- Pourquoi Cardano ? -

1. Introduction

1.1 Motivations

Démarré en 2015, le projet Cardano a pour objectif d'améliorer la manière dont sont conçues et développées les monnaies virtuelles ou "cryptomonnaies". En plus des avancées techniques qui jalonnent sa création, le but de Cardano est de créer un écosystème équilibré et durable prenant aussi bien en compte les besoins de ses utilisateurs que les besoins des systèmes financiers préexistants.

A l'instar de nombreux projets dits en licence libre (''Open Source''), Cardano débuta sans feuille de route établie ni plan d'action figé. Ce projet possède toutefois un cap, dicté notamment par la rigueur et les bonnes pratiques d'ingénierie dans sa mise en œuvre - sans exclure pour autant toute dimension exploratoire. Ceci inclut :

- Une claire séparation entre le maintien du registre distribué (ou livre de compte) et les contrats intelligents manipulant les valeurs sur celui-ci (''Smart Contracts'')
- Un code informatique central développé de façon modulaire et écrit en langage fonctionnel[1]
- Un groupe restreint de chercheurs et d'ingénieurs en informatique suivant les standards définis par la recherche académique, en particulier la revue par les pairs
- Un cycle court entre articles de recherche, mises en œuvre et nouvelles recherches visant à corriger les erreurs éventuelles découvertes durant la revue par les pairs
- La capacité de mettre à jour un système déployé et opérationnel sans détruire le réseau
- La création d'un système décentralisé permettant le financement d'améliorations et modifications futures
- Une conception permettant d'envisager à long-terme son utilisation sur appareils mobiles (''Smartphones''), et ce avec un degré raisonnable de sécurité pour l'utilisateur
- Favoriser l'implication des parties prenantes dans le fonctionnement et la maintenance du système
- Tenir compte du besoin de manipuler plusieurs cryptomonnaies/devises au sein d'un même registre.
- Permettre aux transactions d'inclure de manière optionnelle une gamme de données associées aussi appelées métadonnées afin de pouvoir se conformer aux besoins des cadres législatifs et systèmes bancaires préexistants
- Apprendre des erreurs et des succès des plus de 1000 cryptomonnaies déjà créées
- Mettre en place et suivre des standards, si possible gérés par le biais d'une fondation fixant les choix finaux comme a pu le faire l'Internet Engineering Task Force (I.E.T.F.)
- Explorer la dimension sociale du commerce et des échanges
- Trouver un point d'équilibre satisfaisant pour les régulateurs sans compromettre certains principes fondateurs hérités de Bitcoin.

[1] Ndtr : par opposition aux langages impératifs

C’est en suivant ces principes et ces idées que les ingénieurs et chercheurs commencèrent par faire une revue de la littérature relative aux cryptomonnaies, avant de créer un ensemble d’outils et d’abstractions leur permettant de mieux appréhender leur travail. Les résultats de ces recherches ont fait l’objet de nombreux articles académiques co-signés par I.O.H.K. (Input Output Hong Kong), de revues d’état de l’art (‘’Scripting Language Overview’’, ‘’Ontology of Smart Contracts’’) ou encore le développement du projet Scorex. Il en ressort une meilleure compréhension du monde des cryptomonnaies, autrement difficile à appréhender de par sa croissance exceptionnelle et parfois contre-productive.

Contrairement aux protocoles éprouvés tels que TCP/IP (‘’Transmission Control Protocol / Internet Protocol’’), il n’existe que peu de cryptomonnaies conçues de manière similaire, c.a.d. en couches ou “layers”. La construction d’un consensus autour d'événements enregistrés sur un seul et unique registre distribué semble être un principe respecté par nombre de concepteurs de cryptomonnaies, sans pour autant en questionner la pertinence.

Par exemple, en voulant devenir un ordinateur mondial universel, Ethereum est devenu extrêmement complexe. Malgré tout, ce dernier continue de souffrir de problèmes triviaux pouvant à terme détruire sa capacité à opérer comme système de transfert et/ou de stockage de valeurs. Doit-on par exemple toujours attribuer le même degré d’importance à tous les codes informatiques - ce que Ethereum fait -, indépendamment de leur valeur intrinsèque, de leurs coûts de maintenance, ou des conséquences qu’ils engendrent en terme de régulation financière ?

Aussi, et de façon assez surprenante, ce champ d’application fait assez peu usage des nombreuses recherches faites par les cryptologues. Par exemple, le protocole dit de preuve d’enjeu déléguée mis en place par Bitshares aurait facilement pu bénéficier d’un outil dédié à la création de nombres aléatoires et connu depuis les années 1980s (Rabin and Ben-Or).

Enfin, il est à noter que la plupart des cryptomonnaies - à l’exception notable de Tezos - n’ont rien prévu en ce qui concerne leur mise à jour et donc leur pérennité. La capacité à évoluer, que cela soit sous la forme de changements subtils (‘’soft forks’’) ou plus radicaux (‘’hard forks’’), est néanmoins cruciale pour le succès à long-terme d’une cryptomonnaie.

Une des conséquences évidentes de ce manque de vision à long terme est que de nombreux acteurs économiques, tels que les entreprises, ne peuvent pas engager plusieurs millions de dollars dans des protocoles au mieux éphémères, sinon douteux. Afin de pouvoir faire évoluer un protocole, il est donc impératif qu’un consensus social puisse émerger ; pour atteindre ce dernier, un processus efficace est alors crucial, sans quoi la fragmentation des acteurs et l’arrêt du protocole sont certains.

Pour terminer, il est important de noter que la monnaie est un phénomène social. Dans leur recherche continue d’anonymat et de désintermédiation des acteurs économiques centraux, Bitcoin (la première cryptomonnaie) et ses semblables se sont débarrassés par la même occasion de besoins essentiels dans le jeu des transactions économiques tels que celui d’une identité stable, de la présence de métadonnées ou de la réputation des acteurs impliqués. Ajouter ces manques a posteriori par une autorité centrale éliminerait tout l’intérêt de la technologie Blockchain et ses propriétés fondamentales : la capacité d’audit, l’accessibilité à tous et l’immutabilité.

Les systèmes financiers actuels comme SWIFT, FIX et ACH, sont riches en métadonnées. Pour eux, il n'est pas suffisant d'avoir uniquement accès au montant d'une transaction entre parties. Pour satisfaire les organismes régulateurs, ces systèmes se doivent de connaître les acteurs à l'origine des transactions, savoir si ces derniers se conforment à la loi en vigueur, s'il existe des mouvement suspects ou frauduleux, etc … Ces métadonnées peuvent parfois être plus importantes que les transactions *sensu stricto*.

Il en résulte que la manipulation de ces métadonnées est tout aussi dommageable que la création de fausse monnaie ou la réécriture frauduleuse de l'historique des transactions. Refuser toute participation au protocole à un acteur désireux de faire état de ces métadonnées serait contre-productif puisque cela s'opposerait à la protection des consommateurs et constituerait un frein à une large adoption de cette technologie.

1.2 La Fin du Voyage

Une exploration rigoureuse du monde des cryptomonnaies a aidé à la création de deux groupes de protocoles. Le premier, appelé ''Cardano Settlement Layer'' (CSL), constitue un protocole à preuve d'enjeu (''Proof of Stake'' ou PoS) dont la sécurité a été démontrée. Le second groupe forme le ''Cardano Computational Layer'' (CCL) ou couches des opérations de calculs.

Durant la conception de Cardano, nous avons gardé à l'esprit la dimension sociale des cryptomonnaies. Nous l'avons ainsi construit en séparant d'un côté la tenue du registre et de l'autre les calculs complexes qui s'y réfèrent. Nous avons aussi pensé aux besoins des régulateurs tout en respectant au mieux les principes d'immutabilité propres à la technologie blockchain. De plus, et quand cela semblait indiqué, nous avons soumis nos protocoles à la revue par nos pairs et vérifié la justesse de notre code en le soumettant à des techniques de vérification formelle.

1.2.1 Preuve d'enjeu

La possibilité d'utiliser un protocole de preuve d'enjeu pour maintenir un registre distribué est toujours sujet à controverses parmi les concepteurs de cryptomonnaies. Cependant, parce que ce type de protocole permet l'addition d'un système de vote, peut croître plus facilement et permet une plus grande liberté dans la création d'incitations monétaires à l'attention des participants, nous n'avons pas hésité longtemps à choisir.

Notre protocole à preuve d'enjeu se nomme Ouroboros et a été conçu par une équipe de cryptologues issus de cinq universités et dirigés par le Prof. Aggelos Kiayias de l'Université d'Edinburgh. En plus d'être sûr d'utilisation, sa principale innovation réside dans sa conception modulaire permettant l'ajout de nouvelles fonctionnalités au cours du temps. Cette modularité nous permet de lui ajouter plusieurs fonctions telles que la délégation, le maintien de registres distribués parallèles, les points de contrôle, des clients légers, la production de nombre aléatoires par différentes méthodes ou de prendre en compte différentes hypothèses quant à l'état de synchronie du réseau.

De plus, le niveau de charge d'un réseau passant de quelques milliers à plusieurs millions ou milliards d'utilisateurs au cours du temps fera nécessairement appel à une évolution dans la manière dont le protocole doit fonctionner. Pour s'accommoder de tels changements, il est vital de pouvoir faire évoluer le protocole de façon flexible et donc de le concevoir à l'épreuve du temps.

1.2.2 Les éléments sociaux de l'argent

Les cryptomonnaies sont un bon exemple pour prendre mesure de la dimension sociale de l'argent. Sur les aspects technologiques, il n'existe au fond que peu de différences entre Bitcoin et Litecoin, et encore moins entre Ethereum et Ethereum Classic. Pourtant, Litecoin et Ethereum Classic maintiennent tous les deux une capitalisation boursière solide et conséquente, des communautés actives et leur propre mandat social.

Il peut alors être proposé qu'une grande partie de la valeur intrinsèque d'une cryptomonnaie est issue (i) de la communauté d'acteurs qui l'entretient, (ii) de la manière dont ces acteurs l'utilisent et (iii) de leur niveau d'implication quant aux décisions relatives à son évolution. Certaines cryptomonnaies, comme Dash par exemple, possèdent au cœur même de leur protocole un système intégré leur permettant de faire voter leurs utilisateurs sur le choix des développements prioritaires à financer.

La grande diversité elle-même des cryptomonnaies témoigne de leur dimension sociale. Les divergences philosophiques, de politique monétaire ou les conflits entre concepteurs sont la source des multiples fragmentations observées au sein de cette industrie. A la différence des cryptomonnaies, les monnaies traditionnelles adossées aux superpuissances étatiques (*fiat*) peuvent, elles, survivre à l'effet de forces semblables.

Il apparaît dès lors que certains éléments propres aux monnaies *fiat* font défaut à l'écosystème naissant des cryptomonnaies. Nous supportons l'idée - instillée dans la feuille de route de Cardano - que les utilisateurs d'un protocole doivent être incités à (i) comprendre le contrat social sur lequel repose leur protocole et à (ii) proposer des changements de manière productive. Tous les aspects du système d'échange de valeurs seront concernés, que cela soit la manière dont les marchés doivent être régulés jusqu'aux projets à financer. Cependant, l'exercice de cette liberté ne devra pas être contrôlé par le biais d'acteurs centralisés ni exiger des titres de compétences particuliers, au risque alors d'être coopté par une riche minorité.

Pour répondre aux besoins de ses utilisateurs, Cardano sera construit en une superposition de protocoles empilés sur CSL.

Il est important de réaliser que, indépendamment du succès d'une levée de fonds nécessaire au développement d'une cryptomonnaie, ce fond initial est voué à disparaître. C'est pourquoi Cardano inclura aussi un Trust décentralisé (Trésor), financé par une inflation monotone décroissante et les frais de transaction.

Grâce à un système de vote, n'importe quel utilisateur pourra être en capacité de faire appel à un financement issu de ce Trésor. Les autres parties prenantes ou "stakeholders" voteront alors pour désigner le ou les bénéficiaires. En permettant des débats argumentés sur les projets qui devraient ou

ne devraient pas percevoir de financement, ce fonctionnement produit un cercle vertueux. Cela est déjà observable chez certaines cryptomonnaies possédant un mécanisme de trésorerie similaire, comme Dash. En effet, les discussions relatives au financement de projets imposent une perspective entre court et long terme, forment le contrat social de la cryptomonnaie, organisent les priorités et forgent la croyance en la création de valeur apportée par les projets débattus. Cet échange signifie aussi que la communauté d'utilisateurs évalue de façon répétée les options présentes sur la table.

Notre espoir est de faire en sorte que Cardano possède un système formalisé de vote permettant de s'exprimer sur des changements de type ''soft-forks'' ou ''hard-forks'', le tout enregistré sur la blockchain. Comme l'ont démontré Bitcoin et son débat sur la taille des blocs ou Ethereum et sa modification du DAO, les cryptomonnaies peuvent être le centre de débats interminables et non résolus sur le bien-fondé de certains choix techniques et moraux. Il peut et il doit être opposé à cela que ces problèmes, et l'éclatement des communautés lorsqu'enfin une décision est prise, sont le résultat direct d'un manque de formalisation et d'organisation des débats autour de ces sujets.

A qui doit-on s'adresser lorsqu'il s'agit de convaincre les utilisateurs de Bitcoin d'adopter un nouveau standard ? Comment les développeurs de Ethereum peuvent-ils précisément mesurer l'assentiment de leur base d'utilisateurs quant au choix du renflouement consécutif au piratage du DAO ? Si la communauté des utilisateurs se fracture, peut-on encore réparer la cryptomonnaie ?

Dans le pire des cas, l'autorité morale d'agir pourrait simplement incomber à quiconque contrôle les développeurs, les infrastructures et l'argent, et non au souhait de la majorité des utilisateurs. De plus, comment s'assurer de la légitimité d'une décision si la majorité des utilisateurs est inaccessible ou simplement désengagée par défaut d'incitations ?

