الريكاردي العقد

غريغ إيان

Systemics, Inc.

iang@iang.org

ملخص

إن وصف القيمة الرقمية لأنظمة الدفع ليس بالامر الهين .قد تفشل الآليات المبسطة لإستخدام الأرقام أو رموز البلدان لوصف عملات ورموز التلكس لإصدار السندات والأسهم والأدوات المالية في قدرتها على معالجة المطالب الدينامية والمتباعدة.والواقع أن الاختلافات التعسفية ظاهرياً في معاني مختلف الأدوات يمكن إبرامها باعتبارها عقوداً بين الجهات المصدرة والعملات أصحاب . وبالتالي يمكن النظر إلى الإصدار الرقمي للصكوك على أنه إصدار عقود. يشمل الذي الوثيقة لنموذج وصف ويرد .المسألة هو العقد يكون أن الوثيقة هذه وتقترح يتجزأ. لا جزءا يكون أن متطلبات ذلك مع يتفي ولكنه المالي للصك الاصيل التعاقدي الطابع الدفع نظام من.

I-المقدمة :

ولا يتم القيام إلا بقدر ضئيل من العمل بشأن تصنيف ووصف القيمة المتعلقة بميدان الترميز المالي .وتعرض هذه الورقة العقد الريكاردي كطريقة لتحديد ووصف المسائل المتعلقة بالصكوك المالية على أنها عقود[1]. وقد تم تطويره في الأصل من طرف إيان غريغ و غاري هاولاند كجزء من نظام الدفع ريكاردو.

I)

1- النشأة أو البدايات :

الطلب الأصلي هو نظام تداول السندات [2]. وفيما يتعلق بهذا التداول، يتمثل أحد العناصر الاساسية في نظام تحويل أو دفع يتلقى تعليمات تحويل ويتصرف فيها لنقل الادوات (نقد، سندات) من حساب إلى آخر.ولذلك يجب أن تحدد كل تعليمات الصك.وكانت هناك حاجة إلى وسيلة لإلتقاط وتحديد ووصف الأدوات المتداولة. هناك الآلاف من السندات وربما الملايين من الأدوات الأخرى التي يمكنها إصدار هذه البيانات وتبادلها ولكل منها خصائص فريدة لا يمكن ضغطها في قواعد البيانات. و بالنسبة لمثل هذا النظام، فإن النقد لا يختلف عن السندات وهي تتطلب نفس المواصفات.

(I

2- الاشكالية :

عندما يصدر شخص عملة (أو سند أو مشاركة) عبر الإنترنت، ما الأمر؟ ما الذي لدى المتلقي؟أنظمة قليلة لإصدار القيمة (أنظمة الدفع) يعالج هذه الأسئلة بشكل مناسب . وهي تشير بشكل عام إلى الوحدات الخارجية الموجودة من العملة وترتيب الحواف غير المحكمة في *اتفاقية المستخدم*. على سبيل المثال، يعتمد بايبال كمصدر للدولار على التواؤم مع الدولار الأميركي لتحديد قسم كبير من عرض الخدمات. أما مصدري الذهب فيعتمدون بشكل أكبر على اتفاقيات المستخدمين الخاصة بهم حيث أن الوحدة المعدنية ليست مألوفة إلى هذا الحد. ولكن حتى مع العملات، يجد المستخدم صعوبة في تحديد أمن وسلامة دولار واحد في ما يتعلق بدولار آخر.

إن التصنيف حسب الأرقام أو الرموز هو نقطة بداية. وتحدد جميع نظم الإصدار الرقمي تقريباً هذه المسائل الأساسية من خلال تخصيص الأرقام أو الأحرف كعملات (على سبيل المثال 840 و "USD" و [3]"AUG"). و قد تتعرض هذه الأنظمة للمتاعب بسرعة. والواقع أن أي جهة مصدرة لديها العديد من العملات أو العديد من الجهات المصدرة التي تحمل نفس العملة الاسمية تثير تساؤلات صعبة. هل يمكن أن يحتوي المُصدر على وحدتين دولاريتين أو أكثر؟ على سبيل المثال، ضمن ISO3166-1، هناك ثلاثة دولارات أمريكية مختلفة: 840/دولار أمريكي (نقداً)، USS/998 (في اليوم نفسه)، وUSN/997 (في اليوم التالي). وبالمثل، كيف تميز إحدى عملات الذهب الرقمية ("DGC") ذهبها عن ذهب جهة إصدار أخرى، عندما تعرف جميعها باسم "AUG"؟

(I

3-الحل :

وبما أن السندات تشكل في جوهرها عقوداً بين مصدري السندات والمستخدمين، فإن مشكلتنا هنا تتلخص في *إصدار العقود*. وفي حين أن هناك مسائل أخرى *لها* عقود، فإن العقود هم قضيتنا. تكمن ابتكاراتنا في التعبير عن صك صادر كعقد وربط ذلك العقد بكل جانب من جوانب نظام الدفع. ومن خلال هذه العملية، تتم صياغة وثيقة ذات فائدة واسعة (يمكن قراءتها بواسطة المستخدم والبرنامج) وتوقيعها رقميًا من قبل جهة إصدار الصك. وتشكل هذه الوثيقة وهي العقد الريكاردي الأساس لفهم مسألة معينة وكل معاملة تدخل في نطاق هذه المسألة. وبالتبعية فإن كل قضايا القيمة، مثل العملات والأسهم والمشتقات وأنظمة الولاء والقسائم، من الممكن أن تستفيد من هذا النهج.

