الجمهورية العربية السورية
جامعة تشرين
كلية الهندسة المعلوماتية
قسم النظم والشبكات الحاسوبية

BLOCKCKAIN AND CLOUD COMPUTING
(FILE SHARING:UPLOAD-DELET-DOWNLOAD)

الحوسبة السحابية وتقنية BLOCKCHAIN
(مشاركة الملفات:تحميل -حذف-تنزيل)

إعداد : م. نوح عبود
إشراف: د. منهل جعفر

2024/2023

Contents

3 ..... **Abstract-1**

3 ..... **INTRODUCTION-2**

4 ..... **BLOCKCHAIN-3**

5 ..... **:Block Structure 1.3**

5 ..... **block header (metadata) 1.1.3**

6 ..... **block body 2.1.3**

8 ..... **Blockchain خصائص2.3**

9 ..... **FLEXIBLE CONSENSUS ALGORITHM 3.3**

9 ..... **POW خوارزمية1.3.3**

10 ..... **Cloud Computing-4**

11 ..... **The five essential characteristics of cloud 1.4**

12 ..... **Four Cloud Deployment Models 2.4**

13 ..... **Service Offering Models 3.4**

15 ..... **Uploading on cloud using blockchain-5**

18 ..... **Delete on cloud using blockchain-6**

19 ..... **Downloading on cloud using blockchain-7**

22 ..... **OFF-CHAIN MONITORING-8**

24 ..... **Challenges in blockchain–Cloud integration -9**

25 ..... **REFERENCES -10**

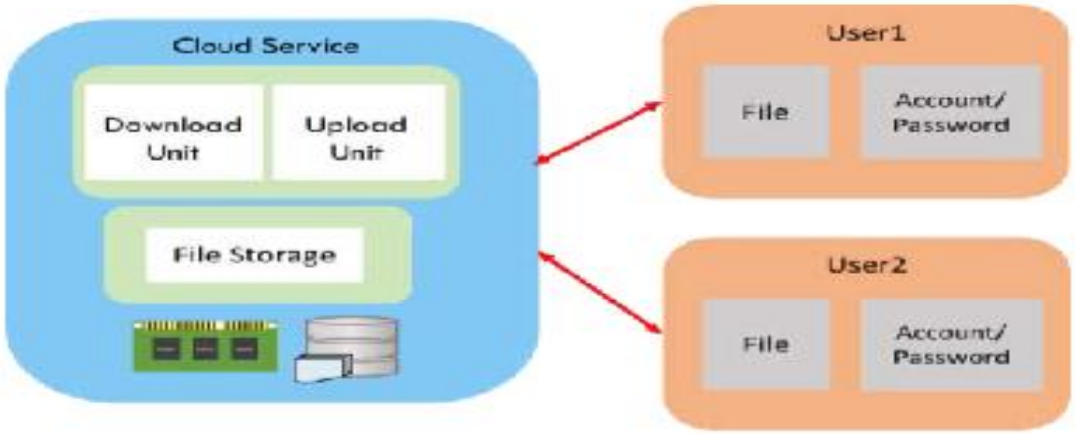
Abstract-1 :

تقنية البلوكشين (Blockchain) قد ثبتت نفسها كتقنية ثورية ومبتكرة في عدة مجالات، واحدة من هذه المجالات هي خدمات الحوسبة السحابية. تعتبر الحوسبة السحابية أساسية في العصر الرقمي الحديث، حيث توفر الموارد الحاسوبية والتخزين و خدمات أخرى عبر الإنترنت للأفراد والشركات. ومع ذلك، تواجه الحوسبة السحابية التحديات المتعلقة بالأمان والخصوصية والمصداقية.
في هذا السياق، تأتي تقنية البلوكشين لتقديم حلاً مبتكرًا وموثوقًا لمشاكل الحوسبة السحابية. تمتاز تقنية البلوكشين بالطابع اللامركزي والشفافية والأمان العالي، مما يوفر بيئة موثوقة وآمنة لتقديم خدمات الحوسبة السحابية.
إحدى الخدمات التي تقدمها الحوسبة السحابية هي مشاركة الملفات files sharing بما فيها عمليات تحميل الملفات على السحابة Uploading on cloud وعمليات تنزيل الملفات من السحابة Downloading on cloud والتي تتطلب الوصول الأمن للسحابة ووجود الثقة للمستخدم وهذا ما تم العمل علية في هذا التقرير لتوضيح أهمية ال Blockchain كطبقة حماية وأمان تعمل ما بين االمستخدم والسحابة .

INTRODUCTION-2 [2] :

تعتمد معظم الخدمات السحابية مثل Google Drive أو Dropbox أو Mega على بنية مركزية(الشكل 1)، ولكن عدم موثوقية التطبيقات المركزية واضح. وفي واحدة من أشهر القضايا ذات الصلة، فشل فيسبوك في حماية خصوصية مستخدميه، مما سمح لشركة كامبريدج للتحليل البريطانية بالحصول على كمية كبيرة من بيانات المستخدمين.

قبل عامين، كان البنك الأول في تايوان ضحية لعملية سرقة ماكينة صراف آلي بعد أن اخترق حصان طروادة الخادم في فرع البنك في لندن. تكشف هاتان الحالتان أن الخدمات التي تتحكم فيها مؤسسة واحدة تكون عرضة للخطأ البشري والأخطاء في النظام، مما قد يؤدي إلى فقدان الممتلكات الشخصية. لتحسين خصوصية البيانات، تم الاستفادة من خصائص ال blockchain لتوفير الحوسبة السحابية الآمنة.



الشكل1The general cloud computing architecture

3- BLOCKCHAIN [3]:

تسمح تقنية Blockchain (BC) بالمشاركة الآمنة والمشفرة للبيانات بطريقة لا مركزية وموزعة. وهو يعمل بمثابة immutable ledger يسجل المعاملات ويتتبع الأصول داخل شبكة الأعمال، مما يقلل من المخاطر وتكاليف الموارد. على الرغم من أن تقنية blockchain تدعم تطبيقات متنوعة، فإن عملة البيتكوين هي عملة رقمية محددة تعتمد على تقنية blockchain في التدابير الأمنية. تشمل الخصائص الرئيسية لـ blockchain اللامركزية، والاستمرارية، و الثبات،والتوافق مما يتيح معالجة المعاملات الآمنة واللامركزية.في blockchain يتم تنظيم بيانات المعاملات في كتل مرتبطة ببعضها البعض في سلسلة, ومع إضافة المزيد من الكتل، تنمو سلسلة الكتل، ويتم تسجل توقيت وتسلسل المعاملات. تتكون كل كتلة في blockchain من ثلاثة أجزاء رئيسية:

- **head** :الذي يحتوي على بيانات وصفية مثل hash الخاص بالكتلة السابقة والطابع الزمني Timestamp.
- **Block Body**: يحتوي على معلومات المعاملة.
- **Hash** : يعمل كمعرف فريد للكتلة وهوبمثابة بصمة رقمية, يتم ربط الكتل من خلال hash الخاص بكل منها وبالتالي فإن blockchain تضمن أنه بمجرد إضافة كتلة، لا يمكن تغييرها أو إدراجها بين الكتل الموجودة، مما يجعل blockchain مقاومة للتلاعب.

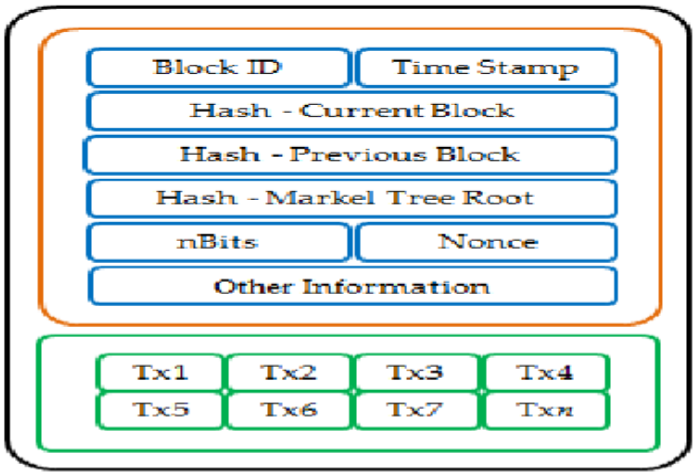
- يعتمد إطار عمل blockchain (BC) على أربعة مكونات رئيسية:

- **Shared Ledger** (الدفتر المشترك): يتمثل الدفتر المشترك في المكان الذي يتم فيه تخزين وتسجيل جميع المعلومات المتعلقة بالعمليات والمعاملات في الـ Blockchain. يتم توزيع نسخة متطابقة من الدفتر المشترك إلى جميع المشاركين في الشبكة، ويتم تحديثه بشكل مستمر عند حدوث معاملات جديدة. يعمل الدفتر المشترك على ضمان التوثيق والشفافية والأمان، حيث لا يمكن تعديل السجلات الموجودة فيه بعد تأكيدها.
- **Permissions** (الصلاحيات): يتعلق هذا المكون بتحديد وإدارة صلاحيات المشاركين في الشبكة. يتم استخدام نموذج الصلاحيات لتحديد من يمكنه الوصول إلى الدفتر المشترك والقيام بالعمليات فيه. يمكن أن تكون هناك نماذج مختلفة للصلاحيات، مثل الـ Public Blockchain حيث يمكن لأي شخص الانضمام والمشاركة، أو الـ Private Blockchain حيث يكون الوصول مقتصرًا على مجموعة محددة من المشاركين.
- **Smart Contracts** (العقود الذكية): العقود الذكية هي برامج قابلة للتنفيذ تعمل على تنفيذ وتنظيم العمليات والمعاملات في الـ Blockchain بشكل آلي. تتم برمجة العقود الذكية لتحمل شروطًا وقواعد

محددة، وعندما تتوافق المعاملة مع هذه الشروط، يتم تنفيذ العقد بشكل تلقائي ومن دون الحاجة إلى وساطة بشرية. العقود الذكية تساهم في زيادة الشفافية والثقة بين الأطراف المتعاملة.

