ورقة بحثية مجلة مفتوحة الوصول

تقنية سلسلة الكتل Blockchain نحو أفق جديد

د. بشرى معلا * ، فاطمة زرقة **

* (قسم الميكاترونيكس ، جامعة المنارة

البريد الإلكتروني: boushra.maala@manara.edu.sy)

**(قسم هندسة الاتصالات والالكترونيات ، جامعة تشرين

البريد الإلكتروني: fatema7zarka@gmail.com)

الملخص

ظهرت فكرة تقنية سلسلة الكتل Blockchain كواحدة من أهم وأحدث التقنيات الأمنية الرائجة حالياً. إنها تقنية ذات مستوى أمنٍ عالٍ، ويعود ذلك إلى بنيتها اللامركزية ، وتحقيقها لتكاملية البيانات المخزنة بها، والشفافية التي تحول دون حدوث أي تناقض في النظام، إذ لا يوجد ما هو مخفي، واستخدامها للعقود الذكية و تقنيات الإجماع. إضافة إلى سرعة الإنجاز، إذ يمكن أن تنفذ عملية الإرسال والاستلام في غضون بضع دقائق.

كلمات مفتاحية – سلسلة الكتل، بيتكوين، العقود الذكية، تقنيات الإجماع، التشفير غير المتناظر.

I. مقدمة

العالم على أعتاب التغيير، كل ما يحيط بنا يدخل بوابة التحول الرقمي. مع التطور التكنولوجي الكبير والسريع الذي يشهده العالم ظهرت تقنيات جديدة حملت معها تحولات مبهرة. لكن عندما نتحدث عن التحول الرقمي نذهب مباشرة إلى فكرة ظهور العملات الرقمية بدءاً من البتكوين، وعندها لابد أن نولي جانب أمن المعلومات أهمية كبيرة . يشكل الأمن حجر الزاوية في جميع النشاطات عبر الانترنت، ولا سيما النشاطات المالية، لتلبية متطلب الأمن ظهرت فكرة تقنية سلسلة الكتل.

غيرت ثورة سلسلة الكتل (Blockchain) سلطة المالك، بما حملته من ميزات كاللامركزية (decentralized) والتوزيع (distributed) والثبات (immutable) والشفافية (transparent) ، تعتمد هذه التقنية بشكل أساسي على توابع البعثرة (hash functions) و التشفير غير المتناظر (asymmetric cryptography) والتوقيع الرقمي (digital signature)[1]، إنها تقنية تدعم السجل الموزع (distributed ledger) في المعاملات في الشبكة، وهي آمنة وقابلة للتوسع و الوصول من قبل كل عقدة في الشبكة. أول تطبيق لها كان عند طرح عملة البتكوين (Bitcoin) والتي هي أول تطبيق لمفهوم العملات الرقمية المشفرة (cryptocurrency) مما يشير إلى فكرة وجود شكل جديد من المال يستخدم التشفير للتحكم في إنشائه ومعاملاته، بدلاً من وجود سلطة مركزية.

اقترحت فكرة هذه العملة الرقمية من قبل شخص أو جهة غير معروفة الهوية تحت اسم "ساتوشي ناكاموتو" حيث قام في العام 2009 بنشر ورقة بحثية بعنوان

Bitcoin: A Peer-to-Peer Electronic Cash System"" [2] وصف فيها مفهوم البتكوين وكيف يعمل واستخدم مصطلح الكتلة والسلسلة لوصف عدة كتل لكنه لم يذكر أبداً مصطلح blockchain في هذه الورقة .

كلمحة تاريخية عن بداية مفهوم سلسلة الكتل كان في عام 1991 في الورقة البحثية لـ Stuart Haber و W.Scott Stornetta بعنوان " How to Time Stamp a Digital Document" اقترحا فيه فكرة الوثائق الرقمية المطبوعة زمنياً والتي تؤكد حدوث المعاملة في وقت محدد [3].

في العام التالي قام الباحثين نفسهما بتضمين فكرة Merkle Tree أو المعروفة بـ Hash Tree في كل كتلة لتخزين المعاملات المتعددة .

في 1996 نشر Ross Anderson ورقة بعنوان "The Eternity Service" وصف فيها نظام تخزين لا مركزي مع عدم إمكانية حذف أي تحديث يحصل في النظام، والذي كان يُعتبَر في ذلك الوقت ثورة في مجال تطوير نظام ند للند آمن[4].

بعد سنتين في عام 1998 كتب J.Kelsey و B.Scheier ورقة استخدما فيها التشفير بحيث وصفا طريقة يمنع فيها الحاسوب المهاجمين من تعديل أو التلاعب في أي سجلات موجودة مسبقاً كما تجعل السجلات غير مقروءة بالنسبة لأي مهاجم.

في عام 2002 كان التطور الأكبر باتجاه سلسلة الكتل حيث اقترح David Mazieres و Dennis Shasha نظام ملفات network file system مع ثقة لامركزية، كان هذا بمثابة سلسلة كتل أولية proto-blockchain حيث أن كتّاب النظام يثقون ببعضهم البعض ولا يثقون بالنظام نفسه، حيث يقومون بالتوقيع الرقمي باستخدام SHA256 أو توابع البعثرة ويلحقونها بالسلسلة الموجودة في Merkel Tree

في 2005 قام Nick Szabo بإنشاء نسخة مبسطة من سلسلة كتل وقدمها مع نموذجه الأولي للعملة المشفرة. ثم في عام 2009 صرح بشكلٍ مباشرٍ عن عملة البتكوين في ورقة ساتوشي ناكاموتو. إن التقنية التي نفذّت مبدأ عمل البتكوين هي تقنية سلسلة الكتل Blockchain. من المهم أن نميز ما بين هذين المفهومين المترابطين ، دون أن نغفل عن حقيقة أن : لا يمكن أن يوجد البتكوين دون سلسلة الكتل، ولكن يمكن أن يكون هناك سلسلة كتل دون البتكوين [5] .

قدمنا في هذا البحث دراسة نظرية كاملة عن هذه التقنية، المبادئ التي اعتمدتها التقنيات التي استخدمتها، وخصائصها، وأصنافها، والآثار الإيجابية لها، والتحديات التي واجهتها، ومقارنة هذه التقنية مع التقنيات التقليدية. اعتمدنا على بناء سلسلة كتل بسيطة والقيام بتبادل مالي من خلالها وتحليل النتائج ومناقشتها من الناحية التقنية.

II. تقنية سلسلة الكتل BLOCKCHAIN

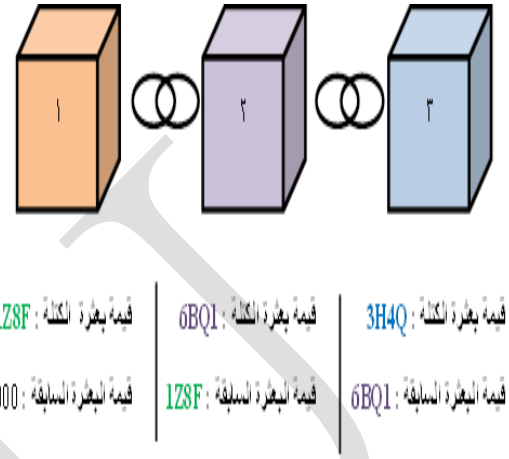
هي عبارة عن سجل لا مركزي موزَّع (Digital Decentralized ledger) لجميع المعاملات عبر شبكة أجهزة مرتبطة ببعضها بتقنية الند للند باستخدام هذه التقنية يمكن للمشاركين تأكيد المعاملات دون الحاجة إلى سلطة مركزية [6].

