مجلة جامعة طرطوس للبحوث والدراسات العلمية_ سلسلة العلوم الأساسية المجلد (5) العدد (4) 2021

Tartous University Journal for Research and Scientific Studies –Basic Sciences Series Vol. (5) No. (4) 2021

دراسة الأوتومات المنتهي الحتمي وتطبيقه على بروتوكول ملف مالي الكتروني بسيط

د. عائدة صائمة*

(تاريخ الإيداع 6/6/ 2021– تاريخ النشر 5/ 9/ 2021)

□ ملخّص □

نقوم في هذا البحث بالتعريف بنموذج الأوتومات المنتهي الحتمي وتطبيقه على بروتوكول ملف مالي الكتروني بسيط من العالم الحقيقي في حالتين الحالة الأولى عندما الأحداث تؤثر فقط على طرف مشارك من أطراف البروتوكول والحالة الثانية عندما الأحداث تؤثر في الأطراف الأخرى من البرتوكول ، ومن ثم التحقق من أداء هذا البرتوكول كنظام متكامل ببناء أوتومات الجداء له وتحليله واكتشاف فيما اذا كان يوجد خلل بهذا البرتوكول أو لا.

الكلمات المفتاحية : الأوتومات المنتهي الحتمي– أوتومات الجداء– ملف مالي– بروتوكول.

*مدرس في قسم الرياضيات – كلية العلوم – جامعة طرطوس

مجلة جامعة طرطوس للبحوث والدراسات العلمية_ سلسلة العلوم الأساسية المجلد (5) العدد (4) 2021

Tartous University Journal for Research and Scientific Studies –Basic Sciences Series Vol. (5) No. (4) 2021

Study of Deterministic Finite Automaton And Its Applying To a Simple Electronic Financial File

Dr.Aaeda Saema*

(Received 6/6/2021.Accepted 5/9/2021)

□ABSTRACT □

In this paper, we define the deterministic finite automaton model and apply it to a simple electronic financing file protocol of the real- world in two cases. The first case is when the actions affect only a participating party from the parties of the protocol. The second case is when the actions affect the other parties of the protocol. Then we check the performance of this protocol as the entire system by building the product automaton, analyzing it, and discovering whether there is a defect in this protocol or not.

Key Words: Deterministic finite automaton**,** Product automaton, Financing file**,** Protocol**.**

* Lecturer, Department of Mathematics, Faculty of Science, Tartous University.

1- مقدمة

يلعب التطور التكنولوجي دوراً حيوياً في حياة البشر . ولقد ظهرت في أواخر القرن العشرين مجموعة من الظواهر المختلفة التي أفرزها التقدم التكنولوجي مثل التجارة الإلكترونية، ووسائل الدفع الإلكترونية، والنقود الإلكترونية[2,8]. ولقد شهدت الحركة المصرفية حديثا تطوراً كبيراً وكان من أحد شواهد هذا التطور السماح لعملاء المصارف بإجراء عمليات الشراء والبيع من خلال شبكة الاتصالات (الانترنت) ، وذلك باستخدام وسائل الدفع الالكترونية التي تتيحها البنوك مثل النقود الالكترونية[4,6] . ومن أهم المشاكل التي تواجه الباعة على الانترنت هي قلة الأمن و كذلك فإن الدفعات المالية تحتاج إلى نظام أمني قوي على الانترنيت بهدف توفير إمكانيات شراء البضائع [2,4,6] ومن الحلول التي تم اقتراحها نظام البرتوكولات التي تدعم الملفات المالية الالكترونية والتي يمكن للزبون استخدامها للدفع مقابل شراء البضائع على شبكة الانترنت وبحيث أن البائع يحصل على النقود بعد أن يتأكد أن النقود حقيقية [4,8]. ونظراُ لأن بعض الأنظمة المالية تتبع سياسة التلاعب بالأموال وتقوم بتزييف لها لذلك علينا التحقق من أن أنظمة البرتوكولات المقترحة تنفذ السياسة التي نتبناها فيما يتعلق بكيفية استخدام الأموال[2,4,6] ومن أجل ذلك سنقوم في هذا البحث بتوصيف هذه البروتوكولات والتحقق من صحتها باستخدام نموذج الأوتومات المنتهي وهو نموذج بياني له مجموعة منتهية من الأوضاع وتحكم موجه يتحرك من حالة لأخرى عند استجابته لدخل ما[1,5].

2- أهمية البحث وأهدافه

تأتي أهمية هذا البحث من أهمية موضوع انتشار التجارة الالكترونية والنقود الالكترونية والمشاكل التي تواجهها مثل قلة الأمن وعدم المصداقية والتزوير والحاجة لإنشاء البروتوكولات التي تدعم الملفات المالية الالكترونية وتوصيفها والتحقق من صحتها باستخدام نموذج الاوتومات المنتهي و أوتومات الجداء. ويهدف هذا البحث إلى التعريف بنموذج الأوتومات المنتهي وتطبيقه على بروتوكول ملف مالي بسيط وتوصيف هذا البروتوكول في حالتين الحالة الأولى عندما تكون الأحداث تؤثر فقط على الطرف المشارك من أطراف البروتوكول والحالة الثانية عندما تؤثر الأحداث فقط في الأطراف الأخرى من البروتوكول ومن ثم التحقق من أداء هذا البرتوكول كنظام كلي ببناء أوتومات الجداء له وتحليله واكتشاف فيما اذا كان يوجد خلل بهذا البرتوكول أو لا .

3-طرق البحث وموارده

لتحقيق هدف البحث ، تم إتباع الخطوات الآتية:

- دراسة نظرية وتعريفية بنموذج الأوتومات المنتهي الحتمي و أوتومات الجداء.
- توصيف بروتوكول ملف مالي بسيط بنموذج الأوتومات المنتهي.
- بناء أوتومات الجداء لهذا البرتوكول وتحليله كنظام كلي واكتشاف فيما إذا كان لا يعاني أي خلل.

4- الدراسة النظرية

4-1- النقود الالكترونية والملف المالي الالكتروني:

4-1-1- تعريف النقود الالكترونية [2,4]:هي أي قيمة نقدية مخزنة على وسائل وأنظمة الكترونية كأنظمة الكمبيوتر المصرفية الالكترونية وتستخدم لتسهيل المعاملات الالكترونية لهذه الأنظمة باستخدام الانترنت.

4-2-1- تعريف الملف المالي الالكتروني[2,4]: هو الملف الذي يخزن ضمنه النقود الالكترونية والمعلومات التي تخصها.

