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

# Electronic voting system based on BlockChain technology

# نظام التصويت الالكتروني المعتمد على تقنية BlockChain

إعداد: م. نوح عبود
إشراف: د. أحمد أحمد

2024/2023

Contents

## 1)ABSTRACT(1) :

يقدم هذا التقرير إطار عمل يعتمد على تقنية blockchain الحديثة التي توفر أقصى قدر من الشفافية والموثوقية للنظام لبناء علاقة ثقة بين الناخبين والسلطات الانتخابية. يوفر إطار العمل المقترح إطارًا يمكن تنفيذه لإجراء نشاط التصويت الكترونيا من خلال blockchain دون إشراك أي مراكز اقتراع فعلية. يدعم إطار العمل المقترح لدينا سلسلة الكتل القابلة للتطوير، وذلك باستخدام خوارزميات الإجماع المرنة FLEXIBLE CONSENSUS ALGORITHM. إن خوارزمية أمان السلسلة المطبقة Chain Security Algorithm في نظام التصويت تجعل معاملة التصويت أكثر أمانًا. توفر العقود الذكية اتصالاً آمنًا بين المستخدم والشبكة أثناء تنفيذ المعاملة في السلسلة. تمت أيضًا مناقشة أمان نظام التصويت القائم على blockchain. بالإضافة إلى ذلك، تم أيضًا تطوير تشفير المعاملات باستخدام تجزئة التشفيرCRYPTOGRAPHIC HASH .وأخيرًا، يوضح تقييم أداء النظام المقترح أنه يمكن تنفيذ النظام على نطاق واسع يحوي تعداد كبير للسكان.

## 2. INTRODUCTION (1):

أجهزة التصويت التقليدية المتصلة بقواعد بيانات مركزية يمكن أن تكون عرضه للتلاعب ويمكن ان تتم مهاجمة قاعدة البيانات المركزية مما يؤدي الى فشل عملية التصويت بالكامل كما ان عملية التصويت التقليدية تتطلب حضور الناخب الى أماكن التصويت ولا يوجد أي ضمان لسلامة عملية التصويت حيث قد يتم التلاعب بنتيجة التصويت من قبل طرف أخر ولا يوجد ضمان للناخب لخصوصية بياناته واعتبار تصويته مما يجعل العملية التقليدية تعاني من قلة الأمان والنزاهه .الامر الذي دفع الى استخدام الرقمنة بعملية التصويت والتي حلت بعض المشاكل المتعلقة بالخصوصية وتسهيل عملية التصويت الا أنها بدورها تعاني من المشاكل المتعلقة بالمركزية والتي تعني أن فشل النظام المركزي سيؤدي الى فشل عملية التصويت بالكامل .وهذا ما دفع الى استخدام blockchain غير قابل للتغيير للتصويت والذي يضمن تخزين البيانات بطريقة لا مركزية، مما يجعلها مقاومة للتلاعب وتوفر نظامًا موثوقًا وآمنًا للتصويت دون التعرض لخطر التخريب الفردي.ويضمن خصوصية المشاركين وأهليتهم للقيام بعملية التصويت وضمان عدم تكرار التصويت أو التلاعب به.

## 3. BLOCKCHAIN (2):

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. 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:

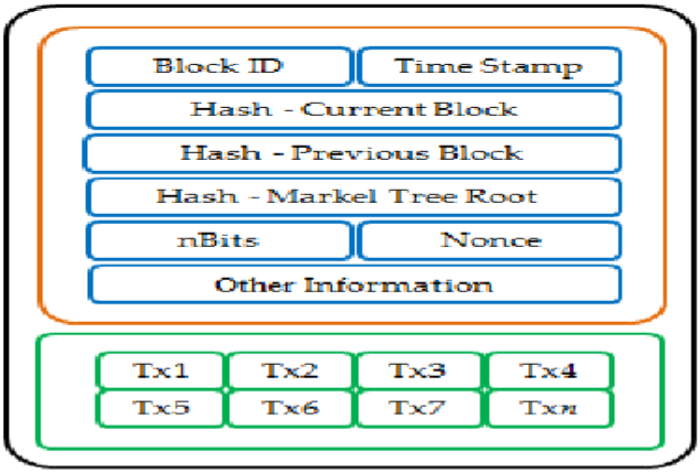
- **head** :الذي يحتوي على بيانات وصفية مثل hash الخاص بالكتلة السابقة والطابع الزمني
- **Block Body**: يحتوي على معلومات المعاملة
- **Hash** : يعمل كمعرف فريد للكتلة وهوبمثابة بصمة رقمية, يتم ربط الكتل من خلال hash الخاص بكل منها وبالتالي فإن blockchain تضمن أنه بمجرد إضافة كتلة، لا يمكن تغييرها أو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

- يعتمد إطار عمل (BC) blockchain 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(2) :




الشكل 1 Block Structure

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

### 1.1.3 block header (metadata):

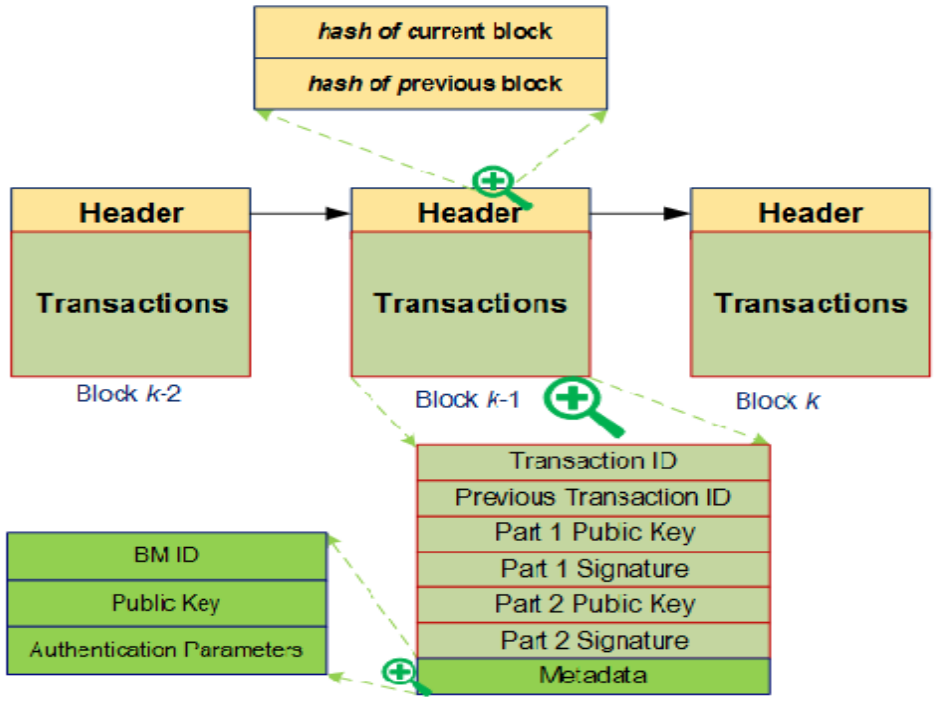
يحتوي رأس الكتلة على القيم التاليه:

- 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 hash تشفير فريدة تمثل جميع المعاملات الموجودة داخل كتلة في blockchain. ويتم حسابها من خلال الجمع بين hash الخاصة بالمعاملات الفردية بطريقة محددة لإنشاء قيمة Hash 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 Hash الكتلة الصالحة. تساعد هذه المعلمة في تحديد مستوى الصعوبة المطلوب لكي تعتبر Hash 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 :

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 2

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 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 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 إنشاءه 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 الـMetadata يتم 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 (2):

- ✓ 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 من خلال 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.

