مجلة البحوث المحاسبية

https://com.tanta.edu.eg/abj-journals.aspx


# أثر الأمن السيبراني على تعزيز تقنيات التحول الرقمي في بيئة الأعمال المحاسبية

**سوزي فاروق النقودي**

**مدرس ،كلية تكنولوجيا الادارة ونظم المعلومات، جامعة بورسعيد،مصر**

**تاريخ النشر الالكتروني: ديسمبر-2024**

للتأصيل المرجعي:النقودي،سوزي فاروق. **أثر الأمن السيبراني على تعزيز تقنيات التحول الرقمي في بيئة الأعمال المحاسبية.**

**، مجلة البحوث المحاسبية** ، المجلد **11 (4)**،

**المعرف الرقمي:**10.21608/abj.2024.392161

للتواصل مع المؤلف: Suzy_elnokoudy@himc.psu.edu.eg

# أثر الأمن السيبرانى على تعزيز تقنيات التحول الرقمي في بيئة الأعمال المحاسبية

سوزي فاروق النقودي

مدرس ،كلية تكنولوجيا الادارة ونظم المعلومات، جامعة بورسعيد،مصر

تاريخ المقال

تم استلامه في5 سبتمبر 2024، وتم قبوله في6 اكتوبر 2024، هو متاح على الإنترنت ديسمبر2024

**المستخلص :**

يهدف البحث إلى فحص أثر الأمن السيبرانى نحو تعزيز التحول الرقمي في بيئة الأعمال المحاسبية، مع التركيز على تقنية البلوكتشين كركيزة لقاعدة البيانات في نظام المعلومات المحاسبي، من خلال رقمنة عمليات التحقق الورقية الحالية، والذي ينعكس على تعزيز كفاءة وأمان العمليات المحاسبية. وقد اختارت الباحثة منهج البحث الاستكشافي أو النوعي نظراً لحداثة موضوع الدراسة، حيث تم مراجعة البحوث المعاصرة المتعلقة بالأمن السيبرانى والبلوكشين والتحول الرقمي في المحاسبة. بالإضافة إلى إجراء مقابلات مع خبراء في المجال لجمع رؤى حول منظورهم عن أثر الأمن السيبرانى على تطبيقات البلوكتشين في بيئة الأعمال المحاسبية اعتماداً على استخدام برنامج MAXQDA

توصلت الباحثة أن تعزيز الأمن السيبرانى يعد عاملاً حاسماً نحو نجاح التحول الرقمي في رقمنة الأعمال المحاسبية، لأنه يعزز من الثقة في البيانات المحاسبية ويقلل من مخاطر الاختراق والتلاعب، ويدعم استمرارية الأعمال من خلال حماية الأنظمة من الهجمات الالكترونية، كما أوضحت الدراسة أن تقنية البلوكتشين توفر منصة آمنة وشفافة لتبادل المعلومات المالية، مما يسهم في تحسين الكفاءة وتقليل التكاليف. بالإضافة إلى تحديد التحديات التي تواجه المؤسسات عند دمج هذه التقنيات، بما في ذلك الحاجة إلى تدريب الموظفين وتطوير السياسات الأمنية والامتثال التنظيمي للمعايير والقوانين العالمية والمحلية لحماية البيانات والمعاملات المحاسبية.

**الكلمات الافتتاحية:** التحول الرقمي، الأمن السيبرانى، تقنية البلوكتشين، بيئة الأعمال المحاسبية .

**Abstract:**

The research aims to examine the impact of cybersecurity on promoting digital transformation in the accounting business environment, with a focus on blockchain technology as a pillar of the database in the accounting information system, through the digitization of current paper-based verification processes, which is reflected in enhancing the efficiency and security of accounting operations. The researcher chose an exploratory or qualitative research approach due to the novelty of the study topic, where contemporary research related to cybersecurity, blockchain, and digital transformation in accounting was reviewed. In addition to conducting interviews with experts in the field to gather insights about their perspective on the impact of cybersecurity on blockchain applications in the accounting business environment based on the use of the MAXQDA program The researcher found that enhancing cybersecurity is a critical factor towards the success of digital transformation in the digitization of accounting business, because it enhances confidence in accounting data, reduces the risk of hacking and manipulation, and supports business continuity by protecting systems from cyber-attacks. The study also showed that blockchain technology provides a secure and transparent platform for the exchange of financial information, which contributes to improving efficiency and reducing costs. In addition to identifying the challenges that organizations face when integrating these technologies, including the need to train employees, develop security policies, and regulatory compliance with global and local standards and laws to protect data and accounting transactions.

**Keywords:** Digital transformation, Cybersecurity, Blockchain technology, Accounting Business Environment

## 1/ الاطار العام للبحث

### 1/1 مقدمة:

أدى تطور تكنولوجيا المعلومات وابتكارها على مدار العقديين الماضيين إلى ثورة معرفية واسعة تعرف ،بالثورة الصناعية الرابعة، والتي ألقت بظلالها على العديد من المجالات وبصفة خاصة على بيئة الأعمال المحاسبة وقد أدى ظهور العديد من التقنيات الجديدة مثل :الذكاء الاصطناعي، وإنترنت الأشياء، والبيانات الضخمة، والعقود الذكية، والأشكال الجديدة من العملات الرقمية والعملات المشفرة مثل البيتكوين التى تتعامل بها تقنية سلاسل الكتل أو ما يُعرف بالبلوكتشين Blockchain إلى تغيير الطريقة التي تتم بها العمليات والمعاملات الماسبية والمالية التقليدية، وأدت إلى التوجه نحو التحول الرقمي بغرض رقمنة المعاملات المالية والمحاسبية

يؤدي التوجه نحو التحول الرقمي إلى تغيير مستمر في متطلبات معالجة ونشر وأمن البيانات المالية وغير المالية، فبصفة خاصة تعد البلوكشين من أبرز التقنيات الرقمية المستخدمة في بيئة التحول الرقمي، فهي طريقة مستحدثة ومختلفة لمعالجة وتخزين المعاملات والمعلومات المالية والمحاسبية .لما تتميز به من ثقة وأمان وسرعة وكفاءة في حفظ المعاملات المالية وعدم التلاعب بها، فهي عبارة عن سجل ثابت وشفاف للمعاملات المالية، كما تعرف بأنها دفتر الأستاذ الرقمي الموزع غير القابل للتغيير، يتم تقييد المعاملات التي تتم بين أطراف الشبكة تلقائياً وتظهر في نفس الوقت الفعلي Real Time

ومع التوجه نحو التحول الرقمي في بيئة المحاسبة، وتطور تقنية البلوكتشين وأنظمة الذكاء الاصطناعي المختلفة والتى تلقي بظلالها على أمن وسلامة البيانات والمعاملات المالية، وظهور بعض تحديات التطبيق العملي .ظهرت التساؤلات عن دور وأهمية تقنيات الأمن السيبرانى في حماية وسلامة المعاملات والبيانات المالية من الانتهاكات والاختراقات الالكترونية .لقد أصبح من الضروري إعادة النظر فى الخصائص التنظيمية ومتطلبات البيئة المحاسبية، والسمات الوجب توافرها في المحاسبون في إطار تنظيم الأمن السيبرانى للمؤسسات\.

**2/1 مشكلة البحث:**

يخطو التحول الرقمي خطوات واسعة وكبيرة في أتمتة أعمال ومعاملات المحاسبة المالية، وكذلك تحليل البيانات وعمليات صنع القرار (Leyer and Schneider , 2021). تبرز أهمية استخدام خوارزميات الذكاء الاصطناعي لإجراء التسويات المعقدة، واكتشاف الحالات الشاذة، وتقديم رؤية لصنع القرار وتقديم البدائل، وتحرير المحاسبين للتركيز على المزيد من المهام الاستراتيجية .كما أن تحليل البيانات استناداً على الذكاء الاصطناعي يزيد من كفاءة التقارير المالية وكفاءة عملية المراجعة .ويمكن لتكامل الذكاء الاصطناعي مع تقنية البلوكتشين تطبيقاً لآليات التحول الرقمي أن يزيد من كفاءة ودقة العمليات المحاسبية، تشير التقديرات إلى أن تقنية البلوكتشين يمكن أن توفر للمؤسسات المالية ما لا يقل عن 20 مليار دولار سنويًا في تكاليف التسوية والتنظيم والدفع عبرالحدود (Fanning and Centers, 2016 )

من أهم التقنيات الرقمية المستحدثة القادرة على إحداث تغيير كبير في Blockchain تعد تقنية البلوكشين ،بيئة الاعمال، فهي تقنية سجل رقمي موزع لامركزي، لمعالجة وتخزين المعاملات والمعلومات المالية والمحاسبية التي يمكن أن تغير المنظور المحاسبي لإعادة تشكيل نظام بيئي متكامل للأعمال، والتي شكلت بداخلها مفاهيم محاسبية جديدة مثل :العملات الرقمية، العملات المشفرة )(مثل البيتكوين)(، العقود الذكية، وسلاسل التوريد.

،تساعد تقنيات البلوكشين المحاسبين في جعل موارد وحقوق والتزامات الشركة أكثر شفافية وأمان ولامركزية كما تتميز بعدم قدرة أطراف الشبكة على التلاعب في العمليات أو تغييرها .إلا أن تطبيقها يؤدي إلى مواجهة العديد من التحديات، على سبيل المثال الحاجة إلى مجموعة من المحاسبين ذو مهارات خاصة وعالية، كما يجب على الأشخاص الوعي بطبيعتها المختلفة وأن يكونوا ماهرين في تطبيقات الأعمال لتوزيع تطبيقاتهم البرمجية ومعاملاتهم على الشبكة، وهو ما يدعم توفير أمان شبكة معزز للبنية التحتية أو ما يسمى بالأمن السيبرانى.

فعلى الرغم مما توفره تقنيات البلوكشين من مميزات مثل الخصوصية والأمان إلا أن غياب مبدأ ،الخصوصية نظراً لأن المعاملات والمعلومات متداولة لكل الأطراف على الشبكة .بالإضافة إلى طبيعتها اللامركزية أظهرت بعض المخاوف التنظيمية الخاصة بها، ولذلك يتم إجراء العديد الأبحاث من أجل تعزيز المفاهيم التنظيمية (Fanning and Centers, 2016) ووضع معايير صناعية لتطبيقات قواعد البيانات المتسلسلة

بالإضافة إلى ذلك، تُظهر الأبحاث أيضاً أن تقنية العقود الذكية لا تخلو من بعض العيوب الأمنية، وتوافقاً (Atzei et al., مع ذلك، من المهم تقييم التقنيات القائمة على العقود الذكية لمواجهة نقاط الضعف أو الانتهاكات

ومع التطور المتزايد في الحياة الرقمية تتزايد التهديدات السيبرانية .كما هو(2017, Tsankov et al., 2018 ،الحال مع إحدى أشهر الحوادث البارزة التي تتعلق بالأمن السيبرانى وتطبيقات تقنية البلوكتشين في المحاسبة Mt. Gox في عام 2014 .على الرغم من أن بورصة Mt. Gox وهي حادثة اختراق بورصة العملات المشفرة هي بورصة للعملات المشفرة وليست شركة محاسبة، إلا أن حادثة الاختراق أفرزت مجموعة من التحديات الأمنية قد تواجهها الشركات عند تطبيق تقنية البلوكتشين.

ومن هنا ظهرت الحاجة إلى أهمية دراسة الأمن السيبرانى للنظام المحاسبي القائم على التحول الرقمي وبصفة خاصة تقنيات البلوكتشين، فالأمن السيبرانى هو الضمان الأساسي لأمن المعلومات المحاسبية، فكلما ازدات العمليات المحاسبية تعقيداً زاد التهديد السيبرانى، سواء التهديد الخارجى مثل سرقة البيانات المحاسبية وخاصة البيانات السرية التجارية، أو التهديد الداخلى مثل تبيض البيانات المحاسبية بشكل خفي غير قانونى .(Mahmood, et al., 2022)

إن التقارب بين الأمن السيبرانى والمحاسبة ليس مجرد انعكاس للتقدم التكنولوجي، هو استجابة للتحديات وقد ،(Kumar, et al., 2021) المعقدة التي تواجهها المؤسسات في حماية البيانات المالية وأصولها الرقمية أصبح التفاعل بين هذين التخصصين ضرورياً وحتمياً بشكل متزايد.

**وهكذا ظهرت مشكلة البحث والتي تتمثل في السؤال البحثي الرئيسي:** "ما هو أثر الأمن السيبرانى على تعزيز التحول الرقمي – بصفة خاصة تقنية البلوكتشين – في بيئة الأعمال المحاسبية " **والذي انبثقت منه الأسئلة الفرعية التالية:**

س1: ما المقصود بالتحول الرقمي وما هي تطبيقاته؟

س2: كيف تعمل تقنية البلوكتشين Blockchain وما هو أثرها علي بيئة الأعمال المحاسبية؟

س3: ماهي التدابير الأمنية المتبعة في تقنية البلوكتشين لضمان حماية المعاملات والبيانات ؟

س4: ما المقصود بالأمن السيبرانى وأهميته لمهنة المحاسبة؟

س5: كيف يمكن تعزيز دور الأمن السيبرانى عند تطبيق تقنية البلوكتشين في المحاسبة؟

**3/1 أهمية البحث:**

**تتمثل الأهمية الأكاديمية للدراسة في:**

- تعزيز البحث العلمي: من خلال تعزيز الاسهام العلمي والاطلاع على أهم مستجدات في مجالات التحول الرقمي لمهنة المحاسبة والأمن السيبرانى وتقنية البلوكتشين، مما يفتح آفاق جديدة للباحثين.
- إثراءالمعرفة الأكاديمية: البحث يساهم في توسيع المعرفة الأكاديمية حول تأثير التحول الرقمي على مهنة المحاسبة (خاصة تقنية البلوكتشين) والأمن السيبرانى.

- التعاون الأكاديمي: يمكن أن يؤدي البحث إلى إحداث تعاون بين المؤسسات الأكاديمية والشركات، مما يساهم في إثراء المعرفة والخبرات.

**تتمثل الأهمية العملية للدراسة في:**

- يمكن أن تساهم البحث في تعزيز متطلبات الأمن السيبرانى في البيئة المحاسبية في ظل التحول الرقمي، مما يحد من مخاطر الاحتيال والانتهاكات.
- تطوير الممارسات الأمنية من خلال محاولة تقديم رؤى لتحسين أمن وسرية المعلومات والعمليات المحاسبية عند تبني تقنيات جديدة في ظل الحول الرقمي مثل البلوكتشين، مما يزيد من الكفاءة والشفافية.

**4/1 أهداف البحث:**

**يتمثل الهدف الرئيسى في دراسة** " دراسة أثر الأمن السيبرانى على تعزيز التحول الرقمي في بيئة الأعمال المحاسبية بصفة خاصة تقنية البلوكتشين"، **والذي انبثقت منه الأهداف الفرعية على النحو التالي:**

1. فهم أثر تطبيق تقنيات التحول الرقمي على بيئة الأعمال المحاسبية.
2. **تقييم فعالية البلوكتشين:** دراسة كيف يمكن لتكنولوجيا البلوكتشين أن تقلل من المخاطر وتعزز الأمان، واستكشاف الفوائد العملية لتطبيق تقنية البلوكتشين في بيئة الأعمال المحاسبية، بما في ذلك من المحاسبة في الوقت الفعلي، الشفافية والكفاءة.
3. **تحليل المخاطر السيبرانية في المحاسبة:** تحديد وفهم المخاطر السيبرانية التي تواجهها الممارسات المحاسبية التقليدية ودورها في زيادة تعزيز رقمنة بيئة الأعمال المحاسبية نحو التحول الرقمي.
4. **تقييم التحديات:** تحديد التحديات التي قد تواجهها المؤسسات عند تطبيق تقنية البلوكتشين في المحاسبة، ومحاولة تقديم مقترحات للتغلب على هذه التحديات.

**5/1 فروض البحث:**

في ضوء مشكلة البحث والتساؤلات الخاصة به، وسعياً لتحقيق أهداف البحث، فإن الباحثة تستند إلى إثبات صحة أو خطأ فروض البحث:

الفرض الأول: لا توجد علاقة ايجابية بين تطبيق تقنية البلوكتشين كأحد تقنيات التحول الرقمي وتحسين بيئة الأعمال المحاسبية.

الفرض الثاني: لا توجد علاقة ايجابية بين تطبيق الأمن السيبرانى وتعزيز دور تقنية البلوكتشين على بيئة الأعمال المحاسبية.

**6/1 حدود البحث:**

سوف تقتصر الباحثة على دراسة أثر تقنية البلوكتشين باعتبارها أحد أهم تقنيات التحول الرقمي، الأكثر تداولاً وممارسة في مهنة المحاسبة، والتي تعرضت لانتهاكات واختراقات أمنية يجب العمل على الحد منها، من خلال دراسة تأثير دور الأمن السيبرانى ومتطلباته لدعم تطبيق تقنية البلوكتشين في ظل التحول الرقمي.

**7/1 منهجية البحث:**

**المنهج الاستقرائي:** استعراض أهم الدراسات العربية والأجنبية السابقة التي تناولت موضوع البحث ودراسة نتائج هذه الدراسات والاستفادة منها في تحديد فجوة بحثية واختيار فروض البحث .

**المنهج الاستنباطي:** لاستخلاص وتفسير وتحليل دور التحول الرقمي في تغيير بيئة الأعمال المحاسبية المتغيرة، ودراسة أهمية الأمن السيبرانى في تعزيز تطبيق تقنيات البلوكتشين في بيئة الأعمال المحاسبية.

**8/1 الدراسات السابقة:**

**1/8/1 الدراسات المتعلقة بـ "تقنية البلوكتشين وأثرها على مهنة المحاسبة"**

- **دراسة(Danach, et. al, 2024):** هدفت الدراسة إلى فحص تقنية البلوكتشين Blockchain و تأثيرها على إجراءات إعداد التقاريرالمالية والمراجعة المعاصرة، بالاضافة إلى استكشاف التداعيات المختلفة لتبني تقنية البلوكتشين في مجال المحاسبة، مع التركيز على كيفية تأثيرها على الامتثال التنظيمي، وسلامة مسار عملية المراجعة، وفعالية التكلفة، والعقود الذكية، كذلك توضيح المشاكل التي يواجهها العاملون والمنظمون ومراجعو الحسابات عند استخدام تقنية البلوكتشين من خلال تحليل إمكاناتها التجريبية وبمساعدة الأطر التنظيمية المتنامية.

توصلت الدراسة إلى تقديم رؤية واضحة لكيفية تغيير عمليات إعداد التقارير المالية والمراجعة المالية في عصر تقنية البلوكتشين. وأكدت على أثر تطبيق البلوكتشين على ممارسات المحاسبة التقليدية وضرورة قيام المؤسسات بدمجها داخل عملياتها المالية لفوائدها المتعددة. كما أكدت الدراسة أيضاً على الحاجة إلى المرونة والامتثال للمتطلبات القانونية لتحقيق إمكاناتها بالكامل في مجالات جودة عملية المراجعة وإعداد التقارير المالية.

- **دراسة (Chowdhury, et al., 2023)** : هدفت الدراسة إلى فحص الآثار المترتبة على استخدام تقنية البلوكتشين في زيادة كفاءة معلومات المحاسبة المالية ، من خلال دراسة حالة إحدى الشركات لفهم أثر تقنية البلوكتشين على الإفصاح المالي.

