مساهمة في دراسة نظام نقد رقمي وتصميمه*

م. آمال محمد زهير دركل** أ.د. غسان فلوح***

الملخص

تطورت التجارة الالكترونية عبر الإنترنيت وتوسعت في المدة الأخيرة حتى تجاوز حجمها في بعض البلدان حجم الصفقات التي تجري عبر وسائل التجارة التقليدية.

تعتمد التجارة الالكترونية على وسائل دفع الكترونية مثل بطاقات الائتمان وبطاقات الاعتماد والمحفظات الالكترونية وغيرها، لكن لهذه الوسائل عدة مساوئ مثل وجود خطر سرقة رقم البطاقة، وكون صفقات المتعامل بها قابلة للتعقب والملاحقة، وارتفاع العمولة نسبياً حال استخدامها من أجل الدفعات الصغيرة.

أدى ذلك إلى استمرار التعامل بالعملة الورقية مع مساوئها المتمثلة في كبر حجمها ووجود كلفة في نقلها وخطر على حاملها، ولأنَّ تبادلها يحتاج إلى التقاء فعلي بين الأطراف المتبادلة.

وقد نجم عما سبق فكرة الحاجة إلى نوع جديد من وسائل الدفع يجمع بين خصائص النقد التقليدي وميزات وسائل الدفع الالكترونية ويتلافى مساوئ كل منهما، أطلق على هذه الوسيلة اسم النقد الرقمي الذي هو عبارة عن بيانات تحمل قيمة نقدية تُوَلَّدُ بطرائق الكترونية.

وقد طورت عدة أنظمة للنقد الرقمي ولكل منها ميزاتها وحدود وقفت عندها. يبيّن هذا البحث أهم هذه الأنظمة ونظاماً جديداً مقترحاً يحقق متطلبات إضافية للنقد الرقمي لا تحققها الأنظمة السابقة مثل الكفاءة والتجزئة.

الكلمات المفتاحية: النقد الرقمي - التوقيع الرقمي – التوقيع الرقمي الأعمى - التوقيع الرقمي الأعمى المحدود – خطة سكنور– نظام أوكاموتو – نظام براند – قضية اللوغاريتم المتفرد – الشجرة الثنائية للنقد – تابع الخلاصة – خوارزميات إثبات الهوية – البرهان الكتوم – خوارزمية اقطع واختر

* أُعِدَّ هذا البحث في سياق رسالة الدكتوراه للمهندسة آمال دركل بإشراف الأستاذ غسان فلوح

** طالبة ماجستير- قسم هندسة الاتصالات – كلية الهندسة الميكانيكية والكهربائية - جامعة دمشق.

*** أستاذ - قسم هندسة الحواسيب والأتمتة – كلية الهندسة الميكانيكية والكهربائية - جامعة دمشق.

1- النقـــد الرقمـــي Digital cash

1-1 تعريف النقد الرقمي [1]:

النقد الرقمي Digital cash (أو مـا يـسمى E-Coins أو E-money) هو وسيلة من وسـائل الـدفع الالكترونـي المستخدمة في الصفقات الالكترونية، وهو عبـارة عـن بيانات الكترونية (أو بيتات) تُوَلَّدُ باستخدام خوارزميـات رياضية وطرائق تشفيرية وتحمل قيمة نقدية معينة بحيث تكون موثقة (غير قابلة للتزوير) ولا تفصح عن هويـة المتعامل بها، ويمكن للنقد الرقمي أن يخزن وأن ينتقـل عبر أي نوع من أنواع وسائط التخزين مثل الحاسوب أو الهاتف الجوال أو بطاقة ذكية أو عبر شبكات الحاسـب مثل الإنترنيت ويمكن اختباره والتحقق من وثوقيته مهما كان الوسط المخزن عليه.

1-2 مميزات النقد الرقمي عن أنظمة الدفع الالكتروني التقليدية [2]:

هناك العديد من أنظمة الدفع الالكترونـي مثـل بطاقـة الاعتماد وبطاقة الائتمان والمحفظة الالكترونية وغيرها، لكن النقد الرقمي يتميّز عن أنظمـة الـدفع الالكترونـي التقليدية بأنه يتلافى المساوئ الموجودة فيها التي يمكـن حصرها في النقاط الآتية:

1- وجود التخوف عند كثيرين من إرسال رقم بطاقـة الاعتماد الخاصة بهم عبر الإنترنيـت، خـشية مـن أن تُسْرَق من قبل أشخاص يتنصتون علـى شـبكة الويـب ولديهم وسائل خاصة لفك التـشفير والحـصول علـى المعلومات السرية، أو من قبل أشخاص يضعون مواقـع مزيفة تنتحل شخصية شـركات ذات سـمعة معروفـة identity theft وتكون في الواقع عبارة عن فـخ لـسرقة أرقام بطاقات الاعتماد ومن ثم استخدامها، إن اسـتخدام قواعد الأمان والتشفير خفض هذه المخاطر إلا أنـه لـم يقضِ عليها تماماً.

2- يجعل التعامل من خلال البطاقات التقليدية صـفقات المتعامل بها قابلة للتعقب والملاحقة من قبل الـشرطة أو المخابرات أو العصابات، إذ يكون لحامل البطاقة رصيد لدى المصرف مرتبط إما بحساب خاص بـه كمـا فـي بطاقة الاعتماد وبطاقة الائتمان أو مرتبط برقم تسلـسلي كما في المحفظة الالكترونية، ولابدَّ للتاجر من الاتـصال بالمصرف وقت إجراء الصفقة ليتم التحقق من امـتلاك الزبون للرصيد الكافي قبل تثبيت الصفقة.

ومن ثَمَّ يكون المصرف على اطلاع كامل بالعمليات التي يقوم بها الزبون، ويمكن معرفة تفاصيل حياة شخص ما من خلال بطاقة الاعتماد الخاصة به فيمكن مثلاً تعـرّف على الأشخاص الذين يتعامل معهم والأماكن التي يشتري منها حاجياته والأندية التي يشترك فيها وحجـم فـواتير الهاتف والأدوية والأطباء وربما الحالة الـصحية، هـذه التفاصيل كلّها يتم الحصول عليها بسهولة ومـن خـلال الجلوس خلف شاشات الحاسب دون الحاجة لتجشم عناء البحث والملاحقة.

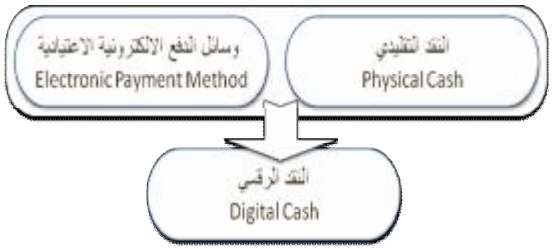
أمَّا النقد الرقمي فهو من وسائل الدفع الالكتروني التي لا يحتاج فيه التاجر إلى الاتصال بالمصرف وقت إجـراء الصفقة وإنَّما فقط يتحقق من قيمة النقد ومن وثوقيته من خلال بيانات النقد الرقمي ذاته.

3- العمولة العالية للصفقات التي تجـري مـن خـلال بطاقات الاعتماد، وذلك لوجـود كلفـة الاتـصال بـين مصرف التاجر ومصرف الزبون من أجل التأكـد مـن الرصيد الذي يحمله الحساب المرتبط بالبطاقة ومـن أن البطاقة ليست في قائمة البطاقات المسروقة أو الضائعة، وهذه الكلفة تكون مرتفعة نسبياً حال استخدامها من أجل الدفعات الصغيرة (Micro Payment) مثلاً ثمـن تـصفح

كتاب الكتروني على الإنترنيت (Digital Browser)، بحيث تصبح العمولة مساوية للثمن المراد دفعه.

هذه المساوئ جعلت كثيرين لا يستغنون عن العملة الورقية على الرغم من مساوئها المتمثلة في كبر حجمها وصعوبة نقلها وتعريض حاملها للخطر، ولأنَّ تبادلها يحتاج إلى التقاء فعلي بين الأطراف المتبادلة، فلذلك طُوِّرَ النقد الرقمي لكي يتلافى سيئات أنظمة الدفع الالكتروني.

ويجمع بين ميزات العملة الورقية Physical Cash وميزات وسائل الدفع الالكترونية الاعتيادية Electronic Payment Method، كما هو موضّح في الشكل الآتي:



والنقد الرقمي مختلف تماماً عن البطاقات المشحونة بمبلغ محدد تخول صاحبها شراء حاجيات أو خدمات معينة مقدمة من قبل مُصدِّر البطاقة، كالبطاقات البلاستيكية التي تتعامل معها كثير من المكتبات في الجامعات الغربية والتي تقبلها آلات نسخ الورق إذْ تحوي هذه البطاقات على الوجه الخلفي شريطاً مغناطيسياً وفي كل مرة يقوم الطالب أو المدرس بنسخ ورقة فإن آلة النسخ تقتطع كلفة النسخ بصورة تلقائية، فإن هذه البطاقات محدودة الاستخدام في حين النقد الرقمي واسع القبول يستخدم في الشراء أوفي الحصول على خدمة من أي جهة، ويمكن أن ينتقل عبر شبكات الويب.

3-1 النقد الرقمي والعملة التقليدية [3]:

إن الهدف من النقد الرقمي كما تم بيانه هو أن يكون بديلاً الكترونياً مريحاً عن العملة التقليدية الورقية والمعدنية والنقد الرقمي يشابه العملة التقليدية في النقاط الآتية:

- كل منهما قيمته النقدية مخزونة فيه وليست مرتبطة بتبعيته لشخص ما أو مصرف أو جهة مالية، خلافاً لأنظمة الدفع الالكتروني الأخرى.
- كل منهما يمكن أن يستخدمه ممتلكه لشراء أي سلعة دون الحاجة لأن يفصح عن هويته.
- كل منهما يوجد بشكل فئات نقدية متعددة كل فئة تمثل قيمة نقدية محددة، وتتميّز قطع النقد التي تنتمي للفئة النقدية ذاتها عن بعضها بأرقام تسلسلية متمايزة لا يمكن أن تتماثل في قطعتين نقديتين.
- كل منهما وسائل حمايته من التزوير مخزونة فيه، فالعملة التقليدية تحوي حبراً مغناطيسياً أو شريطاً معدنياً، أمَّا النقد الرقمي فَتَتَشَكَّلُ بياناته باستخدام خوارزميات رياضية وتشفير تجعل من الممكن التوثق من النقد الرقمي دون الحاجة للاتصال بالمصرف الذي أصدر النقد لأخذ مصادقته.

4-1 الخصائص الأساسية للنقد الرقمي [4]:

يجب أن يتمتع النقد الرقمي بخصائص العملة التقليدية (physical cash) لكي يصحّ إطلاق اسم النقد عليه (digital cash)، التي هي:

1-4-1 الأمان Secure:

يجب أن يكون النقد الرقمي ذا أمان عالٍ بحيث يمنع من تزويره أو تبديل قيمته أو استخدامه للشراء بأكثر من قيمته، ويتم التوصل إلى ذلك من خلال خوارزميات رياضية وتشفير متطورة سيجري بيانها لاحقاً.

2-4-1 سرية هوية المتعامل بها Anonymous:

بمعنى الحفاظ على سرية هوية الشخص المتعامل بهذا

النقد وتسمى هذه الخاصية بحماية الخصوصية privacy protection، وهي تحتاج إلى براعة، واستخدام خوارزميات معقدة بعض الشيء، بحيث تبقى هوية المتعامل بها سرية مادام استخدم النقد الرقمي وفق الشكل الشرعي المسموح به، أمَّا إذا تجاوز هذا الحد فكأنّه استخدمه بكامل قيمته أكثر من مرة فَيُكْشَفُ عن هويته.