(I

4-الهيكل:

تم تصميم هذه الوثيقة كما يلي. في القسم الثاني، سنناقش النهج التقليدية لتحديد ووصف عملية الإصدار ونستكشف المسائل والشكوك المحيطة بهذه المقارابات. ثم في الباب الثالث، يقدم تصميم للتعبير عن الإصدار بوصفه عقدا. وأخيرا، أضيفت في الفرع الرابع ملاحظات ختامية.

II- مسائل ذات قيمة كعقود :

(II
1- نظام الجيل الأول:

ولنتأمل هنا حالة خطة النقد الرقمي الرائدة، "eCash"، كما كانت في الأصل بواسطة Digicash BV. أول عملة قيمة صادرة عن بنك مارك توين بالولايات المتحدة الأمريكية تم تحديدها بالرقم 4. وقد قام النظام المبكر بتخصيص رقم تسلسلي صغير لكل عملة.
وقد حصلت أنظمة الاختبار بالفعل على 2,1, 3 ومن ثم فإن 4 هي التالية .ثم تغيرت بعد ذلك افتراضات شركة Digicash التسويقية بحيث تفترض وجود إصدار واحد لكل بلد. وفي الوقت المناسب، تم تعديل هذا المخطط لإصدار العملات المرقمة بعد رموز الطلب الدولية (على سبيل المثال، 49 بالنسبة لألمانيا و61 بالنسبة لأستراليا). وقد اتضح النقص في هذا المخطط، ولذلك أنشئ تصميم جديد [4]. وقد استخدم رقم واحد من 32 (بت) لوصف هذه المسألة، على افتراض عملي أن ذلك سيكون كبيرا بما يكفي لتغطية الاحتمالات المتوقعة. ورغم هذا فإن الضغوط التي كانت قد تولت على أحد الجهات المصدرة، حيث كانت إحدى العملات واضحة على الفور تقريبا. وقد يستخدم المخطط الأكثر تقدماً مجموعة من (المصدر، العملة) لوصف النظام حيث يكون لكل مُصدر سلطة إصدار عملات منافسة متعددة [5]. من السهل تعميم هذا النظام من خلال زيادة عناصر إضافية إلى المجموعة: (جهة الإصدار، النوع، المعرف) المجموعة [6]. على سبيل المثال، قد يكون لسند القسيمة الذي تم إصداره من قِبل شركة Universal المشتركة وKeiretsu على مستوى البلد والذي يدفع في يناير من عام 2100 مجموعة من (غير هام (JUNK)، صفر، يناير 2100).

(II
2- الإشكال في الأرقام:

إن الأرقام كمساحة لتحديد الأدوات الرقمية محدودة ولا يشكل وجود مجموعات كامتداد إجابة حقيقية. أولاً ما الذي يصفونه؟ وفي حالة النظم النقدية الإلكترونية، يمكن أن تصف العملات والمصدرين. هل هو واحد أو كلاهما وكيف نعمّم بالنسبة إلى الجوانب الأخرى؟ ثانيا، ما هي الضمانة التي لدينا والتي تم وصفها بدقيقة؟ على الرغم من إمكانية تحقيق الكثير من خلال الاعتماد ببساطة على سمعة المُصدر. عرف المطلعون على القطاع المالي أن القيمة الحقيقية يتم التعبير عنها بالتفصيل و بمصداقية المطالبة. وثالثا، كيف يتم اشتقاق الأرقام؟ هل السجل المركزي مطلوب، أو هل يمكن لأي جهة مصدرة للقيمة الرقمية الحصول على رقم وفقًا للمتطلبات المحلية؟ وأخيراً، هل هناك حد للمساحة؟ تقتصر أرقام الأعداد الصحيحة كما يتم التعبير عنها في الحزم (أو ال packets) بشكل عام على بعض كمية وحدات (البت) مثل 32. اما بالنسبة إلى هندسة البرمجيات، يجب أن تكون هناك حدود، ولكن هل تحتاج هذه الحدود إلى الحد من إمكانيات العمل؟

(II
3- تحدي النجاح:

سيتم استخدام أي نظام ناجح بطرق تجعله يبدو معطلاً. ونحن كمهندسين للبرمجيات نحتاج إلى تقديم اختراعاتنا بتواضع صانعي الأدوات لأجيال المستقبل من البناة و ليس كبيروقراطيين يخططون لتقسيم مساحة التجارة الرقمية.

ما الذي يحدث عندما مررنا بالمتبنين الأوائل اللذين سيطروا على الأجداد ثم تتحول المنافسة إلى منافسة شرسة مع مجموعة كبار السن المتقاعدين؟ ولنتخيل معاً حبوب نعناع تملأ جيوب الملايين من المواطنين العاديين الذين يلعبون هذه اللعبة الخاملة أو تخيل عالماً مع جهة إصدار لنقاط الولاء الرقمية على كل مقياس ركن ،أو حيث يجب على الطلاب دفع رسوم التعليم باستخدام أسهم الأرباح المستقبلية. سبق أن رأينا موسيقيين شعبيين يبيعون الروابط المدعومة بموسيقاهم [7] ،ومقترحات لإصلاح أخطاء البرامج الممولة من قضايا التوريق إلى مستخدمين مجهولين [8].