4-2-نموذج الأوتومات المنتهي الحتمي:

4-2-1- تعريف الأوتومات المنتهي الحتمي DFA [3,5,9]: و هو عبارة عن الخماسية $A=(Q,\sum,\delta,q_0,F)$ ، حيث:

- Q- مجموعة منتهية غير خالية من أوضاع الأوتومات.
- $\sum$- مجموعة منتهية غير خالية من رموز الدخل وندعوها قاموس الدخل للأوتومات A.
- δ - دالة الانتقال للأوتومات وهو معرف على النحو الآتي: $\delta: Q\times\sum \longrightarrow Q$

$\delta(q,a)=p \;\; ;q,p\in Q$

حيث: الوضع p هو الوضع الذي ينتقل إليه الأوتومات A عندما يكون في الوضع q، ويقرأ رمز الدخل a من $\sum$.

- q_0 - أحد أوضاع Q وهو الوضع الابتدائي للأوتومات A.
- $F\subseteq Q$ - مجموعة الأوضاع النهائية للأوتومات وهي مجموعة غير خالية.

4-1-2-مخطط الانتقال للأوتومات المنتهي الحتمي[5,9]: يمكن تمثيل الأوتومات deterministic finite automaton DFA **بمخطط انتقال** وهو مخطط graph موجه يكون معرفاً على الشكل الآتي:

1- تمثل عقد هذا المخطط أوضاع المجموعة Q ومن أجل كل $a\in\sum$ وكل $q,p\in Q$ يوجد ضلع موجهة من العقدة q إلى العقدة p من أجل عنصر الدخل a إذا وفقط إذا كان: $\delta(q,a)=p$.

2- يوجد سهم باتجاه وضع البداية q_0 (Start State) .

أما العقد الموافقة للأوضاع النهائية F فتكون محاطة بدائرة مضاعفة ، أما الأوضاع الأخرى والتي ليست من F فتكون محاطة بدائرة واحدة فقط .

4-3-أوتومات الجداء [5,7] : ليكن $A=(Q,\sum,\delta,q_0,F)$ و $A'=(Q',\sum,\delta',q_0',F')$ أوتوماتين منتهيين حتميين DFA عندئذ نعرف أوتومات الجداء للأوتوماتين A و A' بأنه الأوتومات : $M=(Q_M,\sum,\delta_M,q_{0M},F_M)$، حيث:

- $Q_M=Q\times Q'=\{(q,q')\;\;;q\in Q\wedge q'\in Q'\}$ - مجموعة أوضاع أوتومات الجداء M.
- δ_M- دالة الانتقال لأوتومات الجداء وهو معرف من أجل أي وضع (q,q') من Q_M و a من $\sum$ على النحو الآتي:

$\delta_M: Q_M\times\sum\longrightarrow Q_M$

$\delta_M(\underbrace{(q,q')}_{state\ of\ M},a)=(\delta(q,a),\delta'(q',a)) \;\;;(q,q')\in Q_M$

- $q_{0M}=(q_0,q_0')\in Q_M$ - الوضع الابتدائي لأوتومات الجداء .
- $F_M\subseteq Q_M=Q\times Q'$ مجموعة الأوضاع النهائية في الأوتومات M، حيث $F_M=F\times F'$.

5-الدراسة العملية

إن البروتوكول هو مجموعة القواعد والقوانين التي يجري ضمنها تبادل مجموعة من الرسائل ونقل المعلومات بين مجموعة من الأطراف المتفاعلة فيما بينها والتي تشكل نظاماً مادياً.

لنعتمد سياسة التنفيذ الآتية في نظام البروتوكولات التي تدعم الملفات المالية الالكترونية: يحصل البائع في المتجر على النقود بعد أن يتأكد أن النقود حقيقية. كذلك يجب أن يعلم البائع أن الملف المالي ليس مزوراً ولم يتم نسخه وتم إرساله إلى البائع في المتجر بينما يحتفظ الزبون بنسخة من نفس الملف لاستخدامه مرة أخرى. أما الطرف الثالث من هذا البرتوكول وهو البنك فيجب أن يضمن وبسياسة التشفير عدم قابلية الملف للتزوير ولذلك يقوم البنك بإصدار وتشفير الملفات المالية لضمان عدم وجود أي مشكلة تزوير ، وبالإضافة لذلك فإن البنك يحتفظ بقاعدة بيانات من أجل جميع الأموال الصالحة التي يصدرها.

لنأخذ بروتوكول الملف المالي الالكتروني الآتي: وهو بروتوكول بسيط يحوي ثلاثة أطراف وهي المتجر (البائع)، الزبون والبنك. مع افتراض أنه يوجد ملف مالي واحد فقط. يمكن للزبون أن يقوم بتحويل الملف المالي هذا إلى المتجر عن طريق البنك، والمتجر بدوره يقوم باسترداد الملف المالي من البنك، أي الحصول من البنك على إصدار ملف مالي جديد يخص المتجر وليس الزبون ، وشحن البضائع إلى الزبون وبالإضافة لذلك فإن الزبون لديه خيار إلغاء الملف ، أي أن الزبون يمكن له أن يطلب من البنك وضع المال في حساب الزبون وهذا ما يجعل المال غير قابل للإنفاق. ويقتصر التفاعل بين هذه الأطراف على العمليات الخمس الآتية:

1- يمكن للزبون أن يقوم بالدفع pay، أي أن الزبون يقوم بإرسال المال إلى المتجر.

2- يمكن للزبون أن يقوم بالإلغاء cancel ، أي يتم إرسال الأموال إلى البنك مع رسالة مفادها أنه يجب إضافة قيمة المال إلى الحساب المصرفي للزبون.

3- يمكن للمتجر أن يقوم بشحن ship البضائع إلى الزبون.

4- يمكن للمتجر أن يسترد redeem المال، أي يتم إرسال الأموال إلى البنك على أن تعطى قيمته للمتجر.

5- يمكن للبنك أن يقوم بتحويل transfer الأموال عن طريق إنشاء ملف مالي جديد مشفر وإرساله للمتجر.