تتكون من مجموعة من الكتل مرتبطة مع بعضها البعض تمثل ككل قاعدة بيانات موزعة، تمتاز بقدرتها على إدارة قائمة متزايدة باستمرار من السجلات (الكتل) تحتوي كل كتلة على طابع زمني خاص بها، مع رابط يربطها بالكتلة السابقة لها في سلسلة متصلة. صممت سلسلة الكتل بحيث يمكنها المحافظة على البيانات المخزنة بها دون تعديل. أي عندما تخزن معلومة معينة في كتلة تربط بسلسلة الكتل مما يجعل من المستحيل تعديل هذه المعلومة، بحيث يمكن متابعة سجلات الكتل المتسلسلة، ومعرفة أية تغيرات طرأت عليها. تتألف كل كتلة بشكل أساسي من:

1- البيانات Data : هي البيانات التي تسجل في الكتلة وتكون حسب نوع السلسلة مثلاً سلسلة كتل البتكوين تكون بياناتها عن الحوالات المالية (المرسِل و المرسَل إليه و قيمة الحوالة).

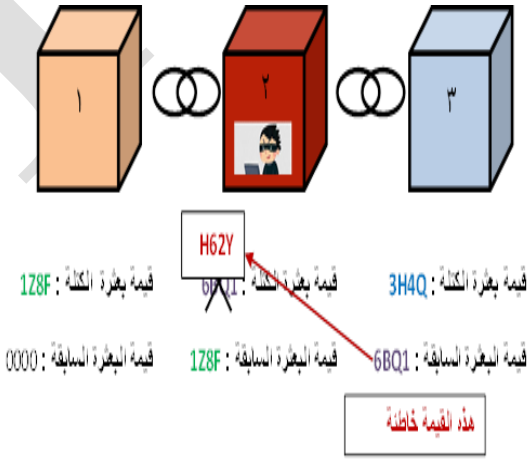
2- تابع البعثرة Hash: يحول الدخل بأي طول كان إلى خرج بطول ثابت، حيث يكون بمثابة معرِّف لكل كتلة وخاص بها مثل البصمة. عند إنشاء أية كتلة تحسب قيمة تابع البعثرة الخاص بها، بالنتيجة أي تغيير داخل الكتلة يؤدي إلى تغيير قيمة تابع البعثرة مما يجعل دوره أساسياً في كشف أية تغييرات قد تطرأ على الكتلة .

3- تابع البعثرة للكتلة السابقةHash of previous block : هو ما يؤلف السلسلة التي تربط الكتل معاً، إذ تحتوي كل كتلة ناتج بعثرة الكتلة السابقة لها كما يوضح الشكل (1).



الشكل 1. بنية تقنية سلسلة الكتل

وكما يوضح الشكل (2) إن أي تغيير في معلومات أية كتلة سيؤدي إلى تغيير قيمة البعثرة الخاصة بها مما يسبب حدوث عدم تطابق مع قيمة البعثرة الموجود في الكتلة التالية، بالنتيجة سيظهر مباشرة أن هناك تعديل قد طرأ على هذه الكتلة .



الشكل 2. تأثير حصول تغيير في أحد الكتل

A. مبدأ عمل سلسلة الكتل

يلخص مبدأ عمل هذه التقنية في الخطوات الأساسية الآتية [7] :

1. شخص ما يطلب إجراء معاملة
2. توزع المعاملة المطلوبة وتبث (broadcast) على شبكة العقد المرتبطة ببعضها
3. تتحقق شبكة العقد من صحة المعاملة المطلوبة، وحالة المستخدم باستخدام خوارزميات معروفة.
4. بمجرد التحقق من صحة المعاملة تربط بجميع المعاملات السابقة، وتنشأ كتلة جديدة من البيانات في السجل.
5. تربط الكتلة الجديدة بسلسلة الكتل الموجودة مسبقاً بطريقة دائمة وغير قابلة للتعديل، عندها تكتمل المعاملة.

B. المبادئ التي اعتمدتها سلسلة الكتل

اعتمدت سلسلة الكتل في تصميمها سبعة مبادئ أساسية هي:

1- تكاملية الشبكة Network Integrity

نُفذ هذا المبدأ من خلال: توزيع الثقة عبر الشبكة أي على كل المشاركين وليس على عضو واحد، استخدام تقنيات الإجماع والتي حلت مشكلة double spend دون الحاجة لطرف ثالث موثوق، وحققت القيم الأربعة للتكاملية (الصدق honesty المراعاة consideration المساءلة accountability الشفافية transparency)

2- السلطة الموزعة Distributed Power

يُبث كل إجراء أو معاملة إلى كامل الشبكة للتحقق أي لا حاجة لطرف ثالث مركزي، ولا يُخزن شيء على خادم مركزي، وإذا دمرت أية عقدة في الشبكة فالنظام لا يتأثر بل يكمل عمله.

3- الحوافز Value as incentive

الحافز هو عنصر مصمّم في النظام يؤثر على سلوك المشتركين، إذ استخدمت سلسلة الكتل مبدأ الحوافز لخدمة مصلحة الشبكة ككل، أي أصبح من مصلحة المستخدم أن يكون لوحده ويعمل لوحده كي يحصل على حوافزه ، أي لا تنفعه السيطرة على عقد أخرى أو انتحال أكثر من هوية .

4- الأمن Security

حُقق الأمن من خلال أن الشبكة موزعة، أي لا توجد نقطة فشل واحدة، و بذلك فإن نتائج السلوك السيء لأحدهم تكون على الشخص نفسه وليس على الشبكة. لكن الإجراءات التقنية لتحقيق الأمن كانت من خلال: استخدام التشفير غير المتناظر واستخدام تابع SHA256 للبعثرة واستخدام التواقيع الرقمية

5- السرية أو الخصوصية Privacy

حققت سلسلة الكتل هذا المبدأ من خلال حماية البيانات الشخصية من التداول حيث لا يضطر أي مستخدم أو مشترك من وضع بياناته (اسمه، عنوانه، بريده الإلكتروني.....) إنما يتم التعريف عنه بثنائية مفاتيح (عام-خاص).

6- الحفاظ على الحقوق Rights Preserved

تحقق ذلك من خلال العقود الذكية Smart contracts يوضع فيها كل الشروط اللازمة والتي تحافظ على حقوق كل الأطراف .

7- الشمولية Inclusion

يتضمن هذا المبدأ مشاركة الناس من جميع الخلفيات الاجتماعية والاقتصادية والعرقية، ووضع حد للتمييز القائم على الصحة أو نوع الجنس أو الهوية أو... وبالنتيجة إسقاط الحواجز أمام الوصول بسبب المكان الذي يعيش فيه شخص ما مما يوصلنا إلى التغيير للأفضل .

يُعنَى هذا المبدأ بكيفية إيصال النظام المالي غير المصرفي للجميع حيث يعمل الاقتصاد العالمي بشكل أفضل عندما يعمل لصالح الجميع، يمكن ملاحظة أن هذا المبدأ مبدأ اجتماعي اقتصادي أكثر مما هو تقني.