سابقاً كان يعتقد أنه لا يمكن إيجاد نظام نقد رقمي يجمع بين المحافظة على خصوصية المستخدم وتأمين المصرف ضد عمليات الاختلاس، ولكن فيما بعد اِكْتُشِفَتْ تقنيات تشفير أسهمت في تحقيق ذلك بطرائق مختلفة، وإلى الآن فإن تحقيق سرية هوية المتعامل موضع تنافس وجدال بين مزودي النقد الرقمي، كما أنه السبب الأساسي الذي جعل الحكومات تحارب النقد الرقمي كما سيجري بيانه لاحقاً.

1-4-3 عدم قابلية الربط بين عمليات الشخص الواحد unlinkability:

بمعنى أن الصفقات التي يقوم بها الشخص الواحد لا يمكن الربط بينها أي لا يمكن للمصرف أن يميّز أنها تابعة للزبون نفسه، إذ إنَّ بعض أنظمة النقد الرقمي تتمتع بالحفاظ على سرية هوية المتعامل بها إلا أنها لا تزود بخاصية عدم الربط بين عمليات الشخص الواحد، ومن ثَمَّ قد يتسبب ذلك في كشف هوية الزبون وتعقب عملياته جميعها إما من خلال تعقب الموقع الجغرافي الذي جرت فيه العمليات، أو من خلال الكشف عن هويته في إحدى العمليات.

1-4-4 قابلية النقل Portable:

بمعنى أن استخدام النقد الرقمي غير مرتبط بوجوده فيزيائياً في مكان مخصص، وإنما يمكن للنقد الرقمي أن ينتقل عبر شبكات الحاسب وخارجها إلى وسائط تخزين أخرى، دون أن يؤثر ذلك في خصائصه الأساسية مثل الحفاظ على الأمان وسرية المتعامل به.

1-4-5 العمل دون اتصال مباشر Off-line capable:

بمعنى أن عملية تسليم النقد الرقمي من طرف إلى آخر (مثل تاجر – زبون) يجب أن تكون متاحة دون الحاجة إلى وجود اتصال مع المصرف الذي أصدر النقد أو مع أي طرف ثالث في أثناء إجراء الصفقة.

1-4-6 ثنائية الاتجاه Two-way:

بمعنى أن الطرف الذي استلم النقد الرقمي في صفقة ما غير مجبر على العودة إلى المصرف لإيداع النقد الرقمي، وإنما يستطيع أن يتعامل بهذا النقد الرقمي من جديد ويمكن أن يسلّمه لشخص آخر في صفقة جديدة.

1-4-7 إمكانية تجزئة النقد Divisible:

بمعنى أن تكون قطعة النقد الرقمي قابلة للتقسيم إلى قطع أصغر منها، أي إنَّ مالك النقد غير ملزم بدفع كامل قيمة قطعة النقد وإنما يمكنه تسليم جزء منه يتناسب مع ثمن السلعة، وكلما كانت الأجزاء التي يمكن التعامل بها أصغر كان النقد الرقمي أكثر مرونة.

1-4-8 الكفاءة Efficiency:

بمعنى أن يكون النظام ذا أداء جيد وسرعة مقبولة ولا يستهلك مصادر حاسوبية مرتفعة ولا كلف اتصالات عالية ناجمة عن تبادل حجم بيانات كبير.

1-4-9 قبول واسع Wide acceptability:

بمعنى أن يكون النقد الرقمي معروفاً بشكل جيد ومقبولاً في كثير من الأوساط التجارية.

1-4-10 سهولة الاستخدام User-friendly:

بمعنى أن يكون النقد الرقمي سهل الاستخدام سواء في أثناء دفعه أو استلامه، أي لا يتطلب من مستخدمه أن يكون على دراية جيدة بالتشفير لكي يستطيع التعامل مع

النقد الرقمي، وإنما فقط أن يكون لديه معلومات بسيطة عن آلية استخدامه.

1-4-11 حرية تحديد فئات النقد Unit-of-value freedom:

بمعنى أن يكون النقد الرقمي بفئات متعددة تُحَدَّدُ من قبل المصرف وليس فئة واحدة، وهذا يتطلب وجود آلية لتمييز فئة قطعة النقد الرقمي أي القيمة التي تحملها.

1-5 النقد الرقمي والتشريعات القانونية[2]:

إن التعامل بالنقد الرقمي حساس بعض الشيء وهناك بعض التشريعات تمنع التعامل بالنقد الرقمي من أجل دفعات أكبر من حد معين لحماية المجتمع من المعاملات المالية غير المشروعة كغسيل الأموال والتزوير، وكذلك شراء بضائع محظورة مثل المخدرات، لأن عدم معرفة هوية المتعامل بها قد يشجع مثل هؤلاء على إنجاز صفقاتهم اللا شرعية، وهناك من أفرد كتابات بعنوان النقد الرقمي والجريمة المتقنة، لأن النقد الرقمي يخفي هوية المتعامل بها أكثر من أي وسيلة نقدية أخرى، فالعملة التقليدية وإن كانت لا تفصح عن هوية المتعامل بها إلا أنها تحتاج على الأقل إلى التقاء على أرض الواقع بين المسلم والمستلم على خلاف النقد الرقمي.

1-6 مواضع المخاطرة في استخدام النقد الرقمي:

1- هناك خطر على الزبون حال استخدام النقد الرقمي لدفع مبالغ كبيرة مقابل سلعة ما، وخاصة أن استلام السلعة في الصفقات الالكترونية ليس فورياً كما هو الحال في الصفقات التقليدية، وقد يحصل أن لا يستلم الزبون السلعة أو قد يستلمها ولكن لا تكون وفق المواصفات المطلوبة، وكما سَيُوَضَحُ لاحقاً فإنه في حال النقد الرقمي لا يوجد دليل على هوية من دفع هذا النقد، ومن ثَمَّ لا يستطيع الزبون تحصيل حقه في مثل هذه الحالات لأنه لا يوجد دليل على أنه دفع نقداً رقمياً.

2- هناك خطر حدوث تدمير لوسط التخزين الذي يحوي النقد الرقمي لأي سبب مثل وجود فيروس أو عطل ما وعندها سيخسر الزبون النقد الرقمي المتوضع على القرص ولن تكون له القدرة على استعادة هذا النقد حتى ولو عاد إلى المصرف الذي أصدره لأن المصرف ليس لديه سجلات تربط بين النقد الرقمي والأشخاص الذين صرف لهم هذا النقد كما سيجري بيانه لاحقاً، وهذه المشكلة يمكن حلّها بإجراءات تخزين احتياطي Backup لهذا النقد على أي وسيط آخر مثل ذاكرة USB التي يمكن أن تكون مزودة ببرامج تشفير بحيث لا يمكن الوصول إلى بيانات النقد إلا بمفتاح خاص.

1-7 الخطوات الأساسية التي يجري من خلالها التعامل بالنقد الرقمي [1]:

1- يقوم الزبون بفتح حساب لدى مصرف النقد الرقمي من خلال الموقع الالكتروني للمصرف على الويب، ويغذي هذا الحساب بأي وسيلة مثل بطاقة اعتماد. وهنا وإن أُرْسِلَ رقم البطاقة وهو أمرٌ غير مرغوب به كما ذُكِرَ سابقاً ولكنه سَيُرْسَلُ مرّة عند كل تغذية جديدة للحساب وليس عند كل عملية شراء، كما يمكن تغذية الحساب تلقائياً من حساب آخر.

2- يقوم الزبون بتنزيل برنامج من موقع المصرف يُدعى برنامج الزبون إذْ يقوم بتركيبه على حاسبه، هذا البرنامج مهمته إدارة النقد الرقمي.

3- عندما يريد الزبون أن يحصل على نقد رقمي فإنه يدخل إلى موقع المصرف ويمر عبر برتوكولات خاصة تنتهي بعملية تنزيل ملف يحوي بيانات قطعة

النقد الرقمي إلى حاسبه، ويقوم المصرف بسحب قيمة قطعة النقد الرقمي من رصيد حساب الزبون، طبعاً قيمة قطعة النقد الرقمي يجب أن تكون محصورة ضمن فئات نقدية محددة يعلن المصرف عنها.

4- عند شراء بضائع أو خدمات من التاجر الذي يقبل هذا النوع من النقد، وذلك عبر موقعه الالكتروني يقوم الزبون بتحميل upload ملف إلى موقع التاجر، هذا الملف يحوي بيانات تتعلق بالجزء المراد صرفه من قطعة النقد الرقمي، أمَّا إعداد هذا الملف فيجري من خلال برنامج الزبون الذي قام بتنزيله سابقاً من موقع المصرف.

5- يقوم التاجر بالتوثق من قيمة بيانات ملف النقد الذي تم تحميله إلى موقعه وصلاحيته، وذلك من خلال برمجيات أُضيفَت سابقاً إلى موقعه بالتعاون مع المصرف، وعند نجاح عملية التوثق يثبّت التاجر الصفقة.

6- يقوم التاجر في وقت لاحق بتسليم ملفات النقد الرقمي التي استلمها من الزبائن خلال عمليات الشراء التي تمت من موقعه إلى المصرف الذي أصدر هذا النقد، وذلك من خلال الموقع الالكتروني للمصرف. فيقوم المصرف بالتأكد من سلامة ملفات النقد وأنه لم يَجْرِ إيداعه مسبقاً ثم يضيف قيمة النقد في الحساب الخاص بهذا التاجر لدى المصرف.

أي إنَّ الأطراف الأساسية المتعاملة في النقد الرقمي هي:

- المصرف Bank.
- الزبون أو المتعامل بالعملة Client.
- التاجر Vender.

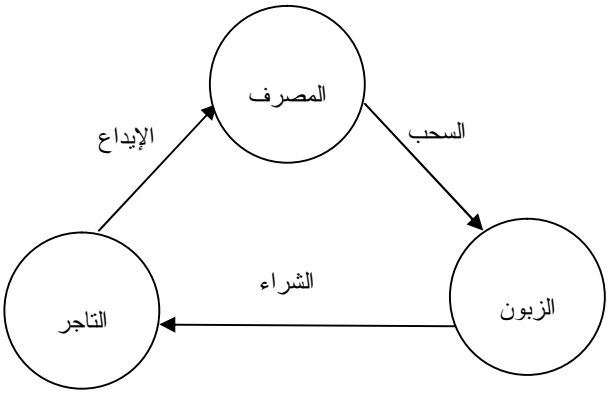
أمَّا العمليات الأساسية التي تجري في نظام النقد الرقمي فهي:

1- عملية السحب (Withdrawal): خلالها يحصل الزبون على النقد الرقمي.

2- عملية الشراء بالنقد الرقمي أو دفع النقد الرقمي (Payment): خلالها يشتري الزبون سلعة ما أو خدمة ما ويدفع مقابلها نقداً رقمياً إلى التاجر.

3- عملية إيداع النقد الرقمي (Debit): خلالها يقوم التاجر بتسليم النقد الرقمي الذي استلمه سابقاً في عمليات البيع الالكترونية إلى المصرف الذي أصدر النقد.

والشكل الآتي يبين مخطط العمليات التي تجري بين الأطراف الثلاثة.



