مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

تأثير الامن السيبراني في تعزيز تقنية سلسلة الكتل وانعكاسه على موثوقية التقارير المالية الرقمية

أ.د كرار سليم عبد الزهرة حميدي
جامعة الكوفة، كلية الإدارة والاقتصاد
Karrars.hameedi@uokufa.edu.iq

امير عيسى زحزوح الزيادي
وزارة الصحة، دائرة صحة النجف
amerri.alziyadi@student.uokufa.edu.iq

المستخلص

يهدف البحث إلى دراسة تأثير الأمن السيبراني على تعزيز تقنية سلسلة الكتل وتأثير ذلك في موثوقية التقارير المالية الرقمية. تزداد أهمية سلسلة الكتل في العصر الرقمي كآلية لامركزية وآمنة تضمن حماية المعاملات المالية، مما يزيد من الشفافية ويقلل من التلاعب بالبيانات. كما يُعد الأمن السيبراني عاملاً أساسياً في حماية هذه المعاملات ضد التهديدات المتزايدة مثل الاختراقات والتلاعب. يتناول البحث مفهوم الأمن السيبراني وأهمية تأمين البيانات في البيئة الرقمية، وكيفية استفادة سلسلة الكتل من تعزيز الأمان. كما يُظهر تأثير هذه التقنية في تحسين عمليات التدقيق المالي والامتثال للأطر القانونية. استخدم البحث المنهج الوصفي التحليلي لجمع البيانات من خلال استبيانات تم توزيعها على المحاسبين والمدققين والمستثمرين، حيث تم استرجاع 125 استمارة. أظهرت النتائج وجود تأثير معنوي للأمن السيبراني في تعزيز فعالية سلسلة الكتل وتحسين موثوقية التقارير المالية. توصي الدراسة بضرورة تعزيز تطبيق الأمن السيبراني والتحول الرقمي لضمان موثوقية التقارير المالية.

الكلمات المفتاحية (الامن السيبراني ، تقنية سلسلة الكتل، موثوقية التقارير المالية الرقمية)

مجلة الغري للعلوم الاقتصادية والادارية

مجلد (21) عدد (2) 2025

The impact of cybersecurity in enhancing blockchain technology and its reflection on the reliability of digital financial reports

Prof. Dr. Karrar SaleemHameedi

University of Kufa, Faculty of Administration and Economic

Karrars.hameedi@uokufa.edu.iq

Ameer Issa Zahzouh Al -Ziyadi

Ministry of Health, Najaf Health Department

amerri.alziyadi@student.uokufa.edu.iq

Abstract

The research aims to study the impact of cybersecurity on enhancing blockchain technology and its effect on the reliability of digital financial reports. The importance of blockchain technology in the digital age is increasing as it provides a decentralized and secure mechanism that ensures the protection of financial transactions, enhancing transparency and reducing data manipulation. Cybersecurity is also a key factor in safeguarding these transactions against growing threats such as hacks and tampering. The research discusses the concept of cybersecurity and the importance of securing data in the digital environment, as well as how blockchain technology benefits from enhanced security. It also demonstrates the impact of this technology on improving financial auditing processes and compliance with legal frameworks. The study employed a descriptive analytical approach to collect data through questionnaires distributed to accountants, auditors, and investors, with 125 forms retrieved. The results showed a significant impact of cybersecurity on enhancing the effectiveness of blockchain technology and improving the reliability of financial reports. The study recommends the need to strengthen the application of cybersecurity and digital transformation to ensure the reliability of digital financial reports.

Keywords*: (*cyber security, bloc technology, reliability of digital financial reports)

1- المقدمة

تواجه الوحدات الاقتصادية تحديات كبيرة في عصر التكنولوجيا الرقمية بسبب تزايد الهجمات الإلكترونية التي تهدد البيانات المالية الحساسة. يُعد **الأمن السيبراني** أداة أساسية لحماية هذه البيانات من المخاطر الرقمية من خلال مجموعة من التدابير التكنولوجية والإدارية التي تضمن سرية

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

وسلامة المعلومات. في المقابل، تعتبر **تقنية سلسلة الكتل** ابتكارًا تكنولوجيًا يحقق ثورة في المعاملات المالية الرقمية، حيث تسجل المعاملات في سلاسل مشفرة تُتحقق منها شبكة لامركزية، مما يساهم في تقليل المخاطر المرتبطة بالتلاعب أو الاحتيال المالي ويعزز الشفافية.في ظل تزايد الاعتماد على **التقارير المالية الرقمية**، أصبح من الضروري تكامل تقنيات مثل **الأمن السيبراني** و **سلسلة الكتل** لضمان دقة وموثوقية البيانات المالية وحمايتها من التلاعب. يهدف البحث إلى دراسة العلاقة بين هذين العنصرين وكيفية تكاملها لتحسين أمان المعاملات المالية وحمايتها من المخاطر الرقمية، كما يسعى لاستكشاف تأثير هذا التكامل على موثوقية التقارير المالية الرقمية. النتائج أظهرت أن الجمع بين هذه التقنيات يعزز حماية البيانات المالية، ويزيد من الشفافية في التقارير المالية، مما يرفع من الثقة في النظام المالي بشكل عام.

المبحث الأول
منهجية البحث وبعض الدراسات السابقة

اولاً: منهجية البحث

يسعى هذا المبحث لدراسة مشكلة البحث، واهمية البحث ، واهداف البحث، وفرضيات البحث، ومنهجية البحث، والمخطط الاجرائي للبحث.

1- مشكلة البحث

في ظل الثورة الرقمية المتسارعة، أصبحت المعلومات المالية جزءًا أساسيًا من العمليات التجارية. تعتمد المؤسسات بشكل متزايد على التقنيات الحديثة لتعزيز الشفافية والكفاءة في التعاملات المالية. ومع ذلك، يزداد الاعتماد على هذه التقنيات بشكل متزايد مع تزايد التهديدات السيبرانية التي يمكن أن تؤدي إلى فقدان البيانات أو تلاعب بها، مما يثير تساؤلات حول مدى موثوقية التقارير المالية التي تعتمد على هذه التقنيات. تتمثل المشكلة الرئيسية في عدم وضوح العلاقة بين الأمن السيبراني وتقنية سلسلة الكتل، وغياب فهم عميق لكيفية تأثير الأمن السيبراني على تعزيز فعالية سلسلة الكتل في تحسين موثوقية التقارير المالية الرقمية. يتفاقم هذا الوضع بسبب التهديدات المتزايدة التي تواجهها الأنظمة المالية الرقمية، مما يجعل المؤسسات تواجه تحديات متعلقة بالأمان والموثوقية. وبذلك يمكن صياغة المشكلة كالتالي:

1- ما هو أثر تطبيق الامن السيبراني وتفرعاته في تعزيز تقنية سلسلة الكتل ؟

2- عند تطبيق الامن السيبراني ما هو دورة في موثوقية التقارير المالية الرقمية ؟

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

3- كيف يؤثر تطبيق تقنية سلسلة الكتل على موثوقية التقارير المالية الرقمية ؟

4- كيف يساعد تطبيق الامن السيبراني في تعزيز تقنية سلسلة الكتل بما يحقق موثوقية التقارير المالية الرقمية ؟

2- اهداف البحث

حول "تأثير الأمن السيبراني في تعزيز تقنية سلسلة الكتل وانعكاسها على موثوقية التقارير المالية الرقمية" يمكن أن تتنوع وتعتمد على الزاوية التي يتم التركيز عليها في الدراسة. ولكن يمكن تلخيص الأهداف الرئيسية التي يمكن أن يتناولها البحث كالتالي:

- تحليل تأثير الأمن السيبراني على تقنية سلسلة الكتل ودوره في تعزيز أمانها.
- دراسة العلاقة بين الأمن السيبراني وموثوقية البيانات في تقنية سلسلة الكتل .
- فحص تأثير الأمن السيبراني على موثوقية التقارير المالية الرقمية.
- استكشاف التحديات الأمنية في تطبيقات تقنية سلسلة الكتل وتأثيرها على التقارير المالية الرقمية.
- اقتراح حلول لتحسين الأمان وزيادة موثوقية التقارير المالية الرقمية باستخدام تقنيات سلسلة الكتل

3- أهمية الدراسة

تتمثل أهمية هذه الدراسة في فحص تأثير الأمن السيبراني على تعزيز فعالية تقنية سلسلة الكتل في القطاع المالي. مع تزايد التهديدات والهجمات الإلكترونية، تصبح حماية البيانات المالية أمرًا حيويًا. تسهم الدراسة في فهم كيفية تكامل الأمن السيبراني مع البلوك تشين لضمان بيئة مالية آمنة وشفافة.كما أن الدراسة تهدف إلى تحسين دقة وموثوقية التقارير المالية الرقمية، مما يعزز الثقة في النظام المالي ويقلل من مخاطر التلاعب أو الاحتيال. هذه الدراسة ذات أهمية للمؤسسات المالية، وصناع القرار، حيث تقدم رؤى حول كيفية تعزيز الأمان في المعاملات المالية الرقمية باستخدام تقنيات متكاملة.

4- فرضيات الدراسة

لتحقيق أهداف البحث والإجابة على التساؤلات المطروحة في مشكلة البحث، يمكن صياغة فرضية الدراسة على النحو التالي :

الفرضية الأولى: يوجد تأثير ذو دلالة إحصائية لتطبيقات الامن السيبراني في تقنية سلسلة الكتل .

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

الفرضية الثانية: يوجد تأثير ذو دلالة إحصائية للأمن السيبراني في موثوقية التقارير المالية الرقمية.

الفرضية الثالثة: يوجد تأثير ذو دلالة إحصائية لتطبيقات تقنية سلسلة الكتل على موثوقية التقارير المالية الرقمية.

الفرضية الرابعة: يوجد تأثير ذو دلالة إحصائية للأمن السيبراني في موثوقية التقارير المالية الرقمية من خلال تقنية سلسلة الكتل.

5- حدود البحث

1- الحدود المكانية : تحديدها من خلال استهداف مجموعة من المدققين الداخليين، مراقبي الحسابات، والمستثمرين في القطاع الخاص و القطاع العام .حيث تم توزيع 150 استمارة استبيان على هؤلاء المشاركين في الدراسة، شملت مؤسسات مالية ومحاسبية متعددة في كلا القطاعين، بهدف جمع بيانات شاملة تساعد في تحليل تأثير الأمن السيبراني على تقنية سلسلة الكتل في التقارير المالية الرقمية.

2- الحدود الزمانية : تم توزيع استمارات الاستبيان خلال الفترة الزمنية الممتدة من 2024/12/1 إلى 2025/2/23.

3- محكمين الاستبيان : تم تحكيم الاستبيان من قبل مجموعة من المحكمين المتخصصين في مجالات التدقيق والحسابات شملت هذه المجموعة أكاديميين وخبراء في مجالات الإدارة المالية والمحاسبة قام المحكمون بمراجعة الأسئلة والتأكد من ملاءمتها للموضوع البحثي وضمان دقتها ووضوحها. وبناءً على ملاحظاتهم تم إجراء التعديلات اللازمة لضمان صلاحية الاستبيان قبل توزيعه على العينة المستهدفة.

