Les blockchains ont-elles quelque chose pour offrir une identité ?

22 février 2018

Introduction

Auteurs
Steve Olshansky
Internet Society

Steve Wilson
Lockstep Consulting
Steve Wilson est un chercheur indépendant, innovateur, conseiller et analyste en identité numérique
et vie privée.
Voir http://lockstep.com.au

Collaborateur
Robin Wilton

Nous avons écrit cet article parce que la gestion des identités et des accès (GIA) est devenue essentielle à nos interactions en ligne. Comme beaucoup d'infrastructures, lorsqu'elles sont bien conçues et mises en œuvre, la GIA est en grande partie invisible pour les utilisateurs. Pour cette raison, bon nombre de ceux qui ne sont pas activement engagés sur ce sujet ne sont pas pleinement conscients de son omniprésence et de son impact sur notre vie quotidienne.

Blockchain (chaîne de blocs) est une large classe de méthodes relativement nouvelles de sécurité des données, avec certaines propriétés de valeur potentielle en GIA. La technologie Blockchain suscite beaucoup d'enthousiasme. De nombreuses start-up en GIA ont lancé des solutions d'enregistrement d'identité « sur la chaîne de blocs », tandis que d'autres développent une nouvelle infrastructure inspirée de la chaîne de blocs pour la distribution des attributs, qui est un élément clé de la GIA. Face au battage médiatique croissant, associé de scepticisme, nous cherchons ici à fournir un point de vue équilibré, et à clarifier les façons dont les technologies blockchain peuvent ou non répondre aux besoins de GIA. Peut-être plus important encore, nous espérons fournir un point de vue utile permettant d'évaluer les solutions GIA actuelles et nouvelles basées sur la blockchain au fur et à mesure qu'elles se présentent.

En réfléchissant à la façon dont ces technologies passionnantes peuvent contribuer à la GIA, il faudrait commencer par comprendre ce à quoi les premières chaînes de blocs ont été destinées, avant de s'en servir prudemment comme base, avec une analyse système précise. Ainsi, le document devrait aider ceux qui conçoivent de nouvelles solutions GIA, et ceux susceptibles d'acquérir des solutions et ayant besoin d'évaluer de nouvelles approches basées sur la technologie blockchain.

Ce document est destiné au personnel et à la direction de la technologie de l'information, et à tous ceux qui travaillent sur ou avec les technologies de GIA, et qui sont curieux d'en savoir plus sur la blockchain et son impact sur la GIA. Nous donnerons tout d'abord des informations sur la blockchain, puis sur la GIA, et ensuite des recommandations pour les lier ensemble.

Résumé

La GIA est devenue une infrastructure essentielle pour nos interactions en ligne. Elle évolue rapidement, les enjeux sont élevés et les entreprises font face à un paysage d'identité numérique de plus en plus complexe et déroutant. On s'inquiète de plus en plus du fait que beaucoup d'entreprises du numérique en savent trop sur nous, et le contrôle de l'identité devrait en quelque sorte être récupéré par les utilisateurs finaux. La GIA est donc un sujet brûlant, avec de nouvelles architectures, modèles commerciaux et philosophies en jeu.

La technologie blockchain[1] attire l'attention, positive et négative, et fait l'objet d'un large battage médiatique. Les adeptes préconisent son utilisation dans une grande variété de situations, y compris la GIA.

Blockchain a surgi à un moment critique, avec une série de promesses liées à la sécurité, dont beaucoup d'entre elles apparemment applicables à l'identité, même si ce n'est que vaguement. De nombreuses entreprises de GIA ont vu le jour « sur la blockchain », et des revendications générales ont été faites selon lesquelles cette nouvelle famille de solutions perturberait la GIA traditionnelle. Bien que les cas d'utilisation et les exigences varient, le fait d'ajouter simplement des technologies blockchain à un système GIA sans prendre soigneusement en compte tous les facteurs, n'apportera pas nécessairement une réelle amélioration et pourrait en fait avoir l'effet inverse. Comme toute technologie, les blockchains sont simplement des outils, à considérer prudemment dans le contexte de votre environnement particulier. Cet article présente une série de questions d'analyse et de conception à prendre en compte lors de l'application des technologies blockchain à la GIA, en consultation avec le personnel technique concerné.

Cet article cherche à explorer impartialement l'adéquation entre la technologie blockchain et la GIA pour les cas d'utilisation d'identité personnelle. Nous discutons de l'évolution de blockchain et de son applicabilité à la GIA, repérons les aspects pertinents de l'espace problème, et identifions les questions clés à traiter lors de l'examen de blockchain. Les technologies blockchain évoluent rapidement, et il faut s'attendre à ce que l'adéquation avec la GIA change, mais à ce stade, il n'y a aucune précipitation à avoir ni aucune raison de craindre de passer à côté. Nous montrons que les blockchains d'origine ne sont généralement pas adaptées à la gestion des identités, et nous essayons d'esquisser, à ce stade précoce, où de nouveaux développements de blockchains pourraient répondre aux besoins de GIA.

Nous présumons que vous êtes familiarisé(e) avec la GIA et la technologie blockchain. Toute personne intéressée à en apprendre davantage sur l'un ou l'autre de ces sujets, trouvera une liste de bonnes références à la fin du document.

1 Au moment de la rédaction, la terminologie dans ce nouveau domaine est en constante évolution. Pour les besoins de cet article, nous utilisons les « blockchains » au sens large pour englober les chaînes de blocs distribuées publiques créées pour Bitcoin et d'autres crypto-monnaies, ainsi que les développements plus récents, parfois appelées technologies du grand livre comptable distribué ou partagé.

