Application de la technologie Blockchain pour l'internet des objets

Moez Krichen

Application de la technologie Blockchain pour l'internet des objets

Moez Krichen

Laboratoire ReDCAD, Université de Sfax, Tunisie
moez.krichen@redcad.org

Résumé. La blockchain est une technologie de pointe qui a changé la façon dont les gens communiquent et commercent. Il s'agit d'une chaîne de blocs dans un réseau peer-to-peer (P2P) distribué et décentralisé qui stocke des informations avec des signatures numériques. Cette méthode a d'abord été utilisée pour développer des monnaies numériques telles que Bitcoin et Ethereum. Cependant, certaines recherches et études industrielles récentes se sont concentrées sur les perspectives que la blockchain présente dans une variété d'autres domaines d'application afin de tirer parti des qualités fondamentales de la technologie, telles que la décentralisation, la persistance, l'anonymat et l'audibilité. Dans cette étude, nous donnons une évaluation approfondie de l'utilisation de la blockchain pour l'Internet des objets (IoT). Nous présentons également les principaux obstacles de la Blockchain afin de permettre aux chercheurs de les résoudre et d'améliorer l'utilisation de la technologie.

1 Introduction

La blockchain (18) est un paradigme révolutionnaire qui a introduit de nouvelles notions pour le partage sécurisé des données et des informations. Cette technologie actuelle comprend une chaîne de blocs qui permet le stockage sécurisé de toutes les transactions engagées sur des réseaux partagés (38). Les hachages cryptographiques, les techniques de consensus distribué et les signatures numériques font partie des technologies de base utilisées pour atteindre cet objectif. Toutes les transactions sont décentralisées, éliminant ainsi le besoin d'intermédiaires pour les authentifier ou les vérifier. La décentralisation, la persistance, l'anonymat et l'auditabilité sont quelques-unes des principales caractéristiques de la blockchain (14).

La blockchain a été initialement proposée pour prendre en charge la crypto-monnaie bien connue Bitcoin (39). Cependant, au cours des dernières années, la blockchain a été adoptée dans plusieurs nouveaux domaines bien au-delà des crypto-monnaies(34; 1; 37), notamment la santé (46; 45), le transport intelligent (12; 4) et l'IoT. (8). En effet, grâce à sa capacité à accroître l'équité et la transparence et à aider les organisations à économiser de l'argent et du temps, cette technologie influence un large éventail d'industries (3; 48) allant des activités de divertissement individuelles de base à la gestion des affaires critiques et sensibles de gouvernements et d'États entiers.

Nos principales contributions à ce travail se concentrent sur les activités de recherche récentes liées à l'inclusion de la technologie blockchain dans les applications modernes en mettant l'accent sur les défis, avantages, limites et défis correspondants. En particulier, nous passons en revue l'architecture de la blockchain dans la Section 2 puis nous présentons une brève revue sur l'utilisation de la blockchain pour l'Internet des Objets (IoT) (Section 3). La section 4 recense les principaux défis ouverts liés à l'utilisation de la technologie Blockchain. La section 5 est une conclusion générale de l'article.

2 Architecture Blockchain

Une blockchain est une collection en expansion continue de blocs de données liés entre eux pour former une longue chaîne (40) comme décrit dans la figure **??**. Ce réseau de blocs de données connectés représente un registre distribué qui est diffusé sur un réseau peer-to-peer (25). Un registre distribué peut être considéré comme une collection de données numériques synchronisées, répliquées, distribuées et partagées via un réseau peer-to-peer. Chaque appareil lié au réseau maintient la dernière version du grand livre commun, c'est-à-dire que chaque pair du réseau a une copie du grand livre qui est identique à l'autre.

Le grand livre se caractérise principalement par sa sécurité et la base de données ne peut être étendue qu'en ajoutant de nouveaux blocs à la chaîne. Les modifications apportées aux enregistrements déjà enregistrés dans la chaîne sont impossibles en termes de calcul. Par conséquent, l'un des principaux avantages du grand livre distribué décrit est sa nature décentralisée. En effet, il n'y a pas d'autorité centrale qui contrôle le grand livre. Cependant, chaque nœud met à jour son registre lorsqu'un nouveau bloc est ajouté à la blockchain, en utilisant un mécanisme de consensus conjoint (13).