ثانياً: دراسات سابقة

دراسات سابقة باللغة العربية	
1 - دراسة (صبر، وأخرون: 2022):	
عنوان الدراسة	تقنية سلسلة الكتل " Blockchai "واثرها في تحسين التقارير المالية الرقمية (دراسة تحليلية)
عينة الدراسة	يتكون مجتمع الدراسة من مجموعة من المحاسبين والمدققين في المصارف العراقية وأساتذة الجامعات.
اداة الدراسة	استبيان من 62 عينة وتم استرجاع 60 عينة.
اهداف الدراسة	يهدف هذا البحث الى التعرف على تقنية سلسلة الكتل و بيان أثرها في تحسين التقارير المالية الرقمية.
أهم الاستنتاجات	أن استخدام تقنية سلسلة الكتل يساعد في توفير درجة عالية من الموثوقية في التقارير المالية الرقمية المنشورة للمصارف عبر شبكة الأنترنت، وضمان سرعة إكمالها وإنجازها، وتحافظ على خصوصية وسرية المعلومات الواردة في التقارير المالية الرقمية للمصارف والوصول إليها في أي وقت وفي أي مكان.
2- دراسة (عبادي :2023)	

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

عنوان الدراسة	تكنلوجيا الامن السيبراني وانعكاس تطبيقه على جودة التقارير المالية .
عينة الدراسة	يتكون مجتمع الدراسة من المدققين الداخليين والخارجيين العاملين في دوان الرقابة المالية في النجف وبابل وكربلاء.
اداة الدراسة	استبيان من 117 استمارة.
اهداف الدراسة	تهدف هذه الدراسة إلى تحديد أدوار المدققين من خلال توضيح مفهوم ومخاطر الامن السيبراني في حماية المعلومات والبيانات المالية في الوحدة الاقتصادية.
أهم الاستنتاجات	ان اعتماد الامن السيبراني يحسن من جودة التقارير المالية عبر ما يحققه من اظهار المعلومات بمصداقية وشفافية وبما يلائم احتياجات المستخدمين للأمن السيبراني من دور في إدارة الموارد الاقتصادية بفعالية اكبر للحصول على منافع وكذلك وجود اثر لخصوصية بيانات الزبائن وإدارة المخاطر وان خصوصية بيانات الزبائن كان لها الأثر الأكبر على جودة التقارير المالية.
دراسات سابقة اجنبية	
1- (Gimenez et al., 2021):	
عنوان الدراسة	Achieving cybersecurity in blockchain-based systems: A survey تحقيق الأمن السيبراني في الأنظمة المعتمدة على تقنية سلسلة الكتل: مسح شامل
عينة الدراسة	تم تحليل 272 ورقة بحثية من عام 2013 إلى 2020، بالإضافة إلى 128 تطبيقًا صناعيًا .لذلك، تشمل العينة الدراسات الأكاديمية والابتكارات الصناعية المتعلقة بالأمن السيبراني في الأنظمة المعتمدة على تقنية سلسلة الكتل
مدة الدراسة	فترة الدراسة تمتد من عام 2013 - 2020
اداة الدراسة	تم استخدام التحليل الأدبي (مراجعة الأدبيات) كأداة رئيسية في الدراسة، حيث تم تحليل الأوراق البحثية والدراسات الصناعية التي تناولت الأمن السيبراني في أنظمة تقنية سلسلة الكتل
اهداف الدراسة	يهدف إلى تقديم مراجعة شاملة للتقنيات والعناصر التي تم اقتراحها لتحقيق الأمن السيبراني في الأنظمة القائمة على ت. يهدف التحليل إلى استهداف الباحثين في هذا المجال، ومتخصصي الأمن السيبراني ومطوري تقنية سلسلة الكتل.
أهم الاستنتاجات	تعتبر تقنية سلسلة الكتل تقنية تمكينيه تمهد الطريق لخدمات أكثر ذكاءً وتعزيزًا، مما يساهم في الأمان السيبراني.

المبحث الثاني

69الجانب النظري

1-2 مفهوم الامن السيبراني Cyber Security Concept:

ظهور مصطلح "الأمن السيبراني" أصبح من الواضح أن الأمن، والفضاء السيبراني يتفاعلان مع بعضهما البعض إذ يُنظر إلى الأمن السيبراني على أنه مجموعة من الأدوات الفنية والإدارية المستخدمة لحماية شبكات الكمبيوتر من سوء الاستخدام والوصول غير المصرح به مع استعادة أي بيانات إلكترونية قد تكون مفقودة إذ أن عمل نظم المعلومات في ضمان وحماية خصوصية بيانات الجهات الفاعلة في الفضاء الإلكتروني (الكرعاوي،35:2024).

2- أهمية الأمن السيبراني:

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

يعد الأمن السيبراني عنصرًا أساسيًا لحماية البيانات في العالم الرقمي، حيث يبرز أهميته على المستويات الشخصية، المؤسسية، والوطنية. على المستوى الشخصي، يساهم في حماية البيانات الحساسة مثل الحسابات البنكية. بالنسبة للمؤسسات، يعد أساسيًا لحماية البيانات الاقتصادية والاجتماعية من المخاطر المتزايدة. أما على المستوى الوطني، فإنه يساهم في حماية المعلومات الاستراتيجية ويقلل من التهديدات التي قد تؤثر على الاستقرار الاقتصادي والأمني للدول AI). Bayati, 2022:5)

3- أنواع الامن السيبراني

الأمن السيبراني يتضمن عدة أنواع لحماية المعلومات والأنظمة من التهديدات. أبرز هذه الأنواع:

1. **أمن التطبيقات** :يركز على حماية البرمجيات والتطبيقات من الثغرات الأمنية، مثل هجمات حقن SQL.يشمل التشفير واختبارات الأمان وتحديث البرمجيات دورياً لتعزيز الحماية (Han et al., 2021:3197)
2. **الأمن السحابي** :يضمن حماية البيانات والتطبيقات التي تعتمد على الخدمات السحابية مثل Google Cloudو .AWSيشمل استخدام تقنيات التشفير والمراقبة المستمرة للكشف عن الأنشطة غير العادية (Chandra, 2019: 2072) .
3. **الأمن التشغيلي** :يركز على حماية البيانات أثناء العمليات النظامية، من خلال سياسات الوصول وإدارة الهوية للتحكم في النظام (Mijwil & Salem, 2023:9) .

4- أسباب ارتكاب الجرائم السيبرانية:

تعد الجرائم السيبرانية من التحديات الكبرى التي تواجه المجتمعات الحديثة، وتنشأ لأسباب متعددة تشمل دوافع مالية، انتقامية، نفسية، واجتماعية. من أبرز هذه الأسباب (Pande,2017:18)

1. المال :يُعتبر الدافع المالي من الأسباب الرئيسية لارتكاب الجرائم السيبرانية، حيث يسهل الحصول على الأموال بسرعة عبر الإنترنت.
2. الانتقام :يسعى بعض الأفراد للانتقام من أشخاص أو مؤسسات عبر تدمير السمعة أو إحداث ضرر اقتصادي.
3. الهواية :يشارك البعض في الجرائم السيبرانية بدافع الفضول أو لاختبار مهاراتهم التقنية دون فهم عواقب أفعالهم.

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

4. التفاخر :يلجأ آخرون للتفاخر بقدراتهم عبر اختراق الأنظمة أو تطوير أدوات غير قانونية.
5. إخفاء الهوية :يتيح الإنترنت إخفاء الهوية، مما يعطي بعض الأفراد شعورًا بالأمان عند ارتكاب الجرائم السيبرانية.
6. التجسس السيبراني :يرتكب بعض الأفراد التجسس على المعلومات الحساسة لأغراض سياسية أو اقتصادية للحصول على بيانات استراتيجية .

5- التهديدات السيبرانية لأنظمة المعلومات المحاسبية:

تشكل التهديدات السيبرانية مخاطر كبيرة على أنظمة المعلومات المحاسبية، التي تتطلب تدابير قوية في مجال الأمن السيبراني لحماية البيانات المالية الحساسة. (Muravskyi et al., 2021:172)

1. تطور التهديدات :يتطلب التطور المستمر للتهديدات السيبرانية مراقبة دائمة وتكييف بروتوكولات الأمان للتخفيف من المخاطر المحتملة .
2. أهمية الجودة :جودة وموثوقية المعلومات المحاسبية تعد أمراً حيوياً، خاصةً مع تزايد التهديدات السيبرانية.
3. زيادة التعقيد :أدت تعقيدات عمليات المعلومات في المحاسبة والتقدم التكنولوجي إلى زيادة استهداف أنظمة المعلومات المحاسبية بالتهديدات السيبرانية .(Cha et al., 2020:641)

2-2 تقنية سلسلة الكتل Series of block technology

ان تقنية سلسلة الكتل تتميز بتعدد فوائدها، وتعود تسميتها إلى طبيعة عملها في تسجيل البيانات وحفظها. تعمل هذه التقنية على تسجيل كل معاملة تتم داخل الشبكة، حيث ترتبط الكتل ببعضها البعض بشكل متسلسل. تعتبر سلسلة الكتل جيلًا جديدًا من تطبيقات البيانات التي تعزز الثقة والمساءلة والشفافية، وتساهم في تبسيط العمليات التجارية. على الرغم من أنها ارتبطت بشكل رئيسي بعملة البيتكوين Bitcoin، إلا أن استخداماتها تمتد إلى ما هو أبعد من ذلك. من خلال تقنية سلسلة الكتل، يمكن إعادة تصور المعاملات التجارية الأساسية، مما يفتح المجال أمام ابتكارات جديدة في التفاعلات الرقمية. أساسًا، تعتبر تقنية سلسلة الكتل وسيلة فعالة لنقل ملكية الأصول والحفاظ على المعلومات بدقة عالية. في مجال المحاسبة، تساهم هذه التقنية في قياس وتحليل البيانات المالية وإصدار التقارير. كما توفر وضوحًا بشأن ملكية الأصول والالتزامات، وتعزز من مهنة المحاسبة عن طريق تقليل

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

تكاليف تسويات البيانات وتوفير الشفافية اللازمة حول ملكية الأصول وتواريخ اقتنائها-Abu Al Khair,2023:44).

1- أنواع تقنية سلسلة الكتل

تقنية سلسلة الكتل تعتمد على أنواع متعددة تستخدم للتحقق والمصادقة على المعاملات الرقمية. تلخص الأنواع الرئيسية كما يلي:

1. **سلسلة الكتل العامة** :سلسلة مفتوحة لا تتطلب إذنًا خاصًا، مثل "البيتكوين"، حيث يمكن لأي شخص الدخول والمشاركة دون قيود.(Wust & Gervais, 2018:46)
2. **سلسلة الكتل الخاصة** :سلسلة مغلقة تتطلب إذنًا للدخول من قبل جهة مركزية، وتُستخدم مثلًا في سلاسل التوريد الخاصة بالشركات.(Dijkstra, 2017:36)
3. **سلسلة الكتل المختلطة** :تجمع بين مزايا السلاسل العامة والخاصة، حيث تُدار من قبل مجموعة أفراد وتسمح بعدد أكبر من المشاركين، مما يوفر الخصوصية والرقابة (Breiki et al., 2019:251).
4. **سلسلة الكتل الهجينة** :مزيج من السلاسل العامة والخاصة، حيث تكون شبه لامركزية وتشمل شبكة متعددة المؤسسات.(Komalavalli et al., 2020:364)
5. **سلسلة الكتل الكونسورتيوم** :سلسلة شبه لامركزية تُدار من قبل مجموعة مؤسسات، وتُستخدم في مجالات مثل البنوك والمنظمات الحكومية.(Paul et al., 2021:9) .