## 4. FLEXIBLE CONSENSUS ALGORITHM (1):

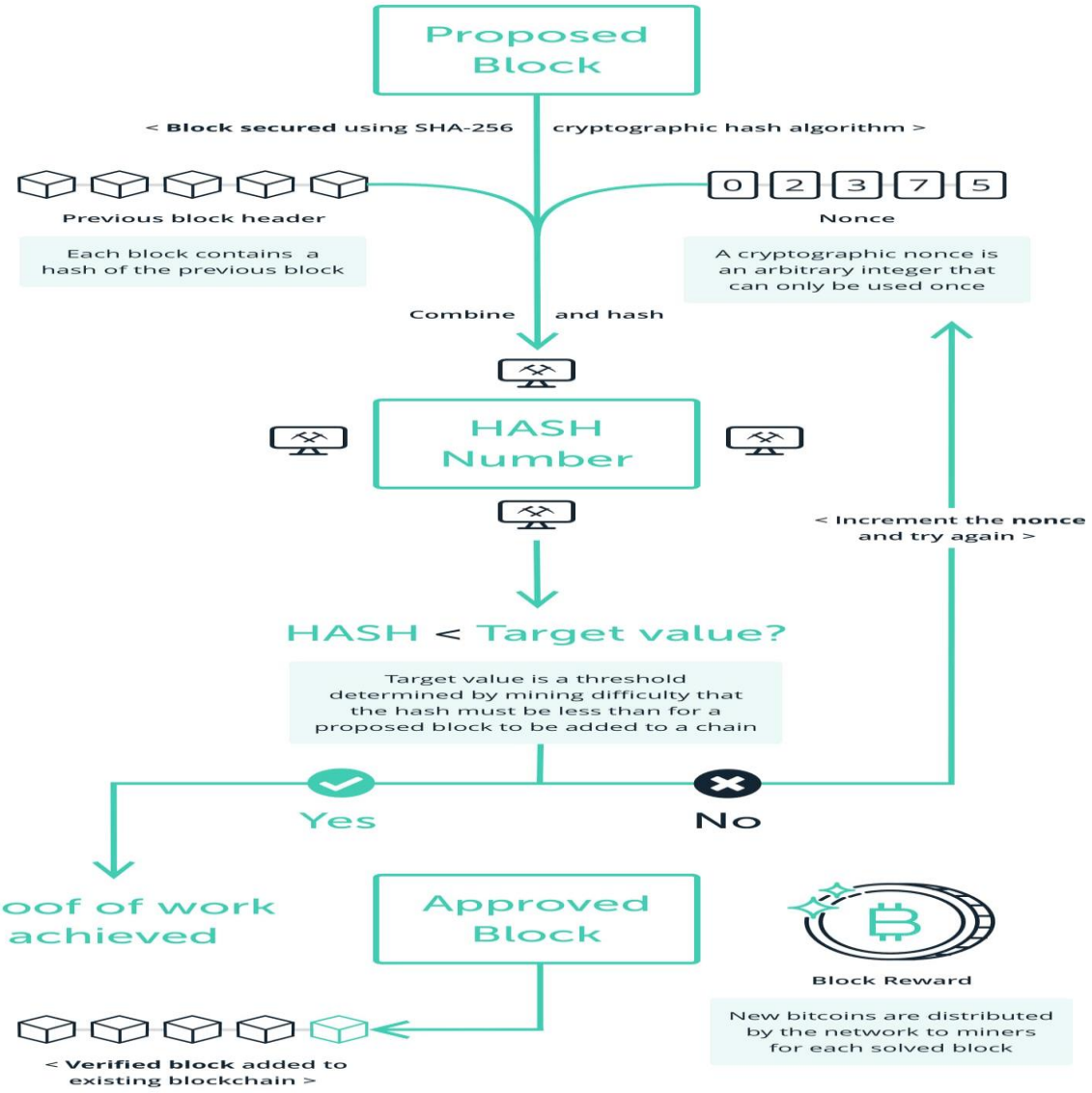
- لكي يتم إضافة كتلة جديدة الى السلسلة يجب ان تتفق جميع العقد الموجودة على شبكة البلوكشين على ذلك .
- يتم استخدم خوارزمية إجماع إثبات العملProof of Work (PoW) لضمان كفاءة blockchain أثناء أنشطة التصويت. تتطلب الخوارزمية مستوى محددًا من القوة الحسابية للتحقق من صحة المعاملات، وتعزيز أمان وأداء النظام.
- يمكن تطبيق خوارزميات إجماع مختلفة مثل Ripple وإثبات التصويت Proof of Vote وإثبات الثقة Proof of Trust وإثبات الحصة Proof of Stake .
- 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.

### 1.4 خوارزمية POW (2):

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 PoWأشهر 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 3):

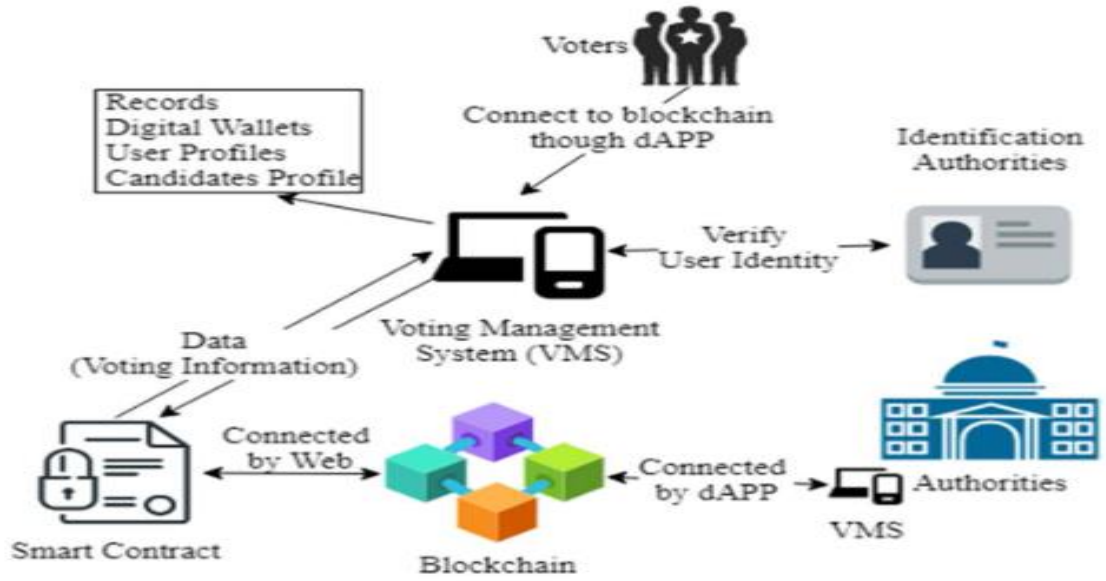
1. يتم جمع مجموعة من المعاملات في بلوك وتشفيرها بواسطة تابع هاش .(Hash function) يتم تضمين قيمة hash للبلوك السابق في بيانات البلوك الجديد.
2. يقوم المُعدّنون بمحاولة حل مشكلة الحصول على دليل العمل (Proof of Work) من خلال تجربة قيم hash مختلفة حتى يتم العثور على قيمة hash تفي بشروط معينة. يتم تجربة القيم 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 3 proof of work

# .5 PROPOSED FRAMEWORK OF VOTING SYSTEM (1) :




الشكل 4 PROPOSED FRAMEWORK OF VOTING SYSTEM

يوضح الشكل 4 إطار العمل المتبع لنظام التصويت الالكتروني وفيما يلي شرح لمكونات هذا الاطار:

- dAPP : تطبيق لامركزي يمكن أن يكون تطبيقًا للهاتف المحمول أو بوابة ويب، يتصل الناخبون بنظام إدارة التصويتVMS من خلاله ,يحوي واجهة سهلة الاستخدام تمكن الناخب من اختيار صوته والحصول على نتيجة التصويت.

