دراسة سلسلة الكتل وإمكانية استخدامها في التحقق من ملكية المفتاح العام في إرسال رسائل معماة

طالب الماجستير: م .محمد خليل

المعهد العالي للعلوم التطبيقية والتكنولوجيا

اشراف الدكتور: محمد الشايطة + د. محمد عصورة

ملخص البحث:

نظرا لتزايد استخدام الشبكات في الوقت الحاضر والحاجة الكبيرة لنقل البيانات من خلالها، ظهرت العديد من التهديدات التي تواجه أمن وسلامة هذه التناقلات وبالمقابل أصبحت طرق التعمية القديمة أكثر هشاشة في مواجهة المخترقين وأبرزها البنية التحتية للمفاتيح العامة PKI التي تبنى عليها الكثير من تطبيقات الويب مثل(Https، S/MIME) وأبرز هذه المشاكل هي المركزية والبنية المعقدة في توزيع الشهادات، لذلك ظهرت الحاجة إلى البحث عن بدائل وآليات جديدة تلبي احتياجات المستخدمين لضمان الأمن والخصوصية.

تعد تقنية سلسلة الكتل من أكثر التقنيات الواعدة التي تتمتع بمزايا أمنية كبيرة ولامركزية في بنية الشبكة، ومن هنا قمنا بإنشاء نموذج بديل عن PKI بالاعتماد على تقنية سلسلة الكتل وخوارزميات التعمية غير المتناظرة وتوظيفها في تطبيق إرسال رسائل معماة بالمفتاح العام، حيث يقوم التطبيق بتسجيل مستخدمين جدد، وقبل إرسال أي رسالة يتم التحقق من ملكية المفتاح العام للمستقبل من سلسلة الكتل في شبكة Ethereum Blockchain، وتطرقنا أيضا إلى حل مشكلة الشهادات الملغاة مثلاً في Https التي تأخذ وقت طويل من أجل تعميم الشهادة الملغاة لكافة المستخدمين والمتصفحات، وذلك من خلال استخدام توابع الحذف في العقد الذكي المرفوع على سلسلة الكتل في

Ethereum والتي توفر لنا بيئة مناسبة لاختبار التطبيقات اللامركزية القائمة على سلسلة الكتل.

الكلمات المفتاحية: البنية التحتية للمفاتيح العامة، المرجع المصدق، سلسلة الكتل، خوارزمية التعمية غير المتناظرة.

Study of the blockchain and its potential use in verifying ownership of the public key in sending encrypted messages

Paper Research of Master Thesis

Eng. Mohammad khalil
Dr. Mohammed Alchaita
Dr. Mohammad Assoura

Abstract:

These days, the use of networks and the transfer of data is increasing, many threats of security and safety for these transmissions have appeared. On the other side, old encryption methods have become weaker for hackers. PKI (public key Infrastructure) is a technology used in web applications to make trust between parties. But there are some problems in the PKI like the central and the complex structure in the distributed certificates. Therefore, it became necessary searching for alternatives and new mechanisms ensure the users' security and privacy. Blockchain technology is one of the most promising technologies; it has terrific security advantages and decentralization network structure. Therefore, we created an alternative model for PKI based on blockchain technology, then employed it in an application for sending encrypted messages, which use asymmetric cryptography algorithms. The application registers new users and generates a public and private key for them, then before sending any message it verifies the owner of the receiver's public key from the Ethereum blockchain. We also worked on solving the problem of revoked certificates. For example, on Https, it takes a long time for publishing the revoked certificate to all users and browsers, we solved this issue by using the deletion methods in the smart contract which uploaded to the Ethereum blockchain. Then, we evaluated the security, functionality, and performance of our model, and compared the time between getting and revoking certificates in Https. The results showed a simple way of registering users,

ensuring that the public key is not either changed or stolen and canceled the central structure in PKI. We also got a speed in performance and solved the revoked certificates problems fast and efficiently during about 1 min.

Keywords: Public key infrastructure, certification authority, blockchain, asymmetric cryptography algorithm

1. مقدمة

في الوقت الحاضر، تعد المراسلة الإلكترونية أكثر تطبيقات الشبكة استخدامًا، لذلك لابد من تلبية المتطلبات الأمنية والخصوصية لأطراف المراسلة ومن أكثر الأساليب المستخدمة لذلك بروتوكولات تعمية البريد الإلكتروني S/MIME وبرنامج التعمية Pretty Good Privacy (PGP) التي توفر السرية مع التعمية والمصادقة عبر التوقيع وشبكة الثقة عبر التحقق من هوية أطراف المراسلة وتستخدم أيضاً بروتوكولات تعمية الاتصال بين الخادم والزبون SSL .

وتعتمد جميع هذه البروتوكولات والبرامج على البنية التحتية للمفتاح العام PKI، ولكنها في الواقع تواجه تهديدات أمنية متعددة، مثل هجوم MITM وهجوم EFAIL.

تعتبر البنية التحتية للمفتاح العام (PKI) مكونًا مهمًا لتأسيس المصادقة في الشبكات، وتوفر ضمانات للثقة في الشهادة الموقعة من المرجع المصدق (CA).

تصادق الشهادات على المفاتيح العامة وتسمح بإجراء عمليات التعمية مثل تعمية البيانات والتوقيع الرقمي، ولكن المصادقة والتحقق من الهوية مركزيان في البنية التحتية للمفتاح العام، مما يخلق إمكانية لفشل النقطة الواحدة.

سلسلة الكتل هي تقنية مبتكرة تتغلب على هذه التهديدات وتسمح بتطبيق اللامركزية على العمليات الحساسة مع الحفاظ على مستوى عال من الأمان، حيث يلغي الحاجة إلى وسطاء موثوق بهم، ويمكن لجميع عقد الشبكة الوصول إلى سلسلة الكتل وتتبع جميع المعاملات التي يتم إجراؤها.

سلسلة الكتل من شأنها أن تجعل المراسلات أكثر أمانا، ونقترح تصميم نموذج للمراسلة مع الحفاظ على أمن البيانات المسجلة على سلسلة الكتل، وذلك باستخدام عقد ذكي للتحقق من الهويات القائمة على نظام لا مركزي بالكامل يسمح للمستخدمين بتبادل الرسائل بأمان.

تم التصميم باستخدام تقنية سلسلة الكتل لجعل العملية أكثر وثوقية، وتعد تقنية سلسلة الكتل حلاً لتحقيق تكامل البيانات، وبالاعتماد على بنية الشبكة اللامركزية وآلية عمل سلسلة الكتل نحصل على مقاومة للتعديل والتزوير مما يحقق تناقل بيانات بشكل آمن وسليم.

إن تقنية سلسلة الكتل لامركزية، ولا يمكن لأي سلطة مركزية الموافقة على المعاملات بطريقة فردية، وإنما يجب أن تتوصل جميع العقد في الشبكة إلى إجماع للتحقق من صحة المعاملات بطريقة آمنة، ولا يمكن تغيير السجلات السابقة. وإذا أراد شخص ما تغيير السجلات السابقة يجب إنفاق تكلفة عالية جدًا حيث يتعين عليه الوصول إلى 51% من أجهزة الكمبيوتر في الشبكة التي تستضيف قاعدة بيانات سلسلة الكتل في نفس الوقت للتعامل معها، وهو أمر مستحيل عمليا[1].

