Journal of Engineering Sciences and Information Technology
Volume (5), Issue (2): 30 Jun 2021
P: 44 - 57

ISSN: 2522-3321

مجلة العلوم الهندسية وتكنولوجيا المعلومات
المجلد (5)، العدد (2): 30 يونيو 2021م
ص: 44 - 57

Achieve distributed and secure Internet of things structure using multi-chains solution of blockchain technology

Sara Mostafa Soleman

Faculty of Information Technology || Al-Baath University || Syria

Abstract: The Internet of Things (IoT) is considered a high-impact technology in many major markets. It promises many opportunities, but there are several risks and drawbacks associated with this technology stand in the way of realizing its potential opportunities, such as the IoT devices limited capabilities (restricted resources) as well as the current access control systems based on central structures and central hierarchies. with all IoT devices, the security risks and threats are enormous. Blockchain is defined as tamper-proof, tamper-resistant digital ledgers that are executed in a distributed fashion, i.e., without a central repository and usually without central authority, allowing all parties to track information over an insecure network without the need for third-party verification. This technology could be a solution to the problems facing the Internet of Things, however the integrating between blockchain and Internet of Things system comes with many challenges as such blockchain suffers from high resource consumption, slow response, etc. In this research we will propose a new architecture for how to integrate blockchain with the Internet of Things. This structure consists of the smart home responsible for its own data (own chain) and the service provider which considered indirect manager of the network. The performance of the proposed architecture will be studied in terms of expansion, decentralization, security and permanent availability.

Keywords: Internet of Things, Consensus Algorithms, Distributed Systems, Proof of Work, Proof of Stake, Byzantine Fault Tolerance Consensus Algorithms.

تحقيق بنى موزعة وآمنة لانترت الأشياء عبر السلاسل المتعددة لتقنية البلوكتشين

ساره مصطفى سليمان

كلية الهندسة المعلوماتية || جامعة البعث || سورية

المستخلص: يعتبر إنترنت الأشياء (IoT) تقنية ذات تأثير كبير في العديد من الأسواق الرئيسية. كما ويَعد بالعديد من الفرص ولكن هناك عدة مخاطر وعيوب مرتبطة بالتكنولوجيا التي تقف في طريق تحقيق الفرص المحتملة له، كالقدرات المحدودة (المقيدة) للعديد من أجهزة إنترنت الأشياء وكذلك أنظمة التحكم في الوصول الحالية القائمة على البنى المركزية والتسلسل الهرمي المركزي، ومع وجود جميع أجهزة إنترنت الأشياء تكون مخاطر تهديدات الأمان هائلة. تعرف Blockchain بأنها دفاتر رقمية (ledgers) غير قابلة للتعديل ومقاومة للعبث يتم تنفيذها بطريقة موزعة أي بدون مخزن مركزي وعادةً بدون سلطة مركزية مما يتيح لكل الأطراف تتبع المعلومات عبر شبكة غير آمنة دون الحاجة للتحقق من طرف ثالث. قد تكون هذه التكنولوجيا حلاً للمشاكل التي تواجه إنترنت الأشياء، ومع ذلك يأتي تطبيق blockchain في نظام إنترنت الأشياء مع العديد من التحديات حيث يعاني blockchain من مشاكل استهلاك الموارد الكبير، والاستجابة البطيئة وغيرها، سنقوم في هذا البحث باقتراح بنية جديدة لكيفية دمج blockchain مع إنترنت الأشياء، وتتكون هذه البنية من المنزل الذكي المسؤول عن بياناته الخاصة (بناء سلسلته الخاصة) ومزود الخدمة الذي يعد مدير غير مباشر للشبكة وسيتم دراسة أداء البنية المقترحة من ناحية التوسع اللامركزية والأمن والتوافرية الدائمة.

الكلمات المفتاحية: إنترنت الأشياء، خوارزميات الاتفاق، الأنظمة الموزعة، إثبات العمل، أثبات الحصة، خوارزميات الاجماع البيزنطي.

المقدمة:

تم تعريف Blockchain من قبل [1](NIST،2018) بأنه عبارة عن دفاتر رقمية (ledgers) غير قابلة للتعديل ومقاومة للعبث يتم تنفيذها بطريقة موزعة (أي بدون مخزن مركزي) وعادةً بدون سلطة مركزية (أي بنك أو شركة أو حكومة). بالشكل الطبيعي، يسجل المستخدمون المعاملات في دفتر الإسناد الموزع، بحيث لا يمكن تغيير أي معاملة بعد القيام بنشر الكتلة (block) في شبكة blockchain.

تم اقتراحها بواسطة [2](Satoshi Nakamoto, 2008) كتقنية وراء Bitcoin، وتبنى blockchain على أساس كل من شبكة نظير إلى نظير (peer to peer)، مفاهيم التشفير بالمفتاح العام، وقواعد البيانات الموزعة لإنشاء إجماع موزع بين المشاركين في الشبكة دون وسيط مركزي للثقة. في شبكة blockchain يتم تجميع المعاملات في كتل، والتي يتم إنشاؤها بواسطة عقد الشبكة عبر إتباع آلية إجماع موزعة، تسمى الكتلة الأولى من blockchain بكتلة التكوين Genesis Block، ويتم ربط كل كتلة تالية لها بالكتلة السابقة بواسطة مؤشر على ناتج تجزئة العقدة الحالية مع سابقاتها لتشكيل سلسلة غير قابلة للتغيير من الكتل.[3]

تتكون نماذج إنترنت الأشياء التقليدية عادة من مركز بيانات مركزي مسؤول عن جمع ومعالجة بيانات الأجهزة المتصلة. ومع ذلك فإن هذه الطريقة لها عيوب في تكاليف دورة الحياة المرتفعة نظراً لارتفاع تكاليف صيانة الخوادم المركزية، كما عند زيادة عدد أجهزة إنترنت الأشياء إلى عشرات المليارات فقد لا يكون نموذج إنترنت الأشياء التقليدي قادراً على تلبية الطلبات المتزايدة لنظام IoT، بالإضافة إلى مشكلة الكم الهائل من بيانات إنترنت الأشياء والزيادة في سرعة توليدها، ومع ذلك يمكن تخزين نسبة صغيرة فقط من هذه البيانات بشكل دائم، كما يعد أمن بيانات إنترنت الأشياء من المشاكل الخطيرة التي يجب العمل على حلها حيث تقوم أجهزة إنترنت الأشياء بتوليد ومعالجة كميات هائلة من البيانات الحساسة للأمان والسلامة وكذلك معلومات مهمة للخصوصية وبالتالي فهي أهداف جذابة لهجمات مختلفة، باختصار من المستحسن تصميم حل مفيد وآمن لإدارة بيانات إنترنت الأشياء.[4]

في الآونة الأخيرة كان هناك اهتمام متزايد بالتقنيات القائمة على blockchain لإنترنت الأشياء بسبب ما يمكن أن يحققه الدمج [5] كأن تكون البيانات منيعة ضد التلاعب، الطبيعة الموزعة للبلوكتشين بالتالي عدم وجود نقطة واحدة من الفشل أو نقطة هجوم واحدة في النظام، والبيانات محمية ضد أعطال جهاز إنترنت الأشياء أو العبث. كما يمكن أن تعمل تقنية Blockchain على تحسين الخصوصية من خلال الحفاظ على سرية معاملات إنترنت الأشياء.