- **Consensus** (التوافق): يتعلق التوافق بآلية تحقيق اتفاق بين المشاركين في الشبكة بشأن حالة الدفتر المشترك. يهدف التوافق إلى ضمان أن جميع المشاركين في الشبكة يتفقون على حالة الدفتر المشترك، وأن النسخ المتواجدة للدفتر المشترك متطابقة. يتم تحقيق التوافق من خلال آلية معينه(الإجماع لاثبات الملكية - والتوقيع المتعدد - والتسامح العملي مع الأخطاء (PBFT)).

1.3 Block Structure [3]:



الشكل 2 Block Structure

تتكون الكتلة بشكل عام من قسمين رئيسيين هما block header وblock body

1.1.3 block header (metadata) [3]:

يحتوي رأس الكتلة على القيم التاليه:

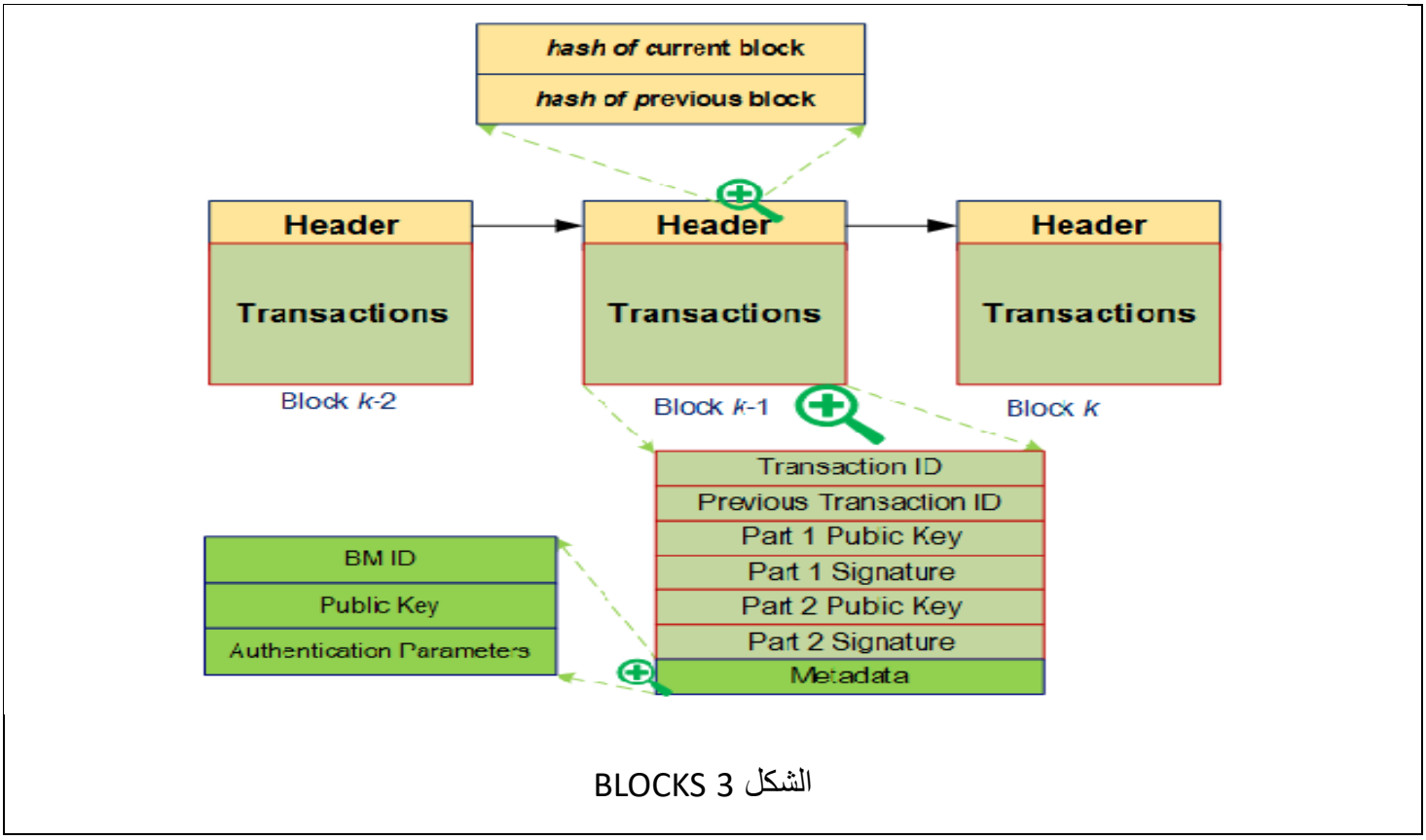
- Timestamp: يشير الطابع الزمني في سياق تقنية blockchain إلى الوقت العالمي المعبر عنه بالثواني عند إنشاء كتلة أو إضافتها إلى blockchain. وهو جزء مهم من المعلومات في رأس الكتلة، حيث يوفر ترتيبًا زمنيًا للكتل ويضمن سلامة وأمن شبكة blockchain عن طريق منع التلاعب بتسلسل المعاملات.

- Hash-current block .
- Hash-previous block .

- The Merkle Tree Root Hash: تعد Merkle Tree Root Hash قيمة تجزئة تشفير فريدة تمثل جميع المعاملات الموجودة داخل كتلة في blockchain. ويتم حسابها من خلال الجمع بين hash الخاصة بالمعاملات الفردية بطريقة محددة لإنشاء قيمة تجزئة واحدة، مما يوفر طريقة آمنة وفعالة للتحقق من سلامة المعاملات داخل الكتلة. يلعب Merkle Tree Root Hash دورًا حاسمًا في ضمان ثبات وشفافية معاملات blockchain.
- nBits: يشير "nBits" في كتلة blockchain إلى الحد الأقصى لعدد البتات التي يمكن أن تحتوي عليها تجزئة الكتلة الصالحة. تساعد هذه المعلمة في تحديد مستوى الصعوبة المطلوب لكي تعتبر تجزئة الكتلة صالحة في شبكة blockchain. إنها تلعب دورًا حاسمًا في الحفاظ على أمان وسلامة blockchain من خلال تنظيم تعقيد عملية التجزئة.
- Nonce: في سياق تقنية blockchain، يشير مصطلح "Nonce" إلى حقل يتكون من أربعة بايتات تبدأ من 0 وتتزايد مع كل عملية حسابية. تعد هذه القيمة الإضافية أمرًا بالغ الأهمية في عملية تعدين كتل جديدة في شبكة البلوكشين، لأنها تساعد القائمين بالتعدين miners في العثور على تجزئة كتلة صالحة تلبي المعايير المطلوبة لإضافة كتلة جديدة إلى السلسلة. يعمل الرقم nonce كطريقة لإدخال العشوائية في عملية إنشاء الكتلة، مما يجعل من الصعب حسابيًا العثور على الرقم الصحيح الذي يلبي قواعد الإجماع الخاصة بالشبكة.
- Blockversion: يشير إصدار Blockversion في كتلة blockchain إلى المجموعة المحددة من قواعد التحقق التي يجب اتباعها عند التحقق من سلامة الكتلة وصحتها. فهو يساعد على ضمان موافقة جميع العقد في الشبكة على القواعد التي تحكم عملية التحقق من الصحة لتلك الكتلة المعينة، مما يساهم في آلية الأمان والإجماع لنظام blockchain. تعتبر هذه المعلومات ضرورية للحفاظ على ثقة وموثوقية شبكة blockchain من خلال فرض معايير التحقق المتسقة عبر جميع المعاملات والكتل.

2.1.3 block body [3]:

يحتوي على البيانات أو السجلات أو المعاملات الفعلية. ويتضمن معلومات مثل تفاصيل المعاملات والتوقيعات الرقمية من المشاركين والبيانات الأخرى ذات الصلة اللازمة لتشغيل شبكة blockchain.
يعد جسم الكتلة عنصرًا حاسمًا في كل كتلة في blockchain لأنه يخزن المعلومات الأساسية التي يتم تسجيلها وتأمينها داخل نظام دفتر الأستاذ اللامركزي وغير القابل للتغيير.



الشكل BLOCKS 3

يحتوي body على العناصر التالية:

1. Transaction ID(معرف المعاملة): يُعرف أيضًا بمعرّف العملية أو معرف البيانات. يتم استخدامه لتمييز المعاملة بشكل فريد في البلوكشين. يتم إنشاء هذا المعرف بناءً على بيانات المعاملة المحددة، مثل المستلم والمرسل والقيمة المنقولة وغيرها. يتم استخدامه للإشارة إلى المعاملة في البلوك الحالي وفي البلوكات المستقبلية التي ترتبط به.
2. Previous Transaction ID(معرف المعاملة السابقة): يُستخدم للإشارة إلى معرّف المعاملة السابقة في سلسلة الكتل. يتم استخدامه لربط الكتل معًا وتأكيد تسلسل المعاملات. من خلال الارتباط بالمعاملة السابقة، يتم بناء سلسلة من الكتل توثق تتابع المعاملات.