تم إنشاء عملة البيتكوين (bitcoin) المعماة من قبل شخص غير معروف باستخدام الاسم المستعار Satoshi Nakamoto في عام 2008، تقوم Bitcoin بإنشاء

المعاملات وإرسالها إلى سلسلة الكتل بمجرد التحقق من صحة عملية النقل، يتم نشر المعاملات من خلال الشبكة وإضافتها إلى كتلة وبمجرد امتلاء الكتلة يتم إلحاق الكتلة بسلسلة الكتل عن طريق إجراء عملية تنقيب.

تحاول العقدة المنقبة حل لغز تعمية صعب عن طريق عملية تسمى Proof of Work (PoW)، وتضيف العقدة التي تحل اللغز أولاً الكتلة الجديدة إلى سلسلة الكتل، تعتمد Bitcoinعلى الثقة اللامركزية، ويتم تحقيق الثقة كخاصية ناتجة عن تفاعلات المشاركين المختلفين في نظام البيتكوين [2] ولا يمكن اختراق البيانات المخزنة على سلسلة الكتل أو تعديلها أو حذفها، ويكون ثبات البيانات في سلسلة الكتل أقوى عندما تكون السلسلة أطول[3].

2. الهدف من البحث

تدور مسألة البحث حول موضوع إيجاد بديل آمن وغير مركزي للبنية التحتية للمفتاح العام واستخدامها في إرسال الرسائل بطريقة آمنة بحيث نبحث عن آلية يتم فيها تسجيل المفتاح العام والتحقق منه بكل شفافية وأمان بالسرعة والأداء المطلوبين وذلك باستخدام تقنية سلسلة الكتل، بحيث نجيب عن الأسئلة التالية:

هل تستطيع تقنية سلسلة الكتل حل مشاكل PKI وأن تكون بديلة عنها في إرسال الرسائل؟

في سلسلة الكتل، البيانات المشتركة هي كل عملية نقل تمت على الشبكة، يتم تخزينها في دفتر الأستاذ الموزع في نسخ متعددة على شبكة من أجهزة الكمبيوتر تسمى العقد في كل مرة يقوم شخص ما بإرسال عملية نقل إلى دفتر الأستاذ، يتم التحقق من العقد للتأكد من صلاحية عملية النقل ويتم إنشاء عملية النقل في هيكل البيانات المتسلسل لسلسلة الكتل و تسجيل طابع زمني جديد في نفس الوقت، ولن يسمح بعد ذلك بأي تعديل لعملية نقل تمت من قبل.

كيف تستطيع تقنية سلسلة الكتل حل مشاكل PKI في إرسال الرسائل ؟

سوف نقوم بعمل تطبيق وبناء عقد ذكي على شبكة Ethereum public blockchain وندرس خصائص النموذج المقترح ومعاملاته وأدائه من حيث معالجته لمشاكل PKI ومدى وثوقيته لاعتماده كحل بديل عن المرجع المصدق(Certificate Authority) CA.

3. مساهمة البحث

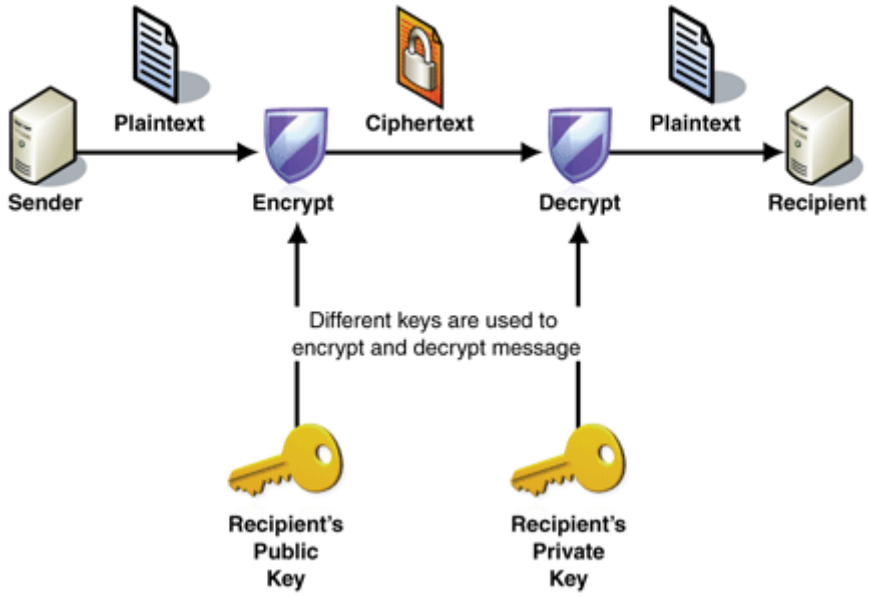
يمكننا تفنيد هذه المساهمة كما يلي:

- ❖ تصميم نموذج بديل عن PKI من حيث الوظيفة يستخدم الشبكات اللامركزية.
- ❖ تحقيق نسبة أمان عالية باستخدام سلسلة الكتل بالتحقق من ملكية المفتاح العام.
- ❖ دراسة وتصميم نموذج لتسجيل المفتاح العام للمستخدمين والتحقق منه بطريقة سريعة وباستخدام Ethereum blockchain.
- ❖ بناء تطبيق ارسال رسائل بطريقة معماة تستخدم سلسلة الكتل لتسجيل المفاتيح العامة والتحقق من ملكيتها.
- ❖ إيجاد حل سريع وفعال لإلغاء تسجيل المستخدم باستخدام سلسلة الكتل الموافق لإلغاء الشهادة في مقدمة عامة عن البنية التحتية للمفتاح العام (PKI).

4. مفهوم البنية التحتية للمفتاح العام (PKI)

PKI هو اختصار لـ Public Key Infrastructure هي تقنية لمصادقة المستخدمين والأجهزة في العالم الرقمي، والفكرة الأساسية هي أن يكون هناك طرف واحد أو أكثر من الأطراف الموثوقة يوقع رقميًا على المستندات التي تثبت أن مفتاح عام معين ينتمي إلى مستخدم أو جهاز معين، يمكن بعد ذلك استخدام المفتاح كهوية للمستخدم في الشبكات الرقمية.