وهنا يمكن ملاحظة أن الصفقة بين التاجر والزبون لا تحتاج إلى مصرف أو أي طرف ثالث وقت إجراء الصفقة كما هو الحال تماماً عند استخدام العملة التقليدية.

2- الأسس التي تقوم عليها أنظمة النقد الرقمي:

تقوم أنظمة النقد الرقمي على أسس رياضية وعلى خوارزميات تشفير معقدة، والكلام عنها واسع تضيق به صفحات هذه المقالة، ولكن سيجري بيان جزء بسيط منها الذي لا بدّ منه لفهم حقيقة النقد الرقمي]5[،]6[، [7]، [8]، [9]

2-1 تابع الخلاصة Hash function:

هو تابع دخله رسالة ذات طول متغيّر (يمكن أن يكون ألف بت أو أقل أو أكثر) و خرجه رسالة ذات طول ثابت (مثلاً 128 bit أو 160 bit) مهما كان طول رسالة الدخل، وفي حال تغيّر بت واحد في رسالة الدخل فإن خرج تابع الخلاصة يتغيّر كلياً.

وهناك نوع خاص من تابع الخلاصة يسمى تابع الخلاصة التشفيري Cryptography Hash function، ويُدعى أحياناً تابع الخلاصة الوحيد الاتجاه One-way hash function إذْ يُستخدم في أنظمة التشفير ويتمتع بوجود حصانة ضد الأمور الآتية:

1- عدم الحصول على الرسالة من خلاصتها.

2- عدم وجود تصادم بين الخلاصات أي عدم وجود رسالتين مختلفتين لهما الخلاصة ذاتها.

يستخدم تابع الخلاصة في أنظمة النقد الرقمي؛ وذلك من أجل التوقيع على بيانات النقد بحيث تُدْمَجُ في رسالة واحدة Concatenation ,ومن ثم تُحْسَبُ خلاصتها، ويتم التوقيع على الخلاصة لا كامل البيانات، إذ إنَّ التوقيع على كامل البيانات مكلفاً من حيث المعالجة وحجم البيانات.

2-2 التوقيع الرقمي Digital Signature:

التوقيع الرقمي يحاكي التوقيع العادي، إذْ يستطيع من خلاله شخصٌ ما ليكن بلالاً الحصول على توقيع شخص آخر لتكن إسراء على مستند ما، ولكن في التوقيع الرقمي يكون المستند المصادَق عليه مستنداً رقمياً وليس ورقياً كما في التوقيع العادي.

ويجب أن يكون التوقيع الرقمي ذا مصداقية بحيث لا تستطيع إسراء بعد مدة أن تنكر أنها وقعت على هذا المستند، وأيضاً يستطيع بلال أن يعرض هذا المستند الموقَّع لطرف ثالث ويثبت له أنه موقع من قبل إسراء.

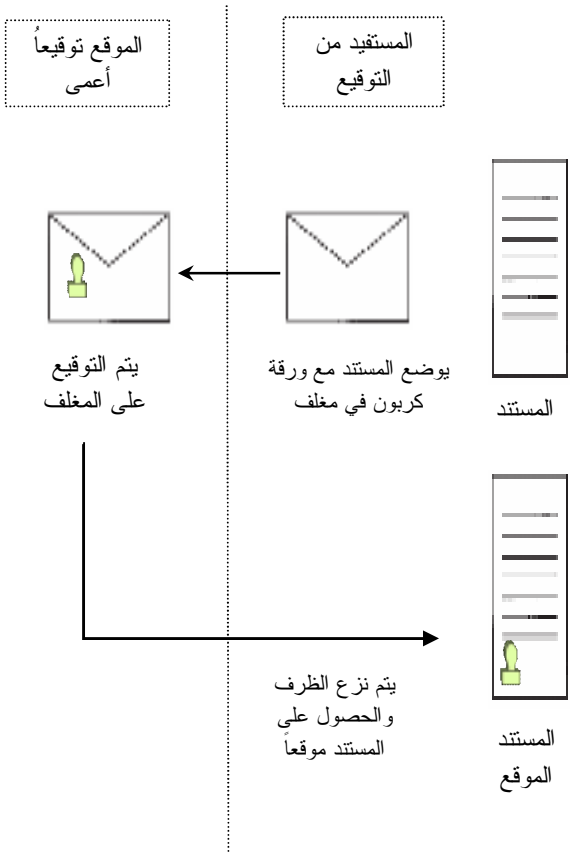
ويستخدم التوقيع الرقمي في النقد الرقمي من أجل توقيع المصرف على البيانات التي تمثل قطع النقد الرقمي، وعندما يستلم التاجر قطعة النقد الرقمي من الزبون فإنه يتأكد من وثوقيتها من خلال اختبار صحة توقيع المصرف عليها، وكذلك عندما يعود النقد إلى المصرف يتأكد أن النقد مصدر من قبله من خلال اختبار صحة توقيعه على بيانات النقد.

2-3 التوقيع الرقمي الأعمى Blind Digital Signature:

هو نوع خاص من التوقيع الرقمي يقوم فيه الموقع بالتوقيع على المستند دون أن يطلع على محتوياته ،أي يوقع على بياض أو على العمياني.

التوقيع الأعمى لا يوجد في الحياة العملية إذ لا أحد يوقع على شيء لم يطلع عليه، لكن لهذا النوع من التوقيع أهمية كبيرة في أنظمة النقد الرقمي، إذ إنَّه_ كما سيتبين لاحقاً_ عندما يريد الزبون أن يحصل على نقد رقمي من المصرف فإن الزبون هو من يقوم بإنشاء بيانات النقد، ومن ثم يقوم بتعميتها باستخدام تابع تعمية ما، بحيث لا يكون للمصرف القدرة على قراءة بيانات النقد ثم يطلب من المصرف أن يوقع عليها توقيعاً أعمى، وبعد توقيع المصرف على بيانات النقد يقوم الزبون بفك تعميتها؛ وذلك باستخدام تابع معاكس لتابع التعمية، وبذلك يكون الزبون قد حصل على بيانات نقد رقمي موقع من قبل المصرف دون أن يراه المصرف ومن ثَمَّ يمكن أن يشتري الزبون بالنقد الرقمي دون أن يكون للمصرف القدرة على تمييزه أن النقد الذي سلمه لزبون معين وإن كان المصرف كغيره يستطيع اختبار توقيع

المصرف والتأكد من أنه موقع من قبله، وبذلك أُلْغِيَ الربط بين النقد وبين الزبون ومن ثَمَّ لا يستطيع المصرف متابعة عمليات الزبون، هناك عدة خوارزميات للتوقيع الرقمي الأعمى مثل خوارزمية[1] RSA وخوارزمية سكنور. والشكل الآتي يبيّن تمثيلاً تقريبياً للتوقيع الرقمي الأعمى:



4-2 خوارزميات إثبات الهوية Identification Schemes:

تعني عملية إثبات الهوية أن يقوم شخص ما ليكن أحمد موجود على شبكة الويب بتقديم البرهان على أنه فعلاً أحمد وليس آخرَ يحاول انتحال شخصيته، ولعملية إثبات الهوية أهمية خاصة في أنظمة النقد الرقمي لأن الزبون عندما يريد من خلال شبكة الويب أن يجري أي عملية تتعلق بحسابه لدى المصرف فإنه ينبغي أولاً أن يبرهن للمصرف على هويته، أي يجب أن يثبت أنه صاحب الحساب وليس شخصاً مخادعاً يحاول القيام بعمليات لا شرعية.

قد يفكر بعضهم أن عملية التحقق هذه يمكن أن تجري بالاعتماد على كلمات سر بحيث يُعْطَى كل زبون كلمة سر خاصة به وتُحْتَفَظُ بكلمات السر الخاصة بالزبائن لدى المصرف. وعندما يريد المصرف أن يتأكد من هوية زبون ما فإنه يطالبه بإدخال كلمة السر، فإذا طابقت مع المخزنة لديه مسبقاً تنجح عملية التحقق، ولكن في الواقع اعتماد هذه الطريقة لا يفي بالغرض فقد يتنصت أحدهم على الشبكة ويحصل على كلمة السر.

ولن يفيد الاستعانة بالتشفير لحماية كلمة السر لأنه إذا تنصت أحدهم على الشبكة وحصل على كلمة السر مشفرةً فإن هذا الشخص يستطيع إعادة إرسالها مشفرة دون الحاجة لفك تشفيرها وعندها، وإن كان ليس لديه المقدرة على معرفتها بشكلها الأصلي إلا أن ذلك لن يمنعه من استخدامها.

لذا كان لا بدَّ من استخدام طرائق إثبات هوية تعتمد على البرهان الكتوم الذي لا يسرب أية معلومات، بحيث يقوم الزبون بالبرهان على امتلاكه لمعلومات سرية مرتبطة بهويته دون أن يبوح بهذه المعلومات أو بجزء منها فتبقى هذه المعلومات محجوبة حتى عن المصرف وفي منأى عن أي مهاجم يتنصت على الشبكة، وفيما يأتي سيجري بيان مفهوم البرهان الكتوم وأوجه استخداماته الأخرى وأهم خوارزمياته.

[1] خوارزمية RSA من خوارزميات التشفير اللامتناظر وتستخدم في التوقيع الرقمي، وكذلك طُوِّرَتْ لتستخدم في التوقيع الرقمي الأعمى.

5-2 البرهان الكتوم Zero-knowledge proof:

البرهان الكتوم يعني أن يبرهن شخص ما ليكن بلالاً لشخص آخر لتكن إسراء على صحة معلومة ما، أو على معرفته لمعلومة ما دون أن يفشي هذه المعلومة لإسراء.

للتقريب بفرض أنَّ هناك مسألة تحتاج إلى حل، وهناك رهان بين بلال وإسراء على أنَّ من يعرف حلها يكن من نصيبه كذا والاثنان يدعيان أنهما يعرفان الحل ويريد كل منهما أن يثبت للآخر أنه يعلم الحل دون أن يفصح عنه، فإن بإمكانه تحقيق ذلك باستخدام إحدى طرائق البرهان الكتوم.

يعتمد النقد الرقمي بشكل أساسي على البرهان الكتوم، وكل نظام من أنظمة النقد الرقمي لا بدَّ أن يستخدم خوارزمية من خوارزميات البرهان الكتوم، والاستخدام الرئيسي لها ليس إثبات الهوية فقط، وإنَّما هناك استخدام آخر أساسي وهو البرهان على صحة بيانات النقد.

إذ إنَّ الزبون في النقد الرقمي كما ذُكِرَ سابقاً هو من يقوم بتشكيل بيانات النقد الرقمي التي يجب أن تحتوي بشكل ما على هويته أو على جزء منها، وذلك بطريقة تضمن بقاء هوية الزبون مخفاة عن كلٍ من المصرف والتاجر مادام استخدم الزبون النقد بالشكل المسموح به، وتكشف هويته في حال استخدام النقد بأكثر من قيمته، وبعد تشكيل الزبون لبيانات النقد يقوم بتعميتها ويسلمها للمصرف الذي بدوره يقوم بالتوقيع عليها توقيعاً أعمى.

ولكي يضمن المصرف حقه فإن عليه أن يتأكد قبل أن يقوم بالتوقيع على بيانات النقد توقيعاً أعمى من أن الزبون قد شكل هذه البيانات وفق هذه الطريقة المطلوبة.

