Improved Blockchain Technologies for Data Storage Compared with Database

Dr. Mohammad Mustafa Hajjoz*

(Received 17 / 2 / 2022. Accepted 25 / 7 / 2022)

□ ABSTRACT □

Databases are used to store and exchange data over the network, but this exchange may have a negative impact in terms of security and the coherence of this data. This is why blockchains, including Bitcoin, have gained special attention in academic and commercial circles. The technology on which Bitcoin (adopts the rest of the cryptocurrency, of course) depends is block chain technology. The core of this technology lies in the distinct data pattern you use to keep records on the network. What distinguishes it from other methods of data preservation is its ability to keep records so that they are immutable so that protects data from tampering or forgery. To achieve this advantage, consensus and cryptography mechanisms are used and information is stored in distributed nodes called Distributed Ledger Technology (DLT)[1]. Through this research, further we will improve this new technology in terms of its ability to use data storage, and a critical analysis of its advantages and disadvantages is presented in this context , finally, we will compare with normal databases.

Keywords: Blockchain, Distributed Ledger, Distributed Databases, Peer-to-peer networks.

* **Assistant Professor- Al- Ba'ath Univversity- Homs- Syria. M.Hajjouz@gmail.com**

تحسين تقنيات سلاسل الكتل لتخزين البيانات مقارنة مع قواعد البيانات

د.محمّد مصطفى حجّوز *

(تاريخ الإيداع 17 / 2 / 2022. قُبِل للنشر في 25/ 7 / 2022)

□ ملخّص □

تستخدم قواعد البيانات لتخزين البيانات و تبادلها عبر الشبكة، لكن قد يكون لهذا التبادل أثره السلبي من حيث الأمان وتماسك هذه البيانات، لهذا ظهرت سلاسل الكتل Blockchain ومن ضمنها البتكوين Bitcoin التي اكتسبت ومثيلاتها من العملات الرقمية اهتماما خاصا في الأوساط الأكاديمية والتجارية. إن التقنية التي تعتمد عليها البتكوين (وبقية العملات الرقمية بطبيعة الحال) هي تقنية سلاسل الكتل. يكمن جوهر هذه التقنية في نمط البيانات المميز الذي تستخدمه لحفظ السجلات على الشبكة. إن ما يميزها عن غيرها من طرق حفظ البيانات قدرتها على حفظ السجلات بحيث تكون غير قابلة للتغيير بشكل يحمي البيانات من التلاعب أو التزوير. لتحقيق هذه الميزة، تستخدم آليات الإجماع consensus والتشفير Cryptography حيث يتم تخزين المعلومات في عقد موزعة والتي تسمى بتقنية السجل الموزع Distributed Ledger Technology (DLT)[1]. من خلال هذا البحث سنقوم بتحسين هذه التقنية الجديدة من حيث إمكانية استخدامها لتخزين البيانات، وتم تقديم دراسة تحليلية لمحاسنها ومساوئها في هذا السياق ومقارنتها مع قواعد البيانات العادية.

الكلمات المفتاحية: سلاسل الكتل، السجل الموزع، قواعد البيانات الموزعة، شبكات الند للند.

* مدرّس – جامعة البعث – حمص – سّورية. M.Hajjouz@gmail.com

مقدمة:

تستخدم قواعد البيانات لتخزين البيانات و تبادلها عبر الشبكة، لكن قد يكون لهذا التبادل أثره السلبي من حيث الأمان وتماسك هذه البيانات، لهذا ظهرت سلاسل الكتل Blockchain ومن ضمنها البتكوين Bitcoin التي اكتسبت ومثيلاتها من العملات الرقمية اهتماما خاصا في الأوساط الأكاديمية والتجارية. إن التقنية التي تعتمد عليها البتكوين (وبقية العملات الرقمية بطبيعة الحال) هي تقنية سلاسل الكتل. يكمن جوهر هذه التقنية في نمط البيانات المميز الذي تستخدمه لحفظ السجلات على الشبكة. إن ما يميزها عن غيرها من طرق حفظ البيانات قدرتها على حفظ السجلات بحيث تكون غير قابلة للتغيير بشكل يحمي البيانات من التلاعب أو التزوير. لتحقيق هذه الميزة، تستخدم آليات الإجماع consensus والتشفير Cryptography حيث يتم تخزين المعلومات في عقد موزعة والتي تسمى بتقنية السجل الموزع(DLT) Distributed Ledger Technology [1]. من خلال هذا البحث سنقوم بتحسين هذه التقنية الجديدة من حيث إمكانية استخدامها لتخزين البيانات، وتم تقديم دراسة تحليلية لمحاسنها ومساوئها في هذا السياق ومقارنتها مع قواعد البيانات العادية.

أهمية البحث وأهدافه:

1- هدف البحث:

تهدف تقنية سلاسل الكتل Blockchain إلى خلق بيئة لا مركزية حيث لا يوجد طرف ثالث يتحكم في المعاملات والبيانات [19]. بشكل عام، فإن سلسلة الكتل هي عبارة عن ختم زمني لسلسة من الكتل يتم الاحتفاظ بها بشكل مشترك من قبل جميع العقد المشاركة بتكوين السلسلة وهي شكل من أشكال نمط بيانات القوائم المترابطة Linked List. وتعتبر الكتل أساساً عبارة عن حاويات لجمع المعاملات التي تم تنفيذها. يتم ربط الكتل معاً بطريقة تشفير حيث كل كتلة يتم توقيعها رقمياً و"تقييدها" بالمجموعة السابقة بواسطة القيمة الناتجة عن تطبيق دالة التجزئة Hash Function لتلك الكتلة. يمكن أن تكون الكتل الجديدة فقط ملحقة بنهاية السلسلة، وبالتالي تقوم سلاسل الكتل بتخزين بيانات غير قابل للتغيير (لا يمكن أن تكون المعاملات الحالية محدثة أو محذوفة). لهذا السبب، تم بناء العديد من الأنظمة التي تساعد في إيجاد تقنية سلاسل كتل التوزيع الآمن للبرامج الرقمية والأصول بين العملاء غير الموثوق بهم.

2- أهمية البحث:

تم استخدام سلاسل الكتل في العديد من المجالات بسبب فوائد تخزين البيانات الموزّعة ومسارات التدقيق غير القابلة للتغيير Immutable Audit Trails. ففي مجال الرعاية الصحية، تم إدخال العديد من الأساليب في مجال السجلات الصحية الإلكترونية [3] [2] [4]. بسبب شفافية هذه التقنية فإن العديد من الحكومات والشركات حاولت تطبيقها أيضًا والاستفادة من ميزاتها [5] [6] كتطبيقات أنظمة النقد الإلكترونية، أنظمة إدارة العمليات، نظم إدارة سلاسل التوريد، المجالات الواعدة لإنترنيت الأشياء Internet of Things كما يمكن استخدام سلاسل الكتل في العديد من الطرق والسيناريوهات المحتملة ومنها إدارة الخصوصية والأمان [9] بالإضافة إلى تطوير سيناريوهات جديدة لفرص جديدة في عالم الأعمال.