وقد تم تطوير PKI لدعم تعمية المفتاح العام (غير المتناظر)، وفي هذا النوع من التعمية تتم تعمية الرسالة من قبل المرسل باستخدام المفتاح العام للمستقبل، ومن ثم يكون هذا المستقبل هو الوحيد الذي يمكنه فك تعمية هذه الرسالة باستخدام المفتاح الخاص به كما يوضح الشكل (4–1)، تم تقديم هذه الطريقة في التعمية منذ عام 1976 في [4] لحل مشكلة إدارة المفاتيح، باستخدام دليل يسمى الملف العام حيث تكون الإدخالات عبارة عن الاسم والرقم والمفتاح العام، يبحث المرسل عن المستلم في الملف العام باسمه للعثور على مفتاحه العام، وفقًا لهذا السيناريو لا يتمتع المرسل بالثقة الكاملة في أن المفتاح



الشكل (4-1) تعمية رسالة بالاعتماد على PKI

ينتمي حقًا إلى المستلم المطلوب، اقترح Kohnfelder في [5] حلاً عن طريق الشهادة أو التوقيع الرقمي على كل إدخال في "الملف العام"، بحيث يمكن توزيع الشهادات من خلال الشبكة بشكل آمن.

في الثمانينيات قرر الاتحاد الدولي للاتصالات (ITU) إنشاء دليل أكبر لتغطية جميع الأشخاص والأجهزة في جميع أنحاء العالم، وبالتالي كانت النتيجة معيارًا يسمى X.500 ويحدد [6] جميع خصائص هذا المعيار، تم اقتراح معيار آخر يسمى X.509 لأغراض المصادقة، ولا يمكن لأي شخص تغيير أي إدخال في الدليل إلا إذا كان لديه إذن، يحدد معيار X.509 تنسيق الشهادة حيث يربط هوية صاحب المفتاح بالمفتاح العام.

أدت جميع التطورات في مجال تعمية المفتاح العام إلى إنشاء بنية تحتية للمفتاح العام (PKI) حيث تلعب الشهادات الرقمية دورا جوهريا فيها، ولمزيد من الوثوقية تم تقديم المرجع المصدق (CA) [7]، وهو طرف موثوق به مسؤول عن التحقق من الشهادات

والتوقيع عليها لذلك ساعد PKI المرسل على استرداد المفتاح العام للمستلم المطلوب مع الثقة في أن هذا المفتاح هو بالفعل المفتاح العام للمستلم.

5. أبرز مشاكل PKI

لنفترض مثلاً أن مستخدم A يريد أن يرسل إلى B رسالة "دعنا نتحدث"، يتولد زوجين من مفاتيح التعمية غير المتناظرة خاصة PrA و PbA عامة.

يقول A: "مرحبا أنا A هذا هو مفتاحي العام، وهذه هي خوارزمية التعمية المتناظرة التي أعرفها"، ينشئ B مفتاحًا متماثلا S، يعميه بالمفتاح العام لـ A PbA(S) والآن لا يمكن فك تعمية S حتى بواسطة B، لأن A فقط يمكنه فك تعمية الرسالة بمفتاحه الخاص، في النهاية لدى B و A مفتاح متماثل لنقل موثوق للرسائل بينهما ومنع أي شخص من قراءة مراسلاتهما.

يتبين لدينا ثلاث وظائف رئيسية لبروتوكول SSL (المصادقة والتعمية والنزاهة)، والأهم هو المصادقة.

و لكن كيف ل A وB التأكد من عدم وجود شخص في المنتصف يمكنه قراءة رسائلهما بحيث ينشئ زوج المفاتيح الخاص به، ويعطي ل B مفتاحه على أنه المفترض من A، وينظم قناتين معماتين ويقرأ الرسائل.

يتم حل هذه المشكلة فقط بالإستعانة بطرف ثالث يسمى CA (Certificate Authority) يمكن أن يضمن أن مفتاح PbA ينتمي إلى A ويحتفظ بسجل المفاتيح العامة للجميع، يستطيع A أن يأخذ مفتاحه العام PbA ويسجله في CA، عندما يتلقىB المفتاح العام من A، يمكنه الذهاب إلى CA والتحقق من ملكية A للمفتاح إذا لم يتطابق المفتاح فهناك شخص في الوسط.

ولكن من غير المريح أن يذهب B إلى CA في كل مرة، لذلك يمكن إجراء المصادقة نفسها مع إدارة وسيطة تأخذ صلاحياتها من CA.

لدى المرجع المصدق (CA) زوج مفاتيح Pb0 وPr0 عندما يأتي A بمفتاحه العام تُصدر CA شيئًا مثل البطاقة التي تقول إنه A، وتحوي المفتاح العام PbA وبعض المعلومات الإضافية (مثل رقم الهوية) وتضيف حقلاً لتوقيعها.

يأخذ CA جميع المعلومات من البطاقة، ويجزئها، ويعميها بمفتاحه الخاص، ويطلق عليها توقيعًا رقميًا.

وتطلق CA الآن على هذه البطاقة شهادة، الآن يمكن ل A تبادل الرسائل مع B ليس فقط الاسم والمفتاح العام ولكن أيضًا شهادته.

سيضطر B للذهاب إلى CA مرة واحدة فقط، ويطلب منهم مفتاحهم العام، تعتبر أي معلومات يمكن لهذا المفتاح فك تعميتها بمثابة معلومات تمت تعميتها من قبل CA، والآن لا يمكن لشخص في المنتصف قراءة الرسائل إلا في حال التقاط المفتاح الخاص بالمرجع CA.

فيجب على كل مستخدم إضافة مفاتيح مراكز التصديق الأخرى إلى قائمته الموثوقة، ويبدأ بالاحتفاظ بسجله من المفاتيح العامة لمراكز التصديق، تصبح المنظمات التي توقع الشهادات كبيرة جدا يتم وصفها في تسلسل هرمي.

المرجع المصدق الجذري RCA لا يوقع على شهادات المستخدمين العاديين، ولكنه يوقع فقط على شهادات مراجع التصديق المتوسطة بعد التحقق منها [8]، يكفي أن يحتفظ B فقط بالمفاتيح العامة لمراكز التصديق، ولا يحصل من A على شهادته فحسب بل أيضًا على شهادات المراكز المتوسطة، بحيث يمكن فحصها حتى مركز الجذر.

مما سبق نجد أن النظام أصبح أكثر تعقيدًا ومركزية، ويكون أمام الشخص في المنتصف فرصة لقراءة الرسائل.

يكون لدى B قائمة صغيرة بمراكز تصديق الشهادات يحوي Windows حوالي 50 مركزًا لتصديق الشهادات أثناء التثبيت، وأيضاً من الصعب عليه اتباع سلسلة مراكز التصديق بأكملها في كل مرة.

يثق B في قائمته لمراكز التصديق بنسبة 99.9 في المائة، يمكن للشخص في المنتصف عن طريق استخدام إحدى الطرق (الهندسة الاجتماعية ، القرصنة ،الاختراق) تسجيل مركز تصديق شهادة مزيف خاص به في سجل B.

قد لا تكون سلطة الشخص في المنتصف كافية للتزوير من مراكز إصدار الشهادات الجذرية، ولكن يوجد طريقة أسهل حيث يذهب إلى مركز تصديق أدنى مستوى وفق التسلسل الهرمي لمراكز التصديق ، ويرشي الإدارة لتوقيع شهادته كشهادة وسيطة مصدقة، عندها يمكنه أن يرى حركة المرور والتعديل عليها، و لن يلاحظ المستخدم أي شيء، فالمتصفح لا يظهر أي تحذيرات.