3. Part 1 Public Key(المفتاح العام الجزء الأول): يُعرف أيضًا بالمفتاح العام للمستلم. يتم استخدامه لتحديد مفتاح التشفير العام الخاص بالجزء الأول من المعاملة. يستخدم هذا المفتاح للتحقق من صحة التوقيع الرقمي في الجزء الأول للمعاملة.
4. Part 1 Signature(التوقيع الجزء الأول): يُستخدم للتحقق من صحة المعاملة وتأكيد أنها تمت بواسطة المرسل المشار إليه في الجزء الأول من المعاملة. يتم إنشاء التوقيع الرقمي باستخدام المفتاح الخاص الخاص بالمرسل والبيانات المحددة للمعاملة.
5. Part 2 Public Key(المفتاح العام الجزء الثاني): يُعرف أيضًا بالمفتاح العام للمرسل. يستخدم لتحديد مفتاح التشفير العام الخاص بالجزء الثاني من المعاملة. يستخدم في التحقق من صحة التوقيع الرقمي في الجزء الثاني للمعاملة.

6. Part 2 Signature(التوقيع الجزء الثاني): يستخدم للتحقق من صحة المعاملة وتأكيد أنها تمت بواسطة المستلم المشار إليه في الجزء الثاني من المعاملة. يتم إنشاء التوقيع الرقمي باستخدام المفتاح الخاص الخاص بالمستلم والبيانات المحددة للمعاملة.
7. Metadata(البيانات الوصفية): تشير إلى أي بيانات إضافية يتم إرفاقها بالمعاملة. يمكن استخدام البيانات الوصفية لتوفير معلومات إضافية حول المعاملة، مثل تفاصيل إضافية عن المرسل والمستلم أو أي بيانات أخرى ذات صلة.يحتوي هذا الحقل على القيم التالية:

- BM ID: يشير إلى Blockchain Metadata ID وهو معرف فريد يتم استخدامه لتمييز Metadataفي البلوكشين. يتم إنشاءهه بناءً على بيانات الـ Metadata المحددة ويستخدم للإشارة إليها والاستفادة منها في العمليات المستقبلية.
- Public Key: هو مفتاح التشفير العام الذي يستخدم لتحديد هوية المستخدم أو العقدة التي أنشأت الـ Metadataيتم استخدامه للتحقق من صحة ومصداقية المعلومات الموجودة في الـMetadata
- Authentication Parameters: تشير إلى معلومات المصادقة المستخدمة للتحقق من صحة Metadataوالتأكد من أنها لم تتغير. يمكن استخدام مجموعة متنوعة من التقنيات والمعايير لتحقيق ذلك، مثل التوقيعات الرقمية والتشفير.

2.3 خصائص Blockchain [3]:

- ✓ Immutability :إن blockchain غير قابل للتغيير، مما يعني أنه لا يمكن تغيير البيانات أبدًا. علاوة على ذلك، يجب على جميع عقد الشبكة الموافقة على البيانات قبل إضافتها إلى الكتلة، وبالتالي تمكين المعاملات الآمنة. حيث تدل عملية التعدين الى إضافة المعاملات إلى الكتل بعد التحقق من صحتها

- ✓ Decentralization :اللامركزية في تقنية blockchain تعني عدم وجود سلطة مركزية تتحكم في الشبكة. وبدلاً من ذلك، تتم صيانة الشبكة من خلال مجموعة من العقد، مما يضمن التحقق من صحة المعاملات من خلال آلية الإجماع دون الحاجة إلى وكالة مركزية. تسمح هذه الخاصية بوجود نظام دفتر أستاذ موزع ومفتوح حيث تكون المعاملات شفافة وعامة ولا يسيطر عليها أي كيان منفرد.

- ✓ Persistency : بمجرد التحقق من صحة المعاملات وإضافتها إلى blockchain، لا يمكن تغييرها أو حذفها، مما يوفر سجلاً آمنًا وشفافًا لجميع المعاملات. تسمح هذه الميزة بالتحقق السريع من المعاملات، والكشف الفوري عن المخالفات، ومنع الإنفاق المزدوج من خلال الحفاظ على دفتر أستاذ واحد عبر جميع العقد في الشبكة، مما يضمن إمكانية تتبع وسلامة البيانات المخزنة. تساهم ثبات بيانات blockchain وإمكانية تتبعها في موثوقيتها وأمانها في الحفاظ على سجل كامل للمعاملات.

- ✓ Anonymity : في المعاملات المتسلسلة، لا يلزم سوى معرف المستخدم، ولا يتم الكشف عن أي معلومات إضافية. وهذا يعني أن الأطراف المشاركة في المعاملة تظل مجهولة المصدر. كل مستخدم لديه عنوان تم إنشاؤه للتفاعل مع blockchain، بحيث لا يتم الكشف عن هويته الحقيقية.

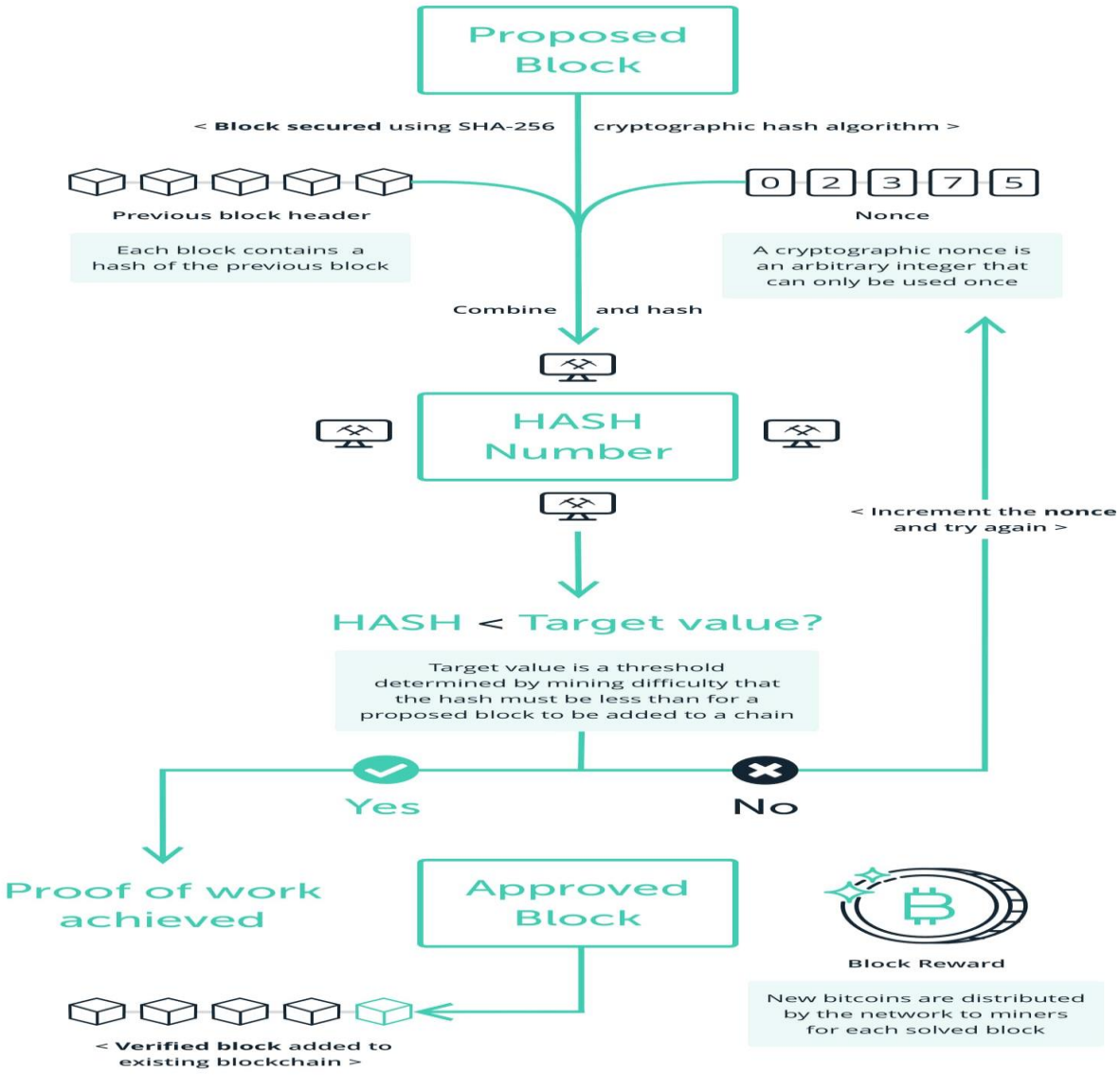
3.3 FLEXIBLE CONSENSUS ALGORITHM [3] :

- لكي يتم إضافة كتلة جديدة الى السلسلة يجب ان تتفق جميع العقد الموجودة على شبكة البلوكشين على ذلك .
- يتم استخدم خوارزمية إجماع إثبات العملProof of Work (PoW) لضمان كفاءة blockchain. تتطلب الخوارزمية مستوى محددًا من القوة الحسابية للتحقق من صحة المعاملات، وتعزيز أمان وأداء النظام.
- يمكن تطبيق خوارزميات إجماع مختلفة مثل Ripple وإثبات التصويت Proof of Vote وإثبات الثقة Proof of Trust وإثبات الحصة Proof of Stake وغيرها .
- على وجه التحديد، يتطلب إثبات الحصة Proof of Stake أن تقوم العقد بالتحقق من صحة المعاملات بناءً على مقدار العملة المشفرة التي تحتفظ بها، بدلاً من القوة الحسابية كما هو الحال في إثبات العمل.