- Identification Authorities : مسؤولة عن التحقق من هوية الناخبين المسجلين في النظام و السماح للناخبين المؤهلين فقط بالمشاركة في عملية التصويت

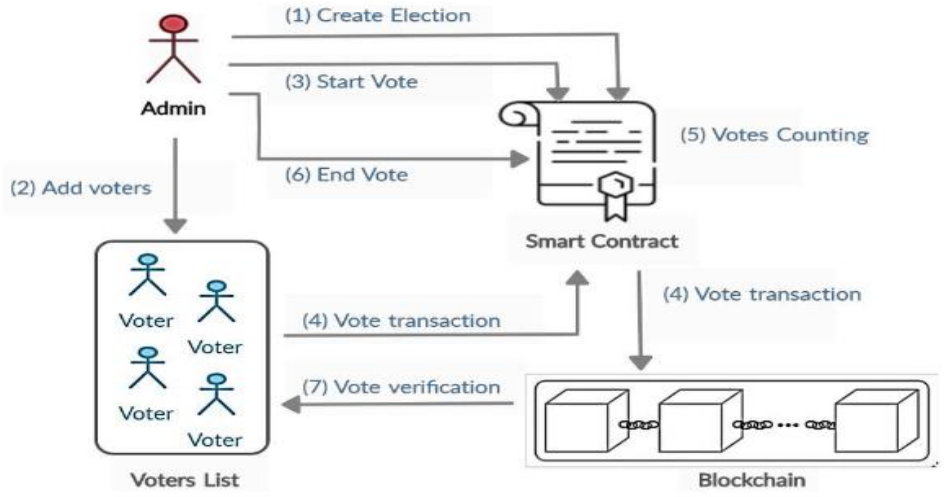
- VMS:voiting management system نظام إدارة التصويت. نظام يستخدم تقنية blockchain لتعزيز الشفافية والأمن والكفاءة في عملية التصويت. يهدف نظام VMS إلى معالجة مشكلات مثل حماية هوية الناخب، وإدارة زمن الوصول، والتحقق الشامل، ومنع الأنشطة الضارة أثناء التصويت من خلال دمج ميزات مثل خوارزميات الإجماع المرنة( flexible consensus

algorithms)، ووظائف تجزئة التشفير(cryptographic hash functions)، والعقود الذكية(smart contracts.)

وهذه بعض النقاط الأساسية حول هذا النظام:

- . يوفر النظام وصولاً كاملاً وعادلاً لكل مستخدم أثناء نشاط التصويت. كما يوفر إمكانية التتبع بعد التصويت.
- يضمن نظام التصويت الوصول المتساوي لجميع المستخدمين أثناء عملية التصويت.
- يقوم الناخبون بالتسجيل باستخدام بيانات اعتمادهم، ويتحقق النظام من هويتهم لمنع تعدد الأصوات من خلال تزويد كل ناخب بعملة تصويت واحدة (VC) للإدلاء بصوته.
- يستخدم نظام VMS تفاصيل هوية الناخبين ويتحقق منها من خلال سجلات Identification Authorities (IA) عبر الإنترنت لتسجيل الناخب في النظام.
- يتلقى المستخدم كلمة مرور لمرة واحدة (OTP) فريدة لتسجيل الدخول إلى النظام.
- بعد التسجيل بنجاح في النظام، تتم إضافة عملة تصويت واحدة (VC) إلى محفظة كل ناخب. لمنع الناخبين من التصويت أكثر من مرة.
- تسمح الطبيعة اللامركزية للنظام بالمعالجة الفعالة عبر جميع العقد، مما يضمن أنه في حالة تعرض عقدة واحدة للخطر، تظل العقد الأخرى غير متأثرة ويمكن أن تساعد في إعادة العقدة المعرضة للخطر.

## 6. **Stages of the blockchain-based electronic voting process.** (3):




الشكل 5 مرحل عملية التصويت

يعمل نظام التصويت الالكتروني المعتمد على تقنية ال blockchain من خلال مجموعة من المراحل (الشكل 5):

1) Create election: عملية يقوم من خلالها مسؤول الانتخابات بتنفيذ عقد ذكي على blockchain. يتضمن هذا الإجراء نشر قواعد ومعايير الانتخابات على blockchain، مما يسمح بعملية تصويت آمنة وشفافة تتم إدارتها بواسطة العقد الذكي

2) Add voters: العملية التي يمكن للمسؤول من خلالها تحديد قائمة الناخبين المؤهلين المصرح لهم بالمشاركة في عملية التصويت. يتم تخصيص محفظة فريدة لكل ناخب، والتي تعمل بمثابة هويته الرقمية للإدلاء بأصواته بشكل آمن وشفاف على شبكة blockchain. تضمن هذه الطريقة أن الناخبين المسجلين الذين لديهم محافظ مخصصة فقط هم من يمكنهم المشاركة في عملية التصويت، مما يعزز أمن ونزاهة النظام الانتخابي.

3) Start vote : بمجرد أن يبدأ المسؤول عملية التصويت، لا يمكن تسجيل أي ناخبين جدد للتصويت. يُسمح فقط للأفراد الذين تم تسجيلهم بالفعل قبل بدء الانتخابات بالمشاركة في عملية التصويت. ويضمن هذا التقييد نزاهة الانتخابات وأمنها من خلال منع أي أفراد غير مرخص لهم من الإدلاء بأصواتهم.

4) Vote transaction: تحدث معاملة التصويت عندما يختار الناخب مرشحًا ويقدم تصويتًا. يتحقق العقد الذكي مما إذا كانت محفظة العنوان مملوكة لناخب مقروء من قائمة الناخبين وأيضًا لم يصوت مسبقًا إذا كان الأمر كذلك، فسيتم تأكيد التصويت و بث المعاملات إلى blockchain .تضمن هذه العملية أن الناخبين الشرعيين فقط هم من يمكنهم المشاركة في الانتخابات ويمنع التصويت المزدوج.

5) Vote counting : تتم عملية فرز الأصوات بشكل آلي من خلال عقد ذكي. تم تصميم هذا العقد الذكي لإحصاء الأصوات من خلال تحليل معاملات التصويت المسجلة على blockchain، مما يضمن عملية تصويت شفافة ودقيقة. يؤدي استخدام تقنية blockchain إلى تعزيز الأمن والخصوصية والشفافية في نظام التصويت الإلكتروني، مما يوفر منصة لا مركزية وآمنة للمواطنين للمشاركة في الانتخابات.

