieurs attaques, mais pour que ces dernières puissent altérer les données de la blockchain, il est impératif que l'attaque touche simultanément 51% des nœuds participant à ce réseau et que l'attaquant ait les ressources nécessaires en termes d'équipements de calcul et en électricité pour pouvoir modifier tous les blocs de la blockchain.

3.8 Problèmes des blockchains :

Certes les blockchains présentent beaucoup d'avantages telles la non-nécessité d'un tiers de confiance, la protection des données contre les modifications non autorisées, et la sécurisation contre de multiples attaques telle que l'attaque de l'usurpation d'identité [42], mais elles présentent aussi des lacunes que nous pourrions résumer comme suit :

- Les blockchains sont très énergivores et nécessitent des équipements puissants en termes de calcul ;

- À chaque création et approbation d'un nouveau bloc, une synchronisation des chaines distribuées dans le réseau est nécessaire. Certainement, cela demande beaucoup de mises à jour, néanmoins, ça évite de perdre la seule chaine du réseau et assure la conformité des données et la sécurité des nœuds participants au réseau.[43]

3.9 Conclusion :

Dans ce chapitre, nous avons tout d'abord présenté les éléments principaux de la technologie blockchain, ensuite nous avons mis en évidence les composants d'un bloc de blockchain ainsi que les composants de cette dernière et nous avons vu aussi les différents types de blockchains tels que : la blockchain privée, publique et la blockchain hybride. Nous avons mis en valeur également l'opération de minage et les algorithmes de consensus en citant quelques exemples de blockchains utilisant ces algorithmes. Et enfin, nous avons introduit dans ce chapitre la sécurité offerte par cette technologie et les lacunes qui peuvent survenir à son utilisation.

Dans le chapitre suivant, nous allons présenter une revue légère de la littérature sur les réseaux Vanet, les réseaux V2G, et les blockchains.

Chapitre 4 Revue de la littérature

Au cours des dernières années, de nouvelles recherches ont proposés plusieurs approches afin de garantir une communication légère, sécuritaire et fiable pour les réseaux V2G.

Dans ce chapitre, nous allons présenter, quelques travaux et études issues de la littérature relativement à la sécurité des réseaux Vanet, des réseaux V2G, ainsi qu'aux blockchains. Nous allons présenter également les points forts et les inconvénients de ces travaux.

Dans [44],les auteurs présentent des recommandations pour corriger les failles de sécurité existantes dans la norme ISO 15118, dans le but de garantir la sécurité du processus de facturation. Dans un premier temps, les auteurs proposent de rendre l'utilisation du protocole TLS (Transport Layer Security) obligatoire en tout temps, et cela même dans les environnements de confiance, afin d'éviter toute falsification ou manipulation. Dans l'étape suivante, les auteurs recommandent de restreindre le temps de révocation des certificats usurpés et de vérifier la validité des certificats EV en utilisant OCSP (Online Certificate Status Protocol), et ensuite de vérifier la validité des certificats TLS en utilisant l'horodatage.

Les auteurs désapprouvent l'utilisation de source non viable pour la synchronisation de l'horloge sécurisée qui ouvre une brèche à une manipulation de la part de l'attaquant. Pour corriger ce problème, ils proposent l'utilisation de mécanismes authentifiés pour la synchronisation et l'extension des exigences de précision de temps, pour éviter toute mauvaise manipulation des certificats expirés. Dans un dernier point, les certificats signés par les sous-CA peuvent être attribués pour assurer plusieurs rôles, les auteurs proposent d'établir des techniques qui permettent de lier les sous-autorités de certification à un certain rôle. Les auteurs ont fait le tour des attaques possibles, mais aucune expérimentation n'a été faite pour valider les recommandations avancées.

Afin de garantir la sécurité du processus de facturation, les auteurs dans [45] ont proposé un protocole d'authentification conditionnel. Ce dernier est composé de six étapes qui sont l'initialisation du système, l'enregistrement de l'EV, l'authentification mutuelle, le processus de transmission des messages, la phase de suivi et la phase de révocation. L'exécution nécessite une TA (autorité de confiance) qui génère les paramètres de sécurité globaux du système, les clés de toutes les entités et un LAG (Local Aggregator) pour la collection des informations d'état en temps réel sur les EVs qui souhaitent rejoindre le réseau intelligent. Ce protocole préserve la confidentialité, l'intégrité l'anonymat, et la non-répudiation. Malheureusement, l'efficacité des protocoles proposés dans [45] n'est pas démontrée ni par la simulation ni par la modélisation, ce qui crée des doutes sur le fonctionnement du protocole dans l'environnent V2G et sur son efficacité fasse à de vraies attaques.

Pour vérifier l'authenticité des identités, la confidentialité des messages ainsi que celle des identités, Shuai Wang & al [46] proposent un schéma de communication V2G basé sur les trois technologies; l'informatique de confiance, la signcryption et la technologie de routage de l'oignon. Pour une communication en dehors de la zone de couverture de l'agrégation, ils utilisent la technologie de routage de l'oignon pour construire un lien de communication anonyme, ou à

l'intérieur de la zone de couverture de l'agrégateur en utilisant la technologie signcryption pour compléter la signature et le cryptage du message. Les auteurs affirment que cette solution assure une certaine sécurité, mais aucun résultat concret ne le prouve, il est également toujours nécessaire de trouver un nœud intermédiaire pour garantir le déroulement du processus.

Les auteurs dans [47] ont conçu un schéma d'authentification mutuelle dans les réseaux V2G, utilisant un protocole d'accord de clé authentifiée établie entre l'EV et le réseau et qui génère une clé de session commune sécurisée utilisable pour toute autre communication. Pour assurer la confidentialité, les auteurs optent pour l'utilisation de pseudonymes choisis aléatoirement. Les auteurs affirment que le schéma proposé est plus efficace et sécurisé que d'autres schémas pertinents tels que ceux basés sur l'appariement [48]. Certes les auteurs ont testé la confidentialité et l'authentification, mais il n'y a pas eu de test sur l'intégrité ni sur la non-répudiation.

D. S. V. Madala et al, ont proposé dans [49] un schéma de partage de données sécurisé basé sur le niveau d'adhésion dans les réseaux V2G. Les EVs ayant un niveau d'adhésion plus élevé ont davantage accès aux informations de service que ceux ayant un niveau d'adhésion plus faible. Ils utilisent également le mécanisme de cryptage basé sur les attributs de la politique de texte chiffré en ligne/hors-ligne combiné à la technologie Fog Computing. Dans ce schéma, le texte est crypté par le centre de contrôle (CC) et décrypté par les EVs qui ont un niveau d'adhésion requis selon la politique d'accès. Les auteurs observent une réduction du temps nécessaire pour crypter/décrypter les données. Selon les auteurs, le schéma proposé réduit le temps nécessaire au cryptage/décryptage des données et garantit la confidentialité des informations. Cependant, l'intégrité et la disponibilité n'ont pas été prises en considération.

La transparence des certificats est une technique créée par Google, qui exige que les autorités de certification (CA) utilisant SSL/TLS émettent des certificats X.509 qui sont visibles par le propriétaire du domaine. Afin de construire une base de données de certificats vérifiable publiquement, les auteurs du projet Certificate Transparency (CT) [50] créent un système de journal public, où les certificats émis par les autorités de certification peuvent être facilement vérifiés par les clients et les entités appelées auditeurs et contrôleurs, qui peuvent effectuer des tâches pour les clients telles que l'édition ou la vérification du journal public. Le certificat de transparence est destiné à contrôler tout certificat émis par les CA. Aucune autorité de certification (CA) ne devrait émettre un certificat pour un domaine sans qu'il ne soit publiquement visible. L'utilisation de journaux publics est largement proposée pour la structure de PKI, mais la coordination des journaux est nécessaire pour la validité des certificats publiés. La sécurité des communications inter-entités équivaut à la sécurisation de l'infrastructure PKI, et elle a surmonté la fragilité des autorités de certification. Par conséquent, les auteurs dans [51] cherchent à donner aux propriétaires de domaines un contrôle absolu sur l'autorisation des certificats pour leurs domaines, et ils proposent donc le système CTB (Certificate Transparency Using Blockchain), dans lequel une CA ne peut pas stocker un certificat pour un domaine sans le consentement du propriétaire. Pour la réalisation du système CTB, les auteurs ont choisi d'utiliser la blockchain Hyperledger Fabric d'IBM avec le contrat intelligent CTB. Les auteurs prévoient également de mettre en œuvre un mécanisme de

révocation des certificats. Cependant, les tâches assignées aux entités CA rendent l'infrastructure blockchain centralisée alors qu'elle est censée être gérée de manière décentralisée.

Dans [52] les auteurs propose l'utilisation de la blockchain pour mettre en œuvre un schéma d'authentification pour la sécurisation des communications entre EV, CS(bornes de recharge) et UC(autorité centrale). Le schéma proposé est divisé en trois étapes : le processus d'enregistrement des entités, le processus de recherche et de génération de clé, et le processus d'authentification mutuelle. Les transactions de la blockchain utilisent le Merkle root hash. Comparé aux propositions existantes, le schéma proposé réduit le coût de communication et le temps de calcul, mais concernant la sécurité aucune justification n'a été apportée.

Dans le but de mettre en œuvre un système décentralisé, respectant la vie privée. Les auteurs dans [53] utilisent une blockchain, une authentification mutuelle et proposent un smart contrat. Le système utilise également un mécanisme d'enchères contraires, où un algorithme de tarification dynamique est mis en œuvre, permettant de charger/décharger les véhicules électriques tels que : les EVs voulant se décharger (autorisés à décharger) proposent des prix, et les stations de charge doivent ajuster les prix proposés de manière dynamique pour avoir un prix final pour l'enchère. En ce qui concerne le temps de traitement, une réduction a été observée, il reste à tester la sécurité du système.

Dans [54], Les auteurs proposent un système de récompense anonyme basée sur la blockchain (BBARS), en utilisant la signature agrégée (un schéma permettant d'agréger de multiples signatures de plusieurs messages émis par différents utilisateurs en une unique signature) basée sur les PKC (Public Key Cryptography: un système cryptographique a une paire de clés: privé et publique) dans l'infrastructure à clé publique (PKI). Un deuxième PKC différent est utilisé pour les opérations effectuées sur la blockchain. La proposition vise à résoudre simultanément l'anonymat du BV (véhicule alimenté par batterie), l'anonymat de l'agrégateur central (CAG), la non-traçabilité et la dissociation entre l'adresse du payeur et celle du bénéficiaire. L'analyse des résultats obtenus montre que les performances du système BBARS en termes de coût de communication sont plus efficaces. Cependant pour l'analyse de la sécurité, les auteurs ont proposé seulement une preuve mathématique sur la base de théorèmes et non sur une base de simulation pour avoir des résultats concrets.

Par souci de manque de confiance, transparence et possibilité de surcharger la facture du client, les auteurs dans [55] proposent l'utilisation de la blockchain pour rendre le système plus robuste en termes de confiance et de confidentialité et pour créer des portefeuilles électroniques et utiliser les contrats intelligents pour un meilleur contrôle. Ils ont aussi développé un système de paiement automatique sous la plate-forme open source Hyperledger fabric. Les auteurs ont établi l'analyse des performances de la solution proposée sur la latence de transaction moyenne, le débit de transaction moyen qui n'a pas été comparé à d'autres solutions existantes. De plus, aucun test n'a été fait pour évaluer la sécurité de la solution proposée.

Dans le but de résoudre les problèmes d'évolutivité et de coût élevé, les auteurs en [56] proposent une solution qui est l'utilisation des SCM (Secure Certificate Management) basées sur les journaux. Ils vont utiliser les certificats de l'autorité de certification dans une blockchain au lieu d'utiliser les PKI. Le SCM sert aussi à révoquer les certificats des autorités malveillants. Une analyse comparative des performances du SCM par rapport aux autres schémas utilisant les PKI basés sur la blockchain et les journaux démontre que les certificats SCM combinés à une blockchain ont réduit considérablement le coût de stockage. Pour l'analyse de la sécurité, les auteurs se sont basés sur des théorèmes et preuves mathématiques et non sur une base de résultats concrets obtenus par le biais de simulations.

Les auteurs dans [57] proposent un système léger d'authentification et de validation de certificat de domaine basé sur la blockchain construite à partir d'Ethereum Smart contrats, qui procure une authentification robuste en utilisant le moins de capacité de stockage et le moins de bande passante. Le système proposé enregistre toute autorité de certification de confiance associée à son domaine dans la blockchain, de sorte que chaque certificat délivré par une CA d'un domaine est un certificat valide. Les résultats du schéma proposé ont été comparés à d'autres méthodes d'authentification, et pour le côté évaluation et performances en termes de frais généraux de communication (lier à la longueur des messages transmis, plus le nombre de bits augmente plus les frais généraux augmentent [58]) et de coût de calcul, les résultats montrent que la solution est meilleure par rapport à d'autres solutions proposées dans la littérature. Cependant, pour l'analyse de la sécurité, les auteurs affirment que leur approche peut résister à plusieurs attaques, mais qu'il est nécessaire d'avoir des résultats concrets et comparatifs.

Pour régler le problème de la diffusion sécurisée et la rapidité des messages d'évènement dans les réseaux VANET. Les auteurs dans [59] n'utilisent pas les blockchains déjà existantes tels que la blockchain pour Bitcoin, mais proposent une nouvelle version de la blockchain publique qui stocke le nœud de confiance. Le schéma proposé utilise la preuve de travail (PoW) comme algorithme de consensus blockchain et un Certificat de localisation (LC) basé sur la preuve de localisation (Pol). Comme perspective, les auteurs proposent de combiner entre l'algorithme PoW et de l'algorithme PoS pour un consensus hybride qui peut être plus rapide et plus évolutif. La solution peut réduire la surcharge du stockage, mais il reste à résoudre le problème d'évolutivité.

Dans cet article [60], les auteurs visent à corriger les problèmes exposés dans les Vanet en utilisant la blockchain tels que le problème de la centralisation et l'absence de confiance mutuelle entre entités communicantes. La solution proposée intègre le hachage SBM (Safety Beacon Messages), ce qui va contribuer à la réduction du temps de traitement et de stockage dans la blockchain. Les auteurs proposent pour sécuriser l'identité du véhicule de diviser l'identité en plusieurs sous-identités, et ces dernières vont être mises à jour périodiquement. Pour sécuriser l'emplacement du véhicule, ils proposent de la protéger par le biais d'une unité d'anonymat "k" (propriété visant à garantir l'anonymat) et un graphe non orienté. Les résultats montrent que la solution proposée réduit le temps système et améliore le niveau de sécurité en ce qui concerne la confidentialité de l'identité et de l'emplacement, mais la disponibilité et la non-répudiation n'ont pas été discutées.

Il existe de multiples mécanismes de consensus blockchain. Dans [61], les auteurs introduisent une technique appelée Preuve de conduite (PoD) qui fonctionne d'une façon à sélectionner aléatoirement des mineurs honnêtes dans une application de covoiturage VANET basée sur la blockchain publique et dans laquelle les véhicules à conduite active gagnent certaines pièces de conduite dans leur portefeuille de compte enregistré en fonction de la distance parcourue. Le PoD proposé est conçu pour consommer moins de ressources. Les auteurs introduisent aussi une technique de filtrage basée sur le score de norme de service (Sc) des nœuds mineurs des véhicules pour détecter et éliminer les nœuds malveillants. Les auteurs affirment que les résultats montrent que le schéma proposé donne de bons résultats en termes de filtrages et qu'il est sécurisé contre certaines attaques d'infiltrations. Il reste à tester sa résistance contre d'autres types d'attaques que l'infiltration telle que des attaques visant l'intégrité ou la disponibilité.

Pour réduire les coûts de calcul pour la génération et la vérification d'une signature au sein d'un réseau VANET, les auteurs dans [62] proposent un schéma de signature de clé publique sans certificat (CL-PKS) utilisant un appariement bilinéaire pour fournir une authentification conditionnelle. Le schéma CL-PKS prend en charge les fonctions de vérification de signature par lots et de vérification de signature agrégée. Les auteurs utilisent aussi la blockchain pour mettre en œuvre la transparence de la révocation des pseudo-identités avant de vérifier les signatures. Les résultats montrent que la solution proposée prend moins de temps en termes de signature et de vérification de signature en comparaison à d'autres propositions citées dans l'article. Mais en ce qui concerne la sécurité, il est nécessaire qu'il y ait des résultats issus de tests pour appuyer les conclusions des auteurs.

Les auteurs dans [63] proposent un schéma d'authentification d'accès basé sur la blockchain utilisant des pseudonymes pour l'anonymat entre les véhicules et les unités en bordure de route, un schéma de stockage cloud distribué combiné avec la blockchain pour stocker les transactions. Le schéma proposé est divisé en 5 étapes : initialisation du système, immatriculation du véhicule, authentification du véhicule, annonce du véhicule, et la transmission de messages. La cryptographie à courbe elliptique est utilisée pour la transmission de message. Certes les résultats montrent que le schéma proposé nécessite moins de coûts de communication par rapport à d'autres propositions d'articles, mais au niveau de la sécurité du schéma, il n'y a pas de résultat qui confirme que le protocole d'authentification est efficace.

Dans [64], les auteurs proposent un schéma de routage de confiance basé sur la blockchain et la logique floue, la blockchain pour résoudre les problèmes de sécurité du protocole OLSR (Optimized Link State outing) qui est basé sur la disponibilité d'un groupe de nœud avec des mécanismes de sécurité à exécuter d'une façon répétitive. La solution proposée par les auteurs vise à faire collaborer les véhicules en évitant toute détection répétitive pour réduire le temps de détection et la surcharge du réseau. Les auteurs optent pour l'utilisation de l'algorithme de consensus Proof-of-Trust (PoT) qui convient au mieux pour les environnements Vanet. Bien que la solution proposée montre de bons résultats en termes de temps et de taux de détection d'attaquants, la participation des véhicules pour ajouter de nouveaux blocs dans leurs blockchains locaux

correspondants fait que des entités limitées en ressource vont consommer plus d'énergie pour effectuer cette opération.

Les auteurs dans [65] proposent d'utiliser une blockchain publique dans les réseaux VANET pour assurer la fiabilité des nœuds et des messages et aussi d'utiliser les messages d'évènement sous forme de transaction blockchain. Un certificat de localisation permet de connaitre la localisation des véhicules ce qui assure le partage d'informations d'événements (tel un accident) entre véhicules voisins. Dans le schéma proposé, le véhicule est amené à effectuer plusieurs tâches telle que la vérification des messages d'événement, l'emplacement et l'ID de l'événement, l'horodatage et biens d'autres tâches, ce qui demande beaucoup d'énergie et de puissance de calcul et qui ne correspond pas aux ressources des nœuds participants dans les réseaux VANET.

Pour conclure ce chapitre, nous pouvons dire que les protocoles et les solutions proposées dans la littérature dans le but de répondre aux exigences du réseau V2G en termes de sécurité et de performance présentent encore des lacunes, parmi lesquelles nous pouvons citer :

- La nécessité d'une entité intermédiaire.
- Le manque de résultats concrets pour soutenir les solutions proposées en termes de performance et de sécurité.
- La négligence de certains piliers de la sécurité informatique tels que : la disponibilité, l'intégrité et la non-répudiation des données.
- Le manque de considération pour les ressources limitées de stockage et d'énergie des entités participantes dans le réseau V2G.

Afin de corriger ces lacunes et de sécuriser les communications au sein du réseau V2G, nous proposons notre approche, qui répond aux exigences de la norme ISO 15118 et qui intègre un schéma d'authentification léger et la technologie blockchain. Cette dernière fournira un moyen de stockage des données, tout en sécurisant les informations et en assurant un contrôle d'accès aux données et en conservant l'historique des événements. Il faut également noter que notre approche ne repose pas sur l'utilisation d'une seule blockchain, mais sur quatre blockchains, dont deux sont publiques et deux sont privées. Pour la sécurité de notre système, nous avons également intégré des solutions pour la détection et l'interruption de l'attaque DOS (Denial of Service), l'attaque d'usurpation d'identité ainsi pour la protection contre l'attaque de l'homme au milieu (MITM).

Chapitre 5 Article Scientifique

HIERARCHICAL BLOCKCHAIN SYSTEM AND LIGHTWEIGHT AUTHENTICATION FOR A SECURE V2G NETWORK.

