La Comptabilité en partie triple

(Travail en cours)

Ian Grigg

Systemics, Inc.

2005

Résumé

Le reçu signé numériquement, une innovation de la cryptographie financière, présente un défi à la comptabilité classique en partie double (à double entrée). Plutôt que de concurrencer, les deux étant fusionnés forment un système plus solide. L'extension de l'utilisation de la comptabilité dans le domaine plus large de la trésorerie numérique donne trois entrées locales pour chacun des trois rôles dont le résultat j'appelle la comptabilisation en partie triple. Ce système crée des systèmes de comptabilité à l'épreuve des balles pour les utilisations et les utilisateurs agressifs. En outre, Il permet non seulement de réduire les coûts en fournissant une comptabilité fiable et soutenue, mais aussi de renforcer la gouvernance d'une manière qui influe positivement sur les besoins futurs de la comptabilité ministérielle et publique.

Introduction

Ce document rassemble des innovations de cryptographie financière telles que le reçu signé avec les techniques de comptabilité standard de la comptabilité à double entrée. La première section présente un bref document d'information pour expliquer l'importance de la comptabilité en double partie. Il s'adresse au technologue, et les professionnels de la comptabilité pourraient passer cette étape. La deuxième section explique comment se présente le reçu signé et pourquoi il remet en question la tenue de livres à double entrée. La troisième section intègre les deux ensemble et la conclusion tente de prévoir des ramifications plus larges en ce qui concerne les questions de gouvernance.

Les mérites

Ce document a bénéficié des commentaires de Graeme Burnett et de Todd Boyle [BC].

Un très bref historique de la comptabilité

La comptabilité ou la pratique comptable est de nos jours pensé pour remonter à la genèse de l'écriture; les textes les plus tôt découverts ont été déchiffrés comme des listes simples des comptes des animaux et des stocks de nourriture. Les Sumériens de Mésopotamie, il y a environ 5000 ans, ont utilisé des marques cunéiformes ou en forme de coin comme forme de de nombre de la base 60 dont nous nous souvenons encore comme secondes et minutes, et au carré, comme les degrés dans un cercle. Les mathématiques et l'écriture eux-mêmes peuvent bien avoir été dérivé de la nécessité d'ajouter, soustraire et en effet tenir compte des actifs de base et des stocks de la société primitive.

Entrée unique

La comptabilité à entrée unique est la façon dont « tout le monde » ferait la comptabilité : démarrer une liste, et ajouter des entrées qui décrivent chaque actif. Un arrangement plus avancé serait de créer de nombreuses listes. Chaque liste ou « livre » représenterait une catégorie, et chaque inscription enregistrerait une date, un montant et peut-être un commentaire. Pour déplacer un actif, on le raye d'une liste et on l'inscrit sur une autre liste. Très simple, mais c'était une méthode qui était lourde avec le potentiel d'erreurs. Pire encore, les erreurs pourraient être accidentelles et difficiles à retrouver et à réparer, ou elles pourraient être frauduleuses. Comme chaque inscription ou chaque liste était distincte, rien n'empêchait un mauvais employé de simplement ajouter de l'information à la liste; même s'il était découvert qu'il n'y avait rien à dire quant à savoir s'il s'agissait d'une erreur de bonne foi ou d'une fraude. La comptabilité fondée sur la comptabilité à entrée unique impose une limite importante à la confiance dans les livres. Il est probable que seuls les membres de la famille du propriétaire ou, dans un passé lointain, ses esclaves pouvaient être confiés aux livres de l'entreprise, ce qui a entraîné une influence favorable sur les familles élargies ou l'esclavage en tant qu'entreprises économiques.

Double entrée

La comptabilité en partie double ajoute une propriété importante supplémentaire au système comptable, celle d'une stratégie claire pour identifier les erreurs et les supprimer. Mieux encore, il a un effet secondaire d'erreurs clairement pare-feu que soit accident ou fraude. Cette propriété est activée au moyen de trois caractéristiques, soit la séparation de