C. خصائص سلسلة الكتل

تتمتع سلسلة الكتل بعدة مزايا ، [8] ، أهمها:

1- اللامركزية (Decentralization) : لا تعتمد تقنية Blockchain على أنظمة معاملات مركزية للتحقق من صحة المعاملات. نظراً لأن الطرف الثالث غير مطلوب لشبكات سلسة الكتل ، لذلك تعتمد سلسلة الكتل على التشفير والخوارزميات للحفاظ على البيانات في الشبكات الموزعة.

2- الشفافية (Transparent) :

نظرًا للطبيعة اللامركزية في سلسلة الكتل ، يمكن عرض جميع المعاملات بشفافية إما من خلال امتلاك عقدة شخصية أو باستخدام مستكشفات سلسلة الكتل التي تسمح لأي شخص برؤية المعاملات التي تحدث مباشرة. لكل عقدة لها نسختها الخاصة من السلسلة التي تحدث عند تأكيد الكتل الجديدة وإضافتها. هذا يعني أنه إذا كنت ترغب في ذلك ، يمكنك تتبع المعاملة أينما ذهبت.

3- الثبات (Immutable) :

إن البيانات المخزنة في سلسلة الكتل غير قابلة للتغيير. تضاف البيانات إلى الكتلة بعد الموافقة عليها من قبل الجميع في الشبكة، وبالنتيجة السماح بالمعاملات الآمنة. المستخدمين الذين يتحققون من صحة المعاملات ويضيفونها في كتلة يطلق عليهم المنقبين(miner) .

4- زيادة السعة (increased capacity) :

من الأشياء المهمة في هذه التقنية أنها يمكن أن تزيد من قدرة الشبكة بأكملها. إذ أنه يمكن أن يكون لوجود الآلاف من أجهزة الكمبيوتر التي تعمل معاً ككل طاقة أكبر من عدد قليل من المخدمات المركزية.

5- المجهولية (anonymity) :

يوفر إخفاء الهوية وسيلة فعالة لإخفاء هوية المستخدمين والحفاظ على خصوصية هوياتهم.

D. أصناف سلسلة الكتل

تقسم هذه التقنية إلى ثلاثة أنواع أساسية [9,10]:

1- سلسلة الكتل العامة public blockchain

تكون السلسلة لا مركزية بالكامل ومفتوحة المصدر بحيث يمكن لأية عقدة الانضمام إليها، تتمتع كل عقدة مشاركة بالسلطة الكاملة لأداء عملية قراءة أو كتابة في السلسة في أي وقت. إنه غير قابل للتغيير هذا يعني أنه عندما ينشأ مدخل في سلسلة كتل لا يمكن أن يعدل أو يحذف عندما يصبح فعالاً.

من تطبيقات سلسلة الكتل العامة مجال الصحة و التعليم مثلاً : تستخدم معاهد العناية الصحية هذه التقنية للحصول على سجل تاريخي لكل العمليات الجراحية . تضاف البيانات من قبل الأطباء و المختصين الآخرين بخصوص تفاصيل المرضى، و تكلفة العلاج والتكاليف الأخرى التي تتضمن العمل في معهد، يمكن أن تشاهد المعلومات من قبل أي شخص في سلسلة الكتل لتحقيق الشفافية ، ولكن لا يمكن التعديل على هذه البيانات بمجرد إضافتها، إضافة إلى أنه سلاسل كتل العملات الرقمية Bitcoin)و (Ethereum هي من النوع العام.

2- سلسلة الكتل الخاصةprivate blockchain

هي سلسلة كتل قائمة على الدعوة فقط (invitation only)، يتحكم بها من قبل فرد محدد أو منظمة محددة، أي لا يمكن لأي مستخدم جديد / غير معروف الوصول إلى السلسة حتى يتلقى المستخدم الجديد دعوة خاصة من السلطة التي تتحكم فيه. عمليات الكتابة مقيدة، ولا يُسمح إلا للعقد المتحكمة بكتابة شيء ما أو التعامل معه في الشبكة، مما يجعل هذا النوع يميل نحو بنية مركزية. ومع ذلك، فإن الخصائص الأخرى له مثل الإجماع والسجل الموزع واتصالات الند للند والعقود الذكية تجعل هذا النوع مناسباً للمؤسسات المالية والبنوك، حيث أنها تضمن مستوى عالٍ من الأمن و السرية والأداء. نتيجة لطبيعة سلسلة الكتل الخاصة الموثوقة يمكن أن يصمم من أجل القطاعات المالية والخدمات الحكومية. لا تكون المعاملات و البيانات مرئية للعامة، فقط يمكن الوصول إليها من قبل العقد المشاركة .

يمكن اعتماد سلسلة الكتل في القطاع التعاوني عندما تكون التفاصيل بحاجة لأن تشارك بين عدد محدد من العقد فقط. مثلاً: يمكن لاتحاد البنوك اعتماد سلسلة كتل خاصة حيث تشارك تفاصيل المعاملات المالية من قبل الأطراف المعنية فقط.

3- سلسلة الكتل المركبة consortium blockchain أوHybrid Blockchain

يُعتبَر هذا النوع بشكل عام دمجاً بين النوعين العام والخاص حيث يمكن أن تكون البيانات مفتوحة أو خاصة وتحوي مزايا المركزية واللامركزية، تكون مجموعة من المنظمات أو الأفراد مسؤولين عن اتخاذ القرارات المتعلقة بالتحقق من صحة الكتلة والإجماع. تقرر هذه المجموعة العقد المشاركة في الشبكة، حيث تعد الكتلة الملغومة كتلة صالحة فقط إذا وافقت العقد المتحكمة عليها وسجلتها. يمكن لعقد التحكم هذه أيضاً أن تقرر أذونات القراءة أو الكتابة، يمكنهم الموافقة أو منع شخص ما من القراءة أو الكتابة. ومع ذلك، فإن أحد العيوب الرئيسية لهذا النوع هو إمكانية العبث به نظراً لأنه يتحكم به بواسطة مجموعة من العقد فيمكنهم التعاون مع بعضهم البعض وقد يعكسون المعاملة أو يعبثون بها .

بالخلاصة نجد أن كل أصناف سلاسل الكتل لها مزايا متعددة، اختيار النوع يعتمد على حاجاتنا والخدمات المقترحة لتلبيتها [11].

E. الحاجة إلى سلسلة الكتل

تعود الحاجة إلى تطبيق سلسلة الكتل انطلاقاً من

عدة أسباب نذكر منها [5]:

1- تأكد الشفافية: إذ أنها تقنية مفتوحة المصدر، لكن في الوقت ذاته لا يمكن للمستخدمين التعديل.
2- تقلل تكاليف المعاملات بشكل ملحوظ : فهي لا تحتاج إلى وسطاء أو طرف ثالث لإتمام المعاملات فهي معاملات ند –للند.
3- تقدم تسويات سريعة للمعاملات مقارنة بالشبكات التقليدية لأن الشبكات التقليدية ترتبط بإجراءات وساعات لا توجد ضمن سلسلة الكتل.
4- تعزز اللامركزية : إذ لا يوجد نقطة مركزية للتحكم مما يسمح بمصادقة المعاملات بشكل فردي.
5- في حال اكتشاف أية مخالفة يمكن للمرء دائماً تتبع نقطة الأصل، مما يجعل التحقيقات سهلة لتنفيذ الإجراءات المطلوبة. هذا يضفي صفة الجودة على العمل.
6- تضمن تقنية سلسلة الكتل عدم حدوث أي خطأ بشري وذلك لأنها تعتمد على تسجيل البيانات وحمايتها من التغيير، من خلال التحقق من السجلات في كل مرة تنتقل فيها من عقدة إلى أخرى. أي أن الدقة محققة .