ويوجد أيضا مشكلة معروفة إذا تم العثور على هذه الشهادات المزيفة ومراكز الوسط والجذر المخترقة، فيجب وضع علامة على هذه الشهادات على أنه تم إبطالها واختراقها (الشهادات المبطلة)، وتقوم بذلك سلطة التسجيل RA بشكل أساسي، وتكون RA مسؤولة عن قبول طلبات الشهادات الرقمية والتحقق من هوية الذي يقدم الطلب [9]،

هذا يعني أنه بالإضافة إلى تخزين شهادات الجذر، يحتاج المستخدم أيضًا إلى مزامنتها باستمرار مع قائمة الشهادات المبطلة عبر الإنترنت، يتم تنفيذ هذه الآلية من خلال بروتوكولات CRL (Certificate Revocation List)[10].

المشكلة في الشهادات الملغاة هي أن هناك بالفعل عددًا كبيرًا منها، في عام 2013 كان هناك حوالي 3 ملايين شهادة ملغاة [11]، و23000 شهادة ملغاة من سيمانتيك فقط في 2018 [12].

عطل Chrome الميزة الافتراضية للتحقق من صحة الشهادات الباطلة بالكامل قبل بضع سنوات [13] لزيادة سرعة تحميل الصفحات، ويتضح أنه إذا تم العثور على الشخص المهاجم لدينا، فإن عملية منع أفعاله ستكون طويلة ولن تكون ناجحة دائمًا.

مما سبق يتضح لدينا أبرز المشاكل لبنية PKI:

- يوجد مركزية في النظام من خلال مفهوم مراكز تصديق الشهادات CA.
- مراجع التصديق المتوسطة كثيرة وغير معروفة وبالتالي يمكن اختراقها.

- صعوبة معرفة وتمييز الشهادات الملغاة وطول المدة الزمنية لتعميمها.

6. حلول مقترحة لمشاكل PKI

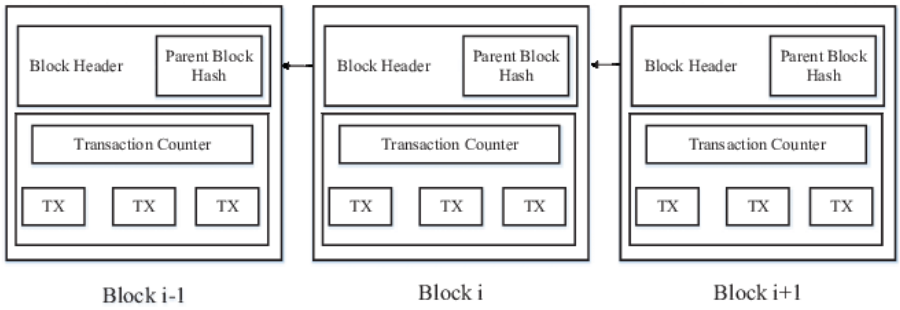
نقترح الإستفادة من تقنية سلسلة الكتل blockchain لما تتمتع من خصائص مميزة وأبرزها أنها لا مركزية، ولا يمكن لأي سلطة الموافقة على المعاملات بشكل فردي، ويجب أن تتوصل جميع العقد في الشبكة إلى إجماع للتحقق من صحة المعاملات بطريقة آمنة، ولا يمكن تغيير السجلات السابقة.

و إذا أراد شخص ما تغيير السجلات السابقة يجب إنفاق تكلفة عالية جدًا حيث يتعين على المهاجمين الوصول إلى 51% من العقد في الشبكة التي تستضيف قاعدة بيانات سلسلة الكتل في نفس الوقت للتعامل معها، وهو أمر مستحيل عمليا.

حيث أثبتت تقنية سلسلة الكتل نجاحا من خلال استخدامها في العملة الرقمية لBitcoin ونقترح في هذا البحث تصميم نموذج بديل عن PKI من خلال سلسلة الكتل وذلك بإنشاء نموذج نتمكن من خلاله من تسجيل وتأكيد هوية المفتاح العام بالتواصل مع شبكة سلسلة الكتل.

7. مفهوم سلسلة الكتل

قواعد بيانات موزعة تُنشئ قائمة مرتبة زمنيًا من السجلات وعمليات النقل المرتبطة ببعضها البعض بطريقة ثابتة عبر سلسلة من الكتل [14] تشكل هذه الكتل سلسلة خطية حيث تحتوي كل كتلة على قيمة تهشير الكتلة السابقة لإنتاج سلسلة من الكتل المترابطة الشكل (7−1)، وجميع سلاسل الكتل يتم الاحتفاظ بها في شبكة من العقد، تقوم كل عقدة بتنفيذ وتسجيل نفس المعاملات لديها وهي قادرة على قراءة أي معاملة تمر عبر الشبكة.



الشكل (7-1) بنية سلسلة الكتل

لا تعتبر سلسلة الكتل تقنية مستقلة، ولكنها تحتوي على تعمية ورياضيات وخوارزميات، تقوم شبكات الند للند بتجميع واستخدام خوارزميات المطابقة الموزعة لحل المشكلات التقليدية لمزامنة قواعد البيانات الموزعة فهي تعتبر بنية تحتية متكاملة ذات مجالات متعددة[15].

8. أهم ميزات سلسلة الكتل

تتمتع سلسلة الكتل بمزايا عديدة [16] أضافت نسبة عالية من الأمان والوثوقية للشبكات ومنها:

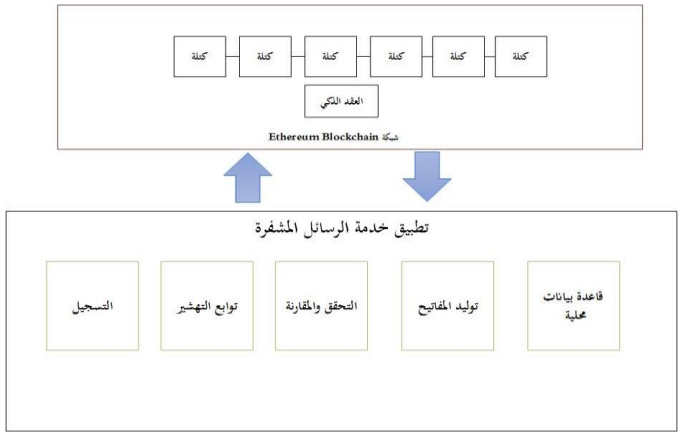
- لامركزية: لا تعتمد على عقدة أو سلطة مركزية واحدة للموافقة على عمليات النقل يمكن إنشاء البيانات وتخزينها وتحديثها بطريقة موزعة، ويجب على جميع المشاركين فيها الوصول إلى الإجماع لقبول عمليات النقل.
- شّفافة: جميع البيانات المخزنة في سلسلة الكتل شفافة لجميع العقد المشاركة، وشفافة أيضًا عند تحديث تلك البيانات، لذلك تعتبر سلسلة الكتل موثوقة.
- آمنة: يمكن توسيع قاعدة البيانات دون تغيير السجلات السابقة.