(II
4- السند الصفري:

ولنتأمل هنا السند الصفري الذي يمثل أداة تدفع *القيمة الإسمية* للعملة في تاريخ معين. ولعل *الصفر* هو أبسط أداة مالية عامة في الاستخدام المشترك وقد شكل المعيار لتصميمنا. لوصف القيمة الاسمية وعملة القيمة الاسمية وتاريخ انتهاء صلاحية هذا السند، سنقوم بإضافة عناصر إضافية إلى المجموعة المذكورة أعلاه. ولكن هذه مجرد بداية. في وصفه لسندات اليورو، يتوقع نويل كلارك عشرات أو مئات الحقول [9]. إذا فحصنا إحدى هذه الخصائص فقط، على سبيل المثال *خيارات الوضع المتعلقة بالحدث*، نجد أن السند يحتاج إلى وصف ما يحدث في الحالات التالية :

- استيلاء عدائي أو ودي على المُصدر
- سيطرة جهة إصدار طرف آخر
- إعادة التمويل
- برنامج إعادة شراء بواسطة جهة إصدار أسهمه، أو
- توزيع أصول أعلى من نسبة مئوية معينة من صافي قيمة المسألة.

ترتبط هذه العناصر بإحكام بالأداة المعنية، ولكنها تمثل صعوبات لمخطط البرامج. هنا يمكننا تقديم عدد من الملاحظات. أولاً، كل حدث ليس بسيطاً. واليوم قد يكون بوسع المرء أن يضيف و بصعوبة فكرة "الاستيلاء العدائي أو الودي" إلى زوج واحد من الأسماء والقيمة،ولكن هذا لن يبقى على الساحة المتطورة من التنظيم والتقاضي التي تنطبق على مثل هذه الأحداث. ثانيا، ليس هناك ما يدعو إلى الاعتقاد بأن القائمة المذكورة أعلاه كاملة. ثالثا، لن يكون من الصعب فقط تصميم حقل واحد من أي نوع لمواكبة ذلك، بل سيكون في الغالب مليئ بنص قانوني. ضع في اعتبارك نقطة عرض تخطيط البيانات. ولوصف المستند الذي يشكل الأساس لسند ما، سوف نحتاج إلى قاعدة بيانات ذات هيكل شجري من المجموعات كحد أدنى. و فضلاً عن ذلك ،فإن هذا التخطيط لن يسجل نجاحا إلا في أداة واحدة، أو مجموعة واحدة شديدة الإحكام من الأدوات التي تكاد تكون قابلة للاستبدال.

(II
5- النقد هو الملك:

وقد تكون العملات أو النقد بمثابة المجموعة الضيقة. فالدولار في نهاية المطاف دولار واحد أحد. هل يمكننا وصف المال ببعض المجموعات البسيطة؟وحتى بالنسبة إلى النقود، فنحن نزعم أن مخططا للمجموعات ليس كافيا. وإذا تناولنا قضية الدولار الرقمي

الصادر عن البنك، ستكون الدولارات الرقمية مشتقات مالية و مدعومة غالباً بودائع بنفس القدر.
قد يكون هذا كافياً لأغراض التسويق ولكنه لن يبقى على قيد الحياة بعد تحليل مالي جاد. لنقارن بين هذه الاستثمارات المشتقة بالدولار وتلك التي أصدرها مجلس الاحتياطي الفيدرالي الأميركي. ولم ينكر بنك الاحتياطي الفيدرالي بعد قبول أوراقه النقدية إذا ما قدمت بنفس الشيء، إذا كان فقط كمطالبة في مجموعة أخرى من نفس الأداة، أو كمطالبة عن الخصوم الضريبية. وإذا نحينا التفسيرات المتطرفة جانبا، فإن بنك الاحتياطي الفيدرالي لم يقدم قط طلباً للإفلاس ويظل رهاناً قوياً إلى حد كبير. ولا يجوز لنا أن نقول نفس الشيء عن أي بنك مصدِر لدولارات المشتقات المالية.
وسوف تكون دولاره الرقمية مدعومة بودائع لدى المؤسسة...بعينها . فمثل هذا البنك قادر على إغلاق أبوابه في أي وقت، ونظراً لتاريخ القطاع المصرفي في القرن العشرين فيتعين على أحد المحللين أن يتعامل مع هذه المجازفة بجدية. وعلاوة على ذلك، في الولايات المتحدة الأمريكية على الأقل، قضت مؤسسة التأمين على الودائع الفيدرالية بالفعل بأن الأموال المودعة على كمبيوتر شخصي للمستخدم تعتبر ودائع غير مؤمَّنة [10]. وهذا لا يعني أن أي بنك على وشك إغلاق الأبواب، بل يعني التساؤل عما يحدث عندما تعجز جهة الإصدار عن الوفاء بوعدها حقا؟ أي مالك لأي أصل ينطوي على مخاطر. يحمل حائز الدولار الإلكتروني خطر فشل المُصدر، أي مالك لأي أصل ينطوي على مخاطر. يحمل حائز الدولار الإلكتروني خطر فشل المُصدر،يحمل صاحب دولار جهة إصدار أخرى خطراً مشابهاً ولكنه مميزا. وينتج عن كل من هذه المخاطر تكلفة ينبغي طرحها من القيمة الاسمية للدولار لحساب قيمة نسبية. وفي هذا التمييز بين المخاطر تكمن حقيقة لا مفر منها وهي أن أي دولار معين ليس له قيمة ثابتة وحتى إذا ما قيس هذا الدولار في مقابل دولار معروف مثل ذلك الذي أصدره بنك الاحتياطي الفيدرالي.