De plus, dans la blockchain, la sécurité des données est renforcée par leur cryptage à l'aide d'algorithmes asymétriques (27). Dans ce type de cryptage, l'émetteur et le récepteur ont une paire de clés composée d'une clé publique et d'une clé privée (44). La clé privée est exclusivement accessible aux nœuds qui l'ont créée, tandis que la clé publique est librement diffusée sur tout le réseau. L'expéditeur crypte les données à l'aide de la clé publique du destinataire. Étant donné que les données sont chiffrées à l'aide de la clé publique du destinataire, elles ne peuvent être déchiffrées qu'à l'aide de la clé privée du destinataire.

De plus, dans le cas de l'envoi de transactions sur un réseau blockchain, une transaction n'est réputée terminée qu'après avoir été signée numériquement. La transaction est signée par l'expéditeur à l'aide de sa clé privée. Pour le destinataire, l'authenticité de la transaction, c'est-à-dire l'identité de l'expéditeur, peut être vérifiée à l'aide de la clé publique associée (appartenant à l'expéditeur). Toutes les transactions sont automatiquement vérifiées et authentifiées par les nœuds, et le réseau rejette toute transaction non authentifiée. Veuillez noter que sur un réseau blockchain, une transaction originale minée est irréversible (35).

Il est difficile d'altérer les données contenues dans les blocs grâce aux qualités cryptographiques de la Blockchain. Pratiquement, les blocs sont connectés via une référence de hachage puisque chaque bloc suivant porte la valeur de hachage du bloc précédent

en plus de la valeur de hachage du bloc réel. La génération d'une valeur de hachage est réalisable à l'aide d'un algorithme de hachage cryptographique mathématique et sophistiqué, qui accepte tout type d'entrée et génère un nombre de longueur fixe appelé valeur de hachage. La principale caractéristique d'une fonction de hachage est que si une seule fraction de l'entrée est modifiée, la valeur entière de la sortie sera modifiée (48).

Par conséquent, si un attaquant tente d'éditer des données dans le bloc 1 (B1), par exemple, la valeur de hachage de ce bloc (B1) sera modifiée dans le bloc suivant (B2), et donc l'intrus devra modifier la valeur de hachage de ce bloc. De plus, comme B2 porte le hachage de B1, toute modification du hachage modifiera la valeur de hachage de B2 dans B3. Par conséquent, si quelqu'un veut modifier un bloc, il doit modifier les données de tous les blocs suivants sur la Blockchain. De plus, même si la valeur de hachage d'un bloc est connue, le calcul de l'entrée de la fonction de hachage est difficile en raison de la fonctionnalité non inversible de la fonction de hachage (44).

La question suivante est de savoir comment ajouter de nouveaux blocs au réseau. En effet, des nœuds appelés "Miners" sont chargés de construire de nouveaux blocs dans la blockchain (35). Le travail des mineurs consiste à mettre à jour les enregistrements du grand livre public de la blockchain à partir des transactions précédentes. Tout nœud de réseau peut être un mineur. Il faut des heures aux mineurs pour créer un nouveau bloc car ils doivent résoudre une énigme mathématique appelée "Proof of Work" (PoW). Plusieurs mineurs peuvent travailler en parallèle pour ajouter un nouveau bloc. Néanmoins, un seul mineur peut ajouter un nouveau bloc à la fois. Le premier mineur à résoudre le problème PoW peut exploiter ce nouveau bloc. Pour résoudre le problème du PoW minier, une énorme puissance de calcul est nécessaire. Nous pouvons décomposer l'ensemble du processus en plusieurs étapes :

- Pour commencer à miner un nouveau bloc, un mineur rassemble les transactions du réseau partagé et les organise dans un bloc.
- Le mineur vérifiera la valeur de hachage précédente de la Blockchain et la déposera avec les transactions dans le nouveau bloc prévu.
- Le mineur va récupérer et enregistrer dans le même bloc une variable appelée "nonce". Cette valeur variable peut être modifiée à tout moment par le mineur.
- Le mineur va maintenant enquêter sur le puzzle PoW du réseau. Le problème consiste à trouver, pour tout le nouveau bloc, une valeur de hachage spéciale commençant par plusieurs zéros (par exemple, 0000000000XXXXX). Cette valeur de hachage spéciale peut être trouvée en modifiant la valeur nonce, qui est le seul paramètre que le mineur peut modifier. Une fois que le mineur découvre le même nombre de zéros de début pour une valeur nonce donnée, il peut diffuser la réponse sur le réseau et démontrer le succès de l'extraction d'un nouveau bloc. Notez que le nombre de zéros successifs indique le niveau de difficulté de minage.

