Vers une gestion d'identités auto-souveraine pour les dispositifs IoT

Lydia Ouaili, Samia Bouzefrane, Elena Kornyshova, Pierre Paradinas

Vers une gestion d'identités auto-souveraine pour les dispositifs IoT

Towards self-sovereign identity management for IoT devices

Lydia Ouaili[1,2], Samia Bouzefrane[1], Elena Kornyshova[1] and Pierre Paradinas[1]

[1] *Conservatoire National des Arts et Métiers, Paris, France*
[2] *Trasna Solutions, Marseille, France*

Abstract

In some IoT ecosystems, entities (humans, organizations, devices) need to participate collaboratively to develop smart applications. In general, this collaboration requires authentication of the entities. In ecosystems where IoT devices may be compromised, each entity must ensure that the information received from IoT devices and exchanged with other entities are trustworthy. In this context, Identity Management Systems (IdMSs) are crutial to represent entities and face an increased demand for security and privacy of sensitive data. The most widely used models of IdMSs to date still rely on a centralized architecture, which has some drawbacks arising from its centralized operations and its lack of transparency. To avoid the traditional models limitations, we explore a decentralized approach using a self-sovereign identity system that relies on Blockchain consensus algorithms, decentralized identifiers (DID) and zero-knowledge proof (ZKP) to build a trust relationship between entities.

Keywords

Identity, Self-Sovereign Identity (SSI), Blockchain, Decentralized Identifiers (DIDs), IoT, distributed systems.

Résumé

Dans certains écosystèmes IoT, les entités (humains, organisations, dispositifs) doivent participer de manière collaborative pour développer des applications intelligentes. En général, cette collaboration nécessite l'authentification des entités. Dans les écosystèmes où les dispositifs IoT peuvent être compromis, chaque entité doit s'assurer que les informations reçues des dispositifs IoT et échangées avec d'autres entités sont dignes de confiance. Dans ce contexte, les systèmes de gestion d'identité sont cruciaux pour représenter les entités et font face à une demande accrue en terme de sécurité et de confidentialité des données sensibles. Les modèles de systèmes de gestion d'identité les plus utilisés à ce jour reposent toujours sur une architecture centralisée, qui présente certains inconvénients liés à ses opérations centralisées et à son manque de transparence. Pour éviter les limites des modèles traditionnels, nous explorons une approche décentralisée utilisant un système d'identités auto-souverain qui s'appuie sur des algorithmes de consensus et Blockchain, sur des identifiants décentralisés (DID) et sur la preuve à divulgation nulle de connaissance pour établir une relation de confiance entre les entités.

lydia.ouaili@lecnam.net (L. Ouaili); samia.bouzefrane@lecnam.net (S. Bouzefrane); elena.kornyshova@cnam.fr (E. Kornyshova); pierre.paradinas@cnam.fr (P. Paradinas)

1. Introduction

Les systèmes de gestion d'identité (IdMSs) désignent un ensemble prédéfini de processus pour assurer la façon dont les identités numériques sont censées être commandées, gérées et révoquées. Ce domaine a été et reste l'un des principaux défis de l'innovation technologique. Il s'agit de faciliter les interactions entre les individus et les organisations d'une manière qui soit sûre, privée et plus efficace. Une identité numérique peut se composer d'identifiants (ID utilisateur, émail, URL, etc.), de justificatifs (certificats, jetons, données biométriques, etc.) et d'attributs (rôles, postes, privilèges, etc.). En raison du nombre croissant des personnes dans le monde utilisant Internet, de nombreux processus sont numérisés. Ce qui signifie que toutes ces personnes ont la possibilité de créer un compte dans n'importe quel service disponible, qui sont tous générés approximativement de la même manière: l'utilisateur doit fournir des informations que l'entreprise qui gère ce service conservera, afin de créer un compte pour cet utilisateur, lui permettant d'accéder au service via une combinaison d'identifiants (généralement l'email ou un nom d'utilisateur) et de mot de passe. Par conséquent, la gestion manuelle de tous les identifiants de connexion devient un défi. Aujourd'hui, l'une des formes les plus répandues de système de gestion des identités repose sur des solutions fédérées, qui permettent aux entreprises de partager des données sur un même utilisateur et à ce dernier de disposer d'un seul identifiant de connexion pour accéder à plusieurs services. Cela résout en quelque sorte le problème du trop grand nombre de mots de passe à mémoriser, mais permet toujours à plusieurs entreprises de détenir les données de leur propriétaire. Ce dernier point est l'une des nombreuses questions que l'identité auto-souveraine (SSI pour Self-Sovereign Identity en anglais) souhaite aborder, au moyen de ses identifiants décentralisés (DID pour Decentralized IDentifiers en anglais) et de ses certificats vérifiables (VCs pour Verifiable Credentials en anglais), dont la gouvernance est gérée par l'utilisateur, en lui permettant de ne divulguer que les informations nécessaires, tout en ayant le pouvoir de les révoquer.

En faisant le lien avec l'Internet des objets (IoT), où l'utilisation des dispositifs IoT a augmenté à un rythme rapide, la conception d'une identité numérique pour les objets connectés est un cas d'utilisation qui n'est pas pris en compte dans de nombreux systèmes de gestion des identités. Les cadres conventionnels de gestion de l'identité et de la confiance sont conçus pour les humains et non pour les appareils, et l'identité numérique est principalement liée à des personnes ou à des systèmes d'information d'entreprise qui sont également gérés par des personnes. Permettre aux équipements IoT d'avoir leur propre identité ouvre de nouvelles possibilités, car il existe aujourd'hui une présence importante de dispositifs "autonomes" ou "intelligents", qui peuvent agir et prendre des décisions seuls ou avec l'aide partielle de l'homme. Ces décisions impliquent généralement une communication entre différents équipements, et l'utilisation de l'identité auto-souveraine pour prouver que les dispositifs sont bien ceux qu'ils prétendent être permet à de nombreux cas d'utilisation d'être plus sûrs et moins sujets aux attaques [1, 2].

2. Contexte et travaux connexes

Dans cette section, on présente les implémentations actuelles qui divisent les IdMSs en deux paradigmes pour gérer les identités sur Internet: les systèmes traditionnels et les systèmes décentralisés, puis le concept de la Blockchain et son lien avec l'identité auto-souveraine (SSI). Cela mettra en avant l'intérêt de la décentralisation et la possibilité de passer des systèmes d'identité numérique centralisés à des systèmes décentralisés grâce à la SSI.