- التعمية: تستخدم سلسة الكتل مجموعة متنوعة من تقنيات التعمية ووظائف التهشير وأشجار Merkle التي سنتحدث عنها في الفقرة 4.2.2، وتقنية المفتاح العام والخاص [17].
- مفتوحة المصدر: معظم أنظمة سلسلة الكتل مفتوحة للجميع، لذلك يمكن التحقق منها بالعموم، ويمكن للمستخدمين استخدام تقنيات سلسلة الكتل لأي تطبيق يريدونه.
- مجهولة الهوية: تحل تقنية سلسلة الكتل مشاكل الثقة في شبكات الند للند، حيث يمكنها نقل البيانات وإرسالها إلى عنوان مجهول الهوية فقط بمعرفة عنوان المستقبل.
- ثابتة غير قابلة للتغيير: حيث يتم الاحتفاظ بأي تسجيل فيها إلى الأبد، ويمكن تغييره فقط في السيطرة على أكثر من 51٪ من العقد في نفس الوقت وهذا أمر شبه مستحيل.
- الإستقلال الذاتي: يمكن لأي عقدة في نظام سلسلة الكتل نقل البيانات وتحديثها بأمان بسبب وجود قواعد الإجماع.

9. النموذج المقترح

نستخدم بعض أجزاء النموذج المقترح في [18] لتصميم نموذج جديد حيث نضيف إليه التحسينات والوظائف التي سنذكرها لاحقاً في القسم العملي وذلك من أجل ضمان الوصول إلى شبكة آمنة محققة لخدمات السرية والخصوصية والسرعة باستخدام سلسلة الكتل.

يتألف النموذج المقترح من عدة أجزاء رئيسية أهمها شبكة Ethereum Blockchain، والعقد الذكي وتوابع التهشير المطبقة داخل تطبيق إرسال الرسائل كما يوضح الشكل (9-1).



الشكل (9–1) النموذج المقترح للتسجيل والتحقق من ملكية المفتاح العام

يقوم النموذج المقترح على تصميم آلية للتسجيل والتحقق من ملكية المفتاح العام، حيث يتم استخدام توابع التهشير للمفاتيح ثم تخزينها في سلسلة الكتل، ويتم التحقق من ملكية المفتاح العام للمستخدم في كل مرة يتم فيها التعامل معه.

نقدم فيمايلي نموذج يتم فيه توليد مفتاح عام وخاص ثم يحفظ تهشير المفتاح العام في سلسلة الكتل Ethereum ونقوم ببرمجة تطبيق يقوم بتسجيل المستخدمين وإرسال رسائل معماة بالمفتاح العام والتحقق من ملكية المستقبل للمفتاح بواسطة سلسلة الكتل قبل عملية الإرسال، ويؤمن آلية لإلغاء تسجيل المستخدم في حال أراد إلغاء التسجيل أو انتهت فترة الصلاحية، وذلك من أجل توظيف فكرة البحث والتحقق من إمكانية تطبيقها على أرض الواقع.

نتعرف فيما يلي على أجزاء النموذج المقترح مع تعريف بسيط عن كل جزء

1- شبكة Ethereum Blockchain

هي شبكة مبنية على تقنية سلسلة الكتل تتيح برمجة التطبيقات اللامركزية فيها عن طريق كتابة عقود ذكية بلغة solidity.

2- العقد الذكي

البرنامج الذي يستقبل وينفذ الطلبات داخل سلسلة الكتل في شبكة Blockchain Ethereum.

3- تطبيق ارسال الرسائل المعماة

يقدم بيئة تفاعلية للمستخدم للتسجيل وإلغاء التسجيل وإرسال الرسائل.

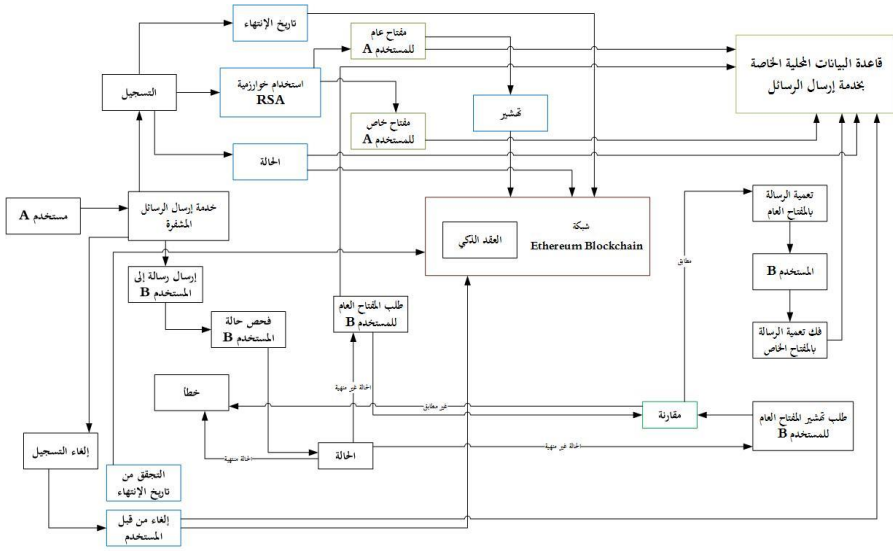
4- قاعدة بيانات محلية

يتم فيها تخزين المفاتيح العامة والخاصة للمستخدمين من أجل عمليات الإرسال والإستقبال.

5- خوارزمية RSA لتوليد المفاتيح

تقوم بتوليد مفتاحين لكل مستخدم من أجل تعمية وفك تعمية الرسائل المتبادلة.

يبين الشكل (9-2) الوظائف التي يقوم بها النموذج بشكل عام.



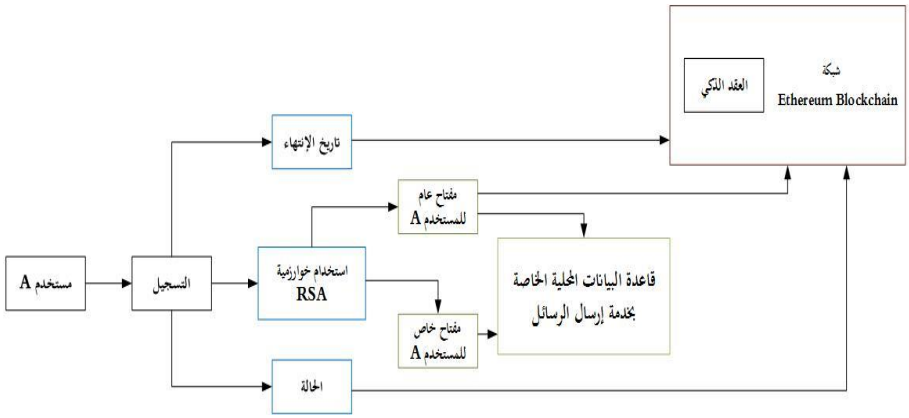
الشكل (9-2) وظائف النموذج المقترح

1.9. نموذج التسجيل لمستخدم

نقدم في الشكل (9–3) نموذج تسجيل لمستخدم جديد في التطبيق والمراحل التي يمر بها.