Les nœuds de type mineurs sont également chargés de vérifier toutes les données contenues dans un bloc. À cette fin, les données d'un bloc sont enregistrées sous la forme d'un arbre Merkle, qui représente une structure de données particulière sous la forme d'un arbre basé sur le hachage. Les arbres simplifient la vérification des données. Pensez à ne pas utiliser la structure de l'arbre de Merkle et au lieu d'utiliser la fonction de

hachage de toutes les transactions. Si une seule transaction est modifiée, le résultat de hachage entier sera modifié, ce qui rendra impossible la détection des données modifiées. Mais en utilisant la structure particulière de l'arbre de Merkle, nous pouvons voir à n'importe quelle fraction de l'arbre quelle partie fournit la valeur de hachage erronée. Supposons qu'un attaquant modifie la transaction Tx3. En conséquence, nous pouvons facilement détecter que seul le côté droit de l'arbre Merkle donne des sorties de hachage incorrectes. Étant donné que les valeurs de hachage de Tx3 et Tx4 seront erronées, nous n'avons pas besoin de vérifier Tx1 et Tx2. Par conséquent, l'arbre de Merkle est extrêmement utile pour la vérification des données dans les systèmes distribués peer-to-peer (36).

3 Blockchain pour l'Internet des Objets

L'Internet des objets (IoT) (17; 11) est la liaison d'appareils intelligents pour la collecte de données et la prise de décision intelligente. Pourtant, l'IoT est sujet à des risques de confidentialité et de sécurité en raison de l'absence de mesures de sécurité inhérentes. L'architecture dispersée et centralisée de l'Internet des objets est un défi important. Chaque nœud d'une infrastructure IoT est généralement un point de faiblesse potentiel qui pourrait être utilisé pour lancer des cyberattaques. La confidentialité et l'authentification des données sont permanentes et constituent probablement l'une des menaces les plus graves. Les données IoT pourraient être piratées et utilisées à mauvais escient si la sécurité des données n'est pas établie (19). L'intégrité des données est un autre problème pour l'IoT. Les systèmes d'aide à la décision sont l'une des applications IoT les plus importantes. Par conséquent, la protection du système contre les attaques par injection, qui tentent d'insérer de fausses mesures et donc d'avoir un impact sur la prise de décision, est essentielle. Pour les systèmes automatisés tels que les secteurs manufacturiers et les réseaux de véhicules (10) qui gèrent des données en temps réel, la disponibilité est cruciale. L'inclusion d'une piste d'audit vérifiable publiquement qui ne dépend pas d'un tiers de confiance est essentielle, car elle résout tous ces problèmes. La blockchain peut aider à résoudre les principaux problèmes de sécurité dans l'IoT grâce à sa fonctionnalité de "sécurité par construction" (26).

L'intégration de crypto-monnaies pour le paiement est l'une des applications les plus importantes de la blockchain pour les réseaux électriques intelligents. BASNederland a été la première entreprise à utiliser Bitcoin pour le paiement des factures d'énergie. Cela a incité de nombreuses autres entreprises à développer des services de facturation et de comptage basés sur la blockchain, plusieurs d'entre elles offrant des incitations aux consommateurs qui paient avec la crypto-monnaie. Par exemple : Bankymoon en Afrique du Sud utilisant Bitcoin, Spectral et Alliander aux Pays-Bas utilisant Juliette, PowerLedger en Australie utilisant Sparkz, LO3Energy et ConsenSys aux États-Unis utilisant Ethereum, etc.