من الواضح أن فكرة دمج Blockchain وInternet of Things قادرة على إحداث نقلة نوعية حيث يمكن أن تستفيد كلتا التقنيتين من بعضهما البعض بطريقة متبادلة، ومع ذلك فإن دمجهما معاً ليس أمراً مباشراً. حيث بالرغم من العديد من المزايا التي يمكن تحقيقها إذا تم دمج blockchain مع إنترنت الأشياء، ك عدم وجود تحكم مركزي الذي من شأنه أن يضمن قابلية التوسع والمتانة robustness، مما سيؤدي إلى القضاء على مشكلة نقطة فشل واحدة [6](A Dorri et al. 2016)، ونظام عدم الكشف عن الهوية، إلا أن blockchain لديه مشاكل استهلاك الموارد الكبير، والاستجابة البطيئة نتيجة لطاقة المعالجة الكبيرة التي يحتاجها، وفي المقابل فإن أنظمة إنترنت الأشياء من المتوقع أن تحتوي على عدد كبير من العقد ذات الموارد المحدودة، كما قد لا يكون نهج الإجماع إثبات العمل (PoW) أو غيره من آليات الإجماع في blockchain مناسباً لبيئة إنترنت الأشياء، لأنه يتطلب كلاً من طاقة الحوسبة

والطاقة الكهربائية إلى حد كبير، في المقابل تعاني أجهزة إنترنت الأشياء بشدة من قدرات المعالجة الضعيفة والمحدودية في سعة أنظمة التخزين. [8][7]

تتولد معظم المشاكل المتعلقة بالدمج بين هاتين التقنيتين من طبيعة خوارزميات الاتفاق في البلوكتشين التي تم تصميمها على أساس العملات الرقمية.

مشكلة الدراسة:

يمكن تحديد مشكلة البحث في التساؤلات التالية:

1- كيف يمكن تحقيق الدمج بين هاتين التقنيتين للتغلب على مشاكل الحماية والخصوصية التي يعاني منها إنترنت الأشياء مع الحفاظ على أداء مناسب لمتطلبات تطبيقات إنترنت الأشياء؟

ويتفرع عن هذا السؤال ما يلي:

1. ما المشكلات التي تجعل خوارزميات الاتفاق غير مناسبة لإنترنت الأشياء؟
2. كيف سيتم حل مشكلة محدودية موارد أجهزة إنترنت الأشياء دون الحاجة لتغيير الأجهزة؟
3. ما خصائص خوارزميات الاتفاق التي تجعلها غير مناسبة للتطبيق في بيئة إنترنت الأشياء؟
4. كيف سيتم حل مشكلة توفر البيانات والتخزين مع الحفاظ على الخصوصية؟
5. كيف نحقق التوزع المناسب للحماية من نقطة فشل واحدة؟

فرضيات الدراسة: تفترض الدراسة أن البلوكتشين قادر على تحقيق كل مما يلي لإنترنت الأشياء:

1- توفر البلوكتشين سجلاً دائماً للمعاملات والاتصالات وتخزين البيانات بشل آمن لإنترنت الأشياء.

2- تضمن الطبيعة الموزعة للبلوكتشين عدم وجود نقطة واحدة من الفشل أو نقطة هجوم واحدة في النظام.

3- تعمل تقنية Blockchain على تحسين الخصوصية من خلال الحفاظ على سرية معاملات إنترنت الأشياء.

أهمية الدراسة:

تنبع الاهمية العلمية للدراسة من:

1. تحقيق الحماية لبيانات انترنت الأشياء التي تعد بيانات ذات حساسية كبيرة ومنع التنصت عليها او تغييرها.
2. مراجعة لأهم خوارزميات الاتفاق التي يعمل بها في البلوكتشين حالياً.
3. العمل على نقل البنية الحالية لانترت الأشياء من الاعتماد على مركز بيانات واحد إلى التوزع دون الحاجة إلى إحداث تغيرات كبيرة في البنى الحالية له.

منهجية الدراسة:

أ- منهجية التحليل: تم استخدام المنهج التجريبي حيث تم تطبيق سيناريو وتجريبه والخروج بنتائج تدعم فرضياتنا.

ب- مصادر البيانات: من الأبحاث التي تم نشرها واعتمادها من مجلات عالمية.

ج- حدود الدراسة: اقتصرت الدراسة على اجراء المحاكاة على جهاز محلي دون نقل العملية إلى التنفيذ في بيئة حقيقة، كما لم يتم تعميم السيناريو المطروح على كافة تطبيقات إنترنت الأشياء وإنما على المنزل الذكي فقط.

هيكلة الدراسة:

تم تقسيم هذه الدراسة إلى أربعة مباحث، يتناول المبحث الأول منها الإطار الدراسات السابقة، بينما يتطرق المبحث الثاني إلى خوارزميات الاتفاق، ثم المبحث الثالث عن النقص في خوارزميات الإجماع فيما يتعلق بإنترنت الأشياء، والمبحث الأخير يتناول البنية المقترحة والتحليل.

المبحث الأول- خوارزميات الاتفاق

هناك العديد من الطرق القائمة على القوة الحسابية وحصة النظام والعلاقة بين الشبكات لتحقيق التوافق. قمنا بإدراج بعض طرق التوافق كما يلي:

- ❖ إثبات العمل PoW (Proof of work)

تستخدم في شبكة لا مركزية حيث يجب اختيار شخص ما لتسجيل المعاملات، إذا أرادت العقدة نشر مجموعة من المعاملات فيجب عليها القيام بالكثير من العمل لإثبات أن العقدة من غير المحتمل أن تهاجم الشبكة في هذه الحالة العمل يعني القوة الحسابيه.

