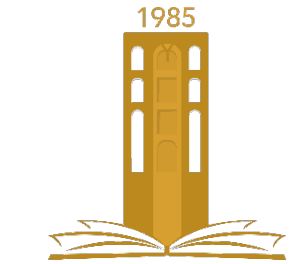
مذكرة تخرج مقدمة في

جامعة محمد بوضياف – المسيلة



جامعة محمد بوضياف - المسيلة
University of Mohamed Boudiaf-Msila

كلية الرياضيات والإعلام الآلي

قسم الإعلام الآلي

تخصص: الشبكات وتكنولوجيا المعلومات والاتصالات

من أجل الاستيفاء الجزئي لمتطلبات شهادة

ماستر في الإعلام الآلي

من طرف

بن البار محمد

سلمانة محمد الأمين

عنوان المذكرة

موقع ويب للتصويت مبني باستخدام البلوك شين

تحت إشراف الأستاذ

حمزة لوصيف

أعضاء لجنة المناقشة

نورالدين عمراوي	جامعة المسيلة	رئيسا
حمزة لوصيف	جامعة المسيلة	مشرفا
مراد بريك	جامعة المسيلة	ممتحنا

06، 2024

إهداء:

إلى شرف الامة وقلبها النابض غزة .. إلى القائد أبو خالد الضيف أدام الله رعبه.. إلى الشيخ المؤسس احمد ياسين والرنتيسي وكل قادتنا الكرام.. إلى أبطال العبور المقدس وغزوة السابع من أكتوبر .. إلى من غيّروا العالم وفضحوا إجرامه ونفاقه .. إلى إخوتنا المجاهدين في كتيبة الخلفاء .. كتيبة مخيم جباليا الراسخ.. إلى من أحبه وأسأل الله أن يحشرني معه .. الشيخ عبد الله عزام .. إلى الأحرار خلف سجون الطغاة .. الثابتين ثبات الجبال .. إلى كل من رفع رأسه في وجه الكفر ليعلي كلمة الله إلى أن يسود إسلامنا العالم مجددا .. نفسي الفداء لكم.

محمد بن البار

إلى الوالدين الكريمين حفظهما الله .. إلى كل أفراد أسرتي .. إلى كل الأصدقاء ومن كانوا برفقتي ومصاحبتي أثناء دراستي في الجامعة .. وإلى كل من ساهم في تلقيني ولو بحرف في حياتي الدراسية .

محمد الأمين سلمانة

تشكرات:
نتوجه إلى الله تبارك و تعالى بالحمد و الثناء و الشكر كما يحبه ويرضاه على نعمه الظاهرة و الباطنة ، أمدنا بالصبر وأعاننا كل العون على إنجاز هذه المذكرة فنحمده حمدا يليق بجلاله ونسأله العفو و الغفران والتوفيق

الفهرس:

المقدمة:---------- 8

I. إشكالية الموضوع:---------- 8
II. أهداف الموقع: ---------- 9
III. فصول المذكرة: ---------- 9

أنظمة التصويت---------- 10

I. مقدمة:---------- 11
II. التصويت عبر الانترنت: شرح تاريخي ومبررات التطوير---------- 11
1) **تعريف التصويت عبر الانترنت: ---------- 11**
2) **السياق التاريخي: ---------- 11**
3) **الأسباب التي أدت إلى تطوير التصويت عبر الإنترنت: ---------- 12**
4) **طرق التصويت التقليدية: نقاط القوة والضعف: ---------- 13**
5) **التحديات التي يواجهها التصويت عبر الانترنت:---------- 14**
6) **التصويت الإلكتروني: إمكانياته ووظائفه المعتادة ---------- 14**
7) **نقاط القوة المقترنة بأنظمة التصويت الإلكتروني: ---------- 15**
8) **نقاط الضعف المقترنة بأنظمة التصويت الإلكتروني: ---------- 16**

III. أنظمة التصويت الإلكتروني في العالم: تقييم تقنيات مختلفة---------- 17
1) **هولندا:---------- 17**
2) **الفلبين: ---------- 17**
3) **أيرلندا:---------- 17**
4) **الولايات المتحدة الأميركية: ---------- 17**
5) **الهند: ---------- 18**

IV. فاتورة التصويت الالكتروني:---------- 18
1) **البرازيل :---------- 18**
2) **إستونيا: ---------- 18**
3) **أيرلندا : ---------- 18**

V. مشكلات قد تواجهها أنظمة التصويت الإلكتروني الحالية:---------- 18
1) **الخصوصية:---------- 18**
2) **مخاوف بشأن الأمان:---------- 19**
3) **التكلفة:---------- 19**
4) **التعقيد:---------- 19**

VI. الخاتمة:---------- 19

البلوك شين والإيثريوم: المفاهيم والتقنيات ---------- 20

I. مقدمة: ---------- 21
II. تقنية البلوك شين: رحلة من خلال المفاهيم الأساسية: ---------- 21
1) **تعريف تقنية البلوك شين:---------- 21**
2) **السياق التاريخي: ---------- 21**

3) بنية البلوك شين:---------- 22
4) كيف يعمل البلوك شين: ---------- 30
5) ميزات تقنية البلوك شين: ---------- 32
III. آليات التوافق: مفتاح ضمان أمان شبكات البلوك شين:---------- 34
1) ما هو إثبات العمل (PoW)؟: ---------- 35
2) ما هو إثبات الحصة (PoS)؟:---------- 36
3) مقارنة بين نظام إثبات العمل (PoW) ونظام إثبات الصحة (PoS): ---------- 37
IV. مفهوم العقود الذكية: آلية عملها وفوائدها:---------- 39
1) ما هو العقد الذكي؟ ---------- 39
2) علاقة العقود الذكية بشبكات البلوك شين:---------- 40
3) كيف تعمل العقود الذكية؟---------- 40
4) هل تدعم جميع شبكات البلوك شين العقود الذكية؟ ---------- 41
5) السياق التاريخي للعقود الذكية. ---------- 41
6) أمثلة على العقود الذكية: ---------- 43
7) قابلية تنفيذ العقود الذكية: ---------- 44
8) فوائد وقيود العقود الذكية ---------- 45
9) الايثريوم: ---------- 48
V. خاتمة: ---------- 51

تصميم وتنفيذ نظام التصويت المقترح ---------- 52

I. مقدمة: ---------- 53
II. الأدوات المستخدمة: ---------- 53
III. اللغات المستخدمة:---------- 56
1) HTML:---------- 56
2) CSS:---------- 56
3) JAVASCRIPT:---------- 56
4) SOLIDITY: ---------- 57
5) BOOTSTRAP: ---------- 57
IV. تخطيط المشروع:---------- 58
1) مخطط المربعات BLOCK DIAGRAM: ---------- 60
2) مخطط التسلسل SEQUENCE DIAGRAM:---------- ERROR! BOOKMARK NOT DEFINED.
3) المخطط المفاهيمي CONCEPTUAL DIAGRAM: ---------- ERROR! BOOKMARK NOT DEFINED.
V. عرض واجهات الموقع: ---------- 62
VI. الخاتمة: ---------- 71

الخاتمة العامة :---------- 72

المراجع: ---------- 74

مراجع الصور: ---------- ERROR! BOOKMARK NOT DEFINED.

المقدمة:

أثبتت التجارب التاريخية والثورات المضادة التي شهدناها كعرب ومسلمين آخر السنين مدى الأضرار التي تسببت فيها حكومات قامت على غير إرادة شعوبها. صحيح أن معظم هذه الدول عرفت منذ "حصولها على الاستقلال" أشكالا متباينة من الانتخابات، بل إن بعضا منها التزم بدوريتها وأعطاها درجة من التنافسية كبلدنا الجزائر مثلا، لكن ذلك لم يكن في الغالب غير وسيلة لإعطاء النظم الحاكمة شرعية شكلية، تتصدى بها للمعارضة الداخلية ولتحسين صورتها أمام العالم الخارجي، بل إن إجراء الانتخابات تحول في بعض الحالات وفي بعض الدول العربية كمصر إلى أفراح وأعراس دورية رسمية لا عائد منها كقيمة مضافة في الحياة السياسية والديمقراطية. مما يدفع بصناع القرار من حين إلى آخر القيام بتعديلات على القوانين العضوية للانتخابات لإعطاء نفس جديد والخروج من الصورة النمطية الروتينية للانتخابات وبالتالي التوجه نحو التقليل من العزوف الانتخابي وتشجيع مشاركة المواطن والأحزاب المعارضة والوقوف على الخلل وإصلاحه لضمان سيرورة الحياة السياسية والمدنية بشكل طبيعي.

تعد الجزائر من الدول التي يرى فيها راسمي السياسة وصناع القرار ضرورة تعديل القانون العضوي للانتخابات كلما دعت الضرورة والذي لم يأت بالجديد فيما يخص إضفاء الشفافية ومصداقية مخرجات العملية الانتخابية، كما أن موضوع الانتخابات غير متناول باستمرار في الحياة الاجتماعية مما أدى إلى بروز موقف سلبي عام نحوه، فالجزائر من الدول المعنية بتحسين وتطوير نظامها الانتخابي فيما يتعلق بتصميم وهندسة آلية اقتراع وتصويت جديدة، تضمن انعدام التزوير وتعطي شفافية ومصداقية للعملية الانتخابية وإفرازاتها.

وعليه أردنا في هذه الدراسة إبراز فكرة استشرافية لنمط اقتراع الكتروني مبني باستخدام تقنية البلوك تشين مشجع على المشاركة السياسية وضامن لشفافية ومصداقية وأمان العملية الانتخابية.

I. إشكالية الموضوع:

إن معضلة التصويت المطروحة في الجزائر وغيرها من بلادنا العربية، لا تتعلق فقط ببناء نظام ديمقراطي يحفظ الدولة واستمرار بناءها السياسي، بل يتعلق أيضا بمدى استجابة هذا النظام للتعبير الجاد والامين عن الإرادة الشعبية وبناء حكم ديمقراطي رشيد يعمل لصالح الشعب ممثلاً له ومديرا لشؤونه وخاضعا لرقابته.

وعلى ضوء ما سبق يمكن أن نحصر أسباب هذه المعضلة في عدة نقاط وهي:

- عدم ثقة الشعوب والمجتمعات في نظام الانتخابات.
- معاناة أنظمة التصويت الحالية من التزوير والاستلاء على مراكز الاقتراع والتلاعب بنتائج الانتخاب واختراق أجهزة التصويت عند الدول التي تعتمد على التصويت الالكتروني.
- لا وجود لأي سجلات للانتخابات يمكن أن يطّلع عليها المواطن باستثناء عدد الأصوات التي يتم الاعلان عنها من قبل الحكومة، مما يعني أن الناخبين لا يملكون أي ضمان بعدم وجود تدخل خارجي خاصة في حالات إعادة فرز الأصوات.
- أنظمة التصويت الحالية سواء كانت إلكترونية أم لا، أثبتت أنها غير مرضية للمواطنين خاصة فيما يتعلق بالشفافية والنزاهة.
- النظام الانتخابي المعيب من أهم المشاكل التي تواجه حتى أكبر الديمقراطيات في العالم مثل الهند، الولايات المتحدة، واليابان.

II. أهداف الموقع:

- تعزيز الأمان والشفافية حيث يسجل كل صوت بشكل مشفر وغير قابل للتغيير.
- إضفاء النزاهة والمصداقية على العملية الانتخابية بحيث يمكن للناخبين التحقق من أن أصواتهم قد تم تسجيلها بشكل صحيح دون أن يتم الكشف عن هويتهم.
- تقليل التكلفة خاصة المتعلقة بإعداد مراكز الاقتراع التقليدية وتوفير المواد الانتخابية وأطقم الحراسة والفرز الخ، كما يسرع من عملية جمع وفرز الأصوات، مما يقلل من الوقت اللازم لإعلان النتائج.
- زيادة الوصولية والمشاركة للمواطنين بحيث يمكنهم الإدلاء بأصواتهم من أي مكان وفي أي وقت باستخدام الإنترنت، مما يسهل عملية التصويت ويشجع على زيادة نسبة المشاركة الانتخابية، خاصة بين الأشخاص الذين يعيشون في مناطق نائية ومن لديهم صعوبات في التنقل إلى مراكز الاقتراع.
- تجنب التزوير والاحتيال حيث أن الأصوات بعد تسجيلها على شبكة البلوك تشين يكون من الصعب للغاية تزويرها أو تغييرها مما يضمن أن نتائج الانتخابات تعبر بدقة عن إرادة الناخبين.
- إتاحة إمكانية التحقق المستقل من عملية التصويت بواسطة الأطراف المعنية (مثل المراقبين الدوليين والمنظمات غير الحكومية)، حيث يمكن تتبع جميع العمليات الانتخابية بشكل شفاف وواضح دون المساس بسرية الأصوات.
- ضمان الحفاظ على خصوصية الناخبين، حيث يمكن أن تكون الأصوات مجهولة الهوية لكن يمكن التحقق من صحتها.
- التكيف مع المستقبل بحيث يكون موقعنا أكثر تكيفًا مع التغيرات المستقبلية والتطورات التكنولوجية، مما يجعله استثمارًا طويل الأمد مقارنة بالأنظمة التقليدية.

III. فصول المذكرة:

تنقسم مذكرتنا إلى ثلاثة فصول كالتالي:

- سنتحدث في فصلنا الأول عن التصويت التقليدي تعريفا وتوضيحا لعيوبه ومشاكله ثم نسلط الضوء على ظروف ظهور التصويت الالكتروني وكذا نقاط ضعفه والمشاكل التي تعترضه.
- أما في الفصل الثاني فسنتطرق إلى مفاهيم البلوك شين بشكل عام وأهميته ودوره في عملية التصويت ثم العقود الذكية وبلوك تشين الايثريوم بشكل خاص كونه أساس موقعنا.
- الفصل الثالث سنعرض فيه تصميم وتنفيذ نظام تصويتنا المقترح.

الفصل الأول:
أنظمة التصويت

I. مقدمة:

التصويت، سواء تم من خلال الاقتراع التقليدي أو كان إلكترونيا، يشكل حجر الأساس الذي تعتمد عليه الديمقراطية في العالم، وهو عادة ما تعبر به الشعوب عن آرائها واختياراتها كما أنه ما يبقيها في دائرة الاستقطاب السياسي للنظم الحاكمة والأحزاب السياسية.

ظل التصويت بالكيفية التقليدية المتمثلة في الذهاب لمراكز الاقتراع والفرز اليدوي للأصوات وما صاحبهما من مشاكل وتحديات ضامنا لمستوى معين من الشفافية والشرعية الانتخابية، الأمر الذي دفع ببعض ديمقراطيات العالم للتوجه لوسائل تصويت الكترونية كابتكار حديث يهدف إلى تحسين الكفاءة وتقليل التكلفة وزيادة الوصولية في مجتمعاتها التي أضحت تعتمد بشكل كبير على التكنولوجيا.

II. التصويت عبر الانترنت: شرح تاريخي ومبررات التطوير

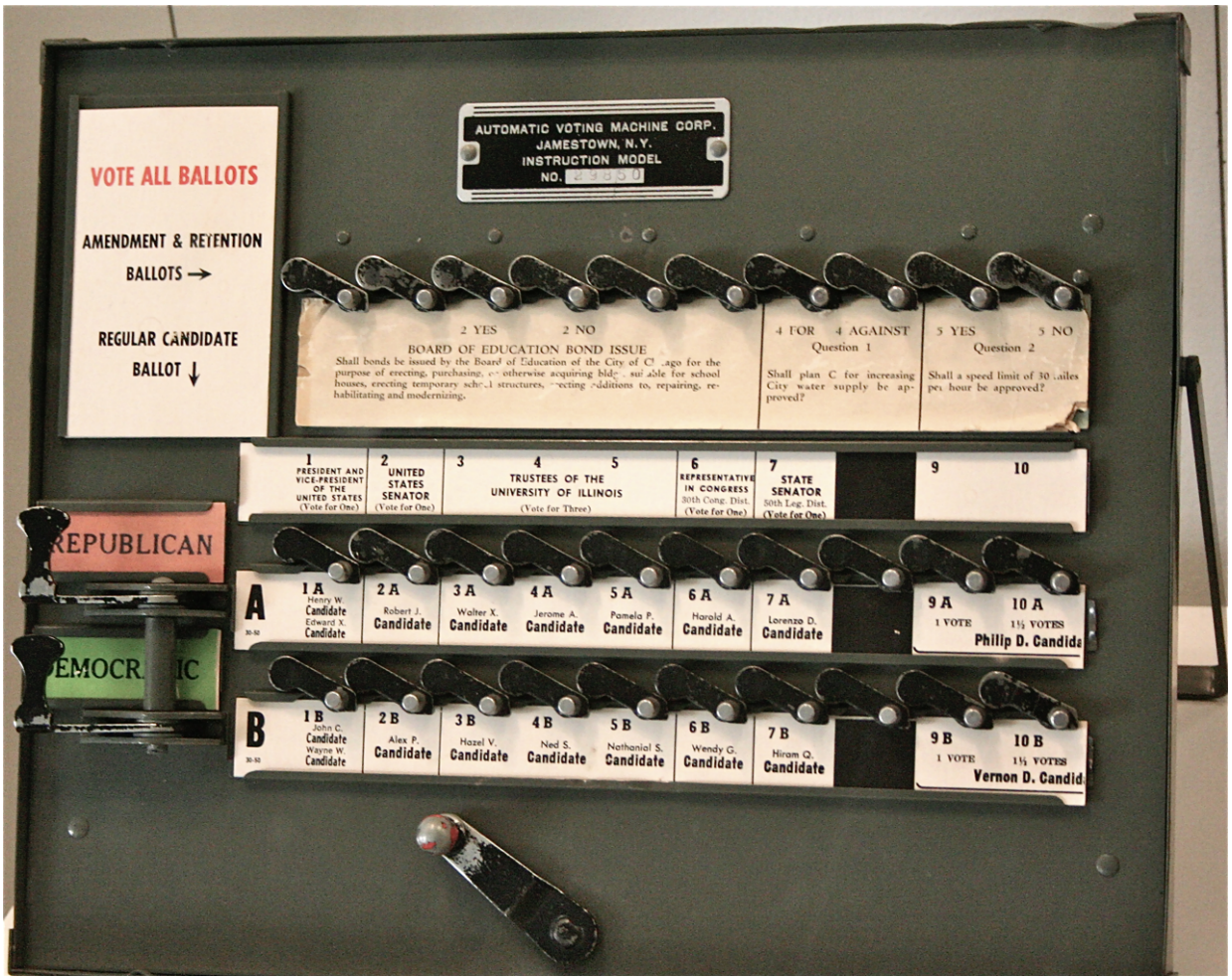
1) تعريف التصويت عبر الانترنت:

ويعرف أيضا بالتصويت الإلكتروني أ "التصويت - إ" ،هو نظام تصويت يستخدم تقنيات إلكترونية بدلاً من الأساليب التقليدية مثل صناديق الاقتراع الورقية. [1]
يشمل ذلك استخدام أجهزة مختلفة مثل:

- أجهزة الكمبيوتر: يمكن للناخبين استخدام أجهزة الكمبيوتر الشخصية أو أجهزة الكمبيوتر العامة في مراكز الاقتراع أو مواقع أخرى للتصويت.
- آلات التصويت الإلكترونية: هي أجهزة مخصصة مصممة خصيصًا لعملية التصويت.
- الهواتف المحمولة: يمكن للناخبين استخدام هواتفهم المحمولة لإرسال رسائل نصية أو استخدام تطبيقات التصويت.

2) السياق التاريخي:

ظهرت فكرة التصويت عبر الإنترنت لأول مرة في أواخر القرن التاسع عشر مع ظهور تقنيات التصويت المبكرة، مثل آلات الاقتراع الميكانيكية. ومع ذلك، لم يتم تطبيق هذه التقنيات على نطاق واسع إلا في أواخر القرن العشرين مع تقدم تكنولوجيا الكمبيوتر والاتصالات.



صورة رقم 1 آلة تصويت ميكانيكية بأسلوب الرافعة. [1]

3) الأسباب التي أدت إلى تطوير التصويت عبر الإنترنت:

تم تطوير التصويت عبر الإنترنت لأسباب متعددة، تشمل:

- زيادة كفاءة العملية الانتخابية: يمكن أن يؤدي التصويت عبر الإنترنت إلى تسريع عملية التصويت وفرز الأصوات، الذي بدوره قد يؤدي إلى إعلان نتائج الانتخابات بشكل أسرع.
- تحسين إمكانية التصويت: يمكن أن يدفع التصويت عبر الإنترنت الأشخاص للتصويت لسهولته، خاصة أولئك الذين يعانون من صعوبة الوصول إلى مراكز الاقتراع، مثل الأشخاص ذوي الإعاقة أو كبار السن أو الذين يعيشون في مناطق نائية.
- خفض تكلفة الانتخابات: يمكن أن يخفض التصويت عبر الإنترنت تكلفة إجراء الانتخابات، حيث يقلل من الحاجة إلى العمال والمواد في مراكز الاقتراع.
- تعزيز الديمقراطية: يعتقد بعض المدافعين عن التصويت عبر الإنترنت بأنه يعزز الديمقراطية من خلال زيادة المشاركة في الانتخابات وجعل من السهل على الناس أن يعبروا عن آرائهم [2].

4) طرق التصويت التقليدية: نقاط القوة والضعف:

ونشير بالطرق التقليدية هنا إلى الأساليب التي يستخدمها الناخبون للإدلاء بأصواتهم في الانتخابات، والتي لا تتضمن استخدام تقنيات التصويت الإلكتروني ونذكر منها :

- **التصويت في مراكز الاقتراع:**

هو الطريقة التقليدية للتصويت، حيث يتوجه الناخبون إلى مراكز اقتراع محددة في يوم الانتخابات للإدلاء بأصواتهم باستخدام آلات التصويت أو بطاقات الاقتراع الورقية. [10]

- **التصويت المبكر:**

هو العملية التي يمكن للناخبين من خلالها التصويت في يوم واحد أو عدة أيام سابقة للانتخابات، وعادة ما يكون الهدف منه زيادة نسبة المشاركة وتخفيف ازدحام مراكز الاقتراع في يوم الانتخابات. [11]

- **التصويت البريدي:**

هو نوع من التصويت المبكر حيث يتلقى الناخبون بطاقة اقتراع عبر البريد، ويملئونها، ويوقعون عليها، ثم يعيدونها إلى مسؤولي الانتخابات قبل يوم الانتخابات. [11]

الجدول التالي يوضح مقارنة بين أنواع التصويت وكذا نقاط القوة والضعف:

نوع التصويت	نقاط القوة	نقاط الضعف
التصويت في مراكز الاقتراع	الأمان	الطوابير الطويلة
	الخصوصية	صعوبة الوصول
	مساعدة الناخبين	التكلفة العالية
التصويت البريدي	الأمان	احتمال الاحتيال
	سهولة الوصول	التأخيرات
	الراحة	التكلفة العالية
التصويت المبكر	زيادة المشاركة	احتمال الاحتيال
	تقليل الازدحام في يوم الانتخابات	صعوبة التصويت لبعض الناخبين
	الراحة	التكلفة العالية

جدول رقم 1 طرق الصويت التقليدية (نقاط القوة والضعف) [1].

5) التحديات التي يواجهها التصويت عبر الانترنت:

مخاوف أمنية :قد يكون التصويت الإلكتروني عرضة للاختراق أو التلاعب، مما يؤدي إلى تزوير الانتخابات.

مخاوف الخصوصية :قد يؤدي التصويت الإلكتروني إلى انتهاك خصوصية الناخبين، بحيث يمكن تتبع أصواتهم.

عدم المساواة الرقمية :قد لا يتمكن جميع الأشخاص من الوصول إلى أجهزة الكمبيوتر أو الإنترنت اللازمة للتصويت عبر الإنترنت، مما قد يؤدي إلى حرمانهم من حقهم في التصويت.

المخاوف التقنية :قد تواجه بعض أنظمة التصويت عبر الإنترنت مشكلات تقنية، مما قد يؤدي إلى تأخيرات أو فقدان للأصوات [3].

6) التصويت الإلكتروني: إمكانياته ووظائفه المعتادة

داخليا، تنطوي أنظم التصويت الإلكتروني على العديد من الوظائف، بما في ذلك التشفير، التوزيع العشوائي، الاتصالات، والأنظمة الأمنية. ولا يتسع المجال في هذا البحث لتقديم تحليل دقيق لهذه الوظائف. ولكن حتى نتمكن من الوصول لفهم مبدئي لها، فمن المفيد أن نأخذ في الاعتبار بعض وظائف التشغيل التي يمكن أن تتيحها أنظم التصويت الإلكتروني لكل من الناخبين ومسؤولي الانتخابات .

- **قوائم الناخبين الإلكترونية والتحقق من هوية الناخبين:** يمكن أن يشتمل نظام التصويت الإلكتروني على قائمة إلكترونية بأسماء الناخبين، بحيث تشمل تلك القائمة الناخبين في أحد مراكز الاقتراع أو في عموم البلاد. ويمكن أن تُستخدم القائمة للتحقق من هوية الناخبين المؤهلين للانتخاب، وتسجيل إدلائهم بأصواتهم.

- **واجهات استخدام العاملين في مراكز الاقتراع:** هناك بعض وظائف التشغيل التي لا تُتاح إلا للعاملين في مراكز الاقتراع، ومنها على سبيل المثال، تصفير عدد الأصوات عند فتح مكتب الاقتراع، إغلاق الاقتراع، وطبع النتائج وإرسالها.

- **واجهات استخدام الناخبين:** ومن أنواعها، الشاشات التي تعمل باللمس، أوراق الاقتراع المزودة بنظام للتعُّرف على العلامات الضوئية (OMR) والتي يجري إدخالها إلى النظام من خلال ماسح ضوئي، الحواسب اللوحية التي تعمل باللمس، والأزرار التي يُضغط عليها، والمواقع الإلكترونية أو البرامج العملية (Client Software) فيما يتعلق بالتصويت من خلال الإنترنت.

- **واجهات استخدام الناخبين من ذوي الاحتياجات الخاصة:** ومن أنواعها، أجهزة القراءة بطريقة برايل، أجهزة المدخلات الصوتية لفائدة الناخبين المكفوفين، تيسير الوصول للاقتراع للناخبين المعاقين جسدياً، وواجهات الاستخدام المبسطة لفائدة الناخبين الأُميين [4].

7) نقاط القوة المقترنة بأنظمة التصويت الإلكتروني:

- تقليص عدد أوراق الاقتراع الباطلة، إذ يمكن لأنظمة التصويت تحذير الناخبين من بطلان أصواتهم (مع مراعاة تمكين الناخبين من الإدلاء بصوت فارغ إذا كانوا يريدون ذلك).
- احتمالية توفير التكاليف على المدى البعيد من خلال توفير عدد ساعات عمل موظفي مراكز الاقتراع، وخفض تكلفة طباعة أوراق الاقتراع وتوزيعها .
- توفير التكاليف من خلال التصويت عبر الإنترنت: إمكانية الوصول للناخبين في جميع أنحاء العالم بتكاليف لوجستية محدودة للغاية، ودون تكاليف بريدية، أو تأخير في إرسال المواد المطبوعة، أو استلامها مرة أخرى .
- بالمقارنة مع التصويت عبر البريد، يحد التصويت عبر الإنترنت من وقوع حالات بيع الأصوات أو التصويت العائلي، عبر السماح بتغيير التصويت بحيث لا يحتسب إلا آخر ما أدلى به الناخب، ويمنع التلاعب في مواعيد وصول البريد من خلال التحكم المباشر في مواعيد التصويت .
- سرعة فرز الأصوات وحصرها.
- زيادة دقة النتائج، حيث لا مجال للخطأ البشري.
- التعامل بكفاءة مع الصيغ التي تتطلب إجراءات فرز شاقة في الأنظمة الانتخابية المعقدة.
- تحسين طريقة عرض أوراق الاقتراع المعقدة .
- التيسير على الناخبين .
- احتمال زيادة معدلات المشاركة والإقبال، خاصة إذا استُخدم التصويت عبر الإنترنت .
- زيادة التوافق مع احتياجات المجتمعات الكثيرة التنقل .
- تجنب التزوير في مراكز الاقتراع، وخلال نقل النتائج وحصرها، من خلال تقليص التدخل البشري .
- زيادة إمكانية الوصول للانتخابات، على سبيل المثال من خلال استخدام أوراق الاقتراع الصوتية لفائدة الناخبين المكفوفين، وكذلك استخدام التصويت عبر الإنترنت لفائدة الناخبين الذين لا يستطيعون مغادرة منازلهم والناخبين المقيمين خارج البلاد .
- إمكانية الاستعانة بواجهة استخدام متعددة اللغات، بما يخدم المجتمعات التي تتسم بالتنوع اللغوي على نحو أفضل من أوراق الاقتراع.

8) نقاط الضعف المقترنة بأنظمة التصويت الإلكتروني:

- انعدام الشفافية .
- عدم وضوح النظام أو سهولة فهمه لغير الخبراء .
- عدم وجود معايير متفق عليها لأنظمة التصويت الإلكتروني .
- بالرغم من اشتراط اعتماد النظام في جميع الأحوال، فلا توجد معايير متفق عليها على نطاق واسع للاعتماد.
- احتمالية انتهاك سرية الأصوات، خاصة في الأنظمة الانتخابية التي تجمع بين التأكد من هوية الناخب والإدلاء بالأصوات .
- خطر التلاعب بالنظام، إما من الداخل من قبل من لديهم امتياز الوصول إلى النظام، أو من الخارج من قبل قراصنة .
- قدرة مجموعة صغيرة من العاملين بالنظام على التلاعب بالنتائج على نطاق واسع .
- التكاليف المتزايدة لشراء أنظمة التصويت الإلكتروني وصيانتها .
- زيادة متطلبات البنية التحتية والمتطلبات البيئية، فيما يتعلق بإمدادات الطاقة، تكنولوجيا الاتصالات، درجة الحرارة والرطوبة .
- زيادة المتطلبات الأمنية لحماية نظام التصويت الإلكتروني أثناء الانتخابات وفيما بينها، بما في ذلك خلال عمليات النقل والتخزين والصيانة .
- الحّد من قدرة الإدارة الانتخابية على التحكم في النظام نظراً لاعتمادها، إلى حد كبير، على البائع أو على التكنولوجيا أو على كليهما معا.
- إمكانية محدودة لإعادة فرز الأصوات.
- الحاجة لحملات إضافية لتوعية الناخبين.
- احتمالية وجود تعارض مع الإطار القانوني القائم .
- احتمالية فقدان الشعب للثقة في الانتخابات التي تُعقد بنظام التصويت الإلكتروني، نظراً لنقاط الضعف المذكورة أعلاه. [5]

III. أنظمة التصويت الإلكتروني في العالم: تقييم تقنيات مختلفة

1) هولندا:

علّق العمل بالتصويت الإلكتروني عام 2008 عقب 20 عاماً من تطبيقه، بعد أن برهن ناشطون على أن الأنظمة المستخدمة يمكن أن تمثل خطراً على سرية الأصوات، في حال توافر ظروف معينة.

ووجدت لجنة رسمية أن وزارة الداخلية وشؤون علاقات المملكة، وهي الجهة المسؤولة عن تنظيم الانتخابات، تفتقر إلى الخبرات في هذا الشأن بين صفوفها، الأمر الذي تسبب في الاعتماد الزائد على المورِّدين ووكالات الاعتماد، وهو ما أضطر الناخبين إلى العودة لاستخدام الأقلام وأوراق الاقتراع.

وعلى الرغم من ذلك، فلا يزال العديد من الأطراف، ولا سيما رؤساء البلديات والناخبين، يثقون في نظام التصويت الإلكتروني، ويطالبون، بناء على التجارب الإيجابية في الماضي، بإعادة استخدامه. [5]

2) الفلبين:

بعد تجارب إقليمية في عام 2008، طبق نظام الفرز بالمسح الضوئي في المراكز الانتخابية (PCOS) في جميع أنحاء البلاد في عام 2010. وبعد بعض التأخير في المرحلة المبكرة من المشروع، تبَّقى أقل من عام واحد من الوقت المتاح لتطبيق النظام.

وقبل نحو أسبوع واحد من الانتخابات، شارف النظام على الانهيار عندما اكتُشف أن جميع آلات المسح الضوئي، وعددها75,000آلة، قد جهز تجهيزا خاطئا. ولم تُحل المشكلة إلا في اللحظة الأخيرة من خلال إعادة تجهيز جميع آلات التصويت يدوياً في عملية لوجستية ضخمة.

وبعد نجاح الانتخابات في نهاية الأمر، كان أحد المخاوف يتعلق بمدى اعتماد هيئة الإدارة الانتخابية على مورد النظام في حل الأزمة. [5]

3) أيرلندا:

ما بين عامي 2005 و2009، استثمرت أيرلندا أكثر من 60 مليون يورو في نظامٍ للتصويت الالكتروني لا يقدم إثباتات تدقيق ورقية، قبل أن تقرر الحكومة أن النظام لا يعتمد عليه ويحتاج إلى المزيد من التعديلات المكلفة قبل أن يكون استخدامه ممكنا. وأدت نتيجة التكاليف المرتفعة مصحوبة بانعدام الثقة، إلى إلغاء التصويت الإلكتروني في عام2009. وفي ظل عدم وجود حل مناسب للتخلص من آلات التصويت غير المستخدمة، فإن أيرلندا سوف تتحمل تكلفة تخزينها في الأمد المنظور. [5]

4) الولايات المتحدة الأميركية:

بعد صدور قانون "ساعد أميركا على أن تنتخب" في عام 2002، شهدت الولايات المتحدة استثمارا ضخما في آلات التصويت، وكان العديد منها لا يقدم إثباتا ورقيا.

وفي عامي 2005 و 2007، نشرت المبادئ التوجيهية لنظام التصويت الطوعي في الولايات المتحدة، وهي حالياً أكثر المبادئ التوجيهية شمولا، وتشتمل على مواصفات اعتماد آلات التصويت ومتطلباتها.

وبحلول عام 2008، صار العديد من الولايات الأميركية يشترط الإثبات الورقي للأصوات، بما يؤدي إلى إنهاء خدمة الآلات التي لا تقدم إثباتا ورقيا في تلك الولايات.
وحتى عام 2010، صارت 40 ولاية تشترط الإثبات الورقي للأصوات [6].

5) الهند:

اقترح S Chakraborty و S Mukherjee في عام 2016 بناء آلة تصويت إلكترونية آمنة باستخدام تقنية بصمات الأصابع، بحيث يمكننا استخدام قاعدة بيانات بطاقة الهوية الوطنية الهندية "آدهار".
يمكن تنفيذ عملية تأكيد التصويت عبر الإنترنت خلال الانتخابات باستخدام كشف أوردة الأصابع، مما يتيح إعادة تعيين للتصويت الإلكتروني للسماح للناخبين بالإدلاء بأصواتهم [7].

IV. فاتورة التصويت الالكتروني:

فيما يلي بعض الأمثلة على تكاليف أنظمة التصويت الإلكتروني. حساب التكاليف يختلف بين البلدان. وبالإضافة إلى ذلك، هناك تأثير ضخم للتكنولوجيا التي يقع عليها الاختيار وللسياق (عدد الناخبين، وعدد الاستحقاقات الانتخابية) على التكلفة لكل ناخب. وتجدر الإشارة أيضا إلى أن تلك ليست إلا تكلفة رأس المال لتطبيق النظام، ويتعين إضافة تكاليف الصيانة والتخلص من النظام إن كان لابد من ذلك إليها.

1) البرازيل :

مليار دولار أميركي كتكلفة مبدئية، بالإضافة إلى 500 مليون دولار أميركي لكل انتخابات يشارك بها 100 مليون ناخب. [8]

2) إستونيا:

مليون ونصف يورو لإنشاء النظام (دون الحاجة إلى نظام للتحقق من هوية الناخب)، تكاليف التشغيل نحو 100,000يورو لـ 100,000 ناخب و مليون مسجل .[5]

3) **أيرلندا :**

أنفق مبلغ 53 مليون يورو لنظام يغطي 2.5 مليون ناخب (21 يورو/ناخب (بالإضافة إلى 800,000 يورو تكاليف التخزين سنويا. [9]

V. مشكلات قد تواجهها أنظمة التصويت الإلكتروني الحالية:

1) الخصوصية:

قد يكون من الصعب ضمان خصوصية الناخبين بأن تكون الأصوات مجهولة الهوية في نظام التصويت الإلكتروني. خاصة إذا تمكن شخص ما من الوصول إلى نظام التصويت، بما في ذلك المشرفين والمسؤولين عليه.

2) مخاوف بشأن الأمان:

قد تكون أنظمة التصويت الإلكتروني عرضة للهجمات الإلكترونية. فقد يتمكن المخترقين من تغيير الأصوات أو منع الناس من التصويت .

3) التكلفة:

قد لا تتمكن جميع الدول خاصة دولنا العربية من تحمل تكلفة نظام التصويت الإلكتروني بسبب التكلفة الباهظة لأنظمة خاصة في الإعداد والصيانة.
قد تكون أنظمة التصويت الإلكتروني باهظة الثمن في الإعداد والصيانة.

4) التعقيد:

قد تكون أنظمة التصويت الإلكتروني معقدة في الاستخدام. مما قد يسبب لبعض الناخبين صعوبة في التصويت.

VI. الخاتمة:

يعد هذا الفصل بمثابة مدخل لفهم أنظمة التصويت، سواء التقليدية أو الإلكترونية، من خلال استعراض تعريفاتها ومميزاتها وعيوبها، مستندين إلى مصادر عربية وأجنبية ذات موثوقية عالية. وقد قمنا بتسليط الضوء على أنظمة التصويت الإلكتروني بشكل مفصل، تقييما لإمكانياتها وفوائدها في تعزيز العملية الانتخابية، مع التطرق إلى التحديات والعقبات التي تواجه تطبيقها على نطاق واسع.

في رحلتنا لاستكشاف حلول مبتكرة لتعزيز نزاهة وفعالية العملية الانتخابية، نتجه في الفصل الثاني نحو تقنية البلوك شين والعقود الذكية. وسنتناول بالتفصيل أهمية هذه التقنيات في مجال التصويت، ومدى إمكانية توظيفها لخلق نظام انتخابي أكثر أمانًا وشفافية وكفاءة.

الفصل الثاني:

البلوك شين والإيثريوم: المفاهيم والتقنيات

I. مقدمة:

التصويت في الانتخابات ربما المجال الوحيد الذي لم يستفد من الثورة التقنية بشكل كبير لحد الآن، فلا زالت القيود هي نفسها التي تتطلب حضور الناخبين فعليا لموقع الاقتراع للإدلاء بأصواتهم الأمر الذي قد يجعل الأمور معقدة في كثير من الأحيان ناهيك عن التجارب الفاشلة للاقتراع الالكتروني الذي لم يأتي بالحل كونه عرضة للاختراق والتلاعب وانتهاك خصوصية الناخبين.
تقنية البلوك شين يمكنها القضاء على الكثير من هذه المشاكل والعقبات التي تعترض عملية الاقتراع وتحييدها سواء تلك المتعلقة بالاقتراع التقليدي أو الالكتروني، وتعزيز الأمان والشفافية وتجنب التزوير، مما يضمن نتائج انتخابات تعبر بدقة عن إرادة الناخبين وتفرز من يرقى لمستوى تطلعاتهم.

II. تقنية البلوك شين: رحلة من خلال المفاهيم الأساسية:

1) تعريف تقنية البلوك شين:

يتم تعريف تقنية Blockchain على أنها نظام دفتر لامركزي وموزع يتيح حفظ سجلات المعاملات بشكل آمن وشفاف ومقاوم للتلاعب عبر شبكة من أجهزة الكمبيوتر. ويشير مصطلح "البلوكشين" إلى سلسلة من الكتل، حيث تحتوي كل كتلة على قائمة من المعاملات. اكتسبت هذه التكنولوجيا مكانة بارزة باعتبارها البنية التحتية الأساسية للعملات المشفرة مثل البيتكوين، لكن تطبيقاتها تمتد إلى ما هو أبعد من العملات الرقمية. [12]

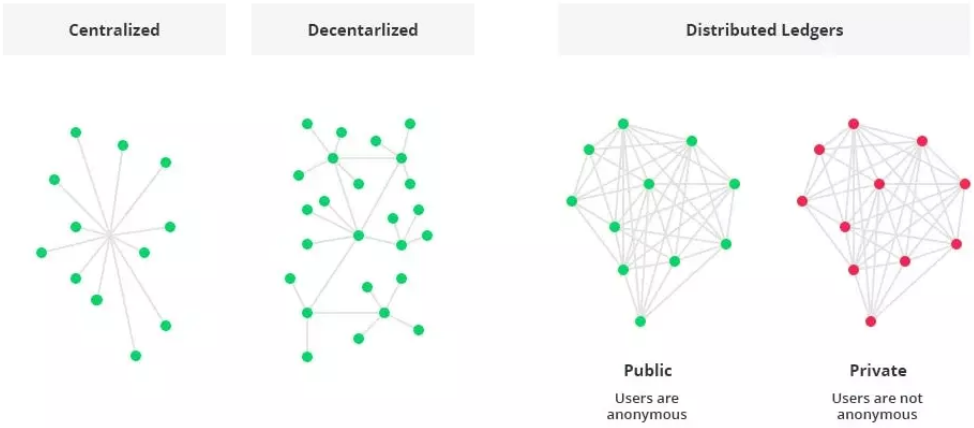
2) السياق التاريخي:

بداية تقنية البلوك شين كانت قبل فترة طويلة من شهرتها الواسعة، حيث تم طرحها لأول مرة عام 1991 على يد مجموعة من الباحثين، وكان الهدف الأساسي منها إنشاء نظام لتأريخ المستندات الرقمية، والتأكد من عدم إمكانية تزويرها أو العبث بها. مهدت هذه الفكرة لأرضية البلوك شين كما نعرفها اليوم. ومع ذلك، ظلت حبرا على ورق حتى عام 2008 ، حينها بفضل "ساتوشي ناكاموتو" تم استخدامها فعليا مع مجموعة من التقنيات في إطلاق عملة البتكوين، وهي عملة مشفرة تعتمد في بنيتها على تقنية البلوك شين، وتحولت التقنية من يومها من مفهوم نظري إلى أداة أحدثت ثورة في عالم العملات الرقمية. [13]

3) بنية البلوك شين:

- لامركزية الشبكة:

منطقيا، البلوك شين عبارة عن سلسلة من الكتل تحتوي على معلومات محددة (قاعدة بيانات)، يتم تجميعها معًا بطريقة آمنة في شبكة (نظير إلى نظير "P2P"). بعبارة أخرى، البلوك شين عبارة عن مجموعة من أجهزة الكمبيوتر المرتبطة ببعضها البعض بدلاً من خادم مركزي، مما يعني أن الشبكة بأكملها لامركزية.



صورة رقم 2 سجلات مركزية، لامركزية وموزعة. [2]

لجعل الأمر أكثر بساطة، يمكن مقارنة مفهوم البلوك شين بالعمل المنجز باستخدام مستندات Google. في وقت مضى قد نقوم لإنجاز بحث ما بإرسال المستندات ذهابًا وإيابا وانتظار الزملاء الآخرين لإجراء التعديلات اللازمة. الآن، وبمساعدة مستندات Google، يمكن العمل كفريق على نفس المستند في وقت واحد.

تتيح تقنية البلوك شين توزيع المعلومات الرقمية بدلا من نسخها. يوفر هذا السجل الموزع الشفافية والثقة وأمان للبيانات.

يتم استخدام بنية البلوك شين على نطاق واسع جدًا في المجال المالي. كما تساعد هذه التقنية في الوقت الحالي على إنشاء وتطوير برامج لامركزية للعملات المشفرة وحفظ السجلات خاصة المهمة منا والتوثيق الرقمي والعقود الذكية. [14]

بالتعمق أكثر في بنية البلوك شين، تظهر لنا خصائصها الأساسية والتي هي بمثابة ركائز لهذه التقنية الثورية، نجد أن بنية البلوك شين تتميز باللامركزية بشكل أساسي، مما يلغي الحاجة إلى أي سلطة مركزية ويعزز بالتالي قوة الشبكة ضد أي أعطال أو هجمات. في بنية البلوك شين، يلعب كل مشارك في الشبكة، أو عقدة "node"، دورا في الحفاظ عليها، وبهذا نصل إلى نظام بيئي رقمي أكثر ديمقراطية وعدالة. هناك جانب رئيسي آخر هو أمان الشبكة والمتأصل في مفهوم بنية البلوك شين، الذي توفره تقنيات التشفير المتقدمة. تضمن هذه الميزة جنبًا إلى جنب مع البنية الدقيقة

للكتلة أو الـ "block" في شبكة البلوك شين، أمان البيانات بحيث بمجرد تسجيلها في الشبكة، تصبح غير قابلة للتغيير أو التعديل. لا تحدد هذه الخصائص بنية البلوك شين فحسب، بل تفتح أيضًا المجال أمام عدد لا يحصى من إمكانات التطبيق في كل الميادين، بدءًا من التمويل وحتى إدارة سلسلة التوريد، وطبعا التصويت. [13]

- الطبقات التقنية لبنية البلوك شين:

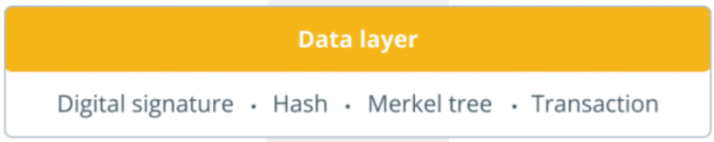
يمكن تصنيف البنية الطبقية للبلوك شين إلى خمس طبقات رئيسية:

- **طبقة البنية التحتية للأجهزة:**

لا يتم تخزين البيانات على شبكة البلوك شين على أي خادم داخل مركز بيانات كباقي الشبكات الضخمة. بدلاً من ذلك، تستخدم تقنية البلوك شين شبكة نظير إلى نظير (P2P) لامركزية البيانات. يتصفح الأشخاص على الويب أو يستخدمون أي تطبيق على الشبكة، ويطلبون المحتوى مباشرة من أجهزة الكمبيوتر الأخرى على الشبكة.

صورة رقم 3 طبقات البلوك شين. [3]

- **طبقة البيانات:**

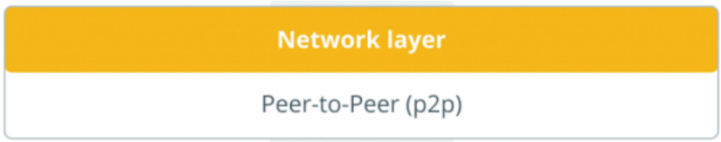


يأخذ البلوك شين شكل سلسلة مرتبطة من الكتل، حيث تحتوي كل كتلة على مجموعة مرتبة من المعاملات. تحتوي كل كتلة على عنصرين رئيسيين:

- قائمة مرتبطة من الكتل المتسلسلة: يتم ربط كل كتلة بالكتلة التي سبقتها باستخدام رابط خاص يُسمى الـ "hash" السابق. يعمل هذا المؤشر كبصمة تشفيرية فريدة للكتلة السابقة، مما يجعل من المستحيل تعديل أي كتلة دون اكتشاف التعديل لتغير الـ hash مباشرة.
- شجرة Merkle: وهي بنية بيانات على شكل شجرة ثنائية تستخدم لتخزين وتحسين سلامة البيانات في كل كتلة. توفر شجرة Merkle ضمانًا ضد التلاعب بالبيانات داخل الكتلة.

يتم توقيع المعاملات رقميًا باستخدام مفاتيح خاصة لمزيد من الأمان. يمكن لأي شخص لديه المفتاح العام التحقق من صحة التوقيع، مما يضمن عدم إجراء أي تغييرات على البيانات بعد توقيعها.

- **طبقة الشبكة:**



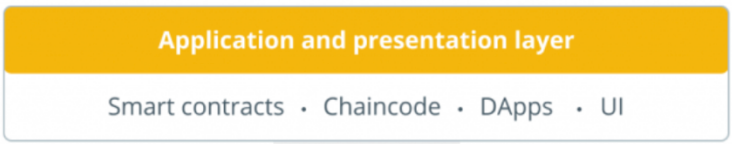
تُعرف أيضًا باسم طبقة P2P ، وتضمن هذه الطبقة أن العقد (أجهزة الكمبيوتر على الشبكة) يمكنها العثور على بعضها البعض والتفاعل ونشر المعلومات ومزامنتها.

يضمن هذا التشغيل السلس لشبكة البلوك شين.

- **طبقة التوافق:**

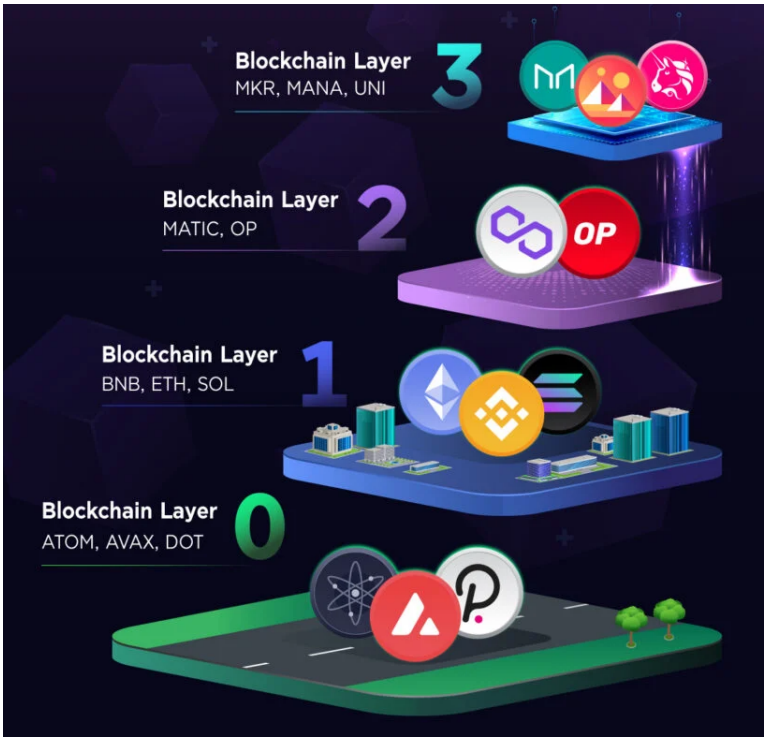
تعتبر طبقة التوافق من أهم طبقات بنية البلوك شين. فهي المسؤولة عن التحقق من صحة الكتل وترتيبها بالشبكة، مع ضمان موافقة جميع المشاركين على هذه العملية.

- **طبقة التطبيقات:**



تحتوي هذه الطبقة على عقود ذكية (برامج ذاتية التنفيذ) وتطبيقات لامركزية (DApps) بالإضافة إلى واجهات برمجة التطبيقات (APIs) وبرامج المستخدم الرسومية (UIs) والإطارات البرمجية التي يستخدمها المستخدمون للتفاعل مع شبكة البلوك شين. [14]

- **الطبقات المفاهيمية لبنية البلوكشين:**



صورة رقم 4 الطبقات المفاهمية لبنية البلوك شين. [4]

- **الطبقة 0 (Layer 0) :**

هي انترنت البلوك شين إن صح التعبير أي البنية التحتية التي تدعم شبكات البلوك شين المتعددة وتسمح لها بالتفاعل مع بعضها البعض.
تشمل بروتوكولات الاتصال بين الشبكات، وأي تقنيات أخرى تدعم عمل الشبكات.
مثال : Polkadotو Cosmos اللذان يوفران إمكانية التشغيل البيني بين شبكات البلوك شين المختلفة.

- **الطبقة 1 (Layer 1) :**

تمثل الشبكة الرئيسية للبلوك شين نفسها وتشمل البروتوكولات الأساسية التي تدير الشبكة.
تتضمن التحقق من المعاملات، إنشاء الكتل، والتوافق بين العقد.
مثال : Ethereum. Bitcoin

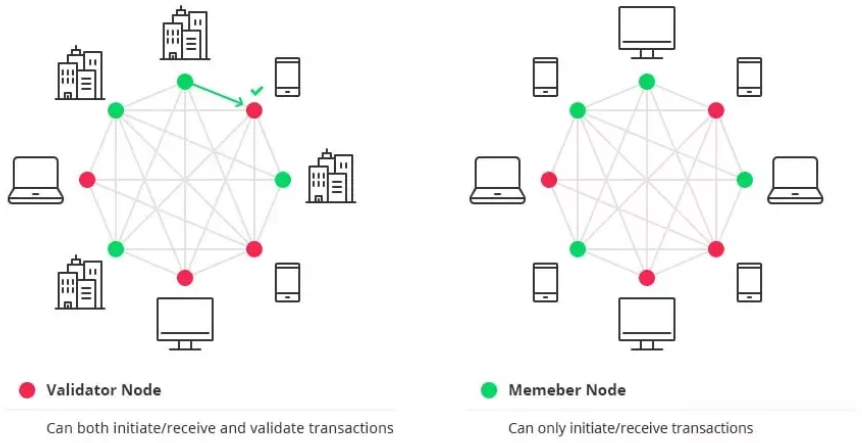
- **الطبقة 2 (Layer 2) :**

تقع فوق الطبقة 1 وتهدف إلى تحسين أداء وكفاءة الشبكة الأساسية من خلال تقليل الحمل عليها. وتستخدم أيضا لحل مشكلة التوسع على الشبكة
مثال: حلول الطبقة الثانية مثل Lightning Network للبيتكوين و Optimistic Rollups للإيثيريوم.

- **الطبقة 3 (Layer 3) :**

هي التطبيقات والخدمات التي تُبنى فوق الطبقات السابقة. تشمل العقود الذكية، التطبيقات اللامركزية (DApps) ، والمحافظ الرقمية.
مثال: Uniswap .[15]

أنواع بنية البلوك شين:



صورة رقم 5 العقد في البلوك شين العام والخاص. [2]

يمكن تصنيف جميع هياكل البلوك شين إلى خمس فئات:

- **البلوك شين العام (Public Blockchain):**

شبكة بلوك شين مفتوحة للجميع ويمكن لأي شخص الانضمام إليها والمشاركة في عملية التحقق من المعاملات.

الميزات:

- **الشفافية :**جميع المعاملات متاحة للجميع ويمكن التحقق منها.
- **اللامركزية:** لا يوجد تحكم مركزي.
- **الأمان :** يعتمد على بروتوكولات التوافق مثل : إثبات العمل (PoW) و إثبات الحصة (PoS) .
- **الأمثلة :** البتكوين، الاثريوم.

- **البلوك شين الخاص (Private Blockchain) :**

شبكة بلوك شين مغلقة حيث يمكن فقط للمشاركين المصرح لهم الوصول والمشاركة.

الميزات:

- **التحكم :**يتحكم فيها كيان واحد أو مجموعة محددة من الكيانات.
- **الأمان :**يتم التحكم في الوصول، مما يعزز الأمان الداخلي.

- **الأداء :**أسرع وأكثر كفاءة مقارنة بالبلوك شين العام بسبب وجود عدد أقل من المشاركين.
- **الأمثلة :**شبكات خاصة للشركات مثل : Hyperledger Fabric

- **البلوك شين الهجين (Hybrid Blockchain) :**

مزيج من البلوك شين العام والخاص، حيث يكون لبعض البيانات العامة الشفافية بينما يتم الاحتفاظ ببعضها الآخر خاصًا.

الميزات:

- **المرونة :**يمكن تخصيص الوصول حسب الحاجة.
- **الأمان :**يمكن أن يكون أكثر أمانًا بفضل التحكم في الوصول.
- **التفاعل :**يتيح التفاعل بين الأجزاء العامة والخاصة.
- **الأمثلة :** بلوك شين ريبل "ripple"جزء عام وجزء خاص.

- **البلوك شين المصرح به (Permissioned Blockchain) :**

نوع من البلوك شين الخاص حيث يُسمح فقط للمشاركين المعتمدين بالوصول والمشاركة.

الميزات:

- **الأمان :**التحكم في الوصول يضمن أمانًا عاليًا.
- **الأداء :**أداء أسرع وأكثر كفاءة.
- **الموثوقية :**يمكن تحديد أدوار ومسؤوليات محددة للمشاركين.
- **الأمثلة** : Corda.

- **البلوك شين الكونزرتيوم (Consortium Blockchain) :**

شبكة بلوك شين تدار من قبل مجموعة من المنظمات بدلاً من كيان واحد.

الميزات:

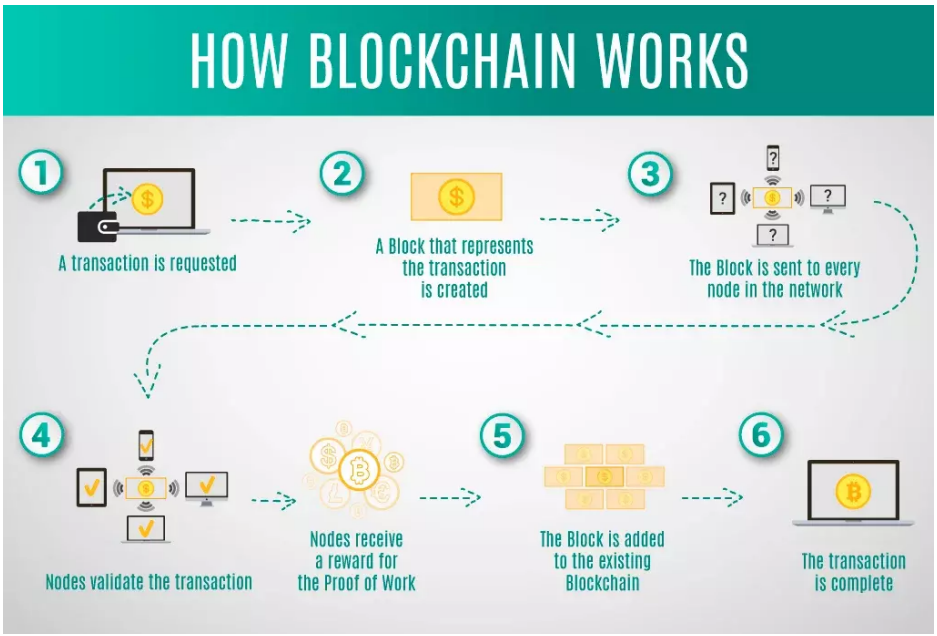
- **التعاون :**تعزيز التعاون بين المؤسسات.
- **اللامركزية الجزئية :**لا يسيطر عليها كيان واحد.
- **الأمان :**أمان معزز بفضل التحقق المشترك بين المنظمات.
- **الأمثلة :**مشاريع مشتركة بين البنوك أو المؤسسات المالية. [16]

☐ المكونات الأساسية لبنية البلوك شين: كيف تعمل؟

فيما يأتي المكونات الأساسية لبنية البلوك شين:

- **العقدة (Node):** وهي عبارة عن مستخدم أو حاسوب ضمن بنية البلوك شين (يحتفظ كل منها بنسخة مستقلة كاملة من سجل البلوك شين بأكمله).
- **المعاملة (Transaction):** أصغر عنصر بناء في نظام البلوك شين (السجلات والمعلومات وما إلى ذلك).
- **الكتلة (Block):** بنية بيانات تُستخدم لحفظ مجموعة من المعاملات التي يتم توزيعها على جميع العقد في الشبكة.
- **السلسلة (Chain):** عبارة عن تسلسل من الكتل بترتيب معين.
- **المعدنون (Miners):** عقد محددة تقوم بعملية التحقق من الكتلة قبل إضافة أي شيء إلى بنية البلوك شين.
- **الإجماع (بروتوكول الإجماع):** مجموعة من القواعد والترتيبات لتنفيذ عمليات البلوك شين.

أي سجل أو معاملة جديدة داخل البلوك شين يعني بناء كتلة جديدة. بعدها يتم إثبات كل سجل والتوقيع عليه رقميًا لضمان صحته. قبل إضافة هذه الكتلة إلى الشبكة، يجب التحقق منها من قبل غالبية العقد في النظام. [17]
فيما يلي رسم تخطيطي لبنية البلوك شين يوضح كيفية عمل ذلك بالفعل في شكل محفظة رقمية.



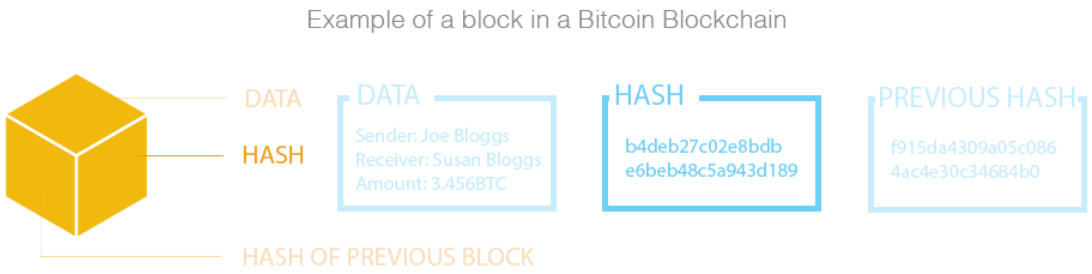
صورة رقم 6 كيف تعمل تقنية البلوك شين. [2]

4) كيف يعمل البلوك شين:

صورة رقم 7 كتل البلوك شين. [5]

لنلقي نظرة فاحصة عن ماهية الكتلة في البلوك شين لنفهم بشكل أعمق آلية عمل البلوك شين.
تكون كل كتلة بلوك شين من:

- **بيانات معينة**
- **هاش الكتلة**
- **هاش الكتلة السابقة**



صورة رقم 8 مثال لكتلة على بلوك شين البتكوين. [6]

تعتمد البيانات المخزنة داخل كل كتلة على نوع البلوك شين .على سبيل المثال، في بنية بلوك شين البيتكوين، تخزن الكتلة بيانات المستقبل والمرسل ومبلغ العملات المعدنية.

يعتبر الهاش "hash" مثل بصمة الإصبع (سجل طويل يتكون من بعض الأرقام والحروف). يتم إنشاء كل هاش كتلة باستخدام خوارزمية تشفير (SHA 256) وبالتالي، يساعد هذا على تحديد كل كتلة في

بنية البلوك شين بسهولة. في اللحظة التي يتم فيها إنشاء كتلة، فإنها تأخذ تلقائيًا هاش، كما تؤثر أي تغييرات يتم إجراؤها في أي كتلة على تغيير الهاش الخاص بها أيضا. ببساطة، يساعد التشفير على اكتشاف أي تغييرات في الكتل وبهذا يستحيل تغيير أي بيانات دون الكشف عن ذلك.

آخر عنصر داخل الكتلة هو هاش الكتلة السابقة. الذي بدوره يخلق سلسلة من الكتل وهو العنصر الرئيسي وراء أمان بنية البلوك شين .على سبيل المثال، يشير الرقم 45 إلى الرقم 46 .

أول كتلة في السلسلة خاصة قليلا - يتم استنتاج جميع الكتل المؤكدة والمصادق عليها من الكتلة الأولى.(genesis block)

أي محاولات لتغيير البيانات ستغير هاش الكتل، الذي بدوره يجعل جميع الكتل التالية تشير إلى معلومات غير صحيحة وتفضي إلى نظام بلوك شين بأكمله غير صالح.

من ناحية أخرى، نظريا قد يكون من الممكن تعديل جميع الكتل بمساعدة معالجات كمبيوتر قوية . ومع ذلك، هناك حل يزيل هذا الاحتمال يسمى إثبات العمل .(proof-of-work) وهذا يسمح للمستخدم بإبطاء عملية إنشاء كتل جديدة .في بنية بلوك شين بيتكوين، يستغرق الأمر حوالي 10 دقائق لتحديد إثبات العمل الضروري وإضافة كتلة جديدة إلى السلسلة .يتم تنفيذ هذا العمل من قبل المعدنين - وهي عقد خاصة ضمن بنية بلوك شين بيتكوين .يحصل المعدنون على رسوم المعاملات من الكتلة التي قاموا بالتحقق منها كمكافأة.

يتلقى كل مستخدم (عقدة) جديد ينضم إلى شبكة نظير إلى نظير للبلوك شين نسخة كاملة من سجل الشبكة .بمجرد إنشاء كتلة جديدة، يتم إرسالها إلى كل عقدة داخل نظام البلوك شين .بعد ذلك، تتحقق كل عقدة من الكتلة وتتحقق مما إذا كانت المعلومات الواردة صحيحة .إذا كان كل شيء على ما يرام، تتم إضافة الكتلة إلى البلوك شين المحلي في كل عقدة.

تشكل جميع العقد داخل بنية البلوك شين **بروتوكول إجماع (Consensus Protocol).** يعد نظام الإجماع مجموعة من قواعد الشبكة، وعندما يلتزم الجميع بها، يتم تطبيقها ذاتيًا داخل البلوك شين. على سبيل المثال، يمتلك بلوك شين بيتكوين قاعدة إجماع تنص على أنه يجب تخفيض قيمة المعاملة إلى النصف بعد كل 200,000 كتلة .وهذا يعني أنه إذا كان مكافأة التحقق قدرها 10 بيتكوين، فيجب تخفيض هذه القيمة إلى النصف بعد كل 200,000 كتلة.

بالإضافة إلى ذلك، لا يمكن تعدين سوى 4 مليون بيتكوين أخرى فقط، حيث يوجد حد أقصى يبلغ 21 مليون بيتكوين محدد في بروتوكول نظام بلوك شين بيتكوين .وبمجرد أن يقوم المعدنون باستخراج هذا العدد، ينتهي عرض عملات البيتكوين ما لم يتم تغيير البروتوكول.

باختصار، هذا يجعل تقنية البلوك شين **غير قابلة للتغيير وآمنة تشفيرياً** من خلال إزالة أي وسطاء . من المستحيل اختراق نظام البلوك شين لأنه يلزم اختراق جميع كتلاته، وإعادة حساب إثبات العمل لكل كتلة، وكذلك التحكم في أكثر من 50٪ من جميع العقد في شبكة نظير إلى نظير وهذا مستحيل في بلوك شين البتكوين. [14]

5) ميزات تقنية البلوك شين:

صورة رقم 9 بلوك شين البتكوين. [7]

<u>دقة سلسلة الكتل:</u> تتم الموافقة على المعاملات على شبكة البلوك شين من قبل آلاف الحواسيب والأجهزة .وهذا يزيل تقريبا العامل البشري من عملية التحقق، مما يؤدي إلى تقليل الأخطاء والحصول على سجل دقيق للمعلومات .حتى لو ارتكب أحد الحواسيب على الشبكة خطأ في الحساب، فقد كان على نسخة واحدة فقط من البلوك شين ولن يتم قبوله من قبل بقية الشبكة.

- **خفض التكاليف:** عادة، يدفع عملاء البنوك مقابل التحقق من معاملة أو لأي كاتب عدل أو موظف لتوقيع مستند .تقضي البلوك شين على الحاجة إلى التحقق من قبل طرف ثالث - وبالتالي، التكاليف المرتبطة بها.

- **اللامركزية:** لا يخزن البلوك شين أيًا من معلوماته في موقع مركزي .بدلاً من ذلك، يتم نسخ البلوك شين ونشره عبر شبكة من الحواسيب .كلما تمت إضافة كتلة جديدة إلى البلوك شين، يقوم كل كمبيوتر على الشبكة بتحديث سلسلة الكتل الخاصة به لتكون مطابقة للتغيير.

- **كفاءة المعاملات:** يمكن أن تستغرق المعاملات التي تتم من خلال سلطة مركزية كالبنوك مثلا عدة أيام حتى تتم .على سبيل المثال، إذا حاولت إيداع شيك مساء يوم الجمعة، فقد لا ترى الأموال في حسابك حتى صباح يوم الاثنين .تعمل المؤسسات المالية خلال ساعات العمل، عادةً خمسة أيام في الأسبوع - ولكن البلوك شين يعمل 24 ساعة في اليوم، وسبعة أيام في الأسبوع، و 365 يومًا في السنة.
في بعض سلاسل البلوك شين، يمكن الانتهاء من المعاملات في بضع دقائق واعتبارها آمنة بعد دقائق قليلة فقط .وهذا مفيد بشكل خاص للمعاملات العالمية، والتي عادة ما تستغرق وقتًا أطول بسبب مشكلات المنطقة الزمنية كما قد يتعين على جميع الأطراف تأكيد معالجة الدفع.

- **المعاملات الخاصة:** تعمل العديد من شبكات البلوك شين كقواعد بيانات عامة، مما يعني أن أي شخص لديه اتصال بالإنترنت يمكنه عرض قائمة بسجل معاملات الشبكة .على الرغم من أن المستخدمين يمكنهم الوصول إلى تفاصيل المعاملة، إلا أنهم لا يمكنهم الوصول إلى معلومات وهويات المستخدمين الذين يقومون بهذه المعاملات .

- **المعاملات الآمنة :** بمجرد تسجيل المعاملة، يجب التحقق من صحتها من قبل شبكة البلوك شين .بعد التحقق من صحة المعاملة، تتم إضافتها إلى كتلة البلوك شين .تحتوي كل كتلة على البلوك شين على رقم تجزئة (Hash) فريد خاص بها والرقم التجزئة الفريد للكتلة التي تسبقها .لذلك، لا يمكن تعديل الكتل بمجرد تأكيدها من قبل الشبكة.

- **الشفافية:** تعتمد العديد من تقنيات البلوك شين على برمجيات مفتوحة المصدر بالكامل . وهذا يعني أنه يمكن لأي شخص رؤية الكود الخاص بها .يتيح هذا للمدققين والمختصين الأمنيين مراجعة العملات المشفرة مثل البتكوين للتأكد من أمانها .ومع ذلك، فهذا يعني أيضًا أنه لا توجد جهة مركزية تتحكم فعليًا في كود البتكوين أو كيفية تعديله .ونتيجة لذلك، يمكن لأي شخص اقتراح تغييرات أو ترقيات على نظام البلوك شين .إذا وافقت غالبية مستخدمي الشبكة على أن الإصدار الجديد من الكود مع الترقية سليم ويستحق، فيمكن تحديث البتكوين.

أما بالنسبة لأنظمة البلوك شين الخاصة أو التي تتطلب إذنًا للوصول، فقد لا تسمح بالشفافية العامة وذلك وفقًا لكيفية تصميمها أو الغرض من استخدامها .على سبيل المثال، قد يتم إنشاء هذا النوع من سلاسل البلوك شين لمؤسسة ترغب في تتبع بياناتها بدقة دون السماح لأي شخص خارج المستخدمين المصرح لهم برؤية هذه البيانات. [17]

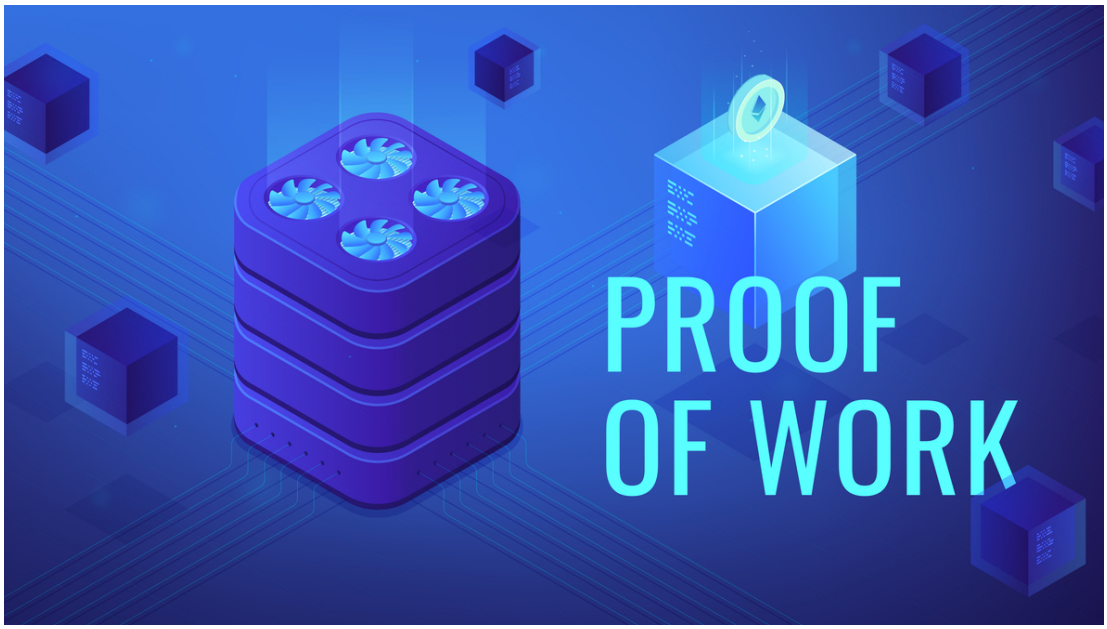
III. آليات التوافق: مفتاح ضمان أمان شبكات البلوك شين:

ببساطة، آليات التوافق هي مجموعة من القواعد والأنظمة التي تحكم كيفية تفاعل العقد مع بعضها البعض وتوصلهم إلى إجماع حول حالة الشبكة.

تُشكل هذه الآليات العمود الفقري لأمان شبكات البلوك شين، حيث تمنع التلاعب بالبيانات والاحتيال، وتضمن أن جميع المشاركين في الشبكة يتبعون نفس القواعد.

وتستخدم الكثير من الأصول المشفرة آليات الإجماع بهدف التحقق من صحة المعلومات المضافة إلى دفتر الحسابات مما يمنع الإنفاق المزدوج أي إرسال معاملتين بنفس الرمز المميز. بالإضافة إلى منع إضافة بيانات خاطئة إلى شبكة البلوك شين. هناك العديد من الآليات التي تحقق نفس الهدف ولكن تختلف في الأسلوب وبخاصة في تعيين مكافأة المعدنيين. ومن بين تلك الطرق طريقة إثبات العمل (PoW) وطريقة إثبات الحصة (PoS).

1) ما هو إثبات العمل (PoW)؟:



صورة رقم 10 إثبات العمل PoW . [8]

ظهر مفهوم إثبات العمل (PoW) قبل عملة البيتكوين BTC في عام 1993 عن طريق Cynthia Dwork وMoni Naor كوسيلة للتخلص من البريد المزيف أو العشوائي ثم توسع المصطلح بعد ذلك، ليتم استخدامه اليوم مع العملات المشفرة.

لإنتاج عملة البيتكوين BTC يتنافس عمال التعدين على حل مجموعة من الألغاز لإكمال كتلة معينة ومن ثم يتم مكافاتهم بعدد من العملات المشفرة التي تم سكها حديثًا، واللغز هنا يسمى بآلية "إثبات العمل".(PoW)

تعد الطريقة الوحيدة لزيادة فرصتك في حل ألغاز آلية إثبات العمل (PoW) هي استخدام قوة حسابية هائلة أو أكبر عدد من الدورات الحسابية لتكوين كتلة.

ويعد نظام إثبات العمل (PoW) الآلية المستخدمة في تعدين معظم العملات المشفرة مثل إيثريوم ETH وبيتكوين BTC على الرغم من ترقية شبكة إيثيريوم في النصف الأول من عام 2020 والانتقال إلى آلية التحصيص أو إثبات الحصة.

2) ما هو إثبات الحصة (PoS)؟:

صورة رقم 11 إثبات الحصة PoS . [9]

لا يعتمد إثبات الحصة (PoS) على حل لغز رياضي بل على احتمالات تتأثر بعدد العملات المشفرة المخزنة في لحظة معينة، حيث تكمن الفرصة في إنشاء كتلة مناسبة في عدد العملات التي تستطيع تخزينها، فمثلاً تزيد فرصة الشخص الذي لديه 30 عملة مشفرة عن الشخص الذي لديه 10 عملات.

في آلية إثبات الحصة يتم إنشاء جميع العملات المشفرة في البداية ولا توجد عملات جديدة والمكافأة تكون برسوم المعاملات وليس بالعملات المشفرة في الفترة الأخيرة.

3) مقارنة بين نظام إثبات العمل (PoW) ونظام إثبات الحصة (PoS):

صورة رقم 12 إثبات الحصة vs إثبات العمل. [10]

- **كمية استهلاك الكهرباء:**

من عيوب إثبات العمل إهدار الطاقة حيث ذكرت مؤسسة Digiconomist أن الاستهلاك السنوي للطاقة لتعدين البيتكوين يبلغ 66.7 تيراواط ساعة بما يعادل ما تستهلكه جمهورية التشيك التي يبلغ عدد سكانها 10.6 مليون نسمة، أما إثبات الحصة فيتسم بانخفاض الطاقة فلا يحتاج عمال التعدين إلى كم الكهرباء الهائل للتنافس والفوز بالكتل، ويمكن لأي شخص الوصول القيام بهذا الأمر فلا يحتاج أجهزة تعدين قوية.

- **الأمان:**

يعد إثبات الحصة نظامًا حديثًا عن إثبات العمل، فلم يُختبر بدقة، ويحجم إثبات العمل بلوك تشين فإذا كانت الشبكة متشبعة يقرر عمال التعدين أي سلسلة يقومون بدعمها أو يقسمون مواردهم الحسابية لدعم جانبي شبكة بلوك تشين. أما في إثبات الحصة (PoS)، يقوم المعدن بالتحقق من كلا الجانبين بل ويحصد ضعف رسوم المعاملة، وتسمى هذه المشكلة الأمنية بمعضلة Nothing-at-stake.

- **اللامركزية:**

يتطلب التعدين استهلاك عالي للكهرباء لذا ينحصر على فئة محدودة من المشغلين مما يهدد مفهوم اللامركزية في التشفير، ولكن يمكن أن تتحقق اللامركزية عن طريق السماح باستخدام أجهزة التعدين وهو ما يحدث بالفعل.

- **توزيع المعروض من العملات المشفرة:**

في إثبات العمل يختار الأشخاص بيع العملات المشفرة بدلاً من الاحتفاظ بها وترتبط التكاليف بالتحقق من وجود هذه العملات وصحتها مما ينتج عنه سيولة متوازنة بالسوق أما إثبات الحصة يشجع التخزين وامتلاك الأشخاص للعديد من العملات المشفرة.

- **احتمالية التعرض لهجوم "attack 51" :**

يحدث هذا الهجوم عندما يتحكم المعدّن أو مجموعة من المعدنيين في أكثر من نصف طاقة الكمبيوتر الخاصة بالشبكة حيث يتمكنوا من إنشاء كتل احتيالية تبطل الكتل الحقيقية، لكن مع آلية إثبات الحصة لا يحدث ذلك ولن يكون من المسموح الاستيلاء على 51% من حصة في عملة ما أو مهاجمة حصة عدد كبير، وإذا انخفضت قيمة العملة المشفرة تنخفض قيمة ما لديك من عملات لذلك يتم تحفيز أصحاب الحصص الأكبر للحفاظ على شبكة آمنة.

توجد خوارزميات إجماع أخرى لم يتم ذكرها هنا ولكل منها مزايا وعيوب وتستخدم بعض العملات المعدنية مثل Peercoin نظام إجماع لتحقيق أكبر كم من الوظائف والأمان والتوسع. نأمل أن يساعدك الدليل على فهم الفرق بين إثبات الحصة وإثبات العمل. [18]

IV. مفهوم العقود الذكية: آلية عملها وفوائدها:

يعرف العقد الذكي بأنه برنامج كمبيوتر لامركزي يعمل على شبكة بلوك شين وينفذ الاتفاقيات بشكل تلقائي وفق شروط حددت مسبقًا. ظهرت العقود الذكية بشكلها الحالي على شبكة الإيثريوم، وهي بمثابة أساس لتطبيقات الويب 3 مثل DeFi و NFTs التي تشهد رواجًا كبيرًا في السنوات الأخيرة.

صورة رقم 13 العقود الذكية. [11]

1) ما هو العقد الذكي؟

العقود الذكية عبارة عن برامج حاسوب يتم استضافتها وتنفيذها على شبكة البلوك شين. يتكون كل عقد ذكي من كود يحدد شروطًا مسبقة محددة. عند استيفاء هذه الشروط، يتم تنفيذ إجراءات معينة بشكل آلي. بفضل تنفيذها على شبكة بلوك شين لامركزية بدلاً من خادم مركزي، تسمح العقود الذكية لأطراف متعددة بالتوصل إلى نتيجة مشتركة بطريقة دقيقة وفي الوقت المناسب وآمنة ضد التلاعب.

تعتبر العقود الذكية بنية تحتية قوية للأتمتة لأنها لا تخضع لسيطرة مسؤول مركزي ولا تكون عرضة لنقاط ضعف يمكن استغلالها من قبل جهات ما.

يمكن بتطبيق العقود الذكية على اتفاقيات رقمية متعددة الأطراف، تقليل مخاطر التعامل مع الطرف الآخر، زيادة الكفاءة، خفض التكاليف، وتوفير مستويات جديدة من الشفافية في العمليات.

2) علاقة العقود الذكية بشبكات البلوك شين:

تتيح شبكات البلوك شين الداعمة للعقود الذكية للمطورين عليها، كتابة منطق تطبيقي خاص فوق نظام الإجماع اللامركزي الذي توفره هذه الشبكات. لذلك يمكن القول بأن العقود الذكية وشبكات البلوك شين والتطبيقات المبنية عليها على أنها مرتبطة هرميًا: بحيث يتم إنشاء التطبيقات (بما في ذلك الرموز الرقمية) بواسطة الكود من عقد ذكي واحد "أو عدة عقود ذكية متصلة". يتم بعد ذلك تنفيذ الإجراءات المحددة في العقد الذكي وتخزينها بواسطة شبكة البلوك شين الأساسية. [19]

3) كيف تعمل العقود الذكية؟

صورة رقم 14 العقود الذكية. [11]

تعمل العقود الذكية على شبكات البلوك شين وفق منطق محدد مسبقًا، على سبيل المثال: "إذا حدث كذا، فنفذ كذا". يمكن لعقد ذكي واحد أن يشتمل على شروط متعددة ويمكن لتطبيق واحد أن يعتمد على عدة عقود ذكية مترابطة لدعم مجموعة

من العمليات المتصلة. توجد أيضًا لغات برمجة متعددة خاصة بالعقود الذكية، مع كون لغة Solidity على شبكة إيثريوم الأكثر شيوعًا.

بإمكان أي مطور إنشاء عقد ذكي ونشره على شبكة بلوك شين عامة لأغراضه الخاصة، على سبيل المثال، إنشاء عقد ذكي كمجمع عائد شخصي يحول أمواله تلقائيًا إلى التطبيق ذي العائد الأعلى. ومع ذلك، تشتمل العديد من العقود الذكية على أطراف مستقلة متعددة قد لا يعرف بعضها البعض ولا يثقون ببعضهم بالضرورة.

يحدد العقد الذكي بالضبط كيفية تفاعل المستخدمين معه، بما في ذلك من يمكنه التفاعل مع العقد الذكي، وفي أي وقت، وما هي المدخلات التي تؤدي إلى أي مخرجات. والنتيجة هي اتفاقيات رقمية متعددة الأطراف تتطور من الحالة الاحتمالية الحالية، حيث من المحتمل أن يتم تنفيذها كما هو مرغوب وفقًا لكودها. [20]

4) هل تدعم جميع شبكات البلوك شين العقود الذكية؟

لا يمكن لجميع شبكات البلوك شين تشغيل العقود الذكية. على سبيل المثال، لا يدعم بلوك شين البيتكوين العقود الذكية. على عكس شبكات البلوك شين و شبكات الطبقة الثانية المبنية على شبكات أخرى بما في ذلك Arbitrum و Avalanche و Base و BNB Chain وEthereum ، و التي تعد أمثلة على شبكات بلوك شين متوافقة مع العقود الذكية. [19]

5) السياق التاريخي للعقود الذكية:

صورة رقم 15 نيك سابو. [12]

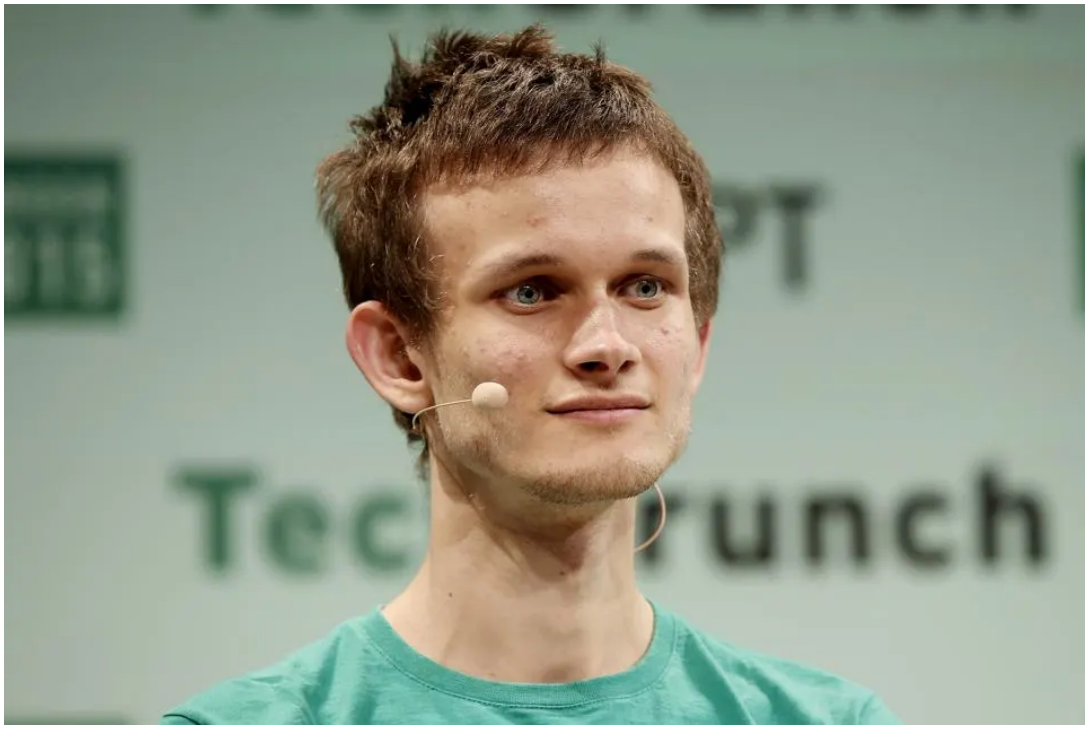
تم صياغة مصطلح "العقد الذكي" لأول مرة من قبل عالم الكمبيوتر الأمريكي نيك سابو في عام 1994. قدم تعريفًا عامًا للعقود الذكية في كتاباته

الأساسية على النحو التالي: "بروتوكول معاملات محوسب ينفذ شروط العقد"، مع أهداف عامة تتمثل في "استيفاء الشروط التعاقدية الشائعة، وتقليل الاستثناءات الخبيثة والعرضية إلى الحد الأدنى، والتقليل من الحاجة إلى وسطاء موثوق بهم."

في حين يمكن رؤية فكرة عامة عن العقود الذكية في أنظمة مثل آلات البيع (على سبيل المثال، يؤدي إدخال رمز معين إلى أخذ وجبة خفيفة)، فإن شبكات البلوك شين شكلت الأساس للعقود الذكية الرقمية والمضمونة ضد التلاعب تأصيلا لمبدأ اللامركزية.

يُعد إطلاق بلوك شين البيتكوين في عام 2009 الداعم لما يجادل البعض بأنه أول عقد ذكي للبروتوكول - حيث يضع مجموعة من الشروط التي يجب استيفاؤها لتحويل عملات البيتكوين بين المستخدمين على الشبكة. تتضمن هذه الشروط توقيع المستخدم للمعاملة باستخدام المفتاح الخاص الصحيح الذي يطابق عنوانه العام (يشبه كلمة المرور المرتبطة بحساب معين) وامتلاك المستخدم لأموال كافية لتغطية المعاملة.

ثم تطور بلوك شين البيتكوين ليقدم نوعًا رئيسيًا آخر من العقود الذكية في عام 2012 يسمى معاملة متعددة التوقيعات. تتطلب معاملة متعددة التوقيعات عددا محددا من الأشخاص (المفاتيح العامة) لتوقيع معاملة بمفاتيحهم الخاصة قبل اعتبارها صالحة. وهذا يزيد من أمان أموال المستخدم من خلال التخفيف من نقاط الفشل الفردية مثل فقدان مفتاح خاص أو سرقته.



صورة رقم 16 فيتاليك بيوتيرين . [13]

دخلت شبكات البلوك شين في عملية تطويرية خلال سنوات مضت بإضافة شروط برمجية جديدة (تسمى رموز التشغيل أو opcodes). ومع ذلك، القفزة الحقيقية للعقود الذكية جاءت مع نشر الورقة البيضاء للإيثريوم من قبل فيتاليك بيوتيرين في عام 2013. في عام 2015، تم إطلاق إيثريوم كنوع جديد من شبكات البلوك شين الداعمة للعقود الذكية القابلة للبرمجة. بدلاً من عمل البلوك شين كتطبيق عقد ذكي واحد أو تقديم عدد قليل من رموز التشغيل المحدودة، قدمت العقود الذكية لإيثريوم كمبيوتر عالمي كبير يمكنه تشغيل العديد من العقود الذكية المستقلة في نفس الوقت. [21]

6) أمثلة على العقود الذكية:

تتمثل إحدى وظائف العقد الذكي في أتمتة عملية تجارية محددة بين مجموعة مميزة من الكيانات. تتفق هذه الكيانات مجتمعة على جميع شروط العقد الذكي مثل المدفوعات وسير العملية وحل النزاعات.

قد يتضمن مثال بسيط لعقد ذكي للتجارة العالمية شروطًا مثل:

- **الشرط الأول:** إذا وصلت البضائع في الموعد المحدد، فقم بتنفيذ عملية دفع من البائع إلى المورد بالكامل.
- **الشرط الثاني:** إذا وصلت البضاعة متأخرة بيوم واحد، فقم بتنفيذ عملية دفع من البائع إلى المورد بنسبة 98٪ من المبلغ الكامل.

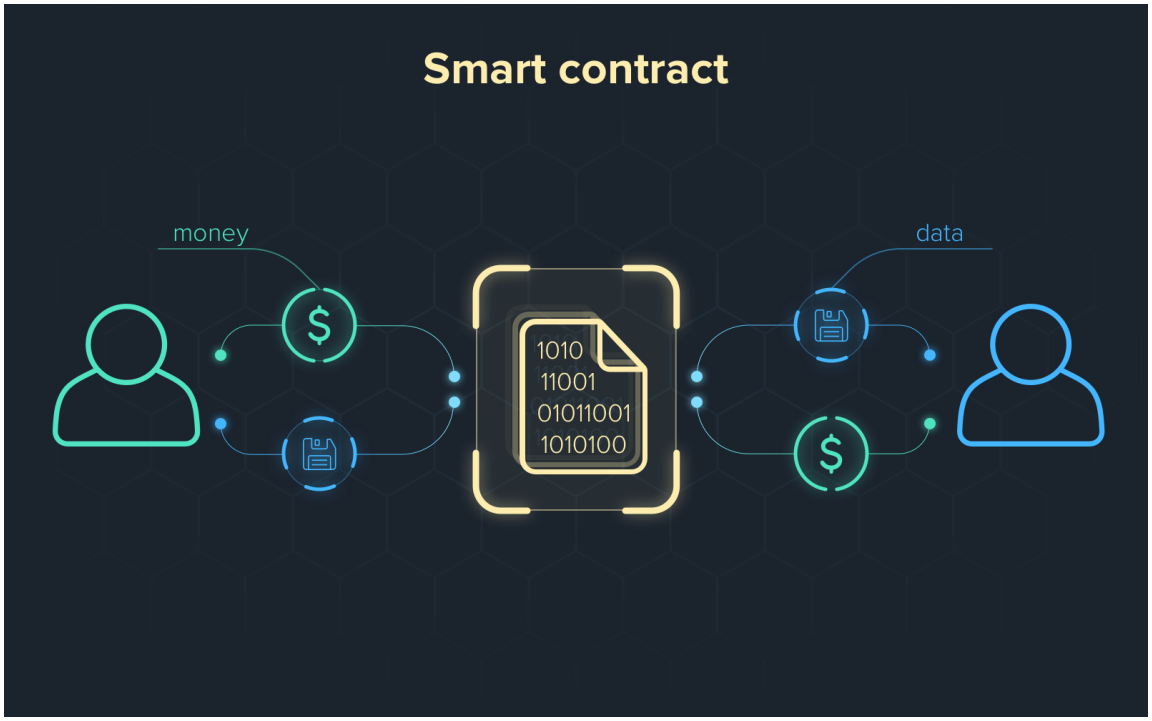
تدعم العقود الذكية الأخرى التطبيقات اللامركزية العامة (dApps) التي يمكن لأي شخص التفاعل معها دون الحاجة إلى أي أذونات. غالبًا ما تكون تطبيقات dApps العامة مفتوحة المصدر بحيث يمكن لأي شخص في العالم فحص كيفية عملها بالضبط قبل اتخاذ قرار بشأن التفاعل معها من عدمه.

من الأمثلة على تطبيق dApp عام سوق إقراض/اقتراض لامركزي، والذي قد يحتوي على الشروط التالية:

- **الشرط الأول:** إذا قام المستخدم بإيداع ضمانات في عقد ذكي معين، فيمكنه الحصول على قرض يصل إلى 50٪ من قيمة ضماناته (على سبيل المثال، إيداع 100 دولار يمكن أن يقترض قرضًا يصل إلى 50 دولارًا).
- **الشرط الثاني:** إذا انخفضت نسبة الضمان للمستخدم (الضمانات / قيمة القرض المستحق) إلى أقل من 200٪، يتم تصفية ضمانات المستخدم تلقائيًا ونقلها إلى المقرضين للتأكد من عدم خسارتهم للأموال.

- **الشرط الثالث:** يمكن للمقرضين إيداع الأموال في عقد محدد يمكن للمستخدمين الآخرين الاقتراض منها بنسب ضمانات محددة مسبقًا، بينما يحصل المقرض على مطالبة بحصة من مدفوعات الفائدة. [19]

7) قابلية تنفيذ العقود الذكية:



صورة رقم 17 العقود الذكية . [14]

بسبب تشغيلها على شبكات البلوك شين، يتم تنفيذ العقود الذكية تلقائيًا كما تمت برمجتها. في سياق التنفيذ، نظريًا لا يمكن لأي طرف مشارك في معاملة عقد ذكي تغيير نتيجتها أو التملص من الشروط المحددة في العقد الذكي.

من الناحية الفعلية، يمكن للعقود الذكية - مع التصميم الصحيح - أن تلغي مخاطر الطرف المقابل، والتي غالبًا ما تُعرف بأنها نسبة المخاطر حين لا يفي الطرف المقابل بالتزاماته. ومع ذلك، للعقود الذكية مخاطر خاصة بها، وهي مخاطر وجود ثغرة أو عيب في كود العقد الذكي يؤدي إلى نتائج غير مرغوبة. تعمل العقود الذكية دائمًا حسب برمجتها، لذا فإذا كان البرنامج معيبًا، فسيقوم العقد الذكي بتشغيل الكود المعيب كما هو. هناك اعتبار رئيسي آخر لقابلية تنفيذ العقود الذكية هو أن بعض العقود ببساطة لا يمكن تنفيذها من خلال الكود. مثال رئيسي على ذلك هو الإقراض - تقدم بروتوكولات DeFi قروضًا بضمانات زائدة بشكل شبه

حصري، حيث يتعين على المقترض وضع أكثر من 100 دولار لاقتراض 100 دولار، لأنه لا توجد طريقة لضمان أن المقرض سيسدد القرض ما لم يكن المبلغ الكامل موجودًا بالفعل في عقد ذكي. في هذه الحالات، يمكن أن يوفر الجمع بين العقود الذكية والأنظمة خارج البلوك شين مثل درجات الائتمان وإثبات الأموال والعقود القانونية آلية أمنية لتخفيف مخاطر الطرف المقابل. [19]

8) فوائد وقيود العقود الذكية

لا شك أن العقود الذكية تقدم للعالم طريقة أكثر أمانا ويمكن التحقق منها لإنشاء اتفاقيات مجتمعية تتضمن نقل الأصول والبيانات. ومع ذلك، لا تزال تقنية البلوك شين والعقود الذكية في مراحلها الأولى، ويجب على المطورين مواجهة مجموعة متنوعة من القيود وهم يتطلعون إلى بناء رؤية جديدة لشبكة الويب قابلة للتحقق.

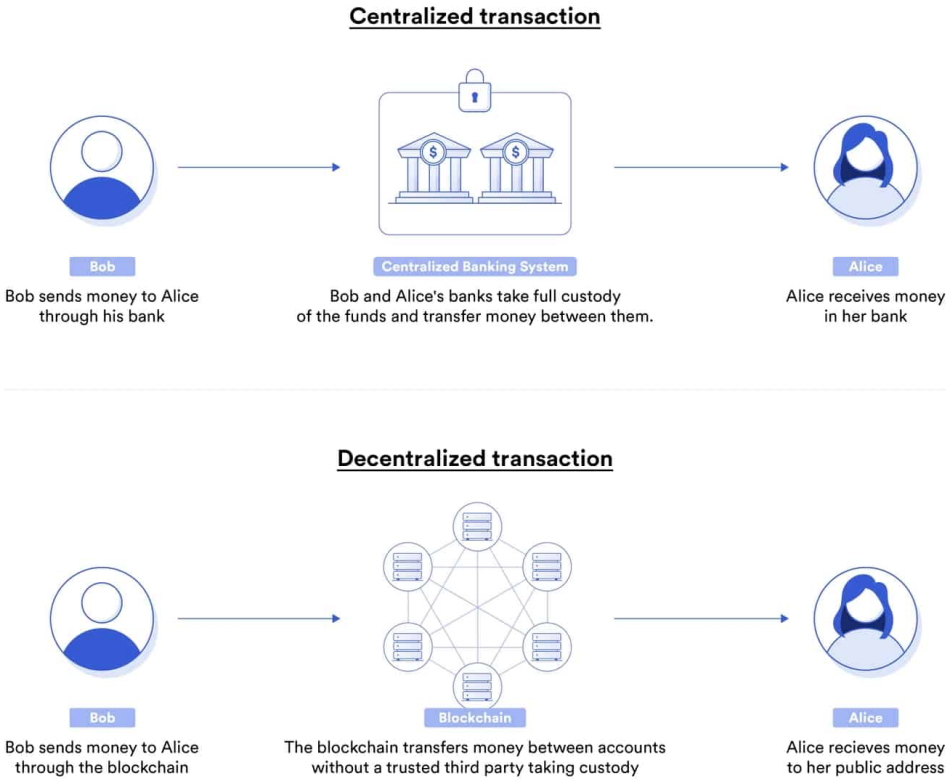
- **فوائد العقود الذكية:**

تتضمن معظم الاتفاقيات الرقمية التقليدية طرفين لا يعرفان بعضهما البعض، مما يؤدي إلى مخاطر عدم التزام أي طرف بالتزاماته. لحل مخاطر الطرف المقابل، غالبًا ما يتم استضافة وتنفيذ الاتفاقيات الرقمية من قبل مؤسسات مركزية أكبر مثل البنك الذي يمكنه فرض شروط العقد. يمكن أن تكون هذه العقود الرقمية مباشرة بين مستخدم وشركة كبيرة ، كما يمكن أن تشتمل على شركة كبيرة تعمل كوسيط موثوق به بين عدة مستخدمين. إشكالية هذه الديناميكية أنها تخلق أيضا وضعا تمارس فيه هذه المؤسسات المركزية نفوذًا غير متماثل على العقود والأشخاص.

تحسن العقود الذكية الاتفاقيات الرقمية من خلال تقديم عدة مزايا:

- **الأمان:** يضمن تشغيل العقد على البنية التحتية اللامركزية للبلوك شين عدم وجود نقطة مركزية للفشل يمكن مهاجمتها، ولا يوجد وسيط مركزي يمكن رشوته، ولا توجد آلية لأي طرف أو مسؤول مركزي لاستخدامها للتلاعب بالنتيجة.
- **الموثوقية:** توفر معالجة البيانات بشكل زائد ومصادقتها من قبل شبكة لامركزية من العقد ضمانات قوية ضد التلاعب، كما تضمن التشغيل المستمر وبأن العقد سيتم تنفيذه في الوقت المحدد وفقًا لشروطه.
- **العادلة:** يقلل استخدام شبكة لامركزية لاستضافة وفرض شروط الاتفاقية من قدرة الوسيط الربحي على استخدام موقعه المتميز لتحقيق مكاسب غير مشروعة واستنزاف القيمة.

- **الكفاءة:** إن أتمتة العمليات الهامشية للاتفاقية (الضمان، والصيانة، والتنفيذ، أو التسوية) تفضي بأنه لا يتعين على أي طرف انتظار إدخال البيانات يدويًا، أو أن يقوم الطرف المقابل بتنفيذ التزاماته، أو أن يقوم وسيط بمعالجة المعاملة. [19]



صورة رقم 18 الفرق في كيفية معالجة أموال المستخدم عند إجراء الدفع من خلال البلوكشين مقابل النظام المصرفي . [15]

- **قيود العقود الذكية:**

سلاسل البلوك شين عبارة عن شبكات معزولة، مما يعني أنها لا تملك اتصالا بالعالم الخارجي .بدون اتصال خارجي، لا يمكن للعقود الذكية التواصل مع أنظمة خارجية لتأكيد ما يحدث في العالم الواقعي ولا يمكنها الوصول إلى موارد حوسبية فعالة من حيث التكلفة .على غرار جهاز كمبيوتر بدون إنترنت، تكون العقود الذكية محدودة للغاية بدون اتصال بالعالم الواقعي .على سبيل المثال، لا يمكنها معرفة سعر أحد الأصول قبل تنفيذ صفقة تداول، ولا يمكنها التحقق من متوسط هطول الأمطار الشهرية قبل صرف مطالبة تأمين المحاصيل، ولا يمكنها التحقق من وصول البضائع قبل التسوية مع المورد.

وعليه، فإن التطور الرئيسي الجاري في صناعة البلوك شين هو العقود الذكية القابلة للبرمجة التي تتصل بالبيانات الواقعية والأنظمة التقليدية خارج البلوك شين، مما يوسع المدخلات والمخرجات المستخدمة في منطق العقد الذكي.

تستخدم هذه العقود الذكية الهجينة شبكة Chainlink وغيرها من شبكات العرافين أو "الأوراكل" دمج الكود داخل البلوك شين بالبنية التحتية خارج البلوك شين - على سبيل المثال، تحريك عقد ذكي باستخدام بيانات خارجية . [19]

9) الايثريوم:

صورة رقم 19 الايثريوم . [16]

الإيثريوم هو نظام بلوك تشين لامركزي مفتوح المصدر يتميز بعملته الرقمية الخاصة إيثريوم (ETH) ، التي تعتبر ثاني أكبر عملة رقمية من حيث القيمة السوقية بعد البيتكوين.

تم إنشاء الإيثريوم على شبكة آمنة تعمل بتكنولوجيا "الند للند"، التي غالبًا ما يشار إليها باسم بلوك تشين الطبقة الأولى. تسمح معاملاتها الشفافة والقابلة للتتبُع للمستخدمين بالعمل بثقة، مما يخلق تجربة سلسة وجديرة بالثقة.

تزايد الطلب على شبكة الإيثريوم بشكل كبير خلال السنين القليلة الماضية، بسبب المزايا والحلول التي تقدمها هذه الشبكة للمستخدمين والمبرمجين، فهي تستفيد من جميع خصائص البلوك تشين التي تعمل عليها، كالعمل بشكل لا مركزي ودون الحاجة لأطراف أخرى، وبمستوى أمان عال جدًا بحيث يكون الاحتيال والتزوير أمرا مستحيلا.

يمكن أيضا للمطورين إنشاء تطبيقات لا مركزية (Dapps) وعملات رمزية (tokens) مستقلة بذاتها من خلال ميزة العقود الذكية (Smart contract) التي تمكن من إنشاء وتسهيل العقود والتعاملات المالية وتنفيذها

بشكل رقمي وموثوق دون الحاجة لطرف آخر لمراقبتها والتحقق منها، الأمر الذي يشكل ركيزة أساسية لعمل التمويل اللامركزي (DeFi) .

علاوة على ذلك، قدم الإيثريوم لغة برمجة تُعرف باسم Solidity ، وتُستخدم هذه اللغة لكتابة العقود الذكية على الشبكة، مما يسمح بإنشاء التطبيقات اللامركزية والعملات الرمزية بكل سهولة.

تم إنشاء الإيثريوم، كاستجابة لنقاط ضعف بلوك شين البيتكوين. تم نشر الورقة البيضاء الخاصة بإيثريوم في عام 2013 من قبل فيتاليك بوتيرين، أحد مؤسسي إيثريوم. في عام 2014، تم طرح عملة "إيثر" للبيع، حيث تمكنت الأطراف المهتمة بالعملةِ من شرائها باستخدام بيتكوين.

في يوليو 2015، تم إطلاق نسخة مصغرة من مشروع إيثريوم، مع تشجيع المطورين والمعدّنين لبدء العمل على الشبكة. تم رفع جميع القيود في وقت لاحق من هذا العام وتحديد رسوم الغاز الافتراضية .

شهدت إيثريوم منذ إنشائها، العديد من عمليات الانقسام (فورك). توفر هذه الانقسامات بعض الفوائد للشبكة، وأحيانًا كرد على الهجمات الضارة. على سبيل المثال، في عام 2017، خفضت Byzantium Fork مكافآت تعدين الكتل وأضافت طرقًا إضافية للتشفير للسماح بقابلية تطوير إضافية.

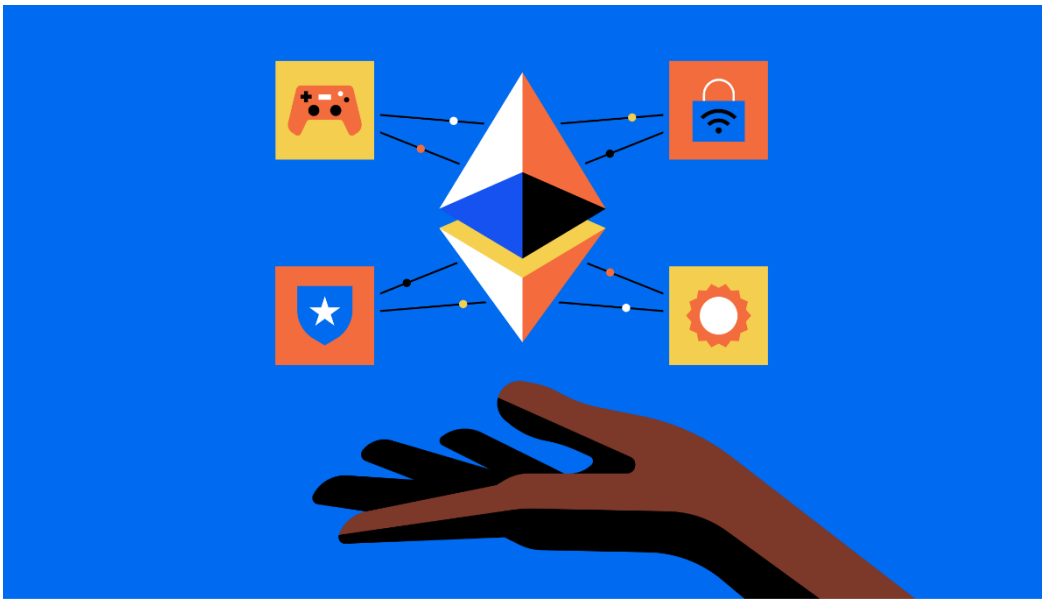
- **<u>عملية الدمج:</u>**

استخدمت إيثريوم آلية إجماع إثبات العمل (PoW) عند إطلاقها، والتي تستخدم قوة حسابية مكثفة لحل المشكلات الرياضية المعقدة لتحديد من سيتحقق من صحة الكتلة التالية من المعاملات. هذه الآلية تستهلك كميات كبيرة من الطاقة.

عملية الدمج كانت بمثابة الانتقال من آلية إثبات العمل إلى إثبات الحصة(PoS) ، وهي آلية إجماع تتضمن قيام حاملي إيثر برهن عملاتِهم كأداة ضمان للتحقق من صحة الكتل على بلوك شين. يتم اختيار المدققين بشكل عشوائي، مما يقلل من الحاجة إلى المنافسة والاستخدام المفرط للطاقة.

تضمنت عملية الدمج جمع طبقتين مختلفتين: الطبقة الأصلية، أي طبقة إثبات العمل، وسلسلة المنارة "Beacon Chain"، أي طبقة إثبات الحصة الجديدة. وقد أدت هذه الخطوة إلى جعل شبكة إيثريوم أكثر قابلية للتطوير وأكثر أمانًا واستدامةً.

- **مزايا الإيثريوم:**



صورة رقم 20 الايثريوم . [17]

يميز الإيثريوم نفسه عن منصات بلوك شين الأخرى بالكثير من الخصائص، وخاصة البيتكوين، من خلال تطبيقاتها الواسعة لتقنية البلوك شين. في حين تم تصميم بيتكوين بشكل أساسي كعملة رقمية لامركزية، **فإن بلوك شين الإيثريوم يستطيع استضافة مجموعة كبيرة من الحلول والتطبيقات على غرار:**

- **إنشاء العملات والأصول المالية:** تتيح إيثريوم تطوير العملات الرمزية الجديدة مباشرة على شبكة بلوكتشين الخاصة بها.
- **ملكية الأصول المادية الأساسية:** تسمح منصة إيثريوم بالحصول على الملكية الرقمية للأصول المادية.
- **تطوير الأصول غير القابلة للاستبدال:** تمكن منصة إيثريوم من إنشاء أصول فريدة معروفة باسم"NFTs" ، والتي تمثل عنصرًا فريدًا أو جزءًا من المحتوى.
- **تنفيذ العقود الذكية:** تم تصميم بلوك شين إيثريوم لتسهيل عمل العقود الذكية. هذه عقود قابلة للبرمجة وذاتية التنفيذ مع كتابة الشروط مباشرة في التعليمات البرمجية.
- **المشاركة مع المنظمات المستقلة اللامركزية (DAOs):** تسمح إيثريوم بإنشاء منظمات DAOs، وهي منظمات تحكمها قواعد مبرمجة تحددها العقود الذكية، وتقدم شكلاً جديدًا من الحوكمة اللامركزية.

كان الإيثريوم عنصرا رئيسيا في ثورة التمويل اللامركزي"DeFi " ، حيث يمكنها التعامل مع المعاملات المالية المعقدة التي، حتى وقت قريب، لم يكن من الممكن معالجتها إلا من قبل المؤسسات المالية. وتسمح منصة إيثريوم أيضًا ببناء سلاسل الطبقة الثانية، مما يساعد على إنشاء العملات الرمزية (توكنز) المتنوعة وغيرها من الأصول الرقمية الأخرى، ما يجعلها منصة رائدة في توسيع نطاق استخدام بلوكتشين وحلول التمويل اللامركزي والحوكمة. [22]

V. خاتمة:

في هذا الفصل، غطينا مفاهيم وتقنيات البلوك شين الأساسية، بدءًا من التعريفات الأساسية وخصائصها وصولا إلى آليات التوافق المختلفة. ثم قمنا بشرح مفهوم العقود الذكية، آلية عملها ، وعلاقتها بالبلوك شين، مع تقديم أمثلة توضيحية. كما ناقشنا قابلية تنفيذ العقود الذكية وفوائدها وقيودها. وأخيرًا، اختتمنا الفصل باستعراض بلوك شين الإيثريوم وميزاته الفريدة.

في الفصل التالي، سننتقل إلى عرض تصميم وتطوير مشروعنا، موضحين الخطوات والمراحل التي قمنا بها، والبرامج والأدوات التي استخدمناها، بالإضافة إلى تقديم عرض عملي للموقع الإلكتروني.

الفصل الثالث:
تصميم وتنفيذ نظام التصويت المقترح

I. مقدمة:

في هذا الفصل سنعمل على شرح وتبسيط مرحلة تصميم وتنفيذ نظام التصويت الذي قدمناه والمبني باستخدام بلوك شين الايثيريوم، ويهدف مشروعنا إلى تعزيز أمان وشفافية العملية الانتخابية. إضافة إلى تقليل التكلفة وزيادة الوصولية ومشاركة المواطنين، والحفاظ على خصوصية الناخبين، إلى جانب القضاء على التزوير ، بحيث يكون من الصعب جدا تغيير أو التلاعب في الأصوات بعد تسجيلها على الشبكة، مما يضمن أن نتائج الانتخابات تعبر عن إرادة الناخبين .

II. الأدوات المستخدمة:

1) Visual Studio Code:

يعتبر visual studio code من البرامج المجانية والمفتوحة المصدر، والتي يمكن تنزيلها على مختلف أنظمة التشغيل. كما يمكن أن تجده باسم VS Code وهو بيئة عمل و محرر أكواد (IDE AND Code Editor) تم تصميمه من طرف شركة Microsoft [23].

كما تم إصدار النسخة الأولى منه في 29 أبريل من عام 2015، وقد تم ترخيصه بوساطة شركة MIT. وهي شركة تراخيص برمجية عالمية. إضافة لذلك تم وضع الكود الخاص بالبرنامج على موقع GitHub.

صورة رقم 21 شعار Visual Studio Code.

2) Truffle:

هو المكون الأساسي لمجموعة Truffle Suite ، ويعمل كإطار تطوير شامل لتطبيقات Ethereum اللامركزية(dApps) . يوفر Truffle للمطورين أدوات تشمل مترجم العقود الذكية، والاختبار الآلي، ونصوص النشر. باستخدام Truffle، يمكن للمطورين كتابة وإدارة العقود الذكية بكفاءة باستخدام لغة البرمجة Solidity. يعمل Truffle على تبسيط عملية التطوير من خلال تقديم ميزات مثل ترحيل العقود وإدارة الشبكة والتصحيح.

كما يتكامل Truffle مع إطارات الاختبار الشائعة ويسمح للمطورين بمحاكاة سيناريوهات واقعية، مما يضمن موثوقية وأمان عقودهم الذكية قبل النشر. [24]

صورة رقم 1 شعار Truffle.

3) Ganache:

عبارة عن بلوك شين شخصي تم تطويره كجزء من مجموعة Truffle Suite . يوفر شبكة Ethereum محلية للمطورين لاختبار تطبيقاتهم اللامركزية (dApps) في بيئة محصورة.

يسمح Ganache للمطورين بإنشاء وإدارة الحسابات، ومحاكاة المعاملات، وفحص نشاط البلوك شين، وكل ذلك ضمن واجهة سهلة الاستخدام. إنه يلغي الحاجة إلى الاتصال بالشبكة الرئيسية Ethereum أو شبكات الاختبار أثناء التطوير، مما يسمح بتكرار أسرع وقدرات تصحيح أفضل. [24]

صورة رقم 23 شعار Ganache.

4) محفظة MetaMask:

ميتا ماسك (MetaMask) عبارة عن محفظة عملات مشفرة وأيضاً ملحق متصفح ويب، يستخدم لحفظ وتلقي إيثريوم و .ERC20بعبارة أخرى، تسمح للمستخدمين بإجراء معاملات إيثريوم من خلال المواقع الإلكترونية العادية. يُمكن استخدام ميتا ماسك (MetaMask) لحفظ مفاتيح العملات المشفرة لإيثريوم فقط [31].

صورة رقم 24 شعار Metamask.

III. اللغات المستخدمة:

1) HTML:

HTML هي اختصار لـ **Hypertext Markup Language**، وهي لغة ترميز تُستخدم لبناء صفحات الويب. تعتمد **HTML** على مجموعة من العلامات (**tags**) التي توفر هيكلًا للصفحة وتحدد كيفية عرض المحتوى. تسمح **HTML** بتضمين النصوص والصور والروابط والوسائط الأخرى داخل صفحات الويب. تُستخدم هذه العلامات لتنظيم المحتوى وتقديمه بشكل منظم للمستخدمين عبر المتصفحات[**25**].

صورة رقم 25 شعار HTML.

2) CSS:

CSS هو اختصار لـ **Cascading Style Sheets**، وهو لغة تنسيق تستخدم لتحديد الشكل (التنسيق والتصميم) لصفحات الويب التي تم كتابتها بلغة **HTML**. تسمح **CSS** بتغيير الألوان والخطوط والهوامش والتسليط على الصور والعديد من الخصائص الأخرى للعناصر على صفحة الويب، مما يتيح للمطورين تخصيص مظهر صفحاتهم وتحسين تجربة المستخدم[**26**].

صورة رقم 26 شعار CSS.

3) JavaScript:

هو لغة برمجة عالية المستوى وديناميكية تستخدم في تطوير تطبيقات الويب وتحسين تفاعل المستخدم مع صفحات الويب. تُستخدم JavaScript عادةً في الجانب العميل (client-side) من تطبيقات الويب لإضافة تأثيرات ديناميكية وتفاعلية، مثل تغيير محتوى الصفحة بدون إعادة تحميلها، والتحقق من مدخلات المستخدم، وإنشاء تأثيرات الرسوم المتحركة، وغيرها الكثير[27].

صورة رقم 27 شعار JavaScript.

4) Solidity:

صورة رقم 28 شعار Solidity.

سوليديتي (**Solidity**) هي لغة برمجة تُستخدم أساسًا لتطوير عقود ذكية على منصة الإيثريوم (**Ethereum**). تم تطوير سوليديتي خصيصًا لدعم تطوير العقود الذكية (Smart Contracts) التي تعمل على بلوك تشين الخاص بشبكة الإيثريوم.

5) Bootstrap:

صورة رقم 29 شعار Bootstrap.

Bootstrap هو إطار عمل (**Framework**) لتطوير الويب (**Web Development**) مفتوح المصدر، والذي يستخدم لبناء تطبيقات الويب بسرعة وسهولة. يوفر **Bootstrap** مجموعة من الأدوات والقوالب والأنماط المسبقة التي تساعد على تصميم وتنسيق المواقع بشكل سريع ومتجاوب مع مختلف الأجهزة. تم تطوير **Bootstrap** من قبل تويتر وأصبح مشهورًا بسبب سهولة استخدامه وقابليته للتخصيص [**28**].

IV. تخطيط المشروع:

I. لغة UML:

لغة النمذجة الموحدة **UML(Unified Modeling Language)** ، تستخدم في عمل التخطيط لمشاريع البرمجة قبل البدء في عمل المشروع البرمجي عمليًا مكوناتها مجموعة من المخططات تستعمل رموزا هندسية - كل رمز من الرموز يرمز إلى شيء في المشروع البرمجي - [29].

تُعرَّف على أنها لغة نمذجة رسومية ونصية تهدف إلى فهم وتعريف الاحتياجات، وتحديد وتوثيق الأنظمة، ورسم هياكل البرمجيات، وتصميم الحلول وإيصال الآراء. نماذج **UML**هي جميع البيانات والمعالجات مطورة ومنظمة في مخططات مختلفة[30].

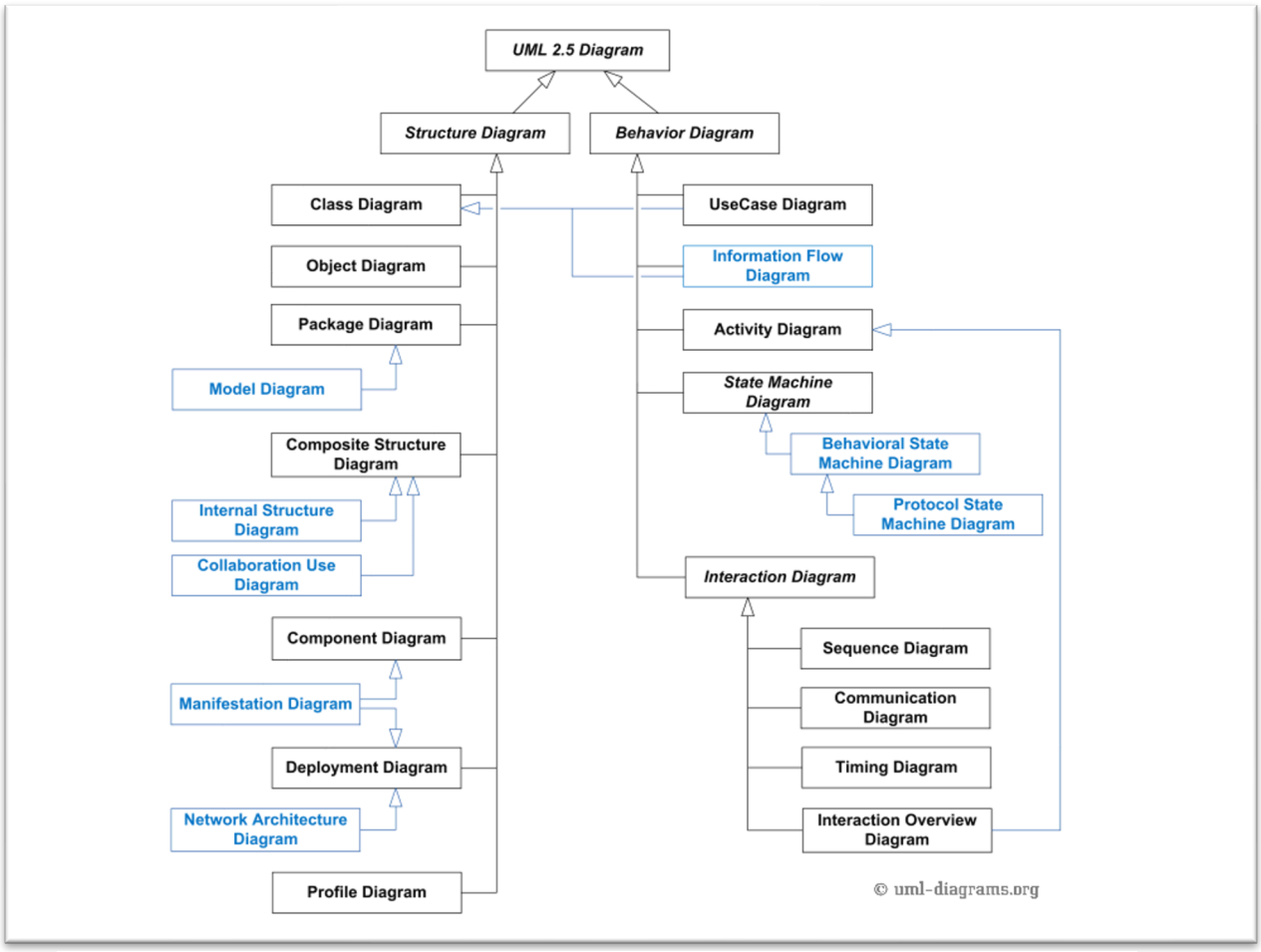
II. أنواع لغة UML:

تُستخدم لغة UMLلعمل نموذج مبدئي للتطبيق أو النظام سهل الفهم و مقروء من قبل المطورين أو المُبرمجين لذلك سُميت لغة النمذجة المُوحدة هناك عدة أنواع من المخططات التي تعتمد عليها UML يُمكن حصرها في نوعين:

1) **Structural Diagrams**

2) **Behavioral Diagrams**

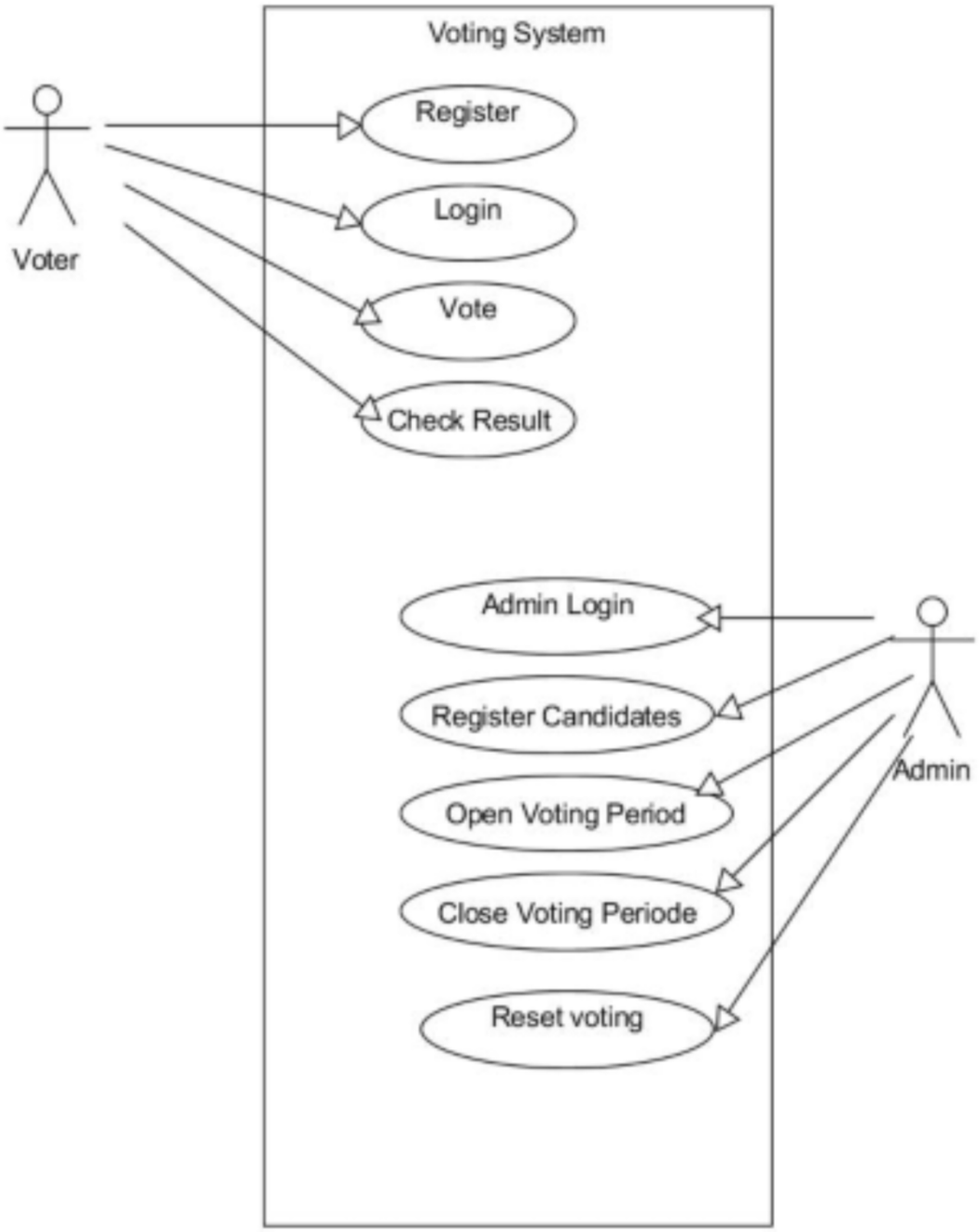
و تحت كل نوع يندرج عدة أنواع من المُخططات:



صورة رقم 30 نماذج - UML.

1) مخطط حالة الاستخدام use case diagram:

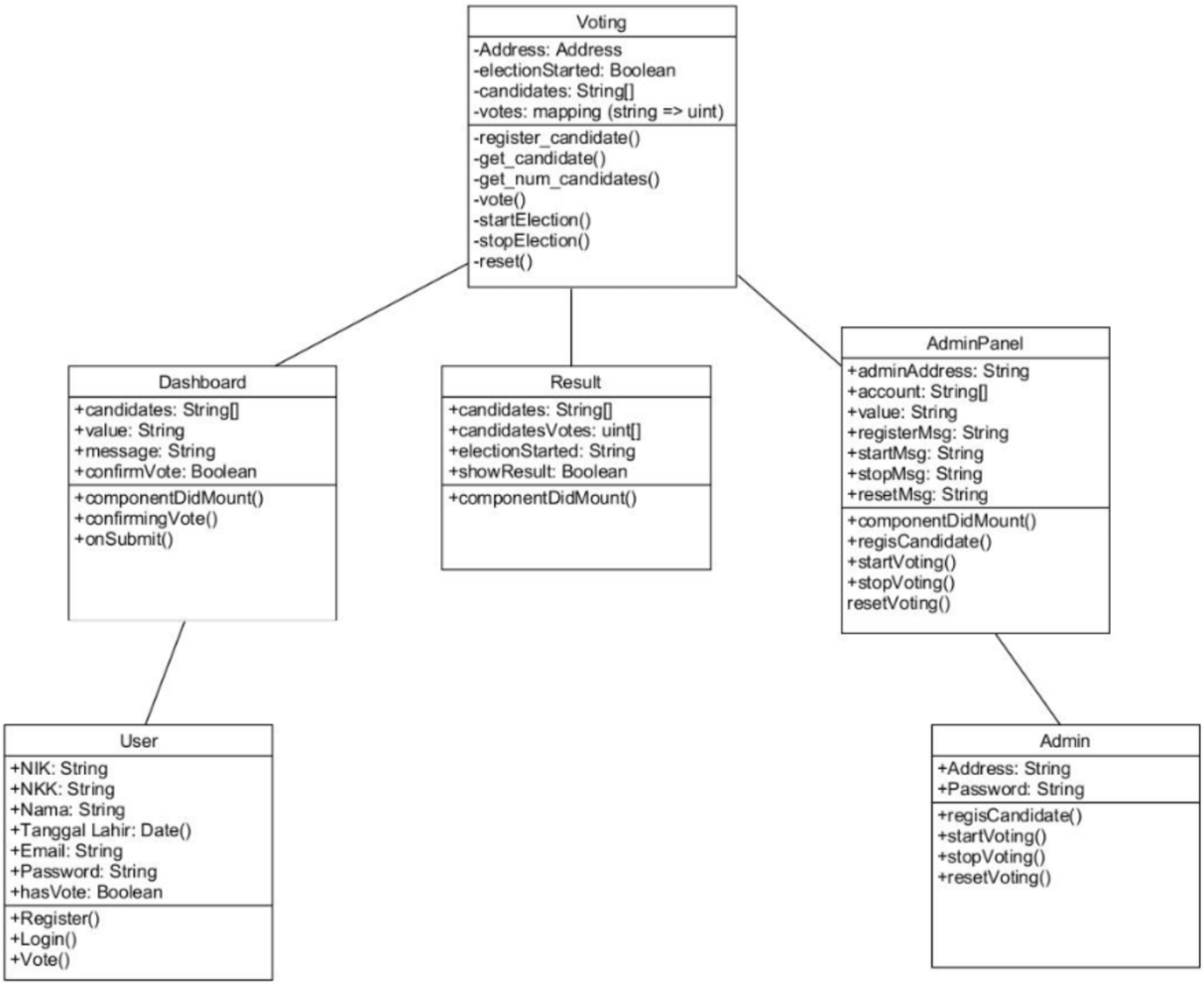
يصف الوظائف الرفيعة المستوى ونطاق النظام. يحدد هذه المخطط التفاعلات بين النظام والجهات الفاعلة فيه. يُظهر المخطط كيفية استخدام المستخدمين للنظام أو التطبيق من خلال عرض مجموعة من حالات الاستخدام (Use Cases) والعلاقات بينها. ، ولكن ليس كيفية عمل النظام داخليًا. [29].



صورة رقم 31 مخطط حالة الاستخدام.

2) **مخطط الفئة class diagram**:

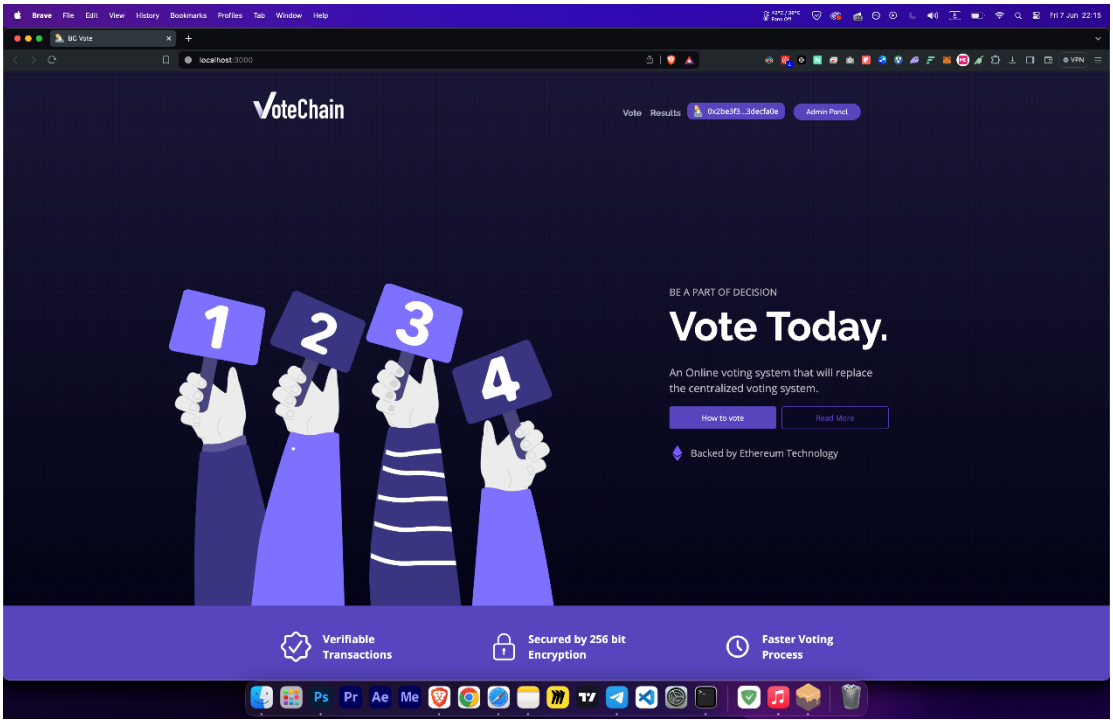
مخطط الفئات (classes) هو جزءٌ مهمٌ جدًا من لغة النمذجة الموحدة UML، وهو مخطط هيكلي مهمته عرض الفئات بنظامٍ معيّن مع جميع العلاقات التي تربط بينها، وهو -برأيي- أشهر نوع من المخططات في هندسة البرمجيات. [27]



صورة رقم 32 مخطط الفئة.

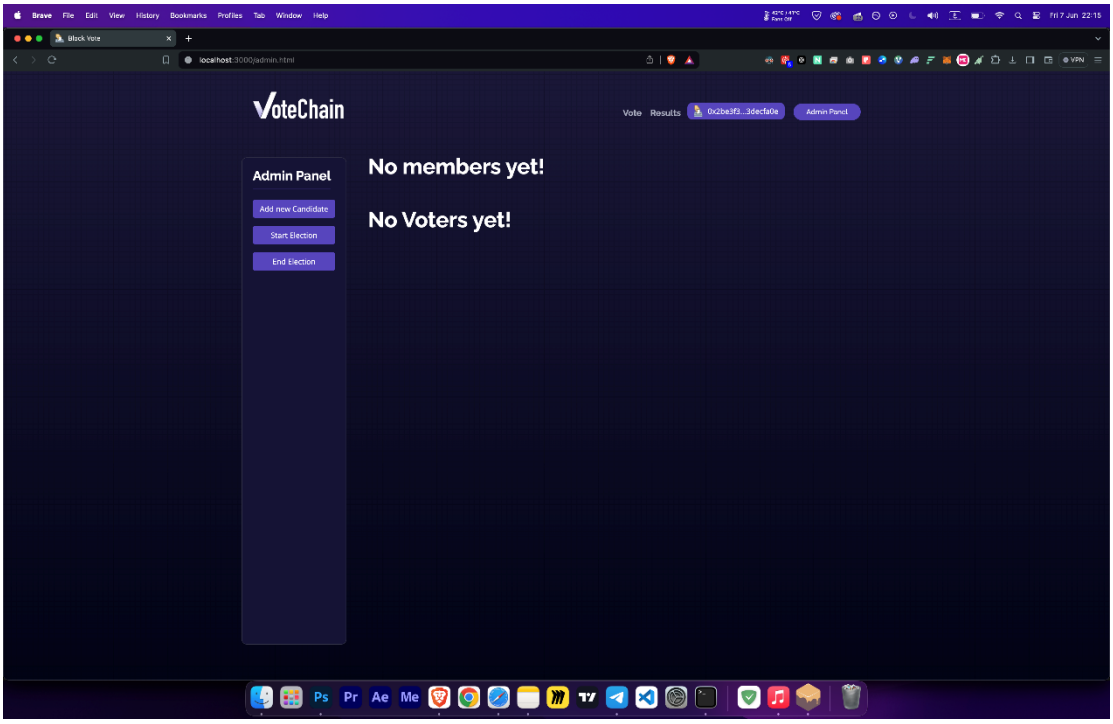
٧. عرض واجهات الموقع:

- **الواجهة الرئيسية:** أول واجهة لكل من مشرف التصويت والناخب يمكن من خلالها ربط محفظة الميتا ماسك وتسجيل الدخول، أو الدخول للوحة تحكم الأدمن بالنسبة للمشرف، تحوي الصفحة الرئيسية أيضا صفحة تعريفية بكيفية التصويت، وصفحة أخرى لشرح



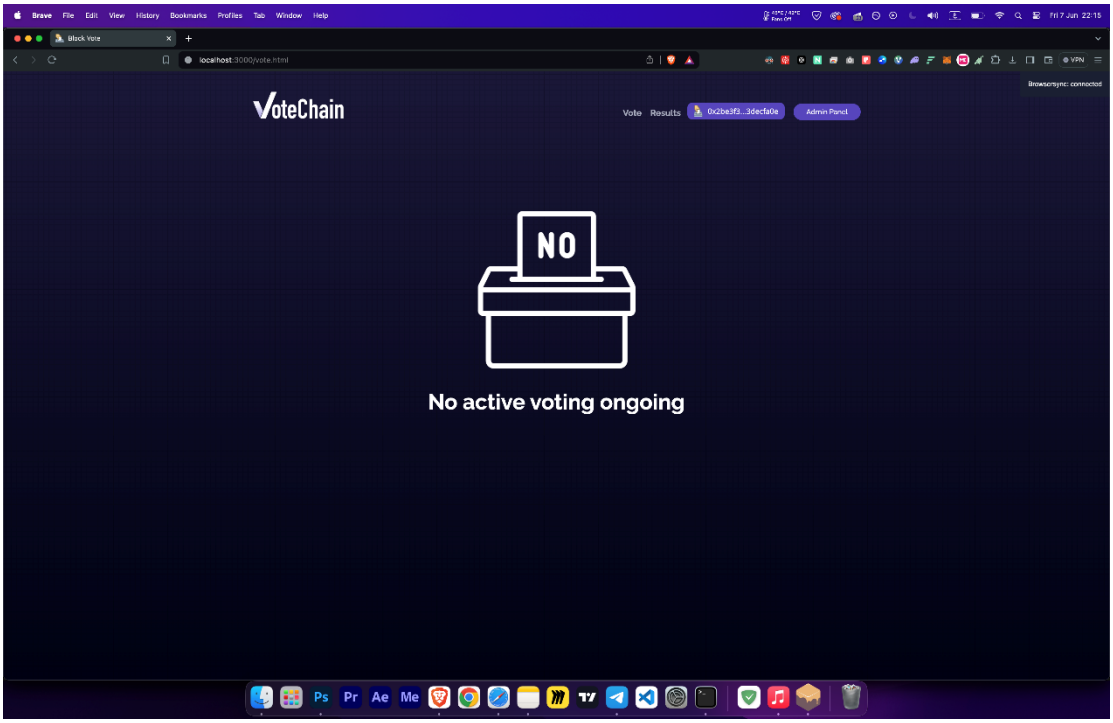
صورة رقم 31 الواجهة الرئيسية.

- **لوحة التحكم:** منها يمكن للمشرف عن التصويت أن يقوم بإضافة المترشحين وبدأ العملية الانتخابية والانتهاء منها.



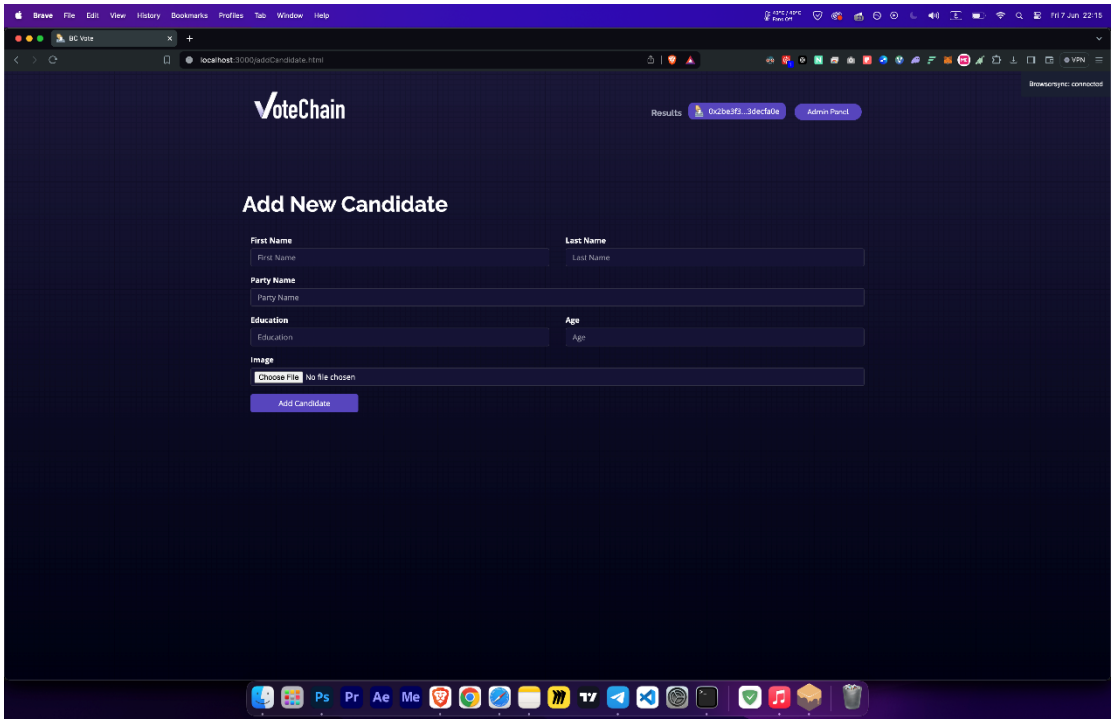
صورة رقم 32 لوحة التحكم.

- **واجهة التصويت:** الصفحة التي يتم اختيار المترشحين منها "الصفحة قبل بدأ الانتخابات".

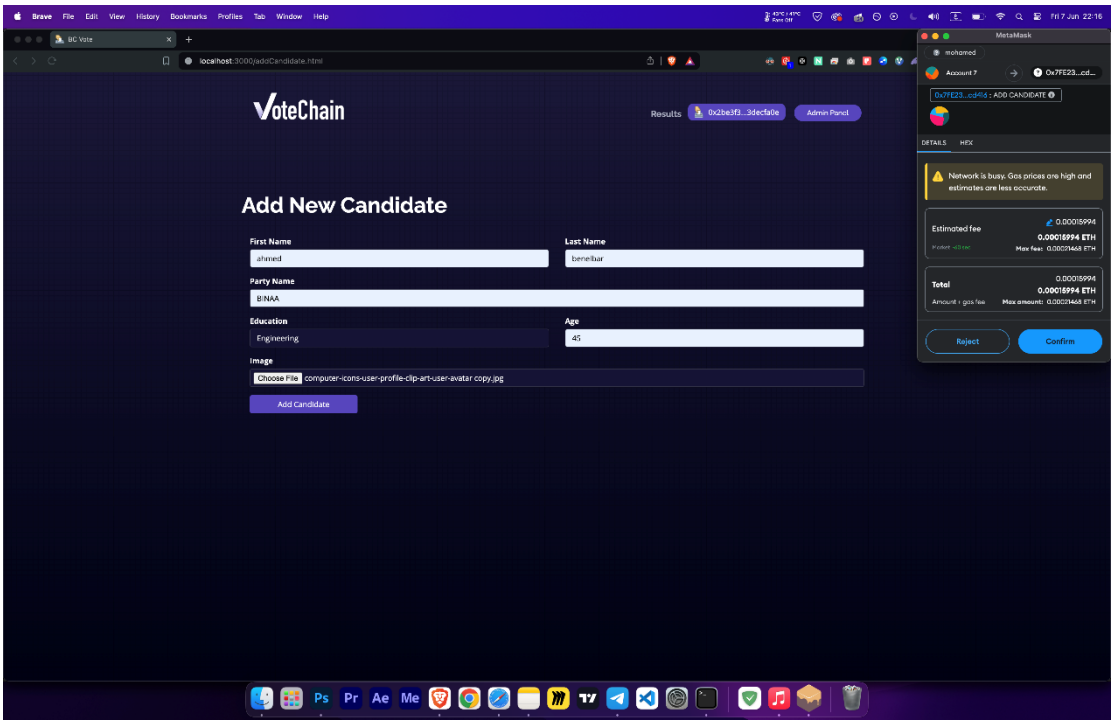


صورة رقم 33 صفحة التصويت.

- **واجهة إضافة المترشحين:** يتم إضافة معلومات مترشحي الانتخابات بما في ذلك القائمة الانتخابية والمستوى التعليمي والمعلومات الشخصية، ثم التوقيع على العقد الذكي لتأكيد إضافة المترشح.

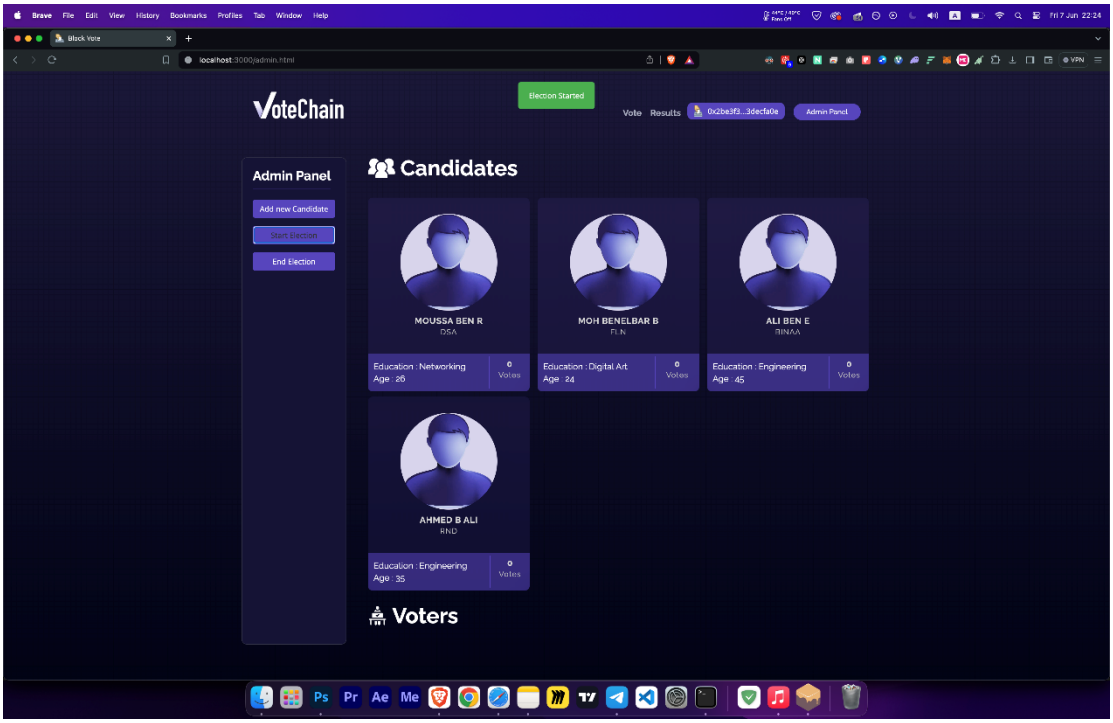


صورة رقم 34 صفحة إضافة المترحشين.



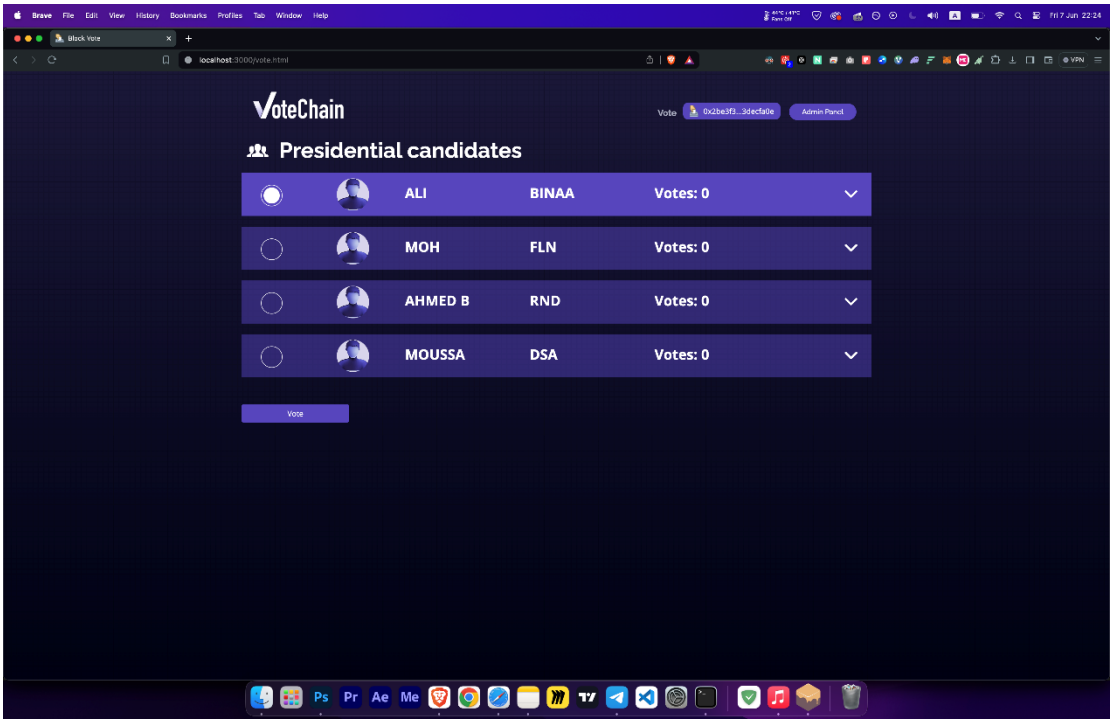
صورة رقم 35 التوقيع على العقد الذكي.

- **بدأ عملية التصويت:** بعد الانتهاء من إضافة المترشحين يقوم المشرف بإطلاق العملية الانتخابية من لوحة التحكم .



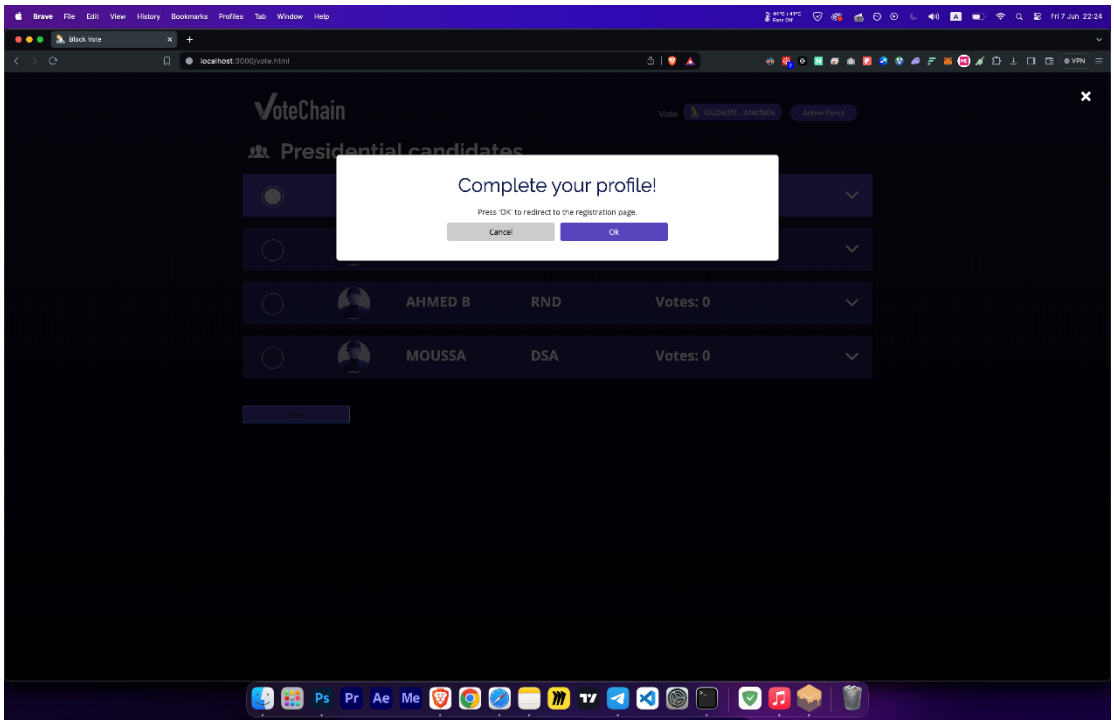
صورة رقم 36 بداية عملية التصويت.

- **واجهة التصويت:** يقوم الناخب باختيار المترشح الذي يلبي تطلعاته للتصويت عليه .

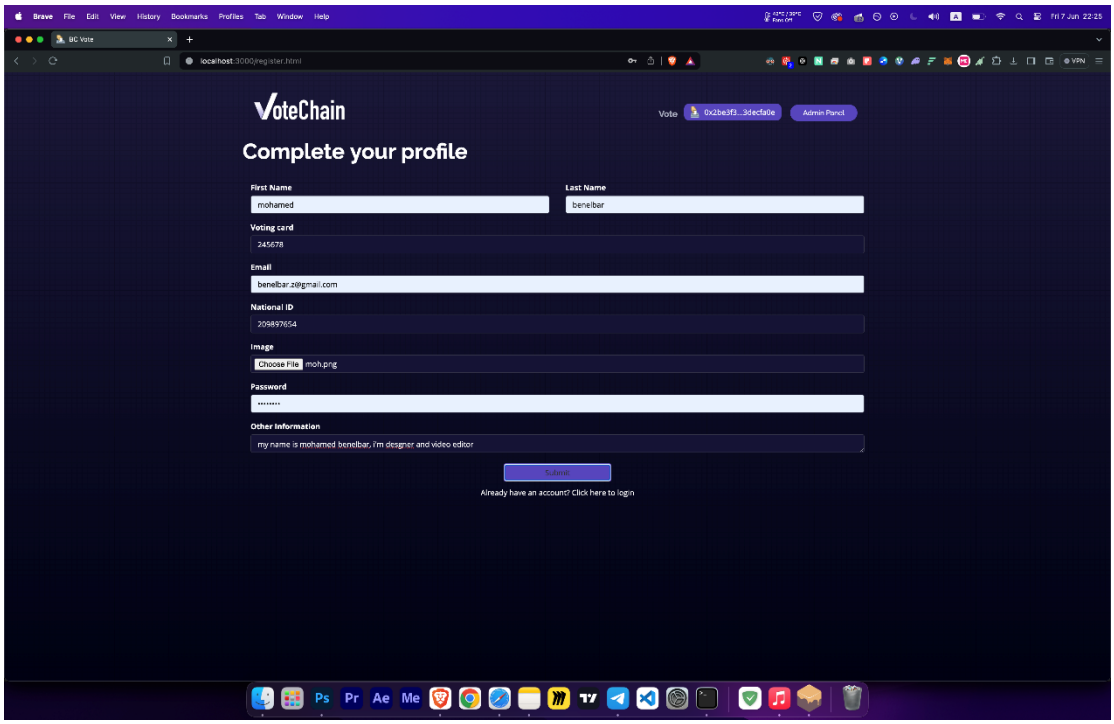


صورة رقم 37 واجهة التصويت.

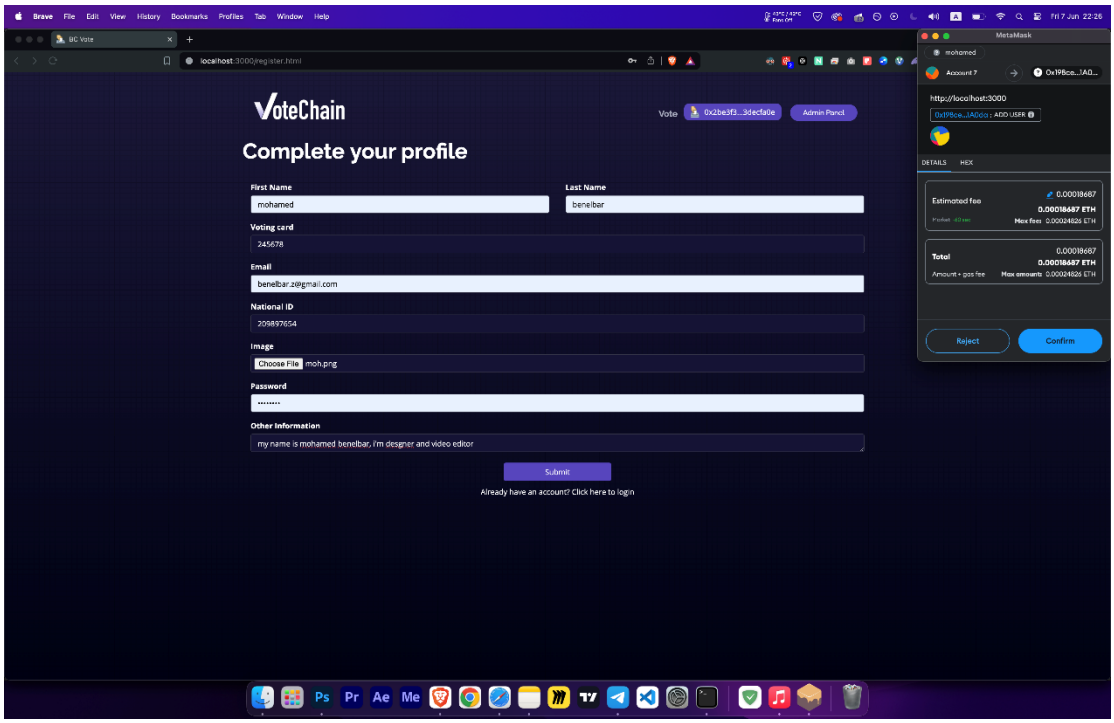
- **إكمال معلومات الناخب:** يطلب من الناخب إكمال معلوماته الشخصية قبل التصويت وذلك لاحتفاظ بها كهيئة ناخبة.



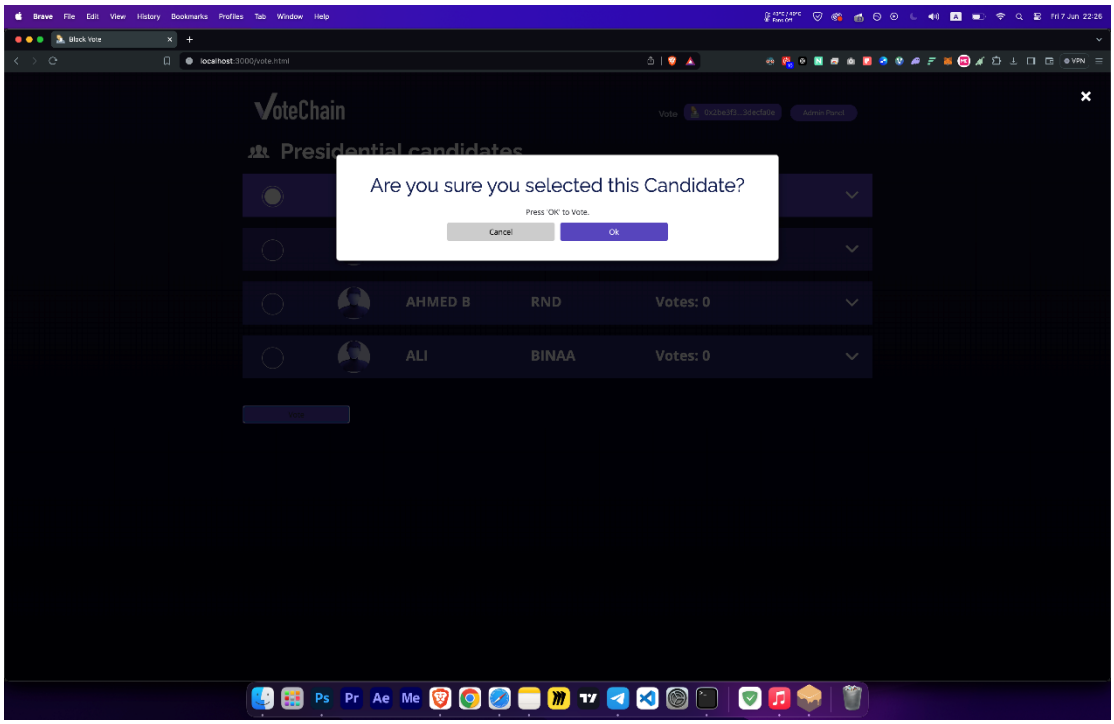
صورة رقم 38 إكمال ملف الناخب.



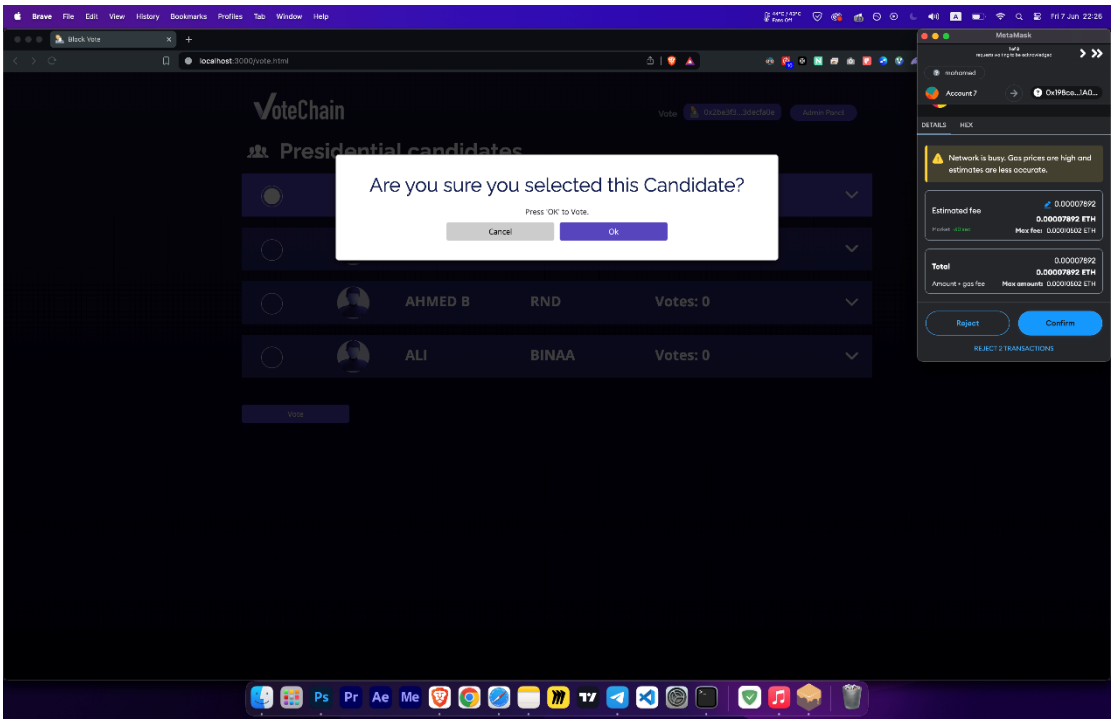
صورة رقم 39 ملئ معلومات الناخب.



صورة رقم 40 التوقيع على العقد الذكي بعد ملء المعلومات.

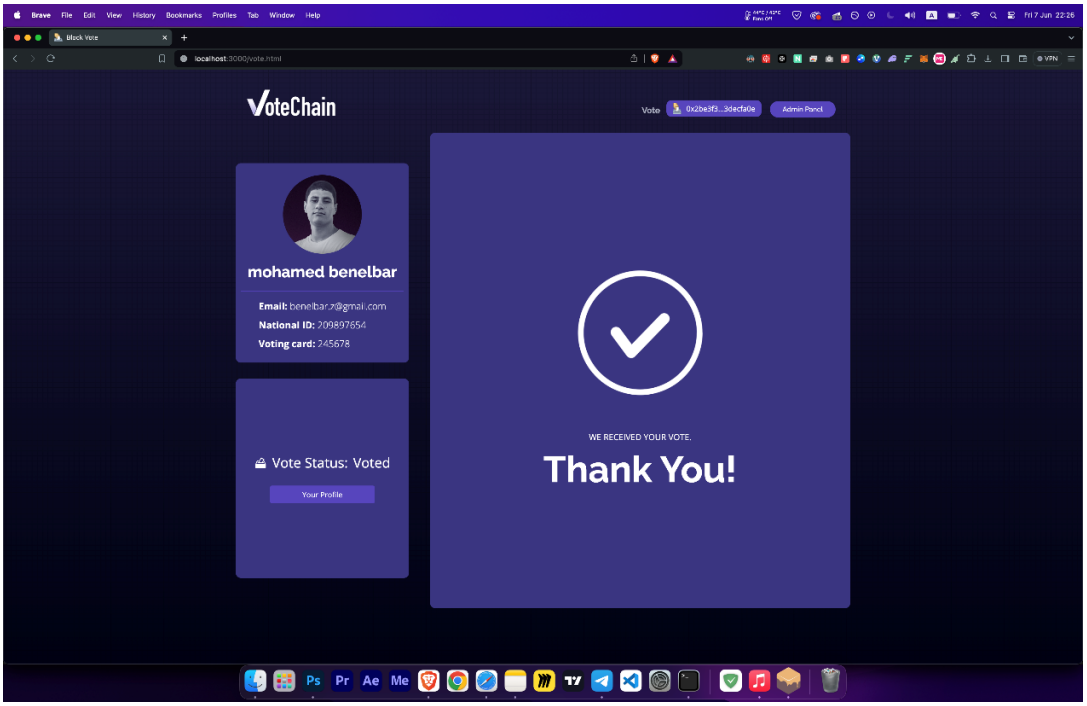


صورة رقم 41 التأكيد على اختيار المترشح المناسب.



