La blockchain au service de l'automobile et de l'IOT

Léa Cavaree, Louis Archenoux, Pierre Mathelin, Guillaume Niay, Driss Essayed [1]

Abstract
Cet article explique le fonctionnement de la blockchain et énumère quelques-unes de ses applications possibles. L'étude se focalisera sur le domaine de l'automobile en abordant des cas concrets. Des pistes d'exploration pour la mise en œuvre d'une blockchain dans un environnement connecté sont également évoquées. Cet article expose les points forts de la blockchain mais aussi ses limites et les contraintes qui peuvent freiner son intégration.

Keywords
Blockchain — Automobile — IOT

[1] *Enseignant & chercheur en cybersécurité, ESAIP, Angers, France*

Contents

Introduction 1
1 Blockchain 1
1.1 Fonctionnement 1
1.2 Sécurité 2
1.3 Exemple d'application: la Blockchain as a Service 3
2 Secteur Automobile 3
2.1 MOBI 3
2.2 Assurer l'unicité 3
2.3 Sécuriser les communications 3
2.4 IOTA 4
La Fondation IOTA • Le Tangle • Microtransactions
3 Application 5
3.1 Mise en œuvre 5
3.2 Possibilités 5
4 Limites de la blockchain 6
4.1 Un système réellement infalsifiable? 6
4.2 Autres limites 6
5 Ouverture 6

Introduction

La blockchain est une technologie émergente depuis la création du Bitcoin en 2008 par Satoshi Nakamoto. En effet, cette monnaie virtuelle (cryptomonnaie) est entièrement construite sur cette technologie et est responsable de son apparition.

Cependant, le domaine financier n'est pas le seul à être concerné par cette révolution technologique. De la cryptomonnaie, à l'industrie culturelle, en passant par l'automobile, la technologie de la blockchain n'a pas fini d'évoluer et de bouleverser nos quotidiens.

Nous avons mené une étude sur les différents apports de la blockchain dans le domaine de l'IoT (objets connectés) et principalement appliquée au secteur de l'automobile.

1. Blockchain

La technologie de la blockchain est prometteuse dans de nombreux secteurs. De plus en plus de compagnies se spécialisent dans cette technologie, dans le but de proposer des services spécialisés. Ces entreprises viennent de divers horizons : banque, logistique, industrie pharmaceutique, luxe...[1]

1.1 Fonctionnement

La blockchain (chaine de bloc en français) est une technologique qui permet d'échanger et de stocker des informations de manière transparente et fiable. Elle rend possibles des transactions sans intermédiaires (tiers de confiance).

Dans l'exemple des transactions financières, une banque joue le rôle d'intermédiaire afin de valider ces transactions. Notre banque stocke celles-ci dans un "grand livre" qui leur permet de contrôler les échanges entre les différents partis.
En étant accessible et décentralisée, la blockchain permet de transférer des données de manière distribuée et fiable.

La structure des blocs peut varier d'une blockchain à l'autre mais on retrouve généralement les informations suivantes : un index [2] pour assurer l'unicité du bloc, une date, un hash[3] qui servira de clé de de cryptage du bloc, le hash du bloc précédent, puis les données.

L'index représente la position du bloc dans la chaîne (ex: 1, 6, 859526, ...). La date (timestamp) correspond au nombre de secondes qui se sont écoulées depuis le premier janvier 1970 (heure UNIX 1). [4]. Le hash est une chaine de caractères calculée à partir d'une donnée d'entrée, qui sert à protéger et anonymiser les données.

Pour ajouter un bloc à la chaine, celui-ci doit être validé par les acteurs de la chaine. Le hash doit être résolu et la puissance de calcul nécessaire à cette résolution contrôlée: cette étape correspond à "la preuve de travail". Le bloc est ensuite approuvé par la majorité du réseau afin être ajouté à la chaine.