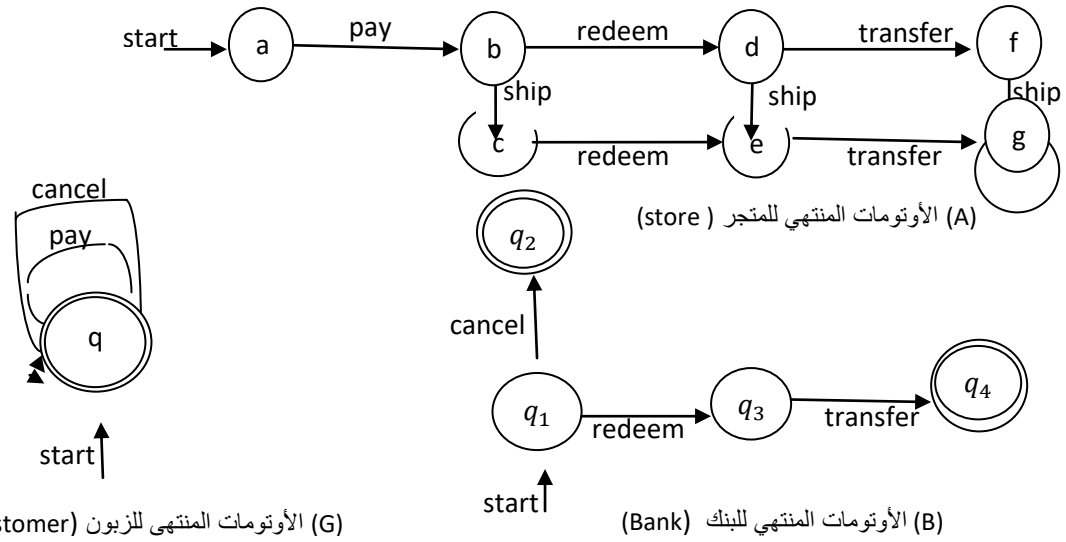
طبعا سنفترض أنه يجب على الأطراف الثلاثة تصميم تصرفاتهم بعناية مع إمكانية حدوث بعض الأشياء الخاطئة .ولذلك سنفترض بشكل منطقي أن الزبون لا يتصرف بمسؤولية وثقة ، إذ أنه قد يحاول نسخ ملف النقود أو استخدام هذا الملف للدفع عدة مرات أو الإلغاء وبالتالي يحصل على البضائع مجاناً. كما أن البنك من واجباته التأكد أنه لا يمكن لمتجرين أن يستردا الملف المالي نفسه وأن لا يسمح لهما بإلغاء الملف المالي أو استرداده على حد سواء.أما بالنسبة للمتجر فيجب أن يكون حذراً في تعاملاته وأن لا يقوم بشحن البضائع قبل أن يتأكد من أنه حصل على نقود غير مزورة مقابل هذه البضائع.

5-1- توصيف أطراف البروتوكول بنموذج الأوتومات المنتهي الحتمي و تحليل آلية تنفيذ كل طرف من أطراف البروتوكول باستخدام هذا الأوتومات :

ونميز هنا حالتين عند توصيف أطراف البروتوكول بنموذج الأوتومات المنتهي الحتمي وهي:

1-الحالة الأولى: التوصيف يشمل فقط الأحداث التي تؤثر على الطرف المشارك من أطراف البروتوكول ويكون كل طرف ممثل كأوتومات منتهي حتمي يوضح سلوك كل طرف من أطراف البرتوكول بشكل مستقل عن الآخر.

ويأخذ البروتوكول بعد التوصيف بنموذج الأوتومات المنتهي لكل طرف من أطرافه في هذه الحالة الشكل الآتي:



الشكل (١): أوتومات منتهي حتمي لكل من المتجر ، والزبون والبنك.

تحليل آلية تنفيذ كل طرف من أطراف البروتوكول باستخدام الأوتومات المنتهي في هذه الحالة: يظهر الشكل (1) تمثيل graph لكل طرف من أطراف البروتوكول الثلاثة كأوتومات منته حتمي، حيث يمثل كل وضع موجود في أي اوتومات منتهي الوضع الذي يمكن أن يكون أحد أطراف البرتوكول فيه. وتحدث الانتقالات بين الأوضاع عندما تحدث واحدة من العمليات الخمس المذكورة سابقاً ، وبحيث يكون كل طرف مسؤول عن بداية عملية واحدة أو أكثر من العمليات السابقة. ووصفنا في هذا التمثيل فقط العمليات (الإجراءات) التي تؤثر على كل طرف فمثلاً إجراء الدفع يؤثر على الزبون والمتجر فقط ، بحيث أن البنك لا يعلم أن الزبون قام بإرسال الأموال إلى المتجر ولكنه يكتشف هذا الإجراء عندما يقوم المتجر بتنفيذ إجراء الاسترداد.

إن الأوتومات المنتهي الحتمي (A) في الشكل (1) الذي يمثل المتجر هو: $A=(Q,\Sigma,\delta,q_0,F)$ ، حيث : $Q=\{a,b,c,d,e,f,g\}$ – أوضاع الأوتومات، $\Sigma=\{pay,redeem,ship,transfer\}$ – قاموس الدخل، $q_0=a$ –الوضع الابتدائي للأوتومات A، $F=\{g\}$ – مجموعة الأوضاع النهائية لهذا الأوتومات.

أما دالة الانتقال δ فتكون معرفة كما يلي : $\delta: Q\times\Sigma\longrightarrow Q$

حيث : $\delta(a,pay)=b$ ، $\delta(b,ship)=c$ ، $\delta(b,redeem)=d$ ، $\delta(b,ship)=c$ ، $\delta(d,ship)=e$ ، $\delta(d,transfer)=f$ ، $\delta(e,transfer)=g$ ، $\delta(f,ship)=g$

يبدأ هذا الأوتومات الممثل للمتجر في الوضع a ، عندما يطلب الزبون البضائع بواسطة إجراء الدفع، عندئذ فإن الأوتومات يشغل الوضع b ، الآن من الوضع b يبدأ الأوتومات بكل من إجراءات الشحن والاسترداد فإذا تم شحن البضاعة أولاً، فإن الأوتومات يشغل الوضع c ، وفي هذا الوضع يجب على المتجر استرداد قيمة الأموال من البنك واستلام تحويل ملف مالي مكافئ من البنك، ولكن بدلاً من ذلك فإن المتجر يقوم من الوضع b بإرسال رسالة الاسترداد أولاً داخلاً الوضع d .الآن من الوضع d فإن المتجر يقوم بالشحن مرة أخرى داخلاً الوضع e، أو من الوضع d يمكن للمتجر أن يتلقى استلام تحويل الأموال من البنك فيدخل الأوتومات الوضع f . من الوضع f يمكن للمتجر أن يقوم بعملية الشحن في النهاية، وبذلك يدخل الأوتومات الوضع النهائي g حيث لا يقوم المتجر بأي عملية

بعد ذلك من هذا الوضع لأن العملية اكتملت. أما عندما يكون الأوتومات في الوضع e فإن المتجر ينتظر تحويل الأموال من البنك داخلاً الأوتومات الوضع g ، ولكن للأسف فإنه حتى لو لم يتم تحويل الأموال من البنك أبداً. فإن المتجر يكون قد قام بعملية شحن البضائع للزبون وهذا من سوء حظ المتجر.

أما الأوتومات المنتهي الحتمي (G) في الشكل(1) الذي يمثل الزبون فهو: $G=(Q,\sum,\delta,q_0,F)$ ،حيث: $Q=\{q\}$ – حالات الأوتومات ، $\sum=\{pay,cance\}$ – قاموس الدخل، $q_0=q$ – الوضع الابتدائي لهذا الأوتومات ، $F=\{q\}$ –مجموعة الأوضاع النهائية لهذا الأوتومات ، أما دالة الانتقال δ فتكون معرفة كما يلي: $\delta: Q\times\sum \longrightarrow Q$ ، حيث: $\delta(q,pay)=q$ ، $\delta(q,cancel)=q$.