3- مشكلة البحث:

استخدمت قواعد البيانات سابقا ولا تزال تستخدم على نطاق واسع في تخزين البيانات، لكن مع تطور التقنيات وازدياد

حجم البيانات وضرورة التوثيق والدقة والأمان في نقل البيانات، ظهرت تقنيات أخرى كسلاسل الكتل تستخدم في تخزين البيانات بشكل قوي وفعّال، لهذا لجأت الحكومات والمنظمات البحثية بتوفير موارد مالية كبيرة لمزيد من الأبحاث في هذا المجال، مؤخرا أعلنت المفوضية الأوروبية عن نيتها في استثمار ما يقارب من ثلاثة مليارات على المبادرات التقنية التي تركز على سلاسل الكتل [12]. ولكن هناك جدال فيما يخص عن إمكانية استخدامها كقواعد بيانات، فعلى سبيل المثال، يؤكد نارايانان Narayanan أن سلاسل الكتل الخاصة هي مجرد اسم آخر لقواعد البيانات المشتركة [13]. فيما أن غيره مثل جرينسبان Greenspan، يرى أن هناك اختلافات عديدة بين سلاسل الكتل الخاصة وقواعد بيانات SQL، بداية من بناء الثقة وانتهاءً بالمتانة robustness [13].

في حين أن سلاسل الكتل هي تقنية قوية ولكن إذا تم تطبيقها بشكل عشوائي على حالات الاستخدام دون مراعاة نقاط قوة التكنولوجيا وضعفها، فسوف نفشل في إدراك الإمكانات الحقيقية لهذه التكنولوجيا. لذلك أجرينا مراجعة تحديد النطاق [16] لفهم كيفية استخدام الباحثين المختلفين لهذه التكنولوجيا. تكشف النتائج التي توصلنا إليها أن معظم المصادر الموجودة تركّز على "كيف" تعمل التقنية، وبدرجة أقل، على "ما" التطبيقات (المحتملة) والاستخدامات التي يمكن لمؤسسات الأعمال الاستفادة منها.

السؤال الرئيسي الذي نتطرق إليه في هذا البحث هو، ما إذا كانت سلاسل الكتل تعتبر كحل جيد للمشكلات المقترحة في التخزين مقارنة مع قواعد البيانات العادية. للإجابة على السؤال أعلاه، قدمنا بما يلي:

1) لقد أجرينا مراجعة النطاق لمعرفة الاتجاه في حجم ومجالات البحث المتعلقة بسلاسل الكتل في السنوات الخمس الماضية.
2) لقد أجرينا تحليل لمقارنة تقنيات سلاسل الكتل بقواعد البيانات.
3) قمنا بتحليل أداء شبكة الإيثيريم.

4- سلاسل الكتل Blockchain:

ظهرت اليتكوين [15]، التي تم تقديمها في عام 2008، كأول عملة رقمية مستخدمة على نطاق واسع في العالم، وقد تم استخدامها في مجموعة واسعة من التطبيقات. ومن المثير للاهتمام، أنها مدعومة بآلية جديدة تسمى تقنية السجل الموزع (DLT)، والمعروفة أيضًا باسم تقنية سلاسل الكتل blockchain، والتي توفر أساسها التقني القوي. على الرغم من استخدام المصطلحين blockchain وDLT بالتبادل في كثير من المراجع، إلا أن هناك فرقاً دقيقاً بينهما يستحق تسليط الضوء عليه. تعد سلاسل الكتل مجرد مثال لنوع معين من السجل الموزع، وهناك أنواع أخرى من السجلات الموزعة. عندما يتم توزيع السجل (بما في ذلك blockchain) عبر شبكة، يمكن اعتباره سجل موزع. للتبسيط، سنستخدم المصطلحين في هذا البحث للإشارة إلى السجل الذي تم توزيعه على الشبكة[7].

حظيت سلاسل الكتل في السنوات القليلة الماضية باهتمام واسع النطاق وقد يعتبرها البعض واحدة من التقنيات الأساسية لإحداث ثورة في العديد من المجالات التطبيقية.

سلسلة الكتل هي السجل الموزع الذي يتكون من كتل متتالية مرتبطة ببعضها البعض باتباع مجموعة قوية من القواعد [11]. يتم توزيع السجل وتخزينه بواسطة عقد شبكة من نوع الند للند P2P حيث يتم إنشاء كل كتلة في فاصل زمني محدد مسبقاً بطريقة لامركزية عن طريق خوارزمية إجماع consensus algorithm. تضمن خوارزمية الإجماع العديد من الخصائص المتعلقة بسلامة البيانات (التي تمت مناقشتها أدناه) في السلسة. لسلسة الكتل العديد من

الخصائص التي تجعلها مرشحاً مناسباً للتطبيق في العديد من المجالات [8].

- **الإجماع الموزع على حالة السلسلة:** تتمثل إحدى الخصائص الأساسية لأي سلسلة كتل blockchain في قدرتها على تحقيق إجماع موزع على حالة السلسلة دون الاعتماد على أي طرف ثالث أو كيان مركزي موثوق به. هذا يفتح الباب أمام الفرص لبناء واستخدام نظام حيث يمكن التحقق من كل حالة أو تفاعل محتمل من قبل الكيانات المعتمدة.
- **ثبات حالة السلسلة وعدم رجوعها إلى حالة سابقة:** يضمن تحقيق إجماع موزع بمشاركة عدد كبير من العقد أن تصبح حالة السلسلة غير قابلة للتغيير عملياً ولا عودة فيها بعد فترة زمنية معينة. ينطبق هذا أيضاً على العقود الذكية ومن ثم تمكين نشر وتنفيذ برامج غير القابلة للتغيير [10].
- **ثبات البيانات (المعاملات):** يتم تخزين البيانات في سلسلة الكتل بطريقة موزعة لضمان ثباتها طالما أن هناك عقد مشاركة في شبكة ند للند P2P.
- **أصل البيانات:** يتم تسهيل عملية تخزين البيانات في أي سلسلة الكتل عن طريق آلية تسمى المعاملة Transaction. يجب توقيع كل معاملة رقمياً باستخدام تقنية تشفير المفتاح العام public key encryption الذي يضمن مصداقية مصدر البيانات. إن استخدام هذه الطريقة مع توفر ثبات سلسلة الكتل وعدم رجوعه أداة قوية لعدم التنصل من مصدر أي معلومة في سلسلة الكتل [11].
- **التحكم في البيانات الموزعة:** تضمن سلسلة الكتل تخزين البيانات في السلسلة بطريقة موزعة بشكل يضمن عدم وقوعها في نقطة الفشل المركزية Single Point of Failure.
- **المسؤولية والشفافية:** نظراً لأنه يمكن التحقق من حالة السلسلة، جنباً إلى جنب مع كل تفاعل فردي بين الكيانات المشاركة، من قبل أي كيان مرخص، فإنه يعزز المسؤولية والشفافية.