(II

6- الطباعة الدقيقة للعقد:

وإذا لم يكن هناك ما قد نطلق عليه الدولار الواحد، فما الذي يتبقى؟ ومن الواضح أننا لابد وأن نصف *كل* دولار عن *كل* دولار. ويبدو أن هذه مهمة طباعة وتفاصيل دقيقة، والواقع أن *كل عملة صادرة متميزة تشكل عقداً واضحاً بين المصدر والحائز*. يمكن أن يقوم العقد بتضمين التفاصيل. ولنتأمل هنا عقود العملة السيادية الأصلية التي وعد فيها المصدر بدفع أوقية من المعدن النفيس لحامله. و بالفعل هاته هي أربعة معطيات في العقد : أي سيادية، "تدفع لحاملها" فماذا ستدفع وكم منها. وهذا يعني أن كل السندات، وكل عملة، وأي أداة مالية تتسم بأي قدر من التعقيد. والواقع أن مسألة كيفية التعامل مع أداة مالية في إطار المجال الرقمي تقلل إلى حد كبير من كيفية التعامل مع العقد. أو المشكلة هي عقد. فالمسائل التي تدخل في نظم الدفع الاخرى لها عقود ولكنها لا تتضمن سوى وثائق ملحقة مثل اتفاقات المستعملين. و في كثير من الأحيان، يكون دورهم وأهميتهم عرضة للمعارك التي تريد التسويق إخفاؤه. بينما حسب ما يقول القانون يجب أن يكونوا موضع اهتمام في وجه المستخدم في جميع الأوقات. وبمجرد أن نقبل أن تكون المشكلة عبارة عن عقد، تصبح المهمة بسيطة ألا وهي إنشاء عقد يمكن ربطه بنظام الدفع كمحور. هذا هو موضوع القسم التالي.

III- نظام العقود الرقمية لعملية الإصدار:

ومن الأفضل أن ينظر إلى جميع جوانب العقود الركاردية تقريبا من خلال دراسة أمثلة ولا يتناول هذا الفرع إلا بإيجاز التفاصيل البارزة قبل مناقشة العواقب. يمكن العثور على أمثلة على الموقع /webfunds.org/ricardo/contracts .

(III

1- تعريف :

ويمكن تعريف العقد الريكاردي على أنه مستند واحد هو : أ) عقد عرضه مُصدر على المُصدِر لحاملي السندات ،ب) لحق قيم يحتفظ به أصحاب العقود ويديره المُصدِر، ت) يسهل قراءتها من قبل أشخاص (مثل عقد على الورق)، ث) يمكن قراءتها بواسطة البرامج (يمكن قراءتها مثل قاعدة البيانات)، ج) الموقع رقمياً، ح) يحمل المفاتيح ومعلومات الخادم، و(خ) متحالف مع معرّف فريد وآمن.
وبكل بساطة ممكنة، يعتبر العقد الريكاردي وثيقة تحدد نوع من القيمة في الإصدار على شبكة الإنترنت [11]. ويحدد الجهة التي وقعت على الوثيقة وأي أحكام وشروط يراها المصدر مناسبة لكي تضاف وتجعل الوثيقة عقداً بالفعل يجب أن يكون المستند نفسه قابلاً للقراءة بواسطة الأشخاص ويمكن قراءته بواسطة البرامج. يتم تنسيق العقد الريكاردي كملف نصي يمكن قراءته بسهولة (عرضه أو طباعته) ويمكن للبرامج تحويله إلى نماذج داخلية للبحث عن أزواج "قيم الأسماء" أو ما يسمى بال "name-value" . وهو يتضمن مقطعاً خاصاً لكل نوع من العقود، مثل السندات والأسهم والعملة، إلخ. تصف الأقسام الأخرى استخدام النقاط العشرية والعناوين والرموز و ذلك باستعمال مصطلحات التحليل البرمجي التي تلقب ب "program-parsable terms" . وكموقع قانوني، يوقع الجهة التي وقعت المستند في نموذج نص OpenPGP واضح بمفتاح توقيع العقد [12]. وهو يتضمن السلسلة الكاملة لمفاتيح OpenPGP داخل المستند للسماح للبرامج بالتحقق والمصادقة مباشرةً.لتحديد العقد بشكل فريد، يمكن لأي مستخدم حساب "ملخص رسالة معيارية" (أوcanonical message digest) عبر المستند الموقع عليه بشكل واضح. يتم تضمين خلاصة الرسالة هذه في كافة سجلات المعاملات، وتوفر ارتباطًا آمنًا (لا يمكن أن يغفر له) من المستند إلى حساب المشكلة. على سبيل المثال، e3b445c2a6d82df81ef46b54d386d23ce8f3775 هو ملخص الرسالة الكاملة لشركة Systemics انك في إصدارها لخدمات الدفع المسبق بالدولار. ويسمى موجز الرسالة عادة التجزئة(Hash)، وهو أسلوب تشفير لإنشاء رقم صغير نسبياً يكونفي علاقة مباشرة مع المستند. أي أنه لكل مستند توجد تجزئة واحدة فقط وتشير التجزئة بشكل فريد إلى ذلك المستند. الخوارزمية(the algorithm) هي المعيار المعروف ألا وهو SHA1.