F. مجالات استخدام سلسلة الكتل:

نظراً للميزات الكثيرة والخواص الاستثنائية التي أبدتها تقنية سلسلة الكتل، توَّجه الاهتمام في السنوات الأخيرة إلى تطبيقها خارج مجال التمويل والبنوك والحوالات، تم العمل على ربطها مع تقنيات الذكاء الاصطناعي وتعلم الآلة وأنظمة إنترنت الأشياء التي كانت أول المستفيدين من خواصها المتمثلة في اللامركزية، والشفافية، والأمان، والمرونة وعدم التعديل، معالجةً بذلك التحدي الأهم الذي يواجه الأنظمة الحديثة حالياً وهو الأمن والثقة [12,13,14].

من أهم المجالات أيضاً لتطبيق سلسلة الكتل في أنظمة إنترنت الأشياء هي شبكات العربات، التطبيقات الزراعية، والمدن والمنازل الذكية، وتطبيقات الرعاية الصحية.

G. مقارنة بين سلاسل الكتل و قواعد البيانات التقليدية:

يوضح الجدول 1 مواصفات كل من سلسلة الكتل وقواعد البيانات التقليدية من حيث عدد من الخصائص

الجدول 1 مقارنة بين سلاسل الكتل وقواعد البيانات التقليدية

الخاصية	سلسلة الكتل	قاعدة البيانات التقليدية
السلطة Authority	لامركزية (لا أحد يملك سلطة)	مركزية (طرف محدد متحكم)
البنية Architecture	تعمل على بنية السجل الموزع	تعمل على بنية زبون-مخدم
التكاملية Integrity	لا يمكن أبدا تعديل البيانات فيها	يمكن تغيير وتعديل البيانات بسهولة
الشفافية Transparency	جميع البيانات أو الأنشطة مفتوحة للجميع ليراها	جميع البيانات أو المعاملات مخفية عن بعضهم البعض
معالجة البيانات Data Handling	تدعم عمليات القراءة والكتابة (إضافة وليس تعديل كُتب سابقاً)	تدعم عمليات الإنشاء، والقراءة، والتحديث والحذف
التكلفة Cost	أقل تكلفة	مكلفة
السرعة Speed	أبطئ بسبب تضمين تقنيات الإجماع والتحقق	أسرع
الثقة Trust	مناسبة للتطبيقات التي فيها المستخدمين لا يثقون ببعضهم البعض	مناسبة للتطبيقات التي فيها يوجد ثقة مشتركة

H. أنواع تقنيات الإجماع

واحدة من أهم التقنيات الجديدة المميزة التي استخدمت مع سلسلة الكتل هي تقنيات الإجماع Consensus Mechanism يوجد العديد من أنواع تقنيات الإجماع المستخدمة لكن أهمها وأولها استخداماً كان تقنية إثبات العمل Proof Of Work (POW)وتقنية إثبات الحصة Proof Of Stack (POS) [15].

1- إثبات العمل Proof Of Work (POW)

هي المصطلح التقني للتعدين mining طرح مع البتكوين في ورقة ساتوشي ناكاموتو، وتُستخدم في شبكات البتكوين والإيثيريوم، تعتمد على حل معادلات رياضية لا يمكن إلا لأجهزة الكمبيوتر حلها، بحيث أن أول منقب قادر على حلها يفوز بإنشاء الكتلة الجديدة ويحصل على الحافز.

تعاني هذه التقنية من مشكلتين كبيرتين، الأولى أنها تستخدم الكثير من الطاقة (محدودية الموارد) والثانية أنها تعالج عدد محدود من المعاملات في وقت واحد (7 معاملات في شبكات البتكوين و30 في شبكات الإيثيريوم) وعادة تستغرق المعاملات عشر دقائق على الأقل حتى تكتمل.

2- إثبات الحصة Proof Of Stack (POS)

طرحت هذه التقنية مع عملة الإيثيريوم في عام 2015 لكن لم تُطبق فعلياً حتى الآن، حسب المسؤولين ستنتقل الإيثيريوم للعمل بها في 2022.

إذ يتم التحقق من صحة المعاملات بواسطة مدقق مُختار بناء على عدد العملات التي يمتلكها والمعروفة باسم "الحصة"، كلما زادت حصة الشخص زادت قوة التعدين لديه وزادت فرص اختياره كمدقق للكتلة التالية، لضمان عدم تحديد الأشخاص الذين لديهم أكبر عدد من العملات دائماً تستخدم طرائق أخرى كاختيار الكتلة العشوائية (الذين لديهم أعلى حصة وأقل قيمة تجزئة) واختيار عمر العملة (بناء على المدة التي حُفظت فيها بالعملات)، والنتيجة هي أوقات معاملات أسرع وتكاليف أقل.

I.العقود الذكية Smart Contracts

العقد الذكي هو اتفاق (مجموعة قواعد) ينشأ بين طرفين، عبارة عن عدة أسطر برمجية تُنفذ عند الاتفاق (عند حدوث حدث أو شرط معين)، يبقى فيه كلا الطرفين مجهول، ويُخزن على سجل عام public ledger،طبق لأول مرة في الإيثيريوم.

ويمكن للعقود الذكية أن تحدد القواعد ، مثل العقد العادي ، وأن تنفذها تلقائياً عن طريق الكود. لا يمكن حذف العقود الذكية، والتفاعلات معها لا رجعة فيها.

إن العقد ذكي ، مثل آلة البيع ، لديه منطق مبرمج فيه. فكما أنن آلة البيع تلغي الحاجة إلى موظف بائع، كذلك العقود الذكية يمكنها أن تحل محل الوسطاء في العديد من الصناعات.

J. تحديات تقنية سلسلة الكتل

تواجه أية تقنيّة حديثة العهد بعض المشاكل في بدايتها وهو أمر طبيعي، ولكن بالنسبة لسلسلة الكتل فقد كان الأمر مختلفاً بعض الشيء، حيث أنّ التقنيّة بحد ذاتها ليست المشكلة الوحيدة وإنّما طبيعتها اللامركزيّة والمفتوحة المصدر التي تتطلّب الكثير من الجهود الجماعيّة لتحقيق أفضل استفادة منها. تواجه هذه التقنية بعض التحدّيات التي تقف في طريقها للانتشار بشكل واسع وإحداث تغييرات فعليّة، أبرز هذه التحديات [16,17]:

- تكلفة التأسيس: تَعد تقنية سلسلة الكتل بفوائد على المدى الطويل بسبب خواصها الاستثنائية، لكن البرمجيات (software) المطلوبة لتثبيت هذه التقنية والتعامل معها طُورت من قبل مؤسسات محددة غالية الثمن، بالإضافة إلى أننا أحياناً نحتاج لمعدات (hardware) خاصة وجديدة لكي

تكون قادرة على التعامل مع هذه البرمجيات، وبسبب الطلب الكبير وقلة المطورين الموجودين حتى الآن تضطر المنظمات أن تدفع أكثر للمطورين المتاحين حالياً.