5- مراجعة نطاق تقنية سلاسل الكتل:

في هذه البحث إعتمدنا على المبادئ التوجيهية الموجودة عند كل من O'Malley's [16] Arksey [17] و Levac et. al.'s [18] والتي تفيد في معرفة كيفية إجراء مراجعة النطاق. والإجراءات التي تقترحها هذه التوجيهات تزيد من المنهجية والشفافية والتي بدورها تضمن مستوى عالٍ من الدقة والموثوقية.

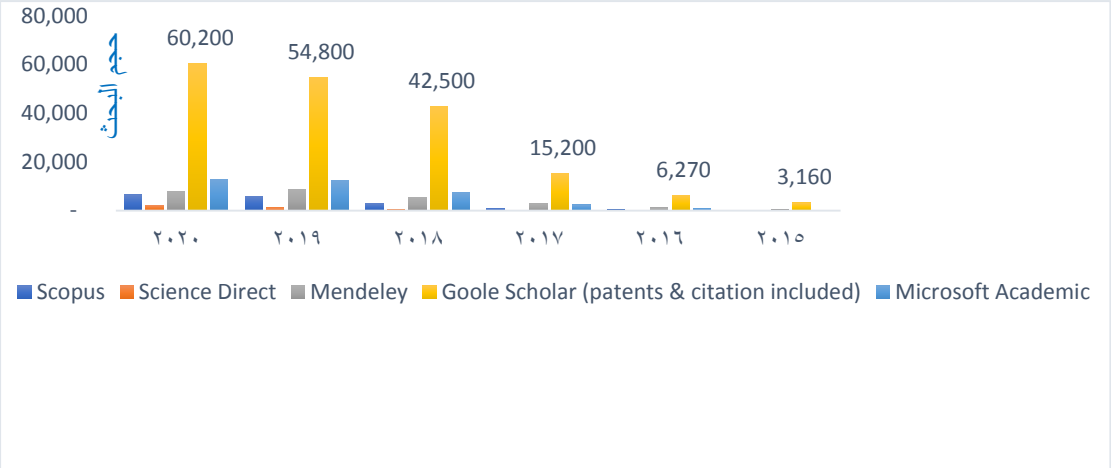
بما أن مراجعات النطاق منهجية بطبيعتها، يجب عدم الخلط بينها وبين المراجعات المنهجية التقليدية. فالمراجعات المنهجية مثل التحليلات الوصفية تحاول دمج النتائج التجريبية السابقة حول موضوع ناضج من أجل تقديم إجابات لأسئلة مثل "ما هي التقنيات التي تعمل" و "ما هي التقنيات التي تعمل بكفاءة أعلى"، تحاول مراجعات النطاق توفير مؤشر أولي حول موضوع ناشئ، لتحديد الثغرات، واقتراح جدول أعمال بحثي للأعمال المستقبلية [20]. في هذه المراجعة، حاولنا تحديد اتجاهات البحث في سلاسل الكتل وأي من المجالات التطبيقية قد حظيت باهتمام أكبر من مجتمع الأبحاث.

6- حجم واتجاه البحث:

قمنا بمسح خمس قواعد بيانات فهرسة علمية رئيسية: الباحث العلمي من Google و Scopus وScience Direct و Web of Science و Microsoft Academic. واستخدمنا "blockchain" ككلمة رئيسية للبحث في قواعد البيانات هذه. ولاحظنا ارتفاعاً حاداً في حجم البحث على مدى السنوات الخمس الماضية (الشّكل (1)).

من خلال تحليل حالات الاستخدام العامة في المجالات، حاولنا معرفة "لماذا" و "كيف" يتم استخدام سلاسل الكتل

في حالات الاستخدام هذه. وستتم مناقشة الخصائص/ المعايير المحددة بعبارات أكثر عمومية فيما بعد [14].



الشّكل (1) مراجع سلاسل الكتل

أولا – في سلاسل التوريد Supply Chain

إن إدارة سلسلة التوريد (Supply Chain Management SCM) هي إدارة تدفقات المواد والمعلومات بين المنشآت وفيما بينها من أقسام ومكونات، مثل البائعين ومعامل التصنيع والتجميع ومراكز التوزيع. يحتفظ بسجلات للتفاعلات المختلفة بين الكيانات المختلفة حتى تسليم المنتج إلى نقطة الاستهلاك النهائية[21].

تستخدم سلسلة متاجر Walmart تقنية من تقنيات سلاسل الكتل المسماة بالسجل الفائق Hyperledger الخاصة بشركة IBM لتتبع مصدر طعامهم وإمكانية التتبع الكلي لجميع المواد الموجودة على رفوف المتجر[22]. أيضا تم استخدام تقنيات مشابهة في صناعة الماس. حيث تم إنشاء مجموعة من السلاسل العامة والخاصة لتوفير التحكم المصرح به وفي نفس الوقت يوفر مسار تدقيق واضح لأصحاب المصلحة [23].

دراسة تحليلية:

• تشارك أطراف متعددة في نظام إدارة سلسلة التوريد وهناك نقص في الثقة بين الأطراف. لذلك لا يكشف اي كيان عن معلوماته لطرف آخر.

• يقوم العديد من الممارسين حالياً بحل هذه المشكلة أو تجاوزها عن طريق تقديم طرف ثالث موثوق به. يثق الطرفان "أ" و "ب" في الطرف الثالث الموثوق به ويكشفان معلوماتهما. ومع ذلك، فإن العثور على طرف ثالث موثوق به يكون خطيراً للغاية وفي كثير من الحالات "مستحيل".

• يمكن لسلاسل الكتل إنشاء الثقة بين الأطراف المتعاملة بدون طرف ثالث موثوق به [25].

ثانيا – في المجال المصرفي:

في النظام المصرفي الحالي، يمكننا إجراء مناقلات في الوقت الفعلي إذا تعاملنا مع نفس البنك. ومع ذلك، قد يستغرق الأمر 2–3 أيام عمل إذا كانت العملية بين بنكين مختلفين. يزداد الوضع سوءاً إذا كانت المناقلة دولية والتي عادة ما تتضمن بنكاً ثالثاً. تحتاج البنوك المتعاملة إلى امتلاك حساب مع هذا البنك الثالث.

نظراً لارتفاع تكاليف المناقلات نسبياً في النظام المصرفي المشترك، يهتم المصرفيون بمعرفة ما إذا كانت تقنية سلاسل الكتل يمكنها تبسيط وتقليل تكلفة المدفوعات بين المصارف.

تعمل بعض البنوك المركزية مثل سلطة النقد في سنغافورة (MAS) وبنك كندا على حلول للاستخدام تكنولوجيا السجل الموزع للمدفوعات بين البنوك [29]، [30]. تم اقتراح الريبل [24]، وهي عملة مشفرة، لتوفير شبكة تسوية عالمية تعتمد على سلاسل الكتل. لقد كان له أكبر تأثير على القطاع المصرفي التقليدي. في الواقع، هذا هو النوع الأول من العملات المشفرة الذي يسد الفجوة بين سوق العملات الافتراضية والقطاع المصرفي التقليدي.