1.3.3خوارزمية POW [3] :

خوارزمية الاجماع Proof of Work (PoW) هي خوارزمية تستخدم في تقنية البلوكشين لضمان أمان الشبكة وتحقيق اتفاق بين المشاركين في الشبكة بشأن حالة سجل المعاملات. تعتبر خوارزمية PoW أشهر وأكثر الخوارزميات استخدامًا في بروتوكولات البلوكشين مثل بتكوين.
فكرة الخوارزمية هي أن المشاركين في الشبكة (المعروفين باسم المُعدّنينMiners)يقومون بحل مشكلة حسابية معقدة جدًا ومكلفة من حيث الوقت والموارد الحاسوبية. يتم تسمية هذه المشكلة بـ "الحصول على دليل العمل(Proof of Work) "، وهي عبارة عن إيجاد قيمة هاش (Hash) تستوفي شروطًا محددة.
يتم تعدين البلوكات في البلوكشين باستخدام خوارزمية PoW على النحو التالي (الشكل 6):

1. يتم جمع مجموعة من المعاملات في بلوك وتشفيرها بواسطة تابع هاش .(Hash function) يتم تضمين قيمة hash للبلوك السابق في بيانات البلوك الجديد.
2. يقوم المُعدّنون بمحاولة حل مشكلة الحصول على دليل العمل (Proof of Work) من خلال تجربة قيم hash مختلفة حتى يتم العثور على قيمة hash تفي بشروط معينة. يتم تجربة القيم باستخدام عملية تجريبية تسمى "التعدين.(Mining) "
3. يتطلب حل مشكلة الحصول على دليل العمل وقتًا وموارد حاسوبية كبيرة. ويتم تعديل صعوبة الحصول على دليل العمل بواسطة معامل يسمى "صعوبة الهدف(Difficulty Target) "، وهو يحدد عدد الاصفار المطلوبة في بداية قيمة hash المقبولة. يتم تعديل صعوبة الهدف بانتظام للحفاظ على وقت إنتاج البلوكات المستقر ومنع التعدين السريع للغاية.
4. عندما يجد أحد المُعدّنين قيمة هاش تفي بشروط الحصول على دليل العمل، يعلن عن حله ويقوم بنشره في الشبكة.
5. يتحقق المشاركون الآخرون في الشبكة من صحة الحل المعلن عنه. إذا كان صحيحًا، يتم قبول البلوك وإضافته إلى سلسلة البلوكات (البلوكشين).



الشكل 6 proof of work

4- Cloud Computing [4]:

يُعرّف المعهد الوطني للمعايير والتكنولوجيا National Institute of Standards (NIST) and Technology الحوسبة السحابية بأنها نموذج يوفر للمستخدمين إمكانية الوصول المريح وعند الطلب convenient and on-demand إلى مجموعة مشتركة من موارد الحوسبة عبر الشبكة. وتشمل هذه الموارد التخزين والخوادم والشبكات والخدمات والتطبيقات، مما يسمح للمستخدمين بالوصول إلى الخدمات مع الحد الأدنى من التفاعل مع مقدمي الخدمة أو متطلبات الإدارة. توفر الحوسبة السحابية المرونة وقابلية التوسع للشركات لإدارة احتياجات تكنولوجيا المعلومات الخاصة بها بكفاءة بناءً على متطلبات الأعمال المتغيرة.

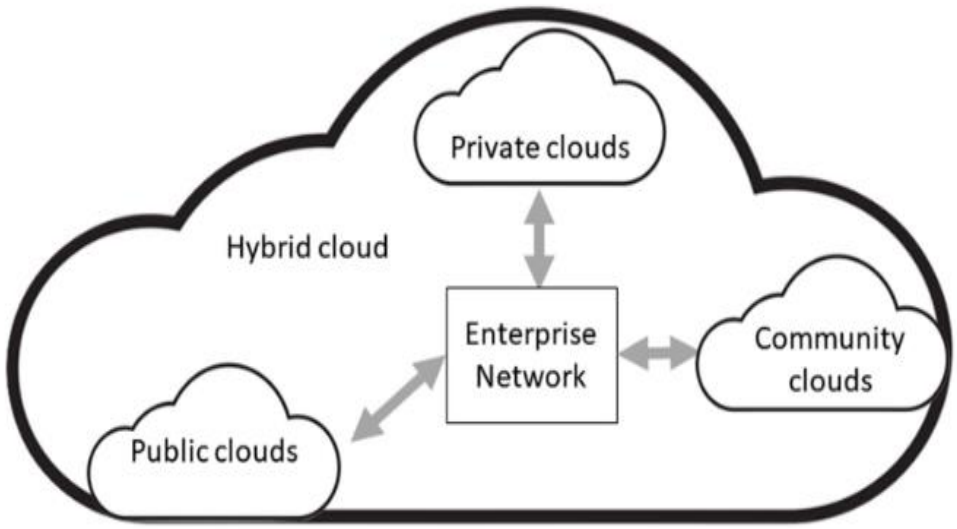
1.4 The five essential characteristics of cloud [4] :

1. On-demand self-servic : يتيح مفهوم الخدمة الذاتية عند الطلب في الحوسبة السحابية للمستخدمين الوصول إلى الموارد وتخصيصها دون الحاجة إلى التفاعل مع مقدمي الخدمة مباشرة. تتيح هذه الميزة للعملاء توفير الموارد بسرعة وتلقائية حسب الحاجة، مما يعزز المرونة والكفاءة في إدارة البنية التحتية لتكنولوجيا المعلومات.
2. Wide network access : هي إحدى الخصائص الرئيسية للحوسبة السحابية والتي تشير إلى القدرة على الوصول إلى الموارد السحابية من خلال شبكة واسعة النطاق. وتتميز هذه الخاصية بالآتي:
   - ✓ إمكانية الوصول من أي مكان:
     - يمكن للمستخدمين الوصول إلى الموارد السحابية والتفاعل معها من أي جهاز متصل بالإنترنت، سواء كان كمبيوتر شخصي، أجهزة محمولة، أجهزة لوحية أو حتى هواتف ذكية.
     - هذا يتيح للمستخدمين المرونة في العمل والوصول إلى البيانات والتطبيقات من أي مكان في العالم.
   - ✓ تعدد أنواع الأجهزة:
     - الوصول السحابي لا يقتصر على أنواع محددة من الأجهزة، بل يمكن الوصول منها جميعًا.
     - هذا يوفر تجربة متسقة للمستخدمين بغض النظر عن نوع جهازهم أو نظام التشغيل.
   - ✓ إمكانية الوصول في أي وقت:
     - المستخدمون قادرون على الوصول إلى الموارد السحابية في أي وقت ممكن، طالما لديهم اتصال بالإنترنت.
     - هذا يمنح المرونة والفعالية في الأداء والعمل عن بعد.
3. Resource pooling :يتضمن تجميع الموارد في الحوسبة السحابية مزود خدمة سحابية يجمع ويدير الموارد من خلال المحاكاة الافتراضية virtualization أو نموذج متعدد المستأجرين multitenant model لخدمة عملاء متعددين. يتم تخصيص هذه الموارد الافتراضية والمادية، وإعادة تخصيصها ديناميكيًا بناءً على طلب المستخدم دون تفاعل العملاء بشكل مباشر مع البنية التحتية المادية. يستفيد المستخدمون من الاستقلالية حيث يمكنهم تحديد مواقع الموارد بشكل تجريدي، مثل الدولة أو مركز البيانات، ولكن قد يظلون بحاجة إلى المساعدة في اختيار مكان تخزين بياناتهم داخل السحابة.
4. Rapid elasticity : تشير المرونة السريعة في الحوسبة السحابية إلى قدرة المستخدمين على توسيع نطاق مواردهم بسرعة وبشكل تلقائي لأعلى أو لأسفل بناءً على الطلب. تتيح هذه الميزة للمستخدمين الوصول إلى موارد إضافية حسب الحاجة، مما يضمن قدرة تطبيقاتهم على التعامل مع أحمال العمل القصوى بكفاءة دون تدخل يدوي. توفر طبيعة المرونة السريعة حسب الطلب للمستخدمين إحساسًا بالموارد اللامحدودة والمرونة للتكيف مع المتطلبات المتغيرة في الوقت الفعلي.

5. Measured service : تشير الخدمة المقاسة في الحوسبة السحابية إلى القدرة على تتبع وتحسين استخدام الموارد بناءً على أنواع خدمة محددة، مثل عرض النطاق الترددي وقوة المعالجة والتخزين

وحسابات المستخدمين. يسمح نظام القياس هذا للأنظمة السحابية بإدارة الموارد تلقائيًا بكفاءة، مما يضمن قدرة كل من مقدم الخدمة والعميل على مراقبة استهلاك الموارد وتنظيمه والإبلاغ عنه بدقة. من خلال تنفيذ خدمة مُقاسة، توفر الحوسبة السحابية الشفافية والتحكم في استخدام الموارد، مما يفيد كلا الطرفين المشاركين في تقديم الخدمة.

2.4 Four Cloud Deployment Models [4]:



الشكل 7 Cloud Deployment

1. السحابة الخاصة(Private Cloud):

السحابة الخاصة هي بنية تحتية سحابية مخصصة لمؤسسة واحدة فقط. يتم تشغيلها عادةً داخل مركز بيانات المؤسسة أو من قبل مزود خدمة طرف ثالث، ولكنها مخصصة حصريًا للاستخدام من قِبَل تلك المؤسسة.
توفر السحابة الخاصة مستويات عالية من الأمان والتحكم، مما يجعلها مناسبة للأعمال التي تتعامل مع معلومات حساسة أو تحتاج إلى الامتثال لمعايير صارمة.
المميزات:

- ✓ أمان عالي :نظرًا لأنها مخصصة لمؤسسة واحدة، فإنها توفر أمانًا أكبر.
- ✓ تحكم كامل :يمكن للمؤسسة التحكم الكامل في الموارد والبنية التحتية.
- ✓ تخصيص :يمكن تخصيصها لتلبية احتياجات المؤسسة الخاصة.

2. السحابة العامة(Public Cloud):

السحابة العامة هي بنية تحتية سحابية تقدمها جهات خارجية مثل Amazon Web Services أو Microsoft Azureويتم تقديمها عبر الإنترنت لعامة الناس أو لمجموعة كبيرة من المستخدمين. يتم مشاركة الموارد (مثل الخوادم والتخزين) بين العديد من العملاء.