tous les livres en deux groupes ou côtés, appelés *actifs* et *passifs*, la redondance des *doubles entrées* avec chaque entrée ayant une correspondance de l'autre côté, et *l'équation du bilan*, qui dit que la somme de toutes les entrées du côté actif doit être égale à la somme de toutes les entrées du côté passif. Une entrée correcte doit faire référence à sa contrepartie, et sa contrepartie doit exister de l'autre côté. Une entrée par erreur peut avoir été créée pour des raisons peut-être frauduleuses, mais pour être correcte au niveau local, elle doit se référer à son portefeuille de contrepartie. Sinon, il peut tout simplement être éliminé comme une entrée incomplète. S'il se réfère, l'existence de l'autre entrée peut être facilement confirmée, voire recréée en fonction de son sens, et la boucle est ainsi fermée. Auparavant, dans les livres à entrée unique, le fraudeur ajoutait simplement son montant à une colonne de choix. Dans les livres à double entrée, ce montant doit venir de quelque part. S'il vient de nulle part, il est éliminé ci-dessus comme une erreur accidentelle, et s'il vient de quelque part en particulier, cet endroit est identifié. De cette façon, la fraude laisse une trace et son but est révélé dans l'autre livre parce que la valeur tirée de ce livre doit aussi provenir de quelque part. Cela mène ensuite à une stratégie de vérification. Premièrement, assurez-vous que toutes les entrées sont complètes, en ce sens qu'elles renvoient à leur homologue. Deuxièmement, veiller à ce que tous les mouvements de valeur aient un sens. Cette stratégie simple a créé un registre des transactions qui a permis à la comptabilité d'une entreprise de se produire, sans facilement cacher des fraudes dans les livres eux-mêmes.

Qui est arrivé en premier - la double entrée ou l'entreprise?

La comptabilité en partie double est l'une des plus grandes découvertes du commerce et son importance est difficile à surestimer. Les historiens pensent qu'il a été inventé autour des années 1300 après JC, bien qu'il y ait des suggestions qu'il existait sous une forme ou une autre aussi loin que l'empire grec. La première preuve forte est un 1494 traité sur les mathématiques par le frère vénitien Luca Pacioli [LP]. Dans son traité, Pacioli a documenté de nombreuses techniques standard, y compris un chapitre sur la comptabilité. Il devait devenir le texte de base de la comptabilité à double entrée pendant de nombreuses années. La comptabilité à double entrée est née de concert avec l'émergence de formes modernes d'entreprise comme pionnier par les marchands vénitiens. Les historiens ont débattu si la double entrée a été inventé pour soutenir les demandes considérablement accrues des nouvelles entreprises alors en cours entourant l'expansion des états de ville tels que Venise ou si la double entrée a été un catalyseur de cette expansion. Nos expériences jouent en faveur de l'habilitation. Je parle de l'expérience des émetteurs de monnaie numérique. Notre premier déploiement d'un système était un système de comptabilité à entrée unique. Même si le codage était serré, son taux d'échec était tel qu'il ne pouvait soutenir plus de vingt comptes avant que des erreurs de comptabilité ne s'introduisent et que le système perde de la cohésion. Cela s'est produit dans les semaines suivant les essais initiaux et n'a jamais pu être mis en service. Le système à double entrée de remplacement a été mis en

service au début de 1996 et n'a jamais perdu une transaction (bien qu'il y ait eu quelques coupes serrées [IG1]). De même, la société néerlandaise Digicash BV a introduit un système d'encaisse numérique dans une banque aux États-Unis. Pendant sa période de test, le système de comptabilité à entrée unique original a dû être remplacé par un système en partie double pour la même raison - les erreurs s'y sont glissées et ont rendu la comptabilité sous le système de trésorerie numérique peu fiable. Un autre grand système de monnaie numérique a duré de nombreuses années sur un système de comptabilité à entrée unique. Pourtant, la société savait qu'il fonctionnait en dépendant sur la chance. Quand un pirate a réussi à trouver une faille dans le système, une attaque du jour au lendemain a permis la création de plusieurs millions de dollars de valeur. Comme il ne s'agissait pas seulement de la question contractuelle de la valeur à ce jour, elle a entraîné des contorsions dramatiques du bilan, notamment en le mettant en violation de son contrat d'utilisation et en grand risque d'une « gestion bancaire ». Heureusement, le cracker a déposé la valeur créée dans le compte d'un jeu en ligne qui a échoué peu de temps après, donc la valeur a pu être neutralisée et blanchie monétairement, sans divulgation et sans scandale. De l'avis de cet auteur au moins, la comptabilité à entrée unique est incapable de soutenir une entreprise plus sophistiquée qu'un ménage. Compte tenu de cela, je suggère que l'évolution des entreprises complexes a nécessité une double entrée en tant que facilitateur.

Calcul de la double entrée en temps rapide

Double Entry a toujours été le fondement des systèmes comptables pour les ordinateurs. La capacité de détecter, classer et corriger les erreurs est encore plus importante pour les ordinateurs que pour les humains . Et comme il n'y a pas de luxe d'intervention humaine, la distance entre l'utilisateur et les bits et octets est beaucoup plus grande que la distance entre le comptable et les marques d'encre sur ses livres. Comment la double entrée est mise en œuvre est un sujet en soi. L'informatique introduit des concepts tels que tels que les transactions, qui sont définies comme des unités de travail qui sont atomiques, cohérentes, isolées et durables (ou ACID pour faire court). La question fondamentale pour les informaticiens est de savoir comment ajouter une entrée du côté des actifs, puis ajouter une entrée du côté des passifs, et ne pas planter à mi-chemin dans cette séquence. Ou pire encore, commencez une autre transaction à mi-chemin. Cela a plus de sens lorsqu'on le considère dans le contexte des millions d'entrées qu'un ordinateur pourrait gérer et une très petite chance que quelque chose se passe mal ; finalement, quelque chose se passe et les ordinateurs ne peuvent pas gérer les erreurs de cette nature très bien. Pour la plupart, ces concepts se réduisent simplement à "comment mettre en œuvre la comptabilité en partie double " ? Comme cette question est bien répondue dans la littérature, nous nous contentons seulement de la mentionner.