وأظهرت الدراسة أن تقنية البلوكتشين يمكن أن تخلق منصة للمؤسسات للإفصاح عن معلوماتها طواعية على المدى القصير، بينما تقلل من الأخطاء في الإفصاحات المالية، وعلى المدى الطويل تعزز جودة المعلومات وتحد من ازدواجية المعلومات. وهو ما قد يُشجع الإدارة العليا وصانعي السياسات على تبني تقنية البلوكتشين في أعمالهم

لزيادة جودة البيانات وكفاءة التقارير. وقد أشارت الدراسة إلى الطرق الضرورية التي يمكن من خلالها زيادة جودة المعلومات المحاسبية من خلال تطبيق تقنية البلوكتشين. وحددت التهديدات المحتملة عند تطبيق تقنية البلوكتشين.

- **دراسة (Qin,2022):** هدفت الدراسة إلى فحص التأثير تقنية البلوكتشين Blockchain على إمساك دفاتر المحاسبة، وجودة المعلومات المحاسبية، والمعلومات الرقمية المالية.

أظهرت الدراسة أن تقنية البلوكتشين تؤثر على إعداد التقارير المالية بشكل إيجابي كبير من خلال زيادة شفافية وكفاءة وأمان المعلومات المحاسبية، حيث يقلل نموذج مسك الدفاتر الموزعة والنظام الدفتري المشترك للبلوكتشين من انتهاكات الاحتيال والتزوير، وهكذا تتميز المعلومات المحاسبية بمزيد من الانفتاح والشفافية، كما أن تكنولوجيا العقود الذكية تساعد في جعل إجراءات المعاملات بين المؤسسات تُنجز تلقائياً، وتُسجل لحظياً لتحقيق رقمنة البيانات المالية، وتحقيق هدف التكامل الاقتصادي للمؤسسات.

- **دراسة (Ibrahim, 2023):** هدفت الدراسة إلى تحليل المنظور الدولي للفرص والتحديات وانعكاسات تقنية البلوكتشين Blockchain على المجال المحاسبى، من خلال إجراء دراسة استكشافية لاستطلاع رأى الأكاديميين والمهنيين في مصر عن تطبيق تقنية البلوكتشين في مجال المحاسبة.

توصلت الدراسة أن تقنية البلوكتشين تزيد من فرص مهنة المحاسبة ولكنها تحمل في طياتها بعض العقبات والتكلفة، بالاضافة إلى العديد من الآثار الايجابية على مهنة المحاسبة المالية وعملية إعداد تقارير الشركات والمراجعة، وكذلك على المحاسبين أنفسهم، ولكن مازال تطبيقها في البيئة المصرية المحاسبية في مهده، ولم ولن يتم اكتشاف إمكاناتها وآثارها المحتملة إلا بعد تطبيقها على نطاق واسع.

**2/8/1 الدراسات المتعلقة بـ"الأمن السيبرانى وأثره على مهنة المحاسبة":**

- **دراسة (Polishchuk, et. al, 2024):** هدفت الدراسة إلى فحص أثر الأمن السيبرانى على استقرار المؤسسات المالية وفعالية التدابير المختلفة للأمن السيبرانى على ضمان مرونة المؤسسات المالية الأوكرانية ضد التهديدات السيبرانية، وذلك من خلال استخدام أساليب البحث النوعي لفحص تجربة المؤسسات الاوكرانية التي تستخدم استراتيجيات دفاعية رقمية متغيرة وتحافظ على وظائفها اعتماداً على نظام فعال للأمن السيبرانى في سياق صراع عسكري عالمي.

توصلت الدراسة إلى أهمية أنظمة الأمن السيبرانى القوية لضمان الاستدامة التشغيلية والمالية، وقد أكدت الدراسة على أهمية البرامج والأجهزة وتحديث الحلول الإدارية لضمان جودة الأمن السيبرانى لمواجهة التهديدات المتصاعدة السيبرانية التي تتعرض لها المؤسسات المالية، والحاجة الملحة إلى الابتكار المستمر .

- **دراسة (Abrahams, et. al, 2024):** هدفت الدراسة إلى استكشاف العلاقة بين المحاسبة والأمن السيبرانى، من خلال دراسة التكامل بينهما لتحقيق الامتثال والشفافية في المؤسسات. وقد اعتمدت الدراسة

على استخدام الأساليب الإحصائية ونماذج تحليلية لتحديد الأنماط والعلاقات بين المحاسبة والأمن السيبرانى، وتحديد الفجوات البحثية والممارسات الحالية.

توصلت الدراسة أن تكامل المحاسبة والأمن السيبرانى بشكل فعال يعزز من حماية البيانات المالية، وكذلك الشفافية، ويحد من المخاطر القانونية، وهو ما يسهم في تحسين الأداء المؤسسي والامتثال التنظيمي. كما اقترحت الدراسة استراتيجيات شاملة تتضمن التعاون بين الفرق المختلفة وتحديث مستمر للتقنيات والإجراءات.

- **دراسة (Dasgupta, et. al ,2023)**: هدفت الدراسة إلى استكشاف أثر الذكاء الاصطناعي في تحديد التهديدات على الخدمات المصرفية الرقمية، وتحديد أثر استخدام الأمن السيبرانى القائم على الذكاء الاصطناعي على دعم كفاءة الأعمال وزيادة الوعي بالتقنيات الجديدة، وإظهار كيفية التعلم من تجارب الآخرين مثل تجربة مالطا لإدارة المخاطر وعلاقتها بتجارب الشركات الأخرى التي نفذت أنظمة الأمن السيبرانى.

وتوصلت الدراسة إلى أن ظهور الذكاء الاصطناعي أدى إلى إحداث تغييرات كبيرة في دورة عمل الشركات، وخاصة الأمن السيبرانى. حيث تزايد الاعتماد على التكنولوجيات الحديثة في العمليات التجارية لتخزين البيانات مما جعل الشركات عرضة أكثر للهجمات الالكترونية. وبالتالي فمن الضروري للمؤسسات دمج أنظمة الأمن السيبرانى بالذكاء الاصطناعي كي تحمي عملياتها. وعلى الرغم من الفوائد العديدة لاستخدام الذكاء االصطناعي في الأمن السيبرانى، لا يزال هناك مخاوف بشأن أمان التكنولوجيا وفعاليتها.

- **دراسة (Daoud & Serag, 2022)**: هدفت الدراسة إلى تطوير إطار لدراسة تأثير الأمن السيبرانى على البيانات المحاسبية لزيادة الثقة في التقارير المالية، في ظل تقنيات الصناعة الخاصة بالبيانات الضخمة وانترنت الأشياء وتكامل أنظمة الحوسبة وزيادة أتمتة المعاملات والواقع الافتراضي. بالاضافة إلى فحص كيفية تمكين الممارسين من تقييم تهديدات الأمن السيبرانى وفهم تأثيرها على استراتيجيات الاستجابة المختلفة، بالاعتماد على نهج الحدث والتأثير والاستجابة لمناقشة آثار الأمن السيبرانى على البيانات المحاسبية لزيادة الثقة والشفافية في التقارير المالية.

توصلت الدراسة إلى دور الأمن السيبرانى في حماية البيانات والمعلومات في المؤسسات، ولكن يتطلب الأمر استجابة من الإدارة والمستثمرين والمراجعين والجهات التنظيمية

اقترحت الدراسة مجموعة من الاستراتيجيات الفعالة الواجب تبنيها من قبل المؤسسات لتعزيز الأمن السيبرانى متمثلة في:

- دراسة المخاطر: إجراء تقييم شامل للمخاطر لتحديد الثغرات والتهديدات المحتملة.
- تدريب الموظفين : زيادة الوعي الأمني من خلال تدريب الموظفين على ممارسات الأمن السيبرانى.

- تحديث البرمجيات : تنفيذ تحديثات دورية للبرمجيات ونظم التشغيل لتقليل الثغرات.
- تطوير استراتيجيات استجابة: وضع خطط استجابة للحوادث لضمان التعامل الفعال مع أي خروقات.
- تعاون داخلي : تعزيز التعاون بين فرق الأمن السيبرانى والمراجعة الداخلية لتحسين فعالية الإجراءات.

**3/8/1 الدراسات المتعلقة بـ" العلاقة بين الأمن السيبرانى وتقنية البلوكتشين" :**

- **دراسة (Zhou, et. Al ,2022)**: هدفت الدراسة إلى استكشاف تكامل تقنية البلوكتشين Blockchain لتعزيز أمن معلومات المحاسبة الإلكترونية، وكيف يُمكن معالجة التهديدات الإلكترونية المتزايدة في المشهد الرقمي الاقتصادي مما يشكل مخاطرة على أمان المعلومات المحاسبية.

أظهرت الدراسة أن تقنية البلوكتشين توفر منصة لا مركزية غير قابلة للتغيير لتأمين البيانات المحاسبية، مما يجعلها مقاومة للوصول غير المصرح به والعبث بها، ومن خلال الاستفادة من مزايا تقنية البلوكتشين Blockchain، يُمكن إنشاء نظم محاسبية آمنة للحد من التهديدات الخارجية الإلكترونية كسرقة البيانات، أوالتهديدات الداخلية كالممارسات المحاسبية الاحتيالية . اقترحت الدراسة حلولاً فعالة لتأمين البيانات المحاسبية بكفاءة لدعم تطبيق تقنية البلوكتشين في مجال المحاسبة.

- **دراسة (Smith, et. Al, 2020)**: هدفت الدراسة إلى تقييم إمكانيات تقنية البلوكتشين Blockchain في تعزيز الأمن السيبرانى للمعاملات المالية، لتوفير نموذجًا للمؤسسات في القطاع المالي لاتخاذ القرارات. وقد اعتمدت الدراسة على تقنيةKeeney للتفكير المرتكز على القيمة (VFT)، كأداة لتحليل القرار متعدد الأهداف.

اقترحت الدراسة نموذجاً لتقييم تقنية البلوكتشين Blockchain قائماً على فهم القيم الاستراتيجية داخل المنظمات لتقييم أهداف الأمن السيبرانى للمساعدة في تحسين أمن المعاملات المالية. ولكن لم تقترح الدراسة آليات لتقييم الفوائد المقترحة بواسطة قواعد البيانات التسلسلية، وتحديدًا في سياق الأمن السيبرانى، بحيث يُمكن للمؤسسات المالية فحص فعالية الحلول المستندة على قواعد البيانات التسلسلية للإدارة الآمنة للمعاملات المالية.

- **دراسة (Ndri, 2023)**: هدفت الدراسة إلى فحص جدوى تطبيق تقنية البلوكتشين Blockchain في الأمن السيبرانى، وخاصة للأمور الخاصة بإنترنت الأشياء، وتخزين البيانات، وأمن الشبكات، من خلال القضاء على نقاط الفشل الفردية وتقديم بروتوكولات اتصال آمنة. بالإضافة إلى ذلك، تناولت الدراسة كيفية ضمان أساليب التشفير مثل خوارزميات التجزئة ودفاتر الأستاذ الموزعة السرية والنزاهة والتوافر كجزء من ثالوث وكالة المخابرات المركزية.

توصلت الدراسة إلى أنه على الرغم من الفوائد العديدة المتعلقة بالثقة الرقمية والعداء التكيفي وما إلى ذلك، فإن عدم النضج التكنولوجي، وتعقد التكلفة العالية، والعقبات التطبيقة لتقنية البلوكتشين في مجال الأمن السيبرانى فإن الأمر يتطلب من المؤسسات المالية إجراء تحليلاً مفصلاً لقابلية تطبيقها داخل المنظمة، وتحديد غرض تنفيذها

بوضوح لتجاوز أي تحديات. مع الاعتراف بالفوائد المحتملة الهائلة التي توفرها تقنية البلوكتشين في ضمان شبكات آمنة، كما يجب على المؤسسات أن تدرس ما إذا كان اعتمادها يتوافق مع متطلباتها الأمنية المحددة.

**التعليق على الدراسات السابقة :**

**:ومن خلال عرض وتحليل الدراسات السابقة، يمكن إستخلاص مجموعة من النقاط أهمها**

- أكدت العديد من الدراسات المؤيدة على أهمية دور تقنية البلوكتشين على إحداث ثورة في الممارسات المحاسبية تلقي بظلالها على تطوير الممارسات المحاسبية، مما ينعكس على زيادة الأمن والشفافية بفضل الطبيعة اللامركزية للبلوكتشين، وعدم القدرة على تغيير المعاملات مما يقلل من مخاطر التلاعب، بالاضافة إلى مما توفره من وقت وتكاليف وهو ما ينعكس على تحسين الكفاءة التشغيلية للمؤسسات.
- بينما كانت هناك مجموعة من الدراسات المعارضة التى ألقت الضوء على مخاطر الأمن السيبرانى فعلى الرغم من تعزيز البلوكتشين للأمان، إلا أن هناك مخاطر سيبرانية مرتبطة بتطبيقها يمكن أن تؤدي إلى خسائر مالية كبيرة، بالاضافة إلى المشاكل التقنية الخاصة بضرورة توافر بنية تحتية تقنية متقدمة وتكاليف صيانة عالية، وكذلك التحديات القانونية والتنظيمية نظرا لعدم وجود تشريعات تنظيمية ملزمة.
- ترى الباحثة أن معظم الأبحاث التي تناولت العلاقة بين تقنية البلوكتشين والأمن السيبرانى توصلت إلى أن تقنية البلوكتشين تمكنت من تعزيز الأمن والخصوصية بتوفير منصة آمنة وشفافة للمعاملات الرقمية ومشاركة البيانات.
- ولكن لم تتوصل الباحثة إلى أية دراسات توضح الدور المتبادل بين تقنية البلوكتشين والأمن السيبرانى، وما هي متطلبات الأمن السيبرانى التى يجب أخذها في الاعتبار لتحقيق الاستفادة القصوى من المزايا التكنولوجية لتقنية البلوكتشين في مهنة المحاسبة.

**9/1 خطة البحث:**

- **القسم الأول** :الاطار العام للبحث، من خلال عرض المقدمة ومشكلة البحث، وأهميته وأهدافه، وحدود البحث ومنهجيته، والدراسات السابقة.
- **القسم الثانى**: الإطار النظري للبحث.
- **القسم الثالث** الإطار المنهجي للبحث ونموذج عرض وتحليل البيانات
- **القسم الرابع** :يعرض الخلاصة والنتائج والتوصيات، ويقدم مقترح لأبحاث مستقبلية.

**2/ الإطار النظري**

**1/2 ما هو التحول الرقمي ؟ وماهي تطبيقاته في بيئة الأعمال المحاسبية؟**

يمكن تعريف التحول الرقمىDigital Transformation من منظور محاسبي، وفقاً لما عرفه (Khanon, 2020) هو عملية تغير جذرى وتطوير للبنية التحتية لنماذج أداء الأعمال، عن طريق تطبيق التقنيات التكنولوجية الحديثة، سواء أكان ذلك بصورة جزئية أو كلية، لاكتساب مزايا تنافسية وتحقيق قيمة مضافة والسعى نحو تحقيق الأهداف المرجوة من استرتيجيات الأعمال، بصفة عامة.

كما أشار (نصر،2022) أنه يمكن النظر لعملية التحول الرقمى لمنشأت الأعمال، بأنه: عملية تغيير جذرى وهيكلى لنماذج أعمال المنشأت، من خلال تبنى التكنولوجيات الرقمية عند أداء مختلف العمليات التشغيلية وبناء علاقاتها مع الموردين والعملاء، من جهة، وكذا عند تفاعلها مع أصحاب المصالح من جهة أخرى.

وقد أشار (شحاته، 2020)، أن التحول الرقمي قد تطور على ثلاث مراحل أساسية لتطوير بيئة الأعمال المحاسبية ، وهي:

- **النمذجة (الرقمنة) Digitization:** تشير لتشفير المعلومات التناظرية "التقليدية" إلى معلومات رقمية يسهل تخزينها ومعالجتها بأجهزة الحاسب الآلى، ويتم ذلك من خلال دمج تقنيات تكنولوجيا المعلومات بالمهام الحالية للمنشأة.
- **التمثيل المرئى Digitalization:** يعبر عن كيفية الاعتماد على التكنولوجيا المعلوماتية فى تنفيذ العمليات التشغيلية وبناء العلاقات مع العملاء، مثل إنشاء قنوات اتصال جديدة عبر الانترنت يسهل من خلالها التواصل بين مختلف الأطراف ذوى الصلة.
- **التحول الرقمى Digital Transformation:** يشير إلى تطوير نماذج الأعمال الحالية أو تبنى نماذج أعمال جديدة، قد تكون قائمة بالفعل بشركات مناظرة أو مبتكرة، وذلك لتحقيق ميزة تنافسية وإضافة قيمة حقيقة للمنشأة.

**وقد تنوعت تطبيقات التحول الرقمي المستخدمة في بيئة الأعمال المحاسبية،** كتقنية سلاسل الكتل أو البلوكتشين Blockchain، البيانات الضخمة Big Data، الحوسبة السحابية Cloud Computing، أدوات الذكاء الاصطناعى Intelligence Artificial، العملات المشفرة Cryptocurrency، والعقود الذكية Contracts Smart.

جدير بالذكر أن التحول الرقمي لا يخلو من المعوقات، من أبرز هذه المعوقات ضرورة تدريب المحاسبين والمراجعين على استخدام التقنيات الجديدة، لضمان أن يكون لدىهم المهارات اللازمة للتكيف مع الأدوات الرقمية، والكشف عن الاختراقات أو الانتهاكات التي يمكن أن تحد وتشكك من فوائد التحول التكنولوجي في بيئة الأعمال المحاسبية لفقدان الأمان والثقة والخصوصية. علاوة على ذلك، تثير قضايا الأمان السيبرانى مخاوف كبيرة في ظل زيادة التوجه نحو التكنولوجيا الرقمية. يجب على المنظمات إدراك المخاطر الخاصة بتسريب البيانات أو الهجمات الإلكترونية، مما يتطلب منها اتخاذ تدابير أمان متقدمة لحماية المعلومات الحساسة.

هو ما جعل الباحثة تسعى إلى التركيز على دراسة تقنية البلوكتشين باعتبارها أحد تطبيقات التحول الرقمي الأكثر انتشاراً، ودراسة أثر الأمن السيبرانى في دعم التحول الرقمي في ظل تطبيق تقنيات البلوكتشين.

**2/2 ما هي تقنية البلوكتشين Blockchain وما هو أثرها علي مهنة المحاسبة؟**

نشر (Nakamoto, 2008) في كتاب "بيتكوين: نظام النقد الإلكتروني من نظير إلى نظير"، وصف للعمود الفقري لتقنية البلوكتشين، بأنها شبكة تقوم بطوابع زمنية للمعاملات عن طريق تجزئتها في سلسلة مستمرة من إثبات العمل، مما يُشكل سجلًا لا يمكن تغييره دون إعادة إثبات العمل، حيث يتم تجزئة المعاملات في كتلة واحدة، وجميع الكتل تشكل سلسلة، ومن هنا جاء اسم سلاسل الكتل أو البلوكتشين

عرف معهد المحاسبين القانونيين في إنجلترا وويلز (ICAEW, 2018): البلوكتشين بأنها ليست تقنية واحدة، بل بروتوكول لتسجيل المعاملات عكس الإنترنت، حيث يتم مشاركة البيانات، ويمكن نقلها من طرف إلى آخر. أو بمعنى آخر: هي تقنية محاسبية لنقل ملكية الأصول والاحتفاظ بدفاتر معلومات مالية دقيقة، حيث ينبع ثبات دفتر الأستاذ من الثقة في النظام. كما أن التوزيع بين جميع المستخدمين يلغي الانقطاعات ويلغي تكلفة دفع سلطة مركزية للحفاظ على دقة دفتر الأستاذ، يُمكن لأي مشارك في دفتر الأستاذ من تتبع جميع المعاملات السابقة، وهو ما يزيد الشفافية.