Certaines propositions, comme celle faite par la cryptomonnaie Tezos, sont un modèle intéressant pour évaluer dans quelle mesure un protocole de cryptomonnaie peut être traité comme une constitution, ici en trois parties (Transaction, Consensus et Réseau) et possédant un ensemble de règles formelles et un processus de révision constitutionnelle. Toutefois, beaucoup de travail de formalisation reste à faire, surtout en ce qui concerne les mécanismes d'incitations des utilisateurs et la manière de procéder pour modifier une cryptomonnaie. L'utilisation de méthodes formelles, de spécifications conçues pour les machines et d'une trésorerie couvrant les aspects incitatifs pour les utilisateurs sont des directions de recherche actuellement en cours d'exploration.

A défaut de pouvoir faire mieux, la capacité de pouvoir proposer un changement de manière transparente, libre de toute censure et dont le vote se déroulera sur la blockchain sont autant de moyens qui ne peuvent qu'améliorer ce processus dans son ensemble.

1.2.3 La couche de règlement de Cardano

Lorsqu'il s'agit de concevoir de bons protocoles et langages, les expériences passées peuvent se révéler d'une grande aide. Tout comme l'exemple des standards ''Open Systems Interconnection'', l'histoire des technologies regorge d'idées excellentes sur le papier mais qui n'ont malheureusement pas survécu. Cette même histoire possède aussi d'heureux accidents tels que le protocole TCP/IP ou le langage JavaScript.

Quelques principes extraits de cette histoire sont les suivants :

- Concevoir en prévoyant de la place pour manœuvrer
- La complexité est séduisante sur le papier mais la simplicité l'emporte presque toujours
- Trop de monde en cuisine gâche le potage
- Optimal ou non, un standard fixé est là pour rester
- Avec de la bonne volonté, les mauvaises idées peuvent devenir bonnes

Cardano est un système financier qui accepte sa nature sociale. Il y aura un besoin énorme de flexibilité et de capacité à résoudre des problèmes complexes propres à chaque utilisateur et à leurs transactions. En cas de succès, il faudra tout autant de capacités de calcul informatique, de stockage et de bande passante pour absorber des millions de transactions simultanées.

Pourtant, il n'existe aucun ''Robin des Bois'' décentralisé prêt à prendre aux riches centres informatiques pour donner aux plus pauvres dans le but de créer un réseau plus juste. De la même manière, nous n'avons pas le luxe de pouvoir compter sur la bienfaisance naturelle et l'altruisme des hommes pour le bien de notre réseau.

C'est pour cela que Cardano emprunte au protocole TCP/IP le concept de séparation des problèmes[2].

Les blockchains ne sont au final que des bases de données, enregistrant les évènements avec une garantie d'horodatage et d'immutabilité. Dans le contexte monétaire, elles garantissent la propriété des biens. Y-adjoindre des calculs complexes par des programmes informatiques constituent un problème totalement indépendant.

Voulons-nous savoir combien Alice a transféré à Bob, ou voulons nous être plus impliqués que cela et aussi connaître la raison qui pousse Alice à payer Bob avant d'en calculer le montant ?

Comme Ethereum a pu le faire, il est extrêmement tentant d'opter pour le deuxième scénario. Ce dernier semble en effet plus flexible. Il viole pourtant les principes de conception évoqués plus haut. Reconstruire tout le scénario de la transaction veut dire que le protocole doit être capable de comprendre le sens d'évènements arbitraires, les traduire en transactions, prendre une décision en cas de fraude et rembourser l'une des parties si de nouvelles informations sont disponibles. Des choix de conception difficiles sont alors à prendre. Quelles métadonnées doivent être stockées pour chaque transaction ? Quels éléments de contexte d'une transaction sont pertinents et pour combien de temps ? Quand pourra-t-on se débarrasser de ces données ? S'en débarrasser viole-t-il la législation dans certains pays ?

De plus, certains calculs informatiques sont secrets par nature. Par exemple, il serait malvenu que les étapes du calcul du salaire moyen au sein d'une entreprise soient connues de tous, révélant alors le salaire de chacun à tout le monde. Et si ce type de calculs étaient connus de tous, n'existe-t-il pas un risque de les biaiser et ainsi d'en modifier les résultats ?

[2] Ndtr: "concerns", problèmes dans le sens de préoccupation

Pour ces raisons, notre position est de dire que l'enregistrement des transactions - la tenue des comptes dans le registre - doit être séparée des contextes et raisons d'être de ces mêmes transactions. En d'autres termes, la séparation stricte entre valeur et méthode de calcul. Cette séparation n'implique pas pour autant de Cardano qu'il ne permettra pas l'exécution de contrats intelligents. Bien au contraire car faire clairement la distinction permet beaucoup plus de flexibilité dans les choix de conception, d'utilisation, d'anonymat et d'exécution de ces contrats.

Notre registre des valeurs se nomme Cardano Settlement Layer (CSL). Puisque sa raison d'être est d'enregistrer les mouvements de valeurs, sa feuille de route est constituée des éléments suivants :

- Utiliser deux langages de script, un pour le mouvement de valeur sensu stricto et un autre pour faciliter l'incorporation de couches supplémentaires
- Utiliser les chaînes greffées KMZ pour lier d'autres registres/livres de compte distribués
- Utiliser plusieurs types de signatures cryptologiques, dont certaines résistantes aux ordinateurs quantiques pour plus de sécurité
- Utiliser plusieurs devises (cryptomonnaies)
- Atteindre une réelle capacité de croissance, en ce sens que l'augmentation du nombre d'utilisateurs sera suivie d'une augmentation des ressources informatiques

1.2.3a Langage de script

Les transactions entre adresses au sein du registre ont besoin d'une forme de langage particulier pour s'exécuter correctement et être valides : c'est le langage de script. Personne ne souhaite qu'un inconnu accède à ses comptes, ni qu'un langage mal conçu permette d'effectuer des transactions vers un compte inactif où les fonds seront irrémédiablement perdus.

Les systèmes comme Bitcoin ont un langage de script extrêmement rigide et draconien, de telle sorte qu'il est très difficile d'y effectuer des transactions sur-mesure, voire même de les lire ou les comprendre. De l'autre côté du spectre, les langages programmables comme Solidity introduisent une complexité extraordinaire dans le système et ces langages ne sont au final utiles qu'à une minorité de personne. C'est pourquoi nous avons choisi de concevoir un langage *de novo* appelé Simon, en hommage à son créateur Simon Thompson et à la personne l'ayant inspiré, Simon Peyton Jones. Simon est un langage de domaine spécifique basé sur "Composing contracts: an adventure in financial engineering".

L'idée directrice est que les transactions financières sont généralement composées d'éléments fondamentaux simples. De la même manière que les éléments de la table périodique[3] permettent la création d'une infinité de molécules, l'assemblage d'élément financiers fondamentaux permet, sans programmabilité générale, la création d'une grande diversité de transactions couvrant la majorité sinon la totalité des transactions. Le premier avantage de ce langage est que sa sécurité et son exécution sont très bien compris. Des preuves de sa justesse de fonctionnement peuvent être dérivées et un large éventail de transactions problématiques peut être testée. Cela permet d'éviter de nombreux bugs

[3] Ndtr : Chimie – La Table périodique des éléments établie par Mendeleïev classe tous les atomes connus.

comme la création de nouvelle monnaie ou le bug de la malléabilité des transactions rencontré par Bitcoin dans le passé. Le second avantage est qu'il est possible de lui ajouter des extensions par le biais de ''soft-forks'' si le besoin de nouvelles fonctionnalités se fait sentir.

Enfin, il existera toujours le besoin de connecter le CSL à d'autre protocoles superposés, qu'il s'agisse du système financier actuel ou de services particuliers. Pour répondre à ces besoins spécifiques, nous avons développé le langage Plutus. Plutus est à la fois un langage généraliste permettant l'écriture de contrats intelligents et un langage de domaine spécifique dédié à l'interopérabilité entre cryptomonnaies. Plutus est un langage fonctionnel[4] typé issu du langage Haskell et qui peut être utilisé pour l'écriture de scripts de transactions sur-mesure. Pour ce qui est du CSL, Plutus sera utilisé pour gérer les transactions complexes nécessitant par exemple de se connecter à des chaînes greffées.

1.2.3b Chaînes greffées

Pour ce qui concerne les chaînes greffées, Cardano utilisera un nouveau protocole développé par Kiayias, Miller and Zindros (KMZ). Ce protocole KMZ est basé sur leurs travaux antérieurs décrivant le principe des "preuves de preuve de travail" ou "NiPoPoW". Le principe de fonctionnement de ce protocole ne fera pas l'objet d'une description plus poussée ici ; le minimum à savoir est que le concept développé par KMZ assure le mouvement de fonds de manière sûre et non interactive entre le CSL et n'importe quel CCL ou même une autre blockchain capable de l'utiliser.

Les chaînes greffées KMZ sont un élément indispensable à l'établissement d'une architecture plus complexe du système. Qu'il s'agisse des registres soumis à une régulation particulière, les opérations privées, les langages de script robustes ou tout autre besoin spécifique, ils sont tous des boîtes noires pour le CSL. Toutefois, cette façon de fonctionner donnera des garanties quant à la traçabilité des opérations et la possibilité d'annuler des transactions une fois le calcul initial terminé.

1.2.3c Signatures

Pour qu'Alice puisse effectuer un transfert de fonds à Bob, cette dernière doit prouver qu'elle a l'autorisation de le faire. Le moyen le plus direct et fiable d'accomplir cela est d'utiliser un schéma employant une clé publique couplée à une clé privée. Dans un tel schéma, les fonds sont connectés à une clé publique dont Alice possède l'unique clé privée associée.

Il existe des centaines de schémas possibles possédant tous des couples [hypothèses - paramètres de sécurité] différents. Certains dépendent de problèmes mathématiques issus des courbes elliptiques quand d'autres utilisent des concepts plus exotiques.

Dans tous les cas, le principe reste le même : résoudre un problème mathématique extrêmement difficile, voire impossible, à moins de disposer d'une donnée secrète. La personne en mesure de résoudre le problème est alors reconnue comme l'authentique propriétaire de la donnée secrète, ici la clé privée.

[4] Ndtr : cf. opposition langage impératif vs. fonctionnel

Le choix d'un schéma de signature cryptologique pour une cryptomonnaie pose deux types de problème.

Le premier est la sécurité à long terme du schéma lui-même. Certains schémas utilisés dans les années 1970s et 1980s, comme le DES, ont depuis été cassés. Il est donc important de s'accorder sur la durée de la période durant laquelle un schéma sera considéré comme sûr.

Le second problème est constitué par le fait que beaucoup d'entreprises, de gouvernements et autres institutions ont préféré imposer l'utilisation d'un schéma cryptologique en particulier. Par exemple, la NSA[5] maintient l'ensemble d'outils appelé Suite B. Il existe aussi des standards issus de la norme ISO ou de groupes de travail du consortium W3C sur la cryptologie. Si une cryptomonnaie fixe l'utilisation d'un seul schéma cryptologique, elle accepte alors que ce schéma pourra être cassé un jour. Dans ce cas, il existe au moins une entité (entreprise ou gouvernement) qui n'acceptera pas d'utiliser cette cryptomonnaie pour des raisons légales ou industrielles. D'un autre côté, une cryptomonnaie ne peut pas non plus utiliser tous les schémas cryptologiques disponibles puisque cela impliquerait que chaque utilisateur soit aussi en mesure de le faire avec son logiciel client.

En ce qui concerne Cardano, nous avons décidé de commencer en utilisant un protocole cryptologique basé sur les courbes elliptiques, en particulier avec le schéma Ed25519. Nous avons aussi décidé d'améliorer les bibliothèques existantes en rendant possible l'utilisation d'un porte-clés dit déterministe hiérarchique (HD) faisant appel aux spécifications des Dr Dmitry Khovratovich and Jason Law.

Cardano utilisera aussi d'autres schémas. En particulier, nous sommes intéressés par l'utilisation de BLISS-B afin de rendre notre schéma de signatures résistant aux capacités de calcul des ordinateurs quantiques[6]. Nous sommes aussi intéressés par l'ajout du schéma SECP256k1 afin d'améliorer l'interopérabilité avec les protocoles déjà en place comme Bitcoin.

Cardano a été conçu de telle manière qu'il nous sera possible d'ajouter plusieurs nouveaux schémas de signature par des mises à jours de type ''soft-fork''. Ils seront ajoutés lors de mises à jour planifiées, quand cela sera nécessaire.

1.2.3d Actifs émis par les utilisateurs (UIAs)

Très tôt dans l'histoire de Bitcoin, plusieurs protocoles ont rapidement été développés afin de permettre aux utilisateurs d'émettre des actifs sur le système comptable de Bitcoin et ainsi de suivre plusieurs devises simultanément. Ces protocoles n'étaient pas utilisés nativement par le protocole Bitcoin mais plutôt mis en œuvre de façon astucieuse.

Dans les cas de ColoredCoins et Mastercoin (aujourd'hui Omni), deux cryptomonnaies superposées au protocole Bitcoin, les clients légers sont obligés de compter sur des serveurs de confiance. De plus, les frais de transactions doivent être payés en Bitcoin. Ces deux propriétés, combinées avec un canal

[5] Ndtr : Agence Nationale de Sécurité Nord-Américaine
[6] Ndtr: Sans commune mesure à celles des architectures classiques utilisés aujourd'hui

unique d'approbation des transactions, rendent Bitcoin peu optimal pour effectuer ce type de comptabilité multi-actifs.

La norme ERC20 utilisée dans le cas de Ethereum rend ce dernier plus riche en fonctionnalités. La devise native, ici l'Ether, est cependant toujours requise pour le paiement des frais de transactions. De plus, le réseau Ethereum a du mal à répondre aux besoins de tous les actifs (ou jetons) de type ERC20 émis.

Le problème fondamental peut être divisé en trois parties: les ressources, les incitations et les préoccupations. En ce qui concerne les ressources, l'ajout d'une monnaie nouvelle au même registre signifie que ce dernier possède deux UTXO[7] indépendants et devant partager la même bande passante, la même quantité de mémoire temporaire, et le même espace au sein des blocs. Les nœuds de consensus, responsables de l'inclusion de ces transactions en monnaie nouvelle dans les blocs, ont besoin d'être incités à le faire. Il n'est pas évident que tous les utilisateurs (ou nœuds de consensus) le feront ou bien se soucieront d'une monnaie en particulier.