(III

2- بعض الملاحظات:

وتبرز الملاحظات التالية مدى قوة النتيجة.
تحد التجزئة من "الغليان الضفدع" أو "frog-boiling". ويُعرف التغيير التدريجي في العقد من قبل الطرف الأقوى بمرور الوقت *باسم "غليان الضفدع"*. الطرف الأقوى هو المُصدر بشكل عام، ويمكن أن يتوقع منه تغيير العقد إذا كانت هناك فائدة. وهذا يعتبر بالهجوم متكرر. ومن نتائج استخدام معرف التجزئة أنه لا يمكن لاي من الطرفين تغيير العقد تعسفيا أو خلسة.
ولكي تتبين لنا صحة هذا الأمر، نحتاج إلى فحص السجلات التي تشير إلى التجزئة. يمكن للتطبيق توقيع كل السجلات المهمة (على سبيل المثال، الدفعات والرموز المميزة والإيصالات والأرصدة) وهذه السجلات الموقعة تتضمن تجزئة العقد الريكاردي. لا يمكن تغيير التجزئة الموجودة داخل السجل دون فقدان قدرتها على اجتياز اختبار صلاحية التوقيع.
وبالمثل، لا يمكن تغيير العقد دون فقدان علاقته بالسجلات التي تم توقيعها وتسليمها بالفعل. وبعبارة أخرى، فإن كل سجل يحتفظ به كل مستخدم يتضمن نسخة غير قابلة للتغيير من هذه التجزئة. ويؤدي أي تغيير في العقد إلى إنشاء تجزئة جديدة، ولا تكون التجزئة الجديدة هي التجزئة التي يكون لدى المستخدمين أو قيمتها.

وهذا يبلور العقد لكلا الطرفين، مما يمنع الطرف الأقوى من تعديل العقد بمهارة في مرحلة لاحقة. وهذا إلى حد ما يعالج عدم توازن القوى بين مقدم الخدمة والعميل في عرض عقد النموذج. ولا خيار للطرف الأقل أهمية للتفاوض، ولكن لا خيار للطرف الأكبر في المطالبة بعقد متميز في وقت لاحق. ويأتي هذا التقييد ببعض التكاليف.إذ يمكن أن يكون مصدر إزعاج لفريق الدعم في تلك الأداة المالية.

و يجعل PKI الريكاردي الأمور واضحة. وتحمل عقود ريكاردو معهم بنيتهم الأساسية العامة الخاصة ("PKI"). المفتاح العام الأعلى لشركة Issuer مدرج في العقد، كما يوقع على مفتاح توقيع العقد، والذي يتضمن أيضاً. يوقع مفتاح توقيع العقد على العقد نفسه. وهذا يحقق عدة أمور. أولاً، يمكن لبرنامج العميل التحقق من سلسلة التوقيع الرقمي بالكامل بتسلسل تلقائي واحد. ثانيا، لا حاجة إلى مرفق المفاتيح العمومية المتعدد الأحزاب المعقد. كل المفاتيح موجودة، ولا حاجة للذهاب للبحث عنها على الشبكة. وهذا يزيل هجمات الاستبدال حيث يمكن إدراج مفتاح قد يجتاز بعض الفحوصات في مرحلة بحث رئيسية معينة. كما أنه يقلل التكاليف بشكل كبير. كان الطلب الأصلي هو نظام تداول السندات [2]. أما بالنسبة للتداول، فإن العنصر الأساسي هو نظام التحويل أو الدفع الذي يتلقى تعليمات التحويل ويتصرف على أساسها لنقل الأدوات (النقدية، السندات) من حساب إلى آخر. وبمجرد تنفيذ العقد لفترة من الوقت، فإنه يحدد مصدر انبعاده من خلال الحضور والاعتماد من قبل الجمهور المستخدم. وهذا يوفر أدلة أكثر إقناعاً من توقيع المُصدر نفسه وبمجرد أن ينفق المُصدر والجمهور الوقت والمال وبالاعتماد على العقد، من خلال عملية التجزئة، من الصعب على المصدر أن يتراجع عن طبيعة العقد أو توقيعه. والنتيجة هي البنية التحتية للمفتاح العمومي التي توفر موثوقية فائقة من طرف إلى آخر، استناداً إلى مستند واحد. وهذا ببساطة غير موجود في تصميمات أخرى للبنية التحتية المفاتيح العمومية(PKIs) [14]. وهذه الموثوقية تجني في مرحلة حل المنازعات، حيث نقترح أن العقد الريكاردي يمكن أن يقف وحده على أساس مزاياه ولا يتطلب أي وصف معقد لملحمة المفاتيح العمومية ،التوقيعات الرقمية، أو الإشارات إلى أطراف ثالثة غير مؤكدة لتعزيز مصدر الدعم.
وبضم المفاتيح، يمكننا رسم خطين بسيطين في العقد، مؤكدين :"هذه العلامات الرئيسية التي هي المفتاح، والتي توقع العقد. المفتاح الأول هو المفتاح الأعلى مستوى للشخص الذي وقع على هذا العقد. هذه هي القصة كاملة ،سيدي القاضي."