لذلك بعد أن يقوم الزبون بتشكيل بيانات النقد وتعميتها فإنه يبرهن للمصرف على صحة بيانات النقد المعماة التي شكلها وذلك باستخدام خوارزمية من خوارزميات البرهان الكتوم قبل أن يقوم المصرف بالتوقيع عليها.

هناك عدة خوارزميات للبرهان الكتوم أهمها خوارزمية اقطع واختر وخوارزمية سكنور، وفيما يأتي بيانهما:

1-5-2 خوارزمية اقطع واختر Cut and Choose Algorithm:

تستخدم خوارزمية اقطع واختر في بعض أنظمة النقد الرقمي مثل نظام شوم وأوكاموتو، وتجري هذه الخوارزمية وفق الخطوات الآتية:

- يقوم الزبون بتشكيل ليس فقط قطعة نقد رقمي واحدة، وإنما عدد من قطع النقد الرقمي ليكن k، ويسمى هذا العدد بمعامل الأمان.
- يقوم الزبون بتعمية قطع النقد الرقمي التي شكّلها.
- يسلم الزبون قطع النقد الرقمي المعماة إلى المصرف.
- يختار المصرف عدداً k-1 من هذه القطع ويطلب من الزبون أن يلغي تعميتها.
- يتأكد المصرف بعد الاطلاع على بيانات هذه القطع من أن الزبون قد شكّلها وفق المطلوب، وأنّها تحوي بطريقة معينة هوية الزبون.
- يوقع المصرف على قطعة النقد المتبقية التي لم يقم الزبون بإزالة تعميتها.
- بعد توقيع المصرف يزيل الزبون تعمية قطعة النقد الرقمي الموقعة، وبذلك يستطيع الزبون استخدام قطعة النقد ولا يكون للمصرف القدرة على متابعته.

يوجد احتمال لحدوث خداع للمصرف من قبل الزبون وهي أن تصادف القطعة التي لم يطلع عليها المصرف أن تكون فقط هي المزورة من قبل الزبون لكن هذا الاحتمال نسبته قليلة ومساوية لـ $1/2^K$.

وسميت هذه الخوارزمية بخوارزمية اقطع واختر لأن الزبون ولّد عدداً من البيانات، كل منها يمثل المعلومة الأساسية (وكأنه قطّعها إلى عدد من التمثيلات)

والمصرف قام باختيار إحداها للتوقيع واختـــار القطـــع الباقية للتأكد من نزاهة الزبون.

ويمكن ملاحظة أنه من أجل توقيع قطعة نقد رقمي واحدة احتيج إلى توليد عدد من القطع مساوٍ إلى معامل الأمان، وهذا له تأثير سلبي في الأداء من حيث بـــطء المعالجـــة وكبر حجم البيانات المتبادلة مما يعنـــي كلفـــة اتـــصال مرتفعة، إذْ إنَّ حجم البيانات المتبادلة أكبر بأضعاف من البيانات الفعلية المراد توقيعها.

2-5-2 خوارزمية سكنور:

تستخدم خوارزمية سكنور للبرهان على حيازة معلومة ما دون الإفصاح عن هذه المعلومة، وعـــادة تكـــون هـــذه المعلومة عبارة عن قيمة مرتبطـــة بهويـــة الـــشخص لا يعلمها إلا صاحب الهوية ومن ثَمَّ فـــإن البرهـــان علـــى معرفة المعلومة يعني إثبات الهوية، وخوارزمية سكنور من أهم خوارزميات إثبات الهوية.

وقد طُوِّرَتْ خوارزمية سكنور وتُوّسِعَ بها بحيث أمكـــن استخدامها في كل من التوقيع الرقمي والتوقيع الرقمـــي الأعمى المحدود الذي هو عماد نظام براند للنقد الرقمي كما سَيُوَضَّحُ لاحقاً.

وتقوم خوارزمية سكنور بشكل أساســـي علـــى نظريـــة اللوغاريتم المتفـــرد The Discrete Logarithm Problem (DLP) .

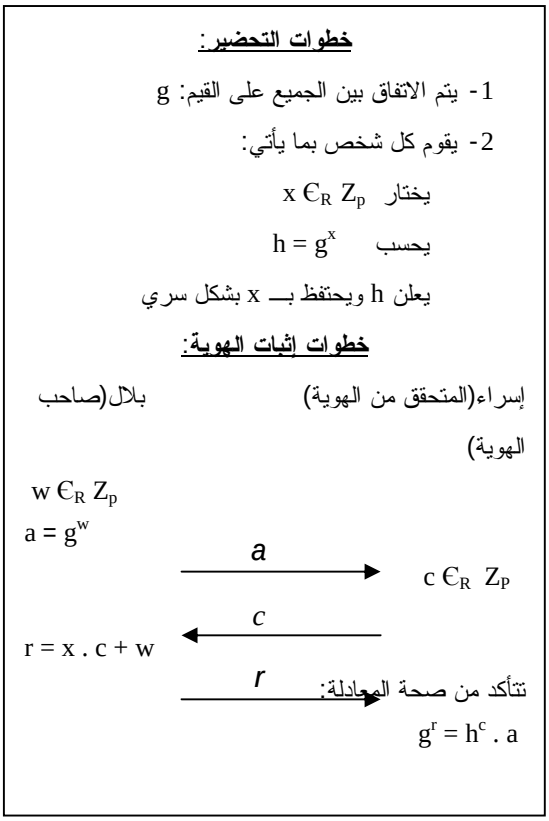
تقوم نظرية اللوغاريتم المتفرد على حقيقة أنه باعتمـــاد أساس معين g فإنه بمعرفة عدد مـــا x يمكـــن بـــسهولة حساب ناتج $y = g^x$ ، أمَّا إذا توافر الناتج y فإنه مـــن الصعوبة حساب x الذي هو عبـــارة عـــن لوغـــاريتم y بالنسبة إلى الأساس g وهذه الصعوبة تصل إلى درجـــة الاستحالة في حال كانت الأرقام كبيرة (أكثـــر مـــن 512 خانة)، وكذلك تنص هذه النظرية علـــى أن قيمـــة هـــذا اللوغاريتم بالنسبة إلى أساس معين تكون وحيدة متفردة.

أمَّا الخطوات المتبعة في خوارزمية سكنور لإثبات الهوية فهي:

- يتم بداية الاتفاق بين الأطراف التي ترغب بالتعامل بهذه الخوارزمية على أساس ما ليكن g.
- يختار كل شخص رقماً عشوائياً خاصاً بـــه؛ وذلـــك ضمن فضاء رقمي واسع سيرمز لـــه Z_P ويـــضم الأعداد جميعها بـــين 1 و P أي $Z_P = [1 .. P]$ إذْ P عدد كبير مؤلف من 512 خانـــة ثنائيـــة أو أكثـــر، وبفرض أن بلالاً اختار القيمة x فإنه يقوم بحـــساب $h = g^x$ ، ومن ثم يعلن بلال للجميع عن h التي تمثل هويته بحيث من يرى h يعلم أنها تمثل بلالاً ويحتفظ بـــ x بشكل سري التي ستعدّ بمنزلة مفتاحه الخاص الذي سيستخدمه فيما بعد في عمليات إثبات الهوية.
- عندما يريد بلال أن يثبت هويته أمام شخص آخـــر لتكن إسراء فإنه يبرهن على امتلاكه للقيمة x مـــن غير أن يفصح عنها وذلك كالآتي:

- يختار بلال رقماً عـــشوائياً w ضـــمن Z_P ومـــن ثـــم يحسب $a = g^w$ ويرسل النتيجة إلى إسراء.
- تختار إسراء رقماً عشوائياً ضمن Z_P ليكن c وترسله إلى بلال، وتسمى c قيمـــة الاختبـــار أو التحـــدي challenge.
- يحسب بلال المقدار $r = x.c + w$ ويرســـله إلـــى إسراء.
- تختبر إسراء صحة المعادلة $g^r = h^c . a$.

فإذا تحققت المعادلة دلَّ على أن بلال يعلـــم قيمـــة x المرتبطة بهويته، وبذلك يكون قد جرى البرهان على هويته، والشكل الآتي يلخص خطـــوات خوارزميـــة سكنور مع العلم أن ϵ_R ترمز للاختيار العشوائي.



يمكن الاستعاضة عن اختيار إسراء للقيمة c وإرسالها إلى بلال وذلك بجعل بلال يحسب القيمة c كتابع خلاصة لكل من a و h، أي بفرض أن H تابع خلاصة متعارفاً عليه بين الأطراف المتعاملة بهذه لخوارزمية فإن c تُحْسَبُ من قبل كل من بلال وإسراء وفق المعادلة c=H(h, a)، وبذلك تجري عملية التأكد من الهوية بخطوة واحدة.

1-2-5-2 التوقيع الرقمي المتحول عن خوارزمية سكنور لإثبات هوية:

كما تم بيانه مسبقاً فإن خوارزمية سكنور طُوِّرَتْ لتستخدم في التوقيع الرقمي، ويمكن بيانها من خلال الخطوات المتبعة فيها كالآتي:

- بفرض أنه كما في خوارزمية سكنور لإثبات الهوية تم بداية الاتفاق على أساس ما ليكن g.
- بفرض أن بلال الذي مفتاحه الخاص (أو ما يسمى المفتاح السري) x وهويته (أو ما يسمى مفتاح عام أو معلن) $h=g^x$ يريد أن يوقع على رسالة ما لتكن m وذلك باستخدام خوارزمية سكنور فإنه يقوم بالخطوات الآتية:
  - يحسب المقدار $z=m^x$، وتسمى z الرسالة الموقعة.
  - يختار رقماً عشوائياً w ضمن فضاء رقمي واسع Z_P، ويحسب المقدارين:
    $a = g^w$, $b = m^w$
  - يحسب المقدار c=H(m, z, a, b)، إذْ H تابع خلاصة لهذه المقادير الأربعة، ويكون تابع الخلاصة عادة تابعاً متعارفاً عليه مسبقاً بين الأطراف المتعاملة بهذا التوقيع.
  - يحسب المقدار $r = c . x + w$.

وتمثل القيم المحسوبة الأربع z, a, b, r بيانات التوقيع أي إنَّ بيانات التوقيع على الرسالة m هي: Sign(m) = (z, a, b, r) ويقوم بتسليمها إلى الشخص المعني بالتوقيع ليكن أحمد.

- عندما يريد أحمد أن يبرهن لآخر لتكن إسراء أن بلالاً فعلاً وقع على المستند m فإنه يقوم بتسليمها بيانات توقيع بلال على الرسالة m التي هي: Sign(m) = (z, a, b, r).

تقوم إسراء التي تعلم أن القيمة h تمثل هوية بلال بالتأكد من صحة توقيع بلال على المستند m وذلك بحساب c=H(m, z, a, b) ثم اختبار تحقق المعادلتين:

$$g^r = h^c . a$$
$$m^r = z^c . b$$

والشكل الآتي يلخص خطوات خوارزمية سكنور للتوقيع الرقمي

كل من القيمة g والتابع H معلن للجميع

و x هي المفتاح الخاص لبلال

إسراء(مختبر التوقيع)	بلال(الموقع)
	$z = m^x$
	$w \in_R Z_p$
	$a \equiv g^w$
	$b \equiv m^w$
	$c = H(m, z, a, b)$
	$r = x \cdot c + w$
	$\xrightarrow{(m, z, a, b, r)}$
تحسب:	
$c = H(m, z, a, b)$	
تتأكد من صحة:	
$g^r = h^c \cdot a$	
$m^r = z^c \cdot b$	

2-2-5-2 خوارزمية سكنور للتوقيع الرقمي الأعمى المحدود Schnorr for Restricted Blind Digital Signature:

يُستخدم هذا النوع من التوقيع في نظام براند للنقد الرقمي؛ وذلك من أجل توقيع المصرف توقيعاً أعمى على بيانات النقد الرقمي التي تضم بشكل أساسي هوية الزبون، وسُمّي هذا النوع من التوقيع الرقمي الأعمى بالمحدود لأن الرسالة التي يوقع عليها المصرف ليست معماة بالكامل، إذ إنَّ المصرف يوقع على رسالة يعلم أنها عبارة عن هوية الزبون، إلا أنها معماة بعامل لا يعلمه المصرف.

