



Les perspectives de la technologie des registres distribués et de la blockchain pour le financement des entreprises

Impressum

CVCI—Chambre vaudoise
du commerce et de l'industrie
Av. d'Ouchy 47, 1006 Lausanne
www.cvci.ch

Direction éditoriale et rédaction :



Florian Ducommun,
HDC



Jacques Iffland,
Lenz & Staehelin



Cédric Portier,
Gros & Waltenspühl

Rédaction :

Ariel Ben Hattar, CMTA
Justin Brodard, avocat, expert-fiscal diplômé
Olivier Cohen, Altcoinomy
Noé Curtz, Altcoinomy
Sébastien Dessimoz, Taurus Group
Linus Gasser, C4DT – EPFL
Morgan Lavanchy, Swissquote Bank
Lars Schlichting, Kellerhals Carrard
Vincent Trouche, Tokenestate

Édition et rédaction :

Jean-François Krähenbühl, CVCI

Graphisme :

DO! L'agence SA
Agence de publicité
www.dolagence.ch

Sommaire

1. PRÉFACE	4
2. TECHNOLOGIE DES REGISTRES DISTRIBUÉS ET BLOCKCHAIN – DE QUOI S’AGIT-IL ?	5
« LA BLOCKCHAIN, C'EST COMME UNE FEUILLE EXCEL PARTAGÉE ».	
Interview d'Émilie Raffo, spécialiste de la blockchain	8
3. TYPE DE BLOCKCHAINS ET FONCTIONNEMENT DES JETONS NUMÉRIQUES	10
4. POURQUOI LA TRD EST-ELLE PERTINENTE POUR LE MARCHÉ DES CAPITAUX, ET COMMENT PEUT-ELLE FACILITER LE FINANCEMENT DES ENTREPRISES ?	11
5. TYPES DE JETONS	14
5.1 Jetons de paiement	
5.2 Jetons d’investissement	
5.3 Jetons de service	
6. ÉMISSION DE JETONS	21
6.1 Initial Coin Offerings (ou ICOs)	
6.2 Jetons d’investissement (security tokens)	
6.3 Security token offerings (STOs)	
6.4 Plateformes de STO	
7. STRUCTURE ET FONCTIONNALITÉ DES SMART CONTRACTS	23
7.1 Préparation de la levée de fonds	
7.2 Levée de fonds: interactions entre investisseur, oracles et smart contracts sur le marché primaire	
8. NÉGOCE DE JETONS	26
8.1 Besoin de marchés secondaires pour actifs digitaux	
8.2 Absence de plateformes pour le négoce de jetons d’investissement	
8.3 Une lacune à combler	
8.4 Adaptations du droit suisse à la blockchain	
LE DIGITAL REQUIERT UN GRAND BESOIN DE CONFIANCE	27
Interview de Philippe Thévoz, SICPA	
9. CONSERVATION DE JETONS	29
9.1 La sécurité des clés privées au cœur du problème	
9.2 Plusieurs mesures de limitation des risques	
9.3 Actifs « tokenisés » : au-delà de la sécurité des clés privées	
9.4 Besoin d’une infrastructure spécialisée	
GLOSSAIRE	31

1. Préface

La Suisse s'enorgueillit à juste titre de la richesse de son tissu économique, de la sophistication de ses entreprises, de la qualité de ses filières de formation et du caractère innovant de sa recherche. Ces conditions-cadre favorables font de notre pays un lieu naturel pour le développement et l'exploitation de nouvelles technologies.

Aujourd'hui, la technologie des registres distribués – dont en particulier la technologie blockchain – ouvre des perspectives pour le financement des entreprises, et pas seulement pour celles du domaine technologique.

Il y a quelques années, le développement de méthodes de levées de fonds alternatives impliquant l'utilisation de jetons numériques – qualifiées d'« *initial coin offerings* » ou « *ICOs* » – a permis d'envisager de nouvelles façons pour les entreprises de financer leurs activités, offrant des alternatives aux financements bancaires traditionnels, aux levées de fonds privées (« *private equity* ») ou aux cotations en bourse, souvent excessivement difficiles à réaliser ou tout simplement hors de portée. Les ICOs ont suscité beaucoup d'intérêt en raison de la simplicité et de la rapidité avec laquelle ces opérations permettent d'accéder au marché et de lever des capitaux. Les instruments utilisés au cours des dernières années se sont cependant souvent révélés imparfaits. Le manque de standardisation a dissuadé les investisseurs institutionnels de s'intéresser à ces produits. Le manque de transparence des levées de fonds a permis des fraudes. L'absence de surveillance adéquate du marché des actifs digitaux a suscité des craintes quant à la légitimité de l'origine des fonds récoltés.

La blockchain continue néanmoins d'intéresser l'industrie financière. Beaucoup d'entreprises et d'organisations non gouvernementales – dont un grand nombre se trouve dans l'Arc lémanique – travaillent à faire progresser cette technologie, le cadre réglementaire qui s'y rapporte et les infrastructures de marché pour faciliter l'accès des entreprises aux marchés des capitaux. Plusieurs de ces entreprises ou organisations ont contribué à cette brochure, dont le but est de mieux faire comprendre le fonctionnement de la blockchain et la façon dont cette technologie peut être utilisée pour des opérations de financement.

À l'heure où la pandémie de Covid-19 met la santé financière de nos entreprises à l'épreuve, ces développements sont particulièrement importants et d'une grande actualité. La Confédération et les cantons sont intervenus pour soutenir l'économie de notre pays, le plus souvent

au moyen de prêts. Ces solutions ne sont cependant pas pérennes. Des opérations de financements seront nécessaires. Que la technologie puisse favoriser ce processus est une perspective réjouissante dans un contexte qui ne l'est guère. Que notre canton et l'Arc lémanique regroupent de nombreuses entreprises, organisations et centres de recherche de pointe dans ce domaine est également une source d'optimisme.

Août 2020



Claudine Amstein,
Directrice de la CVCI

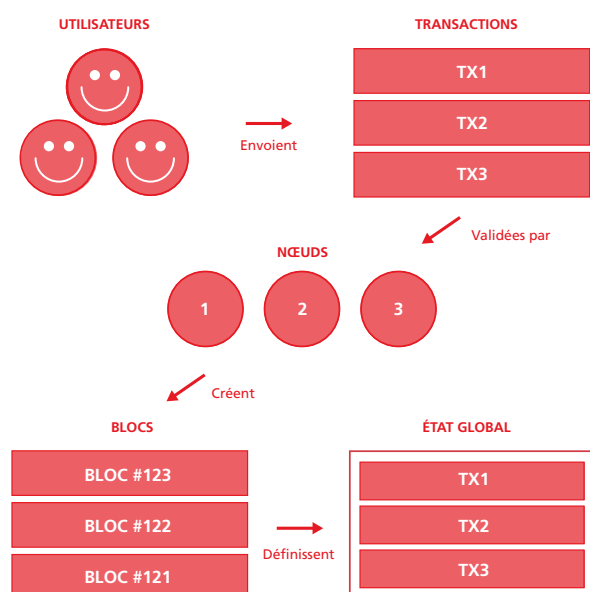
2. Technologie des registres distribués et blockchain – De quoi s’agit-il ?

Depuis l’invention du Bitcoin en 2008, la technologie de la blockchain est passée par plusieurs étapes d’un hype-cycle¹. Cette technologie s’apprêtant à atteindre son « plateau de productivité », la période actuelle est un moment propice pour s’y intéresser, en prenant garde toutefois à ne pas se laisser emporter par des ambitions disproportionnées.

La principale innovation de la blockchain est de permettre à plusieurs participants anonymes d’un marché de parvenir à un consensus sans avoir recours à *un tiers de confiance*. Malheureusement, beaucoup de projets réalisés ces dernières années ont mal intégré cette innovation et ont contribué à ternir l’image de cette technologie. En effet, une base de données traditionnelle est souvent plus rapide, moins complexe et moins onéreuse à mettre en œuvre qu’une blockchain.

Pour mieux comprendre les différents types de blockchain qui existent, la définition suivante sera utilisée :

Une blockchain permet à des utilisateurs de soumettre des transactions à un ensemble de nœuds, qui les valident et les intègrent dans des blocs. Ces blocs sont immuables et contiennent les transactions. L’enchaînement de ces blocs définit l’état global du système.



Types de blockchains

Il y a divers types de blockchains. Il est important de bien comprendre les avantages et inconvénients de chacun d'entre eux pour ne pas utiliser de technologie inadaptée. En se basant sur la définition donnée ci-contre, on peut distinguer les éléments suivants ainsi que leurs variantes :

Utilisateurs

1. Blockchain *publique* : quiconque peut soumettre une transaction, du moment qu'il peut payer pour sa validation au moyen d'un jeton.
2. Blockchain *privée* : l'accès des utilisateurs est limité et réglé le plus souvent par des certificats.

Nœuds

1. Blockchain *participative* : quiconque peut participer à la validation des transactions et à la création de blocs.
2. Blockchain *gouvernée* : il existe un administrateur central qui identifie les nœuds qui ont le droit de valider des transactions et de créer des blocs.

Utilité et contenu des transactions

1. *Horodatage* : prouve qu'une donnée existait à un moment précis. Exemple : KSI
2. *Devise* : permet de transférer des jetons entre utilisateurs. Exemple : Bitcoin
3. *Smart contract* : donne la possibilité de programmer la blockchain. Exemple : Ethereum
4. *Hybride* : offre d'autres prestations que la validation de transactions, comme par exemple la gestion de données encryptées. Exemple : OmniLedger

¹https://en.wikipedia.org/wiki/Hype_cycle

Types de blockchains

	Participatives	Gouvernées
Publiques	Lent, énergivore, ouvert	Rapide, restreint
	Ethereum Bitcoin Waves	Sovrin OmniLedger Ripple
Privées	Rapide, protection des données	Rapide, Business
	Holochain LTO Monet	HyperLedger/Fabric KSI Corda

Blockchains publiques ou privées, participatives ou gouvernées

Il existe plusieurs façons d'organiser un registre distribué. Les plus connus sont dits « publics » et « participatifs ». Cela signifie que tout un chacun peut soumettre des transactions (registre *public*) et participer à la validation des entrées dans le registre s'il possède les compétences techniques nécessaires (registre *participatif*). Il n'est toutefois pas indispensable de participer au processus de validation pour utiliser ces registres.

Certaines grandes entreprises ont toutefois privilégié les blockchains privées, car elles ne désirent pas ouvrir leur système pour y inclure le plus d'acteurs possibles. Ce choix peut parfois être pertinent. Ce peut par exemple être le cas pour des transactions entre des banques qui ne se font pas nécessairement confiance, mais qui ne veulent travailler qu'entre partenaires préalablement « autorisés ». En revanche, les blockchains privées qui ne sont pas gérées par un cercle restreint d'entreprises sont souvent le fruit du « blockchain-hype », car elles pourraient souvent être remplacées par une base de données traditionnelle.

Un autre élément distinctif des différents types de blockchain est la façon dont elles organisent le processus de validation des transactions par les nœuds. Les blockchains publiques lient souvent la validation des transactions à l'émission de jetons. Chaque fois qu'un nœud valide des transactions et crée un bloc, il reçoit des jetons en récompense. Le nœud peut ensuite échanger ses jetons contre des services ou les vendre sur le marché. Cela permet de créer un système ouvert comparable à Internet.

Pour permettre à tout un chacun de participer à la blockchain en qualité de nœud tout en maintenant la cadence de création de blocs constante, les grandes blockchains

participatives utilisent parfois un procédé qualifié de « *proof-of-work* ». Dans un tel système, la création de nouveaux blocs passe par un consensus algorithmique, qui permet d'établir la réalisation d'un travail informatique. Le procédé permet de ralentir le rythme de la création des blocs et de faciliter le consensus final à leur sujet. Les principaux inconvénients de ce type de blockchain sont d'être très gourmands en énergie et très lents. Rien que pour la blockchain Bitcoin, l'utilisation d'électricité au niveau mondial dépasse celle de la Suisse. Ces inconvénients n'existent pas pour les blockchains gouvernées ou « *permissioned* », comme Ripple, qui travaillent exclusivement avec des nœuds agréés. Un tel système augmente considérablement la vitesse de validation des transactions et permet de réduire la consommation d'énergie. Son principal inconvénient est de nécessiter une instance centrale d'autorisation des nœuds qui ait la confiance des utilisateurs.

Un autre procédé utilisé pour gérer la cadence de génération des blocs dans les chaînes participatives est un modèle de consensus appelé « *proof-of-stake* ». Dans un tel système, chaque nœud qui entend valider des transactions doit déposer des fonds pour prouver sa fidélité au système. Les blocs sont créés par un nœud choisi aléatoirement parmi ceux qui ont déposé des fonds. Si le nœud choisi valide un bloc erroné, son dépôt est détruit ou redistribué aux participants au réseau ou aux nœuds intègres. Par rapport à un régime de *proof-of-work*, ce procédé réduit significativement la quantité d'énergie requise. Le *proof-of-stake* pose cependant d'autres problèmes. Par exemple, les nœuds déjà « riches » voient leur capital s'accroître encore, car ils reçoivent davantage de récompenses que les nœuds « pauvres ». Un autre risque est que le processus de validation des transactions soit ultimement placé entre les mains d'un petit nombre de nœuds « riches », ce qui pourrait compromettre l'intégrité du registre. La fondation Ethereum

étudie actuellement les améliorations qui pourraient être apportées au régime de *proof-of-stake*, mais les problèmes propres à ce procédé sont plus difficiles à résoudre que ceux posés par le *proof-of-work*.