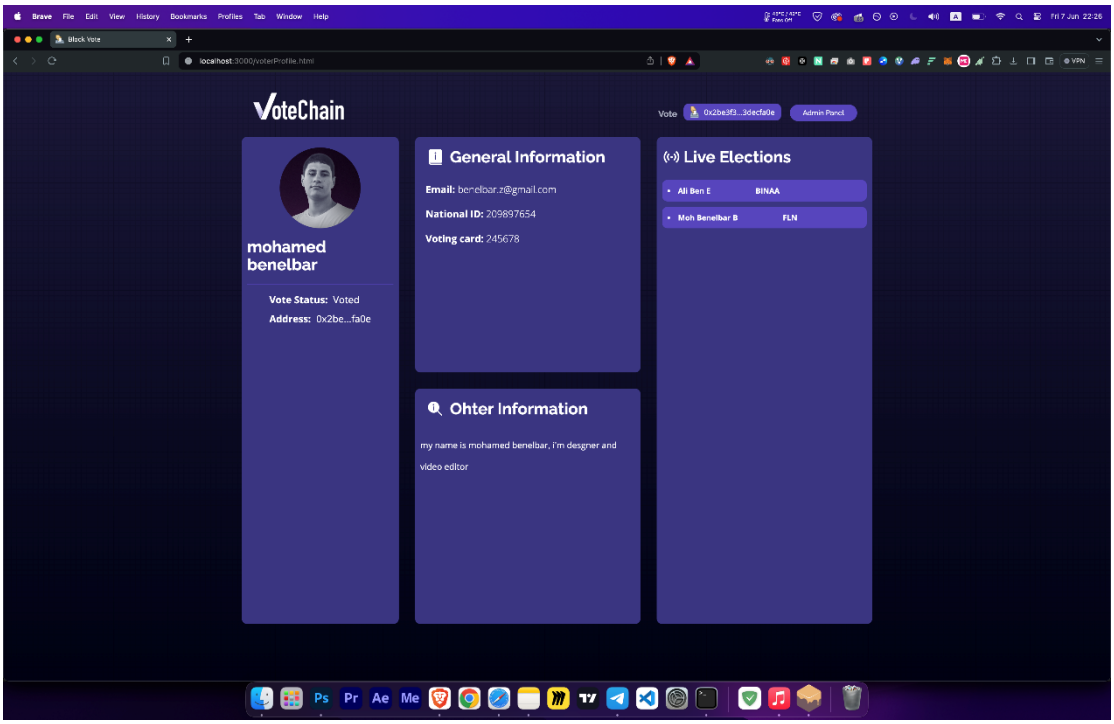
صورة رقم 42 إتمام عملية التصويت.

- **واجهة إتمام التصويت:** بعد إتمام التصويت واختيار المترشح المناسب يتم تسجيل الصوت على شبكة البلوك شين المحلية، ولا يمكن التصويت لمرة ثانية.



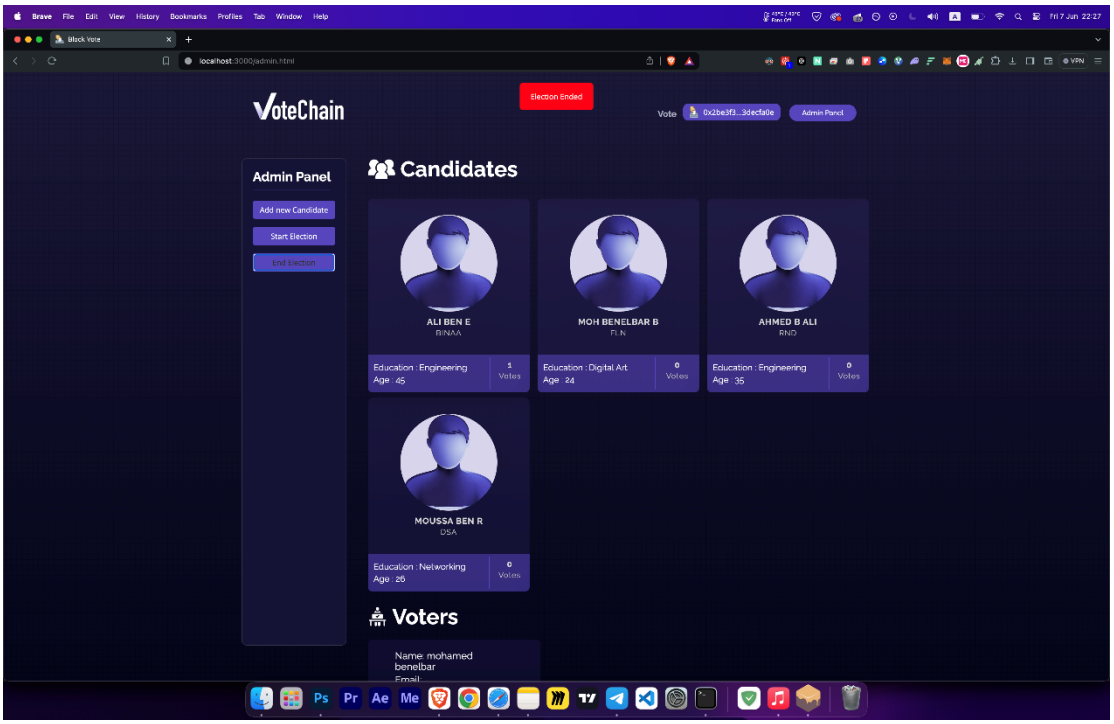
صورة رقم 43 واجهة إتمام التصويت.

- **واجهة حساب المصوت:** يمكن المصوت الدخول لحسابه الشخصي ويحوي معلوماته الشخصية وحالته الانتخابية إن كان قد صوت أم لا.



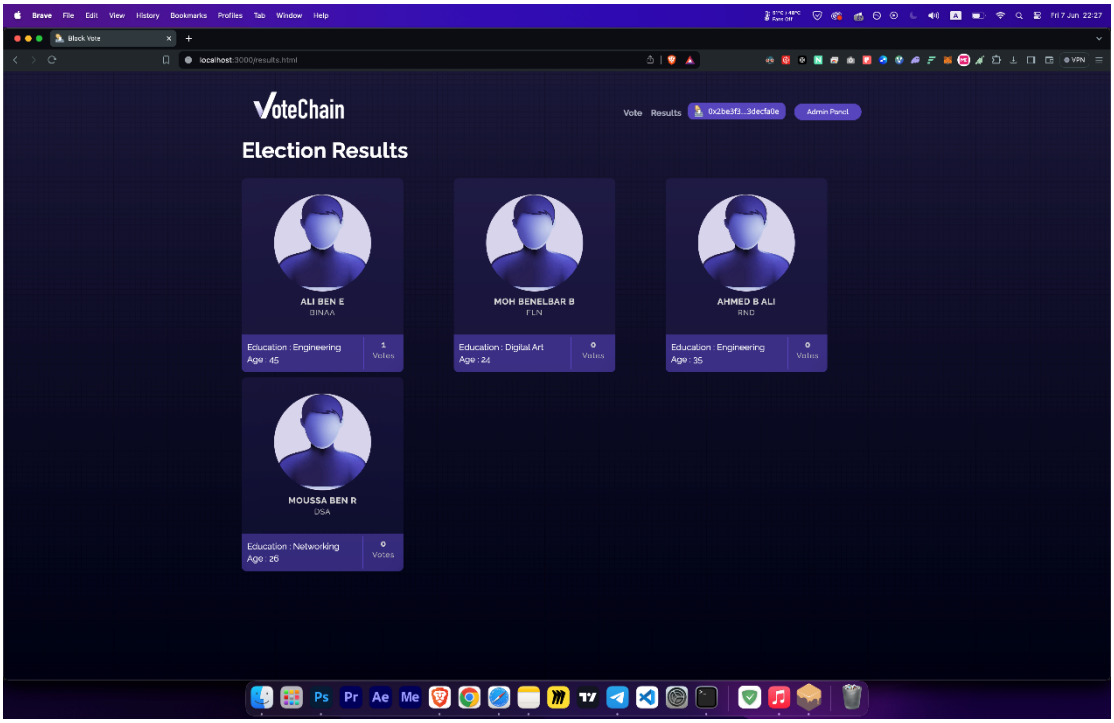
صورة رقم 44 واجهة حساب المصوت.

- **إنهاء عملية التصويت:** بعد انتهاء عملية التصويت، يقوم المشرف بإغلاق صفحة التصويت لعرض النتائج.



صورة رقم 45 إنهاء عملية التصويت.

- **واجهة النتائج:** عرض صفحة النتائج بعد إغلاق عملية التصويت.



صورة رقم 46 واجهة النتائج.

VI. الخاتمة:

في ختام عملنا، تناولنا الأدوات ولغات البرمجة التي استخدمناها لبناء الموقع، مع عرض وشرح للواجهات التي تم إنجازها. كما قدمنا شرحًا موجزًا لكود المصدر للمشروع.

الخاتمة:

مشروعنا هو تصميم وتنفيذ تطبيق ويب للتصويت الالكتروني مبني باستخدام بلوك شين الايثريوم، الهدف منه تعزيز الأمان والشفافية وحماية خصوصية الناخبين وإضفاء النزاهة والمصداقية على العملية الانتخابية، مما يضمن أن نتائج الانتخابات تعبر بدقة عن إرادتهم. ومن أبرز الأهداف التي حققها المشروع:

- تعزيز الأمان والشفافية حيث يسجل كل صوت بشكل مشفر وغير قابل للتغيير.
- إضفاء النزاهة والمصداقية على العملية الانتخابية بحيث يمكن للناخبين التحقق من أن أصواتهم تم تسجيلها بشكل صحيح دون الكشف عن هويتهم.

أما الأهداف التي لم نستطع تحقيقها فهي:

- إعداد هيئة ناخبة ضخمة واستخدمها في التصويت.
- ربط المشروع بآليات موجودة على أرض الواقع، تتعلق بالعملية الانتخابية.

سمح لنا هذا العمل بمعرفة الكثير عن التطوير في شبكات البلوك شين، كما تعلمنا التعامل مع مجموعة متنوعة من الأدوات وبعض لغات البرمجة مثل solidity كانت هذه فرصة لنا لاستكمال مهارات الكمبيوتر لدينا وتوسيع وتعميق معرفتنا وتقدير الحقائق المختلفة للمجال.

الملخص:

في عالمنا الرقمي، باتت مواقع الويب أدوات أساسية لا غنى عنها، فهي تفتح آفاقًا واسعة وتُسهل علينا جوانب متعددة من حياتنا. ولذلك، أصبحت عملية تطوير هذه المواقع والعمل عليها ضرورة حتمية، الغرض من المذكرة هو تصميم وإنجاز موقع ويب للتصويت الالكتروني مبني باستخدام تقنية البلوك شين، ولتطويره استخدمنا العديد من الوسائل نذكر منها : إطار العمل TRUFFLE،ولغات البرمجة (SOLIDITY، HTML، CSS ،JAVASCRIPT) وكذلك لغة UML لتنفيذ أهم المخططات الخاصة بالنظام.

الكلمات المفتاحية: تطبيقات الويب ، البلوك شين ، التصويت.

ABSTRACT:

In our digital age, websites have become essential and indispensable tools, opening up vast horizons and simplifying various aspects of our lives. Consequently, the development and maintenance of these websites have become a necessity. This report aims to design and implement a web-based electronic voting system using blockchain technology. To achieve this, we utilized several tools, including the Truffle framework, programming languages such as Solidity, HTML, CSS, JavaScript, and UML for executing crucial system diagrams.

Keywords: web applications, blockchain, voting.

المراجع:

[1] " "تصويت إلكتروني," ويكيبيديا العربية. [متاح على الإنترنت]. متوفر : https://ar.wikipedia.org/wiki/%D8%AA%D8%B5%D9%88%D9%8A%D8%AA_%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A. تم الدخول: 20 يونيو 2024

[2] "كتاب الأسبوع - مقدمة إلى التصويت الإلكتروني," المفوضية الوطنية العليا للانتخابات، 13 ديسمبر 2022. [متاح على الإنترنت]. متوفر : https://hnec.ly/2022/12/13/%D9%83%D8%AA%D8%A7%D8%A8-%D8%A7%D9%84%D8%A3%D8%B3%D8%A8%D9%88%D8%B9-%D9%85%D9%82%D8%AF%D9%85%D8%A9-%D8%A5%D9%84%D9%89-%D8%A7%D9%84%D8%AA%D8%B5%D9%88%D9%8A%D8%AA-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA/.] تم الدخول: 20 يونيو 2024

[3] "Electronic voting," ويكيبيديا. [متاح على الإنترنت]. متوفر : https://en.wikipedia.org/wiki/Electronic_voting تم الدخول: 20 يونيو 2024[

[4] "Electronic Voting," بيانات الانتخابات المفتوحة. [متاح على الإنترنت]. متوفر : https://openelectiondata.net/ar/guide/key-categories/electronic-voting/. [تم الدخول: 20 يونيو 2024].

[5] المؤسسة الديمقراطية للانتخابات, "مقدمة إلى التصويت الالكتروني," ديسمبر 2011.

[6] "International Journal of Innovative Research in Computer and Communication Engineering," 4 أبريل 2016.

[7] "مجلة جامعة الزيتونة الأردنية للدراسات القانونية," المجلد 2، العدد 1، 2021.

[8] "مرصد الانتخابات," [متاح على الإنترنت]. متوفر : http://www.observatorioelectoral.org/biblioteca/?bookID=26&page. [تم الدخول: 20 يونيو 2024].

[9] م. ماي، "تكلفة التصويت الإلكتروني اعتبارًا من مايو," [متاح على الإنترنت]. متوفر : http://evoting.cs.may.ie/Documents/CostofElectronicvotingAsOfMay.pdf. [تم الدخول: 20 يونيو 2024].

[10] "قواعد التصويت," الديمقراطية العملية. [متاح على الإنترنت]. متوفر : https://practicaldemocracy.tripod.com/rules/voting/voting.htm. [تم الدخول: 20 يونيو 2024].

[11] "تصويت مبكر," ويكيبيديا العربية. [متاح على الإنترنت]. متوفر : https://ar.wikipedia.org/wiki/%D8%AA%D8%B5%D9%88%D9%8A%D8%AA_%D9%85%D8%A8%D9%83%D8%B1. [تم الدخول: 20 يونيو 2024].

[12] "ما هي تقنية Blockchain," IdeaScale. [متاح على الإنترنت]. متوفر : https://ideascale.com/ar/%D8%A7%D9%84%D9%85%D8%AF%D9%88%D9%86%D8%A9/%D9%85%D8%A7-%D9%87%D9%8A-%D8%AA%D9%82%D9%86%D9%8A%D8%A9-blockchain. [تم الدخول: 20 يونيو 2024].

[13] "Blockchain Architecture 101," منصة كومودو. [متاح على الإنترنت]. متوفر : https://komodoplatform.com/en/academy/blockchain-architecture-101/. [تم الدخول: 20 يونيو 2024].

[14] "كيف تبني بنية بلوكشين خاصة بك ," MLSDev. [متاح على الإنترنت]. متوفر : https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture. [تم الدخول: 20 يونيو 2024].

[15] ChatGPT. [متاح على الإنترنت]. متوفر : https://chatgpt.com/c/9905615f-3682-4e36-857daf-942f271e6c7d. [تم الدخول: 20 يونيو 2024].

[16] "نظرة عامة على أمان البلوكشين," معهد InfoSec. [متاح على الإنترنت]. متوفر : https://www.infosecinstitute.com/resources/blockchain-security-overview/blockchain-structure/. [تم الدخول: 20 يونيو 2024].

[17] "البلوكشين Investopedia. ",[متاح على الإنترنت]. متوفر : https://www.investopedia.com/terms/b/blockchain.asp.[تم الدخول: 20 يونيو 2024].
[18] "ما هو إثبات BeinCrypto. ",[متاح على الإنترنت]. متوفر : https://ar.beincrypto.com/learn/%D9%85%D8%A7-%D9%87%D9%88-%D8%A5%D8%AB%D8%A8%D8%A7%D8%AA.[تم الدخول: 20 يونيو 2024].
[19] "العقود الذكية Chainlink. ",[متاح على الإنترنت]. متوفر: https://chain.link/education/smart-contracts.[تم الدخول: 20 يونيو 2024].
[20] "العقد الذكي في البلوكشين Litslink. ",[متاح على الإنترنت]. متوفر : https://litslink.com/blog/smart-contract-in-blockchain.[تم الدخول: 20 يونيو 2024].
[21] "ما هو الإيثريوم Coinbase. ",[متاح على الإنترنت]. متوفر : https://www.coinbase.com/learn/crypto-basics/what-is-ethereum.[تم الدخول: 20 يونيو 2024].
[22] "ما هو الإيثريوم eToro. ",[متاح على الإنترنت]. متوفر : https://www.etoro.com/ar/crypto/what-is-ethereum/.[تم الدخول: 20 يونيو 2024].
[23] Softyfile. "Visual Studio Code,"[متاح على الإنترنت]. متوفر : https://softyfile.com/visual-studio-code/.[تم الدخول: 20 يونيو 2024].
[24] Shardeum. "Truffle,"[متاح على الإنترنت]. متوفر : https://shardeum.org/blog/truffle/#:~:text=Truffle%20is%20a%20development%20framework%20for%20building%20decentralized%20applications%20(dapps,testing%2C%20deployment%2C%20and%20management.[تم الدخول: 20 يونيو 2024].
[25] MDN Web Docs. "HTML,"[متاح على الإنترنت]. متوفر : https://developer.mozilla.org/en-US/docs/Web/HTML.[تم الدخول: 20 يونيو 2024].
[26] MDN Web Docs. "CSS,"[متاح على الإنترنت]. متوفر: https://developer.mozilla.org/en-US/docs/Web/CSS.[تم الدخول: 20 يونيو 2024].
[27] MDN Web Docs. "JavaScript,"[متاح على الإنترنت]. متوفر : https://developer.mozilla.org/en-US/docs/Web/JavaScript.[تم الدخول: 20 يونيو 2024].
[28] GetBootstrap. "Bootstrap,"[متاح على الإنترنت]. متوفر . https://getbootstrap.com/ :[تم الدخول: 20 يونيو 2024].
[29] Miro. "What is a Block Diagram?,"[متاح على الإنترنت]. متوفر : https://miro.com/diagramming/what-is-a-block-diagram/.[تم الدخول: 20 يونيو 2024].
[30] Visual Paradigm. "What is a Sequence Diagram?,"[متاح على الإنترنت]. متوفر : https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-sequence-diagram/.[تم الدخول: 20 يونيو 2024].
[31] Ledger. ؟ MetaMaskما هو "،[متاح على الإنترنت]. متوفر : https://www.ledger.com/ar/metamask#:~:text=%D9%85%D8%A7%20MetaMask,%D9%85%D9%81%D8%A7%D8%AA%D9%8A%D8%AD%20%D8%A7%D9%84%D8%B9%D9%85%D9%84%D8%A7%D8%AA%20%D8%A7%D9%84%D9%85%D8%B4%D9%81%D8%B1%D8%A9%20%D9%84%D8%A5%D9%8A%D8%AB%D8%B1%D9%8A%D9%88%D9%85%20%D9%81%D9%82%D8%B7.[تم الدخول: 20 يونيو 2024].
[32] View1sy. ؟ Solidityما هي "،[متاح على الإنترنت]. متوفر : https://view1sy.com/%D8%B3%D9%88%D9%84%D9%8A%D8%AF%D9%8A%D8%AA%D9%8A-solidity/.[تم الدخول: 20 يونيو 2024].

[33] Wikipedia. (n.d.). Voting machine. Retrieved June 20, 2024, from https://en.wikipedia.org/wiki/Voting_machine#/media/File.png

[34] MLSDev. (n.d.). How to Build Your Own Blockchain Architecture. Retrieved June 20, 2024, from https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

[35] SoluLab. (n.d.). What are Blockchain Layers? Retrieved June 20, 2024, from https://www.solulab.com/what-are-blockchain-layers/

[36] Bitazza. (n.d.). Blockchain Layer 1, 2, 3 Explained. Retrieved June 20, 2024, from https://content.bitazza.com/blockchainlayer0123en/

[37] Internxt. (n.d.). Blockchain Explained. Retrieved June 20, 2024, from https://blog.internxt.com/blockchain-explained/

[38] Petherbridge, M. (n.d.). An Elementary and Slightly Distilled Introduction to Blockchain. Retrieved June 20, 2024, from https://markpetherbridge.co.uk/blog/an-elementary-and-slightly-distilled-introduction-to-blockchain/

[39] Patriot Software. (n.d.). What is Blockchain? Retrieved June 20, 2024, from https://www.patriotsoftware.com/blog/accounting/what-is-blockchain/

[40] Analytics Vidhya. (2022). Blockchain Proof of Work (PoW). Retrieved June 20, 2024, from https://www.analyticsvidhya.com/blog/2022/09/blockchain-proof-of-work-pow/

[41] TabTrader. (n.d.). What is Proof of Stake (PoS)? Retrieved June 20, 2024, from https://tabtrader.com/academy/articles/what-is-proof-of-stake

[42] Nebeus. (n.d.). Proof of Stake vs Proof of Work. Retrieved June 20, 2024, from https://blog.nebeus.com/proof-of-stake-vs-proof-of-work/

[43] LitsLink. (n.d.). Smart Contract in Blockchain. Retrieved June 20, 2024, from https://litslink.com/blog/smart-contract-in-blockchain

[44] 101 Blockchains. (n.d.). Who is Nick Szabo: The Magician? Retrieved June 20, 2024, from https://101blockchains.com/who-is-nick-szabo-the-magician/

[45] Bambysheva, N. (2021, May 12). Ethereum's Co-Founder Vitalik Buterin Donates Over $1 Billion to India COVID Relief Fund and Other Charities. Forbes. Retrieved June 20, 2024, from https://www.forbes.com/sites/ninabambysheva/2021/05/12/ethereums-co-founder-vitalik-buterin-donates-over-1-billion-to-india-covid-relief-fund-and-other-charities/

[46] Pirimid Tech. (n.d.). What is a Smart Contract? How Does It Work? Retrieved June 20, 2024, from https://pirimidtech.com/what-is-a-smart-contract-how-does-it-work/

[47] Chainlink. (n.d.). Smart Contracts. Retrieved June 20, 2024, from https://chain.link/education/smart-contracts

[48] Crypto Valley Journal. (2020). Ethereum 2020. Retrieved June 20, 2024, from https://cryptovalleyjournal.com/education/basics/ethereum-2020/

[49] Coinbase. (n.d.). What is Ethereum? Retrieved June 20, 2024, from https://www.coinbase.com/learn/crypto-basics/what-is-ethereum

[50] SoftyFile. (n.d.). Visual Studio Code. Retrieved June 20, 2024, from https://softyfile.com/visual-studio-code/