المميزات:

- ✓ تكلفة منخفضة :لا تحتاج إلى استثمار كبير في البنية التحتية.
- ✓ قابلية التوسع :يمكن زيادة أو تقليل الموارد بسهولة وفقًا للاحتياجات.
- ✓ سهولة الاستخدام :توفر خدمات جاهزة للاستخدام ويمكن الوصول إليها عبر الإنترنت.

3.السحابة المجتمعية(Community Cloud) :

السحابة المجتمعية هي بنية تحتية سحابية يتم مشاركتها بين عدة منظمات متشابهة في احتياجاتها (على سبيل المثال، المنظمات الحكومية أو المؤسسات التعليمية). يتم تشغيلها وإدارتها من قبل واحدة من هذه المنظمات أو من قبل جهة خارجية.

المميزات:

- ✓ تكلفة مشتركة :يتم تقاسم تكاليف البنية التحتية والصيانة بين المستخدمين.
- ✓ أمان محسّن :توفر مستوى جيد من الأمان مقارنة بالسحابة العامة.
- ✓ تعاون :تسهل التعاون بين المنظمات التي تشترك في نفس الاهتمامات.

4.السحابة الهجينة(Hybrid Cloud) :

السحابة الهجينة تجمع بين السحابة الخاصة والسحابة العامة، مما يسمح للبيانات والتطبيقات بالانتقال بين البيئتين حسب الحاجة. هذا النوع من السحابة يوفر مرونة أكبر للمؤسسات ويتيح لها تحسين أدائها وكفاءتها.

المميزات:

- ✓ مرونة عالية :يمكن توزيع البيانات والتطبيقات بين السحابات العامة والخاصة بناءً على الاحتياجات والأمان.
- ✓ تحسين الأداء :يمكن استخدام السحابة العامة للمهام ذات الطلب العالي، بينما تُستخدم السحابة الخاصة للبيانات الحساسة.
- ✓ تكامل :يمكن للمؤسسات الاستفادة من أفضل ما في السحابتين.

3.4 Service Offering Models [4]:

1. البرمجيات كخدمة(Software as a Service - SaaS)

هذا النموذج يقدم التطبيقات والبرمجيات كخدمة عبر الإنترنت. المستخدمون يصلون إلى هذه التطبيقات من خلال المتصفح دون الحاجة إلى تثبيتها محليًا.

مثال:

Gmail :خدمة بريد إلكتروني تقدمها Google يمكن الوصول إليها عبر المتصفح.

Microsoft Office 365 : مثل Word و Excelو PowerPointالتي يمكن الوصول إليها عبر الإنترنت.

2.المنصة كخدمة(Platform as a Service - PaaS)

في هذا النموذج، تُقدَّم منصة كاملة لتطوير وتشغيل التطبيقات عبر الإنترنت. يتيح هذا للمطورين التركيز على تطوير البرمجيات دون القلق بشأن إدارة البنية التحتية.

مثال:

Google App Engine :منصة تتيح للمطورين بناء ونشر التطبيقات على بنية تحتية تديرها Google.

Heroku :منصة سحابية تُمكِّن المطورين من نشر وإدارة التطبيقات بسهولة باستخدام مجموعة متنوعة من لغات البرمجة.

3 .البنية التحتية كخدمة(Infrastructure as a Service - IaaS)

يوفر هذا النموذج موارد الحوسبة الأساسية كخدمة، مثل الخوادم والتخزين والشبكات. يمكن للمستخدمين إدارة وتشغيل أنظمة التشغيل والتطبيقات الخاصة بهم على هذه الموارد.

مثال:

Amazon Web Services (AWS) - EC2 :خدمة تقدم خوادم افتراضية يمكن استخدامها لتشغيل التطبيقات.

Microsoft Azure

4.العتاد كخدمة(Hardware as a Service - HaaS)

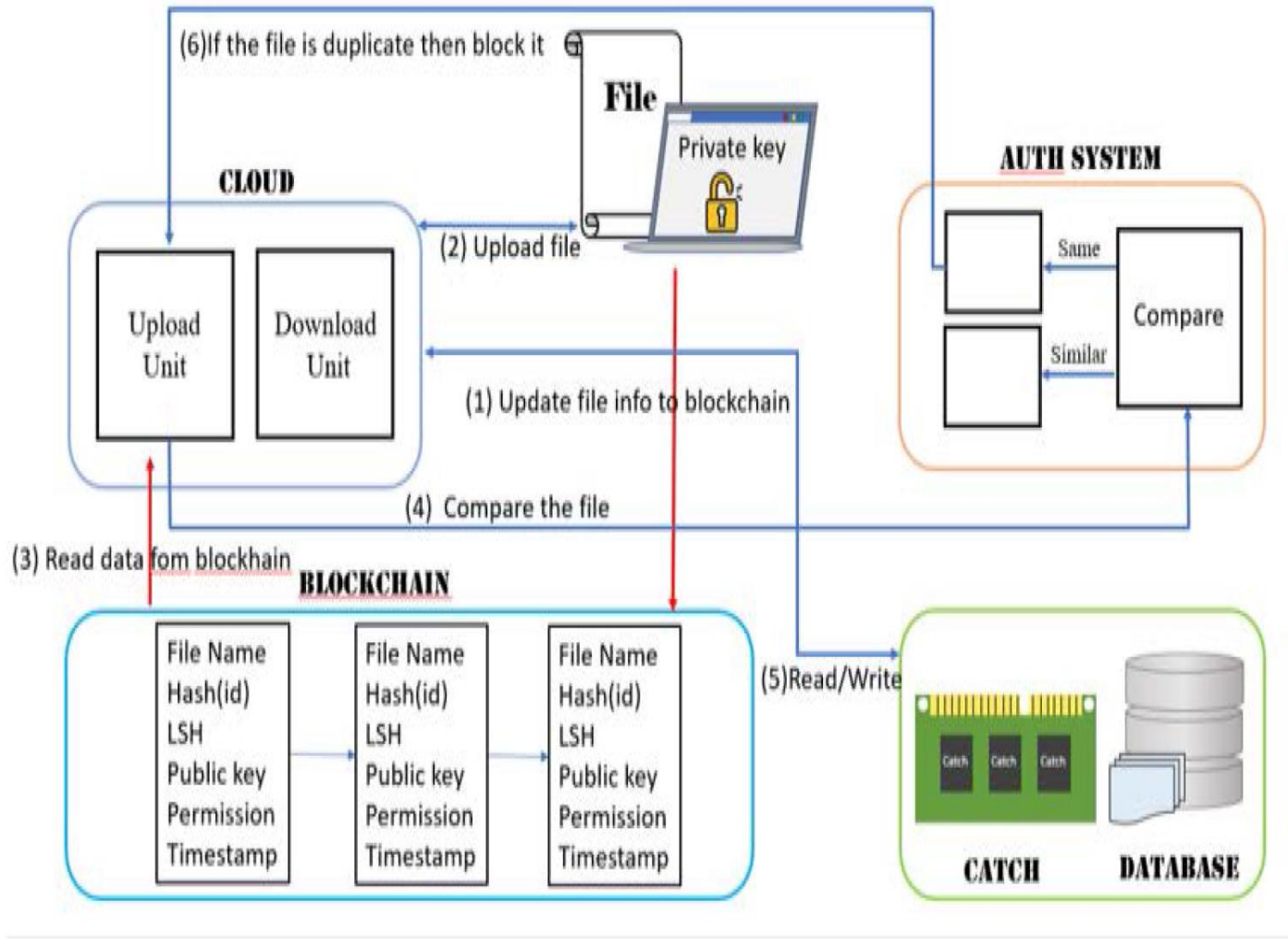
هذا النموذج يقدم عتاد الحوسبة كخدمة. بدلاً من شراء الأجهزة، يمكن للمؤسسات استئجار الأجهزة التي تحتاجها، مع إدارة وصيانة هذه الأجهزة من قبل مزود الخدمة.

مثال:

Dell Managed Services

HP Device as a Service (DaaS)

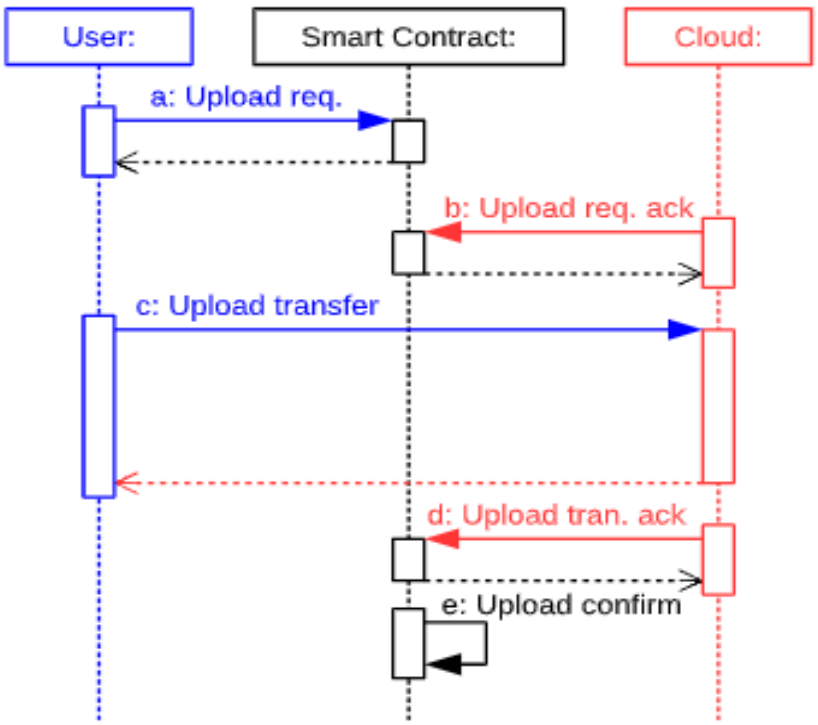
: [1] **Uploading on cloud using blockchain-5**



الشكل 4 Uploading on cloud using blockchain

يوضح الشكل 4 عملية تحميل الملفات على السحابة مع وجود تقنية ال BLOCKCHAIN التي توفر طبقة من الأمان والحماية ما بين المستخدم والسحابة [2].