Un historique légèrement moins bref du reçu signé

Les progrès récents de la cryptographie financière ont remis en question le concept de comptabilité en partie double. La signature numérique est capable de créer un enregistrement avec un certain degré de fiabilité, au moins dans les sens exprimés par ACID ci-dessus. On peut se fier à une signature numérique pour garder un document en lieu sûr, car elle ne permettra pas de vérifier si les détails du dossier sont modifiés. Si nous pouvons supposer que le dossier a été créé correctement, alors des erreurs ultérieures sont révélées, à la fois de nature accidentelle et d'intention frauduleuse. (Les ordinateurs font très rarement des erreurs accidentelles, et lorsqu'ils le font, ils le font normalement d'une manière maladroite plus proche de l'encrier qui est renversé que quelques chiffres.) De cette façon, tout changement apporté à un document qui a un sens comptable ou sémantique est presque certainement une tentative de fraude, et une signature numérique le rend évident.

Signature et encaisse numériques

Une signature numérique nous donne une propriété particulière à savoir :

« À un moment donné, cette information a été vue et marquée par l'ordinateur de signature. »

Il existe plusieurs variantes avec des revendications plus douces , et plus difficiles à cette propriété. Par exemple, les *condensés de messages* avec *enchevêtrement* forment une forme simple et efficace de la signature, et les *crypto-systèmes à clé publique* fournissent un autre formulaire où les signataires détiennent une clé privée et les vérificateurs détiennent une clé publique [MB]. Il existe également de nombreuses façons d'attaquer la propriété de base. Dans cet essai, j'évite les comparaisons et suppose la propriété de base comme une marque fiable d'avoir été vu par un ordinateur à un moment donné dans le temps. Les signatures numériques représentent alors une nouvelle façon de créer des entrées fiables , et dignes de confiance qui peuvent être construites dans les systèmes comptables. Dans un premier temps, il a été suggéré qu'une variante connue sous le nom de *signature aveuglée* permettrait l'argent numérique [DC]. Ensuite, les *certificats* circuleraient en tant que droits ou contrats, de la même manière que les certificats d'actions des anciens et remplaceraient ainsi les systèmes comptables centralisés [RAH]. Ces idées ont pris la cryptographie financière une partie du chemin vers là-bas. Bien qu'ils aient montré comment vérifier fortement chaque transaction, ils ont évité de placer la signature numérique dans un cadre global de comptabilité et de gouvernance. Une étape nécessaire servait à ajouter la redondance implicite dans la comptabilité à double saisie afin de protéger à la fois les agents transactionnels et les opérateurs de système contre la fraude.

Le rôle initial d'un reçu

Les conceptions qui découlent des caractéristiques d'Internet, des capacités de la cryptographie et des besoins de la gouvernance ont mené à l'élaboration du *reçu signé* [GH].Pour développer ce concept, supposons un simple système de paiement à trois parties dans lequel chaque partie détient une clé d'autorisation qui peut être utilisée pour signer ses instructions. Nous appelons ces joueurs *Alice*, *Bob* (deux utilisateurs) et Ivan (l'émetteur) pour plus de commodité. Quand Alice souhaite transférer la valeur à Bob dans une unité ou un contrat géré par Ivan, Elle rédige les instructions de paiement et les signe numériquement, tout comme un chèque est traité dans le monde physique. Elle envoie ça au serveur, Ivan, et il est probablement d'accord et fait le transfert dans ses livres internes. Il émet ensuite un reçu et le signe avec sa clé de signature. Comme partie importante du protocole, Ivan remet ensuite de façon fiable le reçu signé à Alice et à Bob, et ils peuvent mettre à jour leurs livres internes en conséquence.