Etant donné ces problèmes, être la monnaie principale d'un système multi-actifs représente un énorme avantage en ce sens que cela permet de servir de passerelle permettant la création de marchés décentralisés. Des actifs spéciaux pourraient être émis de manière à offrir des fonctionnalités particulières comme une monnaie stable (ex. Tether ou MakerDAO), bien utiles lorsqu'il s'agit de dénommer des demandes de prêts et remises.

C'est avec ces difficultés en tête que Cardano a décidé d'adopter une approche pragmatique en ce qui concerne la comptabilité multi-actifs. Il faut avant toute chose concevoir l'infrastructure nécessaire permettant l'utilisation de milliers de ces actifs différents. En particulier, les avancées suivantes sont requises :

- Des structures de données authentifiées à usage spécial pour permettre le suivi d'une très grande comptabilité de type UTXO
- Posséder une mémoire temporaire partagée pouvant recevoir une grande quantité de transactions en attente de validation
- Partitionner et établir des points de contrôle de manière pouvoir exploiter un très gros registre
- Des incitations à l'attention des nœuds de consensus pour qu'ils aient un intérêt à inclure différents types de transactions
- Une méthode d'enregistrement permettant aux utilisateurs de décider quelles monnaies ils désirent suivre et utiliser
- Des garanties fortes que la sécurité de ces actifs est aussi bonne que celle de la monnaie native
- Soutenir la création de marchés décentralisés pour améliorer la liquidité entre ces actifs et la monnaie native

Nos efforts préliminaires de recherche d'une structure de donnée authentifiée ont abouti au nouveau type AVL+ Tree, développé conjointement par Leo Reyzin, I.O.H.K. et Waves. Des recherches

[7] Ndtr : Unspent Transaction Output : système de comptabilité particulier

supplémentaires sont nécessaires mais il s'agit là d'une avancée fondamentale qui sera présente dans les versions futures de Cardano.

Une mémoire temporaire partagée (distributed mempool) peut être développée en utilisant le protocole RAMCloud de l'Université de Stanford. Nous commencerons nos essais au début de l'année 2017 pour étudier de quelle manière il pourra s'intégrer au protocole de consensus de Cardano.

Les points restants sont interconnectés et nos recherches les concernant sont actuellement en cours. Nous espérons - en fonction des résultats de nos recherches - inclure un protocole de gestion des actifs émis par les utilisateurs lors de la prochaine étape de développement de Cardano appelée Basho et prévue en 2018.

1.2.3e Évolutivité

Les systèmes distribués sont composés d'un ensemble d'ordinateurs (nœuds) acceptant d'exécuter un protocole ou une suite de protocoles pour atteindre un objectif commun. Cet objectif peut être le partage d'un fichier, tel que défini par le protocole BitTorrent, ou les calculs de repliement d'une protéine à l'aide du logiciel distribué Folding@Home[8].

Les protocoles les plus efficaces gagnent des ressources à mesure que des nœuds rejoignent le réseau. Par exemple, un fichier hébergé par BitTorrent peut être téléchargé beaucoup plus rapidement si de nombreux utilisateurs se l'échangent simultanément. La vitesse augmente car les utilisateurs fournissent des ressources en même temps qu'ils en consomment. Cette caractéristique constitue l'évolutivité d'un système distribué.

Le défi avec la conception des cryptomonnaies actuelles est que ces dernières ne sont pas pensées pour être évolutives. Les blockchains étant généralement une liste de blocs ajoutés les uns à la suite des autres, la sécurité d'un tel protocole repose alors sur le fait que chacun des nœuds possède une copie complète de la liste de blocs. Ainsi, un seul octet de données doit être dupliqué autant de fois qu'il existe de nœuds. Les nœuds supplémentaires ne fournissent aucune ressource supplémentaire.

Il en va de même pour le traitement des transactions et la diffusion des messages dans tout le système. L'ajout de nœuds supplémentaires au système de consensus ne fournit pas de puissance supplémentaire pour le traitement des transactions. Cela signifie juste que plus de ressources doivent être dépensées pour faire exactement le même travail. Aussi, plus de relais-réseau signifie simplement que plus de nœuds doivent transmettre les mêmes messages afin que l'ensemble du réseau reste synchronisé sur le bloc le plus récent.

Avec une telle topologie, les cryptomonnaies ne pourront certainement pas devenir des systèmes globaux et égaliser avec les systèmes financiers actuels qui, à l'inverse, peuvent évoluer et possèdent des capacités de calcul et de stockage des données supérieures. Bien qu'étant un réseau modeste en

[8] Ndtr : Projet scientifique s'appuyant sur les ressources inutilisées des consoles de salon PlayStation afin de calculer le repliement des protéines.

comparaison des mastodontes mondiaux du paiement (ex. VISA), c'est avec beaucoup de difficultés que Bitcoin, pour ne citer que lui, gère son flux de transactions actuel.

Pour ce qui concerne l'évolutivité de Cardano, nos objectifs sont bien aidés par la nature même de notre protocole de consensus. En effet, Ouroboros permet d'élire de manière décentralisée un quorum de nœuds de consensus. Ce quorum peut alors exécuter des protocoles plus traditionnels, tels que ceux développés ces 20 dernières années pour accommoder les besoins d'utilisateurs exigeants en ressources comme Google ou Facebook.

Ainsi, l'élection d'un quorum pour la gestion d'une époque (durée pendant laquelle les validateurs du consensus d'Ouroboros sont connus à l'avance) signifie qu'il existe un ensemble de nœuds de confiance pour un temps défini. Il devient alors un jeu d'enfant d'élire simultanément plusieurs de ces quorums de manière à gérer plusieurs groupes de transactions en parallèle.

Des techniques similaires pourraient être appliquées à la gestion du réseau et aussi pour fragmenter la blockchain elle-même en partitions uniques (technique appelée ''Sharding''). Dans notre feuille de route actuelle, ces méthodes dédiées à l'évolutivité seront mises en œuvre au début de l'année 2018 et nous continuerons ces efforts au cours des années 2019 et 2020.

1.2.4 La couche de calcul de Cardano

Comme mentionné précédemment, une transaction est faite de deux composants : (i) le mécanisme permettant l'envoi et l'enregistrement des flux de monnaie, et (ii) les raisons et les conditions d'exécution de la transaction. Ce deuxième composant peut parfois être très complexe. En effet, il peut mettre en jeu des terabytes de données, plusieurs signatures et reposer sur des prérequis d'exécution particuliers. Il peut aussi être remarquablement simple, ne nécessitant qu'une seule signature et l'adresse d'envoi des fonds.

Modéliser les raisons et conditions de la circulation de valeurs pose un défi immense, en ce sens que ces raisons sont éminemment personnelles aux acteurs impliqués et ce, de manière parfois inattendue. Les leçons tirées du droit des contrats produisent une image encore plus problématique, où les acteurs eux-mêmes ne seraient peut-être pas conscient que la transaction ne correspond pas à la réalité commerciale. Nous appelons généralement ce phénomène « l'écart sémantique ».

Pourquoi alors essayer de concevoir une cryptomonnaie voulant capturer tous les niveaux possibles d'abstraction et de complexité ? Cela semble en effet sisyphéen[9] par nature et naïf en pratique. Et cela sans compter que chaque choix d'abstraction implique à la fois des conséquences légales et de sécurité différentes.

Par exemple, il existe de nombreuses activités universellement jugées comme illégales qui se déroulent sur le net, comme le trafic d'images pédopornographiques ou la vente de secrets d'états. En offrant une résistance à la censure, l'existence d'infrastructures décentralisées robustes profite à ces trafics aussi bien qu'aux transactions commerciales. D'un point de vue légal, il est difficile de savoir si les

[9] Ndtr : Dans la mythologie, Sisyphe fut condamné à pousser sans fin un rocher.

nœuds de consensus du réseau - incités à se fédérer avec le temps pour des raisons d'efficacité - seraient tenus pour responsable des contenus qu'ils hébergent.

Le procès des opérateurs du réseau TOR (The Onion Router), le sort brutal réservé aux opérateurs de The Silk Road et le manque de cadre légal général pour la protection des utilisateurs d'un protocole dessinent un avenir incertain. Et l'imagination ne manque pas lorsqu'il s'agit de trouver de nouveaux usages à une cryptomonnaie (voir the Ring of Gyges). Est-il raisonnable de forcer tous les utilisateurs d'une cryptomonnaie à approuver les pires actions rencontrées sur le web?

Malheureusement, il n'existe aucune réponse claire pour guider les concepteurs de cryptomonnaies. A chacun de choisir son camp et d'en défendre ses mérites. Cardano et Bitcoin ont l'avantage d'avoir tous les deux choisi de séparer les problèmes en couches : Rootstock pour Bitcoin et CCL pour Cardano.

Ces actes mentionnés plus haut requièrent une complexité qu'il n'est pas possible d'avoir sur CSL. Ils demandent en effet du protocole de pouvoir exécuter des programmes écrits en langage dits "Turing complete" et une forme d'économie plus ou moins élaborée des ressources informatiques permettant de calculer les coûts d'exécution d'un programme[10]. Ils ont aussi besoin de nœuds de consensus souhaitant inclure leurs transactions au sein des blocs.

Cette restriction des fonctionnalités pourrait donc raisonnablement protéger les utilisateurs. Jusque-là, l'utilisation ou la maintenance de cryptomonnaies ne sont pas des actes illégaux aux yeux de la plupart des gouvernements. La grande majorité des utilisateurs peut donc se sentir confortée dans sa participation à ces protocoles dont les capacités sont comparables aux autres moyens de paiements dématérialisés.

Pour étendre ces capacités, il existe deux possibilités. Cela peut être le fait d'un groupe d'individus partageant un intérêt commun et sera par nature éphémère (par exemple un jeu de poker). Ou alors, cela peut être fait à travers un registre possédant les mêmes propriétés que Ethereum. Dans les deux cas, nous avons choisi d'externaliser les évènements par l'intermédiaire d'un protocole superposé.

Dans le cas d'un évènement privé et éphémère, il est judicieux d'éviter l'écriture de toutes les actions dans le registre distribué. Il est plus indiqué de restreindre les efforts à l'écriture de protocoles MPC (Multi Party Computation) visant des objectifs spécifiques et qui pourraient être invoqués sur demande par un groupe d'individus. Les calculs et activités afférents à ce groupe de personnes seraient coordonnés sur un réseau privé, le registre CSL servant alors uniquement de tableau d'affichage de confiance permettant de faire passer des messages, si nécessaire.

L'élément clé dans ce cas est qu'il y a consentement et encapsulation de la responsabilité et de la vie privée. CSL est utilisé comme une ressource numérique partagée pour que les utilisateurs se rencontrent et communiquent - comme le ferait un parc hébergeant un événement privé - mais ne fournit aucun service ou facilitation particulière. Les protocoles MPC permettront ainsi des interactions rapides sans surcharger inutilement le registre CSL, facilitant par la même occasion la croissance du système tout entier.

[10] Ndtr : C'est ce qui est désigné comme le "gas"

Les efforts de recherche de Cardano autour de ces outils sont centralisés dans notre laboratoire de Tokyo Tech et bénéficient aussi de l'aide de scientifiques basés dans d'autres pays. Nous avons nommé cette bibliothèque d'outils « Tartaglia », d'après un mathématicien contemporain de Girolamo Cardano. La première version sera disponible au cours du premier trimestre 2018.

Dans le second cas évoqué, plusieurs éléments sont requis : une blockchain avec une machine virtuelle, un ensemble de nœuds de consensus et un mécanisme permettant la communication entre deux chaînes. En partenariat avec une équipe de l'université de l'Illinois, nous avons commencé le processus consistant à formaliser rigoureusement la machine virtuelle de Ethereum en utilisant le K-framework[11].

Le résultat de cette analyse nous informera sur la manière optimale de concevoir une machine virtuelle répliquée et éventuellement distribuée, comprenant une sémantique opérationnelle claire et de fortes garanties quant à sa mise en œuvre correcte à partir de spécifications. En d'autres mots, la machine virtuelle doit réellement faire ce que le code lui dit de faire et ce avec des risques de sécurité minimisés.

Il existe toujours des problèmes non résolus quant à l'économie du ''gas'' proposée par Ethereum et ses liens avec des travaux comme ceux de Jan Hoffmann et al sur les langages prenant en compte les ressources informatiques et les études plus large sur la manière d'estimer ces ressources avant exécution. Nous sommes aussi curieux de connaitre le niveau d'indépendance entre un langage et une machine virtuelle. Par exemple, le projet Ethereum a exprimé son désir de changer sa machine virtuelle actuelle pour Web Assembly.

Le prochain effort consistera à créer un langage de programmation permettant d'écrire des contrats d'état[12] qui seront invoqués comme des services par les applications décentralisées. Pour cela, nous avons choisi à la fois d'utiliser le langage existant Solidity pour des applications à faible niveau d'assurance, et de développer un nouveau langage appelé Plutus pour les applications à haut degré d'assurance nécessitant des techniques de vérification formelle.

Comme le projet Zeppelin basé sur Solidity, I.O.H.K. développera aussi une bibliothèque Plutus de référence afin que les créateurs d'applications l'intègre dans leurs projets. Nous développerons aussi des outils dédiés à la vérification formelle, dans la lignée du travail effectué par U.C.S.D. (Université de Californie San Diego) sur le projet LiquidHaskell.

Pour ce qui est du consensus, Ouroboros a été conçu de manière suffisamment modulaire pour permettre l'emploi de contrats intelligents. CSL et CCL partagerons donc le même algorithme de consensus.

Ouroboros peut être configuré de manière à fonctionner à la fois avec des registres distribués privés et des registres distribués publics ; l'autorisation d'utiliser un registre privé se fait alors via une distribution de jetons particuliers. La devise native de CSL, ADA, a été distribuée lors d'une vente qui a eu lieu dans toute l'Asie et sera probablement vendue sur un marché secondaire. Cela signifie que l'algorithme de

[11] Ndtr : Travaux menés par la société Runtime Verification.
[12] Ndtr : Contrats capables de garder des informations en mémoire - "Stateful contracts".

consensus du CSL est contrôlé par un ensemble hétérogène et de plus en plus décentralisé d'acteurs ou de mandataires. Avec CCL, il est possible de créer un jeton spécifique avec lequel des organismes suivant une réglementation propre opèrent sur un registre privé.