يعمل المشاركون في blockchain (عمال المناجم) على حل مشكلة حسابية معقدة ولكن غير مجدية من أجل إضافة كتلة من المعاملات إلى blockchain، بعد إنشاء كتلة جديدة يتم بثها إلى العقد الأخرى، وعند استلام هذه الكتلة الجديدة تقوم العقد المستلمة لها بالتحقق من PoW عن طريق إعادة حساب قيمة التجزئة ومقارنتها مع قيمة التجزئة المدرجة في رأس الكتلة المستلمة. يمكنهم أيضاً التحقق من المعاملات المضمنة في الكتلة قبل إلحاقها بنسختهم من دفتر الإسناد الموزع. [11]

- ❖ إثبات الحصة Proof of Stack

تقوم الفكرة الأساسية للخوارزمية على أنه بدلاً من استخدام القوة الحسابية يجب امتلاك حصة (عملات معدنية) في النظام، أي إذا امتلكت عقدة 10% من الحصة (عملات معدنية) فإن احتمال تعدين تلك العقدة للكتلة التالية سيكون 10%. استخدام الرصيد بهذا الأسلوب له ميزة هي أي شخص يمتلك حصة كبيرة سيكون أكثر ثقة ولا يريد القيام بأي أعمال احتيالية لمهاجمة السلسلة التي تحتوي على الكثير من أرباحه. على الرغم من أن هذه الطريقة تلغي المتطلبات الحسابية لإثبات العمل إلا أنها تخلق مشاكل جديدة أحدها هو المركزية، في حال امتلكت عقدة الحصة الأكبر ستكون المسيطر على عملية إنشاء الكتل والربح.

- ❖ Delegated Proof-of-Stake Consensus (DPoS)

يمكن لكل عقدة اختيار المفوضين (Delegates) على أساس حصتها في الشبكة بالكامل، يتمتع كبار المفوضين الذين رشحوا أنفسهم للتفويض عن العقد وحصلوا على أكبر عدد من الأصوات بالحق في المحاسبة، يقوم المفوضون المنتخبون بإنشاء كتل جديدة واحدة تلو الأخرى على النحو المحدد والحصول على بعض المكافآت. تعد blockchain باستخدام DPoS أكثر كفاءة وتوفير الطاقة من PoW و PoS. عادة ما تنتج جميع العقد المفوضة كتلاً واحدة تلو الأخرى بطريقة مستديرة Round Robin هذا يمنع العقدة من نشر الكتل المتتالية في نفس الوقت مما يمنع من تنفيذ هجمات الإنفاق المزدوج، إذا لم تنتج العقدة المفوضة كتلة في فترتها الزمنية سيتم تخطي تلك العقدة ويقوم المفوض التالي بإنشاء الكتلة التالية. إذا غاب المفوض باستمرار عن دوره في النشر أو نشر معاملات غير صالحة فإن العقد الاخرى تصوت ضده وتستبدله بعقدة مفوضة أفضل. [12]

خوارزميات Byzantine Fault Tolerance

هي آلية في الشبكة الموزعة للوصول إلى إجماع (اتفاق على نفس القيمة) حتى عند فشل بعض عقد الشبكة في الاستجابة أو عند استجابتها بمعلومات غير صحيحة، الهدف من آلية BFT هو الحماية ضد فشل النظام من خلال اتخاذ قرار جماعي (على حد سواء - العقد الصحيحة والخاطئة) مما يهدف إلى تقليل تأثير العقد المعيبة، تم اشتقاق خوارزمية BFT من مشكلة الجنرالات البيزنطيين. وتعرف بأنها خوارزميات إجماع معتمدة على التصويت، والتي يجب أن تكون فيها العقد معروفة داخل شبكة التحقق حتى تتمكن من تبادل الرسائل بشكل أسهل، هذا هو الفرق الرئيسي مقارنة بخوارزميات الإجماع التقليدية والتي تكون العقد في الغالب حرة في الانضمام إلى شبكة التحقق والتحقق منها.

❖ Practical Byzantine Fault Tolerance (PBFT)

يتم ترتيب العقد في النظام الموزع المشغل لـ pBFT بشكل تسلسلي مع عقدة واحدة هي العقدة الأساسية (أو العقدة الرئيسية) ويشار إلى العقد الأخرى على أنها ثانوية (أو العقد الاحتياطية)، أي عقدة مؤهلة في النظام يمكن أن تصبح أولية من خلال الانتقال من ثانوية إلى أولية (عادةً في حالة فشل العقدة الأولية)، الهدف منها هو أن تساعد جميع العقد الصادقة في الوصول إلى توافق في الآراء بشأن حالة النظام باستخدام قاعدة الأغلبية.

يتم تقسيم جولات إجماع pBFT إلى 5 مراحل:

1- الطلب Request: يرسل العميل طلباً إلى عقدة الخادم الرئيسي.
2- الإعداد المسبق Pre-prepare: تسجل عقدة الخادم الرئيسي رسالة الطلب وتعطيها رقم للطلب وطابع زمني، وتشكل رسالة pre-prepare، ثم تبث العقدة الرئيسية رسالة التحضير المسبق لعُقد الخادم المجاورة، التي تحدد بدورها في البداية ما إذا كان سيتم قبول الطلب أم لا عبر معايير خاصة بالشبكة.
3- التحضير prepare: إذا اختارت عقدة الخادم قبول الطلب، فإنها تبث رسالة تحضير لكل عقد الخادم الأخرى وتتلقى رسائل التحضير من العقد الأخرى التي بالمثل قامت بقبول الطلب وبث رسالة التحضير، بعد تجميع الرسائل المستلمة إذا كان عددها 2f+1 (اي اختارت غالبية العقد قبول الطلب) فستدخل حالة الالتزام.
4- الالتزام commit: ترسل كل عقدة في حالة الالتزام رسالة التزام إلى جميع عقد الخادم الأخرى في الشبكة، وفي الوقت نفسه إذا تلقت عقدة الخادم رسائل الالتزام من 2f+1 عقدة بالتالي معظم العقد توصلت إلى توافق في الآراء لقبول الطلب ثم تنفذ العقدة التعليمات في رسالة الطلب.
5- الرد reply: إذا لم يتلق العميل رداً بسبب تأخير الشبكة فسيتم إعادة إرسال الطلب إلى عقد الخادم، إذا تم تنفيذ الطلب فستقوم عقد الخادم بإرسال رسالة الرد بشكل متكرر.