حيث يقوم المستخدم A بالتسجيل في التطبيق عبر الخطوات التالية:

- يدخل المستخدم معلوماته (الإسم ، الإيميل، اسم المستخدم، كلمة المرور).
- يتم توليد مفتاحين (مفتاح عام ومفتاح خاص) باستخدام خوارزمية التعمية غير المتناظرة (RSA).
- يتم حفظ المفتاح العام والخاص في قاعدة البيانات المحلية الخاصة بالتطبيق.
- يتم إرسال المعلومات التالية (تهشير المفتاح العام، تاريخ الانتهاء، الحالة) إلى داخل سلسلة الكتل وتخزينها.



الشكل (9–3) نموذج تسجيل مستخدم جديد

2.9. نموذج إرسال رسالة

نقدم في الشكل (9–4) نموذج عن كيفية تناقل الرسائل بين مستخدمين والمراحل التي تمر بها الرسالة وآلية التحقق عن طريق الخطوات التالية:

1– يقوم المستخدم A بالدخول إلى الحساب الخاص به في تطبيق إرسال الرسائل.

2– يحدد المستقبل المراد إرسال الرسالة له فرضاً المستخدم B.

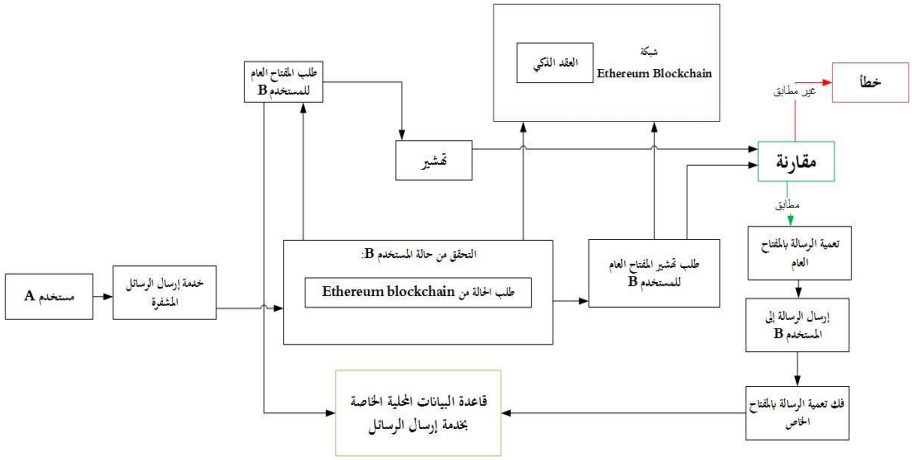
3- تتم آلية التحقق على مرحلتين:

- ❖ التحقق من حالة المستخدم B من سلسلة الكتل فتكون إما صالحة أو منتهية.
- ❖ مقارنة تهشير المفتاح العام للمستخدم B من سلسة الكتل مع الموجود في قاعدة البيانات المحلية الخاصة بالتطبيق.

4- في حال كانت الحالة منتهية حسب التاريخ أو المقارنة غير مطابقة تظهر رسالة خطأ.

وفي حال كانت المقارنة مطابقة تتم عملية تعمية الرسالة باستخدام المفتاح العام للمستخدم B ثم إرسالها له من خلال التطبيق.

5- يقوم المستخدم B بفك تعمية الرسالة باستخدام مفتاحه الخاص الموجود في قاعدة البيانات المحلية.



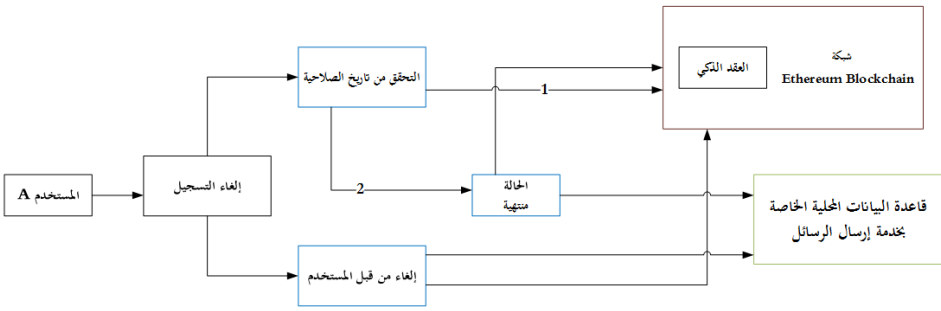
الشكل (9-4) نموذج إرسال رسالة

3.9. نموذج إلغاء التسجيل

نعرض في الشكل (9-5) نموذج إلغاء التسجيل لمستخدم ويشمل الحالتين:

- إنتهاء صلاحية التسجيل: حيث يقارن التاريخ الحالي مع تاريخ إنتهاء الصلاحية من سلسلة الكتل حيث يوضع في خانة الحالة منتهية في سلسلة الكتل وقاعدة البيانات المحلية ليتوقف التعامل معه ريثما يقوم بتجديد التسجيل.

- طلب المستخدم إلغاء التسجيل: حيث يتم حذف حساب المستخدم من سلسلة الكتل وقاعدة البيانات المحلية.



الشكل (9–5) نموذج إلغاء تسجيل المستخدم

10. القسم العملي

1.10. تقييم النموذج المقترح والنتائج العملية

بتطبيق بعض أجزاء النموذج المقترح في [18] وإضافة بعض المزايا تبين لدينا أنه يوجد بطء في النظام حيث كل عملية إرسال تحتاج إلى عملية تنقيب لإضافة المعاملة على سلسلة الكتل وهذا الأمر غير واقعي في حال إرسال الرسالة في كل مرة، فقمنا بإضافة بعض التعديلات على النموذج وإضافة بعض الوظائف والتي أدت إلى الحصول على النتائج المرجوة، وكان أبرز هذه التعديلات:

- إضافة معاملة على سلسلة الكتل فقط في حال إنشاء مستخدم جديد مما يعطي السرعة في الأداء لأن الإضافة تحتاج لعملية تنقيب وبالتالي زمن أكثر.
- جلب البيانات من سلسلة الكتل من أجل التحقق من ملكية المفتاح العام لا يتطلب زمن تنقيب.
- استخدام HashMap في عملية تخزين البيانات في سلسلة الكتل مما يعطي سرعة في البحث.
- إضافة نموذج إرسال للرسائل ونموذج حذف.

- تطبيق النماذج عمليا في Ethereum Blockchain وكتابة النتائج.

- **تقييم النموذج من الناحية الأمنية**

نقدم في الجدول (10-1) كيف يلبي نموذجنا المقترح المتطلبات الأمنية الأساسية.

