Trabajo en curso

Contabilidad por Partida Triple

Ian Grigg
Systemics Inc., 2005

Resumen: El recibo digitalmente firmado, una innovación de la criptografía digital, presenta un desafío a la clásica contabilidad por partida doble. Más que competir, la unión de ambas resulta en un Sistema más fuerte. Expandir el uso de la contabilidad hacia el dominio más amplio del dinero digital resulta en 3 registros locales, uno para cada uno de 3 roles, al resultado de lo cual denomino *contabilidad por partida triple*.

Este esquema crea sistemas contables a prueba de balas para usos y usuarios agresivos. Al ofrecer una contabilidad confiable y respaldada, no solamente reduce los costos, sino que además posibilita una gobernanza mucho más fuerte, en una forma que impacta de manera positiva en las necesidades futuras de la contabilidad corporativa y pública.

Introducción

Este trabajo reúne innovaciones de la criptografía financiera, como el Recibo Firmado, con técnicas contables estándar de la contabilidad por partida doble.

La primera sección presenta un breve trasfondo para explicar la importancia de la contabilidad por partida doble. Está dirigida al lector técnico y puede ser omitida por los profesionales de la contabilidad. La segunda sección presenta cómo emerge el Recibo Firmado y por qué desafía a la contabilidad por partida doble.

La tercera sección integra ambos, en tanto que la Conclusión intenta predecir ramificaciones más amplias en materia de Gobernanza.

Créditos

Este trabajo se benefició de comentarios de Graeme Burnett y Todd Boyle [TB].

Una Breve Historia de la Contabilidad

En el presente, se considera que los orígenes de la contabilidad o contaduría pueden rastrearse hasta la génesis de la escritura. Los textos más antiguos que se han descubierto han sido descifrados como simples listas de las cuentas de existencias de animales y comida. Hace alrededor de 5.000 años, los sumerios de la Mesopotamia utilizaban marcas *cuneiformes* o con forma de cuña en un sistema numérico sexagesimal, que aún hoy recordamos como segundos y minutos y, elevado al cuadrado, como los grados en un círculo. Las mismas matemáticas y escritura bien podrían haberse

derivado de la necesidad de adicionar, sustraer y, ciertamente, dar cuenta de los bienes y existencias de la sociedad primitiva.

Partida Simple

La contabilidad por partida simple es la forma en que "todo el mundo" llevaría sus registros: iniciar una lista y añadir entradas que describan cada activo. Un sistema más avanzado involucraría la creación de muchas listas. Cada lista o "libro" representaría una categoría. Cada asiento registraría una fecha, una cantidad y quizás un comentario. Para desplazar un activo, uno lo tacharía de una lista y lo introduciría en otra.

El método era muy sencillo, pero podía dar lugar a errores. Más aún, estos errores podían ser accidentales y difíciles de localizar y reparar, o ser fraudulentos. Como cada entrada o lista era independiente de las demás, no había nada que impidiera a un mal empleado añadir más asientos a la lista. Incluso de ser esto descubierto, no había nada que indicara si se estaba en presencia de un error honesto o de fraude.

La contabilidad por partida simple impone una importante limitación a la confianza en los libros. Probablemente, sólo a la familia del propietario (o, en tiempos pasados, sus esclavos) se le podía confiar los libros de la empresa. Esto influía a favor de que las familias extensas y la esclavitud funcionaran como empresas económicas.

Partida Doble

La contabilidad por partida doble añade una importante propiedad adicional al sistema contable: una clara estrategia para identificar errores y eliminarlos. Mejor incluso, tiene el efecto secundario de distinguir claramente los errores como, *o bien* accidentales, *o bien* fraude.

Esta propiedad se hace posible mediante tres características. Estas son, primero, la separación de todos los libros en dos grupos o lados, denominados activo y pasivo. Segundo, la redundancia de las duplicativas *entradas por partida doble*, cada una con su contrapartida en el otro lado. Tercero, la *ecuación contable fundamental*, que plantea que la suma de todos los asientos del lado del activo debe ser igual a la suma de todos los asientos del lado del pasivo.

Un asiento correcto debe referirse a su contrapartida y su asiento homólogo debe existir del otro lado. Es posible que un asiento erróneo haya sido creado por razones fraudulentas, pero para ser correcto a nivel local, debe referirse a su libro de contrapartida. Si este no es el caso, simplemente se lo puede eliminar como un asiento incompleto. Si sí existe esta referencia, la existencia de su contrapartida puede confirmarse fácilmente, o incluso volver a crearse, según el sentido que se le dé, quedando así cerrado el bucle.

