

جامعة ميدأوشن

كلية الإدارة

ماجستير إدارة المخاطر



أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية على
خفض مخاطر الخصوصية وتسرب البيانات: دراسة تحليلية تطبيقية

إعداد الطالب/

بركات شميلان العازمي

إشراف/

د. الفیصل عبد الحمید محمد حسن

د.فايز جراد

العام الدراسي:

2026

٣	• مقدمة:
٥	• مشكلة الدراسة
٦	• أهداف الدراسة
٧	• أسئلة الدراسة
٨	• الفرض الرئيسي:
٨	• أهمية الدراسة
١٠	• الدراسات السابقة:
١٠	• أولاً: الدراسات العربية
١٣	• ثانياً: الدراسات الأجنبية
١٨	• الفجوة البحثية
١٩	• المنطلقات النظرية للدراسة
٢٣	• المنهجية وطرق البحث:
٢٣	• مجتمع وعينة الدراسة
٢٤	• مصادر جمع البيانات
٢٤	• أداة الدراسة (الاستبانة)
٢٥	• الأساليب الإحصائية المستخدمة
٢٦	• حدود الدراسة
٢٨	• المراجع:

مقدمة:

يُمثل التحول الرقمي في القطاع الصحي أحد أبرز الملامح المعاصرة للثورة الصناعية الرابعة، حيث أصبحت البيانات الصحية تُشكّل شريان الحياة لمنظومة الرعاية الصحية الحديثة بما تتضمنه من سجلات طبية إلكترونية ونتائج فحوصات مخبرية وصور أشعة وبيانات أجهزة المراقبة عن بُعد وغيرها من المعلومات الحساسة التي تتدفق باستمرار بين المؤسسات الصحية المختلفة. وقد فرض هذا الواقع الرقمي المتنامي حاجة ملحة إلى مشاركة هذه البيانات بين المستشفيات والمراكز البحثية والجهات التنظيمية وشركات التأمين لتحقيق تكامل الرعاية الصحية وتحسين جودة القرارات العلاجية، غير أن هذه المشاركة المتزايدة أفرزت في المقابل تحديات جوهرية تتعلق بأمن البيانات وحماية خصوصية المرضى في ظل اعتماد معظم المؤسسات الصحية على أنظمة مركزية تقليدية لم تُصمّم أصلاً لمواكبة هذا الحجم المتصاعد من تبادل البيانات. (Yaqoob et al., 2022)

و برزت تقنية سلاسل الكتل (Blockchain) بوصفها إحدى أكثر التقنيات الناشئة إثارة للاهتمام في مجال إدارة البيانات الصحية، إذ تقوم فلسفتها على مبدأ اللامركزية في تخزين البيانات ومعالجتها عبر شبكة موزعة من العقد تُسجّل المعاملات في سجل رقمي غير قابل للتعديل ومحمي بتقنيات تشفير متقدمة. وتتميز هذه التقنية بخصائص جوهرية تجعلها ملائمة للسياق الصحي، من أبرزها التشفير اللامركزي الذي يُوزّع البيانات عبر شبكة واسعة بدلاً من تخزينها في نقطة واحدة، والعقود الذكية التي تُؤتمت عمليات التحكم في الوصول وفق قواعد محددة مسبقاً دون الحاجة إلى وسطاء، وخاصية عدم قابلية التعديل التي تحفظ سلامة السجلات من أي تلاعب، فضلاً عن آليات إدارة الموافقة التي تمنح المرضى سيطرة مباشرة على بياناتهم (عبدالمحسن وآخرون ، ٢٠٢٣)

ولقد شهدت التطبيقات العملية لتقنية سلاسل الكتل في المجال الصحي اهتماماً بحثياً متزايداً على المستوى الدولي، حيث استُكشفت إمكانياتها في تأمين تبادل المعلومات الصحية بين المؤسسات المختلفة، وتمكين المرضى من التحكم في بياناتهم ومنح أو سحب صلاحيات الوصول بشكل فوري وشفاف، وتعزيز التشغيل البيئي بين الأنظمة الصحية المتباينة دون المساس بسرية المعلومات. كما أثبتت الدراسات أن دمج تقنيات التشفير المتقدمة مع البنية اللامركزية لسلاسل الكتل يُمكنه أن يُعيد تشكيل نماذج حماية

السجلات الصحية من خلال توفير حماية شاملة من طرف إلى طرف تشمل مراحل التخزين والنقل والمعالجة. (Vanin et al., 2022)

ومن جهة أخرى، تُعدّ مخاطر الخصوصية وتسرب البيانات الصحية من أخطر التهديدات التي تواجه المنظومة الصحية الرقمية المعاصرة، إذ تنتم البيانات الصحية بحساسة استثنائية كونها تتضمن معلومات شخصية وطبية ونفسية ومالية يُمكن أن يؤدي كشفها إلى أضرار بالغة بالمرضى تتراوح بين الضرر المعنوي والتمييز في التأمين والتوظيف والابتزاز الإلكتروني. وتتنوع مصادر هذه المخاطر بين الهجمات السيبرانية الخارجية والتهديدات الداخلية الناجمة عن سوء استخدام صلاحيات الوصول ونقاط الضعف في البنى المركزية التقليدية التي تجعل من قواعد البيانات الموحدة هدفاً مغرياً للمهاجمين (Adeghe et al., 2024).

وتتعاظم أهمية التصدي لهذه المخاطر في السياق السعودي تحديداً، حيث تمضي المملكة العربية السعودية بخطوات حثيثة نحو رقمنة قطاعها الصحي ضمن مستهدفات رؤية ٢٠٣٠ وبرنامج التحول الصحي، مما يجعل حجم البيانات الصحية المتداولة في تصاعد مستمر ويضاعف من الحاجة إلى حلول أمنية متقدمة. وقد أكدت الدراسات المحلية أن واقع مشاركة البيانات الصحية في المملكة لا يزال يُعاني من تحديات مرتبطة بغياب السياسات الموحدة وضعف الوسائل التقنية المتاحة لتبادل البيانات بين الباحثين والمؤسسات الصحية بشكل آمن ومقنّن (الهلال، ٢٠٢٠).

وفي ضوء هذا السياق العلمي والعملية، تتجه هذه الدراسة إلى استقصاء أثر تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية بأبعاده الأربعة على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية، ساعيةً إلى تقديم إسهام علمي وعملي يُثري الأدبيات العربية في هذا المجال البحثي الناشئ ويُزوّد صنّاع القرار في القطاع الصحي السعودي برؤى مبنية على أدلة بحثية حول جدوى تبني هذه التقنية الواعدة في حماية البيانات الصحية وتعزيز خصوصية المرضى (العنزي والرابغي، ٢٠٢٥)

مشكلة الدراسة

يشهد القطاع الصحي على المستوى العالمي والمحلي تحولاً رقمياً متسارعاً أفضى إلى تضاعف حجم البيانات الصحية المتولدة والمتبادلة بين المؤسسات الصحية بصورة غير مسبقة، إذ تشير تقارير المنتدى الاقتصادي العالمي إلى أن القطاع الصحي يُنتج ما يقارب ٣٠٪ من إجمالي حجم البيانات العالمية، مع توقعات بأن يصل معدل النمو السنوي المركّب لهذه البيانات إلى ٣٦٪ بحلول عام ٢٠٢٥. وقد أدّى هذا التضخم الهائل في البيانات الصحية، المقترن بتزايد الحاجة إلى مشاركتها بين المستشفيات والمراكز البحثية وشركات التأمين والجهات التنظيمية، إلى تصاعد مخاطر الخصوصية وتسرب البيانات بشكل يندرج بتهديدات جسيمة تطال سلامة المرضى وسرية معلوماتهم وثقتهم في المنظومة الصحية برمتها.

وتكشف الإحصاءات الدولية عن خطورة هذا الواقع، حيث أظهر تقرير IBM Security لعام ٢٠٢٤ أن متوسط تكلفة اختراق البيانات في القطاع الصحي بلغ نحو ١٠.٩٣ مليون دولار أمريكي لكل حادثة، وهو الأعلى بين جميع القطاعات للعام الرابع عشر على التوالي. كما وثّق مكتب الحقوق المدنية التابع لوزارة الصحة والخدمات الإنسانية الأمريكية أكثر من ٧٢٥ حادثة اختراق كبيرة للبيانات الصحية خلال عام ٢٠٢٣ وحده، أثّرت على أكثر من ١٣٣ مليون سجل صحي. وعلى المستوى المحلي، فإن المملكة العربية السعودية ليست بمعزل عن هذه التحديات، إذ تُصنّف ضمن الدول الأكثر استهدافاً بالهجمات السيبرانية في منطقة الشرق الأوسط، وقد نبّهت الهيئة الوطنية للأمن السيبراني في تقاريرها إلى تصاعد التهديدات الموجهة للقطاع الصحي السعودي، لا سيما في ظل التوسع المتسارع في رقمنة الخدمات الصحية تنفيذاً لمستهدفات رؤية المملكة ٢٠٣٠ وبرنامج التحول الصحي.