تحليل نقدي:

• إمكانية استخدام سلاسل الكتل للدفع السريع بين البنوك.

• الأداء أمر حيوي في النظام المصرفي. لا يمكن لسلاسل الكتل في شكلها الحالي التعامل مع العدد الكبير للمناقلات في النظام المصرفي الحالي. ومع ذلك، يمكن إنشاء تحالف لتشكيل وإدارة عملة رقمية داخل تلك الشبكة. بهذه الطريقة يمكن للتحالف تحديد سعر هذه العملة لتلك الشبكة.

ثالثا – النظام الصحي:

في نظام الرعاية الصحية الحالي، يحتفظ مختلف مقدمي الخدمة بسجلات لمرضاهم وغالباً ما لا يتمكنون أو لا يشاركون بياناتهم مع مقدمي الخدمات الآخرين. البيانات الصحية لها طبيعة خصوصية عالية وغالباً ما يضطر المرضى إلى تقديم الثقة العمياء لمقدم الرعاية الصحية الخاص بهم. بالإضافة إلى ذلك، عادةً ما يستغرق الوصول إلى السجل الصحي ومشاركته الكثير من الوقت الإداري للأطباء والمرضى.

تتمثل رؤية سلاسل الكتل في نظام الرعاية الصحية في تقليل وقت المسؤول للأطباء حتى يتمكنوا من قضاء المزيد من الوقت مع مرضاهم ومشاركة البيانات بسلاسة. اقترح باحثون من معهد ماساتشوستس للتكنولوجيا نظام سجل صحي قائم على سلاسل الكتل يسمى MedRec [2] والذي يعيد معرفة المرضى ببياناتهم الطبية.

تحليل نقدي:

• الرعاية الصحية في الأساس قطاع معقد وحساس للغاية. دائماً ما يكون التكيف التكنولوجي بطيئاً جداً بسبب المتطلبات التشريعية الناظمة. ومع ذلك، فإن التشغيل البيني والتعاون مهمان للغاية في هذا القطاع لتقديم الخدمات والابتكار. يمكن استخدام هذه التقنية لتمكين التشغيل البيني والتعاون دون المساس بأمن مقدمي الرعاية الصحية.

• قد يكون تطبيق سلاسل الكتل في قطاع الصحة دون إجراء بحث دقيق واختبار قابلية الاستخدام كارثياً.

7- المقارنة بين تقنية سلاسل الكتل وقواعد البيانات:

يبين الجدول (1) الفرق بين سلاسل الكتل وقواعد البيانات التقليدية:

الجدول (1) المقارنة بين قاعدة البيانات التقليدية ومثيلتها من سلاسل الكتل

المشكلة/ المعضلة	سلاسل الكتل	قاعدة بيانات مركزية	الأفضلية
بناء الثقة	يمكن أن تعمل دون أي طرف موثوق به	بحاجة طرف مركزي للثقة به	سلاسل الكتل
السرية والخصوصية	(افتراضيًا) تتمتع جميع العقد بإمكانية رؤية البيانات	فقط الشخص المخوّل يمكنه الوصول للبيانات	قواعد البيانات المركزية
المتانة/ تحمل الأخطاء	يتم توزيع البيانات بين جميع العقد	يتم تخزين البيانات في قاعدة البيانات المركزية	سلاسل الكتل
الأداء	تستغرق وقتًا للوصول إلى توافق (على	التنفيذ / التحديث فوري	قواعد البيانات

	سبيل المثال، 5 دقائق في شبكة الإيثيريوم)		المركزية
الأمن	(افتراضيًا) يتم استخدم معايير التشفير الأشد تعقيدا حاليا Elliptic Curve Cryptography	تستخدم التحكم التقليدي في الوصول	سلاسل الكتل

أ. بناء الثقة

أحد أهم ميزات تقنية سلاسل الكتل هو الثبات. يتم تحقيق الثبات من خلال آلية التوافق اللامركزية. تشارك كل عقدة مشاركة في آلية إجماع للتحقق مما إذا كانت أي معاملة معينة صالحة أم لا. كل عقدة في النظام لها نفس مستوى الوصول والقدرة. يوفر هذا أساسًا متينًا لبناء الثقة، لأنه يضفي الطابع الديمقراطي على النظام بأكمله. في قاعدة البيانات التقليدية، يتعين علينا الاعتماد على سلطة مركزية واحدة تتحكم فيمن يمكنه فعل ما في النظام. يكون هذا النوع من النظام جيدًا عندما يكون الطرف الذي يتحكم في النظام موثوقًا به ويتصرف بأمانة [10].

ب. السرية والخصوصية

هناك فكرة خاطئة حول سلاسل الكتل وهي أن البيانات في سلاسل الكتل يتم تشفيرها. لكن هذا ليس صحيحاً. يتم توقيع البيانات رقمياً من قبل الأطراف المتعاملة ولكن غير مشفرة بشكل افتراضي. في الواقع، إن نظام السجل الموزع مفتوح، حيث يمكن لأي شخص الانضمام والتحقق من أي معاملة في الشبكة. ومع ذلك، يتم الاحتفاظ بخصوصية الأطراف المشاركة أو سريتها باستخدام تشفير المفتاح العام. تكشف المعاملات عن الأطراف المتعاملة والبيانات الموجودة في المعاملة (على سبيل المثال، مقدار العملة في حالة العملة المشفرة). في الآونة الأخيرة، يقترح الباحثون إخفاء الهوية باستخدام وسائل تشفير مثل بروتوكول المعرفة الصفرية [31].

ج. المتانة/ تحمل الأخطاء

سلسلة الكتل هي نظام لامركزي ويستخدم آلية الحوسبة الموزعة لتوفير القوة وتحمل الأخطاء Fault Tolerance. يتم تخزين البيانات على السلسلة بشكل موزع وتقوم كل عقدة مشاركة بتخزين نسخة من السلسلة. لذلك فإن هجمات مثل رفض الخدمة (DoS) ورفض الخدمة الموزع (DDoS) غير ممكنة في شبكة سلال الكتل. إذا تعطلت عقدة معينة أو تعرضت للاختراق، فلا يزال بإمكان العقد الأخرى متابعة المهمة.

د. الأداء

تعاني سلاسل الكتل وخاصة عملة البيتكوين من البطئ بشكل ملحوظ حيث يستغرق تأكيد المعاملة في الشبكة حوالي 10 دقائق. قد يصل هذا الوقت إلى 60 دقيقة إذا حدث أي انقسام بسيط [26] في الشبكة. يمكن تصميم أنظمة قواعد بيانات النظام التقليدية للتعامل مع آلاف المعاملات في الثانية. على سبيل المثال، يمكن لشبكات Visa و Mastercard معالجة 50000 معاملة في الثانية. إذا وجد مسؤول النظام عنق زجاجة الأداء، فيمكنه استبدال النظام أو إعادة تصميمه للسماح بحجم كبير من المعاملات. ومع ذلك، هناك أبحاث جارية لتحسين كفاءة آلية التوافق. يمكن لخوارزمية الإجماع مثل Ethash [27] و X13 [28] التوصل إلى إجماع في غضون 10 إلى 20 ثانية.