Anteriormente, en los libros por partida simple, el defraudador se limitaba a añadir su importe a una columna de su elección. En los libros por partida doble, esta cantidad debe provenir de alguna parte. Si no procede de ninguna, el asiento es eliminado como un error accidental, en tanto que, si sí procede de algún lugar en concreto, el mismo es identificado. De este modo, el fraude deja un

rastro y su propósito se revela en el otro libro, porque el valor tomado de ese libro también debe haber salido de algún otro lugar.

Esto nos lleva a una estrategia de auditoría. En primer lugar, asegurarse de que todos los asientos sean completos, en el sentido de que se refieran a su contrapartida. En segundo lugar, asegurarse de que todos los movimientos de valor tengan sentido. Esta sencilla estrategia crea un registro de transacciones que permite llevar la contabilidad de una empresa, sin poderse ocultar fácilmente los fraudes en los libros.

¿Qué Vino Primero, la Partida Doble o la Empresa?

La contabilidad por partida doble es uno de los mayores descubrimientos del comercio, siendo difícil exagerar su significancia. Los historiadores creen que se inventó en torno al año 1300 A.D., aunque existen indicios de que ya se encontraba de una manera u otra en el imperio griego. La primera evidencia sólida es un tratado de matemáticas de 1494 por el fraile veneciano Luca Pacioli [LP]. En su tratado, Pacioli documentó muchas técnicas estándar, incluyendo un capítulo sobre contabilidad. El mismo se convertiría en el texto básico sobre contabilidad por partida doble durante muchos años.

La contabilidad por partida doble surgió en concierto con la emergencia de las formas modernas de la empresa, de las que fueron pioneros los comerciantes venecianos. Los historiadores han debatido si la partida doble se inventó para sustentar las radicalmente ampliadas demandas de las nuevas empresas que entonces aparecían en torno a la expansión de las ciudades-Estado como Venecia, o si la partida doble fue un facilitador de esta expansión.

Nuestras experiencias se decantan por la facilitación. Me refiero a las experiencias de los emisores de dinero digital. Nuestro primer despliegue de un sistema fue con un sistema de contabilidad por partida simple. Su tasa de fracaso, a pesar de la estricta codificación, era tal que no podía sostener más de 20 cuentas antes de que se produjeran errores en la contabilidad y el sistema perdiera cohesión. Esto ocurrió a las pocas semanas de las pruebas iniciales y nunca se pudo desplegar en campo. El sistema por partida doble que lo sustituyó se puso en marcha a principios de 1996 y nunca ha perdido una transacción (aunque se han producido algunos casos límite [IG1]).

Asimismo, la empresa DigiCash BV de los Países Bajos puso en marcha un primer sistema de dinero digital en un banco de Estados Unidos. Durante el periodo de pruebas, el sistema original de contabilidad por partida simple tuvo que ser sustituido por un sistema por partida doble por la misma razón: debido a los errores que habían producido, la contabilidad subyacente al sistema de caja digital había dejado de ser fiable.

Otro importante sistema de dinero digital duró muchos años con un sistema de contabilidad por partida simple. Sin embargo, la empresa sabía que funcionaba con ayuda de la fortuna. Cuando un cracker consiguió encontrar un fallo en el sistema, un ataque de una sola noche permitió la creación de muchos millones de dólares en valor. Como esto superaba a la emisión contractual de valor hasta la fecha, causando contorsiones dramáticas en el balance contable e incluso poniendo a la empresa en incumplimiento de sus términos y condiciones de uso, y en riesgo extremo de una “corrida bancaria”. Por suerte, el cracker depositó el valor creado en la cuenta de un juego en línea que

fracasó poco después, por lo que el valor pudo ser neutralizado y limpiado monetariamente, sin divulgación y sin escándalo.

Es al menos la opinión de este autor que la contabilidad de partida simple es incapaz de sostener cualquier empresa más sofisticada que un hogar. Es por ello que sugiero que la evolución de las empresas complejas requirió de la partida doble como elemento facilitador.

Computar la Partida Doble en Tiempo Rápido

La partida doble siempre ha constituido el fundamento de los sistemas de contabilidad por ordenador. La capacidad de detectar, clasificar y corregir errores es aún más importante para los ordenadores que para los humanos, ya que no existe el lujo de la intervención humana: la distancia entre el usuario y los bits y bytes es mucho mayor que la distancia entre el contador y las marcas de tinta en sus libros.

Cómo se implementa la partida doble es un tema en sí mismo. Las Ciencias de la Computación introducen conceptos tales como las *transacciones*, definidas como unidades de trabajo *atómicas*, *consistentes*, *aisladas* y *duraderas* (ACID, en inglés). La pregunta central para los programadores es cómo añadir un asiento en el activo, luego añadir un asiento en el pasivo, y no tener un *crash* (fallo) a mitad de esta secuencia. O, peor aún, que se inicie otra transacción a mitad de camino. Esto tiene más sentido cuando se lo considera en el contexto de los millones de asientos que puede manejar un ordenador: si existe una muy pequeña posibilidad de que algo salga mal, finalmente algo lo hará. Los ordenadores no pueden manejar muy bien los errores de esa naturaleza.