Les auteurs : Ines Yahia et le Professeur Boucif Amar Bensaber.

Soumis au journal *IEEE Transactions on Vehicular Technology.*

Numéro papier : VT-2022-02866.

Soumis le 22-Juillet-2022

Hierarchical Blockchain System and Lightweight Authentication for a Secure V2G Network.

Ines Yahia, *Student Member, IEEE* and Boucif Amar Bensaber, *IEEE*

Abstract **Electric vehicles represent the future of urban transportation. Vehicle-to-Grid (V2G) technology is a renewable energy exchange system between electric vehicles and the grid, enabling bi-directional charging. It is therefore essential to ensure the efficiency and security of the exchanges established between vehicles and V2G networks. Many researchers have proposed solutions, but limitations remain, such as the need for a trusted intermediary entity, a cumbersome authentication scheme, and the neglect of limited entity resources. To address these limitations, we propose a system based on the requirements of ISO 15118, integrating a lightweight authentication scheme with blockchain technology. Modeling and simulation were performed using Tamarin Prover and RiseV2G tools, respectively. The proposed solution meets security criteria, guaranteeing confidentiality, data integrity, anonymity and non-repudiation. The tests show that the system copes with multiple attacks and alleviates the burden of electric vehicles with limited resources, which leads to less computing time and energy consumption. In the future, we will test our system with IBM's hyperledger fabric blockchain technology.**

***Index Terms*— Attacks, Blockchain, ISO 15118, lightweight authentication, V2G**

I. INTRODUCTION

Green economy is quite desirable these days, with many countries investing in green technologies and renewable energy to promote it. Among these countries is Canada, which is implementing a policy that requires all vehicles and light trucks to be sold as zero-emission vehicles by 2035 [1].

Compared to conventional vehicles, electric vehicles do not emit any environmental pollutants. They can be charged at home, work, and at charging stations available on the planned route to the destination. The charging time of an electric vehicle can vary from 12 min to 8 h depending on the intensity of the electricity supplied by the charging station [2]. Electric vehicles are not only environmentally friendly but also help avoid traffic congestion and accidents by sharing important information via intelligent transportation networks [3].

While electric vehicles make our daily lives more convenient, they need to be part of the vehicle-to-grid (V2G) network to be able to interact with the charging stations and perform charging and discharging operations. However, V2G networks have several limitations and are prone to many attacks. Further, these vehicles have limited resources in terms of storage and computing power. Therefore, it is necessary to lighten their burden and assign more tasks to entities with greater computing and storage power.

Communication within the V2G network involves the exchange of sensitive information. The preservation of the security and privacy of the vehicle is necessary, and this preserves information such as the location of the vehicle, charging schedule, battery rate, operations, and activities performed by the vehicle [4].

Among the technologies used to ensure the security of communication systems is blockchain, which is a secure means of storing data in the form of blocks of processed transactions. This structure is managed by algorithms called consensus, whose role is to enforce the agreements predefined by the founder of the blockchain, allowing the addition and validation of new blocks of transactions in the blockchain. Blockchain technology is based on the use of encryption, hashing algorithms, and smart contracts for the security of communicating entities and data stored in the blockchain blocks. Therefore, this technology ensures transparency, data integrity, and confidentiality.

The non-blockchain-based solutions proposed in the literature have some unresolved drawbacks; for instance, the exchanges performed at the V2G network level are cumbersome, considering the limited resources of electric vehicles in terms of storage and computational power. Moreover, when communicating with a charging station, the vehicle may transmit sensitive information to authenticate itself, which poses a risk of possible attacks, such as identity theft or man-in-the-middle attacks. Furthermore, data integrity and non-repudiation are two pillars of IT security that are often neglected by non-blockchain-based solutions, and therefore, they present a major challenge for V2G networks.

To address the aforementioned challenges and improve the security and performance of V2G networks, we propose an efficient, secure, fast, and low-energy consuming approach. The proposed solution is based on ISO 15118 public key infrastructure (PKI) and blockchain technology, integrating an authentication and upload/output scheme. The use of blockchain not only eliminates the necessity of a trusted entity between the communicating nodes but also allows to have a

The authors work at the Department of Mathematics and Computer Science, University of Quebec at Trois-Rivieres, G8Z 4M3 Trois-Rivieres, Quebec (e-mail: ines.yahia@UQTR.ca; Boucif.Amar.Bensaber@uqtr.ca).

secure database to store and verify all information circulating in the V2G network. The proposed solution also aims to meet security requirements, such as availability, non-repudiation, and integrity.

The remainder of the paper is organized as follows. Section II provides a literature review on V2G networks, VANet networks, and blockchains. Section III describes the proposed solution, including the proposed security solutions that can deal with the most recurrent threats to V2G networks. Section IV discusses the modeling of the proposed scheme using the Tamarin Prover tool. Section V presents the simulation and analysis of the results obtained using the RISE V2G simulation tool. Finally, Section VI concludes the paper.

II. State of art

In this section, we present the existing literature that aimed to secure V2G networks, vehicular ad hoc networks (VANets), and blockchains.

In [5], the authors presented a study on the charging protocol proposed in ISO 15118, proposed recommendations to correct the existing security vulnerabilities in ISO 15118, aimed at ensuring the security of the charging process. The authors considered the tolerated use of transport layer security (TLS), the missing requirement for the provisioning device to verify the validity of the EV certificate using the online certificate status protocol (OCSP), and the lack of secure clock synchronization of the provisioning device as a security risk for the V2G network. To overcome these limitations, the authors recommended using TLS at all times, even in trusted environments, to prevent tampering and manipulation. They also recommended restricting the revocation time of spoofed certificates, verifying the validity of EV certificates using OCSP, and then checking the validity of TLS certificates using timestamps. In addition, the authors indicated that certificates signed by secondary certificate authorities can be assigned to multiple roles that pose security threats. This led the authors to propose techniques that allow binding of subordinate certificate authorities (sub-CAs) to a certain role. This study reviewed the security concepts proposed by the ISO 15118 standards and examined the possible attacks; however, no experimentation was conducted to validate these advanced recommendations.

To ensure the security of the payment process, the authors of [6] proposed a conditional authentication protocol. It comprised six steps: system initialization, VE registration, mutual authentication, message reporting, tracking, and revocation. The fulfillment requires a trusted authority (TA) that generates the global security parameters of the system and keys of all entities, and a LAG for the collection of real-time status information of the EVs that join the smart grid. This protocol preserves anonymity, privacy, unlikability, and non-repudiation. However, the effectiveness of the proposed protocols has not been proven by formal modeling or simulation, which creates serious doubts regarding the functioning of the protocol in the V2G environment and its efficiency against real attacks.

To verify the authenticity of the identities, and confidentiality of the messages and identities, Shuai Wang et al (2018). [7] proposed a V2G communication scheme based on three technologies: trusted computing, signcryption, and onion routing. To communicate outside the aggregator's coverage area, they used onion routing technology to build an anonymous communication link, or inside the aggregator's coverage area, where they used signcryption technology to complete the message signature and encryption. The authors claim that this solution provides some security; however, there are no concrete results to prove this, and it is also necessary to find an intermediate node to ensure that the process is completed.

The authors in [8] designed a mutual authentication scheme in V2G networks using an authenticated key agreement protocol established between the EV and the network, which generates a common secure session key that can be used for any further communication. To ensure confidentiality, the authors opted to use randomly chosen pseudonyms. The authors claim that the proposed scheme is more efficient and secure than other relevant schemes, such as those based on matching. The authors tested it for confidentiality and authentication, but not for integrity or non-repudiation.

Madala et al. [9] proposed a secure data-sharing scheme based on the membership level in V2G networks. As EVs with a higher membership level have more access to service information than those with lower membership levels, they also use the attribute-based encryption mechanism of an online/offline cipher text policy combined with fog computing technology. In this scheme, the text is encrypted by the control center (CC) and decrypted by the EVs that have a required membership level according to the access policy. The authors observed a reduction in the time required to encrypt/decrypt the data. According to the authors, the proposed scheme reduces the time required for data encryption/decryption and guarantees information confidentiality. However, their integrity and availability were not considered.

Certificate transparency is a technique created by Google that requires certificate authorities (CAs) using SSL/TLS to issue X.509 certificates that are visible to the domain owner. To build a publicly verifiable certificate database, the authors of the certificate transparency (CT) project [10] are creating a public log system where certificates issued by certification authorities can be easily verified by clients and entities called auditors and controllers, who can perform tasks for clients, such as editing or verifying the public log. The transparency certificate is intended to control any certificate issued by CAs. No CA should issue a certificate for a domain without it being publicly visible. The use of public logs is widely proposed for PKI structures, but log coordination is necessary for valid published certificates. The security of inter-entity communications is equivalent to securing the PKI infrastructure and overcoming the fragility of certification authorities. As a result, the authors in [11] sought to give domain owners absolute control over authorizing certificates for their domains, and therefore, they proposed the CTB system, where a CA cannot store a certificate for a domain

without the owner's consent. To realize the CTB system, the authors opted to use IBM's hyperledger fabric blockchain with the CTB smart contract. The authors also planned to implement a certificate revocation mechanism. However, the tasks assigned to the CA entities centralize the blockchain infrastructure, whereas they are supposed to be managed in a decentralized manner.

In [12], the authors proposed the use of blockchain to implement an authentication scheme for securing communication between the EV, CS, and UC. The proposed scheme is divided into three stages: entity registration, key search and generation, and mutual authentication. Blockchain transactions use the Merkle root hash. Compared with existing proposals, the proposed scheme reduces the communication cost and computation time, but no justification for security has been provided.

To implement a decentralized, privacy-friendly system, the authors in [13] used blockchain with mutual authentication, and proposed a smart contract. The system also uses a counter-auction mechanism, in which a dynamic pricing algorithm is implemented, allowing charging/discharging of electric vehicles such that EVs wanting to discharge (allowed to discharge) propose prices, and charging stations must adjust the proposed prices dynamically to obtain a final price for the auction. Regarding the processing time, a reduction has been observed, it remains to test the security of the system.

The authors of [14] proposed a blockchain-based anonymous reward system (BBARS) using the aggregated signature (a scheme to aggregate multiple signatures of several messages issued by different users into a single signature) based on PKCs (a cryptographic system that has a pair of keys: private and public) in the public key infrastructure (PKI). A different PKC was used for the operations performed on the blockchain. The proposal aimed to simultaneously solve the BV anonymity (battery-powered vehicle), central aggregator anonymity (CAG), non-traceability, and dissociation between the payer and payee addresses. An analysis of the results shows that the BBARS system's performance in terms of communication costs is more efficient. However, for the security analysis, the authors proposed a mathematical proof based on theorems only and no simulation was performed to obtain concrete results.

Owing to concerns regarding a lack of trust and transparency, and the possibility of overcharging the customer's bill, the authors in [15] proposed the use of blockchain to make the system more robust in terms of trust and privacy, create electronic wallets, and use smart contracts for better control. They also developed an automatic payment system using an open-source hyperledger fabric platform. The authors established a performance analysis of the proposed solution on the average transaction latency and average transaction throughput, which were not compared with other existing solutions. In addition, no tests were conducted to evaluate the security of the proposed solution.

To solve the problems of scalability and high cost, the authors in [16] proposed a solution that uses secure certificate management (SCM) based on logs; they use the certificates of the certification authority in a blockchain instead of using PKI. SCM is also used to revoke certificates from rogue authorities. A comparative analysis of the performance of SCM with that of other schemes using blockchain and log-based PKI shows that SCM certificates combined with blockchain have significantly reduced storage costs. For the security analysis, the authors relied on mathematical theorems and proofs and not on simulation results.

The authors of [17] proposed a lightweight blockchain-based domain certificate authentication and validation system built on Ethereum Smart contracts, which provides robust authentication using the least storage capacity and bandwidth. The proposed system registers any trusted certificate authority associated with its domain in a blockchain. Every certificate issued by the CA of a domain is valid. The results of the proposed scheme were compared with other authentication methods, and for the evaluation and performance side in terms of communication overhead and computational cost, the results showed that the solution is better than the other solutions. However, for security analysis, the authors stated that it can resist several attacks, but concrete and comparative results are still required to confirm the same.

In VANets, the storage and computing resources of the entities are limited. The use of blockchain in these networks has consequences. In addition, several problems occur in terms of efficiency, fairness, and scalability of protocols such as proof of work (PoW), proof of participation (PoS), and practical Byzantine fault tolerance (PBFT). The authors in [18] proposed a new proof of driving (PoD) technique that initiated random and fair selection among nodes to establish the mining process. In addition, they proposed another standard score (Sc) technique for optimizing the number of nodes needed for the mining process according to their performance, as well as detecting and removing malicious nodes. The results of the proposed scheme indicate better results in terms of storage capacity and computational cost compared with the other proposed systems. However, in terms of security, only infiltration attacks were discussed, whereas malicious nodes can also impact the system under other types of attacks.

The authors in [19] proposed to solve the problem of secure broadcast and speed of event messages in VANets in a country using a local blockchain. The authors did not use the existing blockchains, such as the blockchain for Bitcoin, but proposed a new version of the public blockchain that stores the trust node. The proposed scheme uses the PoW as the blockchain consensus and a location certificate (LC) based on the proof of location (PoL). From this perspective, the authors proposed a combination of the PoW and PoS algorithms for a hybrid consensus that can be faster and more scalable. This solution could reduce the storage overhead, but the scalability problem remains to be solved.

With the objective of securing, alleviating, and optimizing the communication between different electric vehicles, the authors in [20] proposed a hybrid blockchain integrating a local directed acyclic graph (DAG) to optimize the communication between electric vehicles. The authors also proposed an asynchronous federated learning scheme to reduce costs. It is true that the use of blockchain makes the system more robust, and the authors claim that the proposed system is secure; however, no attack has been simulated on this system to concretely prove its robustness.

Another study [21] aim to correct the problems exposed in a VANet using blockchain, such as the centralization problem and lack of mutual trust between the communicating entities. The proposed solution integrated Safety Beacon Messages (SBM) hashing, which contributed to a reduction the processing and storage time in the blockchain. The authors proposed to secure the identity of the vehicle by dividing the identity into several sub-identities, which could be updated periodically. Further, to secure the position of the vehicle, they proposed to protect it using the anonymity unit k and an undirected graph. The results show that the proposed solution reduces the system time and improves the security level with respect to identity and location privacy; however, availability and non-repudiation were not discussed.

To reduce the computational cost of generating and verifying a signature within a VANet, the authors of [22] proposed a certificateless public key signature scheme (CL-PKS) using bilinear matching to provide conditional authentication. The CL-PKS scheme supports batch and aggregate signature verification. The authors also used blockchain to implement transparency for revoking pseudo-identities before verifying signatures. The results show that the proposed solution is less time-consuming in terms of signature and signature verification compared with the other proposals cited in this paper. However, as far as security is concerned, there is a need for test results that support the authors' conclusions.

The authors in [23] proposed a blockchain-based access authentication scheme using pseudonyms for anonymity between vehicles and roadside units, and a distributed cloud storage scheme combined with blockchain to store transactions. The proposed scheme is divided into five steps: system initialization, vehicle registration, vehicle authentication, vehicle advertisement, and message transmission. Elliptic curve cryptography was used for message transmission. Although the results show that the proposed scheme requires less communication cost compared to other proposed methods, no results confirm the greater efficiency of the authentication protocol in terms of the security of the scheme.

The authors of [24] proposed a trust routing scheme based on blockchain and fuzzy logic. A blockchain was used to solve the security problems of the optimized link state outing (OLSR) protocol, which is based on the availability of a group of nodes with security mechanisms to be repeatedly executed. The solution proposed by the authors aimed to enable collaboration of the vehicles by avoiding repetitive detection to reduce the detection time and network overload. The authors opted to use the proof of trust (PoT) consensus algorithm, which is best suited to VANet environments. Although the proposed solution shows good results in terms of time and attacker detection rate, the participation of vehicles to add new blocks in their corresponding local blockchains causes resource-limited entities to consume more energy to perform this operation.

The authors in [25] proposed the use of a public blockchain in VANets to ensure the reliability of nodes and messages and to use event messages in the form of blockchain transactions. A location certificate allows us to know the location of the vehicles, which facilitates the sharing of event information (such as an accident) among neighboring vehicles. In the proposed scheme, the vehicle is required to perform several tasks, such as event message verification, location and event ID, time stamping, and many other tasks that require considerable energy and computational power, which is not consistent with the resources of the participating nodes in VANets.

The protocols and solutions proposed in the literature to satisfy the security and performance requirements of the V2G network still have limitations, such as the need for an intermediary entity, lack of concrete results to support the proposed solutions in terms of performance and security, and neglect of some pillars of IT security, such as availability, non-repudiation, and data integrity. Finally, the limited storage and energy resources of the participating entities in the V2G network were not considered.

To address these limitations and further secure communication within the V2G network, we propose a system, which is based on the requirements of the ISO 15118 standard, integrating a lightweight authentication scheme and blockchain technology. The latter provides a means of data storage while securing information, ensuring access control to data, and recording event history. It should also be noted that the proposed system does not rely on the use of a single blockchain, but on four blockchains, two of which are public and two are private. To ensure the security of the system, we also integrated solutions to protect it against various attacks.

III. Methodology

Considering the ISO 15118 standard and PKI infrastructure, we propose a model where we use four interrelated blockchains. As shown in the figure below, we have the OEM, MO, ROOT CA/RA, and transaction blockchains.

Each blockchain is specific to the certification level except for the transaction blockchain. The two highest blockchains, OEM (level 4) and MO (level 3), are private, whereas the other two are public. Each blockchain of level i offers an additional security for level i-1; a level i cannot publish a certificate without ensuring that the certificate has not been registered at its level (no duplicates) and that the certificate corresponding to level i+1 has already been published.

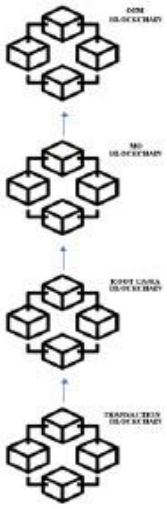


Fig. 1. Blockchain structure.

A. Blockchain Levels

Level 4 is the highest, comprising the OEM blockchain, which is responsible for the security of the OEM PROV certificates specific to the manufacture of each new vehicle. Only trusted OEM nodes can publish in this blockchain. Entities of the MO blockchain can access the OEM blockchain, but only for verification of the availability and authenticity of a certificate; they cannot modify or publish in it.

Level 3 is the MO blockchain, which is responsible for registering the certificates of contracts established with the mobility operator, ensuring that the new vehicle to be registered is already registered at the OEM blockchain level and not be registered more than once in the MO. Root CA/RA blockchain entities can access the MO blockchain for verification, but these entities cannot publish in the MO blockchain under any circumstances.

Level 2 is the ROOT CA/RA blockchain that ensures that the vehicle is registered at the MO level and that it is the owner of a genuine certificate by verifying the signature of the certificates (OEM, MO). It also ensures that the LAGs are registered and that they are non-malicious nodes. The ROOT CA/RA blockchain retains the signed index of the blocks containing the corresponding MO and OEM certificates to the vehicle and charging station. It can be called an intermediary between the private blockchains OEM, MO, and the public blockchain transaction.

The OEM, MO, and ROOT CA/RA blockchains are used to publish authentic certificates. Level 1, which represents the transaction blockchain, is managed by the LAGS, where all transactions are recorded and payments or rewards are made.

In the proposed model, we also consider a smart contract at the level of each blockchain, which is concerned with the management of the access authorizations to the blockchains and the data to be recorded, verification of the duplication, correspondence between the certificate of the node and the blacklist, verification of the blocks and certificates, and management of the payments/rewards.

In the proposed scheme the following types of entities are used:

- When a new vehicle is manufactured at the OEM level, the OEM entity SUB-CA2 assigns to the vehicle an OEM PROVISIONING CERTIFICATE. This certificate allows the vehicle to be uniquely identified. The OEM entity that assigns this certificate must sign and publish it on the OEM blockchain, if the block is authentic and the entity is part of the list of recognized OEMs; then the block is accepted. Otherwise, the block is rejected, the certificate is placed in a revocation list, and the responsible node is blacklisted.

- The MO SUB-CA2 entity is responsible for assigning a signed CONTRACT CERTIFICATE to the vehicle, which is published in the MO blockchain after verifying that the block is valid, that there are no duplicates by means of a unique index representing the block linked to the vehicle, and that the corresponding OEM PROVISIONING CERTIFICATE exists in the OEM blockchain.