وبعد قيام المصرف بحساب القيم التي تمثل توقيعه على هوية الزبون المعماة وتسليمها للزبون، فإن الزبون يقوم بتعمية قيم التوقيع هذه، وفي أثناء عملية الشراء يقدم الزبون بيانات النقد التي هي عبارة عن كل من هويته وقيم التوقيع المعمى كلٍ منهما ويقوم التاجر باختبار قيم التوقيع ليتأكد من وثوقية النقد.

أمَّا الخطوات العملية المتبعة في هذا البرتوكول فإنها تشبه خطوات خوارزمية سكنور للتوقيع الرقمي العادي (غير المعمى) إلا أن الرسالة الموقعة m (التي تكون عادة هوية الزبون مضافاً إليها بعض البيانات) تجري تعميتها برقم عشوائي من قبل الزبون بحيث تصبح 'm، وكذلك القيمتان a, b اللتان يحسبهما الموّقع الذي هنا هو المصرف تجري تعميتهما من قبل الزبون فتصبحان a', b'، وللتوضيح سيجري فيما يأتي بيان الخطوات العملية المتبعة في هذا النوع من التوقيع خلال عملية سحب الزبون لنقد رقمي من المصرف:

- بفرض أنه اِعْتُمِدَتِ القيمة g كأساس في عمليات الحساب، واِعْتُمِدَ تابع الخلاصة H (يعدُّ g و h من الثوابت التي يعتمدها المصرف).
- بفرض أن المصرف له مفتاح خاص هو x وأن هويته المقابلة لهذا المفتاح أو ما يسمى المفتاح العام هو $h = g^x$ ، فإن توقيع المصرف على بيانات النقد (الرسالة المراد توقيعها التي تضم بشكل أساسي هوية الزبون) سيرمز لها كالسابق m يتم وفق الخطوات الآتية:

- يحسب المصرف القيمة $z = m^x$.
- يختار المصرف رقماً عشوائياً w ضمن فضاء رقمي واسع Z_P ويقوم بحساب القيمتين $a = g^w$ و $b = m^w$ ويرسل القيم الثلاث z, a, b إلى الزبون.
- يقوم الزبون باختيار ثلاث قيم عشوائية s , v , u من فضاء رقمي واسع Z_P، إذْ يستخدم القيمة s لتعمية هويته m بحيث تصبح $m' = m^s$ وتعمية الرسالة الموقعة z بحيث تصبح $z' = z^s$، أمَّا القيمتان u , v فيستخدمهما لتعمية a و b كالآتي:

$$a' = a^u \cdot g^v$$
$$b' = b^{s.u} \cdot m'^v$$

- يقوم الزبون بحساب تابع الخلاصة لهذه القيم الأربع المعماة: $c'= H(m', z', a', b')$ ومن ثم يقوم بتعمية الخلاصة الناتجة باستخدام القيمة u؛ وذلك بحساب $c = c'/u$ ويرسل النتيجة إلى المصرف.
- يحسب المصرف القيمة $r = c . x + w$ ويرسلها إلى الزبون.
- يختبر الزبون صحة بيانات التوقيع المسلمة من قبل المصرف؛ وذلك بالتحقق من صحة المعادلتين الآتيتين:

$g^r = h^c . a$
$m^r = z^c . b$

- يحسب الزبون القيمة $r' = r . u + v$.

وتشكل القيم المحسوبة z', a' , b', r' توقيعاً أعمى محدوداً للمصرف على بيانات النقد 'm أي إنَّ التوقيع على بيانات النقد هومجموعة القيم:

$Sign (m') = (z', a' , b', r')$

o عندما يريد الزبون أن يشتري بهذا النقد من تاجر ما فإن الزبون يقوم بتسليمه هويته المعماة 'm (التي تمثل بيانات النقد) وقيم توقيع المصرف عليها z', a', b', r'.

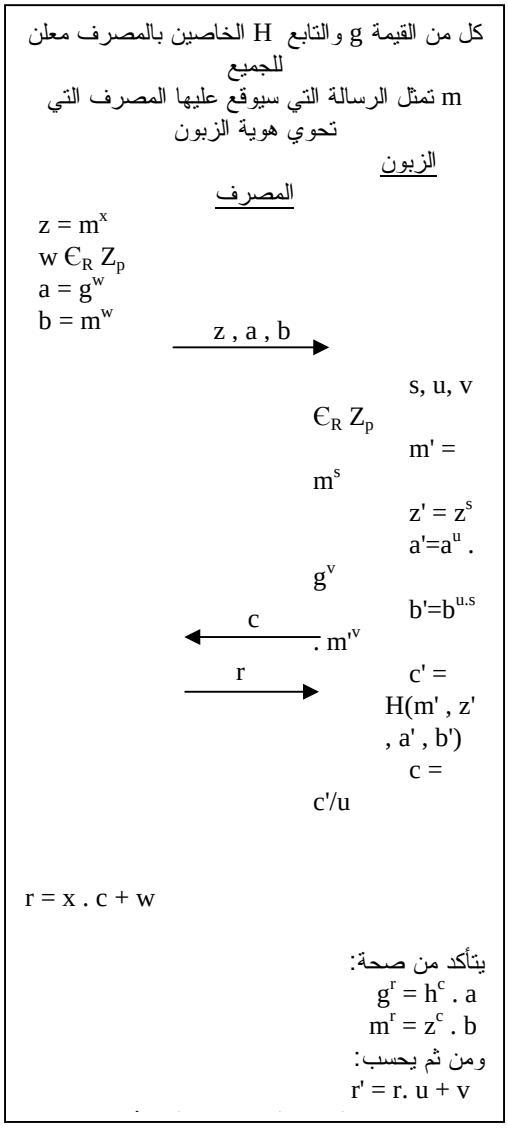
يقوم التاجر الذي يعلم أن القيمة h تمثل هوية المصرف بالتأكد من صحة توقيع المصرف على بيانات النقد؛ وذلك باختبار تحقق المعادلتين:

$g^{r'} = h^{H(m', z', a', b')} . a'$
$m'^{r'} = z'^{H(m', z', a', b')} . b'$

اللتين تُسميان معادلتي التوقيع ويمكن كتابتهما كالآتي:

$c' = H (m' , z' , a' , b')$
$g^{r'} = h^{c'} . a'$
$m'^{r'} = z'^{c'} . b'$

والشكل الآتي يبيّن يلخص خطوات خوارزمية التوقيع الرقمي الأعمى المحدود



o عندما يريد التاجر أن يودع النقد الرقمي الذي استلمه في حسابه لدى المصرف الذي أصدر النقد فإنه يقوم بتسليم بيانات النقد والقيم الخاصة بالتوقيع.

يتحقق المصرف من أن النقد مصدر من قبله؛ وذلك بالتأكد من تحقق معادلتي التوقيع قبل أن يقبل إيداع النقد الرقمي.

ومن هنا يتبيّن أنه باستخدام خوارزمية سكنور للتوقيع الرقمي الأعمى المحدود استطاع كل من التاجر

والمصرف التأكد من صحة توقيع المصرف على النقد دون أن يكون لأي منهما القدرة على تمييز هوية الزبون. إن هذا النوع من التوقيع يغني عن استخدام خوارزمية اقطع واختر التي مرت سابقاً ذات الكلفة العالية والحجم الكبير للبيانات التي تستخدم للتأكد من أن بيانات النقد تحوي هوية الزبون، وذلك لأنه في توقيع سكنور الأعمى المحدود لن يكون التوقيع صحيحاً ما لم تكن الرسالة الموقعة تحوي هوية الزبون.

3- أنظمة النقد الرقمي السابقة [10]:

طُوِّرَتْ عدة أنظمة للنقد الرقمي، إذ قامت العديد من الشركات مثل PayPal وCyberCoins وCyberCash وPioneering وDigiCash وeCash وInfoSpace بتطوير أنظمة للنقد الرقمي وكل من هذه الأنظمة يحقق جزءاً فقط من متطلبات النقد الرقمي ويعجز عن كثير منها، ومعظم هذه الشركات أفلست فيما بعد لمحدودية مجال استخدام النقد الرقمي الذي تصدره وعدم تحقيقه لمتطلبات النقد الرقمي.

وقد أُجرِيَتْ دراسات متعددة لأنظمة نقد رقمي أسفرت عن التوصل إلى العديد من أنظمة النقد الرقمي مثل نظام شوم وبراند وأوكاماتو وأوهتا وغيرها، ولكل من هذه الأنظمة ميزاته وخصائصه ويحقق جزءاً من متطلبات النقد الرقمي ويعجز عن بعضها، وفيما يأتي بيان مختصر لأهم هذه الأنظمة وهي نظام براند ونظام أوكاموتو.

3-1 نظام براند Brand للنقد الرقمي [11]:

كان العالم Stefan Brands أول من اكتشف خوارزمية سكنور للبرهان الكتوم والتوقيع الرقمي الأعمى المحدود، هذا الاكتشاف مكّنه من تطوير نظام نقد رقمي يمتاز عن الأنظمة السابقة بكفاءة مرتفعة تصل إلى أضعاف كفاءة الأنظمة التي سبقته لأنَّ خوارزمية سكنور للتوقيع الرقمي الأعمى لا تتطلب عملية تأكد من البيانات كما هو الحال عند استخدام خوارزمية RSA للتوقيع الرقمي الأعمى التي كانت تجري باستخدام خوارزمية اقطع واختر ذات الكلفة العالية لكل من المعالجة وحجم البيانات.

هذه الكفاءة المرتفعة لنظام براند جعلته لا يقف عند حدود الدراسة النظرية وإنما دخل في التطبيق العملي.

يحقق نظام براند جزءاً كبيراً من متطلبات النقد الرقمي التي هي: الأمان وسرية هوية المتعامل وعدم الربط بين عمليات الشخص الواحد وقابلية النقل والعمل دون اتصال مباشر.

إلا أنه عجز أن يحقق خاصية أساسية وهي أن يكون قابلاً للتجزئة، كما أنه لم يطرح آلية للتعامل مع فئات نقدية مختلفة.

3-2 نظام أوكاموتو Okamoto للنقد الرقمي [12]:

كان أوكاموتو أول من اخترع نظاماً نقداً رقمياً قابلاً للتجزئة، وهذا النظام وإن امتاز عن نظام براند بأنه يحقق خاصية التجزئة إلا أنه ليس ذا كفاءة كافية تجعله يدخل التطبيق العملي لذا بقي ضمن حدود الدراسة النظرية.