Transactions par seconde

L'unité couramment utilisée pour mesurer la rapidité d'une blockchain est le nombre de transactions par seconde (tps) qui peut être validé. Les blockchains publiques et participatives comme celles de Bitcoin ou d'Ethereum peuvent actuellement valider jusqu'à sept transactions par seconde. À titre de comparaison, le service de la carte de crédit Visa en valide entre 2000 et 10 000 dans le même intervalle. Les échanges monétaires ne pourront donc pas être intégralement pris en charge par des blockchains publiques et participatives telles qu'elles existent aujourd'hui.



Linus Gasser,
C4DT, EPFL

Divers protocoles permettent d'augmenter le nombre de tps des blockchains publiques et participatives :

- **Bitcoin-ng²** : ce protocole améliore le Bitcoin en donnant à un nœud le droit de ne pas créer un bloc unique seulement, mais autant de blocs qu'il le souhaite jusqu'à ce qu'un autre nœud établisse avoir réalisé le travail informatique requis (« *proof-of-work* »). Des versions améliorées de ce protocole ont été proposées, comme par exemple Byzcoin³, mais aucune n'est actuellement utilisée à grande échelle.
- **Partitionnement** : la responsabilité de valider une transaction est attribuée à un groupe de nœuds plutôt qu'à un nœud spécifique. Ce procédé permet au système

de gagner en rapidité si le nombre de nœuds augmente. Des transactions qui impliquent plusieurs partitions peuvent néanmoins ralentir considérablement le système.

- **Avalanche** : chaque utilisateur communique les transactions qu'il réalise. Le système se charge seulement de résoudre d'éventuels conflits entre transactions annoncées.

Les blockchains publiques mais gouvernées peuvent atteindre jusqu'à 10 000 transactions par seconde, et même jusqu'à 20 000 pour des chaînes privées et gouvernées comme HyperLedger ou Fabric.

2. <https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf>

3. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kokoris-kogias.pdf

« La blockchain, c'est comme une feuille Excel partagée ».

Interview d'Émilie Raffo, spécialiste de la blockchain.

Spécialiste des cryptomonnaies, Émilie Raffo voit dans cette technologie un moyen de créer de la confiance dans le monde des transactions numériques.

Titulaire d'un master en business acquis en Belgique, Émilie Raffo aide ses clients à comprendre les actifs digitaux et à exploiter leur potentiel. Interview.

Comment expliquer la blockchain à un profane ?

La blockchain, c'est comme une feuille Excel partagée, comme un Google doc qui, au lieu d'être hébergé par Google, l'est par une multitude d'ordinateurs en même temps, par une communauté décentralisée. Pour enregistrer une nouvelle information dans ce document, il faut parvenir à un consensus de la communauté. Une fois que les informations sont enregistrées dans la blockchain selon un processus sécurisé, il est presque impossible de les modifier a posteriori.

Quelle est l'utilité de cette technologie ?

Elle permet avant tout de créer de la confiance. Elle donne la possibilité d'enregistrer des transactions et des informations importantes via un système sécurisé sans avoir recours à un intermédiaire, de prendre des décisions importantes en se basant sur des informations vérifiables. C'est un peu comme un notaire qui acte la vente de votre maison et l'inscrit dans le Registre foncier, et assure ainsi l'irrévocabilité de cette inscription. À ce propos, l'organisation Bitland, active au Ghana, envisage de mettre sur pied un Registre foncier sur une blockchain. Dans ce pays, la confiance dans le registre national est faible. Bitland veut ainsi sécuriser les ventes de maisons et bénéficier du niveau de décentralisation de la blockchain. Bitland souhaite une collaboration avec l'État, qui doit être impliqué pour qu'il y ait une reconnaissance du titre.

Quels sont les avantages des transactions en cryptomonnaies par rapport aux transactions traditionnelles ?

Cela dépend. Si l'on n'appartient pas à une minorité opprimée, qu'on dispose d'un compte bancaire et que nos banques ont des accords entre elles, les cryptomonnaies ne sont pas forcément optimales. En revanche, si on veut envoyer de l'argent à l'étranger, avec des taux de change, des frais de transactions et des délais très élevés, il vaut

mieux privilégier une opération en cryptomonnaie. Elle est quasi instantanée (environ 30 minutes pour le Bitcoin) et les frais ne sont pas excessifs, même lors de transactions importantes. D'où l'idée de l'inclusion financière, qui consiste à offrir des services bancaires de base à faible coût. Dans le monde, 1,7 milliard d'adultes n'ont pas accès à un compte bancaire. La cryptomonnaie est ouverte à tous. Dans des pays totalitaires à inflation très forte, une monnaie libre comme le Bitcoin peut servir de rempart stable face à une monnaie nationale instable.

En quoi la blockchain va-t-elle révolutionner la finance ?

Le souci, dans le monde de la finance, c'est la fragmentation des données, des acteurs. Le morcellement des processus ralentit la communication. Typiquement, si vous voulez acheter un produit financier, avec un intermédiaire, ils devront communiquer entre eux. Au bout du compte, cela peut prendre trois à quatre jours pour acheter de tels produits. La blockchain permettrait d'accélérer le processus. L'idée est de créer des systèmes interoperables, automatisés et sécurisés. Des acteurs même en compétition pourraient collaborer d'une certaine manière. On parle de « coopétition ».

Ces technologies constituent-elles une menace pour le monde bancaire ?

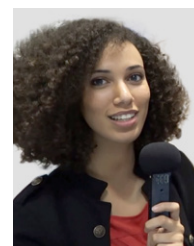
Une quantité énorme d'exigences légales pèsent sur le système financier. Les banques doivent remplir tels critères, les licences bancaires sont extrêmement chères, les frais de conformité élevés, etc. Aux yeux de la loi, la blockchain ne suffit pas : dans la finance comme dans le commerce, il faut qu'une personne morale ou physique engage sa responsabilité. Tant que la loi ne s'adapte pas à la blockchain, celle-ci ne pourra pas disrupter le monde de la finance. Le jour où la loi considérera qu'un token (un jeton) représente vraiment la part d'un fonds, et qu'il a une valeur légale, cela pourrait changer. Mais tant que sa valeur n'est pas reconnue légalement, je pense que non. Les Chambres fédérales ont le dossier en main. Au Liechtenstein, les élus ont voté une loi, le « Blockchain Act », permettant de lier le monde de la blockchain au monde réel. C'est une révolution à observer de près. La Suisse, assez innovante, pourrait suivre.

« La blockchain permet
avant tout de créer de
la confiance »

La pandémie qui a sévi ce printemps a-t-elle eu des incidences sur les cryptomonnaies ?

Alors que les marchés traditionnels, les Bourses, ont chuté en mars, le Bitcoin a chuté encore plus fortement. Ce phénomène a remis en question le statut de « valeur refuge » du Bitcoin. Ceci dit, les investisseurs cherchaient des liquidités et l'or, valeur refuge de référence, a également chuté, mais dans une moindre mesure : probablement car le marché du Bitcoin est bien plus petit. En revanche, du côté des monnaies officielles, les banques centrales ont « imprimé » sans compter pour lutter contre les effets économiques de la pandémie. Quelles seront les conséquences sur la stabilité de nos devises étatiques ? Au même moment, la vitesse d'émission monétaire du Bitcoin a été divisée par deux. Le taux d'inflation de « l'or digital » est maintenant de 1,8 %, en dessous de l'objectif d'inflation de la FED. Pas étonnant que le Bitcoin compte de nombreux nouveaux utilisateurs en 2020.

Propos recueillis par
Jean-François Krähenbühl



Émilie Raffo,
spécialiste des cryptomonnaies

3. Type de blockchains et fonctionnement des jetons numériques

Les registres distribués sont des registres dans lesquels des données sont enregistrées. Tous les registres distribués ne fonctionnent cependant pas de la même manière.

3.1 Fonctionnalités des registres distribués et smart contracts

Les registres les plus simples sont conçus pour enregistrer des données se rapportant à un seul instrument ou objet. Par exemple, la blockchain Bitcoin est un registre distribué qui permet d'enregistrer des données relatives à des transactions réalisées sur une seule valeur : le Bitcoin.

Certains registres distribués permettent cependant de réaliser d'autres types d'opérations. Certains d'entre eux permettent ainsi à leurs utilisateurs de créer des « contrats intelligents » (« *smart contracts* »). Les smart contracts sont de petits programmes informatiques, intégrés dans le registre distribué, qui peuvent servir à créer une infinité de contrats et d'instruments. Tous ces contrats et instruments n'ont pas forcément de lien avec les marchés financiers.

3.2 Fonctionnement des smart contracts utilisés pour représenter des actifs

Une utilisation possible des smart contracts est de garder trace de la propriété d'un actif choisi par son créateur. Le smart contract tient alors lieu de sous-registre, qui existe au sein du registre distribué. Dans son expression la plus simple, le smart contract répertorie les actifs et identifie les adresses publiques de ceux qui les détiennent.

les smart contracts servent à représenter la titularité. S'il est très utilisé, ce terme n'en est pas moins source de confusion. Dans le langage courant, un jeton est un objet ; il a une existence physique. Par contraste, le jeton auquel il est fait référence dans le domaine de la technologie des registres distribués est une entrée dans un sous-registre créé par un smart contract. Lorsqu'une personne « détient » un jeton, cela signifie que le smart contract attribue un actif à l'adresse publique que cette personne contrôle.



Ariel Ben Hattar,
CMTA

ACTIF	ADRESSE
Actif N° 1 à 10	0xABC
Actif N° 11 à 100	0xDEF

Illustration simplifiée d'un registre tenu par un smart contract.

Les entrées dans le sous-registre sont possibles aux conditions définies par le smart contract et le registre distribué. Cela signifie que toute opération impliquant le smart contract doit être validée par les nœuds du registre concerné. Ce fonctionnement assure également une traçabilité, puisque toutes les opérations validées par les nœuds sont enregistrées dans le registre distribué. On parle parfois de « jetons » (ou « *tokens* ») pour désigner les actifs dont

4. Pourquoi la TRD est-elle pertinente pour le marché des capitaux, et comment peut-elle faciliter le financement des entreprises ?

Sur les marchés des capitaux, les entreprises vendent des valeurs mobilières (typiquement des titres de participation ou de dette) à des investisseurs pour financer leurs activités.

À l'heure actuelle, les transactions du marché des capitaux se réalisent par l'intermédiaire d'établissements financiers, typiquement des banques. Ces intermédiaires ont un accès exclusif aux infrastructures des marchés (en particulier aux bourses, aux systèmes de paiement des banques centrales et aux dépositaires centraux) indispensables à la réalisation d'opérations sur titres.

La nécessité de recourir à des dépositaires professionnels et d'entretenir des infrastructures de marché complexes est cependant source de frais importants, qui se répercutent sur les émetteurs et renchérissent les opérations de financement. Pour cette raison, les marchés des capitaux sont actuellement *de facto* réservés aux entreprises les plus importantes. Sur les 586 214 entreprises qui étaient répertoriées en Suisse à fin 2016, moins de 300 (247) avaient des titres de participation cotés à une des deux bourses suisses. Les financements privés (opérations dites de *private equity*) sont certes en progression. Ils restent cependant peu importants au regard de la taille de l'économie suisse. Ils sont aussi difficiles à organiser et coûteux pour les entreprises concernées.

Dans ce contexte, la TRD présente un intérêt particulier. La tenue de registres est une question centrale pour les marchés des capitaux. Pour les émetteurs, l'aptitude à identifier leurs investisseurs (actionnaires, créanciers) en tout temps est une nécessité pratique. Cette tâche est complexe, car les titres émis étant souvent traités sur des marchés organisés, leur propriété change continuellement et les registres sont donc en constante mutation. Pour les investisseurs, il est aussi essentiel de pouvoir documenter la propriété des titres détenus.

Dans l'organisation actuelle du marché des capitaux, la tenue des registres est déléguée aux dépositaires professionnels (le plus souvent des banques ou des maisons de titres). Ces derniers délèguent à leur tour une partie de cette responsabilité à des dépositaires centraux (par exemple en Suisse à la société SIX SIS SA). La loi tient compte de cette situation, puisque la propriété de titres intermédiés (c'est-à-dire des titres qui sont déposés auprès de dépositaires profession-

nels) se transfère par le débit et le crédit des comptes de dépôt dont les investisseurs concernés disposent auprès de ces intermédiaires. Ce sont donc les dépositaires qui peuvent attester de la propriété des titres détenus par les investisseurs.

La TRD offre la possibilité de simplifier ce régime, en permettant que le registre des investisseurs – au lieu d'être tenu par des dépositaires professionnels – soit tenu de façon décentralisée, transparente et fiable par une communauté de personnes (typiquement les « nœuds » d'une blockchain).

Cette décentralisation peut apporter deux types de bénéfices. D'une part, elle peut simplifier le fonctionnement du marché des capitaux, en éliminant certaines infrastructures complexes et coûteuses, telles que les dépositaires centraux ou les contreparties centrales. D'autre part, elle permet aux émetteurs d'interagir directement avec les investisseurs, sans qu'il soit nécessaire de faire intervenir des maisons de titres, des banques ou d'autres intermédiaires professionnels dans le processus comme c'est actuellement le cas. Ces deux éléments peuvent réduire le coût des opérations de marché des capitaux, et ainsi faciliter l'accès des entreprises à ces marchés. À titre d'exemple, à l'heure actuelle, une offre publique de titres de participation portant sur moins de CHF 100 millions est généralement considérée comme trop petite pour être viable. Dans une infrastructure décentralisée fondée sur la TRD, cette limite peut être bien inférieure.