- Registration of the new vehicle and charging stations are established in the ROOT CA/RA blockchain. The vehicle sends its index signed by the MO to the CA/RA entity, which is responsible for the creation and registration of the certificate contracts at the CA/RA blockchain level, and checks with the provided signed index. If the corresponding block at the MO blockchain level exists, is valid, corresponds to the vehicle, and the signature of the index corresponds to the signature of MO, the block is created and published at the CA/RA blockchain level.

- The transaction blockchain is held by the LAGs entities that participate in the registration of the new vehicle and authentication, allowing the charging stations to start the charging or discharging process and calculating the rewards to be awarded or the charging fees. The contact with the charging station leads directly to the contact with the LAG as it occurs when the vehicle sends its index to the charging station, the LAG receives the index, and checks with the CA/RA blockchain the availability of the certificate corresponding to the index; if it is valid, the process continues according to the choice of the operation.

After the registration of a new vehicle at the CA/RA level or a charge/discharge operation, a block is created at the transaction blockchain level and will only be published if it has been signed and approved by both the EV and LAG participating entities.

IV. Proposed scheme

The scheme is divided into two parts: the first is the registration of a new vehicle, which is the first contact with the charging station, and the second is the charging/discharging of the vehicle. Subsequently, we integrated the schemes explaining the authentication phase.

A. Registration of a New Vehicle

When a new vehicle is manufactured, the OEM entity SUB-CA2 issues an OEM PROVISIONING CERTIFICATE, which is registered at the OEM blockchain level through the smart contract that checks the signature on the certificate, the issuing node of the certificate, and the uniqueness of this certificate at the blockchain level. If all the information is valid, the smart contract adds a new block containing the certificate of the new vehicle with all the necessary information; otherwise, the block is rejected, the responsible OEM SUB-CA2 node is blacklisted, and the certificate is revoked.

At Level 3, the new vehicle already registered at the OEM blockchain level must register at the MO blockchain level. The MO entity SUB-CA2 provides a CONTRACT CERTIFICATE for the vehicle, which must go through the smart contract MO. The latter will first check if the signature of the MO is valid and the issuing entity is not blacklisted, at which point it transmits the index of the block to the smart contract OEM to verify that the certificate is already registered at the level of the blockchain OEM; if this is the case, the new block is created and published on the MO blockchain; otherwise, the block is refused, the certificate is revoked, and the issuing node is blacklisted.

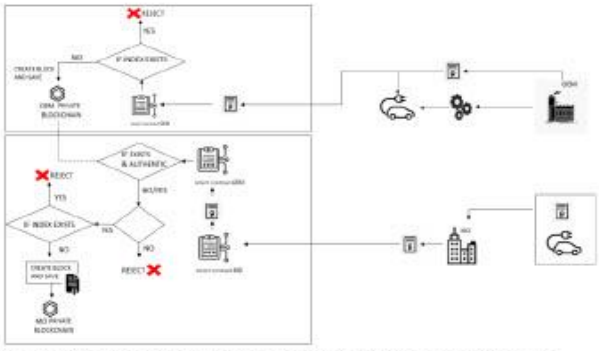


Fig. 2. Diagram showing the registration of a new EV on the OEM and MO blockchains.

The same process occurs for the two blockchains ROOT CA/RA and TRANSACTION with the exception that these two blockchains are public, and that in the ROOT CA/RA blockchain, each block contains the two indexes referencing the two certificates OEM, MO, signed by OEM, MO, and also contains a CONTRACT CERTIFICATE issued and signed by CA/RA. The ROOT CA/RA blockchain also holds the certificate corresponding to each charging station in the transaction blockchain, and the LAGs manage the blockchain instead of the charging stations, so that the back end of the blockchain is lightened. All transactions as well as the type of operation, charging fee or reward rate, charging station index, and vehicle index are recorded. The smart contract also stores the fees or rewards to be awarded until the end of the operation. Before the approval of the new blocks, a signature of the vehicle, LAG, and CA/RA are required.

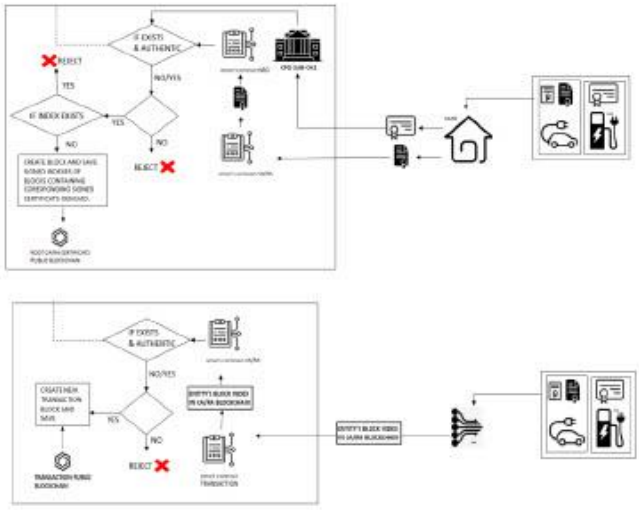


Fig. 3. Diagram showing the registration of a new EV on the CA/RA and Transaction blockchains.

B. Charging or Discharging the Vehicle

After the vehicle is registered, it is charged or discharged. In the proposed model, the first contact with the charging station differs from the upcoming contacts. For the first contact, the vehicle has a list of charging stations containing their corresponding addresses (or indexes) signed by the MO, and the vehicle must send the signed address or index to the corresponding charging station. After the charging station verifies the signature, the vehicle is considered as a new vehicle and the first authentication is started.

that the following diagram illustrates the various exchanges between the charging station and the vehicle described as follows.

- The vehicle establishes initial contact with the charging station by sending a charge/discharge request accompanied by the charging station index signed by MO.
- The charging station transmits its corresponding index in the ROOT CA/RA blockchain.
- The vehicle checks the availability of the index then in turn transmits its corresponding index in the ROOT CA/RA blockchain to the charging station.
- After its verification by the charging station, the vehicle sends the charging/discharging parameters under the request of the charging station.
- Finally, a block is created, signed and recorded at the level of the Transaction blockchain after its approval. The details of the operation are shown in the following figure.

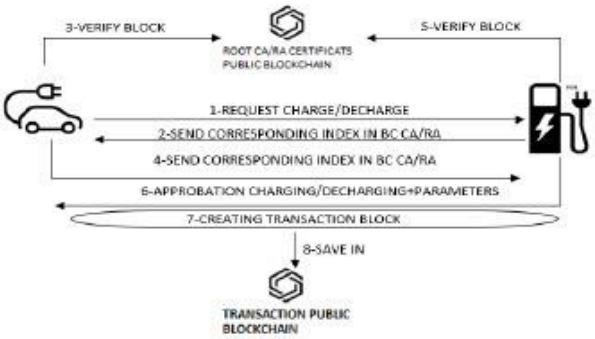


Fig. 4. Diagram showing the charging /discharging of the EV.

C. Authentication Process

In this section, we discuss the different exchanges between the EV, LAG, and CA/RA entities for the registration and charging/discharging of vehicles. The definitions of the corresponding symbols are listed in Table I.

TABLE I
KEYWORD DEFINITION

Keyword	Signification
SK, PK	Private key, Public key
E (), D ()	Encryption, Decryption
Sig	Signature
I, I'	Index received, Index verified
BC	Blockchain
RAuth	Authentication request
@	Address
H	Hach
sigC	Computed signature
signed	Signed message
OPP	Operation
RSO	Start operation request
CSO	Confirmation start operation
TRANSACC	Transaction completed
END OPP	Request end operation

1. New Vehicle Registration

The following diagram presents the exchanges among the EV, LAG, and CA/RA entities for vehicle registration in the ROOT CA/RA blockchain.

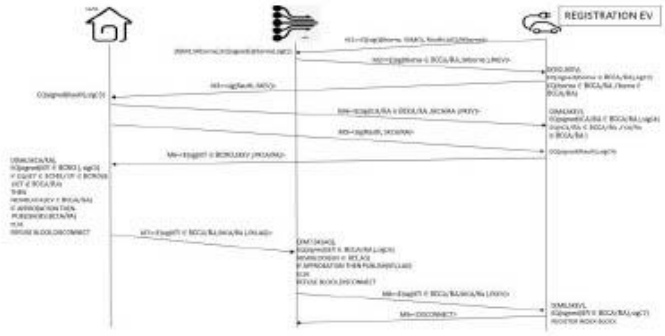


Fig. 5. Diagram presenting the registration process of the EV.

Considering that the LAG also represents the tasks performed by the charging station, the EV holds its key pair (public, private) and its index corresponding to its certificate at the MO blockchain level.

All the messages transmitted between the entities are signed and then encrypted; therefore, decryption and verification of the signature are necessary before any answer; the details of the algorithms used are provided in the simulation section.

- During the first contact with the charging station, the EV transmits the address of the charging station signed by the private key MO and an authentication request, all encrypted with the public key of the charging station.
- After decrypting the M1 message and verifying the signature, the charging station sends an M2 message containing its corresponding index in the ROOT CA/RA blockchain.
- EV then checks with the ROOT CA/RA blockchain that the charging station is still authentic; if yes, it ensures the authenticity of the CA/RA by sending an authentication request M3.
- the CA/RA in response transmits M4 containing its index and M5 containing the authentication request to the EV. If the information is valid, the EV responds by transmitting its index to the MO blockchain through the M6.
- The CA/RA node checks the availability of the EV index at the blockchain level and that there are no duplicates at the CA/RA blockchain level; then, a new block containing the index and the necessary

information is created. If the block has been approved, the corresponding index is sent to the LAG through M7 to record it at the transaction blockchain level and is also sent to the EV through M8. If the block has not been approved, the EV is automatically disconnected from the charging station.

2. Charging and Discharging the Vehicle

For a charging/discharging operation, the authentication and transaction registration processes are described as follows.

The EV communicates an authentication request to the charging station, which in turn sends its corresponding index in the CA/RA blockchain, along with an authentication request to the EV. After verifying the charging-station index, the EV transmits its index. If the authentication is validated, the charging station sends a request for the choice of operation and the estimated time required for the process. The latter responds with the choice of the established parameters. The charging station transmits the information received by the LAG to calculate the fees to be paid or the rewards, which depends on the level of the network load. The charging station transmits this information to the EV, and if it is a payment, the fees paid by the EV are stored by the smart contract until the end of charging; if it is discharging, the rewards are attributed after the end of discharging by the smart contract.

The process continues with the creation of a new block containing all the necessary information related to the transaction. The signature of the LAG, EV, and CA/RA is required before the publication of this block in the transaction blockchain, and the EV adds the number of established transactions in its temporary transaction list. The upload begins after the block is signed. At the end of the operation, the transaction block is approved, the charge station sends a disconnect request, and the EV is disconnected.

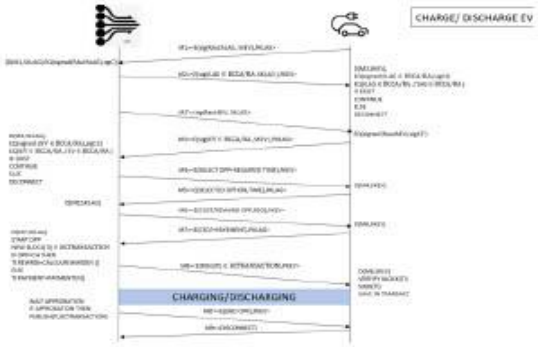


Fig. 6. Diagram showing the EV charging/discharging process.

D. Security Measure against Attacks

The most recurring attacks on V2G networks are denial of service (DOS), impersonation, and man in the middle (MITM) attacks.

1. DOS Attack

The aim of the DOS attack is to disrupt the proper functioning of the V2G network by clogging it with successive packets sent at a defined time. Several types of DOS attacks exist; however, our choice is based on the types of DOS user datagram protocol (UDP) flooding attacks (toward EVCC and SECC) and DOS internet control message protocol (ICMP) attacks (Echo EVCC reply to SECC, Echo SECC reply EVCC). Thus, this work is mainly based on the detection and blocking of the most harmful attacks in terms of the energy consumption and computation time.

- DOS UDP attack or UDP Flooding:

Attacker to EVCC: Flood the EVCC with UDP packets sent by a malicious entity.

Attacker to SECC: Flood SECC with UDP packets sent by a malicious entity.

- DOS ICMP: Echo EVCC reply to SECC:

To flood the SECC, the attacker sends several ICMP packets to the vehicle, which in turn respond to the charging station.

- DOS ICMP: Echo SECC reply EVCC:

The attacker sends several ICMP packets to the charging station, which in turn, sends the responses back to the EVCC.

Before protecting the system from DOS attacks, it is necessary to detect them. For this purpose, we detect unusual network traffic by counting the packets originating from the same source. In the proposed solution, if the number of unusual UDP or ICMP packets is equal to or greater than 100, we disconnect the communication with the sender. The pseudocode below explains the solution.

Algorithm 1: the DOS solution

```
Variables
UDPmessage : udp packet
ListOfBlockedSenderIP: ArrayList
T: integer // the number of incoming messages threshold
    1. While True Do
    2.  UDPmessage = recieveIncommingMessages ()
    3.    If UDPmessage.getSenderIP() not in ListOfBlockedSenderIP then
    4.       If numberOfMessagesFrom (UDPmessage.getSenderIP()) > T then
    5.           ListOfBlockedSenderIP.add (UDPmessage.getSenderIP())
    6.       End If
    7.    Else
    8.       Reject (UDPmessage)
    9.    End If
    10. EndWhile
```

2. Spoofing

Appropriating the identity of a legitimate node to gain access to important information in V2G networks opens a loophole for the attacker to tamper with the system and use this information illegally.

In the proposed scheme, each block in the CA/RA blockchain is represented by an index. For each communication between the EV and the charging station, authentication must be performed on both sides, using the index corresponding to the entity against its block in the CA/RA blockchain. Each block in the CA/RA blockchain includes the information required to authenticate the vehicle, such as the signed certificate and public key.

To avoid, detect, and block any impersonation attacks on the system, we propose a solution, which is illustrated in the diagram below. The EVCC transmits to the SECC the index and signed index corresponding to its block in the CA/RA blockchain, which in turn verifies the authenticity of the identity of the EV by recovering the public key of the EV stored at the level of the indicated block. Then, SECC uses the latter to check if INDEXEV and SIGNED_INDEXEV match. If this is the case, the authentication phase is established and the communication continues; however, if INDEXEV and SIGNED_INDEXEV do not match, the EV is automatically disconnected.

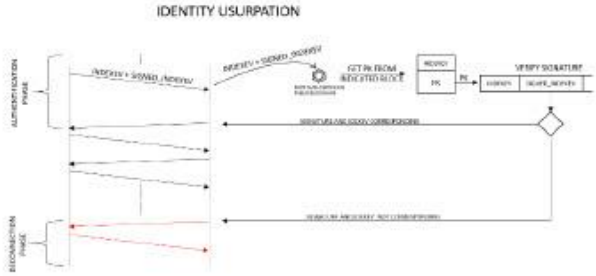


Fig. 7. Diagram of the proposed solution against spoofing

The following algorithms describe the proposed solution.

Algorithm 2: the solution against Spoofing representing EV side

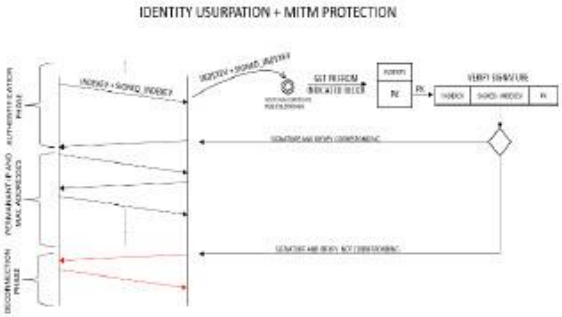
```
//// SENDER PART: LIGITIM EV
Variables
INDEXEV: Index
SIGNATURE: Signature
PK: Public Key
MESSAGE: IPV6 Packet
    1.  PRK = READ_PRIVATE_KEY ()
    2.  SIGNATURE = SIGN (INDEXEV, PRK)
    3.  MESSAGE.setIndexEv(INDEXEV)
    4.  MESSAGE.setSignature(SIGNATURE)
    5.  SEND_TO_SECC(MESSAGE)
```

Algorithm 3: The solution against Spoofing representing SECC side

```
//// Receiver PART: SECC
    1. While True Do
    2.      MESSAGE = Receive_From_EVCC ()
    3.      INDEXEV = MESSAGE.getIndexEv()// get the EV Index
    4.      SIGNATURE = MESSAGE.getSignature()// get the signature
    5.      PK = Retrieve_PK_From_Block (INDEXEV)
    6.      If Check_SIGNATURE (INDEXEV, SIGNATURE, PK) == FALSE Then
    7.         STOP_COMMUNUCATION ()
    8.      Else
    9.         sendMessage (NewMessage)
    10.     End If
    11. End While
```

3. Man-in-the-Middle (MITM) Attack

As the name of the attack indicates, an illegitimate node enters a communication between two legitimate nodes and



becomes an intermediary node in the communication. The MITM attack allows impersonation of the speaker and the interlocutor using Neighbor Discovery Protocol (NDP) poisoning, DNS poisoning, DOS, and many other attacks. In this work, we deal with an MITM attack using NDP poisoning.

The neighbor discovery protocol (NDP) based on ICMPV6 is used in IPV6 networks for neighbor discovery, similar to the ARP table in IPV4 networks; the NDP table allows us to access the IPV6 addresses of neighbors with their corresponding MAC addresses.

Fig. 8. Diagram of the proposed solution against the MITM attack

The MITM attack using the NDP poisoning table causes contamination of the NDP table at the level of the communicating legitimate entities, which includes the addresses of the legitimate entities, and that of the attacker has the same MAC address (MAC address of the attacker).

We can protect our communication against the MITM attack using NDP poisoning by retaining the IPV6 addresses used for the authentication phase as permanent addresses until the end of the communication. Thus, we can avoid the contamination of the NDP table because once made permanent, the system rejects any resulting modification of the NDP solicitation messages sent by the attacker, thereby indicating to the machines the new MAC address to which the IPV6 addresses are linked. The proposed solution is illustrated in the following diagram.

The pseudocode against MIMT attack is as follows:

Algorithm 4: the solution against MITM representing EV side

```
//// Receiver PART: LIGITIM EV
      Variables
      MESSAGE: IPV6 Packet
         1.  MESSAGE = Receive_From_SECC ()
         2.  setPermanant (MESSAGE.getSenderIP,MESSAGE.getSenderMAC)
         3.  SendMessage (NewMessage)
```

Algorithm 5: the solution against MITM representing SECC side

```
//// Sender PART: SECC
      1.  While True Do
      2.     MESSAGE = Receive_From_EVCC ()
      3.     INDEXEV = MESSAGE.getIndexEv()// get the EV Index
      4.     SIGNATURE = MESSAGE.getSignature()// get the signature
      5.     PK = Retrieve_PK_From_Block (INDEXEV)
      6.     If Check_SIGNATURE (INDEXEV, SIGNATURE, PK) == FALSE Then
      7.        STOP_COMMUNOCATION ()
      8.     Else
      9.        setPermanant (MESSAGE.getSenderIP, MESSAGE.getSenderMAC)
      10.       sendMessage (NewMessage)
      11.    End If
      12. End While
```

V. Protocol Analysis

In this section, we present and analyze the results obtained from the modeling and simulation, as well as the tools used to validate and test the proposed scheme by using Tamarin Prover and Rise V2G. Subsequently, we analyze the performance of the proposed solution regarding the computational energy.

A. Modeling

To model of the proposed scheme, we used the Tamarin Prover tool, which allows the symbolic modeling and analysis of security protocols [26].

This tool allows us to model and formally verify the different exchanges established between the entities. We could also verify the security of the scheme by using the adversary Dolev-Yao, proposed by Tamarin Prover, which can control the network, delete, inject, modify, and intercept messages.