وتتمحور جذور هذه المشكلة في أن أنظمة إدارة البيانات الصحية التقليدية تعتمد في معظمها على بنى مركزية تُخزّن البيانات في قواعد بيانات موحّدة، مما يجعلها عرضة لنقطة فشل واحدة تُتيح للمهاجمين الوصول إلى كميات ضخمة من البيانات الحساسة في حادثة اختراق واحدة. كما أن آليات التحكم في الوصول وإدارة صلاحيات المشاركة في هذه الأنظمة غالباً ما تقتصر إلى الشفافية والمرونة الكافية، حيث لا يملك المرضى سيطرة فعلية على بياناتهم ولا يمكنهم تتبّع من يصل إليها أو يتداولها. ويزداد هذا الوضع تعقيداً مع غياب آليات موحّدة لضمان سلامة البيانات وعدم التلاعب بها أثناء عمليات النقل

والمشاركة بين المؤسسات الصحية المتعددة، فضلاً عن ضعف أنظمة إدارة الموافقة التي تُعاني من بطء الإجراءات وعدم القدرة على التحقق التلقائي من صلاحيات الوصول.

وفي هذا السياق، برزت تقنية سلاسل الكتل (Blockchain) بوصفها حلاً تقنياً واعداً يحمل في بنيته الجوهرية خصائص قد تُعالج هذه التحديات المتشابكة، من خلال التشفير اللامركزي الذي يُلغي الاعتماد على نقطة تخزين مركزية واحدة، والعقود الذكية التي تُؤتمت عمليات التحكم في الوصول وفق شروط محددة مسبقاً دون الحاجة إلى وسيط، وخاصية عدم قابلية التعديل التي تضمن سلامة السجلات الصحية وعدم التلاعب بها، وآليات إدارة الموافقة اللامركزية التي تمنح المرضى ملكية بياناتهم والتحكم الكامل في مشاركتها. غير أن الأدبيات العربية تكاد تخلو من دراسات تحليلية تطبيقية تقيس أثر هذه الأبعاد مجتمعة على خفض مخاطر الخصوصية وتسرب البيانات في السياق الصحي السعودي، وهو ما أكّده مراجعة الدراسات السابقة التي كشفت عن فجوة بحثية واضحة في هذا المجال.

وعليه، تتبلور مشكلة الدراسة في السؤال الجوهرى التالي: **ما أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية؟**

أهداف الدراسة

تهدف هذه الدراسة إلى التعرف على أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية.

ويتفرع من هذا الهدف الرئيسى الأهداف الفرعية التالية:

1. التعرف على أثر التشفير اللامركزي للبيانات عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

٢. التعرف على أثر العقود الذكية للتحكم في الوصول عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.
٣. التعرف على أثر سلامة البيانات وعدم قابليتها للتعديل عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.
٤. التعرف على أثر آليات إدارة الموافقة والتفويض عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.
٥. تقديم إطار مقترح لتبني تقنية سلاسل الكتل في مشاركة البيانات الصحية بما يُعزّز حماية الخصوصية ويُخفّض مخاطر تسرب البيانات في المؤسسات الصحية السعودية.

أُسئلة الدراسة

السؤال الرئيسي:

ما أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية؟

الأسئلة الفرعية:

١. ما أثر التشفير اللامركزي للبيانات عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟
٢. ما أثر العقود الذكية للتحكم في الوصول عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟
٣. ما أثر سلامة البيانات وعدم قابليتها للتعديل عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟
٤. ما أثر آليات إدارة الموافقة والتفويض عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية؟

فروض الدراسة

الفرض الرئيسي:

يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده مجتمعة (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية.

الفروض الفرعية:

الفرض الفرعي الأول: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للتشفير اللامركزي للبيانات عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

الفرض الفرعي الثاني: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للعقود الذكية للتحكم في الوصول عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

الفرض الفرعي الثالث: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لسلامة البيانات وعدم قابليتها للتعديل عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

الفرض الفرعي الرابع: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لآليات إدارة الموافقة والتفويض عبر تقنية سلاسل الكتل على خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية بالمملكة العربية السعودية.

أهمية الدراسة

الأهمية العلمية (النظرية):

- تُسهم هذه الدراسة في سدّ فجوة واضحة في الأدبيات العربية التي تفتقر إلى دراسات تربط بين تقنية سلاسل الكتل ومشاركة البيانات الصحية في إطار تحليلي متكامل، إذ تُعدّ من الدراسات العربية الأولى التي تتناول هذا الموضوع بأبعاده الأربعة مجتمعة في السياق الصحي.
- تُقدّم الدراسة إطاراً مفاهيمياً يجمع بين أبعاد تقنية سلاسل الكتل (التشفير اللامركزي، العقود الذكية، سلامة البيانات، إدارة الموافقة (وعلاقتها بخفض مخاطر الخصوصية وتسرب البيانات، مما يُوفّر أساساً نظرياً يمكن للباحثين البناء عليه في دراسات مستقبلية.
- تُسهم الدراسة في تعميق الفهم العلمي لكيفية تأثير الخصائص الجوهرية لتقنية البلوكتشين (كاللامركزية وعدم قابلية التعديل) على حماية البيانات الصحية من الاختراقات والتسريبات.
- تُضيف الدراسة إلى المعرفة العلمية من خلال استكشاف التحديات الواقعية التي تواجه تطبيق تقنية سلاسل الكتل في القطاع الصحي، بما يُمكن الباحثين من تحديد الثغرات البحثية واقتراح حلول مبتكرة.

الأهمية العملية (التطبيقية):

- تُوفّر الدراسة نتائج وتوصيات عملية يُمكن لصنّاع القرار في القطاع الصحي السعودي الاستفادة منها في اتخاذ قرارات مدروسة بشأن تبني تقنية سلاسل الكتل لتعزيز حماية البيانات الصحية.
- تتوافق الدراسة مع مستهدفات رؤية ٢٠٣٠ في التحول الرقمي للقطاع الصحي، حيث تُقدّم رؤية حول كيفية الاستفادة من التقنيات الناشئة في تحسين أمن البيانات الصحية وحماية خصوصية المرضى.
- تُقدّم الدراسة إرشادات عملية تُساعد المؤسسات الصحية على الامتثال لمتطلبات نظام حماية البيانات الشخصية الصادر في المملكة العربية السعودية من خلال تبني حلول تقنية متقدمة.
- تُسهم نتائج الدراسة في توعية المؤسسات الصحية بالأثر الاقتصادي لتسرب البيانات الصحية وتقديم حلول تقنية قائمة على البلوكتشين لخفض هذه التكاليف والمخاطر القانونية.

الدراسات السابقة:

أولاً: الدراسات العربية

دراسة (العنزي والرابغي، ٢٠٢٥): حماية المعرفة في المدن الصحية الذكية بين مشاركة البيانات وضمان الأمن والخصوصية.

هدفت الدراسة إلى التعرف على واقع حماية المعرفة في المدن الصحية الذكية بأبعاده (مشاركة البيانات الصحية، أمن المعلومات الصحية، خصوصية البيانات) وتأثيرها على تحقيق التوازن بين إتاحة البيانات للمستفيدين وحمايتهم من المخاطر الأمنية في بيئة المدن الذكية. واستخدمت الدراسة المنهج الوصفي التحليلي لتحليل الأدبيات والدراسات المتعلقة بالموضوع. وتوصلت نتائج الدراسة إلى أن المدن الصحية الذكية تواجه تحديات جوهرية في تحقيق التوازن بين مشاركة البيانات الصحية وضمان أمنها وخصوصيتها، وأن التقنيات الحديثة مثل التشفير والبلوكشين تُسهم في تعزيز حماية المعرفة الصحية، غير أن غياب الأطر التنظيمية الموحدة يُشكل عائقاً أمام تحقيق الحماية الشاملة. وأوصت الدراسة بضرورة تطوير سياسات واضحة ومتكاملة لحماية البيانات الصحية في المدن الذكية، وتبني الحلول التقنية المتقدمة القائمة على التشفير والبلوكشين، وتعزيز التعاون بين الجهات الصحية والتقنية لتحقيق مشاركة آمنة وفعّالة للبيانات.