❖ RIPPLE

يكون لكل خادم قائمة خاصة به تسمى قائمة العقدة الفريدة Unique Node List(UNL) والتي تتضمن بعض الخوادم الأخرى، وعند إجراء التحقق من معاملة ما، بدلاً من بثها لجميع العقد، كل خادم سيجمع مجموعة من المعاملات ويتحقق منها ويرسلها إلى العقد في UNL لديه.

يقوم كل خادم بتجميع جميع المعاملات المنشأة من خوادم أخرى في UNL لديه في المجموعة الخاصة به، ثم التحقق من المعاملات داخل هذه المجموعة، سيتم إجراء تصويت "نعم" على كل معاملة من المعاملات إذا تم التحقق منها بنجاح فهي معاملة صحيحه وسيتم تجاهل أي معاملات لا تحصل على عدد كافٍ من أصوات "نعم" من مجموعة المرشحين (تتطلب الجولات النهائية ما لا يقل عن 80% من أصوات نعم لكل معاملة).

❖ Delegated Byzantine Fault Tolerance (dBFT)

على غرار pBFT فإنه يحقق الإجماع على المعلومات الجديدة على أساس الأصوات، ومع ذلك في dBFT يتم اختيار أدوات التحقق (العقد التي تصادق وتصوت) من قبل الطالب لكل توافق في الآراء، إذا لم يثق مقدم الطلب في المدقق المختار فيمكن لمقدم الطلب اختيار عقدة أخرى كمصدق لإجراء التوافق التالي، بعد ذلك يختار المدققون عقدة لتكون القائد الذي سينشئ الكتلة ويبدأ إجراء الإجماع وبالتالي يتم استخدام مجموعة فرعية صغيرة فقط من العقد لأداء الإجماع في dBFT، عندما يقوم أكثر من ثلثي العقد المنتخبة بالتحقق من صحة المعلومات فإنها تعتبر صالحة.

❖ TANGLE – IOTA

تتكون شبكة Tangle على مناقلات (معاملات) وعُقد (أجهزة)، لإصدار معاملة جديدة يجب أن تساهم العقدة (الجهاز) في شبكة IOTA في تأكيد (التحقق من) المعاملات الأخرى، نظراً لتأكيد المعاملات من خلال المزيد والمزيد من العقد التي تحتاج بدورها إلى نشر معاملاتها الخاصة، ذلك يزيد مستوى اليقين في أن المعاملات صحيحة، بسبب هذه الميزة فإن أي عقدة تصدر معاملة تساعد في تحسين أمان الشبكة بالكامل.

لا يتطلب هذا البروتوكول عملية إجماع معقدة تستغرق الكثير من الوقت والحساب المكثف، كما أنه لا يستخدم الكتل لتخزين المعاملات، كل معاملة هي كتلة فريدة في حد ذاتها والتي يجب أن توافق على اثنين من المعاملات القديمة من أجل إضافتها إلى دفتر الأسناد، تتم الموافقة على اثنين من المعاملات القديمة عن طريق إثبات العمل، يستخدم Tangle Directed Acyclic Graph (DAG) حيث يتم ربط كل معاملة بمعاملتين قديمتين تمت الموافقة عليهما.

نظراً للتصميم الفريد ل tangle فهو إطار سريع وقابل للتوسعة بشكل جيد يجعله مناسباً تماماً لشبكات إنترنت الأشياء.

المبحث الثاني- النقص في خوارزميات الاتفاق

تبتعد متطلبات إنترنت الأشياء عن متطلبات التداول المالي التي تم تصميم معظم خوارزميات الاتفاق من أجلها، نحتاج لتصميم خوازمية اتفاق تعمل مع إنترنت الأشياء لتحقيق السرعة، النهاية الجيدة، التوسع الكبير، توفير الطاقة وغيرها. بناء على هذه المتطلبات ستتم المقارنة بين الخوارزمية المذكورة مسبقا كالتالي:

- يحتاج PBFT إلى معرفة هوية كل عقدة (عامل منجم) من أجل تحديد العقدة الرئيسية في كل جولة، بينما يحتاج Tendermint إلى معرفة المدققين من أجل اختيار منشأ الكتلة في كل جولة، أما بالنسبة إلى PoW وPoS وDPOS وRipple يمكن للعقد الانضمام إلى الشبكة والانفصال عنها بحرية.
- في PoW يقوم المعدون بتطبيق تابع التجزئة على رأس الكتلة header باستمرار عبر تغيير nonce للوصول إلى القيمة المستهدفة بالتالي يزيد ذلك استهلاك الكهرباء والقدرات المطلوبة للمعالجة إلى مستوى هائل، بالنسبة إلى PoS وDPOS لا يزال يتعين على المعدنين تطبيق تابع التجزئة على رأس الكتلة header للبحث عن القيمة المستهدفة ولكن تم تقليل هذا العمل إلى حد كبير حيث تم تصميم مساحة البحث لتكون محدودة بالتالي استهلاك موارد أقل من سابقه. بالنسبة إلى PBFT وRipple لا يوجد تعدين في عملية الإجماع لذلك فهو يوفر الطاقة بشكل كبير.

- بشكل عام تعتبر 51% من قوة التجزئة (العقد) هي الحد الأدنى للسيطرة على الشبكة في POW، POS، وتم تصميم PBFT وTendermint للتعامل مع ما يصل إلى 3/1 من العقد المعيبة، ثبت أن Ripple تحافظ على صحتها إذا كانت العقد المعيبة في UNL أقل من 20%.
- تعد كل من PoW وIOTA عرضة للتفرع (الشوكة) مما يضيف تأخير على عملية الانتهاء من الإجماع على الكتل، بينما الخوارزميات التي تعتمد على bft وPOS وغيرها لا يتشكل فيها أي شوكة بالتالي تسرع عملية الوصول إلى اتفاق حقيقي على الكتل التي يتم نشرها في الشبكة، غير أن الكتلة الصحيحة لا تحتاج انتظار بمجرد نشرها في الشبكة (منتهية).
- الخوارزميات القائمة على BFT تفتقر إلى التوسع الكبير ويعود ذلك إلى الحاجة لمعرفة جميع العقد في الشبكة وعمليات التصويت التي تستهلك عرض الحزمة بالتالي يتم اعتمادها عادة في شبكات Blockchain الخاصة اما بالنسبة ل POW، POS تعد خوازميات قابلة للتوسع بشكل كبير.