2 -عناصر تقنية سلسلة الكتل:

تتكون تقنية سلسلة الكتل من عناصر رئيسية تعمل معًا لضمان أمان وموثوقية المعاملات. يمكن تلخيص هذه العناصر كما يلي:

1.الكتلة: وفقًا لما ذكره (Gatteschi et al., 2018:10) تُعد الوحدة الأساسية في السلسلة، حيث تحتوي على معلومات العمليات مثل تحويل الأموال أو تسجيل البيانات. تحتوي كل كتلة على عدد محدد من المعاملات ولا يمكن إضافة أكثر منها حتى تتم المعالجة، مما يضمن دقة التسجيل.

2. المعلومة: تُشير إلى العمليات الفرعية التي تحدث داخل كتلة معينة، مثل سجلات صفقات البيع أو الشراء أو التسويات المصرفية (Lin and Liao, 2017:2) .

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

3. بصمة الوقت :تُسجل وقت إنشاء المعاملة وترتبط مع عملية الهاش. تمنح بصمة الوقت كل عملية طابعًا زمنيًا مميزًا مما يزيد من الأمان ويساهم في الحفاظ على سرية العمليات (Berryhill et al., 2018:27).

3-2 مفهوم التقارير المالية الرقمية The concept of digital financial reports

أشارت دراسة (Schnackenberg & Tomlinson, 2016: 7) إلى أن أهمية التقارير المالية الرقمية ودورها في الافصاح عن المعلومات المالية وغير المالية المنشورة ترتبط بالتحول الذي طرأ على دور المحاسبة. فقد انتقلت المحاسبة من كونها وسيلة لإثبات حقوق الملكية إلى نهج يركز على ضمان جودة وسلامة التقارير المالية ومصداقية المعلومات المحاسبية التي تحتويها، مما يعزز ثقة المستثمرين في تلك التقارير. تتجلى منفعة الإفصاح للمستخدمين في ضمان خلو المعلومات من التحريف والتضليل، وإعدادها وفقًا لمجموعة من المعايير القانونية والرقابية والمهنية والفنية. ومع التطورات الكبيرة في نظم الاتصالات وتكنولوجيا المعلومات، إضافة إلى تطور النظم المحاسبية، أصبح من الضروري على الوحدات الاقتصادية تبني الإفصاح عن تقاريرها المالية الكترونيا. فقد بات الإنترنت أداة رئيسية لنشر المعلومات المالية وغير المالية عبر مواقع الوحدات الاقتصادية الإلكترونية، مما يتيح للمستثمرين والمستفيدين الوصول بسهولة إلى تلك المعلومات.

يرجع التوجه نحو اعتماد التقارير المالية الرقمية إلى المزايا العديدة التي تقدمها، مثل تحسين جودة المعلومات المالية، تسهيل الوصول إليها، وزيادة الكفاءة والشفافية في عملية الإفصاح المالي وتم الإشارة الى هذه المزايا من قبل كل من (Wells & CAANZ, 2020:4) و (Afaq,2018:4).

وكما يلي :-

1- تعزيز فهم المعلومات المالية وزيادة دقتها مع تسهيل الوصول إليها بسرعة.

2- دعم الشفافية والارتقاء بجودة التقارير المالية.

3- رفع مستوى الموثوقية في البيانات المالية المعلنة.

4- تبسيط وإدارة معالجة البيانات التجارية بفعالية.

5- المساهمة في أتمته الإيداعات التنظيمية وتوفيرها بشكل متاح للجمهور.

6- تسهيل تحليل البيانات المالية للمستثمرين، بما في ذلك إجراء مقارنات فعالة بين الوحدات الاقتصادية.

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

7- تعزيز القدرة على إجراء تحليلات شاملة للتقارير المالية، مما يدعم تطبيق اللوائح التنظيمية وتحسين القرارات المالية.

8- تقليل التكاليف على مستخدمي التقارير المالية من خلال توفير إمكانية التنقل السريع واستخراج المعلومات بكفاءة.

4-2 بيان العلاقة وتأثير الامن السيبراني على تقنية سلسلة الكتل وانعكاسه على موثوقية التقارير المالية الرقمية Specify the relationship and the impact of cyber security on the technique of the series of blocs and its reflection on the reliability of digital financial reports

تعد تقنية سلسلة الكتل من الأدوات القوية في تعزيز الأمان السيبراني، حيث توفر العديد من الفوائد مثل حماية البيانات، نقل البيانات الآمن، ومقاومة الهجمات الإلكترونية. بالرغم من هذه المزايا، تواجه تقنية البلوك تشين تحديات مثل قابلية التوسع، وقابلية التشغيل البيني، والمخاوف التنظيمية التي قد تؤثر على فعاليتها في التصدي للهجمات السيبرانية .(Varghese, 2019:423) تساعد الخصائص الجوهرية لتقنية سلسلة الكتل، مثل اللامركزية والتشفير، في تعزيز تدابير الأمان السيبراني، حيث يمكنها تحسين بروتوكولات الأمان في الأنظمة الرقمية من خلال السجلات الشفافة والدائمة للتهديدات والاعتداءات السيبرانية.(Hassija, 2019:82721)

وتعد تقنية سلسلة الكتل أداة فعالة لتعزيز الأمان في المعاملات المالية وحفظ البيانات الحساسة، حيث تستخدم دوال التجزئة الرياضية لضمان ثبات البيانات واكتشاف التعديلات بشكل واضح .(Han et al., 2023:48)في حين يسهم الأمن السيبراني في حماية المعاملات المالية من خلال تشفير البيانات وتقنيات المصادقة المتعددة لضمان الأمان، مثل استخدام البنية التحتية للمفتاح العام والتوقيعات الرقمية (Taylor, 2020:147).

من جهة أخرى، يعزز الأمان السيبراني في التقارير المالية الرقمية من خلال ضمان سرية البيانات وسلامتها، وهو أمر بالغ الأهمية في حماية المعلومات الحساسة داخل المؤسسات المالية (Ayugi, 2021:14).تعتمد سلامة البيانات على منع التعديلات غير المصرح بها وتجنب الأخطاء أو الفساد، مما يساعد في الحفاظ على دقة المعلومات وموثوقيتها .(Duggineni, 2023:29) تهدف تدابير

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

الأمان السيبراني إلى ضمان أن البيانات المالية تظل آمنة ودقيقة، مما يضمن الثقة في المعاملات المالية والامتثال للمعايير التنظيمية.(Liaw et al., 2021:19) .

كذلك يرى الباحث أن تأثير الأمن السيبراني في تعزيز تقنية سلسلة الكتل يعد ذا أهمية كبيرة على موثوقية التقارير المالية الرقمية في العالم اليوم حيث تتزايد التهديدات السيبرانية، أصبح من الضروري استخدام تقنيات متقدمة مثل البلوك تشين لتحسين حماية البيانات المالية وضمان دقتها وموثوقيتها يعد الدمج بين الأمن السيبراني وتقنية سلسلة الكتل خطوة محورية نحو تحقيق بيئة آمنة للمعاملات المالية.

الجدول 1: وصف متغيرات الدراسة

اسم المتغير	نوع المتغير	رمز المتغير
الامن السيبراني	مستقل	CS
تقنية سلسلة الكتل	وسيط	SB
التقارير المالية الرقمية	تابع	DFR

المبحث الثالث
الجانب العملي

نتائج اختبار فرضيات البحث

الفرضية الاولى:- الفرضية الأولى: يوجد تأثير ذو دلالة إحصائية لتطبيقات الامن السيبراني في تقنية سلسلة الكتل.

لغرض القيام بالاختبار المناسب لهذه الفرضية تم تكوين معادلة الانحدار الخطي الاتية:-

$$BT = B_0 + B_1\, CS + \varepsilon$$

حيث:-

BT = المتغير الوسيط i(تقنية سلسلة الكتل).

CS = المتغير المستقل (الامن السيبراني).

ε = اخطاء التقدير او ما تسمى بالبواقي الإحصائية.

B_0 = ثابت معادلة الانحدار والتي تمثل قيمة المتغير التابع عندما تكون قيمة المتغير المستقل مساوية للصفر.

B_1 = ميل دالة الانحدار والتي تقيس تاثير المتغير المستقل في المتغير التابع.

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

وباستخدام البرنامج الاحصائي SPSS كانت النتائج كالاتي:-

جدول (29) موجز نموذج اختبار الفرضية الاولى

Model Summary[b]				
Mode	R	R Squar	Adjusted R Squ	Std. Error of the Es
1	.755[a]	.570	.565	.315
a. Predictors: (Constant), CS				
b. Dependent Variable: BT				

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

ظهر جدول موجز النموذج أعلاه أن قيمة الارتباط (R) بين المتغيرات بلغت 0.755، وهي قيمة تُشير إلى قوة ارتباط مرتفعة بين المتغيرات. كما بلغ معامل التفسير0.570 (R Square) ، مما يعكس "القوة التفسيرية" للنموذج المستخدم. وهذا يعني أن (الأمن السيبراني) يفسر حوالي 57% من التباين في (تقنية سلسلة الكتل). أما بالنسبة للانحراف المعياري لأخطاء التقدير (Std. Error of the Estimate)، فقد كان 315.0، وهي قيمة منخفضة جدًا، مما يُعتبر مؤشرًا جيدًا حيث يُعتبر انخفاض هذه الأخطاء دلالة على دقة التنبؤات.

جدول (30) تباين اختبار الفرضية الأولى

ANOVA[a]						
Model		Sum of Squ	df[i]	Mean Squ	F	Sig
	Regressio	13.451	1[ii]	13.451	134.9	.000
	Residua	10.164	102	.100		
	Total	23.614	103			
a. Dependent Variable: BT						
b. Predictors: (Constant), CS						

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

يُظهر جدول التباين (ANOVA) أن قيمة F المحسوبة بلغت 134.986، وهي أعلى من القيمة المجدولة التي تبلغ 3.93، بناءً على درجات الحرية (df: 102,1) عند مستوى دلالة 5%. كما بلغ مستوى معنوية الاختبار0.000 (Sig) ، وهو أقل من الحد المقبول للخطأ في تخصصات العلوم الاجتماعية، الذي يُعتبر 0.05. وهذا يشير إلى ملاءمة النموذج الإحصائي المستخدم لاختبار الفرضية.