التحقق من صحة مفتاح جهة الإصدار. وتنقسم كافة بروتوكولات التشفير الجيدة إلى جزأين، الأول يقول للثاني "ثق بهذا المفتاح بالكامل."
ويقوم المفتاح ذو المستوى الأعلى لمصدره في النهاية بمصادقة العقد. كما تسمح المفاتيح والمعلومات الأخرى الواردة في العقد بالبروتوكول مثل (SOX) الخاص بتمهيد اتصال آمن للغاية بالخادم [15]. و كيف بعد ذلك لك أن تتحقق أنّ هذا المفتاح النهائيّ هو حقّا ملك المصدر؟ وهذا ليس بالأمر الصعب.
تشمل عملية إصدار التكنولوجيا الرقمية في الأعمال التجارية الكثير من بناء العلاقات بين المُصدرين والمستخدمين. تنطوي العديد من التفاعلات المختلفة على فرص لبناء الثقة. على سبيل المثال، من موقع الويب خاصته، يمكن للمصدر نشر العقد والمفاتيح والأغماد، وجعل مواقع أخرى تعكس مضامينهم. سيتم توزيع القيمة الصادرة عن طريق الدفعات التي تتضمن التجزئة. وعادة ما تقوم جهة موثوق بها بالفعل بتسليم هذه الدفعات. وتحدد المدفوعات العقد على نحو سليم وتستمد صحته من التجزئة.
قارن ذلك بالافتراضات في x.509 بنية المفاتيح(أو PKI) وراء استعراض SSL/HTTPS (ما يلي قابل للنقاش بدرجة كبيرة، ولكن يتم تقديمه للمقارنة فقط). وفي تلك البنية التحتية للمفتاح العمومي، كان هناك زعم في الأصل بأن المستخدم سيقدم بطاقة الائتمان الخاصة به إلى مواقع لا علاقة لها بها سابقاً ولا طريقة لها لتحديد مصدر مفتاح الموقع. وهكذا تم وضع طرف ثالث موثوق به ، وهو هيئة إصدار الشهادات للتأكد من المفتاح.

فالمدفوعات والتجارة ومسائل التمويل هي أساسا غنية بالعلاقة. طبيعة المال والتمويل هي أن المشاركين دائماً ما يجتهدون على النحو الواجب، فهم يفضلون الاستماع إلى أقرانهم الذين يثقون بهم بالفعل، ولا يقبلون كلمة حزب مستقل بسهولة. وبالتالي، لا يوجد مكان لطرف ثالث مركزي للوقوف ومصادقة المشغلات. قبل أن يرغب المستخدم في وضع أي قيمة على دفعة معينة من المؤكد أن يكون على معرفة بالعقد عن طريق وسائل أخرى.

افتراض الحيازة. استخدام التجزئة كمعرّف هو حل وسط حيث أنه غير واضح للإنسان [16]. ومع ذلك فإن هذه التسوية تحقق فائدة غير متوقعة. *فإن استخدامها يجعلنا نفترض أن المستخدم لديه العقد.* لكي نوظف مسألة القيمة، مثل عملة، يجب أن يكون لدى المستخدم التجزئة في السجلات المنطبقة. أي إذا تلقى المستخدم دفعة، فسيشمل سجل الدفع هذا التجزئة. وبما أن التجزئة ليست وصفية، فإن ذلك يعني أن المستخدم بحوزته العقد من أجل ترجمة المسألة. ولكي تتثبت من صحة هذا الأمر، تخيل أن لديك سجلاً مع التجزئة ولكن دون الحصول على العقد. أول ما سيحتاج إليه المستخدم هو قاعدة بيانات للمعلمات التي تخبره بما تشير إليه التجزئة. على عكس المبلغ المدفوع في 10 من "GBP"، لا يمكن فهم المبلغ المدفوع w الذي قدره 1000 في "bb972097...". كيف يمكن للبرنامج أن يتنبأ بما يحتاج المستخدم إلى معرفته عن التجزئة؟ و سرعان ما يتضح أن البرنامج أفضل حالاً عند تخزين مصدر المعلومات - العقد الكامل نفسه - حيث إنه يزيل درجة غير محدودة من التعقيد في تخزين المعلومات المتوسطة أو الثانوية.