Historiquement, les premières applications de la TRD pour le financement d'entreprises ont pris la forme d'*initial coin offerings* (ou ICOs), c'est-à-dire d'émissions de jetons numériques – souvent enregistrés sur des blockchains publiques telles qu'Ethereum – payés en cryptomonnaie (typiquement la monnaie de la blockchain sur laquelle le jeton a été créé, soit par exemple en Ether pour des jetons émis sur la blockchain Ethereum).

Certaines de ces transactions ont permis de lever des dizaines de millions. Les formes initiales d'ICOs ont cependant présenté certaines faiblesses, qui ont limité leur essor. D'une part, ces opérations étant réalisées sans la participation d'intermédiaires financiers, elles échappent aux règles anti-blanchiment auxquelles les opérations de marché des capitaux sont généralement soumises. Cette situation peut rendre difficile la conversion des cryptomonnaies obtenues

en monnaies fiduciaires et leur dépôt sur des comptes bancaires. D'autre part, les droits incorporés dans les jetons sont souvent de nature peu claire, et ne sont pas toujours documentés de façon rigoureuse. Ces deux éléments ont empêché les ICOs de première génération d'attirer les investisseurs institutionnels.

Des progrès ont cependant été réalisés. De nouveaux types de jetons digitaux ont été développés, et le régime juridique applicable à ces instruments a été clarifié. Ainsi, la façon dont des titres de participation ou de dette peuvent être associés à des jetons digitaux a été conceptualisée. Les principaux modèles juridiques développés à cet égard reposent sur l'idée que le processus de digitalisation (ou de « tokenisation ») des valeurs mobilières s'inscrit dans le prolongement de la théorie des papiers-valeurs, telle qu'elle a été développée au cours des siècles passés. La différence essentielle réside dans le fait que, au lieu d'associer des instruments financiers à des supports physiques tels que des certificats en papier, la TRD permet d'associer de tels instruments à des jetons digitaux. C'est sur cette base que la Capital Markets and Technology Association a développé le premier modèle de tokenisation pour titres de participation de sociétés anonymes suisses en 2018. C'est également sur cette base que repose le projet de loi fédérale sur la TRD actuellement en discussion devant les Chambres fédérales.

En matière de financement d'entreprises, la TRD a ainsi le potentiel de combiner la flexibilité et la rapidité des ICOs à la sécurité juridique et la transparence des instruments traditionnels du marché des capitaux. L'espoir est ainsi que, correctement déployée, la technologie permette d'assurer un meilleur fonctionnement des marchés financiers, un transfert plus fluide de l'épargne des ménages vers l'économie réelle, ainsi que de meilleures perspectives pour les entreprises suisses et – de manière générale – pour l'économie et la prospérité de notre pays.

Le projet législatif sur la TRD – Quelles innovations ?

Sur la base d'un rapport publié en décembre 2018⁴ et d'un avant-projet de loi publié en mars 2019⁵, la Conseil fédéral a présenté un projet de loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués au mois de novembre 2019⁶. Ce dernier est actuellement examiné par les Chambres fédérales.

Contrairement à ce qui a été le cas dans d'autres pays, le Conseil fédéral n'a pas cherché à créer un régime spécifique et indépendant pour les actifs digitaux. L'approche choisie a été de procéder à des adaptations ponctuelles du droit civil et public fédéral, pour tenir compte des spécificités de ces actifs.

Le projet prévoit en particulier:

- Une adaptation du droit des papiers-valeurs, permettant d'associer des droits et des créances non seulement à des supports physiques comme des certificats en papier, mais à des jetons numériques. Le projet de loi consacre à cet égard le nouveau concept de « droit-valeur inscrit » pour désigner un droit-valeur inscrit dans un registre dont l'intégralité est protégée par des mesures organisationnelles et techniques adaptées (typiquement la TRD) et y applique un régime identique à celui des papiers-valeurs (en particulier pour ce qui concerne la protection des acquéreurs de bonne foi).
- Une adaptation du droit de la faillite (tant ordinaire que bancaire), facilitant la revendication des actifs numériques dans la faillite des dépositaires et l'accès de leurs titulaires aux données qui les concernent détenues par les dépositaires.
- Une adaptation de la loi sur les titres intermédiés, réglant la relation entre le régime applicable aux valeurs mobilières détenues de façon « classique » auprès de dépositaires professionnels et aux valeurs mobilières « tokenisées ».

4. <https://www.news.admin.ch/news/message/attachments/55152.pdf>

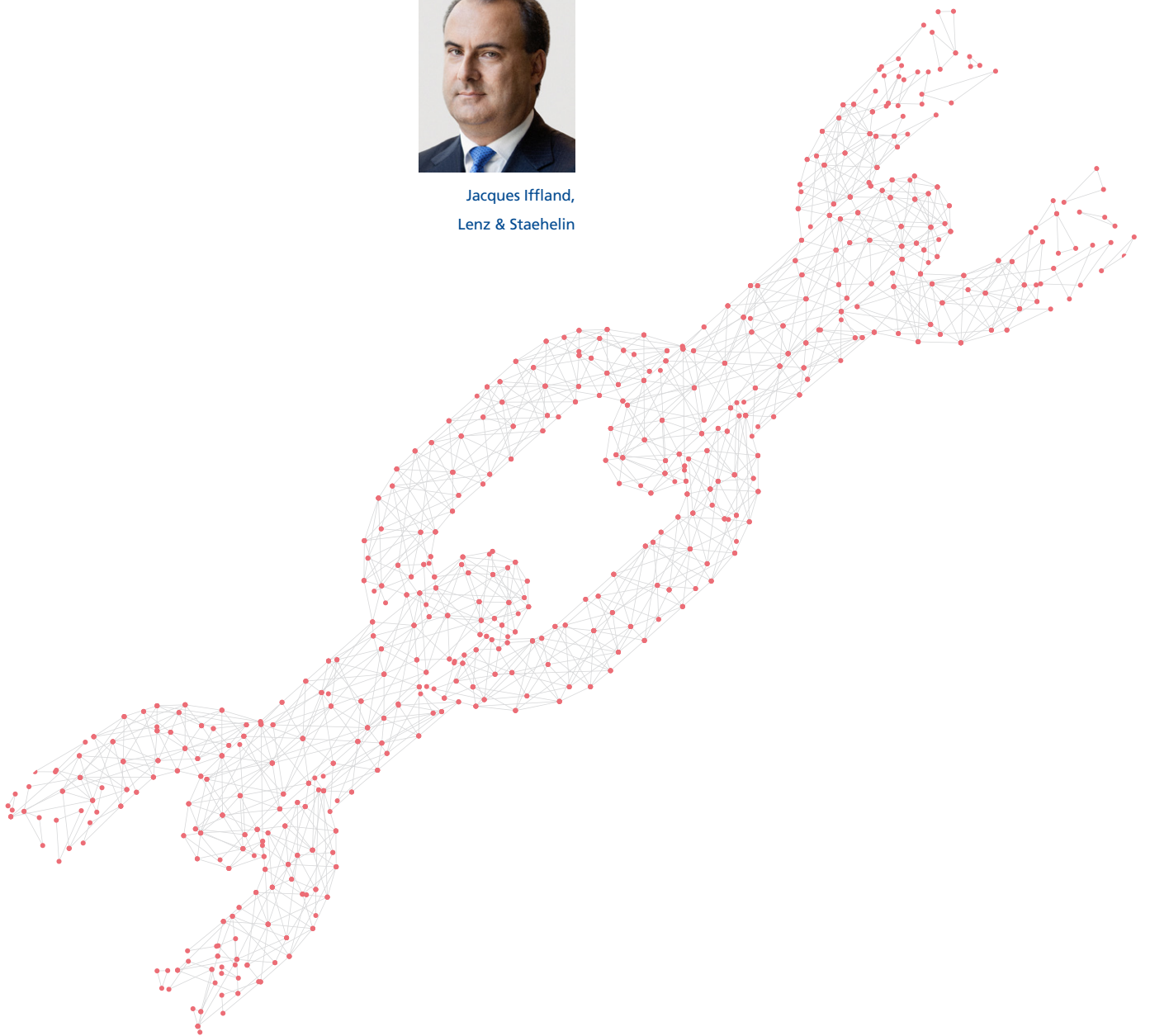
5. <https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-74420.html>

6. Projet de loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués, Feuille fédérale 2020, pp. 319 ss. Voir aussi le Message du Conseil fédéral du 27 novembre 2019 relatif à cette loi, Feuille fédérale 2020, pp. 223 ss.

- Une adaptation du droit de la surveillance des intermédiaires, par la création d'un régime d'autorisation spécifique pour les « systèmes de négociation fondés sur la TRD », c'est-à-dire d'organisations spécialisées dans le négoce de valeurs mobilières tokenisées et dont l'activité regroupe des éléments caractéristiques de plusieurs types d'établissements financiers ou d'infrastructures financières comme par exemple des maisons de titres, des systèmes multilatéraux de négociation, des dépositaires centraux ou des contreparties centrales.



Jacques Iffland,
Lenz & Staehelin



5. Types de jetons

5.1 JETONS DE PAIEMENT

(a) Nature et cas d'application

La catégorie des jetons de paiement inclut les jetons qui sont acceptés comme moyen de paiement pour l'achat de marchandises ou de services ou qui doivent servir à la transmission de fonds et de valeurs. Cette catégorie comprend, d'une part, les cryptomonnaies au sens strict (Bitcoin, Ether, Monero, etc.) et, d'autre part, les nombreuses cryptomonnaies résultant de bifurcations (« forks ») (Bitcoin Cash, Bitcoin Gold, Litecoin, etc.). Elle comprend également les jetons dit « stables » (« stable coins ») comme la Libra.

Les jetons de paiement permettent concrètement d'effectuer des paiements électroniques sans qu'il soit nécessaire d'avoir recours à une tierce partie comme une banque. Ils ont pour but de permettre l'achat de marchandises ou de services, notamment mais pas exclusivement en ligne. Il s'est agi du premier cas d'application concret de la TRD en matière financière.

Les jetons de paiement peuvent être qualifiés de *monnaie virtuelle*⁷ ou de *valeurs patrimoniales incorporelles*⁸, de fait, sécurisés par des algorithmes. Par *monnaie virtuelle*, on entend une représentation numérique d'une valeur, négociable sur Internet et remplissant les fonctions de la monnaie⁹, soit :

- (i) un instrument de mesure ;
- (ii) un instrument d'échange ou de paiement ;
- (iii) un instrument de réserve de valeur.

Les monnaies virtuelles se distinguent de la monnaie électronique (« e-money ») en ceci que leur objet n'est pas de stocker une monnaie ayant cours légal sur un support électronique¹⁰. S'agissant des jetons dits « stables », leur valeur est dérivée d'un actif sous-jacent (par exemple une ou plusieurs devises ayant cours légal) auquel ce type de jeton se rattache pour limiter la volatilité de sa valeur et ainsi favoriser sa reconnaissance comme moyen de paiement. La frontière entre jetons dits « stables » et monnaie électronique peut parfois être difficile à tracer.

Du fait que les jetons de paiement se négocient sur le marché des changes, ils ont une valeur de marché objectivement mesurable.

Les jetons de paiement sont généralement considérés comme des moyens de paiement décentralisés, en ce sens qu'ils ne confèrent aucun droit (de nature obligationnelle ou réelle) à l'égard d'un émetteur en particulier. Ils ne sont pas nécessairement émis par une banque centrale, mais par un réseau d'ordinateurs faisant usage de la TRD.

Compte tenu du fait que leur fonction économique ne présente aucune analogie avec les valeurs mobilières traditionnelles, la FINMA ne traite les jetons de paiement ni comme des valeurs mobilières ni, en principe, comme des instruments financiers au sens de l'article 3 lit. a ch. 1 de la loi sur les services financiers (LSFin). En revanche, les dépôts de jetons de paiement peuvent constituer des instruments financiers si leur valeur de remboursement ou le taux d'intérêt dépend d'un risque ou d'un cours (art. 3 let. a ch. 6 LSFin).

(b) Traitement réglementaire

Du point de vue réglementaire, ce sont en particulier les dispositions relatives au blanchiment d'argent qui sont pertinentes en lien avec les jetons de paiement.

La loi sur le blanchiment d'argent (LBA; RS 955.0) a pour but de protéger le système financier du blanchiment d'argent et du financement du terrorisme. Quiconque fournit des services dans le domaine du trafic des paiements et émet ou gère notamment des moyens de paiement est un intermédiaire financier assujéti à la LBA (art. 2 al. 3 let. b LBA).

L'émission de jetons de paiement représente une émission de moyens de paiements assujéti à la LBA, dès lors que les jetons de paiement peuvent être techniquement transmis sur une infrastructure de type blockchain. Dès le moment où le jeton de paiement peut être utilisé pour payer des biens ou des services à des tiers, le fait de faciliter sa transmission à titre professionnel est susceptible de constituer un service dans le domaine du trafic des paiements au sens de l'article 2 al. 3 let. b, LBA et de l'article 4 al. 1^{er} lit. c et al. 2 OBA.

