International Journal for Scientific Research (IJSR)

المجلة الدولية للبحوث العلمية

IJSR

Vol. (5), No. (10) October 2026 الإصدار (5)، العدد (10)

تكامل الحوسبة الطرفية مع البلوكشين: مراجعة شاملة للأمن وإدارة الثقة والتحكم الديناميكي بالوصول وإدارة الموارد والتطبيقات

يزن حسن حسن

طالب ماجستير، قسم هندسة الحاسبات والتحكم الآلي، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية (تشرين سابقاً)، سورية
yazan.hasan@latakia-univ.edu.sy

خلدون عدنان فاقي

مدرس، قسم هندسة الحاسبات والتحكم الآلي، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية (تشرين سابقاً)، سورية
khaldoun.faqi@latakia-univ.edu.sy

ملخص البحث

تستعرض هذه المقالة الدراسات والأبحاث المتعلقة بتكامل الحوسبة الطرفية مع تقنية البلوكشين، بهدف بيان دور هذا التكامل في تحسين الأمن والثقة واللامركزية مع الحفاظ على الأداء وانخفاض زمن الاستجابة .وتتناول المراجعة معماريات التكامل، والعقود الذكية، وإدارة الهوية والتحكم بالوصول، وإدارة الثقة، وإدارة الموارد وتفريغ المهام، إضافة إلى أبرز التطبيقات في إنترنت الأشياء والبيئات الصناعية والصحية والمدن الذكية والمركبات المتصلة. كما تناقش أهم التحديات المرتبطة بمحدودية الموارد، وزمن الإجماع، والتخزين، وقابلية التوسع، والخصوصية. وتبين المراجعة أن الاتجاهات الحديثة تتجه نحو حلول هجينة وخفيفة وقابلة للتكيف تجمع بين سرعة المعالجة عند الحافة وقدرات البلوكشين في الثقة والتدقيق، مع توظيف العقود الذكية والذكاء الاصطناعي وآليات الإجماع والتجزئة لتحسين كفاءة الأنظمة.

الكلمات المفتاحية: الحوسبة الطرفية، البلوكشين، الأمن والتحكم بالوصول وإدارة الثقة.

Blockchain–Edge Computing Integration: A Comprehensive Review of Security, Trust Management, Dynamic Access Control, Resource Management, and Applications

Yazan Hasan Hasan

Masters Student, Computer and Automatic Control Engineering, Faculty of Mechanical and Electrical Engineering, Latakia University (formerly Tishreen), Syria
yazan.hasan@latakia-univ.edu.sy

Khaldoun Adnan Faqi

Assistant Professor, Computer and Automatic Control Engineering, Faculty of Mechanical and Electrical Engineering, Latakia University (formerly Tishreen), Syria
khaldoun.faqi@latakia-univ.edu.sy

Abstract

This review examines research on the integration of Edge Computing and Blockchain, with a focus on how this integration can enhance security, trust, and decentralization while maintaining low latency and acceptable performance. The review covers integration architectures, smart contracts, identity management and access control, trust management, resource management and

task offloading, as well as major applications in the Internet of Things, industrial and healthcare environments, smart cities, and connected vehicles. It also discusses key challenges related to limited edge resources, consensus latency, storage, scalability, and privacy. The literature indicates a shift toward lightweight, adaptive, and hybrid solutions that combine the processing speed of the edge with the trust and auditability of Blockchain, supported by smart contracts, suitable consensus mechanisms, sharding, and artificial intelligence to improve system efficiency.

Keywords: Edge Computing, Blockchain, Security, Access Control, and Trust Management.

1. مقدمة حول الحوسبة الطرفية والبلوكشين

أصبحت الحوسبة الطرفية (Edge Computing) أحد الاتجاهات المهمة في تطوير البنى التحتية للحوسبة الموزعة، نتيجة الحاجة إلى معالجة البيانات بالقرب من مصادر إنتاجها وتقليل الاعتماد على مراكز البيانات السحابية البعيدة. وفي المقابل، يوفر البلوكشين (Blockchain) نموذجًا موزعًا لإدارة السجلات والمعاملات دون الاعتماد على جهة مركزية واحدة، مع توفير خصائص سلامة البيانات وقابلية التتبع والثقة اللامركزية. وقد أدى الجمع بين التقنيتين إلى ظهور نموذج Blockchain-Enabled Edge Computing الذي يهدف إلى معالجة بعض التحديات الأمنية والإدارية في البيئات الطرفية، مع الاستفادة من قدرات Edge في تقليل زمن الاستجابة. وقد تناولت الدراسات المبكرة هذا التكامل، ثم تطورت الأبحاث لاحقًا نحو الأمن، والثقة، والتحكم بالوصول، وإدارة الموارد، وقابلية التوسع. [4] [1]