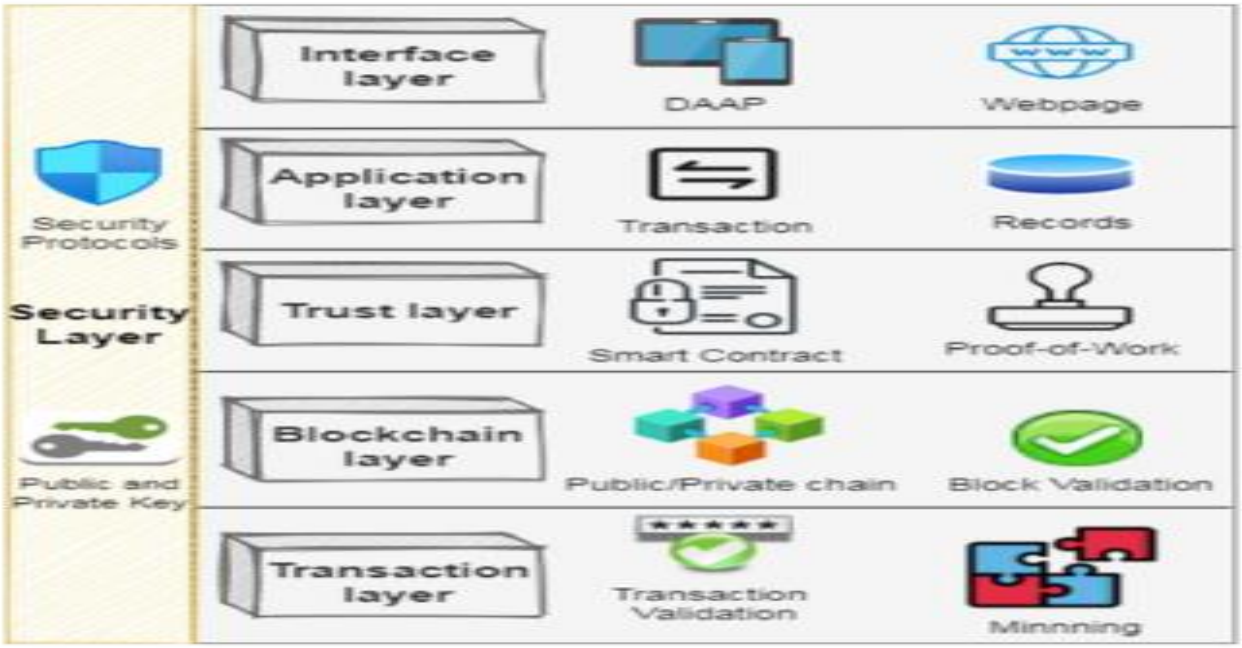
6) End vote : يشير إجراء "إنهاء التصويت" إلى قدرة المسؤول على إغلاق عملية الانتخابات رسميًا بمجرد اكتمال التصويت. ويمنع هذا الإجراء أي تصويت آخر ويدل على انتهاء الانتخابات، مما يضمن نزاهة وأمن عملية التصويت.

7)Vote verification : تتيح عملية التحقق من التصويت للناخبين استخدام معرف المعاملة الفريد الخاص بهم للوصول إلى تفاصيل معاملاتهم وعرض نتائج الانتخابات. وتضمن آلية التحقق هذه الشفافية والمساءلة في عملية التصويت، مما يمكّن الناخبين من تأكيد مشاركتهم والتحقق من نتائج الانتخابات بشكل آمن من خلال شبكة البلوكشين .

## 7. WORKFLOW OF PROPOSED MODEL (1) :

- يقوم الناخب بالاتصال ب VSM من خلال ال VSM. DAPP يرتبط مع وحدة Identification Authorities المسوؤلة عن التحقق من صحة البيانات التي قام المستخدم بادخالها والتأكد بأنة يحق له التصويت .
- يتحقق نظام إدارة الناخبين (VMS) من أهلية الناخب للتصويت عن طريق التحقق من blockchain بحثًا عن تجزئة المعاملات الحالية المرتبطة بالهوية الوطنية المحوسبة للناخب. إذا تم العثور على تجزئة معاملة مقابل بطاقة الهوية الوطنية المحوسبة للناخب، فإن نظام VMS يرفض الطلب ويسجل خروج الناخب من النظام. إذا لم يصوت الناخب بعد، فسيتم تحويل الطلب إلى minors .
- تتم مراقبة المعاملة بمساعدة تجزئة المعاملة ويتم تنفيذها بواسطة minors. ثم تتم إضافة المعاملة إلى سلسلة ال blockchain.
- يتم إنشاء معاملة مقابل الهوية الوطنية للناخب لكل صوت يتم الإدلاء به.
- يُمنح كل ناخب عملة تصويت واحدة (VC) للإدلاء بصوت واحد. بمجرد أن يستخدم الناخب عملة التصويت الخاصة به للإدلاء بصوته، فلن يتمكن من الإدلاء بصوت أخر حيث يتم تحديث محفظة الناخب إلى عملات تصويت صفرية(قيمتها 0)، مما يمنعه من التصويت عدة مرات.
- يمكن لأي شخص أن يشارك في التصويت من أي مكان، يتم التحقق من هويته الوطنية المحوسبة من خلال قاعدة البيانات الوطنية حتى يتمكن من الإدلاء بصوته.
- يضيف كل صوت كتلة جديدة في السلسلة و لا يتم تحديث رصيد عملة التصويت vote coin وبالتالي يضمن النظام عدم الإدلاء بأي أصوات مزدوجة من قبل الناخب.
- يضمن النظام سلامة الأصوات باستخدام وظائف التجزئة المشفرةcryptographic hash لتأمين كل صوت ككتلة جديدة في السلسلة.
- عند اكتمال المعاملة وإضافة العقدة بنجاح إلى سلسلة التصويت، يتم إخبار الناخب بمعاملة التصويت المحددة هذه من خلال رسالة نصية قصيرة إلى رقم هاتفه المسجل أوبريده الإلكتروني تحوي تجزئةhash معاملتة الفريدةوالتي يمكنه من خلالها التحقق من تصويته.