جدول (1) مقارنةالأداء بين خوارزميات الاتفاق فيما يتعلق بإنترنت الأشياء

Algorithm	Throughput	LATENCY (Confirmation Delay)	Resource consumption	forks	Scalability
POW	7(Bitcoin) – 30 (Ethereum) TPS [20] [21] [23]	[20] [21] [23] – 60 min	High	Yes	Strong [21]
POS	100 –1000 TPS [20][22]	10 sec – 10 min (Nxt) [20][23]	Low	No	Strong [21]
PBFT	000 TPS ،100 [22][21]	Network Related 100 ms [21]	Low	No	Weak [21]
DPOS (EOS)	000 ،10 to 100 and theoretically even millions of TPS [12]	0.5 sec	Low	No	Strong [21]
Tangle	No technical up bound [20]	Depend on transaction arrival rate [20] no upper [23] 10ms bound of TPS [21]	low	Yes	Strong [21]

يظهر الجدول أنه من غير الممكن تطبيق أي من الخوارزميات السابقة ضمن الوضع الراهن لها أو بالشكل الذي يتم العمل به حالياً لأنها لا تحقق عدد المناقلات المطلوب لإنترنت الأشياء وتحتاج طاقة حسابية أو تستهلك موارد الشبكة عبر التصويت.

المبحث الثالث- الدراسات السابقة

الدراسات السابقة

أكد [6] على النمو الكبير لإنترنت الأشياء Internet of Things (IoT) في مجالات البحوث والصناعة لكنه لا يزال يعاني من ثغرات أمنية وثغرات في الخصوصية. تعد إحدى التحديات التقنية ل IOT وفق [13] هي نشر مليارات الأجهزة في جميع أنحاء العالم والقدرة على إدارتها. بالرغم من وجود تقنيات إدارة الوصول في إنترنت الأشياء فهي تعتمد على نماذج مركزية تعاني من مجموعة من القيود التقنية لإدارة هذه الأعداد الكبيرة.

تعتبر Blockchains وفق [14] واحدة من أكثر التقنيات الواعدة في مجال إنترنت الأشياء (IoT)، كما تعد عملية -اقتراح بنية آمنة تستند إلى هذا الإطار- باهظة من الناحية الحسابية وتتطلب نطاق ترددي عالي وقدرة حسابية إضافية وبالتالي فهي غير مناسبة تماماً لمعظم أجهزة إنترنت الأشياء المقيدة للموارد.

اقترح [15] Lightweight Scalable BC (LSB) إطاراً يحقق أمن وخصوصية إنترنت الأشياء. يتكون الإطار من مستويين رئيسيين هما المنزل الذكي وoverlay يتم اعتبار المعاملة وسيلة الاتصال الأساسية لتبادل المعلومات بين الكيانات المختلفة واقترح [16] إطار عمل متعدد السلاسل لدمج عدة Blockchains معاً لإدارة بيانات إنترنت الأشياء بشكل فعال وآمن. تم استخدام Consortium blockchain كمحطة تحكم وربط بين عدة سلاسل بينما تعمل Tangle Blockchain مع أجهزة إنترنت الأشياء المترابطة. اقترح [17] نموذج يعمل على إدارة الهوية باستخدام المفاتيح العامة بحيث تحافظ البنية المقترحة على هوية أجهزة الحساسات لإنترنت الأشياء في blockchain لمنع أي تعديل بيانات غير مرغوب به ولكنه يخفف جزء من عبئ برنامج blockchain غير المهم للأمان ليضعها في Proxy خفيف منفصل.

اقترح [18] إطار جديد لنماذج blockchain المناسبة لأجهزة إنترنت الأشياء التي تعتمد على طبيعتها الموزعة وغيرها من خصائص الخصوصية والأمان الإضافية للشبكة. يتكون النظام المقترح من خمسة أجزاء: شبكة التراكب والتخزين السحابي ومقدمي الرعاية الصحية والعقود الذكية والمريض المجهز بأجهزة إنترنت الأشياء القابلة للارتداء للرعاية الصحية.

المبحث الرابع- الخوارزمية المقترحة

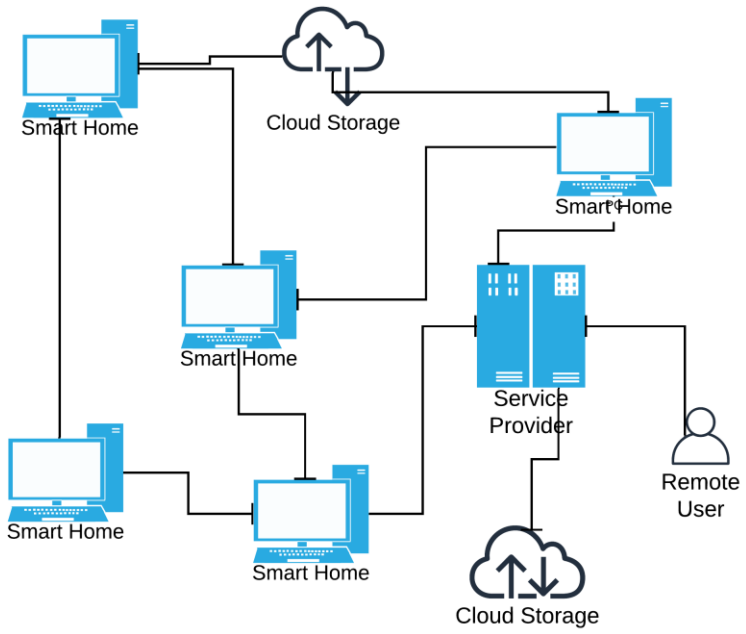
يختلف التعامل مع بيانات إنترنت الأشياء تماماً عن التعامل مع البيانات المالية من ناحية الشفافية، التحقق من المعاملات، آلية التخزين، الخصوصية والحماية وفق التالي:

- البيانات لا يجب أن يتم معرفتها من قبل العقد الاخرى في الشبكة.
- مزود الخدمة قادر على الوصول إلى البيانات للقيام بعملية التخزين والتحليل وغيرها بحسب الخدمة المقدمة.
- العقد غير معروفة في الشبكة وحرة في الانضمام والخروج من الشبكة دون أن يؤثر على أداء الشبكة.
- المعاملات في إنترنت الأشياء غير مرتبطة فمن غير المنطقي التحقق منها كما في المعاملات المالية (التحقق من الرصيد) بل يجب التأكيد على إمكانية حدوث التغيير المفاجئ في أي لحظة هنا يكمن السؤال ما الطريقة المناسبة للتحقق من صحة المعاملة؟

نقترح بنية جديدة لتطبيق الدمج بين إنترنت الأشياء والبلوكتشين لتحقيق سرعة وأداء يتناسب مع متطلبات إنترنت الأشياء، بحث لا تحتاج العقد إلى التوافق على بيانات العقد الاخرى وذلك لسرية البيانات فلا يمكن

رؤيتها إلا من قبل الأشخاص المخولين بذلك، كل عقدة تدير بياناتها الخاصة، وتتحقق من صحة الكتل للعقد الأخرى دون أن تتمكن من الاطلاع على محتوى البيانات في الكتلة، كما تخزن كل عقدة بياناتها محليا وتخزن بيانات عقد أخرى بشكل مشفر لتحقيق التوافر للبيانات.