المتطلب الأمني	كيفية تحقيق المتطلب الأمني
السرية	استخدام آلية التحقق من ملكية المفتاح العام للمستخدم ثم استخدام المفتاح العام في تعمية الرسائل
السلامة	تحوي كل كتلة على قيمة تهشير لكل محتوياتها في سلسلة الكتل ولكل مستخدم عنوانه الخاص في سلسلة الكتل يتم التعامل معه من خلاله
التوافرية	تقوم شبكة Ethereum Blockchain بمعالجة كافة الطلبات ولأن الشبكة مؤلفة من عدة عقد فعند توقف إحدى العقد لا تتأثر الخدمة

الجدول (10-1) المتطلبات الأمنية وكيفية تحقيقها في النموذج المقترح

- **تقييم النموذج من ناحية الوظائف والأداء**

تم توظيف بيئة تفاعلية تسمح بالتسجيل والتحقق من ملكية المفتاح العام بطريقة تضمن السرعة في الأداء والفاعلية وذلك بتحقيق الوظائف (التسجيل والصلاحية وإلغاء التسجيل)، وقمنا بإجراء الاختبارات عليه لنقوم بالإجابة عن مسألة البحث كالتالي:

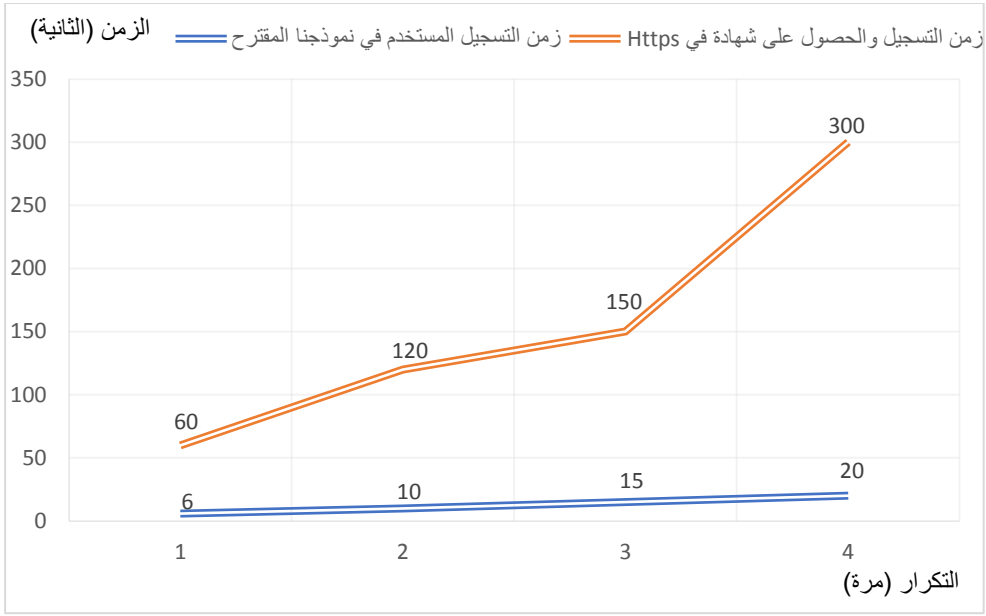
هل تستطيع تقنية سلسلة الكتل حل مشاكل PKI وأن تكون بديلة عنها في إرسال الرسائل ؟

نعم يمكن لشبكة سلسلة الكتل أن تحل مشاكل البنية التحتية للمفتاح العام PKI وأن تكون بديلة عنها حيث برهنا على ذلك من خلال تطبيق النموذج المقترح، عن طريق برمجة العقد الذكي والتخاطب معه وإضافة المفاتيح العامة على سلسلة الكتل حيث يتم حفظ تهشير المفتاح العام مع اسم المستخدم في سجل عام موزع على جميع عقد سلسلة الكتل في Ethereum Blockchain لنضمن بذلك عدم إمكانية التعديل على السجل، وتتم عملية إرسال رسالة إلى مستخدم ما مسجل في النظام بعد التحقق من ملكية المفتاح العام من خلال مقارنة التهشير المحفوظ في سلسلة الكتل مع الموجود في قاعدة البيانات المحلية باستخدام تطبيق الويب حيث كانت نتائج الوظائف للنموذج كما يلي:

- **عملية تسجيل المستخدم**

تمت العملية بنجاح حيث تم توليد مفاتيح التعمية غير المتناظرة وتخزينها في قاعدة البيانات، وتم استخدام توابع التهشير من أجل تهشير المفتاح العام وإرساله إلى سلسلة الكتل بسرعة عالية،

ومن ناحية الأداء يبين الشكل (10-1) مقارنة بين زمن تسجيل المستخدم في نموذجنا المقترح وزمن الحصول على الشهادة التي تستخدم PKI في برتوكول Https حسب موقع godaddy [19]و comodo [20].



الشكل (10-1) مقارنة زمن تسجيل المستخدم في نموذجنا المقترح وزمن الحصول على الشهادة في Https

نلاحظ من الشكل (10-1) أن زمن التسجيل في نموذجنا يأخذ حوالي (6-20 ثانية)، بينما الحصول على شهادة مصدقة من CA نحتاج إلى حوالي (1- 5 دقائق).

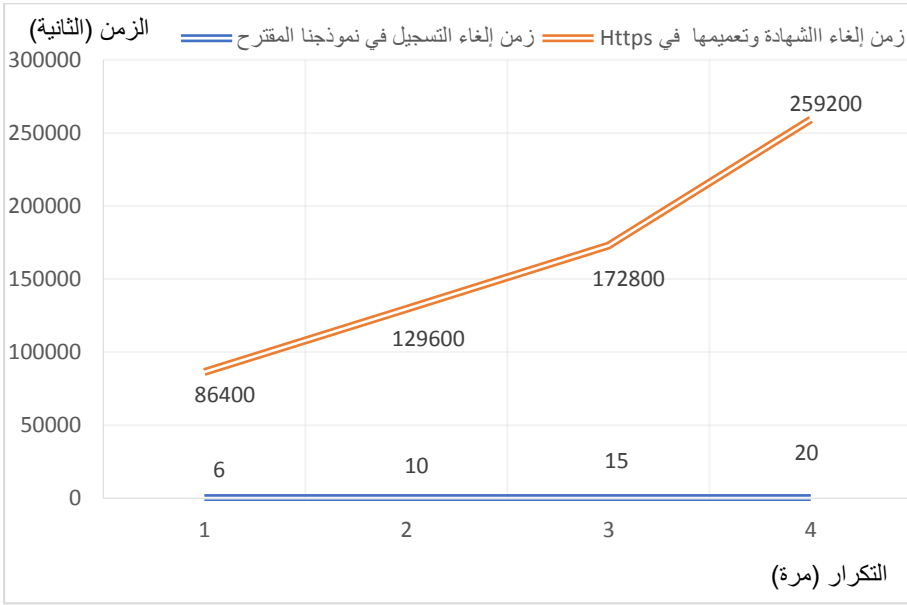
- **عملية الإرسال والمقارنة والاستقبال**

تتم العملية من خلال دخول المستخدم إلى حسابه ثم تحديد المستقبل الذي يريد الإرسال له، وبعدها تتم عملية التحقق من صلاحية المستخدم ومقارنة المفاتيح، وفي حال صحة العملية يتم تعمية الرسالة بالمفتاح العام للمستقبل وإرسالها له ليقوم بقراءة الرسالة باستخدام مفتاحه الخاص.