La flexibilité de cette approche permet la cooccurrence de plusieurs CCL possédant tous des règles différentes pour traiter leurs transactions. Par exemple, les activités liées aux paris et aux jeux pourraient être restreintes aux utilisateurs ayant décliné à la fois leur identité et l'origine de leurs fonds (règles dites KYC/AML - Connaître son client/Anti-blanchiment) ; les transactions émanant d'utilisateurs non vérifiés seraient simplement ignorées.

Le dernier point de conception concerne l'utilisation des modules de sécurité associés au matériel de confiance ("Trusted Hardware Security Modules" ou HSMs). Il existe en effet deux énormes avantages à pouvoir se servir de cette technologie en association avec notre protocole. (i) Les HSMs apportent un gain conséquent de performances sans introduire de vulnérabilités autre que celle consistant à faire confiance au vendeur de ce matériel. (ii) Grâce à l'utilisation de preuves particulières ("Sealed Glass Proofs" ou SGP), les HSMs sont capables de certifier que des données peuvent être vérifiées puis détruites, sans avoir été copiées ni divulguées à un acteur extérieur.

Ce deuxième point pourrait avoir un impact révolutionnaire sur la mise en conformité. D'habitude, lorsqu'un consommateur fournit une information personnelle pour authentifier son identité ou prouver un droit de participation, ces informations sont transmises à un tiers de confiance avec l'espoir que ce dernier n'agira pas de manière malveillante. Dans ce cas, le consommateur perd tout contrôle sur les informations qu'il fournit. De plus, le devenir de ces informations sera soumis à divers règlements en fonction des juridictions.

Avoir des organismes de certification et pouvoir stocker leurs attestations nous concernant dans une enclave matérielle (ici les HSMs) signifie que n'importe quel acteur pourra vérifier des faits nous concernant sans jamais avoir à connaître notre identité. Par exemple, untel n'est pas citoyen des Etats-Unis d'Amérique. Untel est un investisseur accrédité. Untel est un contribuable Américain, etc …

La stratégie HSM de Cardano consistera à essayer des protocoles spécialisés durant les deux prochaines années en utilisant les enclaves matérielles SGX et Trustzone produites par Intel et ARM, respectivement. Ces deux modules sont d'ores et déjà présents dans des milliards de produits informatiques, du PC portable au téléphone mobiles. Leur utilisation ne fera donc appel à aucun effort supplémentaire de la part des consommateurs. Ces deux modules sont également fortement contrôlés, bien conçus et basés sur des années de travail de la part des équipes de sécurité matérielle les plus importantes et les mieux financées.

1.2.5 Réglementation

La dure réalité de tous les systèmes financiers modernes est qu'à mesure qu'ils grossissent, ils développent un besoin ou du moins un désir de réglementation ou régulation. Ce résultat est généralement la conséquence d'effondrements récurrents causés par la négligence d'un ou plusieurs acteurs sur un marché.

Par exemple, la crise Knickerbocker de 1907 a entraîné 6 ans plus tard la création de la Réserve Fédérale Américaine, jouant le rôle de prêteur en dernier ressort. Les excès des années 1920 aux États-Unis ont entraîné la Grande Dépression (1929) et la création en retour de la Securities Exchange Commission (SEC) en 1934. Le but de la SEC est d'empêcher un événement similaire ou au moins d'en tenir les mauvais acteurs pour responsables.

Il peut être débattu du besoin, de la portée et de l'efficacité des réglementations, mais personne ne peut nier leurs existences ni le zèle des principaux gouvernements à les mettre en application. A mesure que la globalisation avance et que l'argent devient numérique, le défi rencontré par tous les régulateurs devient alors double.

Tout d'abord, quelles sont les règles qui priment lorsque de multiples juridictions sont concernées ? La doctrine quelque peu désuète de Souveraineté Westphalienne[13] fond comme neige au soleil quand une seule transaction peut toucher trois douzaines de pays en moins d'une minute. Devrions-nous simplement appliquer les règles de l'État qui exerce la plus grande influence géopolitique?

Le second point concerne les améliorations apportées à la technologie assurant le caractère confidentiel des transactions. Ces améliorations ont créé une course technologique au coude à coude dans laquelle il devient de plus en plus difficile de déterminer qui a participé à une transaction, et plus encore de savoir qui détient quoi. Dans un monde où des millions de dollars d'actifs peuvent être contrôlés avec rien de plus qu'un code secret constitué de 12 mots[14], comment appliquer une réglementation efficace ?

Comme tout autre système financier, le protocole Cardano doit avoir une opinion sur ce qu'il considère juste et raisonnable. Nous avons décidé de chercher l'équilibre entre les droits individuels et les droits des marchés.

Les individus devraient toujours avoir seul accès à leurs fonds sans coercition ni saisie des biens possible. Ce droit doit être mis en œuvre parce que, comme au Venezuela ou au Zimbabwe, les gouvernements ne peuvent pas tous être considérés de confiance lorsqu'il s'agit de ne pas abuser de leur pouvoir pour le gain personnel de quelques politiciens corrompus. Les cryptomonnaies doivent être conçues avec le plus petit dénominateur commun.

L'histoire ne devrait jamais être altérée ou modifiée. La technologie Blockchain offre la promesse d'immutabilité. Rendre possible l'annulation ou la modification des enregistrements officiels introduit le risque trop grand de voir de tels changements se faire au bénéfice d'un ou de plusieurs acteurs.

Les flux de valeurs ne devraient pas être limités. Le contrôle des capitaux et autres obstacles artificiels réduisent les droits de l'homme. En dehors de la futilité d'essayer de les faire respecter, dans une économie mondiale où de nombreux citoyens des pays les moins développés s'expatrient pour trouver un salaire décent, restreindre les flux de capitaux finit généralement par nuire aux plus pauvres.

[13] Ndtr : Doctrine de la souveraineté territoriale.
[14] Ndtr : Ici cette phrase de 12 mots *est* la clé privée

Une fois ces principes énoncés, il faut rappeler que les marchés sont des organes bien différents des individus. Alors que nous, concepteurs de Cardano, croyons aux droits des individus, nous pensons également que les places de marché ont le droit d'indiquer ouvertement leurs conditions d'accès. Si une personne accepte de faire des affaires sur un marché, alors elle doit s'en tenir aux normes édictées par ce dernier afin de maintenir l'intégrité de l'ensemble du système.

Le défi des réglementations a toujours été leur coût et leur praticité de mise en application. Les petites transactions multi-juridictionnelles sont trop onéreuses au sein des systèmes financiers actuels pour pouvoir garantir des recours en cas de fraude ou de contentieux commercial. Lorsque l'on envoie un virement au Prince Nigérian[15], il est généralement trop coûteux d'essayer de récupérer ses fonds perdus.

Pour Cardano, nous pensons pouvoir innover sur trois niveaux :

Les contrats, les termes et conditions des relations commerciales peuvent être mieux contrôlés. Si tous les actifs sont numériques et peuvent être présents uniquement sur CSL, alors de fortes garanties de commerce sans fraude peuvent être obtenues.

L'utilisation de modules HSMs peut fournir un espace d'identification où les informations personnelles ne sont pas divulguées mais utilisées pour l'authentification. Les référents à l'origine de l'identification première seraient alors en mesure de fournir un système de réputation mondial permettant aux activités réglementées, comme les jeux en ligne avec conformité fiscale automatisée ou les plateformes d'échange décentralisées, d'avoir des coûts beaucoup plus bas.

Enfin, dans la feuille de route de Cardano, il y a la création d'un DAO ("Decentralized Autonomous Organization" - Organisation Décentralisée Autonome) réglementé de manière modulaire. Il peut être personnalisé pour interagir avec les contrats intelligents rédigés par les utilisateurs afin d'ajouter la mutabilité, la protection des consommateurs et l'arbitrage. La portée de ce projet sera décrite dans un document ultérieur.

1.3 Pourquoi tout cela ?

Cardano est un projet-marathon construit sur les retours de centaines d'esprits brillants, qu'ils viennent de l'industrie des cryptomonnaies ou de l'extérieur. Cela signifie une remise à l'ouvrage infatigable, l'utilisation active de l'évaluation par les pairs et le vol éhonté d'idées géniales lorsque nous en prenons connaissance.

Les sections qui vont suivre couvrent chacune un élément essentiel de notre projet. Certains de ces éléments ont été sélectionnés en raison du désir que nous avons d'améliorer les pratiques existantes dans le monde des cryptomonnaies en général tandis que d'autres sont spécifiques à l'évolution de Cardano lui-même.

[15] Ndtr : Nom donné à une arnaque par email originaire du Nigéria et faisant passer l'envoyeur pour un Prince ayant besoin d'un service.

Aucun projet ne peut couvrir tous les objectifs ou satisfaire tous les utilisateurs, néanmoins nous tentons d'envisager ce à quoi devrait ressembler un système financier évolutif à destination des juridictions qui en sont dépourvues. Le but des cryptomonnaies n'est pas de perturber les systèmes financiers existants. Ces derniers sont de toute façon capables de faire avec le changement et de conserver leurs formes et fonctions.

Il faut plutôt regarder du côté des endroits où il est trop coûteux de déployer des systèmes bancaires identiques à ceux des pays développés, où beaucoup vivent avec moins d'un dollar par jour, sans aucune identité stable ni accès au crédit.

Dans ces endroits, pouvoir regrouper un système de paiement, les droits de propriété, une identité, le crédit et la protection contre les risques en une seule application fonctionnant sur un téléphone portable n'est pas seulement utile, mais change la vie. La raison pour laquelle nous construisons Cardano est que nous pensons avoir une réelle opportunité de pouvoir mettre en action - ou du moins faire avancer - cette vision pour le monde en développement.

Même en cas d'échec, si nous arrivons seulement à changer la manière dont les cryptomonnaies sont conçues, évoluent ou financées, alors cela sera déjà un bel accomplissement.

2. Science et ingénierie

2.1 Concevoir par itérations

Les cryptomonnaies sont des protocoles mis en œuvre comme des logiciels. Les protocoles sont une forme de conversation intelligente entre participants et les logiciels permettent la manipulation de données afin d'atteindre des buts précis. Entre un logiciel fiable ou un protocole sécurisé et leurs contraires respectifs, la différence résulte uniquement de choix de conception humains.

Un bon logiciel nécessite de la responsabilité, une exigence professionnelle bien définie, des processus reproductibles, des tests approfondis et une itération inlassable. Un bon logiciel a également besoin de développeurs raisonnablement talentueux, ayant suffisamment de connaissances spécifiques dans leurs domaines pour concevoir correctement un système capable de résoudre les problèmes pour lesquels il est conçu.

Quant aux protocoles utiles et sécurisés, en particulier ceux faisant appel à la cryptologie et aux systèmes distribués, ils naissent d'un processus plus académique et axé sur le respect de normes établies. L'examen par les pairs, les débats interminables et la bonne compréhension des compromis en jeu sont autant de prérequis nécessaires pour s'assurer de l'utilité d'un protocole. Toutefois, ceux-ci ne suffisent pas et les protocoles ont aussi besoin être mis en œuvre et testés en conditions réelles.

Le défi particulier de l'industrie des cryptomonnaies est qu'elle mélange en son sein deux philosophies complètement différentes et qu'aucune synthèse Hégélienne n'a été faite. Il existe une mentalité de start-up « bouger vite et tout casser » conduite par la jeunesse, la cupidité et la passion. Son antithèse

est une approche lente, méthodique, académique et axée sur une volonté de consolider les innovations de notre industrie pour en faire une niche prestigieuse bénéficiant de financements importants.

Le résultat est qu'aujourd'hui, beaucoup de cryptomonnaies sont spécifiées sur un livre blanc uniquement (''white paper''), ou bien directement codées à la va-vite. Aucune des cryptomonnaies appartenant au Top 10 des capitalisations de marché n'est basée sur un protocole ayant subi l'examen par les pairs et aucune n'a été mise en œuvre en suivant des spécifications formelles[16].

Pourtant, des milliards de dollars sont en jeu et une cryptomonnaie est extrêmement difficile à modifier une fois déployée. Comment un utilisateur peut-il savoir si son système est sécurisé ? Comment un utilisateur peut-il savoir si les annonces de marketing sont légitimes ? Que se passe-t-il si le protocole ne peut pas tenir les promesses faites ?

Ce manque de méthode est l'une des principales raisons pour lesquelles I.O.H.K. a souhaité construire Cardano. Notre espoir était de concevoir un projet de référence et qu'il serve d'exemple pour faire les choses de façon plus efficace, saine et honnête.

Le but n'est pas de proposer une manière radicalement nouvelle de développer des logiciels et des protocoles, mais plutôt de reconnaître que des logiciels et protocoles performants existent déjà et que nous pouvons reproduire les conditions ayant conduit à leur création. Si possible, nous voulons faire en sorte que ces conditions soient publiquement connues et libres d'accès, au bénéfice de notre discipline toute entière.

2.2 Les faits et les opinions

L'autre soucis est de déterminer où les faits prennent fin et où les opinions commencent. Il existe des centaines de langages de programmation, des dizaines de paradigmes de développement et plusieurs philosophies de gestion de projet. Le monde universitaire est confronté à ses propres défis, résultant principalement de sa distance par rapport aux préoccupations des entreprises.

Pour Cardano, nous avons d'abord tenté de saisir les lacunes évidentes de notre discipline qui peuvent être intéressantes à combler du point de vue de l'ingénieur. La cryptographie et les systèmes distribués sont tous deux des sujets extrêmement complexes, et il existe beaucoup trop d'exemples de mises en œuvre naïves menant à des erreurs catastrophiques. Par conséquent, tout protocole nécessitant un apport de ces domaines doit être conçu par des experts reconnus et soumis à l'examen par d'autres experts.

Dans ce domaine, Ouroboros est notre première étude de cas. Comme en atteste les nombreuses publications vérifiables par tout un chacun, ce dernier a été conçu par une équipe de cryptologues possédant une expérience solide et diverse. Il a été construit en suivant une méthode standard en cryptologie, avec hypothèses de sécurité, un modèle contradictoire et des preuves. Ces preuves ont été vérifiées lors de soumissions à des conférences et aussi de manière indépendante par une équipe de l'Université de Cambridge utilisant des preuves informatiques écrites en langage Isabelle.