7. Rapport du Conseil fédéral sur les monnaies virtuelles du 25 juin 2014, p. 8

8. Rapport du Conseil fédéral sur la TRD du 14 décembre 2018, p. 54 et réf. cit.

9. Rapport du Conseil fédéral sur les monnaies virtuelles du 25 juin 2014, p. 8

10. Rapport du Conseil fédéral sur les monnaies virtuelles du 25 juin 2014, pp. 8 et 29

Ceci implique différentes obligations de diligence (vérification de l'identité du cocontractant (art. 3 LBA), vérification de l'ayant droit économique (art. 4 LBA), clarification de l'arrière-plan économique (art. 6 LBA), obligation d'établir et de conserver des documents (art. 7 LBA, etc.) et obligation de s'affilier à un organisme d'autorégulation (OAR) ou de se soumettre directement à la FINMA en vue de la surveillance au sens de la LBA.

S'agissant des « stable coins », leur objectif étant habituellement de mettre à disposition des moyens de paiement, ils sont pratiquement toujours soumis aux obligations de la LBA.

S'agissant des actifs sous-jacents utilisés pour stabiliser ce type de jetons, ils pourront être soumis à la loi sur les banques (LB; RS 952.0) si l'émetteur des jetons stables accepte à titre professionnel des dépôts du public, ce qui suppose que des engagements en remboursement soient pris à l'encontre des déposants (art. 5 al. 1^{er} de l'Ordonnance sur les banques; OB). Ainsi, si les jetons stables sont liés à une monnaie fiduciaire, qu'il existe une prétention de rachat d'un montant fixe, et qu'ils sont gérés aux frais et aux risques de l'émetteur, ils seront généralement considérés comme des dépôts du public au sens du droit bancaire. Dans ce cas, une autorisation de banque ou une licence « Fintech » devra être obtenue auprès de la FINMA, à moins que l'émetteur n'agisse pas à titre professionnel au sens de l'article 6 al. 2 OB (exception dite « sandbox »).

Si les actifs auxquels le jeton est rattaché sont gérés aux frais et aux risques du propriétaire du jeton, une application de la loi sur les placements collectifs de capitaux (LPCC; RS 951.31) est envisageable. Les placements collectifs sont des apports constitués par des investisseurs pour être administrés en commun pour le compte de ces derniers (art. 7 al. 1 LPCC). Les éléments constitutifs d'un placement collectif sont traditionnellement au nombre de trois, soit :

- (I) un patrimoine
(composé des apports des investisseurs);
- (II) un investissement géré en commun
(notion de « *pooling* ») aux fins d'un rendement
et/ou d'un gain en capital; et
- (III) une gestion par un tiers
(notion de « *Fremdverwaltung* »).¹¹.

Pour les jetons stables qui n'offrent aucune prétention au remboursement à leurs détenteurs, mais un mécanisme de stabilisation alternatif, d'autres lois sur les marchés financiers (en plus de la loi sur le blanchiment d'argent) peuvent entrer en ligne de compte, en particulier la loi sur l'infrastructure des marchés financiers (LIMF; RS 958.1) concernant les exploitants de systèmes de paiement.

Si un système de paiement de grande ampleur est développé en lien avec la création d'un « stable coin » (comme c'est le cas de la Libra), la société, l'association ou la fondation émettrice peut également être soumise à la loi sur l'infrastructure des marchés financiers (LIMF; RS 958.1) en tant que système de paiement incluant des services auxiliaires accroissant les risques, voire à la loi sur la Banque nationale (LBN; RS 951.11) si le système exploité est considéré comme étant d'importance systémique.

(c) Traitement fiscal

De manière générale, le traitement fiscal des jetons numériques soulève plusieurs questions, tant pour les sociétés émettrices de jetons que pour les investisseurs. Fin août 2019, l'Administration fédérale des contributions a rendu public un document de travail qui tente de clarifier le traitement fiscal de certains états de fait¹². Ce document n'a pas la vocation d'être exhaustif. En effet, toutes les questions n'ont pas encore été soulevées et de nouvelles situations ne manqueront pas de se présenter en pratique.

Le présent aperçu du traitement fiscal des différents types de jetons de paiement se concentre sur les impôts directs, c'est-à-dire principalement l'impôt sur le bénéfice, l'impôt sur le revenu et l'impôt sur la fortune. Il fait également mention de l'impôt anticipé. De manière systématique, pour chacun des différents types de jetons, il sera d'abord fait état du traitement fiscal au niveau de la société émettrice, puis des investisseurs.

Fiscalité au niveau de la société émettrice

L'émission de jetons de paiement est rare en pratique. Lorsque toutefois cela arrive, un gain fiscalement imposable est réalisé par la société émettrice. Il correspond à la différence entre la valeur comptable des jetons émis, correspondant au prix de revient, et le prix de vente.

11. ATF 2C_571/2009 du 5 novembre 2010

12. Administration fédérale des contributions, Cryptomonnaies, Document de travail, Les cryptomonnaies et les initial coin/token offerings (ICO/ITO) comme objet de l'impôt sur la fortune, le revenu et le bénéfice, l'impôt anticipé et les droits de timbre, du 27 août 2019.

Fiscalité au niveau des investisseurs

Pour les investisseurs personnes physiques, les jetons de paiement font partie des capitaux mobiliers. Il ne fait plus de doute que les jetons doivent être soumis à l'impôt sur la fortune. Ceux-ci doivent ainsi être estimés à leur valeur vénale au 31 décembre. En pratique, l'Administration fédérale des contributions publie la valeur imposable des cryptomonnaies dans sa liste des cours. Ce procédé s'avère parfois trop schématique dans la mesure où l'illiquidité du marché et sa volatilité ne sont pas suffisamment prises en considération. Partant, des mesures d'estimation alternatives devraient pouvoir être présentées de cas en cas à l'autorité fiscale. En l'absence d'un cours d'évaluation, les jetons de paiement doivent être déclarés à leur prix d'achat converti en francs suisses.

La simple détention de jetons de paiement n'entraîne aucune conséquence fiscale en matière d'impôt sur le revenu. Par contre, le paiement d'un salaire au moyen de jetons de paiement constitue un élément imposable dans le chef du travailleur. La valeur déterminante est celle au moment de la perception.

L'achat et la vente de jetons de paiement détenus dans la fortune privée peuvent constituer des gains en capital non imposables ou des pertes en capital non déductibles. En se basant sur l'ensemble des circonstances, une telle activité pourrait être considérée comme une activité lucrative indépendante et donc soumise à l'impôt sur le revenu. En guise d'interprétation, l'Administration fédérale des contributions fait une application analogique des critères définis en matière de commerce professionnel de titres.

L'activité de minage peut être considérée comme une activité lucrative indépendante. Partant, si elle est rémunérée par le biais de jetons de paiement, l'impôt sur le revenu est dû.

En ce qui concerne les personnes morales ou les personnes physiques détenant leurs jetons dans la fortune commerciale, le bilan commercial est le point de départ du résultat fiscal imposable (principe de déterminance). Sur le plan fiscal, les revenus provenant de jetons peuvent prendre différentes formes en fonction de la qualification du jeton (dividendes, redevances, intérêts, autres). Ainsi, ces revenus ont un impact fiscal et sont soumis à l'impôt sur le bénéfice. Il en va de même pour les gains en capital. Les pertes sont quant à elles déductibles.

5.2 JETONS D'INVESTISSEMENT

(a) Nature et cas d'application

Alors que les jetons de paiement ne confèrent généralement aucun droit à la remise d'actifs spécifiques, les jetons d'investissement représentent eux des *valeurs patrimoniales*. Ces dernières peuvent être de nature diverse, mais représentent en principe des instruments financiers tels que des titres de participation ou de dette, des instruments dérivés ou encore des parts de placements collectifs.

Les jetons d'investissement ont souvent (quoique pas nécessairement) vocation à être standardisés et diffusés en grand nombre sur le marché. Si tel est le cas, ils peuvent constituer des « valeurs mobilières » au sens des lois suisses sur les marchés financiers. Cette particularité explique que ces instruments sont souvent désignés par le terme de *security tokens* (« *security* » étant l'expression anglaise utilisée pour désigner des valeurs mobilières).

L'acronyme « STO » (pour « *security token offering* ») est souvent utilisé pour désigner l'émission de jetons d'investissement. Ainsi définis, les STOs forment une sous-catégorie du concept plus large d'ICO (« *initial coin offering* »), qui désigne l'émission de toute forme de jetons numériques, qu'il s'agisse de jetons de paiement, d'investissement ou d'utilité. Le terme STO couvre cependant des opérations variées. Il peut viser tant l'émission de simples prétentions contractuelles que de véritables titres de participation tels que des actions, des bons de participation ou des bons de jouissance émis conformément au droit des sociétés. La nature exacte des jetons offerts dans le cadre d'une STO doit donc être analysée au cas par cas.

La FINMA définit les jetons d'investissement de façon large. Elle considère que les *jetons qui tendent à financer la création ou la fourniture future de biens ou de services* doivent être qualifiés de jetons d'investissement, et non de jetons d'utilité (tels qu'ils sont définis ci-dessous). Cette distinction est importante, car le régime réglementaire applicable aux jetons d'investissement diffère de celui applicable aux jetons d'utilité sur de nombreux points.

Sur le plan légal, la question s'est posée de savoir comment des valeurs mobilières non incorporées dans des titres physiques (c'est-à-dire des « droits-valeurs » selon la terminologie du Code suisse des obligations) peuvent être valablement associées à des jetons numériques, de façon à ce qu'il ne soit pas possible de faire valoir ou de transférer l'un sans l'autre. Le procédé est comparable à celui par lequel le droit

des papiers-valeurs associe des prétentions à des supports physiques (typiquement des certificats papier). La différence réside dans le fait que, s'agissant de jetons d'investissement, les droits-valeurs sont associés à des jetons numériques plutôt qu'à des supports physiques. Le projet de loi fédérale sur la technologie des registres distribués donne une base légale explicite à ce procédé (*voir à ce sujet la section 4 ci-dessus*). Des organismes privés tels que la Capital Markets and Technology Association à Genève ont cependant établi des procédés permettant de « tokeniser » valablement des droits-valeurs selon le droit actuel déjà.

(b) Traitement réglementaire

Le fait que des valeurs patrimoniales soient « tokenisées » – c'est-à-dire émises sous la forme de jetons numériques – n'a en principe pas d'incidence sur leur traitement réglementaire. Le régime réglementaire des jetons dépend donc de la nature des valeurs patrimoniales qui leur sont attachées.

Contrairement aux jetons de paiement, les jetons d'investissement ne relèvent pas du trafic des paiements. De ce fait, leur émission n'est pas assujettie à la réglementation contre le blanchiment d'argent et n'implique donc pas d'affiliation obligatoire à un organisme d'autorégulation. L'émission de jetons d'investissement n'implique pas non plus l'exploitation d'un système de paiement au sens de la législation sur les infrastructures des marchés financiers ou sur la Banque nationale suisse (BNS). Elle ne requiert donc pas d'autorisation spécifique de la FINMA ou de surveillance de la BNS.

En revanche, comme pour ce qui concerne les jetons de paiement et sous réserve de certaines exceptions, l'émission de jetons d'investissement nécessite une autorisation de la FINMA si les jetons incorporent des dépôts du public au sens de la loi sur les banques. Elle peut aussi être assujettie à la loi sur les placements collectifs de capitaux si les jetons émis sont associés à des parts de placements collectifs. De même, le négoce professionnel de jetons d'investissement (en particulier l'acquisition et l'offre au public de valeurs mobilières émises par des tiers), ainsi que l'exploitation professionnelle de plateformes de négociation pour de tels instruments, sont des activités soumises à autorisation, qui requièrent une autorisation de la FINMA.

Contrairement à l'offre au public de valeurs mobilières émises par des tiers, l'émission pour compte propre de jetons incorporant des droits de participation ou de créance ne requiert pas d'autorisation de la FINMA. Une telle activité peut nécessiter l'établissement d'un prospectus et l'appro-

bation de ce document par un organe de contrôle agréé si les jetons sont offerts au public ou que leur émetteur en demande l'admission sur une plateforme de négociation, et qu'aucune des exceptions à l'obligation d'établir un tel document prévue par la loi sur les services financiers n'est applicable. Le contrôle du prospectus est cependant un acte ponctuel de l'autorité, qui n'entraîne pas d'assujettissement durable de l'émetteur à une surveillance étatique.

(c) Traitement fiscal

Le traitement fiscal lors de l'émission de jetons incorporant des valeurs mobilières dépend des relations de droit civil entre la société émettrice et les investisseurs.

Fiscalité au niveau de la société émettrice

Lors de l'émission, deux hypothèses doivent être distinguées.

En premier lieu, si les fonds levés constituent du capital étranger ou des fonds propres, leur obtention ne devrait alors générer aucun bénéfice imposable. Si ces fonds sont assimilés à des obligations, le paiement des intérêts y relatifs constitue des charges fiscalement déductibles, entraînant également le prélèvement de l'impôt anticipé. L'émission de tels jetons ne devrait en principe pas générer de conséquences fiscales en matière de droit de timbre d'émission.

En second lieu, si aucun droit de participation n'est émis, les fonds reçus par la société émettrice constituent un revenu imposable avec comptabilisation au niveau du compte de résultat. Dans cette seconde hypothèse, la pratique fiscale permet à la société émettrice de comptabiliser une provision. Le but de cette provision est de tenir compte de l'obligation contractuelle lui incombant pour la réalisation d'un projet déterminé. La dissolution de la provision générera un produit imposable pour la société émettrice. L'idée est que les revenus provenant d'une émission de jetons ne l'enrichissent pas immédiatement. Ils devront simplement lui permettre de couvrir les frais liés au développement du projet. En dissolvant la provision durant la phase de développement du projet, la société émettrice pourra neutraliser une partie importante de son bénéfice imposable durant un laps de temps considérable. Les conditions précises d'application de ce mécanisme doivent être toutefois analysées de cas en cas.