نلاحظ أن هذا الأوتومات الممثل للزبون لديه وضع واحد فقط هو q وبالتالي يمكن لهذا الزبون أن يقوم بإجراء الدفع و إجراء الإلغاء (العمليتان (1) و (2) من العمليات الخمس المذكورة سابقاً) بأي عدد من المرات وبأي ترتيب دون وجود أي تقييد. وفي كل إجراء يقوم به يبدأ من نفس الحالة q ويرجع للحالة نفسها.

أما الأوتومات المنتهي الحتمي (B) في الشكل(1) الذي يمثل البنك فهو: $B=(Q,\sum,\delta,q_0,F)$ ،حيث $Q=\{q_1,q_2,q_3,q_4\}$ أوضاع الأوتومات ، $\sum=\{cancel,redeem,transfer\}$ قاموس الدخل، $q_0=q_1$ الوضع الابتدائي للأوتومات B ، $F=\{q_2,q_4\}$ مجموعة الأوضاع النهائية لهذا الأوتومات.

أما دالة الانتقال δ فتكون معرفة كما يلي: $\delta: Q\times\sum \longrightarrow Q$ ، حيث:

$$\delta(q_1,cancel)=q_2 \quad ,\delta(q_1,redeem)=q_3 \quad ,\delta(q_3,transfer)=q_4$$

يبدأ هذا الأوتومات من الوضع الابتدائي q_1 الذي يمثل إصدار البنك للملف المالي المطلوب دون أن يطلب منه استرداد هذا الملف أو إلغاءه. والأوتومات في الوضع q_1 لديه خياران:

الخيار الأول: في حالة طلب الزبون من البنك إلغاء هذا الملف فإن البنك يقوم بإعادة الأموال إلى حساب الزبون ويدخل الأوتومات الوضع q_2 والذي يمثل قيام البنك بإجراء إلغاء الملف المالي.ومن هذا الوضع لا يسمح البنك للزبون بالقيام بإجراء إلغاء نفس الملف المالي أو استخدامه مرة أخرى.

الخيار الثاني: في حال تلقي البنك طلب استرداد للأموال من المتجر عندئذ فإن الأوتومات يشغل الوضع q_3 ويقوم البنك من هذا الوضع بإرسال رسالة تحويل للمتجر مع ملف نقود جديد يخص المتجر وعند إرسال رسالة التحويل هذه ينتقل الأوتومات للوضع q_4. ومن هذا الوضع فإن البنك لا يقوم بتنفيذ أي إجراء جديد يخص الملف المالي المتعلق بالمتجر.

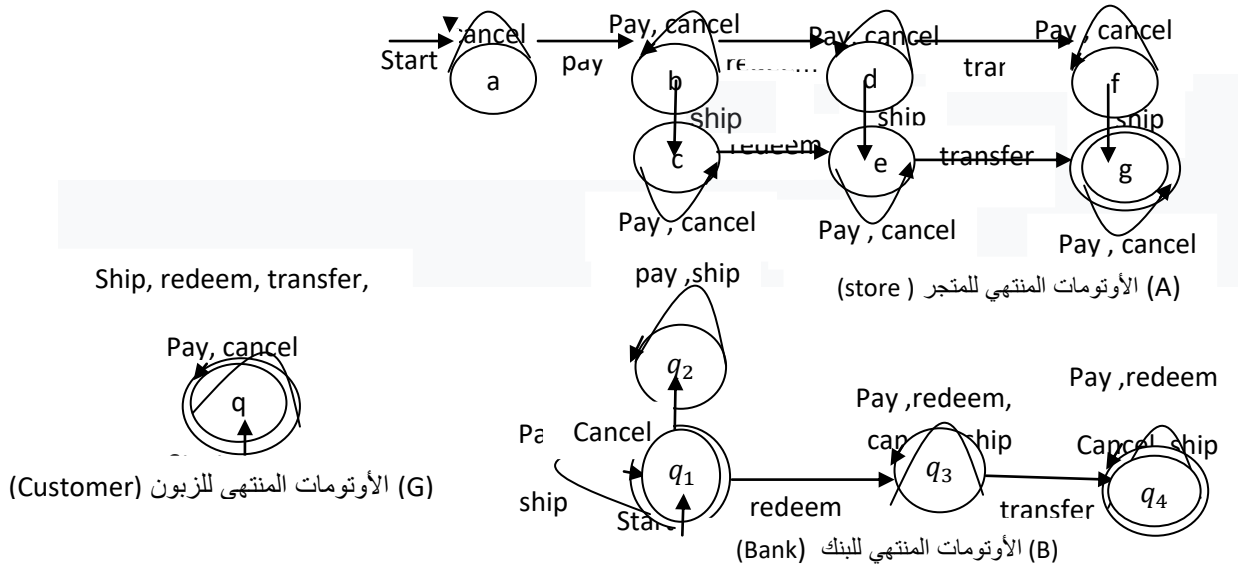
الحالة الثانية: التوصيف يشمل الأحداث التي تؤثر على الطرف المشارك بالإضافة للأطراف المشاركة الأخرى: هناك بعض الإجراءات (العمليات) التي تم تجاهلها في الحالة الأولى ويجب إضافتها في هذه الحالة كانتقالات جديدة لكل من الأوتوماتات الثلاث الممثلة لأطراف البروتوكول في الشكل (1) لأن عدم إضافتها يؤدي لتوقف أحد الأوتوماتات السابقة عن التنفيذ وهي نوعان:

النوع الأول: الإجراءات التي ليس لها علاقة بالطرف المشارك نفسه: على سبيل المثال الإجراء الوحيد الذي ليس له علاقة بالمتجر هو إجراء الإلغاء، إذ أن المتجر لا يتأثر بهذا الإجراء، لذلك إذا قام الزبون بتنفيذ إجراء الإلغاء فإن المتجر يجب أن يبقى في الحالة التي يكون فيها ولذلك نضيف لجميع أوضاع أوتومات المتجر (A) السبعة انتقالات ذات عناصر دخل cancel تبدأ من كل وضع في هذا الأوتومات وترجع للوضع نفسه أي نضيف خط ارتباط ذو عنصر الدخل cancel لأوضاع الأوتومات A السبع .لأن عدم إضافة هذه الانتقالات يؤدي لتوقف أوتومات

المتجر عن التنفيذ وعندئذ لا يستطيع أن ينتقل لأي حالة ولا يمكنه تنفيذ إجراءات جديدة .أيضاً بالنسبة للبنك فإن إجرائي الدفع pay والشحن ship وبشكل مشابه لما سبق ليس لها علاقة بالبنك، ولذلك نضيف لأوضاع أوتومات البنك B الأربع خط ارتباط ذو عنصري الدخل pay، ship. أما بالنسبة للزبون فإن الإجراءات التي ليس لها علاقة بالزبون فهي ship، redeem وtransfer ولذلك نضيف خط ارتباط ذات عناصر الدخل ship ، redeem و transfer لوضع أوتومات الزبون الوحيد. وبما أن أوتومات الزبون لديه وضع واحد فقط وبالتالي فإنه بعد أي عدد من الإدخالات يبقى أوتومات الزبون في نفس الوضع ولذلك فإن هذا الأوتومات ليس لديه تأثير على تشغيل نظام البروتوكول الكلي كوحدة متكاملة، ولكنه يبقى أحد الأطراف المشاركة في نظام البروتوكول الكلي طالما أنه هو الذي يقوم بأحداث الدفع pay و الإلغاء cancel.