Les véhicules électriques peuvent être considérés comme des terminaux mobiles du réseau électrique qui fournissent des services clés. C'est ce qu'on appelle la technologie V2G, et elle a le potentiel d'augmenter la fiabilité, l'efficacité et la stabilité du réseau électrique. D'autre part, les véhicules électriques ne sont pas correctement connectés aux réseaux électriques intelligents, et il existe plusieurs problèmes tels que les pénuries

d'énergie, les risques de sécurité et les fuites de données. Dans ce contexte, une charge de charge excessive et une tension instable dans les véhicules électriques peuvent être résolues grâce à la technologie blockchain, comme indiqué dans (28). De plus, l'utilisation de la blockchain pour connecter les réseaux électriques intelligents et les véhicules électriques peut réaliser une optimisation des coûts grâce à des contrats intelligents. De plus, l'utilisation de la technologie blockchain pour connecter les réseaux électriques intelligents et les véhicules électriques pourrait réduire les coûts en utilisant des contrats intelligents, comme proposé dans (29).

Bien que la technologie blockchain pour les réseaux électriques intelligents semble prometteuse, la conversion complète à cette nouvelle technologie reste difficile, comme cela a été prouvé précédemment. La mise en œuvre de la blockchain dans le réseau électrique intelligent, par exemple, entraîne d'énormes coûts d'infrastructure pour la réarchitecture des réseaux de grille existants, ce qui empêche les opérateurs de réseau d'inclure la blockchain dans leur structure de réseau.

La blockchain est le casse-tête final pour résoudre les problèmes de confidentialité et de fiabilité de l'IoT. Les caractéristiques inhérentes de confiance, autonomes et décentralisées de la blockchain la rendent adaptée à divers scénarios. La technologie Blockchain, par exemple, peut stocker un enregistrement permanent des gadgets intelligents (21). De plus, les contrats intelligents peuvent permettre aux appareils intelligents de fonctionner de manière autonome, évitant ainsi le besoin d'un contrôle humain ou d'une autorité centralisée. De plus, la blockchain peut établir un moyen sécurisé permettant aux appareils intelligents de communiquer entre eux (41).

La contribution de (42) peut être considérée comme une solution générique pouvant être utilisée dans n'importe quel domaine de l'environnement IoT. En effet, les auteurs de cet article ont développé un mécanisme qui permettrait aux capteurs d'échanger des Bitcoins contre des données. Chaque nœud a une adresse unique qui correspond à la clé de pub Bitcoin. Lorsqu'un utilisateur a besoin de données d'un capteur après les avoir localisées dans un référentiel de capteurs, il envoie une transaction dirigée vers la clé publique de ce capteur. Le capteur répondra en envoyant une transaction contenant des données au client. Cette stratégie est une extension de la solution fournie dans (47).

Pour résumer, l'utilisation de la blockchain pour les applications IoT offre d'excellents niveaux de sécurité qui empêchent l'accès indésirable aux données. Pourtant, l'évolutivité (30) est toujours une question ouverte car la blockchain peut grossir avec le temps, ce qui rend difficile l'acquisition et la sauvegarde du grand livre.

4 Défis ouverts

Afin de produire des applications basées sur la blockchain plus utilisables et plus performantes, plusieurs difficultés industrielles non résolues doivent être résolues et étudiées plus avant (Tableau 1).