دراسة (الهلال، ٢٠٢٠): مشاركة البيانات الصحية بين الباحثين الحاصلين على منح برنامج دعم أبحاث كوفيد-١٩ من وزارة الصحة السعودية.

هدفت الدراسة إلى التعرف على مدى مشاركة البيانات الصحية بين الباحثين الحاصلين على منح برنامج دعم أبحاث كوفيد-١٩ من وزارة الصحة السعودية بأبعاده (وسائل مشاركة البيانات، معوقات المشاركة، مستوى الدعم المؤسسي) وأثرها على جودة الأبحاث العلمية الموجهة لمواجهة الجائحة في المملكة العربية السعودية. واستخدمت الدراسة المنهج الوصفي المسحي، وتكونت العينة من الباحثين الحاصلين على منح البرنامج، حيث وُزعت عليهم استبانة لجمع البيانات. وتوصلت نتائج الدراسة إلى أن ٩٠٪ من الباحثين يدركون أن مشاركة البيانات ترفع من مستوى جودة الأبحاث للتصدي لكوفيد-١٩، وأن ٨٠٪ يستخدمون البريد الإلكتروني وسيلةً أساسيةً لمشاركة البيانات، بينما تمثلت أبرز المعوقات في عدم وجود

سياسات داعمة للمشاركة بنسبة ٨٠%، وقلة وسائل المشاركة وضعف الوعي المعلوماتي بنسبة ٧٠%. وأوصت الدراسة بضرورة وضع سياسات واضحة لمشاركة البيانات الصحية بين الباحثين، وتوفير منصات إلكترونية آمنة ومتخصصة لتبادل البيانات، وتعزيز الدعم المؤسسي من وزارة الصحة لتحفيز الباحثين على المشاركة المقننة والمنظمة.

دراسة (السلمي، ٢٠٢٢): واقع تكامل البيانات الضخمة في المركز الوطني للمعلومات الصحية بالمملكة العربية السعودية.

هدفت الدراسة إلى التعرف على واقع تكامل البيانات الضخمة في المركز الوطني للمعلومات الصحية بأبعاده (البنية التحتية للبيانات، آليات التكامل، تحديات الإدارة) ومدى قدرته على تحقيق تكامل فعال في إدارة المعلومات الصحية في المملكة العربية السعودية. واستخدمت الدراسة منهج دراسة الحالة لتحليل واقع التكامل في المركز الوطني للمعلومات الصحية. وتوصلت نتائج الدراسة إلى أن المركز الوطني يبذل جهوداً ملموسة في تكامل البيانات الصحية الضخمة من مصادر متعددة، إلا أنه يواجه تحديات تتعلق بتوحيد المعايير بين المؤسسات الصحية المختلفة، وضمان جودة البيانات وسلامتها، فضلاً عن التحديات المتعلقة بالخصوصية والأمن. وأوصت الدراسة بتطوير أطر تنظيمية موحدة لتكامل البيانات الصحية، وتبني تقنيات متقدمة لضمان جودة البيانات وحمايتها، وتعزيز التعاون بين الجهات الصحية المختلفة لتحقيق تكامل شامل.

دراسة (عبدالمحسن ومحمد وعبدالمجيد، ٢٠٢٣): التحول الرقمي باستخدام تكنولوجيا سلاسل الكتل "Blockchain".

هدفت الدراسة إلى التعرف على تقنية سلاسل الكتل (Blockchain) بأبعاده (المفهوم والأنواع، آلية العمل، التطبيقات في القطاعات المختلفة) ودورها في تحقيق التحول الرقمي في المؤسسات الحكومية والخاصة. واستخدمت الدراسة المنهج الوصفي النظري القائم على مراجعة وتحليل الأدبيات ذات الصلة. وتوصلت نتائج الدراسة إلى أن تقنية سلاسل الكتل تُعدّ من أبرز ركائز الثورة الصناعية الرابعة إلى جانب الذكاء الاصطناعي، وأنها تُسهم في خفض التكاليف وتسريع الأداء وتحقيق الشفافية في مختلف القطاعات، وأن الحكومات والشركات الخاصة حول العالم بدأت في تبنيها لتحقيق التحول الرقمي.

وأوصت الدراسة بضرورة تكثيف الجهود البحثية لتطوير تطبيقات سلاسل الكتل في القطاعات الحيوية كالصحة والتعليم والمالية، والعمل على بناء بنية تحتية رقمية داعمة لتبني هذه التقنية.

دراسة (المزيد، ٢٠٢٤): واقع استخدام سلاسل الكتل "Block Chain" في المصارف السعودية: دراسة حالة مصرف الراجحي.

هدفت الدراسة إلى التعرف على واقع استخدام تقنية سلاسل الكتل في المصارف السعودية بأبعاده (الشفافية، أمان المعاملات، كفاءة العمليات المصرفية) وذلك من خلال دراسة حالة مصرف الراجحي. واستخدمت الدراسة منهج دراسة الحالة القائم على التحليل الوصفي. وتوصلت نتائج الدراسة إلى أن تطبيق تقنية البلوكتشين في المصارف يُسهم في زيادة شفافية وأمان المعاملات المالية وتحسين كفاءة العمليات المصرفية، كما تُسهّل عمليات التحويل وتخفيض التكاليف عبر القضاء على الوساطة في القطاع المصرفي، فضلاً عن مساهمتها في حماية البيانات وتعزيز موثوقية مجال إنترنت الأشياء. وأوصت الدراسة بتكثيف الجهود والأبحاث لتطوير هذه التقنية وتكييفها مع المصارف الإسلامية وفق مبادئ الشريعة الإسلامية، والاهتمام بإيجاد حلول للتحديات التي تواجه تطبيقها.

دراسة (الضعيلة وعوض، ٢٠٢٤): أثر استخدام تقنية سلاسل الكتل على إدارة سلاسل التوريد في شركات الصناعات الدوائية الأردنية.

هدفت الدراسة إلى التعرف على أثر استخدام تقنية سلاسل الكتل بأبعاده (اللامركزية، التشفير، العقود الذكية، الشفافية) على إدارة سلاسل التوريد في شركات الصناعات الدوائية الأردنية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من العاملين في الإدارات ذات الصلة بسلاسل التوريد وتكنولوجيا المعلومات في شركات الأدوية الأردنية. وتوصلت نتائج الدراسة إلى وجود أثر إيجابي ذي دلالة إحصائية لاستخدام تقنية سلاسل الكتل على إدارة سلاسل التوريد، حيث تُسهم في تعزيز الشفافية وتتبع المنتجات الدوائية وخفض مخاطر التزوير والتلاعب. وأوصت الدراسة بضرورة تبني شركات الأدوية لتقنية البلوكتشين لتحسين كفاءة سلاسل التوريد، وتطوير البنية التحتية التقنية اللازمة، وتدريب الكوادر البشرية على استخدام هذه التقنية.

دراسة (سراج، ٢٠٢٤): أثر استخدام تقنية سلاسل الكتل على إدارة سلاسل الإمداد لدعم الميزة التنافسية: دراسة تطبيقية على شركات الأدوية العاملة في السوق المصرية.

هدفت الدراسة إلى التعرف على الأثر المباشر وغير المباشر لتقنية سلاسل الكتل بأبعاده (اللامركزية، الشفافية، الأتمتة، الأمان) من خلال الدور الوسيط لإدارة سلاسل الإمداد على الميزة التنافسية لشركات الأدوية العاملة في السوق المصرية. واستخدمت الدراسة المنهج الوصفي التحليلي بأسلوب الحصر الشامل، وتكونت العينة من رؤساء مجالس الإدارات ومديري إدارات تكنولوجيا المعلومات في ١٧٠ شركة دوائية مصرية، حيث تم جمع 242 استمارة استقصاء صحيحة. وتوصلت نتائج الدراسة إلى معنوية التأثير المباشر وغير المباشر لأبعاد تقنية سلاسل الكتل على الميزة التنافسية، وذلك من خلال الدور الوسيط لإدارة سلاسل الإمداد، كما تبين وجود اختلافات معنوية بين أنواع الشركات الثلاثة (عامة، خاصة، استثمار أجنبي ومشارك) من حيث توافر أبعاد التقنية. وأوصت الدراسة بضرورة تبني تقنية البلوكتشين في سلاسل الإمداد الدوائية لتعزيز الميزة التنافسية، وتوفير البنية التحتية والتدريب اللازمين.

دراسة (عبدالقادر، ٢٠٢٢): أثر تطبيق تقنية سلاسل الكتل على المراجعة الخارجية.

هدفت الدراسة إلى التعرف على أثر تطبيق تقنية سلاسل الكتل (Blockchain) بأبعاده (سلامة البيانات، التشفير، العقود الذكية، السجل الرقمي الموزع) على المراجعة الخارجية وكيفية إحداثها تحولاً في عمليات المراجعة. واستخدمت الدراسة المنهجين الاستقرائي والاستنباطي لتحليل الأدبيات والدراسات ذات الصلة. وتوصلت نتائج الدراسة إلى أن تطبيق تقنية سلاسل الكتل أحدث تحولاً جوهرياً في مهنة المراجعة تمثل في تخفيض وقت عملية المراجعة، وتعزيز دقة المعلومات، والتحقق من سلامة العمليات، وإنشاء مسارات مراجعة أكثر كفاءة، وإجراء عمليات مراجعة مستمرة، وسرعة اكتشاف الأخطاء وكشف الاحتيال. وأوصت الدراسة بضرورة تطوير المهارات التكنولوجية للمراجعين الخارجيين للتعامل مع بيئة البلوكتشين، وتبني أساليب مراجعة حديثة تتلاءم مع البيئة الإلكترونية.

ثانياً: الدراسات الأجنبية

دراسة (Adeghe, Okolo & Ojeyinka, 2024): Evaluating the Impact of Blockchain Technology in Healthcare Data Management: A Review of Security, Privacy, and Patient Outcomes.

هدفت الدراسة إلى التعرف على أثر تقنية البلوكتشين في إدارة البيانات الصحية بأبعاده (أمن البيانات وسلامتها، خصوصية المرضى والتحكم في بياناتهم، التشغيل البيئي وتحسين نتائج المرضى (وتقييم إمكانياتها التحويلية في قطاع الرعاية الصحية. واستخدمت الدراسة المنهج الوصفي التحليلي القائم على المراجعة المنهجية للأدبيات ودراسات الحالة الواقعية. وتوصلت نتائج الدراسة إلى أن تقنية البلوكتشين تضمن سلامة البيانات وعدم قابليتها للتغيير من خلال الهياكل اللامركزية والعقود الذكية، كما تمنح المرضى ملكية بياناتهم الصحية والتحكم فيها مع الحفاظ على السرية، فضلاً عن تعزيز التشغيل البيئي وتبسيط العمليات الصحية. وأوصت الدراسة بضرورة مواصلة البحث في معالجة التحديات التقنية والأخلاقية وتكامل البلوكتشين مع الأنظمة الصحية القائمة لتحقيق تبني واسع النطاق.

دراسة (Chianumba, Ikhalea, Mustapha, Forkuo & Osamika, 2022): Integrating AI, Blockchain, and Big Data to Strengthen Healthcare Data Security, Privacy, and Patient Outcomes.

هدفت الدراسة إلى التعرف على إمكانية دمج الذكاء الاصطناعي وسلاسل الكتل والبيانات الضخمة بأبعاده (حماية البيانات بالتشفير المدعوم بالذكاء الاصطناعي، سلامة البيانات عبر البلوكتشين اللامركزي، تحليلات البيانات الضخمة للتنبؤ بنتائج المرضى) لتعزيز أمن البيانات الصحية والخصوصية وتحسين نتائج المرضى. واستخدمت الدراسة المنهج الوصفي النظري القائم على بناء نموذج مفاهيمي تكاملي. وتوصلت نتائج الدراسة إلى أن الذكاء الاصطناعي يُعزز أمن البيانات من خلال التشفير المتقدم واكتشاف التهديدات الأمنية، وأن البلوكتشين يضمن سلامة البيانات من خلال التخزين اللامركزي والعقود الذكية، وأن تحليلات البيانات الضخمة تُسهم في التنبؤ بنتائج المرضى وضمان الامتثال لمعايير الخصوصية. وأوصت الدراسة بتبني استراتيجيات شاملة لدمج هذه التقنيات في البنية التحتية الصحية مع التركيز على معالجة التحديات التنظيمية والتشغيلية.

دراسة (Handayani, Apriani, Mulyati, Zahra & Yusuf, 2023): Enhancing Security and Privacy of Patient Data in Healthcare: A SmartPLS Analysis of Blockchain Technology Implementation.

هدفت الدراسة إلى التعرف على أثر تطبيق تقنية البلوكتشين بأبعاده (أمن البيانات، خصوصية البيانات، إدارة البيانات) على تعزيز أمن وخصوصية بيانات المرضى في منظومة الرعاية الصحية. واستخدمت الدراسة المنهج الكمي التحليلي باستخدام أسلوب SmartPLS لنمذجة المعادلات البنائية، وتكونت العينة من مؤسسات الرعاية الصحية التي طبقت تقنية البلوكتشين في إدارة بياناتها، حيث جُمعت البيانات من خلال استبيانات. وتوصلت نتائج الدراسة إلى وجود تأثير إيجابي ذي دلالة إحصائية لتطبيق تقنية البلوكتشين على تعزيز أمن وخصوصية بيانات المرضى، كما حدّدت الدراسة تحديات تتعلق بقبالية التوسع والتشغيل البيئي تحتاج إلى معالجة لضمان نجاح التطبيق. وأوصت الدراسة بضرورة معالجة تحديات التوسع والتكامل مع الأنظمة القائمة لتحقيق تطبيق فعال وشامل للبلوكتشين في المؤسسات الصحية.

دراسة (Yaqoob, Salah, Jayaraman & Al-Hammadi, 2022): Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations.

هدفت الدراسة إلى التعرف على كيفية الاستفادة من تقنية البلوكتشين في إدارة البيانات الصحية بأبعاده (الشفافية وتتبع المعاملات، أمن السجلات الصحية الإلكترونية، التشغيل البيئي ومشاركة البيانات، تتبع سلاسل التوريد الدوائية) في قطاع الرعاية الصحية. واستخدمت الدراسة المنهج الوصفي التحليلي القائم على المراجعة الشاملة للأدبيات وتحليل التجارب التطبيقية الدولية (مثل تجربة إستونيا والإمارات). وتوصلت نتائج الدراسة إلى أن أنظمة إدارة البيانات الصحية الحالية تواجه تحديات جوهرية في الشفافية والتتبع وسلامة البيانات، وأن تقنية البلوكتشين تُقدّم حلولاً فعّالة لهذه التحديات من خلال السجل الموزع غير القابل للتعديل، إلا أن عقبات مثل قابلية التوسع وتكاليف التنفيذ والامتثال التنظيمي لا تزال تُعيق التبني الواسع. وأوصت الدراسة بتطوير حلول بلوكتشين هجينة (عامة/خاصة) مُخصّصة للرعاية الصحية، والعمل على تحسين قابلية التوسع وخفض التكاليف التشغيلية.

دراسة: (Afrihyia, Chianumba, Mustapha, Forkuo & Omotayo, 2025)
Developing Privacy-Preserving Data Sharing Protocols for Healthcare Systems Using Cryptographic and Blockchain-Based Techniques.

هدفت الدراسة إلى التعرف على تطوير بروتوكولات مشاركة البيانات المحافظة على الخصوصية في الأنظمة الصحية بأبعاده (التشفير المتماثل الكامل، إثباتات المعرفة الصفرية، التشفير القائم على السمات، العقود الذكية عبر البلوكتشين) من خلال دمج التقنيات التشفيرية وتقنية البلوكتشين. واستخدمت الدراسة المنهج الوصفي التحليلي القائم على المراجعة المنهجية المنظمة للأدبيات مع تحليل مقارنة بين الأنظمة المقترحة والأنظمة المركزية التقليدية. وتوصلت نتائج الدراسة إلى أن الإطار المقترح يُخفف بشكل ملحوظ من مخاطر الوصول غير المصرح به وتسرب البيانات ونقاط الفشل الأحادية، وأن التحليل المقارن مع الأنظمة المركزية التقليدية أظهر تحسناً في الكفاءة وقابلية التوسع والأمن في إدارة البيانات الصحية. وأوصت الدراسة بالتركيز المستقبلي على تحسين الكفاءة الحسابية ومعالجة تحديات قابلية التوسع لتسهيل التبني الواسع في بيئات الرعاية الصحية الواقعية.

دراسة- (Masood, Daud, Wang, Banjar & Alharbey, 2024): A Blockchain-Based System for Patient Data Privacy and Security.