تتكون البنية من المنازل الذكية ومزود الخدمة. سيتم تنفيذ آلية sharding، كل منزل ذكي سيقوم ببناء سلسلته الخاصة به عبر خوارزمية PoW ولكن ستكون مساحة البحث لحل اللغز صغيرة جدا، ولن تتسابق العقد على نشر كتلة جديدة في السلسة ولكن كل عقدة في الشبكة ستنشر كتلة عند الحاجة في سلسلتها الخاصة بها وترسل هذه الكتلة إلى الشبكة للتحقق منها، أي سيقوم المنزل بعملية تشفيره كل مناقلة وإنشاء كتلة جديدة وحساب POW وإرسالها إلى الشبكة. المنزل مسؤول أيضاً عن عملية تخزين سلسة hashes لعدد من المنازل الذكية والتحقق من الكتل القادمة منها وتسمى العقد هنا العقد الخفيفة. كما سيخزن سجل لمُعرفات العقد (nodeId) ضمن الشبكة. كما يمكن لبعض المنازل أن تقوم بما سنسميه التعدين وستسمى العقد الكاملة هنا وسنأتي على ذكره لاحقاً. مزود الخدمة سيكون مدير غير مباشر للمنازل الذكية. يوضح الشكل رقم 1 البنية التي نقترحها في هذه الورقة.



الشكل (1) البنية المقترحة

المنزل الذكي:

يتكون المنزل الذكي من مجموعة متنوعة من أجهزة إنترنت الأشياء ونظراً لأن أجهزة إنترنت الأشياء عادة ما تكون مقيدة بالموارد، سيديرها جهاز محليLocal Manager، وينضم المنزل إلى الشبكة عبر الاتصال مع مزود الخدمة والاتفاق معه على شروط الخدمة وآليات التعدين وغيرها، عندها سيرسل مزود الخدمة Genesis Block الذي يحوي على البيانات المتفق عليه مع المنزل الذكي مشفر بالمفتاح العام للشهادة الرقمية للمنزل الذكي وعند فك تشفير البيانات بالمفتاح الخاص له سيتم استخراج عناوين العقد المجاورة التي سيتصل بها لينضم بشكل فعلي إلى الشبكة، ومتحولات Diffie Hellman لتوليد المفتاح المشترك مع مزود الخدمة لتشفير البيانات مما يمنع العقد الأخرى من رؤية محتوى البيانات مما يحقق الخصوصية وتواجد عدة نسخ من البيانات يحقق توافر دائم لها.

يتم تشفير المعاملات المحلية باستخدام التشفير المتماثل، يخزن البيانات ضمن Blockchain محلي يُدار محلياً من قبل LM.

يمكن توصيف عمل المنزل الذكي على دورين:

- **إدارة البيانات الخاصة:**

سيدير LM بيانات المنزل الذكي عبر إضافة المناقلات إلى الكتلة التي سيقوم بعميلة توليدها، وحساب اللغز لها، وإرسالها إلى العقد في الشبكة لعملية التوثق منها، إضافة إلى ذلك سيقوم بعمليات حفظ المفاتيح والتشفير الخاص بالمنزل.

- **إدارة بيانات العقد:**

في حال إرسال Genesis Block من قبل مزود الخدمة إلى الشبكة بحيث يكون Previous Hash له هو 0، تقوم العقد التي تستقبل هذه الكتلة سواء خفيفة أو كامله باختيار إما تخزينه لديها أو تجاهله وفق قرار التعدين الخاص بها وبكل الأحوال ستقوم بتسجيل معرف العقدة الجديدة NodeId وتوجيهه إلى العقد الأخرى المتصلة معها.

في حال التخزين ستقوم بتخزين إما سلاسل hash أو سلاسل الكتل كاملة وفق طبيعة العقدة (خفيفة أو كامله) مع معرف العقدة ليتم عملية التحقق من أي كتلة تابعه له في المستقبل وفق المعرف الخاص بالعقدة.

- العقد الخفيفة not Miner

ويسمى المنزل الذكي بهذه الحالة بالعقد الخفيفة وتكمن وظيفته ب:

يخزن سلاسل hashes لعدد من العقد وفق الاتفاق الذي تم في مرحلة التسجيل مع مزود الخدمة دون تخزين السلسة بالكامل ويتم تخزين سلاسل hashes الخاصة بكل عقدة بشكل منفرد وفق المعرف الخاص بالعقدة وعند وصول أي كتلة جديدة يتم استخراج hashes الخاصة بالعقدة عبر المعرف الخاص والتحقق من أنه من العقد التي تديرها هذه العقدة ثم التأكد من صحة الكتلة الجديدة (عبر اعادة حساب لغز PoW) وتخزين hash الجديد إلى السلسلة في حال كان حل اللغز صحيح.

- العقد الكاملة

تقوم بجميع عمليات العقد الخفيفة إلا أنها لا تخزن فقط hash وإنما تخزن السلاسل بالكامل ل n عقدة أو جميع العقد في منطقة ما بحسب الاتفاق مع مزود الخدمة وهذه العقد تشبه miner في Bitcoin من ناحية الربح ولكن لا عملية سباق على نشر الكتلة التالية (الربح على أساس التخزين).