En principe, les paiements issus de jetons de capital propre ou de jetons de participation ne sont pas soumis à l'impôt anticipé. L'Administration fédérale des contributions a toutefois prévu des cautions lors de certaines distributions en faveur de détenteurs de jetons qui sont également actionnaires. Il n'est pas possible d'exclure le prélèvement

d'un droit de timbre de négociation. Cela peut par exemple être le cas si les jetons de participation se rapportent à des documents imposables.

Fiscalité au niveau des investisseurs

Pour les personnes physiques, les jetons incorporant des valeurs mobilières sont soumis à l'impôt sur la fortune. Leur estimation est effectuée à la valeur vénale à la fin de la période fiscale. Ils doivent être déclarés à leur prix d'acquisition en l'absence d'un cours d'évaluation.

De manière générale, l'émission de jetons incorporant des valeurs mobilières est sans incidence sur l'impôt sur le revenu. En revanche, la rémunération de ces jetons, que cela soit sous la forme d'intérêts versés périodiquement, d'une rémunération unique ou d'un paiement, sont soumis à l'impôt sur le revenu au moment de la réalisation. La question de savoir si le remboursement du capital initialement investi constitue un élément imposable dépend du type de jeton incorporant une valeur mobilière. Une telle hypothèse doit être analysée de cas en cas.

En ce qui concerne le paiement d'un salaire au moyen de jetons de capital étranger, de même qu'en ce qui concerne une potentielle requalification en activité lucrative indépendante (quasi-professionnalité), il est renvoyé au chiffre 5.1 (c) ci-dessus.

Pour les personnes morales et les personnes physiques détenant leurs jetons dans leur fortune commerciale, le principe général de détermination s'applique. Cela signifie que les comptes commerciaux sont déterminants sur le plan fiscal (sous réserve de l'application de règles correctrices par le fisc). À noter toutefois que la rémunération provenant de certains jetons d'investissement s'assimile au paiement d'un dividende. Pour autant que les conditions légales soient remplies, le mécanisme de la réduction pour participation devrait trouver application en ce qui concerne le paiement à des personnes morales.



Cédric Portier,
Gros & Waltenspühl



Florian Ducommun,
HDC



Justin Brodard,
avocat,
expert-fiscal diplômé

5.3 JETONS DE SERVICE

(a) Nature et cas d'application

Le jeton de service (ou utility token) est une représentation sur la blockchain (jeton) d'un droit d'usage ou d'accès à un service fourni par son émetteur. Selon le guide pratique FINMA pour les questions d'assujettissement concernant les *initial coin offerings* (ICOs) du 16 février 2018¹³, le jeton de service est défini comme un jeton censé donner accès à un usage ou à un service numérique et qui s'appuie sur l'utilisation d'une infrastructure de type blockchain. Le jeton confère à son propriétaire le droit que l'émetteur y a incorporé. L'infrastructure de type blockchain est utilisée pour rendre le jeton transférable à quiconque en cas d'utilisation d'une blockchain publique telle qu'Ethereum, ou à l'intérieur d'un réseau prédéterminé en cas d'usage d'une blockchain privée.

Le jeton de service se distingue du jeton de paiement (*payment token*) en ce qu'il n'est en principe accepté comme moyen de paiement que par son émetteur. Toutefois, si un jeton de service est recherché et a une valeur intrinsèque de marché, il est possible qu'il soit aussi accepté comme moyen de paiement par des tiers, et qu'il doive alors aussi être traité comme jeton de paiement.

Le jeton de service se distingue aussi du jeton d'investissement (*security token*) par le fait que le premier ne représente pas de droit à la remise de valeurs patrimoniales par l'émetteur (par exemple le paiement d'un dividende ou d'un intérêt) ni d'une valeur sous-jacente (par exemple un droit à la remise de certaines quantités de métaux précieux). Toutefois, si la prestation à laquelle le jeton donne droit n'est pas disponible au moment de son émission, le jeton doit alors être qualifié de jeton d'investissement. Dans ce cas, en effet, le jeton n'est pas acquis pour le service qu'il permet d'obtenir (ce dernier n'étant pas encore disponible) mais dans la perspective d'une plus-value lorsque le service aura été développé et pourra être obtenu. Pour les émetteurs, les jetons de service permettent d'offrir de nouvelles prestations, de créer des communautés et de fidéliser leurs clients. Un jeton ne donnant accès qu'à des prestations courantes n'aura généralement que peu de valeur, car la prestation pourra alors être obtenue directement sans que le recours à un jeton apporte un avantage. Le jeton de service n'a de raison d'être que dans des cas particuliers. La pratique offre divers exemples :

- Jetons permettant d'obtenir un rabais sur les prestations de l'émetteur. Par exemple, le client qui utilise le jeton pour payer les services de l'émetteur obtient un tarif préférentiel.
- Obtention d'une prestation particulière selon le nombre de jetons détenus et/ou la durée de détention. Plus le nombre de jetons détenus est important et/ou la durée de détention est longue, plus l'avantage obtenu est important. Par exemple, l'utilisateur qui détient un nombre de jetons déterminé pendant une période donnée peut obtenir une prestation gratuite.
- Jeton permettant d'obtenir un avantage pour une prestation effectuée en faveur de l'émetteur. Par exemple, l'utilisateur reçoit un jeton de service après avoir visionné une publicité, avoir participé à un sondage ou avoir communiqué ses données personnelles.

Le jeton de service peut aussi être utilisé comme un outil de fidélisation du client plutôt que comme moyen de paiement. Par exemple, les « points de fidélité » octroyés par certains commerces peuvent être incorporés dans des jetons de service, ce qui peut en faciliter l'usage et le transfert par exemple entre amis ou membres de la famille.

D'autres cas d'application peuvent être trouvés au sein de structures associatives comme des clubs sportifs, où les jetons remis aux supporters peuvent leur permettre de participer à certaines décisions (comme par exemple le choix de la couleur du maillot de la saison suivante) ou d'accéder à des loges VIP.

Le jeton de service peut aussi avoir un usage exclusivement technique. Il peut ainsi être utilisé pour la création de signatures électroniques, d'une identité digitale ou d'un dossier médical sur la blockchain. Dans de tels cas, le jeton permet d'apporter la preuve qu'un document a été signé par une personne déterminée (à savoir le détenteur de la clé privée du jeton concerné). Le jeton de service permet donc de réaliser de nombreuses opérations digitales avec un degré de sécurité élevé.

13. <https://www.finma.ch/fr/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=fr>

(b) Traitement réglementaire

Les jetons de service ne confèrent aucun droit financier. Bien qu'ils possèdent certaines caractéristiques des valeurs mobilières (ils sont standardisés et susceptibles d'être diffusés en grand nombre sur le marché¹⁴), ils n'incorporent pas d'instruments financiers et ne constituent donc juridiquement pas de telles valeurs.

L'usage de jetons de service est donc intéressant à plus d'un titre : les frais nécessaires à leur mise en œuvre sont peu élevés et aucune autorisation n'est requise pour leur émission ou leur négoce. De plus, au regard de leur qualification juridique, l'émetteur ne doit pas nécessairement publier de prospectus conforme au droit des marchés financiers dans les juridictions dans lesquelles il entend les distribuer. Lors de l'émission de jetons de service sur le marché, l'émetteur publie généralement un document décrivant le fonctionnement technique du jeton et les services qui y sont associés (document qualifié de « *white paper* » en pratique) pour informer les investisseurs initiaux du droit auquel ils souscrivent.

En outre, dans la mesure où ils ne constituent pas des valeurs mobilières, les jetons de service peuvent être échangés sur des plateformes de négociation, que ce soit par des personnes souhaitant les acquérir pour utiliser les services de l'émetteur, par ceux souhaitant les vendre faute d'en avoir l'utilité, ou encore par ceux qui entendent spéculer sur leur valeur future.

Faute d'incorporer des instruments financiers, les jetons de service ne sont en principe pas assujettis à la réglementation contre le blanchiment d'argent s'ils n'ont pas vocation à servir de moyen de paiement. L'émission de jetons de service n'implique donc pas nécessairement d'affiliation à un organisme d'autorégulation au sens de la loi sur le blanchiment d'argent (LBA; RS 955.0). En pratique toutefois, les banques refusent (pour l'heure) d'accepter des fonds issus de l'émission de jetons de service sans connaître l'identité des acheteurs. De ce fait, lors de l'émission de tels jetons dans le cadre d'une ICO, l'identification de l'acheteur et de l'origine des fonds est nécessaire comme pour l'émission d'un jeton de paiement.

(c) Traitement fiscal

Fiscalité au niveau de la société émettrice

Le rapport juridique entre la société émettrice et les investisseurs peut être qualifié de mandat. Partant, les fonds reçus par celle-ci constituent un revenu imposable

sable avec comptabilisation au niveau du compte de résultat. Une provision peut être constituée selon les modalités décrites au chiffre 5.2 (c) ci-dessus. Les prétentions découlant d'un rapport de mandat ne sont pas soumises à l'impôt anticipé.

Fiscalité au niveau des investisseurs

Les jetons de service, en tant qu'ils sont réputés négociables, ont une valeur de marché. Ils sont donc soumis à l'impôt sur la fortune des personnes physiques. Les mêmes règles d'évaluation s'appliquent que pour les jetons de paiement. Il est donc renvoyé au chiffre 5.1 (c) ci-dessus. On précisera que les jetons de service ne sont pas des documents imposables. Partant, leur négoce n'est pas soumis au droit de timbre de négociation.

Concernant l'impôt sur le revenu, le traitement fiscal est identique à celui applicable aux jetons de paiement comme développé sous chiffre 5.1 (c) ci-dessus. L'impôt n'est dû qu'en cas de paiement de la société émettrice à l'investisseur. L'investisseur n'a pas droit à un remboursement en neutralité fiscale des montants investis.

En ce qui concerne le paiement d'un salaire au moyen de jetons de capital étranger, de même qu'en ce qui concerne une potentielle requalification en activité lucrative indépendante (quasi-professionnalité), il est également renvoyé au chiffre 5.1 (c) ci-dessus.

Pour les personnes morales et les personnes physiques détenant les jetons de la fortune commerciale, le principe de déterminance s'applique. Cela signifie que les comptes commerciaux sont déterminants sur le plan fiscal (sous réserve de l'application de règles correctrices par le fisc).



Cédric Portier,
Gros & Waltenspühl



Lars Schlichting,
Kellerhals Carrard



Justin Brodard,
avocat,
expert-fiscal diplômé

14. Art. 2 let. b loi sur l'infrastructure des marchés financiers.

6. Émission de jetons

De la création du Bitcoin aux ICOs : un phénomène technologique et sociétal

La première blockchain, le Bitcoin, est apparue dans le sillage de la crise financière de 2008. La technologie est adoptée dans un premier temps dans des cercles libertariens et « crypto-anarchistes » ne désirant plus dépendre d'institutions financières dans lesquelles ils ont perdu confiance.

6.1 Initial Coin Offerings (ou ICOs)

Les jetons émis par ce biais sont peu ou pas régulés et les fonds sont levés en cryptomonnaies. Ces levées de fonds d'un nouveau type permettent de réunir des sommes importantes à l'échelle planétaire en quelques jours en s'appuyant sur les réseaux sociaux. Dans certains cas, les investisseurs qui y participent réalisent d'importants bénéfices en peu de temps.

Ces premiers succès nourrissent une explosion d'ICOs. De plus en plus de projets apparaissent, certains sans substance et portés par des campagnes marketing à gros budget. Leurs lancements peuvent être financés par des investisseurs cherchant à réaliser un profit à très court terme, en reprenant les codes et les recettes qui ont fait le succès d'ICOs précédentes.

Des difficultés apparaissent ensuite : afin que les initiateurs des ICOs puissent utiliser les fonds levés, les cryptomonnaies collectées doivent être converties en monnaie fiduciaire. Les banques reviennent alors dans l'équation. Les autorités de surveillance des marchés financiers prennent alors conscience de l'ampleur du phénomène et établissent un cadre contraignant voire, dans certains cas, interdisent l'émission d'actifs digitaux.

Enfin – et c'est le plus gros problème – les modèles d'affaires basés sur la création d'économies distribuées facilitées par des cryptomonnaies ne paraissent pas fonctionner au-delà de quelques blockchains d'envergure ayant le potentiel de devenir des infrastructures sur lesquelles un écosystème de fournisseurs et de clients peut venir se greffer.

Avec l'avènement des ICOs, des prestataires de services sont apparus. Ils fournissent les solutions technologiques permettant de détenir des jetons numériques ou d'organiser l'échange. Des universités offrent des formations dédiées. Des réviseurs indépendants évaluent la qualité des codes des contrats intelligents (*smart contracts*) déployés sur les blockchains.

Des conseils d'administrations aux quidams, tout le monde a entendu parler de la blockchain et certains ont investis dans des ICOs. Dans certains pays, en particulier en Suisse, les autorités de surveillance des marchés se positionnent et clarifient le régime réglementaire applicable aux cryptomonnaies et aux autres actifs digitaux.