TAB. 1 – *Défis ouverts.*

Avantages de la solution	Lorsqu'elle est appliquée pour remplacer les solutions existantes, la blockchain est une nouvelle technologie qui a le potentiel de déstabiliser le marché en introduisant des moyens révolutionnaires susceptibles de transformer la société. Par conséquent, il est essentiel d'établir si une blockchain est vraiment nécessaire pour une application donnée (43).
Mise en œuvre correcte	Parce que la blockchain est une méthode polyvalente de manipulation de données qui peut être utilisée dans divers systèmes pour diverses raisons, sa mise en œuvre a un certain degré de compréhension ou de maturité concernant son importance et les compromis. Ainsi, son intégration dans différentes applications nécessite une étude approfondie et complète (34).
Mécanisme de test standard	Il est essentiel d'adopter des applications basées sur la blockchain pour divers domaines.
Résilience aux risques de sécurité	La résilience aux risques de sécurité doit être formellement prouvée car la blockchain peut être confrontée à des dysfonctionnements dus à la conception des systèmes ou à des cyberattaques destinées à compromettre sa sécurité avec des applications à grande échelle.
Évolutivité	Ce problème est soulevé car les transactions basées sur la blockchain sont très lentes à être traitées et vérifiées. Le traitement des transactions dépend des performances du système de traitement. Dans (9), les limites des méthodes de mise à l'échelle proposées sont soulignées.
Intégration avec d'autres systèmes	Ce problème a un impact direct sur les organisations désireuses d'adopter des solutions compatibles avec la blockchain. En effet, le processus d'intégration impliquera des coûts liés au changement d'infrastructure, au personnel formé, aux développeurs spécialisés et aux attentes de la direction (9).
Défis énergétiques	L'utilisation de la blockchain nécessitera sans aucun doute une consommation d'énergie bien supérieure à celle habituelle. Ce défi se transforme en un problème environnemental lorsque l'énergie utilisée dépasse la puissance de charge et que l'équipement est pleinement utilisé (7).
Les questions réglementaires	Les réglementations sont extrêmement importantes pour généraliser, réglementer et accepter l'utilisation de solutions compatibles avec la blockchain.
Stockage	L'intégration de la blockchain avec des applications gourmandes en données -telles que celles basées sur l'IoT- pose le problème du stockage des données. En effet, la blockchain stocke les données dans des blocs qui ne peuvent pas supporter un grand volume de données (46; 45).

5 Conclusion

Cette recherche visait à faire la lumière sur certaines études récentes impliquant l'intégration de la technologie blockchain dans le domaine de l'Internet des objets (IoT). Nous avons proposé des exemples de technologies de blockchain connexes pour chaque domaine, en mettant l'accent sur les avantages, les limites et les problèmes associés à chacun. Le tableau 2 résume les solutions qui ont été passées en revue.

Tab. 2 – *Résumé des principaux résultats concernant l'utilisation de Blockchain dans différents domaines.*

Domaine	**Papiers**	**Applications principales**	**Limites et risques**
Internet des objets (IoT)	(19; 10; 26; 21; 41; 42; 47)	1. Stocker et traiter les données en même temps tout en préservant la confidentialité 2. Établir un moyen sécurisé pour que les appareils intelligents communiquent entre eux 3. Permettre aux appareils intelligents de fonctionner de manière autonome 4. Éviter le besoin d'un contrôle humain ou d'une autorité centralisée.	1. L'évolutivité reste une question ouverte car la blockchain peut grossir avec le temps, ce qui rend difficile l'acquisition et la sauvegarde du grand livre.

Par exemple, il serait intéressant d'étudier comment les techniques d'apprentissage automatique (ML) (2; 33; 5) peuvent être utilisées dans le contexte de la technologie Blockchain pour augmenter les niveaux de sécurité et pour augmenter les performances des systèmes basés sur la blockchain considérés. . Il sera également important d'appliquer des approches de test formelles (16; 31; 6; 32; 20; 15) pour les systèmes basés sur la blockchain afin d'améliorer leur qualité et d'augmenter leur robustesse (22; 24; 23).

Références

[1] Joe Abou Jaoude and Raafat George Saade. Blockchain applications–usage in different domains. *IEEE Access*, 7 :45360–45381, 2019.

[2] Qasem Abu Al-Haija, Moez Krichen, and Wejdan Abu Elhaija. Machine-learning-based darknet traffic detection system for iot applications. *Electronics*, 11(4) :556, 2022.

[3] Jameela Al-Jaroodi and Nader Mohamed. Blockchain in industries : A survey. *IEEE Access*, 7 :36500–36515, 2019.

[4] Azza Allouch, Omar Cheikhrouhou, Anis Koubâa, Khalifa Toumi, Mohamed Khalgui, and Tuan Nguyen Gia. Utm-chain : blockchain-based secure unmanned traffic management for internet of drones. *Sensors*, 21(9) :3049, 2021.

[5] Ouissem Ben Fredj, Alaeddine Mihoub, Moez Krichen, Omar Cheikhrouhou, and Abdelouahid Derhab. Cybersecurity attack prediction : a deep learning approach. In *13th International Conference on Security of Information and Networks*, pages 1–6, 2020.

[6] Nathalie Bertrand, Amélie Stainer, Thierry Jéron, and Moez Krichen. A game approach to determinize timed automata. *Formal Methods in System Design*, 46(1) :42–80, 2015.