تتم عملية تحميل الملفات على السحابة عن طريق مجموعة من الخطوات او التوابع كالأتي:



الشكل 5 UML sequence diagram for the interactions involved in the file upload operation.

a) Upload req : قبل إرسال ملف إلى السحابة، يبدأ المستخدم عملية التحميل باستخدام تابع العقد الذكي الذي يسمى UploadRequest(). يسجل هذا التابع طلب التحميل في blockchain، بما في ذلك معرف فريد للملف و hash للتحقق من سلامة الملف دون الكشف عن محتواه. . تتطلب هذه الطريقة(UploadRequest) معلمات إدخال مثل مسار الملف، الذي يعمل كمعرف فريد لملف المستخدم في مساحة تخزين السحابة، مما يضمن إدارة الملفات بشكل آمن وقابل للتتبع داخل النظام. يتم تخزين معرف الملف الذي تم تحميله إلى السحابة في دفتر الأستاذ blockchain للحفاظ على الخصوصية والأمان. ويجب ألا يحتوي هذا المعرف على تفاصيل من شأنها الكشف عن محتوى الملف أو الموقع الفعلي لضمان السرية وحماية البيانات داخل النظام.وكذلك تحتاج الطريقة الى ادخال hash لل hash الخاصة بالملف(يتم تشفير ال hash الخاصة بالملف). تعرف هذه العملية ب hash masking .

تضمن عملية التجزئة المزدوجة أمان وسلامة الملف الذي يتم تحميله عن طريق إخفاء hash الخاصة بالمحتوى الأصلي وتمكين التحقق عند الانتهاء من عملية التحميل. يساعد هذا الإجراء الأمني على منع الوصول غير المصرح به أو التلاعب بالملف أثناء عملية التحميل.

b) UploadRequestAck : بمجرد أن تتلقى السحابة المعاملة التي تخبرها بطلب التحميل من blockchain، يمكنها تأكيد القبول عن طريق إرسال رسالة إقرار التحميل (ACK) إلى المستخدم باستخدام طريقة UploadRequestAck(). يشير هذا الإقرار إلى أن السحابة جاهزة لاستقبال الملف للتحميل حسب طلب المستخدم، مما يضمن عملية آمنة وقابلة للتحقق داخل النظام القائم على blockchain.

c) upload transfer : بمجرد أن يتلقى المستخدم تأكيدًا لطلب التحميل من السحابة من خلال حدث ACK، يمكنه متابعة تحميل البيانات إلى وحدة التخزين السحابية. تضمن هذه العملية أن المستخدم يمكنه بدء نقل الملف بعد تلقي الإقرار من السحابة، والحفاظ على سلامة وأمن عملية التحميل.

d) upload tran .ask : بعد اكتمال تحميل الملف، تؤكد السحابة نجاح العملية عن طريق تخزين hash الملف في blockchain باستخدام طريقة UploadTransferAck(). يضمن هذا الإجراء إمكانية التحقق من سلامة الملف الذي تم تحميله من خلال مقارنة hash المخزن في blockchain مع الملف الذي قدمه المستخدم، مما يسمح بالتحقق من الصحة واحتمال رفض التحميل إذا لزم الأمر.

e) upload confirm : يتم استدعاء طريقة UploadConfirm() للتحقق من سلامة الملف الذي تم تحميله. تقارن هذه الطريقة hash الذي توفره السحابة مع البيانات التي حددها المستخدم في البداية، مما يؤكد أو يرفض hash الذي تقدمة السحابة. إذا فشلت المقارنة، فيجب على السحابة حذف الملف الذي تم تحميله. تضمن هذه العملية سلامة البيانات والمساءلة في عملية تحميل الملفات داخل النظام القائم على blockchain.

من خلال المراحل الموضحة، يمكن للأفراد ضمان دقة الملف الذي تم تحميله من خلال مقارنة hash المقدم من السحابة مع hash المقدم من المستخدم. تسمح آلية التحقق هذه بالتحقق من سلامة الملف واحتمال رفض التحميل في حالة العثور على تناقضات، مما يضمن الشفافية والمساءلة في عملية تحميل الملف داخل النظام القائم على blockchain.

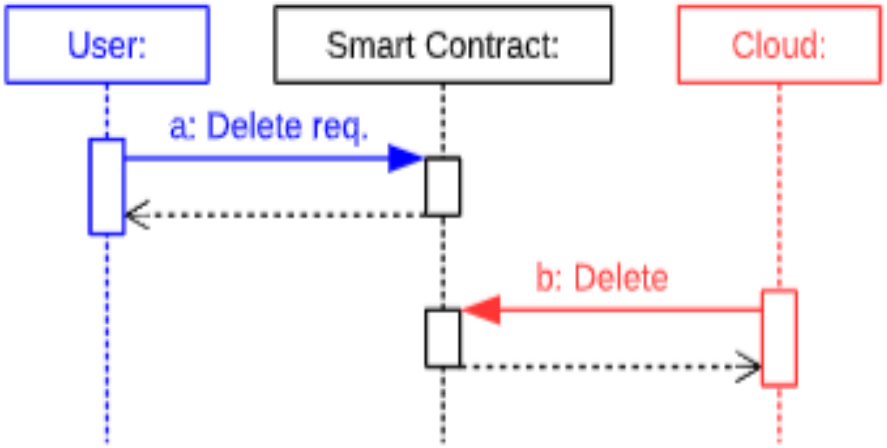
مزايا إضافية لاستخدام ال BLOCKCHAIN مع تحميل الملفات على السحابة [1]:

- ✓ في النظام القائم على blockchain لتحميل الملفات، لا يمكن لكل من المستخدم وموفر السحابة رفض تقديم طلب التحميل. وذلك لأن طلب التحميل الخاص بالمستخدم يتم تسجيله علنًا على blockchain (الطلب a)، تأكده السحابة بالرسالة b. حتى إذا كانت السحابة غير متاحة مؤقتًا أو لفترة من الوقت، فلا

يزال بإمكانها الوصول إلى الطلب على blockchain بمجرد تشغيلها مرة أخرى، مما يضمن الشفافية والمساءلة في عملية التحميل.

- ✓ لا يمكن لكل من المستخدم وموفر السحابة رفض نقل ملف لأنه يتم تخزين إقرار نقل التحميل الصريح الذي يحتوي على ملخص تجزئة الملف في blockchain. يمكن للمستخدم التحقق من صحة التجزئة وإعادة التحميل إذا كان هناك عدم تطابق، مما يضمن تطابق التجزئة مع التجزئة في طلب التحميل الأولي. تضمن هذه العملية المساءلة والنزاهة في عمليات نقل الملفات بين المستخدم وموفر السحابة.

Delete on cloud using blockchain-6 [1] :



الشكل 6 UML sequence diagram for the interactions involved in the file delete operation

يظهر الشكل 6 التفاعلات المطلوبة لحذف ملف من السحابة. وفيما يلي وصف لتنفيذ عملية الحذف

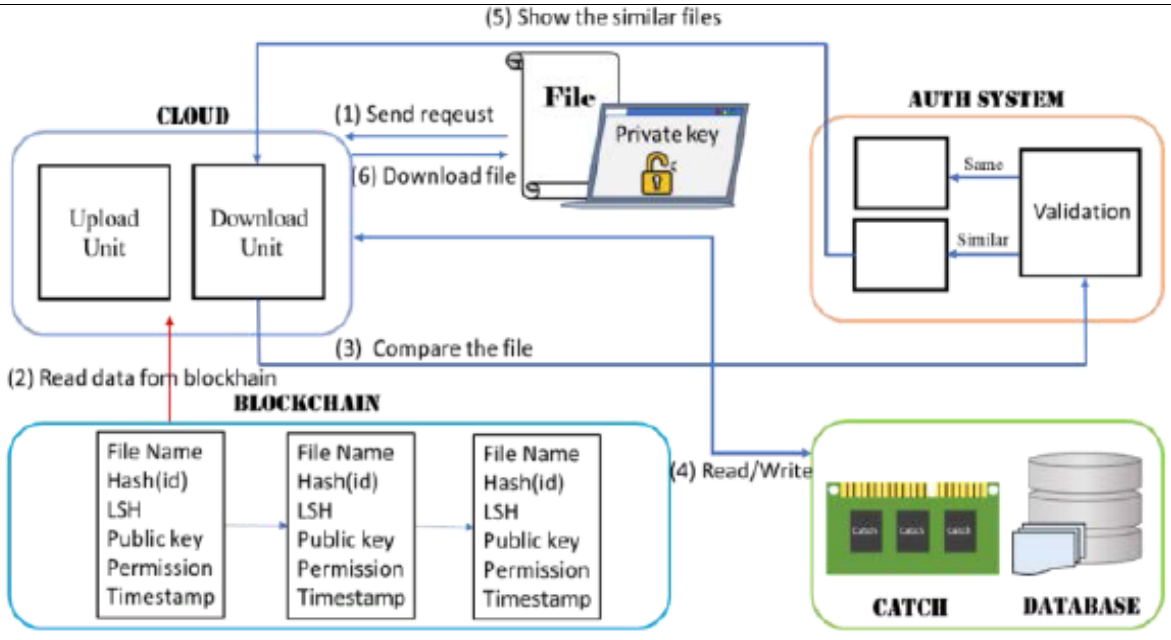
a) Delet req : عندما يريد المستخدم حذف ملف من السحابة، فإنه يبدأ العملية باستخدام طريقة RemoveRequest() مع معلمة مسار الملف. يؤدي هذا الإجراء إلى تشغيل السحابة لتلقي حدث طلب الحذف ومتابعة حذف الملف المحدد من وحدة التخزين الخاصة به. ويضمن التفاعل بدء عملية إزالة الملف وإكمالها بناءً على طلب المستخدم من خلال الطريقة المحددة.

b) delete : تتلقى السحابة حدث طلب حذف، وتحذف الملف المحدد، وتؤكد الاكتمال عن طريق تسجيل الحدث في blockchain باستخدام طريقة delete ()). تضمن هذه العملية المساءلة والشفافية من خلال توفير سجل دائم لعملية حذف الملف، والذي يمكن التحقق منه لاحقًا لحل النزاعات أو ضمان الامتثال لاتفاقيات مستوى الخدمة (SLAs).