- احتكار التنقيب: يحاول المنقبون أن يزيدوا حوافزهم بإبقاء الكتل خاصة (private blocks)
- هجوم الـ 51%: عندما يملك أحد المنقبين 51% من قوة البعثرة يمكن له أن ينفذ هجوم 51% في الشبكة، يسمح هذا الهجوم للمهاجم بالسيطرة على معظم الشبكة.
- هجوم Double spending :

يؤدي مستخدم واحد عدة معاملات بنفس العملة المشفرة، حيث تبث المعاملة لكل عقدة في الشبكة وتحتاج لتأكيدها من قبل هذه العقد، يستهلك هذا التأكيد الوقت بالتالي الوقت بين تأسيس المعاملات والتأكيد يمكن أن يكون نافذة للمهاجم لتنفيذ هجومه.

III. مفهوم البتكوين Bitcoin

تعد البتكوين أول عملة رقمية مشفرة لامركزية تم طرحها، حيث أنها نظام دفع الكتروني يعتمد شبكات الند للند، ورغم أن هذه العملة غير موجودة فيزيائياً على أرض الواقع، لكن لها وجود اقتصادي وتجاري، و تزداد أهميتها يوماً بعد يوم. يمكن استخدام هذه العملة في عمليات الدفع والشراء الالكتروني، ويمكن تبادلها وتداولها مثل أية عملة أخرى عبر شبكات الند للند دون أية سلطة مركزية تتحكم في هذه التحويلات المالية .

تعتمد فكرة البتكوين بشكل أساسي على خلق نظام مالي الكتروني لا مركزي متكامل، لا يرتبط بسلطة مركزية من أجل سرية و تفعيل المعاملات. إنه نظام ند للند موزع بشكل كامل، هكذا لا يوجد نقطة تحكم واحدة للنظام، بل على العكس أنشئت البتكوين من خلال إجرائية تسمى التنقيب(mining) ، وتعني أن أي مشارك في شبكة البتكوين يمكن أن يعمل كمنقب (miner) مستخدماً قدراته الحسابية.

يعمل تنقيب البتكوين على إضفاء الصفة اللامركزية وتسوية الإجراءات المختلفة. هناك نوعين من العقد[5]:

1- العقد المنقبة (mining nodes) هم المستخدمون الذين يشاركون في إنشاء الكتل و يُحفَزون بمقدار من البتكوين لضمان بقاءهم في الشبكة، حيث أنه أول منقب يكمل كتلة جديدة يتلقى قيمة بتكوين محددة (مثلا BTC 50) هذه القيمة تُخفَّض إلى النصف كل فترة معينة كي لا تستحوذ عقدة معينة على الشبكة وعندها يمكن أن نعاني من هجوم 51 %. إن التنقيب في شبكات البتكوين يعتمد على تقنية POW . (Proof Of Work)

2- العقد غير المنقبة (non-miner nodes) هم الذين يستفيدون من نظام البتكوين دون المشاركة في إنشاء الكتل.

تعتمد المعاملة بشكل أساسي على زوج المفاتيح (العام / الخاص) وعلى توابع البعثرة . إذ توقع المعاملات وتوزع في الشبكة، ثم تجمع المعاملات في كتل، وتشارك وتفعل من قبل عقد الشبكة. حيث يحدد الإجماع في الشبكة الكتل المقبولة وتقنية الإجماع المستخدمة في شبكات البتكوين هي POW (Proof Of Work).

يمتلك كل مستخدم في شبكة البتكوين محفظة افتراضية تتكون على الأقل من مفتاح خاص ومفتاح عام ، بحيث يكون لكل معاملة مفتاح جديد وعنوان جديد، و ذلك لتجنب هجوم التحليل الذي يعتمد على مقارنة التواقيع الرقمية و حركة تدفق المعاملات . تتكون كل محفظة من قائمة من المداخل و المخارج بحيث لا يمكن استخدام خرج المعاملة إلا مرة واحدة فقط كدخل في سلسلة الكتل.

A. الاختلاف بين البتكوين والعملة التقليدية

تختلف البتكوين باعتبارها عملة مشفرة عن العملة التقليدية بعدة نقاط يمكن أن نلخص الفرق [18] في الجدول الآتي:

الجدول 2 مقارنة بين العملة التقليدية و المشفرة

العملة التقليدية	العملة المشفرة البتكوين
وسط التبادل هو وسط فيزيائي	وسط التبادل هو وسط رقمي
تمثل العملة إما بقطع معدنية أو ورقية	تمثل بترميز أحدهما عام و الآخر خاص
صادرة عن الحكومة	منتجة من قبل الحواسيب
مركزية ، تخضع لسلطة القانون والبنوك	لا مركزية، لا يتحكم بها أحد
قيمتها تتحدد تبعاً للأنظمة والسوق	قيمتها تحدد تبعاً للعرض و الطلب

IV. القسم العملي

نستعرض في هذا القسم الشبكة التي تم العمل عليها، حيث بنينا شبكة بسيطة وطبقنا تقنية سلسلة الكتل فيها لمحاكاة العملية الواقعية للمعاملات المالية باستخدام هذه التقنية. وذلك باستخدام لغة البرمجة بايثون والأداة pycharm [19] إضافة إلى استخدام لغات HTML لتخطيط البنية العامة والواجهات وهيكلتها و **CSS** لإضافة التأثيرات الجمالية كالألوان والأشكال للبنية المصممة باستخدام لغة HTMLو Javascript للتفاعل مع البنية حيث الأكواد المكتوبة بـ JS تم تنفيذها في طرف العملاء

تتألف هذه الشبكة من عقد منقبة miners وعقد غير منقبة non miners أو ما يسمى بالعملاء clients كما هو موضح في الجدول التالي

الجدول(3): مكونات الشبكة

clients	miners
Alice	Node1
Bob	Node2
	Node3

يمكن لأي عميل الاتصال بأي عقدة من العقد المنقبة لتنفيذ المعاملة، حيث كل عقدة منقبة لها local copy من السلسلة كاملة.

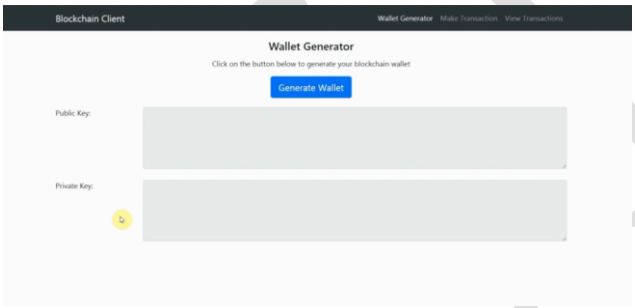
تم استخدام خوارزمية RSA لتوليد زوج من المفاتيح (عام، خاص) لكل عميل، يُستخدَم المفتاح العام للمرسل للإرسال والمفتاح العام للمستقبل للاستقبال، ويستخدم المفتاح الخاص للمرسل من أجل توليد توقيع signature يستخدم للتأكد من المرسل، كما اعتمدت خوارزمية SHA265 من أجل القيام بتطبيق Hash على محتوى المعاملة قبل توقيعها، وتحتوي كل كتلة بشكل أساسي المعلومات الموضحة في الشكل التالي، والتي هي ما يميز كل بلوك عن الآخر ويربط البلوكات مع بعضها البعض