En su mayor parte, estos conceptos se reducen simplemente a "¿Cómo implementamos la contabilidad por partida doble?" Como esta pregunta está bien contestada en la literatura, nos limitamos a mencionarla aquí.

Una Historia Algo Menos Breve del Recibo Firmado

Los recientes avances en la criptografía financiera han supuesto un reto para el concepto de contabilidad por partida doble. La firma digital es capaz de crear un registro con cierto grado de fiabilidad, al menos en el sentido anteriormente expresado por ACID. Se puede confiar en una firma digital para mantener un registro seguro, ya que no se verificará si algún detalle del registro es modificado.

Si podemos suponer que el registro fue creado originalmente de forma correcta, entonces se revelan los errores posteriores, tanto los de naturaleza accidental como los de intención fraudulenta. (Los ordenadores rara vez cometen errores accidentales y, cuando lo hacen, lo más usual es que lo hagan de una forma más torpe, más similar a derramar el tintero que a unos pocos números.) De este modo, cualquier cambio en un registro que tenga algún tipo de sentido contable o semántico es, casi con toda seguridad, un intento de fraude, y la firma digital lo hace evidente.

La Firma Digital y el Dinero Digital

Una firma digital nos da una propiedad particular, a saber

> *"En un momento determinado, esta información fue vista y marcada por el ordenador firmante".*

Existen diversas variantes, algunas con una pretensión más sólida de arrogarse esta propiedad que otras. Por ejemplo, los resúmenes criptográficos con *entrelazamiento* ("*message digests* with *entanglement*") constituyen una forma de firma que es simple y eficaz. Los *criptosistemas de clave pública* ofrecen otra vía en la que los firmantes tienen una clave privada y los verificadores una clave pública [MB]. Existen asimismo muchas formas de atacar la propiedad básica. En este ensayo evito las comparaciones y asumo la propiedad básica como una marca fiable de haber sido vista por un ordenador en algún momento.

Las firmas digitales representan entonces una nueva forma de crear entradas fiables y de confianza, que pueden ser construidas en los sistemas contables. Inicialmente, se sugería que una variante conocida como la *firma digital ciega* haría posible el dinero digital [DC]. Habría *certificados* circulando como derechos o contratos, de forma muy similar a los antiguos certificados de acciones, sustituyendo así a los sistemas contables centralizados [RAH]. Estas ideas llevaron a la criptografía financiera a recorrer (sólo) una parte del camino. Aunque mostraron cómo verificar fuertemente cada transacción, no alcanzaron a colocar a la firma digital en un marco generalizado de contabilidad y gobernanza. Restaba el paso pendiente de añadir la redundancia implícita en la contabilidad por partida doble para proteger del fraude tanto a los agentes que realizan las transacciones como a los operadores del sistema.

La Función Inicial de un Recibo

Los diseños derivados de las características de Internet, de las capacidades de la criptografía y de las necesidades de gobernanza llevaron al desarrollo del *recibo firmado* [GH]. Para desarrollar este concepto, supongamos un sencillo sistema de pago de tres partes, en el que cada una de ellas posee una clave de autorización que puede utilizarse para firmar sus instrucciones. Por comodidad, llamaremos a estas partes Alice, Bob (dos usuarios) e Ivan (el emisor).

1: Un Recibo Provisorio

De	Alice
Para	Bob
Unidad	Euro
Cantidad	100
Fecha	2005.12.25
firma digital	

Cuando Alice desea transferir valor a Bob en alguna unidad o contrato administrado por Ivan, escribe la instrucción de pago y firma digitalmente la misma, de forma muy similar a como se hace con un cheque en el mundo físico. Envía esta instrucción al servidor (Iván) y este, presumiblemente, acepta y realiza la transferencia en su conjunto interno de libros. A continuación, emite un recibo y lo firma con su clave de firma. Como parte importante del protocolo, Iván entrega de manera fidedigna el recibo firmado a Alice y Bob, y estos pueden actualizar sus libros internos en consecuencia.

El Recibo *es* la Transacción

Nuestro concepto de valor digital buscaba eliminar tantos riesgos como fuera posible. Esto se derivaba simplemente de uno de los requisitos de alto nivel: El de ser extremadamente eficiente en la emisión de valor. La eficiencia en la emisión digital es, primariamente, una función de los costes de atención al cliente, y un determinante importante de los costes de atención al cliente son los costes de fraude y robo.