[16] Ndtr : A la date de traduction, Cardano reste le seul à respecter ces deux critères

Pourtant, ce travail ne fournit à lui seul aucune garantie d'utilité - juste une vérification rigoureuse d'un modèle de sécurité compte tenu de certaines hypothèses. Pour être utile, encore faut-il mettre en œuvre et tester le protocole. Nos développeurs l'ont fait à la fois en langage Haskell et en Rust. Ce travail a révélé que d'avantage d'efforts devaient être consacrés au modèle de synchronisation, ce qui a conduit à la création de Ouroboros Praos.

Cet art de l'itération est ce qui produit d'excellents protocoles. Chaque étape apporte de nouvelles leçons et nous impose de vérifier à nouveau l'exactitude des étapes précédentes. Ce processus est coûteux, parfois fastidieux et prend du temps. Il est toutefois nécessaire pour garantir que le protocole est correctement conçu.

Les protocoles - en particulier ceux utilisés par des milliards de personnes - ne sont pas conçus pour une courte durée et n'évoluent pas rapidement. Ils seront au contraire présents pendant des années, voire des décennies. Avant d'imposer au monde un nouveau système financier avec lequel nous allons vivre les 100 prochaines années, il semble tout à fait raisonnable d'exiger un peu pénibilité et de rigueur à ses concepteurs.

2.3 Péchés fonctionnels

En poussant un peu la critique, on pourrait dire que les choix des outils, des langages et des méthodologies utilisés pour le développement de logiciels sont plus des produits du hasard que des choix objectifs. Le code source est semblable à de la prose. Tout le monde a un avis sur ce qui est bon, le contenu étant parfois moins important que le médium par lequel il s'exprime. Nous devons commettre le péché de choisir et accepter que ce choix sera rejeté par au moins une personne. Il existe toutefois de nombreuses justifications à ce choix.

Les protocoles qui rendent Cardano possible sont mis en œuvre en utilisant le langage Haskell. L'interface utilisateur, Daedalus, a été encapsulée dans une branche de Electron. Nous avons choisi d'utiliser le modèle d'architecture web dans la mesure du possible et, pour notre base de données, nous avons opté pour un paradigme de valeur-clé utilisant RocksDB.

Cette manière de procéder se traduit en une maintenance des composants et un basculement futur vers une technologie supérieure beaucoup plus aisés. Notre approche profitera indirectement aussi des travaux de développement menés par d'autres sociétés telles que GitHub et Facebook.

L'utilisation d'une interface graphique Web nous permet de tirer parti de React et de créer pour l'utilisateur des fonctionnalités à l'aide d'outils compris par des centaines de milliers de développeurs JavaScript. L'utilisation d'une architecture Web signifie que les composants peuvent être traités comme des services et que le modèle de sécurité associé est pertinent.

Même dans le monde des langages fonctionnels, les alternatives sont nombreuses et notre choix du langage Haskell pour la mise en œuvre du protocole Cardano était le choix le plus difficile à faire. D'un côté, il existe des langages plus flexibles et impurs comme Clojure, Scala et F# qui bénéficient d'énormes bibliothèques Java et des écosystèmes .Net, tout en préservant certains des meilleurs aspects de la

programmation fonctionnelle. De l'autre côté, il existe des langages plus académiques tels que Agda et Idris qui ont un lien étroit avec les techniques permettant une vérification rigoureuse de l'exactitude du code. Agda et Idris manquent toutefois de bibliothèques raisonnables et sont moins agréables pour les développeurs.

Pour Cardano, le choix s'est porté sur Ocaml et Haskell. Ocaml est un langage formidable avec une communauté d'acteurs de qualité, de bons outils, une expérience de développement raisonnable et un excellent ancrage dans la vérification formelle à travers Coq. Pourquoi avons-nous donc choisi le langage Haskell ?

2.3.1 Pourquoi Haskell ?

Les protocoles qui composent Cardano sont distribués, pétris de cryptologie et requièrent un haut niveau de tolérance aux erreurs. Même les meilleurs jours, il existera toujours des acteurs byzantins (malicieux), et des messages malformés ou des logiciels clients défectueux qui causeront de manière non intentionnelle le chaos sur le réseau.

Tout d'abord, nous voulions utiliser un langage bénéficiant d'un système fortement typé sur lequel nous pourrions facilement (i) faire fonctionner des outils tels que QuickCheck et d'autres techniques plus élaborées telles que ''Refinement Types'', (ii) le tout avec des attentes raisonnables en terme de tolérance aux erreurs. Si Erlang respecte la deuxième condition, les langages Haskell et Ocaml satisfont plutôt la première.

Avec l'arrivée de Cloud Haskell, Haskell gagna beaucoup des avantages de Erlang sans sacrifier aucun des siens. De plus, la modularité et la composabilité[17] de Haskell nous a permis d'utiliser pour Cardano plusieurs bibliothèques légères et sur-mesure appelées Time Warp.

Deuxièmement, les bibliothèques Haskell ont beaucoup évoluées ces dernières années grâce aux efforts de nombreuses sociétés commerciales telles que Gallois, FP Complete et Well-Typed. Haskell peut dès lors être employé pour développer des applications de niveau industriel.

Troisièmement, l'évolution rapide de PureScript nous a donné l'opportunité très attendue de pouvoir créer un pont avec le monde du JavaScript, dans l'esprit de ce qu'a été l'arrivée de ClojureScript pour Clojure. Nous anticipons que PureScript sera particulièrement important quand viendra le moment de faire fonctionner Cardano dans un navigateur ou pour développer des porte-clés sur mobiles.

Quatrièmement, en ce qui concerne la gestion des dépendances, Haskell a pu bénéficier ces dernières années d'un engagement social et technologique fort mené principalement par des personnalités telles que Micheal Snoyman à travers la création de la plateforme Stackage. Cette dernière est facile d'utilisation et bien maintenue par FP Complete. Au-delà de la gestion des dépendances, notre objectif est aussi de faire en sorte que la construction de nos logiciels soit reproductible. En d'autres termes, une même configuration utilisant les mêmes versions de dépendances doit produire les mêmes

[17] Ndtr: Un système avec des composants pouvant être facilement assemblés et réarrangés en fonction des besoins.

artefacts de construction. Grâce à Stackage, nous avons pu utiliser NixOps avec succès afin d'atteindre un haut niveau de reproductibilité.

Enfin, le vivier de talents au sein des développeurs Haskell est raisonnablement grand en comparaison des autres langages, plutôt bien formé et avec un bon mélange de compétences académiques et industrielles. Haskell agit ici en filtre de compétences en ce sens qu'il est assez rare de rencontrer un développeur expérimenté en Haskell n'ayant aucune connaissance approfondie des sciences informatiques.

2.3.2 Spécifications et vérification formelle

L'une des principales forces d'un protocole dont la construction a suivi un modèle de sécurité avec preuve formelle de justesse est que ce protocole offre une garantie sur les marges de manœuvre d'un adversaire. Il est alors offert à l'utilisateur de ce protocole un contrat stipulant que si le protocole est suivi correctement et que les preuves sont justes, alors un adversaire ne pourra pas violer les barrières de sécurité établies.

Les implications de l'assertion précédente sont évidemment énormes. En effet, les adversaires étant intelligents et capables et ce sans limites préétablies, affirmer alors qu'ils seront battus par la seule force d'un modèle mathématique est pour le moins extraordinaire. Et cela n'est bien entendu pas totalement vrai.

Le monde réel introduit de nombreux facteurs qui empêchent l'existence d'une utopie de la sécurité totale et des comportements vertueux. Par exemple, (i) les mises en œuvre d'un protocole peuvent être erronées, (ii) les machines physiques où un protocole est exécuté peuvent également introduire des vecteurs d'attaque non soupçonnés, (iii) le modèle de sécurité envisagé peut être insuffisant et non conforme aux réalités d'une utilisation quotidienne.

Un choix doit alors être fait sur la quantité de spécifications, de rigueur et de vérifications qu'un protocole doit suivre. Le projet ''Sel4 Microkernel'' est un excellent exemple de l'aventure qui résulte d'une chasse totale aux ambiguïtés présentes dans un code. Ce projet a en effet requis l'écriture de presque 200 000 lignes de code Isabelle afin de vérifier l'exactitude de moins de 10 000 lignes de code C initiales. Toutefois, le noyau d'un système d'opérations est tellement important que cela poserait de sérieux problèmes s'il n'était pas correctement mis en œuvre.

Est-ce que pour autant tous les logiciels de cryptologie requièrent un même effort Herculéen ? Peut-on choisir un chemin plus aisé produisant un résultat équivalent ? Aussi, cela est-il vraiment important que le protocole soit parfaitement mis en œuvre si le système d'opération qui l'exécute est aussi vulnérable aux attaques que ne l'est Windows XP ?

Pour Cardano, nous avons choisi la voie du compromis. Tout d'abord, et à cause de la complexité inhérente aux domaines de la cryptologie et des systèmes distribués, les preuves de justesse ont tendance à être très subtiles, longues, compliquées et techniques. Cela a pour conséquence que leurs vérifications par l'homme sont fastidieuses et sujettes aux erreurs. C'est pourquoi nous pensons que

chaque preuve de justesse d'envergure - c.a.d touchant à une structure centrale du protocole et généralement présentée dans un ''white paper'' - doit être vérifiée par une machine.

Afin de vérifier que le code Haskell correspond bien à nos ''white papers'', nous pouvons choisir entre deux options bien établies : les solutionneurs SMT à travers LiquidHaskell et l'utilisation de Isabelle.

Les solutionneurs SMT (''Satisfiability Modulo Theories'') prennent en charge le problème de découvrir les paramètres fonctionnels qui satisfont une équation ou une inéquation. Alternativement, ils peuvent aussi démontrer que de tels paramètres n'existent pas. Comme discuté par De Moura et Bjørner, les cas d'utilisation pour les SMT sont variés. Le point clé est que ces techniques sont puissantes et peuvent réduire drastiquement le nombre de bugs et les erreurs sémantiques.

Isabelle quant à lui est un outil plus expressif et variable qui peut être utilisé à la fois pour spécifier et vérifier une mise en œuvre. Isabelle est un solutionneur générique de théorèmes basé sur des constructions logiques de haut niveau. Isabelle est aussi capable de représenter des groupes et autres objets mathématiques utilisés pour la construction de preuves et intègre le solutionneur SMT Z3 pour travailler sur des problèmes impliquant ces contraintes.

Ces deux approches apportent de la valeur et c'est pourquoi nous avons décidé de les utiliser toutes les deux et par étapes. Les preuves écrites par l'homme seront encodées dans Isabelle pour vérifier leur justesse, satisfaisant ainsi la règle mentionnée de vérification par la machine. Aussi, nous prévoyons d'inclure graduellement l'utilisation de LiquidHaskell pour tous les codes de Cardano en 2017 et 2018.

Comme point final, il est important de souligner que les résultats d'une vérification formelle dépendront toujours de la qualité des spécifications initiales que l'on vérifie. L'une des premières raisons pour laquelle nous avons choisi Haskell est que ce langage offre le bon équilibre entre théorie et pratique. Les spécifications tirées de nos ''white papers'' ressemblent beaucoup à du code Haskell. Connecter les deux devient alors considérablement plus aisé que si cela avait dû être fait avec un langage impératif.

Capturer des spécifications correctes n'est pas chose facile, de même que leurs mises à jour après des changements tels que des améliorations, réparations de bugs ou autre ; cependant, cette réalité ne doit en aucun cas diminuer la valeur globale de cet effort. Si l'on s'attaque à la construction d'une fondation basée sur la preuve de sécurité, alors sa mise en œuvre se doit de correspondre en tous points à ce qui a été promis sur le papier.

2.4 Transparence

Une question enfin se pose lorsque la science et l'ingénierie sont appliquées au développement d'une cryptomonnaie : comment régler le problème de la transparence ? Les décisions relatives à l'architecture ne sont pas des choix binaires et éthérés, survenant aux développeurs dans leurs rêves pour devenir de nouveaux canons de conception dès le lendemain. Ces choix sont le fruit de l'expérience, du débat et des leçons tirées des erreurs passées.

La difficulté est qu'une transparence totale du processus de développement pourrait influencer les discussions jusqu'au point où ces dernières deviendraient plus un jeu théâtral qu'un débat argumenté sur des faits. Les égos, les tentatives de gagner à sa cause une communauté, et la peur de paraître stupide forceraient les conversations à devenir stériles et contre-productives. De plus, des acteurs extérieurs pourraient essayer de pirater la conversation pour mettre leurs agendas à l'ordre du jour. Tout le monde ne possède-t-il pas une marotte ? Comment alors conjuguer ce besoin de transparence - un devoir envers la communauté qui a donné sa confiance en un groupe restreint de développeurs - avec le besoin d'une expression libre et sans peur ?

Avec Cardano, nous avons décidé d'utiliser une procédure standardisée et une modération directe. La communauté a besoin de savoir que la science et le code sont bien pensés, vérifiés et qu'ils font bien ce que les développeurs affirment qu'ils font. Pour cela, la revue par les pairs devrait satisfaire la partie scientifique, puisque c'est exactement pour cela qu'elle existe. Nous lui devons par ailleurs le monde moderne dans lequel nous vivons. Pour ce qui est du code, des divergences d'opinion sont encore bien présentes. Pour Cardano, nous avons voté pour confier la mission d'audit final du travail de I.O.H.K. à la Fondation Cardano. En particulier, la fondation a pour mission :

1- Une revue régulière du code source déposé sur le GitHub de Cardano afin de s'assurer de sa qualité, de la couverture des tests, des commentaires du code et de son entièreté.
2- Une revue de toute la documentation relative à Cardano, son utilité et sa justesse.
3- S'assurer que toutes les promesses du protocole sont bien mises en œuvre. Pour accomplir cette mission, I.O.H.K. soumettra de manière régulière des rapports pour évaluation. La fondation délivrera l'évaluation de ces rapports à la communauté avec une périodicité au minimum trimestrielle.

Nous espérons que cet effort marquera le début d'une conversation plus large sur la manière dont doit être géré le devoir de transparence d'un projet décentralisé. La surveillance des opérations par une entité externe de confiance est un moyen effectif de s'assurer que les développeurs restent concentrés sur leur mission, mais cela n'est toutefois pas suffisant pour garantir l'exécution complète du projet.