مزايا إضافية لاستخدام ال BLOCKCHAIN مع حذف الملفات على السحابة [1]:

- ✓ يمكن حل النزاعات المستقبلية حول وجود أو عدم وجود ملف من خلال النظر في السجل. إذا طلب المستخدم ملفًا غير موجود في السحابة، فإن العقد الذكي يتحقق تلقائيًا مما إذا كان المستخدم قد طلب مسبقًا حذف هذا الملف. إذا كان هذا الطلب موجودًا، فهذا يعني أن السحابة قد حذفت هذا الملف بشكل صحيح؛ إذا لم يتم تسجيل أي طلب حذف لهذا الملف، فهذا يعني انتهاك اتفاقية مستوى الخدمة. علاوة على ذلك، إذا تبين أن السحابة تحتوي على نسخة من ملف يوجد طلب حذف ناجح وشرعي له في blockchain، فستكون السحابة مرة أخرى تنتهك اتفاقية مستوى الخدمة لأنها لم تقم بإزالة الملف بشكل صحيح كما هو مطلوب.
- ✓ بمجرد تسجيل عملية الحذف في blockchain (الرسالة b)، لا يمكن لكل من المستخدم والسحابة رفض الطلب (الرسالة a) أو الادعاء بفشل الحذف، حيث يتم تخزين الإقرار (الرسالة b) في blockchain. تضمن هذه الشفافية والثبات في blockchain المساءلة وتمنع النزاعات المتعلقة بعمليات الحذف في النظام السحابي.أي بشكل عام لا يمكن للمستخدم ولا السحابة الادعاء بأنه لم يتم طلب أي عملية حذف بالفعل، حيث تم تخزين الطلب المرئي للعامة في blockchain. علاوة على ذلك، لا يمكن للمستخدم ولا السحابة الادعاء بفشل عملية الحذف، وذلك بسبب تخزين الإقرار في blockchain أيضًا.

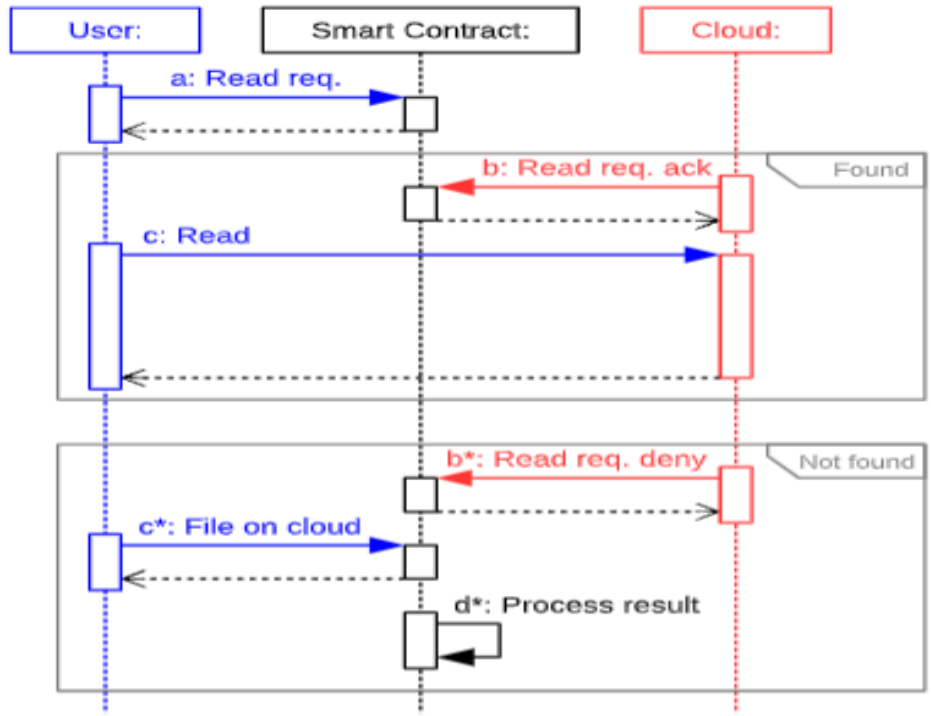
7-Downloading on cloud using blockchain [1] :



الشكل 7 Uploading on cloud using blockchain

يوضح الشكل 7 عملية تنزيل الملفات من السحابة مع وجود تقنية ال BLOCKCHAIN التي توفر طبقة من الأمان والحماية ما بين المستخدم والسحابة [2].

تتم عملية تنزيل الملفات من السحابة عن طريق مجموعة من الخطوات او التوابع كالأتي:



الشكل 8 UML sequence diagram for the interactions involved in the read request operation. Note the two branches that describe the behavior depending on the file's existence

يوضح الشكل 8 التفاعلات المطلوبة لقراءة ملف مخزن في السحابة. ما يلي هو وصف تنفيذ عملية القراءة:

a) **Read req** : للوصول إلى ملف مخزن في السحابة، يبدأ المستخدم طلبًا باستخدام طريقة ReadRequest() وتوفير مسار الملف كمدخل. يؤدي هذا الإجراء إلى تشغيل السحابة لمنح حق الوصول إلى الملف وتخزين عنوان URL في blockchain حتى يتمكن المستخدم من استرداد الملف. وتضمن العملية الشفافية والمساءلة من خلال تسجيل جميع التفاعلات في البلوكشين، مما يسمح بالتحقق من توفر الملف وسجل الوصول.

b) **Read req .ask** : ، يقوم النظام السحابي بتشغيل طريقة ReadRequestAck() ويسجل عنوان URL في blockchain للمستخدم لاسترداد الملف. تعمل هذه العملية كدليل على أن السحابة سمحت للمستخدم بالوصول وتؤكد صحة الملف الذي يتم الوصول إليه. يضمن حفظ السجلات الشفاف في blockchain المساءلة والنزاهة في عمليات الوصول إلى الملفات بين السحابة والمستخدم.

Read (c : بمجرد أن توفر السحابة للمستخدم عنوان URL، يمكن للمستخدم الوصول إلى الملف وقراءته باستخدام عنوان URL هذا. تضمن هذه العملية أن السحابة قد منحت حق الوصول للمستخدم وأن الملف صالح، كما هو مسجل في blockchain لأغراض التحقق.

read req.deny (b* : عندما تتلقى السحابة طلبًا لقراءة ملف لم يتم العثور عليه، فإنها تستجيب عن طريق إرسال رسالة تشير إلى أن الملف مفقود من خلال عملية ReadRequestDeny().يتم تسجيل التفاعل في blockchain، مما يسمح لكل من السحابة والمستخدم بالتحقق من حالة طلب الملف ومنع أي انتهاكات محتملة لاتفاقية مستوى الخدمة.

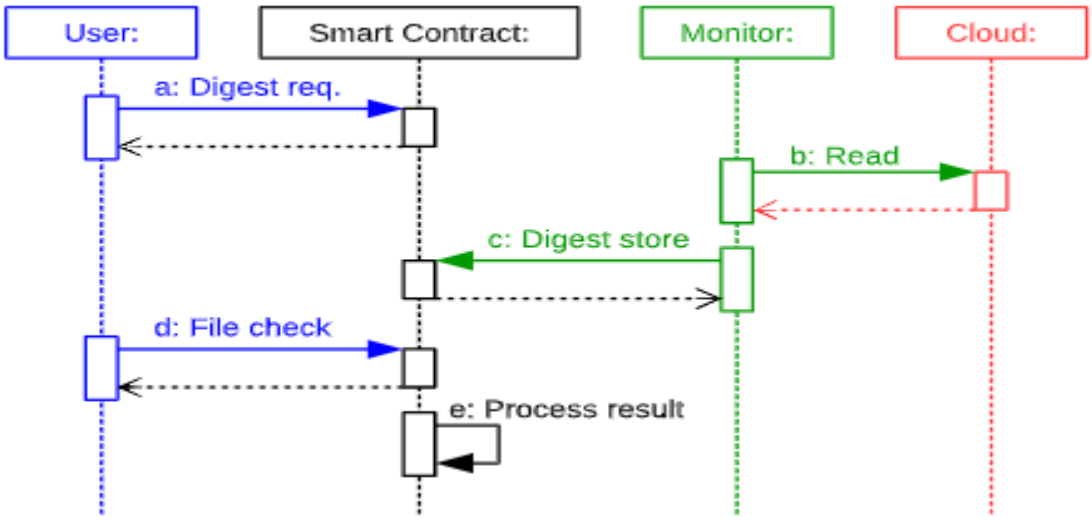
file on cloud (c* : يمكن للمستخدم تقييم ما إذا كان هناك انتهاك لاتفاقية مستوى الخدمة (SLA) عن طريق تنفيذ عملية FileOnCloud(). تقوم هذه الطريقة بتحليل تخزين العقد الذكي الذي يسجل كافة العمليات ويحدد ما إذا كانت هناك أي انتهاكات لاتفاقية مستوى الخدمة (SLA) قد حدثت.

process result(d* : نتيجة عملية FileOnCloud، والتي تتحقق من انتهاكات اتفاقية مستوى الخدمة من خلال تحليل تخزين العقد الذكي. يتم تسجيلها على blockchain من أجل الشفافية والمساءلة، مما يضمن تخزين جميع التفاعلات والنتائج بشكل دائم وإمكانية التحقق منها من قبل جميع الأطراف المعنية.