هدفت الدراسة إلى التعرف على التحديات المعقدة في بيئة البنية التحتية للسحابة القائمة على أجهزة الاستشعار (S-CI) بأبعاده (التحكم في الوصول، أمن البيانات، الخصوصية، قابلية التوسع، إتاحة المعلومات الصحية الشخصية) واقتراح نظام شامل قائم على البلوكتشين لتعزيز خصوصية وأمن بيانات المرضى. واستخدمت الدراسة المنهج التجريبي التطبيقي من خلال تطوير نموذج التحكم في الوصول القائم على البلوكتشين (BBACM) واختباره عبر حالة استخدام واقعية لمريض شلل. وتكونت العينة من بيانات واقعية لمريض شلل تم جمعها عبر أجهزة استشعار متصلة بالبنية السحابية. وتوصلت نتائج الدراسة إلى أن النموذج المقترح يُحقق تحسينات جوهرية في التحكم بالوصول والأمن والخصوصية وقابلية التوسع وإتاحة المعلومات الصحية الشخصية مقارنةً بالبنية التقليدية التي تعتمد على جهة موثوقة واحدة. وأوصت الدراسة بتبني نماذج البلوكتشين اللامركزية في إدارة البيانات الصحية ضمن بيئات إنترنت الأشياء الطبية لتحقيق حماية شاملة لبيانات المرضى.

دراسة (Esmaeilzadeh, 2022): Benefits and Concerns Associated with Blockchain-Based Health Information Exchange (HIE): A Qualitative Study from Physicians' Perspectives.

هدفت الدراسة إلى التعرف على الفوائد والمخاوف والعوائق المرتبطة باستخدام تقنية البلوكتشين في تبادل المعلومات الصحية بأبعاده (الميزات التقنية المبتكرة، النظام التعاوني، أداء النظام) والمخاوف بأبعاده (القضايا الفردية، التنظيمية، التقنية، السوقية) من وجهة نظر الأطباء في الولايات المتحدة. واستخدمت الدراسة المنهج النوعي القائم على النظرية المجذرة وإطار PARIHS ، وتكونت العينة من ٣٦ طبيباً من تخصصات ومؤسسات صحية متنوعة في الولايات المتحدة، حيث أجريت مقابلات شبه مهيكلة ومعمّقة عبر الإنترنت وحُلّت البيانات باستخدام برنامج NVIVO. وتوصلت نتائج الدراسة إلى تحديد سبعة محاور رئيسية: ثلاثة للفوائد تشمل الميزات التقنية المبتكرة (التشفير والتحكم بنسبة ٩٢٪)، والنظام التعاوني (التشغيل البيئي واللامركزية)، وأداء النظام (السرعة وخفض التكاليف)؛ وأربعة للمخاوف تشمل قضايا فردية (نقص المعرفة بنسبة ٨٩٪)، وقضايا تنظيمية (مشكلات التنفيذ بنسبة ٨٤٪)، وقضايا تقنية (تعقيد النظام)، وقضايا سوقية (غياب التنظيم بنسبة ٧٨٪). وأوصت الدراسة بضرورة معالجة فجوة المعرفة لدى الأطباء حول البلوكتشين، وتطوير أطر تنظيمية داعمة، وإجراء دراسات جدوى شاملة قبل تبني أنظمة تبادل المعلومات الصحية القائمة على البلوكتشين.

دراسة (Vanin, Policarpo, Righi, Heck, Silva, Goldim & da Costa, 2022): A Blockchain-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach.

هدفت الدراسة إلى التعرف على تطوير نموذج معماري لحماية السجلات الصحية الشخصية من طرف إلى طرف بأبعاده (التخزين اللامركزي عبر البلوكتشين وIPFS، التشفير المتماثل الكامل FHE ، فصل البيانات الوصفية عن البيانات الفعلية، التحكم الشخصي في الوصول) من خلال الجمع بين تقنية البلوكتشين والتشفير المتماثل الكامل. واستخدمت الدراسة المنهج التجريبي التطبيقي من خلال تطوير النموذج المعماري واختباره باستخدام قاعدة بيانات تضم ١.٣ مليون سجل لحالات كوفيد-١٩ من مراكز السيطرة على الأمراض الأمريكية (CDC) لتقييم الأداء وسعة التخزين. وتوصلت نتائج الدراسة إلى أن

الجمع بين التشفير التماثل الكامل والشبكات الموزعة يُمكنه إعادة تعريف نماذج الصحة الإلكترونية، حيث يُتيح النموذج المقترح للأفراد إدارة تشفير بياناتهم وطلبات المشاركة وتقييد الوصول لفترة محددة مسبقاً، مع دعم إجراء الحسابات على البيانات المشفرة دون الكشف عن محتواها، مما يُخفف من مخاطر الخصوصية ويُحسن التشغيل البيئي الدلالي بين المؤسسات الصحية. وأوصت الدراسة بمواصلة تطوير النموذج لتحسين كفاءة الأداء الحسابي ومعالجة تحديات التوسع في بيانات الرعاية الصحية الواقعية، مع التأكيد على أهمية الالتزام بمعايير HIPAA و GDPR.

الفجوة البحثية

من خلال الاستعراض المعمق للدراسات السابقة العربية والأجنبية ذات الصلة بموضوع الدراسة، يتّضح وجود فجوة بحثية واضحة ومتعددة الأوجه تُبرّر إجراء هذه الدراسة وتؤكد أصالتها العلمية. فعلى صعيد الدراسات العربية، يُلاحظ أن الجهود البحثية تركّزت بشكل رئيسي على تطبيقات تقنية سلاسل الكتل في قطاعات بعيدة عن المجال الصحي كالقطاع المصرفي (المزيد، ٢٠٢٤) وسلاسل التوريد الدوائية (الضعايلة وعوض، ٢٠٢٤؛ سراج، ٢٠٢٤) والمراجعة المالية (عبدالقادر، ٢٠٢٢)، بينما ظلّت الدراسات العربية التي تتناول تقاطع البلوكتشين مع مشاركة البيانات الصحية وحماية الخصوصية شحيحة للغاية واقتصرت على مقاربات نظرية عامة (العنزي والرابغي، ٢٠٢٥) أو تناولت مشاركة البيانات الصحية دون ربطها بحلول البلوكتشين (الهلال، ٢٠٢٠؛ السلمي، ٢٠٢٢). أما على صعيد الدراسات الأجنبية، فرغم ثرائها في تناول العلاقة بين البلوكتشين وأمن البيانات الصحية، إلا أن معظمها اتخذ طابعاً نظرياً مراجعياً (Adeghe et al., 2024; Yaqoob et al., 2022) أو نوعياً استكشافياً (Esmaeilzadeh, 2022) أو تقنياً بحثاً يركّز على بناء النماذج المعمارية (Vanin et al., 2022; Masood et al., 2024) دون قياس كمّي لأثر أبعاد التقنية على خفض مخاطر الخصوصية وتسرب البيانات من وجهة نظر الممارسين في الميدان الصحي. وبذلك تتبلور الفجوة البحثية في غياب دراسات تحليلية تطبيقية — لا سيما في السياق العربي والسعودي — تقيس بشكل كمّي ومتكامل أثر تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية بأبعاده الأربعة مجتمعة (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات من منظور العاملين في المؤسسات الصحية، وهو ما

تسعى الدراسة الحالية إلى سدّه من خلال تقديم إسهام بحثي أصيل يجمع بين هذه الأبعاد في إطار تحليلي تطبيقي موحد ضمن بيئة المؤسسات الصحية السعودية.

المنطلقات النظرية للدراسة

أولاً: تقنية سلاسل الكتل — (Blockchain) المفهوم والنشأة والخصائص

تُعرّف تقنية سلاسل الكتل بأنها سجل رقمي موزّع ولا مركزي يُستخدم لتسجيل المعاملات والبيانات عبر شبكة من الحواسيب المترابطة (العقد)، بحيث تُخزّن كل مجموعة من المعاملات في كتلة (Block) مُشفّرة ترتبط بالكتلة التي تسبقها بتسلسل زمني من خلال بصمة تشفيرية فريدة (Hash)، مكوّنة بذلك سلسلة متصلة غير قابلة للكسر أو التعديل بأثر رجعي. ويعود الظهور الأول لهذه التقنية إلى عام ٢٠٠٨ حين قدّمها الشخص أو المجموعة المعروفة باسم "ساتوشي ناكاموتو" بوصفها البنية التحتية لعملة البيتكوين الرقمية، إلا أن تطبيقاتها سرعان ما تجاوزت نطاق العملات المشفرة لتمتد إلى قطاعات حيوية متعددة من بينها الرعاية الصحية والمالية وسلاسل التوريد والحوكمة الإلكترونية، وذلك بفضل ما تتمتع به من خصائص جوهرية تتمحور حول اللامركزية والشفافية وعدم قابلية التعديل والأمان التشفيري (عبدالمحسن، محمد، وعبدالمجيد، ٢٠٢٣).

وتقوم تقنية سلاسل الكتل على عدة مبادئ تأسيسية تُميّزها عن أنظمة قواعد البيانات التقليدية. فمبدأ اللامركزية يعني أن البيانات لا تُخزّن في خادم مركزي واحد بل تُوزّع على شبكة واسعة من العقد المتساوية في الصلاحيات، مما يلغي وجود نقطة فشل واحدة ويُقلّل من مخاطر الاختراقات الشاملة. ومبدأ الإجماع يتطلب موافقة أغلبية العقد المشاركة في الشبكة على صحة أي معاملة قبل إضافتها إلى السلسلة، مما يمنع أي طرف منفرد من التلاعب بالبيانات. أما مبدأ عدم قابلية التعديل فيضمن أنه بمجرد تسجيل أي معاملة في كتلة والتحقق منها، يُصبح تغييرها أو حذفها شبه مستحيل من الناحية الحسابية، وهو ما يُوفّر مستوى غير مسبوق من سلامة البيانات وموثوقيتها. وتُصنّف شبكات سلاسل الكتل إلى ثلاثة أنواع رئيسية: الشبكات العامة المفتوحة لأي مشارك، والشبكات الخاصة المقتصرة على جهات محددة، والشبكات الهجينة التي تجمع خصائص النوعين وتُعدّ الأكثر ملاءمة للتطبيقات الصحية نظراً لما تُوفّره من توازن بين الشفافية والخصوصية (Yaqoob, Salah, Jayaraman & Al-Hammadi, 2022).

ثانياً: أبعاد تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية

تتبنّى هذه الدراسة أربعة أبعاد رئيسية لقياس تطبيق تقنية سلاسل الكتل في مشاركة البيانات الصحية، وفيما يلي تعريف كل بُعد وتأثيره نظرياً:

البُعد الأول — التشفير اللامركزي للبيانات: ويُقصد به توزيع البيانات الصحية المشفرة عبر شبكة لا مركزية من العقد بدلاً من تخزينها في قاعدة بيانات مركزية واحدة، بحيث تُستخدم أزواج المفاتيح التشفيرية (العامة والخاصة) لضمان أن الأطراف المخولة فقط هي من يستطيع الوصول إلى البيانات وفك تشفيرها. ويُوفّر هذا النهج حماية مزدوجة تتمثل في تشفير محتوى البيانات ذاته وتوزيع تخزينها جغرافياً وتقنياً بما يُلغي وجود هدف مركزي واحد للمهاجمين (Masood, Daud, Wang, Banjar & Alharbey, 2024).

البُعد الثاني — العقود الذكية للتحكم في الوصول: وتُعرّف بأنها برامج حاسوبية ذاتية التنفيذ تُكتب شروطها مباشرة في أسطر برمجية وتُنشر على شبكة سلاسل الكتل، بحيث تُنفذ تلقائياً عند تحقق شروط محددة مسبقاً دون الحاجة إلى تدخل بشري أو وسيط. وفي السياق الصحي، تُستخدم العقود الذكية لتحديد من يحق له الوصول إلى بيانات مريض مُعيّن ونوع البيانات المسموح بالاطلاع عليها والمدة الزمنية لهذا الوصول، مع توثيق كل عملية وصول في سجل شفاف وقابل للتدقيق. (Esmaeilzadeh, 2022)

البُعد الثالث — سلامة البيانات وعدم قابليتها للتعديل: ويُشير إلى الخاصية الجوهرية في تقنية سلاسل الكتل التي تضمن أنه بمجرد تسجيل أي سجل صحي أو معاملة بيانات في كتلة مُتحقّق منها، يُصبح تعديلها أو حذفها أو التلاعب بها مستحيلاً عملياً دون أن يتم رصد ذلك فوراً من قبل جميع العقد المشاركة في الشبكة. وتضمن هذه الخاصية حفظ مسار تدقيق كامل وشفاف لجميع التغييرات التي تطرأ على السجلات الصحية، مما يُعزّز الموثوقية والمساءلة في بيئة مشاركة البيانات (Chianumba, Ikhalea, Mustapha, Forkuo & Osamika, 2022).

البُعد الرابع — آليات إدارة الموافقة والتفويض: وتُعرّف بأنها المنظومة التقنية القائمة على سلاسل الكتل والتي تُمكن المرضى من منح أو تعديل أو سحب موافقتهم على مشاركة بياناتهم الصحية مع أطراف محددة ولأغراض معيّنة وفترات زمنية مُحدّدة مسبقاً، وذلك بشكل رقمي مُوثّق وغير قابل للإنكار. وتُعيد

هذه الآليات السيطرة الفعلية على البيانات الصحية إلى أصحابها (المرضى) بدلاً من أن تبقى حكرًا على المؤسسات الصحية، وهو ما يتوافق مع المتطلبات التنظيمية الحديثة لحماية البيانات الشخصية (Afrihyia, Chianumba, Mustapha, Forkuo & Omotayo, 2025).

ثالثاً: مخاطر الخصوصية وتسرب البيانات الصحية — المفهوم والأبعاد

تُعرّف مخاطر الخصوصية وتسرب البيانات الصحية إجرائياً في هذه الدراسة بأنها مجموعة التهديدات والاحتمالات التي تؤدي إلى كشف أو فقدان أو وصول غير مصرّح به أو استخدام غير مشروع للبيانات الصحية الشخصية للمرضى، سواء نتج ذلك عن هجمات سيبرانية خارجية أو تهديدات داخلية أو أخطاء بشرية أو ثغرات تقنية في أنظمة إدارة البيانات. وتشمل هذه المخاطر انتهاك سرية المعلومات الطبية والكشف عن هويات المرضى والتلاعب بالسجلات الصحية والوصول غير المصرّح به من قبل جهات غير مخوّلة، وهي مخاطر تتفاقم في البيئات الصحية الرقمية التي تنتم بتعدد الأطراف المشاركة في تداول البيانات. (Adeghe, Okolo & Ojeyinka, 2024)

وتتسم البيانات الصحية بخصوصية استثنائية تُميّزها عن غيرها من أنواع البيانات الشخصية، فهي تتضمن معلومات طبية وتشخيصية ونفسية وجينية ومالية ترتبط ارتباطاً وثيقاً بالهوية الأكثر حميمية للفرد، ويمكن أن يُفضي كشفها إلى تبعات جسيمة تتجاوز الضرر المادي لتطال الكرامة الإنسانية والسلامة النفسية والفرص الاجتماعية والمهنية. ولذلك فرضت التشريعات الدولية والمحلية أطراً صارمة لحماية هذه البيانات، كقانون قابلية نقل التأمين الصحي والمساءلة (HIPAA) في الولايات المتحدة، واللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، ونظام حماية البيانات الشخصية في المملكة العربية السعودية الصادر عام ٢٠٢٢. وتؤكد هذه التشريعات مجتمعة على ضرورة ضمان سرية البيانات الصحية وسلامتها وإتاحتها للأطراف المخوّلة فقط، وهي المبادئ ذاتها التي تسعى تقنية سلاسل الكتل إلى تحقيقها من خلال بنيتها اللامركزية وآلياتها التشفيرية (Handayani, Apriani, Mulyati, Zahra & Yusuf, 2023).

رابعاً: العلاقة النظرية بين تقنية سلاسل الكتل وخفض مخاطر الخصوصية وتسرب البيانات

يرتكز الأساس النظري لهذه الدراسة على فرضية مفادها أن الخصائص البنيوية لتقنية سلاسل الكتل تمتلك القدرة على معالجة نقاط الضعف الجوهرية في أنظمة إدارة البيانات الصحية التقليدية التي تُشكل المصدر الأساسي لمخاطر الخصوصية والتسرب. فالتشفير اللامركزي يُعالج مشكلة نقطة الفشل الواحدة الكامنة في البنى المركزية، والعقود الذكية تُعالج مشكلة ضعف آليات التحكم في الوصول وبطئها، وخاصية عدم قابلية التعديل تُعالج مشكلة إمكانية التلاعب بالسجلات الصحية، وآليات إدارة الموافقة تُعالج مشكلة غياب سيطرة المرضى على بياناتهم. وقد أكدت الدراسات الحديثة أن النماذج القائمة على البلوكتشين لحماية السجلات الصحية الشخصية أظهرت فاعلية ملموسة في خفض مخاطر الوصول غير المصرح به وتسرب البيانات من خلال التشفير الشامل من طرف إلى طرف وإدارة الوصول اللامركزية (Vanin et al., 2022) كما أن دمج تقنيات التشفير المتقدمة مع البنية اللامركزية للبلوكتشين يُقدّم إطاراً أمنياً متعدد الطبقات يُقلّل بشكل جوهري من احتمالات الاختراق والتسريب مقارنة بالأنظمة المركزية التقليدية (Afrihyia et al., 2025).