Pour cette raison, et après que le Trésor sera intégré au sein même du CSL, la fondation encouragera d'autres équipes de développeurs à construire des logiciels clients alternatifs basés sur les spécifications formelles écrites par I.O.H.K. De ce point de vue, la diversité a été une excellente technique utilisée par le projet Ethereum pour se prémunir d'une culture monolithique qui ne manque jamais de se former lorsqu'un seul un groupe restreint de développeurs est à l'œuvre.

En ce qui concerne les spécifications, il y a beaucoup à apprendre des standards suivis par le WC3 et l'I.E.T.F. Au final, chaque protocole intégré par Cardano devrait posséder une spécification indépendante du travail académique et du code source qui l'a vu naître. Il serait alors souhaitable que ces spécifications possèdent un format adéquat tel que le format RPC.

L'une des missions centrales de la fondation est d'être une entité garante des standards appliqués aux différents protocoles de Cardano et d'organiser les discussions autour des mises à jour ou autres changements pertinents relatifs à ces standards. Si Internet - un pur produit des standards – à travers l'I.E.T.F. peut atteindre un consensus sur ce à quoi doit ressembler un protocole central, alors il est

parfaitement raisonnable d'attendre de la part d'une entité dédiée (ici, la fondation) des résultats similaires.

Pour finir, il est important d'explorer la possibilité de pouvoir déplacer ces discussions sur une plateforme décentralisée, tenue sur le registre distribué lui-même. Ce concept est appelé un DAO (''Decentralized Autonomous Organization'') et un travail préliminaire en ce sens a déjà débuté. I.O.H.K. développera un modèle de DAO de référence à l'attention des organisations utilisant Cardano et désireuse de faire usage de cette fonctionnalité. L'une des prérogatives de la Fondation Cardano sera de décider d'utiliser ou non un tel DAO pour ses propres activités.

3. Interopérabilité

3.1 La grande myopie

La finance et plus largement le commerce sont des aventures éminemment humaines. Il existe des langages élégants, des outils extrêmement précis pour rendre l'intention palpable, et un puit sans fond de techniques permettant les retours en arrière en cas de problème, sans compter sur les quelques millénaires de construction de la loi cherchant à mettre en place une forme de justice dans les échanges. De fait, l'une des premières formes d'écriture scripturale était un contrat commercial.

Pour autant, quelle que soit l'intervention de la logique, des machines ou du pouvoir terrifiant de quelques organisations gouvernementales, l'élément humain ne peut pas être évité. C'est bien de là que naît la grande myopie des cryptomonnaies. Ces dernières ont pour la plupart divorcé de cette réalité humaine.

Les gens font des erreurs. Les gens changent d'avis. Les gens ne comprennent pas toujours parfaitement les relations d'affaires dans lesquelles ils s'engagent. Les gens sont parfois mal conseillés et abusés. Les circonstances peuvent changer à l'échelle individuelle et à l'échelle d'un état et cela nécessite des solutions uniques. D'ailleurs, la plupart des contrats n'ont-ils pas des clauses de force majeure ?

Cependant, les cryptomonnaies cherchent à se débarrasser de l'élément humain - de sa compassion et de son jugement - pour prendre fait et cause d'un juge informatisé, le tout sans considération envers les conséquences ou le principe de justice. Cela dit, étant donné que les hommes ont toujours essayé et continueront d'essayer de modifier les règles pour leurs gains personnels, il est particulièrement rafraichissant de posséder enfin un système parfaitement incorruptible.

Mais qu'advient-il lorsqu'un utilisateur doit faire coexister ce nouveau système avec le système financier traditionnel ? Que se passe-t-il lorsque l'on vit dans le monde des hommes ? Par exemple, les titres de propriété ne s'ancrent-t-ils pas totalement dans le monde physique ? Même si l'on représente sous forme de jetons[18] une parcelle de terrain, cela requiert toujours une forme de reconnaissance par la juridiction responsable.

[18] Ndtr : Processus appelé ''tokenization''

Un lingot d'or ne peut se mouvoir seul. Le juge informatique peut ordonner son mouvement, mais ne peut pas l'acter sans intervention humaine. C'est en ce sens qu'un registre distribué peut dériver et se retrouver coupé du monde réel.

Un concepteur de cryptomonnaie doit donc décider dans quelle mesure la réalité humaine a droit de cité dans sa cryptomonnaie. Plus la cryptomonnaie sera flexible, mois elle sera fidèle à l'absolu initial. Plus elle intègre la protection du consommateur, plus elle ouvre la porte aux possibilités d'annulation des transactions, retours en arrière et autres éditions du registre.

Cette section et la suivante sur la régulation expliquent l'approche pragmatique de Cardano sur ce sujet. Pour ce qui est de l'interopérabilité, il existe deux grand domaines à couvrir. Premièrement, l'interopérabilité avec le système financier actuel (le monde non-crypto) et deuxièmement, l'interopérabilité entre les cryptomonnaies.

3.2 Le système financier actuel en héritage

La technologie financière ou ''fintech'' n'est pas composée d'un seul standard ou même d'un langage commun. Il existe une grand diversité d'approches, d'organisations responsables des paiements, de chambres de compensation, de processus comptables, de transformations et de mouvements des valeurs.

Il n'est pas raisonnable de penser que l'écosystème actuel dans son entier va admettre sa défaite et adopter notre technologie simplement parce que cette dernière lui est supérieure. Par exemple, beaucoup utilisent encore aujourd'hui Windows XP, 16 années après sa sortie. Cet état de fait plutôt déprimant est équivalent à une personne utilisant toujours en l'an 2000 le premier Macintosh sorti en 1984.

Au-delà du comportement des consommateurs, les entreprises sont souvent encore plus lentes dans leur processus de mise à jour. Beaucoup de banques utilisent encore des logiciels internes écrits en Cobol. Lorsqu'une infrastructure fonctionne et remplit sa mission, il n'y a aucune motivation à faire évoluer les logiciels et les protocoles pour le bien des consommateurs, si ce n'est dans les cas extrêmes d'adaptation à de nouvelles règlementations ou des problèmes de sécurité.

Pour Cardano, nous devons tout d'abord évaluer les implications qu'auraient une intégration avec le système actuel. Quels systèmes, quels standards, quelles organisations et protocoles devrions nous cibler pour assurer un minimum d'interopérabilité ? Ces ponts doivent-ils être organisés en fédération - et donc sous contrôle restreint - ou totalement décentralisés ? Deviendront-ils des points centraux et fragiles, à la merci des hackers, propriétaires malhonnêtes ou organisations gouvernementales zélées comme le sont aujourd'hui les plateformes d'échanges ?

Il y existe trois points à régler de manière urgente : (i) la représentation de l'information et la croyance en sa véracité ; (ii) la représentation de la valeur et de ses propriétaires ; (iii) la représentation

d'organisations et d'un utilisateur, en même temps que l'agrégation des niveaux de confiance au sein de ces organisations.

Pour être utiles, les informations et les valeurs doivent pouvoir diffuser librement entre les systèmes financiers actuels et Cardano. Les résultats de ses échanges doivent être établis et enregistrés de manière à pouvoir construire une réputation et éventuellement former les bases d'un recours. Toutefois, il est à noter que ces éléments ont un intérêt surtout pour les acteurs impliqués. Les inscrire sur le registre distribué les rendrait alors indélébiles et accessibles à tous.

De plus, les valeurs ne peuvent pas toujours être déplacées librement dans les systèmes financiers actuels. Les embargos, les sanctions commerciales, le contrôle des capitaux et les décisions judiciaires ont le pouvoir de geler les avoirs. A seule fin d'être interopérable, il n'est pas possible de prendre le risque d'offrir une sortie de secours permanente aux avoirs concernées par ces cas de figure.

Enfin, l'image de marque et la réputation des organisations est la pierre angulaire des relations commerciales. Des milliards de dollars sont dépensés chaque année dans des campagnes publicitaires ayant pour but d'établir, de maintenir ou de réparer des images de marques. Si de fausses informations circulent au sujet d'une personne physique ou morale, cette personne aura le droit d'exiger réparation par des moyens légaux. A l'inverse aujourd'hui, les blockchains conservent indéfiniment leur historique.

Tout comme notre choix de langage de programmation, il n'existe pas de solution idéale qui résoudrait ces problèmes d'une seule et unique bonne façon. Au lieu de cela, nous devons encore une fois faire un choix éclairé.

Le flux d'informations est connu sous le nom de « source de confiance de contenus » (''trusted data feed''). Il possède des sources émettrices et du contenu émis. Les sources[19] ont une notion de crédibilité et des motivations à tromper ou au contraire à maintenir une relation honnête avec leurs clients. Le contenu est encodé de façon arbitraire.

Etant donné qu'avec nos protocoles nous envisageons d'utiliser du matériel possédant des enclaves de sécurité (cf. HSMs), nous explorerons la possibilité de prendre en charge le protocole ''Town Crier'' (« Crieur public ») établi par le Prof. Ari Juel. Si l'on fait l'hypothèse qu'il existe des sources crédibles d'informations sur internet, ''Town Crier'' permettrait d'en récolter les contenus afin de les utiliser au sein de contrats intelligents ou autres applications. Une première liste de sources de confiance sera créée par Emurgo, I.O.H.K. et la Fondation Cardano. Cette liste initiale sera par la suite complétée par le travail de curation de la communauté des utilisateurs. Ils seront récompensés pour ce travail par des fonds du Trésor. Notre espoir est qu'un système de réputation émerge autour des bonnes sources d'informations, créant une boucle de rétroaction positive améliorant leur fiabilité.

La représentation de la valeur est un sujet plus complexe. Contrairement à l'information - avec laquelle les protocoles peuvent se comporter de manière fiable et déterministe une fois sa véracité établie - la valeur est plus délicate.

[19] Ndtr : De la même manière que l'AFP ou Reuters

Une fois mise sous forme de jetons (ou ''tokens''), la valeur doit se comporter comme un objet unique. Si l'information peut être copiée et transmise, un jeton représentant une valeur ou un titre de propriété ne peut, lui, pas être dupliqué et exister sur différents registres. Cela détruirait en effet l'intégrité de tout le système.

Lorsque l'on traite la valeur sous forme de jetons, le défi de l'interopérabilité avec le système financier actuel est que la confiance, la fiabilité et la capacité d'audit changent à mesure que les jetons transitent entre les registres. Par exemple, si Bob possède un Bitcoin et le dépose sur une plateforme d'échanges, alors Bob transforme son Bitcoin en une représentation de celui-ci sur le registre de la plateforme d'échanges. Dans le cas de la plateforme MtGOX, le registre ne se conformait plus à la réalité, laissant alors les utilisateurs devant leurs pertes.

Le problème se complique encore un peu plus à cause du besoin qu'ont les systèmes financiers actuels de reconnaitre les jetons qui vivent sur un registre d'un nouveau type, ici une cryptomonnaie. Comme mentionné précédemment, les entreprises sont historiquement réticentes à améliorer leurs logiciels et à prendre en charge de nouveaux protocoles. Cette situation n'a pas de solution évidente. Pour Cardano, notre meilleur espoir est de proposer aux utilisateurs la possibilité d'associer un jeu de métadonnées relativement riche à leurs transactions, en attendant que des standards de l'industrie se dessinent et utilisent ces métadonnées. Des progrès en ce sens ont été faits avec le groupe de travail Interledger et des efforts tels que R3Cev pour mettre à jour les protocoles financiers.

Le plus grand défi reste toutefois la quantification et la qualification des avoirs transférés entre les systèmes traditionnels et un registre de cryptomonnaie. Par exemple, si Bob est banquier et décide de lancer un jeton adossé au dollar, alors Bob peut toujours construire un pont de manière à envoyer ses jetons sur un registre comme Cardano en tant que UIA (cf. ''User Issued Assets''). Si Cardano permet de connaitre les propriétaires, tout en fournissant les fonctionnalités qui font que l'on adore les registres distribués comme l'horodatage et la capacité d'audit, aucune cryptomonnaie ne peut faire une Bob un banquier honnête. Bob aurait ainsi toujours la possibilité de faire fonctionner une réserve fractionnaire en ne respectant pas intégralement la convertibilité de ses jetons avec des dollars de réserve. Cette fraude ne peut pas être détectée par une cryptomonnaie à moins que le dollar lui-même ne soit un jeton existant sur un autre registre distribué.

Enfin, la représentation des organisations est un problème classique des réseaux qui date des débuts d'Internet. Les universités, les entreprises, les ministères et les utilisateurs en général ont besoin, à un moment ou un autre, d'établir leur identité. A cette fin, des solutions pragmatiques quoique centralisées comme le Public Key Infrastructure et le système DNS de l'I.C.A.N.N. ont été développées. Compte tenu du fait que nous profitons tous d'Internet aujourd'hui, ces solutions peuvent être considérées comme pratiques et évolutives. Cependant, elles ne répondent pas aux questions plus orientées que posent la fiabilité, la mise en confiance et tout autre caractéristique nécessaire à l'établissement d'une relation commerciale.

Les plateformes d'e-commerce comme eBay ont construit leur modèle sur la fourniture de ce type d'informations et de métadonnées au sein même de leur infrastructure. La qualité des produits et des vendeurs sont souvent fortement influencées par la seule présence de notes attribuées par des sources de confiance. La centralisation du système d'attribution de la réputation est ici le point qui nous

intéresse. Un des buts de Cardano est de proposer un système financier à l'attention des pays en voie de développement. L'une des clés de cet effort réside dans la capacité à établir une relation de confiance avec quelqu'un que l'on n'a jamais rencontré. Si une seule entité ou un consortium d'acteurs contrôle qui sera jugé bon ou mauvais en lieu et place d'un processus organique émergeant des interactions entre les membres d'une communauté, alors on ouvre la voie aux décisions arbitraires. Cela va à l'encontre des valeurs que nous souhaitons insuffler à notre projet et à l'encontre de la raison d'être des cryptomonnaies.

Heureusement, les mécanismes qui seront utilisés pour les votes d'attribution des fonds du Trésor, pour l'ajout de sources de confiance ou pour la modification du protocole pourront être réutilisés ici pour établir un système de gestion de la réputation. Il s'agit là d'un domaine de recherche actif et nous espérons qu'il aboutira en 2018-2019 sous la forme d'un protocole, une fois d'autres éléments plus fondamentaux achevés.