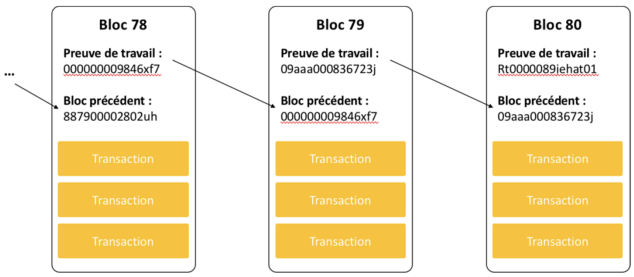

Figure 1. Construction d'un bloc

Exemple de transaction Afin de comprendre le fonctionnement d'une transaction au sein d'une blockchain, nous pouvons imaginer le scénario suivant:

Un individu A souhaite transmettre une donnée à un individu B. Il envoie alors des données par le biais d'une transaction sur la blockchain. Celle-ci devra être vérifiée puis validée.

Les individus qui constituent la chaîne vont alors pouvoir vérifier la possibilité pour l'individu A d'écrire cette nouvelle donnée en effectuant des calculs afin de vérifier la transaction.

Cette vérification s'effectue sans passer par un tiers de confiance et dépend de l'approbation ou non de la majorité des acteurs : c'est le consensus. Il permet d'assurer une certaine sécurité sur la blockchain et est composé de deux éléments :

- La vérification de la transaction: l'émetteur possède-t-il les ressources nécessaires pour effectuer la transaction?
- La preuve de travail: le mineur[1] a-t-il fourni la puissance de calcul nécessaire à la résolution du hash du nouveau bloc?

Lorsque le problème est résolu, la solution est alors soumise à l'ensemble du réseau. Si le consensus est validé, le bloc est alors daté et ajouté à la chaine. Le mineur ayant résolu le problème se verra rémunéré (par exemple, en obtenant une certaine quantité de Bitcoins dans le cas du Bitcoin) et l'individu B pourra recevoir les données qui lui sont destinées.[5]

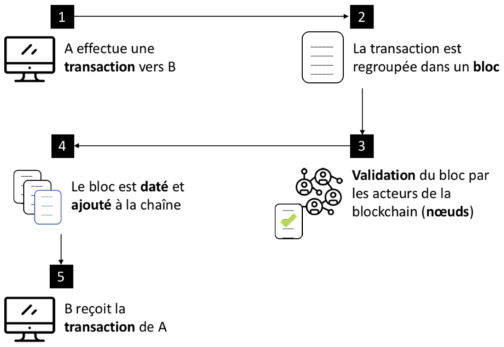

Figure 2. Validation d'une transaction

1.2 Sécurité

La blockchain est un registre distribué qui fonctionne avec la cryptographie. Elle permet des échanges vérifiés par tous les acteurs de la chaîne de manière sécurisée et fiable.

La fiabilité d'une blockchain dépend directement du nombre d'acteurs qui sont présents. En effet, plus le nombre de personnes qui partagent ce registre est élevé, plus la falsification d'une donnée sera compliquée. La preuve de travail est responsable de cette fiabilité. Pour falsifier les informations qui transitent, il faudra que l'attaquant soit capable de corrompre la majorité des acteurs: c'est l'attaque des 51%.

"Depuis la création de la blockchain Bitcoin, il n'y a eu aucune tentative réussie de modification rétroactive d'une transaction, ou plus généralement aucun exemple d'attaque réussie sur ce réseau."