Les systèmes traditionnels de gestion des identités reposent sur trois acteurs: Les sujets, les fournisseurs de services (SP pour Service Provider en anglais) et les fournisseurs d'identité (IdP Identity Provider). Les IdMS traditionnels dépendent principalement d'un IdP centralisé qui effectue les opérations de création, de mise à jour, de gestion et de suppression des identités des utilisateurs [3]. Les parties dépendent les unes des autres de la manière suivante: le sujet demande l'accès aux services du RP, qui à son tour demande à l'IdP de vérifier l'identité du sujet par le biais d'un protocole d'authentification. Dans le paradigme centralisé, l'évolution des implémentations a commencé par des modèles isolés, ensuite centralisés, puis à fédérés/centrés sur l'utilisateur. Tous ces modèles dépendent toujours d'une architecture centralisée.

Face à des problèmes tels que le point de défaillance unique d'un système centralisé de gestion de l'identité et les problèmes de confidentialité qui ont été signalés (comptes Facebook piratés [1] [2] [4, 5]), les systèmes traditionnels présentent des inconvénients majeurs: comme les données nécessaires de l'utilisateur pour accéder à un service appartiennent à l'IdP, les IdP sont plus sujets aux attaques étant donné qu'un serveur centralisé peut être visé. En outre, dans un scénario IoT, avec l'explosion du nombre de dispositifs, la centralisation pose des problèmes inhérents d'évolutivité, d'authentification et du transfert sécurisé d'informations pour la structure centralisée [6]. Enfin, la plupart des systèmes traditionnels fonctionnent de manière non transparente [6]. Cela soulève des questions de confidentialité, puisque les utilisateurs ne sont pas pleinement conscients des pratiques d'une organisation, par exemple inclure la vente de leurs données à des tiers.

Avant d'aborder le sujet de la SSI, rappelons que pour accéder à un service sur le web un système de confiance est parfois nécessaire, les utilisateurs échangent des informations pour valider leurs affirmations, cet échange numérique correspond à ce que nous faisons dans le monde réel: l'utilisateur prouve une déclaration qui dépend du service et de ce qui est exigé de lui en envoyant un justificatif qui prouve qu'il est éligible pour cette déclaration (certificat de naissance ou de conduite par exemple). Pour garantir la validité du certificat, un système de confiance est établi entre le détenteur, celui qui va vérifier et celui qui délivre le certificat. Puisqu'il n'existe pas de méthode pour prouver qu'une déclaration est réelle dans le monde numérique, jusqu'à présent, la confiance accordée aux informations échangées se fait via des documents signés par des autorités officielles, ces documents sont souvent scannés et utilisés de manière dématérialisée. Cette méthode n'est malheureusement pas fiable puisqu'il est possible de falsifier les documents officiels

[1] https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
[2] https://www.bbc.com/news/technology-46065796

et de créer de fausses copies.

La SSI est considéré comme une nouvelle façon de gérer les identités vu comme un changement profond de technologie capable de faire face aux défis actuels des IdMSs, où les assertions tels que les certificats sont signées numériquement (par cryptographie), ce qui les rend infalsifiables. Bien que les concepts de SSI existaient déjà (une identité unique (DID) contrôlée par son utilisateur et la notion de certificat vérifiable), la question était de savoir comment les combiner dans un système décentralisé pour créer des standards et gérer les identités numériques. Et c'est là que le potentiel de la technologie blockchain est apparu, sa nature décentralisée peut être appliquée au-delà des crypto-monnaies, comme par exemple le transfert, la validation et l'échange d'informations dans un système décentralisé sans passer par un tiers. Les concepts de base du SSI et la façon dont ils sont combinés sont présentés ci-dessous :

- Certificats vérifiables (en anglais: Verifiable credentials VCs);
- Identifiants décentralisés (DIDs);
- Registre distribué tel que la Blockchain.

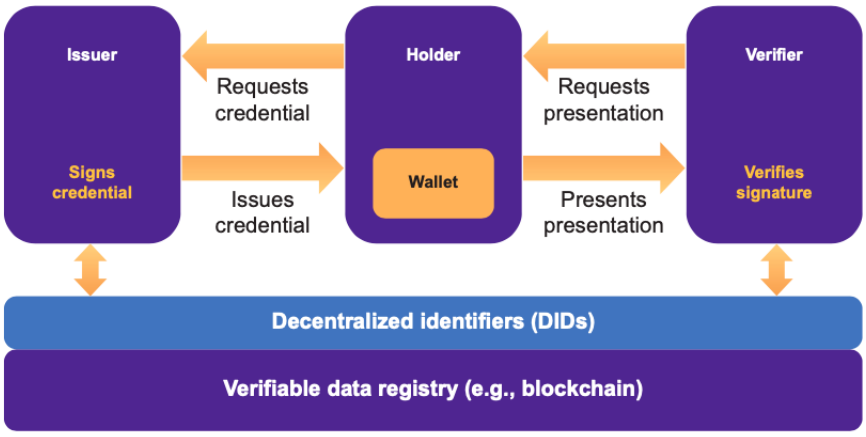

Figure 1: Les principaux rôles impliqués dans l'échange de VCs. La vérification de la signature numérique est la partie du processus permise par les réseaux de blockchain publics ou à permission. Tirée de [7].

Le diagramme ci-dessus montre les différents rôles et les flux d'informations associés aux 3 acteurs : Émetteur, Détenteur et Vérificateur, avec des différences fondamentales aux modèles précédents des IdMSs. Dans l'architecture de base de la SSI, la création des certificats VCs est séparée de l'identification, la génération des certificats VCs est associée à un identifiant DID indépendant des services et les processus de leurs gestion dépendent de la blockchain.