هـ. الأمن

يأتي أمان سلاسل جزئياً من قدرته على التكيف. كلما زاد عدد مستخدمي النظام، يمكن أن يتطلب الأمر المزيد من

المستخدمين لتحقيق الإجماع. في بروتوكول سلاسل الكتل، سيتم قبول الكتلة إذا وافقت 51% من عقد التعدين. لذلك، إذا تم التحكم في 51% من عقد التعدين بواسطة مستخدمين ضارين، فيمكن قبول "معاملة غير صالحة" على أنها "معاملات صالحة". إذا كان هناك عدد كافٍ من الأشخاص في الشبكة، فسيبدو ذلك مستحيلاً ولكن يمكن أن يحدث من ناحية نظرية. في حين إن قاعدة البيانات التقليدية، يتم الحفاظ على حالة قاعدة البيانات من خلال نظام مركزي. الوصول إلى البيانات مقيد بآلية التحكم في الوصول التي حددها ذلك النظام. يعد هذا النظام ضعيف، إذا تم اختراق مسؤول النظام نظرا لطبيعته المركزية.

8- حالات سلاسل الكتل المفيدة:

من المناقشة أعلاه، يجب أن يكون واضحاً أن تقنية سلاسل الكتل ليست تقنية للأغراض العامة ولكن يجب تطبيقها بحكمة لجني فوائدها. لكن يمكن القول بشكل عام، أنّ هذه التقنية مفيدة في حالات الاستخدام تلك حيث يوجد أكثر من سلطة إدارية وهناك نقص في الثقة بين تلك الأطراف. يمكن أن يكون أحد الأمثلة النموذجية نظام إدارة سلسلة التوريد، حيث تتعاون أطراف متعددة معاً لتسليم البضائع أو المشاريع الحكومية التي تعمل على تعزيز الثقة بين الأطراف. حاليًا، إذا كان هناك نقص في الثقة بين الأطراف المتعاونة، فعادة ما يختارون طرفاً ثالثاً موثوقاً لدى الطرفين. على سبيل المثال، يثق كل من المشتري والبائع في البنك لإجراء المعاملات المالية فيما بينهم. ومع ذلك، في بعض الأحيان يكون العثور على طرف ثالث موثوق به أمراً صعباً أو حتى خطراً.

إذا كانت جميع المعايير المذكورة أعلاه متطابقة، فيمكننا القول إن السلاسل هي تقنية مفيدة لحالة الاستخدام هذه. ومع ذلك، يتعين علينا الآن أن نقرر ما إذا كان ينبغي علينا استخدام سلاسل الكتل العامة أو الخاصة. إذا كانت القيمة المخزنة بحاجة إلى أن تكون قابلة للتحقق بشكل عام، فيجب علينا استخدام سلاسل الكتل العامة، بينما إذا كانت البيانات لأطراف معينة فقط، فإن سلاسل الكتل الخاصة هي خيار أفضل لأنها يمكن تبسيط آليات الإجماع.

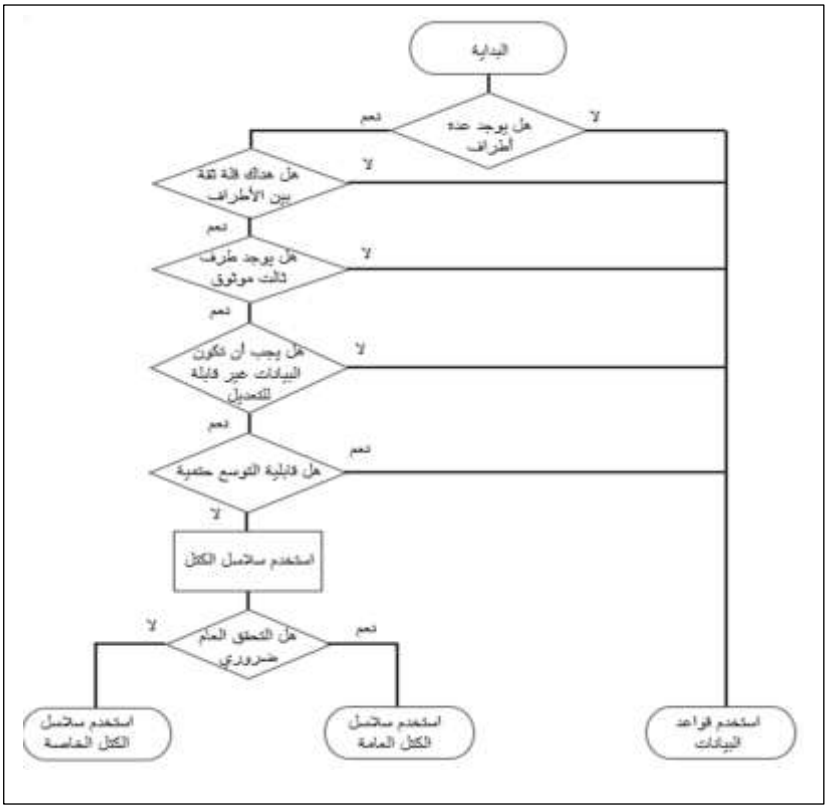
تعد سلسلة الكتل العامة غير مقيدة ولا تتطلب صلاحيات، أي يمكن لأي شخص لديه إمكانية الوصول إلى الإنترنت من تسجيل الدخول إلى منصة سلسلة كتل عامة ما ليقوم بتكوين عقدة مرخصة. يمكن لهذا المستخدم الوصول إلى السجلات الحالية والسابقة وإجراء أنشطة التعدين والحسابات المعقدة المستخدمة للتحقق من المعاملات وإضافتها إلى السجل الموزع. لا يمكن تغيير أي سجل أو معاملة صالحة على الشبكة، ويمكن لأي شخص التحقق من المعاملات أو العثور على الأخطاء أو اقتراح التغييرات لأن الرمز المصدري عادة ما يكون مفتوح المصدر.

بينما الشبكات الخاصة فهي تعمل في بيئة مقيدة مثل شبكة مغلقة، أو التي تخضع لسيطرة كيان واحد، في حين تعمل الشبكة العامة بمعنى أنها تستخدم اتصالات من نظير إلى نظير واللامركزية، إلا إن الشبكات الخاصة تكون على نطاق أصغر بكثير حيث لا يمكن لأي شخص من الانضمام وتوفير قوة الحوسبة، عادةً ما يتم تشغيل السلسة الخاصة على شبكة صغيرة داخل شركة أو مؤسسة. تُعرف أيضاً باسم سلاسل الكتل المصرح بها أو سلاسل كتل المؤسسات. وفيما يلي جدول (2) يلخص أبرز فروق هذين النوعين.