3.3 Interopérabilité entre cryptomonnaies

Passé le problème de l'interopérabilité avec le monde traditionnel, celui de l'interopérabilité entre cryptomonnaies est bien plus facile à résoudre. Chaque registre ou cryptomonnaie possède un protocole réseau, des standards de communication et des hypothèses de sécurité qui définissent son algorithme de consensus. Ces derniers sont facilement quantifiables.

Le transfert d'informations est alors établi en connectant deux réseaux entre eux et en traduisant leurs messages respectifs. Le transfert de valeurs peut alors s'effectuer par un système de relai, des échanges atomiques entre chaines ou par un système ingénieux de chaines greffées. Sans acteur central, les problèmes se cantonnent ici à la question de savoir si l'on accorde sa confiance à un groupe de développeurs, de mineurs ou un vendeur.

Pour Cardano, nous intégrons un nouveau protocole de chaine greffée élaboré par Kiayias, Miller et Zindros. Ce protocole permet le mouvement sécurisé de valeurs entre deux chaines et il sera aussi le moyen primaire utilisé pour les transferts de valeurs entre CSL et CCL.

Pour ce qui est des autres cryptomonnaies, des ponts fédérés devraient se former à mesure que Cardano croit en valeur et que son nombre d'utilisateurs augmente. Pour accélérer cette croissance, CSL prend en charge une version restreinte de Plutus spécialisé dans l'écriture de scripts d'interopérabilité. De nouveaux types de transactions seront ajoutés durant notre phase de développement nommée ''Shelley'' et les phases suivantes, de manière à répondre spécifiquement à ces besoins.

3.4 Le labyrinthe de Daedalus

L'interopérabilité ne peut pas se penser sans vision globale. Les protocoles spécialisés, les nouveaux types de transactions, les systèmes de vérification de la crédibilité et les flux d'informations ne peuvent pas être restreints à, ou contrôlés par une seule entité ou un seul utilisateur. Ils doivent être accessibles à tous sans aucune forme de censure ou droit d'entrée.

Toutefois, que se passera-t-il si jamais Cardano ne prend pas en charge un protocole, un type de transactions ou une application dont un utilisateur ne peut pas se passer ? Le web fut confronté à un problème similaire dans les années 1990s.

Les solutions trouvées par le web à ces problèmes sont, ironiquement, parfaitement adaptées au monde des cryptomonnaies. (i) L'introduction de JavaScript permit d'ajouter la programmabilité à n'importe quel site web et l'addition de fonctionnalités arbitraires. (ii) L'introduction de plugins et d'extensions au sein même des navigateurs donna naissance au quasi sur-mesure à tous ceux souhaitant les installer. Ces deux approches nous ont donné le web moderne mais aussi les pires horreurs en terme de sécurité.

Ethereum adopta la première approche en autorisant les utilisateurs à inclure des sous-protocoles sur le registre d'Ethereum sous la forme de contrats intelligents. Cardano prend en charge le même type de fonctionnalités à travers le CCL. Mais qu'en est-il des extensions sur-mesure ?

Prenons l'exemple d'un trader en cryptomonnaies et d'une plateforme d'échange décentralisée (ED) qui propose plusieurs cryptomonnaies. Ce trader veut automatiser ses stratégies d'échanges sur ED. Dans un écosystème fragmenté, ce trader devra installer une douzaine de logiciels clients différents, un pour chaque cryptomonnaie, et devra écrire un logiciel sur-mesure capable de converser avec chacun de ces logiciels clients pour coordonner ses échanges automatiques. Si un des logiciels clients est mis à jour, cela rendra caduque le logiciel sur-mesure que le trader aura écrit. De plus, que faire dans le cas où ce trader souhaiterait vendre ce logiciel sur-mesure ?

Si l'interface avec plusieurs cryptomonnaies pouvait ressembler au code web, dans l'inspiration de ce que font les extensions de navigateurs, alors le tâche du trader deviendrait beaucoup plus simple. Une interface universelle peut être établie. L'installation se ferait en un seul clic. La distribution des logiciels se ferait sur le modèle du Chrome Web Store.

Pour Cardano, nous avons décidé d'expérimenter autour de cette idée en déployant notre porte-clés de référence sur Electron. Electron est un projet libre présent sur GitHub combinant Node et Chrome. Le résultat de ce travail se nomme Daedalus.

La première génération de Daedalus sera un porte-clés HD (''Hierarchical Deterministic'') prenant en charge la plupart des fonctionnalités comptables et de sécurité issues de standard de cette industrie, comme un mot de passe protégeant les dépenses et le standard BIP39. Les générations suivantes de Daedalus se focaliseront sur les applications avec un magasin pour ces dernières, des API universelles pour leur intégration et un SDK.

Les innovations clés sont la facilité de développement en autorisant l'utilisation de JavaScript, HTML5 et CSS3 pour la construction d'applications, et une communication entre applications fonctionnant de manière unifiée. Les parties complexes telles que la cryptologie, la gestion du réseau distribué et la mécanique des bases de données sont soustraites aux préoccupations des développeurs, laissant ces derniers se concentrer uniquement sur leur application et à l'expérience de l'utilisateur final.

Puisque Daedalus est pensé comme une architecture universelle, sa feuille de route et son évolution sont indépendantes de celle de Cardano. Dans l'année 2017, Daedalus et Cardano étaient intimement liés, mais à terme Cardano ne sera qu'une application parmi d'autres aux yeux d'un utilisateur de Daedalus. Nous prévoyons également d'explorer l'usage des fonctionnalités uniques de Intel SGX, comme le service de gestion universel des clés.

Au final, en tant que concepteurs de protocoles, nous ne pouvons pas prendre en charge tous les besoins existants. Nous espérons que la flexibilité apportée par Daedalus combinée aux contrats d'état présents sur CCL satisfera ceux qui se sentiront laissés pour compte par nos choix de conception. Nous espérons aussi que de meilleurs standards émergeront, de manière à encourager toutes les cryptomonnaies à profiter de l'interopérabilité et de la sécurité.

4. Réglementation / Régulation

4.1 Fausse dichotomie

Aussi impénétrables soient-ils pour le profane, les processus de régulation peuvent néanmoins être vus comme l'histoire sans cesse renouvelée du gendarme et du voleur. Les réglementations sont les outils de la loi et comme tous les outils, ils peuvent être inadéquats ou mal utilisés.

L'apparition des cryptomonnaies n'a en rien changé cet état de fait. Il y aura toujours des escrocs, des mauvais acteurs et des conséquences terribles en dépit des meilleures intentions. Si les cryptomonnaies peuvent se passer du jugement humain, elles ne peuvent en revanche se débarrasser des comportements humains.

Un concepteur de cryptomonnaie doit alors prendre position sur les outils qu'il offrira aux régulateurs et qui permettront de corriger les erreurs éventuelles. En tous cas, cela reste un défi pour les cryptomonnaies précisément parce que ces dernières ont été créées en réponse aux errements passés des processus de réglementaires et de la politique monétaire.

Culturellement, beaucoup de cryptomonnaies considèrent que les gouvernements prennent des décisions corrompues, ineptes ou inefficaces. En conséquence, elles n'ont que peu de patience et de respect pour ces derniers. Elles n'ont aucune envie de donner un accès par portes dérobées aux régulateurs ou aux législateurs pour corriger d'éventuelles erreurs et considèrent que cela serait contraire à leur raison d'être.

D'un autre côté, plus de 10 % des Bitcoin ont été perdus ou volés depuis le lancement du protocole le 3 Janvier 2009 à cause de problèmes survenus sur les plateformes d'échanges et autres évènements historiques. Au 30 Juin 2017, cela représentait un peu plus de 4 milliards de dollars. Et ce chiffre ne prend même pas en compte la valeur en Bitcoin ou autres cryptomonnaies escroquées ou perdues lors d'ICOs[20] mal conçues.

[20] Ndtr : ICO pour ''Initial Coin Offering'', un moyen de lever des fonds

Ensuite vient la question de la vie privée. Vu d'en haut, la valeur circule à travers des canaux spécialisés, régulés, riches en métadonnées et activement surveillés par la police, les gouvernements et les régulateurs internationaux. Il s'agit là d'un jeu bien compris de tous où tricher n'est possible que du côté de l'économie de l'argent liquide et cela tend à décroître à mesure que le monde entier se tourne vers l'informatisation des flux d'argent.

Si les cryptomonnaies n'existaient pas, le paradigme serait celui d'un monde dans lequel les aspects financiers de notre vie privée seraient traités comme du contenu de réseaux sociaux. La vie privée n'existerait tout simplement pas, et personne ne pourrait faire autrement. De là découle un dilemme produisant une apparente dichotomie.

Un concepteur de cryptomonnaie peut en effet abandonner ses principes et se plier aux exigences que pourraient avoir des juridictions locales sur le code informatique, compromettant alors la vie privée des utilisateurs. Ou bien par principe, il peut décider de ne rien céder, suivant ainsi une philosophie plus anarchiste qui se détache des meilleures pratiques actuelles et de la loi.

Nous pensons que cette manière de voir les choses est une fausse dichotomie basée sur un manque d'imagination. La réalité est que la grande majorité des utilisateurs ne sont pas concernés par les règles établies à l'attention des marchés. Ils sont plus attentifs aux changements soudains des règles au bénéfice d'un ou plusieurs acteurs. Ils sont inquiets du manque de transparence relatif aux droits spéciaux et à leurs bénéficiaires.

Nous devons faire la distinction entre droits des individus et droits des marchés. Etant donné que les cryptomonnaies concernent tout le monde, ces droits doivent être les plus centrés possibles sur ceux des utilisateurs.

La protection de la vie privée doit être raisonnable et sous contrôle de l'utilisateur, non pas d'une organisation s'en portant garante. Le flux de valeur ne devrait pas être restreint, et les avoirs ne devraient pas être pouvoir être confisqués sans consentement.

Pour ce qui est des marchés, ils doivent être transparents sur l'utilisation qui est faite des données et sur la manière dont les fonds y sont manipulés. Tout le monde doit y fonctionner en suivant les mêmes règles. De plus, une fois que les utilisateurs ont consentis à ces règles, ils ne peuvent pas changer d'avis pour convenances personnelles. Les autres parties prenantes ont en effet aussi besoin de certitudes.

Mais comment mettre en pratique cette abstraction ? A quoi devrait ressembler quelque chose de pratique qui respecte la loi ? Nous avons construit notre solution en trois volets : les métadonnées, l'identification et la légalité, et les marchés DAOs.

4.2 Métadonnées

Un acte est parfois beaucoup moins intéressant que le contexte dans lequel il se déroule. Par exemple, conduire de Paris à Berlin est un acte. Conduire de Paris à Berlin dans une Ferrari à 250 km/h de vitesse

moyenne est une métadonnée. Assurément, cela n'a pas la même saveur que de faire le même trajet en Toyota Prius à 60 km/h.

Les transactions financières ne sont pas différentes. Leur contexte est extrêmement important pour les économistes, les impôts, la police, les entreprises ou autre entité. Il est assez triste de constater qu'avec notre système basé sur la monnaie *fiat*, la majorité des consommateurs ne réalisent pas à quel point leurs transactions sont riches en métadonnées ni avec qui elles sont partagées.

Pour Cardano, nous reconnaissons que les utilisateurs pourraient avoir besoin - ou être légalement obligés - de partager ces métadonnées de transactions avec certaines autorités. Nous croyons toutefois que cela doit se faire de manière consentie.

Nous pensons aussi que grâce à leur capacité d'audit, l'horodatage et leur immutabilité, les systèmes de blockchain ont le pouvoir d'éliminer la fraude et les abus. En ce sens, certaines métadonnées devraient pouvoir être inscrites sur la blockchain de Cardano.

La recherche du bon équilibre, celui qui ne condamnerait pas notre système à enfler de manière incontrôlée suite à l'intégration de ces données, est la partie la plus délicate. Nous avons choisi une approche pragmatique tenant compte de ces contraintes.

Premièrement, au cours des 12 prochains mois, Daedalus prendra en charge une grande variété de fonctionnalités permettant d'annoter les transactions et autres activités financières. Ces métadonnées pourront être exportées et partagées sur demande par les utilisateurs. De plus, ces données pourront être manipulées par des logiciels tiers remplissant des fonctions particulières comme le calcul de l'impôt.

Deuxièmement, nous explorons la prise en charge d'adresses spéciales qui pourraient inclure des ''hash'' et des champs d'attributs cryptés. Cette structure permettrait aux utilisateurs d'inscrire des métadonnées sur la blockchain sans en révéler le contenu publiquement. Dans l'hypothèse où ils souhaiteraient les partager, ces informations bénéficieraient des garanties d'horodatage, de capacité d'audit et d'immutabilité propres à toutes les transactions d'une blockchain.

Nous avons déjà mis en place ce type d'adresses avec champs d'attributs. Pour l'instant, ce champ est utilisé pour y stocker la version cryptée de la structure d'un porte-clés HD dans le but d'accélérer sa restauration. Les versions suivantes généraliseront cette construction.

4.3 Identification et légalité

La propriété des avoirs et le droit d'effectuer une transaction sont deux choses fortement liées aux transactions elles-mêmes. Vous pourriez en effet avoir assez d'argent pour acheter quelque chose (par exemple de l'alcool) et ne pas pouvoir le faire à cause de restrictions particulières (à cause de votre âge).

La propriétés et l'origine des avoirs sont classiquement le pré-carré des réglementations dites KYC (Know Your Customer – Connaître son client). Lorsqu'une entreprise délivrant des services financiers ouvre un compte pour un client, comme une banque ou une plateforme d'échange, elle demande généralement de connaître un minimum de faits concernant ce client et notamment l'origine de ses avoirs.

Le défi technologique est qu'après ce processus d'envoi de ces informations, l'utilisateur perd toute garantie sur les utilisations futures qui en seront faites, sur les méthodes de stockage (sécurisées ou non) et sur la durée de ce stockage. Ces informations légales ont pourtant une valeur commerciale. Elles pourraient être revendues si le cadre légal le permet ou bien même volées pour commettre des fraudes.

Pour Cardano, nous souhaitons innover autant que possible. Du côté logiciel des protocoles, aucune garantie ne peut malheureusement être donnée sur le comportement de l'entité recevant ce type d'informations. Toutefois, du côté des machines exécutant ces protocoles, l'utilisation de matériel de confiance comme Intel SGX ou tout autre HSM permet de s'assurer que les règles de conduite seront respectées.