- مزود الخدمة

يعتبر بمثابة مدير للشبكة فهو المسؤول عن تسجيل العقد عند الانضمام إلى الشبكة وتحديد الأدوار للعقد وآلية التواصل مع بعض وتخزين البيانات في السحابة ويعتبر كنقطة إدارة للشبكة لا يمكن الاستغناء عنه وينبع ذلك من طبيعة إنترنت الأشياء فلا يمكن الاستغناء عن هذا الكيان المركزي ويقوم دوره كالتالي:

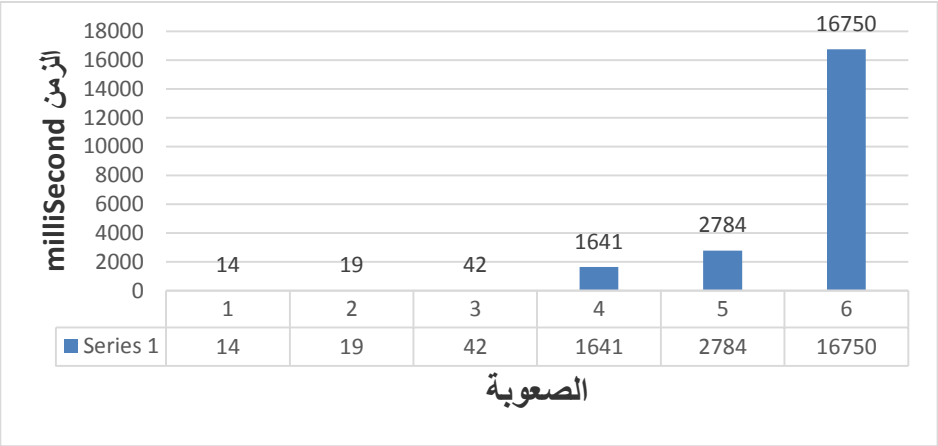
- تسجيل العقد الجديدة في الشبكة ويتم ذلك كالتالي:

استلام طلب الاشتراك من عقدة ما مع الشهادة الرقمية ومعلومات الخاصة بالخدمة عندها ستقوم بتوليد متحولات Diffie Hellman وعناوين العقد المجاورة للمنزل الذكي وغيرها من معلومات الخدمة وتشفير هذه البيانات باستخدام المفتاح العام للعقدة وتوليد Genesis Block وإرساله في الشبكة إلى العقدة بشكل مباشر ومن ثم إلى overlay.

مناقشة النتائج.

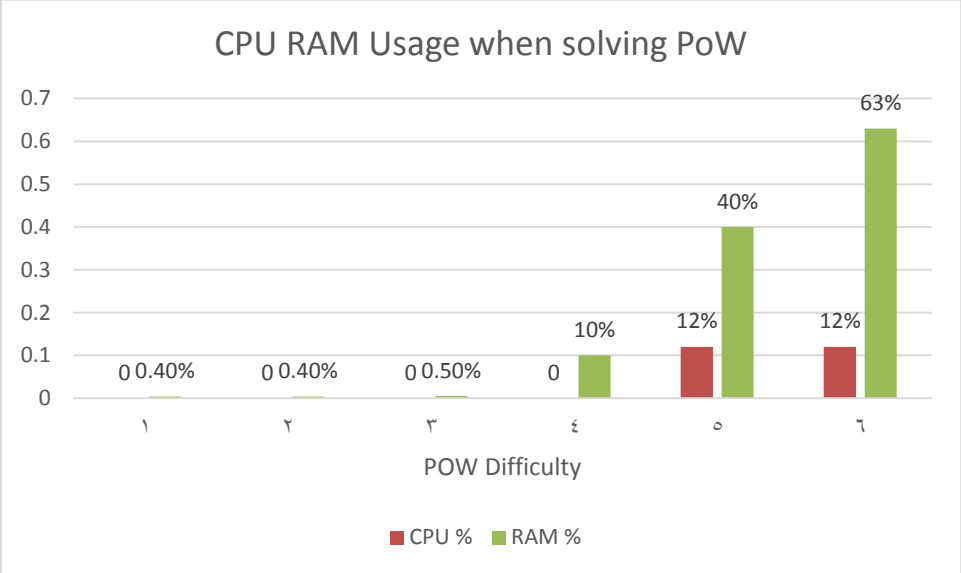
نهدف إلى تقييم الأداء والوقت الذي يستهلكه الجهاز لحل برنامج POW، المطلوب من كل LM البحث عن nonce الصحيح بحيث تحقق الكتلة شرط اللغز، على وجه التحديد مطلوب أن تحتوي تجزئة SHA-256 للكتلة على عدد معين من الأصفار البادئة والسبيل الوحيد لإيجاد nonce الصحيح هي التجريب، يتحكم عدد الأصفار البادئة في صعوبة حل اللغز. وكلما طال طول هذا التسلسل زادت الموارد ووقت المعالجة، هنا سنقوم بتجريب صعوبات مختلفة لإيجاد ما يناسب أداء المنزل الذكي.

تم تطبيق ذلك باستخدام لغة java كما تم اختباره على عدد صعوبات مختلفة وكانت النتائج كالتالي:



الشكل 2 الزمن المستهلك لحل لغز PoW

كما يظهر الشكل التالي استهلاك الذاكرة والمعالج خلال حل اللغز.



الشكل 3 استهلاك الذاكرة والمعالج خلال حل لغز PoW

يظهر الشكل 2 أن التأخيرات التي تفرضها الصعوبات من 1 إلى 3 مقبولة لإنترنت الأشياء وذلك بحسب [19] الذي قام بتحليل خصائص بيانات إنترنت الأشياء ووجد أنه من أجل تطبيقات المنازل الذكية ذات مرور البيانات المنتظم و/أو غير المنتظم يمكن أن تتحمل تأخير يصل إلى 3 ثانية مع المحافظة على جودة الخدمة وبالتالي اختيار قيم من فئة الصعوبة 2 أو 3 مقبولة وتم استبعاد 1 وذلك لفرض القليل من العبء على المنزل الذكي في حال كان عقدة مهاجمة في الشبكة وخاصة في حال هجوم DOS.

لا يستهلك حل لغز POW سوى كمية بسيطة من قدرات المعالجة والذاكرة بالتالي لن يكون هنالك عبئ كبير على الاجهزة التي تتعامل مع إنترنت الأشياء.

الحماية:

عملية POW التي تحتاج العقد للقيام لإصدار كتلة في الشبكة تستغرق وقتاً وموارد أكبر نسبياً من عملية التحقق من قبل العقد الباقية بالتالي تستغرق عقدة ما 19 ميلي ثانية لإنشاء كتلة جديدة بالمقابل تحتاج عقدة في الشبكة إلى 0.03 ميلي ثانية للتحقق من هذه الكتلة بالتالي تحتاج العقدة المهاجمة لإنشاء 634 عقدة جديدة لتستهلك عقدة تتحقق من الكتلة المنشأة إلى 19 ميلي ثانية في التحقق من الكتلة فالجهد المبذول في إنشاء العقد أكبر بمقدار 634 مرة من الجهد الذي تستغرقه عقدة من التحقق. كما لا يمكن لعقد ان تصدر أي كتلة دون حساب PoW ولا يمكن لأي عقدة أن ترسل كتلة بشكل مباشر إلى مزود الخدمة ولكن يجب أن يتم التحقق منه من قبل عقد أخرى في الشبكة وفقط في حال كان الكتلة صحيحه سيتم ارسالها إلى مزود الخدمة، بالتالي محاولة الهجوم على نقطة واحدة في الشبكة غير ممكن.