Cela démontre la robustesse cette technologie et ouvre les portes à de nouvelles possibilités dans l'industrie. [6]

[1] Les individus essayant de résoudre le calcul

1.3 Exemple d'application: la Blockchain as a Service

De nombreuses grandes compagnies informatiques telles que Amazon Web Service, Microsoft Azure ou IBM Watson proposent un service de Blockchain As A Service (BaaS). Cela permet au client d'utiliser une blockchain sans avoir à se préoccuper de la structure et ainsi, diminuer le coût et le risque de l'investissement tout en gardant la liberté du choix de la technologie rest.[7]

Différents types de registres distribués sont disponibles selon les fournisseurs. De plus ces systèmes évitent d'avoir à payer et recruter des experts (qui se font rares sur le marché.)[8]
Pour choisir la blockchain ou le système le plus adapté à votre entreprise, plusieurs points nécessitent d'être évalués:

- Le sujet du projet (Dapp[2],IOT[3],Finance)
- L'étude de faisabilité et la portée du projet sur le long terme[4]
- Une équipe informatique compétente & disponible
- Registre distribué adapté

En fonction des besoins identifiés, il faudra choisir le fournisseur de blockchain ou l'intégration d'une blockchain qui est le mieux adapté.
Dans la majorité des cas, si le projet est un POC[5] ou que l'équipe informatique n'est pas qualifié sur cette technologie, alors il est recommander de choisir un BaaS[6].

2. Secteur Automobile

Les applications de la blockchain dans le secteur de l'automobile sont de plus en plus fréquentes. En effet, certains fabricants cherchent à proposer des produits plus fiables et uniques en utilisant cette technologie tout en assurant une traçabilité auprès de leurs clients.

2.1 MOBI

Le 2 mai 2018 ,une trentaine de partenaires se sont réunis afin d'annoncer la création du consortium MOBI[7]. Pilotée par Chris Ballinger, cette collaboration regroupe les plus grands acteurs du marché automobile (BMW, General Motors, Renault...).

C'est en 2017 que les premiers travaux autour de la blockchain et de l'automobile ont eu lieu. La startup Oaken Innovations (aujourd'hui membre de MOBI) a créé un système d'ouverture de véhicule grâce à une application basée sur la blockchain Ethereum.

De nombreux autres cas d'usage peuvent alors être imaginés tels que le partage de véhicule ou encore le paiement des péages.[9]

2.2 Assurer l'unicité

Certains fabricants de voitures de luxe perçoivent la blockchain comme une opportunité de certifier l'unicité de leurs produits.

En proposant le modèle de l'Aventador S labélisée, Lamborghini certifie ses voitures grâce à cette technologie. En effet, la marque italienne a développé en collaboration avec Salesforce sa propre blockchain "Sicura". Leur blockchain permet de lutter face à la contrefaçon en enregistrant et en stockant les différentes informations du modèle.

Elle fut utilisée pour la première fois dans le but de certifier l'unicité d'un de leur modèle. L'artiste de rue Skyler Gray a permis à cette voiture de devenir une véritable œuvre d'art, unique et certifiée grâce à la blockchain.

Daimler, société mère de Mercedes-Benz a également décider d'utiliser la technologie de la blockchain pour mettre en place un portefeuille cryptographique physique.

En travaillant en collaboration avec Riddle & Code, la société a mis en place le crypto wallet[8] afin de sécuriser les échanges d'informations trafic en temps réel entre leurs véhicules. Cette innovation va permettre de certifier les données qui ont été échangées et de retrouver l'origine de la cause de certains accidents.

Mercedes-Benz n'en est pas à son premier coup d'essai. La marque allemande a déjà mis en place une blockchain auparavant afin d'assurer et optimiser leur logistique de chaînes d'approvisionnement.

2.3 Sécuriser les communications

La principale révolution de la blockchain repose dur la sécurisation et la fiabilité des données qui transitent. Volkswagen l'a compris et a décidé de prendre les devants avec l'avènement de la voiture autonome.

[2] Decentralize Application
[3] Internet of Things
[4] Proof of Concept
[5] Proof Of Concept ou étude de faisabilité
[6] Blockchain as a Service
[7] Mobility Open Blockchain Initiative
[8] portefeuille

L'entreprise utilise une blockchain qui permet de fiabiliser les messages qui transitent entre leurs véhicules.