جدول (2) الفروقات بين شبكات سلاسل الكتل العامة والخاصة

	الشبكات العامة	الشبكات الخاصة
الإيجابيات	+ الاستقلالية + الشفافية + الثقة	+ الولوج المصرحAccess Control + الأداء
السلبيات	– الأداء – النمو – الأمن	– الثقة – التدقيق Auditability
حالات الاستخدام	العملات المشفرة التحقق من الوثائق	سلاسل التوريد إثبات ملكية الأصول

يوضح الشّكل (2) متى يمكن استخدام سلاسل الكتل من عدمه:

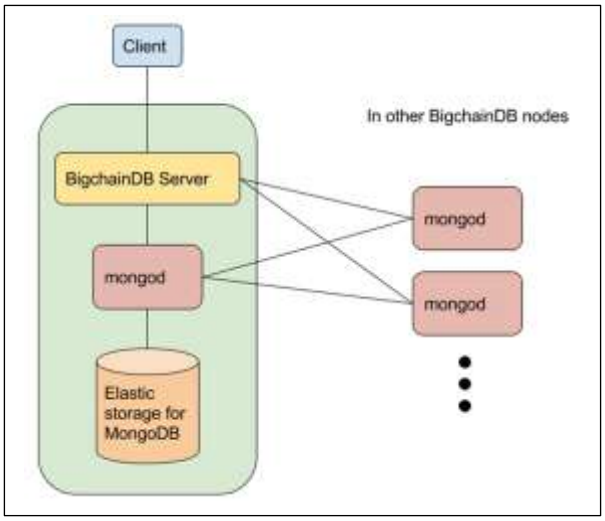


الشّكل (2) مخطط شجرة القرار لتحديد امكانية استخدام سلاسل الكتل

9- الدراسات المرجعية

تم استخدام تقنيات سلاسل الكتل و تقنيات السجل الموزع سابقاً في عدة مجالات إلا أن معظمها كان يتمحور حول الجانب الاقتصادي منها المتمثل باستخدام المحافظ الإلكترونية والعملات المشفرة و إحدى أهم الأمثلة على هذه الأنظمة هي التي قامت بإنشائه منظمة الغذاء العالمي التابعة للأمم المتحدة المسمى Building Blocks و التي قامت بتطويره عام 2017 لاستبدال توزيع المساعدات المالية بواسطة بطاقات الائتمان التقليدية [30] .

إحدى أهم الدراسات المعنية بمعالجة البيانات لأنظمة blockchain [30] تقترح اتخاذ عدد من المبادرات من منظور تخزين البيانات واسترجاعها. على سبيل المثال BigChainDB [31]، تجمع بين قدرات قواعد البيانات المستندة إلى المستندات NoSQL للاستعلامات السريعة وموثوقية Blockchain ليتم تحقيق مقاومة التلاعب من خلال النسخ المتماثل المشترك، أو منع عمليات الحذف للمناقلات والتوقيع المشفر لجميع المعاملات. ومع ذلك، يدعم BigChainDB فقط MongoDB ويفتقر إلى دعم قواعد بيانات SQL.



الشّكل(3) مكان سلاسل الكتل في المخدم والشبكة

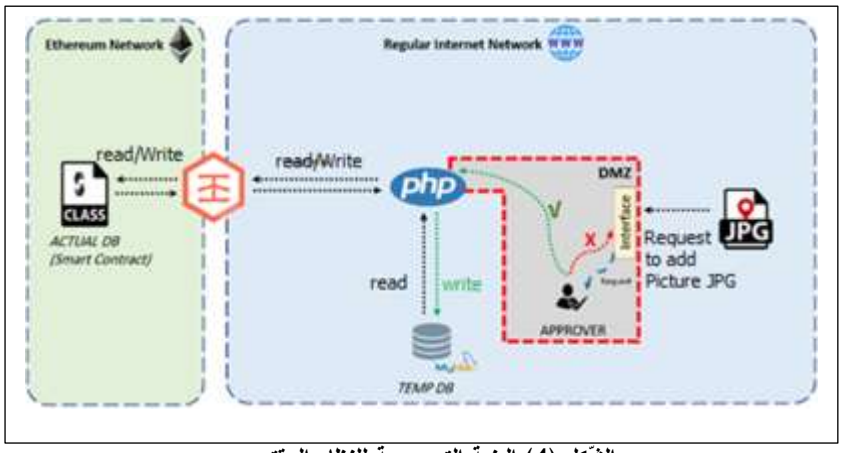
من خلال النظام المقترح الموضح لاحقاً تم اتباع طريقة مختلفة لتخزين البيانات على سلسلة كتل من نوع الإيثيريوم من خلال الاستعانة بمقدرة الإيثيريوم على توفير طبقة قابلة للبرمجة تتمثل بالعقود الذكية التي تسمح لنا بتصميم الشكل المراد من قاعدة البيانات الموزعة بالإضافة لتوفير توابع التعامل مع هذه القيم المخزنة. كما تم استخدام مزيج من سلاسل الكتل هي شبكة الإيثيريوم والعقود الذكية الخاصة بها بالإضافة إلى قاعدة بيانات علائقية من نوع MySQL على خلاف[31] التي تدعم فقط قواعد MongoDB التي هي من نمط NoSQL. ما يميز هذا النظام هو الفصل الكلي بين المكونين السابقين بحيث لا تسبب أي تعديل على البيانات بحد ذاتها وبذلك نحافظ على سلامة النظام ككل ونستفيد من ميزات سلاسل الكتل من حيث الأمان والشفافية. لتحسين الأداء ما بين سلاسل الكتل وقواعد البيانات قمنا بالسناريو الآتي:

10- التطبيق العملي وتحليل الأداء:

بعد تجهيز المعلومات الاساسية من خلال واجهة المستخدم Front End التي سيتم تخزينها لاحقاً في سلسلة الكتل بواسطة العقد الذكي، قمنا ببرمجة مخدم من نوع node.js يقوم بتهيئة بيئة التواصل ما بين سلسلة الكتل وقاعدة البيانات العلائقية حيث يقوم بالاستماع إلى port محدد. بعد تخزين المعلومات الاساسية في قاعدة البيانات، يتم استدعاء هذا المخدم لتجهيز package المعلومات وارسالها إلى سلسلة الكتل ليتم تخزينها ككتلة على السلسلة. بعد ذلك يتواصل هذا المخدم مع السلسة للحصول على العنوان الفريد للكتلة التي تم تخزينها على السلسة وتتم إضافته إلى قاعدة البيانات العلائقية.