تقنية البلوكتشين هي عبارة عن تقنية دفاتر حسابات لامركزية وموزعة تسجل المعاملات عبر شبكة من أجهزة الكمبيوتر بطريقة آمنة ومضادة للتلاعب. ترتبط كل معاملة، أو كتلة بشكل مشفر بالكتلة السابقة، وهو ما يُشكل سلسلة من الكتل (Odeyemi, et al., 2024). وتتميز تقنية البلوكتشين (Sarker & Datta , 2020) بالشفافية والثبات واللامركزية، مما يجعلها مناسبة للمعاملات الآمنة وغير الموثوقة.

من الناحية التقنية، يسمى كل مشارك في سلسلة الكتلة/البلوكتشين يحتفظ بنسخة من دفتر الأستاذ "بالعقدة". نظرًا لأن جميع العُقد تحتفظ بنسخة من دفتر الأستاذ، فهذا يعني أن دفتر الأستاذ لا مركزي ولا يوجد في موقع واحد، وبالتالي لا يُمكن للسلطة المركزية تغيير دفتر الأستاذ بأي شكل من الأشكال، حيث يجب على جميع العُقد "الموافقة" على أي إضافات إلى دفتر الأستاذ. لذلك، فإن أهم دور للعقد هو إضافة كتل إلى السلسلة، وهو ما يتم م خلال معالجة المعاملات (التي تتكون منها الكتل) من خلال دالة تشفير أحادية الاتجاه لا يمكن تغييرها بأثر رجعي(Iansiti and Lakhani ,2017)

وفي سياق ظهور تقنية البلوكتشين ظهرت العديد من التطبيقات التي صاغت مفاهيم محاسبية حديثة مثل العملات الرقمية والعقود الذكية والعملات المشفرة (على سبيل المثال: البيتكوين Bitcoin، والايثريومEthereum، ولايتكوين Litecoin). كما تختلف أنواع منصات البلوكتشين (أبوالخير وآخرون،2023، عبدالحميد،2023) وهي:

1. **البلوكشين العام:** مثل البلوكشين المستخدم في البيتكوين، يمكن لأي شخص الانضمام إلى الشبكة والتحقق من المعاملات
2. **البلوكشين الخاص:** يُستخدم داخل مؤسسة واحدة أو مجموعة محددة من المؤسسات، ويكون الوصول إليه محدودًا.
3. **البلوكشين الهجين:** يجمع بين ميزات البلوكشين العام والخاص، حيث يمكن التحكم في من يمكنه المشاركة في الشبكة، ولكن البيانات يمكن أن تكون متاحة للجميع.
4. **البلوكشين المتحد:** يُدار من قبل مجموعة من المؤسسات التي تعمل معًا، ويكون الوصول إليه مقتصر على الأعضاء فقط

**مما سبق ترى الباحثة** أن تقنية البلوكتشين عبارة عن تقنية دفاتر حسابات لامركزية موزعة، تُسجل المعاملات بين مختلف الأطراف بطريقة فعالة وقابلة للتحقق ولحظية، تتميز المعاملات على الشبكة بالخصوصة والأمان وعدم القدرة على التغيير . يسمى كل مشارك في سلسلة الكتل أو البلوكتشين يحتفظ بنسخة من دفتر الأستاذ "بالعقدة".

**3/2 سمات المحاسبة القائمة على تقنية البلوكتشين في ظل التحول الرقمي:**

| طرق المحاسبة التقليدية | محرك القيمة | فوائد تقنية البلوكتشين |
|---|---|---|
| المستندات وتسجيل المعاملات يدوياً | تبسيط العمليات وتحقيق الكفاءة | رقمنة الوثائق، زيادة الكفاءة، تقليل التكاليف، تقليل الأخطاء البشرية، أتمتة التسويات |
| تستغرق العملية وقتًا طويلاً | تقليص وقت تسوية المعاملات | يمكن للعقود الذكية المدعومة بتقنية البلوكتشين أن تنفذ تلقائيًا بمجرد الانتهاء من تنفيذ الشروط المحددة مسبقًا، مما يسهل المعاملات في الوقت الحقيقي. |
| عدم وجود آلية لتتبع المعاملات من دفاتر الأستاذ المختلفة | الحد من المخاطر النظيرة | يتم تدوين الاتفاقيات وتنفيذها في بيئة مشتركة وغير قابلة للتغيير ، ومراجعة الحسابات |
| عرضة للاحتيال | تقليل الاحتيال | توفر الشفافية والرؤية والموثوقية والسجلات غير القابلة للتغيير، مما يعزز الأمان والسرية. ويتم ملاحظة أي تحويلات مالية مشبوهة واكتشافها لحظياً. |
| تعقيد اللوائح، مكلف للمنظمات | تحسين الكفاءة التنظيمية | توفر تقارير أسرع وأكثر دقة من خلال أتمتة العمليات بالعقد الذكي، وتسمح بالمراقبة في الوقت الفعلي بين المنظمين والكيانات الخاضعة للتنظيم. |
| مشاركة الوسطاء في العديد من العمليات | تحسين السيولة ورأس المال | إزالة اختلال توازن المعلومات بين المشاركين في السوق، وزيادة الشفافية |

**المصدر: (Han , et al., 2023, Deloitte, 2020)**

**4/2 دور تقنية البلوكتشين في تعزيز الخدمات المالية في ظل التحول الرقمي:**

يتمثل دور تقنية البلوكتشين كقوة تحويلية في تعزيز التدابير الأمنية عند إجراء التحويلات الرقمية في القطاعات المالية من خلال الاستفادة من مميزاتها الفريدة، مثل: الثبات واللامركزية والعقود الذكية. حيث توفر تقنية البلوكتشين منصة قوية لتأمين المعاملات والبيانات المالية. ويتبلور دور تقنية البلوكتشين في (Odeyemi, et al., 2024):

**1.. تعزيز أمن المعاملات المالية:** من خلال توفير دفتر أستاذ غير قابل للتغيير، وهو ما يعزز من سلامة وشفافية المعاملات المسجلة على المنصة. حيث ترتبط كل معاملة بشكل مشفر بالمعاملة السابقة، مما يشكل سلسلة من الكتل التي لا يمكن تغييرها أو التلاعب بها بمجرد تأكيدها وإضافتها إلى البلوكتشين (Khan, et. al., 2021, Schär, 2021) ، كما أنها تعزز أيضًا آلية الثقة في السوق المالى من خلال تحسين الأمان وإمكانية تتبع البيانات، من خلال إنشاء معرفات أجهزة غير قابلة للتغيير وتنظيم الوصول.

**2.. التحقق من صحة المعاملات المالية:** ميزة الثبات التي تتميز بها تقنية البلوكتشين تجعل منها منصة مثالية لتسجيل المعاملات المالية والتحقق منها، كما أنها تحارب تزوير الهوية وتضمن الاتصال الآمن، فيُمكن للمؤسسات المالية الاعتماد على تقنية البلوكتشين للحفاظ على سجل آمن ومضاد للتلاعب بالمعاملات، والحد من مخاطر اختراق البيانات والنزاعات والأنشطة الاحتيالية.

**3.. تعزيز الثقة والمساءلة:** شفافية تقنية البلوكتشين تُمكن كافة المشاركين على الشبكة من الوصول إلى سجلات المعاملات والتحقق منها، مما يعزز الثقة والمساءلة، وذلك من خلال توفير سجل شفاف وقابل لمراجعة المعاملات، وتزيد من تعظيم الثقة في المعاملات المالية وتعزز سلامة النظام المالي (Politou, et. al., 2019) .

**4.. توفير المصادقة الآمنة:** تقنية البلوكتشين تعمل على تعزيز أمان البيانات المالية بشكل كبير بواسطة توفير منصة لامركزية وشفافة لتخزين المعاملات المشفرة، يعمل تكامل البلوكتشين مع إنترنت الأشياء (IoT) على تعزيز الإجراءات الأمنية بالاستفادة من البيانات في الوقت الفعلي من أجهزة إنترنت الأشياء وتسجيلها بأمان على منصة البلوكتشين، حيث تتيح المصادقة الآمنة والقابلة للتحقق للأفراد والكيانات في المعاملات المالية، مما يمنع الاحتيال والوصول غير المصرح به .

**5.. تقليل المخاطر السيبرانية:** تعتبر تقنيات البلوكتشين فعالة في الحد من المخاطر السيبرانية الخاصة بالبيانات المالية عند استخدامها بصورة صحيحة، يمكن للبلوكتشين تحقيق سرية البيانات، وسلامتها، وهذا يجعلها مفيدة في الحفاظ على البيانات من الهجمات السيبرانية. علاوة على ذلك، تحتاج جميع المعاملات إلى المصادقة من قبل عدة عقد، مما يجعل التلاعب بها أكثر صعوبة.

**ترى الباحثة،** أن تقنية البلوكتشين تعزز أمان المعلومات والمعاملات المحاسبية بتوفير بيئة أكثر أمانًا وشفافية وكفاءة في ظل تصاعد متطلبات بيئة الأعمال الرقمية، حيث أنها تقدم نتائج واعدة في القطاع المالي على مستوى

العالم. بشكل عام، تساهم الطبيعة اللامركزية لبلوكتشين والتجزئة المشفرة والشفافية في رفع معايير الأمان للبيانات والمعاملات المالية، مما يجعلها أداة مهمة في حماية وأمان المعلومات المحاسبية الحساسة وكذلك حماية الأطراف على الشبكة، وذلك من خلال عدة طرق:

1. **التشفير القوي:** كافة البيانات والمعاملات على البلوكتشين مشفرة، مما يجعل من الصعب على المتسللين الوصول إلى المعلومات المحاسبية الحساسة أو تعديلها.
2. **اللامركزية:** البلوكتشين تقوم على شبكة موزعة من العقد (nodes) ، مما يعني أنه لا يوجد نقطة فشل واحدة يمكن استهدافها. هذا يحد من مخاطر الهجمات السيبرانية.
3. **الشفافية:** جميع المعاملات مسجلة بشكل دائم ومرئي للجميع، مما يقلل من فرص الاحتيال والتلاعب. يمكن للمراجعين تتبع كل معاملة بسهولة.
4. **المراجعة الفورية:** البلوكتشين توفر سجلات دقيقة وغير قابلة للتغيير، مما يسهل عملية المراجعة ويزيد من الثقة في البيانات المحاسبية والمالية.
5. **التوافق مع المعايير** :يمكن للبلوكتشين مساعدة الشركات في الامتثال للمعايير القانونية والتنظيمية من خلال توفير سجلات شفافة ودقيقة.

**باختصار**، تقنية البلوكتشين تعزز أمن المعلومات المحاسبية من خلال توفير بيئة أكثر أمانًا وشفافية وكفاءة.

ولكن من ناحية أخرى، على الرغم من أن تقنية البلوكتشين أحدثت ثورة في مختلف القطاعات، بصفة خاصة القطاع المالي والمحاسبي من خلال تقديم حلول مبتكرة، ولكنها جلبت أيضًا تحديات كبيرة للأمن السيبرانى . تشكل العلاقة المعقدة بين إدارة مخاطر الأمن السيبرانى والأهداف الاستراتيجية تحديًا كبيرًا في تحديد نقاط الضعف في الأمن السيبرانى وتحليلها والتحكم فيها في ظل تقنيات التحول الرقمي وبصفة خاصة تقنية البلوكتشين. تواجه المؤسسات المالية صعوبات في إدارة التكنولوجيا الجديدة وتخصيص الموارد بشكل فعال لتعظيم قيمة التقنيات الناشئة مثل تقنية البلوكتشين، والتي تبشر بضرورة تعزيز الأمن السيبرانى في المعاملات المالية. ومن هنا ظهرت هدف البحث للباحثة وهو أهمية مواءمة استراتيجيات الأمن السيبرانى مع الأهداف التنظيمية للتخفيف من المخاطر الأمنية السيبرانية بشكل فعال وضمان أمن المعاملات والبيانات المالية باستخدام تقنية البلوكتشين. يعد فهم هذه التحديات ومعالجتها أمرًا بالغ الأهمية للمؤسسات في القطاع المالي للاستفادة من إمكانات بلوكتشين مع حماية البيانات والمعاملات المالية.

### 5/2 أثر التحول الرقمي والتحديات التي تواجه تطبيقات تقنية البلوكتشين على بيئة الأعمال المحاسبية:

في بداية الثورة الصناعية الرابعة وظهور عصر التحول الرقمي والذكاء الاصطناعي وأتمتة العمليات وانتشار تقنية البلوكتشين، تباينت الأثار التكنولوجية على البيئة المحاسبية ما بين مزايا متعددة وثغرات أمنية كبيرة، يُمكن أن تؤدي لانتهاكات واختراقات وسرقات للمعاملات والبيانات المالية والأصول الرقمية للأطراف على الشبكة.

اقتصر الأمر في البداية على التعامل في العملات الافتراضية/ العملات المشفرة، إلا أنه مع انتشار تقنية البلوكتشين تعددت مجالات التطبيق والاستخدام وبصفة خاصة على مهنة المحاسبة، كي تعزز من كفاءة وأمان العمليات المالية والتعاقدية. على سبيل المثال: العقود الذكية، محاسبة القيد الثلاثي، والعملات المشفرة، كي تعزز وتيسر من التحول الرقمي الذي يجتاح مهنة المحاسبة.

فيما يلي توضيح لتطبيقات تقنية البلوكتشين التي أثرت على البيئة المحاسبية من حيث طبيعتها ومميزاتها وعيوبها:

**1/5/2 العقود الذكية:**

هي بروتوكول خاص يعمل بطريقة مشفرة، من خلال برمجيات قادرة على إرسال العقود من حساب شخص إلى حسابات آخر (مراح وطويلب، 2022)، بالتسجيل على منصات البلوكتشين دون تدخل طرف ثالث كموثق أو وسيط أو أي جهة مركزية، والقانون المرجعي لهذه العقود هو الكود (code).

أو بمعنى آخر، هي عقود ذاتية التنفيذ مع كتابة شروط الاتفاقية مباشرةً في التعليمات البرمجية. تقوم هذه العقود تلقائيًا بتنفيذ شروط الاتفاقية وتنفيذها عند استيفاء الشروط المحددة مسبقًا، دون الحاجة إلى وسطاء أو تدخل يدوي(Ivanov, et al., 2023). تتيح تقنية البلوكتشين نشر العقود الذكية وتنفيذها على شبكة لا مركزية، مما يوفر منصة غير قابلة للتلاعب ومراجعة المعاملات آلياً. يمكن للعقود الذكية تبسيط العمليات المالية المختلفة، مثل المدفوعات والتسويات وتحويلات الأصول، من خلال أتمتة تنفيذ الاتفاقيات التعاقدية بناءاً على شروط محددة مسبقًا. تضمن طبيعة تقنية البلوكتشين المقاومة للتلاعب أنه لا يمكن تغيير العقود الذكية أو التلاعب بها بمجرد نشرها، مما يوفر قدرًا أكبر من الأمان والثقة في المعاملات المالية. فهي تستخدم في مجالات محاسبية مختلفة، كتوثيق الممتلكات، إصدار القروض من البنوك، تحويل الأموال بين طرفين دون وسطاء، معالجة طلبات مبالغ التأمين من طرف مؤسسات التأمين وغيرها (مراح وطويلب، 2022) .

على صعيد أخر ترى الباحثة، أن العقود الذكية هي مفهوم أساسي يعزز مفهوم محاسبة القيد الثلاثي على نهج القيد المزدوج. على الرغم من توفير العقود الذكية لفوائد عديدة لتعزيز التدابير الأمنية للمعاملات المالية، لكنها تنطوي على ثغرات أمنية سيبرانية كبيرة، وهي:

- **الثغرات البرمجية:** حيث تعتمد العقود الذكية على الشفرات المبرمجة، وأي خطأ في هذه الشفرات يمكن أن يؤدي إلى انتهاكات أمنية، كسرقة الأصول الرقمية (Ivanov, et al., 2023)
- **عدم إمكانية التعديل:** بمجرد نشر العقد الذكي على المنصة، يصبح من الصعب تعديله .وبالتالي إذا تم اكتشاف أيه

(Zaazaa & Bakkali, 2023) أخطاء أو ثغرات بعد النشر فإن تصحيحها يصبح معقداً ومكلفاً

- **هجمات الـ51: %** إذا تمكنت مجموعة من المتسللين من السيطرة على أكثر من 51 %من شبكة البلوكتشين (Zaazaa & Bakkali, 2023) يمكنهم التلاعب بالعقود الذكية وتنفيذ معاملات غير مشروعة
- **هجمات إعادة التشغيل:** يمكن للمهاجمين استغلال الثغرات في العقود الذكية لتنفيذ نفس المعاملة عدة مرات (Zhang, et al., 2023) مما يؤدي إلى خسائر مالية كبيرة

**2/5/2 محاسبة القيد الثلاثي:**

الثلاثي الذي يقدم دفتر أستاذ مشترك يمكن مشاهدته لكافة القيد محاسبة على تقوم تقنية البلوكتشين كما تتم .(Han , et al., 2023) الأطراف داخل الشبكة، مما يُحسن من شفافية وثقة استخدام سجلات التحقق .الخصم والائتمان الحالية إلى قيود لشرحَ لإضافة دخل إضافي "trebit" إضافة طبقة ثالثة من الإدخالات تسمى ،وتختلف محاسبة القيد الثلاثي لأنه يوفر دليلاً قوياً من خلال إضافة إيصالات موقعة رقميًا يشاركها كل وكيل ومشاركة السجلات حيث يكون الإيصال موقع رقميًا هو المعاملة الثالثة، وبالتالي ضمان الثقة والشفافية في .(Cai,2021) السجلات المحاسبية

**اعتماداً على ماسبق ترى الباحثة،** أن محاسبة القيد الثلاثي تحقق نمطًا مستقلًا وآمنًا لتحسين موثوقية البيانات (McCallig, et al., 2019) كما أشار .المالية، ويزيد من مشاركة المعلومات المالية مع المشاركين على منصة أنه يمكن زيادة التمثيل المالي للتقارير بأمانة باستخدام البيانات المشتركة من الكيانات المستقلة، لما توفره تقنية البلوكتشين من نظام شفاف، وتخزين غير قابل للتغيير مفتوح الوصول.

تأسيساً على ما سبق **ترى الباحثة،** أنه سيكون لدى المؤسسات المختلفة احتياجات متعددة لأنظمة محاسبة ثلاثية القيد .على سبيل المثال، البنوك تحتاج متطلبات قانونية لتتبع المعاملات الفردية، بينما الشركات الأخرى لديها متطلبات أكثر إجمالاً .يجب أن يتناسب تصميم أنظمة المحاسبة ثلاثية الإدخال مع الغرض من استراتيجية العمل طويلة الأجل.