Number of blocks
Nonce
Data
Hash
Previous Hash

الشكل 3. بنية البلوك المستخدمة

A. آلية العمل والنتائج

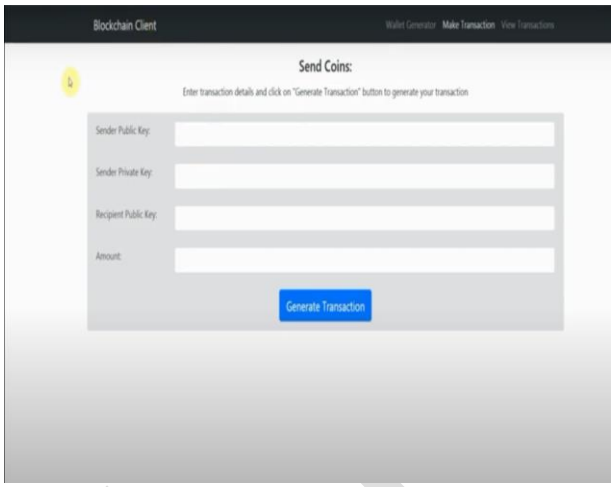
1. تولید محفظة زوج مفاتيح (عام–خاص) لكل عميل باستخدام خوارزمية RSA



الشكل 4. واجهة العميل

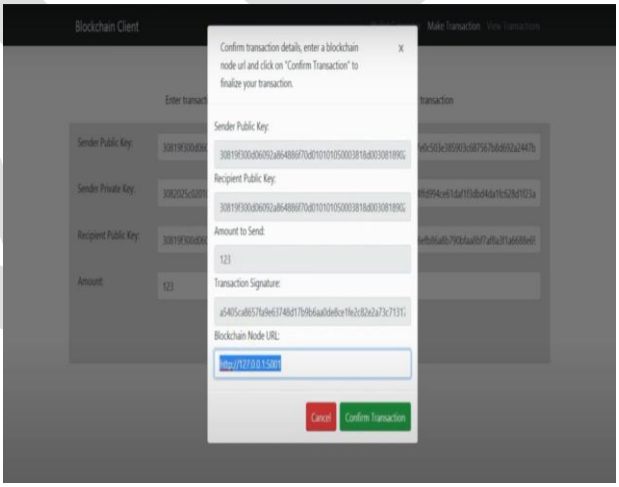
2. إرسال المعاملة:

لتكن أليس تريد إرسال مبلغ لبوب، نحدد في هذه الواجهة المفتاح العام لأليس للإرسال والمفتاح العام لبوب للاستقبال والمفتاح الخاص لأليس كي يُتستخدمه لتوليد توقيع للمعاملة و تحدد أيضاً المبلغ الذي تريد إرساله.



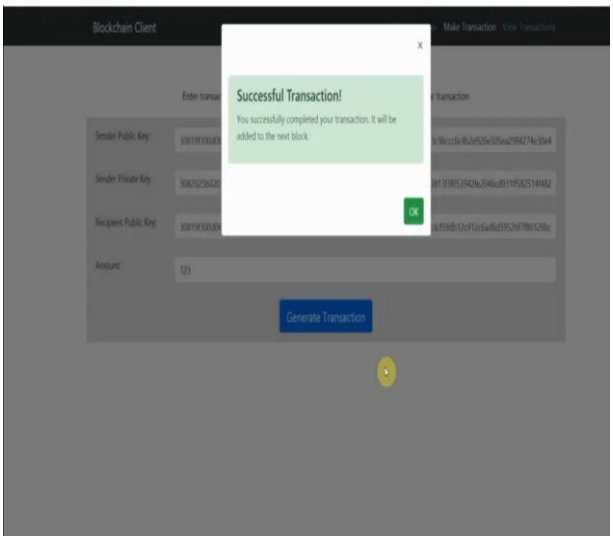
الشكل 5. مدخلات إرسال معاملة

3. تأكيد المعلومات المدخلة وتوليد التوقيع إضافة إلى تحديد العقدة المنقبة التي نريد التعامل معها ولتكن Node1، مع الإشارة إلى أن المعلومات في هذه الواجهة للعرض فقط لا يمكن تغييرها



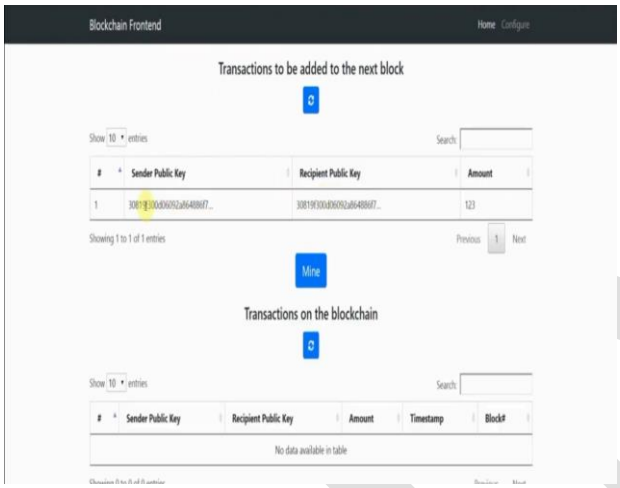
الشكل 6. تأكيد المعلومات المدخلة

4. تأكيد نجاح عملية الإرسال



الشكل 7. نجاح إرسال المعاملة

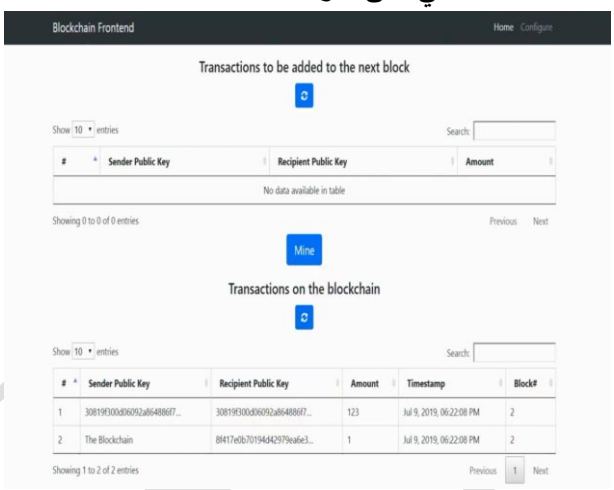
5. الآن Node1 تحوي معاملة واحدة لكن لم يتم بعد إنشاء بلوك لهذه المعاملة



الشكل 8. واجهة العقدة المنقبة

6. في هذه الخطوة تبدأ عملية الـ mining حيث تسعى العقدة لإضافة بلوك جديدة لهذه المعاملة وذلك بإيجاد قيمة nonce تحقق معيار معين متفق عليه من قبل الشبكة، عندما تجد العقدة هذه القيمة تنشىء بلوكاً جديداً يحوي المعاملة التي أرسلت ومعاملة أخرى عبارة عن reward من السلسلة نفسها تعطيها للعقدة التي قامت بإنشاء بلوك جديدة، هذه الـreward هي مبلغ يتم الاتفاق عليه في الشبكة غير ثابت إنما متغير تبعاً

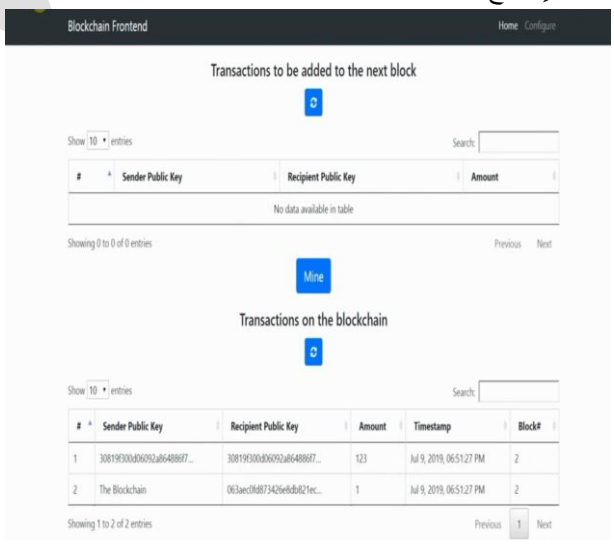
للعمل يحقق مبدأ التنافسية بين العقد، وبالتالي العمل أكثر لبناء بلوكات جديدة وبالتالي كسب rewards أكثر. مجمل هذه العملية هو مبدأ الـ POW والتي تعتمد بشكل أساسي على القوة الحسابية للعقد.



الشكل 9. واجهة العقدة المنقبة بعد التنقيب

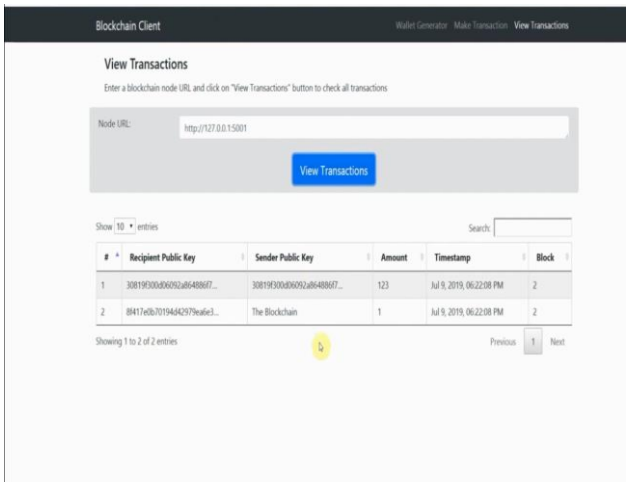
كما نلاحظ أن البلوك الذي بني رقمه 2 وذلك بسبب وجود البلوك الأول دائماً وهو الـgenesis block يكون الـ previous hash له أصفار .

7. تحدث كل عقدة أخرى منقبة في الشبكة نسختها من البلوك تشين اعتماداً على مبدأ "السلسلة الأطول تربح" وباستخدام تقنية الإجماع المستخدمة



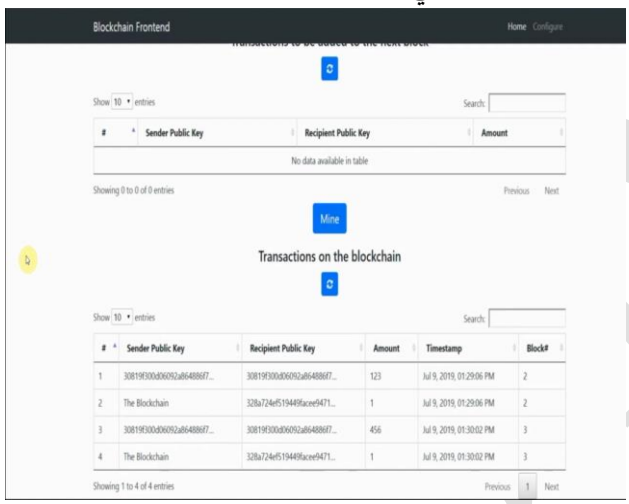
الشكل 10. Node2 بعد تحديث نسختها

8. كل عقدة تكون على علم بكل العقد الأخرى معها في الشبكة من خلال بروتوكول خاص، إضافة إلى أن كل عميل يكون قادر على رؤية جميع المعاملات في كل عقدة وهو ما يحقق مبدأ الشفافية



الشكل 11. واجهة العميل لرؤية معاملات كل عقدة

9. عند قيام عقدة أخرى بإنشاء بلوك جديد يضاف إلى السلسلة بالشكل التالي



الشكل12. السلسلة بعد كل إضافة لبلوك جديد

B. مناقشة النتائج والاستنتاجات

اعتماداً على النموذج السابق نلاحظ أنَّ:

- إمكانية القيام بالعمل من قبل أي عقدة منقبة في الشبكة دون العودة لجهة مركزية محددة مما أتاح الاتصال اللامركزي بين عقد الشبكة ككل.

- بعد إدخال العميل لبياناته لا يمكن تغييرها ولا بأي شكل كان ولا من قبل أي طرف في الشبكة.
- استخدام المفاتيح العامة كمرسل ومستقبل حافظ على سرية هوية العميل.
- استخدام الـ rewards من قبل السلسلة يزيد التنافسية بين المنقبين وبالتالي زيادة العمل وتسريعه، فنحصل على عمل منته بغضون بضع دقائق
- رؤية كل العقد لبعضها وإمكانية معرفة كل المعاملات في الشبكة (دون معرفة خصوصياتها) يحقق مبدأ الشفافية.
- إرسال التوقيع الرقمي للمرسل مع المعاملة يسمح بالتأكد من هوية المرسل في طرف المنقب واكتشاف أي خلل إضافة إلى أنه يمنع تنصل المرسل من أي مسؤولية فيما بعد.
- وجود الـ previous hash في كل كتلة يربط الكتل مع بعضها ويكشف وجود أي عمل غير شرعي مما يزيد السوية الأمنية للشبكة بشكل كبير.

المراجع:

[1]. I. Priyadarshini, "Introduction to Blockchain Technology", in book: Cybersecurity in Parallel and Distributed Computing, Publisher: John Wiley and Sons, March 2019

[2]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", October 31, 2008

[3]. S. Haber and W. Scott Stornetta, "How to time-stamp a digital document", Journal of Cryptology, pages 99-111, 1991

[4]. R. Anderson, "The Eternity Service", Cambridge University Computer Laboratory, 1997

[5]. H. Hellani, A .Samhat, C . Maroun and H. EL Ghor, "On Blockchain Technology: Overview of Bitcoin and Future Insights", IEEE International Multidisciplinary Conference on Engineering Technology, Beirut, Lebanon, November 2018.

[6]. S. Sayadi, S.Ben Rejeb and Z. Choukair, "Blockchain Challenges and Security Schemes: A Survey", Seventh International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, IEEE, 1-3 Nov. 2018

[7]. J.Locki, V.Schlatt, A.Schweizer, N.Urbach and N.Harth, "Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications", IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, 2020.

[8]. H.Atlam, A.Alenezi, M.Alassafi ana G.Wills, "Blockchain with Internet of Things: benefits, challenges, and future directions", International Journal of Intelligent Systems and Applications, 10 (6), 40-48, 2018

[9]. M.Hassan, M.Rehmani and J.Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", Science Direct Journal, Future Generation Computer Systems, 2019, 512-529.

[10]. D.Jeyabharathi, D.Kesavaraja and D.Sasireka, "Cloud-Based Blockchaining For Enhanced Security", Research on Blockchain Technology, Ch.7, Pages 171-181, 2020.