L'idée du fabricant allemand est de mettre en œuvre un système de communication entre leurs véhicules autonomes afin d'aider les conducteurs à anticiper et réduire les risques d'accidents de la route. Avant que Volkswagen n'instaure la blockchain dans les communications, les messages étaient échangés entre les véhicules de la marque afin de prévenir le conducteur d'événements imminents (collision de voitures, ralentissement du trafic...).

Désormais avec la blockchain, ces informations trafic son enregistrées et sécurisées avant d'être redistribuées aux véhicules.
D'après Sébastien Henot (chef du projet MOBI chez Renault), "la blockchain permettra l'émergence d'un écosystème ouvert". Cet écosystème est incontournable si l'on veut une approche standardisée ouverte à la totalité des acteurs.

En restant dans cette optique, nous pouvons facilement imaginer la technologie de Volkswagen mise à disposition à l'ensemble des véhicules. La généralisation d'une blockchain telle que celle-ci pourrait limiter considérablement les accidents de la route.

Les applications de la blockchain dans le secteur automobile peuvent être diverses et variées. C'est dans cette optique que les constructeurs se tournent vers cette technologie, afin d'assurer plus de transparence et de fiabilité. La blockchain reste toutefois une technologie récente avec peu de cas concret en production à grande échelle.

2.4 IOTA

L'IOT est de plus en plus présent dans les voitures avec les milliers de composants et de capteurs qui la composent. Les technologies d'échange d'informations devenant considérables, la sécurisation de celle-ci et l'intégrité des données deviennent un facteur primordial. La blockchain améliorerait ces différents points afin d'assurer une meilleure communication.

2.4.1 La Fondation IOTA

La fondation IOTA créée en 2015 propose une blockchain spécialisée dans les objets connectés. Produit par une fondation allemande, IOTA est le leader actuel dans le domaine de l'IOT. La fondation est en collaboration avec la MOBI et les principales grandes entreprises de l'industrie automobile.[10].

2.4.2 Le Tangle

IOTA est une blockchain d'échange pair à pair, sans intermédiaire et sans frais de transaction. Elle utilise le "tangle", une technologie unique basée sur une blockchain évolutive. Elle utilise un flux de transactions individuelles enchevêtrées les unes à la suite des autres. Elle a aussi un système de vérification sur deux transactions ultérieures qui sont sélectionnées aléatoirement.

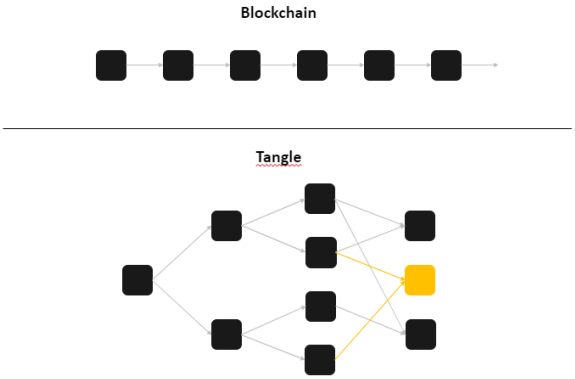

Figure 3. Différence entre la blockchain "classique" et le Tangle

Ce système permet d'éviter une attaque par DDoS[9] qui consiste à inonder le service d'informations, afin de le rendre indisponible. C'est la preuve de travail qui va permettre d'éliminer les tentatives transactions vides émises par l'assaillant.

Comme précisé ci-dessus le "tangle" propose une vérification aléatoire des deux dernières transactions effectuées. Ce système permet d'éviter la création de blockchain en parallèle qui pourraient se vérifier entre elles.
Elles pourraient être intentionnellement falsifiées et les transactions corrompues.