[7] Sanjeev Kumar Dwivedi, Priyadarshini Roy, Chinky Karda, Shalini Agrawal, and Ruhul Amin. Blockchain-based internet of things and industrial iot : a comprehensive survey. *Security and Communication Networks*, 2021, 2021.

[8] Tarek Frikha, Faten Chaabane, Nadhir Aouinti, Omar Cheikhrouhou, Nader Ben Amor, and Abdelfateh Kerrouche. Implementation of blockchain consensus algorithm on embedded architecture. *Security and Communication Networks*, 2021, 2021.

[9] Md Rafiqul Islam, Muhammad Mahbubur Rahman, Md Mahmud, Mohammed Ataur Rahman, Muslim Har Sani Mohamad, et al. A review on blockchain security issues and challenges. In *2021 IEEE 12th Control and System Graduate Research Colloquium*, pages 227–232. IEEE, 2021.

[10] Rateb Jabbar, Mohamed Kharbeche, Khalifa Al-Khalifa, Moez Krichen, and Kamel Barkaoui. Blockchain for the internet of vehicles : A decentralized iot solution for vehicles communication using ethereum. *Sensors*, 20(14) :3928, 2020.

[11] Rateb Jabbar, Mohammed Shinoy, Mohamed Kharbeche, Khalifa Al-Khalifa, Moez Krichen, and Kamel Barkaoui. Urban traffic monitoring and modeling system : An iot solution for enhancing road safety. In *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, pages 13–18. IEEE, 2019.

[12] Faisal Jamil, Omar Cheikhrouhou, Harun Jamil, Anis Koubaa, Abdelouahid Derhab, and Mohamed Amine Ferrag. Petroblock : a blockchain-based payment mechanism for fueling smart vehicles. *Applied Sciences*, 11(7) :3055, 2021.

[13] Sumaira Johar, Naveed Ahmad, Warda Asher, Haitham Cruickshank, and Amad Durrani. Research and applied perspective to blockchain technology : A comprehensive survey. *Applied Sciences*, 11(14) :6252, 2021.

[14] Mahtab Kouhizadeh and Joseph Sarkis. Blockchain practices, potentials, and perspectives in greening supply chains. *Sustainability*, 10(10) :3652, 2018.

[15] Moez Krichen. *Model-based testing for real-time systems.* PhD thesis, PhD thesis, PhD thesis, Universit Joseph Fourier (December 2007), 2007.

[16] Moez Krichen. *Contributions to model-based testing of dynamic and distributed real-time systems.* PhD thesis, École Nationale d'Ingénieurs de Sfax (Tunisie), 2018.

[17] Moez Krichen and Roobaea Alroobaea. A new model-based framework for testing security of iot systems in smart cities using attack trees and price timed automata. In *14th International Conference on Evaluation of Novel Approaches to Software*

Engineering - ENASE 2019, 2019.

[18] Moez Krichen, Meryem Ammi, Alaeddine Mihoub, and Mutiq Almutiq. Blockchain for modern applications : A survey. *Sensors*, 22(14) :5274, 2022.

[19] Moez Krichen, Mariam Lahami, Omar Cheikhrouhou, Roobaea Alroobaea, and Afef Jmal Maâlej. Security testing of internet of things for smart city applications : A formal approach. In *Smart Infrastructure and Applications*, pages 629–653. Springer, Cham, 2020.

[20] Moez Krichen and Stavros Tripakis. State identification problems for timed automata. In *IFIP International Conference on Testing of Communicating Systems*, pages 175–191. Springer, Berlin, Heidelberg, 2005.

[21] Nir Kshetri. Can blockchain strengthen the internet of things ? *IT professional*, 19(4) :68–72, 2017.

[22] Mariam Lahami and Moez Krichen. A survey on runtime testing of dynamically adaptable and distributed systems. *Software Quality Journal*, 29(2) :555–593, 2021.

[23] Mariam Lahami, Moez Krichen, Hajer Barhoumi, and Mohamed Jmaiel. Selective test generation approach for testing dynamic behavioral adaptations. In *IFIP International Conference on Testing Software and Systems*, pages 224–239. Springer, Cham, 2015.