لا يزال البرنامج يعمل مع التجزئة فقط. ومع ذلك، سيكون أعمى تماما عن دلالات الصك. وقد يكون هذا النهج المتعجرف مقبولاً في الاتصالات والتخزين، ولكنه يعادل بالنسبة لبرامج المستخدم الفشل المؤلم ولمواجهة هذا الأمر، فإن البرنامج الذي يقوم على جانب العميل يهتم بشكل خاص بالحصول على العقود والاحتفاظ بها. ولمواجهة هذا الأمر، فإن البرنامج الذي يقوم على (الطريقة الأولى أو "client-side") يهتم بشكل خاص بالحصول على العقود والاحتفاظ بها. ومن ثم، يمكننا أن نبين الافتراض بقدر من الثقة: ففي نظام فعال، يكون المستخدم قد توفر لديه العقد الريكاردي كاملا (وإن كان ذلك تحت سيطرة البرامج).
هذه خطوة صغيرة فقط لبرنامج العميل، ولكنها قفزة عملاقة إلى الأمام للعلاقة بين المصدر والحامل. وعلى وجه التحديد، فإن وجود افتراض قوي بأن المستخدم لديه العقد الكامل المتاح سيبسط العديد من الجوانب القانونية المتعلقة بمسؤوليات المُصدر. (فنحن نقترح وبالتالي نعترف بالعواقب القانونية المترتبة عن مصطلح *الافتراض*، ولكن لا المجال ولا الخبرة تسمح بالمزيد في هذه الوثيقة.)

(III
3- الأركان الأربعة للصفحة :

ويوفر العقد الريكاردي مصدرا ثرياً للمعلومات الاولية الكاملة. القصة الكاملة موجودة في شكل نصي، في المعلمات القابلة للتحليل، وفي سلسلة التوقيع. وهكذا، فإن الهجوم القانوني المعادي لا يحظى، في إطار نزاع، بقدر أقل من المناورة، ولا يمكن إلا أن يؤكد الوقائع كما ينص عليها العقد. ونيتنا هنا هو أن العقد هو بداية المناقشة ونهايتها ؛ ونحن نطلق على هذا المبدأ *قاعدة العقد الواحد*. وتشير الأخوية القانونية إلى "العقد الذي تحده *أركان الصفحة الأربعة*". من خلال توضيح كيفية وضع مستند قابل للقراءة بعناية، مع توقيع رقمي يمكن التحقق منه، ومعرّف لا يغتفر يرتبط بكل سجل، ويمكننا أن نطلب من السلطة القضائية أن تقبل بسهولة أكبر أن الوثيقة الوحيدة التي تقدم هي بالفعل العقد الصحيح الذي اتفق عليه الطرفان.

IV- الخاتمة:

العقد هو حجر الأساس في الإصدار [17]. إن ابتكاراتنا هي التعبير عن جميع التفاصيل البارزة لإصدار ما كعقد لا يغتفر و يرتبط بشكل غير قابل للتغيير أو التزوير بكل إجراء داخل نظام الدفع. وبهذه الطريقة، يمكن أن يتطور الابتكار المالي وفقا للخطوط التي كان يقوم بها دائما، عن طريق الابتكار في إطار العقود. بترجمة مؤسسة العقد إلى المجال الرقمي، نبني على خبرة القرون وحتى إلى ألفية في التوثيق، تقاسم معنى الاتفاقات بين الأطراف والنزاع بينهما.

(IV
1- تحدي التعقيد :

ولتسجيل التعقيد، يمكننا وضع المستندات مثل العقود في شكل إلكتروني وتوقيعها باستخدام تقنيات التوقيع الرقمي مثل OpenPGP. والنتيجة هي تناظرية معقولة لعقود الورق والحبر التي يعتاد عليها معظم الأشخاص والشركات، مدعومة بتكامل التشفير ومع تعيين التجزئة كمعرّف، يمكن للبرنامج الآن أن يقوم بتبيين الترتيب المالي المعطى و ذلك بشكل فريد، كما يمكنه تأكيد سلسلة قوية من التواقيع. وتعني التجزئة أن المستخدم لديه العقد المتوفر في جميع الأوقات، ولا يمكن تغييره دون أن تتم ملاحظته.
يوفر العقد الريكاردي فائدة كبيرة للمُصدر ألا وهي الوضوح في العديد من الأسئلة القانونية ومسائل دعم العملاء. ويستفيد المستخدم من انخفاض التكاليف العامة وتحسين عرض المعلومات في إطار أكثر اتساقا.

(IV
2- الدروس المستخلصة:

وقد تم استخدام هذا النموذج بنجاح منذ عام 1996. ومنذ ذلك الوقت، قدمت نحو 20 أداة مالية من دون أي فشل.

النزاعات. وقد ظهر العقد الريكاردي في محفلين متميزين لحل المنازعات لحل المطالبات [18].ومن الناحية السردية، تم حل كل مطالبة بصورة مباشرة وفعالة ودون أي جلبة لا داعي لها، بمجرد الإشارة إلى العقد الريكاردي المنطبق.

التشغيل التلقائي. ولم يكن هناك حاجة إلى آلية تُبرمجة إلا قليلاً نسبياً. في الممارسة العملية، تم إدراج الحقول وتوحيدها بحيث يمكن للبرامج استخراج التعشرية (بالدولار مقابل السنتات) ،ملصقات للوحدات (بالدولار الأمريكي مقابل الدولار)، وعناوين المُصدر والمشكل. وعلى النقيض من التوقعات، لم يكن هناك طلب بتحليل كل حقل.