1: Un reçu provisoire

De: Alice

À : Bob

Unité : Euro

Quantité : 100

Date : 2005.12.25

Signature numérique

Le reçu *est* l'opération

Notre concept de valeur numérique visait à éliminer le plus de risques possible . Cela découle simplement de l'une des exigences de haut niveau, celle d'être extrêmement efficace à l'émission de valeur. L'efficacité de l'émission numérique est principalement une fonction des coûts de soutien, et les coûts de la fraude et du vol sont un facteur déterminant des coûts de soutien. L'un des risques qui a systématiquement balayé toute conception de valeur numérique efficace à un coût raisonnable était le risque de *fraude interne*. Dans notre modèle de nombreux utilisateurs et d'un serveur centralisé unique, les émetteurs de l'unité

de valeur numérique (en tant que signataire du contrat) , et tous les partenaires de gouvernance tels que les opérateurs de serveur sont des candidats puissants pour la fraude interne. Les événements des dernières années, comme les scandales des fonds communs de placement et des stocks, sont des cas canoniques de risques que nous avons décidé de traiter. Afin de contrer le risque de fraude d'initié, le reçu écrit a toujours été présenté comme une source principale de preuves. Généralement oublié par le public acheteur ces jours-ci, le but d'un reçu écrit dans le commerce de détail normal n'est pas de permettre les retours et les plaintes par le client, mais plutôt pour l'engager dans un protocole de documentation qui lie le vendeur à la garde de l'argent. Un bon client remarquera la fraude par le commerçant et avertira le propriétaire de surveiller les sommes identifiées par le reçu ; la même histoire s'applique à l'invention de la caisse ou du registre qui n'était à l'origine qu'une boîte séparant les recettes du propriétaire des fonds dans les poches du préposé. Nous étendons ce motif principal dans le monde numérique en utilisant un reçu signé pour lier l'émetteur dans un protocole de gouvernance avec les utilisateurs. Nous allons également plus loin. Tout d'abord, pour parvenir à un engagement complet, l'autorisation initiale d'Alice est également incluse dans le dossier. Le reçu comprend alors toutes les preuves de l'intention de l'utilisateur et de l'action du serveur en réponse, et il devient maintenant *un enregistrement dominant* de l'événement. Cela signifie que la stratégie de tenue des dossiers la plus efficace consiste à laisser tomber tous les dossiers antérieurs et à garder en lieu sûr le reçu signé.

Cette domination affecte à la fois l'émetteur et l'utilisateur, et nous permet d'énoncer le principe suivant :

L'Utilisateur et l'émetteur détiennent les mêmes informations.

Comme le reçu signé est remis par l'émetteur aux deux utilisateurs, les trois parties détiennent le même dossier dominant pour chaque événement. Cela réduit les coûts de soutien en réduisant considérablement les problèmes causés par les différences d'information. Deuxièmement, nous relions un contrat d'émission signé connu sous le nom d'un *Contrat Ricardien* au reçu [IG2]. Cette invention établit un lien entre un document signé numériquement et le reçu signé au moyen d'un identificateur unique appelé *un condensé de messages* encore fourni par la cryptographie. Il prévoit des obligations fermes pour l'unité de compte, la nature de l'émission, les modalités, les conditions et les promesses faites par l'émetteur , et bien sûr l'identité de l'émetteur.

Enfin, grâce à ces mesures habilitantes, nous pouvons maintenant introduire le principe suivant :

Le reçu est la transaction.

Dans l'enregistrement complet du reçu signé, l'intention de l'utilisateur est exprimée et entièrement confirmée par la réponse du serveur. 800Les deux sont couvertes par des

signatures numériques qui verrouillent ces données. Un examinateur comme un vérificateur peut confirmer les deux ensembles de données et vérifier les signatures.

De: Alice

À : Bob

Unité : Euro

Qté : 100

Com : Stylos

Sign d'Alice

Chèque

De

l'utilisateur

De : Alice

À : Bob

Unité : Euro

Quantité : 100

Date : 2005.04.10

Signature d'Ivan

2 : Un reçu signé

Le reçu signé comme système de tenue de livres

Le principe du Reçu en tant que Transaction est devenu sacro-saint au fil du temps. Dans notre logiciel client, le principe a été intégré à la conception de façon constante, ce qui a permis de simplifier le régime comptable et d'offrir une grande fiabilité. Des problèmes subsistent, comme la perte de reçus et le comptage des soldes par le logiciel-client propriétaire, mais ceux-ci deviennent raisonnablement traitables une fois que l'objectif des reçus comme transactions est placé au premier plan dans l'esprit du concepteur.

En tant qu'entrée unique

Afin de calculer les soldes sur un jeu de reçus connexe, ou de présenter un historique de transaction, un livre serait construit à la volée à partir de l'ensemble. Celà revient à utiliser le reçu signé comme base pour la tenue de livres à entrée unique. En fait, la tenue de livres est fondée sur les recettes brutes, ce qui soulève la question de savoir s'il faut maintenir les livres en place. Les principes des bases de données relationnelles fournissent ici une orientation. La quatrième forme normale exige que nous stockions les documents primaires, dans ce cas l'ensemble des reçus et nous construisons des documents dérivés et les livres comptables à la volée [4NF].