1.1 مفهوم الحوسبة الطرفية وخصائصها:

تمثل الحوسبة الطرفية نموذجًا حاسوبيًا يهدف إلى نقل عمليات معالجة البيانات والخدمات الحسابية من مراكز البيانات المركزية إلى مواقع أقرب إلى المستخدمين والأجهزة ومصادر البيانات. ويأتي هذا النموذج استجابة للزيادة الكبيرة في عدد الأجهزة المتصلة وتنامي التطبيقات التي تتطلب زمن استجابة منخفضًا، مثل إنترنت الأشياء، والمركبات المتصلة، والتطبيقات الصناعية، وأنظمة المدن الذكية. وبدل إرسال جميع البيانات إلى السحابة لمعالجتها، تسمح الحوسبة الطرفية بتنفيذ جزء من عمليات المعالجة والتخزين والتحليل على عقد قريبة من الأجهزة النهائية، مما يقلل زمن الاتصال وحجم البيانات المنقولة إلى السحابة. [3], [1]

وتتميز بيئة Edge Computing بطبيعتها الموزعة، إذ تتكون عادةً من مجموعة من العقد الطرفية ذات قدرات حاسوبية وتخزينية مختلفة. وتختلف هذه العقد عن البنية السحابية التقليدية من حيث محدودية الموارد، والتوزيع الجغرافي، وتعدد الجهات التي قد تدير العقد. وقد جعلت هذه الخصائص الحوسبة الطرفية مناسبة للتطبيقات التي تتطلب استجابة سريعة ومعالجة محلية للبيانات. وفي المقابل، يؤدي التوزيع الكبير للعقد إلى ظهور تحديات تتعلق بالثقة، وأمن الاتصالات، وإدارة الهوية، وحماية البيانات، والتحكم في الموارد. [10] ,[3]

كما أن قرب العقد الطرفية من مصادر البيانات يجعلها هدفًا مهمًا للهجمات الأمنية، خاصة عندما تكون منتشرة في مواقع مختلفة وتعمل في بيئات غير متجانسة. وقد أشارت الأدبيات إلى أن غياب جهة مركزية موثوقة في بعض سيناريوهات Edge يجعل إدارة الثقة والتحقق من سلوك العقد مسألة أساسية .ولهذا ظهرت حلول تعتمد على البلوكشين لتوفير سجل موزع للعمليات وتعزيز إمكانية التحقق من الأنشطة التي تتم بين العقد. [9] ,[4]

ومن الخصائص المهمة أيضًا قابلية الحوسبة الطرفية لدعم التطبيقات ذات القيود الزمنية، حيث يمكن تنفيذ عمليات حسابية قريبة من المستخدم بدل الاعتماد الكامل على Cloud Computing. ومع ذلك، فإن محدودية موارد Edge Nodes تجعل استخدام تقنيات ثقيلة مثل Blockchain بحاجة إلى تصميمات محسنة، وخاصة فيما يتعلق بآليات الإجماع، والتخزين، وحجم المعاملات، واستهلاك الطاقة. ومن هنا نشأت الحاجة إلى تطوير نماذج تكامل تجمع بين مزايا Edge في سرعة المعالجة ومزايا Blockchain في اللامركزية والثقة وسلامة البيانات. [10] ,[3] ,[1]

2.1 مفهوم البلوكشين وآلية عمله:

البلوكشين هو تقنية دفتر أستاذ موزع تسمح بتسجيل المعاملات والعمليات بصورة مشتركة بين مجموعة من العقد دون الاعتماد بالضرورة على خادم مركزي واحد. وتُجمع المعاملات في كتل مترابطة تشفيريًا، بحيث تحتوي كل كتلة على معلومات ترتبط بالكتلة السابقة، الأمر الذي يوفر درجة مرتفعة من سلامة السجل ويجعل التلاعب بالبيانات المسجلة أكثر صعوبة: وتُعد اللامركزية، وقابلية التتبع، وسلامة السجل، والتحقق الموزع من أهم الخصائص التي جعلت Blockchain جذابًا في التطبيقات التي تتطلب بيئة موثوقة بين أطراف قد لا تثق ببعضها بصورة كاملة. [5] ,[4]