**على صعيد آخر ترى الباحثة،** على الرغم من توفير محاسبة القيد الثلاثي لفوائد عديدة لزيادة التدابير :الأمنية للمعاملات المالية ، لكنها تنطوي على ثغرات أمنية سيبرانية كبيرة، وهي

- **ضعف التحقق من الأخطاء** :تعاني نظم المحاسبة القائم على التسجيل الثلاثي من صعوبة في تتبع الأخطاء .(Petratos, 2024) مما قد يؤدي إلى صعوبة في التعرف على المخالفات والاحتيال
- **تعقيد العملية:** استخدام محاسبة القيد الثلاثي مازالت حديثة العهد في الممارسات لعملية لهذا تحتاج مزيدًا من الفهم والمعرفة التكنولوجية مقارنة بالطرق التقليدية، مما قد يجعلها تتطلب مهارات خاصة من .(Rahmawati, 2023)المحاسبين

- **الاعتماد على التكنولوجيا:** تعتمد محاسبة القيد الثلاثي على تقنيات التشفير والتوزيع بشكل كبير، مما يعرضها لمخاطر أمنية سيبرانية في حالة عدم تأمين هذه الأنظمة بشكل صحيح.
- **الهوية المجهولة:** عدم وجود هوية مركزية يمكن أن يسهل الأنشطة غير القانونية ويزيد من صعوبة تتبع المهاجمين(Petratos, 2024).

**2/5/3 العملات المشفرة:**

هي عملات افتراضية مشفرة تم تصميمها باستخدام تقنية البلوكشين، تعتمد على الشفافية والتشفير والتوزيع اللامركزي والتحقق الذاتي، ولا يتم إدارتها أو تنظيمها بواسطة الحكومات أو البنوك المركزية .على سبيل المثال: بيتكوين وإيثريوم وليتكوين .تحويل الأموال باستخدام العملات المشفرة يكون أسرع وأقل تكلفة مقارنة بالطرق التقليدية.

**على صعيد أخر ترى الباحثة،** على الرغم مما تتمتع به العملات المشفرة من فوائد عديدة لتعزيز أمن المعاملات المالية على منصة البلوكتشين، لكنها تنطوي على بعض الثغرات الأمنية، وهي كما ذكرها (Kalat,2020):

- التقلبات السعرية: تقلب أسعار العملات المشفرة بشكل كبير يجعلها استثمارًا محفوفًا بالمخاطر.
- الاستهلاك العالي للطاقة: تعدين العملات المشفرة عملية تتطلب كميات كبيرة من الطاقة، مما يثير مخاوف بيئية.
- استخدامات غير قانونية :العملات المشفرة قد تُستخدم في أنشطة غير قانونية بسبب صعوبة تتبعها.
- نقص التنظيم :عدم وجود تنظيم حكومي يمكن أن يؤدي إلى مخاطر إضافية للمستثمرين.

وتأسيساً على ماسبق ترى الباحثة، أن تقنية البلوكتشين هي تقنية متطورة، تلعب دورًا حيوياً ومحورياً لتطوير البيئة المحاسبية في ظل التحول الرقمي، فمن خلال توفير دفتر الأستاذ الموزع الغير قابل للتغيير نأمن لسلامة المعاملات، وإدارة لامركزية للهوية من أجل المصادقة الآمنة، والعقود الذكية للمعاملات الآلية والمقاومة للتلاعب، وبالتالي فهي منصة قوية لتأمين المعاملات والبيانات المالية. ومع استمرار المؤسسات في تطبيق تقنية البلوكتشين، يمكنها زيادة التدابير الأمنية والحد من المخاطر وتعزيز الثقة في النظام المالي.

ولكن على الجانب الآخر تقابل الشركات تحديات تقنية وتنظيمية وقانونية لاعتماد تقنيات البلوكتشين. على سبيل المثال، أكثر العقبات التي يتم مواجهتها هي اهلاك الطاقة، وسعة التخزين، والخصوصية، والقابلية للتوسع، والتشغيل البيني، والأمن السيبرانى(Han, et al., 2023, O'Leary, 2019) ، ودعم الإدارة العليا، والاستعداد التنظيمي، والوصول للأموال، وكفاءة التقنيات، وقضايا الحوكمة، والافتقار إلى توحيد قواعد البيانات المتسلسلة (Hilary& Liu, 2021).

**6/2 أثر الأمن السيبرانى على تعزيز تقنية البلوكتشين لحماية البيانات المالية والمحاسبية :**

**1/6/2 مفهوم الأمن السيبرانى:**

عرف المعهد الأمريكي للمحاسبين القانونيين المعتمدين AICPA الأمن السيبرانى بأنه مجموعة من الممارسات والإجراءات المصممة لحماية البيانات والمعلومات من التهديدات السيبرانية. (Daoud & Serag, 2022).

وقد طور المعهد الأمريكي الـ AICPA مجموعة من المعايير المتعلقة بالأمن السيبرانى للمحاسبين، مثل بيانات المعايير الخاصة بخدمات المحاسبة والمراجعة SSARS (Statements on Standards for Accounting and Review Services) ، والتي تساعد المحاسبين في تأمين بيئة الأعمال الرقمية وتطبيق تدابير فعالة للتحكم في الأمن وخصوصية البيانات. بهدف تعزيز الثقة في الأنظمة والعمليات التي تدعم تقديم الخدمات المهنية (www.aicpa.org) .. حيث يسعى المعهد الأمريكي AICPA من خلال هذه المعايير إلى مساعدة المؤسسات على حماية بياناتها وضمان استمرارية الأعمال. وتشمل هذه المعايير:

1. تقييم المخاطر: دراسة التهديدات المحتملة وتحديد المخاطر المرتبطة بالنظم والبيانات.
2. التحكم في الوصول: تنظيم من يمكنه الوصول إلى المعلومات الحساسة وكيفية استخدامها.
3. التشفير: استخدام الأساليب المشفرة بهدف حماية البيانات أثناء التخزين والنقل.
4. التوعية والتدريب: تعليم الموظفين حول أفضل الممارسات للأمان السيبرانى وكيفية التعرف على الهجمات.
5. الاستجابة للحوادث: وضع خطط للاستجابة السريعة والفعالة عند حدوث خرق أمني.

عرفت هيئة الأوراق المالية والبورصات(SEC) الأمن السيبرانى: هو حماية الأنظمة والشبكات والبيانات الرقمية من الهجمات الإلكترونية، والوصول غير المصرح به. بمعنى آخر، تهتم هيئة الأوراق المالية والبورصات (SEC) بالأمن السيبرانى في سياق حماية المعلومات الحساسة للمستثمرين والشركات المسجلة لديها (Rabinowitz,2020).

حيث هدفت هيئة الأوراق المالية والبورصات(SEC) إلى:

أ) حماية المستثمرين : من خلال حماية المستثمرين من خسائر الهجمات السيبرانية التي قد تؤثر على سلامة البيانات المالية أو تشوه المعلومات المتاحة للمستثمرين لاتخاذ قرارات استثمارية.

ب) ضمان سلامة الأسواق: ت من خلال ضمان سلامة وشفافية أسواق الأوراق المالية من خلال منع التلاعب بالأسعار أو نشر معلومات مضللة نتيجة للاختراقات السيبرانية.

ج) الحفاظ على الثقة في الأسواق: يساهم الأمن السيبرانى القوي في تعزيز ثقة المستثمرين في الأسواق المالية، مما يشجع على الاستثمار ويدعم النمو الاقتصادي.

عُرف الأمن السيبرانى وفقا لـ COBIT (Control Objectives for Information and Related Technologies) وهو إطار عمل لإدارة تقانة المعلومات، أنشأته منظمة المراجعة والتحكم في نظم المعلومات ISACA ( Information Systems Audit and Control Association) ، بأنه إطار عمل يهدف إلى إدارة وحوكمة تكنولوجيا المعلومات في المؤسسات، تم تطويره من قبل جمعية ISACA ويعد أداة قياسية لتوجيه المؤسسات عن كيفية إدارة التكنولوجيا المعلوماتية بطريقة تحقق الأهداف التجارية. وتتمثل فوائده في :

1) تحسين إدارة المخاطر: يساعد COBIT المؤسسات على تحديد وإدارة المخاطر المرتبطة بتكنولوجيا المعلومات.
2) تعزيز الفعالية :من خلال تقديم إطار عمل منظم، يساعد COBIT على تحسين الكفاءة التشغيلية.
3) تحقيق الأهداف التجارية : يعزز من توافق تكنولوجيا المعلومات مع أهداف الأعمال، مما يساهم في تحقيق النجاح المؤسسي.

يساهم إطار عمل تقانة المعلومات COBIT بشكل كبير في تعزيز الأمن السيبرانى من خلال التركيز على:

- تحديد نتائج أمان المعلومات: مثل السرية، والنزاهة، وتوافر البيانات.
- إدارة العمليات والموارد: ما يضمن اتخاذ تدابير أمنية فعالة.
- استجابة الحوادث: من خلال تقديم إرشادات لإدارة المواقف السيبرانية والتعافي منها.

**مما سبق يتضح للباحثة،** أن إطار عمل تقانة المعلومات COBIT يوفر إطارًا شاملًا للمؤسسات لتوجيه أعمالها لتكنولوجيا المعلومات، مع التركيز على تحسين الأداء، وتقليل المخاطر، وتعزيز الأمن السيبرانى.

بينما عرف المعهد الوطنى للمعايير والتكنولوجيا (NIST) وهو مؤسسة أمريكية تقدم إرشادات وأطر عمل للأمان السيبرانى. واحدة من أهم إصدارات NIST للأمان السيبرانى(NIST Cybersecurity Framework) ، الذي يهدف إلى تحسين القدرة على إدارة مخاطر الأمان السيبرانى، وتمثلت العناصر الأساسية لإطار عمل الأمن السيبرانى في (Krumay, et al.,2018):

1) تحديد(Identify) : فهم المكونات والموارد التي تحتاج إلى حماية، وتقييم المخاطر المرتبطة بها.
2) حماية(Protect) : اعتماد التدابير الملائمة لضمان سلامة الأنظمة والمعلومات.
3) كشف(Detect) : تطوير أنظمة لمراقبة الأنشطة الحادثة والتعرف على التهديدات.
4) استجابة(Respond) : وضع خطة للاستجابة للحوادث عند حدوثها وتقليل أثرها.
5) استعادة (Recover) : إنشاء استراتيجيات للعودة إلى العمليات الطبيعية بعد الحادث.

كما قامت منظمة المعايير الدولية (ISO) بوضع مجموعة من المعايير للأمن السيبرانى، وأحد المعايير الأكثر شهرة هو معيار ISO/IEC 27001 ، والذي يحدد متطلبات نظام إدارة أمن المعلومات (ISMS) ويساعد على إدارة الأصول المعلوماتية بشكل آمن. وتتمثل عناصر معيار ISO/IEC 27001 في:

أ) تقييم المخاطر: إجراء تحليل شامل للمخاطر المحتملة على المعلومات وتحديد الإجراءات اللازمة لإدارتها.
ب) سياسات أمن المعلومات: تطوير سياسات واضحة توضح كيفية إدارة المعلومات وحمايتها.
ج) التوعية والتدريب: تدريب الموظفين على كيفية التعرف على التهديدات والحفاظ على الأمان.
د) تقييم الأداء: قياس وتحليل أداء نظام إدارة أمن المعلومات بشكل دوري.

ترى الباحثة أنه تباينت وجهات النظر بين الجهات التي وضعت مفهوم ومعايير للأمن السيبرانى، يمكن توضيحها كما يلي:

| المعيار | AICPA | الجهات والمنظمات الدولية (ISO, NIST, COBIT) |
|---|---|---|
| التركيز | المحاسبون والبيانات المالية | الأمن السيبرانى بشكل عام |
| النطاق | أضيق، يركز على احتياجات المحاسبين | أوسع، يشمل جميع القطاعات |
| المعايير | SSARS، Trust Services Principles | ISO/IEC 27001، NIST Cybersecurity Framework، COBIT |
| الهدف | ضمان سلامة البيانات المالية والعمليات المالية | حماية الأصول الرقمية بشكل عام |

**و يمكن للباحثة تعريف الأمن السيبرانى** بأنه هو مجموعة من الممارسات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبرمجيات من الهجمات الرقمية، سواء كان ذلك من خلال تقنيات القرصنة، أو البرمجيات الضارة، أو أي نوع آخر من التهديدات. يهدف الأمن السيبرانى إلى الحفاظ على سرية وسلامة المعلومات، ويشمل مجموعة مختلفة من التهديدات مثل:

- **البرمجيات الضارة:** مثل الفيروسات، وبرامج الفدية.
- **الهجمات المستهدفة:** مثل هجمات التصيد الاحتيالي وهجمات يوم الصفر.
- **المشكلات المتعلقة بالسرية:** كتسريبات البيانات.
- **فقدان الخدمة:** كهجمات DDoS النفي الموزع للخدمة.

وجدير بالذكر أنه من الأهمية للمحاسبين فهم هذه المعايير وتطبيقها للحفاظ على سلامة المعلومات والامتثال للمتطلبات القانونية والتنظيمية المتعلقة بالأمن السيبرانى.

### 2/6/2 دور الأمن السيبرانى على تعزيز تقنية البلوكتشين:

تلعب تقنية البلوكتشين Blockchain دورًا حيوياً في تعزيز الأمان السيبرانى في مجال المحاسبة. حيث تتميز تقنية البلوكتشين بالعديد من الفوائد التي تجعلها ملائمة لتطبيقات الأمان السيبرانى، خاصة في ظل المعاملات المالية وتخزين البيانات الحساسة.

**تأسيساً على ما سبق عرضه، توصلت الباحثة** أن تقنية البلوكتشين تعزز من مقاومة التلاعب بسبب ميزات الأمان المتأصلة فيها مثل آليات التشفير والبنية اللامركزية وخوارزميات الإجماع. يضمن استخدام دوال التجزئة الرياضية في البلوكتشين ثبات البيانات، مما يجعل أي تعديلات واضحة من خلال مخرجات تجزئة مختلفة اختلافًا جذريًا (Han, et al., 2023). بالإضافة إلى ذلك، تمنع الطبيعة اللامركزية لتقنية البلوكتشين من إنشاء أو تغيير المعاملات على الشبكة بواسطة أحد الأفراد دون موافقة باقي أعضاء الشبكة، مما يعزز الأمن والشفافية (Hilary, Liu, 2021). تتطلب خوارزميات الإجماع، سواء كانت قائمة على الإثبات أو قائمة على المؤسسة، التحقق من صحة العديد من الأفراد قبل إضافة كتلة إلى السلسلة، مما يزيد من تأمين سلامة البيانات. هذه المميزات مجتمعة تجعل تقنية البلوكتشين مقاومة للتلاعب، وهكذا فهي تعتبر منصة آمنة وموثوقة لكافة التطبيقات، بما في ذلك أمن الشبكة، والتحقق من صحة المعاملات، والتحقق من سلامة البيانات.

وعلى الجانب الأخر، يلعب الأمن السيبرانى دورًا حاسماً في حماية أمن البيانات المحاسبية والمالية من خلال تنفيذ آليات دفاع استباقية ضد التهديدات الرقمية والأنشطة الاحتيالية. حيث يحمي الأمن السيبرانى البيانات والمعاملات المالية بواسطة تشفيرها للحد من مخاطر الهجمات الإلكترونية، وضمان بيئة رقمية آمنة، وهو أمر هام جداً لحماية المعلومات المحاسبية والمالية الحساسة (Jadwani, et al., 2024).

كما تعد الضوابط المحاسبية في منظمات التقاعد ضرورة للتاكد من دقة وسلامة المعلومات المالية، متضمنة ممارسات الفصل بين الواجبات وعمليات المراجعة الداخلية والتسويات المنتظمة لمنع الأخطاء والاحتيال والوصول غير المصرح به إلى السجلات المالية (Frank, et al., 2019)

تقوم ضوابط الأمن السيبرانى على حماية الأنظمة والأصول والبيانات الرقمية من التهديدات السيبرانية والوصول غير المصرح به، تتضمن عناصر التحكم هذه تقنيات مثل التشفير والبلوكتشين واكتشاف أي تلاعب أو تغيير للتقليل من المخاطر السيبرانية وتعزيز أمن البيانات.

وقد أشار (Anyanwu ,et al., 2024, Temitayo, et al., 2023) أن بيئة الأعمال المحاسبية التكنولوجية المتطورة تتطلب لمواجهة التهديدات السيبرانية دمج التقنيات المتقدمة مثل: التشفير والبلوكتشين والتحليلات القائمة على الذكاء الاصطناعي لتعزيز سرية البيانات وسلامتها داخل الأنظمة المالية. حيث يجب على المؤسسات المالية اعتماد أطر الأمن السيبرانى الشاملة التي تشمل تشفيرًا قويًا للبيانات والمصادقة متعددة

العوامل وأنظمة كشف اختراق المعلومات المحاسبية والمراقبة الأمنية المستمرة للحد من المخاطر ومنع الاحتيال المالي (Iryna, 2023).

كما تتفق الباحثة مع أن استخدام الذكاء الاصطناعي والتعلم الآلي يعزز قدرات أنظمة الأمن السيبرانى في اكتشاف المخالفات والهجمات المحتملة، مع التأكيد على أهمية النهج الاستباقي والديناميكي لتأمين معلومات العميل والحفاظ على الثقة في القطاعات المالية (Dorosh, 2023)

أكد (Frank, et al., 2019) على أهمية المواءمة الاستراتيجية للمحاسبة والأمن السيبرانى، مشيراً إلى أن إصدار تقرير الإدارة دون ضمان يكون أكثر فعالية عندما لا تكشف الشركة عن هجوم إلكتروني سابق. علاوة على ذلك، فإن إصدار الإدارة لتقرير مستقل عن ضمان الأمن السيبرانى قد يزيد من قدرة الشركة على جذب الاستثمار.

جدير بالذكر أن الضوابط المحاسبية تساعد في إدارة المعلومات المالية بدقة، بينما تحمي ضوابط الأمن السيبرانى هذه البيانات من التهديدات الإلكترونية، مما يضمن الأمن العام وسلامة السجلات المالية للمؤسسة. حيث تحدد تنظيمات المحاسبة، مثل المعايير الدولية لإعداد التقارير المالية (IFRS) والمبادئ المحاسبية المقبولة (GAAP) القواعد الأساسية لشفافية ودقة إعداد التقارير المالية. ومن ناحية أخرى، تُحدد تنظيمات الأمن السيبرانى، ممثلة بمعايير مثل ISO 27001 وإطار عمل NIST للأمن السيبرانى، الأسس اللازمة لحماية الأصول الرقمية والمعلومات الحساسة، وضمان سرية البيانات وسلامتها وتوافرها (Musa, 2019).

تهدف كلا من المحاسبة والأمن السيبرانى إلى الحفاظ على ثقة أصحاب المصلحة – سواء في دقة التقارير المالية أو التعامل الآمن مع المعلومات الحساسة (Benaroch, 2020) . وهو ما يعد تحدياً للمواءمة بين متطلبات الإبلاغ المالي الصارمة والحاجة إلى تدابير قوية للأمن السيبرانى. فيجب على المنظمات التنقل في توازن دقيق لضمان الامتثال دون التضحية بالأمن أو الشفافية المالية (Hassan, and Ahmed, 2023).

يعد تنفيذ نهج متعدد الأبعاد يدمج التقنيات المتقدمة والضوابط المحاسبية التقليدية أمرًا أساسيًا لإنشاء دفاع مرن ضد التهديدات الإلكترونية في قطاع التقاعد. يتضمن هذا النهج برامج تدريب الموظفين واستراتيجيات الاستجابة للحوادث وتقييمات المخاطر من طرف ثالث كمكونات أساسية لوضع الأمن السيبرانى الشامل لإدارة حوادث الأمن السيبرانى والتخفيف من حدتها بشكل فعال.