Récupération de la double entrée

Des problèmes similaires se posent pour Ivan l'émetteur. Le serveur doit accepter chaque nouvelle transaction sur la base du solde disponible dans les livres en vigueur; pour cette raison, Ivan a besoin de ces livres pour être disponible efficacement. En raison du plus grand nombre de reçus et de livres (un pour chaque compte d'utilisateur) , les recettes et les livres ont tendance à exister, contrairement à la quatrième forme normale. Une fusion entre des ensembles de recettes relationnellement solides et des livres à double entrée vient aider ici. Alice et Bob reçoivent chacun un livre dans l'architecture du serveur. Comme d'habitude, nous plaçons ces livres du côté du passif. Les recettes peuvent alors être placées dans un seul livre distinct, ce qui pourrait logiquement être placé du côté de l'actif. Chaque transaction d'Alice à Bob a maintenant une contre-entrée logique, et est ensuite représentée à trois endroits dans les comptes du serveur. Pourtant, le côté actif demeure en quatrième position normale à mesure que les écritures de passif sont dérivées, chaque paire provenant d'une entrée du côté actif. Par extension, un agent logiciel plus sophistiqué côté client, travaillant pour Alice ou Bob, pourrait employer les mêmes techniques. À cet extrême, les entrées sont maintenant en place à trois endroits distincts, et chacune contient potentiellement trois enregistrements.

Comptabilité en partie triple Le reçu signé numériquement, avec toute l'autorisation d'une transaction, représente un défi de taille pour la comptabilité en partie double au moins au niveau conceptuel. L'invention cryptographique de la signature numérique donne une force probante puissante à la réception, et en pratique réduit le problème de comptabilité à l'un de la présence de la réception ou son absence. Ce problème est résolu en partageant les enregistrements - chacun des agents a une bonne copie. Dans un sens strict de la théorie des bases de données relationnelles, la comptabilité à double entrée est désormais redondante ; elle est normalisée par la quatrième forme normale. Pourtant, il s'agit plus d'un énoncé de théorie que de pratique, et dans les systèmes logiciels que nous avons construits, les deux restent ensemble, travaillant la plupart du temps main dans la main. Ce qui conduit à des paires d'entrées doubles reliées par la liste centrale des reçus ; trois entrées pour chaque transaction. Non seulement chaque agent comptable est conduit à tenir trois entrées, mais les rôles naturels d'une transaction sont de trois parties, conduisant à trois entrées par trois. Nous appelons cela la comptabilité à trois entrées. Bien que le reçu signé numériquement domine en termes d'information, en termes de traitement, il est insuffisant. La comptabilité à entrée double comble l'écart de traitement, et donc les deux fonctionneront mieux ensemble que séparément. En ce sens, notre terme de *comptabilité à triple entrée* recommande un progrès en comptabilité, plutôt qu'une révolution.

Considérations relatives au logiciel

La disposition précise des entrées en termes de logiciels et de données n'est pas réglée, et peut finalement devenir l'un de ces *problèmes de mise en œuvre* éphémère. Les recettes signées peuvent constituer un compte de contrepartie côté actif naturel, ou elles peuvent

constituer une liste distincte hors livre relevant du système de tenue de livres et de ses deux côtés. Des problèmes de vérification surviennent lorsque la construction des livres découle des reçus, et des problèmes de normalisation surviennent lorsqu'un reçu est perdu. Ce sont des questions pour la recherche future. De même, il convient de préciser que la technique de signature des reçus fonctionne à la fois avec des signatures de clé privée et aussi avec des signatures de condensé de messages enchevêtrés ; si les aspects de sécurité de ces techniques est adéquate à la tâche ou pas, cela dépend de l'environnement commercial.