C'est pourquoi nous envisageons l'utilisation des « preuves en verre » ou ''Sealed Glass Proofs / SGPs''[21]. Ces dernières permettent en effet de s'assurer qu'un récipiendaire d'informations respectera les règles ayant conditionné leurs transmissions. Nous pensons que des standards de ce type émergeront et que ces méthodes réduiront les risques associés à la perte ou au piratage d'informations sensibles.

De plus, en séparant la tenue du livre de compte (CSL) et la couche des calculs (CCL), Cardano peut aussi profiter de cette approche. Si le CCL est maintenu par une entité régulée (par ex. un casino ou une plateforme d'échanges), des vérifications d'identité ou des taxes sur les gains peuvent ainsi être rendus obligatoires.

En utilisant les SGPs, l'utilisateur peut envoyer des fonds en même temps que des informations permettant son identification sans se soucier de leur diffusion sur internet ou de leur conservation par les nœuds de consensus. De plus le CCL gagnerait la certitude que ses utilisateurs sont identifiés et légitimes.

Ce paradigme permet aussi la portabilité entre entités régulées pour les utilisateurs. Les plateformes d'échanges pourraient ainsi transférer les comptes et crédits pour leurs clients à travers ces canaux sécurisés et aussi – si les règles l'autorisent – à partager ces informations avec les régulateurs.

Nous espérons que notre première version beta de cette technologie sera testée courant 2018 avec une intégration au sein de Cardano à la fin 2018 ou début 2019, en fonction de l'avancée de nos recherches. Ce planning suppose aussi que nous serons capables de collaborer avec ARM et Intel afin qu'ils nous autorisent à exécuter notre code sur leur matériel.

[21] Ndtr : Assurant la destruction de la preuve une fois celle-ci vérifiée

4.4 Place de marché de type DAO

Les deux sections précédentes ont présenté la création et le mouvement d'information en prenant pour principe l'existence d'une organisation gestionnaire. Ces fonctionnalités seront toujours nécessaires afin d'assurer l'interopérabilité avec le système financier traditionnel, toutefois elles ne s'attaquent pas au problème de la régulation gérée par et sur la blockchain.

Les contrats intelligents rendent possibles un système complètement nouveau dans lequel les relations sont déterministes, s'exécutent seules et sont libres de toute ambiguïté. Ces relations peuvent donc être utilisées pour créer des règles applicables aux places de marché et sans limites de complexité, telles que l'arbitrage, les remboursements ou la révélation de faits sous conditions spécifiques.

Nous appelons ces structures construites à partir de contrats intelligents des places de marché DAOs. Elles ne nécessitent pas de protocoles spéciaux ni la capacité de modifier des données au sein du registre distribué. Elles peuvent être entièrement construites à partir d'une collection de contrats intelligents interdépendants.

Les principes fondamentaux consistent en une collection de contrats minimaux[22] ou CMs inspirés de la loi et des meilleures pratiques en vigueur dans le monde des affaires. Ces CMs peuvent être connectés à un autre contrat intelligent développé par quelqu'un d'autre de manière à rendre obligatoire le suivi des règles en vigueur sur une place de marché.

Par exemple, un développeur pourrait décider de créer un jeton ERC20 sur CCL de manière à effectuer une levée de fonds. Une place de marché DAO pourrait exister spécialement pour ce type d'activités avec des conditions d'accès existant sous formes de paramètres. Des fonctions telles que le remboursement, la réallocation des fonds ou le gel des paiements seraient alors directement importées au sein du contrat ERC20 de ce développeur.

Cela nous permet d'avoir une discussion plus globale sur la manière dont une place de marché doit être contrôlée pour assurer la protection du consommateur. Aussi, nous pouvons discuter de la manière de modéliser une transaction afin de prendre en charge automatiquement les protections et les droits de juridictions spécifiques.

En collaboration avec la Fondation Cardano, I.O.H.K et d'autres organisations, le projet Cardano créera à l'attention des développeurs une bibliothèque de CMs de référence pour les places de marché DAOs. Nous espérons que des assurances et des marchés régulés se formeront autour de ces DAOs et qu'ils évolueront par eux-mêmes en fonction des premiers résultats.

5. Durabilité

Une immersion dans le marché de la cryptomonnaie s'accompagne de nombreuses contradictions conceptuelles. Les cryptomonnaies sont conçues pour être difficiles à modifier. Mais, comme toutes

[22] Ndtr : Contrats ou éléments de bases

les technologies, elles doivent évoluer pour tenir compte des défauts de conception initiale et des avancées de la science. Les blockchains visent à empêcher la centralisation, pourtant elles requièrent des acteurs forts afin d'en diriger les changements et de maintenir le code.

Malgré l'accord de la plupart des participants sur l'existence de lacunes évidentes devant être corrigées, le consensus reste difficile à atteindre et les changements aussi. Cela rend l'expérience frustrante.

Le débat sur la taille des blocs du Bitcoin est une question importante depuis plus de deux ans. Chaque jour, des transactions d'un montant global supérieur à un milliard de dollars sont en attente parce que le réseau est à pleine capacité.

Si le changement d'un simple paramètre - même lors de solutions temporaires - ne peut être effectué, alors comment les entreprises et les gouvernements pourraient-ils se sentir à l'aise avec l'idée d'investir des milliards de dollars dans la construction d'infrastructures qui reposeront sur ces systèmes ? Aussi, comment une entreprise peut-elle faire le pari d'intégrer stratégiquement des protocoles irresponsables ne permettant même pas les mise à niveau les plus rationnelles ?

En examinant l'histoire, on constate que l'évolution d'Internet a suivi la même tendance lorsque de simples changements, comme la transition de l'IPv4 à l' IPv6, ont pris des décennies à se réaliser. Pourtant, il existe un fort contraste entre la technologie de la blockchain et celle d'Internet, en ce sens qu'elles protègent les données de façon bien différente.

Internet était un projet militaire issu de la DARPA qui a ensuite rejoint les milieux universitaires, avec un fort soutien du gouvernement et un groupe bien défini de gardiens initiaux. Il s'est développé dans des conditions non commerciales, sans manœuvres d'entreprises influentes et désireuses de monopoliser le réseau. En fait, le commerce électronique viola l'AUP de la ''National Science Foundation'' jusqu'à son abrogation en 1992.

Au moment où les entreprises ont pu s'offrir le luxe de commercialiser Internet, il existait déjà un ensemble solide de normes, de principes et disciples engagés. Cela n'a pas empêché des entreprises comme AOL et Microsoft d'essayer de construire leur système fermé et de créer une technologie propriétaire comme ActiveX. Cela n'a pas non plus empêché les acteurs de la génération suivante, tels que Google, de suivre leur propres agendas, étant donné leurs énormes bases d'utilisateurs et leur capitalisation boursière.

Avec leurs multitudes d'acteurs en quête de rentes, allant des traders aux mineurs, les cryptomonnaies sont les hôtes les plus aboutis de la motivation commerciale. De ce fait, les protecteurs des cryptomonnaies ont évolué en acteurs cherchant à optimiser leur intérêt personnel.

Par exemple, le minage sans validation commence à être plus fréquent car il améliore la marge de profit d'un mineur. Cependant, cela ne tient absolument aucun compte du but et de l'utilité du minage. La centralisation du minage a déjà eu lieu avec une poignée d'opérateurs contrôlant la majorité de la puissance de calcul nécessaire au Bitcoin.

Comme Internet, les cryptomonnaies requièrent un consensus pour changer. Mais quand une telle centralisation rapide du pouvoir entre les mains de quelques courtiers se produit, que se passe-t-il lorsque le changement ne leur convient pas ?

Contrairement à Internet, le lancement de la plupart des cryptomonnaies ne se fait pas de manière désintéressée à partir de ressources non commerciales ou académiques. Dès le départ, certains groupes cherchent à réaliser des gains. De fait, de puissants courtiers sont affectés à la maximisation de ces profits.

La centralisation est donc une réalité à laquelle chaque cryptomonnaie doit faire face dès le début de son existence. Nous ne pouvons pas y échapper entièrement. Cependant, en tant que concepteurs, nous devrions au moins planifier une décentralisation progressive.

En ce qui concerne Cardano, nous avons soigneusement réfléchi aux facteurs qui favorisent la centralisation et aux techniques à appliquer afin d'aider notre protocole à devenir progressivement une infrastructure publique comme le Web.

Nous admettons sans réserve que la décentralisation totale est à la fois impossible et peut-être même contre-productive. Cependant, certaines démarches sont souhaitables afin de produire un système plus équilibré.

C'est un fait que les financements participatifs centralisés des cryptomonnaies permet, dans un premier temps, un développement rapide et flexible du protocole. Ce financement doit toutefois devenir plus diversifié tout en évitant les biais culturels, linguistiques et géographiques. Le rythme de développement doit aussi passer de la frénésie à une allure choisie et systématique.

Deuxièmement, à mesure que la communauté devient plus informée sur la nature même de la technologie de la cryptomonnaie, les décisions concernant la feuille de route ne peuvent plus être réservées qu’aux développeurs initiaux du projet. Il doit y avoir une méthode basée sur la blockchain pour proposer, vérifier et mettre en œuvre les modifications du protocole.

Troisièmement, les mesures incitatives nécessaires au maintien de CSL doivent être directement alignées sur les souhaits de l'ensemble des utilisateurs. Nous ne pouvons pas laisser émerger une cabale de spécialistes qui agiront indépendamment de la volonté de la majorité.

Pour le premier point, nous avons choisi d'intégrer un système de trésorerie à même Cardano. Pour le second, nous allons donc déployer un processus formel et coordonné par CSL lui-même, dont l'objectif sera de recevoir les propositions d'amélioration de Cardano. Enfin, pour le troisième point, nous pensons que Ouroboros fournit une solution élégante.

De nombreux détails supplémentaires pourraient être fournis sur ces sujets abordés ci-dessus, mais cela dépasse le cadre de ce document de réflexion. La conception de ces mécanismes est l'un des champs académiques les plus complexes et les plus interdépendants, qui plus est supporté par une théorie incomplète et n'ayant aucun modèle canonique solide sur lequel s'appuyer.

Et de fait, notre approche axée sur la science et décrite en Section 2 nous sert bien. L'équipe Veritas d'I.O.H.K., en partenariat avec un groupe de chercheurs de l'Université de Lancaster dirigés par le professeur Bingsheng Zhang, développe le modèle de trésorerie de référence pour Cardano. Avec comme objectif une intégration en 2018, nous prévoyons une publication spécifique révisée par des pairs d'ici la fin de 2017.

En ce qui concerne la description formelle et la vérification des modifications apportées au protocole de la cryptomonnaie, ce sujet est le moins bien compris car il nécessite à la fois des notions ontologiques et un mécanisme incitant à une large participation. Peut-être qu'une forme de processus démocratique représentatif pourra émerger ou que l'utilisation de boucles de rétroaction permettront un vote plus rationnel.

Nous nous attendons à ce que les recherches dans ce sens consomment la plus grande partie de la participation officielle d'I.O.H.K. au développement de Cardano. Comme point de départ, nous déploierons aux côtés du modèle de trésorerie de référence plusieurs mécanismes permettant de saisir la notion de consentement. Une étude plus approfondie est nécessaire pour une solution définitive.

Enfin, le professeur Elias Koutsoupia (Université d'Oxford, U.K.) supervise les travaux visant à améliorer les mesures incitatives pour l'utilisation d'Ouroboros. Une fois les bases cryptographiques d'Ouroboros consolidées ainsi que les travaux requis de mise à l'échelle, une étude plus large des obligations, des pénalités et des mesures d'incitation exotiques sera ajoutée au protocole de référence.

6. Conclusion

Une cryptomonnaie est plus que la somme de ses protocoles, de ses codes source et utilités. En fin de compte, il s'agit d'un système social qui inspire, offre de nouvelles capacités aux gens et les connecte. Frustrés par les nombreuses demi-mesures, échecs et promesses non tenues des protocoles antérieurs, nous avons entrepris de faire mieux.

Ce processus n'est pas simple et nous n'avons non plus jamais cru qu'il puisse prendre fin un jour. Les protocoles sociaux changent indéfiniment, à mesure que les personnes et la société changent eux-mêmes. Nous voulons utiliser la puissance de cette évolution et la transférer dans Cardano.

L'évolution n'est pas guidée par une main ou par un grand dessein. Elle est le résultat d'un heureux hasard, une suite sans fin d'erreurs et de problèmes. Cardano cherche à être l'incarnation numérique de ce processus — suffisamment mûr pour pouvoir survivre aux marchés d'aujourd'hui tout en étant capable d'évoluer afin de répondre aux besoins futurs.

Les sections précédentes décrivent brièvement comment nous nous rapprochons de cet objectif. Nous avons diligemment essayé de reconnaître les biais cognitifs, d'apprendre de l'histoire et de suivre un processus rigoureux. Nous avons essayé d'équilibrer le besoin d'un développement rapide avec l'utilisation de méthodes formelles lesquelles, traditionnellement, en ralentissent le rythme.

Ce fut un privilège extraordinaire de s'engager dans ce projet grandiose. Au cours des deux dernières années, nous avons déjà développé un protocole de preuve d'enjeu fiable et sûr. Nous avons aussi recruté une petite armée de développeurs en langage Haskell et fait du développement de Cardano la préoccupation de nombreux scientifiques de talent.

Alors que nous passons du laboratoire à un système déployé en milieu non contrôlé, il y aura de nombreux problèmes. Cependant et si Cardano était Homme, nous espérons que son avenir pourra se comparer simplement à celui d'un jeune rêveur ou rêveuse pragmatique qui apprend de ses aînés, est un(e) bon(ne) citoyen(ne) dans sa communauté et trouve toujours un moyen de payer ses factures.

Nous ne pouvons connaître l'avenir, mais nous sommes heureux d'essayer de le rendre meilleur pour tous.

Merci d'avoir lu.

Charles Hoskinson, 2015

Traducteurs
Section 1 à 4 : Malick Mbengue - Twitter @psychomb - Telegram @Panshir_Lion
Section 5 et 6 : Claude Cormier - Telegram @cryptoactifs