Un riesgo que consistentemente echaba por tierra cualquier diseño de valor digital eficiente a un coste razonable era el riesgo de fraude interno (*insider fraud*). En nuestro modelo de muchos usuarios y un único servidor centralizado, los emisores de la unidad de valor digital (como firmantes del contrato) y cualquier socio en la gobernanza (tal como los operadores de los servidores), son poderosos candidatos al fraude interno. Los acontecimientos de los últimos años, tales como los escándalos de los fondos mutualistas y el *stockgate*, son casos canónicos de riesgos que decidimos abordar.

Para hacer frente al riesgo de fraude interno, históricamente se introdujo el recibo escrito como una fuente primaria de evidencia. Mayormente olvidado por el público comprador hoy en día, el propósito de un recibo escrito en el comercio minorista normal no es permitir reclamos y devoluciones por parte del cliente, sino comprometerlo en un protocolo de documentación que obliga al empleado del vendedor a custodiar el dinero. Un buen cliente advertirá el fraude cometido por el empleado y dará aviso al propietario para que vigile los fondos identificados por el recibo. La misma historia se aplica a la invención de la caja registradora, que originalmente era sólo una caja que separaba la recaudación del propietario del dinero en los bolsillos del dependiente. Nosotros ampliamos este motivo principal al mundo digital utilizando un recibo firmado para vincular al Emisor a un protocolo de gobernanza con los usuarios.

2: Un Recibo Firmado

Cheque del Usuario

De	Alice
Para	Bob
U.	Euro
Cnt.	100
Com	Pens

De	Alice
Para	Bob
Unidad	Euro
Cantidad	100
Fecha	2005.12.25

firma de Ivan

Nosotros avanzamos a su vez varios pasos más. En primer lugar, para lograr una inalterabilidad completa, la autorización original de Alice también se incluye en el registro. El recibo incluye entonces toda la evidencia, tanto de la intención del usuario como de la acción del servidor en respuesta, y se convierte ahora en un *registro dominante* del evento. Esto significa entonces que la estrategia más eficiente para el mantenimiento de registros es el abandono de todo registro anterior y mantener a salvo el recibo firmado.

Esta dominación afecta tanto al Emisor como al usuario, y nos permite enunciar el siguiente principio:

> *El Usuario y el Emisor poseen la misma información.*

Como el recibo firmado es entregado desde el Emisor a ambos usuarios, las tres partes poseen el mismo registro dominante para cada evento. Esto reduce los costes de atención al cliente al disminuir drásticamente los problemas causados por discrepancias en la información.

En segundo lugar, vinculamos al recibo un contrato firmado de emisión conocido como *Contrato Ricardiano* [IG2]. Esta invención relaciona un documento firmado digitalmente de forma segura con el recibo firmado mediante un identificador único llamado *resumen criptográfico* (*message digest)* proporcionado, una vez más, criptográficamente. Proporciona así una fuerte e inmutable fijación de la unidad de cuenta, la naturaleza de la emisión, los términos, condiciones y promesas hechas por el emisor y, por supuesto, la identidad del emisor.

Por último, con estos pasos establecidos, podemos introducir el principio:

> *El Recibo* es *la Transacción.*

Hacia el interior del registro entero del recibo firmado, se encuentra la expresión de la intención del usuario, que es confirmada plenamente por la respuesta del servidor. Ambas están cubiertas por firmas digitales, que fijan estos datos. Un revisor, tal como un auditor, puede confirmar los dos conjuntos de datos y verificar las firmas.

El Recibo Firmado como Sistema de Contabilidad

Con el tiempo, el principio del Recibo como Transacción se ha convertido en sacrosanto. En nuestros programas informáticos para clientes, el principio ha sido introducido en el diseño de forma sistemática, dando lugar a un régimen contable simplificado y de gran fiabilidad. Siguen existiendo cuestiones tales como la pérdida de recibos y la validación de saldos con el software del lado-cliente, pero estos se vuelven razonablemente manejables una vez que el objetivo de los recibos como transacciones se coloca en un lugar primordial en la mente del diseñador.

Como Partida Simple

Para calcular los saldos de un conjunto de recibos interrelacionados o para presentar un historial de transacciones, se construiría un libro sobre la marcha a partir de dicho conjunto. Esto equivale a utilizar el Recibo Firmado como base para la contabilidad por partida simple. En efecto, la contabilidad se deriva de los recibos en bruto, lo que plantea la cuestión de si hay que conservar los libros.

Los principios de las bases de datos relacionales nos orientan en este sentido. La *cuarta forma normal* nos indica que almacenemos los registros primarios (en este caso el conjunto de recibos) y construyamos los registros derivados (los libros contables) sobre la marcha [4NF].