[11]. S.Sayadi, S.Ben Rejeb and Z.Choukair, "Blockchain Challenges and Security Schemes: A Survey", IEEE, 2018

[12]. I. Joseph and S. D. Sawarkar, "Study on Integration of Blockchain and IoT in Smart City Applications", International Journal of Innovative Science and Research Technology, vol.5, No.2456-2165, 2020.

[13]. T. A. Telia, F. Masoodib and R. Yousufc, ""Security Concerns and Privacy Preservation in Blockchain based IoT Systems: Opportunities and Challenges". International Conference on IoT based Control Networks and Intelligent Systems (ICICNIS), 2020.

[14]. A. Dorri, S. S. Kanhere, R. Jurdaky and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home". IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things, 2017.

[15]. D.Sukheja, L.Indira, P.Sharma and S.Chirgaiya, "Blockchain Technology: A Comprehensive Survey", Jour of Adv Research in Dynamical & Control Systems, Vol. 11, 09-Special Issue, 2019

[16]. L. Madaan, A.Kumar and B.Bhushan, "Working principle, Application areas and Challenges for Blockchain Technology", 9th IEEE International Conference on Communication Systems and Network Technologies, 2020.

[17]. S.Jojar, N. Ahmad, W.asher, H. Cruickshank and A.Durrani, "Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey", Applied Sciences, 2021.

[18]. /https://www.e-zigurat.com/innovation-school/blog/crypto-vs-banking-system, last visit 6-11-2021

[19]. /https://www.jetbrains.com/pycharm/ last visit 6-11-2021

منشورات المؤلف (د. بشرى معلا):

[1]. Maala, B., and Zarka, F. (2021). Blockchain Technology to a new View. *Al-Manara University Journal*, Vol.1, No.4.

[2]. Alkubeily, M., and Maala, B. (2021). An overview of the Internet of Things-IoT. *Al-Manara University Journal*, Vol.1, No.1.

[3]. Maala, B., alradwan, H., and Mahfoud, A. (2020) . Barycentric Jamming localization (BJL). *Tartous University*, Vol.4, No.8.

[4]. Maala, B., alradwan, H., and Mahfoud, A. (2020). Adaptive Detect and Protect Against Jamming Attacks on Ad Hoc Networks using Game Theory and Channel Switching (GTCS). *International Journal of Computer Science and Technology IJCST*, Vol.8, Issue.3, PP: 49-56.

[5]. Maala, B., and Abd Alhameed, M. (2020). Studying the ARP spoofing attack effect on SDN networks. *Tishreen University Journal of Science and Engineering*, Vol.42, No.2, PP: 183-199 .

[6]. Maala, B., alradwan, H., and Mahfoud, A. (2019). Analyzing Study of the Effect of Jamming Attack on Ad Hoc Network Performance. *Tishreen University Journal of Science and Engineering*, Vol.41, No.5, PP: 81-98.

[7]. Maala, B., and Mohammed, H. (2018). Enhanced Secure Data Aggregation in Mobile Wireless Sensor Networks. *Tishreen University Journal of Science and Engineering*, Vol.40, No.4, PP: 499-515.

[8]. Sweekat, Kh., Zarka, F., Maala, B., Ahmad, S.A. (2018). A New Secure Wireless Body Sensor Network Architecture. *International Journal of Engineering Trends and Application (IJETA)*, Volume 5 Issue 1, PP: 41-45.

[9]. Raya, Gh., Alkubeily, M., Ali, S., and Maala, B. (2018). A New Multi-Objective QoS Multicast Routing Protocol Based on Ant Colony Optimization for Mobile Ad Hoc Networks. *International Journal of Computer Science Trends and Technology (IJCST)*, Vol.6, No.1, PP: 17-23.

[10]. Abo Ajeeb, A., Mahmod, A., Maala, B., Ahmad, S.A. (2017). Enhanced DNA Cryptography for Wireless Body Sensor Networks. *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)*, Vol.5, Issue.12, PP: 16953-16958.

[11]. Maala, B., and Iskander, Kh. (2017). Performance Evaluation of MQQ- SIG Algorithm in Wireless Multimedia Sensor Networks. *Tishreen University Journal of Science and Engineering*, Vol.39, No.6.

[12]. Sliman, A., Madi, K., Khadour, A., Maala, B., Ahmad, S.A. (2017). Fabrication Attack Effect on Medical Applications based on VANETs. *International Journal of Computer Science Trends and Technology (IJCST)*, Volume 5 Issue 2.

[13]. Maala, B., and Mahfoud, A. (2017). Dynamic Black List (DBL) algorithm to defense against DDoS attack in Vehicular Ad-hoc Network. *Tishreen University Journal of Science and Engineering*, Vol.39, No.3.

[14]. Alkubeily, M., Ali, S., Maala, B., and Raya, G. (2017). A New Stable and Reliable On-Demand QoS Routing Protocol Based on Ant Colony Optimization for Mobile Ad-hoc Networks. *Tishreen University Journal of Science and Engineering*, Vol.39, No.3.

[15]. Maala, B., Alkubeily, M. (2016). A New Fault Tolerance Protocol in Application-Level Multicast Networks. *Tishreen University Journal of Science and Engineering*, Vol.38, No.6.

[16]. Hasan, B., and Maala, B. (2016). Performance Evaluation for GPSR and AODV Routing Protocols at the Junctions in VANET. *Tishreen University Journal of Science and Engineering*, Vol.38, No.4.

[17]. Maala, B. (2016). Performance Study of APS Algorithm for position Determination in Underwater Wireless Sensor Networks. *Tishreen University Journal of Science and Engineering*, Vol.38, No.3.

[18]. Maala, B. (2015). Study of DDOS Attack Impact on Vehicular Ad Hoc Network in City. *Tishreen University Journal of Science and Engineering*, Vol.37, No.3.

[19]. Maala, B., Alkubeily, M. (2015). Fault Tolerance in Application-Level Multicast Networks. *Tishreen University Journal of Science and Engineering*, Vol.37, No.1.

[20]. Maala, B., Alkubeily, M., Raya, G. (2014). Improving Packet Delivery Ratio for On-Demand Multicast Routing Protocol (ODMRP). *Tishreen University Journal of Science and Engineering*, Vol.36, No.1, pp: 169-184.

[21]. Maala, B., Bettahar, H., Bouabdallah, A. Performances of Key Management schemes in Wireless Sensor Networks. Handbook on Sensor Networks, chapter 11. World Scientific Publishing Co.

[22]. Maala, B., Challal, Y., Bettahar, H., Bouabdallah, A. (2009). *Node Capture Attack Impact on Key Management Schemes For Heterogeneous Wireless Sensor Networks.* IEEE Global Information Infrastructure Symposium (GIIS2009).

[23]. Maala, B., Bettahar, H., Bouabdallah, A. (2008). TLA: A Tow Level Architecture for Key Management in Wireless Sensor Networks. In Proceeding of IEEE SensorComm. pages:639-644.

[24]. Maala, B., Challal, Y., Bouabdallah, A. (2008). HERO: Hierarchical Key Management Protocol for Heterogeneous Wireless Sensor Networks. In Proceeding of IFIP Conference on Wireless Sensors and Actor Networks (IFIP-WSAN'08), pages:125-136.