التكلفة. وقد قورنت تكلفة هذا المفهوم إيجابيا مع تكلفة نظم الدفع الاخرى. وينطوي إعداد نص العقد على بعض التكاليف، ولكن ليس أكثر من مجرد اتفاق من اتفاقات المستعملين. تضيف متطلبات البنية الأساسية لـ OpenPGP (المفاتيح والتوقيع) بعض التكاليف الثانوية إلى المُصدرين، ولكن يمكن تعويضها بسهولة عن طريق فوائد تقليل المخاطر من توزيع العقود . وقد ساعد محررو التوقيع على العرف في خفض هذه التكاليف [19].

(IV
3- تحديات المستقبل:

التصفيف. إن وضع العقود في طبقات هو حاجة وشيكة. يمكن للعديد من الشركات أن تتخذ مجموعة قياسية ومحددة من المصطلحات وأن تعتمد عليها مباشرة. وهناك عقود أخرى ناجمة عن عقود سابقة وتحتاج إلى الرجوع إليها.

XML (أو أكس أم ال). وقد أشارت المجهودات الأولية إلى أن XML سيكسر قاعدة عقد واحد, ولكن يبدو أننا سنحتاج إلى شيء أفضل من صيغة هذا العقد القديمة [20]. و من احدى أحد العروض الحديثة نجد إيصال XML والذي يتوقف عن تقديم نفسه كعقد [21].

قانون العقد. وقد تثير معاملة العقد الريكاردي كعقد أسئلة قانونية أكثر مما تجيب عليه. على سبيل المثال، هل هذا النموذج عقد حقا؟ كيف تنظر السلطات القضائية إلى مفاهيم (القانون العام، القانون المدني، UCC ، و القانون القرآني)؟ هل هذا عقد تم التفاوض عليه أم نموذج؟ متى قبل المستخدم العقد؟ ما مدى قوة الافتراض بأن المستخدم لديه العقد أو إمكانية الطعن فيه؟

العقود الذكية. ومن خلال توحيد جميع المعلومات في ملف يمكن قراءته بواسطة البرامج، هناك إمكانيات معززة للعقود الذكية [22]. لم نتجاوز هذا الاتجاه عن طرق معالجة الأعداد العشرية. ويرجع هذا في مرحلة أولى إلى الافتقار إلى الطلب، و في مرحلة ثانية يرجع إلى عدم وضوح الكيفية التي قد تتعامل بها المحكمة مع برنامج كمبيوتر مقترح كعقد.

فهرس

[1] Originally introduced in Ian Grigg, "Financial Cryptography in 7 Layers," *4th Conference on Financial Cryptography,* Anguilla, 2000, Springer-Verlag LNCS 1962. All papers are at http://iang.org/papers/
[2] Ian Grigg, "Digital Trading," *Virtual Finance Report*, November 1997.
[3] Country and Currency Codes, ISO3166-1.
[4] Bryce Wilcox, open design review, *DigiCash's developer list,* <ecash-dev@digicash.com>, August 1997.
[5] Ibid, Rachel Willmer, 14 August 1997.
[6] Robert Hettinga, " What's a Digital Bearer Bond?" *e$ rants* , 19th November, 1995
[7] Alex Tajirian, " David Bowie Bonds,"
[8] Ian Grigg and C. Petro, "Using Electronic Markets Achieve Efficient Task Distribution," *1st Conference on Financial Cryptography* , Anguilla, 1997, Springer-Verlag LNCS 1318.
[9] Noel Clarke, *Guide to Eurobonds*, The Economist Intelligence Unit, 1993.
[10] FDIC General Counsel's Opinion No. 8; Stored Value Cards, *Federal Register*, August 2, 1996. Also see the (readable) Press Release entitled FDIC will Continue to rely on General Counsel Opinion rather than issue rules on Stored-Value Cards, 24 June 97.
[11] Ian Grigg, Guide to Ricardian Contracts, *WebFunds project*.
[12] Jon Callas, et al, "OpenPGP Message Format," *Internet Draft*, RFC2440bis (-10 draft).
[13] Petros Maniatis, Mary Baker "Secure History Preservation through Timeline Entanglement" , *11th USENIX Security Symposium*, San Francisco, USA. August 2002.
[14] Jane K. Winn, " Couriers without Luggage" 49 *South Carolina Law Review* 739 (1998)
[15] Gary Howland, "Development of an Open and Flexible Payment System" 1996.
[16] Bryce Wilcox, "Names: Decentralized, Secure, Human-Meaningful: Choose Two", 2003
[17] Metaphor by Martin (Hasan) Bramwell. See "The Contract is the Keystone of Issuance," *Financial Cryptography blog,* 19th September 2003.
[18] *DigiGold v. Systemics*, before the Supreme Court of Anguilla (2001), and thereafter referred to the American Arbitration Association (2002).
[19] Edwin Woudt, ContractSignWizard, *WebFunds project*.
[20] Erwin van der Koogh, "Ricardian Contracts in XML," (presented at) *Edinburgh Financial Cryptography Engineering* (EFCE-2), 2001.
[21] Ko Fujimura and Masayuki Terada, XML Voucher: Generic Voucher Language, *Internet Draft*.
[22] Nick Szabo, " The Idea of Smart Contracts," 1997.