تعتمد عملية تسجيل المعاملة على مجموعة من الخطوات تبدأ بإنشاء المعاملة وإرسالها إلى شبكة البلوكشين، ثم التحقق من صلاحيتها وفق القواعد المحددة للنظام. وبعد ذلك تدخل المعاملات المقبولة في عملية إجماع يتم من خلالها الاتفاق بين العقد على الحالة الجديدة لدفتر الأستاذ. وتختلف آلية تنفيذ هذه العملية باختلاف نوع الشبكة وآلية الإجماع المستخدمة. ففي الشبكات العامة يمكن استخدام آليات مثل Proof of Work أو Proof of Stake، بينما تميل البيئات المؤسسية والطرفية إلى استخدام آليات إجماع أكثر ملاءمة للبيئات المصرح بها، مثل PBFT ومشتقاته، بسبب انخفاض زمن المعالجة مقارنة ببعض الآليات التقليدية. [8] ,[3]

ومن العناصر المهمة في Blockchain أيضًا العقود الذكية (Smart Contracts)، وهي برامج تنفذ مجموعة من القواعد أو الإجراءات تلقائيًا عند تحقق شروط معينة. وقد جعلت العقود الذكية البلوكشين أكثر ملاءمة للتطبيقات التي تتطلب اتخاذ قرارات آلية، مثل إدارة الوصول إلى البيانات، أو تسجيل عمليات تبادل الموارد، أو إدارة المعاملات بين الأجهزة الطرفية. [10],[14]

وتكتسب هذه الخصائص أهمية خاصة عند دمج Blockchain مع Edge Computing. فبيئة Edge تتكون من عدد كبير من الأجهزة والعقد التي قد تحتاج إلى تبادل البيانات أو الموارد دون وجود جهة مركزية تتحكم بجميع العمليات. ويمكن استخدام Blockchain لتسجيل العمليات المهمة والتحقق منها وتوفير سجل مشترك للأنشطة. وقد تناولت دراسات مختلفة استخدام البلوكشين في المصادقة، وإدارة الثقة، ومشاركة البيانات، وتفريغ المهام، وتخصيص الموارد ضمن البيئات الطرفية. [15], [21], [32]

ومع ذلك، فإن استخدام Blockchain في Edge لا يخلو من مشكلات، إذ تحتاج عملية الإجماع إلى تبادل رسائل بين العقد، كما يحتاج دفتر الأستاذ إلى موارد تخزين وحوسبة .لذلك فإن تطبيق البلوكشين بصورة مباشرة على عقد Edge محدودة الموارد قد يؤدي إلى زيادة زمن الاستجابة واستهلاك الموارد. ولهذا تركز الدراسات الحديثة على Blockchain خفيف، وآليات إجماع فعالة، وتقنيات مثل Sharding، بهدف تحقيق توازن بين الأمن واللامركزية والأداء. [51] ,[41] ,[35]

3.1 دوافع دمج البلوكشين مع الحوسبة الطرفية:

ينطلق دمج Blockchain مع Edge Computing من وجود مجموعة من المشكلات المشتركة التي يصعب التعامل معها بكفاءة باستخدام نموذج مركزي تقليدي. فالحوسبة الطرفية تعتمد على عدد كبير من العقد الموزعة التي قد تنتمي إلى جهات مختلفة، بينما تحتاج هذه العقد إلى مشاركة البيانات والخدمات والموارد بصورة آمنة .ويؤدي الاعتماد على جهة مركزية واحدة إلى إنشاء نقطة ثقة مركزية يمكن أن تصبح هدفًا للهجمات أو مصدرًا للاختناق في النظام. ومن هنا يوفر البلوكشين نموذجًا لامركزيًا يمكن أن يساعد في توزيع الثقة وتسجيل العمليات بين العقد. [4] [1]

أحد أهم دوافع التكامل هو تعزيز الثقة بين Edge Nodes. ففي بيئة موزعة، قد لا تكون جميع العقد معروفة أو موثوقة مسبقًا، ولذلك تحتاج العمليات المتبادلة بينها إلى آلية تسمح بتقييم الأنشطة والتحقق منها .يوفر Blockchainسجلًا غير قابل للتعديل نسبيًا للمعاملات والأحداث، ويمكن استخدامه لبناء آليات لإدارة الثقة والسمعة واكتشاف العقد التي تتصرف بصورة غير طبيعية. [34] ,[9]