## 8. LAYERED STRUCTURE OF THE PROPOSED VMS (1):




الشكل 6 LAYERED STRUCTURE OF THE PROPOSED VMS

يوضح الشكل 6 طبقات نظام إدارة التصويت المقترح :

- interface layer : تعمل طبقة الواجهة كنقطة دخول للمستخدمين والمسؤولين من خلال التطبيقات الموزعة (dAAPs). تهدف هذه الطبقة إلى توفير واجهة سهلة الاستخدام للتعامل مع النظام وتسهيل الاتصالات لجميع المشاركين في عملية التصويت. تتيح dAAPs الموجودة داخل طبقة الواجهة التفاعل السلس مع نظام إدارة التصويت (VMS) للحصول على تجربة تصويت شفافة
- Application Layer : تعمل طبقة التطبيق كواجهة أمامية تدير التحقق من المستخدم باستخدام مصادر خارجية مثل بطاقات الهوية الوطنية.
- Trust layer : وهي مسؤولة عن التحقق من صحة كل كتلة جديدة تضاف إلى blockchain، ونقل البيانات بشكل آمن من خلال العقود الذكية.
- blockchain layer : تقوم طبقة blockchain بتخزين المعلومات الأساسية مثل المفاتيح العامة والخاصة وبيانات المعاملات . تضمن هذه الطبقة أمان وثبات blockchain من خلال إدارة المعلومات الأساسية ومراقبة السلسلة بحثًا عن أي مخالفات أو تغييرات غير مصرح بها. فهي تلعب دورًا حاسمًا في حماية عملية التصويت والحفاظ على شفافية النظام ومصداقيته.
- transaction layer: تشير طبقة المعاملات في الإطار إلى الجزء الذي تتم فيه جميع المعاملات بين نظام إدارة التصويت (VMS) والناخبين باستخدام العقود الذكية. هذه الطبقة مسؤولة عن معالجة

وتسجيل جميع المعاملات من خلال عملية تسمى التعدين، والتي تضمن أمان وسلامة شبكة البلوكشين من خلال التحقق من المعاملات وإضافتها إلى البلوكشين. تعمل العقود الذكية على تسهيل التفاعلات الشفافة والآمنة بين نظام إدارة التصويت (VMS) والناخبين داخل نظام blockchain.

- security layer : تهتم بحماية النظام من الهجمات. يتم استخدم الخوارزميات والقواعد لردع التهديدات الخارجية وحماية السلسلة. من خلال تنفيذ بروتوكولات الأمان واستخدام المفاتيح الخاصة والعامة، تظل البيانات داخل النظام مشفرة وآمنة، مما يضمن سلامة شبكة blockchain بأكملها.

## 9. ELECTION AS A SMART CONTRACT (1):

- تساعد العقود الذكية في الحفاظ على سلامة نظام التصويت من خلال التحقق من إجراءات المستخدم وتسجيل المعاملات بدقة على blockchain.
- تعمل العقود الذكية كقواعد آمنة تحكم المعاملات داخل الشبكة. وهي تضمن التزام جميع العقد في النظام بشروط محددة عند حفظ الأصوات.

### 1. مستخدم جديد(الشكل 7):

أثناء تسجيل مستخدم جديد في النظام. يجب أن يتأكد العقد الذكي من عدم تسجيل الناخب مطلقًا في نظام التصويت مرتين. بالنسبة لكل طلب تسجيل جديد، يتحقق النظام من خلال العقد الذكي من أن الناخب المحدد لا ينبغي أن يكون موجودًا بالفعل في السلسلة. في حالة عدم وجود بطاقة هوية وطنية، يقوم النظام بتسجيل الناخب الجديد في النظام وإضافة عملة تصويت واحدة (VC) في محفظته.
يتحقق هذا العقد الذكي أيضًا من عمر المستخدم في جانب آخر حتى لا يملأ السلسلة بالتسجيل المفرط غير المفيد. يتم التحقق من العمر بمساعدة سلطات تحديد الهوية من خلال بطاقة الهوية الوطنية الخاصة به.

**Algorithm 2: Smart Contract: Registering in VMS**

```
1: Require:  Initialization of parameters
2: Initialize voter_id = this voter_id
3: Initialize voter_name = this voter_name
5: Func (Register Voter)
6: Input: voter_id
7: Require: voter_id=! Null
9: If voter_id exist
10: then revert back to voter_id else
11: if voter_age < 18
12: then revert back to voter_id else
13: Add Voter successfully
14: End Func
15: End Smart Contract
```

الشكل 7. Smart contract casting vote in VMS

**2. مستخدم ليس جديد:**

- أول عقد ذكي في نظام التصويت هو للتحقق من المستخدم (الشكل 8)ويكون بين Identification Authorities (IA) ونظام إدارة التصويت (VMS).ويستخدم تابع Can-Cast-Vote للتحقق مما إذا كان ناخب معين يستوفي المتطلبات اللازمة للإدلاء بصوته, بمجرد التحقق منها، يتم تسجيل تفاصيل الناخب للرجوع إليها مستقبلاً.
- ثم يتم ربط الناخب بعقد التصويت الذكي الذي يحدد المرشحين الذين سيتم تقديمهم للاختيار.
- العقد الذكي يتحقق مما إذا كان الناخب لديه عملة تصويت في محفظته لتحديد أهليته للإدلاء بالتصويت. ويتحقق العقد الذكي من توفر عملة التصويت المرتبطة بالهوية الوطنية للناخب وعنوان المحفظة، مما يسمح للناخب بالإدلاء بالتصويت في حالة وجود العملة، أو رفض طلب التصويت في حالة عدم توفر العملة.

**Algorithm 1: Smart Contract: Casting Vote in VMS**

```
1: Require:  Initialization of parameters
2: Initialize voter_Coin = this voter_Coin
3: Initialize vote = this vote
4: Initialize casted_vote = this casted _vote
5: Func (Cast Vote)
6: Input: reciever_address
7: Require: voter_Coin =1
8: Select Candidate1,2,...,n
9: If voter_Coin = 0
10: then casted_Vote = Vote
11: else revert to reciever_address
12: End Func
13: End Smart Contract
```

الشكل 8 Smart contract registering in VMS

- يتم تخزين كل صوت في المعاملة كما هو موضح في الجدول 1 ويحصل كل ناخب على معرف المعاملة لصوته. يتم تشفير جميع المعلومات المخزنة في المعاملة بشكل كبير باستخدام cryptographic hash..

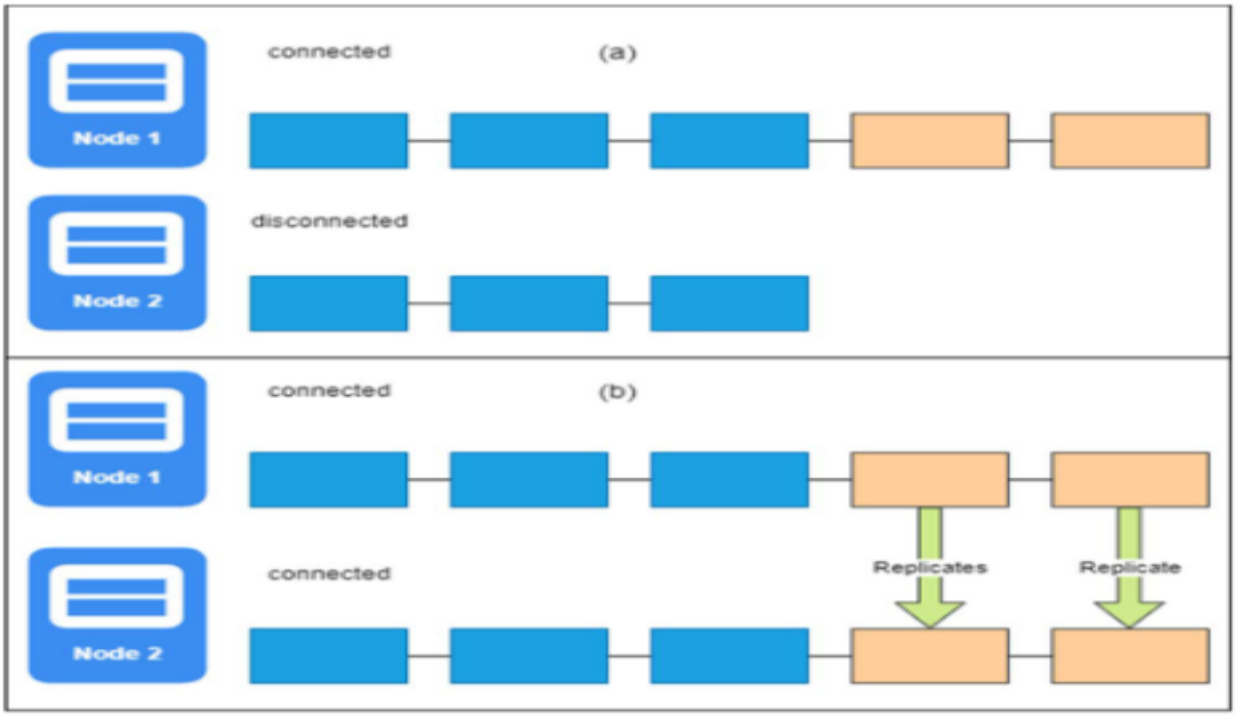
| TxHash | Block | From | To | Value |
|---|---|---|---|---|
| 0xG244e... | 1011 | 0xIUHiu... | T1SC | Voter Info (NIN, Wallet, etc.) Candidate A Candidate E |
| 0xL1345... | 1012 | 0xU98hi... | T2SC | Voter Info (NIN, Wallet, etc.) Candidate B Candidate F |
| 0xOpl21... | 1013 | 0xIpda4... | T3SC | Voter Info (NIN, Wallet, etc.) Candidate A Candidate D |