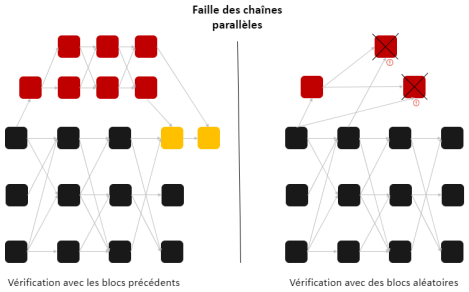

Figure 4. Sécurisation du réseau par un algorithme de sélection aléatoire

[9] Distributed Denial of Service

Cette blockchain unique possède divers points de sécurité afin de protéger le réseau et le rendre pleinement autonome. Il est d'ailleurs possible de l'utiliser hors connexion. [11] Contrairement aux blockchains classiques qui sont proportionnellement énergivores que le nombre de transitions augmente (Proof of work), IOTA est une blockchain scalable. Cela signifie que plus le nombre de transactions augmente, plus elle pourra réaliser de transactions par seconde.

2.4.3 Microtransactions

Le marché des microtransactions est en plein essor. En 5 ans le nombre de microtransactions dans les jeux vidéo a doublé pour atteindre les 22 milliards en 2017. [12] Epic Games, le nouveau géant de l'industrie du jeux vidéo grâce à "Fortnite" a par ailleurs dégagé 2.4 milliards de dollars. D'autre part Ubisoft, leader français dans ce domaine, génère 47.9% de son chiffre d'affaire grâce aux microtransactions. [13]

IOTA est donc une technologie amenée à évoluer. Les constructeurs automobiles pourraient tirer profit de ce système et nous pourrions par exemple imaginer payer des options supplémentaires pour nos voitures (stationnement automatique, service de conciergerie...). Avec ce système de microtransactions, il serait possible de louer une voiture comme on loue un vélo. Les entreprises pourrait détecter les anomalies grâce aux différentes informations récupérées par les capteurs et analyser l'état de la voiture à chaque rente.

Sans frais, IOTA pourrait apporter une évolution dans le domaine des microtransactions. Elle deviendrait le moteur de ce changement en apportant sa contribution dans le développement des microtransactions. D'autant plus qu'elle a la capacité de supporter les millions de microtransactions effectuées chaque jour dans le monde.

3. Application

Nous avons donc observé les différents cas d'usage possibles avec cette technologie. Nous avons voulu voir s'il était possible d'utiliser la blockchain pour répondre à des besoins industriels dans l'automobile.

3.1 Mise en œuvre

Nous avons observé qu'avec une Raspberry Pi il était possible de mettre en œuvre des transactions d'informations sécurisées avec la blockchain. Il faut pour cela configurer le Raspberry Pi 3 avec Raspbian et un capteur pour mesurer les données (capteur d'humidité, de température, ou autre). Il faut également une connexion internet. [14] Ensuite nous continuons le processus en installant et configurant les différents éléments selon le guide MAM[10].[15] Finalement, nous pouvons utiliser le "tangle" avec les données reçues par le capteur. Ensuite ces données peuvent être retrouvées sur internet(récepteur) grâce au hash transmis par le capteur (émetteur). Cette transaction permet ici de transmettre des données vérifiées de manière sécurisée.

3.2 Possibilités

Avec les Smart Contract[11] nous pourrions voir plus loin dans l'utilisation de cette technologie. Par exemple, imaginons qu'un capteur qui enregistre le kilométrage d'un véhicule. On pourrait créer un Smart Contract qui, lorsque le véhicule atteint un certain nombre de kilomètres, envoie un e-mail à l'utilisateur. Le conducteur recevra donc une alerte qui lui conseillera de passer un entretien de son véhicule.

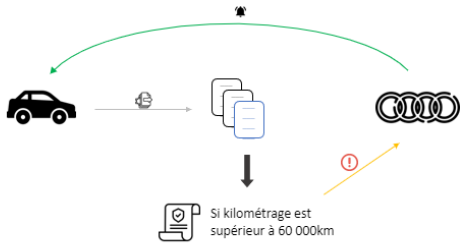

Figure 5. Exemple d'un Smart Contract

L'entreprise quant à elle pourrait aussi avoir un feedback sur l'état du véhicule. A partir de ces retours, ils pourront prendre des décisions et voir ainsi les axes d'améliorations qu'il faudrait retravailler sur les futurs modèles. L'industrie automobile pourrait progresser de manière exponentielle avec une incroyable rapidité à s'adapter comparée à ce que l'on peut faire aujourd'hui.