مزايا إضافية لاستخدام ال BLOCKCHAIN مع تنزيل الملفات من السحابة [1]:

- ✓ بعد تخزين الرسالة (طلب القراءة) في blockchain، يمكن توقع النتيجة المتوقعة من خلال مراجعة سجل جميع العمليات السابقة المتعلقة بنفس الملف. في الواقع، لا يمكن للمستخدم تحميل السحابة مسؤولية عدم توفر ملف لم يقم المستخدم بتحميله، حيث يمكن للسحابة ببساطة الإشارة إلى عدم وجود عملية تحميل مطابقة في السجل القابل للقراءة بشكل عام. وبالمثل، لا يمكن للسحابة تحميل المستخدم مسؤولية عدم توفر الملف الذي يجب أن يكون موجودًا بالفعل، حيث يمكن للمستخدم الإشارة إلى عملية تحميل سابقة لم يتبعها أي طلب حذف في دفتر الأستاذ العام. المبدأ الأساسي هو أن تاريخ جميع التفاعلات يتم تخزينه بشكل دائم في blockchain بطريقة مقاومة للتلاعب، بحيث يمكن لأي شخص التحقق من توفر (أو عدم وجود) كل ملف في أي وقت من خلال مراجعة سجل المعاملات.

8- OFF-CHAIN MONITORING :[1]



الشكل 9 UML sequence diagram for the interactions involved with a monitoring request operation

- عند كل تنفيذ لطريقة ما في العقد الذكي ، يتم تنفيذ بعض عمليات التحقق من سلامة التشغيل والملفات بشكل مستقل قبل أن تتمكن الطريقة من متابعة سلوكها المطبق. على سبيل المثال، يتحقق ReadRequest() من أن الملف قد تم تحميله بالفعل قبل إنشاء الطلب، ويتحقق UploadTransferAck() من سلامة الملف.
- إن قراءة ملف مباشرة من السحابة باستخدام عنوان URL الخاص بـ blockchain تتطلب عملية خارج السلسلة تتضمن monitor، والتي تعمل كوسيط بين blockchain والسحابة لسيناريوهات مراقبة محددة.
- بعد عملية الحذف، يمكن للمراقب التحقق مما إذا كانت السحابة لا تزال تحتفظ بنسخة من الملف الذي كان من المفترض حذفه. يعمل المراقب ككيان مستقل للإشراف على إجراءات مزود الخدمة السحابية والتحقق من صحتها، مما يعزز الشفافية والثقة في النظام.
- بعد عملية القراءة، يمكن للمراقب التحقق مما إذا كانت السحابة قد أفسدت محتوى الملف، أي إذا كان hash المخزن أثناء التحميل مختلفًا عن hash البيانات التي تمت قراءتها مرة أخرى باستخدام عملية القراءة.
- يوضح الشكل 9 سلوك الكيانات المعنية عندما يطلب المستخدم من المراقب فحص ملف. ما يلي هو وصف عملية monitor :

a) digest req. : يبدأ المستخدم عملية فحص عن طريق استدعاء طريقة العقد الذكية DigestRequest(). يسجل هذا الإجراء طلبًا لاسترداد ملف من السحابة وتخزين hash على blockchain، مع استخدام عنوان URL للملف كمدخل لهذه العملية.

b) read: عندما يتلقى جهاز المراقبة معاملة تتضمن حدث طلب digest من blockchain، يمكنه المتابعة لتلبية الطلب من خلال قراءة الملف من السحابة باستخدام عنوان URL المحدد. تسمح هذه العملية للمراقب بالتحقق من سلامة الملف من خلال مقارنة digest ل hash الخاص به مع الملف المخزن مسبقًا أثناء عملية التحميل، مما يضمن اتساق البيانات وأمنها في النظام السحابي.

c) Digest store: : بمجرد أن يقرأ جهاز المراقبة الملف ويحسب المعرف الفريد الخاص به والذي يسمى Hash Digest، يمكنه تخزين هذا المعرف بشكل آمن في blockchain باستخدام طريقة DigestStore(). تضمن هذه العملية إمكانية التحقق من سلامة الملف لاحقًا من خلال مقارنة Hash Digest المخزن مع تلك المحسوبة من الملف، مما يوفر طريقة موثوقة لتتبع صحة الملف والتحقق منها داخل شبكة blockchain.

d) file check : بعد أن يقوم جهاز المراقبة بتخزين Hash Digest للملف في blockchain، يتلقى المستخدم معاملة تحتوي على هذه المعلومات. يمكن للمستخدم بعد ذلك تشغيل طريقة FileCheck() بمعاملة جديدة لمقارنة Hash Digest لملف جهاز المراقبة مع Hash Digest الأصلي المخزن بواسطة السحابة أثناء عملية التحميل. تساعد هذه المقارنة في تحديد أي اختلافات وانتهاكات محتملة لاتفاقية مستوى الخدمة (SLA) بين المستخدم وموفر السحابة.

e) process result : تؤدي طريقة FileCheck() هذه إلى تشغيل بعض العمليات التي يتم من خلالها استرداد Hash Digest لملف جهاز المراقبة ومقارنته Hash Digest للملف الأصلي، الذي تم تخزينه مسبقًا بواسطة السحابة أثناء عملية التحميل. إذا كان الملخصان مختلفين، فقد حدث انتهاك لاتفاقية مستوى الخدمة. وبالتالي، اعتمادًا على الحالة، قد يؤدي ذلك إلى فرض عقوبة، يدفعها مزود السحابة تلقائيًا من خلال العقد الذكي.

مزايا إضافية لاستخدام ال BLOCKCHAIN مع MONITORING [1]**:**

- ✓ كما هو الحال مع طلبات التحميل والحذف، يمكن التحقق من نتائج عملية المراقبة من قبل أي شخص لديه حق الوصول إلى blockchain من خلال مراجعة تسلسل العمليات المتعلقة بملف معين.
- ✓ موفر السحابة لا يمكنه إنشاء عمليات تحميل أو حذف زائفة نيابة عن المستخدم لأن بيانات الاعتماد الخاصة للمستخدم مطلوبة لتوقيع المعاملات على blockchain.

- ✓ لا يمكن للمستخدم اختلاق عملية تحميل أو حذف ملف لم تحدث لأنه لا يمكنه التوقيع على معاملة blockchain بدون بيانات اعتماد السحابة. يضمن هذا النظام سلامة العمليات وصحتها من خلال طلب بيانات الاعتماد المناسبة لكل طرف مشارك في عملية المعاملة.
- ✓ جهاز المراقبة لا يمكنه التلاعب بنتائج عملية Digest Store من خلال الادعاء الكاذب بوجود تناقضات في محتوى الملف أو توفره. وذلك لأنه يمكن التحقق من أي انحراف عن النتيجة المتوقعة بشكل مستقل عن طريق التحقق من Hash Digest للملف المضمنة في عمليات الملف السابقة المخزنة على blockchain.

9- Challenges in blockchain–Cloud integration [4]:

- ➢ ان دمج تقنية blockchain مع أنظمة الحوسبة السحابية يتطلب ضرورة توقيع المعاملات على شبكة blockchain رقميًا، مما يستلزم أنظمة حوسبة سحابية تدعم هذه الوظيفة. تطرح عملية التكامل هذه تعقيدات مختلفة تحتاج إلى معالجة لضمان التشغيل السلس بين تقنيات blockchain والسحابة.
- ➢ العدد الهائل من التطبيقات والتقنيات في الحوسبة السحابية، مما قد يؤدي إلى تعقيد عملية التكامل.
- ➢ في تقنية Blockchain، تمثل سعة التخزين وقابلية التوسع تحديات كبيرة. مع نمو سلسلة Blockchain مع كل كتلة جديدة، تزداد متطلبات التخزين، مما يؤثر على أداء النظام وقابلية التوسع. يجب أن تقوم العقد الكاملة، التي تتحقق من صحة المعاملات، بتخزين السلسلة بأكملها، مما يؤدي إلى تأخير المزامنة وزيادة الطلب على الموارد مع توسع حجم Blockchain.
- ➢ الهجمات الأمنية التي تتعرض لها BLOCKCHAIN

:REFERENCES -10

1. Zichichi, M., D'Angelo, G., Ferretti, S., & Marzolla, M. (2023). Accountable clouds through blockchain. *IEEE Access*, *11*, 48358-48374.

2. Tsai, W., Chou, T., Chen, J., Ma, Y. (2020). Blockchain as a platform for secure cloud computing services. *2020 22nd International Conference on Advanced Communication Technology (ICACT)*.

3. Karthik Kumar Vaigandla, Mounika Siluveru, Madhavi kesoju, & RadhaKrishna Karne. (2023). Review on blockchain technology : Architecture, characteristics, benefits, algorithms, challenges and applications. *Mesopotamian Journal of Cyber Security*.

4. Alshinwan, M., Shdefat, A. Y., Mostafa, N., AlSokkar, A. A., Alsarhan, T., & Almajali, D. (2023). Integrated cloud computing and blockchain systems: A review. *International Journal of Data and Network Science*, *7*(2), 941-956.