In our modeling, the blockchain is represented by block indexes, the charging station is represented by the LAG agent, and we also have the MO, CA/RA, and EV agents. The following figures illustrate some parts of the code.

```
//1- Generate_key_pair

[ Fr(~ltk) ] // generate a new private key EV
  -->
   [ !Ltk($A, ~ltk), !Pk($A, pk(~ltk)),Out(pk(~ltk)) ]


rule Reveal_ltk:[ !Ltk($A, ltk) ] --[ Reveal($A) ]-> [ Out(ltk) ]
```

Fig. 9. Identity and public/private key generation phase.

As shown in the above figure, we generate our private key ~ltk with Fr(~ltk), associate it with Agent A, and then generate its public key with ! Pk ($EV, pk(~ltk)). Using the Out (pk(~ltk)) primitive, we allow the propagation of the public key in the network. The Reveal_ltk rule indicates that the long-term key of agent 'A' has been compromised. The first phase allows the generation of the keys of the entities participating in the exchanges.

```
// Role MO sends first message TO EV (1)-
rule MO_1_send:
let m = <$MO, ~na>
in
[ Fr(~na)//na for addresse
, !Ltk($MO, ltkMO)
, !Pk($EV, pkEV)
]
--[ Send($MO, m), Secret_MO(m)
]->
[ St_MO_1($MO, ltkMO, pkEV, $EV, ~na)
, Out_S($MO,$EV,<m,sign(m,ltkMO)>)
]

// Role EV receives first message
rule EV_1_receive:
[ !Ltk($EV, ltkEV)
, !Pk($MO, pkMO)
, In_S($MO,$EV,<m,sig>)
]
--[ Recv($EV, m)
, Eq(verify(sig,m,pkMO),true)
,Secret_EV(m), Authentic($EV,m), Honest($EV), Honest($MO)
]->
[ St_EV_1($EV, ltkEV, pkMO, $MO, m)
]
```

Fig. 10. Phase of sending the LAG address signed by the MO to the EV.

Figure (10) models the first message sent by the entity MO to EV containing the address of the LAG signed by MO. The address is represented by the randomly generated value ~na, and the message is sent in a secure channel. Rule EV_1_receive allows the receipt of the message and verification of the signature of MO; if the signature is authentic, we would then consider that MO and EV are honest agents.

The following figures illustrate the result of the execution of the command Tamarin Prover interactive MODELISATION.spthy. The lemma is colored in green, which shows that the model is successfully approved.

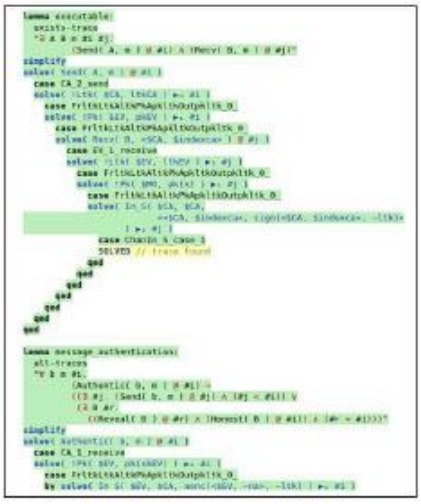


Fig. 11. Results of the execution of a part of the model.

The lemmas are intended to test message confidentiality using the secrecy lemma, agent authenticity using the authentication lemma, signature verification using the restriction equality lemma, and secure channel lemmas for channels that provide secure authentication, integrity, and transmission.

B. *Protocol Simulation*

To simulate the proposed system, we used the simulation tool RiseV2G [27], which is an open-source simulator implementing the ISO 15118 standard and implemented a code representing a simulation of our blockchains and the respective smart contracts. For security of the exchanges established between different entities, we used the cryptographic suite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256.

For the security tests, we implemented a simulation of spoofing and DOS attacks, and used the Ettercap tool [28] for the simulation of the MITM attack.

1. *DOS Attack*

In the simulation section, we conducted a study on the four states of the proposed system. The following states indicate the system characteristics as follows.

- SPSA state: system without DOS attacks and without protection against them.
- SPAA state: system with DOS attacks and without protection against them.
- APSA state: system without DOS attacks, in which protection against these attacks is implemented.
- APAA state: system undergoes DOS attacks and includes protection.

Table II summarizes the system states.

TABLE II
SYSTEM STATES

System status	DOS attacks	Protection against attack
SPSA		
SPAA	✓	
APSA		✓
APAA	✓	✓

For each state, we performed five different simulations. A charging station and 20 vehicles were used in this study. The UDP-ICMP messages were sent by a code executed by the malicious node, allowing continuous transmission. The goal of these simulations was to determine the estimated time and behavior of the system according to its state.

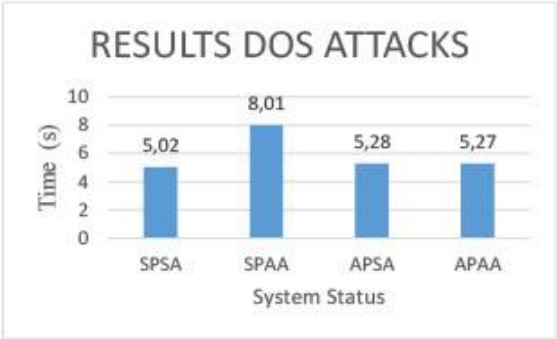


Fig. 12. Graph representing the results of the simulation of the DOS attacks.

The above graph indicates the average time (in ms) elapsed for the five simulations corresponding to each state of the system for the communication of the 20 vehicles with the charging station.

By comparing the system in the first two states, SPSA and SPAA, we can observe that the execution time in the presence of an attack is much higher than that without an attack, from which we can conclude that the system has been impacted by these attacks.

By comparing our system in the two states, SPAA and APAA, we can also observe that the security solution has improved the efficiency of the system in terms of computation time.

We then compared the results of the simulations of the APSA and APAA states; the average of the five simulations of APSA takes 5.28 s and the average of the five simulations of APAA returns to 5.27 s; the results remain very close. This means that the different types of DOS attacks do not affect our system in terms of the computation time.

The following figure shows that our system detected a DOS attack and then terminated this communication.

Fig. 13. Detection of DOS attack.

Considering the obtained results, we can conclude that our solution is effective, protects the system against DOS attacks, and does not alter the system with regard to execution time, in addition to the energy consumed by the calculations.

2. *Spoofing Attack*

Here, we present the results of the simulation of the spoofing attack. As explained previously, we generated an EV index signature with a private key (random key) not linked to the public key registered in the CA/RA blockchain. We can observe that our scheme could detect that the EV was not legitimate; therefore, the communication was terminated by the charging station.

Fig. 14. Detection of a non-legitimate vehicle.

We conclude that our system is resistant to the spoofing attack.

3. *Man-in-the-Middle Attack*

Before launching the MITM attack on the vehicle and charging station, we observe the IPV6 and MAC address of the SECC in the EV NDP table.

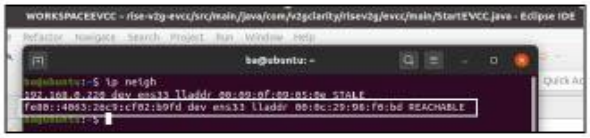


Fig. 15. EVCC NDP table before MITM attack.

In the SECC NDP table of the charging station, we can observe the IPV6 and MAC addresses of the EV.

Fig. 16. SECC NDP table before MITM attack.

After launching the MITM attack on both machines, we observed a change in both the NDP tables.

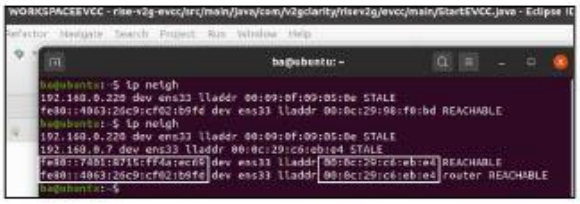


Fig. 17. EVCC NDP table after MITM attack.

We noticed a contamination of the NDP table of EVCC; the MAC address of the SECC is in correspondence with the MAC address of the attacker.

The same observation was repeated for SECC, and the attacker could impact the NDP table.

Fig. 18. SECC NDP table after MITM attack.

After applying the proposed solution and re-launching the attack, we noticed that the MAC address corresponding to the IPV6 address of the SECC could not be impacted by the attacker. We also noticed that the MAC and IPV6 addresses are permanent during the communication.

Fig. 19. EVCC NDP table after applying the solution against MITM attack.

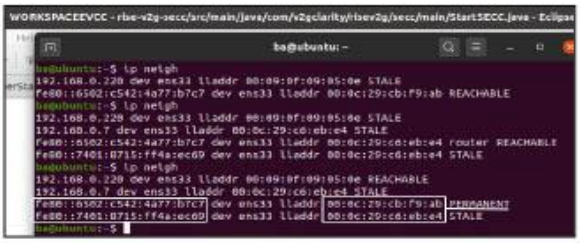


Fig. 20. SECC NDP table after applying the solution against MITM attack.

4. *Comparative Analysis*

To prove the efficiency of our protocol in terms of authentication time, the different authentication times found in the V2G literature and those reported by the authors are presented in Table III.

TABLE III
COMPARISON TABLE OF THE AUTHENTICATION TIMES OF THE PROPOSED SCHEME

Authors	Time required for authentication (second)
Nicanfar et al. [12]	63.77
Tsai et al. [12]	23.22
Xia and Wang. [12]	0.085
Proposed Scheme	0.0738

We can observe that the authentication time obtained for most of the protocols proposed in the V2G literature exceeds 20 s, which translates to high energy consumption. However, in the proposed system, the average time of five authentication simulations between a charging station and 20 vehicles in the absence of an attack was 0.0738 s.

These results demonstrate that the proposed authentication system is lightweight and fast. Moreover, this leads us to conclude that our system consumes less computational energy.

VI. CONCLUSION

In this study, we proposed a lightweight authentication scheme for V2G networks based on ISO 15118 and blockchain technology.

The proposed system comprises four blockchains, and accessibility to these blockchains is defined according to the sensitivity of the information contained in their respective blocks. The more sensitive the information stored, the more restricted the access. Each block of a blockchain is referenced by a unique index representing the vehicle information. Vehicles starting the first communication with the charging station or a charging/discharging operation only have to transmit the index and necessary information. This secures the communication, preserves the privacy of the vehicle, and alleviates the burden on the vehicles, which are limited in storage and computing resources.

With the Tamarin Prover tool, we modeled our scheme and simulated it using the RISEV2G tool, implementing the exchanges established between the charging station and the vehicle, considering the description of the ISO 15118 standard. We then integrated the implementation of the authentication scheme, four blockchains, and the proposed security solutions.

The results of the modeling and simulations show that our system is reliable; satisfies the security requirements, such as availability, non-repudiation, and integrity; resists multiple attacks, such as DOS attacks, MITM attacks, and spoofing attacks; and consumes less computation time and energy.

In the future, we propose to test this solution using the blockchain hyper-leader fabric for its advantages. Alternatively, NTF technology, which allows the storage and digitization of copyrights, can be used to store the certificates of electric vehicles and charging stations in a unique way, in combination with a blockchain that consumes the least amount of computing resources and energy.

REFERENCES

[1] *Bâtir une économie verte : le gouvernement du Canada exigera que la totalité des voitures et camions légers à passagers vendus soit des véhicules zéro émission d'ici 2035*, in *Gouvernement of Canada*. 2021.

[2] HydroQuebec. *HydroQuebec*. Accessed: Accesse.2022; Available from: https://www.hydroquebec.com/electrification-transport/voitures-electriques/recharge.html.

[3] Intel.*intel.ca*. Accessed: Accesse.2022; Available from: https://www.intel.ca/content/www/ca/fr/transportation/overview.html.

[4] N. Saxena, and B. J. Choi, "Authentication scheme for flexible charging and discharging of mobile vehicules in the V2G networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 7, pp. 1438–1452, Jul. 2016, doi: 10.1109/TIFS.2016.2532840.

[5] K. Bao, H. Valev, M. Wagner, and H. Schmeck, "A threat analysis of the vehicle-to-grid charging protocol ISO 15118," *Comput. Sci. Res. Dev. J.*, vol. 33, no. 1–2, pp. 3–12, Feb. 2018, doi: 10.1007/s00450-017-0342-y.

[6] Q. Wang, M. Ou, Y. Yang, and Z. Duan, "Conditional privacy-preserving anonymous authentication scheme with forward security in vehicle-to-grid networks," *IEEE Access*, vol. 8, pp. 217592–217602, 2020, doi: 10.1109/ACCESS.2020.3040112.

[7] S. Wang, B. Wang, and S. Zhang, "A secure solution of V2G communication based on trusted computing," in *2018 12th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, 2018.

[8] Y. Zhang, J. Zou, and R. Guo, "Efficient privacy-preserving authentication for V2G networks," *Peer Peer Netw. Appl.*, vol. 14, no. 3, pp. 1366–1378, May 2021, doi: 10.1007/s12083-020-01018-w.

[9] G. Shen, Y. Su and M. Zhang, "Secure and Membership-Based Data Sharing Scheme in V2G Networks," in IEEE Access, vol. 6, pp. 58450-58460, 2018, doi:

10.1109/ACCESS.2018.2874622.

[10] Google. *Working together to detect maliciously or mistakenly issued certificates*. Accessed: Accesse.2021; Available from: https://certificate.transparency.dev/.

[11] D. S. V. Madala, M.P. Jhanwar, and A. Chattopadhyay, "Certificate transparency using blockchain," in *IEEE International Conference on Data Mining Workshops (ICDMW)*, 2018.

[12] S. Aggarwal, N. Kumar, and P. Gope, "An efficient blockchain-based authentication scheme for energy-trading in V2G networks," *IEEE Trans. Industr. Inform.*, vol. 17, no. 10, pp. 6971–6980, Oct. 2021, doi: 10.1109/TII.2020.3030949.

[13] A. Iqbal, A. S. Rajasekaran, G. S. Nikhil, M. Azees, "A secure and decentralized blockchain based EV energy trading model using smart contract in V2G network," *IEEE Access*, vol. 9, pp. 75761–75777, 2021, doi: 10.1109/access.2021.3081506.

[14] H. Wang, Q. Wang, D. He, Q. Li, and Z. Liu, "BBARS: blockchain-based anonymous rewarding scheme for V2G networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3676–3687, Apr. 2019, doi: 10.1109/JIOT.2018.2890213.

[15] P. W. Khan and Y.-C. Byun, "Blockchain-based peer-to-peer energy trading and charging payment system for electric vehicles," *Sustainability*, vol. 13, no. 14, p. 7962, Jul. 2021, doi: 10.3390/su13147962.

[16] S. Khan, Z. Zhang, L. Zhu, M. A. Rahim, S. Ahmad, and R. Chen, "SCM: secure and accountable TLS certificate management," *Int. J. Commun. Syst.*, p. e4503, Jul. 2020, doi: 10.1002/dac.4503.

[17] A. Garba, Z. Chen, Z. Guan, and G. Srivastava, "LightLedger: a novel blockchain-based domain certificate authentication and validation scheme," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1698–1710, Apr. 2021, doi: 10.1109/TNSE.2021.3069128.

[18] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Inf. Sci.*, vol. 545, pp. 170–187, Feb. 2021, doi: 10.1016/j.ins.2020.07.060.

[19] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 177–186, May 2020, doi: 10.1016/j.dcan.2019.04.003.

[20] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, p. 4298–4311, Apr. 2020, doi: 10.1109/TVT.2020.2973651.

[21] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets VANET: an architecture for identity and location privacy protection in VANET," *Peer Peer Netw. Appl.*, vol. 12, no. 5, pp. 1178–1193, Sep. 2019, doi: 10.1007/s12083-019-00786-4.

[22] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *J. Syst. Archit.*, vol. 99, p. 101636, Oct. 2019, doi: 10.1016/j.sysarc.2019.101636.

[23] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019, doi: 10.1109/ACCESS.2019.2936575.

[24] Y. Inedjaren, M. Maachaoui, B. Zeddini, and J.-P. Barbot, "Blockchain-based distributed management system for trust in VANET," *Veh. Commun.*, vol. 30, p. 100350, Aug. 2021, doi: 10.1016/j.vehcom.2021.100350.

[25] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Blockchain-based message dissemination in VANET," in *IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, Kathmandu, Nepal, Oct. 2018.

[26] GitHub. *TAMARIN-PROVER*. Accessed: Accesse.2020; Available from: http://tamarin-prover.github.io/.

[27] GitHub.*RISEV2G*. Accessed: Accesse.2021; Available from: https://github.com/SwitchEV/RISE-V2G.

[28] Ettercap Dev. Team, A., NaGA. *Ettercap*. Accessed: Accesse.2021; Available from: https://www.ettercap-project.org/downloads.html.

Boucif Amar Bensaber received the Ph.D degree in computer science from University Renée Descartes, Paris V, France, in 1998. He worked as researcher at CRED (Centre of Research of Diagnostics Evaluation), Sherbrooke, Quebec, Canada. He is currently Professor, at the Mathematics and Computer Science Department of Université du Québec à Trois-Rivières Canada. He directs the LAMIA Applied Mathematics and Computer Science LAb. His research interests include security, ad hoc networks, sensor networks, vehicular networks and data mining.

Ines yahia received a master's degree in networks and distributed systems from the University of Batna 2, Algeria, in 2018. She is currently a student in applied mathematics and computer science at the University of Quebec in Trois-Rivières, Canada. her research interests include security, vehicular networks, and blockchain technology.

Chapitre 6 Méthodologie

Respectant la norme ISO 15118 et l'infrastructure PKI, nous proposons un modèle qui utilise quatre blockchains interreliés. Comme on peut le voir dans la figure 13, on a : la blockchain OEM ; la blockchain MO ; la blockchain Root CA/RA et la blockchain Transaction.

Chaque blockchain est propre à un niveau de certification sauf pour la blockchain Transaction. Les deux blockchains les plus élevés OEM (niveau 4) et MO (niveau 3) sont privées tandis que les 2 autres sont publiques. Chaque blockchain d'un niveau i offre une sécurité supplémentaire pour le niveau i-1 et un niveau i ne peut publier un certificat sans s'assurer que le certificat n'a pas été déjà enregistré à son niveau (pas de doublons) et que le certificat correspondant au niveau i+1 a déjà été publié.

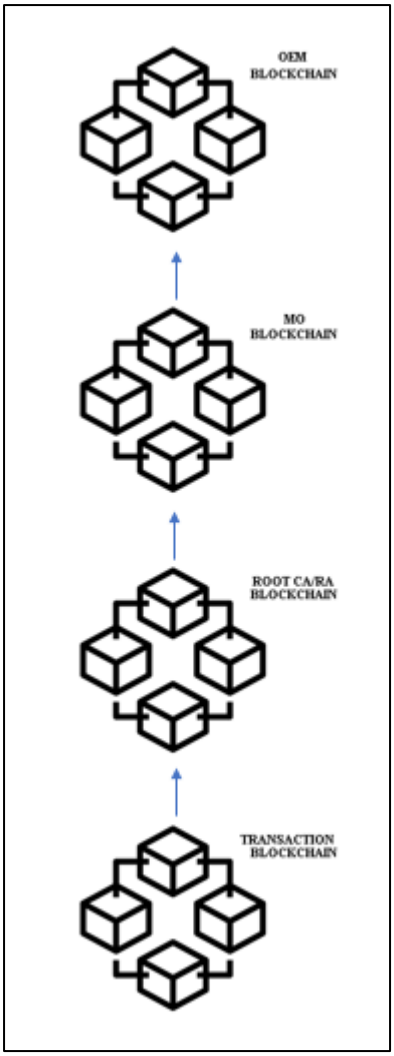


Figure 13 Structure Blockchains

Le niveau 4 est le plus élevé, étant la blockchain OEM, qui est responsable de la sécurité des certificats OEM PROV Certificates spécifique à la fabrication de chaque nouveau véhicule, seuls les nœuds OEM de confiance peuvent publier dans cette blockchain. Les entités de la blockchain MO peuvent avoir accès à la blockchain OEM, mais seulement pour la vérification de la

disponibilité et de l'authenticité d'un certificat, ils ne peuvent en aucun cas modifier ou publier dans celle-ci.

Le niveau 3 est la blockchain MO, qui est responsable d'enregistrer les certificats de contrats établis avec le Mobility Operator. Elle s'assure que le nouveau véhicule à enregistrer est déjà enregistré au niveau de la blockchain OEM, et qu'il ne sera pas enregistré plus d'une fois dans la MO. Les entités de la blockchain Root CA/RA peuvent accéder à la blockchain MO pour la vérification, mais ces entités ne peuvent en aucun cas publier dans la blockchain MO.