[24] Mariam Lahami, Moez Krichen, and Mohamed Jmaïel. Runtime testing approach of structural adaptations for dynamic and distributed systems. *International Journal of Computer Applications in Technology*, 51(4) :259–272, 2015.

[25] Victoria Louise Lemieux. Trusting records : is blockchain technology the answer ? *Records Management Journal*, 2016.

[26] Daming Li, Lianbing Deng, Zhiming Cai, and Alireza Souri. Blockchain as a service models in the internet of things management : systematic review. *Transactions on Emerging Telecommunications Technologies*, page e4139, 2020.

[27] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107 :841–853, 2020.

[28] Yuancheng Li and Baiji Hu. A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles. *IEEE Transactions on Industrial Informatics*, 17(3) :1968–1977, 2020.

[29] Chao Liu, Kok Keong Chai, Xiaoshuai Zhang, Eng Tseng Lau, and Yue Chen. Adaptive blockchain-based electric vehicle participation scheme in smart grid platform. *IEEE Access*, 6 :25657–25665, 2018.

[30] Afef Jmal Maâlej and Moez Krichen. A model based approach to combine load and functional tests for service oriented architectures. In *VECoS*, pages 123–140, 2016.

[31] Afef Jmal Maâlej, Moez Krichen, and Mohamed Jmaiel. Conformance testing of ws-bpel compositions under various load conditions. In *2012 IEEE 36th annual computer software and applications conference*, pages 371–371. IEEE, 2012.

[32] Afef Jmal Maâlej, Moez Krichen, and Mohamed Jmaiel. Model-based conformance testing of ws-bpel compositions. In *2012 IEEE 36th annual computer software and applications conference workshops*, pages 452–457. IEEE, 2012.

[33] Alaeddine Mihoub, Ouissem Ben Fredj, Omar Cheikhrouhou, Abdelouahid Derhab, and Moez Krichen. Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. *Computers & Electrical Engineering*, 98 :107716, 2022.

[34] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 2019.

[35] Satoshi Nakamoto. Bitcoin : A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[36] Marc Pilkington. Blockchain technology : principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[37] C. V. Ravishankar and K. S. Kavitha. *Blockchain Applications that are Transforming the Society*, pages 23–39. Springer International Publishing, Cham, 2022.

[38] Khaled Salah, M Habib Ur Rehman, Nishara Nizamuddin, and Ala Al-Fuqaha. Blockchain for ai : Review and open research challenges. *IEEE Access*, 7 :10127–10149, 2019.

[39] Linda Schilling and Harald Uhlig. Some simple bitcoin economics. *Journal of Monetary Economics*, 106 :16–26, 2019.

[40] Gautam Srivastava, Shalini Dhar, Ashutosh Dhar Dwivedi, and Jorge Crichigno. Blockchain education. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, pages 1–5. IEEE, 2019.

[41] Ahmed Suliman, Zainab Husain, Menatallah Abououf, Mansoor Alblooshi, and Khaled Salah. Monetization of iot data using smart contracts. *IET Networks*, 8(1) :32–37, 2019.

[42] Dominic Wörner and Thomas von Bomhard. When your sensor earns money : exchanging data for cash with bitcoin. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing : Adjunct Publication*, pages 295–298, 2014.

[43] Karl Wüst and Arthur Gervais. Do you need a blockchain ? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54. IEEE, 2018.

[44] Bo Yan, Zijiang Yang, Yitian Ren, Xing Tan, and Eric Liu. Microblog sentiment classification using parallel svm in apache spark. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 282–288. IEEE, 2017.

[45] Bessem Zaabar, Omar Cheikhrouhou, Meryem Ammi, Ali Ismail Awad, and Mohamed Abid. Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things. In *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 200–205. IEEE, 2021.

[46] Bessem Zaabar, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, and Moha-

med Abid. Healthblock : A secure blockchain-based healthcare data management system. *Computer Networks*, 200 :108500, 2021.

[47] Yu Zhang and Jiangtao Wen. An iot electric business model based on the protocol of bitcoin. In *2015 18th international conference on intelligence in next generation networks*, pages 184–191. IEEE, 2015.

[48] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities : A survey. *International Journal of Web and Grid Services*, 14(4) :352–375, 2018.