Les certificats vérifiables (VCs) sont un ensemble d'affirmations sur le sujet, qui imitent le certificat réel, comme les cartes de crédit et les passeports. Le format standard des VCs suit la norme répertoriée par le World Wide Web Consortium W3C et qui sont alimentés

par la cryptographie, ce qui les rend authentiques et inviolables. Pour faciliter la mise en œuvre du modèle papier, la recommandation du W3C [3] propose une architecture pour les VCs, qui contient les informations suivantes : un identifiant du sujet, un ensemble de revendications associées au sujet. Des métadonnées sur les revendications elles-mêmes, telles que l'entité qui les a faites, une date d'expiration et une signature numérique par l'émetteur des revendications. Les VCs sont censés être privés et stockés dans un portefeuille personnel et ne doivent être partagés que si c'est nécessaire. Afin d'améliorer la confidentialité, la spécification des VCs prend en charge un algorithme de cryptographie ZKP (les preuves théoriques de l'algorithme sont présentés dans [8]), où les détenteurs du VC présentent une preuve avec une divulgation minimale de données sensibles et personnelles aux vérificateurs. Avec la ZKP, il est possible de prouver des affirmations telles que "J'ai une signature", sans rien dire de plus (c'est-à-dire sans révéler à quoi ressemble la valeur associée à cette signature). Pour qu'un détenteur puisse utiliser un justificatifs vérifiable à connaissance zéro, il faut qu'un émetteur ait émis une signature "une preuve", de sorte que le détenteur puisse présenter les informations à un vérificateur d'une manière qui renforce la confidentialité. La pratique courante consiste à prouver la connaissance de la signature, sans révéler la signature elle-même. Selon le W3C, il existe deux exigences pour les justificatifs vérifiables lorsqu'ils doivent être utilisés dans des systèmes de preuve à connaissance zéro.

- Le certificat vérifiable doit contenir une preuve, utilisant la propriété de preuve (l'algorithme [8]), afin que le détenteur puisse dériver une présentation vérifiable qui ne révèle que les informations que le détenteur a l'intention de révéler.
- Si un standard de certificat est utilisé, celui-ci doit être définie dans le schéma général d'un certificat vérifiable, de sorte qu'il puisse être utilisé par toutes les parties pour effectuer diverses opérations cryptographiques à connaissance zéro.

L'utilisation des VCs pour prouver des revendications ou des déclarations au vérificateur, est souvent associée à un sujet (personne, dispositif IoT, organisation). Dans ce cas, il est utile d'utiliser un identifiant qui représente les mêmes objets. Dans le Web, l'identification d'une ressource (la ressource est utilisée au sens général : images, service, personne...) se fait par un identifiant de ressource uniforme (URI) divisé en deux sous-classes : URLs et URNs (voir [7] pour plus de détails). Dans la SSI, le DID est un nouveau type d'identifiant créé pour chaque entité et ne contient que des informations pseudonymes, il peut être soit un URL soit un URN, et peut être résolu via le résolveur de DID pour obtenir des informations sur la ressource identifiée par le DID. Cette première définition peut être similaire au processus du système des noms de domaine (DNS), mais ce qui différencie le DID des autres URL est l'identifiant cryptographique vérifiable et les couches de décentralisation. Il est important de noter que la production et le contrôle d'un identifiant sont séparés de la production de VCs à cet identifiant. Les solutions les plus connues pour supporter le cadre SSI sont uPort[4], Sovrin3[5], et Hyperledger Indy[6], elles diffèrent

[3]https://www.w3.org/TR/vc-data-model/#zero-knowledge-proofs
[4]https://www.uport.me/
[5]https://sovrin.org/
[6]https://www.hyperledger.org/projects/hyperledger-indy

principalement au niveau des mécanismes de consensus incorporés dans les technologies Blockchains comme le mécanisme de tolérance aux pannes [9, 10].

La Blockchain est un registre introduit pour la première fois en 2008 dans le contexte de la crypto-monnaie Bitcoin [11], il est composé de plusieurs blocs liés entre eux et contenant des informations qu'on appelle transactions. Ce qui caractérise ce registre par rapport aux autres, c'est sa décentralisation, sa persistance, son anonymat et son auditabilité [12]. Il n'est pas nécessaire de faire valider les transactions par une autorité centrale (par exemple, une banque), de plus, elles sont visibles par tous les utilisateurs du réseau, et doivent être confirmées pour être ajoutées au bloc. Il est presque impossible de falsifier un bloc et de l'ajouter à la Blockchain puisque chaque bloc est vérifié et validé par d'autres nœuds. Les blocs sont protégés par le consensus de l'ensemble du réseau grâce à l'arbre de Merkle utilisé pour vérifier l'intégrité des transactions du bloc, ce qui permet l'immuabilité du grand livre.

Bien que les concepts fondamentaux de la SSI soient indépendants de la technologie Blockchain, ils sont utilisés ensemble. La technologie Blockchain permet un consensus décentralisé pour gérer des identités uniques et évite le passage par un tiers de confiance (TTP). Cependant, au-delà de la centralisation, un problème subsiste : les systèmes classiques de gestion des identités (par exemple OAuth, OpenID) basés sur des comptes et des certificats numériques posent des problèmes de confidentialité. Les certificats contiennent des informations sensibles d'identité, ce qui compromet la vie privée des détenteurs de certificats et, par conséquent, peut ne pas convenir au stockage dans des grands registres distribués et immutables. Pour résoudre ces problèmes, l'utilisation des DIDs a été proposée et la Blokchcain va servir en partie à stocker ces DIDs.

3. État de l'art sur l'identité auto-souveraine

Dans cette section, nous examinerons les travaux de recherche connexes sur les SSI, dont certains couvrent une étude exhaustive sur les concepts, d'autres évoquent les défis et les avantages. Enfin, nous identifierons les problématiques de recherche les plus pertinentes. Pour ce faire, nous nous appuyons sur plusieurs ressources que nous résumons dans le tableau suivant pour capturer les travaux pertinents du sujet:

SSI	2018	2019	2020	2021	2022
IEEE	[13] [24] [25]	[14] [15] [16]	[17][18] [19] [20] [21] [26] [27] [28] [34] [35] [40] [41]	[22] [29] [30] [31] [32] [36] [37] [38] [39] [42] [43] [44]	[23] [33]
ACM	-	- -	[45] [46] [49] [50] [52] [53]	-	[47] [48] [51]
Science direct:	[54] -	- -	- -	[55] [56] [57]	

D'après ces travaux publiés dans les bibliothèques numériques les plus célèbres, la SSI semble être relativement récente, mais il y avait déjà des discussions sur le sujet par des industries et des travaux de thèse et de master. Les plus cités d'entre eux sur google scholar ont été publiés en 2016. Un ouvrage de la fondation indépendante Sovrin [58], qui propose des implémentations open source de la SSI et la vision de Christopher Allen [7]. Ils rappellent l'évolution chronologique des modèles d'identité existants (fédérés, centrés sur l'utilisateur) ainsi que leur architecture centralisée qui pose de multiples inconvénients, ils donnent leur vision de l'identité souveraine et la considèrent comme la prochaine et dernière étape de cette évolution ainsi qu'un modèle successeur du modèle user-centric. Une preuve de concept et une architecture pour un système d'identité décentralisé ont été proposés [59]. En ce qui concerne la gestion décentralisée de l'identité, le potentiel des registres distribués tels que la blockchain pour assurer le rôle de l'interaction des acteurs (émetteur, détenteur et vérificateur) a été mis en avant dans ces travaux.