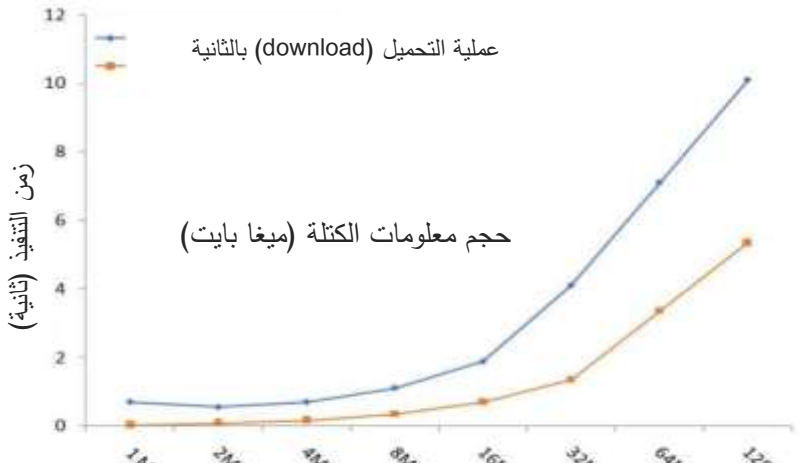
عند الحاجة لاستدعاء معلومات مخزنة على الكتلة لا داعي للانتظار لمدة طويلة للحصول على المعلومات فالعنوان مخزن مسبقاً في قاعدة البيانات العلائقية التي تمتاز بسرعة تنفيذ استعلامات استرجاع البيانات. ومن جهة أخرى نضمن صحة البيانات المخزنة على قاعدة البيانات وأنه لم يتم التلاعب بها من قبل طرف ما إذ أن عنوان الكتلة الذي يتم اضافته لا يمكن تعديله أو تعديل محتوى الكتلة من معلومات نظراً لوجود التشفير والتوقيع الرقمي وتوابع التجزئة التي تعمل على سلسة الكتل وتضمن عدم التلاعب بمحتوى المعلومات.

سنقوم بعرض النتائج التي تم الوصول إليها عن طريق تطوير نظام يقوم بتخزين معلومات نصية متمثلة ببعض الواصفات المتعلقة بإحداثيات موقع جغرافي ما والتي يقوم الموقع باستخراجها من صورة رقمية موسومة بإحداثيات مكان التقاطها بمساعدة حساس نظام التموضع العالمي GPS المدمج في معظم أجهزة المحمول الذكية. يتم تجميع بيانات المستخدمين على شكل اغراض Objects ومن ثم استخدام مكتبة Caliper التي توفر طرق لقياس متحولات أداء سلسلة الكتل هذه على المراحل التي تمر بها:



الشّكل (4) البنية التصميمية للنظام المقترح

سنقوم بعرض النتائج الآتية التي تم الوصول إليها بعد تجميع بيانات المستخدمين على شكل اغراض Objects ومن ثم استخدام مكتبة Caliper التى توفر طرق لقياس متحولات أداء سلسلة الكتل هذه على المراحل التي تمر بها:



الشّكل (5) زمن تنفيذ رفع وتحميل الكتلة

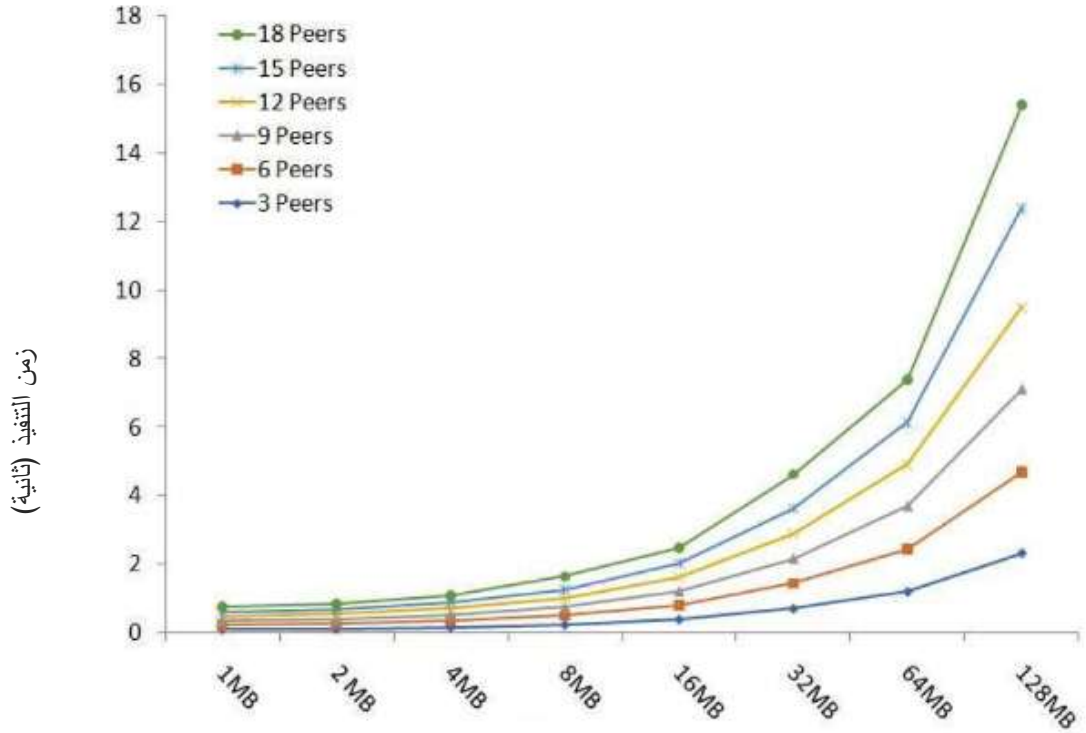
أولا: مرحلة رفع البيانات ومشاركتها مع بقية العقد:

يتم في هذه المرحلة تجميع المعلومات التي يجب مشاركتها على شكل غرض ويتم رفعها على شبكة سلسلة الكتل والتي كانت في حالتنا عبارة عن معلومات نصية تم رفعها على شبكة رينكبي Rinkeby إحدى شبكات اختبار سلاسل الكتل عوضاً عن الشبكة النشطة. من خلال الشّكل (5) نلاحظ أنه تم اختبار عدة كتل بأحجام مختلفة ولاحظنا أن عملية رفع هذه الكتل يتطلب مجهود حوسبي أكبر مما يتطلبه عملية تحميل هذه الكتل عند بقية العقد.

ثانياً: مرحلة التنقيب:

في هذه المرحلة يتم تطبيق خوارزمية الإجماع للتأكد من صحة الكتلة قبل إضافتها إلى السلسلة ككتلة جديدة. خلال مرحلة التنقيب يتم خلق الكتلة الجديدة التي تحوي المعلومات التي يحتويها الغرض من المرحلة السابقة، ونلاحظ ايضا أن هذه العمليه تتعلق بحجم الكتلة المراد إنشاؤها بل وإن عملية التنقيب تستغرق وقتاً أطول من عملية إنشاء الكتلة الجديدة.