Recuperando la Partida Doble

Surgen problemas similares para Iván el Emisor. El servidor debe aceptar cada nueva transacción sobre la base del saldo disponible en los libros efectuados. Por esta razón, Iván necesita que esos

libros estén disponibles de forma eficiente. Debido al mayor número de recibos y libros (uno por cada cuenta de usuario), tanto recibos como libros tenderán a existir, en contraste directo con la cuarta forma normal. Aquí resulta de ayuda una fusión entre conjuntos relacionalmente sólidos de recibos y libros por partida doble.

Se concede un libro a cada uno, Alice y Bob, dentro de la arquitectura del servidor. Como es habitual, colocamos esos libros del lado del pasivo. Los recibos entonces pueden ser colocados en un solo libro separado y esto puede ser colocado lógicamente del lado del activo. Cada transacción de Alice a Bob tiene ahora una contrapartida lógica, estando entonces representada en 3 lugares dentro de las cuentas del servidor. Sin embargo, el lado del activo permanece dentro de los términos de la cuarta forma normal, ya que cada registro del pasivo se deriva de un equivalente proveniente del activo.

Por extensión, un agente más sofisticado de software del lado-cliente (*client-side)* que trabaje para Alice o Bob podría emplear las mismas técnicas. Llevado a este extremo, los asientos se encuentran ahora en tres lugares distintos, cada uno de ellos conteniendo potencialmente tres registros.

Contabilidad por Partida Triple

El recibo digitalmente firmado, con la autorización completa de una transacción, representa un reto dramático para la contabilidad por partida doble, al menos a nivel conceptual. La invención criptográfica de la firma digital confiere una gran fuerza probatoria al recibo y, en la práctica, reduce el problema contable a la presencia o ausencia del recibo. Este problema se resuelve compartiendo los registros: cada uno de los agentes tiene una copia fiable.

En un sentido estricto, la contabilidad por partida doble es ahora redundante para la teoría de las bases de datos relacionales: ha sido normalizada mediante la cuarta forma normal. Empero, esto es más una afirmación teórica que práctica. En los sistemas de software que hemos construido, ambos permanecen juntos, trabajando por lo general codo a codo.

Esto nos lleva a los pares de entradas dobles conectadas por la lista central de recibos: tres asientos por cada transacción. No sólo cada agente contable es llevado a mantener tres registros, sino que los roles naturales de una transacción son de tres partes, lo cual lleva a tres por tres asientos.

Llamamos a esto contabilidad por partida triple. Aunque el recibo digitalmente firmado domina en términos de información, se queda corto en términos de procesamiento. La contabilidad por partida doble llena ese vacío de procesamiento. Por lo tanto, ambas funcionan mejor juntas que separadas. En este sentido, nuestro término de contabilidad por partida triple recomienda más bien un avance en la contabilidad, en lugar de una revolución.

Consideraciones Sobre Software

La disposición exacta de los asientos (*entries*) en términos de software y datos no está resuelta, y puede convertirse finalmente en una de esas efímeras *cuestiones de implementación*. Los recibos firmados pueden formar una contrapartida natural del lado del activo, o conformar una lista

separada del plan de cuentas, es decir por fuera de la contabilidad (*non-book list*) y subyacente al sistema contable con sus dos lados.

Cuando la construcción de los libros se deriva de los recibos, surgen problemas de auditoría, en tanto que, cuando se pierde un recibo, surgen problemas de normalización. Estas son cuestiones para futuras investigaciones.

Similarmente, cabe señalar que la técnica de firmar recibos funciona tanto con firmas de clave privada como con firmas de resúmenes criptográficos con entrelazamiento. Depende del entorno de negocios si los aspectos de seguridad de estas técnicas las vuelven adecuadas o no para la tarea a la que se las destina.

Funciones de los Agentes

Cabe notar que el diseño anterior de la contabilidad por partida triple suponía que Alice y Bob eran agentes con cierta independencia. Esta independencia resultaba de que las especificaciones originales eran propias del diseño de un sistema de dinero digital, en lugar de un sistema contable clásico.

Lejos de minimizar la relevancia de nuestro trabajo para la profesión contable, esto introduce el dinero digital como una alternativa a la contabilidad corporativa. La experiencia demuestra que, si el sistema de contabilidad para una empresa u otra entidad administrativa es reestructurado como un sistema de dinero digital o dinero *interno*, la organización obtiene beneficios.

Aunque el núcleo del sistema se vea exactamente igual a un sistema contable, los libros de cada departamento se trasladan a cuentas digitales de dinero. Los departamentos ya no trabajan tanto con presupuestos como con el control de su propio dinero corporativo. El control fundamental de la gobernanza sigue estando en manos del departamento de contabilidad debido a que manejan el sistema y al alcance limitado del dinero, que sólo puede ser utilizado dentro de la organización. El departamento de contabilidad puede intervenir como creador de mercado (*market maker)*, intercambiando pagos en dinero interno por pagos en dinero externo hacia proveedores externos.