كما يمثل الأمن والتحكم بالوصول دافعًا أساسيًا للتكامل. فانتشار أجهزة IoT وعقد Edge يؤدي إلى زيادة عدد نقاط الدخول المحتملة إلى النظام. ويمكن استخدام Blockchain لتسجيل عمليات المصادقة والتفويض وإدارة الهويات بصورة موزعة، بينما يمكن للعقود الذكية تنفيذ سياسات محددة تلقائيًا. وقد ظهرت بالفعل نماذج تستخدم Blockchain للمصادقة الآمنة وإدارة المفاتيح والتحكم في الوصول إلى الموارد والبيانات. [36] ,[21] ,[20]

ومن الدوافع كذلك حماية سلامة البيانات وإمكانية تتبعها. ففي التطبيقات الصناعية والصحية والطاقة، قد يكون من الضروري معرفة مصدر البيانات والتحقق من عدم تغييرها أثناء انتقالها بين الأجهزة والخوادم. ويسمح Blockchain بتسجيل عمليات البيانات بطريقة يمكن مراجعتها لاحقًا، مما يعزز قابلية التدقيق والمساءلة. [60] ,[26] ,[18]

كذلك يمكن للتكامل أن يدعم إدارة الموارد وتبادلها بين العقد الطرفية. وقد درست مجموعة من الأبحاث استخدام Blockchain في تخصيص الموارد، وتفريغ المهام، وتبادل الخدمات، وإنشاء آليات حوافز بين الأطراف [22] ,[33], [45]. وفي بعض التطبيقات، يتم الجمع بين Blockchain وتقنيات الذكاء الاصطناعي والتعلم المعزز لتحسين قرارات تخصيص الموارد وتفريغ المهام.

ومع ذلك، فإن الهدف من دمج التقنيتين ليس إضافة Blockchain إلى Edge بصورة مباشرة، وإنما تصميم تكامل يحقق توازنًا بين الأمن واللامركزية والثقة من جهة، وزمن الاستجابة واستهلاك الموارد وقابلية التوسع من جهة أخرى. ولذلك أصبحت الأبحاث تتجه نحو Blockchain خفيف، وآليات إجماع مناسبة، وهياكل تخزين موزعة، وحلول للتحكم بالوصول وإدارة الثقة تتوافق مع طبيعة .[51] ,[41] ,[35] Edge Computing.

2. معماريات دمج البلوكشين مع الحوسبة الطرفية

تتنوع معماريات دمج Blockchain مع Edge Computing وفق موقع طبقة البلوكشين وطبيعة العلاقة بين Cloud وEdge والأجهزة النهائية. وقد ظهرت نماذج مركزية، ولامركزية، وهرمية، وموزعة، بحيث يحاول كل نموذج تحقيق توازن مختلف بين الأمن والأداء وقابلية التوسع. وتبرز أهمية المعمارية لأن وضع Blockchain بالكامل على عقد Edge محدودة الموارد قد يؤدي إلى عبء حوسبي واتصالي مرتفع، بينما يؤدي وضعه بالكامل في Cloud إلى تقليل بعض مزايا اللامركزية والقرب من مصادر البيانات. لذلك اتجهت الدراسات إلى توزيع وظائف Blockchain بين مستويات الشبكة واستخدام Smart Contracts لإدارة العمليات والسياسات. [10] ,[3] ,[1]

1.2 المعمارية المركزية واللامركزية:

يمكن تصنيف معماريات Blockchain–Edge بصورة أولية إلى نماذج مركزية وأخرى لامركزية. في النموذج المركزي، توجد جهة أو خادم رئيسي مسؤول عن إدارة البيانات أو المصادقة أو اتخاذ القرارات، بينما تعمل عقد Edge كمكونات تنفيذية أو كمصادر للبيانات. يوفر هذا النموذج بساطة في الإدارة وانخفاضًا نسبيًا في تكلفة التنسيق، لكنه يحتفظ بمشكلة الاعتماد على نقطة مركزية قد تمثل نقطة فشل واحدة أو هدفًا للهجمات. ولهذا السبب بدأت الدراسات في البحث عن نماذج لامركزية يمكنها توزيع الثقة بين عدة عقد. [3] ,[1]