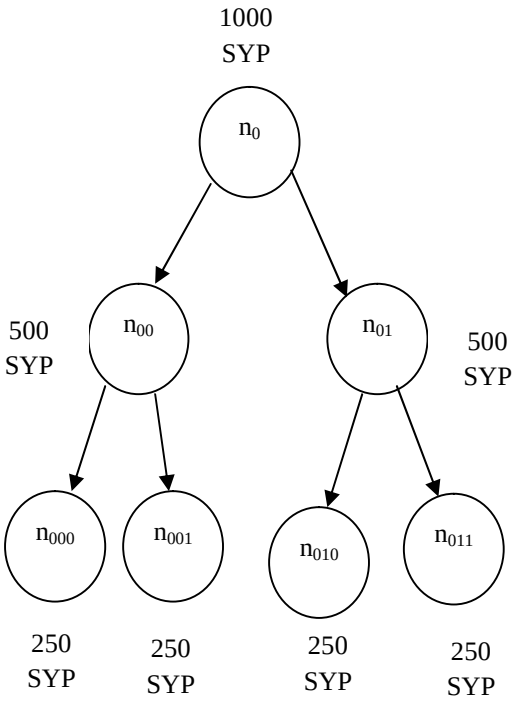
يعتمد نظام أوكاموتو في تجزئة النقد الرقمي على مفهوم شجرة النقد الثنائية التي سيجري بيانها فيما يأتي:

3-2-1 الشجرة الثنائية لتمثيل النقد الرقمي القابل للتجزئة Cash Binary Tree:

للتمكن من التعامل مع قطعة نقد رقمي قابلة للتجزئة فإنَّها تُقَابَلُ بشجرة ثنائية وسميت ثنائية لأنه يتفرع من كل عقدة عقدتان ولكل عقدة من الشجرة إحداثيات ثنائية، وتبدأ الشجرة بعقدة الجذر root التي تقابل كامل قيمة قطعة النقد الرقمي التي إحداثياتها 0 ويتفرع عن الجذر عقدتان اثنتان كل عقدة منهما تقابل نصف قيمة قطعة

النقد إحداثياتهما 01 و 00 ويتفرّع عن كل منهما أيضاً عقدتان كل منهما تقابل نصف قيمة عقدة الأم ويستمر التفرع عّدة مستويات يرمز لها بـ L تختلف بحسب معامل التجزئة، وكل عقدة من عقد الشجرة الثنائية تمثل جزءاً من قطعة النقد الرقمي.

وللتوضيح في الشكل الآتي مثال عن شجرة نقد ثنائية تقابل قطعة نقد رقمي بقيمة 1000 SYP ذات عدد من المستويات L=3 وتحقق معامل تجزئة $w=2^{L-1}=4$ (معامل التجزئة يمثل نسبة كامل قيمة النقد إلى أصغر جزء يمكن التعامل به ويساوي عدد عُقد المستوى الأخير):



في هذه الشجرة تقابل عقدة الجذر كامل القيمة[1] n_0 = 1000 SYP في حين تقابل كل من العقدتين المتفرعتين عنها: $n_{00} = n_{01}$ = 500 SYP وتقابل عقد الصف الثالث 250 SYP أي: $n_{000} = n_{001} = n_{010} = n_{011}$ = 250 SYP.

3-2-2 قاعدتا شجرة النقد الثنائية:

من أجل أن تقوم شجرة النقد الثنائية بعملها على الوجه الصحيح يجب أن تتحقق القاعدتان التاليتان اللتان تسميان قاعدتي شجرة النقد:

1- قاعدة المسار إلى الجذر: التي تنص على أنه إذا صُرِفَتْ أي عقدة من الشجرة الثنائية فإنه يجب عدم صرف أي عقدة أم لها أو أي عقدة متفرعة عنها، أي إنَّ المسار بين عقدة الجذر وأي عقدة من عُقد المستوى الأدنى يجب أن يحوي عقدة مصروفة واحدة لا أكثر.

2- قاعدة العقدة ذاتها: التي تنص على أنه ينبغي عدم صرف العقدة ذاتها أكثر من مرّة.

وهاتان القاعدتان مهمتان لضمان عدم حصول صرف النقد الرقمي بأكثر من قيمته over-spend.

3-2-3 آلية عمل نظام أوكاموتو:

يعتمد نظام أوكاموتو على أسس رياضية متعددة أهمها نظريتان رياضيتان هما:

- صعوبة تحليل عدد إلى عوامله الأولية حال كانت عوامله كبيرة ذات عدد خانات فوق 256 خانة ثنائية (bit).

- صعوبة إيجاد اللوغاريتم، في حال كان الأساس كبيراً ذا عدد خانات فوق 256 خانة ثنائية (bit).

إذْ لا توجد طريقة لحساب كل من العوامل واللوغاريتم أسرع من التجريب العشوائي.

كما يعتمد نظام أوكاموتو على استخدام نوع معين من الأعداد يسمى عدد وليام William Integer وهو عبارة

[1] رُمِّزَتِ العقدة بالحرف n (من كلمة node أي عقدة) مرفقاً بإحداثيات العقدة.

عن جداء عددين أوليين أحدهما من الشكل[1] $p = 3 \bmod 8$ والآخر من الشكل $q = 7 \bmod 8$، وعدد وليام له خاصية أساسية وهي أنه يمكن معرفة عامليه فقط في حال توافرت معلومات خاصة[2]، وهذه المعلومات لا تكون متاحة وفق تصميم أوكاموتو إلا في حال قام الزبون باختراق أي من قاعدتي شجرة النقد الثنائية، وفيما يأتي سيجري بيان الملامح الأساسية لنظام أوكاموتو من خلال بيان أهم الخطوات المتبعة فيه دون الخوض في تفاصيله وتعقيداته الرياضية:

- عندما يريد الزبون أن يحصل على قطعة نقد رقمي فإنه يقوم بتشكيل بيانات النقد، وذلك باختيار لا على التعيين عددين أوليين أحدهما من الشكل $p = 3 \bmod 8$ والآخر من الشكل $q = 7 \bmod 8$ ويحسب مضروبهما ليحصل على عدد وليام $N = p \cdot q$، ويجب أن يكون كلٌ من p و q ذا عدد خانات كبير (512 bits) بحيث يصعب تحليل N إلى عامليه p و q وفق الإمكانيات الحاسوبية المتوافرة ويضمن اختيارهما من فضاء رقمي واسع.
  - يقوم الزبون بتعمية العدد وليام الذي حسبه N؛ وذلك باستخدام تابع تعمية ما ليحصل على N' ويحسب القيمتين g^p, g^q، إذْ g عدد ثابت معلوم للجميع (من ثوابت المصرف) ثم يسلّم القيم N', g^p, g^q للمصرف، وبحسب نظرية اللوغاريتم فإن المصرف لا يمكنه حساب p, q من خلال معرفة g^p, g^q.
  - يقوم المصرف بالتأكد من وثوقية القيم المسلمة N', g^p, g^q وذلك باستخدام خوارزمية اقطع واختر، إذْ كما مر سابقاً عند الكلام عن خوارزمية اقطع واختر فإن الزبون لا يختار عدد وليام واحداً وإنما يختار عدد k من أعداد وليام $N'_k = p_k \cdot q_k$ ويقوم بتسليم المصرف القيم N'_k , g^{p_k} , g^{q_k} المقابلة لها، يختار المصرف $k'=k-1$ عينة منها ويطلب من الزبون الكشف عن القيم $N_{k'}, p_{k'}, q_{k'}$ المقابلة لها ويتأكد من صحة هذه القيم المسلمة، أمَّا العينة المتبقية التي لم يكشف الزبون عن القيم المرتبطة بها ولتكن N'_s , g^p_s , g^q_s فأصبح المصرف شبه متأكد من صحتها بنسبة $1-\frac{1}{2^K}$.
  - يقوم المصرف بالتوقيع على عدد وليام المعمى N'_s وذلك وفق خوارزمية[3] RSA للتوقيع الرقمي الأعمى، ليحصل على $sign(N'_s)$ ويسلمها للزبون، ومن ثم يقوم المصرف بتخزين القيم N'_s , g^q_s , g^p_s فضلاً عن هوية الزبون الذي صرفت له قطعة النقد؛ وذلك في جدول خاص في قاعدة بياناته.
  - يقوم الزبون بفك تعمية القيمة الموقعة من قبل المصرف $sign(N'_s)$ ليحصل على توقيع المصرف على N_s أي $sign(N_s)$.
- عندما يريد الزبون الشراء باستخدام النقد الرقمي فإنه يسلم التاجر كلاً من بيانات النقد الممثلة بالقيمة N_s وتوقيع المصرف عليها $sign(N_s)$.
  - يقوم التاجر بالتأكد من صحة توقيع المصرف على بيانات النقد الرقمي وفق خوارزمية RSA للتوقيع

[1] mod هو تابع باقي القسمة، وكمثال على عدد وليام:
$437 = 19 \cdot 23 \,,\; 19 = 3 \bmod 8 \,,\; 23 = 7 \bmod 8$

[2] هذه المعلومات بيانها مرتبط بمفاهيم رياضية تضيق صفحات هذه المقالة عن شرحها مثل الجذر التربيعي النسبي، والباقي التربيعي والباقي اللاتربيعي، رمز جاكوبي ورمز ليجندري.

[3] خوارزمية RSA من خوارزميات التشفير اللامتناظر وتستخدم في التوقيع الرقمي، وكذلك طُوِّرَتْ لتستخدم في التوقيع الرقمي الأعمى.

الرقمي الأعمى؛ وذلك من أجل التحقق من أن النقد موثوق به وموقع من قبل المصرف.

- يقوم الزبون بتحديد العقد التي يريد صرفها من شجرة النقد الثنائية التي تمثل قطعة النقد الرقمي التي يريد الشراء بها، بحيث تقابل هذه العقد الجزء الذي يريد الشراء به من قطعة النقد الرقمي وبحيث تحقق قاعدتي شجرة النقد الثنائية، ومن ثم يقوم بحساب قيم خاصة بكل عقدة من العقد المختارة، هذه القيم تحسب وفق معادلات خاصة[1] معدة بطريقة تجعل المصرف قادراً على تحليل العدد وليام الخاص بقطعة النقد N_s في حال قام الزبون باختراق أي من قاعدتي شجرة النقد الثنائية، ومن ثم يقوم الزبون بتسليم قيم العقد المراد صرفها للتاجر.
- يتأكد التاجر من صحة قيم العقد وفق معادلات اختبار خاصة، ومن ثم يخزن كلاً من بيانات النقد N_s وتوقيع المصرف عليها $sign\ (N_s)$ فضلاً عن القيم الخاصة بالعقد من أجل عملية إيداعها في المصرف.

o عندما يريد التاجر أن يودع المبلغ الذي استلمه من الزبون وذلك في حسابه لدى المصرف الذي أصدر النقد فإنه يقوم بتسليم N_s و$sign(N_s)$ وقيم العقد إلى المصرف.

يتأكد المصرف من صحة توقيعه على بيانات النقد، ومن ثم يتأكد من أن عُقَد قطعة النقد التي يحاول التاجر إيداعها غير مودعة في عملية سابقة، فإذا وجدها غير مودعة سابقاً فإنه يقبل النقد ويضيف الرصيد الذي يحمله إلى حساب التاجر ويقوم بتخزين القيم المودعة في جدول خاص بالنقد المودع ضمن قاعدة بياناته، أمَّا إذا وجد هذه العقد مودعة في عملية سابقة فإنه من خلال قيم العقد المسلمة في كلٍ من العملية السابقة والعملية الحالية يستطيع المصرف حساب عاملي العدد وليام، وإذا تم معرفة عاملي العدد وليام فإنه يمكن حساب القيمتين g^p, g^q، وبالرجوع إلى قاعدة بيانات المصرف التي تحوي القيم g^p, g^q الخاصة بجميع قطع النقد الرقمي المصدرة من قبل المصرف وهويات الزبائن التي سلمت لهم يجري تعرّف هوية الزبون المتلاعب.