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

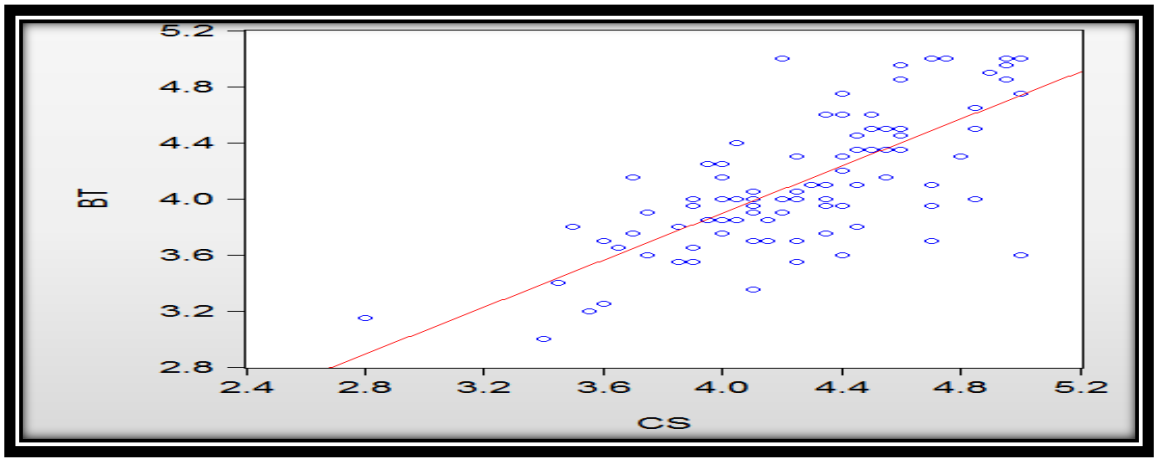
جدول (31) معاملات دالة الانحدار للفرضية الاولى

Coefficients[a]						
Model		Unstandardized Coeffic		Standardized Coeff		Sig
		B	Std. Err	Beta		
	(Consta	.545	.311		1	.08
	CS	.838	.072	.755	1	.00
a. Dependent Variable: BT						

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

يُظهر جدول معاملات دالة الانحدار (Coefficients) أن قيمة ثابت معادلة الانحدار بلغت 0.545، بينما بلغت قيمة ميل معادلة الانحدار 0.838، مما يوضح مقدار ونوع التأثير (من خلال المعامل .B) وتشير القيمة الموجبة للمعامل إلى وجود تأثير طردي بين المتغيرين، بمعنى أنه كلما زاد أحد المتغيرات، يزداد المتغير الآخر أيضًا في (الامن السيبراني) بمقدار درجة واحدة يؤدي الى الزيادة بمقدار 83.8% في (تقنية سلسلة الكتل) مع ثبات كل المتغيرات المستقلة الأخرى، ويلاحظ من الجدول أعلاه أيضا ان مستوى معنوية إحصاءه T للمتغير المستقل بلغت 0.00 وهي اقل بكثير من الخطأ المقبول في العلوم الاجتماعية والمحدد سلفا بمقدار 0.05 وهذا يعني ان بيانات العينة قد وفرت دليلا مقنعا على قبول الفرضية لثبوت الاثر احصائيا.

والشكل الاتي يؤكد العلاقة الطردية بين المتغيرين من خلال الاتجاه الصاعد للمنحنى:



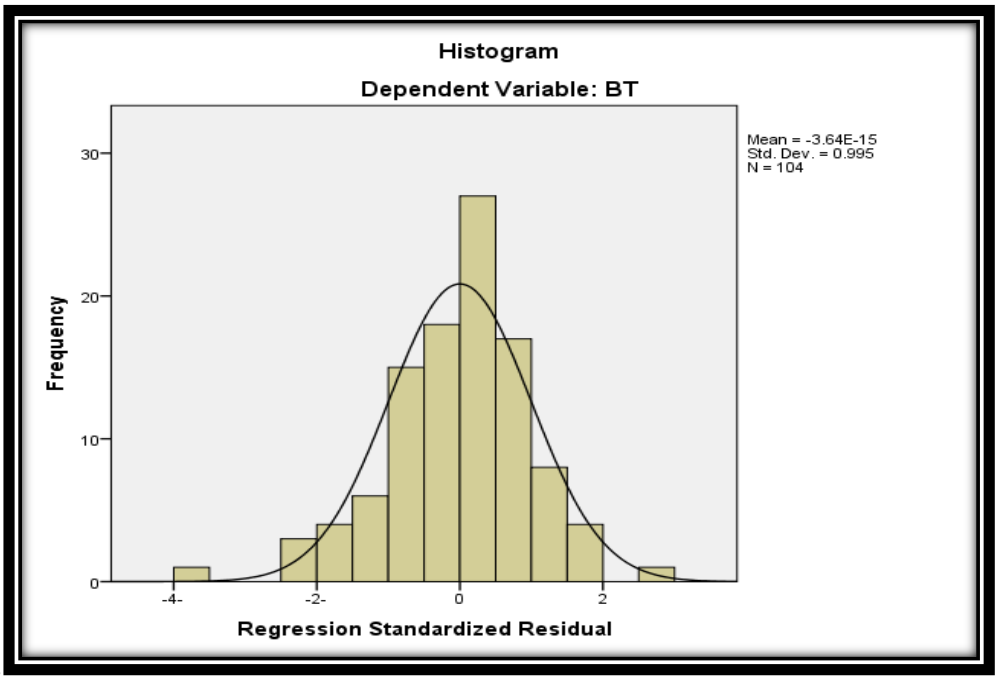
شكل (18) تأثير الامن السيبراني في تقنية سلسلة الكتل

مكن إعادة صياغة معادلة الانحدار التي تم اعتمادها في اختبار الفرضية بناءً على النتائج التي تم التوصل إليها، بحيث يمكن استخدامها للتنبؤ بالشكل التالي:-

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

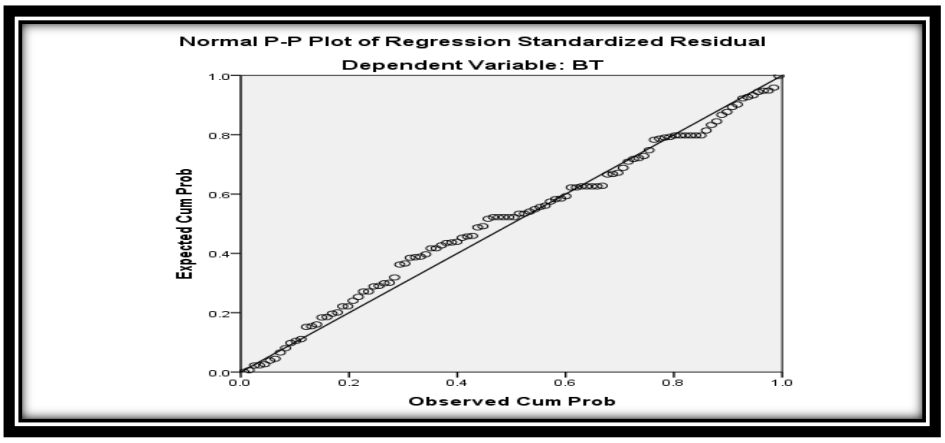
$$BT = 0.545 + 0.838 * CS$$

ويعرض الشكل التالي المدرج التكراري الذي يوضح التوزيع الطبيعي للبواقي الإحصائية لمعادلة الانحدار، مما يعكس دقة معادلة الانحدار السابقة .



شكل (19) المدرج التكراري لبواقي الفرضية الأولى

ويعرض الشكل التالي استيفاء شروط اختبار تحليل الانحدار بشكل بياني، حيث يوضح توزيع النقاط حول الخط المستقيم، مما يثبت أن البواقي الإحصائية تتبع التوزيع الطبيعي.



الشكل (20) التوزيع الطبيعي لبواقي الفرضية الاولى

الفرضية الثانية: - يوجد تأثير ذو دلالة إحصائية للأمن السيبراني في موثوقية التقارير المالية الرقمية

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

لغرض انجاز بالاختبار المناسب لهذه الفرضية تم تكوين معادلة الانحدار الخطي الاتية:-

$$DFRR = B_0 + B_1 CS + \varepsilon$$

حيث:-

DFRR = المتغير التابع (موثوقية التقارير المالية الرقمية).

وباستخدام البرنامج الإحصائيSPSS ، كانت النتائج على النحو التالي:-

جدول (32) موجز نموذج اختبار الفرضية الثانية

Model Summary[b]				
Mod	R	R Squar	Adjusted R Squ	Std. Error of the Es
1	.753[a]	.567	.563	.299
a. Predictors: (Constant), CS				
b. Dependent Variable: DFRR				

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

يبين جدول موجز النموذج (Model Summary) أن قيمة الارتباط (R) بين المتغيرات بلغت 0.753، وهي قيمة عالية تشـــير إلى قوة العلاقة بين المتغيرات. كما بلغ معامل التفســـير (R Square) 0.567، مما يعكس القوة التفسيرية للنموذج المستخدم. وهذا يعني أن (الأمن السيبراني) يفســـر 56.7% من التباين في (موثوقية التقارير المالية الرقمية). أما الانحراف المعياري لأخطاء التقدير (Std. Error of the Estimate) فقد بلغ 299.0، وهو رقم منخفض جداً، مما يعكس دقة التنبؤ. من الناحية الإحصـــائية، كلما انخفضـــت هذه الأخطاء، كان ذلك مؤشـــراً أفضـــل على دقة النموذج.

جدول (33) تباين اختبار الفرضية الثانية

ANOVA[a]						
Model		Sum of Squ	df	Mean Squ	F	Sig
	Regressio	11.989	1	11.989	133.6	.000
	Residual	9.153	101	.090		
	Total	21.142	103			
a. Dependent Variable: DFRR						
b. Predictors: (Constant), CS						

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

يبين جدول التباين (ANOVA) أن قيمة F المحسوبة بلغت 133.604، وهي أكبر من القيمة الجدولية المحددة وفقًا لدرجات الحرية (df = 102, 1) والبالغة 3.93 عند مستوى دلالة 5%. كما

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

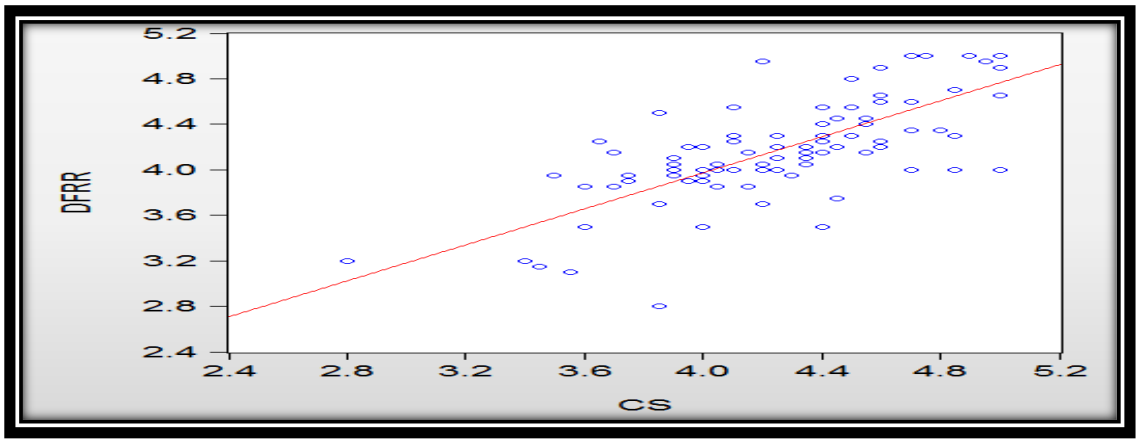
أن مستوى معنوية الاختبار (Sig) بلغ 0.00، وهو أقل من الحد المسموح به للخطأ في تخصصات العلوم الاجتماعية، والذي يتم الاتفاق عليه بأنه 0.05. مما يدل على ملائمة النموذج الإحصائي المستخدم لاختبار الفرضية.

جدول (34) معاملات دالة الانحدار للفرضية الثانية

Coefficients[a]						
Model		Unstandardized Coeffi		Standardized Coe	t	Sig
		B	Std. Err	Beta		
	(Consta	.80	.295		2.74	.00
	CS	.79	.068	.753	11.5	.00
a. Dependent Variable: DFRR						

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

يبين جدول معاملات دالة الانحدار (Coefficients) أن قيمة الثابت في معادلة الانحدار بلغت 0.808، بينما بلغت قيمة الميل 0.791، مما يعكس مقدار ونوع التأثير (من خلال المعامل .(B تشير القيمة الموجبة للمعامل إلى وجود تأثير طردي بين المتغيرين، أي أن زيادة مقدار درجة واحدة في (الأمن السيبراني) تؤدي إلى زيادة قدرها 79.1% في (موثوقية التقارير المالية الرقمية) مع ثبات جميع المتغيرات المستقلة الأخرى. كما يظهر من الجدول أن مستوى معنوية إحصاء T للمتغير المستقل بلغ 0.000، وهو أقل بكثير من الحد المقبول للخطأ في العلوم الاجتماعية والمحدد مسبقاً بـ 0.05. مما يعني أن بيانات العينة قد قدمت دليلاً قوياً لدعم فرضية البحث من حيث ثبوت التأثير إحصائياً. والشكل الاتي يؤكد العلاقة الطردية بين المتغيرين من خلال الاتجاه الصاعد للمنحنى:



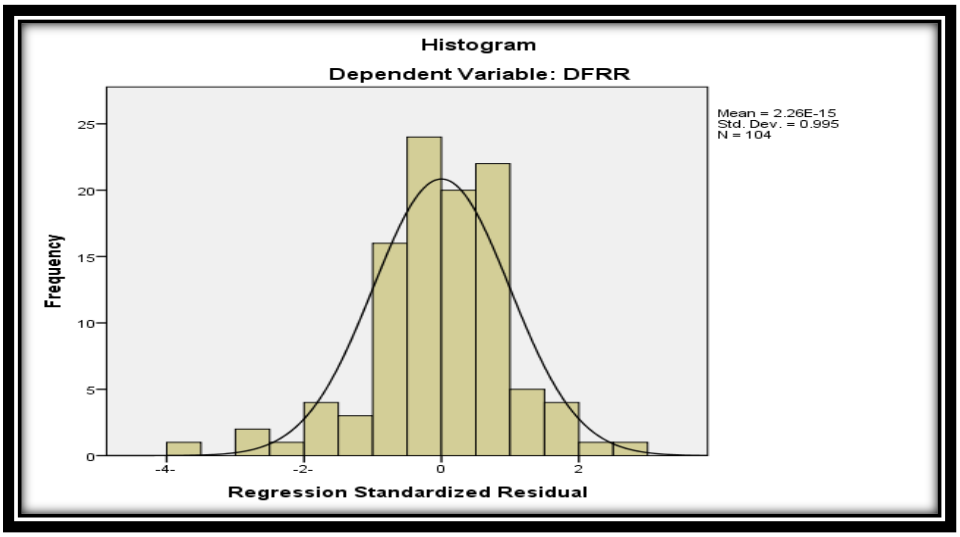
شكل (21) تأثير الامن السيبراني في موثوقية التقارير المالية الرقمية

بناءً على النتائج التي تم التوصل إليها، يمكن إعادة صياغة معادلة الانحدار التي تم اعتمادها في اختبار الفرضية لتصبح قابلة للاستخدام في التنبؤ بالشكل التالي:-

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

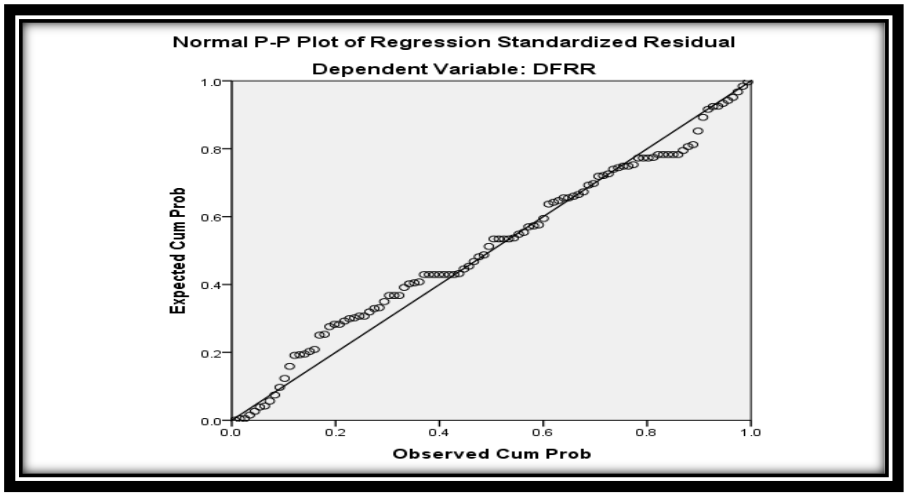
$$DFRR = 0.808 + 0.791 * CS$$

يعرض الشكل التالي المدرج التكراري الذي يوضح التوزيع الطبيعي للبواقي الإحصائية لمعادلة الانحدار، مما يعكس دقة معادلة الانحدار السابقة



شكل (22) المدرج التكراري لبواقي الفرضية الثانية

يوضح الشكل التالي استيفاء شروط اختبار تحليل الانحدار بشكل بياني، حيث يظهر توزيع النقاط حول الخط المستقيم، مما يثبت أن البواقي الإحصائية تتبع التوزيع الطبيعي.



الشكل (23) التوزيع الطبيعي لبواقي الفرضية الثانية

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

الفرضية الثالثة: - وجد تأثير ذو دلالة إحصائية لتطبيقات تقنية سلسلة الكتل على موثوقية التقارير المالية الرقمية

لغرض انجاز بالاختبار المناسب لهذه الفرضية تم تكوين معادلة الانحدار الخطي الاتية:-

$$DFRR = B_0 + B_1 BT + \varepsilon$$

وباستخدام البرنامج الاحصائي SPSS كانت النتائج كالاتي:-

جدول (35) موجز نموذج اختبار الفرضية الثالثة

Model Summary[b]				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.816[a]	.665	.662	.263
a. Predictors: (Constant), BT				
b. Dependent Variable: DFRR				

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

يبين جدول موجز النموذج (Model Summary) أن قيمة الارتباط (R) بين المتغيرات بلغت 0.816، وهي قيمة عالية تشـــير إلى قوة العلاقة بين المتغيرات. كما بلغ معامل التفســـير (R Square) 0.652، مما يعكس القوة التفسيرية للنموذج المستخدم، أي أن (تقنية سلسلة الكتل) تفسر 66.5% من التباين في (موثوقية التقارير المالية الرقمية). أما الانحراف المعياري لأخطاء التقدير (Std. Error of the Estimate)فقد بلغ 263.0، وهو رقم منخفض جداً، مما يعكس دقة التنبؤ. من الناحية الإحصائية، كلما انخفضت هذه الأخطاء، كان ذلك أفضل.

جدول (36) تباين اختبار الفرضية الثالثة

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.006	.226		4.460	.000
	BT	.772	.054	.816	14.242	.000
a. Dependent Variable: DFRR						

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

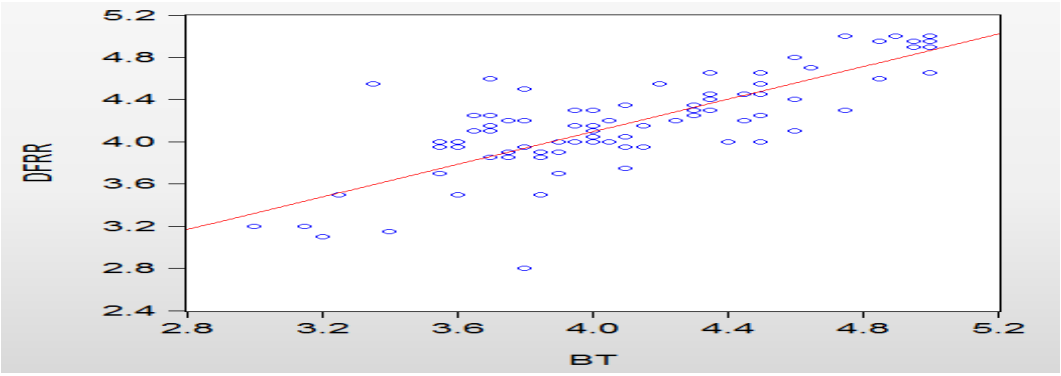
يبين جدول التباين اعلاه anova ان قيمة F المحســـوبة بلغت 133.604 وهي اكبر من القيمة المجدولة المحددة طبقا لدرجات حرية df (102,1) والبالغة 3.93 عند مســـتوى دلالة 5%.وان مســـتوى معنويـة الاختبـار Sig بلغت 0.00 وهي تنخفض عن مقدار الخطـأ الممكن قبولـه في تخصـصـات العلوم الاجتماعية والذي متفق عليه بانه يبلغ 0.05, وهذا ما يدل على ملائمة النموذج الاحصائي المستخدم لاختبار الفرضية.

جدول (37) معاملات دالة الانحدار للفرضية الثالثة

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.006	.226		4.460	.000
	BT	.772	.054	.816	14.242	.000
a. Dependent Variable: DFRR						

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

يبين جدول معاملات دالة الانحدار (Coefficients) أن قيمة الثابت في معادلة الانحدار بلغت 1.006، بينما بلغت قيمة الميل 0.772، مما يعكس مقدار ونوع التأثير (من خلال المعامل .(B تشير القيمة الموجبة للمعامل إلى وجود تأثير طردي بين المتغيرين، أي أن زيادة مقدار درجة واحدة في (تقنية سلسلة الكتل) تؤدي إلى زيادة بنسبة 77.2% في (موثوقية التقارير المالية الرقمية) مع ثبات جميع المتغيرات المستقلة الأخرى. كما يظهر من الجدول أن مستوى معنوية إحصاء T للمتغير المستقل بلغ 0.000، وهو أقل بكثير من الحد المسموح به للخطأ في العلوم الاجتماعية والمحدد مسبقاً بـ 0.05. مما يعني أن بيانات العينة قد قدمت دليلاً قوياً لدعم فرضية البحث من حيث ثبوت التأثير إحصائياً. والشكل الاتي يؤكد العلاقة الطردية بين المتغيرين من خلال الاتجاه الصاعد للمنحنى:



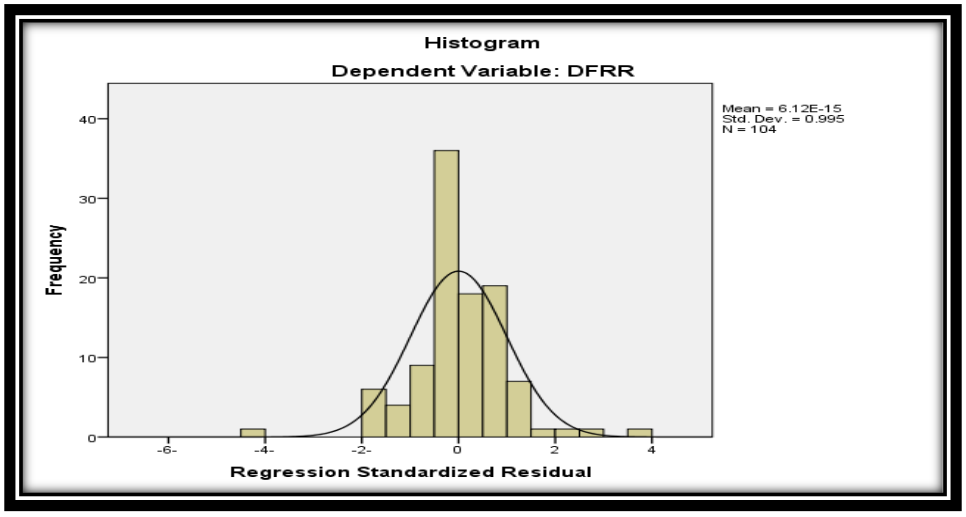
شكل (24) تقنية سلسلة الكتل في موثوقية التقارير المالية الرقمية

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

بناءً على النتائج التي تم التوصل إليها، يمكن إعادة صياغة معادلة الانحدار التي تم استخدامها في اختبار الفرضية لتصبح قابلة للتنبؤ بالشكل التالي:ـ

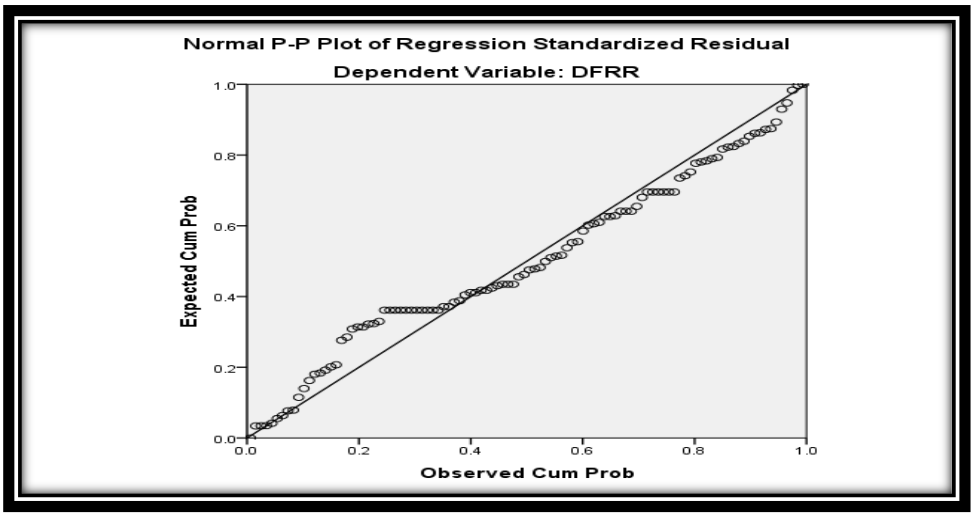
$$DFRR = 1.006 + 0.772 * BT$$

يعرض الشكل التالي المدرج التكراري الذي يوضح التوزيع الطبيعي للبواقي الإحصائية لمعادلة الانحدار، مما يعكس دقة معادلة الانحدار السابقة.



شكل (25) المدرج التكراري لبواقي الفرضية الثالثة

يوضح الشكل التالي استيفاء شروط اختبار تحليل الانحدار بشكل بياني، حيث يظهر توزيع النقاط حول الخط المستقيم، مما يثبت أن البواقي الإحصائية تتبع التوزيع الطبيعي.



الشكل (26) التوزيع الطبيعي لبواقي الفرضية الثالثة

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

الفرضية الرابعة:- : يوجد تأثير ذو دلالة إحصائية للأمن السيبراني في موثوقية التقارير المالية الرقمية من خلال تقنية سلسلة الكتل.

لغرض اختبار هذه الفرضية سيتم استخدام تحليل المسار Path Analysis وهو تحليل يأخذ بنظر الاعتبار العلاقة بين المتغير المستقل والمتغير الوسيط عند قياس تأثيرهما في المتغير التابع، اذ أظهرت نتائج الفرضيات السابقة تحقق شروط تحليل المسار وكالاتي:-

1- ان هناك تأثير للمتغير المستقل (الامن السيبراني) في المتغير الوسيط (تقنية سلسلة الكتل) وهذا ما تم اثباته في الفرضية الاولى.
2- ان يكون هناك تاثير للمتغير الوسيط (تقنية سلسلة الكتل) في المتغير التابع (موثوقية التقارير المالية الرقمية) هذا ما تم اثباته في الفرضية الثالثة.

وباستخدام برنامج Amos الاحصائي كانت النتائج كالاتي:-

جدول (38) نتائج تحليل المسار لاختبار الفرضية الرابعة

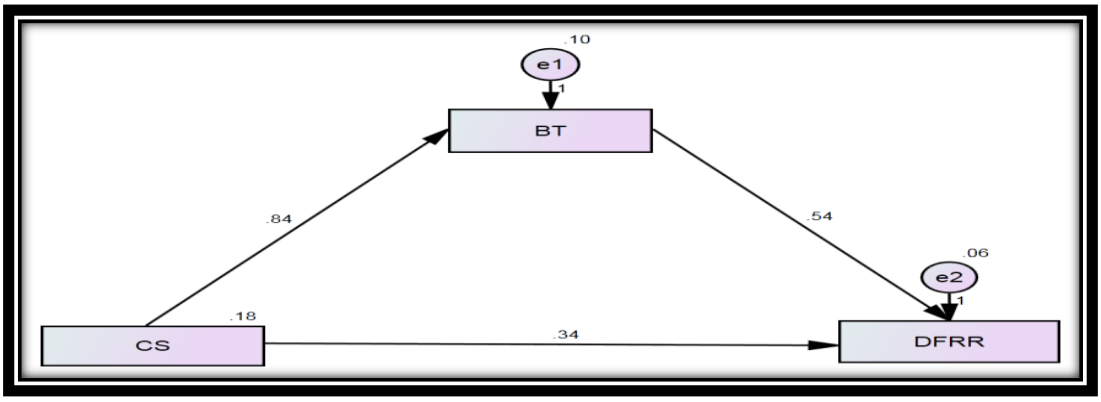
Regression Weights: (Group number 1 - Default model)						
Path			Estimate	S.E.	C.R.	P
BT	<---	CS	0.838	0.072	11.675	0.000
DFRR	<---	BT	0.544	0.077	7.097	0.000
DFRR	<---	CS	0.336	0.085	3.942	0.000

المصدر: من اعداد الباحث استناداً إلى برنامج (spss.23)

يلاحظ من نتائج جدول تحليل المسار path analyses أعلاه ان المتغير المستقل (الامن السيبراني) لا يزال يؤثر في المتغير الوسيط (تقنية سلسلة الكتل) لان قيمة P-Value لها بلغت 0.000 وهي اقل من قيمة الخطأ المقبول في العلوم الاجتماعية والبالغة 0.05، وكذلك فأن المتغير الوسيط (تقنية سلسلة الكتل) لايزال يؤثر في المتغير التابع (موثوقية التقارير المالية الرقمية) لان قيمة P-Value لها بلغت 0.000 وهي اقل من قيمة الخطأ المقبول في العلوم الاجتماعية والبالغة 0.05، كما اننا نلاحظ ان المتغير المستقل (الامن السيبراني) لا يزال له التاثير المعنوي في المتغير التابع (موثوقية التقارير المالية الرقمية) لان قيمة P-Value له بلغت 0.000 وهي اقل من قيمة الخطأ المقبول في العلوم الاجتماعية والبالغة 0.05، وهذا يعني ان متغير تقنية سلسلة الكتل له الوساطة الجزئية في تأثير المتغير المستقل (الامن السيبراني) في المتغير التابع (موثوقية التقارير المالية الرقمية)، أي يوجد تأثير للأمن السيبراني في موثوقية التقارير المالية الرقمية من خلال تقنية

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

سلسلة الكتل وبالتالي يتم قبول فرضية البحث. والشكل الاتي يبين نموذج تحليل المسار لمتغيرات البحث الثلاث.



الشكل (27) نموذج تحليل المسار لاختبار

المبحث الرابع

النتائج والمناقشة والاستنتاجات

اولاً: الاستنتاجات

1. يعزز الأمن السيبراني موثوقية تقنية سلسلة الكتل من خلال توفير بيئة رقمية آمنة تقلل من مخاطر الاختراق والتلاعب بالبيانات المالية المخزنة على الشبكة.
2. تسهم تقنية سلسلة الكتل في تحسين شفافية التقارير المالية الرقمية عبر آليات التحقق اللامركزي، مما يقلل من التلاعب المالي ويعزز مصداقية التقارير.
3. تؤدي تكاملات الأمن السيبراني مع تقنية سلسلة الكتل إلى تقليل مخاطر الجرائم الإلكترونية، مما يعزز استدامة الأنظمة المالية الرقمية وثقة المستخدمين بها.
4. يؤدي الاعتماد المتزايد على الأمن السيبراني وسلسلة الكتل إلى إعادة تشكيل ممارسات التدقيق المالي، حيث يصبح التدقيق أكثر كفاءة وموثوقية بفضل السجلات غير القابلة للتغيير.

ثانياً: التوصيات

1. تعزيز بنية الأمن السيبراني في بيئات تقنية سلسلة الكتل من خلال تطوير بروتوكولات تشفير متقدمة واعتماد معايير أمنية متشددة لضمان حماية البيانات المالية المخزنة والحيلولة دون التهديدات السيبرانية.

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

2. تشجيع المؤسسات المالية والمحاسبية على تبني تقنية سلسلة الكتل في إعداد التقارير المالية الرقمية لما توفره من شفافية وموثوقية، مع ضرورة تطوير أطر تنظيمية تدعم تكامل هذه التقنية مع المعايير المحاسبية الدولية.
3. إجراء دراسات معمقة حول تكامل الأمن السيبراني مع تقنية سلسلة الكتل في العمليات المالية بهدف دراسة تأثير هذه التقنيات على تقليل الاحتيال المالي وتحسين كفاءة عمليات التدقيق والمحاسبة الرقمية.
4. تطوير سياسات وإجراءات رقابية متقدمة لضمان الامتثال التنظيمي عند استخدام تقنية سلسلة الكتل في التقارير المالية الرقمية، مع التركيز على تعزيز دور التدقيق الداخلي والخارجي في تقييم المخاطر السيبرانية.

يوصي الباحث بتكثيف برامج التدريب والتوعية للعاملين في مجال المحاسبة والتدقيق حول الأمن السيبراني وتقنية سلسلة الكتل، لضمان الاستخدام الأمثل لهذه التقنيات في حماية وتحليل البيانات المالية.

المبحث الرابع: المصادر

المصادر العربية

1. الكرعاوي، زهراء مسافر عبيد. (2024)**." دور التدقيق الداخلي القائم على أدارة مخاطر الامن السيبراني وانعكاسه في خفض كلفة التامين"**. مجلة الغري للعلوم الاقتصادية والإدارية. العدد 2. المجلد 20.
2. صبر, ختام رحيم والتميمي, امل محمد سلمان و الشمري, نهلة عبيس طلال.(2022)**." تقنية سلسلة الكتل" Blockchai " واثرها في تحسين التقارير المالية الرقمية "**, مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية, المجلد الرابع عشر . العدد الثاني .
3. عبادي، دعاء سرحان .(2023)**." تكنلوجيا الامن السيبراني وانعكاس تطبيقه على جودة التقارير المالية"**، رسالة ماجستير، جامعة الكوفة، كلية الإدارة والاقتصاد، قسم المحاسبة.

Foreign sources

Abu Al-Khair, Osama Ahmed Mahmoud. (2023). **"A Proposed Framework for Using Blockchain Technology as a Pillar to Enhance the Quality of the Auditing Process in the Context of Digital**

Transformation," Scientific Journal of Administrative Studies and Research, Volume 15, Issue 1.

1. Afaq, Adnan, (2018),**"Digital Financial Reporting, Accounting"** available at The International Journal of Digital Accounting Research Vol. 13.
2. Al Bayati, Q. A. O. (2022). **"The role of cyber security in the efficiency of financial reports in Iraqi universities"** A field study on workers at the AL-Furat AL-Awsat Technical University. Resmilitaris, 12(2), 4777-4792**.**
3. Al Breiki, H., Al Qassem, L., Salah, K., Rehman, M. H. U. & Sevtinovic, D. (2019). **"Decentralized access control for IoT data using Blockchain and trusted oracles"**, In IEEE International Conference on Industrial Internet (ICII) .
4. Ayugi, E. D. (2021). Information Security Strategies and Patient Data Privacy Among Health Facilities in Nairobi (Doctoral dissertation, University of Nairobi).
5. Berryhill, J., Bourgery, T. & Hanson, A. (2018) **"Blockchains unchained: Blockchain technology and its use in the public sector"**,OECD Working Papers on Public Governance,No.28,PP.1-53.
6. Cha, J., Singh, S., Pan, Y., & Park, J. (2020). **"Blockchain-Based Cyber Threat Intelligence System Architecture For Sustainable Computing**". Sustainability, 12(16), 6401.
7. Chandra‹Vijaya, J., Challa, N., & Pasupuletti, S. K. (2019). **"Authentication and authorization mechanism for cloud security"**. *International Journal of Engineering and Advanced Technology*, 8(6), 2072-2078.

8. Dijkstra, M. (2017). " **Blockchain: Towards Disruption in the Real Estate Sector: An Exploration on the Impact of Blockchain Technology in the Real Estate Management Process"**, Master Degree Thesis, Delft University of Technology, Delft, the Netherlands.
9. Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. Science and Technology, 13(2), 29-35.
10. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. & Santamaría, V.(2018). "**Blockchain and smart contracts for insurance: Is the technology mature enough",** Future Internet, Vol.10,No.2, PP.1-16.
11. Gimenez-Aguilar, M., De Fuentes, J. M., Gonzalez-Manzano, L., & Arroyo, D. (2021). **"Achieving cybersecurity in blockchain-based systems: A survey",** Future Generation Computer Systems, 124, 91-118.
12. Han, Dongqi, et al. **"DeepAID: interpreting and improving deep learning-based anomaly detection in secure applications."** Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security.
13. 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.
14. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B.(2019). Sikdar, "A Survey on IoT Security: Application Areas Security Threats and Solution Architectures", IEEE Access, vol. 7, pp. 82721-82743.
15. Komalavalli, C., Saxena, D., & Laroiya, C. (2020). **"Overview of blockchain technology concepts"**, In Handbook of research on blockchain technology (pp. 349-371). Academic Press.

16. Liaw, P., Aithal, P. S., Saavedra, R., & Ghosh, S. (2021). **"Blockchain Technology and its Types—A Short Review",** International Journal of Applied Science and Engineering (IJASE), 9(2), 189-200.
17. Lin, I. C. & Liao, T. C. (2017). "**A survey of Blockchain security issues and challenges",** Ij Network Security,Vol.19, No.5,PP.1-2.
18. Mijwil, M., Salem, I. E. (2023). "**The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity**", A Comprehensive Review. Iraqi Journal For
19. Muravskyi, V., Sverstiuk, A., Andrushchak, I., Chudovets, V., & Koshelyuk, V. (2021). **"Aspects of Protection of Accounting Data in The Conditions of Use of Innovation and Information Technologies".** Computer-Integrated Technologies, (42), 172-176.
20. Pande, J. (2017). **"Introduction to cyber security"**. Technology, 7(1), 11-26
21. Paul, P., Aithal, P. S., Saavedra, R., & Ghosh, S. (2021). **"Blockchain Technology and its Types—A Short Review",** International Journal of Applied Science and Engineering (IJASE), 9(2), 189-200.
22. Schnackenberg, A.K and Tomlinson. (2016) . **"Organizational transparency : A new perspective on managing trust in organization-stakeholder relationships"**, Journal of Management, 42(7) .
23. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," Digital Communications and Networks, vol. 6, no. 2, pp. 147–156, 2020.
24. Varghese V, Sundeep Desai S, Nene MJ. (2019). Decision making in the battlefield-of-things. Wireless Personal Communications. 2019; 106(2): 423-438.

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

25. Wells, Peter,& CA ANZ, Chartered Accountants Australia and New Zealand .(2020). **"The Future of Financial Reporting: What size do you want"** available at.

26. Wust, K. & Gervais, A. (2018)."**Do you need a Blockchain**" In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) IEEE.

الملاحق

الملحق (1) استمارة استبيان

المحور الأول: الامن السيبراني Cybersecurity

الأمن السيبراني: هو نظام شامل يهدف إلى حماية الأنظمة الرقمية، الشبكات، الأجهزة، والبيانات من التهديدات والهجمات الإلكترونية التي قد تستهدفها. يشمل هذا المجال مجموعة واسعة من الإجراءات التقنية والتنظيمية التي تهدف إلى ضمان سرية المعلومات، سلامتها، وتوافرها في مواجهة التحديات الأمنية الحديثة.

1- السرية: هي أحد المبادئ الأساسية في مجال الأمن السيبراني وإدارة البيانات، وهي تتعلق بالحفاظ على المعلومات الحساسة والمحافظة على عدم تسريبها أو الوصول إليها من قبل أفراد أو جهات غير مصرح لهم. الهدف الأساسي من السرية هو ضمان حماية المعلومات الشخصية والتجارية والمالية وغيرها من البيانات الحساسة من التهديدات التي قد تؤدي إلى سرقتها أو استخدامها بشكل غير قانوني.

ت	السؤال	اتفق تماماً	اتفق	محايد	لا اتفق تماماً	لا اتفق
1	استخدام تقنيات التشفير المتقدمة لضمان حماية البيانات الحساسة من الاختراق والهجمات السيبرانية.					
2	تتم مراقبة الوصول إلى البيانات الحساسة بانتظام مع تطبيق مبدأ "أقل امتياز" لضمان اقتصار الوصول على الأشخاص المصرح لهم فقط.					
3	يتم تقييم وتحديث أدوات وتقنيات الأمن السيبراني بشكل مستمر لضمان قدرتها على مواجهة التهديدات السيبرانية الحديثة.					
4	يتم تطبيق تدابير قوية لحماية البيانات أثناء عمليات النقل عبر الشبكات لمنع تسريبها أو اختراقها.					
5	تُطبَّق إجراءات صارمة لتحديث حقوق وصلاحيات الوصول إلى البيانات الحساسة بما يتناسب مع تغييرات الأدوار والاحتياجات داخل المؤسسة					

2- الخصوصية :هي حق الأفراد والمؤسسات في التحكم في كيفية جمع واستخدام ومشاركة بياناتهم الشخصية والمعلومات الحساسة. تشمل الخصوصية حماية هذه البيانات من الوصول غير المصرح به أو التسريب أو الاستخدام غير القانوني. هذا الحق يمتد إلى توفير الأمان والحفاظ على سرية البيانات الشخصية، وضمان عدم تعرضها للتلاعب أو الاستغلال من قبل أطراف غير مخولة.

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

ت	السؤال	اتفق تماماً	اتفق	محايد	لا اتفق تماماً	لا اتفق
1	اتباع سياسات الأمان بجدية والعمل على تطبيق جميع الأحكام المتعلقة بها لضمان حماية البيانات والمعلومات.					
2	استخدام الوحدات الاقتصادية مجموعة متنوعة من التقنيات مثل المصادقة، الترخيص، والتشفير لحماية الأنظمة والبيانات الحساسة من التهديدات المحتملة.					
3	مراقبة أنظمة أمن المعلومات لمحاولات القرصنة على رسائل البريد الإلكتروني الخاصة بالموظفين وكشف أي نشاط غير قانوني.					
4	ضمان تشغيل جدار الحماية بشكل دائم مع تحديثات مستمرة لمنع المتسللين من الوصول إلى معلومات المصرف والعملاء.					
5	تشجيع الوحدات الاقتصادية على تبني التطورات الحديثة في سياسات الأمن السيبراني للحماية من السرقة الرقمية والتجسس.					

3- الجاهزية: هي قدرة الأفراد أو الأنظمة أو المؤسسات على الاستعداد التام والقدرة على الاستجابة بشكل فعال للمواقف أو الأحداث الطارئة أو غير المتوقعة. تشير الجاهزية إلى استعداد جميع الموارد والقدرات اللازمة للتعامل مع الأزمات أو التحديات المحتملة في أي وقت.

ت	السؤال	اتفق تماماً	اتفق	محايد	لا اتفق تماماً	لا اتفق
1	تضمن المؤسسة استعداد أنظمتها للتعامل مع الطوارئ المفاجئة من خلال تطبيق بروتوكولات جاهزية فعالة في جميع أقسامها					
2	يتم تحديد وتحليل المخاطر المحتملة التي قد تؤثر على جاهزية المؤسسة للرد السريع، بالإضافة الى وضع الخطط المعتمدة لتقليل هذه المخاطر مثل (مخاطر الاختراق) ..					
3	تساهم أنظمة الإدارة والتكنولوجيا الحديثة في رفع مستوى الجاهزية وتنسيق الاستجابة بين الفرق المتنوعة في المؤسسة أثناء الأزمات					
4	دور التدريب المستمر والمحاكاة في تحفيز الموظفين على تعزيز جاهزيتهم للاستجابة السريعة والفعالة في مواجهة الطوارئ					
5	ضمان أن جميع الأنظمة الحيوية داخل المؤسسة محمية من الأعطال المفاجئة، مع القدرة على استعادة البيانات والخدمات بأقصى سرعة ممكنة					

4- التعزيز: يشير إلى جميع الإجراءات والتقنيات التي تُستخدم لتعزيز قدرة الأنظمة والبيانات على مقاومة التهديدات السيبرانية وحمايتها من الهجمات. يشمل ذلك تقوية الدفاعات الرقمية، تحسين أطر الأمان، وتعزيز استجابة الأنظمة في حال حدوث أي تهديدات أو اختراقات.

ت	السؤال	اتفق تماماً	اتفق	محايد	لا اتفق تماماً	لا اتفق
1	يقوم المصرف بتحديث البرمجيات والأنظمة بشكل دوري لسد الثغرات الأمنية المعروفة.					

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

2	يتم حماية أنظمة التشـــغيل باســـتخدام أجهزة وبرمجيات متقدمة، بالإضـافة إلى آليات حماية صـممت خصـيصًـا من قبل المصـرف لضمان استدامة الأمان السيبراني.					
3	تستخدم أساليب تخزين آمنة في المصرف، حيث يتم الحفاظ على نســـخة احتياطية من جميع الملفات والمعلومات على الأقراص الصلبة أو إلكترونيًا عبر السحابة لضمان استمرارية الوصول إلى البيانات					
4	تستخدم الوحدات الاقتصـادية بانتظام برامج مكافحة الفيروسـات على الأجهزة المصـــرفية لضـــمان حماية البيانات من البرامج الضارة والتهديدات الإلكترونية.					
5	يقوم المصـــرف بإجراء تقييمات دورية للمخاطر لتحديد نقاط الضعف واتخاذ الإجراءات اللازمة لتعزيز الأمان .					

المحور الثاني : تقنية سلسلة الكتل

تقنية سلسلة الكتل : هي نظام رقمي لتخزين ونقل البيانات بشكل آمن وشفاف وغير قابل للتغيير. تعتمد التقنية على سـلسـلة من الكتل المتصـلة ببعضـها البعض، حيث تحتوي كل كتلة على بيانات محددة، وطابع زمني، ورابط إلى الكتلة السـابقة. يتم تأمين البيانات في تقنية سـلسـلة الكتل باسـتخدام تقنيات التشـفير، مما يجعلها مقاومة للتزوير أو التعديل.

ت	السؤال	اتفق تماماً	اتفق	محايد	لا اتفق تماماً	لا اتفق
1	مفاتيح التشـفير العامة التي تعتمدها تقنية سـلسـلة الكتل تُسـهم في حماية هوية المستخدمين وضمان سرية المعلومات المتبادلة.					
2	تقليل تكلفة تخزين البيانات باستخدام تقنية سلسلة الكتل يساهم في تحسين كفاءة إدارة المعلومات المالية على المدى الطويل.					
3	تقنية سلسلة الكتل تُعزز سرعة ودقة التقارير المالية.					
4	توفر سـلسـلة الكتل سـجلاً شـفافاً وموثوقاً للمعاملات، مما يسـهل تدقيق البيانات المالية ويزيد من ثقة المساهمين.					
5	تطبيق تقنية سـلسـلة الكتل في المصـارف العراقية يسـهم في منع التزوير في البيانات المالية وتحقيق مســـتويات عالية من الأمان والشفافية.					
6	تقليل تكاليف التحويل المالي باسـتخدام تقنية سـلسـلة الكتل يتيح إجراء عمليات مالية منخفضة التكلفة مقارنة بالأنظمة التي تعتمد على الوسطاء.					
7	يمكن لتقنية سلسلة الكتل أن تعيد تشكيل أسواق العملات الرقمية وتعزيز مصداقيتها لدى الجهات التنظيمية					
8	تستخدم سلسـلة الكتل لتطوير أنظمة هوية رقمية اكثر اماناً، مما يســاعد المصـــارف في التحقق من هوية العملاء وتقليل مخاطر الاحتيال.					

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

9	ميزة اللامركزية في تقنية سلسلة الكتل تُسهم في تقليل احتمالية تعرض البيانات للاختراق من خلال توزيعها على أكثر من نقطة تخزين					
10	تقنية سلسلة الكتل تقلل التكاليف المالية من خلال توفير بدائل مبتكرة تقلل الاعتماد على الوسائل التقليدية ذات التكلفة العالية.					
11	المعاملات الرقمية عبر تقنية سلسلة الكتل تتيح تنفيذ عمليات مالية آمنة.					
12	عدم قابلية تقنية سلسلة الكتل للتعديل أو التزوير يجعلها خيارًا مثاليًا لتحقيق الأمان في البيانات المالية.					
13	القضاء على الفساد المالي باستخدام تقنية سلسلة الكتل يعتمد على تعزيز الشفافية وإلغاء دور الطرف الثالث.					
14	تساهم تقنية سلسلة الكتل في تسهيل الوصول إلى الخدمات المصرفية للأفراد غير المتعاملين مع البنوك.					
15	يمكن اعتبار تقنية سلسلة الكتل أداة فعّالة لتسجيل حقوق الملكية الفكرية وحمايتها من التعدي أو التزوير.					
16	المعاملات عبر تقنية سلسلة الكتل تتميز بمستويات أمان مرتفعة مع الحفاظ على خصوصية البيانات المخزنة.					
17	يمكن لمفهوم العقود الذكية في سلسلة الكتل أن يحدث ثورة في إدارة العقود بين الشركات والأفراد.					
18	سهولة نقل الأصول المشفرة عبر تقنية سلسلة الكتل يعزز من كفاءة العمليات المالية ويتيح تداول الأصول بشكل آمن وسريع.					
19	يمكن أن تواجه تقنية سلسلة الكتل مقاومة من المؤسسات المالية التقليدية بسبب التهديدات المحتملة لنموذج أعمالها.					
20	يُمكن لتقنية سلسلة الكتل أن تخلق بيئة أعمال أكثر إنصافًا للشركات الصغيرة مقارنة بالشركات الكبرى من خلال (التقليل من التكاليف).					

المحور الثالث: موثوقية التقارير المالية الرقمية

موثوقية التقارير المالية الرقمية: تشير إلى درجة الثقة التي يمكن أن يوليها المستخدمون لتلك التقارير بناءً على دقة البيانات المعروضة، والشفافية، والامتثال للمعايير المحاسبية الدولية والمحلية. كما تشمل قدرة الأنظمة الرقمية على توفير تقارير مالية يمكن الاعتماد عليها، والتي تم جمعها، معالجتها، وتخزينها بطريقة تحميها من التلاعب أو الأخطاء، مما يعزز من مصداقية هذه التقارير ويجعلها أكثر قدرة على دعم اتخاذ القرارات المالية والإدارية.

يمكن اعتبار الموثوقية بمثابة **التمثيل الصادق** في السياق المحاسبي والمالي. في مجال المحاسبة، يشير التمثيل الصادق إلى أن البيانات المالية تمثل بشكل دقيق وواقعي الوضع المالي والعمليات المالية للمؤسسة، دون أي تحريف أو تلاعب.

يمكن قياس **التمثيل الصادق** من خلال خصائصه الفرعية **(الاكتمال، الحياد، الخلو من الخطأ).** هذه الخصائص تساهم في ضمان أن التقارير المالية الرقمية تمثل الوضع الفعلي والواقعي للمؤسسة أو الكيان، مما يعزز موثوقيتها ويساعد في اتخاذ قرارات سليمة من قبل المستخدمين.

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

الاكتمال: ضمان أن جميع المعلومات المالية الضرورية والمعاملات الاقتصادية يتم تضمينها بشكل دقيق في التقارير، مما يساعد على تقديم صورة شاملة وصحيحة عن الوضع المالي للمؤسسة.

ت	السؤال	اتفق تماماً	اتفق	محايد	لا اتفق تماماً	لا اتفق
1	التقارير المالية الرقمية تضمن اكتمال المعلومات المالية من خلال تضمين جميع المعاملات المالية التي تمت في الفترة المحاسبية.					
2	التقارير المالية الرقمية تعزز اكتمالها عند تضمين التفسيرات والتوضيحات المتعلقة بالسياسات المحاسبية لتوضيح المعاملات المالية بشكل كامل.					
3	الاكتمال في التقارير المالية الرقمية يتحقق عندما تشمل جميع الفترات الزمنية ذات الصلة بالأحداث المالية وتغطي كافة الأنشطة المالية للمؤسسة.					
4	التقارير المالية الرقمية تتميز بالاكتمال عند احتوائها على كافة البيانات الضرورية التي تقدم صورة شاملة ودقيقة عن الوضع المالي للمؤسسة.					
5	التقارير المالية الرقمية تحقق الاكتمال عندما تشمل جميع التفاصيل المتعلقة بالمعاملات المالية عبر كافة الفئات الاقتصادية المختلفة.					
6	الاكتمال في التقارير المالية الرقمية يتحقق عندما يتم تضمين جميع المعاملات المالية دون استثناء أو إغفال أي تفاصيل تؤثر على الوضع المالي للمؤسسة.					

الحياد: يشير إلى تقديم المعلومات والبيانات المالية بطريقة غير متحيزة وخالية من أي تأثيرات أو مصالح شخصية قد تؤثر على صدقها ودقتها. يعني الحياد أن التقارير المالية تُعد وتُعرض بشكل يعكس الحقيقة الموضوعية للوضع المالي للمؤسسة دون محاولة التأثير على القرارات التي قد يتخذها المستخدمون بناءً على تلك التقارير.

ت	السؤال	اتفق تماماً	اتفق	محايد	لا اتفق تماماً	لا اتفق
1	تعكس التقارير المالية الرقمية حياد المؤسسة من خلال تقديم المعلومات بشكل خالٍ من التحيز لصالح أي طرف محدد.					
2	التزام التقارير المالية الرقمية بمعايير المحاسبة الدولية يعزز الحياد ويضمن تقديم المعلومات بشكل موضوعي.					
3	الحياد في التقارير المالية الرقمية يظهر عندما تكون المعلومات المالية خالية من أي تأثيرات خارجية قد تغير من دقتها.					
4	تعتمد التقارير المالية الرقمية على الحقائق والأدلة دون التأثر بالآراء الشخصية، مما يضمن حياد المعلومات المقدمة.					
5	التقارير المالية الرقمية تعبر عن الحياد عند عرض البيانات المالية بشكل منصف يعكس الواقع المالي دون تضخيم أو تقليل.					
6	الحياد في التقارير المالية الرقمية يتحقق عندما يتم عرض البيانات المالية بشكل موضوعي دون التأثير من أي جهة أو طرف له مصلحة معينة.					

مجلة الغري للعلوم الاقتصادية والادارية
مجلد (21) عدد (2) 2025

7	التقارير المالية الرقمية تضـــمن الحياد من خلال تقديم المعلومات المالية دون أي تحريف أو تغيير يعكس مصـــلحة شـــخصـــية أو تأثيرات خارجية قد تؤثر على القرارات المالية للمستخدمين.					

الخلو من الخطأ: هو أحد الخصائص الفرعية الأساسية للتمثيل الصادق في التقارير المالية. يشير إلى أن المعلومات المالية المقدمة يجب أن تكون خالية من الأخطاء المهمة التي قد تؤثر على القرارات التي يتخذها مستخدمو التقارير. لا يعني هذا المفهوم أن التقارير المالية يجب أن تكون خالية تمامًا من أي أخطاء، ولكن يعني أن الأخطاء الجوهرية والتقديرات غير المبررة يجب تجنبها.

ت	السؤال	اتفق تماماً	اتفق	محايد	لا اتفق تماماً	لا اتفق
1	تعكس التقارير المالية الرقمية خلوها من الأخطاء من خلال تقديم معلومات دقيقة تعكس الواقع المالي للمؤسسة بشكل موضوعي.					
2	تعزز التقارير المالية الرقمية خلوها من الأخطاء باســـتخدام تقديرات محاسبية معتمدة على أسس علمية ومنهجيات واضحة.					
3	إجراءات المراجعة والتدقيق تساهم في تقليل الأخطاء في التقارير المالية الرقمية وتعزز موثوقيتها.					
4	توثيق العمليات المحاسبية في التقارير المالية الرقمية يضمن تقديم بيانات خالية من الأخطاء الجوهرية.					
5	التزام التقارير المالية الرقمية بالمعايير المحاســـبية يســـاعد في تحقيق خلوها من الأخطاء وتقديم معلومات موثوقة.					
6	تســـهم التقارير المالية الرقمية في خلوها من الأخطاء من خلال توفير آليات فحص دقيقة للبيانات المدخلة والمعاملات المالية.					
7	تســـاعد الأنظمة المحاســـبية المتطورة في التقارير المالية الرقمية على تحسين دقة المعلومات المالية وتقليل الأخطاء الجوهرية.					

[i] يعد المتغير الوسيط بمثابة المتغير التابع عن اختبار تأثره بالمتغير المستقل، ويعد بمثابة المتغير المستقل عند اختبار تأثيره بالمتغير التابع.

[ii] **df** تعني درجات الحرية وهي مختصر **degrees of freedom** وتمثل عدد القيم القابلة للتغير في حساب خاصية إحصائية ما . يعتمد حساب الخصائص الإحصائية المختلفة على مجموعة من المعلومات أو البيانات. يسمى عدد المعلومات المستقلة عن بعضها والتي تدخل في حساب خاصية إحصائية معينة.

[iii] تشير الى درجة الحرية الأولى والتي تساوي عدد المتغيرات المستقلة في نموذج الانحدار المستخدم في قياس الفرضية.

[iv] تشير الى درجة الحرية الثانية وتساوي مجموع درجتي الحرية مطروحا منها درجة الحرية الأولى.

[v] تشير الى مجموع درجتي الحرية الأولى والثانية وتساوي حجم العينة مطروح منها واحد.