في النموذج اللامركزي، يتم توزيع دفتر الأستاذ ووظائف التحقق بين مجموعة من العقد، بحيث لا تعتمد صحة المعاملة على خادم واحد. ويمكن لعقد Edge المشاركة بصورة مباشرة أو غير مباشرة في عملية التحقق من المعاملات. وتوفر هذه المعمارية خصائص مهمة مثل مقاومة نقطة الفشل الواحدة، وتحسين قابلية التتبع، وتقليل الاعتماد على جهة موثوقة مركزية [4], [9]

لكن اللامركزية الكاملة ليست دائمًا الحل الأمثل لبيئة Edge. فكلما زاد عدد العقد المشاركة في الإجماع، زادت الرسائل المتبادلة بينها وزاد العبء الناتج عن عمليات التحقق والتخزين. ولذلك قد تصبح آلية Blockchain التقليدية غير مناسبة للعقد الطرفية ذات الموارد المحدودة. وتشير الدراسات إلى أهمية تصميم شبكات Blockchain مخصصة تتناسب مع خصائص Edge، سواء من خلال تقليل عدد العقد المشاركة في الإجماع أو استخدام آليات Consensus Lightweight [41] ,[35]

ومن النماذج المهمة أيضًا Blockchain-as-a-Service at the Edge، حيث يمكن وضع طبقة Blockchain في مجموعة محددة من Edge Nodes ذات قدرات أعلى، بينما تتعامل بقية الأجهزة مع هذه العقد باعتبارها طبقة ثقة موزعة. ويساعد ذلك في تخفيف العبء عن الأجهزة الطرفية محدودة الموارد، مع الحفاظ على خصائص السجل الموزع.

وقد ظهرت أيضًا معماريات تجمع بين المركزية واللامركزية فيما يعرف بالتصميمات الهجينة. ففي هذه النماذج قد تُستخدم Cloud لإدارة بعض الوظائف واسعة النطاق، بينما تُستخدم Blockchain وEdge لمعالجة العمليات الحساسة والقريبة من المستخدم. ويتيح هذا الأسلوب الاستفادة من قدرة Cloud على التخزين والحوسبة، مع الاستفادة من Edge في تقليل زمن

الاستجابة ومن Blockchain في توفير الثقة وسلامة العمليات. [32] ,[3]

وعليه، فإن اختيار المعمارية لا يعتمد فقط على مستوى اللامركزية المطلوب، بل يرتبط أيضًا بعدد Edge Nodes، ونوع التطبيق، ومتطلبات التأخير، وحجم المعاملات، وقدرات العقد، ومستوى الأمان المطلوب.

2.2 المعماريات الهرمية والموزعة لـ Blockchain–Edge:

ظهرت المعمارية الهرمية كحل للتعامل مع التحديات التي تنتج عن تطبيق Blockchain مباشرة على عدد كبير من عقد Edge. وفي هذا النموذج يتم تقسيم البنية إلى مستويات، يمكن أن تتضمن الأجهزة النهائية، وعقد Edge، وعقد Blockchain ذات القدرات الأعلى، ثم Cloud. ويسمح هذا التنظيم بتوزيع الوظائف وفق قدرات كل مستوى بدل تحميل جميع العقد الوظائف نفسها. [10][3]

في المستوى الأدنى توجد الأجهزة أو مصادر البيانات التي تنتج المعلومات وتحتاج إلى خدمات Edge قريبة. وفي المستوى التالي توجد Edge Nodes التي تقوم بمعالجة البيانات أو تنفيذ المهام. ويمكن تخصيص مجموعة من العقد الأكثر قدرة لتشغيل خدمات Blockchain والتحقق من المعاملات. أما Cloud فتستطيع توفير التخزين والمعالجة واسعة النطاق عند الحاجة. ويقلل هذا التنظيم من العبء الناتج عن تشغيل Blockchain على كل جهاز، ويحافظ في الوقت نفسه على آلية موزعة لإدارة العمليات المهمة.