النوع الثاني: الإجراءات الخاطئة غير المسموح بها لأنها تؤدي لتوقف تنفيذ أحد الأتوماتات : وهي أن يقوم أحد الأطراف بتنفيذ إجراء ما بشكل خاطئ أو غير مقصود مما يؤدي لتوقف أحد الأوتوماتات الممثلة لأطراف البروتوكول، على سبيل المثال لنفرض أن الزبون قرر تنفيذ إجراء الدفع مرة ثانية، بينما أوتومات المتجر في الوضع e وبما أن الوضع e ليس لديه أي انتقال خارج منه ذو عنصر دخل pay وبالتالي فإن أوتومات المتجر سيتوقف عن التنفيذ قبل أن يتمكن من الحصول على تحويل للأموال من البنك ، ولكي لا نسمح للزبون بتوقيف أوتومات المتجر نضيف خطوط ارتباط ذات عناصر الدخل pay لجميع أوضاع أتومات المتجر باستثناء الوضع الابتدائي للمتجر a لأنه يوجد انتقال للزبون بالإجراء pay من الوضع a إلى الوضع b. كذلك لمنع الزبون من توقيف أوتومات البنك من خلال تنفيذه إجراء إلغاء الأموال التي تم استردادها ، نضيف خط ارتباط ذات عناصر الدخل cancel و redeem لكل من الوضعين q_3 و q_4 لأوتومات البنك.

بعد إضافة الانتقالات الجديدة لكل من الأوتوماتات الثلاث الممثلة لأطراف البروتوكول في الشكل (1) وفقاً للحالة الثانية فإن البروتوكول يأخذ الشكل التالي:



الشكل (2): المجموعات الكاملة لانتقالات الأوتوماتات المنتهية التي تمثل كل من المتجر ، والزبون والبنك.

ونبين التعديلات والإضافات التي طرأت على كل من الأوتوماتات الثلاثة الممثلة لأطراف البروتوكول في الشكل (1) والموضحة في الشكل (2) كالآتي:

أولاً: التعديلات الجديدة التي طرأت على الأوتومات المنتهي الحتمي $A=(Q,\Sigma,\delta,q_0,F)$ **الذي يمثل المتجر** كما في الشكل (2) فإن كلاً من F,Q و q_0 تبقى كما عرفت في الحالة الأولى أما مجموعة قاموس الدخل $\Sigma=\{pay,redeem,ship,transfer\}$ فنضيف إليها عنصر الدخل $cancel$ لتصبح $\Sigma=\{cancel,pay,redeem,ship,transfer\}$، أما دالة الانتقال δ فتكون معرفة كما في الحالة الأولى ولكن مع إضافة الانتقالات التالية :

$$\delta(d,pay)=d\ ،\delta(d,cancel)=d\ ،\quad \delta(b,pay)=b\ ،\delta(b,cancel)=b\ ،\ \delta(a,cancel)=a$$
$$\delta(f,pay)=f\ ،\delta(e,cancel)=e\quad \delta(e,pay)=e\ ،\ \delta(c,cancel)=c\ ،\ \delta(c,pay)=c$$
$$\delta(g,cancel)=g\in F\ ،\delta(g,pay)=g\in F\ ،\delta(f,cancel)=f$$

ثانياً: التعديلات الجديدة التي طرأت على الأوتومات المنتهي الحتمي $G=(Q,\Sigma,\delta,q_0,F)$ **الذي يمثل الزبون** في الشكل (1) والمبين في الشكل (2) فإن كلاً من F,Q و q_0 تبقى كما عرفت في الحالة الأولى، أما مجموعة قاموس الدخل $\Sigma=\{cancel,pay\}$ فنضيف إليها عناصر الدخل $redeem,ship,transfer$ لتصبح $\Sigma=\{cancel,pay,redeem,ship,transfer\}$ أما دالة الانتقال δ فتكون معرفة كما في الحالة الأولى ولكن مع إضافة الانتقالات التالية :

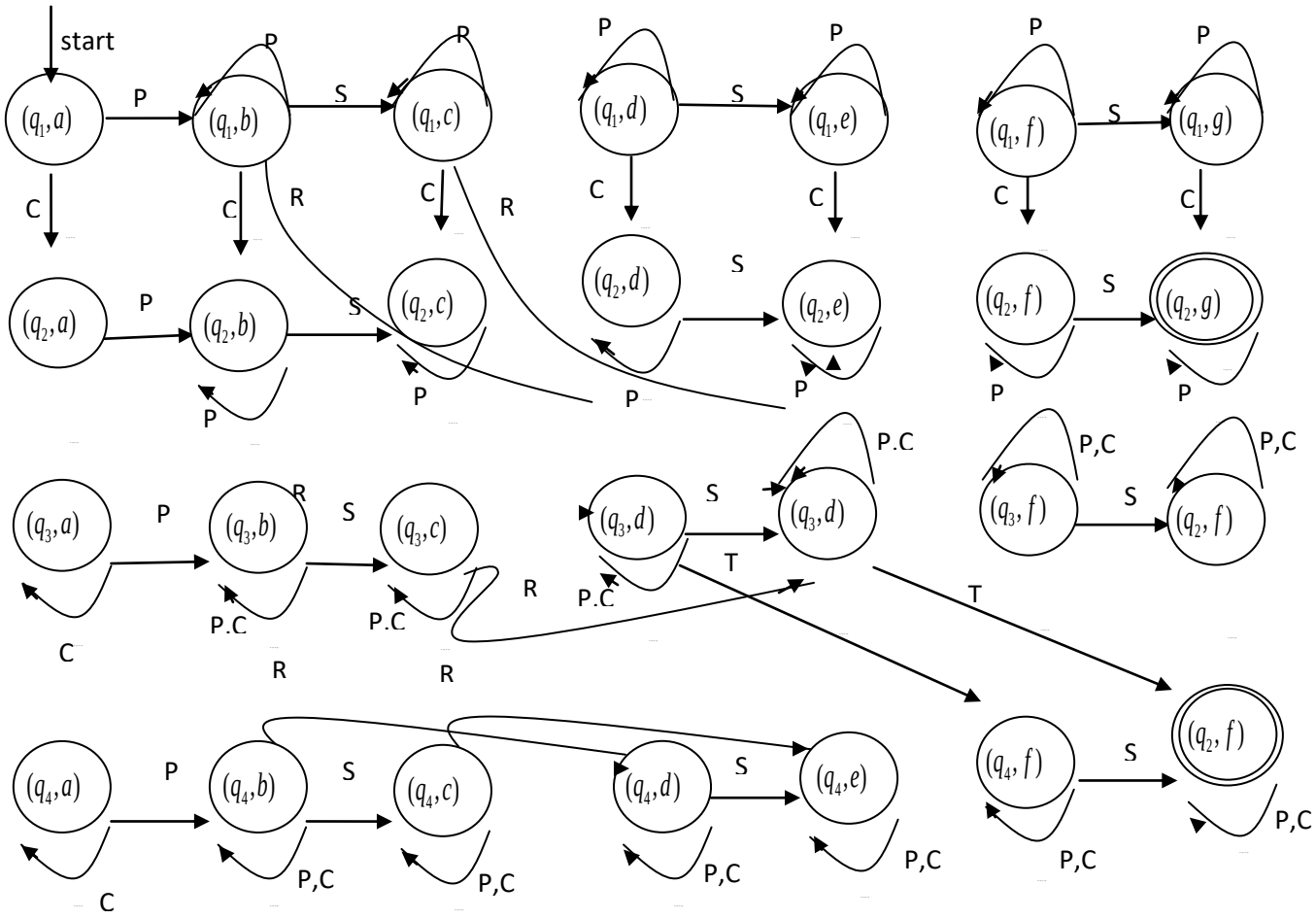
$$\delta(q,transfer)=q\ ،\delta(q,ship)=q\ ،\delta(q,redeem)=q$$