إن نظام أوكاموتو مع أنه أول نظام يحقق خاصية تجزئة النقد الرقمي إلا أن كفاءته متدنية بسبب اعتماده على خوارزمية اقطع واختر للتأكد من صحة بيانات النقد قبل أن يوقع عليها المصرف توقيعاً أعمى.

4- تصميم نظام النقد الرقمي المقترح

يجمع نظام النقد الرقمي المقترح بين أكبر قدر من خصائص النقد الرقمي من حيث الأمان وسرية هوية المتعامل وقابلية النقل والتجزئة والكفاءة العالية، والتعامل مع فئات نقدية متعددة، وعدم الربط بين عمليات الشخص الواحد التي تجري على قطع نقدية، أي أنه حقق خصائص إضافية للنقد الرقمي لم تستطع الأنظمة السابقة تحقيقها، أهمها أنه أول نظام يحقق خاصية التجزئة للنقد الرقمي بكفاءة جيدة.

إن نظام أكاموتو هو النظام الوحيد الذي يحقق تجزئة النقد الرقمي إلا أن كفاءته متدنية منعته من دخول التطبيق العملي وبقي في حدود الدراسة النظرية، لذلك اِستُثْمِرَ في نظام النقد الرقمي المقترح بعض الأفكار المستخدمة في نظام أكاموتو مثل شجرة النقد الثنائية وأعداد وليام وتوابعها؛ وذلك من أجل تحقيق خاصية تجزئة النقد إلا أنه تم استخدام خوارزمية سكنور للتوقيع

[1] إن المعادلات الخاصة بقيم العقد يصعب بيانها هنا لأنها تحتاج إلى مفاهيم رياضية، من الصعوبة الإحاطة بها من خلال هذه المقالة.

الرقمي الأعمى المحدود من أجل توقيع النقد الرقمي بدلاً من خوارزمية RSA للتوقيع الرقمي الأعمى.

إن خوارزمية سكنور للتوقيع الرقمي الأعمى المحدود تغني عن الحاجة إلى عملية التأكد من بيانات النقد التي كانت تجري في نظام أوكاموتو باستخدام خوارزمية اختر واقطع ذات الكلفة العالية لكل من المعالجة وحجم البيانات والوقت وتتسبب في بطء النظام وتدني كفاءته.

في نظام النقد الرقمي المقترح من أجل التمكن من استخدام خوارزمية سكنور للتوقيع الرقمي الأعمى المحدود بجانب المفاهيم المستخدمة في نظام أوكاموتو أُضِيفَ مفهوم جديد وهو مفهوم هوية النقد الرقمي، إذْ إنَّ النقد الذي يوقعه المصرف لا يحتوي فقط هوية الزبون وإنما أضاف إليها مقداراً آخَر خاصاً بكل قطعة نقد وعُدَّ كهوية لقطعة النقد، وهوية قطعة النقد كما سيتضح سيكون لها دور أساسي في تجزئة النقد.

في نظام النقد الرقمي المقترح ويُحَلَّلُ العدد وليام إلى عامليه في حال قام الزبون باستخدام الزبون للنقد الرقمي بأكثر من قيمته، وذلك بالطريقة المتبعة نفسها في نظام أوكاموتو، ولكن في هذا النظام رُبِطَتْ بيانات هوية قطعة النقد بأحد عاملي العدد وليام كما سيجري بيانه لاحقاً، بحيث إذا حُلِّلَ العدد وليام فإنه يكتشف هوية النقد، ومنه بالرجوع إلى قاعدة بيانات المصرف التي تحوي جدولاً خاصاً بهويات قطع النقد وهويات الزبائن التي صرفت لهم تُكْشَفُ هوية الزبون المتلاعب.

وللتوضيح سيجري بيان الخطوات الأساسية المتبعة في هذا النظام.

- بفرض أن المصرف اختار عدة أسس g, g_1, g_2 كثوابت خاصة به، وتكون هذه الأسس أعداداً كبيرة.
- بفرض أن المصرف له مفتاح خاص هو x وأن هويته المقابلة لهذا المفتاح أو ما يسمى المفتاح العام هو $h = g^x$.
- بفرض أن الزبون مفتاحه الخاص هو u_1 وأن مفتاحه العام هو $I = g^{u1}$.
- عندما يريد الزبون سحب نقد رقمي من المصرف فإنه يقوم بتشكيل هوية النقد التي سيرمز لها I' وذلك باختيار عدد وليام $N = p.q$ إذْ $p=3 \bmod 8$ و $q=7 \bmod 8$ وذلك بالطريقة نفسها التي تم بيانها في نظام أوكاموتو[1]، ومن ثم تُحْسَبُ هوية النقد $I'=g_2^q$ وتُسَلَّمُ للمصرف.

- يوقع المصرف باستخدام خوارزمية سكنور للتوقيع الرقمي الأعمى المحدود على بيانات النقد التي هي في هذا النظام المقترح عبارة عن هوية الزبون مضروبة بهوية النقد أي $m = I \,.\, I'$.
- وكما مرَّ في بيان خوارزمية سكنور للتوقيع الرقمي الأعمى المحدود فإن المصرف يوقع بشكل أعمى على بيانات النقد $m = I \,.\, I'$ وفق الخطوات الآتية:

§ يحسب المصرف القيمة $z = m^x$.

[1] يُخْتَارُ p و q بحيث يكونا ذوي عدد خانات كبير يضمن اختيارهما من فضاء رقمي واسع وتكون نسبة تطابقهما مع قيم تمثل قطعة نقدية أخرى ضئيلة يمكن إهمالها، فمثلاً إذا كان q بعدد خانات 512 فإن نسبة تطابقه مع q لقطعة نقدية أخرى $1/2^{512}$ وهذا مقدار صغير لا يعتد به، ويمكن من أجل زيادة الحيطة جعل برامج المصرف تقوم بعملية مقارنة من أجل كل قطعة نقد رقمية تُنْشَأُ، وذلك بين القيم المسلمة الخاصة بهذه القطعة وبين القيم الخاصة بالقطع النقد الرقمية السابقة والمخزنة في قاعدة البيانات الخاصة بالمصرف.

§ يختار المصرف رقماً عشوائياً w ضمن فضاء رقمي واسع Z_P ويقوم بحساب القيمتين $a = g^w$ و $b = m^w$ ويرسل القيم الثلاث z, a, b إلى الزبون.

- يقوم الزبون[1] بتعمية كل من الرسالة وقيم التوقيع، ولكن ليس برقم عشوائي كما هو في نظام براند وإنما باستخدام q كالآتي:

$$m' = m^q = (I.I')^q$$

- أما قيم التوقيع التي يحسبها المصرف:

$$a = g^w,\ b = m^w$$

فيجري تعميتهما بشكل مشابه لسكنور، إذْ يختار الزبون قيمتين عشوائيتين u, v أيضاً من Z_P ويحسب:

$$a' = a^u \cdot g^v$$

$$b' = b^{s.u} \cdot m'^v$$

- يقوم الزبون بحساب تابع الخلاصة للقيم الأربع المعماة فضلاً عن العدد وليام، أي إنّه في هذا النظام أُضيفَ العدد وليام إلى البيانات الموقعة وذلك بشكل جزئي أي:

$$c' = H(N, m', z', a', b')$$

- ومن ثم يقوم بتعمية الخلاصة الناتجة باستخدام القيمة u وذلك بحساب $c = c'/u$ ويرسل النتيجة إلى المصرف.
- يحسب المصرف القيمة $r = c \cdot x + w$ ويرسلها إلى الزبون.
- يحسب الزبون القيمة $r' = r \cdot u + v$.

أي إنَّ قيم التوقيع الناتجة هي:

$$Sign\ (m', N) = (z', a', b', r')$$

التي تحقق معادلتي التوقيع الآتيتين:

$$g^{r'} = h''^{\,H(N, m', z', a', b')} \cdot a'$$

$$m'^{r'} = z'^{\,H(N, m', z', a', b')} \cdot b'$$

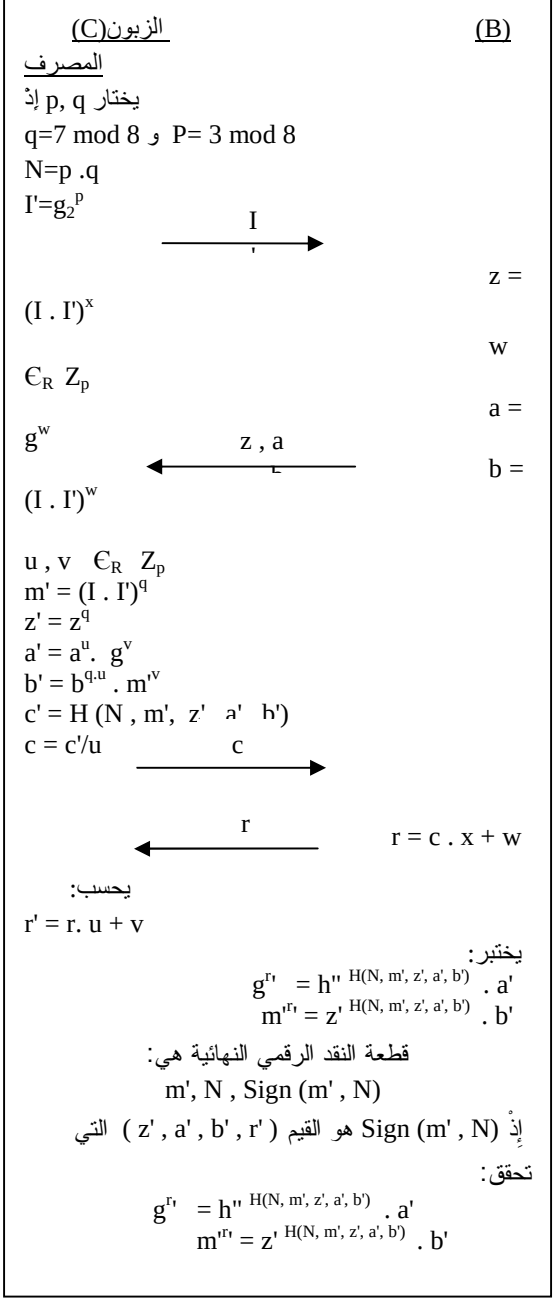
التي تعدُّ بمنزلة توقيع المصرف على بيانات النقد.

وعند إتمام عملية سحب قطعة النقد الرقمي فإن المصرف يقوم بتخزين كل من هوية الزبون I وهوية قطعة النقد I' في جدول خاص يحوي قطع النقد جميعها التي أصدرها المصرف.

والشكل الآتي يلخص الخطوات الأساسية المتبعة في عملية السحب في النظام المقترح.

[1] في الواقع العملي فإن الخطوات التي يقوم بها الزبون من اختيار قيم وحساب معادلات لا تجري بشكل يدوي وإنما من خلال برنامج يقوم الزبون بتنزيله على حاسبه من موقع المصرف، ويضم هذا البرنامج مكتبات قادرة على التعامل مع أرقام بعدد خانات كبير.