Les rôles des agents

Il sera à noter que la conception ci-dessus de la comptabilité en partie triple a supposé qu'Alice et Bob étaient des agents d'une certaine indépendance. Cela a été rendu possible et reflète l'utilisation du système comme un système de trésorerie numérique, et non comme un système de comptabilité classique. Loin de réduire la pertinence de ce travail pour la profession comptable, il introduit l'argent numérique comme alternative à la comptabilité d'entreprise. Si un système comptable pour une société ou une autre entité administrative est refondu en tant que système de trésorerie numérique ou monnaie interne, alors l'expérience montre que les avantages reviennent à l'organisation. Bien que le noyau du système ressemble exactement à un système comptable, les livres de chaque ministère sont poussés dehors comme des comptes d'argent numérique. Les ministères ne travaillent plus tant avec les budgets qu'avec leur propre argent. Le contrôle fondamental de la gouvernance est toujours exercé au sein du service de la comptabilité en raison de leur fonctionnement du système, et de la portée limitée de l'argent comme étant uniquement utilisable au sein de l'organisation; le service comptable pourrait intervenir en tant que *teneur de marché*, échangeant des paiements en monnaie interne contre des paiements en monnaie externe à des fournisseurs extérieurs. Nous avons utilisé ce système à petite échelle. Plutôt que d'être inefficace à une aussi petite échelle, le système a généré des économies considérables en matière de coordination. Les factures et les salaires ne sont plus payés à l'aide de fonds conventionnels; de nombreuses transactions sont traitées par des transferts de fonds internes et à la périphérie de la société , et les agents formels et informels travaillent à *l'échange* entre l'argent interne et l'argent externe. La paperasse diminue considérablement, car les dossiers du système monétaire sont suffisamment fiables pour résoudre rapidement les questions, même des années après l'événement. Les innovations présentes dans la monnaie interne vont au-delà du présent document, mais il suffit de dire qu'ils répondent à la question évidente de savoir pourquoi cette conception de la triple comptabilité d'entrée est née du monde de la trésorerie numérique, et a relégué dans le monde des entreprises. Les innovations présentes dans la monnaie interne vont au-delà du présent document, mais il suffit de dire qu'ils répondent à la question évidente de savoir pourquoi cette conception de la comptabilité en triple partie est née du monde de la trésorerie numérique, et a de nouveau pertinence avec le monde des entreprises.

La structure du commerce

Todd Boyle a examiné un problème similaire du point de vue des besoins des petites entreprises à l'ère de l'Internet et en est arrivé à la même conclusion - la comptabilité à triple entrée [1]. Ses prémisses de départ étaient les suivantes :

1. Le besoin majeur n'est pas la comptabilité ou les paiements en soi, mais les schémas d'échange - les schémas complexes du commerce;

2-Les petites entreprises ne pouvaient pas se permettre d'avoir de grands systèmes complexes qui comprenaient ces tendances;

3-Ils ne s'enfermeraient pas dans des cadres exclusifs;

À partir de ces fondations, Boyle a conclu que, par conséquent, ce qu'il faut, c'est un dépôt à accès partagé qui offre un accès sans lien de dépendance. Fondamentalement, ce référentiel est proche du grand livre comptable classique à double entrée des lignes de transaction ("GLT" pour General Ledger – Transactions ou opérations du grand livre général) mais ses entrées sont dynamiques et partagées. Des exemples simples aideront. Quand Alice fait une transaction, elle la saisit dans son logiciel. Chaque transaction (GLT) nécessite de nommer sa contrepartie externe, Bob. Lorsqu'elle affiche la transaction, son logiciel la stocke dans sa (GLT) locale et la soumet également à la (GLT) du service de dépôt partagé. Le dépôt partagé des transactions (« DOD ») transmet ensuite la transaction à Bob. On s'attend maintenant à ce que Bob et Alice stockent la poignée de la transaction sous forme d'index ou de talon, et la (DOD) stocke alors la transaction entière. Les idées de Boyle sont logiquement comparables à celles de Grigg et Howland, bien qu'elles proviennent de directions différentes (la (DOD) est Ivan de Grigg, ci-dessus) et ne soient pas totalement équivalentes. Là où ces derniers se limitaient aux paiements, à l'exactitude des montants et à la protection par des enveloppes cryptographiques dures, Boyle a examiné les tendances plus larges des transactions et a montré que la (DOD) pouvait les traiter, si les données de base partagées pouvaient être extraites et transformées en un seul document partagé. Boyle a mis l'accent sur la substance économique de la transaction.

Prolongation de l'humble facture

Imaginez une simple procédure de facturation. Alice crée une facture et la poste sur son logiciel (GLT). Comme elle l'a nommé Bob, le GLT le poste automatiquement à Ivan, le STR, et il le transmet à Bob. À ce stade, Bob a une décision à prendre, à accepter ou à rejeter. En supposant l'acceptation, son logiciel peut alors répondre en envoyant un message d'acceptation à Ivan. Le DOD assemble maintenant un enregistrement de facture accepté pour remplacer le précédent enregistrement de facture spéculative et affiche les trois voies.

Tendances des transactions

Un logiciel pourrait être écrit pour faciliter et surveiller ce flux et des flux similaires. Si le système de paiement est suffisamment flexible et intégré aux besoins des utilisateurs, il est

possible de fusionner la facture ci-dessus avec le paiement lui-même, au niveau des recettes. Vu sous cet angle, le reçu signé de Ricardo est tout simplement le motif le plus petit et le plus simple de l'ensemble plus général de motifs. Nous pourrions alors suggérer que le principe étroit de *La réception est que la transaction* pourrait être étendue *dans La facture est la transaction*. Une transaction particulière dans le monde des affaires n'est presque jamais isolée. Elle est structurée. Par exemple, les offres et les acceptations constituent une transaction plus vaste, mais elles encapsulent rarement l'ensemble du cycle d'exécution et de paiement. Même s'il y a eu un paiement accompagnant un message de bon de commande, le client attend l'exécution. Il existe un vaste corpus scientifique et littéraire autour de *ces schémas de transactions*. Ceux-ci ont été adoptés par le groupe de travail Business Process d'ebXML et d'autres organismes de normalisation, où ils sont appelés "transactions commerciales." Où cependant le présent travail se distingue est en décomposant ces transactions en éléments atomiques. C'est à cela que nous nous tournons maintenant.

Les exigences de la comptabilité en partie triple

La mise en œuvre de la comptabilité en partie triple évoluera avec le temps pour soutenir les tendances des transactions. Ce qui est devenu clair, c'est que la partie double ne soutient pas suffisamment ces tendances, car il s'agit d'un cadre qui tombe en panne dès que le nombre de partis dépasse un. Pourtant, même si la partie double est "cassée" sur le net et incapable de soutenir les demandes commerciales, la partie triple n'est pas largement comprise, ni les exigences d'infrastructure qu'elle impose sont bien reconnues.

Voici la liste des exigences que nous jugeons importantes [2] [3].

1. **Force du pseudonymat, Au moins.** Comme il y a de nombreux cycles dans les modèles, le système doit soutenir une relation claire des participants. Au minimum cela nécessite une architecture nyme de la nature de Ricardo ou AADS. (Cette exigence est très claire, mais l'espace empêche toute discussion de celui-ci.)

2. **Signature des entrées.** Afin de neutraliser les menaces qui pèsent sur les parties et par celles-ci, un mécanisme qui gèle et confirme les données de base est nécessaire. Il s'agit d'une signature, et nous exigeons que toutes les entrées soient capables de porter des signatures numériques (voir 1, ci-dessus, qui suggère des signatures de clé publique).

3. **La transmission de messages.** Le système est fondamentalement une transmission de messages, contrairement à une grande partie de l'architecture de connexion du réseau. Boyle a reconnu très tôt qu'une composante critique était la nature générique du message qui passe et Systemics l'a proposé et l'a intégré à Ricardo au cours de la période 2001-2004 [4].

4. **Élargissement et migration des entrées**. Chaque nouvelle version d'un message qui arrive représente une entrée qui doit être mise à jour ou ajoutée. Comme chaque message ajoute à une conversation précédente, l'entrée stockée doit agrandir et absorber les nouvelles informations, tout en préservant les autres propriétés.

5. **Stockage des entrées locales et rapports.** L'enregistrement persistant et la disponibilité réactive des entrées. Dans la pratique, il s'agit du grand livre général comptable classique, au moins en termes de stockage. Il doit se plier quelque peu pour gérer des entrées beaucoup plus flexibles, et ses capacités de rapport deviennent plus essentielles à mesure qu'ils procèdent à une réconciliation interne sur demande ou en direct**.**

6. **Paiements obligatoires intégrés.** Le commerce ne peut être aussi efficace que le paiement. Cela signifie que le paiement doit être au moins aussi efficace que toute autre partie; ce qui, en pratique, signifie qu'un système de paiement devrait être intégré au niveau de l'infrastructure. C.f., Ricardo.

7. **Messagerie intégrée au niveau de l'application.** Contrairement aux messages des niveaux inférieurs du protocole (1 ci-dessus), Alice et Bob doivent être en mesure de communiquer. C'est parce que la grande majorité des modèles tourne autour des communications de base des agents. Il ne sert à rien d'établir un meilleur mécanisme de paiement et de facturation que les moyens de communication et de négociation. Ce concept est peut-être mieux vu dans le système SWIFT qui est un système de messagerie, d'abord et avant tout, pour livrer des instructions pour les paiements.

La Conclusion

La comptabilité en partie double fournit des preuves de l'intention et de l'origine, ce qui mène à des stratégies pour faire face aux erreurs d'accident et de fraude. L'invention de la cryptographie financière du reçu signé offre les mêmes avantages, et défie ainsi le règne de 800 ans de partie double. En effet, en termes de preuve, le reçu signé est plus puissant que les enregistrements à double entrée en raison des qualités techniques de sa signature. Il reste quelques faiblesses dans la comparaison stricte avec la comptabilité à double entrée. Tout d'abord, dans l'instanciation Ricardo de la comptabilisation à triple entrée, les reçus eux-mêmes peuvent être perdus ou supprimés, et pour cette raison nous insistons sur le principe que *la saisie est la transaction.* Il en résulte trois agents actifs qui sont chargés de sécuriser l'inscription signée comme leur dossier de transaction le plus important. Deuxièmement, les ramifications logicielles du système à trois entrées sont moins