ثالثاً: التعديلات التي طرأت على الأوتومات المنتهي الحتمي $B=(Q,\Sigma,\delta,q_0,F)$ **الذي يمثل البنك** والتي تم رسمها في الشكل (2) فإن كلاً F,Q و q_0 تبقى كما عرفت في الحالة الأولى، أما مجموعة قاموس الدخل $\Sigma=\{cancel,redeem,transfer\}$ فنضيف إليها عنصري الدخل $pay,cancel$ لتصبح $\Sigma=\{cancel,pay,redeem,ship,transfer\}$، أما دالة الانتقال δ فتكون معرفة كما في الحالة الأولى ولكن مع إضافة الانتقالات التالية:

$$\delta(q_3,ship)=q_3\ ،\delta(q_2,pay)=q_2\ ،\delta(q_2,ship)=q_2\ ،\delta(q_1,pay)=q_1\ ،\ \delta(q_1,ship)=q_1$$
$$\delta(q_4,cancel)=q_4\ ،\quad \delta(q_3,redeem)=q_3\quad ،\delta(q_3,pay)=q_3\quad ،\delta(q_3,cancel)=q_3$$
$$\delta(q_4,pay)=q_4\ ،\delta(q_4,redeem)=q_4\ ،\ \delta(q_4,ship)=q_4$$

5-2- توصيف وتحليل نظام البروتوكول الكلي باستخدام أوتومات الجداء : يظهر في الشكلين (١) و(٢) تمثيلات graph لنماذج الأوتومات المنتهي الممثلة لأطراف البروتوكول الثلاثة المتجر، البنك والزبون وبحيث أن كل أوتومات منها يوصف سلوك وآلية تنفيذ كل طرف من أطراف البروتوكول ، ولكن حتى الآن ليس لدينا تمثيل graph أو نموذج يوصف تفاعل أطراف البروتوكول الثلاثة كنظام كلي والطريقة الأنسب لاستكشاف هذا التفاعل وتحليله يكون ببناء أوتومات الجداء للأوتوماتات الثلاث التي تمثل كلا من المتجر والبنك والزبون. و بما أن الزبون ليس لديه أي قيود على السلوك والأوتومات المنتهي الذي يمثله له وضع واحد فقط و أي تسلسل من الأحداث يبقى الأوتومات في الوضع نفسه، وبالتالي النظام الكلي لا يمكن أن يتوقف عن التنفيذ .ولذلك فإن أوتومات الزبون لا نأخذه بعين الاعتبار عند بناء أوتومات الجداء الذي يمثل نظام البروتوكول الكلي. إنما نكتفي ببناء أوتومات الجداء فقط لأوتوماتي المتجر والبنك.

5-2-1- بناء أوتومات الجداء :إن الشكل (3) يظهر تمثيل graph لأوتومات الجداء للبروتوكول كنظام كلي ومن أجل التبسيط وتوفير مساحة الرسم سنستخدم الاختصارات P,S,C,R and T بدلاً من عناصر مجموعة قاموس الدخل Pay ,Ship ,Cancel ,Redeem and Transfer



الشكل (3): أوتومات الجداء لأوتوماتي البنك والمتجر.

ويكون أوتومات الجداء M الممثل لنظام البروتوكول الكلي والمبني من كل أوتومات البنك $B=(Q,\sum,\delta,q_0,F)$ و أوتومات المتجر $A=(Q',\sum,\delta',q_0',F')$ هو الأوتومات $M=(Q_M,\sum,\delta_M,q_{0M},F_M)$ وفقاً للشكل (3)، حيث:

- مجموعة أوضاع أوتومات الجداء M هي المجموعة Q_M :

$$Q_M=Q\times Q'=\{(q,q')\ ;q\in Q\wedge q'\in Q'\}$$

$$=\left\{\begin{matrix}(q_1,a),(q_1,b),(q_1,c),(q_1,d),(q_1,e),(q_1,f),(q_1,g),(q_2,a),(q_2,b),(q_2,c),\\(q_2,d),(q_2,e),(q_2,f),(q_2,g),(q_3,a),(q_3,b),(q_3,c),(q_3,d),(q_3,e),(q_3,f),\\(q_3,g),(q_4,a),(q_4,b),(q_4,c),(q_4,d),(q_4,e),(q_4,f),(q_4,g)\end{matrix}\right\}$$

و عدد أوضاع أوتومات الجداء M هو: $|Q_M|=|Q\times Q'|=4\times 7=28$.

- قاموس الدخل للأوتوما ت M

$\sum = \{cancel, pay, redeem, ship, transfer\} = \{C, P, R, S, T\}$

- الوضع الابتدائي لأوتومات الجداء M هو: $q_{0M} = (q_1, a)$.
- مجموعة الأوضاع النهائية لأوتومات الجداء M $F_M = F \times F' = \{(q_2, g), (q_4, g)\}$.
- أما دالة الانتقال $\delta_M : Q_M \times \sum \longrightarrow Q_M$ لأوتومات الجداء M بحيث من أجل أي وضع (q, q') من Q_M و عنصر الدخل a من $\sum$ فإن دالة الانتقال δ_M تكون معرفة وفقاً لأوتومات الجداء المرسوم في الشكل(3) كما يلي :

1- من أجل الوضع (q_1, a) فإن: $\delta_M((q_1, a), P) = (\delta(q_1, P), \delta'(a, P)) = (q_1, b)$

$\delta_M((q_1, a), C) = (q_2, a)$

2- من أجل الوضع (q_1, b) فإن : $\delta_M((q_1, b), P) = (q_1, b), \delta_M((q_1, b), S) = (q_1, c)$

$\delta_M((q_1, b), R) = (q_3, d), \delta_M((q_1, b), C) = (q_2, b)$

3- من أجل الوضع (q_1, c) فإن:

$\delta_M((q_1, c), P) = (q_1, c)$ $\delta_M((q_1, c), C) = (q_2, c)$ $\delta_M((q_1, c), R) = (q_3, e)$,

4- من أجل الوضع (q_1, d) فإن:

$\delta_M((q_1, d), P) = (q_1, d), \delta_M((q_1, d), S) = (q_1, e)$, $\delta_M((q_1, d), C) = (q_2, d)$

5- من أجل الوضع (q_1, e)فإن: $\delta_M((q_1, e), P) = (q_1, e), \delta_M((q_1, e), C) = (q_2, e)$

6- من أجل الوضع (q_1, f) فإن: $\delta_M((q_1, f), P) = (q_1, f), \delta_M((q_1, f), S) = (q_1, g)$

$\delta_M((q_1, f), C) = (q_2, f)$

7- من أجل الوضع (q_1, g) فإن : $\delta_M((q_1, g), P) = (q_1, g), \delta_M((q_1, g), C) = (q_2, g)$

8- من أجل الوضع (q_2, a) فإن: $\delta_M((q_2, a), P) = (q_2, b)$

9- من أجل الوضع (q_2, b) فإن: $\delta_M((q_2, b), P) = (q_2, b), \delta_M((q_2, b), S) = (q_2, c)$

10- من أجل الوضع (q_2, c)فإن: $\delta_M((q_2, c), P) = (q_2, c)$

11- من أجل الوضع (q_2, d)فإن: $\delta_M((q_2, d), P) = (q_2, d), \delta_M((q_2, d), S) = (q_2, e)$

12- من أجل الوضع (q_2, e) فإن: $\delta_M((q_2, e), P) = (q_2, e)$

13- من أجل الوضع (q_2, f)فإن $\delta_M((q_2, f), P) = (q_2, f), \delta_M((q_2, f), S) = (q_2, g) \in F_M$

14- من أجل الوضع (q_2, g) فإن: $\delta_M((q_2, g), P) = (q_2, g) \in F_M$

15- من أجل الوضع (q_3, a)فإن: $\delta_M((q_3, a), P) = (q_3, b), \delta_M((q_3, a), C) = (q_3, a)$

16- من أجل الوضع (q_3, b) فإن: $\delta_M((q_3, b), P) = (q_3, b), \delta_M((q_3, b), S) = (q_3, c)$

$\delta_M((q_3, b), R) = (q_3, d), \delta_M((q_3, b), C) = (q_3, b)$

17- من أجل الوضع (q_3, c)فإن: $\delta_M((q_3, c), P) = (q_3, c)$

$\delta_M((q_3, c), R) = (q_3, e), \delta_M((q_3, c), C) = (q_3, c)$

18- من أجل الوضع (q_3, d) فإن: $\delta_M((q_3, d), P) = (q_3, d), \delta_M((q_3, d), S) = (q_3, e)$

$\delta_M((q_3, d), T) = (q_4, f), \delta_M((q_3, d), C) = (q_3, d)$

19- من أجل الوضع (q_3,e) فإن:

$$\delta_M((q_3,e),P)=(q_3,e),\delta_M((q_3,e),T)=(q_4,g)\in F_M,\delta_M((q_3,e),C)=(q_3,e)$$

20- من أجل الوضع (q_3,f) فإن:

$$\delta_M((q_3,f),P)=(q_3,f),\delta_M((q_3,f),S)=(q_3,g),\delta_M((q_3,f),C)=(q_3,f)$$

21- من أجل الوضع (q_3,g) فإن: $\delta_M((q_3,g),P)=(q_3,g),\delta_M((q_3,g),C)=(q_3,g)$

22- من أجل الوضع (q_4,a) فإن: $\delta_M((q_4,a),P)=(q_4,b),\delta_M((q_4,a),C)=(q_4,a)$

23- من أجل الوضع (q_4,b) فإن: $\delta_M((q_4,b),P)=(q_4,b),\delta_M((q_4,b),S)=(q_4,c)$

$$\delta_M((q_4,b),R)=(q_4,d),\delta_M((q_4,b),C)=(q_4,b)$$

24- من أجل الوضع (q_4,c) فإن:

$$\delta_M((q_4,c),R)=(q_4,e),\delta_M((q_4,c),P)=(q_4,c),\delta_M((q_4,c),C)=(q_4,c)$$

25- من أجل الوضع (q_4,d) فإن:

$$\delta_M((q_4,d),P)=(q_4,d),\delta_M((q_4,d),S)=(q_4,e),\delta_M((q_4,d),C)=(q_4,d)$$

26- من أجل الوضع (q_4,e) فإن: $\delta_M((q_4,e),P)=(q_4,e),\delta_M((q_4,e),C)=(q_4,e)$

27- من أجل الوضع (q_4,f) فإن:

$$\delta_M((q_4,f),P)=(q_4,f),\delta_M((q_4,f),S)=(q_4,g),\delta_M((q_4,f),C)=(q_4,f)$$

28- من أجل الوضع (q_4,g) فإن:

$$\delta_M((q_4,g),P)=(q_4,g),\delta_M((q_4,g),C)=(q_4,g)\in F_M$$

5-2-2- تحليل آلية تنفيذ البرتوكول كنظام كلي باستخدام أوتومات الجداء: نلاحظ من أوتومات الجداء M والمرسوم في الشكل (3) أنه من بين الأوضاع الـ 28 لأوتومات الجداء M والموجودة في المجموعة Q_M يوجد عشر أوضاع فقط قابلة للوصول من الوضع الابتدائي $q_{0M}=(q_1,a)$ لهذا الأوتومات وهي:

$$(q_1,a),(q_1,b),(q_1,c),(q_2,a),(q_2,b),(q_2,c),(q_3,d),(q_3,e),(q_4,f),(q_4,g)$$