On pourrait imaginer un échange d'informations entre véhicules, des mises à jour logiciel pour tous les véhicules de manière sécurisée. Les idées concernant l'usage de cette technologie sont innombrables et c'est pourquoi elle suscite l'intérêt des plus grandes entreprises.

[10] Masked Authenticated Messaging
[11] Contrat intelligent avec du code

De plus les Smart Contracts peuvent être rédigés via les langages de l'IOT comme le Python, le Go ou le C# par exemple.

Malgré la confusion entre blockchain et crypto monnaie pour les particuliers, les entreprises ont pour la plupart compris que la blockchain est une technologie qui, comme internet il y a quelques années, pourrait apporter un avantage concurrentiel.

4. Limites de la blockchain

4.1 Un système réellement infalsifiable?

Comme nous l'avons dit précédemment dans notre document, il est très peu probable qu'une blockchain subisse une attaque. Seulement, en théorie, cela reste possible. Pour arriver à cela, un individu ou un groupe d'individu doit réussir à monopoliser une certaine partie de la puissance de calcul de la blockchain. Cette certaine partie varie selon les blockchains. Par exemple, pour celle du Bitcoin et toutes les blockchains se basant sur celle-ci, la part à atteindre est 51%: "l'attaque des 51"%.

C'est ce qui est récemment arrivé pour la cryptomonnaie Vertcoin. L'attaque a été réalisée avec succès. Cependant, elle aurait rapporté au hacker environ 0,4 Bitcoin alors qu'il aurait dépensé l'équivalent de 0,5 à 1 Bitcoin pour la réaliser [16]. En réponse, tous les wallets de cette blockchain ont été bloqués afin que l'attaque ne prenne pas de plus grande ampleur. Il est donc évident que faire une attaque de ce type n'est absolument pas rentable et que de ce fait, elle est dissuasive. Pour terminer, ce type d'attaque n'est pas possible sur toutes les blockchains car elles ne sont pas toutes construites de la même façon.

4.2 Autres limites

La blockchain ne permet pas forcément de supprimer tous les intermédiaires de confiance. Prenons l'exemple d'une blockchain certifiant l'exactitude d'un diplôme. Au début de la chaine, il faut bien un organisme de confiance chargé d'entrer la donnée véritable dans la chaine.

De plus, la consommation énergétique et l'avenir de la planète est une problématique mondiale majeure. On peut donc s'interroger sur cet aspect de la technologie blockchain qui est en contradiction avec nos besoins écologiques actuels.

En effet, le calcul nécessaire à fournir pour résoudre les problèmes mathématiques et ainsi trouver le hash du nouveau bloc demande une grande ressource en énergie. Plusieurs machines travaillent en même temps afin de résoudre le problème. Il existe partout dans le monde plusieurs entrepôts entièrement dédiés à la résolution de ces énigmes mathématiques. On les appelle les "Fermes de minage". A l'heure actuelle les plus répandues sont relatives au Bitcoin, car c'est une des blockchains les plus rentables.[17]

5. Ouverture

Aujourd'hui, les blockchains tendent à évoluer. Les développeurs implémentent de nouvelles règles. L'objectif est de diminuer l'impact environnemental en réduisant les ressources de calcul. Ils cherchent également à limiter les attaques de type 51%. Dans ce cadre, les développeurs proposent de nouvelles stratégies comme le Proof of Stake[12].