وتكتسب المعمارية الهرمية أهمية خاصة في البيئات التي تحتوي على عدد كبير من الأجهزة، مثل IoT وIIoT. فإجبار كل جهاز على الاحتفاظ بنسخة كاملة من دفتر الأستاذ أو المشاركة في الإجماع قد يكون غير عملي بسبب محدودية الذاكرة والطاقة. لذلك يمكن اعتماد Edge Nodesكوسيط بين الأجهزة وشبكة Blockchain، بحيث تتم معالجة العمليات الأولية محليًا، بينما تُسجل الأحداث المهمة في Blockchain. [18] ,[10]

أما المعماريات الموزعة فتسعى إلى توزيع وظائف Blockchain وEdge على مجموعة أكبر من العقد. ويمكن أن تساهم هذه المعمارية في زيادة المرونة ومقاومة الأعطال، لكنها تحتاج إلى آليات فعالة لإدارة التنسيق والثقة. وقد تناولت الدراسات استخدام Blockchain في البيئات الموزعة لإدارة الموارد، ومشاركة البيانات، وتفريغ المهام، وإدارة الثقة. [22]

ومن الاتجاهات المهمة أيضًا استخدام Sharding لتقسيم شبكة Blockchain إلى مجموعات أصغر من العقد، بحيث لا تحتاج كل عقدة إلى معالجة جميع المعاملات. ويمكن لهذه الآلية تقليل عبء الإجماع وتحسين قابلية التوسع، وهو أمر مهم خصوصًا عندما تتوسع شبكة Edge إلى أعداد كبيرة من العقد. [51]

وعلى الرغم من فوائد التصميمات الهرمية والموزعة، فإنها تفرض تحديات إضافية تتعلق بإدارة الهوية بين المستويات، وتزامن البيانات، والثقة بين المجالات الإدارية المختلفة، وآليات اختيار العقد التي تشارك في الإجماع. ولذلك ما تزال المعمارية المناسبة تعتمد على طبيعة التطبيق ومتطلبات الأداء والأمن.

2 .3 دور العقود الذكية في بيئات الحوسبة الطرفية:

تمثل العقود الذكية إحدى أهم الآليات التي تجعل Blockchain قابلاً للاستخدام في تطبيقات Edge Computing، لأنها تسمح بتحويل القواعد والسياسات إلى منطق برمجي يمكن تنفيذه تلقائيًا داخل شبكة Blockchain. وبدل الاعتماد على جهة مركزية لتنفيذ كل عملية، يمكن للعقد الذكي التحقق من الشروط المحددة وتنفيذ الإجراء المناسب عند تحققها. ولهذا السبب أصبحت Smart Contracts مكونًا أساسيًا في عدد من معماريات Blockchain–Edge [14] ,[10]

في مجال التحكم بالوصول، يمكن استخدام العقد الذكي لتخزين أو تنفيذ سياسات تسمح لمستخدم أو جهاز بالوصول إلى مورد معين وفق مجموعة من الشروط. فعلى سبيل المثال، يمكن للعقد الذكي التحقق من هوية الجهاز، أو خصائصه، أو صلاحياته، ثم تسجيل عملية الوصول على Blockchain. ويتيح ذلك بناء آليات تفويض موزعة بدل الاعتماد على خادم مركزي واحد [20], [21], [36]

كما يمكن استخدام Smart Contracts في إدارة الموارد. فعندما يحتاج جهاز Edge إلى استخدام مورد موجود على Edge Node أخرى، يمكن للعقد الذكي إدارة الاتفاق بين الطرفين، وتسجيل عملية تخصيص المورد، وتنفيذ قواعد الحوافز أو الدفع

عند تحقق الشروط. وقد تناولت دراسات مختلفة استخدام Blockchain في أسواق الموارد وتخصيصها ضمن Mobile Computing Edge [45], [33]

وفي مجال مشاركة البيانات، يمكن للعقود الذكية تحديد من يحق له الوصول إلى البيانات، ومتى يمكنه الوصول إليها، وما العمليات المسموح بتنفيذها عليها. ويمكن تسجيل عمليات المشاركة والوصول في Blockchain بما يعزز قابلية التدقيق والمساءلة. وهذا الأمر مهم بصورة خاصة في تطبيقات IoT وIIoT التي تتبادل كميات كبيرة من البيانات بين جهات متعددة [18], [26]

ومع ذلك، فإن استخدام Smart Contracts في Edge Computing يواجه تحديات. فتنفيذ العقد الذكي وإجراء معاملات Blockchain يضيفان زمنًا واستهلاكًا للموارد، كما أن وجود خطأ في منطق العقد قد يؤدي إلى تنفيذ سياسة غير صحيحة بصورة تلقائية. كما أن تخزين البيانات الكبيرة مباشرة داخل Blockchain غير مناسب غالبًا بسبب القيود المرتبطة بالحجم والتكلفة. ولذلك تميل التصميمات العملية إلى تخزين البيانات خارج السلسلة Off-chain مع تسجيل بصماتها أو معلوماتها الوصفية على Blockchain.