الجدول 1.VMS Transaction in

- يضمن العقد الذكي في نظام التصويت إضافة المعاملات الضرورية والكاملة فقط إلى blockchain.إذا تم استيفاء جميع الشروط، فسيتم إرسال المعاملة إلىmemPool .
- تعد memPool منطقة تخزين مؤقتة حيث يتم الاحتفاظ بالمعاملات غير المؤكدة بواسطة كل عقدة في الشبكة. تنتظر هذه المعاملات أن يتم تضمينها في كتلة وإضافتها إلى blockchain بواسطة القائمين بالتعدين. بمجرد استيفاء المعاملة لجميع الشروط اللازمة، يتم نقلها من memPool لتتم معالجتها وإضافتها إلى blockchain.

## 10. Chain Security Algorithm (1):

- تضمن خوارزمية أمان السلسلة سلامة blockchain من خلال التحقق تلقائيًا من صحة كل كتلة جديدة تضاف إلى السلسلة. فهي تؤكد أمان وصلاحية الكتلة من خلال مقارنة قيم HASH مع الكتل السابقة قبل تكرارها عبر جميع العقد في الشبكة. إذا تم اكتشاف أي نشاط ضار، فإن الخوارزمية تحدد السلسلة على أنها غير صالحة و تخبر جميع العقد في الشبكة، وبالتالي الحفاظ على أمان نظام blockchain.




الشكل 9

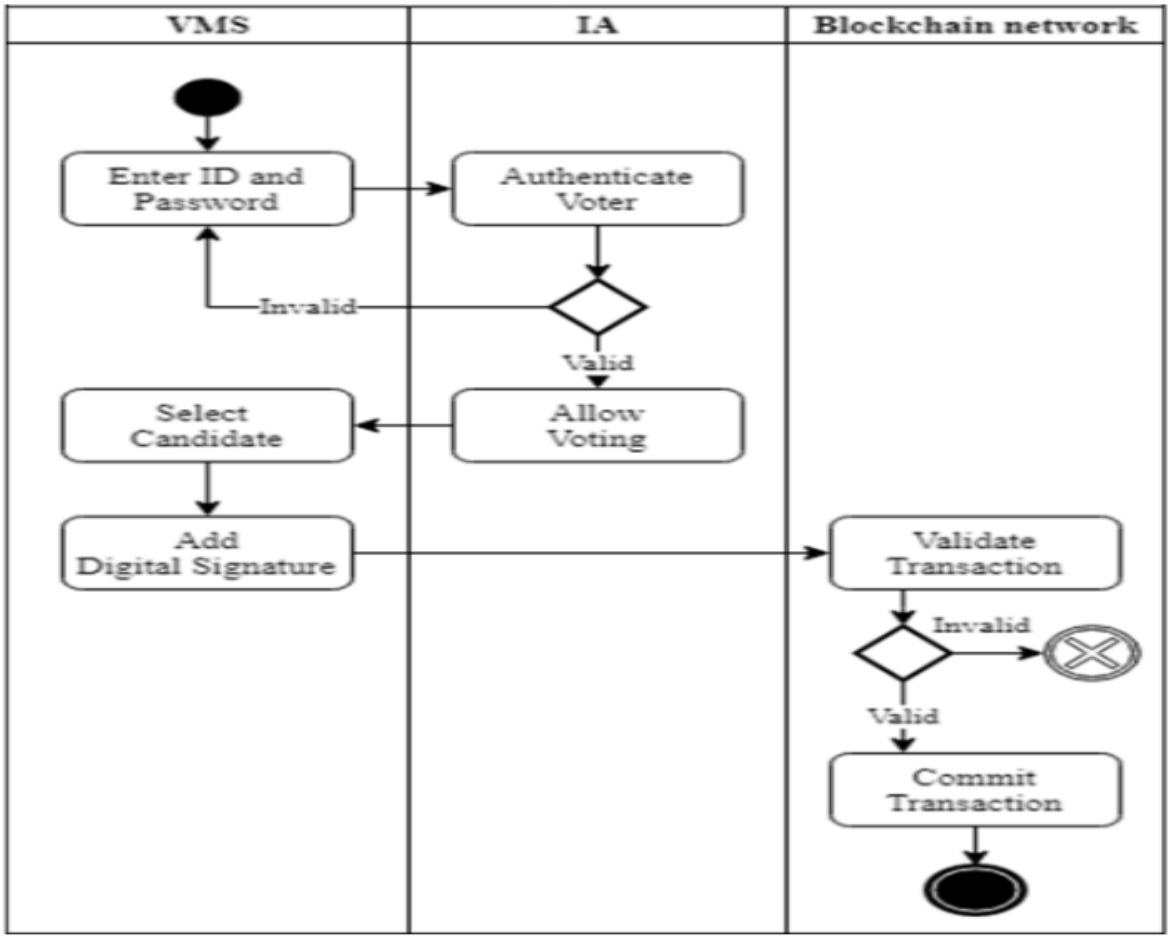
Chain recovery during partial failure of the network (a): Node 2 is disconnected from network, while Node 1 is mining normally. (b) Node 2 joins network and replicate the blocks from Node 1, as the Node 1 is the longest chain in network

- يتم أيضااسترداد السلسلة أثناء حدوث فشل جزئي في الشبكة،مثلا في الشكل السابق(الشكل 9) إذا تم قطع اتصال العقدة 2 بينما تستمر العقدة 1 في التعدين(الاضافة) بشكل طبيعي، فيمكن للعقدة 2 إعادة الانضمام إلى الشبكة وتكرار الكتل من العقدة 1. تحدث هذه العملية لأن العقدة 1 تمتلك أطول سلسلة في الشبكة مما يضمن قيام Node 2 بمزامنة بيانات blockchain الخاصة بها مع بقية الشبكة عند إعادة الاتصال.
- هذا يعني أن البيانات الموجودة على العقدة 1، والتي تعد جزءًا من السلسلة الأطول، يتم نسخها على العقدة 2 للحفاظ على الاتساق والتكامل عبر الشبكة. تضمن هذه العملية موافقة جميع العقد في شبكة blockchain على سلسلة المعاملات الصحيحة، مما يمنع التناقضات ويضمن الشفافية في نظام التصويت.