6.2 Jetons d'investissement (*security tokens*)

En anglais, le terme « *security* » désigne un instrument financier standardisé comme, par exemple, une action, une obligation ou encore une part de fonds. En Suisse, il existe une liberté de forme dans l'émission de telles valeurs mobilières. Il est notamment possible d'associer un jeton numérique à une valeur patrimoniale telle qu'une action ou un bon de participation. C'est ce que l'on appelle un jeton d'investissement (*security token*).

Les jetons d'investissement présentent plusieurs avantages par rapport aux cryptomonnaies ou aux instruments financiers classiques.

Premièrement, ils sont digitaux et font usage de procédés cryptographiques. À la différence d'un fichier Excel dont le contenu peut facilement être altéré, un registre d'actionnaires ou d'obligataires tenu au moyen d'une blockchain publique est en principe incorruptible. La blockchain constitue alors un « tiers de confiance » entre émetteurs et les investisseurs.

Deuxièmement, les droits accordés aux investisseurs sont forts. Un jeton d'investissement associé aux actions d'une société suisse donne aux investisseurs les mêmes droits que ceux d'actions incorporés dans des certificats physiques : droit de vote, droit aux dividendes, droit à l'information. Ces droits d'actionnaires peuvent être mis en œuvre devant un tribunal. C'est une différence importante par rapport aux jetons de service, qui ne confèrent aucun droit social aux investisseurs.

Troisièmement, les jetons d'investissement peuvent être facilement distribués et détenus par des tiers. Leur nature digitale facilite les opérations à grande échelle impliquant des centaines, voire des milliers d'investisseurs. Ces jetons peuvent être conservés auprès de banques ou de maisons de titres. Une société qui lève des fonds peut ainsi distribuer ses jetons d'investissement par l'intermédiaire d'une banque, ce qui permet aux clients de cette dernière d'investir au travers de leur interface de e-banking ou d'une application mobile.

Quatrièmement, les jetons d'investissement peuvent améliorer l'efficacité opérationnelle de façon importante. Il est possible de coder certaines règles directement dans le « *smart contract* » dont les jetons d'investissement sont issus. Cela permet d'automatiser la prise en charge des restrictions qui doivent être mises en œuvre dans certaines juridictions, ou encore d'assurer le respect des droits préférentiels qui peuvent trouver application en cas d'émission, autant de règles qui sont aujourd'hui difficiles à mettre en œuvre.

Enfin, la tokenisation des valeurs mobilières facilite la négociation de ces dernières. Que ce soit pour des transactions conclues de gré à gré ou sur des plateformes de négociation, l'utilisation de jetons permet d'automatiser l'exécution des contrats d'achat et de vente de manière sûre et décentralisée.

6.3 Security token offerings (STOs)

L'intérêt des jetons d'investissement est de pouvoir être utilisés pour les levées de fonds d'entreprises.

D'un point de vue légal, une entreprise qui réalise une STO doit en principe satisfaire, d'un côté, aux règles applicables en matière d'offre au public de valeurs mobilières (si les jetons sont standardisés et émis en grand nombre) et, d'un autre côté, aux exigences d'identification et de clarification qu'imposent les lois contre le blanchiment et le financement du terrorisme. Satisfaire à ces exigences était jusqu'à récemment difficile pour les entreprises. Une offre publique de jetons d'investissement nécessitait notamment la préparation d'un prospectus, un document qui peut être onéreux, complexe et chronophage à établir.

Toutefois, après l'entrée en vigueur des règles pertinentes de la loi sur les services financiers, il ne sera plus nécessaire d'établir un prospectus pour les offres au public de valeurs mobilières qui portent sur moins de 8 millions de francs. Cette exception à l'obligation d'établir un prospectus correspond à celle que prévoit la réglementation européenne et constitue un allègement d'importance.

6.4 Plateformes de STO

Des prestataires de services dédiés à la conduite de STOs sont apparus. Ces prestataires fournissent des solutions en marque blanche qui permettent aux entreprises levant des fonds de satisfaire à leurs réglementations réglementaires, que ce soit en Suisse ou à l'étranger, ainsi qu'aux exigences des lois anti-blanchiment. Ils fournissent des interfaces digitales, fonctionnant sur ordinateur ou téléphone portable, permettant aux sociétés émettrices d'accepter les investis-

seurs en conformité avec les exigences légales et de réunir les informations nécessaires pour les identifier et vérifier l'origine des fonds.

D'un point de vue opérationnel et technologique, la société qui procède à une STO doit être en mesure de gérer un grand nombre de relations investisseurs dans la durée, ainsi que les jetons d'investissement émis. Là aussi, des prestataires fournissent des services spécifiques. Les solutions offertes permettent généralement de créer une interface privée entre investisseurs et émetteurs, au travers de laquelle les investisseurs peuvent accéder aux documents partagés par l'émetteur et participer à la vie sociale de ce dernier. L'interface permet à l'émetteur de communiquer avec un grand nombre d'investisseurs, d'émettre et de gérer des jetons d'investissement et d'organiser les corporate actions telles que le paiement de dividendes ou le remboursement d'emprunts.

À mesure qu'évolue la réglementation et la technologie, les jetons d'investissement peuvent devenir un instrument important pour le financement des entreprises. On peut penser que, dans une dizaine d'années, les STOs seront l'un des modes de financement courant des start-up, et que les entreprises recourront largement aux jetons d'investissement. De par sa flexibilité, le cadre légal et réglementaire suisse présente de nombreux avantages dans ce contexte.



Vincent Trouche,
Tokenestate

7. Structure et fonctionnalité des smart contracts

Dans le cadre du financement d'un projet au moyen d'une levée de fonds sur la blockchain et de la digitalisation d'un actif sous-jacent, il est important de différencier les deux principaux *smart contracts* en jeu.

Un premier contrat régit l'actif tokenisé (jeton) et en définit les caractéristiques internes comme par exemple :

- les fonctions de base (e.g. « ERC-20 »);
- le nom du jeton, ainsi que son identifiant (*ticker* ou symbole);
- la quantité de jetons à mettre en circulation et la possibilité éventuelle d'augmenter ou diminuer cette quantité;
- la classe d'actif et les propriétés associées, comme par exemple la divisibilité, le droit de vote ou le droit aux dividendes;
- le registre des détenteurs (conservé sous forme pseudonymique), avec mention des montants détenus;
- le moteur de règles de transférabilité;
- le mode de signature des transactions; et
- les fonctionnalités de saisie.

Un deuxième contrat – le contrat de vente – chapeaute le processus d'émission sur le marché primaire. Il gère les flux financiers entrants et sortants tout en contrôlant leur conformité. Ce contrat incorpore les caractéristiques de la vente elle-même telles que :

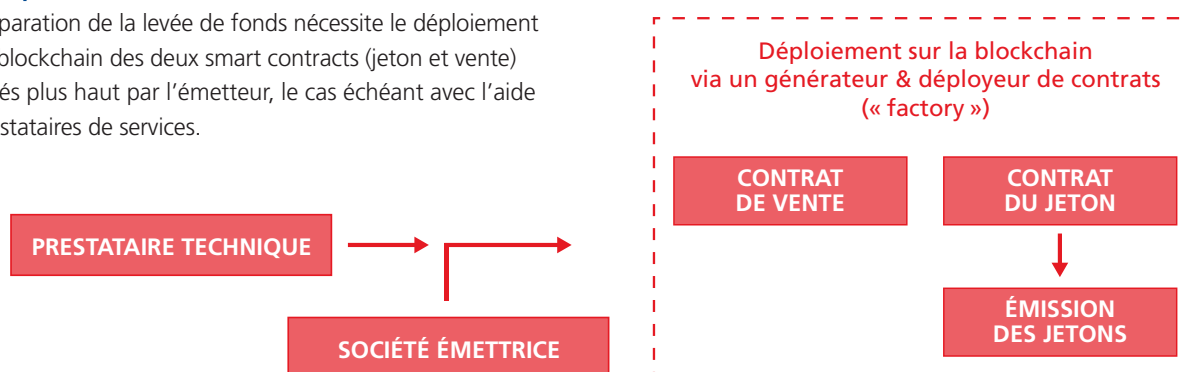
- la quantité de jetons vendus;
- le début et la fin de l'offre sur le marché primaire;
- le prix du jeton et la devise ou cryptomonnaie de référence pour son paiement;
- l'éventuel bonus accordé aux premiers investisseurs;
- l'adresse de la réserve de jetons;
- l'adresse du « portefeuille froid » (*cold wallet*);
- l'adresse des personnes qui administrent la mise en œuvre du smart contrat ainsi que le registre de conformité. Ces opérateurs peuvent éditer les registres et sont appelés « Oracles » en pratique.

Il existe aujourd'hui plusieurs solutions qui permettent de générer, déployer et gérer des smart contracts pour des jetons d'investissement. Citons par exemple :

- C-Layer (par la fondation éponyme) sur Ethereum;
- Bridge Protocol (Mt Pelerin) sur Ethereum;
- ERC 1400 (Polymath/Consensys) sur Ethereum;
- Polymesh (Polymath) sur une blockchain dédiée.

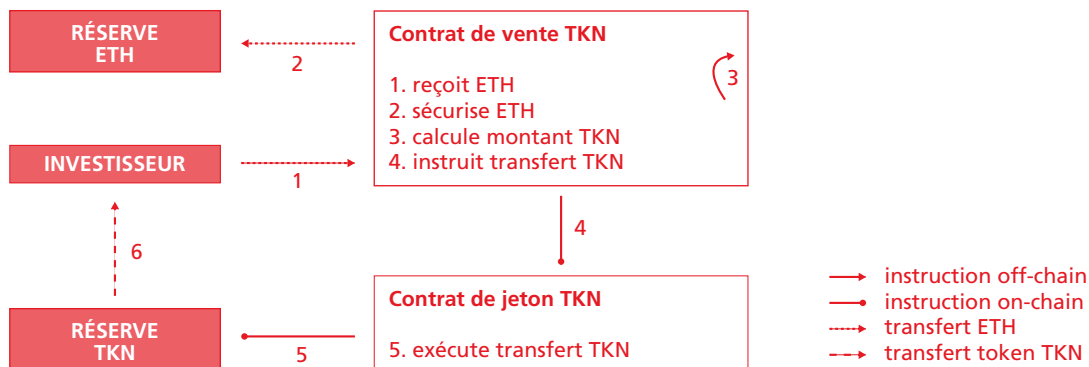
7.1 Préparation de la levée de fonds

La préparation de la levée de fonds nécessite le déploiement sur la blockchain des deux smart contracts (jeton et vente) évoqués plus haut par l'émetteur, le cas échéant avec l'aide de prestataires de services.

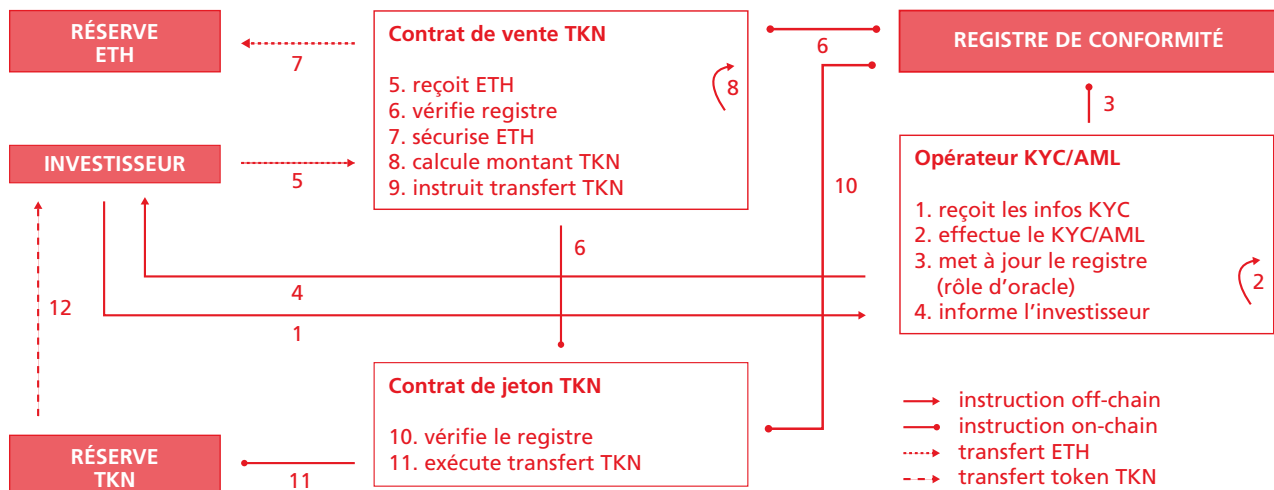


7.2 Levée de fonds: interactions entre investisseurs, oracles, et smart contracts sur le marché primaire

À titre d'exemple, prenons le cas d'un investisseur souhaitant acheter des jetons avec la devise native de la blockchain Ethereum, l'Ether (ETH). Si la vente intervient sans identification de l'investisseur et porte sur un jeton dont l'acquisition ne fait l'objet d'aucune restriction (ce qui historiquement a été le cas des premières ICOs), le processus se déroule schématiquement de la façon suivante :



Si une couche de mise en conformité est maintenant ajoutée, un prestataire de services de vérification KYC va se faire conférer la faculté d'administrer un registre sur la blockchain, au moyen duquel les règles de transférabilité du jeton (adresses, quantités) seront vérifiées. On aboutit alors à la structure suivante :



Noé Curtz,
Altcoinomy



Olivier Cohen,
Altcoinomy



8. Négoce de jetons

8.1 Besoin de marchés secondaires pour actifs digitaux

Lorsqu'une entreprise cherche à lever des fonds mais qu'elle ne souhaite pas effectuer une entrée en bourse (IPO), elle peut faire ce que l'on appelle une « *security token offering* » (STO), c'est-à-dire une levée de fonds par l'émission de jetons d'investissement. Ces jetons représentent des valeurs patrimoniales et peuvent avoir les mêmes fonctions économiques qu'une action, une obligation ou un instrument financier dérivé. Une levée de fonds a cependant de moindres chances d'être couronnée de succès si les jetons ne peuvent pas être traités sur un marché secondaire après l'émission. C'est en effet le marché secondaire qui permet aux investisseurs initiaux de revendre leurs jetons, si possible avec une plus-value.