خامساً: مصطلحات الدراسة الإجرائية

تقنية سلاسل الكتل (Blockchain): سجل رقمي لا مركزي وموزّع يُسجّل المعاملات في كتل مُشفرة ومتراكبة زمنياً وغير قابلة للتعديل، وتُقاس في هذه الدراسة من خلال أربعة أبعاد هي التشفير اللامركزي والعقود الذكية وسلامة البيانات وإدارة الموافقة.

مشاركة البيانات الصحية: عملية تبادل البيانات الطبية والصحية بين المؤسسات الصحية والباحثين والجهات المعنية وفق بروتوكولات وسياسات محددة تهدف إلى تحسين جودة الرعاية الصحية.

مخاطر الخصوصية وتسرب البيانات: مجموعة التهديدات والاحتمالات التي تؤدي إلى كشف أو فقدان أو وصول غير مصرح به للبيانات الصحية، وتُقاس في هذه الدراسة من خلال محور أحادي مكون من عشر فقرات.

المنهجية وطرق البحث:

ستعتمد هذه الدراسة على المنهج الوصفي التحليلي باعتباره المنهج الأكثر ملاءمة لطبيعة الدراسة وأهدافها، إذ يُتيح وصف الظاهرة موضع الدراسة وصفاً دقيقاً وتحليل العلاقات بين متغيراتها تحليلاً كمياً. ويُعدّ هذا المنهج مناسباً لقياس أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده الأربعة (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات في المؤسسات الصحية بالمملكة العربية السعودية، وذلك من خلال جمع البيانات من مصادرها الأولية وتحليلها إحصائياً للوصول إلى نتائج قابلة للتعميم.

وسيتم تطبيق هذا المنهج من خلال مرحلتين أساسيتين: مرحلة نظرية تشمل مراجعة الأدبيات والدراسات السابقة العربية والأجنبية ذات الصلة بموضوع الدراسة لبناء الإطار النظري وتحديد أبعاد المتغيرات وتطوير أداة الدراسة، ومرحلة ميدانية تتضمن تصميم استبانة إلكترونية وتوزيعها على عينة الدراسة لجمع البيانات الأولية، ثم تحليلها باستخدام الأساليب الإحصائية المناسبة لاختبار فروض الدراسة والإجابة عن أسئلتها، بما يُمكن من الوصول إلى نتائج علمية دقيقة وتوصيات عملية قابلة للتطبيق.

مجتمع وعينة الدراسة

سيكون مجتمع الدراسة من جميع العاملين في مجالات تقنية المعلومات والأمن السيبراني وإدارة البيانات الصحية والسجلات الطبية الإلكترونية في المؤسسات الصحية الحكومية والخاصة بالمملكة العربية السعودية، وتحديداً في المستشفيات الكبرى ومراكز المعلومات الصحية التابعة لوزارة الصحة والمركز الوطني للمعلومات الصحية (NPHIES) ومستشفيات الشؤون الصحية بالحرس الوطني ومستشفيات القطاع الخاص الكبرى. ويُقدّر حجم مجتمع الدراسة بنحو (٤,٥٠٠) متخصص يعملون في هذه المجالات وفقاً للبيانات المتاحة من وزارة الصحة السعودية والهيئة السعودية للتخصصات الصحية، ممن يمتلكون معرفة مباشرة بأنظمة إدارة البيانات الصحية وإجراءات مشاركتها وحمايتها.

ونظراً لصعوبة حصر جميع أفراد مجتمع الدراسة والوصول إليهم، ستعتمد الدراسة على أسلوب العينة العشوائية الطبقية النسبية لضمان تمثيل متوازن لفئات المجتمع المختلفة (حسب نوع المؤسسة الصحية

وطبيعة الوظيفة والمنطقة الجغرافية). وسيتم تحديد حجم العينة وفقاً لمعادلة ستيفن ثومبسون (Steven Thompson) للمجتمعات المحدودة، حيث يُقدّر الحد الأدنى لحجم العينة بنحو (٣٥٤) مفردة عند مستوى ثقة ٩٥٪ وهامش خطأ ٥.٠٪ وستسعى الدراسة إلى توزيع (٤٢٠) استبانة لتعويض نسبة الاستبانات غير المستردة أو غير الصالحة للتحليل، بحيث يُستهدف الحصول على (٣٥٤) استبانة صالحة كحد أدنى لضمان التمثيل الإحصائي الملائم.

مصادر جمع البيانات

ستعتمد الدراسة على نوعين من مصادر جمع البيانات:

- **المصادر الثانوية:** وتشمل الكتب والمراجع العلمية المتخصصة، والدوريات والمجلات العلمية المحكمة العربية والأجنبية، والرسائل الجامعية (ماجستير ودكتوراه)، وأبحاث المؤتمرات العلمية، وقواعد البيانات الإلكترونية مثل (دار المنظومة، Scopus، Web of Science، PubMed، IEEE Xplore)، والتقارير والوثائق الرسمية الصادرة عن وزارة الصحة السعودية والمركز الوطني للمعلومات الصحية والهيئة الوطنية للأمن السيبراني. وستُستخدم هذه المصادر في بناء الإطار النظري وتحديد أبعاد المتغيرات وتطوير أداة الدراسة.
- **المصادر الأولية:** وتتمثل في الاستبانة الإلكترونية التي ستُصمم خصيصاً لهذه الدراسة وتوزع على أفراد العينة لجمع البيانات الميدانية اللازمة للإجابة عن أسئلة الدراسة واختبار فروضها.

أداة الدراسة (الاستبانة)

ستُصمم استبانة إلكترونية بوصفها الأداة الرئيسية لجمع البيانات الأولية، وستتكون من ثلاثة أقسام رئيسية:

القسم الأول: البيانات الديموغرافية

ويتضمن المتغيرات الشخصية والوظيفية لأفراد العينة (المؤهل العلمي، سنوات الخبرة، طبيعة الوظيفة، حجم المؤسسة الصحية).

القسم الثاني: المتغير المستقل — تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية

ويتكون من أربعة أبعاد تشمل (١٦) فقرة موزعة كالتالي:

البُعد	عدد الفقرات
التشفير اللامركزي للبيانات	4 فقرات
العقود الذكية للتحكم في الوصول	4 فقرات
سلامة البيانات وعدم قابليتها للتعديل	4 فقرات
آليات إدارة الموافقة والتفويض	4 فقرات
الإجمالي	16 فقرة

القسم الثالث: المتغير التابع — خفض مخاطر الخصوصية وتسرب البيانات

وهو محور أحادي يتكون من (١٠) فقرات تقيس مستوى خفض مخاطر الخصوصية وتسرب البيانات الصحية في المؤسسات الصحية.

إجمالي فقرات الاستبانة (26) فقرة، بالإضافة إلى فقرات البيانات الديموغرافية.

وسيُستخدم مقياس ليكرت الخماسي (Likert Scale) لقياس استجابات أفراد العينة، وفقاً للتدرج التالي: (موافق بشدة = ٥، موافق = ٤، محايد = ٣، غير موافق = ٢، غير موافق بشدة = ١).

الأساليب الإحصائية المستخدمة

سُحِّلَ البيانات باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS V.26) وبرنامج (SmartPLS 4) لنمذجة المعادلات البنائية، وسيتم توظيف الأساليب الإحصائية التالية:

- التحليل الوصفي: التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لوصف خصائص العينة واتجاهات الاستجابات.

- **اختبارات الصدق والثبات:** معامل ألفا كرونباخ (Cronbach's Alpha) لقياس ثبات أداة الدراسة، والصدق الظاهري (عرض الاستبانة على محكمين متخصصين)، وصدق الاتساق الداخلي (معامل ارتباط بيرسون) للتحقق من صدق البناء.
- **تحليل الانحدار المتعدد: (Multiple Regression Analysis)** لاختبار أثر أبعاد المتغير المستقل مجتمعة ومنفردة على المتغير التابع واختبار الفروض الأربعة الأولى.
- **معامل الارتباط: (Pearson Correlation)** لقياس قوة واتجاه العلاقة بين المتغيرات المستقلة والمتغير التابع.
- **معامل تضخم التباين (VIF) واختبار التباين المسموح: (Tolerance)** للتحقق من عدم وجود ازدواجية خطية بين المتغيرات المستقلة.
- **تحليل التباين الأحادي: (One-Way ANOVA)** لاختبار الفروق في استجابات أفراد العينة تبعاً للمتغيرات الديموغرافية متعددة المستويات (سنوات الخبرة، حجم المؤسسة).
- **اختبار (T-Test) للعينات المستقلة:** لاختبار الفروق في استجابات أفراد العينة تبعاً للمتغيرات الديموغرافية ثنائية المستويات.
- **اختبار شيفيه (Scheffé) للمقارنات البعدية:** لتحديد اتجاه الفروق ولصالح أي فئة في حال وجود فروق دالة إحصائية.