Le niveau 2 étant la blockchain Root CA/RA. Cette blockchain s'assure que le véhicule est enregistré au niveau MO et qu'il est propriétaire d'un certificat authentique en vérifiant la signature des certificats (OEM, MO). Elle s'assure également que les LAGS sont enregistrés et que ce sont des nœuds non malveillants. La blockchain Root CA/RA va retenir l'index signé des blocs contenant les certificats correspondants MO, OEM, au véhicule et à la station de charge. On peut dire qu'elle est l'intermédiaire entre les blockchains privées OEM, MO et la blockchain publique Transaction.

Les blockchains OEM, MO, ROOT CA/RA sont utilisées pour la publication des certificats authentiques, alors que le niveau 1 qui représente la blockchain Transaction, est géré par les LAGS où toutes les transactions sont enregistrées, et les payements ou récompenses sont effectués.

Notre modèle dispose aussi d'un smart contrat au niveau de chaque blockchain, qui a la tâche de :

- Gérer les autorisations d'accès aux blockchains.
- Gérer l'enregistrement des données en blocs.
- Vérifier la duplication de blocs.
- Assurer la sécurité en vérifiant la correspondance entre le certificat d'un nœud émetteur et la liste noire.
- Gérer les payements/récompenses.

6.1 Schéma proposé :

Notre schéma est présenté par deux parties, la première partie constitue l'étape de l'enregistrement d'un nouveau véhicule qui désigne le premier contact avec la borne et la seconde partie constitue le chargement/déchargement du véhicule. Nous avons intégré par la suite des schémas expliquant le déroulement de la phase de l'authentification dans ces deux parties. La signification des symboles correspondants est décrite dans le tableau 1.

6.1.1 Enregistrement d'un nouveau véhicule :

À la fabrication d'un nouveau véhicule, l'entité OEM SUB-CA2 lui délivre un OEM PROVISIONING CERTIFICATE, ce dernier va être enregistré au niveau de la blockchain OEM par le biais du smart contrat, qui va vérifier la signature sur le certificat, le nœud émetteur du certificat et l'unicité de ce certificat au niveau de la blockchain. Si toutes les informations sont valides, le smart contrat ajoute le nouveau bloc contenant le certificat du nouveau véhicule avec toutes les informations nécessaires, sinon le bloc est rejeté, le nœud OEM SUB-CA2 responsable sera mis dans la liste noire et le certificat révoqué.

Au niveau 3, le nouveau véhicule ayant été enregistré au niveau de la blockchain OEM doit être enregistré au niveau de la blockchain MO. L'entité MO SUB-CA2 délivre un CONTRACT CERTIFICATE au véhicule. Ce certificat doit être validé par le smart contrat MO, en vérifiant la validité de la signature du MO et l'authenticité de l'entité MO. À ce moment, le smart contrat MO va transmettre l'index du bloc au smart contrat OEM pour vérifier que le certificat est déjà enregistré au niveau de la blockchain OEM si c'est le cas, le nouveau bloc sera créé et publié au niveau de la blockchain MO. Dans le cas contraire, le bloc sera rejeté, le CONTRACT CERTIFICATE du véhicule révoqué et le nœud émetteur sera mis dans la liste noire.

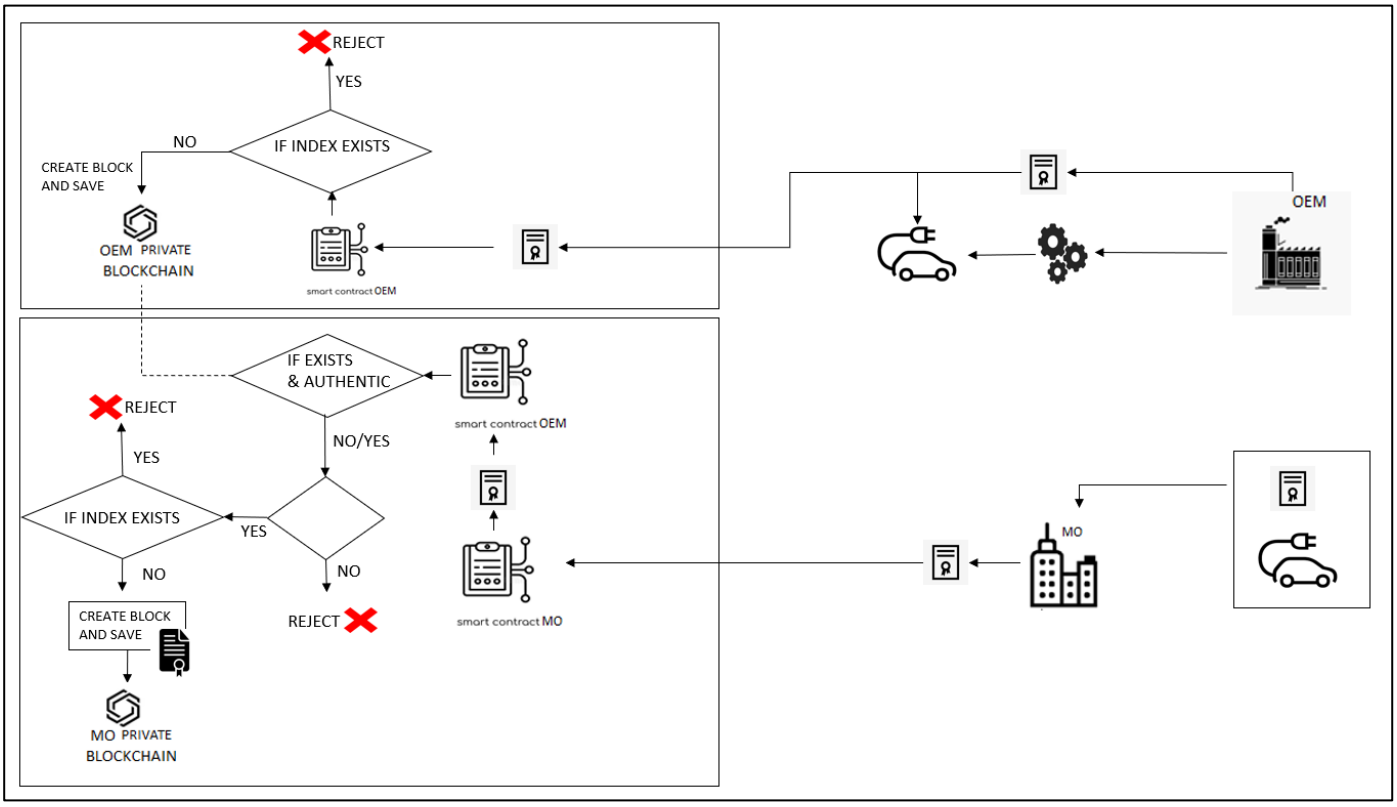


Figure 14 Schéma représentant l'enregistrement d'un nouveau EV au niveau des blockchains OEM et MO

Le même processus va se dérouler pour les deux blockchains ROOT CA/RA et Transaction à l'exception que ces deux blockchains sont publiques, et que :

- Dans la blockchain ROOT CA/RA, chaque bloc contient les deux index référençant les deux certificats OEM, MO et un CONTRACT CERTIFICATE délivré et signé par l'entité CA/RA. La blockchain ROOT CA/RA détient également le certificat correspondant à chaque station de charge.
- Au niveau de la blockchain Transaction, les LAGS sont responsables de gérer les transactions afin d'alléger les stations de charges. Toutes les transactions effectuées ainsi que le type d'opération, frais de chargement ou taux de récompenses, index station de charge et index de véhicule seront enregistrés. Avant l'approbation des nouveaux blocs, une signature du véhicule, du LAG et du CA/RA sera nécessaire.

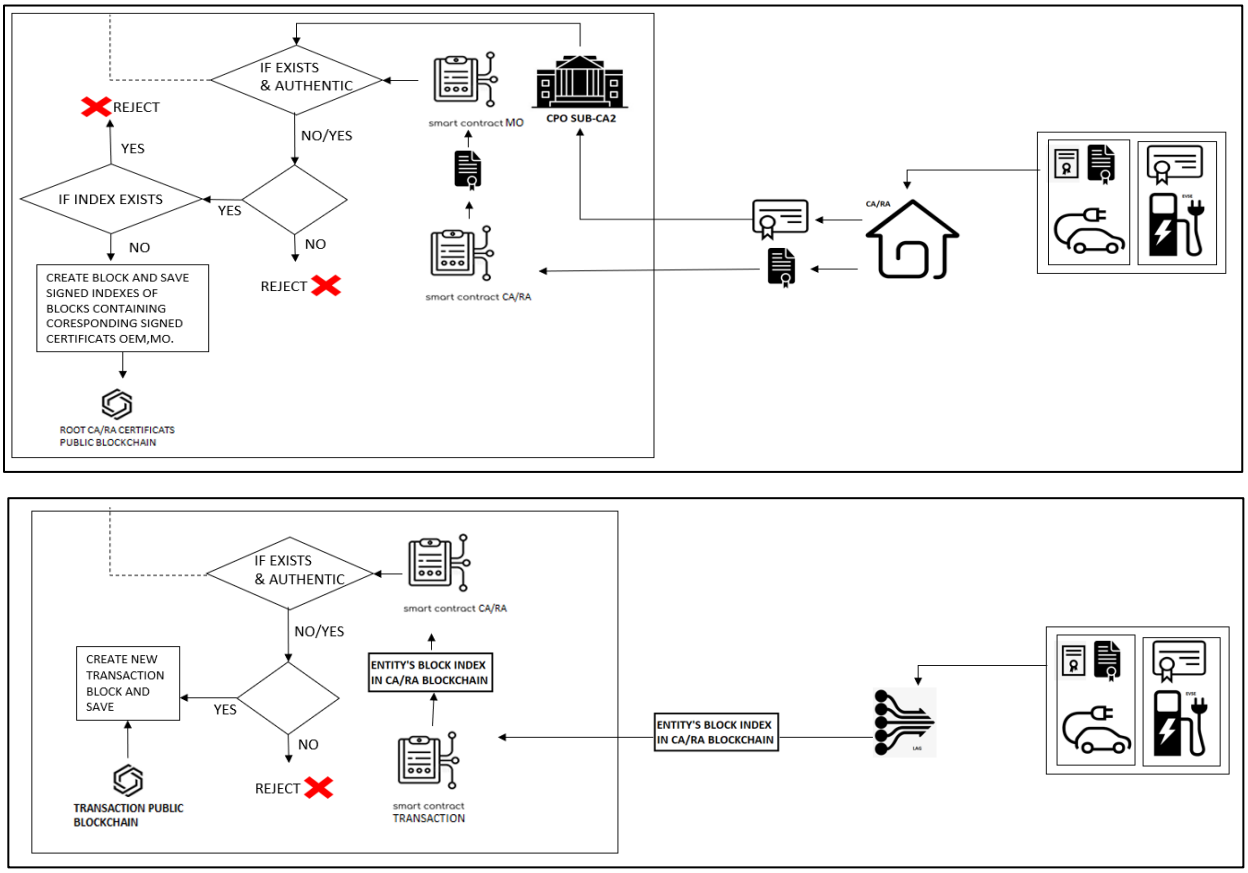


Figure 15 Schéma représentant l'enregistrement d'un nouveau EV au niveau des blockchains CA/RA et Transaction

6.1.2 Chargement/ déchargement du véhicule :

Après l'enregistrement du véhicule, suit l'étape du chargement ou du déchargement de ce dernier. Dans notre modèle, le premier contact avec la station de charge diffère des futurs contacts. Pour le premier contact, le véhicule détient une liste de station de charge contenant des adresses (ou index) signée par le MO. Le véhicule doit transmettre l'adresse (l'index) signé à la station de charge correspondante, après la vérification de la signature par la station de charge, le véhicule sera considéré comme un nouveau véhicule qui entame une première authentification.

La figure 16 ci-dessous illustre les différents échanges entre la station de charge et le véhicule. Ce dernier établi un premier contact avec la station de charge en émettant une requête charge/décharge accompagnée de l'index station de charge signé par MO, ensuite la station de charge transmet son index correspondant dans la blockchain ROOT CA/RA, le véhicule vérifie la disponibilité de l'index puis à son tour il transmet son index correspondant dans la blockchain ROOT CA/RA à la station de charge. Après sa vérification par la station de charge, le véhicule envoie les paramètres de chargement/déchargement sous la demande de la station de charge. À la fin, un bloc sera créé ; signé et enregistré au niveau de la blockchain Transaction suite à son approbation.

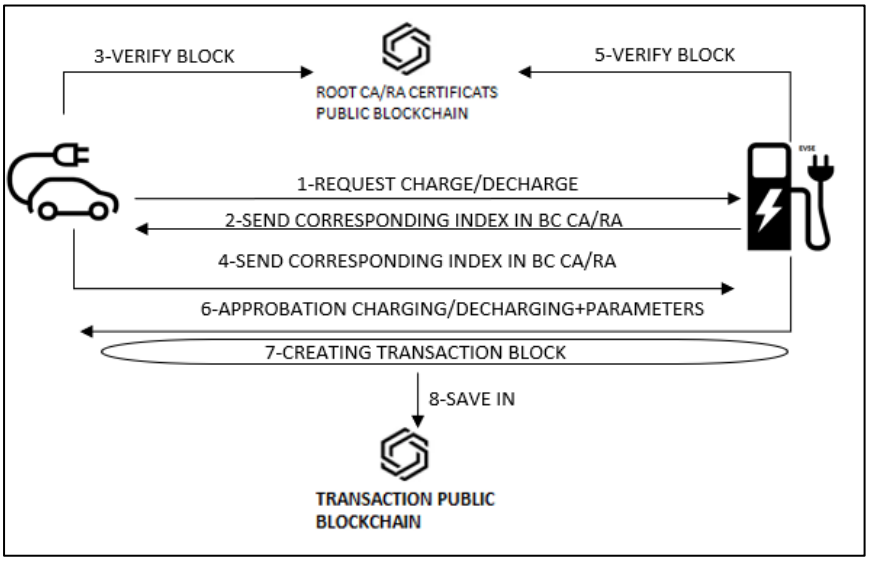


Figure 16 Schéma représentant le chargement/déchargement de l'EV.

6.2 Déroulement de l'authentification :

6.2.1 Enregistrement d'un nouveau véhicule :

La figure 17 ci-dessous présente les échanges entre les entités EV, LAG, CA/RA pour l'enregistrement du véhicule au niveau de la blockchain ROOT CA/RA. La définition des mots clés utilisés est présenté dans le tableau des abréviations suivant :

Mots clés	Signification
SK, PK	Clé privé, Clé publique
E (), D ()	Chiffrement, Déchiffrement
sig	Signature
I, I'	Index reçu, Index vérifié
BC	Blockchain
RAuth	Demande authentification
@	Adresse
H	Hach
sigC	Signature calculée
signed	Message signé
OPP	Opération
RSO	Demande démarrage opération
CSO	Confirmation démarrage opération
TRANSACC	Transaction accomplie
END OPP	Demande fin opération

Tableau 1 Tableau récapitulatif des abréviations utilisées

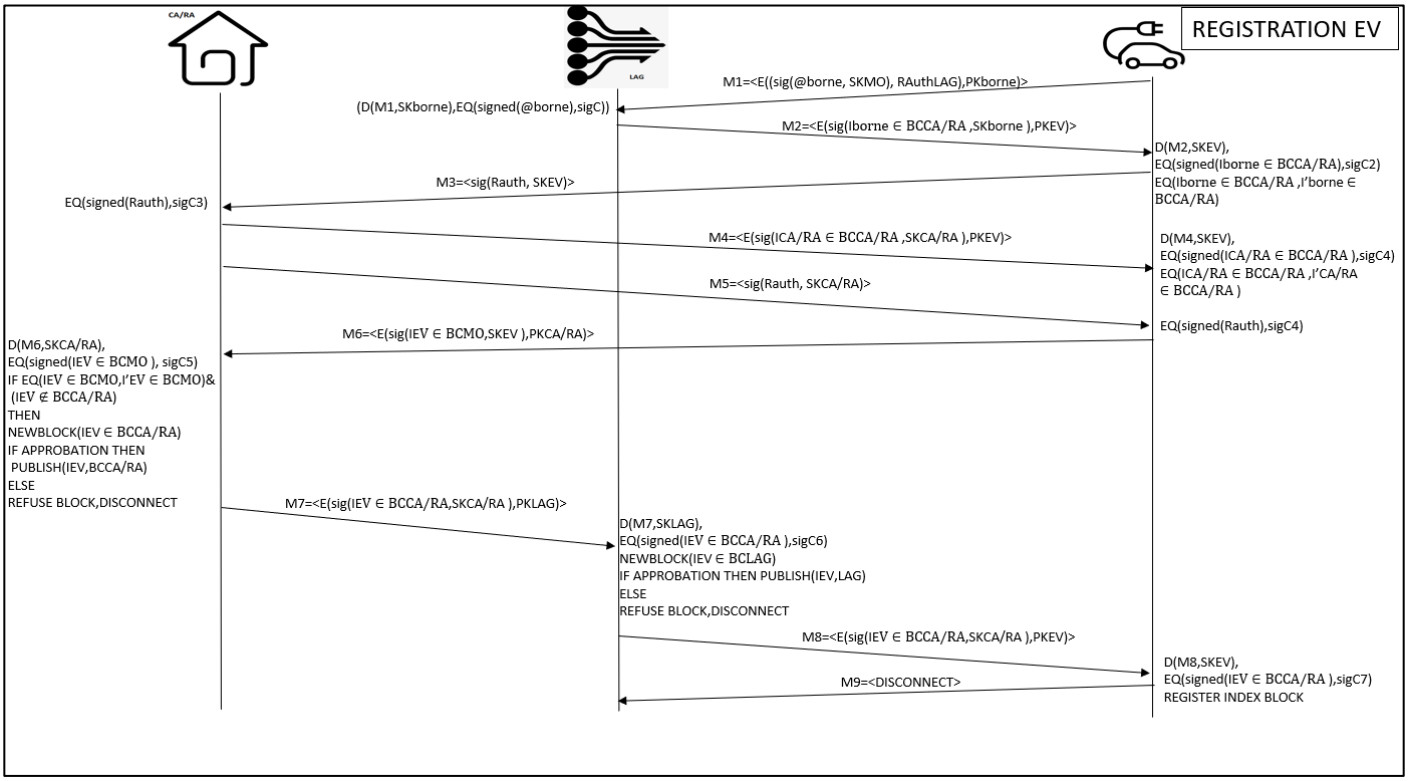


Figure 17 Schéma explicatif représentant le déroulement de l'opération de l'enregistrement de l'EV

En considérant que le LAG va représenter aussi les tâches effectuées par la station de charge, EV détient son couple de clés (publique, privé) et son index correspondant à son certificat au niveau de la blockchain MO.

Tous les messages transmis entre les entités sont signés puis cryptés, donc un décryptage et une vérification de la signature s'imposent avant toute réponse.

Lors du premier contact avec la station de charge, l'EV transmet l'adresse de la station de charge signée par la clé privée MO et une demande d'authentification, le tout crypté avec la clé publique de la station de charge.

Après avoir décrypté le message M1 et vérifié la signature, la station de charge envoie le message M2 contenant son index correspondant dans la blockchain ROOT CA/RA.

EV doit vérifier alors au niveau de la blockchain Root CA/RA que la station de charge est toujours authentique. Si c'est le cas, il doit s'assurer de l'authenticité du CA/RA en envoyant une demande d'authentification. Le CA/RA en réponse transmet son index et une demande d'authentification pour l'EV. Si les informations sont valides, EV répond en transmettant son index au niveau de la blockchain MO. Le nœud CA/RA vérifie la disponibilité de l'index EV au niveau de la blockchain et qu'il n'y a pas de doublons au niveau de la blockchain CA/RA, alors un nouveau bloc contenant l'index et les informations nécessaires sera créé. Si le bloc a été approuvé, l'index correspondant sera envoyé au LAG pour l'enregistrer au niveau de la blockchain Transaction et il sera envoyé également à l'EV. Dans le cas contraire où le bloc n'a pas été approuvé, l'EV sera automatiquement déconnecté de la station de charge.