Blockchain, chaînes de blocs et « grands livres comptables distribués »

Pourquoi la blockchain (ou, plus généralement, les « technologies blockchain ») est-elle promue comme une solution utile aux problèmes actuels de GIA en ligne ? Bien qu'il y ait beaucoup de battage médiatique à ce sujet, et en même temps des gens proposant son utilisation dans divers contextes, il y a des problèmes particuliers à l'identité que certains considèrent comme résolubles avec des algorithmes de chaînes de blocs et dérivés associés.

Caractéristiques et propriétés de sécurité des technologies blockchain en pleine évolution

Blockchains publiques de première génération p. ex. Bitcoin, Ethereum	**Technologies blockchain avancées/spéciales** p. ex. Corda, Fabric, Plenum, Hashgraph
Réseaux largement distribués et fortement décentralisés	Tendent à être plus concentrés ; plus petit nombre de participants ou de nœuds
Sans droit d'accès	Contrôles d'accès pour écrire et/ou lire
Réseau pair-à-pair public de nœuds	Peut être un réseau physique ou virtuel privé
Immuable par le poids des chiffres dans le réseau	Avec un plus petit groupe de participants, la résistance à l'altération peut exiger une sécurité traditionnelle au niveau des nœuds
Libre et open source	Peut être un logiciel propriétaire et/ou un réseau commercial

La chaîne de blocs d'origine a été développée pour résoudre un problème particulier : la « double dépense » de crypto-monnaie sans administrateur central. Le problème intrinsèque de la monnaie purement virtuelle est que rien n'interdit fondamentalement la duplication de l'argent ; une sorte de surveillance est nécessaire pour éviter les doubles dépenses. Même si divers systèmes de paiement électronique existent depuis des décennies (l'un des premiers étant *Digicash* fondé en 1989), ils ont toujours impliqué une autorité centrale pour surveiller les doubles dépenses. Blockchain a permis à la première crypto-monnaie pair-à-pair, à savoir Bitcoin, de fonctionner sans intermédiaires et sans « banque de réserve » numérique. Un réseau public massif surveille chaque mouvement Bitcoin, en conservant un registre grand public toujours croissant - la chaîne de blocs - de chaque transaction réalisée. Les nœuds de réseau exécutent chacun un logiciel blockchain open source et sont récompensés pour leur participation par des allocations aléatoires de Bitcoin.[2]

La chaîne de blocs Bitcoin d'origine est fortement distribuée, [3]sans point de contrôle unique (ou échec) et ne peut pas être modifiée une fois écrite. Décentralisé, pratiquement

2 Les détails ne doivent pas nous intéresser ici, mais en bref, certains nœuds « pleins » du réseau Bitcoin sont récompensés par un paiement de prime qui va au premier nœud qui termine une tâche de « preuve de travail » en force brute, dont la difficulté immunise le grand livre comptable contre la falsification et la contrefaçon. Les chances de gagner la prime augmentent avec la quantité de puissance de calcul mise dans la tâche ; l'exécution d'un nœud complet est appelée « minage ».

3 Notez avec attention qu'il existe plusieurs aspects de la décentralisation dans les technologies blockchain, et que le degré de décentralisation envisagé par ses concepteurs originaux n'a pas été égal. Le problème est trop vaste pour être couvert dans ce document, mais en résumé, les architectures de blockchain peuvent décentraliser *le stockage et la disponibilité* du grand livre comptable, et/ou le *processus pour parvenir à un consensus* sur l'état du livre. Ce dernier, connu sous le nom de « minage » dans les blockchains publiques, était censé rester fortement distribué et donc résistant à la corruption, mais en fin de compte, le minage de Bitcoin est devenu si lucratif qu'il a concentré massivement cette activité et compromis la sécurité de Bitcoin, au moins en théorie. Un autre aspect de la décentralisation est la *gouvernance*, qui doit encore être correctement organisée dans les blockchains publiques de Bitcoin et Ethereum. La prise de décision pour la maintenance logicielle importante s'est révélée difficile ou même impossible avec Bitcoin, et à l'occasion, elle est tombée à une seule personne avec Ethereum.

immuable et cryptographiquement vérifiable, ce type de blockchain semble se prêter à d'innombrables applications au-delà des paiements, y compris la GIA, pour réduire la fraude, supprimer les goulots d'étranglement et retracer la provenance de données multipartites complexes. Ces propriétés sont importantes pour la GIA et il y a donc eu une vague de recherche et de développement sur blockchain pour la GIA, parmi beaucoup d'autres choses. Les quatre ou cinq dernières années ont connu une évolution frénétique. Le système Bitcoin d'origine et ses dérivés étroitement liés représentent une classe de blockchains *publiques*. Des algorithmes descendants plus avancés, développés pour des cas d'utilisation plus complexes que la crypto-monnaie, fournissent différentes combinaisons de propriétés.

Authentification et autorisation

Comme indiqué ci-dessus, la GIA évolue rapidement, les enjeux sont élevés et les entreprises font face à un paysage d'identité numérique de plus en plus complexe et déroutant. Lorsque tout fonctionne bien, la plupart des mécanismes de GIA restent soigneusement cachés aux utilisateurs, qui sont généralement plus intéressés par un accès pratique et fiable aux services que d'être « identifiés » comme tels. Les technologies mobiles avec une cryptographie et une biométrie intégrées puissantes sont devenues des authentificateurs populaires. En même temps, il y a une frustration généralisée et une inquiétude grandissante face au fait que de nombreuses entreprises numériques en savent trop sur nous, et que le contrôle de nos informations et de notre identité devrait en quelque sorte être récupéré par les utilisateurs finaux.