ومن هنا أصبحت العقود الذكية عنصرًا وسيطًا بين Blockchain وEdge Services، حيث يمكن استخدامها في المصادقة، والتحكم بالوصول، وإدارة الموارد، ومشاركة البيانات، وتسجيل العمليات. إلا أن تصميمها يجب أن يأخذ في الاعتبار محدودية الموارد، وزمن الاستجابة، وقابلية التوسع، والأمن البرمجي.

3. الأمن والخصوصية في الحوسبة الطرفية المعتمدة على البلوكشين

تُعد حماية الأمن والخصوصية من أهم دوافع دمج Blockchain مع Edge Computing، إذ يؤدي انتشار Edge Nodes وأجهزة IoT إلى زيادة عدد نقاط الدخول المحتملة إلى النظام. وتواجه هذه البيئات تهديدات تتعلق بانتحال الهوية، والتلاعب بالبيانات، والوصول غير المصرح به، والعقد الخبيثة. ويمكن للبلوكشين أن يقدم طبقة ثقة موزعة من خلال السجل غير القابل للتعديل نسبيًا، والتوثيق الموزع، والعقود الذكية .ومع ذلك، فإن Blockchain لا يحل جميع المشكلات الأمنية تلقائيًا، بل يضيف بدوره تحديات تتعلق بالخصوصية، والإجماع، وإدارة المفاتيح، وحجم البيانات. [20] ,[5] ,[4]

1.3 التهديدات والهجمات الأمنية في Edge Computing:

تتميز بيئة Edge Computing بعدد كبير من الأجهزة والعقد الموزعة جغرافيًا، مما يجعل سطح الهجوم أكبر من بعض البنى المركزية التقليدية. ويمكن أن تكون Edge Nodes موجودة في مواقع لا تخضع جميعها لإدارة جهة واحدة، وقد تختلف مستويات الحماية الفيزيائية والبرمجية بينها. ولذلك يمكن أن تستهدف الهجمات أجهزة المستخدم، أو Edge Nodes، أو قنوات الاتصال، أو آليات إدارة الخدمات. وقد أشارت الأدبيات إلى أن غياب الثقة الكاملة بين العقد يمثل أحد التحديات الرئيسية أمام بناء بيئة Edge آمنة. [4] ,[3]

من التهديدات المهمة هجمات انتحال الهوية، حيث يحاول مهاجم تقديم نفسه باعتباره جهازًا أو مستخدمًا شرعيًا. وتزداد خطورة هذا النوع من الهجمات مع ارتفاع عدد أجهزة IoT المتصلة بعقد Edge. ولهذا ركزت بعض الدراسات على Blockchain-based Authentication بهدف توزيع عملية التحقق وتسجيل الأحداث المتعلقة بالهوية. [21] ,[20]

كما تمثل العقد الخبيثة مشكلة أخرى، إذ يمكن لعقدة Edge أن تتصرف بصورة غير صحيحة أو تحاول تقديم بيانات مزيفة أو تعطيل العمليات. وفي بيئة مركزية يمكن للجهة الإدارية اكتشاف العقدة وعزلها، بينما تحتاج البيئة الموزعة إلى آليات ثقة ومراقبة أكثر تعقيدًا. وقد استخدمت بعض الحلول Blockchain لتسجيل سلوك العقد وبناء نماذج ثقة أو سمعة يمكن استخدامها في اتخاذ القرار. [37] ,[34] ,[9]

ومن التهديدات كذلك التلاعب بالبيانات أثناء انتقالها بين الأجهزة وEdge Nodes أو بين Edge وCloud. ويمكن أن يؤدي تغيير البيانات إلى قرارات خاطئة في التطبيقات الصناعية أو الصحية أو أنظمة الطاقة. وهنا يمكن استخدام Blockchain لتسجيل Hash للبيانات أو العمليات المهمة، مما يسمح بالتحقق لاحقًا من سلامة البيانات. [26] ,[18]

كما يجب مراعاة هجمات Denial-of-Service، والهجمات التي تستهدف آليات الإجماع، وسرقة المفاتيح الخاصة، وتسريب معلومات المعاملات. ولا يعني استخدام Blockchain أن النظام يصبح محصنًا ضد هذه الهجمات؛ فالبلوكشين نفسه يحتاج

إلى حماية للعقد والمفاتيح وآليات الإجماع.