Hemos operado este sistema en pequeña escala. En lugar de ser ineficiente a esta muy reducida escala, el sistema ha generado un ahorro dramático en la coordinación. Facturas y sueldos ya no son abonadas con fondos convencionales; muchas transacciones son resueltas mediante transferencias de dinero interno y, en los límites de la empresa, agentes formales e informales trabajan para *intercambiar* dinero interno por dinero externo. El papeleo se reduce sustancialmente, puesto que los registros del sistema monetario son lo suficientemente fiables como para resolver cuestiones rápidamente, incluso años después del suceso.

Las innovaciones presentes en el dinero interno exceden lo descrito en el presente documento. Basta con decir que contestan a la pregunta obvia de por qué este diseño de contabilidad por partida triple surgió del mundo del dinero digital, y por qué tiene relevancia en el mundo corporativo.

Patrones de Comercio

Todd Boyle analizó un problema similar desde el punto de vista de las necesidades de las pequeñas empresas en la era de Internet, llegando a la misma conclusión: la Contabilidad por Partida Triple [1]. Sus premisas de partida fueron las siguientes:

1. La necesidad principal no es ni la contabilidad ni los pagos *per se*, sino los patrones de intercambio; patrones complejos de comercio;
2. Los pequeños comercios no podían permitirse grandes y complejos sistemas que entendieran estos patrones;
3. No se encerrarían en marcos protegidos por propiedad intelectual;

A partir de estos fundamentos, Boyle llegó a la conclusión de que, consiguientemente, lo que se necesita es un repositorio independiente de acceso compartido, al cual las partes tengan acceso de forma imparcial. Fundamentalmente, este repositorio es análogo al clásico libro de contabilidad por partida doble de filas de transacciones ("GLT" por *General Ledger for Transactions* en inglés*,* u operaciones del Libro Mayor), pero sus entradas son dinámicas y compartidas.

Unos sencillos ejemplos ayudarán. Cuando Alicia realiza una transacción, la ingresa en su software. Cada transacción GLT requiere nombrar a su contraparte externa, Bob. Cuando Alice publica la transacción, su software la almacena en su GLT local y también la envía al GLT del servicio de Repositorio de Transacciones Compartidas ("STR" por *Shared Transaction Repository* en inglés).

El STR envía entonces la transacción a Bob. Se espera que tanto Bob como Alice almacenen la referencia de la transacción como un índice o talonario,[1] y que el STR almacene la transacción completa.

Las ideas de Boyle son lógicamente comparables a las de Grigg y Howland, aunque provienen de direcciones diferentes (el STR es el Iván de Grigg mencionado anteriormente) y no son totalmente equivalentes. Mientras que estos últimos limitaban su trabajo a pagos, la exactitud de los importes y la protección con una dura estructura criptográfica, Boyle se concentró en patrones más amplios de transacciones, y demostró que el STR podía intermediar en estas transacciones, siempre que los datos centrales compartidos pudieran extraerse y convertirse en un único registro compartido. Boyle se centró en la sustancia económica de la transacción.

Extendiendo la Humilde Factura

Imaginemos un sencillo procedimiento de facturación. Alice crea una factura y la publica en su programa informático (GLT). Como ella ha nombrado a Bob, el GLT se la reenvía ("*postea")*

[1] Nota del Traductor: en el diseño original de Boyle, los talonarios eran espacios en los que las partes podían almacenar notas o documentos privados, lo cual les permitiría evitar la necesidad de llevar ellas mismas un sistema contable localmente. Un equívoco lingüístico llevó a que Grigg interpretara que el talonario consistía en la referencia (hash, link, índice) a la transacción almacenada en el STR. Esto no era a lo que Boyle se refería con este término y, si bien efectivamente Boyle consideraba posible que las partes almacenen la referencia de la transacción, también concebía un modelo con almacenamiento 100% "en la nube" (webledger).

automáticamente a Iván, el STR, quien a su vez lo remite a Bob. En este punto, Bob debe tomar una decisión: aceptar o rechazar. Si acepta, su software puede responder enviando un mensaje de aceptación a Iván. El STR crea ahora un registro de factura aceptada que sustituye al anterior registro de factura especulativa y lo envía (*"postea"*) triplemente. En algún momento de este patrón de transacciones (vinculado con la política de pagos), Bob también publica una transacción separada para pagar la factura. Esto podría funcionar de la misma manera que una transacción separada, enlazando directamente con la factura original.

Ahora, como el pago está vinculado, y la factura se ha vuelto una transacción viva dentro de los tres asientos en los tres sistemas contables, es posible que un nuevo y actualizado registro de factura refiera nuevamente a la actividad de pago. Cuando el pago se liquida, el nuevo registro puede volver a sustituir a la antigua copia impaga y promulgarla hacia las tres partes.