Stratégie	Comment miner ?	Utilisation des ressources	Degré de décentralisation	Rapidité des transactions	Frais de transaction
Proof of work	Équipement informatique	Très forte	Faible	Lente	Assez élevés
Proof of stake	Grand nombre de tokens de la crypto-monnaie	Faible	Elevé	Assez élevée	Faibles

Figure 6. Différence entre le Proof of Work et le Proof of Stake [18]

Les mentalités évoluent également dues à l'intérêt grandissant pour la blockchain. Près de 1 américain sur 10 détiendrait des Bitcoins selon l'étude de Spencer Bogart [19]. L'intérêt des entreprises s'accroit également, comme nous avons pu le constater dans cet article, avec de nombreux projets. Elles investissent dans cette technologie qui pourrait leur permettre d'innover et d'avoir un avantage concurentiel important.

Le changement est aussi conséquent dans les institutions étatiques. L'état chinois prévoit d'investir 2 milliards de dollars pour développer une blockchain d'état. De nombreux pays et communautés suivent le pas. Ces pays tentent de sortir du système du dollar qui régit les lois commerciales.

La Blockchain ne cesse d'évoluer et de provoquer des révolutions dans de nombreux domaines. La formation de personnes maitrisant l'écosystème va devenir primordiale. L'apport de chacun aidera à développer les nombreux projets qui constitueront le monde de demain.

[12] Preuve de conservation

References

[1] Vechain partners. https://vechaininsider.com/partnerships/a-complete-list-of-vechain-partnerships/.

[2] Index. http://glossaire.infowebmaster.fr/index-/.

[3] Fonction de hashage. https://fr.wikipedia.org/wiki/Fonction_de_hachage.

[4] Timestamp. http://glossaire.infowebmaster.fr/timestamp/.

[5] Fonctionnement d'une blockchain. https://blog.ippon.fr/2018/01/08/fonctionnement-dune-blockchain/.

[6] la cryptographie, pierre angulaire de la blockchain. https://adameo.com/2018/03/15/2-la-cryptographie-pierre-angulaire-de-la-blockchain/.

[7] How to blockchain as a service. https://www.ledgerinsights.com/how-to-blockchain-as-a-service-baas/.

[8] Blockchain as a service: quelle solution choisir? https://www.journaldunet.com/solutions/cloud-computing/1206955-blockchain-as-a-service-quelle-solution-choisir/.

[9] Initiative mobility open blockchain (mobi) – l'industrie automobile s'imprègne des vertus de la blockchain. https://cryptoactu.com/initiative-mobility-open-blockchain-mobi/.

[10] Iota joins the mobility open blockchain intitiative mobi. https://blog.iota.org/iota-joins-the-mobility-open-blockchain-initiative-mobi-1c017a8c00f0.

[11] What is iota? https://www.iota.org/get-started/what-is-iota.

[12] Chiffre d'affaire microtransitions a doublé en cinq ans. https://www.jeuxonline.info/actualite/53650/chiffre-affaires-microtransactions-double-cinq-ans.

[13] Microtransaction: Origines et histoires d'un modèle qui dérange. http://www.jeuxvideo.com/dossier/1117854/microtransaction-origines-et-histoire-d-un-modele-qui-derange/1117929.html.

[14] Iota tutorial 28: How to send sensor data to the tangle using masked authenticated messaging. https://www.youtube.com/watch?v=atJ-ZT7aKoA.

[15] Iota: Quick guide. www.mobilefish.com/developer/iota/iota_quick-guide_raspi_mam.html.

[16] Un hackeur tente une attaque des 51 contre vertcoin… à perte ! https://journalducoin.com/altcoins/hackeur-attaque-51-vertcoin-perte/.

[17] Quelles sont les limites de la technologie de la blockchain? https://www.cryptoencyclopedie.com/single-post/Quelles-sont-les-limites-de-la-technologie-Blockchain-.

[18] Quelles sont les différences entre pos (proof-of-stake) et pow (proof-of-work) ? https://cryptoast.fr/difference-pos-proof-of-stake-et-pow-proof-of-work/.

[19] Bitcoin is a demographic mega trend data analysis? https://medium.com/blockchain-capital-blog/bitcoin-is-a-demographic-mega-trend-data-analysis-160d2f7731e5?