6.2.2 Chargement / déchargement du véhicule :

Pour une opération de chargement/déchargement, le processus d'authentification et d'enregistrement de la transaction illustré par la figure 18 ci-dessous se déroule comme suit :

L'EV communique une demande d'authentification à la station de charge, qui à son tour renvoie son index correspondant dans la blockchain CA/RA accompagnée d'une demande d'authentification à l'EV. Après la vérification de l'index de la station de charge, l'EV transmet son index. Si l'authentification est validée, la station de charge envoie une demande de choix d'opération, et l'estimation du temps nécessaire du processus. L'EV répond avec le choix des paramètres établi. La station de charge transmet les informations reçues au LAG pour établir un calcul des frais à payer ou des récompenses et cela dépend du niveau de la charge du réseau. La station de charge transmet ensuite ces informations à l'EV. S'il s'agit d'un payement, les frais payés par EV seront gardés par le smart contrat jusqu'à la fin du chargement et s'il s'agit d'un déchargement, les récompenses seront attribuées également après la fin du déchargement par le smart contrat.

Le processus continue avec la création d'un nouveau bloc contenant toutes les informations nécessaires reliées à la transaction. La signature du LAG, EV et CA/RA est requise avant la publication de ce bloc dans la blockchain transaction et l'EV ajoute le numéro de la transaction établie dans sa liste de transaction temporaire. Le chargement débute après la signature du bloc. À la fin de l'opération, le bloc de la transaction sera approuvé, la station de charge envoie une requête de déconnexion et l'EV se déconnecte.

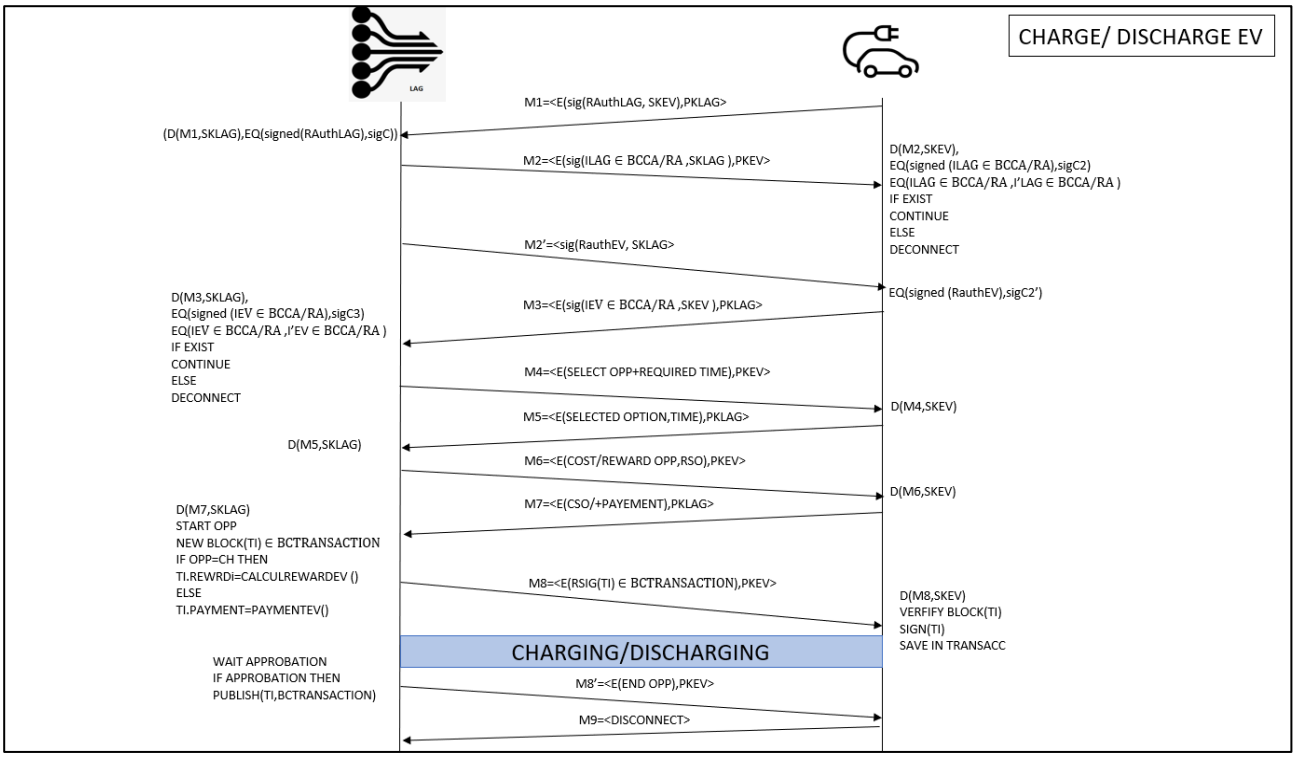


Figure 18 Schéma explicatif représentant le déroulement des opérations de Chargement/Déchargement de l'EV

6.3 Mesure de sécurité contre les attaques :

Les attaques les plus récurrentes sur les réseaux V2G sont : l'attaque DOS, l'attaque d'usurpation d'identité et l'attaque MITM.

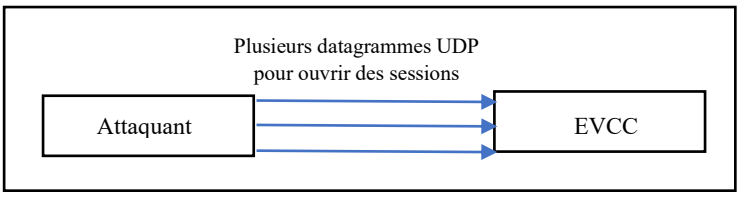
6.3.1 L'Attaque DOS :

Elle vise à troubler le bon fonctionnement du réseau V2G en l'encombrant avec l'envoi successif de paquets en un temps défini. Plusieurs types d'attaques DOS existent, cependant notre choix s'est posé sur les types d'attaques DOS UDP Flooding (vers EVCC, vers SECC) et DOS ICMP (Echo EVCC replay to SECC, Echo SECC replay EVCC). Ainsi notre travail s'appuie principalement sur la détection et le blocage de ces attaques les plus nuisibles en termes de consommation d'énergie et de temps de calcul.

6.3.1.1 Attaque DOS UDP ou UDP Flooding:

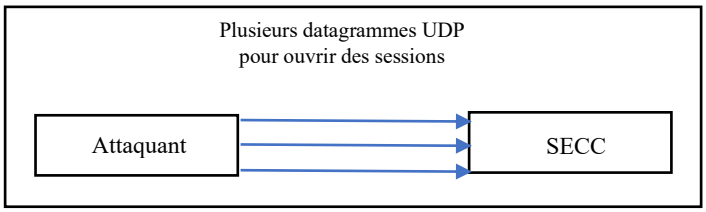
- Attaquant vers EVCC :

Inonder l'EVCC avec des paquets UDP envoyés par une entité malveillante.



- Attaquant vers SECC :

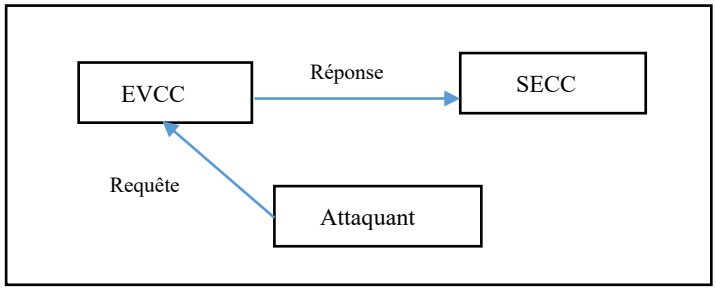
Inonder l'SECC avec des paquets UDP envoyés par une entité malveillante.



6.3.1.2 DOS ICMP:

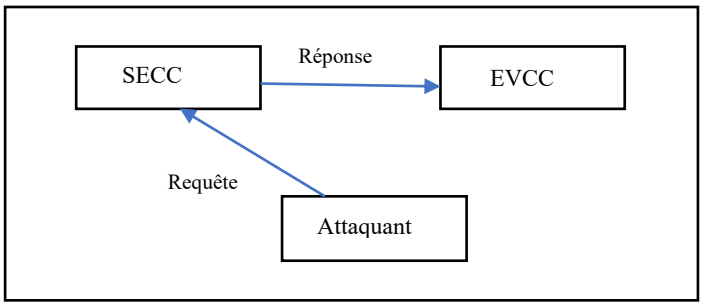
- Echo EVCC replay to SECC:

Dans le but d'inonder SECC, l'attaquant envoie plusieurs paquets ICMP au véhicule, et à son tour le véhicule répond à la station de charge.



- Echo SECC replay EVCC:

L'attaquant envoie plusieurs paquets ICMP à la station de charge, et à son tour la station de charge renvoie les réponses à l'EVCC.



6.3.1.2 Solution appliquée pour protéger contre l'attaque DOS :

Avant de protéger notre système contre l'attaque DOS, il est nécessaire de la déceler. Pour cela, nous détectons tout Traffic réseau inhabituel en comptant les paquets venant de la même source. Dans notre solution, si le nombre de paquets UDP ou ICMP inhabituel est égal ou supérieur à 100 paquets par seconde, on coupe la communication avec l'émetteur. Le pseudo code en dessous explique notre solution.

```
Variables
UDPmessage : udp packet
ListOfBlockedSenderIP: ArrayList
T: integer // the number of incoming messages threshold
Begin
While True Do
      UDPmessage = recieveIncommingMessages ()
  If UDPmessage.getSenderIP() not in ListOfBlockedSenderIP Then
      If numberOfMessagesFrom (UDPmessage.getSenderIP()) > T Then
            ListOfBlockedSenderIP.add (UDPmessage.getSenderIP())
      End If
   Else
      Reject (UDPmessage)
   End If
End While
End          //T =100
```

Figure 19 Pseudo code de la solution DOS

6.3.2 Usurpation d'identité(spoofing) :

L'attaque consiste à s'approprier l'identité d'un nœud légitime pour avoir accès aux informations importantes dans les réseaux V2G, ce qui ouvre une brèche à l'attaquant pour altérer le système et utiliser ces informations de façon illégitime.

Dans notre schéma chaque bloc dans la blockchain CA/RA est représenté par un index. A chaque communication entre l'EV et la station de charge, une authentification doit être faite des deux côtés, et cela en utilisant l'index correspondant à l'entité par rapport à son bloc dans la blockchain CA/RA. Chaque bloc dans la blockchain CA/RA comprend les informations nécessaires pour authentifier le véhicule, tel que le certificat signé, et la clé publique.

Pour éviter, détecter et bloquer toute attaque d'usurpation d'identité sur notre système, on propose notre solution qui est illustrée sur la figure 20 ci-dessous. L'EVCC va transmettre à l'SECC l'index et l'index signé correspondant à son bloc dans la blockchain CA/RA et à son tour SECC va vérifier l'authenticité de l'identité de EV en récupérant la clé publique PK d'EV stockée au niveau du bloc indiqué. Ensuite, SECC va utiliser cette dernière pour vérifier si INDEXEV et SIGNED_INDEXEV correspondent. Si c'est le cas, la phase de l'authentification est établie et la communication suit son court, mais dans le cas où INDEXEV et SIGNED_INDEXEV ne correspondent pas, l'EV est automatiquement déconnecté.

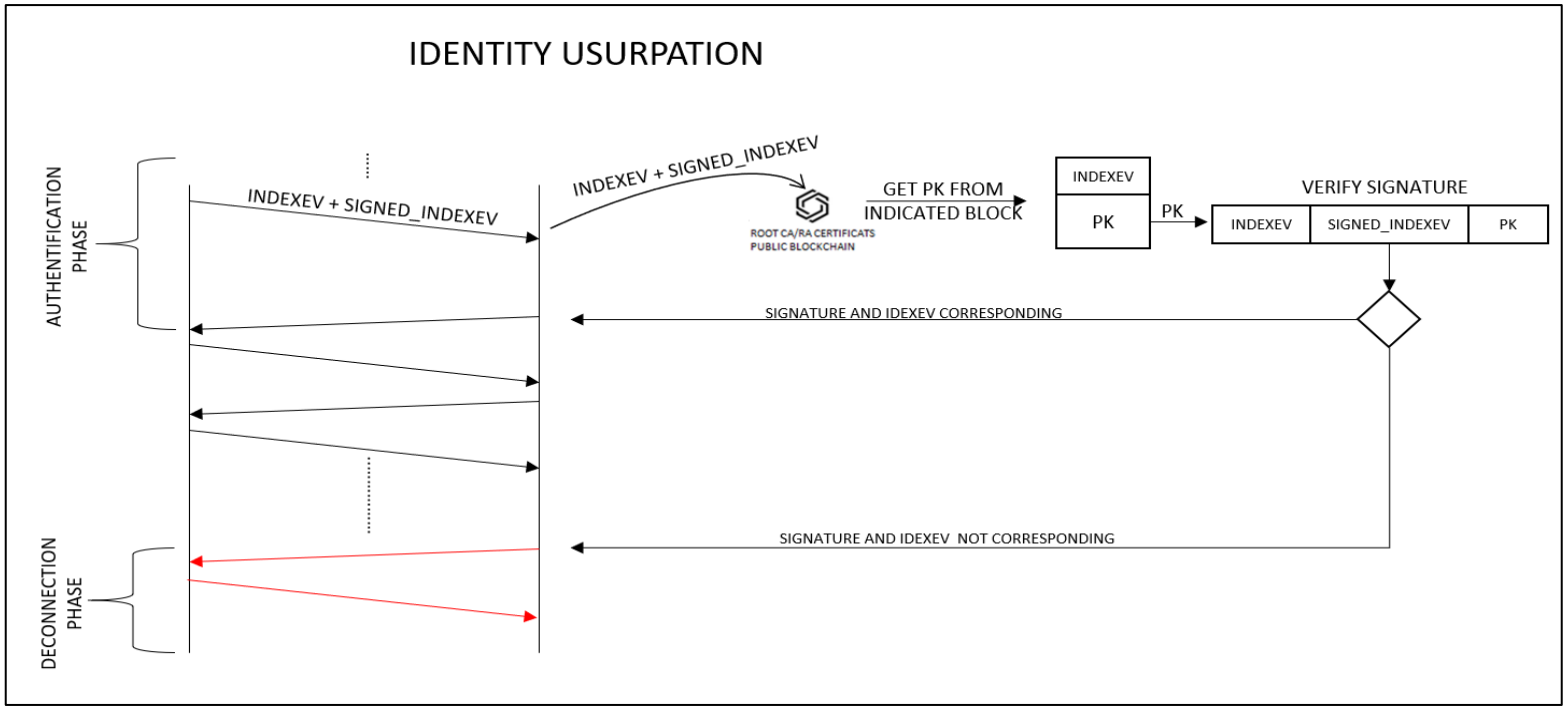


Figure 20 Schème explicatif de la solution proposée contre l'attaque d'usurpation d'identité

Le pseudo code en dessous décris notre solution.

```
//// SENDER PART: LIGITIM EV
Variables
INDEXEV: Index
SIGNATURE: Signature
PK: Public Key
MESSAGE: IPV6 Packet
Begin
PRK = READ_PRIVATE_KEY ()
SIGTNATURE = SIGN (INDEXEV, PRK)
MESSAGE.setIndexEv(INDEXEV)
MESSAGE.setSignature(SIGNATURE)
SEND_TO_SECC(MESSAGE)
End
```

Figure 21 Pseudo code de la solution contre l'attaque Usurpation d'identité coté EV

```
//// Receiver PART: SECC
Begin
While True Do
        MESSAGE = Receive_From_EVCC ()
        INDEXEV = MESSAGE.getIndexEv()// get the EV Index
        SIGNATURE = MESSAGE.getSignature()// get the signature
        PK = Retrieve_PK_From_Block (INDEXEV)
        If Check_SIGNATURE (INDEXEV, SIGNATURE, PK) == FALSE Then
                STOP_COMMUNUCATION ()
        Else
                        .
                        .
                        .
                sendMessage (NewMessage)
        End IF
End While
End
```

Figure 22 Pseudo code de la solution contre l'attaque Usurpation d'identité coté SECC

6.3.3 Attaque l'homme au milieu (MITM) :

Dans ce type d'attaque, un nœud illégitime s'introduit dans une communication entre deux nœuds légitimes et devient un nœud intermédiaire dans la communication. L'attaque MIMT permet d'usurper l'identité du locuteur et de l'interlocuteur en utilisant les attaques de NDP Poisoning, DNS Poisoning, DOS et bien d'autres. Dans notre travail, nous allons traiter l'attaque MITM utilisant le NDP Poisoning.

Le protocole NDP (Neighbor Discovery Protocol) basé sur ICMPV6 est utilisé dans les réseaux IPV6 pour la découverte des voisins, comme la table ARP dans les réseaux ipv4, la table NDP nous permet de consulter les adresses ipv6 des voisins avec leurs adresses MAC correspondantes.

L'attaque MITM utilisant la table NDP Poisoning va provoquer une contamination de la table NDP au niveau des entités légitimes communicantes, les deux adresses celles des entités légitimes et celle de l'attaquant auront la même adresse MAC (adresse MAC de l'attaquant).

On peut protéger notre communication contre l'attaque MITM utilisant le NDP Poisoning, en gardant les adresses IPv6 utilisées pour la phase d'authentification comme adresses permanentes jusque-là fin de la communication, de cette manière on pourra éviter la contamination de la table NDP car une fois rendu permanentes, le système va rejeter toute modification résultante des messages de NDP-sollicitation envoyé par l'attaquant permettant d'indiquer aux machines la nouvelle adresse MAC dont les adresses ipv6 sont liées. Notre solution est illustrée par la figure 23 ci-dessous.

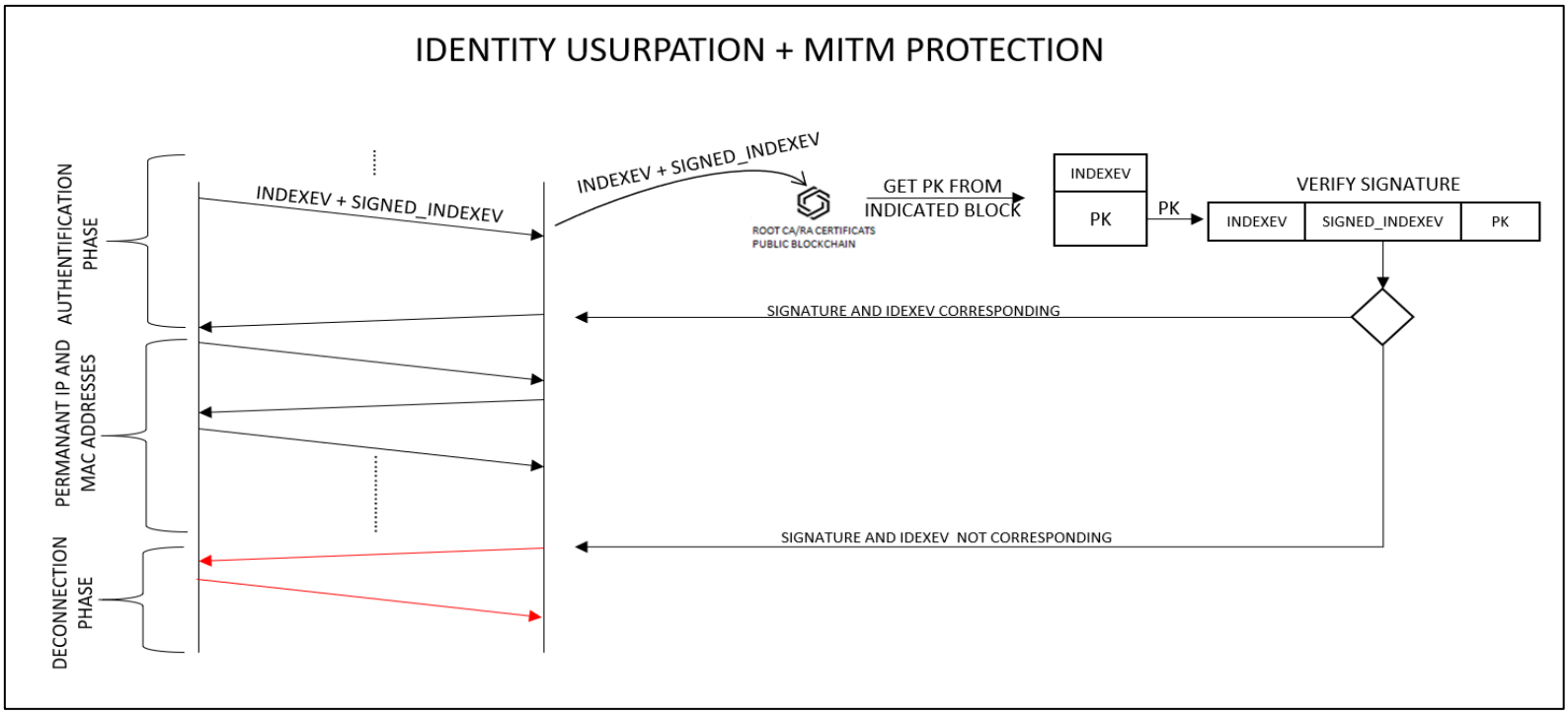


Figure 23 Schème explicatif de la solution proposée contre l'attaque MITM

Notre pseudo-code pour la protection contre l'attaque MITM :

```
//// Receiver PART: LIGITIM EV
Variables
        MESSAGE: IPV6 Packet
Begin
        MESSAGE = Receive_From_SECC ()
        setPermanant (MESSAGE.getSenderIP,MESSAGE.getSenderMAC)
                                .
                                .
                                .
        sendMessage (NewMessage)
End
```

Figure 24 Pseudo code de solution contre l'attaque MITM coté EV

```
//// Sender PART: SECC
Begin
        While True Do
                MESSAGE = Receive_From_EVCC ()
                INDEXEV = MESSAGE.getIndexEv()// get the EV Index
                SIGNATURE = MESSAGE.getSignature()// get the signature
                PK = Retrieve_PK_From_Block (INDEXEV)
                If Check_SIGNATURE (INDEXEV, SIGNATURE, PK) == FALSE Then
                        STOP_COMMUNUCATION ()
                Else
                        setPermanant (MESSAGE.getSenderIP,
MESSAGE.getSenderMAC)
                                .
                                .
                                .
                        sendMessage (NewMessage)
                End If
        End While
End
```

Figure 25 Pseudo code de la solution attaque MITM coté SECC

6.4 Conclusion

Dans ce chapitre, nous avons tout d'abord présenté notre modèle qui utilise quatre blockchains interreliés, la blockchain OEM et la blockchain MO qui sont des blockchains privées ainsi que la blockchain Root CA/RA et la blockchain Transaction qui sont des blockchains publiques. Par la suite, nous avons détaillé les deux principales étapes, la première étape qui concerne l'enregistrement d'un nouveau véhicule et la seconde qui concerne l'opération de chargement/ déchargement du véhicule.