Patrones de Transacciones

Se podría escribir un software para facilitar y supervisar este flujo y otros similares. Si el sistema de pagos es lo suficientemente flexible y se integra con las necesidades de los usuarios, podría ser posible fusionar la factura anterior con el propio pago, a nivel de Recibos. Visto así, el Recibo Firmado de Ricardo es simplemente el patrón más pequeño y sencillo dentro del conjunto más general de patrones posibles. Podríamos entonces sugerir que el estrecho principio de que *el Recibo es la Transacción* podría ampliarse hasta *la Factura es la Transacción*.

Una transacción particular en el mundo de los negocios casi nunca se produce en soledad. Se producen en patrones. Por ejemplo, ofertas y aceptaciones forman una transacción más amplia, pero rara vez encapsulan todo el ciclo de cumplimiento y pago. Incluso si se ha producido un pago que acompaña a un mensaje de pedido, el cliente espera a continuación el cumplimiento.

Existe un amplio corpus científico y bibliográfico en torno a estos modelos o *patrones de transacciones*. Estos han sido adoptados por el grupo de trabajo de Procesos Comerciales de ebXML y otros organismos de normalización, en donde se denominan "Transacciones Comerciales". Sin embargo, el presente trabajo se distingue por desglosar estas transacciones en sus elementos atomísticos. A ellos nos referimos a continuación.

Los Requisitos de la Contabilidad por Partida Triple

La implementación de la contabilidad por partida triple evolucionará con el tiempo para dar soporte a patrones de transacciones. Lo que ha quedado claro es que la partida doble no provee suficiente sustento a estos patrones, ya que es un marco que se rompe tan pronto como el número de partes es superior a uno. Sin embargo, así como la partida doble está "rota" en la red y es incapaz de dar soporte a las demandas comerciales, la partida triple no es ampliamente entendida, ni son bien reconocidos los requisitos de infraestructura que impone.

A continuación, se encuentran los requisitos que consideramos importantes [2] [3].

1. **Fuerte Pseudonimato, como Mínimo**. Dado que hay muchos ciclos en los patrones, el sistema debe dar soporte a un claro mapeo de relaciones entre participantes (identidad). Como mínimo, esto requiere una arquitectura pseudonímica de la naturaleza de Ricardo o AADS. (Este requisito es muy claro, pero no podemos discutirlo en mayor extensión por razones de espacio).
2. **Firma de Asientos**. Para neutralizar las amenazas hacia y por las partes, es preciso un mecanismo que congele y confirme los datos básicos. Esta es la firma, y exigimos que todos los asientos sean capaces de llevar firmas digitales (véase el punto 1, más arriba, que sugiere firmas de clave pública).
3. **Paso de Mensajes**. El sistema es fundamentalmente de paso de mensajes (*message-passing*), en contraste con gran parte de la arquitectura de la red basada en conexiones (TCP). Boyle reconoció tempranamente que la naturaleza genérica del paso de mensajes era un componente crítico, y Systemics propuso y construyó esto en Ricardo durante el periodo 2001-2004 [4].
4. **Ampliación y Migración del Asiento**. Cada nueva versión de un mensaje que arriba representa un asiento que debe ser actualizado o añadido. Dado que cada mensaje se añade a una conversación anterior, el asiento almacenado debe ampliarse y absorber la nueva información, conservando las demás propiedades.
5. **Almacenamiento Local de Asientos y Reportes**. El almacenamiento persistente y la disponibilidad responsiva de los asientos/entradas. En la práctica, este es el clásico libro mayor de contabilidad, al menos en términos de almacenamiento. Debe doblarse un poco para manejar entradas mucho más flexibles, y sus capacidades de reportaje se vuelven más fundamentales a medida que llevan a cabo reconciliación intrínseca bajo demanda o en vivo.
6. **Pagos Inmutables Integrados**. El comercio sólo puede ser tan eficiente como el pago. Esto significa que el pago debe ser al menos tan eficiente como cualquier otra parte, lo que en la práctica implica que un sistema de pagos debe estar integrado a nivel de infraestructura. cf. Ricardo.
7. **Mensajería Integrada a Nivel de Aplicación**. A diferencia de la mensajería en los niveles inferiores del protocolo (1 más arriba), existe el requisito de que Alice y Bob puedan comunicarse. Esto se debe a que la gran mayoría de los patrones giran en torno a las comunicaciones básicas de los agentes. No tiene sentido establecer un mecanismo de pago y facturación superior a sus medios de comunicación y negociación. Este concepto quizá se vea mejor en el sistema SWIFT, que es ante todo un sistema de mensajería para dar instrucciones de pago.