قد حدد (Lehenchuk, et al., 2021) قائمة شاملة بالوسائل التي تضمن سلامة المعلومات المحاسبية في ظل الأمن السيبرانى، ومن بين التدابير الفعالة:

- استخدام وإعداد نظام مناسب للسيطرة على البيانات المحاسبية، والذي ينص على وسائل مستقلة للضوابط والموازنة.
- تحديد المسئولية المهنية للمحاسبين لضمان التحكم السليم في البيانات.

- تطوير آلية لتحديد التناقضات بين الوثائق الأولية والحسابات والتقارير، ويجب توفير الظروف اللازمة لاتخاذ الإجراءات التصحيحية إذا لزم الأمر.
- ضمان الحماية السيبرانية المناسبة لنظم المحاسبية وغيرها من نظم المعلومات الخاصة بالمؤسسة، والتي تستخدم لإعداد المعلومات المحاسبية.
- تحسين واجهة برامج المحاسبة بهدف تنفيذ وظائف التحكم التي توفر المزامنة والتنسيق للبيانات المحاسبية في الأنظمة الفرعية المختلفة.
- استخدام قنوات اتصال موثوقة ومستقرة وآمنة لنقل السجلات .

**تعقيب على الاطار النظري:** ترى الباحثة أن التحول الرقمي في ظل تقنية البلوكتشين تساهم بشكل كبير في تحسين أمن وشفافية بيئة الأعمال المحاسبية، من خلال تعزيز أمان المعاملات المالية والخصوصية والسرية، والحد من المخاطر السيبرانية، والتكامل مع الذكاء الاصطناعى بهدف دعم الدفاعات السيبرانية.

**3/ الإطار المنهجي للبحث**

يتم في هذا القسم عرض لإجراءات البحث النوعية، والتى تقوم على جمع البيانات من خلال المقابلات النوعية شبة المنظمة Semi-structured interviews والأسئلة المفتوحة لتحقيق هدف البحث، ثم تحليل محتواها باستخدام برنامج تحليل البيانات النوعي MAXQDA 2024 .

**1/3 أداة ومنهج البحث:**

البحث الحالي ليس من فئة البحوث الكمية Research Quantitative، بل من فئة البحوث الاستكشافية أو النوعية Research Qualitative التي تركز علي فهم وشرح واستطلاع، واكتشاف وتوضيح التصورات والمواقف والقيم والمعتقدات والخبرات ذات الصلة بمشكلة البحث.

وقد تعمدت الباحثة إختيار منهج البحث النوعي الذي يقوم على المقابلات شبه المنظمة وطرح الأسئلة المفتوحة نظراً لحداثة الموضوع محل البحث، كما أنه يسمح للباحثة باستخلاص المزيد من المعلومات من المشاركين ومتابعة الإجابات على تلك المعلومات من خلال إضافة أسئلة أثناء المقابلة، لأن منهجية البحث تتمثل قدر الامكان في استطلاع رأي الخبراء حول الموضوع محل البحث وخبراتهم (Creswell & Clark, 2018) .

يعد برنامج التحليل النوعي للبياناتMAXQDA وهو اختصار لـ Maximum Qualitative Data Analysis من أحدث برمجيات تحليل البيانات النوعية الرائدة التي تلقى قبولاً ورواجاً واسعاً في الأونة الأخيرة. وقد اعتمدت الباحثة في تحليل بيانات المقابلات على برنامج MAXQDA 2024، والذي تراه الباحثة اختيارًا مناسبًا وحديثاً لتقييم البيانات النوعية. نظراً لتميزه بسهولة الاستخدام وقدرته على التعامل مع مجموعة متنوعة من أنواع

البيانات. ويتميز برنامج MAXQDA بالقدرة على إدارة البيانات بكفاءة، والترميز المرن، وإنشاء السمات، وإنشاء تصور لأنواع البيانات، وترميز النصوص.

### 2/3 مجتمع وعينة البحث:

**مجتمع البحث:** يتمثل مجتمع البحث في الخبراء والمهنيين من المحاسبين المحترفين وخبراء الأمن السيبرانى والبلوكتشين وأعضاء هيئة التدريس بالجامعات، وقد تم الاتصال بالمشاركين تليفونياً وعبر البريد الإلكتروني وتليجرام وصفحة لينكدإن Linked IN الخاصة بهم لطلب موافقتهم. ركزت المقابلات على مجموعة من الأسئلة الموجهة حول فهم المشاركين لتقنيات البلوكتشين ومخاوف الأمن السيبرانى التي تظهر عند تبني هذه التقنية في مجال المحاسبة.

**عينة البحث:** استخدمت الباحثة طريقة أخذ عينات كرة الثلج Snowball sampling لتحديد المشاركين المحتملين في البحث، حيث تعتبر طريقة أخذ عينات كرة الثلج طريقة فعالة للوصول إلى المشاركين الذين يصعب العثور عليهم (Biernacki & Waldorf, 1981)، حيث تعتمد هذه الطريقة على أفراد العينة أنفسهم لترشيح أفراد جدد لإضافتهم إلى العينة(Creswell & Creswell, 2017). بالاضافة إلى الطريقة العمدية لاختيار مشاركين ذو خصائص معينة.

كما قامت الباحثة بالتزامن مع استخدام طريقة العينة العمدية وطريقة كرة الثلج باستخدام طريقة العينات المتتالية للوصول الى التشبع النظري. حيث يتضمن ذلك مطالبة المشاركين المحتملين باقتراح مشاركين إضافيين يستوفون معايير البحث. وقد ساعد هذا في الحصول على المزيد من الخبراء من شبكات المشاركين.

**وقد اختارت الباحثة** أولاً عينة صغيرة من المشاركين الذين يستوفون أهداف البحث، ثم اقترح هؤلاء المشاركون المختارون مجموعة أخرى من المشاركين ذوى الخبرة أو الخلفية ذات الصلة بهدف البحث. ولقد استقرت الباحثة على إجراء مقابلات مع **اثني عشر** خبيرًا في مجال الأمن السيبرانى والبلوكتشين والمحاسبة. تم تحديد الفئات المستهدفة التي كانت على استعداد للمشاركة في هذه البحث ولديهم علم وخبرة بالمجال المحاسبي والتقنيات الحديثة في تكنولوجيا البلوكتشين والعملات المشفرة وخبراء الأمن السيبرانى، من خلال استخدام عينات غير احتمالية هادفة (عمدية/ مقصودة) يتبعها أخذ عينات متتالية.

### 3/3 نموذج البحث:

#### أ) جمع البيانات

تم إجراء المقابلات هاتفياً وتسجيلها صوتياً، ثم نسخ جميع ما ذكر في التسجيلات إلى برنامج Microsoft Word حيث أصبحت المقابلات مكتوبة حرفياً. ثم قامت الباحثة بعملية تنظيف البيانات حيث ثم استبعاد البيانات

غير اللازمة والتي لا تتفق مع هدف البحث، وقامت الباحثة بتحميل جميع الملفات والنصوص المكتوبة إلى برنامج MAXQDA للبدء في عملية ترميز للبيانات (Coding) ثم فرزها في مجموعات واعطاء كل مجموعة رمز (code). لاستخدام هذا الترميز في استخراج النتائج النهائية للدراسة أو ما يعرف بـ (themes).

**ب) اختبار صدق وثبات أداة البحث:**

تحققت الباحثة باستخدام برنامج MAXQDA من دقة النتائج ومصداقيتها من خلال تنفيذ إجراءات معينة مثل رأي الخبراء وعينات أخرى (Creswell and Clark, 2018) أو ما يعرف بأسلوب member check للتحقق من صدق أداة البحث ، فمن خلال هذا الأسلوب يستطيع الباحث التأكد وتحسين دقة ومصداقية ما تم تسجيله أثناء المقابلات البحثية، وبشكل تفصيلي يمكن وصف هذا الأسلوب بأنه يقوم بتحليل البيانات واستخراج النتائج أو ما يعرف بـ (themes) ومن ثم إعطائها لمحكمين خارجيين من ذوي الخبرة لإعادة النظر في طريقة تحليل البيانات ومقارنة النتائج (Harper & Cole, 2012).

لتحديد موثوقية البحث، وثقت الباحثة إجراءات البحث وخطوات الإجراءات، فقد تم إجراء مقابلات شبه هيكلية بأسئلة مفتوحة، كانت البيانات التي تم جمعها موثوقة لنتائج البحث. قامت الباحثة بتدوين الملاحظات وتسجيل المقابلات وتم نسخ المقابلات، وتم تحديد جميع المصطلحات بوضوح لتجنب الارتباك.

**ج) خطوات تحليل البيانات :**

قامت الباحثة بتحليل البيانات النوعية باستخدام برنامج MAXQDA، حيث يتميز البرنامج بإمكانية تحديد الموضوعات والموضوعات الفرعية والرموز والمجموعات لتنظيم العديد من خطوات التحليل بشكل أكثر منطقية. وقد ساعد هذا في تحديد المصطلحات التي يستخدمها المشاركون في البحث بشكل متكرر. فعلى سبيل المثال، يجعل برنامج MAXQDA من السهل إنشاء تمثيل مرئي للنص. ويساعد البرنامج في قراءة البيانات بطريقة أكثر فعالية، حيث يقوم بتبسيط عملية مقارنة نتائج التجارب وجعل ذلك ممكنًا من خلال استخدام واجهة مرئية يقدمها البرنامج. وقد قامت الباحثة بذلك وفقاً للخطوات التالية :

1. **إعداد البيانات:** وتم ذلك من خلال:

أ- **استيراد البيانات:** قامت الباحثة باستيراد البيانات الخام إلى البرنامج، سواء كانت نصوصًا، أو ملفات صوتية، أو مقاطع فيديو، حيث يدعم MAXQDA مجموعة واسعة من صيغ الملفات سواء Excel, Word, Pdf, audio,

ب- **تنظيم البيانات:** قامت الباحثة تنظيم البيانات في مشروع واحد، وتم تسمية الملفات بشكل واضح ومترابط

2. **الترميز:** وتم ذلك من خلال:

أ- **إنشاء الرموز:** قامت الباحثة إنشاء رموز (Codes) تعبر عن المفاهيم الرئيسية والفرعية التي تبحث عنها في البيانات.

ب- **تطبيق الرموز:** قامت الباحثة بتطبيق هذه الرموز على الأجزاء ذات الصلة من النصوص، أي وضع علامة على كل جزء يتعلق برمز معين. يمكن للرمز أن يكون كلمة واحدة، أو عبارة، أو حتى فقرة كاملة.

ج-**الترميز المفتوح والمحوري:** يمكنك البدء بالترميز المفتوح (Open Coding) حيث تقوم بتحديد الرموز بشكل عفوي أثناء قراءة البيانات، ثم الانتقال إلى الترميز المحوري (Axial Coding) حيث تقوم بتجميع الرموز ذات الصلة في فئات أوسع.

3. **البحث:** وتم ذلك من خلال:

أ- **البحث عن الرموز:** قامت الباحثة باستخدام أدوات البحث المتقدمة في البرنامج للبحث عن رموز معينة، أو مجموعات من الرموز، أو حتى عبارات نصية محددة.

ب- **إنشاء المصفوفات:** قامت الباحثة إنشاء مصفوفات (Matrices) لعرض العلاقات بين الرموز المختلفة، مما يساعد على فهم العلاقات المعقدة بين المفاهيم.

4. **التحليل:** وتم ذلك من خلال:

أ- **إنشاء الشجرات المفاهيمية:** قامت الباحثة إنشاء شجرات مفاهيمية (Concept Trees) لتصور الهيكل المفاهيمي للبيانات، وكيف ترتبط الرموز المختلفة ببعضها البعض.

ب- **إنشاء الشبكات:** قامت الباحثة إنشاء شبكات (Networks) لعرض العلاقات بين الرموز بشكل مرئي، مما يساعدك على تحديد الأنماط والاتجاهات.

5. **التفسير والتقرير:**

أ- **تفسير النتائج:** قامت الباحثة تفسير النتائج التي حصلت عليها، وربطها بسياق هدف البحث وسؤال البحث الرئيسي.

ب- **كتابة التقرير:** قامت الباحثة بكتابة تقرير بحثي شامل يقدم نتائج التحليل بشكل واضح وموجز.

**د) خطوات تحليل بيانات البحث:**

هدفت هذه البحث إلى مناقشة تقنيات الأمن السيبرانى لتعزيز تبني تقنية البلوكتشين في مهنة المحاسبة. بالإضافة إلى مناقشة التحديات الأمنية الناتجة عن تطبيق البلوكتشين وتأثيرها على العمليات المحاسبية والقوائم المالية. تم إجراء اثنا عشر مقابلة مع خبراء المحاسبة والبلوكتشين والأمن السيبرانى، ناقش تحليل البيانات استجابات المقابلات مع المشاركين، تم فحص الخصائص الديموغرافية للمشاركين ومجال خبراتهم في الجدول(1)، مع الحفاظ على سرية هوية المشاركين، وتم استبدال أسماء المشاركين بحروف من (A : L) ، تم فحص استجابات المشاركين لكل سؤال بحثي. كما تم تغطية ملفات جداول التعليمات البرمجية وملفات جداول الاقتباس، بحيث يتلقى كل موضوع بحثي توحيدًا للأفكار وتقييم البيانات، تم إجراء مجموعة من اثني عشر مقابلة، تم تسجيل جميع المقابلات ثم تم تفريغ الاجابات وفقًا للنهج الخاص بتحليل المحتوى النوعي باستخدام برنامج MAXQDA 2024.

**جدول1:** الخصائص الديموغرافية للمشاركين في عينة البحث

| اسم المشارك | الفئة العمرية | المنصب | سنوات الخبرة | مجال العمل أو الخبرة |
|---|---|---|---|---|
| المشاركA | 40-50 | الرئيس التنفيذي لإحدى الشركات التكنولوجية | 2 | أكاديمي ومسئول مالي |
| المشاركB | 40-50 | المدير المالي والمحاسبي لإحدى الشركات | 3 | المحاسبة |
| المشاركC | 30-40 | كبير موظفي أمن المعلومات لإحدى الشركات | 2 | التكنولوجيا والأمن السيبرانى |
| المشاركD | 30-40 | مطور تكنولوجيا البلوكتشين | 4 | المحاسبة |
| المشاركE | 20-30 | مهندس شبكات | 6 | الأمن السيبرانى |
| المشاركF | 20-30 | خبير في سلاسل التوريد والتكنوجيا الرقمية | 5 | **أكاديمي وسلاسل التوريد والبلوكتشين** |
| المشاركG | 40-50 | اكاديمي في مجال نظم المعلومات الأعمال | 5 | أكاديمي والمحاسبة والبلوكتشين |
| المشاركH | 40-50 | أكاديمي في المحاسبة | 7 | أكاديمي |
| المشاركI | 20-30 | أكاديمي في نظم المعلومات | 7 | أكاديمي |
| المشاركJ | 40-50 | محاسب وخبير مالي | 8 | المحاسبة والبلوكتشين |
| المشاركK | 40-50 | أستاذ مساعد في تكنولوجيا المعلومات IT | 7 | الأمن السيبرانى والبلوكتشين وأكاديمي |
| المشاركL | 30-40 | خبير في العملة المشفرة | 4 | الأمن السيبرانى/ العملة المشفرة |

أسفرت الأسئلة البحثية الثلاثة الرئيسية عن استنباط ثمانية أسئلة فرعية أثناء المقابلات، أجاب عليها كل مشارك أثناء المقابلة أو المحادثة التي استغرقت من 45 إلى 60 دقيقة. كان المشاركون في البحث خبراء في الأمن السيبرانى والمحاسبة والبلوكتشين. تم توجيه المقابلات للوصول إلى التشبع النظري، والذي عرفه (Saunders, et al. 2018) بأن تشبع البيانات هو المكان الذي لا تظهر فيه أفكار جديدة حول أسئلة البحث. **وقد تمثلت الأسئلة الرئيسية للمقابلات في الأسئلة الثلاثة الآتية:**

(Q1): ما هو التحول الرقمي بصفة خاصة تقنية البلوكتشين، وما أثره علي مهنة المحاسبة؟

(Q2): ماهي التدابير الأمنية المتبعة في تقنية البلوكتشين لضمان حماية البيانات والمعاملات؟

(Q3): كيف يمكن تعزيز الأمن السيبرانى عند تطبيق تقنية البلوكتشين في المحاسبة؟

تم استخدام العينة الهادفة والعينة المتقطعة لتحقيق التجانس الديموغرافي للمشاركين، مما دعم الإطار النظري، لم يتم النظر في العمر أو الجنس أو أي سمة أخرى في هذه البحث. علاوة على ذلك، تم إجراء أخذ عينات متعمدة غير احتمالية في هذه البحث بحجم عينة يبلغ اثني عشر. بالإضافة إلى ذلك، من الصعب مقارنة مجتمع البحث بمجتمع أوسع لأن هناك دراسات أكاديمية محدودة حول تقنيات الأمن السيبرانى عند تبني تقنية البلوكتشين في مجال المحاسبة.

تم تمثيل التحليل النوعي للمحتوى في المقابلات في سحابة كلمات Worldcloud تولد تمثيلًا مرئيًا للكلمات الأكثر استخدامًا أو تكراراً في المقابلات، كما هو موضح في الشكل (1). يرتبط حجم كل كلمة في السحابة بتكرارها في ملف المقابلة لكل مشارك. يزداد تكرار الكلمة في المقابلات مع توسع حجمها في سحابة الكلمات. كلما زاد حجم الكلمة في سحابة الكلمات، زاد تكرار ظهورها في المقابلات. وهو ما يمكن ايضاحه في الشكل (2) (السحابة المرئية لمقابلات المشاركين في البحث). والتي تعبر عن تكرار (أهمية وتداخل) كل كلمة في مقابلات المشاركين.


**الشكل 1:** تمثيلًا مرئيًا لسحابة كلمات

**وفيما يلي عرض للأسئلة البحثية الرئيسية وما تم استنباطه من أسئلة فرعية أثناء المقابلات:**

**(Q1): كيف تعمل تقنية البلوكتشين Blockchain وماهو أثرها على مهنة المحاسبة؟**

وعند قيام الباحثة بتكويد إجابات هذا السؤال لاحظت تكرار الحديث عن المفاهيم أو العناصر التالية، وهي:

(1) أمن البلوكتشين والتشفير

(2) آليات الإجماع في البلوكتشين

(3) الأصول والمعاملات الرقمية على البلوكتشين

(4) الشفافية والتحكم في الوصول.

**فيما يلي ما تم استنباطه من إجابة كل مشارك عن السؤال الأول**

| | |
|---|---|
| المشاركA | تكنولوجيا شفافة وموزعة توزع المعلومات عبر مشاركين متعددين وتستخدم آليات الإجماع وحوافز التكنولوجيا. |
| المشارك B | قاعدة بيانات شفافة مقاومة للتلاعب يصعب للغاية حذف المعلومات وتعديلها. |
| المشارك C | دفتر أستاذ موزع شفاف مقاوم للتلاعب |
| المشاركD | دفتر أستاذ موزع، وقاعدة بيانات محاسبية ثلاثية القيد يمكن للجميع الوصول إليها. |
| المشاركE | سلسلة من العمليات لإجراء المعاملات واستلامها، كما أنها شفافة وتعتمد على الأصول الرقمية |
| المشاركF | دفتر شفاف عالمي، مثل جدول بيانات Excel حيث يمكن أن تكون كل معاملة واحدة للبلوكتشين شفافة للجميع إذا كانت تريد ذلك |
| المشاركG | محاسبة القيد الثلاثي وتجعل كل شيء متاحًا للجمهور. |
| المشاركH | دفتر أستاذ موزع |
| المشاركI | دفتر أستاذ لامركزي. |
| المشاركJ | لا يختلف عن جدول بيانات Excel، إنه فقط موزع عبر عقد متعددة ويأتي مع ذلك الكثير من التداعيات الأمنية والقدرة على التحقق من صحة المعاملات. |
| المشاركK | يهدف القيد الثلاثي إلى استخدام خوارزميات تشفير تعتمد على شبكات موزعة لامركزية حيث لا تتطلب العقد ثقة طرف ثالث. |
| المشاركL | تقنية موزعة تسمح بتخزين البيانات عبر شبكة من أجهزة الكمبيوتر بطريقة آمنة ومقاومة للتلاعب، والتي ترتبط ببعضها البعض وتؤمنها باستخدام تقنيات التشفير. |

**<u>وأثناء الإجابة على السؤال الرئيسي الأول(Q1) قامت الباحثة بطرح ثلاث أسئلة فرعية، وهي:</u>**

**(Q11):** كيف يتم استخدامه تقنية البلوكتشين لخدمة مهنة المحاسبة حالياً أو مستقبلاً؟

**(Q12):** ماهو تأثير تقنية البلوكتشين على مستقبل وظائف المحاسبة والمراجعة؟

**(Q13):** كيف تختلف تقنية البلوكتشين عن الطرق التقليدية في المحاسبة؟

**وعند قيام الباحثة بتكويد إجابات السؤال الفرعي:**

**(Q11): كيف يتم استخدامه تقنية البلوكتشين لخدمة مهنة المحاسبة حالياً أو مستقبلاً؟**

لاحظت الباحثة تكرار الحديث عن أربعة مواضيع وقد قامت بتكويدهم ، وهي:

(1) أدوات وإجراءات التحول

(2) تقنية البلوكتشين كآلية للتحقق.

(3) المحافظ الرقمية والعملات المشفرة

(4) تحديات واعتبارات التنفيذ.

**فيما يلي إجابة كل مشارك عن هذا السؤال الفرعي (Q11)**

| | |
|---|---|
| المشارك C | أعتقد أن شركات المحاسبة يجب أن تستكشف فوائد استخدام العقود الذكية في عمليات المراجعة. فيمكن أن تكون بمثابة أداة لمراجعة وضمان دقة تنفيذ التعليمات البرمجية. |
| المشارك D | يمكن للعقود الذكية أتمتة العديد من العمليات، مثل توليد الفواتير وعمليات الدفع، والتسوية، مما يقلل من الحاجة إلى التدخل اليدوي. |
| المشاركH | تجعل تقنية البلوكتشين العقود الذكية التي توزع الأشخاص والقرارات مرئية |
| المشاركI | العقود الذكية تعد حقبة جديدة في المراجعة، ويُنظر إليها باعتبارها تقنية حديثة ستساعد كثيراً في المراجعة. |
| المشاركJ | –تساعد العقود الذكية على التحقق من المعاملات تلقائياً، حيث تستخدم كوسيط في المبادلات بطريقة أكثر فعالية من الأنظمة التقليدية التي تعتمد على الوسطاء المركزين، وهو ما يعد مثالاً واضحاً على تأثير تقنية البلوكتشين على إحداث ثورة في كيفية معالجة المعاملات المالية والتحول من طريقة من نظير إلى نظير.<br>– تساعد العقود الذكية تلقائيًا في أدوار محاسبية معينة.<br>– يمكن استخدام أحد تطبيقات البلوكتشين للتمويل اللامركزي (DeFi) في المحاسبة، حيث لا نحتاج إلى الاعتماد على الوسطاء (المؤسسات مثل البنوك) لإدارة تدفق المعاملات. |
| المشاركK | العقود الذكية للعملات المشفرة مثل الإيثيريوم Ethereum والتطبيقات اللامركزية (DApps) ستكون مفيدة في مجال المحاسبة ومراجعة الحسابات. |
| المشاركL | – عند استخدام العقود الذكية، يقوم المراجعون باستخدام أدوات جديدة للمراجعة ومراجعة الشفرات البرمجية وتنفيذ هذه العقود، تتمتع العقود الذكية بقدرة على أتمتة مجموعة متنوعة من عمليات المحاسبة، مثل إصدار الفواتير ومعالجة المدفوعات والتسويات المالية. إن المصطلحات المحددة مسبقًا والمشفرة للعقود الذكية تميزها بشكل كبير عن أسلوب المحاسبة القائم على القيد المزدوج، مما يجعل العمليات أكثر كفاءة وشفافية.<br>– العقود الذكية لديها القدرة على إحداث ثورة في أتمتة ودقة العمليات المالية المختلفة .<br>– بالنسبة للمحافظ الرقمية وإدارة العملات المشفرة: قد يستخدم المحاسبون ومراجعو الحسابات المحافظ وأدوات الإدارة لتأمين التعامل مع الأصول الرقمية.<br>– التطبيقات اللامركزية Decentralized Applications (DApps) التي تتعامل مع الخصوصية والأمن والتمويل اللامركزي (DeFi) لديها القدرة على إحداث ثورة في مجال المحاسبة. |

**(Q12) : ماهو تأثير تقنية البلوكتشين على مستقبل وظائف المحاسبة والمراجعة؟**

لاحظت الباحثة تكرار الحديث عن ثلاث مواضيع فرعية وقد قامت بتكويدهم ، وهي:

(1) تطور أدوار المحاسبين في عصر البلوكتشين

(2) تقنية البلوكتشين وتطبيقاتها تعد أداة للمراجعين

(3) تحديات ومميزات تبني تقنية البلوكتشين في المحاسبة

**فيما يلي إجابة كل مشارك عن هذا السؤال الفرعي (Q12)**

| | |
|---|---|
| المشارك B | لا أعتقد أن هذا سيقضي على أدوار المحاسبة، بل أعتقد أن إجراءات عمليات المراجعة سوف تغير. كماسيكون هناك حاجة للمزيد من المحاسبين المستقلين. |
| المشاركC | أشعر أنه لن يلغي وظائف المحاسبة، ولكن أعتقد أنها ستكون أداة يُمكنها المساعدة في عملية المراجعة، لأنها ربما تُغير مسار وظائفهم إلى حد ما فربما يكون أسهل، ويمكنهم التركيز على دفتر الأستاذ الفعلي نفسه مقابل التأكد من صحة كل شيء هناك، وأشعر أنه سيعزز عملية المراجعة. |
| المشاركD | ستكون هناك حاجة للمحاسبين دائماً ، ولكن ربما سيكون هناك حاجة أكثر للمحاسبين القضائيين. |
| المشاركF | ما زلت هناك حاجة للعنصر البشري، تعد تقنية البلوكشين مجرد أداة لمساعدة المحاسبين في مهنتهم، لذلك لن تلغي وظيفة المحاسبين، لكن سوف تجعل مهنة المحاسبة أكثر كفاءة . |
| المشاركG | سيتم استبعاد عدد من المحاسبين ولكن ليس جميعهم حيث ستظل بحاجة إلى محاسبين ومراجعين. |
| المشاركI | لن تلغي تقنية البلوكتشين وظيفة المحاسب، لأننا في نهاية المطاف بحاجة إلى أشخاص يعرفون المحاسبة، وإلا فلن تصبح تقنية البلوكتشين مفيدة. ربما تكون جودة المحاسبين أعلى بكثير وسيحتاجون إلى امتلاك قدرات ومهارات أعلى. |
| المشاركJ | من المحتمل أن يتم التخلص من وظيفة المحاسبين بمرور الوقت، حيث ستقل أعداد مسك الدفاتر بالطرق التقليدية. ومع ذلك، عندما تضع اعتماداً أكبر على أي تقنية حديثة، هناك حاجة لأفراد قادرين على فهم تلك التقنية والتعامل معها. |
| المشاركK | لن يحدث ذلك، لأننا نحتاج إلى بشر للتحقق مما يحدث، لكنه سيضيف المزيد من مهام المحاسبة. |

**(Q13): كيف تختلف تقنية البلوكتشين عن الطرق التقليدية في المحاسبة؟**

لاحظت الباحثة تكرار الحديث عن ثلاث مواضيع فرعية وقد قامت بتكويدهم ، وهي:

(1)العقود الذكية والمحاسبة في الوقت الفعلي.

(2) اللامركزية والقضاء على الطرف الثالث.

(3) الثبات والكفاءة في المحاسبة.

**فيما يلي ما تم استنباطه من إجابة كل مشارك عن هذا السؤال(Q13)**

| | |
|---|---|
| المشارك A | إن الطبيعة الموزعة للبلوكتشين هي محور الاختلاف، فغالبًا ما يحتاج المحاسبون إلى الوصول إلى أنظمة المحاسبة بطريقة تقليدية. ولكن مع طبيعة البلوكتشين الموزعة، فإن المحاسبين أنفسهم ربما سيكون لديهم القدرة على الحصول على نظرة وحق الوصول دائماً على العمليات الواقعة على منصات البلوكتشين. |
| المشارك B | إن امتلاك عقدة موزعة للدفع هي أحد المميزات، بالاضافة إلى أنها تعتمد على الحوسبة أو التكنولوجيا، أي أن المعلومات متاحة في الوقت الفعلي بكفاءة. وبالتالي يمكنهم إجراء تحليلات في الوقت الفعلي، واكتشاف الأهداف، والتحكم في الوقت الفعلي، والضمان، والمراجعة، والرقابة وإعداد التقارير. |

| | |
|---|---|
| المشارك C | محاسبة القيد الثلاثي |
| المشارك D | استخدام برامج معينة لتطبيق تقنية البلوكتشين Blockchain |
| المشاركE | الشفافية وعدم القابلية للتغيير من أهم المزايا، فالمعاملات المسجلة في البلوكتشين بمجرد إضافتها إلى السلسلة لا يمكن تغييرها، وهذا يعد أحد أهم أشكال التباين عن الطرق التقليدية. |
| المشاركF | كل معاملة ستظهر في الوقت الفعلي وكذلك شفافية المعاملات. فمن وجهة نظر المراجعة التقليدية، إذا حدث شيء الآن سيتم مراجعته لاحقًا. ولكن مع تقنية البلوكتشين والتطبيقات اللامركزية، كل المعاملات موجودة على السلسلة في الوقت الفعلي. |
| المشاركG | مع تقنية البلوكتشين يتم التحقق لحظياً من المعاملات. |
| المشاركH | أهم ميزة أن تقنية البلوكتشين غير قابلة للتغيير ويمكنك وضع علامة زمنية، وهو ما يعد أكبر عنصر يميزها عن أي شيء آخر، واستخدام العقود الذكية أيضاً. |
| المشارك I | مع الطبيعة اللامركزية للبلوكتشين، إذا قمت بتغيير أي شيء، فستحتاج إلى موافقة باقي الأطراف. بالإضافة إلى أن الطبيعة الديناميكية للبلوكتشين، تُمكن من التحقق من المعاملات في الوقت الفعلي. |
| المشاركJ | مع تقنية البلوكتشين يمكننا الحصول على ضمانات لكل معاملة على حدة في الوقت الفعلي. كما أنها تدعم خوارزميات التحقق بدلاً من الاعتماد على شخص واحد. |
| المشاركK | تساعد طبيعة دفتر الأستاذ الموزع وقيد الادخال الثلاثي والتحقق في الوقت الفعلي من تخفيض ساعات العمل مقارنة بالطرق التقليدية التي تستلزم وقتًا طويلاً. |
| المشاركL | إن المصطلحات المحددة مسبقًا والمشفرة في جانب الكود للعقود الذكية هي أهم ما يميز محاسبة قيد الإدخال الثلاثي عن القيد المزدوج. |

**(Q2) : ما هي التدابير الأمنية المتبعة في تقنية البلوكتشين لضمان حماية البيانات والمعاملات؟**

**لاحظت الباحثة تكرار الحديث عن خمسة مواضيع وقد قامت بتكويدهم ، وهي:**

(1) نقاط الضعف الأمنية في الحلول القائمة على البلوكتشين

(2) الحوسبة الكمية quantum computing والمرونة [1]

(3) سلامة البيانات في تقنية البلوكتشين العامة.

(4) اللامركزية والتبني الداخلي للبلوكتشين من قبل المراجعين.

(5) تقنيات التشفير للبيانات المالية.

**فيما يلي ما تم استنباطه من إجابة كل مشارك عن هذا السؤال (Q2)**

| | |
|---|---|
| المشارك A | –طبيعة دفتر الأستاذ الموزع تجعلها آمنة للغاية، ولكن تكمن المشكلة مع التطبيقات والإنترنت.<br>– الأمان عامل مهم في مجال المحاسبة، لأنه إذا وُجدت ثغرات في أمان المعاملات القائمة على تقنية البلوكتشين، سيحتاج المراجعين لتحديد هذه الثغرات وتقييمها وضمان الضوابط ضدها. |

[1] **الحوسبة الكمية** تشير إلى نوع من الحوسبة تستخدم مبادئ الميكانيكا الكمية. تتميز هذه الحوسبة بقدرتها على معالجة المعلومات بطرق لا تستطيع الحواسيب التقليدية القيام بها. على سبيل المثال:
تستخدم الحوسبة الكمية "الكيوبتات (qubits) "بدلاً من "البتات(bits) " أي (0 أو 1) في الحواسيب التقليدية، مما يسمح لها بتنفيذ العديد من العمليات في وقت واحد. يمكن للحواسيب الكمومية حل مسائل رياضية معقدة بشكل أسرع بكثير من الحواسيب التقليدية.

| | |
|---|---|
| المشارك B | تعد تقنية البلوكتشين آمنة نظرت لوجود الأكواد، تعد تقنية البلوكتشين جيدة بقدر جودة الكود الخاص بها. عندما تنظر إلى الحوسبة الكمومية، عليك التأكد من أن المطورين يفهمون الكود الخاص بهم. |
| المشارك C | هي تقنية آمنة، ولكنها تكمن الخطورة في إدخال البينات، فإذا أدخلت البيانات بشكل خاطئ فستبقى كما هي. يعتمد الأمر على نوع البلوكتشين (العام أو الخاص)، حيث تعد التقنيات الخاصة أكثر أماناً مقارنة بالتقنيات العامة. |
| المشارك D | تعد تقنية البلوكتشين هي الأكثر أمانًا في قطاع الأعمال التجارى، بسبب عمليات التشفير التى تعمل بها تجعلها الأكثر أماناً. إن تقنية البلوكتشين هي الأكثر ملائمة لعلم المحاسبة لأنها الأكثر أمانًا. |
| المشارك E | تعزز تقنيات التشفير في البلوكتشين من أمان وخصوصية البيانات المالية، فالوصول للمعلومات يُمكن التحكم فيه من خلال كلا من المفاتيح الخاصة والعامة، مما يضمن وصول الأفراد المصرح لهم فقط إلى المعلومات المالية الحساسة. |
| المشارك F | فيما يتعلق بالأمان، تعد الطبقة الأولى للبلوكتشين آمنة للغاية، فكلما كانت طبقة البلوكتشين أكبر أصبحت أكثر أمانًا، لأنه لديك الآن العديد من الأشخاص الذين يؤكدون أن هذه المعاملات دقيقة بالفعل. بينما إذا كانت طبقة البلوكتشين صغيرة فلا يوجد الكثير من الأمان المرتبط بها. لذا، كلما كانت طبقة البلوكتشين أكبر، أصبحت الشبكة أكثر أمانًا. |
| المشارك G | تساعد تقنية البلوكتشين في حل الكثير من المشكلات في المحاسبة لأنه ستوفر مستوى أعلى من الحماية. |
| المشارك I | فيما يتعلق بالبلوكتشين والأمن السيبرانى، فإن طبقة البلوكتشين ليست آمنة بنسبة 100٪ لأنه إذا كان لدى شخص واحد المفتاح فقد يؤثر ذلك الشخص على طبقة البلوكتشين بأكملها، وعلى الرغم من أن باقي الأطراف الأخرى ستتلقى تحذيرات. ولكن قد يكون الأوان قد فات. |
| المشارك J | إن البنية اللامركزية للبلوكتشين تجعلها آمنة للغاية لأنها تحتوي على أشكال أمان متعددة، وطبيعتها اللامركزية تعني أنها أكثر أمانًا لأن يوجد العديد من الأشخاص الذين لديهم إمكانية الوصول إلى المعاملات والذين سيكتشفون ما إذا كان هناك خطأ ما. |
| المشاركK | تقنية البلوكتشين ستكون محمية وسوف تساعد كثيرًا في الحد من مشاكل الاحتيال التي تمر بها شركات المحاسبة. كماأن سمات اللامركزية والتجزئة المشفرة وآليات الإجماع والشفافية، تجعل منها تقنية أقوى، فهذه السمات الأمنية ملائمة جداً لمهنة المحاسبة حيث يعتمد المراجعون على دقة وسلامة السجلات المالية لضمان الامتثال التنظيمي. |
| المشاركL | إن اللامركزية و غير القابلية للتغيير ومقاومة التلاعب والشفافية كأهم سمات تقنية البلوكتشين تجعلها آمنة للغاية. كما أنها تستخدم تقنيات تشفير قوية لتأمين البيانات، مما يجعلها مقاومة للاختراق والاحتيال. |

**(Q3): كيف يمكن تعزيز الأمن السيبرانى عند تطبيق تقنية البلوكتشين في مهنة المحاسبة؟**

يناقش هذا السؤال تحديات ومخاطر الأمن السيبرانى التي تأتي مع تقنية البلوكتشين وما يمكن القيام به للحماية منها. وقد لاحظت الباحثة تكرار الحديث عن خمسة مواضيع فرعية وقد قامت بتكويدهم ، وهي:

(1) تقنيات الأمن السيبرانى في تبني تقنية البلوكتشين في المحاسبة

(2) نقاط ضعف العقود الذكية

(3) الأمن والتحكم في بيئات تقنية البلوكتشين الخاصة.

(4) التخفيف من تحديات الأمن السيبرانى في تقنية البلوكتشين

(5) النهج الشامل لتقنية البلوكتشين.

**فيما يلي ما تم استنباطه من إجابة كل مشارك عن هذا السؤال (Q3)**

| | |
|---|---|
| المشارك A | – كل تقنية جديدة لها نقاط ضعف أمنية وثغرات، تعد حداثة تقنية البلوكتشين هي نقطة الضعف من منظور الأمن السيبرانى.<br>– تتدرج تقنية البلوكتشين بشكل متزايد في البنية التحتية على مستوى القاعدة ثم التطبيقات والخدمات ذات المستوى الأعلى. ستكون هناك ثغرات أمنية أثناء تطوير هذه الخدمات الهجينة الجديدة، بالإضافة إلى طريقة تفاعلها معًا.<br>– الأمن السيبرانى له أهمية قصوى في سياق تقنية البلوكتشين والعقود الذكية، حيث يلعب دوراً حاسماً في ضمان سلامة وسرية وتوافر الأنظمة القائمة على تقنية البلوكتشين، وخاصة القائمة على العقود الذكية. |
| المشارك B | يوجد العديد من تقنيات البلوكتشين التي تم اختراقها. حيث شملت المخاطر هجومًا بنسبة 51٪ على الشبكة، والمطورون يجب أن يفهموا أكوادهم. |
| المشارك C | تحتاج العقود الذكية إلى توخي الحذر عن كيفية برمجتها، فكلما ظهرت مشكلة مع تقنية البلوكشين العام، فعادةً ما يرجع ذلك لأن العقود الذكية لم تتم كتابتها بشكل جيد. تعد هذه هي أكبر مشاكل الأمن السيبرانى والتي يجب مراقبتها عندما يتعلق الأمر بالعقود الذكية، وبالتالي لا يهم مدى الأمان، إذا كنت لا تقوم بالبرمجة بشكل جيد، وتعد هذه مشكلة تتعلق بالأمن السيبرانى. |
| المشارك D | – قد لا تكون كافة تقنيات البلوكتشين لامركزية، وإذا حدث هجوم على الشبكة أو إذا كانت هناك نقطة ضعف فقد تتعطل بسهولة، وهو ما يجعلها غير آمنة لأنه يمكن التأثير عليها بسهولة.<br>– في كثير من الأحيان، تتعرض تقنية البلوكتشين للاختراق لأن تطبيقاتها معرضة للخطر بسبب بعض التطبيقات على السلسلة، أو الأشياء التي يتفاعل معها الأشخاص أو كتابة الكود بشكل سيئ أوكان عامًا، فيمكن للأشخاص استغلاله. مما قد يجعله عرضة لخسارة كل شيء.<br>– إذا لم يكن أمان الشبكة قويًا وكان به ثغرة، فيمكن لأي شخص الاستيلاء على الشبكة واحتجاز الجميع وأموالهم. وبالتالي فإن الهندسة الجيدة مهمة جدًا لحمايتهم. |
| المشارك E | ثغرات العقود الذكية، ومخاوف الخصوصية، وهجمات 51%، ومخاطر آليات الإجماع.<br>العقود الذكية: على الرغم من قوتها فليست محصنة ضد الهجمات، يجب على مجال المحاسبة، الذي يعتمد على المعاملات المالية الدقيقة والخالية من الأخطاء، معالجة العيوب المحتملة في أكواد العقود الذكية، حيث تعد أكواد المراجعة أمرًا ضروريًا لتحديد الثغرات وتصحيحها، مما يقلل من خطر التناقضات المالية الناتجة عن الأخطاء أو الاحتيالات الضارة. |
| المشارك F | – لا يمكن لشركات المحاسبة أن تعتبر نفسها آمنة بنسبة 100% من الهجمات الإلكترونية لمجرد أنها تستخدم تقنية البلوكتشين فكل بروتوكول معرض للخطر، لذلك هناك دائمًا فرصة للاختراق.<br>– الأشخاص الذين يبحثون عن الثغرات هم الأشخاص الذين يحاولون الاختراق. هناك فجوة هائلة للمطورين الذين يعملون تحت تقنية البلوكتشين وهناك حاجة ملحة لموظفي الأمن السيبرانى والبلوكتشين. |
| المشارك G | – تتمثل المشكلة في تقنية البلوكتشين في سهولة اختراقها لأن هناك عقدة واحدة في مكان واحد لجميع المعلومات المشفرة، ولكن إذا كان لديك عدة عقد، فإن الأمر يصبح أكثر تعقيدًا.<br>– المصادقةAuthentication : التعريف الموزع هو شيء جيد يمكن القيام به للحماية من المخاطر السيبرانية المرتبطة بتقنية البلوكتشين، ويتطلب الأمر أكثر من بروتوكول لتحديد هوية الشخص. |
| المشارك H | تحتاج تقنية البلوكتشين إلى النضج والتنظيم، ويحتاج مستخدموها إلى فهم كيفية عملها كي يتم تبنيها بشكل أكبر، لقد تعرضت محافظ العملات المشفرة للاختراق، وغير منصف محاولة الترويج أن تقنية البلوكتشين محصنة تماماً ضد الهجمات الإلكترونية. |
| المشارك I | يعتبر الأمن السيبرانى جزءًا أساسيًا من تقنية البلوكتشين. لذلك نحتاج إلى تثقيف البشر ولا ينبغي إعطاء مفاتيح العقد عشوائيًا لمستخدمين غير مصرح لهم. |

| | |
|---|---|
| المشارك J | – يجب التعامل مع المفاتيح الخاصة باعتبارها أحد الامتيازات الإدارية وأحد أنواع المخاطر الأمنية. عند إنشاء بلوكتشين خاص، يجب التأكد من أن الأشخاص المناسبين هم في الأماكن المناسبة على السلسلة وأن هناك ضوابط مناسبة على من يمكنه الوصول إليها؟ على سبيل المثال: إذا كان لدينا أصول في محفظة، يجب التأكد من تأمين مفاتيح هذه الأصول؟ ، وإذا كنا نتعامل مع العقود الذكية، يجب التأكد من العقود الذكية والتحقق من صحتها؟<br>– في إطار الأمن السيبرانى العام، هناك اختبارات خاصة باختراق وإدارة الثغرات الأمنية. فيجب مراجعة إذا كانت الثغرات الأمنية موجودة، وهل اختبرناها باختبار الاختراق، وهل قمنا بتصحيح نظامها بشكل مناسب؟ |
| المشاركK | – هناك مخاطر خاصة بالخصوصية، وثغرات التعليمات البرمجية، والخطأ البشري، ونقص التوحيد القياسي، والمخاطر القانونية والتنظيمية، وقضايا التوسع، والعيوب الأمنية في منصات البلوكتشين، فيجب الاطلاع دائماً على تطور التهديدات الأمنية السيبرانية والتشريعات التنظيمية للحفاظ على بيئة عقود ذكية آمنة. |
| المشارك L | – يتم تنفيذ العقود الذكية بناءاً على التعليمات البرمجية، ويمكن أن تؤدي الثغرات الأمنية في التعليمات البرمجية إلى مخاطر أمنية كبيرة. لذلك، تعد عمليات مراجعة التعليمات البرمجية ومراجعات الأمان المنتظمة أمرًا بالغ الأهمية لتحديد الثغرات الأمنية وتصحيحها. إن الطبيعة الثابتة للبلوكتشين مع ضمان سلامة البيانات، تفرض تحديات في تصحيح الأخطاء بمجرد نشر العقود الذكية. يعد الاختبار المكثف وضمان الجودة قبل النشر أمراً ضرورياً لتقليل خطر نشر العقود الذكية المعيبة.<br>– يحتاج المحاسبون والمراجعون إلى التدريب على آليات الأمن السيبرانى وفهم المخاطر وتنفيذ تدابير أمنية قوية. بالاضافة إلى فهم آليات الخصوصية ، وخاصة في نمط البلوكتشين الذى لا يتطلب أذونات لأنها ستكون بالغة الأهمية.<br>– إن اللامركزية وأمن الشبكات ضروريان، لأن اللامركزية وهي سمة أساسية للبلوكتشين، تعني أنه يجب الحفاظ على الأمان عبر جميع العقد في الشبكة.<br>– يجب إعطاء الأولوية لتقنيات الأمن السيبرانى للتخفيف من المخاطر المحتملة. |

**وأثناء الإجابة على السؤال الرئيسي الثالث (Q3) قامت الباحثة بطرح سؤالين فرعيين ، وهما:**

**(Q31):** هل يجب تدريب المحاسبين/المراجعين على تقنيات البرمجة الحديثة والأمن السيبرانى؟

**(Q32):** ما هي أكبر التحديات التي يواجهها المحاسبون/المراجعون عند تبني تقنية البلوكتشين في عمليات المحاسبة والمراجعة؟

**وعند قيام الباحثة بتكويد إجابات السؤال الفرعي:**

**(Q31): هل يجب تدريب المحاسبين/المراجعين على تقنيات البرمجة الحديثة والأمن السيبرانى؟**

لاحظت الباحثة تكرار الحديث عن :

(1) استعدادات الأمن السيبرانى للمحاسبين والمراجعين.

(2) رفع مهارات وقدرات المحاسبين والمراجعين

**فيما يلي ما تم استنباطه من إجابة كل مشارك عن هذا السؤال (Q31)**

| | |
|---|---|
| المشارك A | لا أعتقد أن المحاسبون والمراجعون يحتاجون إلى فهم التقنيات البرمجية الحديثة، ولكن ربما سيحتاجون إلى التدريب على الأمن السيبرانى. لأن لهم دورًا خاصاً في الأمن السيبرانى وفي اختبار عناصر التحكم ومشاركتها. لذلك، فإنه يجب تطوير تلك التقنيات للسيطرة عليها، ومن ثم ضمانها، لن يصبح المحاسبون/ المراجعون مبرمجين، لكنهم سيصبحون بارعين في استخدام أدوات وتقنيات البلوكتشين. |
| المشارك E | يجب علي المحاسبين/المراجعين التعرف على هيكل الأكواد والرموز لفهم أهميتها، مما يعني أنه يجب عليهم التعرف على الأمن السيبرانى. |
| المشارك F | لا أعتقد أنه سيُطلب من جميع الموجودين على السلسلة التدريب على الأمن السيبرانى، ولكن سيُطلب من كافة المنظمات أن يكون لديهم أفراد وموظفون على دراية بهذه التقنيات. |
| المشارك H | نظرًا لأن الأمن السيبرانى في حد ذاته مجال كبير، فإن المحاسبين والمراجعين بحاجة لفهمه ، وأن يكونوا منتبهين لأي مشكلة سيبرانية قد تنشأ، وأن يكونوا قادرين على البحث عن أي تغير في البيانات والمخاطر المرتبطة بها وتحديثات البرامج. |
| المشارك I | يجب تدريب المحاسبين والمراجعين على التقنيات المتعلقة بتطور الكمبيوتر والأمن السيبرانى. |
| المشارك J | يجب تدريب المحاسبين والمراجعين على البرمجة. |

**(Q32):ما هي أكبر التحديات التي يواجهها المحاسبون/المراجعون عند تبني تقنية البلوكتشين في عمليات المحاسبة والمراجعة؟**

لاحظت الباحثة تكرار الحديث عن :

(1) العقود الذكية في مجال المحاسبة.

(2) تحديات الحوكمة التنظيمية.

(3) الكفاءة الفنية والتعليم.

(4) الأمن وإدارة المخاطر.

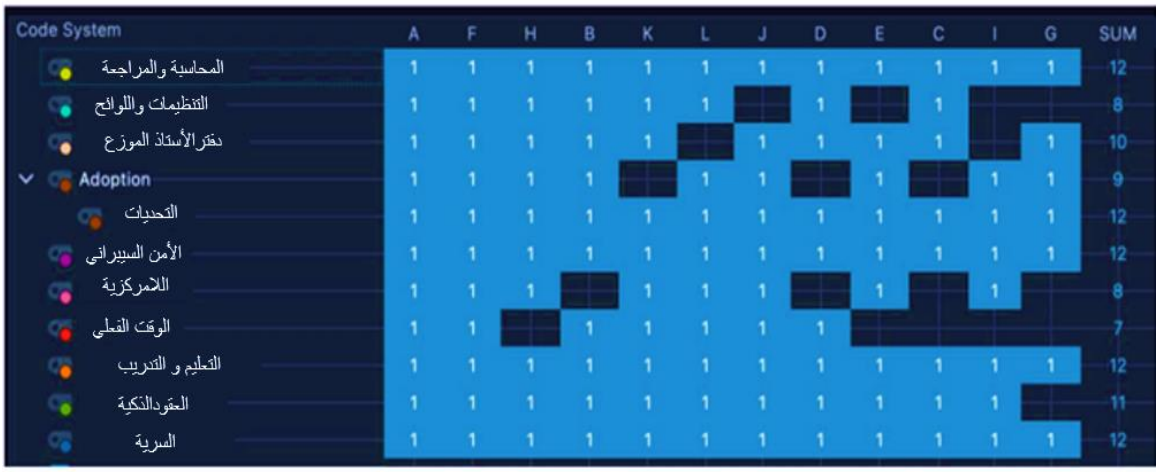
**فيما يلي ما تم استنباطه من إجابة كل مشارك عن هذا السؤال(Q32)**

| | |
|---|---|
| المشارك A | يجب على المحاسبين التدريب على كيفية استخدام تقنية البلوكتشين نظراً لتغير طبيعة عملهم. |
| المشارك B | أكبر تحدي ستواجهه مهنة المحاسبة هو الأطر واللوائح التنظيمية، فمن الضروري جعل المنظمات الحكومية توفر أطر واضحة. |
| المشارك C | يجب زيادة علم المحاسبين والمراجعين بالتكنولوجيا والأدوات المستحدثة. |
| المشارك D | عدم معرفة التطورات التكنولوجية هو أحد التحديات التى يواجهها المحاسبون. |
| المشارك E | يحتاج المهنيين في المحاسبة والمراجعة إلى تطوير الوعي بقضايا الأمن السيبرانى الخاصة بالبلوكتشين، ودمج مؤشرات الأمان في ممارساتهم، ويحتاجون إلى امتلاك عقلية قابلة للتكيف. |
| المشارك F | التحدي الأكبر الذي سيواجه المحاسبون/المراجعون هو التعليم والتدريب لفهم تقنية البلوكتشين. |

| | |
|---|---|
| المشارك L | يمكن أن تكون العقود الذكية معقدة، فيجب معالجة التحديات مثل أخطاء الترميز والاعتبارات القانونية والحاجة إلى بروتوكولات موحدة، حيث يتطلب مراجعة شفرتها وتنفيذها مهارات متخصصة. قد يحتاج المحاسبون/المراجعون إلى اكتساب أو توظيف خبراء في مراجعة العقود الذكية، والتعاون مع خبراء في تقنية البلوكتشين Blockchain. |

**(هـ) نتائج تحليل البيانات باستخدام برنامج MAXQDA:**

1) قامت الباحثة باستخدام برنامج MAXQDA بإعداد الشكل(2) الذي يمثل تصورًا لآراء واستجابات المشاركين الاثنا عشر على الموضوعات الرئيسية التي تمت مناقشتها في المقابلات، وما ظهر خلال المقابلات من مناقشة لبعض الموضوعات الفرعية.




**شكل 2:** تصورًا لآراء المشاركين على موضوعات البحث

2) قامت الباحثة باستخدام برنامج MAXQDA بإعداد تمثيلًا مرئيًا للموضوعات الفرعية التي ظهرت أثناء المقابلات من مفاهيم وأساليب حديثة اشتقت عند تطبيق تقنيات الأمن السيبراني والبلوكتشين في الواقع العملي، باستخدام الشكل (3).


**شكل 3:**تمثيلًا مرئيًا للموضوعات الفرعية

**بعد التحليل السابق للمقابلات**، توصلت الباحثة أن البيانات التي المجمعة وثيقة الصلة بموضوع البحث، تم تصوير الموضوعات الأساسية التي ظهرت من المقابلات في الشكل (1) وتم عرضها في التصور في الشكل (2). أظهرت المقاييس الأكبر الموضوعات المتكررة للغاية، وأظهرت المقاييس الأصغر موضوعات منخفضة المستوى

تمت مناقشتها. والجدير بالذكر أن المشاركين أكدوا على مدى أهمية أمن البلوكتشين والأمن السيبرانى والعقود الذكية عند التفكير في تبني تقنية البلوكتشين في العمليات المحاسبية. كما أكد المشاركون على أهمية الأمن السيبرانى عند التفكير في تطبيق محاسبة البلوكتشين.

جدير بالذكر، حصدت العقود الذكية على الكثير من تعليقات المشاركين في المقابلات حيث ذكر المشاركون أنها ميزة هامة ورئيسية. وقد أوضح الشكل (3) الموضوعات الفرعية التي ذكرها المشاركون بشكل متكرر. وقد لاحظت الباحثة أن هذه الموضوعات الفرعية تمثل عناصر حاسمة وضرورية للتبني الفعال وتطبيق تقنية البلوكتشين في المحاسبة بشكل آمن.

**ختاماً، توصلت الباحثة** بعد التركيز على هدف البحث وهو أثر تقنيات الأمن السيبرانى لتبني تقنية البلوكتشين في مجال المحاسبة. ناقشت إجابات المشاركين بشكل جماعي تقنية البلوكتشين كقوة تحويلية لمتطلبات العمل المحاسبى والمراجعة. تم اختيار طريقة جمع البيانات في هذه البحث عن قصد لضمان استكشاف شامل لهدف البحث، مع تطور عملية جمع البيانات، كان هناك تكرار للموضوعات والمفاهيم والرؤى داخل البيانات المجمعة، يعد تحقيق تشبع البيانات في هذا البحث أمرًا ضروريًا، لأنه يعزز من موثوقية ومصداقية نتائج البحث، وأن النتائج تستند إلى فهم شامل لموضوع البحث.

تم تسليط الضوء على الأمور الرئيسية للأمن السيبرانى التى يجب الانتباه لها عند تطبيق تقنيات البلوكتشين فيما يخص مجالات المحاسبة والمراجعة لتحقيق كفاءة البيانات والأمن الشبكى، والتنظيم والامتثال، وتحديات وثغرات أمن البلوكتشين، واحتياجات التعليم والتدريب، ومعوقات الأمن السيبرانى والتدابير المخففة.

وبشكل عام، أظهر المشاركون فهماً عميقاً لتأثيرات تقنية البلوكتشين على تحول مهنة المحاسبة والمراجعة، بما في ذلك الاعتبارات الفنية والتنظيمية والعملية، قدم جميع المشاركين فهماً دقيقاً للتطبيقات والمتطلبات التكنولوجية المحتملة والتحديات وقضايا الأمن السيبرانى الواجب أخذها في الاعتبار.

جدير بالذكر أن هناك بعض العناصر لم يتفق المشاركون على نفس الرأي. على سبيل المثال، عندما يتعلق الأمر بالحاجة إلى تدريب البلوكتشين والأمن السيبرانى بين المحاسبين، أكد بعض المشاركين على حقيقة أن التدريب سيكون ضروريًا، بينما رأى آخرون أن التدريبات المكثفة على البلوكتشين والأمن السيبرانى قد لا تكون ضرورة

علاوة على ذلك، بينما أعرب أحد عشر مشاركاً من أصل اثني عشر مشاركاً عن مخاوفهم بشأن افتقار اللوائح التنظيمية لتطبيق تقنية البلوكتشين، فإن المشارك (A) خالفهم الرأي ولم يرى افتقار البلوكتشين الى التنظيمات واللوائح مستنداً على التطور السابق واللوائح المطبقة والجهات التنظيمية التي تشمل البلوكتشين .