8.2 Absence de plateforme pour le négoce de jetons d'investissement

Pour l'heure, les plus grandes plateformes d'échange de jetons étrangères comme Binance ou Coinbase se concentrent sur le négoce de jetons qui ne sont pas des valeurs mobilières, dont en particulier les cryptomonnaies telles que le Bitcoin, l'Ether, le Litecoin ou le Ripple.

En Suisse, il n'y a pas de grande plateforme d'échange de jetons d'investissement. SIX Swiss Exchange, la principale bourse suisse, exige que les titres admis à la cotation soient déposés auprès d'un dépositaire central et traités sous la forme de titres intermédiés, ce qui exclut en l'état la cotation de jetons d'investissement. SIX a initié le projet SIX Digital Exchange (SDX). Il s'agit cependant d'un projet à long terme dont le résultat final n'est pas encore déterminé. En Suisse, il existe bien des infrastructures pour le négoce de jetons de service, comme la plateforme de transmission d'ordres d'achat et de vente de jetons lancée par Swissquote où les ordres sont conciliés (« *matchés* ») selon un modèle d'enchères périodiques. Ces infrastructures ne supportent toutefois pas les jetons d'investissement pour le moment.

Les émetteurs de jetons d'investissement ne disposent donc actuellement pas de plateformes pour assurer le négoce des instruments qu'ils émettent.

8.3 Une lacune à combler

Il y a toujours plus de demandes de sociétés qui souhaiteraient émettre des jetons d'investissement et faire bénéficier les investisseurs d'une plateforme d'échange. Que faire pour répondre à cette demande ?

Selon la loi sur l'infrastructure des marchés financiers (LIMF), une banque ou une maison de titres suisse peut développer une plateforme pour le négoce de valeurs mobilières « tokenisées » comme des actions ou des bons de participation sous la forme d'un « système organisé de négociation » (SON). Pour admettre des valeurs mobilières au négoce sur un SON, l'établissement concerné doit assurer le respect de règles strictes en matière notamment de prévention des conflits d'intérêts, de garantie d'une négociation ordonnée et de transparence pré- et post-négociation. L'établissement doit aussi surveiller la négociation pour prévenir d'éventuels abus de marché.

Les exigences sont ainsi élevées, puisqu'une autorisation de la FINMA pour opérer en tant que banque, maison de titres ou plateforme de négociation est requise. Le cadre légal suisse offre néanmoins d'ores et déjà des possibilités qui n'existent pas dans des juridictions étrangères. Il faut donc espérer que cette opportunité sera vite saisie par les acteurs du marché suisse.

8.4 Adaptations du droit suisse à la blockchain

Un projet de loi visant à intégrer les technologies de blockchain dans le droit suisse est actuellement débattu aux Chambres fédérales suisses. Il verrait la création d'une nouvelle catégorie d'autorisation pour les systèmes de négociation fondés sur la blockchain, soumis à la surveillance de la FINMA. Cette catégorie sera notamment disponible pour les entreprises Fintech qui ne sont pas encore des banques ou des maisons de titres, mais qui font la demande d'autorisation correspondante à la FINMA. Ainsi, si le droit suisse actuel offre d'ores et déjà la possibilité aux banques et maisons de titres de mettre à disposition un marché secondaire pour les jetons d'investissement, la nouvelle loi ouvrira la porte à un plus grand nombre d'acteurs.

C'est un pas dans la bonne direction. Nul doute que les banques et sociétés Fintech innovantes sauront saisir les opportunités actuelles et futures dans le domaine et que cela aura une influence positive considérable sur le développement du marché des levées de fonds en Suisse.



Morgan Lavanchy,
Swissquote Bank

Le digital requiert un grand besoin de confiance

SICPA, leader mondial des encres de sécurité et des solutions sécurisées pour les billets de banque et les documents officiels, utilise la blockchain pour garantir l'intégrité des données numériques.

La société SICPA, fondée en 1927 à Lausanne, accompagne gouvernements et autorités dans leurs missions critiques, telles que la sécurisation des billets de banque, des documents officiels, la lutte contre la contrefaçon ou encore la collecte des taxes d'accises via une traçabilité sécurisée.

Vice-président eGovernment Systems chez SICPA, Philippe Thévoz participe au développement de nouvelles plateformes numériques à l'intention des gouvernements qui, depuis quelques années, s'engagent de plus en plus dans le digital. « De nouvelles missions critiques émergent de ce fait, explique-t-il. Il était donc tout naturel pour nous de les accompagner. Générer de la confiance est notre devise, et ce besoin est énorme dans le numérique, car il y a beaucoup de risques de fraude, de hacking, etc. Nous nous devons d'appliquer la même recherche d'excellence pour sécuriser le numérique que celle mise en œuvre dans le monde physique. La blockchain s'est révélée comme l'un des éléments qui le permettent. Car que l'on parle de documents sécurisés ou de processus gouvernementaux en ligne, il nous faut répondre à la même double exigence : garantir les plus hauts niveaux de sécurité tout en les rendant « industrialisables ». La blockchain permet cela. »

« Dès lors, pour quelle solution opter ? Le Bitcoin est souvent cité pour la sécurité de son protocole, mais il n'a pas de dimension industrielle avec ses 3 ou 4 transactions par seconde pour le monde entier. Or, sécuriser les documents d'une administration ou d'un gouvernement nécessite un grand nombre d'opérations; la question de la consommation énergétique se pose également. Restait enfin un choix-clé : blockchain publique ou privée ? En schématisant, la première nécessite un consensus tellement large au sein d'une communauté qui ne se connaît pas que cela devient très difficile à gérer pour un gouvernement. Une blockchain privée, quant à elle, n'est rien d'autre qu'un groupe de gens qui en fixe les règles, qui pourra décider de les changer et ainsi de modifier le passé.

« En analysant le marché, nous nous sommes tournés vers l'Estonie et l'entreprise Guardtime (voir encadré), qui a résolu ces problèmes de dualité publique-privée, explique Philippe Thévoz. Nous avons décidé de créer une joint-venture, car ils

disposent de cette « trust anchor ». Basée sur un système très différent de ceux sur lesquels s'appuient le Bitcoin ou d'autres protocoles, la Blockchain KSI® est indépendante, complète, et constitue un outil industriel très stable. »

Ingénieur formé à l'EPFL et actif dans le numérique depuis trente ans, Philippe Thévoz appartient au groupe Integrity Solutions, qui œuvre à garantir l'intégrité des données digitales. Par exemple en mettant un « time stamp » sur la blockchain d'un fichier, pour en garantir l'authenticité. « Mais cela ne suffit pas : l'intégrité de la donnée est parfaite, mais il faut également garantir l'intégrité du processus... ». En effet, certains pourraient « time stamper » sur la blockchain plusieurs versions de ce fichier et produire celui qui les arrange le moment venu. Cette sécurité serait ainsi contournée.

« De nouvelles missions critiques émergent. Il était donc tout naturel pour nous de les accompagner. »

SICPA innove sans cesse, et propose depuis peu la solution CERTUS™, qui permet à une entité de réaliser un certificat ou une attestation dont le contenu sera sécurisé par un QR code, lui-même sécurisé via la blockchain. La société l'a proposé ce printemps dans le cadre de la crise sanitaire du Covid-19 en créant des attestations sérologiques, qui certifient le résultat d'un test. Pour ses concepteurs, ce document infalsifiable, digital ou imprimé, permettra par exemple à un aéroport ou à une compagnie aérienne de laisser entrer des passagers testés récemment négatifs au virus. Le produit existe, et la firme était en contact en juin avec plusieurs pays pour définir les contours de son utilisation. La société lausannoise travaille également sur une nouvelle génération de signature et d'identité digitales sécurisées par blockchain, ainsi que sur des registres sécurisés de nouvelle génération, comme des dossiers médicaux. « L'idée sous-jacente, relève Philippe Thévoz, est la suivante : pour générer de la confiance, il faut que le titulaire puisse prouver les choses personnellement, indépendamment de toutes les autres personnes ou organisations. »

La cybersécurité constitue naturellement un paramètre incontournable dès lors que des opérations sont effectuées

sur internet, comme peuvent l'être celles de la blockchain. De ce point de vue, SICPA a misé sur le haut de gamme en s'alliant à Guardtime, qui a débuté ses activités dans le domaine de la sécurité numérique. « Le choix de cette blockchain particulière nous apporte ce qui se fait de mieux dans le domaine, en complément de l'état de l'art en matière de cybersécurité. »

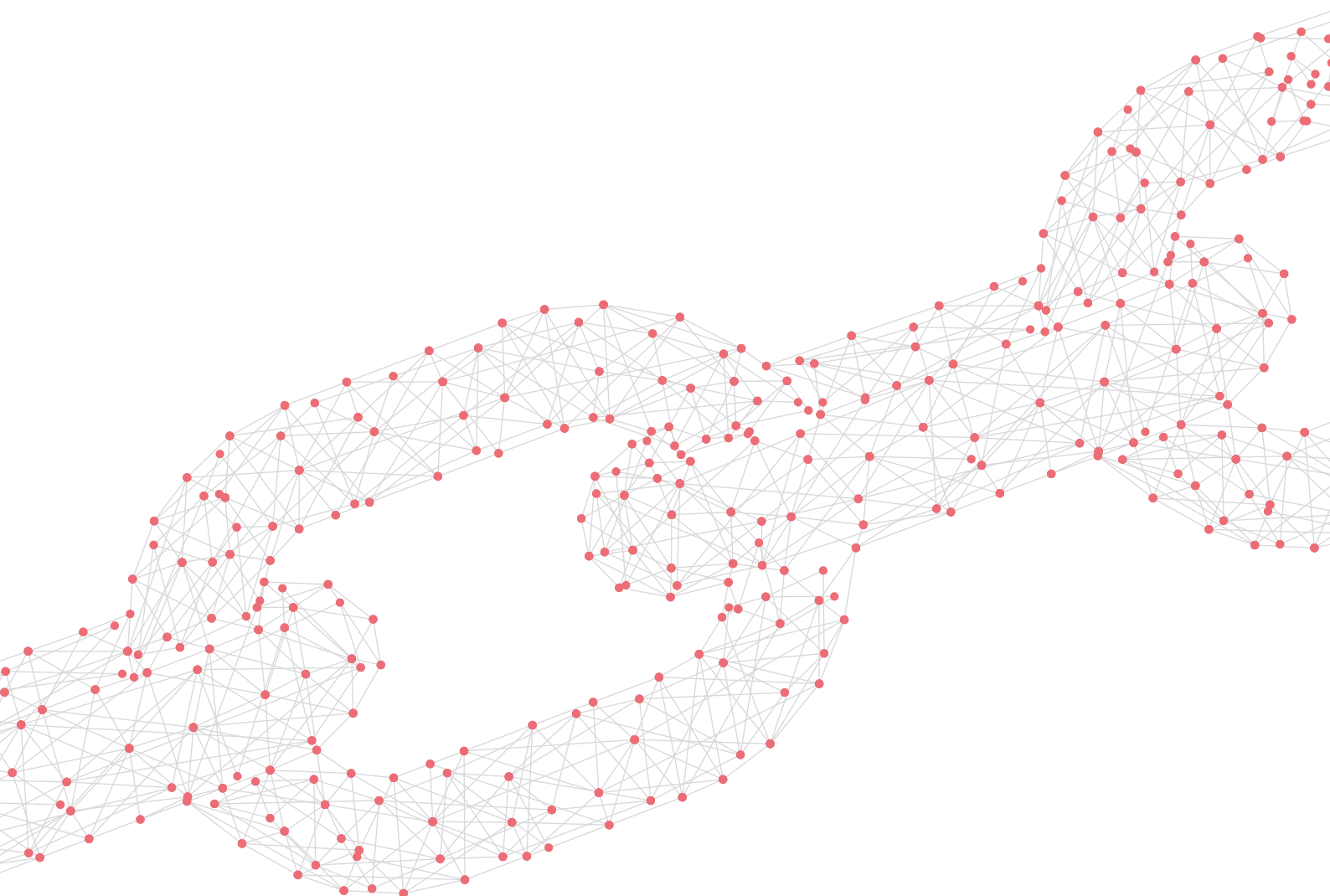
Propos recueillis par
Jean-François Krähenbühl

L'Estonie à la pointe

Fondée en 2007 en Estonie, à Tallinn, la société Guardtime a établi son siège mondial à Lausanne en 2019. Cette entreprise technologique est peu connue en dehors du cercle des initiés. L'Estonie est l'un des pays les plus à la pointe dans le domaine de la sécurité numérique. Le Centre d'excellence de cyberdéfense coopérative de l'OTAN est d'ailleurs installé à Tallinn.