Lorsque l'on considère le potentiel perturbateur de technologies comme blockchain, il est d'autant plus important d'être clair sur le problème que nous essayons de résoudre. Si l'on pense que blockchain a le potentiel d'améliorer la qualité et la disponibilité des informations sur les parties avec lesquelles nous essayons de négocier, examinons d'abord ce sur quoi portent l'authentification et l'autorisation.

La question essentielle quant à la GIA peut être formulée comme suit : dans un contexte particulier, que doit-on savoir sur une contrepartie pour pouvoir traiter avec elle (c'est-à-dire accepter une transaction ou un objet numérique) ? Dans la plupart des milieux d'affaires, il est moins important de savoir *qui* est quelqu'un que *ce* qu'il est. Par exemple, quelle est sa qualification professionnelle ? Ou quelle est son appartenance à une organisation, sa relation avec un fournisseur de services, son pays d'origine, ses droits à un service gouvernemental, son statut de client commercial ou son âge, le cas échéant ? Ce sont les sortes de données (attributs alias) qui sont utilisées dans les décisions de contrôle d'accès à granularité fine (ou basées sur des attributs).

Ces types de questions doivent être posés au moment de la conception, lors de l'évaluation des risques de la transaction envisagée et de l'analyse des exigences d'authentification et d'autorisation. Différents moyens peuvent être explorés pour que les systèmes de transaction obtiennent les attributs d'identité nécessaires au bon moment, par exemple lorsque les utilisateurs s'enregistrent pour des services ou lorsqu'ils effectuent des transactions. Ceci introduit un autre ensemble de décisions de conception : l'identification initiale lors de l'enregistrement ne doit pas être aussi rigoureuse, par exemple, si d'autres atténuations des risques (telles que la notation des risques en temps réel pour détecter la fraude) sont disponibles. Lors de la conception de systèmes d'identification, nous devons

décider quelle qualité d'information est nécessaire, où cette information sera obtenue et comment elle sera validée.

Terminologie : Les principaux intervenants de l'analyse et de la conception de la gestion des identités GIA
s'articulent autour d'un ensemble d'acteurs ou de rôles, comme suit :

Le **Sujet** (alias utilisateur) est la personne ou l'entité qui est identifiée ou nommée dans une transaction et qui reçoit généralement des services en fonction de son identité ou de ses attributs. Les sujets sont généralement des clients, des employés, des titulaires de comptes, etc.

Relying Party (RP, alias Service Provider - SP) est une entité effectuant des transactions avec un Sujet, fournissant des services, et dépendant généralement d'un tiers pour confirmer l'identité ou les attributs du Sujet. Les RP typiques sont les détaillants, les employeurs, les institutions financières, les organismes gouvernementaux, les services publics et autres.

Le **Fournisseur d'identité (IdP, Identity Provider)** est une partie qui garantit l'identité d'un Sujet selon un protocole d'identification convenu. Dans les architectures GIA classiques, l'IdP est généralement une tierce partie (comme une agence gouvernementale, un établissement d'enseignement, un employeur ou un service d'identification commerciale), mais dans les affaires conventionnelles, de nombreux RP comme les banques assument la responsabilité de l'identification et agissent donc comme étant leurs propres IdP.

L'**Autorité/le fournisseur d'attribut** est souvent l'IdP mais peut également être une entité distincte échappant au contrôle direct du fournisseur d'identité. De même, il pourrait y avoir des « courtiers d'attributs » externes qui se procurent et regroupent les attributs d'un nombre quelconque de sources. Il appartient en fin de compte au RP de décider de la confiance à accorder aux sources d'attributs.

Certains paramètres de GIA impliquent des fournisseurs d'attributs distincts et des intermédiaires supplémentaires. En général, les RP ont tendance à supporter la plus grande partie du risque dans une transaction et ont généralement le dernier mot quant à savoir si un protocole d'identification est adapté à l'objectif ou non. Les obligations contractuelles des fournisseurs d'accès à l'égard des RP, des garanties et des dispositions en matière de responsabilité sont des sujets de discussion récurrents en GIA. Ainsi, dans les applications conservatrices ou à risque plus élevé, telles que les services gouvernementaux, les soins de santé et les services financiers, les RP agissent souvent comme étant leurs propres IdP.

Revendications / Attributs / Assertions

En GIA, les choses que nous devons savoir sur les contreparties sont appelées revendications, attributs ou assertions. De nombreuses formalités de gestion des risques, comme les règles d'identification des clients des banques, se concentrent sur des sous-ensembles communs d'attributs, tels que le « nom légal » d'un document gouvernemental officiel, la date de naissance et l'adresse résidentielle.

En structurant la GIA pour se concentrer sur des attributs spécifiques dans des contextes différents, nous pouvons réduire l'accumulation d'informations superflues (ce qui représente de plus en plus une responsabilité pour de nombreuses entreprises, à la lumière de l'épidémie de violations de données). Le « Principe du besoin de savoir »[4] s'applique en

4 https://security.berkeley.edu/need-know-access-control-guideline

minimisant la collecte et la divulgation de données, ce qui est bon pour la confidentialité. La pertinence pour l'authentification des technologies blockchain devrait ainsi devenir plus claire. En fonction des risques inhérents à l'application prévue, les concepteurs de GIA doivent décider de la confiance nécessaire dans les attributs présentés (déclarés) par les utilisateurs.
Les données auto-déclarées sont-elles suffisantes ou une validation externe par un tiers de confiance est-elle nécessaire ? Le groupe de travail sur les revendications vérifiables du Consortium World Wide Web (W3C) [5]réalise un travail prometteur pour permettre la vérification externe des revendications, quel que soit l'endroit où elles sont stockées.