## 4/ الخلاصة والنتائج والتوصيات

### 1/4 الخلاصة والنتائج :

في هذا القسم، تعرض الباحثة ملخص للبحث وأهم النتائج التي تم التوصل إليها خلال البحث حول تأثير الأمن السيبرانى على تعزيز تقنية البلوكتشين في ظل التحول الرقمي لبيئة الأعمال المحاسبية. والتي يمكن إيجازها في النقاط التالية:

1) **أثر التحول الرقمي على تبني التكنولوجيا:** أشارت النتائج أن التحول الرقمي في بيئة الأعمال المحاسبية يعزز من تبني تقنيات البلوكتشين والأمن السيبرانى. وفقًا لدراسة أجراها (Qin, 2022) الشركات التي تتبنى التحول الرقمي بشكل فعال تكون أكثر استعدادًا للاستثمار في تقنيات جديدة مثل تقنية البلوكتشين. هذا التحول يعكس الحاجة إلى الابتكار والتكيف مع التغيرات في السوق، ويساعد على تحسين الأداء العام للمؤسسة. كما أن وجود إطار قوي للأمن السيبرانى يسهم في تسريع عملية التحول الرقمي، حيث يقلل من المخاوف المتعلقة بالسلامة والأمان.
2) **تعزيز أمان المعاملات المحاسبية:** أظهرت النتائج أن تطبيق تقنيات الأمن السيبرانى بشكل فعال يُعزز من أمان المعاملات والبيانات والمحاسبية المخزنة على شبكات البلوكتشين. إن استخدام أساليب التشفير المتقدمة يحد من قدرة المهاجمين من الوصول إلى البيانات الحساسة، إن طبيعة تقنية البلوكتشين اللامركزية تحد من الثغرات التي يمكن أن يستغلها المهاجمون. وقد أظهرت بيانات دراسة (Han, et al., 2023) أن الشركات التي استثمرت في تحسين أمان شبكات البلوكتشين شهدت انخفاضًا ملحوظًا في حالات الاختراق والاحتيال. وبالتالي، فإن المؤسسات التي تعتمد في التحول الرقمي على تطبيق تقنيات البلوكتشين تكون أكثر قدرة على حماية بياناتها المالية والامتثال للمعايير المحاسبية الدولية.
3) **تعزيز الشفافية والمصداقية:** توصلت الباحثة أن الأمن السيبرانى يلعب دورًا حاسمًا في زيادة الثقة بين اطراف الشبكة في البيئة المحاسبية. فعندما تكون البيانات محمية بشكل جيد ويُمكن الحصول عليها في الوقت الفعلي، فإن ذلك يزيد من ثقة العملاء والمستثمرين في العمليات المحاسبية (Smith, 2022) كما أن استخدام تقنية البلوكتشين يضمن شفافية المعاملات المالية، مما يعزز من مصداقية التعاملات. وقد أظهرت الاستبيانات أن 75% من المشاركين يشعرون بزيادة في الثقة في الشركات التي تتبنى تقنيات الأمن السيبرانى والبلوكتشين بشكل متكامل.
4) **تحسين الكفاءة التشغيلية:** أظهرت نتائج البحث أن دمج الأمن السيبرانى مع تقنية البلوكتشين يسهم في زيادة الكفاءة التشغيلية لبيئة الأعمال المحاسبية. توصلت دراسة (Hilary & Liu, 2021) أن استخدام تقنية البلوكتشين يقلل من الوقت المطلوب لمعالجة المعاملات، حيث يتم تنفيذها بشكل آلي وشفاف، هذا يؤدي إلى تقليل الأخطاء البشرية وتوفير الموارد، مما يمكن الشركات من التركيز على الأنشطة الاستراتيجية بدلاً

من العمليات الروتينية. بالإضافة إلى ذلك، فإن وجود تدابير أمنية قوية يضمن استمرارية الأعمال ويقلل من فترات التوقف الناتجة عن الهجمات السيبرانية.

5) **مواجهة التحديات الأمنية:** على الرغم من الفوائد العديدة، أظهرت النتائج أن هناك تحديات تتعلق بالأمن السيبرانى في تطبيق تقنية البلوكتشين في الأعمال المحاسبية. وفقًا لتقرير صادر عن معهد الأمن السيبرانى عام 2023، فإن هناك عقبات تتعلق بالهجمات السيبرانية التي تستهدف الشبكات القائمة على البلوكتشين. تتطلب هذه التحديات استراتيجيات متقدمة للأمن السيبرانى، بما في ذلك تشفير البيانات، وإدارة الهوية، والتقييم المستمر للمخاطر. لذا، تحتاج المؤسسات إلى استثمار المزيد من الموارد في تعزيز أنظمتها الأمنية لضمان سلامة بياناتها المالية.

6) **التوافق مع المعايير التنظيمية:** أظهرت نتائج البحث أن تطبيق الأمن السيبرانى في بيئة الأعمال المحاسبية المدعومة بتقنية البلوكتشين يسهل التوافق مع المعايير التنظيمية. حيث أن العديد من الهيئات التنظيمية تتطلب مستويات عالية من الأمان لأمن البيانات المالية. حيث أن الشركات التي تعتمد على هذه التقنيات تتمتع بمستوى عالٍ من الالتزام بالمعايير، مما يقلل من المخاطر القانونية والمالية. وقد أشار بعض المشاركين في البحث إلى أن استخدام تقنية البلوكتشين مع الأمن السيبرانى يُمكن أن يساعدهم في الامتثال للمعايير بشكل أفضل.

7) **الابتكار في الخدمات المحاسبية:** أظهرت النتائج أن الأمن السيبرانى يعزز من الابتكار في تقديم الخدمات المحاسبية أثناء التحول الرقمي. حيث أن الأمان والثقة في المؤسسات وبين أطراف الشبكة يجذب الشركات لتطوير حلول جديدة تعتمد على هذه التقنية، مثل العقود الذكية والتحليلات المتقدمة. وقد ذكر بعض المشاركين في الدراسة أن الشركات التي استثمرت في الأمن السيبرانى وتقنية البلوكتشين قد أطلقت خدمات جديدة خلال العامين الماضيين، مما ساهم في توسيع قاعدة عملائها وزيادة حصتها في السوق.

**خلاصة القول،** تظهر النتائج أن التكامل بين الأمن السيبرانى وتقنية البلوكتشين يعزز من فعالية بيئة الأعمال المحاسبية في ظل التحول الرقمي. وأن الاستثمار في الأمن السيبرانى لا يساهم فقط في حماية البيانات، بل يعزز أيضًا من الثقة والكفاءة والامتثال والابتكار، مما يجعل من هذه التقنيات ضرورة للمؤسسات التي تسعى للبقاء في المنافسة. يتطلب هذا التكامل استراتيجيات شاملة ومتكاملة لضمان الأمان والكفاءة والشفافية، مما يسهم في نجاح المؤسسات في عصر التكنولوجيا الحديثة.

### 2/4 التوصيات:

من خلال دراسة تأثير الأمن السيبرانى على تعزيز تقنية البلوكتشين في ظل التحول الرقمي لبيئة الأعمال المحاسبية، يمكن للباحثة استخراج التوصيات التالية:

- **تعزيز البنية التحتية للأمن السيبرانى:** يجب على المؤسسات زيادة الاستثمار في تقنيات الأمن السيبرانى المتقدمة لحماية البيانات والمعاملات على شبكات البلوكتشين.
- **تطوير السياسات المحاسبية والإجراءات الأمنية:** وضع إجراءات وسياسات ملزمة وواضحة للتعامل مع الاختراقات السيبرانية وضمان استمرارية الأعمال.
- **التوعية والتدريب:** ضرورة تدريب المحاسبون والمراجعون على أفضل ممارسات الأمن السيبرانى واستخدام تقنيات البلوكتشين بشكل آمن.
- **التعاون بين القطاعات:** تعزيز التعاون والشراكة بين المؤسسات والقطاعات المختلفة لتبادل المعلومات والخبرات في مجال الأمن السيبرانى والبلوكتشين.
- **الابتكار في تقنيات التشفير:** السعي والاستثمار نحو تطوير تقنيات تشفير جديدة وأكثر أمانًا لحماية البيانات والمعاملات المحاسبية والمالية.

**5/ الأبحاث المستقبلية:**

1. تحليل تأثير تقنيات الذكاء الاصطناعي على الأمن السيبرانى في شبكات البلوكتشين
2. تطوير نماذج جديدة للأمن السيبرانى تتناسب مع طبيعة شبكات البلوكتشين.
3. تأثير الأمن السيبرانى على الأداء التشغيلي وقيمة المؤسسة
4. تأثير الأمن السيبرانى على المخاطر التشغيلية والسمعة والامتثال والتقاضي

**6/ قائمة المـراجع**

**1/6 المراجع العربية:**

أبو الخير، أسامة أحمد محمد، أبو موسى، أحمد عبدالسلام أحمد، و البغدادي، رجب محمد عمران أحمد. (2023). إطار مقترح لاستخدام تكنولوجيا البلوك تشين Block chain كمرتكز لتعزيز جودة عملية المراجعة في ظل

بيئة التحول الرقمي مع دراسة ميدانية في بيئة الأعمال المصرية .*المجلة العلمية للدراسات والبحوث المالية والإدارية*، مج15، عدد خاص ، 1 .44 - مسترجع من http://search.mandumah.com/Record/1438922

السيد محمد عبدالله، ايمان. (2024). دراسة العلاقة بين تفعيل أدوات الأمن السيبرانى وأنظمة محاسبة التكاليف الرقمية دراسة تطبيقية علي شركات القطاع العقاري بمصر .*المجلة العلمية للبحوث والدراسات التجارية*. كليةالتجارة. جامعة حلوان. 38(1). ص.ص:63-100.

شحاته، محمد موسى. ٢٠٢٠. قياس أثر تفعيل أنشطة المراجعة الدخلية لآليات التحول الرقمى على تعزيز المساءلة والشفافية وتحسين الأداء الحكومى مع دليل ميدانى بالبيئة المصرية. *المجلة العلمية للدراسات المحاسبية*، كلية التجارة، جامعة قناة السويس، ١(٢): ٧٠٣ – ٧٨٧.

عبدالحميد، رانيا سلطان محمد. (2023). أثر استخدام تكنولوجيا سلاسل الكتل "Blockchain" على البيئة المحاسبية في مصر: دراسة نظرية ميدانية .*المجلة المصرية للدراسات التجارية، مج47، ع2* ، 1 .36 - مسترجع من http://search.mandumah.com/Record/1403618

عبدالكافي، أشرف سالم، و علي، سالمة مصباح القذافي. (2023). مدى مساهمة التحول الرقمي والحوسبة السحابية في تعزيز مهنة المحاسبة، من وجهة نظر الأكاديميين والمختصين في مجال المحاسبة .*مجلة جامعة سرت العلمية - العلوم الانسانية، مج13، ع2* ، 44 .59 - مسترجع من http://search.mandumah.com/Record/1441442

مراح، نورالهدى ، طويلب، محمد. (2022). مستقبل مهنة المحاسبة في ظل تقنيات التحول الرقمي –تقنية البلوكشين نموذجا –. مجلة الميادين الإقتصادية, 5(1), 23-48. https://www.asjp.cerist.dz/en/article/210391

## 2/6 المراجع الأجنبية:

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews*, *20*(3), 1743-1756.

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: a comprehensive review of regulatory

frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal, 5*(1), 120-140. Doi: 10.51594/csitrj.v5i.709

American Institute of Certified Public Accountants (AICPA, 2018a),"*Cybersecurity risk management reporting fact sheet*", available at: www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices /downloadabledocuments/cybersecurity-factsheet. pdf (accessed 13 November 2018)

Anyanwu, A., Olorunsogo, T., Abrahams, T. O., Akindote, O. J., & Reis, O. (2024). Data confidentiality and integrity: a review of accounting and cybersecurity controls in superannuation organizations. *Computer Science & IT Research Journal*, *5*(1), 237-253. doi: 10.51594/csitrj. v5i1.735

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (sok). In *Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6* (pp. 164-186). Springer Berlin Heidelberg**.**

Benaroch, M. (2020). Cybersecurity risk in IT outsourcing—Challenges and emerging realities. *Information systems outsourcing: The era of digital transformation*, 313-334.

Cai, C. W. (2021). Triple-entry accounting with blockchain: How far have we come? *Accounting & Finance*, *61*(1), 71-93.

Chowdhury, E., Stasi, A., & Pellegrino, A. (2023). Blockchain technology in financial accounting: emerging regulatory issues. *Review of Financial Economics*, *21*, 862-868.

Creswell, J. W., & Clark, V. L. P. (2018). *Designing and conducting mixed methods research.* Sage publications.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Danach, K., Hejase, H. J., Faroukh, A., Fayyad-Kazan, H., & Moukadem, I. (2024). Assessing the Impact of Blockchain Technology on Financial Reporting and Audit Practices. *Asian Business Research*, 9(1), 30.

Daoud, M. M., & Serag, A. A. (2022). A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach. *Trade and Finance*, 42(1), 20-61

Dasgupta, S., Yelikar, B. V., Naredla, S., Ibrahim, R. K., & Alazzam, M. B. (2023, May). AI-Powered Cybersecurity: Identifying Threats in Digital Banking. In 2023 *3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2614-2619). *IEEE*.

Deloitte., 2020. Thriving in the era of pervasive AI Deloitte's State of AI in the Enterprise, 3rd Edition. Available at. https://www2.deloitte.com/content/dam/ Deloitte/nl/Documents/innovatie/deloitte-nl-exec-deck-state-of-ai-in-the-enterprise-3rd-edition-final.pdf (Accessed: 19 February 2021)

Dorosh, I. (2023). Cyber security and its role in the financial sector: threats and protection measures. Economics. Fi-finances. Law, 10, 48–51. doi: 10.37634/efp.2023.10.10

Emon, Kalyan, Chowdhury. (2023). Blockchain Technology and the Future of Accounting. Deleted Journal, 1-7. doi: 10.18311/dbijb/2023/33982

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*, *33*(3), 183-200. https://doi.org/10.2308/isys-52374

Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, *48*, 100598.

Hassan, A., & Ahmed, K. (2023). Cybersecurity's impact on customer experience: an analysis of data breaches and trust erosion. *Emerging Trends in Machine Intelligence and Big Data*, *15*(9), 1-19.

Hilary**,** G., & Liu, L. X. (2021). Blockchain and other distributed ledger technologies in finance. *The Palgrave Handbook of Technological Finance*, 243-268.

Ibrahim, D., (2023). Opportunities, Challenges and Implications of Blockchain Technology for Accounting: An Exploratory Study. *Alexandria Journal of Accounting Research*, *7*(3), 173-220. doi: 10.21608/aljalexu.2023.320489

Ivanov, N., Li, C., Yan, Q., Sun, Z., Cao, Z., & Luo, X. (2023). Security Defense For Smart Contracts: A Comprehensive Survey. *arXiv preprint arXiv:2302.07347*.

Jadwani, H., Shukla, H., Verma, R., & Dhanda, N. (2024). 22 Cybersecurity Techniques for Business and Finance Systems. *Data-Driven Modelling and Predictive Analytics in Business and Finance: Concepts, Designs, Technologies, and Applications*, 391.

Kalat, D. (2020). Demystifying Blockchain and Cryptocurrencies. *The Journal of Robotics, Artificial Intelligence & Law*, *3*.

Kumar, A., & Sharma, K. (2021). Digital transformation and emerging technologies for COVID-19 pandemic: Social, global, and industry perspectives. *artificial intelligence and machine learning for covid-19*, 73-96.

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, 14, 2901-2925.

:Khanom, T. 2020. The Accountancy Profession in the Age of Digital Transformation Challenges and Opportunities. International Journal of Creative Research Thoughts (IJCRT) 8(2).

Krumay**,** B., Bernroider, E. W., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In *Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23* (pp. 369-384). Springer International Publishing.

Lehenchuk, S. F., Tsaruk, I. M., & Nazarenko, T. P. (2021). Pryntsypy zakhystu danykh u systemi obliku: upravlinski aspekty [Principles of data protection in the accounting system: management aspects]. Ekonomika, upravlinnia ta administruvannia–Economics, management and administration, 2 (96), 61–69.

Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies*, *2022*(1), 7384000**.**

Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies*, *2022*(1), 7384000**.**

McCallig, J., Robb, A., & Rohde, F. (2019). Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain. *International Journal of Accounting Information Systems*, *33*, 47-58.

Musa, A. (2019). The role of IFRS on financial reporting quality and global convergence: a conceptual review. *International Business and Accounting Research Journal*, *3*(1), 67-76.

Ndri, A. (2023). *The* Applications of Blockchain to Cybersecurity. *Culminating Projects in Information Assurance*. 141. https://repository.stcloudstate.edu/msia_etds/141

Odeyemi, O., Okoye, C. C., Ofodile, O. C., Adeoye, O. B., Addy, W. A., & Ajayi-Nifise, A. O. (2024). *Integrating* AI with blockchain for enhanced financial services security. *Finance & Accounting Research Journal*, *6*(3), 271-287.

O'Leary, D. E. (2019). Some issues in *blockchain* for accounting and the supply chain, with an application of distributed databases to virtual organizations. *Intelligent Systems in Accounting, Finance and Management*, *26*(3), 137-149.

Petratos, P. (2024). Triple-Entry Accounting and System Integration. *Journal of Risk and Financial Management*, *17*(2), 45.

Polishchuk, V., Fedirko, N., Grytsyshen, D., Ohdanskyi, K., & Kotkovskyy, V. (2024). Analysis of the Impact of Cybersecurity on The Stability of Financial Institutions. *International Journal of Religion*, *5*(9), 302-309. doi: 10.61707/hfrv6059

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, 9(4), 1972-1986.

Qin, S. (2022). A Review of Research on the Impact of Blockchain on Financial Reporting. Accounting, Auditing and Finance, 3(1), 51-58. http://dx.doi.org/10.23977/accaf.2022.030108

Rabinowitz, R. (2020). From Securities to Cybersecurity: The SEC Zeroes in on Cybersecurity. *BCL Rev.*, *61*, 1535.

Rahmawati, M. I., Sukoharsono, E. G., Rahman, A. F., & Prihatiningtias, Y. W. (2023, June). Demistifying of Triple-Entry Accounting (TEA): Integrating the Block. In *Ninth Padang International Conference on Economics Education, Economics, Business and Management, Accounting and Entrepreneurship (PICEEBA 2022)* (pp. 23-31). Atlantis Press.

Sarker, I. & Datta, B., (2020). BLOCK CHAIN: AN EMERGING TECHNOLOGY SET TO REWIRE THE FINANCE AND BANKING SECTOR. http:// www.researchgate.net

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, 52, 1893-1907.

Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. FRB of St. Louis Review.

Smith, K. J., & Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance*, *46*(6), 833-8*48*. https://doi.org/10.1108/MF-06-2019-0314

Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Buenzli, F. and Vechev, M. (2018), "Securify: practical security analysis of smart contracts", Proceedings

of the 2018 ACM SIGSAC *Conference on Computer and Communications Security*, October, pp. 67-82.

Zaazaa, O., & Bakkali, H. E. (2023). Unveiling the landscape of smart contract vulnerabilities: A detailed examination and codification of vulnerabilities in prominent blockchains. *arXiv preprint arXiv:2312.00499*

Zadorozhnyi, Z., Muravskyi, V., & Shevchuk, O. (2020). The accounting system as the basis for organising enterprise cybersecurity. *Financial and credit activity: problems of theory and practice*, *3*(34), 147-156.

Zhang, J., Zhang, X., Liu, Z., Fu, F., Nie, J., Huang, J., & Dreibholz, T. (2023, November). A Survey of Security Vulnerabilities and Detection Methods for Smart Contracts. In *International Conference on Computer Engineering and Networks* (pp. 436-446). Singapore: Springer Nature Singapore.

Zhou, W., & Sun, M. (2022, April). Accounting Cyber Security Based on Blockchain. In 2022 IEEE Asia-Pacific *Conference on Image Processing, Electronics and Computers* (IPEC) (pp. 1254-1257). IEEE. doi: 10.1109/ipec54454.2022.9777549