## 11. CRYPTOGRAPHIC HASH (1) :

- يتم استخدام خوارزمية SHA256 للقيام بعمليات التشفير في blockchain .
- تعمل هذه التقنية على الحفاظ على أمان المعاملة عندما يتم نقلها على الشبكة لإضافتها إلى السلسة.

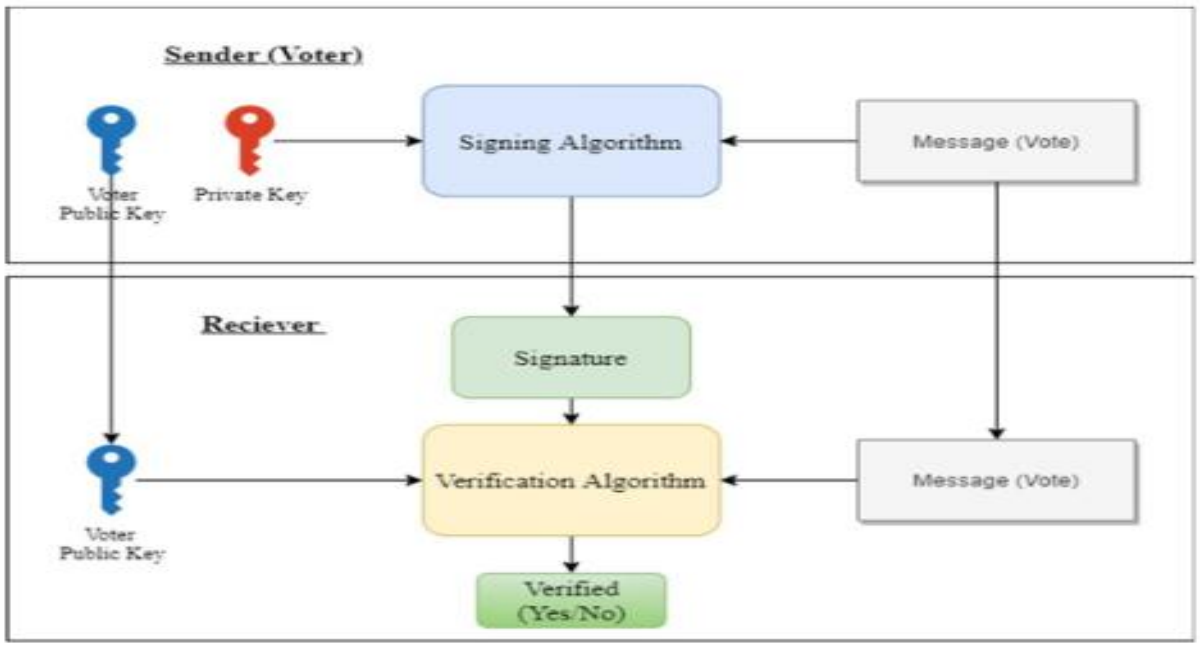
- إجراء أمني يخفي البيانات من الوصول غير المصرح به داخل النظام، مما يضمن خصوصية المستخدم.
- قيمة hash الخاصة بالمعاملة يتم ارسالها الى الناخب عن طريق رسائل البريد الالكتروني او رقم الهاتف المسجل مما يمنحه حق الوصول لتتبع تصويته والتحقق منه.
- أثناء الإدلاء بالتصويت يضيف الناخب توقيعًا رقميًا إلى المعاملة (الشكل 10 ). يحافظ هذا التوقيع الرقمي على أمان المعاملةحيث يمكن للمالك المصرح له فقط فك تشفير المعاملة وعرض المحتوى باستخدام مفتاحه الخاص.
- يتم حفظ المعاملة في كتلة ويتم قفلها باستخدام المفتاح العام للناخب. أثناء تتبع التصويت، يتم تحديد العقدة بواسطة المفتاح العام للناخب. يستخدم الناخب مفتاحه الخاص لعرض المعاملة التي تتم بواسطة محفظته. يمكن للناخبين فقط مشاهدة التصويت؛ ولا يمكنهم مطلقًا تغيير التصويت أو حذفه بمجرد الإدلاء به.




الشكل 10.Process of transaction

## 12 – ألية signature (1):

يوضح الشكل 11 ألية التوقيع



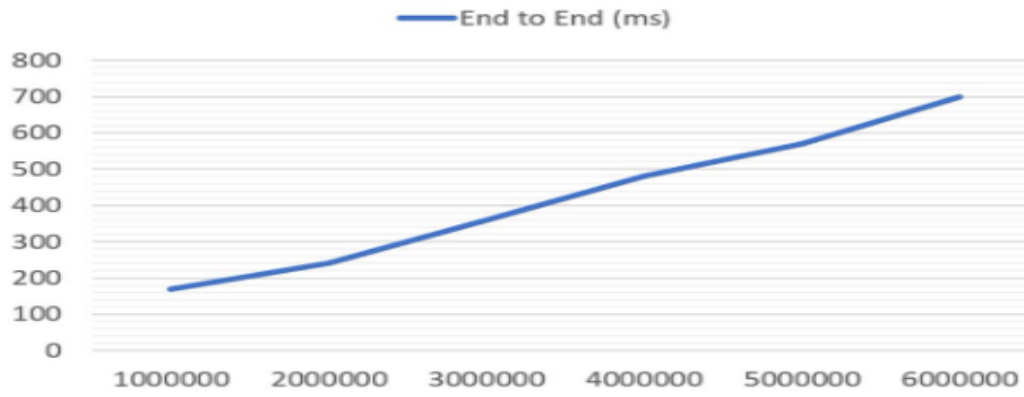

الشكل 11 Signature

## 13. PERFORMANCE EVALUATION (1):

- تم تقييم فعالية إطار العمل المقترح من خلال اختباره بسيناريوهات واقعية باستخدام Remix، وهي أداة Blockchain القائمة على المتصفح. يتم استخدام لغة البرمجة Solidity في تجربة النموذج، مما يسمح بتقييم أدائه ووظائفه في التطبيقات العملية داخل نظام blockchain.
- Remix : هي أداة تطوير قائمة على المتصفح تستخدم في تطوير واختبار العقود الذكية على منصات البلوكشين. تهدف الأداة إلى تسهيل عملية تطوير العقود الذكية وتجربتها وتصحيح الأخطاء بهدف تعزيز أمان وثقة التطبيقات المبنية على التكنولوجيا اللامركزية.
- توفر Remix محررًا للعقود الذكية يدعم عدة لغات لبرمجة العقود مثل Solidity و Vyper وغيرها. يمكن للمطورين إنشاء وتحرير وتنسيق العقود الذكية باستخدام هذا المحرر.