خطوات سحب النقد الرقمي في النظام المقترح



o عندما يريد الزبون أن يشتري بقطعة النقد هذه يقوم بتسليم التاجر جزئي قطعة النقد m', N والتوقيع عليهما $Sign(m', N)=(z', a', b', r')$ ، فضلاً عن القيمة J التي يحسبها الزبون كالآتي $J=g_1^{u_1.q}$ ، إذْ u_1 كما تم بيانه مسبقاً هو المفتاح الخاص للزبون التي يُستخدم كما سيتبيّن لاحقاً من أجل التأكد من أن الزبون هو المالك الحقيقي للنقد.

- كما يقوم الزبون بحساب القيم المقابلة للعقد التي تمثل المبلغ الذي يريد صرفه وفق المعادلات الخاصة المستخدمة ذاتها في نظام أوكاموتو ويسلمها للتاجر.

- يقوم التاجر بالتأكد من صحة توقيع المصرف على قطعة النقد الرقمي؛ وذلك باختبار معادلتي التوقيع على بيانات النقد:

$$g^{r'} = h''^{H(N, m', z', a', b')} . a'$$
$$m'^{r'} = z'^{H(N, m', z', a', b')} . b'$$

- يقوم التاجر باختبار صحة المعادلة الآتية؛ وذلك للتأكد من الربط بين الزبون وقطعة النقد فإنه:

$$m' = J . g_2^N$$

وذلك لأن:

$$m' = (I . I')^q = (g_1^{u_1} . g_2^p)^q = J . g_2^N$$

- لكي يتأكد التاجر من أن الزبون هو المالك الحقيقي للنقد، يقوم باختبار معرفة الزبون للمعلومات السرية الخاصة بهويته أي u_1 الخاصة بالنقد أي q؛ وذلك باستخدام خوارزمية سكنور لإثبات الهوية، وذلك وفق الخطوات الآتية:

§يقوم الزبون باختيار o بشكل عشوائي وحساب المقادير الآتية:

$$Y = g_1^o$$
$$e = H(N, m', Y)$$
$$x = e . u_1 . q + o$$

ويسلم القيم Y و e و x للتاجر.

§يقوم التاجر باختبار صحة المعادلة الآتية:

$$g_1^x = J^e . Y$$

والشكل الآتي يلخص الخطوات الأساسية المتبعة في عملية الشراء في النظام المقترح.

برتوكول الشراء بالنقد الرقمي في النظام المقترح

الزبون (C)

التاجر (V)

$J = g_1^{u_1 . q}$

o $\in_R Z_p$

$Y = g_1^o$

e = H(N, m', Y)

d = e . u_1 . q + o

Node $m', N, Sign(m', N), J, Y, d,$ →

يتأكد التاجر من Sign (m' , N) وذلك باختبار:

$g^{r'} = h$

$H(N, m', z', a', b')$. a'

$m^{r'} = z'$

$H(N, m', z', a', b')$. b'

يتأكد التاجر من تحقق:

- عندما يريد التاجر أن يودع المبلغ الذي استلمه في المصرف الذي أصدر النقد فإنه يقوم بتسليم بيانات النقد وقيم التوقيع عليها فضلاً عن القيم الخاصة بالعقد المصروفة إلى المصرف، وبصورة مشابهة لنظام أوكاموتو فإن القيم الخاصة بالعقد محسوبة أيضاً بطريقة تكفل القدرة على حساب عاملي العدد وليام في حال استخدم الزبون قطعة النقد خارج الحد المسموح به أي قام باختراق أيٍ من قاعدتي شجرة النقد الثنائية، وإذا عُرِفَ عاملا N فإنه يمكن التوصل إلى هوية قطعة النقد $I'=g^q$ وبالرجوع إلى قاعدة بيانات المصرف التي فيها جدول يحوي هويات قطع النقد الرقمي المصدرة من قبل المصرف جميعها وهويات الزبائن التي سلمت لهم يتم تعرّف هوية الزبون المتلاعب.

كما أُعِدَّ النظام المقترح بحيث يتعامل مع عدة فئات نقدية وليس مع فئة نقدية واحدة كما هو في نظام براند، وذلك من خلال جعل المصرف يستخدم أكثر من مفتاح خاص من النوع سكنور بحيث يختار المصرف مفتاحاً خاصاً بكل فئة نقدية يريد إصدارها $x_1, x_2, \ldots$، ويقوم بحساب الهويات المقابلة لهذه المفاتيح أو ما يسمى المفاتيح العامة $h_1 = g^{x_1}$, $h_2 = g^{x_2}$, ...

5- أهم التحديات:

في نظام النقد الرقمي المقترح يوجد نوع من المخاطرة يتعرض لها المصرف، وهي أنه مع قدرته على اكتشاف هوية الزبون المختلس إلا أنه لا يستطيع تحصيل المبلغ الذي سُرق منه، ويمكن للحد من هذه المخاطرة جعل النظام يصدر فقط فئات نقدية ذات قيمة قليلة، كما يمكن اشتراط أن يكون للزبون لدى المصرف رصيد إضافي عن قيمة النقد الذي يريد سحبه وخاصة للزبائن الذين ليس لهم سجل تاريخي كافٍ لبناء الثقة بهم.

ولكن ماذا لو قام الزبون بالشراء بهذا النقد العديد من المرات قبل أن يقوم التجار بإيداع النقد الرقمي الذي حصلوا عليه من خلال عمليات بيع لهذا الزبون، يمكن للتقليل من هذه المخاطرة الطلب من التجار إيداع النقد الرقمي بشكل يومي.

ولكن تبقى هناك مخاطرة كبيرة وهي أنه مادام النقد بحوزة الزبون فإن بإمكانه الاستمرار في استخدامه بشكل لا شرعي ومن ثَمَّ لديه المقدرة على الاستمرار في استنزاف المصرف من خلال هذا النقد، ولحل هذه المشكلة يمكن اعتماد قوائم سوداء للزبائن المحرومين من التعامل تُحَمَّلُ من قبل التجار عند كل عملية إيداع لهم، ولكن قد يكون هذا غير عملي من الناحية التقنية ومكلفاً إذْ إنَّه يحتاج إلى تناقل بيانات قد يكون حجمها كبيراً.

لذا يمكن جعل نظام النقد الرقمي يتعامل مع بطاقات ذكية بحيث يُخَزَّنُ النقد الرقمي عليها وتُجْعَلُ هذه البطاقات تحتوي على مراقب داخلي observer وهو عبارة عن برنامج صغير مرفق بقاعدة بيانات صغيرة الحجم تُخَزَّنُ

فيها العمليات كلّها التي يقوم بها الزبون وتمنع من إنجاز أي عملية في حال تجاوز الزبون الحد المسموح له، وفي هذه الحالة يجب أن يكون حاسب الزبون مزوداً بقارئ بطاقات.

6- آفاق مستقبلية Future Work:

إن النظام المقترح مع بعض الإنجازات التي حققها إلا أنه ما زال عاجزاً أمام تحقيق خاصية أن يكون النقد الرقمي ثنائي الاتجاه، أي إمكانية تناقله بين الأشخاص أكثر من مرة دون الاضطرار إلى إيداعه في المصرف بعد كل عملية، وهذه الخاصية لا يوجد إلى الآن نظام للنقد الرقمي يحققها، لأن النقد الرقمي إذا انتقل أكثر من مرة بين عدة أشخاص قبل أن يُودَعَ في المصرف وحدث أن قام أحدهم بعملية لا شرعية، فلن يكون للمصرف القدرة على اكتشاف هوية من قام بهذه العملية.

كما أن النظام المقترح في هذه البحث يحتاج من الزبون القيام بعدة خطوات قبل حصوله على نقد رقمي وهذا قد لا يكون مرغوباً فيه عند بعض الزبائن.

فضلاً عن أن تفاصيل العمليات التي تُحْسَبُ معقدة وصعبة بعض الشيء وخاصة فيما يتعلق بحساب القيم الخاصة بعقد شجرة النقد؛ مما يجعل صيانة هذا النظام وتعقب أخطائه أمراً صعباً.

إن النقد الرقمي لكي يدخل إلى السوق بشكل منافس لوسائل الدفع الأخرى فإنه يجب بذل المزيد من الجهود بغية تطوير نظام رقمي أقل تعقيداً وأقرب إلى تقبل الزبائن ويحقق خاصية أن يكون ثنائي الاتجاه، إن التوصل إلى نظام نقد رقمي بهذه الخصائص سيجعله يهيمن على وسائل الدفع الأخرى جميعها بما فيها العملة التقليدية.

مسرد المصطلحات

تشفير لامتناظر	Asymmetric Encryption
توقيع رقمي أعمى	Blind Digital Signature
خوارزمية اقطع واختر	Cut and Choose Algorithm
شجرة نقد ثنائية	Cash Binary Tree
نقد رقمي	Digital Cash
نقد قابل للتجزئة	Divisible Cash
فك التشفير	Decryption
قضية اللوغاريتم المتفرد	Discrete Logarithm Problem (DLP)
توقيع رقمي	Digital Signature
النقد الرقمي	E-Coins - E-money
كفاءة	Efficiency
تشفير	Encryption
خطة التحقق من الهوية	Identification Scheme
متوافر للاتصال	On-Line
قادر على العمل دون وجود اتصال مباشر	Off-line capable
نظام أوكاموتو	Okamoto System
محمول	Portable
حماية الخصوصية	Privacy protection
توقيع رقمي أعمى محدود	Restricted Blind Digital Signature
خوارزمية للتشفير اللامتناظر	RSA
ثنائي الاتجاه	Two-way
عدم قابلية الربط بين عمليات الشخص الواحد	Unlinkability
ودود	User-Friendly
حرية تحديد فئات النقد	Unit-of-value Freedom
العدد وليام	William Integer
البرهان الكتوم	Zero-knowledge proof

المراجع*

[1] Guilin Wang, "Digital Cash", University of Birmingham, Handout of Network Security: 3 March 2008.

[2] Bruce Schneier, (1996) "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source", John Wiley & Sons, Inc.01/01/96, ISBN: 0471128457, pp. 126-132.

[3] Max Schmidt, Matthias Schunter and Arnd Weber, (1998) "Is Electronic Cash Possible?", Technischer Bericht Nr. A/03/98.

[4] Haejung Park., "VARIOUS ASPECTS OF DIGITAL CASH", (2008), Haejung University of Maryland, College Park.

[5] William Stallings, (1998) "Cryptography and Network Security: Principles and Practice , Prentice-Hall Second Edition, ISBN: 0-13-869017-0, pp. 19- 320

[6] Santa Clara, "An Introduction to Cryptography", 1990-1998 Network Associates, Inc. and its Affiliated Companies.

[7]Alfred J. Menezes - Paul C. van Oorschot - Scott A. Vanstone , (1996) "Handbook Of Applied Cryptography", Massachusetts Institute of Technology - ISBN: 0-8493-8523-7 , pp. 1-242

[8] Yiannis S. Tsiounis, (1997) "Efficient Electronic Cash New Notion and Techniques" , Northeastern University, pp. 1- 108.

[9] Bruce Schneier, (1996) "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source", John Wiley & Sons, Inc.01/01/96, ISBN: 0471128457, pp. 1-466.

[10] Wedelin D. (1997), "Digital Cash" , Goteborg University – 27 December 1997 - pp. 59-63.

[11] Brand Steven., (1991) "An Efficient Off-line Electronic Cash System Based on Representation Problem".

[11] Okamato T. and Ohta K. (1998), "Universal Electronic Cash" , Springer-verlag , ISBN 978-3-540-55188-1 pp.324-337 .

* تاريخ ورود البحث إلى مجلة جامعة دمشق 2012/12/9