حدود الدراسة

- **الحدود الموضوعية:** ستقتصر الدراسة على قياس أثر تطبيق تقنية سلاسل الكتل (Blockchain) في مشاركة البيانات الصحية بأبعاده الأربعة (التشفير اللامركزي للبيانات، العقود الذكية للتحكم في الوصول، سلامة البيانات وعدم قابليتها للتعديل، آليات إدارة الموافقة والتفويض) على خفض مخاطر الخصوصية وتسرب البيانات.
- **الحدود المكانية:** ستطبق الدراسة على المؤسسات الصحية الحكومية والخاصة في المملكة العربية السعودية، وتحديدًا المستشفيات الكبرى ومراكز المعلومات الصحية في مناطق الرياض وجدة والدمام.
- **الحدود الزمانية:** ستجرى الدراسة الميدانية خلال الفصل الدراسي الثاني من العام الجامعي ١٤٤٨/١٤٤٧ هـ الموافق ٢٠٢٥/٢٠٢٦ م.

- **الحدود البشرية:** ستقتصر الدراسة على العاملين في مجالات تقنية المعلومات والأمن السيبراني وإدارة البيانات الصحية والسجلات الطبية الإلكترونية في المؤسسات الصحية المستهدفة.

المراجع:

أولاً: المراجع العربية

- العنزي، حنان عواد، و الرابعي، ريم علي محمد. (٢٠٢٥). حماية المعرفة في المدن الصحية الذكية بين مشاركة البيانات وضمان الأمن والخصوصية. المجلة العربية للنشر العلمي، ع ٨٦ ، ٢٥٤ - ٢٧٢. مسترجع من <http://search.mandumah.com/Record/1657549>
- الهلال، محمد بن ناصر. (٢٠٢٠). مشاركة البيانات الصحية بين الباحثين الحاصلين على منح برنامج دعم أبحاث كوفيد-١٩ من وزارة الصحة السعودية: دراسة وصفية. مجلة دراسات المعلومات، ع ٢٥٤ ، ١٠٠ - ١١٦. مسترجع من <http://search.mandumah.com/Record/1186328>
- السلمي، أماني عبدالقوي عبيد. (٢٠٢٢). واقع تكامل البيانات الضخمة في المركز الوطني للمعلومات الصحية بالمملكة العربية السعودية: دراسة حالة. كتاب أعمال الملتقى الافتراضي الثاني لجمعية المكتبات المتخصصة فرع الخليج العربي :مشاركة المعرفة بين المؤسسات ذات المصالح المشتركة - الفرص والتحديات والممارسات، المنامة: جمعية المكتبات المتخصصة فرع الخليج العربي، ٩ - ٢٨. مسترجع من <http://search.mandumah.com/Record/1301987>
- الفهمي، أصايل عبدالله، المالكي، ندى حمدان، و حمبشي، ناريمان خالد. (٢٠٢٥). دور تقنية سلاسل الكتل "Blockchain" في حفظ المخطوطات وإدارتها: دراسة نظرية. المؤتمر الثامن والعشرون: نحو استدامة المعرفة والحفاظ على الثقافة والتراث - إدارة الوثائق النادرة والمخطوطات والمواد التراثية في عصر التقنيات الناشئة والذكاء الاصطناعي، جدة: جمعية المكتبات المتخصصة فرع الخليج العربي، ٢٦١ - ٢٧٤. مسترجع من <http://search.mandumah.com/Record/1653494>
- الخرابشة، محمد هاشم علي، الوشاح، سليمان راجي سليمان، و أبو حمور، أيمن محمود جميل. (٢٠٢٤). الأثر المتوقع لاستخدام تقنية سلاسل الكتل في جودة التقارير المالية: دراسة ميدانية:

البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع

<http://search.mandumah.com/Record/1497736> من

- المزيّد، عبدالعزيز بن حسين متعب. (٢٠٢٤). واقع استخدام سلاسل الكتل "Block Chain" في المصارف السعودية: دراسة حالة مصرف الراجحي. المجلة العلمية للدراسات التجارية والبيئية، مج ١٥، ع ٣، ٤١٢ - ٤٤١. مسترجع من

<http://search.mandumah.com/Record/1553038>

- عبدالمحسن، محمد عبدالمعز محمد، محمد، وائل فوزي عبدالباسط، و عبدالمجيد، عيد رشاد عبدالقادر. (٢٠٢٣). التحول الرقمي باستخدام تكنولوجيا سلاسل الكتل "Blockchain": دراسة نظرية. المجلة العلمية للاقتصاد والتجارة، ع ٣، ١٩٥ - ٢١٦. مسترجع من

<http://search.mandumah.com/Record/1418060>

- الضعائيلة، معتز محمود بركات، و عوض، حسين أحمد. (٢٠٢٤). أثر استخدام تقنية سلاسل الكتل على إدارة سلاسل التوريد في شركات الصناعات الدوائية الأردنية (رسالة ماجستير غير منشورة). جامعة عمان العربية، عمان. مسترجع من

<http://search.mandumah.com/Record/1580754>

- عبداللاه، محمود محمد عبدالمعز. (٢٠٢٣). أثر تكنولوجيا سلاسل الكتل على كفاءة وفعالية الخدمات السياحية. مجلة كلية السياحة والفنادق، مج ٧، ع ١، ٢٧ - ٤٨. مسترجع من

<http://search.mandumah.com/Record/1479854>

- الزهراني، سعيد بن محمد. (٢٠٢٤). تقنية سلاسل الكتل "البلوكتشين" ومهنة المحاسبة. مجلة المحاسبة، س ٢٥، ع ٦٧، ٢٥ - ٢٦. مسترجع من

<http://search.mandumah.com/Record/1534653>

- عبدالقادر، محمد فتحي أحمد. (٢٠٢٢). أثر تطبيق تقنية سلاسل الكتل على المراجعة الخارجية. مجلة الدراسات والبحوث التجارية، س ٤٢، ع ٤، ١ - ٤٣. مسترجع من

<http://search.mandumah.com/Record/1405445>

- سراج، سامح عبدالمنعم. (٢٠٢٤). أثر استخدام تقنية سلاسل الكتل على إدارة سلاسل الإمداد لدعم الميزة التنافسية: دراسة تطبيقية على شركات الأدوية العاملة في السوق المصرية. المجلة العلمية للدراسات والبحوث المالية والتجارية، مج ٥، ع ١٤، ١٤٨٧ - ١٥٣٣. مسترجع من <http://search.mandumah.com/Record/1616726>

المراجع الأجنبية

- Adeghe, E. P., Okolo, C. A., & Ojeyinka, O. T. (2024). Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes. *Open Access Research Journal of Science and Technology*, 10(2), 013–020.
- Chianumba, E. C., Ikhalea, N., Mustapha, A. Y., Forkuo, A. Y., & Osamika, D. (2022). Integrating AI, blockchain, and big data to strengthen healthcare data security, privacy, and patient outcomes. *Journal of Frontiers in Multidisciplinary Research*, 3(1), 124–129
- Handayani, I., Apriani, D., Mulyati, M., Zahra, A. R. A., & Yusuf, N. A. (2023). Enhancing security and privacy of patient data in healthcare: A smartpls analysis of blockchain technology implementation. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 5(1), 8–17
- Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 34(14), 11475–11490.

- Afrihyia, E., Chianumba, E. C., Mustapha, A. Y., Forkuo, A. Y., & Omotayo, O. (2025). Developing privacy-preserving data sharing protocols for healthcare systems using cryptographic and blockchain-based techniques. *International Journal of Advanced Multidisciplinary Research and Studies*, 5.
- Masood, I., Daud, A., Wang, Y., Banjar, A., & Alharbey, R. (2024). A blockchain-based system for patient data privacy and security. *Multimedia Tools and Applications*, 83(21), 60443–60467
- Esmailzadeh, P. (2022). Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. *BMC Medical Informatics and Decision Making*, 22(1), 80.
- Vanin, F. N. D. S., Policarpo, L. M., Righi, R. D. R., Heck, S. M., da Silva, V. F., Goldim, J., & da Costa, C. A. (2022). A blockchain-based end-to-end data protection model for personal health records sharing: a fully homomorphic encryption approach. *Sensors*, 23(1), 14.

Mid Ocean University

College of Management

Department of risk management



**The impact of implementing governance, risk, and
compliance (GRC) digitally on improving the
effectiveness of internal control and reducing
operational risks: a field study on government
companies in Riyadh.**

Prepared by:

Barakat Shmelan Al-Azmi

Supervision:

Dr. Al-Faisal Abdelhamid Mohamed Hassan

Dr. Fayez Jarad

1447-2026