وفي حال تم الهجوم على التخزين السحابي لإزالة البيانات أو تغييرها لن يكون الهجوم ذا تأثير لوجود عدة سلاسل تحوي البيانات للعقد مخزنة في العقد المعدنة (miner) أو العقدة المولد (صاحبة السلسلة) أو حتى العقد الخفيفة والتي سيكون لديها نسخة عن hashes للسلسة الأصلية.

أما بالنسبة لهجمات مثل Sybil attack فلا يمكن تزوير هوية اي عقدة ضمن الشبكة لأنه لا يمكن لعقدة أن تنضم للشبكة دون التسجيل مع مزود الخدمة، أما في حال تزوير عقدة مشتركة بالخدمة للكتل التي ترسلها باستخدام ID مختلف فسيتم تجاهل الكتل ذات المعرف الغير موجود وعدم تمرير أي كتلة من العقدة هذه.

الاستنتاج.

قدمت البنية المقترحة حل آمن باستخدام تقنية Blockchain دون الحاجة إلى تغيير بنية إنترنت الأشياء ولا تغيير الحساسات المنزلية وتحقق البنية لمقترحة ما يلي:

- البنية الموزعة: عبر استقلالية العقد فالخطأ في عقدة لن يؤثر على باقي العقد.
- أمن البيانات: عبر آليات التشفير المتناظر والتشفير بالمفتاح العام.
- الخصوصية (منع الكشف عن معلومات لأشخاص غير مصرح لهم بالاطلاع عليها أو الكشف عنها) ويتم ذلك عبر عملية التشفير المتناظر ووجود عدة نسخ من البيانات محفوظة في عدة نقاط بالإضافة إلى سلاسل hash لحمايتها من تعديل البيانات.
- التوافر الدائم للبيانات: عبر تعدد النسخ المحمية للبيانات.
- مقاومة للعبث وذلك من طبيعة Blockchain، حيث لا يمكن تعديل كتلة دون تعديل السلسلة كاملة.
- قابلة للتوسع لإن كل منزل سيقوم بعملية الحساب الخاصة به وتخزين سلاسل لمنازل أخرى.

التوصيات والمقترحات.

بناءً على النتائج التي تم التوصل إليها توصي الباحثة وتقترح الآتي:

- ضرورة استخدام البلوكتشين من حماية وموثوقية في مجال إنترنت الأشياء وغيره من المجالات.
- نحتاج إلى المزيد من الأبحاث فيما يخص مجال حماسة انترنت الأشياء وذلك للحساسية العالية للبيانات.

قائمة المراجع

المراجع بالإنجليزية

[1] Yaga, Dylan, et al. "NISTIR 8202 Blockchain Technology Overview." National Institute of Standards and Technology. Recuperado de: https://nvlpubs. nist. gov/nistpubs/ir/2018/NIST. IR 8202.(2018)

[2] Nakamoto, S. Bitcoin, and A. Bitcoin. "A peer-to-peer electronic cash system. 2008." URL: https://bitcoin. org/bitcoin. pdf (дата обращения: 28.04. 2018).(2018)

[3] Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R.C., Michelin, R.A., Zorzo, A.F. and Kanhere, S.S.,2020 . Blockchain technologies for iot. In Advanced Applications of Blockchain Technology (pp. 55-89). Springer, Singapore.

[4] Burhan, Muhammad, et al. "IoT elements, layered architectures and security issues: A comprehensive survey." Sensors 18.9 (2018): 2796

[5] Kim, S.K., Kim, U.M. and Huh, J.H.,2019 . A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security. Energies,12 (3), p.402.

[6] Dorri, A., Kanhere, S.S. and Jurdak, R.,2016 . Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.

[7] Miraz, M.H.,2020 . Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies. In Advanced Applications of Blockchain Technology (pp. 141-159). Springer, Singapore.

[8] Dorri, A., Kanhere, S.S., Jurdak, R. and Gauravaram, P.,2019 . LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. Journal of Parallel and Distributed Computing, ،134 pp.180-197.

[9] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I.S., Mazura, M., Harrison, M., Eisenhauer, M. and Doody, P.,2011 . Internet of things strategic research roadmap. Internet of things-global technological and societal trends,1 (2011), pp.9-52.

[10] Peña-López, I.,2005 . ITU Internet report 2005: the internet of things.

[11] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., ،2017 June. An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.

[12] Bach, L.M., Mihaljevic, B. and Zagar, M., ،2018 May. Comparative analysis of blockchain consensus algorithms. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1545-1550). IEEE.

[13] Novo, O.,2018 . Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal,5 (2), pp.1184-1195.

[14] Attia, O., Khoufi, I., Laouiti, A. and Adjih, C., ،2019 June. An Iot-blockchain architecture based on hyperledger framework for healthcare monitoring application. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.

[15] Dorri, A., Kanhere, S.S., Jurdak, R. and Gauravaram, P.,2019 . LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. Journal of Parallel and Distributed Computing, ،134 pp.180-197.

[16] Jiang, Y., Wang, C., Wang, Y. and Gao, L.,2019 . A cross-chain solution to integrating multiple blockchains for IoT data management. Sensors,19 (9), p.2042.

[17] Dittmann, G. and Jelitto, J., ،2019 June. A Blockchain proxy for lightweight IoT devices. In 2019 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 82-85). IEEE.

[18] Dwivedi, A.D., Srivastava, G., Dhar, S. and Singh, R.,2019 . A decentralized privacy-preserving healthcare blockchain for IoT. Sensors,19 (2), p.326.

[19] .[81] Mocnej, J., Pekar, A., Seah, W.K. and Zolotova, I.,2018 . Network traffic characteristics of the IoT application use cases. School of Engineering and Computer Science, Victoria University of Wellington.

[20] Cao, B., Li, Y., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z. and Peng, M.,2019 . When Internet of Things meets blockchain: Challenges in distributed consensus. IEEE Network,33 (6), pp.133-139.

[21] Salimitari, M. and Chatterjee, M.,2018 . An overview of blockchain and consensus protocols for IoT networks. arXiv preprint arXiv:1809.05613.

[22] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W. and Qijun, C., ،2017 October. A review on consensus algorithm of blockchain. In 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 2567-2572). IEEE.

[23] Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M. and Li, Y.,2020 . Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks.