Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
EISSN: 3006-9149
PISSN: 1813-1719

Hardening financial data: How blockchain and cybersecurity converge to provide impenetrable security

Jamal Nori Daham Al-Halbousi*[A], Hamza Khaled Harhoush[B], Ghalib Jalawi Aswad alkhadm[C]

[A] College of Administration and Economics/University of Anbaar
[B] Department of Financial Affairs/ University of Anbaar
[C] Internal Control and Auditing Department/ University of Anbaar

Keywords:
Financial data fortification, blockchain, cybersecurity, data protection

Article history:
Received 05 Dec. 2024
Accepted 19 Jan. 2025
Available online 25 Jun. 2025

©2023 College of Administration and Economy, Tikrit University. THIS IS AN OPEN ACCESS ARTICLE UNDER THE CC BY LICENSE
http://creativecommons.org/licenses/by/4.0/

*Corresponding author:
Jamal Nori Daham Al-Halbousi
College of Administration and Economics/University of Anbaar

Abstract: The study aimed to analyze the role of encryption and blockchain technologies in protecting financial data and enhancing transparency by reducing reliance on intermediaries. Data was collected from Iraqi university professors using a questionnaire, where 69 valid questionnaires were analyzed using SPSS. The results showed that blockchain contributes to improving data protection through encryption and decentralized distribution, which enhances trust and reduces manipulation. Cybersecurity practices also reduce cyberattacks and maintain data confidentiality. The study recommended adopting advanced encryption technologies and regular mechanisms for assessing security risks, while addressing vulnerabilities to ensure data protection and continued security.

تحصين البيانات المالية: كيف تتلاقى سلسلة الكتل والأمن السيبراني لتوفير أمان لا يُخترق

جمال نوري دحام
كلية الادارة والاقتصاد
جامعة الانبار

حمزة خالد حرحوش
قسم الشؤون المالية
جامعة الانبار

غالب جلوي اسود
قسم الرقابة والتدقيق الداخلي
جامعة الانبار

المستخلص

هدفت الدراسة إلى تحليل دور تقنيات التشفير وسلسلة الكتل في حماية البيانات المالية وتعزيز الشفافية عبر تقليل الاعتماد على الوسطاء. تم جمع البيانات من أساتذة جامعات عراقية باستخدام استبانة، إذ تم تحليل 69 استبانة صالحة ببرنامج SPSS. أظهرت النتائج أن سلسلة الكتل تسهم في تحسين حماية البيانات من خلال التشفير والتوزيع اللامركزي، مما يعزز الثقة ويقلل التلاعب. كما أن ممارسات الأمن السيبراني تقلل الهجمات الإلكترونية وتحافظ على سرية البيانات. أوصت الدراسة بتبني تقنيات تشفير متطورة وآليات منتظمة لتقييم المخاطر الأمنية، مع معالجة نقاط الضعف لضمان حماية البيانات واستمرارية الأمان.

الكلمات المفتاحية: تحصين البيانات المالية، سلسلة الكتل، الامن السيبراني، حماية البيانات.

المقدمة:

في ظل التطور التكنولوجي وتسارع التحولات الرقمية وتزايد التهديدات السيبرانية، أصبحت حماية البيانات المالية امرا ضروريا في الوقت الحالي. فالوحدات الاقتصادية تواجه اليوم العديد من التحديات الغير مسبوقة من اجل الحفاظ على سرية وسلامة البيانات من الاختراق، التلاعب، أو التسريب. وفي ظل هذا المشهد المعقد فقد برزت لنا تقنيتان محوريتان تشكلان جبهة دفاع متقدمة: سلسلة الكتل (Blockchain) والأمن السيبراني.

سلسلة الكتل، التي بدأت كقاعدة لتداول العملات الرقمية مثل "البيتكوين"، اذ أثبتت أنها أكثر من مجرد تقنية مالية؛ فهي بنية بيانات موزعة وغير قابلة للتغيير، توفر سجلات شفافة وآمنة يصعب اختراقها أو التلاعب بها. أما الأمن السيبراني، فهو المجال المسؤول عن تصميم وتنفيذ الاستراتيجيات والبروتوكولات التي تحمي الأنظمة والمعلومات من الهجمات الإلكترونية. عندما تتكامل سلسلة الكتل مع ممارسات الأمن السيبراني، تُبنى بيئة دفاعية متعددة الطبقات توفر مستويات غير مسبوقة من الحماية للبيانات المالية. هذا التكامل لا يعزز فقط سلامة المعاملات والعمليات المالية، بل يضع الأسس لنموذج أمني جديد، أكثر مرونة وموثوقية في مواجهة التحديات الرقمية. لذلك يسعى هذا البحث إلى سد هذه الفجوة من خلال تحليل دور التكامل بين سلسلة الكتل والأمن السيبراني في تحصين البيانات المالية وتعزيز الثقة في العمليات المالية.

يركز البحث على دراسة كيفية توظيف تقنيات التشفير واللامركزية في سلسلة الكتل بالتكامل مع ممارسات الأمن السيبراني، لتقديم حلول شاملة تقلل الاعتماد على الوسطاء، وتواجه التهديدات الأمنية، وتحقق مستويات عالية من الأمان المالي والشفافية في المعاملات.

أولاً. منهجية البحث:

1. مشكلة البحث: يمكن اظهار مشكلة الدراسة من خلال الأسئلة الآتية:

أ. ما مدى فعالية تقنية سلسلة الكتل في تعزيز حماية البيانات المالية وتحقيق مستويات أعلى من الأمان والشفافية في العمليات المالية؟

ب. كيف يمكن لأبعاد تقنية سلسلة الكتل، مثل التشفير واللامركزية وآليات الإجماع، تحسين الكفاءة وتقليل الاعتماد على الوسطاء في الأنظمة المالية؟

2. فرضية البحث: إن فرضيات البحث الحالي هي كما يأتي:

الفرضية الأولى: يوجد تأثير ذو دلالة احصائية لسلسلة الكتل على حماية البيانات المالية وامانها.

الفرضية الثانية: يوجد تأثير ذو دلالة احصائية للأمن السيبراني على حماية البيانات المالية وامانها.

3. أهداف البحث: تهدف الدراسة الحالية إلى تحقيق الآتي:

أ. تحليل دور تقنيات التشفير في سلسلة الكتل في حماية البيانات المالية من الاختراق والتلاعب.

ب. تقييم تأثير اللامركزية في سلسلة الكتل على تقليل الاعتماد على الوسطاء الماليين وتعزيز شفافية المعاملات.

ج. استكشاف مدى فعالية العقود الذكية في تحسين كفاءة وموثوقية العمليات المالية.

د. دراسة آليات الإجماع المستخدمة في سلسلة الكتل، مثل إثبات العمل وإثبات الحصة، وتأثيرها على الثقة والأمان في الأنظمة المالية.

4. أهمية البحث

أ. يساهم في تعزيز الفهم العملي لدور تقنية سلسلة الكتل في تقوية نظم الأمان المالي وتقليل الثغرات المحتملة.

ب. يوفر رؤى حول كيفية توظيف اللامركزية في تعزيز الشفافية المالية وتقليل الاعتماد على الهياكل التقليدية.

ج. يعد هذا البحث أساسًا لفهم آفاق استخدام العقود الذكية في تطوير أنظمة مالية أكثر كفاءة وأقل عرضة للأخطاء.

د. يساعد على توجيه السياسات المالية وتقديم رؤى علمية لمتخذي القرار حول آليات تعزيز الأمان المالي باستخدام تقنيات حديثة مثل سلسلة الكتل.

5. دراسات سابقة:

أ. على واخرين، (2022)، دراسة أساليب الخصوصية والأمن المستخدمة في سلسلة الكتلة.

تهدف الدراسة إلى تحليل الأمان والخصوصية في تقنية "بلوكشين"، مع التركيز على تحديد خصائصها الأساسية وطرق تحسينها. أظهرت النتائج أن "بلوكشين" تعزز الأمان في التطبيقات الرقمية، لكن هناك تحديات تتعلق بالمرونة وحماية البيانات. توصي الدراسة بتطوير تقنيات جديدة وتعزيز التعاون بين الباحثين والصناعات لضمان الأمان الشامل. اعتمدت الدراسة على منهج تحليلي استكشافي من خلال مراجعة الأدبيات وتحليل التطبيقات العملية.

ب. علي سيد إسماعيل، (2021)، تقنية البلوك تشين Blockchain آليةً لحوكمة المؤسسات المالية الإسلامية المعاصرة

تتناول هذه الدراسة تقنية البلوكشين، والتي من المتوقع أن تلعب دورًا محوريًا في النظام المالي العالمي نظرًا لكونها آمنة وغير قابلة للتلاعب، فضلا عن سرعتها وموثوقيتها ودقتها في

تسجيل المعاملات. تكتسب الدراسة أهميتها من الاهتمام المتزايد بتقنية البلوكشين كأداة حديثة عالمية، خاصةً في تطبيق الحوكمة داخل المؤسسات المالية الإسلامية ودورها في تحسين الأداء الاقتصادي. تهدف الدراسة إلى تقديم فهم واضح لآليات البلوكشين، وفوائدها، وتطبيقاتها، مع التركيز على دورها كأداة متكاملة للحوكمة في المؤسسات المالية الإسلامية.

ج. بدر الحيمودي، (2023)، الأمن السيبراني وحماية الأنظمة المعلوماتية

حقق التقدم الكبير في تقنية المعلومات والاتصالات أهمية كبيرة للأمن السيبراني في المجتمع المغربي والمملكة المغربية. يُعد الأمن السيبراني ضروريًا على المستوى الفردي لحماية البيانات الشخصية، الصور، الملفات، الحسابات الشخصية، كلمات المرور، الحسابات المصرفية، وغيرها من الأمور المرتبطة بحياة المواطن المغربي. وعلى مستوى المجتمع، يلعب دورًا في حماية المجتمع من الهندسة الاجتماعية واستهداف السلوك الاجتماعي، فضلا عن حماية البيانات والخصوصية المجتمعية. أما على مستوى الشركات والمؤسسات، فيساهم الأمن السيبراني في حماية الأصول الإلكترونية، البيانات، معلومات الموظفين والعملاء، والمواقع الإلكترونية. وعلى مستوى الدولة، يُعد حماية الأمن الإلكتروني والمالي أمرًا بالغ الأهمية.

ثانياً. الجانب النظري

مقدمة

في ظل التطور التكنولوجي السريع وزيادة الاعتماد على الأنظمة الرقمية في العمليات المالية، أصبحت حماية البيانات المالية من التهديدات السيبرانية والتلاعب أولوية استراتيجية للمؤسسات المالية. تقدم تقنية سلسلة الكتل (Blockchain) حلولًا مبتكرة لتعزيز الأمان والشفافية بفضل خصائصها المتمثلة في التشفير المتقدم، واللامركزية، وآليات الإجماع. في المقابل، يلعب الأمن السيبراني دورًا حيويًا في مواجهة الهجمات الإلكترونية وحماية البيانات المالية من الاختراق . ورغم الجهود البحثية السابقة التي تناولت أهمية سلسلة الكتل في تحسين الأمان المالي، أو دور الأمن السيبراني في حماية البيانات، إلا أن هناك نقصًا واضحًا في الدراسات التي تستكشف التكامل بين هاتين التقنيتين. يسعى هذا البحث إلى سد هذه الفجوة من خلال تحليل دور التكامل بين سلسلة الكتل والأمن السيبراني في تحصين البيانات المالية وتعزيز الثقة في العمليات المالية .

يركز البحث على دراسة كيفية توظيف تقنيات التشفير واللامركزية في سلسلة الكتل بالتكامل مع ممارسات الأمن السيبراني، لتقديم حلول شاملة تقلل الاعتماد على الوسطاء، وتواجه التهديدات الأمنية، وتحقق مستويات عالية من الأمان المالي والشفافية في المعاملات.

1. **تقنية سلسلة الكتل:** تُعد سلسلة الكتل نظامًا أنيقًا وآمنًا ولا مركزيًا، وهي ليست مجرد التكنولوجيا التي تقف وراء العملات الرقمية فقط، بل أكثر من ذلك بمجرد فهم المبادئ الأساسية لها بشكل أعمق. في جوهرها، تتكون سلسلة الكتل من سلسلة من الكتل التي يتم تأمينها بواسطة تقنيات التشفير. تحتوي كل كتلة على بيانات وطابع زمني و"هاش سابق"، وترتبط بالكتلة السابقة باستخدام "هاش" تشفيري، مما يشكل "سلسلة الكتل". يُعرف هذا النوع من السلاسل باسم "دفتر الحسابات الموزع"، حيث تكون جميع العُقد الكاملة قادرة على الوصول إلى السلسلة. تجعل الهاشات التعديلات غير القانونية أمرًا مستحيلًا، ويتم "ربط" الكتلة بكتلة سابقة باستخدام "الهاش السابق". يتميز هذا النظام بسلسلة غير قابلة للتغيير، إذ لا يمكن حذف البيانات أو تعديلها. في حالة حدوث اختلاف نادر بين سلسلتين

متعارضتين تحتويان على "هاش سابق" مختلف، يتم تحديث السلسلة لتكون الأكثر توافقًا (علي وآخرين، 2022: 355).

وتُعالج البيانات في سلسلة الكتل باستخدام آلية توافق، تعمل كبروتوكول بناء ثقة ديمقراطي. يمثل تحسين النزاهة ميزة كبيرة لتطبيقات سلسلة الكتل المرتبطة بالقطاع المالي، وتوجد العديد من التطبيقات الأخرى التي تتمتع بإمكانات هائلة. على عكس مراكز البيانات المركزية، تُدير سلسلة الكتل البيانات من خلال بنية موزعة، وهي الأساس الذي يستند إليه النظام اللامركزي. فعلى الصعيد الأساسي، "النظام اللامركزي يعارض النظام المركزي في إدارة البيانات"، إذ يتم "توزيع عبء معالجة البيانات على مئات أو حتى آلاف الحواسيب". تُقلل البُنى اللامركزية من المخاطر السيبرانية من خلال توزيع البيانات عبر الشبكة بدلاً من تجمعها في موقع واحد يمكن استغلاله. ومن المزايا الكامنة في الأنظمة اللامركزية أن الشبكة بأكملها تبقى متاحة حتى في حالة فشل أو توقف أحد "العُقد". لا تستطيع أي جهة معترف بها التحكم في أو منع تشغيل سلسلة الكتل العامة التقليدية. (Komalavalli et al., 2020: 350)

2. **أساسيات الأمن السيبراني:** أكبر اهتمامات أي مؤسسة هي حماية بياناتها من الوصول غير المصرح به أو التلف. نظرًا لأن الهجمات قد تأتي من أي مكان، فإن الحاجة الأساسية هي آلية لمراقبة حركة البيانات – أي إجراء تحليل للتهديدات. يُشير مفهوم إدارة المخاطر إلى أن أي نظام يجب أن يتم إعداده دائمًا مع مراعاة الأضرار المحتملة في حالة تعرضه للاختراق. وبناءً على ذلك، ينبغي تصميم الشبكات مع الأخذ في الاعتبار اعتبارات الأمان. بمجرد الانتهاء من تصميم الشبكة، يصبح التحديث الدوري وتطبيق التصحيحات الأمنية أمرًا ضروريًا لحمايتها من أي ثغرات جديدة. يؤدي ذلك إلى الحاجة إلى التشفير وأمن الشبكات (علي، 2021: 149).

ويمثل القطاع المالي تحديات أكبر مقارنة بالقطاعات الأخرى؛ إذ إن أي هجوم سيبراني – والذي يحتمل وقوعه بشكل كبير – قد يؤدي إلى نتائج كارثية، خصوصًا عندما يعتمد القطاع المصرفي على التكنولوجيا لتنفيذ المعاملات المالية .كما أن أمن المؤسسات المالية يُعتبر ضروريًا للامتثال التنظيمي؛ حيث يجب حماية البيانات المالية. إن تأمين بوابات الاستثمار الخاصة أو المعاملات السرية أمر مهم للأعمال. إن حماية المعلومات الشخصية والمالية الحساسة، والامتثال لعدد كبير من القوانين المتداخلة والمعقدة الخاصة بالخصوصية، يصبح أكثر أهمية من أي وقت مضى، خاصة مع تحول شركات الخدمات المالية إلى أمناء على البيانات الكبيرة .(Komalavalli et al., 2020: 350)

يرى الباحثون أن تتطلب حماية البيانات في المؤسسات استراتيجية شاملة تركز على منع الوصول غير المصرح به والتصدي للتلف، خاصةً في القطاع المالي الذي يواجه تحديات كبيرة. يعتمد نجاح الأمن السيبراني على تصميم شبكات آمنة تتضمن الجدران النارية والتشفير وبرامج مكافحة الفيروسات، مع تحديث مستمر للتصدي للثغرات. يُعد التشفير أداة فعالة لتحويل البيانات إلى صيغة غير قابلة للقراءة، ما يجعلها عديمة الفائدة للجهات غير المصرح لها، بينما تمنع الجدران النارية حركة المرور غير المرغوب فيها. الامتثال للتنظيمات وتوفير حماية فعالة للبيانات المالية والشخصية يمثلان ضرورة أساسية لحماية سمعة المؤسسات وضمان الثقة فيها.

3. **تحديات تأمين البيانات المالية:** تأمين البيانات الشخصية والمؤسسية والحكومية في قطاع مالي مفتوح وغير محمي تمامًا يمكن أن يسهل سرقة البيانات، والتزوير في الهوية، والمعاملات المالية غير

القانونية. لم تُصمم أنظمة الأمان التقليدية للدفاع ضد هذه التهديدات، بل وُضعت لحماية البيانات ضد الانتهاكات العرضية وفقدانها. تعتمد هذه الأنظمة على بروتوكولات أمان قديمة وتكنولوجيا قديمة. علاوة على ذلك، تُعزى أكثر من 80% من الانتهاكات الأمنية للحاسوب إلى خطأ بشري ناجم عن قلة الثقة في التكنولوجيا، خاصة بين المستخدمين غير القادرين على إدارة المعلومات. وعلى المؤسسات المالية والشركات والهيئات الحكومية أن تدرك أهمية تأمين البيانات السرية، وأن تقوم بإنشاء آليات حماية مناسبة لمواجهة الثغرات المعروفة، وتقديم خدمات آمنة لمتلقي الخدمات الرقمية. تعتمد التجارة الإلكترونية بشكل كبير على المعاملات الآمنة، والتي تمثل مصدرًا كبيرًا للدخل. تقوم المؤسسات المالية بنقل وإدارة ومعالجة البيانات الحساسة للعملاء، وهي متصلة بعدد من الشبكات، مما يجعلها أكثر عرضة للتهديدات السيبرانية مقارنة بنظيراتها في قطاعات التصنيع والخدمات . (علي، 2021: 149)

وعلى الرغم من تطور بنى تكنولوجيا المعلومات الحالية، إلا أنها لا تزال مليئة بالثغرات الأمنية التقليدية. على سبيل المثال، إذا لم تكن البيانات في نظام مالي مُشفرة، يمكن اختراقها بسهولة إذا قام القراصنة باعتراض الإشارات. يمكن للمجرمين السيبرانيين اختراق أنظمة التحكم المركزية، مما يتيح التلاعب في أسعار الأسهم .ورغم توظيف تدابير أمان باهظة الثمن، فإن كل وحدة في النظام تبقى عرضة للخطر. يُشكل الموظفون غير المدربين بشكل كافٍ نقطة ضعف أخرى في سلسلة الأمان، إذ إن الاختراق غالبًا ما يتطلب التسلل إلى شبكة طرف ثالث متصلة بالهدف الرئيس. فضلا عن حماية البرامج والشبكات، فإن الامتثال غير المحدث يزيد من نقاط الضعف .وتؤدي سرقة البيانات من الأنظمة المالية إلى خسائر إضافية، لا سيما في ظل عدم القدرة على التعامل بفعالية مع التحول إلى الأعمال السحابية. هذه الثغرات لا تشكل فقط مخاطر اقتصادية، بل تؤثر أيضًا على سمعة الصناعات المالية (Wang et al., 2020: 2366).

4. **أهمية التدريب والتوعية في تعزيز الأمن السيبراني:** يُعد تدريب الموظفين وتوعيتهم بالأمن السيبراني جزءًا لا يتجزأ من استراتيجية الحماية. فحتى أفضل الأنظمة الأمنية يمكن أن تتعرض للخطر إذا لم يكن المستخدمون على دراية بالمخاطر المحتملة وكيفية التعامل معها. لذلك، يجب على المؤسسات المالية أن تستثمر في برامج تدريبية دورية لتعزيز الوعي الأمني وتقديم الإرشادات حول أفضل الممارسات. وتشمل هذه التدريبات كيفية التعرف على رسائل البريد الإلكتروني المشبوهة، وتجنب النقر على الروابط غير المعروفة، واستخدام كلمات مرور قوية، والإبلاغ عن أي نشاط مشبوه على الفور. كما ينبغي إجراء اختبارات دورية للأمان (مثل اختبارات التصيد الإلكتروني) للتحقق من استجابة الموظفين وتقييم فعالية برامج التدريب. كما تتطلب مواجهة التهديدات السيبرانية الابتكار المستمر في مجال تقنيات الحماية. على الرغم من أن أدوات مثل الجدران النارية، والتشفير، وبرامج مكافحة الفيروسات لا تزال أساسية، إلا أن التقنيات الحديثة مثل الذكاء الاصطناعي، والتعلم الآلي، وتقنيات سلسلة الكتل أصبحت تلعب دورًا محوريًا في تعزيز الأمن السيبراني. ويمكن لتقنيات الذكاء الاصطناعي والتعلم الآلي التعرف على الأنماط الشاذة في البيانات واكتشاف الهجمات المحتملة بشكل أسرع من الطرق التقليدية. أما سلسلة الكتل، فتُستخدم لتأمين السجلات وتوفير سجل غير قابل للتغيير للمعاملات المالية، مما يقلل من مخاطر التلاعب ويعزز الثقة .وبشكل عام، يتطلب الحفاظ على قطاع مالي صحي وآمن نهجًا متكاملاً يجمع بين الابتكار التقني، والتدريب المستمر، وتحديث

البروتوكولات الأمنية، والتعاون بين المؤسسات المالية لضمان تبادل المعلومات حول التهديدات والتقنيات الأمنية (Idrees et al., 2021: 3).

5. **التهديدات الناشئة في القطاع المالي:** في السنوات الأخيرة، ظهرت مجموعة متنوعة من الهجمات التي تستهدف تعطيل وخداع المؤسسات المالية. تشمل الهجمات السيبرانية الشائعة التصيد الاحتيالي (Phishing)، وهجمات الفدية (Ransomware)، وهجمات الحرمان من الخدمة الموزعة (DDoS). غالبًا ما تكون هذه الهجمات غير مرتبطة بتكنولوجيا معينة، بل تتكيف مع التكنولوجيا الجديدة عند ظهورها. من المتوقع أن تستغل التهديدات السيبرانية البنية التحتية للبث. البروتوكولات مثل 5 Gوالإنترنت عبر الأقمار الصناعية تعد بتقديم العديد من التقنيات الناشئة للأسواق، مما يزيد من إمكانية تنفيذ هجمات سيبرانية موزعة واسعة النطاق بتكلفة أقل وأسهل من أي وقت مضى. وقد تكون الأنظمة المالية والبيع بالتجزئة من الجيل التالي، التي تسعى إلى توظيف شبكات دفع كبيرة الحجم وتمكين سلاسل التوريد الموسعة وتسهيل تسليع المنتجات، عرضة لهذا النوع من الهجمات. يمكن أن يؤدي الضرر الذي يلحق بقطاع الخدمات المالية إلى نقص الثقة في النظام، وقد يؤدي في الحالات القصوى إلى فشل دفع أجور الموظفين وعدم قدرة الأفراد أو الشركات على شراء السلع والخدمات الأساسية (علي وآخرين، 2022: 355).

تُعد العوامل البشرية في القطاع المالي من المحددات الأساسية للأمان. لذلك، تتمثل إحدى الاستراتيجيات للتعامل مع هذه الهجمات في تقديم التعليم والتدريب والتعلم المستمر لجميع الموظفين في مجال الأمن. يعد التدريب والوعي الأمني ضرورة في كل من التجارة الإلكترونية والمعاملات التقليدية التي أصبحت أقل شيوعًا. يجب على الشركات التجارية والمصرفية أن تخصص موارد أكبر لتعزيز التدابير الأمنية على الشبكة للحفاظ على توفر العمليات وسلامة الودائع (Wang et al., 2020: 2366)

يرى الباحثين أن التطورات الأخيرة تُظهر تنوعًا في الهجمات السيبرانية التي تستهدف المؤسسات المالية، مثل التصيد الاحتيالي وهجمات الفدية وهجمات الحرمان من الخدمة. مع ظهور تقنيات مثل G5 والإنترنت عبر الأقمار الصناعية، أصبح من السهل تنفيذ هجمات سيبرانية موزعة بتكلفة أقل، مما يعرض الأنظمة المالية للخطر. يؤدي ذلك إلى تهديد الثقة بالنظام المالي، ويؤثر بشكل مباشر على قدرة الأفراد والشركات على تنفيذ المعاملات الأساسية. لتعزيز الأمان، يُعد تدريب الموظفين وزيادة الوعي الأمني من الاستراتيجيات الفعالة، مما يتطلب من المؤسسات التجارية والمالية تخصيص موارد أكبر لتطوير التدابير الأمنية وحماية العمليات المالية والودائع.

6. **دور سلسلة الكتل في تعزيز الأمان:** يمكن لتقنية سلسلة الكتل أن تلعب دورًا حيويًا في جعل البيانات المالية أكثر أمانًا، وهو أمر قد يُحدث تغييرًا كبيرًا من منظور الأمن السيبراني. تتيح دفاتر الحسابات اللامركزية تخزين البيانات بشكل آمن، بحيث تكون محمية من التلاعب بفضل شفافيتها، وتقلل الاعتماد على جهة واحدة لحفظ البيانات، مما يمثل ثغرة كبيرة أمام المهاجمين السيبرانيين .وبفضل هذه التقنية، يمكن تخطي بعض الثغرات الموجودة في أنظمة الأمن السيبراني التقليدية، إذ يمكن تأمين العملية من إيداع البيانات وحتى استرجاعها باستخدام التوقيعات الرقمية. فضلا عن ذلك، يمكن أن تعزز العقود الذكية من عمليات التحقق، مما يجعلها أكثر أمانًا وخصوصية؛ إذ يمكن تجزئة البيانات وتشفيرها للوصول الآمن. وتشمل الهجمات السيبرانية عادةً سرقة الهوية والوصول غير المصرح به إلى البيانات الحساسة، ويعزز ذلك ضعف التشفير المستخدم. ومع ذلك، يمكن للعقود الذكية تعزيز

الأمان بشكل كبير من خلال استخدام توقيعات رقمية قوية وضوابط وصول محكمة، مع تبسيط وتطوير سير العمل أيضًا .كما تتميز سلسلة الكتل بقدرتها على تسجيل المعاملات تلقائيًا وبأمان، مع التحقق من مكان حدوثها، ومن قام بها، ومتى، فضلا عما إذا كانت الأصول والقيم موجودة في أي وقت. كما أن الأنظمة القائمة على سلسلة الكتل تجعل من غير الضروري الوثوق بوسطاء أو جهات تحكم لإدارة المعاملات (Yadav et al., 2022: 2).

7. **تكنولوجيا دفتر الحسابات اللامركزي:** تمثل تكنولوجيا دفتر الحسابات اللامركزي (DLT) آلية أمان تتمتع بثلاث خصائص رئيسة (i) :الانفتاح، مما يعني أن سجلات دفتر الحسابات يمكن مشاهدتها من قبل جميع مستخدمي الشبكة؛ (ii) مقاومة التلاعب، مما يعني أن تغييرات سجل دفتر الحسابات يمكن أن تتم فقط من قبل مستخدمين محددين يمتلكون الأذونات اللازمة؛ (iii) حقوق التحكم على سجلات دفتر الحسابات (القراءة والكتابة)، والتي يمكن ممارستها فقط من قبل المالكين والمستخدمين الشرعيين. هذا يوفر سلسلة معاملات غير قابلة للتغيير وقابلة للتتبع، يتم تأمينها بآليات التشفير. تختلف DLT بشكل كبير عن الأنظمة التقليدية لأنها غير مركزية، ففي الأنظمة المركزية مثل البنوك، تُحتفظ سجلات دفتر الحسابات على خادم واحد، ومن ثم يمكن تغيير القواعد والأمان بسهولة. هذا يجعل النظام المركزي عرضة للمخاطر مثل التلاعب بالسجلات أو تنفيذ معاملات احتيالية بسهولة. في المقابل، لا تنتمي أنظمة DLT لأي كيان أو شخص واحد. وتقدم اللامركزية عدة فوائد لتكنولوجيا DLT، فهي تقاوم التلاعب بالبيانات وتمنعه، وتوفر الشفافية لعدة مستخدمين مصادق عليهم في الشبكة، كما تقلل من الاحتيال في الأنظمة المالية وتلغي الحاجة إلى الاعتماد على طرف ثالث .وفي القطاع المالي والمصرفي، يتم تحويل عمليات معالجة المعاملات لتصبح أكثر أمانًا وكفاءة باستخدام DLT. تُستخدم التقنية حاليًا لتسريع عمليات التحويلات المالية وخفض تكاليفها للمؤسسات المالية. ولكن لا تزال هناك بعض التحديات التي تواجه تبني DLT، منها أنها تقنية جديدة نسبياً ولم تثبت فعاليتها على نطاق واسع، كما إن تعقيد النظام قد يزيد بسبب عدم استضافته من قبل كيان واحد، مما يتطلب فهمًا عميقًا لآليات DLT وخوارزميات الإجماع (Abbasi et al., 2021: 20).

8. **استخدام الذكاء الاصطناعي والتعلم الآلي لتحسين الأمن السيبراني:** يمكن للذكاء الاصطناعي والتعلم الآلي أن يسهما بشكل كبير في تعزيز القدرات الأمنية للمؤسسات المالية. من خلال تحليل كميات هائلة من البيانات، يمكن لهذه التقنيات التعرف على الأنماط الشاذة والتنبؤ بالهجمات قبل وقوعها. يشمل ذلك (Luo et al., 2021: 2):

- ❖ الكشف عن التهديدات في الوقت الفعلي: تحليل البيانات المتدفقة للكشف عن أي نشاط مشبوه أو غير مألوف.
- ❖ التعلم من الحوادث السابقة: استخدام التعلم الآلي لتحليل الهجمات السابقة واكتساب الدروس منها لتحسين استراتيجيات الأمان المستقبلية.
- ❖ تطبيق الأتمتة: تحسين سرعة ودقة استجابة النظام للحوادث الأمنية من خلال تطبيق أتمتة الإجراءات الأمنية.

ثالثاً. الجانب العملي: في إطار دراسة "تحصين البيانات المالية: كيف تتلاقى سلسلة الكتل والأمن السيبراني لتوفير أمان لا يُخترق"، تم التركيز على جمع البيانات الأولية من خلال استبانة تم توزيعها على عدد من الأساتذة في الجامعات العراقية، والذين يمثلون مجتمع البحث. تم توزيع 80 استبانة، تم استرجاع 69 منها وتحليلها، بينما تم استبعاد الاستبانات المتبقية لعدم كفاية المعلومات الواردة فيها .

وتم استخدام برنامج SPSS لتحليل استجابات عينة الدراسة، إذ ساعد البرنامج في الكشف عن مدى تأثير استخدام تقنيات سلسلة الكتل والأمن السيبراني على تحسين أمان البيانات المالية. يهدف التحليل إلى تقديم نتائج دقيقة وموثوقة تسهم في فهم كيفية دمج هذه التقنيات بشكل فعال لتحقيق حماية بيانات مالية غير قابلة للاختراق.

1. **صدق الأداة:** لتأكيد صدق الأداة المستخدمة في هذه الدراسة، تم عرض الاستبانة على أربعة أساتذة متخصصين في مجالات الأمن السيبراني وسلسلة الكتل والمحاسبة المالية لتحكيمها. وقام هؤلاء الأساتذة بمراجعة محتوى الاستبانة وتقييم مدى ملاءمتها ووضوحها في قياس متغيرات الدراسة. بناءً على توصياتهم وآرائهم، تم إجراء التعديلات اللازمة لتحسين صياغة بعض البنود وضمان توافقها مع أهداف البحث ومحتواه، مما يعزز من صدق الأداة ويجعلها أكثر ملاءمة لقياس المفاهيم المستهدفة بدقة. وتم استخدام معامل ألفا كرونباخ (Cronbach's Alpha) لتقييم الثبات الداخلي للأداة وللتأكد من مدى اتساق البنود في قياس كل من المتغيرات الرئيسية في الدراسة. أظهر التحليل أن جميع متغيرات البحث قد حققت معاملات ألفا كرونباخ ضمن الحدود المقبولة (0.70 أو أعلى)، مما يشير إلى درجة عالية من الاتساق والثبات للأداة المستخدمة في قياس تأثير تقنيات سلسلة الكتل والأمن السيبراني على أمان البيانات المالية. ويُظهر هذا التحليل أن الأداة تمتاز بمستوى جيد من الثبات والاتساق، مما يجعل نتائج الدراسة أكثر موثوقية ويسهم في تقديم فهم دقيق للعلاقة بين المتغيرات المدروسة.

وتم اختيار الأساتذة الجامعيين في الجامعات العراقية كفئة مستهدفة لهذه الدراسة نظرًا لإلمامهم الأكاديمي والمعرفي العميق بالتقنيات الحديثة مثل سلسلة الكتل والأمن السيبراني، مما يتيح استجابات علمية وتحليلية تعزز دقة النتائج. تضم العينة أساتذة من مجالات المحاسبة، الإدارة، والاقتصاد، وهي تخصصات ترتبط مباشرة بموضوع البحث، مما يضمن توافق مخرجات الدراسة مع أهدافها. يتمتع الأساتذة بقدرتهم على تقييم التقنيات الحديثة، ما يساعد في فهم أعمق لتأثيرها على حماية البيانات المالية.

وتمثل العينة المختارة والتي تشمل 69 مشاركًا مصدرًا غنيًا للمعلومات حول دور التشفير وسلسلة الكتل في حماية البيانات المالية وتعزيز الشفافية. اختيار هذه الفئة يسهم في تحقيق أهداف البحث من خلال تحليل جدوى تطبيق هذه التقنيات في بيئات مالية حقيقية. كما أن تنوع التخصصات والخبرة العملية للمشاركين يضمن استخلاص نتائج موثوقة وقابلة للتطبيق، مما يعزز فعالية التوصيات العملية المقدمة في الدراسة.

جدول (1): معامل Cronbach's Alpha لمتغيرات البحث

المتغيرات	الفقرات	معامل كرونباخ الفا
سلسلة الكتل	5	.861
الامن السيبراني	5	.834
حماية البيانات	8	.857

اعداد الباحث بالاعتماد على مخرجات برنامج SPSS.

2. البيانات الديموغرافية

أ. الجنس:

جدول (2): عينة البحث حسب الجنس

الفئة	التكرار	النسبة
ذكر	51	73.9
انثى	18	26.1
Total	69	100.0

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

يعرض الجدول رقم (2) توزيع عينة البحث حسب الجنس، إذ يوضح نسبة الذكور والإناث المشاركين في الدراسة. يتبين من الجدول أن الذكور يشكلون النسبة الأكبر من العينة، إذ يمثلون 73.9% من إجمالي المشاركين، بعدد تكرار يبلغ 51 مشاركًا. اما الإناث يمثلن نسبة أقل، حيث يشكلن 26.1% من العينة، بعدد تكرار قدره 18 مشاركة.

ب. العمر:

جدول (3): عينة البحث حسب العمر

الفئة	التكرار	النسبة
20-30سنة	7	10.1
اكثر من 40- 30 سنة	16	23.2
أكثر من 50-40 سنة	27	39.1
50سنة فأكثر	19	27.5
Total	69	100.0

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول توزيع العينة حسب العمر، حيث تُمثل الفئة أكثر من 40-50 سنة النسبة الأكبر بنسبة 39.1%، تليها فئة 50 سنة فأكثر بنسبة 27.5%. الفئة العمرية أكثر من 30-40 سنة تأتي بنسبة 23.2%، بينما تسجل الفئة 20-30 سنة أقل نسبة عند 10.1%. يشير التوزيع إلى اهتمام أكبر بالمجال من قبل الفئات العمرية الأكبر.

ج. المؤهل العلمي:

جدول (4): عينة البحث حسب المؤهل العلمي

الفئة	التكرار	النسبة
اعدادية	7	10.1
دبلوم فني	7	10.1
بكالوريوس	37	53.6
دبلوم عالي	9	13.0
ماجستير	2	2.9
دكتوراه	5	7.2
محاسب قانوني	2	2.9
Total	69	100.0

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول أن غالبية العينة من حملة البكالوريوس بنسبة 53.6%، يليهم حملة الدبلوم العالي بنسبة 13%. تُمثل فئتا الإعدادية والدبلوم الفني نسبة متساوية قدرها 10.1% لكل منهما، بينما تشكل فئة الدكتوراه نسبة 7.2%، وأخيرًا كل من الماجستير والمحاسبين القانونيين بنسبة 2.9% لكل منهما. يعكس التوزيع تنوعًا في مستويات التأهيل العلمي.

د. سنوات الخبرة:

جدول (5): عينة البحث حسب سنوات الخبرة

الفئة	التكرار	النسبة
أقل من 5 سنوات	7	10.1
من 10 – 5 سنوات	10	14.5
من 15 – 10 سنة	36	52.2
أكثر من 15 سنة	16	23.2
Total	69	100.0

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول أن غالبية العينة لديهم خبرة من 10-15 سنة بنسبة 52.2%، تليها فئة أكثر من 15 سنة بنسبة 23.2%. أما فئتا من 5-10 سنوات وأقل من 5 سنوات فتمثلان نسبًا أقل، بواقع 14.5% و10.1% على التوالي. يعكس التوزيع حضورًا قويًا لأصحاب الخبرة المتوسطة والطويلة.

ه. نوع المؤهل:

جدول (6): عينة البحث حسب نوع المؤهل

الفئة	التكرار	النسبة
محاسبة	33	47.8
ادارة	9	13.0
اقتصاد	13	18.8
علوم مالية	5	7.2
اخرى	9	13.0
Total	69	100.0

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول رقم (6) توزيع عينة البحث حسب نوع المؤهل:

- ❖ محاسبة تشكل النسبة الأكبر بنسبة 47.8% (33 مشاركًا)، مما يعكس تركيزًا رئيسيًا على المؤهلات المحاسبية.
- ❖ فئتا إدارة وأخرى تمثلان نسبة متساوية قدرها 13% (9 مشاركين لكل منهما).
- ❖ اقتصاد يشكل نسبة 18.8% (13 مشاركًا).
- ❖ علوم مالية تأتي في النهاية بنسبة 7.2% (5 مشاركين).

يشير هذا التوزيع إلى أن غالبية المشاركين لديهم خلفية محاسبية، مع تمثيل جيد لتخصصات أخرى عدة ذات صلة.

3. تحليل اجابات العينة:

أ. **سلسلة الكتل:** الجدول التالي يعرض الاوساط الحسابية والانحرافات المعيارية والترتيب ومستوى الأهمية لفقرات المتغير (سلسلة الكتل) وكما يأتي:

جدول (7): الاوساط الحسابية والانحرافات المعيارية لمتغير سلسلة الكتل

ت	الفقرات	الوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الاهمية
1	تساهم تقنية سلسلة الكتل في تعزيز حماية البيانات المالية من التهديدات الخارجية.	4.30	.626	1	مرتفع
2	تزيد اللامركزية في سلسلة الكتل من أمان البيانات المالية وتحد من مخاطر التلاعب بها.	4.12	.814	4	جيد
3	توفر العقود الذكية في سلسلة الكتل حماية إضافية للمعاملات المالية وتقليل مخاطر الاحتيال.	4.29	.688	2	مرتفع
4	تعزز سلسلة الكتل من شفافية البيانات المالية مما يزيد من مصداقيتها وأمانها.	3.88	.796	5	جيد
5	تساهم آليات الإجماع في سلسلة الكتل في التحقق الدقيق من صحة البيانات المالية.	4.17	.874	3	جيد
	المجموع الكلي	4.013	.494		جيد

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول رقم (7) الأوساط الحسابية والانحرافات المعيارية لمتغير سلسلة الكتل، إذ يشمل تقييم أثر تقنيات سلسلة الكتل على حماية البيانات المالية:

- ❖ تعزيز الحماية من التهديدات الخارجية يأتي في المرتبة الأولى بأعلى وسط حسابي (4.30) وانحراف معياري (0.626)، مما يعكس أهميته المرتفعة.
- ❖ العقود الذكية تحتل المرتبة الثانية بوسط حسابي (4.29) وانحراف معياري (0.688)، مما يُبرز دورها في زيادة الأمان وتقليل الاحتيال.
- ❖ آليات الإجماع تأتي في المرتبة الثالثة بوسط حسابي (4.17) وانحراف معياري (0.874)، مما يعكس دورها في التحقق من صحة البيانات.
- ❖ اللامركزية تحقق وسطًا حسابيًا قدره (4.12) وانحرافًا معياريًا (0.814)، مما يشير إلى دورها في الحد من مخاطر التلاعب.
- ❖ تعزيز الشفافية يسجل أقل وسط حسابي (3.88) وانحرافًا معياريًا (0.796).
- ❖ المجموع الكلي يعكس وسطًا حسابيًا عامًا قدره (4.013) وانحرافًا معياريًا (0.494)، مما يُظهر تأثير تقنيات سلسلة الكتل على تحسين أمان البيانات المالية بشكل جيد إلى مرتفع.

ب. **الامن السيبراني:** الجدول الآتي يعرض الاوساط الحسابية والانحرافات المعيارية والترتيب ومستوى الأهمية لفقرات المتغير (الامن السيبراني) وكما يأتي:

جدول (7): الاوساط الحسابية والانحرافات المعيارية لمتغير الأمن السيبراني

ت	الفقرات	الوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الاهمية
1	تساهم تقنيات التشفير في الأمن السيبراني في حماية البيانات المالية من الاختراقات الإلكترونية.	4.17	.822	2	جيد
2	تساعد أنظمة الكشف عن التهديدات في منع محاولات الوصول غير المصرح به للبيانات المالية.	4.39	.691	1	مرتفع
3	تعزز بروتوكولات المصادقة من سرية وأمان البيانات المالية في النظام المالي.	4.04	.830	4	جيد
4	تعمل الجدران النارية (Firewalls) على منع التهديدات السيبرانية المحتملة لحماية البيانات المالية.	4.03	.766	5	جيد
5	تسهم استمرارية الأعمال في الأمن السيبراني في تقليل خسائر البيانات المالية الناتجة عن الهجمات الإلكترونية.	4.10	.710	3	جيد
	المجموع الكلي	4.158	.539		جيد

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول رقم (7) الأوساط الحسابية والانحرافات المعيارية لمتغير الأمن السيبراني وتأثيره على حماية البيانات المالية:

- ❖ أنظمة الكشف عن التهديدات تأتي في المرتبة الأولى بوسط حسابي 4.39 وانحراف معياري 0.691، مما يشير إلى أهميتها المرتفعة في منع الوصول غير المصرح به.
- ❖ تقنيات التشفير تحتل المرتبة الثانية بوسط حسابي 4.17 وانحراف معياري 0.822، مما يُبرز دورها في حماية البيانات من الاختراقات الإلكترونية.
- ❖ استمرارية الأعمال تأتي في المرتبة الثالثة بوسط حسابي 4.10 وانحراف معياري 0.710، مما يدل على فعاليتها في تقليل خسائر البيانات.
- ❖ بروتوكولات المصادقة تحتل المرتبة الرابعة بوسط حسابي 4.04 وانحراف معياري 0.830، مما يعكس دورها في تعزيز سرية البيانات.
- ❖ الجدران النارية تأتي في المرتبة الخامسة بوسط حسابي 4.03 وانحراف معياري 0.766، مما يشير إلى فعاليتها في منع التهديدات السيبرانية.
- ❖ إن المجموع الكلي للمتغير يعكس وسط حسابي قدره 4.158 وانحراف معياري 0.539، مما يعبر عن تأثير تقنيات الأمن السيبراني بشكل جيد في حماية البيانات المالية.

ج. **حماية البيانات وامنها:** الجدول الآتي يعرض الأوساط الحسابية والانحرافات المعيارية والترتيب ومستوى الأهمية لفقرات المتغير التابع (حماية البيانات وامنها) وكما يأتي:

جدول (7): الأوساط الحسابية والانحرافات المعيارية لمتغير التابع حماية البيانات وامنها

ت	الفقرات	الوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الاهمية
1	تساهم الإجراءات التقنية المتبعة في حماية البيانات المالية من الوصول غير المصرح به.	3.8986	.80704	6	جيد
2	توفر أنظمة الأمان المستخدمة مستوى عالٍ من الحماية للبيانات المالية المحفوظة إلكترونيًا.	3.8841	1.06462	7	جيد
3	تساعد التحديثات المستمرة للأمان في الحفاظ على سرية وسلامة البيانات المالية.	4.0000	.85749	4	جيد
4	تقلل الحلول التقنية المتبعة من مخاطر فقدان البيانات المالية أو تعرضها للتلف.	3.9565	.91450	5	جيد
5	تساهم إجراءات الأمان المتبعة في تحسين ثقة المستخدمين بحماية بياناتهم المالية.	3.8261	.93866	8	جيد
6	تعزز تقنيات الأمان المتكاملة من كفاءة حماية البيانات المالية وموثوقيتها.	4.2176	.59085	1	مرتفع
7	توفر الحلول التكنولوجية المستخدمة مستوىً متقدمًا من حماية البيانات المالية الحساسة.	4.2174	.72497	2	مرتفع
8	تساهم تقنيات الأمان في تقليل وقت استعادة البيانات المالية بعد الهجمات السيبرانية.	4.0870	.70166	3	جيد
	المجموع الكلي	4.126	.561		جيد

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول أن مستوى الأهمية لمتغير "حماية البيانات وأمنها" يتراوح بين جيد ومرتفع، إذ تُظهر الفقرات الأعلى أهمية تقدير المستجيبين للتقنيات المتقدمة والتكامل الأمني في تعزيز الحماية. الفقرة الأكثر أهمية كانت تعزيز كفاءة الحماية من خلال تقنيات الأمان المتكاملة، بينما كانت الأقل أهمية هي تأثير إجراءات الأمان على ثقة المستخدمين. بشكل عام، بلغ الوسط الحسابي الكلي 4.126 مما يعكس فعالية جيدة للإجراءات الحالية، ولكن لا تزال هناك حاجة للتحسين، خاصةً في جوانب الثقة وتكامل الأنظمة.

تُظهر النتائج أهمية الاستثمار المستمر في التقنيات الحديثة وتحديث الأنظمة الأمنية لتعزيز حماية البيانات المالية وزيادة موثوقيتها لدى المستخدمين. كما يُسلط التحليل الضوء على الحاجة لتحسين الوعي لدى المستخدمين بإجراءات الأمان المتبعة، مما قد يُسهم في تعزيز الثقة والاستجابة بشكل أفضل للمخاطر المحتملة.

4. اختبار الفرضيات

اختبار الفرضية الاولى: يوجد تأثير ذو دلالة احصائية لسلسلة الكتل على حماية البيانات المالية وأمانها.

جدول (8): اختبار تأثير سلسلة الكتل على حماية البيانات وامنها

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.		
		B	Std. Error	Beta			R	R^2
1	(Constant)	.139	.280		.496	.000	[a]69.8	.756
	متغير سلسلة الكتل	.982	.068	.869	14.401	.000		
a. Dependent Variable: حماية البيانات وامنها								

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS.

توضح النتائج في الجدول رقم (8) تأثير سلسلة الكتل على حماية البيانات وأمنها، إذ يمكن تحليلها كما يأتي:

- ❖ المعامل غير المعياري (B) لمتغير سلسلة الكتل يبلغ 0.982، مما يشير إلى وجود تأثير إيجابي قوي لسلسلة الكتل على حماية البيانات وأمنها. وهذا يعني أنه عند زيادة تطبيقات سلسلة الكتل، يتحسن مستوى حماية البيانات بشكل ملحوظ. والقيمة التائية (t) بلغت 14.401، وهي قيمة كبيرة جدًا، مما يعكس قوة العلاقة بين سلسلة الكتل وحماية البيانات وأمنها، ويعزز من مصداقية التأثير.
- ❖ القيمة الاحتمالية (.Sig) تساوي 0.000، وهي أقل من مستوى الدلالة المعتاد (0.05)، مما يعني أن التأثير معنوي وإحصائي بشكل قوي، وهو ما يدعم رفض فرضية العدم التي تنص على عدم وجود تأثير معنوي لسلسلة الكتل على حماية البيانات وأمنها.
- ❖ معامل الارتباط (R) بلغ 0.869، مما يدل على وجود علاقة ارتباط قوية بين استخدام سلسلة الكتل وحماية البيانات. ومعامل التحديد (R^2) بلغ 0.756، وهذا يعني أن حوالي 75.6% من التغيرات في مستوى حماية البيانات وأمنها تُفسَّر بتطبيقات سلسلة الكتل، بينما يمكن أن تكون النسبة المتبقية ناجمة عن عوامل أخرى لم تُدرج في النموذج.

بناءً على هذه النتائج، يمكن القول إن فرضية البحث الأولى قد تم إثباتها، حيث يوجد تأثير ذو دلالة إحصائية لسلسلة الكتل على حماية البيانات وأمنها. النتائج تشير إلى أن اعتماد سلسلة الكتل يعزز حماية البيانات ويزيد من أمنها، مما يعزز من أهمية استخدام هذه التكنولوجيا في المؤسسات المصرفية لتقليل المخاطر وزيادة الأمان.

اختبار الفرضية الثانية: يوجد تأثير ذو دلالة احصائية للأمن السيبراني على حماية البيانات المالية وأمانها.

جدول (9): نتائج اختبار تأثير الأمن السيبراني على حماية البيانات المالية وامنها

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.		
		B	Std. Error	Beta			R	R^2
1	(Constant)	1.023	.367		2.791	4.00	.724[a]	524.
	متغير الامن السيبراني	.752	.088	.724	8.591	.000		
a. Dependent Variable: حماية البيانات وامنها								

اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS

توضح نتائج اختبار تأثير الأمن السيبراني على حماية البيانات المالية وأمنها في الجدول ما يأتي:

- ❖ المعامل غير المعياري (B) لمتغير الأمن السيبراني يبلغ 0.752، مما يشير إلى وجود تأثير إيجابي للأمن السيبراني على حماية البيانات المالية وأمنها. هذا يدل على أن تحسين الأمن السيبراني يؤدي إلى تعزيز مستوى حماية البيانات المالية. والقيمة الاحصائية ل (t) بلغت 8.591، وهي قيمة كبيرة، مما يعكس قوة التأثير بين الأمن السيبراني وحماية البيانات المالية، مما يعزز من مصداقية النموذج الإحصائي.
- ❖ القيمة الاحتمالية (.Sig) تساوي 0.000، وهي أقل من مستوى الدلالة التقليدي (0.05)، مما يعني أن التأثير معنوي وإحصائيًا قويًا، مما يسمح برفض فرضية العدم التي تفترض عدم وجود تأثير معنوي للأمن السيبراني على حماية البيانات وأمنها.
- ❖ معامل الارتباط ® بلغ 0.724، مما يدل على وجود علاقة ارتباط قوية بين تطبيقات الأمن السيبراني وحماية البيانات المالية، وهو ما يعزز الفرضية بوجود تأثير معتبر. ومعامل التحديد (R^2) بلغ 0.524، وهذا يشير إلى أن 52.4% من التغيرات في مستوى حماية البيانات المالية وأمنها يمكن تفسيرها بواسطة الأمن السيبراني، بينما يمكن أن تُعزى النسبة المتبقية إلى عوامل أخرى لم تُدرج في النموذج.

تشير هذه النتائج إلى إثبات الفرضية الثانية، حيث يوجد تأثير ذو دلالة إحصائية للأمن السيبراني على حماية البيانات المالية وأمنها. يُبرز هذا التأثير أهمية تبني إجراءات الأمن السيبراني لتعزيز حماية البيانات المالية في المؤسسات المصرفية، ويؤكد على دور الأمن السيبراني كعامل رئيسي في تقليل المخاطر وتحقيق حماية أفضل للبيانات.

رابعاً. النتائج والتوصيات

أ. الاستنتاجات

1. أثبتت الدراسة أن تكامل سلسلة الكتل والأمن السيبراني يُعدّ ضروريًا لتحسين حماية البيانات المالية وأمنها في المصارف، إذ يعزز هذا التكامل الثقة ويقلل المخاطر التشغيلية، مما يسهم في تحقيق الاستدامة المالية وتعزيز فعالية الأنظمة المصرفية .
2. أوضحت النتائج أن سلسلة الكتل تقدم حلولًا فعالة لحماية البيانات المالية من خلال التشفير المتقدم واللامركزية، ما يقلل التلاعب ويعزز الأمان والثقة في المعاملات المصرفية .
3. يمثل الأمن السيبراني ركيزة أساسية لحماية البيانات المالية، إذ تسهم تقنيات الدفاع السيبراني في التصدي للهجمات الإلكترونية وتعزيز سرية البيانات وسلامتها .
4. يؤكد التكامل بين سلسلة الكتل والأمن السيبراني أهمية التقدم التكنولوجي في تحقيق أمان البيانات المالية، مما يُعزز الاعتمادية على الأنظمة المصرفية ويضمن فعالية حماية المعلومات .
5. يتطلب نجاح تطبيق هذه التقنيات دعمًا تنظيميًا وسياسات حوكمة فاعلة، مما يضمن الامتثال للقوانين وتحقيق الأمان المالي المستدام داخل المصارف.

ب. التوصيات: بناءً على الاستنتاجات أعلاه فأننا نوصي بالآتي:

1. توصي الدراسة بتطوير استراتيجيات تكاملية تجمع بين تقنيات سلسلة الكتل والأمن السيبراني لضمان حماية شاملة للبيانات المالية. يجب أن تركز هذه الاستراتيجيات على تحسين الأمان وتقليل المخاطر التشغيلية لتحقيق استدامة مالية فعّالة.

2. يُوصى بتبني أوسع لتقنيات سلسلة الكتل في الأنظمة المصرفية، مع التركيز على خصائصها المتمثلة في التشفير والتوزيع اللامركزي. ينبغي تخصيص استثمارات لدعم التطبيقات الجديدة لهذه التقنية وزيادة الاعتماد عليها في إدارة البيانات المالية.
3. يفضل تطبيق تقنيات متقدمة للأمن السيبراني مثل أنظمة كشف التهديدات، التشفير القوي، وبروتوكولات المصادقة لتعزيز حماية البيانات المالية من الهجمات الإلكترونية وضمان سلامتها وسريتها.
4. وضع أطر تنظيمية وقوانين تدعم استخدام سلسلة الكتل وتقنيات الأمن السيبراني في القطاع المالي. كما يجب أن تشمل هذه الأطر متطلبات الحوكمة الجيدة لضمان التطبيق السليم والامتثال الفعّال للمعايير المحلية والدولية.
5. يُوصى بتقديم برامج تدريبية للعاملين في المصارف لتطوير مهاراتهم في التعامل مع تقنيات سلسلة الكتل والأمن السيبراني. يجب أن تُركز هذه البرامج على تعزيز الوعي الأمني وتطوير قدرات الموظفين في استخدام الأدوات الرقمية بكفاءة.

المصادر

اولاً. المصادر العربية:

1. على، ع. ا.، عبد المؤمن، أبو الصفا، وسليمان. (2022). دراسة أساليب الخصوصية والأمن المستخدمة في سلسلة الكتلة. مجلة الدراسات والبحوث البيئية، 12(4)، 342-354.
2. علي سيد إسماعيل. (2021). تقنية البلوك تشين Blockchain آليةً لحوكمة المؤسسات المالية الإسلامية المعاصرة. مجلة جامعة القاسمية للاقتصاد الإسلامي، 1(1)، 147-188.

ثانياً. المصادر الأجنبية:

1. Abbasi, M., Shahraki, A., & Taherkordi, A. (2021). Deep learning for network traffic monitoring and analysis (NTMA): A survey. Computer Communications, 170, 19-41.
2. Idrees, S. M., Nowostawski, M., Jameel, R., & Mourya, A. K. (2021). Security aspects of blockchain technology intended for industrial applications. Electronics, 10(8), 951.
3. Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In Handbook of research on blockchain technology (pp. 349-371). Academic Press.
4. Luo, F., Jiang, Y., Zhang, Z., Ren, Y., & Hou, S. (2021). Threat analysis and risk assessment for connected vehicles: A survey. Security and Communication Networks, 2021(1), 1263820.
5. Wang, J., Chen, W., Wang, L., Sherratt, R. S., Alfarraj, O., & Tolba, A. (2020). Data secure storage mechanism of sensor networks based on blockchain. Computers, Materials & Continua, 65(3), 2365-2384