أما الأوضاع الثمانية عشر الباقية من أوضاع المجموعة Q_M فهي غير قابلة للوصول من الوضع الابتدائي $q_{0M}=(q_1,a)$ أي لا يوجد مسار من الوضع الابتدائي لأي من هذه الأوضاع وطالما لا يمكن الوصول إليها من الوضع الابتدائي (الوضع الابتدائي الذي يمثل بداية تشغيل نظام البروتوكول) وبالتالي يتم إهمالها . والهدف من تحليل آلية تنفيذ هذا البرتوكول كنظام كلي باستخدام أوتومات الجداء M هو الإجابة عن بعض الأسئلة المتعلقة بالبروتوكول للتنبوأ بسلوكه من الشكل "هل يمكن لخطأ من نوع محدد أن يحدث" ، على سبيل المثال نسأل فيما إذا كان باستطاعة المتجر أن يشحن البضائع من دون الحصول على أموال أي هل بإمكان أوتومات الجداء أن ينتقل للوضع الذي يكون أتم فيه المتجر عملية الشحن والموافق لحالة أن المتجر في أحد الأوضاع التالية: c أو g أو e وهي تمثل المركبة الثانية من أوضاع أوتومات الجداء التالية: $(q_i,c),(q_i,e),(q_i,g)$; $i=1,2,3,4$ وبالتوازي مع المركبة الثانية فإن المركبة الأولى من الأوضاع السابقة والموافقة لأحد أوضاع البنك التالية q_1 ، q_2 ، q_3 و q_4 فلم يتم إجراء أي انتقال من أجل الدخل T إطلاقاً ولن يتم إجراءه وبحيث أن أوتومات الجداء لن يدخل بمركبته الأولى والتي تمثل البنك أحد الأوضاع q_i من أجل $i=1,2,3,4$ لأن البنك لا يقوم بعملية تحويل الأموال إلى المتجر بشكل متوازي مع عملية إتمام شحن البضائع إلى المتجر. فمثلا في الوضع (q_3,e) فإن البضائع تم شحنها ولكن الأموال لم

يتم تحويلها من قبل البنك إلى المتجر ولكن أخيراً من الوضع (q_3, e) هنالك انتقال يتم من أجل الدخل T ويدخل أوتومات الجداء للوضع النهائي (q_4, g) . أما فيما يتعلق بما يفعله البنك، فإنه قبل وصوله وانتقاله إلى الوضع q_3 ، وعند تلقيه طلب الاسترداد Redeem فإنه يتم معالجة هذا الطلب وهذا يعني أن البنك كان في الوضع q_1 قبل تلقيه طلب Redeem ولذلك فإن رسالة Cancel لم يتم استلامها وسيتم تجاهلها إذا تم استقبالها مستقبلاً سواء عندما يكون البنك بالوضع q_1 أو الوضع q_3 وسيقوم البنك بنقل الأموال إلى المتجر عند وصوله للوضع q_4 .

أيضا نلاحظ من هذا الأوتومات أن الوضع (q_2, c) قابل للوصول من الوضع الابتدائي ولكن القوس الوحيد الخارج منه يعود إليه مرة أخرى وهذا الوضع مطابق لحالة أن البنك استلم رسالة Cancel قبل رسالة Redeem وأما المتجر فيستلم رسالة Pay وهذا يدل على أن الزبون كان يتصرف بازدواجية في المعايير فهو قد أنفق(دفع) الأموال ثم ألغاها و أن المتجر قام بعملية شحن البضائع قبل أن يقوم بإجراء استرداد الأموال وعندما يقوم المتجر بتنفيذ إجراء الاسترداد redeem فإن البنك لن يستلم الرسالة لأنه يكون في الوضع q_2 حيث يكون البنك ألغى الأموال ولن يعالج عملية طلب استرداد الأموال للمتجر. وبالتالي نلاحظ أن أوتومات الجداء يخبرنا عن الوضع الذي يكون فيه كل طرف من أطراف البروتوكول وكيفية التفاعل فيما بينها، وعن وجود خلل بآلية تنفيذ البروتوكول وكيف يتصرف بهذه الحالة . طبعاً لا ننسى أن تصرفات الزبون لا تؤثر على أي طرف من أطراف البروتوكول الأخرى.

٦- الاستنتاجات والتوصيات

- تم في هذا البحث التعريف بنموذج الأوتومات المنتهي كنموذج لتوصيف برتوكولات الملفات المالية الالكترونية والتحقق من صحتها وتحليل أداءها.
- تم تطبيق هذا النموذج لتوصيف ونمذجة بروتوكول ملف مالي بسيط في حالتين الحالة الأولى عندما تكون الأحداث تؤثر فقط على طرف مشارك من أطراف البروتوكول والحالة الثانية عندما تكون الأحداث تؤثر في الأطراف الأخرى من البروتوكول.
- تم استخدام هذا النموذج لتحليل سلوك وآلية تنفيذ كل طرف من أطراف هذا البروتوكول.
- تم التحقق من أداء هذا البرتوكول كنظام كلي ببناء أوتومات الجداء له وتحليله واكتشاف فيما اذا كان يوجد خلل بآلية تنفيذ البروتوكول وكيف يتصرف بهذه الحالة.
- تم رسم تمثيل graph لأوتومات الجداء لكل من أوتوماتي المتجر والبنك بعد بناءه وبشكل يسمح بتحديد الحالات القابلة للوصول من الحالة الابتدائية من الحالات غير القابلة للوصول من أجل إهمالها مع الانتقالات المرافقة لها من أجل توفير مساحة الرسم وفضاء الحالات.
- نلاحظ أن هذا البحث هام وفعال نظراً لتطبيقاته المتعددة في مجال التجارة الالكترونية والنقود الالكترونية والبروتوكولات التي تدعم الملفات المالية الالكترونية .

ونظراً لما قدمته هذه الدراسة من نتائج هامة نوصي بضرورة تعميم هذه الدراسة على بروتوكولات ملفات مالية أكثر تعقيداً.

المراجع

[1] AGRAWAL, S. ; Singh, A.P.(2017). *Reusable Garbled Deterministic Finite Automata from Learning With Errors.* ICALP. Vol.36,pp. 1-13.

[2] ALQAHTANI, F.(2014). *A Fair Exchange & Customer Anonymity Protocol Using A Trusted Third Party for Electronic Commerce Transactions & Payments*., IJNSA,pp. 40-66.

[3] CABRAL ,F. G.; MOREIRA, M. V.; DIENE, O.; BASILIO,J. C.(2014). *A Petri Net Diagnoser for Discrete Event Systems Modeled by Finite State Automata.* IEEE Transactions on Automatic Control vol. 11,PP .21-46.

[4] EHIKIOYA, S. A.; GUILLEMOT, E.(2020). *A critical assessment of the design issues in e-commerce systems development. Engineering Reports,* John Wiley & Sons, Ltd.pp. 1-24.

[5] GOPALAKRISHNAN, G. (2006). *Computation Engineering Applied Automata Theory and Logic,* Springer ,U.S.A,pp. 1- 492.

[6] HARSHITA ; Tanwar, S.(2016). *Implementation of Fair-exchange and Anonymous Online E-cash Protocol for E-commerce*. IJITCS Vol.8, No.8, PP.66-74.

[7] PARTHASARATHY, M .(2010),*The product construction: Closure un-der intersection and union* ,Theory of Computation Madhusudan Parthasarathy, CS Vol. 373,pp. 1-3.

[8] SOVA, K. (2013).Electronic Money Trends In User's Perspective.PHD, Turku University of Applied Sciences, Turun Ammattiorkeako ,pp.1-76.

[9]ZHANG , J.; QIAN , Z . (2013) . *The Equivalent Conversion between Regular Gram- mar and Finite Automata.* JSEA. Vol. 6,PP. 33-37.

.