pratiques que celles offertes par la comptabilité à deux entrées. Pour cette raison, nous étendons l'information contenue dans le reçu dans un ensemble de livres à double entrée ; de cette façon , nous avons le meilleur des deux mondes sur chaque nœud : le pouvoir probatoire des entrées signées et le pouvoir de vérification croisée pratique et locale du concept de double entrée. Ces deux impératifs ont fusionné les reçus signés et la comptabilité à double entrée. Comme nous nous retrouvons avec un arrangement logique de trois par trois entrées, nous pensons que le terme de comptabilité triple entrée est utile pour décrire l'avance sur l'ancien formulaire. Ces deux impératifs ont fusionné les reçus signés et la comptabilité à double entrée. Comme nous nous retrouvons avec un arrangement logique de trois par trois entrées, nous pensons que le terme de *comptabilité en partie triple* est utile pour décrire l'avance sur l'ancien formulaire.

Le financement des agents

Pour profiter pleinement de la comptabilité à entrées multiples, nous devons étendre les systèmes comptables aux agents et leur offrir des capacités directes pour effectuer des transactions, c'est-à-dire que nous faisons participer les agents en leur donnant des fonds internes [5]. L'utilisation de l'argent numérique pour faire des comptes d'entreprise permet d'utiliser ce concept comme un remplacement général pour la comptabilité à l'aide des livres et des budgets ministériels, et est un facilitateur pour vérifier et vérifier le système de comptes centralisés au moyen de reçus signés.

Résolution des fraudes

Une fois sur place, la gouvernance reçoit des avantages substantiels. Les comptes sont maintenant beaucoup plus difficiles à modifier et beaucoup plus transparents. Nous sommes d'avis que divers scandales et échecs de gouvernance auraient été impossibles compte tenu de ces techniques : le scandale des fonds communs de placement aurait montré une piste de vérification claire des transactions et, par conséquent, un calendrier tardif et des transactions autrement perverties ou abandonnées auraient été clairement identifiées ou complètement éliminées [NG]. Le scandale naissant aux États-Unis connu sous le nom de Stockgate aurait été impossible car la contrefaçon d'actions et la valeur à des fins de manipulation commerciale est révélée par des reçus signés .De même, Barings serait toujours une force dans la banque d'investissement si les comptes avaient été organisés autour d'espèces numériques facilement transparentes avec des reçus signés ouverts et

irréductibles qui témoignent de comptes invisibles (88888). Les scandales de style Enron auraient permis une gouvernance plus directe nommée "suivre l’argent" levant le voile sur divers swaps innovants mais économiquement sans signification.

Références

[TB] *Une ébauche de ce document crédité Todd Boyle comme un auteur, mais cela a été retiré plus tard à sa demande en raison de différences plus larges entre les points de vue.*

[LP] *Friar Luca Pacioli, Summa de Arithmetica, Geometria, Proportioni et Proportionalita 1494, Venice.*

[IG1] *Ian Grigg " The Twilight Zone ," Financial Cryptography blog 16th April 2005*

[MB] *Entanglement is discussed in: Petros Maniatis and Mary Baker, "Secure History Preservation through Timeline Entanglement," Proc. 11th USENIX Security Symposium, August 2002.*

[DC] *David Chaum, "Achieving Electronic Privacy," Scientific American, v. 267, n. 2 Aug 1992.*

[RAH] *Robert A. Hettinga " The Book-Entry/Certificate Distinction " 1995, Cypherpunks*

[GH] *Gary Howland " Development of an Open and Flexible Payment System 1996, Amsterdam, NL.*

[IG2] *Ian Grigg " The Ricardian Contract ," First IEEE International Workshop on Electronic Contracting (WEC) 6th July 2004*

[4NF] *E.F. Codd, " A Relational Model of Data for Large Shared Data Banks ," Comm. ACM 13 (6), June 1970, pp. 377-387.*

[1] *Todd Boyle, " GLT and GLR: conceptual architecture for general ledgers," Ledgerism.net, 1997-2005.*

[2] *Todd Boyle, " STR software specification," Goals, 1-5. This section adopts that numbering convention.*

[3] *Ian Grigg, various design and requirements documents, Systemics, unpublished.*

[4] *A substantial part of the programming and design was conducted by Edwin Woudt (first demo, SOX layers, UI) and Jeroen van Gelderen (message passing client architecture).*

[5] *Using internal money instead of an accounting system is not a new idea but has only been recently experienced: Ian Grigg, How we raised capital at 0%, saved our creditors from an accounting nightmare, gave our suppliers a discount and got to bed before midnight. Informal essay (rant), 7 Jul 2003.*

[NG] *James Nesfield and Ian Grigg " Mutual Funds and Financial Flaws ," U.S. Senate Finance Subcommittee 27th January, 2004.*

Traduit par *INES BOUSSOFFARA*