Enfin, nous avons introduit dans ce chapitre la partie sécurité, ou nous avons exposé les attaques les plus nuisibles en termes de consommation d'énergie et de temps de calcul, ainsi que les solutions proposées et les pseudo codes associés.

Dans le chapitre suivant, nous allons présenter les résultats obtenus en utilisant les outils de modélisation et de simulation afin de démontrer la faisabilité de notre solution.

Chapitre 7 Analyse des résultats

Dans ce chapitre, nous allons récapituler les résultats obtenus à travers notre modélisation et nos simulations.

7.1 Modélisation et analyse des résultats :

Pour notre modélisation, nous avons utilisé l'outil Tamarin-Prover [66], qui est un outil de modélisation symbolique. Cet outil permet d'établir une vérification formelle de la communication entre les entités et de faire une analyse des protocoles de sécurité.

Dans notre simulation, on a vérifié la sécurité du schéma proposé en utilisant l'adversaire Dolev-Yao, proposé par TAMARIN PROVER, qui peut contrôler le réseau, supprimer, injecter, modifier et intercepter des messages.

Notre modèle est divisé en deux parties. La première partie du modèle représente l'enregistrement d'un nouveau véhicule et la deuxième partie représente le chargement/déchargement du véhicule. Les résultats obtenus sont illustrés sur les figures 26 et 27.

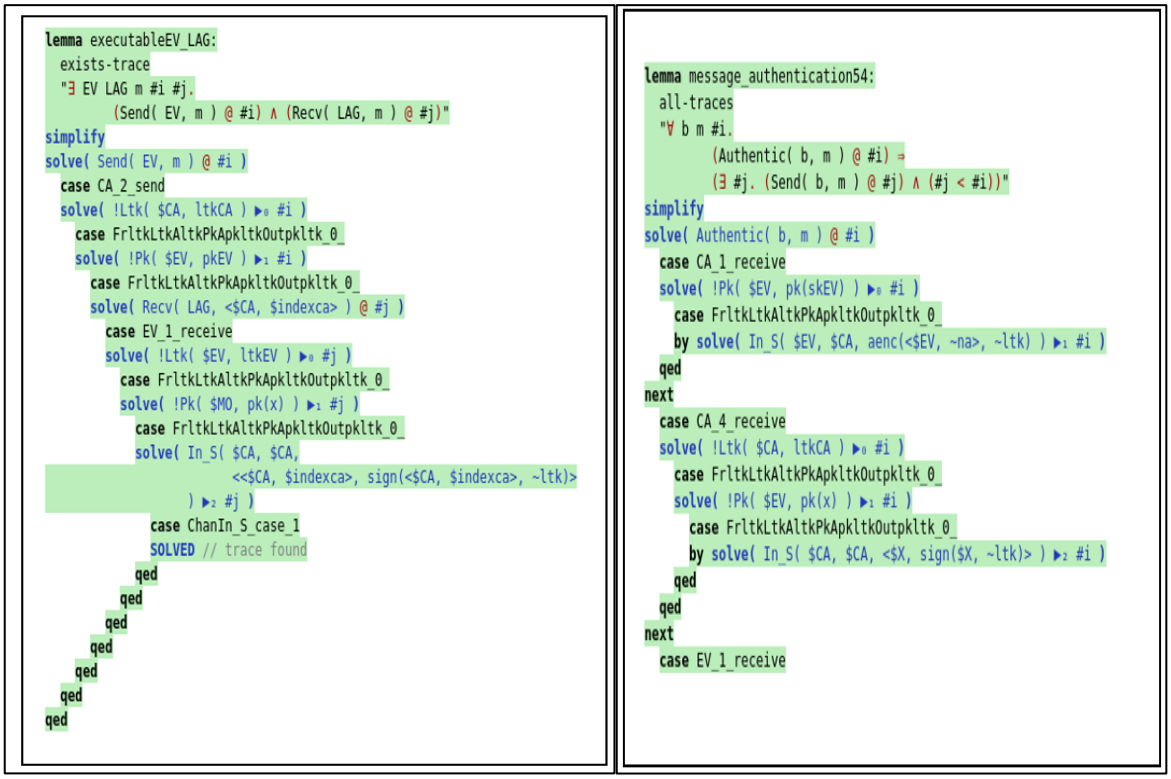


Figure 26 Résultats de l'exécution de la partie un (1) du modèle

Figure 27 Résultats de l'exécution de la partie deux (2) du modèle

Les figures 26 et 27 illustrent respectivement les résultats d'exécution des lemmas de la partie un (1) et la partie deux (2) de notre modèle. A travers les lemmas, on peut tester : la confidentialité du message avec le lemma Secrecy, l'authenticité de l'agent avec le lemma Authentication, la vérification des signatures en utilisant le lemma Restriction Equality, et les lemmas Secure Channel pour tester l'authentification, l'intégrité et la sécurité des transmissions des canaux.

On peut observer que ces résultats sont colorés en vert, ce qui révèle que le modèle proposé est sécurisé. Et à travers les lemmas utilisés, on peut conclure que notre modèle assure également la confidentialité, l'authentification et l'intégrité.

7.2 Simulation et analyse des résultats :

Pour notre simulation, nous avons utilisé l'outil RiseV2G [67] qui est un simulateur Open Source implémentant la norme ISO 15118. Par la suite, nous avons implémenté le code permettant de faire une représentation de nos quatre blockchains et leurs smart contrats respectifs. Pour la sécurité de la communication entre les entités participantes, on a utilisé la suite cryptographique **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256**. Et enfin, nous avons pu tester notre système contre les attaques les plus récurrentes. Pour les attaques DOS et l'attaque d'usurpation d'identité, on a mis en œuvre leurs simulations respectifs et on a obtenu les résultats d'avant et d'après l'application de notre solution. Pour l'attaque de l'homme au milieu, on a utilisé l'outil de simulation Ettercap. Les résultats obtenus sont présentés dans la suite de ce chapitre.

7.2.1 Attaques DOS :

Pour la simulation de l'attaque DOS, nous avons accompli notre étude sur 4 états de notre système :

- L'état SPSA : désigne notre système sans attaque DOS et sans protections contre celles-ci.
- L'état SPAA : désigne notre système avec des attaques DOS et sans protection contre celles-ci.
- L'état APSA : désigne notre système sans attaque DOS et où les protections contre ces attaques sont implémentées.
- L'état APAA : désigne notre système subissant des attaques DOS et comportant des protections contre celles-ci.

État du système	Attaques DOS	Protection contre les attaques
SPSA		
SPAA	✓	
APSA		✓
APAA	✓	✓

Tableau 2 États du système

Dans l'objectif d'observer le comportement de notre système dans les états cités ci-dessous et d'établir une estimation par rapport au temps d'exécution, nous avons établi 5 simulations différentes pour chaque état, où nous avons utilisé une station de charge et 20 véhicules. La communication avec ces véhicules se fait d'une façon séquentielle (un véhicule à la fois). Les messages UDP-ICMP sont envoyés par un code exécuté par un nœud malveillant qui envoie ces messages de façon continue.

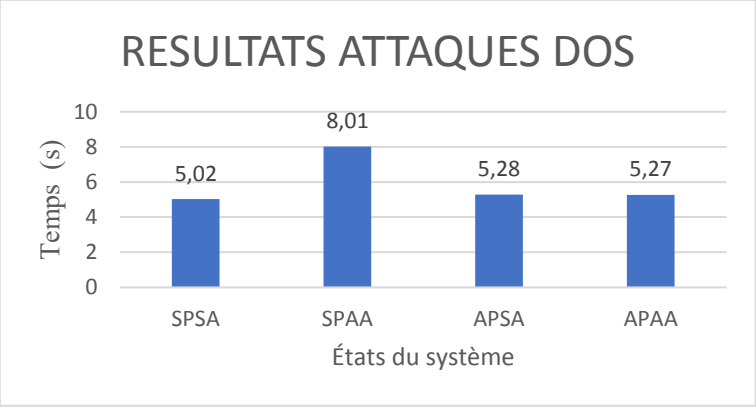


Figure 28 Graphique représentant les résultats de la simulation de l'attaque DOS

La figure 28 ci-dessus nous permet de voir le temps moyen en (s) écoulé des cinq simulations correspondant à chaque état de notre système pour la communication des 20 véhicules avec la station de charge.

En observant notre système dans les deux premiers états qui sont SPSA et SPAA (où le système n'inclut aucune protection contre ces attaques DOS), nous pouvons remarquer que le temps d'exécution en présence d'une attaque est beaucoup plus élevé que sans attaque, ce qui nous permet de conclure que le système a été impacté par ces attaques.

Par la suite, en comparant notre système dans les deux états SPAA et APAA, nous pouvons remarquer que le temps d'exécution est plus lent dans l'état SPAA. De cela, on peut conclure que la solution apportée au niveau de la sécurité a permis à notre système de devenir beaucoup plus efficace en termes de temps de calcul.

Puis en comparant notre système dans les deux états APSA et APAA, la moyenne des cinq simulations d'APSA prend (5.28s) et la moyenne des cinq simulations d'APAA revient à (5.27s), nos résultats restent très proches. Ce qui signifie que les différents types d'attaques DOS n'affectent pas notre système en termes de temps de calcul.

À la figure 29, on peut voir que notre système détecte l'attaque DOS et met fin à cette connexion.

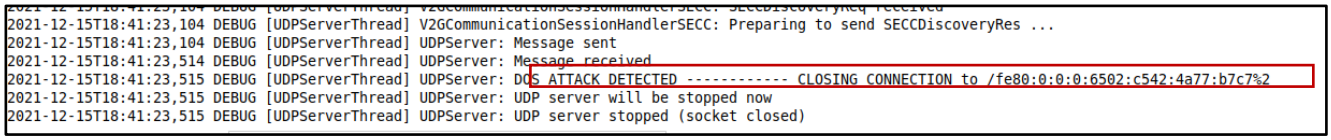


Figure 29 Détection de l'attaque DOS

Les résultats des expérimentations de l'attaque DOS sur notre système nous ont permis d'aboutir à la conclusion suivante :

La solution proposée a non seulement protégé notre système contre les différents types d'attaques DOS, mais elle a apporté aussi une amélioration en termes de temps d'exécution.

7.2.2 Attaque d'usurpation d'identité :

Pour la simulation de l'attaque d'usurpation d'identité, comme expliqué dans le chapitre précédent, on a généré une fausse signature de l'index EV en utilisant une clé privée (clé générée aléatoirement) non liée à la clé publique enregistrée au niveau de la blockchain CA/RA.

Par le biais du résultat illustré ci-dessous (figure 30), où on peut voir que notre système arrive à détecter que l'EV n'est pas légitime et par conséquent la communication est coupée par la station de charge.

Figure 30 Détection d'un véhicule non légitime

Ainsi, on peut conclure que notre système est sécurisé contre l'attaque d'usurpation d'identité.

7.2.3 Attaque de l'homme au milieu :

Avant l'attaque l'homme au milieu:

On peut apercevoir l'impact de l'attaque de l'homme au milieu via la table NDP (Neighbor Discovery Protocol). Avant de lancer l'attaque, on observe les deux figures 31 et 32 qui illustrent respectivement le contenu de la table NDP du véhicule et de la station de charge.

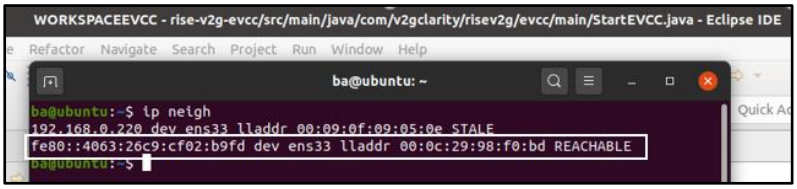


Figure 31 La table NDP du véhicule avant l'attaque MITM

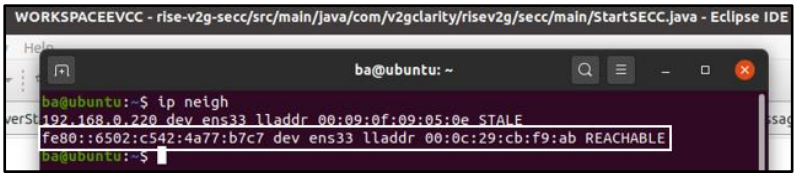


Figure 32 La table NDP de la station de charge avant l'attaque MITM

Dans la table NDP du véhicule électrique EV, on a l'adresse IPV6 et l'adresse MAC de la station se charge (SECC) et dans la table NDP de la station de charge, on a l'adresse IPV6 et l'adresse MAC de l'EV.

Après l'attaque l'homme au milieu:

Après l'exécution de l'attaque de l'homme au milieu sur les deux machines, on observe dans la figure 33 ci-dessous une contamination au niveau des deux tables NDP. Au niveau de la table du

véhicule, les deux adresses; celle de la borne et celle de l'attaquant, sont en correspondance avec la même adresse MAC (adresse MAC de l'attaquant).

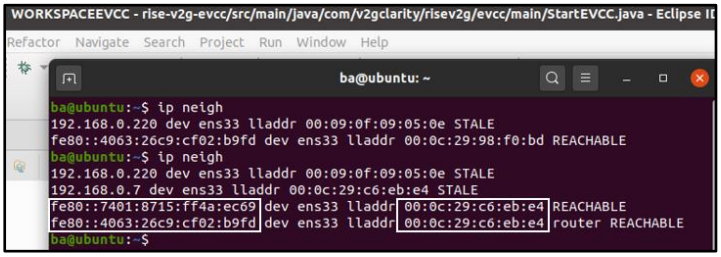


Figure 33 La table NDP du véhicule après l'attaque MITM

Dans la figure 34 ci-dessous, on remarque au niveau de la borne de recharge, une contamination de la table NDP. Donc, l'attaquant a pu impacter la table NDP.

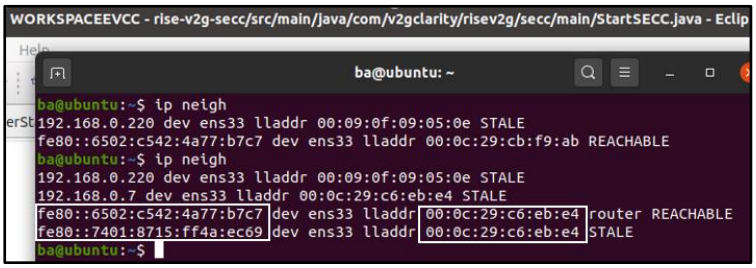


Figure 34 La table NDP de la station de charge après l'attaque MITM

Résultats après application de la solution proposée :

Après avoir appliqué notre solution et relancé l'attaque, on remarque au niveau de la figure 35 que dans la table NDP du véhicule, l'adresse MAC correspondante à l'adresse IPV6 de la borne n'a pas pu être impactée par l'attaquant. Et au niveau de la figure 36, on remarque que dans la table NDP de la borne, l'adresse MAC correspondante à l'adresse IPV6 du véhicule n'est pas impactée également. On peut voir aussi que les adresses MAC et IPV6 sont rendues permanentes durant la communication pour les deux entités.

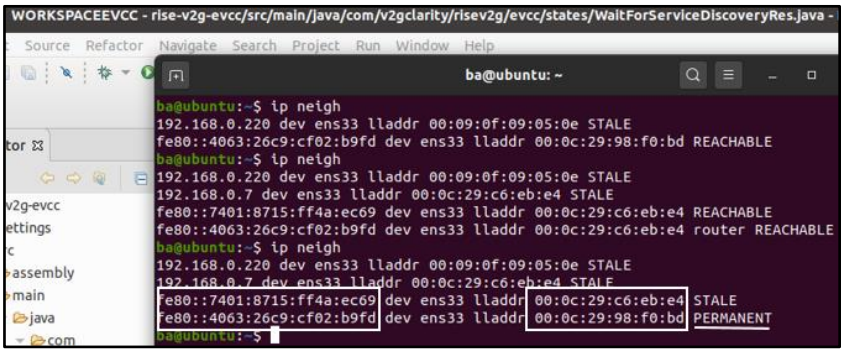


Figure 35 La table NDP du véhicule après application de la solution contre MITM

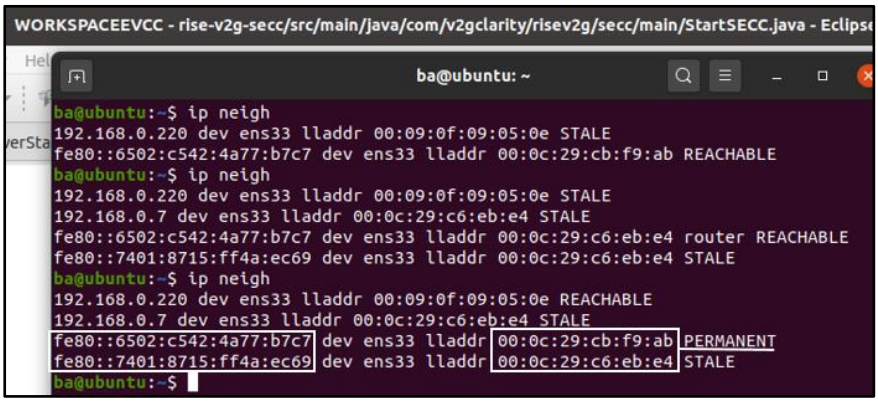


Figure 36 La table NDP de la station de charge après application de la solution MITM

Par ce fait, on peut conclure que notre solution protège la communication contre cette attaque.

7.3 Performance du système :

Les performances du système dépendent du temps d'exécution et de l'énergie consommée par ce dernier, plus le temps d'exécution est lent et plus la consommation de l'énergie augmente. Pour notre système, le temps moyen d'authentification pour 5 simulations entre une station de charge et 20 véhicules, en l'absence d'attaque, est de (0,0738 s). Le tableau 3 ci-dessous présente les différents temps d'authentification de 3 travaux issus de la littérature. Le temps obtenu par nos simulations atteste que notre système d'authentification est léger, rapide, et consomme moins d'énergie en calcul.