Philippe Thévoz,
SICPA



9. Conservation de jetons

La question de la conservation de jetons est centrale dans le monde de la blockchain, en particulier dans le cas d'actifs numériques de valeur. La conservation de jetons consiste en la mise en œuvre de moyens technologiques et humains, ainsi que de mesures adéquates, afin d'assurer la garde et la restitution des jetons. Cette thématique revêt une grande importance aussi bien pour les détenteurs que pour les émetteurs de jetons.

9.1 La sécurité des clés privées au cœur du problème

Dans le cas d'un registre distribué, la conservation de jetons revient à garantir la sécurité et l'intégrité des clés privées contrôlant les adresses des portefeuilles (plus communément appelés « wallets ») sur lesquelles sont déposés les jetons. En effet, une sortie de fonds d'une adresse donnée requiert la signature de cette transaction par la clé privée y relative.

La sécurité des clés privées est particulièrement cruciale dans le cas des cryptomonnaies : toute personne qui a accès aux clés privées est en mesure de transférer ces cryptomonnaies de façon irréversible. De la même manière, une perte de clés privées entraîne l'impossibilité définitive de débloquent les cryptomonnaies concernées. Comme une cryptomonnaie est décentralisée par nature, il est impossible de se retourner vers une autorité centrale (dans le monde traditionnel - une entité émettant des cartes de débit ou de crédit) ou un acteur du réseau afin de demander une extourne ou la création d'une nouvelle clé privée donnant accès à l'adresse.

9.2 Plusieurs mesures de limitation des risques

Afin de limiter ces risques de vol ou de perte de fonds, il existe plusieurs techniques de sécurisation. Les principales sont les suivantes :

Une première approche est de mettre en place un mécanisme dit de multi-signatures, afin de valider les sorties de fonds. Autrement dit, le transfert d'un jeton nécessite la signature de la transaction correspondante par plusieurs clés privées, détenues par différentes entités (ou personnes), au lieu d'une seule. Le principal défi avec ce type de solutions est que la multi-signature n'est pas supportée de façon « native » par tous les protocoles blockchains. De plus, selon les cas de figure, un risque dit de « collusion » peut exister. D'ailleurs, il convient de noter que la multi-signature ne règle en rien le problème du stockage et de la protection des clés privées individuelles.

Une seconde technique classique de protection consiste à stocker les clés privées (et à effectuer la signature des transactions) dans un environnement et/ou sur un support sécurisé. Il peut s'agir d'un simple papier, d'un logiciel ou alors d'un support physique sécurisé (« *hardware wallet* ») qui ne permet pas de lire son contenu ni d'en extraire les données. Ces médias ne sont idéalement pas connectés à Internet ou au monde extérieur. Dans le jargon, on parle souvent de stockage « à froid » (« *cold wallet* ») pour désigner ce type de régime, par opposition au stockage dit « à chaud » (« *hot wallet* »).

Les solutions professionnelles de conservation de jetons, utilisées par exemple par les banques, font appel à des solutions de ce type. Elles stockent typiquement les clés privées dans des modules de sécurité matériel (*Hardware Security Module* ou *HSM*). Les *HSM* protègent l'infrastructure cryptographique de certaines des organisations les mieux sécurisées au monde en gérant, traitant et conservant de manière sécurisée les clés cryptographiques à l'intérieur d'un appareil renforcé inviolable.

Les meilleures solutions de conservations institutionnelles sont loin d'être de simples « machines à signer », puisqu'elles intègrent aujourd'hui des mécanismes de sécurité avancés, de gestion du risque, de redondance et de résistance aux défaillances, ainsi que des mécanismes de recouvrement en cas de désastre, même en cas de destruction totale des *HSMs* et des clés privées.

9.3 Actifs « tokenisés » : au-delà de la sécurité des clés privés

Comme indiqué, dans le cas d'une cryptomonnaie, la conservation se limite principalement à la garde des clés privées. Dans le cas de titres ou de valeurs mobilières « tokenisés » ayant un émetteur, telles que des actions ou de titres de dette, la conservation revêt une tout autre dimension. Il ne s'agit plus seulement d'assurer la garde des clés privées et la signature de simples « ordres de virement », mais surtout de pouvoir gérer les différents événements et actions liés à un titre tout au long de son cycle de vie, aussi bien du côté des émetteurs que du côté des investisseurs. En effet, tout comme pour un produit financier classique, des « opérations sur titres » (dividendes, split, etc.) peuvent se produire.

Dans le cas d'un actif tokenisé, il est intéressant de remarquer que la clé privée contrôlant le compte d'un émetteur

joue un rôle primordial. Cette clé permet à l'émetteur d'accéder à des fonctions à haut risque, comme par exemple de forcer le transfert, la confiscation ou la destruction de jetons. Du côté de l'investisseur, le principal défi est de s'équiper d'une solution qui va largement au-delà des aspects liés à la sécurité et la conservation. La solution utilisée doit permettre à l'investisseur d'exercer tous ses droits, comme par exemple participer à un vote des actionnaires.

Ces nouvelles solutions doivent pouvoir également gérer des événements propres à la technologie blockchain, comme par exemple les bifurcations (hard forks), qui peuvent selon les cas donner droit aux porteurs d'obtenir gratuitement un jeton « bis ». Elles doivent aussi permettre aux utilisateurs de bénéficier des avantages liés à la détention des jetons, comme par exemple le « *staking* ». En effet, sur les réseaux blockchain qui fonctionnent avec une méthode de consensus/validation de type « *proof of stake* », la seule détention de jetons permet de prétendre à des récompenses.

9.4 Besoin d'une infrastructure spécialisée

En conclusion, la conservation et la gestion professionnelle et sécurisée de jetons requiert une infrastructure spécialisée, ainsi que des compétences pointues, tant dans les domaines liés à la cyber-sécurité et la technologie que dans ceux liés à la finance et au cycle de vie des titres. Il est dès lors essentiel de s'équiper des bons outils et de collaborer avec les Fintechs qui maîtrisent les deux côtés de l'équation. La bonne nouvelle est qu'il existe aujourd'hui des solutions et des Fintechs de ce type.



Sébastien Dessimoz,
Taurus Group

Glossaire

Florian Ducommun – HDC

Actifs digitaux : valeurs patrimoniales prenant la forme de jetons numériques (tokens) enregistrés dans un registre distribué, typiquement une blockchain, comme par exemple des jetons de paiement, des jetons d'investissement ou des jetons de service.

Bifurcations (forks) : nouvelle blockchain répondant à d'autres règles de gouvernance créée sur la base d'un code source existant.

Blockchain : base de données distribuée et sécurisée dans laquelle sont stockées chronologiquement, sous forme de blocs liés les uns aux autres, les transactions successives effectuées entre ses utilisateurs depuis sa création. La blockchain est un cas d'application de la TRD.

Contrat intelligent (smart contract) : protocole informatique qui permet l'exécution d'un contrat et/ou le contrôle de transfert d'actifs numériques à certaines conditions.

Cryptomonnaie : monnaie émise par des personnes privées en faisant usage de la technologie des registres distribués. Les cryptomonnaies appartiennent à la catégorie des jetons de paiement.

Initial Coin Offering (ICO) : mode de financement s'apparentant au financement participatif consistant à émettre des jetons en faisant usage de la TRD et à les vendre à des investisseurs à un prix initial payé soit en monnaie fiduciaire, soit en cryptomonnaie.

Initial Exchange Offering (IEO) : mode de financement assimilable à une ICO, mais réalisé par le biais d'une plateforme d'échange.

Jeton (token) : entrée dans un registre distribué créé par un contrat intelligent et sécurisée par des méthodes cryptographiques.

Jeton d'investissement : jeton incorporant une valeur assimilée à un instrument financier ou à une valeur mobilière (comme, par exemple, un titre de participation ou de dette).

Jeton de paiement : jeton dont le but est de servir de moyen de paiement ou qui est utilisé comme moyen de paiement.

Jeton de service : jeton donnant accès à une prestation ou à un service.

Jeton stable (stable coin) : catégorie de jeton de paiement adossé à un ou des actif(s) sous-jacent(s).

Know your customer (KYC) : processus permettant de vérifier l'identité des investisseurs d'une société émettrice de jetons. Le terme est également utilisé pour faire référence aux lois anti-blanchiment.

Oracle : entité de confiance faisant partie d'un réseau informatique, transportant des informations du monde physique à un contrat intelligent¹⁵.

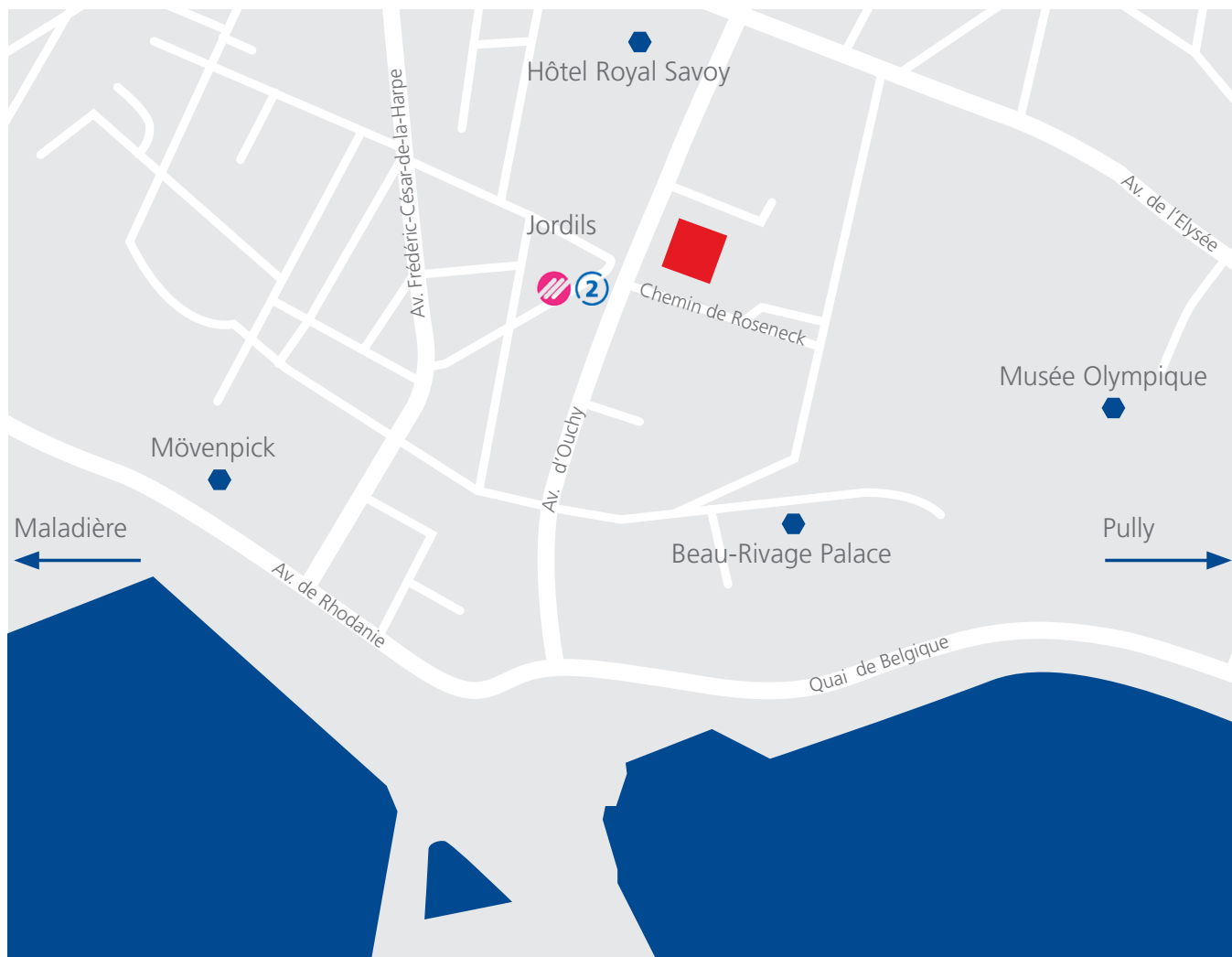
Portefeuille chaud (« Hot wallet ») : dispositif de stockage d'actifs digitaux faisant usage d'un programme informatique connecté à Internet.

Portefeuille froid (« Cold Wallet ») : dispositif de stockage d'actifs digitaux faisant usage de matériel informatique non connecté à Internet.

Security Token Offering (STO) : émission de jetons d'investissement.

Technologie des registres distribués (TRD) : système permettant la tenue, l'enregistrement, la distribution et la synchronisation d'un registre sur un réseau d'ordinateurs. Le registre évolue par l'addition d'informations ou de transactions validées par le réseau d'ordinateurs sur la base d'un algorithme de consensus. Un registre distribué n'a ni administrateur central ni centralisé.

15. Vanessa RABESANDRATANA, « L'Oracle hardware : la couche de confiance entre les blockchains et le monde physique », Réalités Industrielles, août 2017



Contact

Chambre vaudoise du commerce et de l'industrie

Av. d'Ouchy 47
1006 Lausanne
T. +41 (0)21 613 35 35
F. +41 (0)21 613 35 05
cvci@cvci.ch

Horaires d'ouverture

Lundi au vendredi
07 h 45 – 12 h 00
13 h 30 – 17 h 00

Transports publics

M2 ou bus TL n°2
Maladière-Désert:
Arrêt Jordils