Concernant l'approche abordée sur la SSI, il existe un fossé entre les industries, les fondations indépendantes et la recherche académique. Les deux premiers étant axés sur le code open source et les architectures logicielles pour la mise en œuvre de la SSI en tant que service. Bien qu'il s'agisse de codes open source, il manquait une analyse approfondie et de cadre formel sur les différentes solutions pour expliquer certains choix de mise en œuvre, par exemple le choix du registre (blockchain ou autre comme The Tangle). Ceci a conduit à la publication de nombreux travaux listés dans le tableau ainsi que d'autres trouvés sur google scholar. Certains d'entre eux proposent un cadre formel ou une étude complète de la SSI [14] [25][29] [31] [17] [19] [54], ainsi que sa compatibilité avec le règlement général sur la protection des données (RGPD) [16] [50]. D'autres travaux se concentrent sur les workflows pour sa création (étapes de création du DID et des VC jusqu'au vérificateur) [52], discutant des difficultés et des limites de ces concepts [45][30]. Des analyses et des comparaisons des implémentations de Sovrin et de uPort basées sur les exigences de la SSI ont été effectuées (par exemple en termes de longévité, de sécurité, de confidentialité, d'interface, d'évolutivité) [15]. Des architectures et des modèles de conception caractérisant la SSI ont été proposés pour le développement de logiciels [46] [22].

Notons que la SSI s'affranchit des autorités centrales, en se basant sur une gestion décentralisée, dans le sens où non seulement plusieurs entités collaborent pour gérer les VC, les DID, mais assurent également la réplication des données, leur persistance, et leur intégrité entre ces entités avec un code open source, contrairement aux solutions centralisées (modèle fédéré et centré sur l'utilisateur) qui sont généralement non transparentes. Les registres distribués tels que la blockchain semblent être de bons candidats pour répondre à ces exigences [20] [21] [26] [20].

De nombreux cas d'utilisation ont été proposé, nous en citons quelques-uns. Un système d'identité pour l'eGovernement a été proposé [13], où il est possible de déplacer et de connecter les identités centralisées et qualifiées du gouvernement au système SSI en convertissant le format des données pour qu'il corresponde au format SSI et passer à la gestion décentralisée en utilisant Hyperledger Indy, la transformation est faite via un

[7] https://www.coindesk.com/markets/2016/04/27/the-path-to-self-sovereign-identity/

agent agissant comme une interface. Un autre travail propose un modèle qui remplace le modèle classique de contrôle d'accès aux ressources [17], où le stockage de données sensibles telles que les attributs des utilisateurs est nécessaire. Dans leur modèle, la SSI permet l'accès aux ressources en associant les VCs et le registre distribué aux politiques d'accès. Le processus de révocation dans la SSI est une étape importante, un modèl a été proposé dans les scénarios du monde réel (par exemple, lorsqu'un officier de police révoque un VC) [18], Il permet la révocation des VCs lorsque le vérificateur est hors ligne.

Bien que la partie conceptuelle ait été abordée par la majorité des travaux cités ci-dessus, il manque un travail approfondi sur les SSI et la décentralisation basée sur les technologies des registres distribués. En effet, les blockchains dépendent principalement de protocoles, plus précisément d'algorithmes de consensus qui sont nécessaires pour assurer le fonctionnement et la gestion de ces registres. Ces consensus dépendent de plusieurs facteurs, tels que le cas d'utilisation qui influencera le choix du type de registre (avec permission ou public), la sécurité et l'intégrité du registre (par exemple PoW utilisant la chaîne de hachage [60] dans le bitcoin a été choisi pour éviter l'attaque sybil [61] et la falsification de la blockchain, RBFT (Redundant Byzantine Fault Tolerance) a été choisi dans Hyperedger Indy, où la blockchain est avec permission), l'autorisation ou non du fork (Bitcoin autorise le fork Hyperledger et Ripple [8] ne l'autorisent pas). Ceci nous amène à des axes de recherche avec plusieurs directions que nous résumons dans ce tableau:

Identité auto-souveraine (Self-Sovereign identity)		
Décentralisation		Conception et cas d'utilisation
Les algorithmes de consensus	Registre distribué	
PoW, PoS, Ripple PBFT, PoET RBFT, Paxos	Nécéssité d'une blockchain ou pas Type de Blockchains avec ou sans permission	Développement logiciel, cas d'applications standardisation, diagrammes et architectures du système concepts et modélisation

Où : PoW (Proof of Work), PoS (Proof of Stake), RBFT (Redundant Byzantine Fault Tolerance), (PoET) Proof of Elapsed Time.

Dans le paragraphe suivant nous examinons quelque travaux sur la SSI liés à l'environnement IoT, cela nous permettra d'identifier deux axes de recherche dans cette thématique.

Des cas d'utilisation, les technologies et les défis liés à l'application de la SSI dans le contexte de l'IoT ont été présentés [24]. Les auteurs fournissent une comparaison détaillée des cadres les plus prometteurs axés sur les SSI (Hyperledger Indy, uPort, BlockStack, VeresOne, Jolocom). Les défis soulignés par cet article illustrent les questions clés pour l'adoption et l'utilisation des SSI dans les domaines utilisant l'IoT. Dans l'article [34], les auteurs fournissent une analyse et une comparaison des modèles de données standard (PGP, X.509, SSI) en fonction de l'unicité de l'identifiant, de la gestion centralisée, des points de terminaison des services et soulignent que seul la SSI permet les schémas sémantiques. Ils discutent également des avantages de la SSI dans le contexte de l'IoT, tels que la confidentialité et la décentralisation, et établissent qu'il s'agit de la meilleure

[8] https://ripple.com/files/ripple_consensus_whitepaper.pdf

option pour la gestion de l'identité numérique dans les écosystèmes IoT. D'autres défis sont abordés, tels que les capacités de stockage des dispositifs IoT, le traitement limité et les ressources énergétiques pour les algorithmes de cryptographie très utilisés dans la SSI.

Une explication des contraintes de gestion d'identité des dispositifs IoT et une présentation des cadres les plus utilisés pour mettre en œuvre la gestion d'identité décentralisée (uPort, Hyperledger et Indy) a été considérée [40]. Les auteurs proposent également une nouvelle solution pour la gestion de l'identité des dispositifs IoT basée sur la SSI et le Tangle IOTA [62], qui est l'un de ces nouveaux modèles de technologie de registre distribué, comme une alternative à la Blockchain et fondamentalement axée sur l'IoT.

L'identification unique des dispositifs IoT via la SSI a été envisagée. Un travail se basant sur la blockchain Ethereum pour émettre un identifiant depuis le processus de fabrication basé sur la SRAM (Static random access memory) et la PUF (Physically Unclonable Function) a été proposé [27]. Un autre travail publié plus tard [63], où les auteurs considèrent l'identification des dispositifs depuis leur fabrication jusqu'à leur utilisation pour avoir une transparence sur leur origine et leur historique, ce qui assure une preuve d'origine pour la traçabilité des dispositifs. Leur approche est basée sur l'application du concept de SSI pour identifier les dispositifs et sur Blockchain pour assurer l'immuabilité et l'autonomie. Ils considèrent également l'enregistrement dans l'environnement du client en utilisant le bootstrapping des infrastructures de clés sécurisées à distance (BRSKI) [64]. Un prototype de mise en œuvre de la solution a été réalisé en utilisant la blockchain Ethereum et des jetons Web JSON (JWT). Ils fournissent une analyse des forces et des faiblesses d'un tel système.

Une preuve de concept d'un système basé sur la SSI a été développée pour le cas d'utilisation des réseaux de chargement des véhicules électriques [65], en utilisant Hyperledger Indy et Aries.

Une analyse approfondie est faite sur la façon d'utiliser SSI pour garantir que les taux d'émission produits par les dispositifs de l'Internet des véhicules (IoV) (un sous-type de dispositifs IoT) sont vérifiables et non falsifiés [2]. Dans cet article, Hyperledger Indy est utilisé pour authentifier et autoriser des entités sur un réseau Hyperledger Fabric.

Du point de vue de la recherche académique, la plupart des IdMSs basés sur la blockchain pour l'IoT représentent des solutions génériques, où la SSI est appliquée pour un cas d'utilisation particulier. Un autre sujet de recherche intéressant est l'intégration de la SSI dans l'environnement IoT en termes de décentralisation. Un environnement IoT présente de nombreux défis tels que les contraintes de ressources et de capacité de stockage comparé à l'utilisation de serveurs ou de dispositifs à haute performance tels que les GPU. Maintenant que le nombre d'IoT augmente, l'étude de la possibilité de décentraliser les tâches dans l'IoT, permettrait l'évolutivité lorsque des millions de dispositifs auront besoin d'une identité pour accéder aux ressources.

Dans [28], les auteurs se basent sur le Tangle, un registre différent de la blockchain et adapté à l'IoT, il ne nécessite ni processus de minage ni frais de transaction. Dans leur concept, chaque IoT crée sa propre identité. Il évalue la scalabilité avec une mise en œuvre de la preuve de concept, mais les capacités et les contraintes de l'IoT n'ont pas été précisées.

Le plus récent et premier article sur la décentralisation dans l'IoT en termes d'algorithmes de consensus a été publié en 2022 [51], ses auteurs proposent des algorithmes de consensus pour la blockchain adaptés à l'environnement IoT. Mais il n'y a pas de spécification sur son intégration dans la SSI. Il concerne principalement la thématique systèmes distribués.

Comme le titre de cet article l'indique, l'investigation de la SSI dans l'IoT, peut être interprétée par deux axes :

- Donner une identité aux dispositifs IoT, c'est-à-dire utiliser les concepts déjà existants et proposer des identités adaptées à un cas d'utilisation.
- Gérer la décentralisation de la SSI dans un environnement IoT, qui comprend des algorithmes de consensus et des registres distribués, gérés par des dispositifs IoT, en tenant compte des contraintes de l'environnement IoT, tels que les capacités de stockage et la performances du calcul ([24],[34]).

4. Le lien entre les systèmes distribués et la blockchain: niveau de décentralisation et type d'attaques dans un milieu décentralisé

Le cadre de gouvernance Hyperledger Indy/Sovrin est le cadre le plus largement utilisé pour gérer l'identité auto-souveraine selon les travaux précédents. Pour situer le contexte, le projet Hyperledger Indy fait partie de l'écosystème Hyperledger, hébergé par la Fondation Linux, et son objectif principal est de fournir un écosystème pour développer des solutions d'identité décentralisée. La blockchain d'Indy se caractérise par une blockchain à permission, le consensus est obtenu à l'aide de l'algorithme Plenum utilisant RBFT (Redundant Byzantine Fault Tolerance), une famille des algorithmes des systèmes distribués similaires aux PBFT, mais plus robustes [66].

L'objectif de cette section et de lier les systèmes distribués à la blockchain, pour expliquer les choix des industries dans les applications décentralisées, notamment Hyperledger Indy. Cette section nous permettra de comprendre le niveau de décentralisation d'un système reposant sur la blockchain et le type d'attaques considérées.

Le lien se situe principalement dans la réplications des machines à états (SMR: State Machine Replication) et l'ordre d'exécution des requêtes qui se ramène à un problème fondamentale dans les systèmes distribués: le problème du consensus.

Une décentralisation d'une tache en informatique nécessite la collaboration de plusieurs noeuds (processeurs) séparés pour réaliser un but spécifique. Par exemple, dans l'identité décentralisée, lorsque des requêtes de création du DID sont lancées, les noeuds participants du système qui maintiennent le registre distribué, exécutent un protocole pour se mettre d'accord sur l'ordre et la validité de la transaction. La disponibilité de cette information (DID dans le registre) à travers différents noeuds et le protocole de son exécution est un processus de réplication qui améliore la fiabilité et la performance des systèmes et s'affranchit d'un serveur central vulnérable aux attaques. La conservation de plusieurs copies fournit une meilleur protection et accessibilité à la donnée.

L'exemple ci-dessus s'inscrit dans la théorie des systèmes distribués dans un axe classique et bien étudié : Distributed information Systems. La représentation la plus courante pour modéliser un problème de réplication est les machines à états, dont l'objectif est d'assurer la copie d'une donnée vers plusieurs noeuds, sous plusieurs défis: cohérence, disponibilité, tolérance aux fautes byzantines (arrêt inopiné de la machine, exécution d'opération incorrecte, faute arbitraire (processus géré par un attaquant),etc.).

La cohérence d'un système sous le modèle SMR, consiste en sa capacité à converger vers un état unique lorsque les transactions sont mises à jour. Une base de donnée incohérente engendre des conflits qui mettent en cause la fiabilité du système.

Pour gérer une requête dans un système cohérent, le problème de coordination, qui exige que les noeuds se mettent d'accord sur une sortie commune sur la base d'une d'entrées (éventuellement conflictuelles); est fondamentale. Pour considérer des éventualités réelles, le système suppose l'existence de noeuds défaillants dont le fonctionnement est byzantin (faulty, explication de byzantin présentée dans le paragraphe précédent) et non défaillants dans le processus fonctionne correctement. D'où la problématique du consensus. Tout algorithme de consensus doit garantir les propriétés suivantes :

- Propriétés de vivacité: tous les nœuds non défaillants finissent par prendre une décision.
- Propriétés de sûreté: tous les nœuds non défaillants s'accordent sur les mêmes valeurs.

La blockchain du Bitcoin rentre bien dans ce cadre, puisque l'objectif est d'ordonner totalement les transactions sur un registre distribué, constitué d'une chaîne de hachage de blocs. Le consensus est ici obtenu par le biais de ce que l'on appelle Preuve de travail (PoW), un défi mathématique basé sur le hachage qu'on appelle le minage, il est très exigeant en termes de calcul. N'importe qui peut télécharger le code du minage du Bitcoin et commencer à participer au protocole, en ne connaissant qu'un seul noeud au départ. C'est une caractéristique très puissante des blockchains basées sur PoW, elle traitent de manière inhérente l'attaque Sybil [67] [68].

Une famille particulièrement intéressante proche de la blockchain est celle avec des protocoles de réplication de machine à états tolérants aux fautes byzantines (BFT), qui promettent un consensus même en présences de noeuds malveillants (byzantins). Historiquement, ils ont été reconnus comme étant très difficiles à concevoir et à mettre en oeuvre. Le premier protocole (PBFT) garantissant des propriétés de sûreté et de vivacité utilisable dans un système réel a été conçu par Barbara Liskov et Miguel Castro [69]. Les protocoles de telles famille (BFT) font l'objet d'un examen académique détaillé et sont accompagnés de preuves mathématiques pour démontrer les propriétés du consensus. Ceci n'est pas courant dans les nouvelles blockchain où même celle du Bitcoin qui sont rarement accompagnée d'analyse formelle de la sécurité du système distribué.

Bien que nous ne détaillerons pas le fonctionnement du BFT, les éléments de cette section nous permettent d'évoquer des différences fondamentales entre la blockchaine et les algorithmes classiques de BFT, notamment en terme de décentralisation et le type d'attaques considérées [67] [68]:

- **Niveau de décentralisation.** La blockchain basée sur la PoW est entièrement décentralisée. Connaître l'identité des noeuds n'est pas obligatoire contrairement à la Famille de protocoles BFT, qui exige que chaque noeud doit connaître l'identité des noeuds impliqués dans le protocoles. Ce qui nécessite une gestion centralisée de l'identité, où un tiers de confiance émet des identités et des certificats d'authenticité des noeuds. D'où la notion blockchain avec permission (où l'exigence des identité peut être imposée) et Blockchain public basée sur la PoW qui dépendent du cas d'application. Ce qui explique en partie le choix des industriels sur les types de blockchain.
- **Type d'attaques considérées** Dans la blockchain basées sur la PoW on tient compte de la puissance du hashage qui dépend de la puissance de calcul. Au début du Bitcoin, on pensait que tant que l'adversaire contrôle moins de 50% de la puissance de calcul, le système est invulnérable. Plus tard il a été démontré qu'il est vulnérable même si l'attaquant contrôle 25 % de la puissance de calcul. En revanche, les familles de protocoles BFT avec n noeuds dans le système, peuvent tolérer au maximum $\frac{n}{3}$ noeuds byzantins. Cette assertion se généralise lorsqu'un adversaire contrôle un sous-ensemble de noeuds[70].

Notons qu'il existe d'autres facteurs associés aux deux précédents qui justifient les choix industriels, tels que la scalabilité, la performance, des hypothèses de synchronisation du réseau et l'existence de preuves formelles d'exactitude des protocoles [67] [68].

Lorsqu'un projet nécessite un système pérenne, répliqué dans un registre cohérent, de manière décentralisée (plusieurs niveaux de décentralisation sont possibles), qui fournit un historique complet de transactions vérifiées, alors la blockchain serait un bon candidat. En revanche, si le système ne requiert pas de telles exigences, une simple base de donnée chiffrée peut être utilisée. Si la blockchain est choisi, les éléments cités précédemment impactent les prises de décisions liées à l'architecture du système, tels que le problème du consensus et les types de blockchain.

5. Conclusion

Comme pour la finance décentralisée, la Blockchain inspire une transformation fondamentale sur la vision de l'identité et la confiance en ligne. Pourtant, l'identité et l'argent sont très étroitement liés en terme de valeur, et ce n'est qu'en 2015 que le modèle décentralisé de l'identité a émergé. Dans ce travail une explications des concepts et le potentiel de la SSI a été rappelé ainsi qu'un état de l'art permettant d'identifier les problématiques, les cas d'applications et les axes de recherche majeurs pour la mise en place de l'identité décentralisé dans l'IoT. Ce travail présente aussi une comparaison entre la blockchain et les algorithmes de consensus en terme de décentralisation et de sécurité et les éléments importants à considérer pour des projets décentralisés. Les travaux menés dans cet article ouvrent des pistes pour de futurs travaux. Nous envisageons de nous diriger vers l'axe de la décentralisation dans l'IoT, une première piste dans cette direction est de proposer un algorithme du leader election adapté à l'environnement IoT qui sera ensuite testé et comparé avec le consensus de Hyperledger Indy.

References

[1] S. Asiri, A. Miri, A sybil resistant iot trust model using blockchains, in: 2018 IEEE International Conference on Internet of Things (iThings), IEEE, 2018, pp. 1017–1026.

[2] S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras, I. Stamelos, Securing emission data of smart vehicles with blockchain and self-sovereign identities, in: 2020 IEEE International Conference on Blockchain, IEEE, 2020, pp. 462–469.

[3] E. Bertino, K. Takahashi, Identity management: Conceptite, technologies, and systems, Artech House, 2010.

[4] X. Zhu, Y. Badr, Identity management systems for the internet of things: a survey towards blockchain solutions, Sensors 18 (2018) 4215.

[5] D. Van Bokkem, R. Hageman, G. Koning, L. Nguyen, N. Zarin, Self-sovereign identity solutions: The necessity of blockchain technology, arXiv preprint arXiv:1904.12816 (2019).

[6] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair, Z. Cui, Distributed, secure, self-sovereign identity for iot devices, in: 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), IEEE, 2020, pp. 1–6.

[7] A. Preukschat, D. Reed, Self-sovereign identity, Manning Publications, 2021.

[8] J. Camenisch, A. Lysyanskaya, A signature scheme with efficient protocols, in: International Conference on Security in Communication Networks, Springer, 2002, pp. 268–289.

[9] L. M. Bach, B. Mihaljevic, M. Zagar, Comparative analysis of blockchain consensus algorithms, in: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Ieee, 2018, pp. 1545–1550.

[10] S. M. H. Bamakan, A. Motavali, A. B. Bondarti, A survey of blockchain consensus algorithms performance evaluation criteria, Expert Systems with Applications 154 (2020) 113385.

[11] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Decentralized Business Review (2008) 21260.

[12] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, International Journal of Web and Grid Services 14 (2018) 352–375.

[13] A. Abraham, K. Theuermann, E. Kirchengast, Qualified eid derivation into a distributed ledger based idm system, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1406–1412.

[14] M. S. Ferdous, F. Chowdhury, M. O. Alassafi, In search of self-sovereign identity leveraging blockchain technology, IEEE Access 7 (2019) 103059–103079.

[15] N. Naik, P. Jenkins, uport open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain, in: 2020 IEEE International Symposium on Systems Engineering (ISSE), 2020, pp. 1–7.

[16] N. Naik, P. Jenkins, Your identity is yours: Take back control of your identity using gdpr compatible self-sovereign identity, in: 2020 7th International Conference on Behavioural and Social Computing (BESC), 2020, pp. 1–6. doi:10.1109/BESC51023.2020.9348298.

[17] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, S. Guerreiro, Ssibac: Self-sovereign identity based access control, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1935–1943. doi:10.1109/TrustCom50675.2020.00264.

[18] A. Abraham, S. More, C. Rabensteiner, F. Hörandner, Revocable and offline-verifiable self-sovereign identities, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1020–1027. doi:10.1109/TrustCom50675.2020.00136.

[19] N. Naik, P. Jenkins, Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology, in: 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2020, pp. 90–95. doi:10.1109/MobileCloud48802.2020.00021.

[20] J. Kaneriya, H. Patel, A comparative survey on blockchain based self sovereign identity system, in: 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1150–1155. doi:10.1109/ICISS49785.2020.9315899.

[21] M. P. Bhattacharya, P. Zavarsky, S. Butakov, Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain, in: 2020 International Symposium on Networks, Computers and Communications (ISNCC), 2020, pp. 1–7. doi:10.1109/ISNCC49221.2020.9297357.

[22] A. Grüner, A. Mühle, C. Meinel, Atib: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider, IEEE Access 9 (2021) 138553–138570.

[23] E. Samir, H. Wu, M. Azab, C. Xin, Q. Zhang, Dt-ssim: A decentralized trustworthy self-sovereign identity management framework, IEEE Internet of Things Journal 9 (2022) 7972–7988.

[24] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, J. Ferreira, Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot, in: 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1173–1180.

[25] N. Naik, P. Jenkins, Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems, in: 2020 IEEE International Symposium on Systems Engineering (ISSE), 2020, pp. 1–6.

[26] K. Gilani, E. Bertin, J. Hatin, N. Crespi, A survey on blockchain-based identity management and decentralized privacy for personal data, in: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020, pp. 97–101.

[27] S. R. Niya, B. Jeffrey, B. Stiller, Kyot: Self-sovereign iot identification with a physically unclonable function, in: 2020 IEEE 45th Conference on Local Computer Networks (LCN), 2020, pp. 485–490.

[28] M. Luecking, C. Fries, R. Lamberti, W. Stork, Decentralized identity and trust

management framework for internet of things, in: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1–9.
[29] N. Naik, P. Jenkins, Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology, in: 2021 IEEE International Symposium on Systems Engineering (ISSE), 2021, pp. 1–7.
[30] Q. Stokkink, G. Ishmaev, D. Epema, J. Pouwelse, A truly self-sovereign identity system, in: 2021 IEEE 46th Conference on Local Computer Networks (LCN), 2021, pp. 1–8.
[31] S. Cucko, M. Turkanovik, Decentralized and self-sovereign identity: Systematic mapping study, IEEE Access 9 (2021) 139009–139027.
[32] H. Yildiz, C. Ritter, L. T. Nguyen, B. Frech, M. M. Martinez, A. Kupper, Connecting self-sovereign identity with federated and user-centric identities via saml integration, in: 2021 IEEE Symposium on Computers and Communications (ISCC), 2021, pp. 1–7.
[33] D. Drusinsky, Cryptographic;biometric self-sovereign personal identities, Computer 55 (2022) 96–102.
[34] G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. Calcina Ccori, W. T. Pereira, M. K. Zuffo, Self-sovereign identity for iot environments: A perspective, in: 2020 Global Internet of Things Summit (GIoTS), 2020, pp. 1–6.
[35] J. Liu, A. Hodges, L. Clay, J. Monarch, An analysis of digital identity management systems - a two-mapping view, in: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020, pp. 92–96.
[36] D. Kirupanithi, A. Antonidoss, Self-sovereign identity creation on blockchain using identity based encryption, in: 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 299–304.
[37] S. Terzi, C. Savvaidis, A. Sersemis, K. Votis, D. Tzovaras, Decentralizing identity management and vehicle rights delegation through self-sovereign identities and blockchain, in: 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), 2021, pp. 1217–1223.
[38] A. Küpper, Decentralized identifiers and self-sovereign identity - a new identity management for 6g integration? : Mobilecloud 2021 invited talk, in: 2021 IEEE International Conference on Joint Cloud Computing (JCC), 2021, pp. 71–71.
[39] A. Abraham, K. Koch, S. More, S. Ramacher, M. Stopar, Privacy-preserving eid derivation to self-sovereign identity systems with offline revocation, in: 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2021, pp. 506–513.
[40] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair, Z. Cui, Distributed, secure, self-sovereign identity for iot devices, in: 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 2020, pp. 1–6.
[41] M. Kuperberg, Blockchain-based identity management: A survey from the enterprise and ecosystem perspective, IEEE Transactions on Engineering Management 67 (2020) 1008–1027.
[42] S. Lim, M.-H. Rhie, D. Hwang, K.-H. Kim, A subject-centric credential management method based on the verifiable credentials, in: 2021 International Conference on

Information Networking (ICOIN), 2021, pp. 508–510.
[43] K.-H. Kim, S. Lim, D.-Y. Hwang, K.-H. Kim, Analysis on the privacy of did service properties in the did document, in: 2021 International Conference on Information Networking (ICOIN), 2021, pp. 745–748.
[44] N.-C. Ursache, Swarm communication using self sovereign identities, in: 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2021, pp. 1–6.
[45] C. Brunner, U. Gallersdörfer, F. Knirsch, D. Engel, F. Matthes, Did and vc:untangling decentralized identifiers and verifiable credentials for the web of trust, in: 2020 the 3rd International Conference on Blockchain Technology and Applications, ICBTA 2020, Association for Computing Machinery, New York, NY, USA, 2020, pp. 61–66.
[46] Y. Liu, Q. Lu, H.-Y. Paik, X. Xu, Design patterns for blockchain-based self-sovereign identity, in: Proceedings of the European Conference on Pattern Languages of Programs 2020, EuroPLoP '20, Association for Computing Machinery, New York, NY, USA, 2020.
[47] V. Bolgouras, A. Angelogianni, I. Politis, C. Xenakis, Trusted and secure self-sovereign identity framework, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22, Association for Computing Machinery, New York, NY, USA, 2022.
[48] S. Liu, T. Mu, S. Xu, G. He, Research on cross-chain method based on distributed digital identity, in: The 2022 4th International Conference on Blockchain Technology, ICBCT'22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 59–73.
[49] X. Fan, Q. Chai, L. Xu, D. Guo, Diam-iot: A decentralized identity and access management framework for internet of things, in: Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, BSCI '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 186–191.
[50] G. Kondova, J. Erbguth, Self-sovereign identity on public blockchains and the gdpr, in: Proceedings of the 35th Annual ACM Symposium on Applied Computing, SAC '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 342–345.
[51] H. Niavis, K. Loupos, Consenseiot: A consensus algorithm for secure and scalable blockchain in the iot context, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22, Association for Computing Machinery, New York, NY, USA, 2022.
[52] R. Nokhbeh Zaeem, K. C. Chang, T.-C. Huang, D. Liau, W. Song, A. Tyagi, M. Khalil, M. Lamison, S. Pandey, K. S. Barber, Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study, in: IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, WI-IAT '21, Association for Computing Machinery, 2021, pp. 128–135.
[53] W. Song, R. Nokhbeh Zaeem, D. Liau, K. C. Chang, M. R. Lamison, M. M. Khalil, K. S. Barber, Self-sovereign identity and user control for privacy-preserving contact tracing, in: IEEE/WIC/ACM International Conference on Web Intelligence and

Intelligent Agent Technology, WI-IAT '21, Association for Computing Machinery, New York, NY, USA, 2021, pp. 438–445.
[54] A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, A survey on essential components of a self-sovereign identity, Computer Science Review 30 (2018) 80–86.
[55] M. Shuaib, S. Alam, M. S. Nasir, M. S. Alam, Immunity credentials using self-sovereign identity for combating covid-19 pandemic, Materials Today: Proceedings (2021).
[56] M. Shuaib, S. Alam, M. S. Alam, M. S. Nasir, Self-sovereign identity for healthcare using blockchain, Materials Today: Proceedings (2021).
[57] V. Schlatt, J. Sedlmeir, S. Feulner, N. Urbach, Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity, Information & Management (2021) 103553.
[58] A. Tobin, Sovrin: What goes on the ledger?, Evernym/Sovrin Foundation (2018) 1–11.
[59] D. Baars, Towards self-sovereign identity using blockchain technology, Master's thesis, University of Twente, 2016.
[60] C. Dwork, M. Naor, Pricing via processing or combatting junk mail, in: Annual international cryptology conference, Springer, 1992, pp. 139–147.
[61] J. R. Douceur, The sybil attack, in: International workshop on peer-to-peer systems, Springer, 2002, pp. 251–260.
[62] S. Popov, The tangle, White paper 1 (2018).
[63] T. Weingaertner, O. Camenzind, Identity of things: Applying concepts from self sovereign identity to iot devices, The Journal of The British Blockchain Association (2021) 21244.
[64] M. Pritikin, M. Richardson, M. Behringer, S. Bjarnason, K. Watsen, Bootstrapping remote secure key infrastructures (brski), Internet-Draft draft-ietf-anima-bootstrapping-keyinfra-18, IETF (2019).
[65] F. Capela, Self-Sovereign Identity for the Internet of Things: A Case Study on Verifiable Electric Vehicle Charging, Ph.D. thesis, 2021.
[66] P.-L. Aublin, S. B. Mokhtar, V. Quéma, Rbft: Redundant byzantine fault tolerance, in: 2013 IEEE 33rd International Conference on Distributed Computing Systems, IEEE, 2013, pp. 297–306.
[67] M. Vukolić, The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in: International workshop on open problems in network security, Springer, 2015, pp. 112–125.
[68] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone, Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain (2018).
[69] M. Castro, B. Liskov, et al., Practical byzantine fault tolerance, in: OsDI, volume 99, 1999, pp. 173–186.
[70] R. Guerraoui, M. Vukolić, Refined quorum systems, in: Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing, 2007, pp. 119–128.