Auteurs	Temps nécessaire à l'authentification (seconde)
Nicanfar et al. [52]	63.77
Tsai et al. [52]	23.22
Xia and Wang.[52]	0.085
Schéma proposé	0.0738

Tableau 3 Tableau comparatif des temps d'authentification des systèmes proposés

7.4 Conclusion :

Dans ce chapitre, nous avons présenté les résultats liés à la modélisation et la simulation en utilisant respectivement les outils Tamarin-Prover et Rise-V2G. Les résultats issus de la modélisation ont montré que les échanges établis entre les différentes entités du réseau V2G ont été sécuritaires. Pour la simulation, on a pu tester notre système contre trois attaques différentes : l'attaque DOS, l'attaque d'usurpation d'identité et l'attaque de l'homme au milieu. Les résultats révèlent que les modifications apportées, telles que : le protocole d'authentification proposé contre l'attaque de l'usurpation d'identité, le maintien des adresses IP et MAC du véhicule et la borne

stockée de manière permanente durant la communication proposée contre l'attaque MITM, et le rejet de requêtes spécifiques suite à la détection d'un trafic inhabituel en provenance d'un véhicule malveillant proposée contre l'attaque DOS, ont pu rendre notre système plus robuste et sécuritaire.

Enfin concernant les performances du système, ce dernier s'est avéré léger, rapide, et il consomme moins d'énergie en calcul comparativement à 3 autres protocoles issus de la littérature.

Chapitre 8 Conclusion générale

Dans le but d'assurer la sécurité des réseaux V2G et d'améliorer les performances liées à l'énergie consommé par les calculs, nous avons dans le cadre de ce mémoire proposé et réalisé un système de sécurité portant sur un schéma d'authentification léger basé sur la norme ISO 15118 et l'utilisation de la technologie blockchain.

Notre système intègre quatre chaines de blocs (blockchains) de deux types différents, deux blockchains sont publiques et deux sont privés. L'accessibilité à ces blockchains est définie selon la sensibilité des informations contenues dans leurs blocs respectifs. Plus les informations stockées sont sensibles, plus les accès sont restreints de sorte que seulement les entités autorisées peuvent y effectuer des opérations. Chaque bloc d'une blockchain est référencé par un indexe unique représentant les informations d'un véhicule. Les véhicules entamant une opération de première communication avec la station de charge ou une opération de chargement/déchargement n'auront qu'à transmettre l'index et les informations nécessaires qui ne sont pas sensibles et qui ne mettent pas en risque la vie privée du véhicule. Ce qui permet de sécuriser la communication et d'alléger les échanges entre la borne et les véhicules qui sont limités en ressources de stockage et de calcul.

Pour notre modélisation, on a utilisé l'outil Tamarin-Prover avec lequel on a analysé la sécurité des échanges entre les entités participantes. Ensuite, avec l'outil RISEV2G, on a implémenté notre schéma d'authentification, les quatre blockchains ainsi que les solutions de sécurité proposées.

Les résultats issus de la modélisation ainsi que des simulations ont démontré que notre système est fiable et assure la disponibilité, la confidentialité, la non-répudiation et l'intégrité. Les simulations des différentes attaques de sécurité comme : DOS, MITM, et l'attaque d'usurpation d'identité ont montré aussi que notre système est sécurisé et robuste. Du côté des performances, notre système s'est révélé rapide et consomme moins de temps et d'énergie pour faire les calculs comparés à d'autres travaux issus de la littérature.

Comme perspective, on propose d'utiliser la blockchain hyperleader fabric sur notre système pour les différents avantages qu'elle offre comme la rapidité et la flexibilité. Notre intérêt se pose également sur la technologie NTF appelée aussi certificat de propriété, qui permet de stocker et de numériser les droits d'auteurs. On pourrait les utiliser pour des opérations d'authentifications et pour stocker les certificats des véhicules électriques ainsi que ceux des stations de charges de façon unique. Ensuite, on pourrait l'associer à une blockchain qui coûterait le moins en ressources de calcul et en énergie.

Références

[1]. Chimie, CultureSciences. (2015). *Les carburants : une source d'énergie chimique*. Retrieved mai 2022 from https://culturesciences.chimie.ens.fr/thematiques/chimie-organique/synthese-et-retrosynthese/les-carburants-une-source-d-energie-chimique

[2]. Canada, Gouvernement du. (2017). *Les carburants et la pollution atmosphérique*. Retrieved mai 2022 from https://www.canada.ca/fr/sante-canada/services/sante-environnement-milieu-travail/carburants-pollution-atmospherique.html

[3]. Canada, Gouvernement du. (2014). *Smog : causes et effets*. Retrieved mai 2022 from https://www.canada.ca/fr/environnement-changement-climatique/services/pollution-atmospherique/enjeux/smog-causes-effets.html

[4]. *Pic pétrolier : à quand la fin du pétrole ?* (2021). Retrieved janvier 2022 from https://finance-heros.fr/pic-petrolier/#:~:text=Le%20pic%20p%C3%A9trolier%20est%20le,sur%20le%20prix%20du%20p%C3%A9trole

[5]. *La voiture électrique : une histoire ancienne*. (2020). Retrieved janvier 2022 from https://eua.hypotheses.org/4185

[6]. *Bâtir une économie verte : le gouvernement du Canada exigera que la totalité des voitures et camions légers à passagers vendus soit des véhicules zéro émission d'ici 2035*. (2021). Retrieved mars 2022 from https://www.canada.ca/fr/transports-canada/nouvelles/2021/06/batir-une-economie-verte-le-gouvernement-du-canada-exigera-que-la-totalite-des-voitures-et-camions-legers-a-passagers-vendus-soit-des-vehicules-zer.html

[7]. *The basics of Plug & Charge*. (2021). Retrieved fevrier 2021 from https://www.switch-ev.com/knowledgebase/basics-of-plug-and-charge

[8]. *Voiture électrique : le protocole Plug & Charge accélère*. (2021). Retrieved mai 2022 from https://www.automobile-propre.com/breves/voiture-electrique-le-protocole-plug-charge-accelere/

[9]. Neetesh Saxena, Member, IEEE, and Bong Jun Choi, Member, IEEE. (2016). Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, *11*, 15. https://ieeexplore.ieee.org/document/7414504

[10]. 15118-1, ISO. (2013). Road vehicles — Vehicle to grid communication interface —

In *Part 1: General information and use-case definition*

(https://www.iso.org/standard/55365.html).

[11]. Japan, Society of Automotive Engineers of. (2014). Industry Standards. In (https://www.jsae.or.jp/en/publications/yearbook_e/2014/docu/28_industry_standards.pdf).

[12]. Paul Danquah, Henoch Kwabena-Adade. (2020). Public Key Infrastructure: An Enhanced Validation Framework. *Journal of Information Security 11*. https://doi.org/10.4236/jis.2020.114016

[13]. 15118-2, ISO. (2014). Road vehicles Vehicle-to-Grid Communication Interface In *Part 2: Network and application protocol requirements*

(https://www.iso.org/standard/55366.html).

[14]. Cisco. (2013). *Formats de données PKI*. cisco. Retrieved mai 2022 from https://www.cisco.com/c/fr_ca/support/docs/security/vpn-client/116039-pki-data-formats-00.html

[15]. Globe, Pki. *Inroduction to PKI Models*. Retrieved mai 2022 from http://www.pkiglobe.org/pki_models.html

[16]. Balachandra Muniyal, Prema K.V, Sushma Nayak. (2012). International Journal of Computer Applications (0975 – 8887) Volume 41– No.9, March 2012 7 Creating Virtual Hierarchy in Peer-to-Peer PKI to Simplify Certificate Path Discovery. *ResearchGate*, *41*. https://www.researchgate.net/publication/258651000_Creating_Virtual_Hierarchy_in_Peer-to-Peer_PKI_to_Simplify_Certificate_Path_Discovery

[17]. Canada, Gouvenement Of. (2011). *Guideline on the Management of Public Key Infrastructure in the Government of Canada*. Retrieved avril 2022 from https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=20008

[18]. Afirev. (2019). Recommandation sur la sécurité de la communication pour l'itinérance de la recharge des véhicules électriques. *Afirev*, https://www.afirev.fr/wp-content/uploads/2019/11/AFIREV_Reco_PKI_ISO15118_2019-Fr.pdf.

[19]. VARRETTE, sébastien. *Cours "Cryptographie & Securit´e R´eseau" Master Info Universit´e de Yaound´*. Retrieved mai 2022 from https://varrette.gforge.uni.lu/teachings/crypto/intro_PKI.pdf

[20]. Huirui Han, Mengxing Huang, Yu Zhang & Uzair Aslam Bhatti (2018). *An Architecture of Secure Health Information Storage System Based on Blockchain Technology* International Conference on Cloud Computing and Security, https://link.springer.com/chapter/10.1007/978-3-030-00009-7_52#citeas

[21]. Lars, Ludovic. (2019, 2020). *CRYPTOAST Qu'est-ce qu'un bloc dans la technologie blockchain ?* Retrieved mai 2022 from https://cryptoast.fr/bloc-blockchain-crypto-explication/#:~:text=Un%20bloc%20commence%20toujours%20par,pour%20un%20changement%20du%20protocole

[22]. Lars, Ludovic. (2020, 2020). *CRYPTOAST Les arbres de Merkle dans Bitcoin*. Retrieved mai 2022 from https://cryptoast.fr/arbres-merkle-bitcoin/

[23]. blockchain.com. (2022). *Bitcoin explorer* Retrieved mai 2022 from https://www.blockchain.com/btc/block/000000000000000000059331d124ada55a67200fefa511c782bbc175b9cfcff?page=2

[24]. Associates, 2AB &. (2022). *BLOCKCHAIN : FONCTIONNEMENT DU MINAGE EN 7 ÉTAPES*. Retrieved mai 2022 from http://www.ab-consulting.fr/blog/blockchain/minage-7-etapes#:~:text=Dans%20le%20cas%20classique%20(Bitcoin,non%20pr%C3%A9sentes%20dans%20la%20blockchain

[25]. Dickson, Ben. (2018, 2021). *Everything you need to know about bitcoin wallets*. Retrieved mai 2022 from https://www.dailydot.com/debug/bitcoin-wallets-cryptocurrency-hardware/

[26]. Journalducoin. (2022). *LES PRINCIPAUX PROTOCOLES DE CONSENSUS*. Retrieved mai 2022 from https://journalducoin.com/lexique/blockchain-consensus-pow-pos-dpos/#:~:text=Un%20consensus%20blockchain%20suit%20des,r%C3%A9seau%20pour%20pouvoir%20%C3%AAtre%20valid%C3%A9e

[27]. Peh, Bernard. (2018). *What are Public, Private and Hybrid Blockchains?* Retrieved mai 2022 from https://medium.com/@blockchain101/what-are-public-private-and-hybrid-blockchains-e01d6e21eb41

[28]. Equisafe. (2019). *Enfin comprendre la différence entre Blockchain Privée et Blockchain Publique !* Retrieved mai 2022 from https://medium.com/@Equisafe/enfin-comprendre-la-diff%C3%A9rence-entre-blockchain-priv%C3%A9e-et-blockchain-publique-c9cf4eb003bd

[29]. Investopedia. (July 24, 2022). *Hyperledger Fabric*. JAKE FRANKENFIELD. Retrieved decembre 2022 from https://www.investopedia.com/terms/h/hyperledger-fabric.asp

[30]. Geroni, Diego. (2021). *Hybrid Blockchain: The Best Of Both Worlds*. Retrieved mai 2022 from https://101blockchains.com/hybrid-blockchain/

[31]. team, LCX. (2022). *A Guide to Quorum Blockchain*. LCX team. Retrieved novembre 2022 from https://www.lcx.com/a-guide-to-quorum-blockchain/

[32]. Digiconomist. (2021, 2022). *Bitcoin Energy Consumption Index*. Retrieved mai 2022 from https://digiconomist.net/bitcoin-energy-consumption

[33]. naturelles, Ministère de l'Énergie et des Ressources. *Consommation d'électricité*. Gouvernement du Québec. Retrieved aout 2022 from https://mern.gouv.qc.ca/energie/statistiques-energetiques/consommation-electricite/#:~:text=La%20consommation%20qu%C3%A9b%C3%A9coise%20d'%C3%A9lectricit%C3%A9,2%20%25%20par%20rapport%20%C3%A0%202017.

[34]. Bobée, Floriane. (2022). *PROOF OF STAKE : DÉFINITION ET EXPLICATION*. Retrieved mai 2022 from https://journalducoin.com/lexique/proof-of-stake/

[35]. Campus, Greenbull. (2021). *Preuve d'enjeu et preuve de travail, des protocoles bien distincts*. Retrieved mai 2022 from https://greenbull-campus.fr/immobilier/guide/patrimoine/diversifier/preuve-enjeu-ou-preuve-de-travail

[36]. Bouvet, Rémi. (2021). *La consommation d'énergie de la blockchain Ethereum va diminuer de 99% grâce au Proof-of-Stake et à ETH 2.0*. Retrieved fevrier 2022 from https://www.clubic.com/antivirus-securite-informatique/cryptage-cryptographie/crypto-monnaie/actualite-372300-la-consommation-d-energie-de-la-blockchain-ethereum-va-diminuer-de-99-grace-au-proof-of-stake-et-a-eth-2-0.html

[37]. p3c-bot. (2019). *Change the ETC Proof of Work Algorithm to Keccak-256* Retrieved mai 2022 from https://github.com/ethereumclassic/ECIPs/issues/13

[38]. *Tout sur les algorithmes de hachage et leur fonctionnement*. https://www.frank-gehry.com/7401/#:~:text=Le%20hachage%20et%20son%20utilisation,m%C3%A9moire%20pour%20le%20calcul%20mat%C3%A9riel

[39]. *Qu'est-ce qui relie la clé publique à l'adresse Bitcoin ?* (2010-2022). Retrieved janvier 2022 from https://bitcoin.fr/qu-est-ce-qui-relie-la-cle-publique-a-la-cle-privee/#:~:text=La%20signature%20des%20transactions%20Bitcoin,cl%C3%A9%20publique)%20n%C3%A9cessaire%20aux%20signatures.

[40]. RiskInsight. (2016, janvier 2022). Peut-on avoir une confiance sans limite dans la Blockchain ? https://www.riskinsight-wavestone.com/2016/09/blockchain-peut-on-avoir-confiance-sans-limite/#:~:text=La%20cr%C3%A9ation%20de%20cas%20d,attaques%20pr%C3%A9sent%C3%A9es%20t%C3%A9moignent%20du%20contraire

[41]. HAYES, ADAM. (2022). *blockchain explained*. Retrieved mai 2022 from https://www.investopedia.com/terms/b/blockchain.asp

[42]. Crochet-Damais, Antoine. (2017). *Comment la blockchain révolutionne la sécurité informatique*. Retrieved mai 2022 from https://www.journaldunet.com/solutions/dsi/1196920-comment-la-blockchain-revolutionne-la-securite-informatique/

[43]. GUO Chuangxin, HUANG Xiaobo, ZHU Chengzhi, WANG Xueping and CAO Xiu. (2019). *Distributed Electric Vehicle Control Model Based on Blockchain* Asia Conference on Power and Electrical Engineering https://www.researchgate.net/publication/334375090_Distributed_Electric_Vehicle_Control_Model_Based_on_Blockchain

[44]. Schmeck, Kaibin Bao · Hristo Valev · Manuela Wagner · Hartmut. (2017). A threat analysis of the vehicle-to-grid charging protocol. *Springer-Verlag GmbH Germany*, 10.

[45]. Wang, Qinglong, Ou, Min, Yang, Yun, & Duan, Zongtao. (2020). Conditional Privacy-Preserving Anonymous Authentication Scheme With Forward Security in Vehicle-to-Grid Networks. *IEEE*, *8*, 10.

[46]. Shuai Wang, Baoyi Wang, Shaomin Zhang. (2018). A Secure Solution of V2G Communication Based on Trusted Computing. 2018 12th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID),

[47]. Yinghui Zhang, Jian Zou, Rui Guo. (2021). Efficient privacy-preserving authentication for V2G networks. *SPRINGER*.

[48]. Luis F.A. Roman, Paulo R.L. Gondim, Jaime Lloret. (2019). Pairing-based authentication protocol for V2G networks in smart grid, . *ScienceDirect Ad Hoc Networks*, *90*. https://doi.org/10.1016/j.adhoc.2018.08.015.

[49]. Gang Shen, Yixin Su, Mingwu Zhang. (2018). Schéma de partage de données sécurisé et basé sur l'adhésion dans les réseaux V2G. *IEEE*, *6*, 11.

[50]. Google. *Working together to detect maliciously or mistakenly issued certificates.* Certificate Transparency Retrieved aout 2021 from https://certificate.transparency.dev/

[51]. Madala, D S V, Jhanwar, Mahabir Prasad, & Chattopadhyay, Anupam. (2018). Certificate Transparency Using Blockchain. IEEE International Conference on Data Mining Workshops (ICDMW),

[52]. S. Aggarwal, N. Kumar and P. Gope. (Oct. 2021). An Efficient Blockchain-Based Authentication Scheme for Energy-Trading in V2G Networks. *IEEE Transactions on Industrial Informatics*, *17*(10), 6971-6980.

[53]. Iqbal, A., Rajasekaran, AS, Nikhil, GS, & Azees, M. (2021). A Secure and Decentralized Blockchain Based EV Energy Trading Model Using Smart Contract in V2G Network. *IEEE Access 9*, 75761-75777.

[54]. Wang, H., Wang, Q., He, D., & Liu, Q. Li and Z. (April 2019). BBARS: Blockchain-Based Anonymous Rewarding Scheme for V2G Networks. *IEEE Internet of Things Journal*, *6*(2), 3676-3687.

[55]. Khan, Prince Waqas, & Byun, Yung-Cheol. (July 2021). Blockchain-Based Peer-to-Peer Energy Trading and Charging Payment System for Electric Vehicles. *MDPI*, *13*(14), 7962.

[56]. Salabat, Khan & All. (may 2020). SCM: Secure and accountable TLS certificate management. *John Wiley & Fils*, 23.

[57]. A. Garba, Z. Chen, Z. Guan, G. Srivastava. (avril-juin 2021). LightLedger: A Novel Blockchain-Based Domain Certificate Authentication and Validation Scheme. *IEEE Transactions on Network Science and Engineering*, *8*(2), 1698-1710.

[58]. all, Kuljeet Kaur &. (2019). A Secure, Lightweight, and Privacy-Preserving Authentication Scheme for V2G Connections in Smart Grid. *IEEE SociaL and mobile connected Smart objects*, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8845140.

[59]. A new type of blockchain for secure message exchange in VANET. (May 2020). *ScienceDirect*, *6*(2), 177-186.

[60]. Li, Hui, Pei, Lishuang, Liao, Dan, Soleil, Gang, & Xu, Du. (2019). Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET. *Springer Peer-to-Peer Netw. Appl*, *12*, 1178–1193

[61]. Sowmya Kudva, Shahriar Badsha, Shamik Sengupta, Ibrahim Khalil, Albert Zomaya. (2021). Towards secure and practical consensus for blockchain based VANET. *Information Sciences*, *545*(0020-0255), 170-187.

[62]. Ikram, Ali, Mwitende, Gervais, Emmanuel, Ahene, & Fagen, Li. (2019). A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *Journal of Systems Architecture*, *99*(101636).

[63]. D, Zheng, C, Jing, R, Guo, S, Gao, & L, Wang. (2019). A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs. *IEEE Acces*, *7*, 117716-117726.

[64]. Youssef, Inedjaren, Mohamed, Maachaoui, Besma, Zeddini, & Jean-Pierre, Barbot. (2021). Blockchain-based distributed management system for trust in VANET. *Vehicular Communications*, *30*(100350).

[65]. Shrestha, R., Bajracharya, R., & Nam, S. Y. (2018). Blockchain-based Message Dissemination in VANET. IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu (Nepal).

[66]. Prover, Tamarin. *Tamarin Prover*. Retrieved mai 2022 from https://tamarin-prover.github.io/

[67]. *RISE-V2G*. (2020). Retrieved mars 2021 from https://github.com/SwitchEV/RISE-V2G