عند إنشاء كتلة جديدة فإننا نقوم بتطبيق تابع التجزئة الذي تعتمده السلسلة والذي هو في حالة شبكة الإثيريم تابع SHA-256 بالإضافة إلى تضمين معرف زمني Timestamp. الشّكل (6) يوضح الوقت المستغرق حتى تصبح الكتلة الجديدة قابلة للوصول من بقية الأنداد المشاركين بالسلسلة وكمية الوقت المستغرق تتناسب طردياً مع حجم الكتلة المضافة وعدد الأنداد Peers الذين يستخدمونها.



الشّكل (6) زمن تنفيذ عملية الوصول للكتل بحسب حجم الكتلة وعدد الأنداد

نستنتج مما سبق أن سلاسل الكتل تمر أولاً بمرحلة تجميع المعلومات وتحويلها إلى سلاسل كتل ثم التأكد من صحة الكتلة قبل إضافتها إلى السلسلة ككتلة جديدة، ثم تبدأ مرحلة التنقيب والتي فيها يتم خلق الكتلة الجديدة ثم تطبيق تابع التجزئة عيها ووضعها في مكانها المخصص، ومن ثم تصبح الكتلة الجديدة قابلة للوصول.

الخاتمة:

هناك الكثير من أنظمة سلاسل الكتل وعلى الرغم من عدم ثبات معظمها فإن هناك عدة أنظمة وصلت إلى مستوى عالٍ من الثبات ولديها قاعدة مستخدمين ضخمة. تم في هذا البحث سبر المجالات المستقبلية لهذه التقنية، والقيام بتحليل نقدي لهذه المجالات وتم مقارنتها مع تقنيات قواعد البيانات التقليدية ووجدنا أنه إذا كان العامل الأهم من الناحية التصميمية هو بناء الثقة وشفافية المعلومات ومتانتها فإن سلاسل الكتل هو الخيار الأمثل. بينما في حال الأداء فإن قواعد البيانات التقليدية لا تزال هي الحل الأفضل علماً انه يوجد حلول يمكن أن يكون لها دوراً فعالاً في تحسين أداء سلاسل الكتل في المستقبل القريب. لم يتم التطرق في هذا البحث على أداء سرعة تنفيذ العمليات وحجوم البيانات المستخدمة، وتركنا البابا مفتوحاً لأبحاث أخرى في هذا الخصوص بعون الله.

References:

[1] Wust, K. G, Do you need a blockchain? IACR Cryptology ePrint Archive, A 2017 375p.

[2] Azaria, A. Ekblaw, A. Vieira. T, Using blockchain for medical data access and permission management. IEEE InOpen and Big Data International Conference, Lippman A 2016 - Medrec.

[3] Dubovitskaya A. Xu Z. Ryu S. Schumacher M, Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annual Symposium, Wang F 2017.

[4] Yang H. A Blockchain-based Approach to the Secure Sharing of Healthcare Data. Wiley Online Library, Norway, B 2019.

[5] Tian, F. An agri-food supply chain traceability system for China based on RFID and blockchain technology, IEEE 13th International Conference on 2016 (pp. 1-6).

[6] lnes, S. Beyond bitcoin enabling smart government using blockchain technology., S 2016 (pp. 253-264).

[7] Garca, B. L, Ponomarev A, Dumas M, Optimized execution of business processes on blockchain. Springer International Conference on Business Process Management Weber I 2017, (pp. 130-146).

[8] Samaniego M. Blockchain as a Service for IoT, 2016 IEEE International Conference, Deters R 2016 (pp. 433-436).

[9] Dorri, A. Kanhere S, Jurdak R, Gauravaram Blockchain for IoT security and privacy: The case study of a smart home, IEEE International Conference on 2017 Mar 13 (pp. 618-623).

[10] Turkanovi, M. Hlbl, M. Koi, K. Heriko, M. EduCTX: A blockchain-based higher education credit platform, IEEE Access Kamiali A 2018.

[11] ROBERT, M, S. A timeline and history of blockchain technology, Vol 93 No.1, Newyork, 2021, 243.

[12] EU Government Pegs BLockchain, https://www.coindesk.com/ eu-government-pegs-blockchain-beneficiary-e30-billion-research-fund/

[13] Private blockchain is just a confusing name for a shared database, https://freedom-to-tinker.com/2015/09/18/ private-blockchain-is-just-a-confusing-name-for-a-shared-database/

[14] Blockchains vs centralized databases,https://www.multichain.com/blog/ 2016/03/blockchains-vs-centralized-databases/

[15] Bhme, R. Christin, N. Edelman, B, Bitcoin: Economics, technology, and governance, Journal of Economic Perspectives. Moore T 2015, Vol 29 No.2, (pp.83-213).

[16] Collomb, A. Sok, K. Blockchain: Distributed Ledger Technology (DLT): What

Impact on the Financial Sector? Digiworld Economic Journal. 2016, No.103 pp.93.
[17] Dennis, R. Owen G. Rep on the block: A next generation reputation system based on the blockchain. 2015 10th IEEE International Conference for Internet Technology and Secured Transactions pp. 131-138
[18] Dennis, R. Owenson, G. Rep on the Roll: A Peer to Peer Reputation System Based on a Rolling Blockchain. International Journal for Digital Society. 2016, Vol. 7, No. 1 pp. 1123-1134.
[19] Pilkington, M. Blockchain technology: principles and applications. Edward Elgar Publishing, United Kingdom, 2016, pp.480.
[20] Li, Y. Marier, B. Perron, B. A. Blockchain Technology in Business Organizations: A Scoping Review. Par G 2018 NO.89 PP.54.
[21] E.coli break out, https://en.wikipedia.org/wiki/2006 North American E. coli O157:H7 outbreak in spinach
[22] Walton Food Safety, https://tinyurl.com/ybu9xff7
[23] Everledger, https://www.everledger.io/
[24] Riple, https://ripple.com/files/ripple consensus whitepaper.pdf
[25] PRIMA, V.D, FILIPP, M.M, WESSEL, R. E, Blockchain as a confidence machine: The problem of trust & challenges of governance, India, Vol 23,2020,320.
[26] Lin. I, Liao, T. A Survey of Blockchain Security Issues and Challenges. IJ Network Security. 2017, vol 19 pp.9-653.
[27] Mukhopadhyay, U. Skjellum, A. Hambolu, O. Oakley, J. A brief survey of cryptocurrency systems. InPrivacy, Security and Trust (PST), 2016 14th Annual Conference on 2016 Dec 12 (pp. 745-752). IEEE.
[28] Rabah K 2017, Overview of Blockchain as the Engine of the 4th Industrial Revolution. Mara Research Journal of Business and Management pp.35-125.
[29] http://www.mas.gov.sg/News-and-Publications/Media-Releases, 2018.
[30] Carolyn, A. Fintech and the financial ecosystem: Evolution or revolution?, 2018.
[31] Fortnow, L. The complexity of perfect zero-knowledge- Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing. Association for Computing Machinery, USA 1987, pp 6.