Provenance

L'un des sujets d'actualité de la GIA est la *provenance*. Si nous nous concentrons sur les attributs précis qui sont utilisés pour authentifier les personnes avec lesquelles nous traitons, comment savons-nous que les attributs sont fiables ? Autrement dit, que devons-nous savoir sur les attributs ? Les métadonnées d'authentification d'intérêt les plus évidentes comprennent l'attribut émetteur : quelle école a délivré le diplôme universitaire ? L'âge de quelqu'un est-il obtenu à partir d'un registre public des naissances, d'un département des véhicules à moteur (DVM) ou d'un réseau social ? Il peut également être important de connaître l'âge d'un attribut, sa date d'expiration, où et comment il a été stocké et protégé contre la falsification, et comment l'attribut est lié au sujet.

Pour certains attributs personnels, il existe une source d'autorité évidente. Les qualifications professionnelles, par exemple, sont généralement délivrées par des organismes professionnels et les numéros de cartes de crédit sont créés par les banques émettrices. Mais d'autres revendications, comme l'adresse de l'employeur ou du domicile, pourraient provenir de plusieurs sources. Le concept d'une « économie d'attributs » surgit dans certaines discussions sur les données personnelles[6] et nous pouvons nous attendre à voir émerger un marché contestable de fournisseurs d'attributs. Mais dans tous les cas, un attribut est aussi fiable que notre certitude quant à sa provenance et notre confiance dans la source.

Évolution des blockchains

Fondamentalement, les problèmes inhérents à la crypto-monnaie pair-à-pair comme Bitcoin sont différents de ceux de la gestion des identités et des accès ; ces différences doivent être comprises avant d'essayer de faire correspondre les technologies blockchain à la GIA. Les tentatives d'aborder ces problèmes pour différents cas d'utilisation ont entraîné des changements significatifs dans la manière dont les chaînes de blocs opèrent et fonctionnent.

Les blockchains ont surgi comme une nouvelle façon de superviser certaines transactions entre des personnes qui n'ont pas besoin de se connaître ou de se faire confiance, et qui choisissent de ne compter sur aucun administrateur central. Dans un sens plus général, les technologies blockchain peuvent être utilisées pour établir un consensus sur l'état d'un ensemble de données partagées, composé de multiples contributions en temps réel, sans surveillance centrale. Avec Bitcoin, le consensus porte spécifiquement sur l'ordre dans lequel des tentatives sont faites pour déplacer la crypto-monnaie, afin de détecter et

5 https://www.w3.org/2017/vc/charter.html
6 https://www.linkedin.com/pulse/youre-become-part-attribute-economy-nathan-kinch

d'empêcher les doubles dépenses. La capacité d'obtenir et d'enregistrer un consensus sur l'ordre des données stockées dans un enregistrement peut être utile dans des contextes autres que les crypto-monnaies, et cela a été l'un des principaux moteurs des autres utilisations proposées - y compris pour la GIA.

Dans certains cas, les participants à une transaction complexe sont soit des concurrents (comme des banques commerciales ou des sociétés pharmaceutiques), soit des secteurs éloignés sans supervision commune (tels que les divers expéditeurs et fournisseurs impliqués dans le commerce international). Les technologies blockchain promettent de rationaliser la façon dont les ensembles de données transactionnelles tels que les manifestes commerciaux, les enregistrements de la chaîne d'approvisionnement et les transactions financières complexes sont assemblés en temps réel et réglés.

La crypto-monnaie pair-à-pair est une application hautement spécialisée, avec des hypothèses et des contraintes de conception inhabituelles. Au fur et à mesure de l'émergence de cas d'utilisation plus complexes pour les blockchains, les caractéristiques et les options de conception des architectures se sont sensiblement modifiées, comme expliqué dans les sections suivantes.

Publique ou privée

La blockchain du Bitcoin est une structure de données publique et notoirement « immuable ». Pour prendre en charge la surveillance des doubles dépenses, la blockchain conserve toutes les transactions Bitcoin à tout moment, sans restriction quant à qui peut lire l'historique. Mais lorsque les applications d'entreprise pour la technologie blockchain ont été envisagées, la priorité était la confidentialité, et ainsi, certaines des premières retombées étaient des blockchains *privées* de différentes formes, avec des contrôles d'accès pour savoir qui pouvait lire et/ou écrire l'enregistrement. Il y a beaucoup de subtilités à faire avec les autorisations de blockchain que nous explorons plus loin.

« Trustless » ou gérée

Les premières blockchains étaient résolument « trustless ». La philosophie de crypto-monnaie pair-à-pair rejette les banques centrales de réserve, la surveillance du gouvernement, et en fait toute l'administration. La réalisation singulière de la blockchain du Bitcoin d'origine était de permettre à des inconnus de déplacer de manière fiable une valeur réelle sans vraiment se connaître les uns les autres et sans dépendre d'un tiers. La sagesse conventionnelle soutient que tout système de sécurité repose sur la triade des technologies, des processus et des personnes. Les transactions Bitcoin sont sécurisées par la technologie seule, et c'est ce que « trustless » signifie dans ce contexte.[7]

La blockchain d'origine n'avait pas non plus besoin de gestion de clé cryptographique hors chaîne. La plupart des systèmes de cryptage exigent une certitude quant aux clés qui vont avec quels utilisateurs (et quelles sont les principales métadonnées, comme la durée de vie de la clé et l'état de révocation). Et ils ont besoin d'une *gestion essentielle du cycle de vie*

7 Bien sûr, tout logiciel implique des processus et des personnes au *niveau de la conception*. Les utilisateurs en général doivent avoir confiance que les développeurs de logiciels savent ce qu'ils font, sont à l'affût - et corrigeront rapidement - les bogues inévitables ou les erreurs lorsqu'ils se révèlent et sont engagés dans le fonctionnement correct et efficace du système comme un tout. Ou, si nous ne faisons pas vraiment confiance à un développeur de logiciel, nous pouvons compter sur les garanties d'un auditeur indépendant « de confiance ». Donc, la confiance est inévitable à un certain niveau, et avec cette mise en garde, « trustless » est un descripteur approprié pour le *fonctionnement* essentiellement automatique des blockchains publiques et le manque de relation requis entre les parties qui négocient ces crypto-monnaies.

pour renouveler, révoquer et remplacer les clés des utilisateurs si nécessaire. Mais Bitcoin n'a pas besoin de cela. Les détenteurs de compte Bitcoin s'auto-enregistrent (en ignorant ignominieusement les règles d'identification des clients des régulateurs financiers) et acceptent l'entière responsabilité de la protection de leurs portefeuilles et de leurs clés privées. C'est chacun pour soi ; si vous perdez votre clé de portefeuille Bitcoin, il n'y a pas personne ni aucun processus pour garantir votre dépôt ou vous aider à la récupérer.

Les cas d'utilisation au-delà de la crypto-monnaie deviennent beaucoup plus complexes. D'une part, ils nécessitent généralement des *autorisations*, car il n'est normalement pas acceptable que les documents d'entreprise soient publics, et les entreprises n'externalisent généralement pas leurs opérations et la maintenance de logiciels à des bénévoles anonymes. Les autorisations de lecture et d'écriture sur une chaîne de blocs gérée nécessitent le type de gestion que Bitcoin a supprimé pour ses besoins. Lorsque la gestion doit être repliée, différents algorithmes de consensus provenant de la « preuve de travail » de Bitcoin peuvent être plus efficaces et le système peut être concentré en quelques nœuds plutôt que réparti sur des milliers. L'exigence de Bitcoin pour un grand livre comptable entièrement distribué, sans source d'autorité centralisée, ne fonctionne tout simplement pas pour de nombreux cas d'utilisation d'entreprise.

Un autre facteur à considérer pour les blockchains hybrides administrées vient du fait que les cas d'utilisation de GIA à haut risque nécessitent souvent des tiers de confiance pour valider les identités et/ou les attributs des utilisateurs. La chaîne de blocs d'origine ne prend pas en charge la validation externe des revendications, mais est simplement construite à dessein simplement pour fournir un grand livre comptable distribué vérifiable et pratiquement immuable.[8]

L'objectif principal des blockchains publiques d'origine, de parvenir à un consensus sur un grand livre comptable en l'absence de tout administrateur, peut devenir théorique si, après tout, un tiers reçoit un rôle central dans le système. Certains des récents développements de blockchains axées sur la GIA ont suivi un examen détaillé des blockchains disponibles et une constatation selon laquelle elles ne répondent pas aux besoins de la gestion des identités.

Décentralisée ou concentrée

Les réseaux distribués massifs des blockchains de crypto-monnaie archétypales offrent une grande résilience et redondance. L'une des hypothèses de conception qui sous-tend la blockchain d'origine est qu'une majorité simple des nœuds de réseau restera toujours indépendante ; par conséquent, l'une des vulnérabilités de Bitcoin est connue sous le nom de « Attaque à 51 % »[9], au cas où l'enregistrement peut être perturbé, en particulier en déformant secrètement le consensus.[10] Comme mentionné précédemment, les blockchains plus axées sur l'entreprise, comme R3 Corda[11] et Hyperledger Fabric[12], ne sont pas massivement distribuées, mais *concentrées* et exploitées en privé. Plutôt que de supposer que la majorité des nœuds resteront intacts, la sécurité dans les blockchains privées

8 Voir la discussion « Revendications / Attributs / Assertions » à la section 4 ci-dessus.

9 https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

10 Rappelez-vous qu'avec les blockchains publiques, un « consensus » est atteint sur l'ordre des entrées et la véracité globale du grand livre comptable ; une attaque à 51 % peut en principe voir le grand livre comptable trafiqué, mais il existe d'autres moyens de créer des transactions frauduleuses, par exemple prendre le contrôle du portefeuille d'un détenteur de compte et des clés privées.

11 http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

12 https://hyperledger.org/projects/fabric
https://www.ibm.com/developerworks/cloud/library/cl-top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/index.html

nécessite des approches plus conventionnelles. IBM par exemple met en œuvre sa blockchain en tant que service sous forme de pool de nœuds virtuels pouvant fonctionner physiquement sur un seul ordinateur central, avec des mesures de protection comprenant des modules de sécurité matérielle, la conteneurisation et des opérateurs hautement approuvés[13].

« Immutabilité »

C'est l'une des propriétés historiques des blockchains d'origine. Il est vrai que l'effort nécessaire pour subvertir un réseau de blockchains publiques et ensuite contrefaire et réinstaller toute l'histoire des blocs, est tout à fait infaisable.[14] Cette résistance extrême à l'altération est un moyen de résister aux doubles dépenses, car selon la philosophie du Bitcoin, la communauté doit être capable de référencer chaque transaction jamais réalisée, sans bénéficier d'un journal de transactions central. Pour la communauté Bitcoin, le coût du maintien d'un grand livre comptable décentralisé est accepté comme le prix payé pour un système monétaire libre de banques centrales et de régulateurs (avec l'algorithme de consensus « preuve de travail », le coût se traduit directement par des charges de calcul gigantesques). Dans d'autres applications, cependant, les dépenses énormes encourues par les blockchains *publiques* peuvent être disproportionnées, et les mesures traditionnelles de résistance à l'altération peuvent être adéquates. Il convient également de noter que l'immutabilité des blockchains publiques est qualifiée par la puissance conservée par leurs équipes de maintenance logicielle pour créer des branches (ou « fourches ») via des mises à jour logicielles qui peuvent rendre les anciens enregistrements inactifs à la date de création de la branche.

Technologies blockchain et authentification

À l'heure actuelle, nous voyons un concours d'idées autour des méthodes de livraison des attributs et des mécanismes pour prouver leur provenance. Pendant une décennie ou plus, les structures de fédération classiques[15] prévoyaient que les *autorités d'attribut* fonctionneraient parallèlement aux *fournisseurs d'identité* (IdP) et fourniraient des informations d'attribut en temps réel. Une approche alternative consiste à équiper les utilisateurs finaux de magasins de données personnelles ou de portefeuilles d'attributs, basés sur le cloud ou sur des appareils mobiles, et à organiser la transmission plus ou moins directe des détails pertinents aux fournisseurs de services (SP) sur demande.

Désormais, les blockchains fournissent un autre type de plate-forme pour la distribution des attributs**.** Un avantage de nombreuses blockchains, en particulier les instances publiques, est la découvrabilité. Leur nature distribuée et leur logiciel transparent et open source, installé à travers le monde, signifient que la recherche d'enregistrements est simple et ne nécessite aucun répertoire central ou schéma d'adressage.[16]

13 http://www-03.ibm.com/press/us/en/pressrelease/51840.wss

14 Cependant, trafiquer directement un grand livre comptable n'est pas le seul moyen d'attaque. Il convient de noter que, selon les termes du chef de la sécurité Bruce Schneier, seuls les amateurs cherchent à attaquer la technologie ; les criminels professionnels attaquent les gens. Aucune blockchain n'est immunisée contre les attaques, par exemple, sur les clés des utilisateurs individuels ; l'immutabilité des données écrites dans une blockchain n'empêche pas que des transactions frauduleuses soient formées hors chaîne et injectées dans le grand livre comptable. https://www.schneier.com/crypto-gram/archives/2000/1015.html

15 Voir par exemple le « Métasystème d'identité » de Microsoft https://www.identityblog.com/?p=355, la Stratégie nationale des États-Unis pour les identités de confiance dans le cyberespace NSTIC https://obamawhitehouse.archives.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace, et le programme GOV.UK Verify, https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

16 Il convient de noter que trouver des enregistrements sur une blockchain publique est une chose, mais les interpréter en est une autre. Avec les crypto-monnaies, les transactions et leur signification sont simples, mais lorsque des informations plus complexes sont stockées dans des entrées de

Il convient de noter à ce stade que la transparence des blockchains publiques crée des tensions avec les principes de confidentialité. L'architecture originale du Bitcoin expose au monde chaque entrée de blockchain unique, de sorte que la surveillance du système monétaire pourrait être externalisée ; l'ensemble de l'historique des transactions doit être disponible pour tous. Lorsque ces types de blockchain sont réutilisés pour des applications comme la GIA, des contrôles de confidentialité supplémentaires sont nécessaires, tels que le chiffrement séparé des charges de transaction avant qu'elles ne soient insérées ou référencées à partir des entrées de blockchain, ou l'encapsulation des couches de contrôle d'accès supplémentaires autour de l'algorithme blockchain natif pour restreindre qui peut lire (ou écrire) dans le grand livre comptable. D'autres défis relatifs à la protection de la vie privée sont présentés, tels que l'unicité des paires de clés des titulaires de compte. Chaque transaction effectuée avec un compte est enregistrée de façon indélébile pour tous les temps ; une clé Bitcoin ou « adresse » peut être non nommée et, en tant que telle, anonyme, mais elle forme un index permanent (ou « poignée de corrélation ») pour son historique de blockchain et représente donc un risque important pour la vie privée. On peut trouver tous les enregistrements en utilisant une clé particulière et les corréler à un profil particulier.

En GIA, un sujet particulier est associé aux concepts de blockchain - *Identité auto-souveraine* (SSI, Self Sovereign Identity). Les partisans de la SSI rejettent le contrôle étroit habituellement exercé par les gouvernements et les grandes entreprises sur les identités des citoyens et des clients et appellent à une plus grande autodétermination de la façon dont les individus se représentent et se révèlent en ligne, et à la décentralisation des identités. Cependant, pour certains cas d'utilisation à plus haut risque, une autorité externe de confiance pour valider les revendications ou les assertions est nécessaire. Les objectifs et les préceptes de la SSI ont pris du temps et sont souvent antérieurs à la blockchain, mais ils se sont développés autour de l'émergence de grands livres comptables distribués pratiques, inspirés par les blockchains publiques. La qualité de l'« auto-souveraineté » évoque la propriété littérale ou métaphorique des identités par les personnes concernées et un regain de contrôle.[17] La décentralisation et la disponibilité des blockchains sont considérées par beaucoup comme un bon choix pour la SSI, et une grosse opération de R&D est actuellement en cours ; voir par exemple la *Fondation Sovrin*[18] et son nouvel algorithme de consensus *Plenum* qui met l'accent sur la fiabilité de certains attributs, en particulier en ce qui concerne son graphe en ligne. Une importante R&D est également en cours sous la *Distributed Identity Foundation*[19] pour gérer les métadonnées de GIA comme l'état de révocation, et par le projet *Rebooting Web of Trust* pour distribuer les clés publiques sans dépendre des autorités centrales, réduisant ainsi les points de défaillance uniques.[20]

Éléments importants des blockchains

Si vous évaluez des solutions GIA candidates impliquant des blockchains ou si vous effectuez votre propre R&D originale en gestion des identités, vous devez examiner les

blockchain, la sémantique doit être élaborée au nom de tous les utilisateurs. L'établissement de règles exige généralement une autorité politique centrale, ce que les premières conceptions de blockchain cherchaient expressément à bannir. L'interopérabilité sémantique des enregistrements de blockchains dans des cas d'utilisation complexes tels que la GIA nécessite un examen attentif.

17 Le mouvement d'identité auto-souveraine a beaucoup en commun avec la gestion des relations fournisseurs (VRM, Vendor Relationship Management) ; voir https://cyber.harvard.edu/projectvrm/Main_Page

18 https://sovrin.org

19 http://identity.foundation

20 http://www.weboftrust.info/

problèmes suivants. À des fins d'authentification et d'autorisation, les propriétés suivantes des technologies blockchain sont particulièrement importantes :

Disponibilité et résilience : les blockchains publiques sont massivement distribuées et presque universellement accessibles (elles doivent être hautement disponibles pour pouvoir supporter constamment leurs crypto-monnaies). La synchronisation et la réplication sont prises en charge automatiquement, avec des blockchains maintenant un état convenu de l'enregistrement à tous les nœuds.

Découvrabilité (des attributs) : l'une des propriétés les plus sous-déclarées des blockchains est la découvrabilité. Aucun adressage compliqué ni schéma de répertoire n'est nécessaire pour atteindre la plupart des blockchains ; le logiciel de tous les participants sait où se trouve le grand livre comptable. Cette accessibilité peut être utile pour les systèmes de GIA évolutifs à l'échelle mondiale ; les attributs des utilisateurs seront disponibles 24 heures sur 24 dans un emplacement virtuel uniforme. D'un autre côté, **la signification sémantique des attributs sur une blockchain doit être comprise et acceptée pour être *hors chaîne (c'est-à-dire séparément)***. Bien qu'une blockchain distribuée soit techniquement disponible pour tous les utilisateurs, il semble possible que des communautés distinctes dans le système au sens large aient leurs propres interprétations (ou codes de classification) uniques de ce que signifient leurs attributs ; l'*interopérabilité* sémantique ne résulte donc pas nécessairement de la découvrabilité.

Conseils sur les technologies blockchain pour l'authentification

Le but des blockchains de la crypto-monnaie était d'avoir un réseau sans chef maintenant un consensus sur l'état d'un grand livre comptable, de sorte que des transactions fiables puissent se produire sans aucun administrateur central. La décentralisation est coûteuse ; dans un sens, c'est un « état d'énergie élevée » qui nécessite un effort constant de soutien. Le surcoût partagé de l'algorithme de consensus est le prix payé par les utilisateurs de Bitcoin dans la gestion précédente. La plupart des applications de GIA sont intrinsèquement différentes de l'idéal décentralisé de la crypto-monnaie.

Envisagez des processus hors chaîne. Un système de gestion des identités relie généralement plusieurs domaines, afin de fournir des informations sur les utilisateurs aux systèmes avec lesquels ils interagissent. Des décisions doivent être prises au sujet des données d'identité pertinentes, des personnes qui se portent garantes de ces données et de la façon dont elles sont tenues à jour. Ces processus de conception et d'exploitation impliquent souvent des tiers ou des autorités quelconques, ce qui peut ne pas fonctionner avec la décentralisation d'une blockchain. Rappelez-vous que les blockchains publiques utilisent des réseaux extrêmement gourmands en calcul, principalement à cause de l'hypothèse qu'aucun tiers ou administrateur n'est impliqué. Si en fait des autorités hors chaîne sont requises dans un système GIA, les architectes doivent accepter au moins un certain degré d'administration centrale, et la philosophie d'une blockchain distribuée peut ne pas être si importante ou avantageuse.

De quoi avez-vous besoin pour parvenir à un consensus ? Le consensus est un sujet de niche important en informatique depuis de nombreuses années, et de nombreux algorithmes sont antérieurs à la fameuse « preuve de travail » utilisée par les premières blockchains[21]. Les concepteurs de bases de données et les développeurs de jeux se sont

21 https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work.

longtemps penchés sur la question de savoir ce qui s'est passé en premier. Rappelez-vous qu'avec la crypto-monnaie et la plupart des blockchains orientées transaction, le consensus concerne l'*ordre des événements* afin de résoudre les doubles dépenses sans arbitre. D'un autre côté, dans la gestion des identités, il peut ne pas y avoir l'équivalent d'un problème de « doubles dépenses ». Fondamentalement, l'identité n'est pas aussi transactionnelle que la monnaie. Donc, dans les cas d'utilisation de la GIA, prenez le temps d'examiner ce que serait le consensus décentralisé, et quel serait le facteur déterminant.

Tenez également compte des différentes exigences en matière de sécurité et d'enregistrement tout au long du cycle de vie de l'identité. Lorsqu'un utilisateur est inscrit dans un système GIA, certains faits à son sujet doivent être (généralement) vérifiés et enregistrés pour être accessibles plus tard. Lorsque l'utilisateur doit accéder à un système, certains de ces faits peuvent devoir être présentés aux contreparties et vérifiés par ces dernières en temps réel. Certaines transactions exigent que l'identité de l'utilisateur ou d'autres attributs soient liés à des artéfacts numériques ; les journaux d'audit peuvent devoir être conservés selon diverses normes et mentionnés plus tard avec une intégrité raisonnable. Tous ces types d'activités imposent des exigences différentes aux enregistrements GIA, qu'il s'agisse de répertoires traditionnels ou de blockchains plus récentes. Une considération spéciale est un retard important impliqué par certains algorithmes de consensus. La blockchain du Bitcoin prend *en moyenne* 10 minutes pour actualiser le grand livre comptable, ce qui peut limiter le temps de réponse pour certaines opérations de cycle de vie d'identité.

Envisager la gestion du cycle de vie des clés - ce qui signifie, en général, s'assurer que les bonnes clés sont entre de bonnes mains et y restent - est au cœur de la gestion des identités, mais sans rapport avec les premières plates-formes de blockchain. Avec Bitcoin, on n'est pas censé se soucier des personnes avec qui l'on traite, de sorte que le système n'a pas besoin de s'assurer de la garde des clés privées, ni de l'association des clés publiques avec certaines personnes. Pour cette seule raison, le fait d'assortir la GIA avec des blockchains publiques peut créer un gaspillage d'efforts : il n'est pas évident que la décentralisation du consensus soit bénéfique lorsqu'une autorité est nécessaire pour la gestion des clés. Les nouvelles technologies de blockchain spécifiques à la GIA doivent être attentives à ce besoin de contrôles de cycle de vie de clé fondamentalement plus forts que ceux requis par les premières blockchains.

Pensez à la sécurité des clés privées. La gestion des clés est liée au problème spécifique des clés privées de l'utilisateur final. Le système de blockchain du Bitcoin ne s'intéresse aucunement à la façon dont ses utilisateurs finaux s'occupent de leurs clés privées (c'est-à-dire de leurs portefeuilles de crypto-monnaie). Une fois qu'il est devenu évident que des pirates pouvaient perdre ou voler des clés privées, un marché vigoureux de solutions de portefeuille a vu le jour, notamment des magasins de clés, des services de stockage et des modules de sécurité matérielle personnels. Dans les blockchains les plus avancées, la gestion des clés matérielles devient également d'actualité.

Maintenance des blockchains. L'un des points de différenciation les plus visibles entre les premières blockchains et leurs descendants est la gestion du logiciel de base. Les blockchains publiques ont tendance à être maintenues par des volontaires à source ouverte tandis que certaines des nouvelles plates-formes sont fermées ou propriétaires (ou du moins elles peuvent démarrer de cette manière avant d'être à source ouverte). Alors que l'objectif de source ouverte tend à dominer, une préoccupation pratique pour certains

exécutants de GIA d'entreprise est la fiabilité de la maintenance logicielle. Lorsque des bogues ou des améliorations de conception urgentes surviennent, les entreprises peuvent vouloir savoir avec certitude quand les correctifs seront déployés. Avec la blockchain du Bitcoin, certains problèmes de conception ont pris des années à être résolus ; avec Ethereum, un bogue majeur a conduit le fondateur à décider unilatéralement de créer un « embranchement » à cette blockchain, ce qui a conduit à de multiples enregistrements incompatibles et à des variations de la monnaie.[22]

Conclusion

Les technologies blockchain sont collectivement un travail en cours. Malgré un intérêt précoce pour leurs propriétés de sécurité générales, nous constatons, à y regarder de plus près, que les blockchains publiques d'origine ne sont généralement pas adaptées à la gestion des identités et des accès. L'objectif de la crypto-monnaie - échanger de l'argent électronique sans intermédiaires et sans confiance - est fondamentalement différent de celui de la GIA d'entreprise, qui nécessite généralement une gestion du cycle de vie et un contrôle d'accès beaucoup plus rigoureux que ne l'offrent les blockchains publiques. D'un autre côté, plusieurs nouveaux développements de la technologie blockchain sont prometteurs pour améliorer des aspects particuliers de la GIA, tels que la provenance des attributs et des clés d'identité. Nous recommandons que tout examen en cours des technologies blockchain pour l'identité commence par un énoncé clair du problème, et une appréciation des nuances dans la sécurité de la blockchain.

22 https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds.

Références et autres lectures

« Want to really understand how bitcoin works? Here's a gentle primer »
https://arstechnica.com/tech-policy/2017/12/how-bitcoin-works/

« Immutable agreement for the Internet of value », Sigrid Seibold et George Samman, KPMG, 2016 https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

« Blockchain plain and simple », Steve Wilson, Constellation Research, 30 janvier 2017
https://www.constellationr.com/blog-news/blockchain-plain-and-simple

« Blockchain Security for Digital Identity », Adam Migus, septembre 2016
https://medium.com/@amigus/blockchain-Security-for-digital-identity-e10c8750cf9c

Decentralized Identity Foundation - DIF
http://identity.foundation

« Corda: An Introduction », Richard Gendal Brown, James Carlyle, Ian Grigg et Mike Hearn, R3, 2016 https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

« Overview of Swirlds Hashgraph », Leemon Baird, Swirlds, 2016
http://www.swirlds.com/wp-content/uploads/2016/06/2016-05-31-Overview-of-Swirlds-Hashgraph-1.pdf

« Still don't understand blockchain? Let's untangle the wires »
https://www.weforum.org/agenda/2017/11/blockchain-bitcoin-ethereum-tech-explained/

« Do You Need a Blockchain? », Morgan E. Peck, IEEE Spectrum, septembre 2017
https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

« Introduction to Identity Management »
https://meetings.internet2.edu/media/medialibrary/2014/11/06/20141028-dors-intro-to-idm.pdf

Online Identity: Who, Me?
https://www.internetsociety.org/resources/doc/2016/online-identity-who-me/

Ressources sur l'identité de l'Internet Society
https://www.internetsociety.org/issues/identity/