Conclusión

La contabilidad por partida doble proporciona evidencia de la intención y del origen, lo que da lugar a estrategias para hacer frente a los errores por accidente y al fraude. La invención del recibo firmado por la criptografía financiera proporciona los mismos beneficios, desafiando por lo tanto el reinado de 800 años de la partida doble. De hecho, en términos probatorios, el recibo firmado es más poderoso que los registros por partida doble debido a las cualidades técnicas de su firma.

Siguen existiendo algunos puntos débiles en la comparación estricta con la contabilidad por partida doble. En primer lugar, en la instanciación de Ricardo de la contabilidad por partida triple, los propios recibos pueden perderse o ser eliminados, y por esta razón subrayamos como principio *que el registro es la transacción*. Esto da lugar a tres agentes activos que se encargan de asegurar el asiento firmado como su registro más importante de la transacción.

En segundo lugar, las ramificaciones informáticas del sistema por partida triple son menos convenientes que las que ofrece la contabilidad por partida doble. Por este motivo, ampliamos la información contenida en el recibo a un conjunto de libros por partida doble. De este modo, tenemos lo mejor de ambos mundos en cada nodo: la fuerza probatoria de los registros firmados y la conveniencia y el poder de verificación cruzada local del concepto de partida doble.

Estos dos imperativos funden los recibos firmados con la contabilidad por partida doble. Como acabamos con una disposición lógica de tres asientos por tres, creemos que el término contabilidad por partida triple (o contabilidad de triple entrada) es útil para describir el avance respecto de la forma más antigua.

Cómo Atraer a los Agentes

Para beneficiarse plenamente de la contabilidad por partida triple, debemos ampliar los sistemas contables a los agentes y ofrecerles capacidades directas de realizar transacciones. Es decir, convertimos a los agentes en partes interesadas al darles dinero interno [5]. El uso del dinero digital para llevar las cuentas de la empresa permite utilizar este concepto como sustituto general de la contabilidad general y presupuestos departamentales, y es un elemento habilitador de la verificación y auditoría por medio de recibos firmados de los sistemas de contabilidad centralizada.

Resolver los fraudes

Una vez allí, la gobernanza recibe beneficios sustanciales. Las cuentas son ahora mucho más transparentes y difíciles de modificar. En nuestra opinión, varios escándalos y fallos de gobernanza habrían sido imposibles con estas técnicas: el escándalo de los fondos mutualistas habría mostrado una clara pista de auditoría de las transacciones y, por tanto, se habrían identificado claramente o eliminado por completo las transacciones tardías pervertidas o abandonadas [NG]. El incipiente escándalo en EE.UU. conocido como *Stockgate* habría sido imposible, ya que la falsificación de acciones y valor con fines de manipulación de las operaciones se revela mediante recibos firmados. Del mismo modo, Barings seguiría siendo una fuerza en la banca de inversión si las cuentas se hubieran organizado en torno a un dinero digital fácilmente transparente con recibos firmados abiertos e irreductibles que evidencian las cuentas invisibles (*88888*). Los escándalos al estilo de Enron habrían permitido una gobernanza más directa de “seguir el dinero”, levantando el velo de varias permutas (swaps) innovadoras, pero sin sentido económico.

Referencias

[TB] Un borrador de este documento daba crédito a Todd Boyle como autor, pero posteriormente fue retirado a petición suya, debido a diferencias más amplias de puntos de vista.

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

[IG1] Ian Grigg "The Twilight Zone", *Financial Cryptography blog*, 16 de abril de 2005.

[MB] El enredo se discute en: Petros Maniatis y Mary Baker, "Secure History Preservation through Timeline Entanglement", *Proc. 11th USENIX Security Symposium*, agosto de 2002.

[DC] David Chaum, "Achieving Electronic Privacy", *Scientific American*, v. 267, n. 2 de agosto de 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)*, 6 de julio de 2004.

[4NF] E.F. Codd, "A Relational Model of Data for Large Shared Data Banks", *Comm. ACM* 13 (6), junio de 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. Esta sección adopta esa convención de numeración.

[3] Ian Grigg, varios documentos de diseño y requisitos, Systemics, sin publicar.

[4] Una parte sustancial de la programación y el diseño fue realizada por Edwin Woudt (primera demo, capas SOX, UI) y Jeroen van Gelderen (arquitectura de cliente de paso de mensajes).

[5] La utilización de dinero interno en lugar de un sistema contable no es una idea nueva, pero sólo ha sido intentada recientemente: 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. Ensayo informal ("rant"), 7 de julio de 2003.

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

Traducción por Juan Ignacio Ibañez
Centre for Blockchain Technologies
University College London

Esta traducción se benefició de los comentarios de
Santiago Fernández Quiroz, Ramón Quesada,
Luis Saiz Gimeno y Enrique Agudo Fernández.