- **عملية إلغاء تسجيل المستخدم وحذفه**

تتم هذه العملية من خلال ضغط المستخدم على زر الحذف بحيث يتم حذف حساب المستخدم من قاعدة البيانات المحلية وسلسلة الكتل وبذلك يتم حل مشكلة الشهادات الملغاة بحيث تأخذ العملية عدة ثواني حتى يتم تعميم الإلغاء.

ومن ناحية الأداء يبين الشكل (10-2) مقارنة بين زمن إلغاء الشهادة في النموذج المقترح والآلية المطبقة في إلغاء الشهادات في PKI.



الشكل (10-2) مقارنة زمن إلغاء تسجيل مستخدم في نموذجنا مع زمن إلغاء الشهادة في PKI في Https

نلاحظ من الشكل (10-2) أن زمن إلغاء التسجيل في نموذجنا يأخذ حوالي (6 – 20 ثانية)، بينما في إلغاء شهادة مصدقة من CA نحتاج إلى حوالي (24 ساعة) حسب شركة godaddy [21] .

كيف تستطيع تقنية سلسلة الكتل حل مشاكل PKI وأن تكون بديلة عنها في إرسال الرسائل ؟

تمت عملية تصميم النظام من خلال استخدام سلسلة الكتل في Ethereum حيث تم إنشاء حساب تجريبي من أجل إضافة العقد الذكي والتخاطب معه، وتم ذلك بسهولة وبسرعة جيدة وذلك باستخدام توابع API وواجهات التخاطب وبيئات التطوير التي توفرها Ethereum.

11. الاستنتاجات والتوصيات

نستنتج مما سبق أن النموذج المقترح الذي قمنا بطرحه قد أعطى نتائج فعالة في بناء نموذج بديل عن PKI واستخدامها في إرسال الرسائل بطريقة آمنة تضمن السرية والخصوصية عن طريق التسجيل والتحقق من ملكية المفتاح العام وذلك من خلال استخدام سلسلة الكتل في Ethereum وهو الهدف الأساسي من بحثنا كما تقدم.

قدمنا في هذا البحث عرضا لتقنية سلسلة الكتل وقمنا بتوصيف البنية التحتية للمفتاح العام PKI وتحدثنا عن المشاكل التي تعاني منها، ثم قدمنا حلول مقترحة للتغلب على هذه المشاكل باستخدام تقنية سلسلة الكتل.

بعدها عرضنا النموذج المقترح من قبلنا لامكانية تطبيق بنية بديلة عن PKI واستخدامها في تطبيق إرسال الرسائل بطريقة آمنة عن طريق خوارزميات التعمية غير المتناظرة وبالاعتماد على سلسلة الكتل في Ethereum من خلال العقد الذكي.

وقد أثبت النموذج فاعليته في تسجيل المفتاح العام لمستخدم وضمان عدم تغييره وسرقته وإلغاء البنية المركزية التي تقوم عليها PKI، كما أثبت أيضا سرعة في الأداء وحل لمشاكل إلغاء الشهادات بطريقة سريعة وفعالة.

واستطاع النموذج المقترح إضافة العديد من الميزات على استخدام سلسلة الكتل في التحقق من المفتاح العام أهمها:

- سهولة تسجيل المستخدم.
- سرعة إجراء التحقق من ملكية المفتاح العام.
- سهولة إرسال الرسائل بطريقة معماة.
- سرعة إلغاء التسجيل لمستخدم وتعميمها على جميع عقد السلسلة.

ولا ننسى أيضاً أن بيئة Ethereum قد وسعت آفاق العمل على برمجة تطبيقات لامركزية تستفيد من ميزات سلسلة الكتل فيها، مما يقدم سهولة في تطوير تطبيقات تضمن السرعة والأمان لمستخدميها.

12. الأعمال المستقبلية

- دراسة كفاءة النظام في استخدام عدد كبير من المستخدمين.
- تطوير وظائف العقد الذكي.
- إضافة إمكانية تجديد الإشتراك في حال انتهاء الصلاحية.
- إضافة خيارات من أجل حالة المستخدم.

المراجع

[1] F.Schuermann, "Bitcoin and Beyond-A Technical Survey on Decentralized Digital Currencies,"*IEEE communication surveys and tutorials, 2016.*

[2] S.Bano,A.Sonnino,M.Bassam,S.Azouvi,P.McCorry,S.Meiklejohn,G. danezis, "SoK: Consensus in the Age of Blockchains," *1st ACM Conference on Advances in Financial Technologies, 2019.*

[3] C.Cachin,M.Vukoli, "Blockchain Consensus Protocols in the Wild," *IBM Research - Zürich, Rüschlikon, Switzerland, 2017.*

[4] W.Diffie. and M.E.Hellman, "New Directions in Cryptography," *IEEE Transactions On Information Theory, VOL. IT-22, NO. 6, november 1976.*

[5] L.M Kohnfelder, "Towards a Practical Public-key Cryptosystem," *Massachusetts Institute of Technology, Cambridge, 1978.*

[6] ITU-T, "The Directory Overview Of Concepts, Models And Service," *X.500 Series of Recommendations, International Telecommunications Union, Geneva, 1993.*

[7] M.S.Baum and W.Ford, "Public Key Infrastructure Interoperation," *IEEE Aerospace Conference, 21-28 March 1998.*

[8] Michael Alan Specter, "Understanding Certificate Authorities," *Massachusetts Institute of Technology, 2015.*

[9] "An Overview of Public Key Infrastructures (PKI)," *Techotopia. Retrieved March 26, 2015.*

[10] Jayanth Rajakumar and KN Subrahmanya , "Overview Of Tls Certificate Revocation Mechanisms, " *International Journal of Advanced Research in Computer Science; Udaipur, May 2019.*

[11] https://www.grc.com/revocation/crlsets.html

[12] https://searchsecurity.techtarget.com/news/252436120/23000-Symantec- certificates-revoked-following-leak-of-private-keys

[13] https://scotthelme.co.uk/certificate-revocation-google-chrome/

[14] A. Bahga and V. K. Madisetti, "Blockchain Platform For Industrial Internet Of Things," *eorgia Institute of Technology, Atlanta, GA, USA, 2016.*

[15] I. C. Lin and T. C. Liao, "A Survey Of Blockchain Security Issues And Challenges," *International. Journal of Network Security, 2017.*

[16] A. M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," *O'Reilly Media, Inc Sebastopol in California, 2015.*

[17] Mauro Conti, E.Sandeep Kumar,Chhagan Lal and Sushmita Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *IEEE 2017.*

[18] Kahina Khacef, Guy Pujolle, "Secure Peer-to-Peer communication based on Blockchain," *33rd International Conference on Advanced Information Networking and Applications (AINA-2019), Mar 2019.*

[19] https://www.godaddy.com/help/how-long-will-it-take-to-issue-my-certificate-858

[20] https://comodosslstore.com/ssl-validation-process/dv/how-long-to-issue-dv-certificate

[21] https://in.godaddy.com/help/uninstall-an-ssl-certificate-from-my-godaddy-hosting-31931