- تعمل Remix كتطبيق قائم على المتصفح، مما يجعلها قابلة للتكامل مع متصفح الويب . يمكن للمطورين الوصول إليها واستخدامها مباشرة من المتصفح دون الحاجة إلى تنزيل أو تثبيت أدوات إضافية.

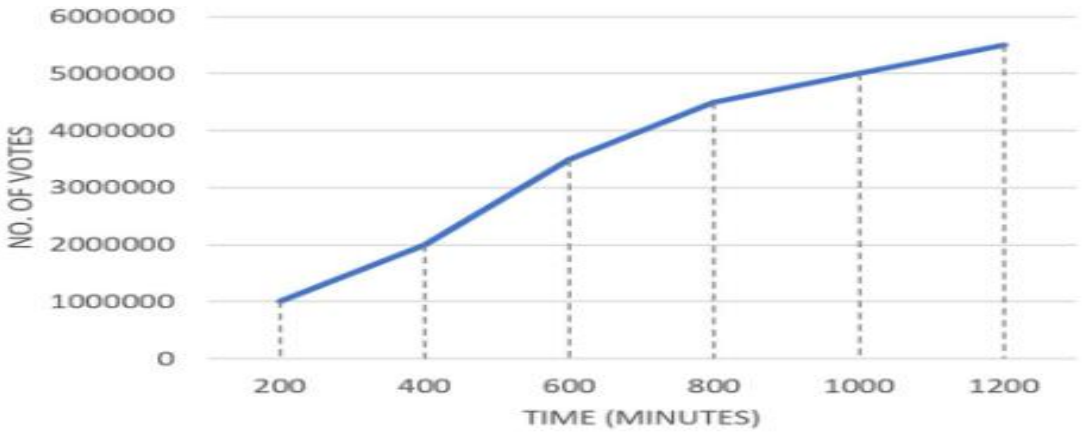
## :(1) RESPONSE TIME OF VMS 1.13




الشكل 12 Response time of VMS

- يشير وقت استجابة نظام إدارة التصويت (VMS) إلى الوقت المستغرق لمعالجة كل معاملة داخل blockchain. ومع إضافة المزيد من الأصوات، يزداد وقت استجابة نظام VMS تدريجيًا (الشكل 12). ويرجع ذلك إلى الطبيعة اللامركزية لتقنية blockchain، حيث تقوم كل عقدة بمعالجة المعاملات بناءً على قوتها الحسابية، مما يؤدي إلى اختلافات في أوقات الاستجابة.
- يتم زيادة وقت الاستجابة تدريجيًا مع وجود المزيد من المعاملات المنتظرة في memPool. يتم تطبيق خوارزميات الإجماع المرنة هنا للحفاظ على كفاءة السلسلة الموحدة.

## 2.13 SIZE OF CHAIN (1) :




الشكل 13Behavior of size of chain

- حجم blockchain الذي يخزن بيانات المعاملات، يزداد تدريجياً مع إضافة المزيد من الكتل إليه. يبدأ حجم السلسلة في البداية بحوالي 0.004 ميجابايت إلى 0.2 ميجابايت لكل 500 كتلة، وينمو حجم السلسلة بمرور الوقت بسبب عملية التصويت التي تستمر من يوم إلى يومين. من المحتمل أن يؤدي هذا النمو في الحجم إلى مشكلات تتعلق بزمن الوصول حيث تتوسع السلسلة بسرعة خلال فترات التصويت المكثفة.

## 3.13 LATENCY (1):

- يتم تحديد زمن الوصول لنظام التصويت من خلال قياس الوقت المستغرق لمعالجة طلبات المعاملات، والذي يمكن أن يزيد مع زيادة عدد الطلبات في الثانية. يتم تسجيل الأصوات عبر العقد المختلفة لتعزيز الكفاءة ومنع اختناقات المعالجة في عقدة واحدة. تُستخدم خوارزميات العقود الذكية لحظر العقد الدخيلة والتأكد من إضافة المعاملات المكتملة التي تستوفي معايير محددة فقط إلى blockchain أثناء عملية التصويت.
- أثناء عملية التصويت، تتم إدارة حركة المرور على blockchain بشكل فعال للتحكم في زمن الوصول. يعتمد زمن الوصول في blockchain على قوة الحوسبة للعقد، ويساعد استخدام خوارزميات الإجماع المرنة في الحفاظ على الكفاءة أثناء التصويت.

| Number of Blocks | Latency (ms) |
|---|---|
| 1000000 | 170 |
| 2000000 | 254 |
| 3000000 | 545 |
| 4000000 | 670 |
| 5000000 | 701 |
| 6000000 | 852 |

الشكل14 .Latency in VMS

## : CONCLUSION -14

يهدف تنفيذ الحل القائم على blockchain لأنظمة التصويت إلى تعزيز الثقة بين الحكومة والناخبين من خلال ضمان نزاهة وشفافية عملية التصويت. ومن خلال استخدام تقنية البلوكشين، تصبح عملية التصويت أكثر فعالية من حيث التكلفة والكفاءة والأمان، مما يؤدي في نهاية المطاف إلى تحسين العلاقة بين المواطنين ومؤسساتهم الديمقراطية. ويؤكد الإطار على أهمية ميزات مثل الثبات، وحماية الخصوصية، وإمكانية التتبع في ضمان موثوقية النظام الانتخابي ومصداقيته. يشتمل النظام على خوارزمية أمان السلسلة للتحقق من سلامة blockchain ويستخدم العقود الذكية لمنع المعاملات الاحتيالية، مما يؤدي إلى إنشاء منصة آمنة وموثوقة لكل من السلطات والناخبين. يُظهر الإطار أداءً واعدًا في التعامل مع حجم كبير من المعاملات مع الحفاظ على الأمن والشفافية في نظام التصويت الإلكتروني القائم على blockchain.

## : Future challenges - 15

- ✓ على الرغم من أن البلوكشين يمكن أن يوفر مستوى عالٍ من الأمان، إلا أن حماية هوية الناخبين من الكشف العلني لا تزال تحديًا كبيرًا.

- ✓ تظل النظم الإلكترونية عرضة للهجمات السيبرانية مثل هجمات رفض الخدمة (DDoS)ومحاولات الاختراق. تأمين نظم التصويت ضد هذه الهجمات يتطلب تقنيات أمان متقدمة ومتطورة.
- ✓ التحقق من صحة المعاملات على البلوكشين يمكن أن يكون بطيئًا، مما قد يؤثر على سرعة التصويت وإعلان النتائج.
- ✓ بناء نظام تصويت إلكتروني يعتمد على البلوكشين قد يكون مكلفًا من حيث البنية التحتية اللازمة والتطوير المستمر.
- ✓ العمليات الحسابية المرتبطة بتقنية البلوكشين تستهلك كميات كبيرة من الطاقة، مما قد يزيد من التكلفة البيئية.

## : REFERENCES -16


1. Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. *IEEE Access*, *10*, 59959-59969.

2. Review on blockchain technology : Architecture, characteristics, benefits, algorithms, challenges and applications. (2023). *Mesopotamian Journal of Cyber Security*, 73-85.

3. Chentouf, F. Z., & Bouchkaren, S. (2023). Security and privacy in smart city: A secure E-voting system based on blockchain. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1848.