وبالتالي، فإن التحدي الأساسي هو تصميم طبقة أمنية متعددة المستويات تجمع بين التشفير، والمصادقة، والتحكم بالوصول، وإدارة الثقة، وBlockchain، مع مراعاة محدودية موارد Edge.

2.3 آليات حماية الخصوصية وسلامة البيانات باستخدام Blockchain:

تُعد الخصوصية وسلامة البيانات من الجوانب الأساسية في بيئات Edge Computing، خصوصًا عندما تتعامل الشبكة مع بيانات شخصية أو صناعية أو حساسة. وتكمن أهمية Blockchain في أنه يسمح بتسجيل العمليات بطريقة موزعة وقابلة للتدقيق، مما يقلل الحاجة إلى الاعتماد على سجل مركزي واحد. ويمكن استخدام Hashing لتوفير وسيلة للتحقق من سلامة البيانات، بحيث يتم تسجيل البصمة الرقمية للبيانات على Blockchain، ثم مقارنتها لاحقًا بالبصمة الناتجة من البيانات الحالية [18] ,[4] وتساعد هذه الآلية على اكتشاف التغيير غير المصرح به، لكنها لا تعني بالضرورة أن البيانات نفسها يجب تخزينها داخل Blockchain. وفي الواقع، يمثل تخزين البيانات الكبيرة مباشرة على Blockchain مشكلة بسبب محدودية حجم الكتل وكلفة التخزين والتكرار بين العقد. لذلك تستخدم العديد من التصميمات مفهوم Off-chain Storage، بحيث يتم الاحتفاظ بالبيانات خارج السلسلة، بينما يتم تخزين Hash أو مؤشر أو سجل للبيانات على Blockchain [51] ,[26]

أما من ناحية الخصوصية، فإن الشفافية التي يوفرها Blockchain قد تتحول إلى تحدٍ إذا كانت المعاملات تحتوي على معلومات تكشف هوية المستخدم أو سلوكه. ولذلك تحتاج الأنظمة إلى تقنيات مثل إخفاء الهوية، والتشفير، وإدارة المفاتيح، والتحكم الدقيق فيمن يمكنه الوصول إلى السجلات. وقد تناولت بعض الدراسات نماذج Blockchain-based Anonymous Authentication لحماية هوية الأجهزة والمستخدمين مع الحفاظ على إمكانية التحقق من صحة العمليات.

كما يمكن استخدام Blockchain لدعم Data Provenance، أي تتبع مصدر البيانات والعمليات التي مرت بها. وهذه الخاصية مفيدة في التطبيقات الصناعية والرعاية الصحية والمدن الذكية، حيث قد تحتاج الجهة المستفيدة إلى معرفة مصدر البيانات والتحقق من عدم تغييرها. ويمكن تسجيل الأحداث المهمة على دفتر الأستاذ بطريقة تسمح بمراجعتها لاحقًا [18, 60]

ومن الاتجاهات المهمة أيضًا الجمع بين Blockchain وتقنيات التشفير أو آليات مشاركة البيانات ذات التحكم الدقيق. ويمكن للعقود الذكية أن تحدد شروط الوصول، بينما يستخدم Blockchain لتسجيل عملية منح الصلاحية أو سحبها. ويساعد ذلك على الجمع بين Data Integrity وAccess Control وAuditability.

لكن استخدام Blockchain لا يضمن الخصوصية بصورة تلقائية؛ فالشفافية وقابلية التتبع قد تؤديان إلى تسريب معلومات وصفية حتى عندما تكون البيانات نفسها مشفرة. ولذلك تتجه الأبحاث إلى نماذج تجمع Blockchain مع Privacy-Preserving Techniques، وOff-chain Storage، وFine-Grained Access Control، بحيث يتم تحقيق التوازن بين قابلية التدقيق وحماية خصوصية المستخدم.

3.3 التوثيق والتشفير وحماية الاتصالات:

يمثل التوثيق (Authentication) الخطوة الأولى في حماية بيئة Edge Computing، إذ يجب التأكد من أن الجهاز أو المستخدم الذي يطلب خدمة هو بالفعل الطرف الذي يدعيه. وتزداد أهمية هذه العملية في البيئات التي تحتوي على أعداد كبيرة من أجهزة IoT وعقد Edge، حيث يمكن أن يؤدي ضعف آليات الهوية إلى وصول مهاجمين إلى الموارد والخدمات. وقد اقترحت عدة دراسات استخدام Blockchain لتوفير آليات توثيق موزعة تقلل الاعتماد على خادم مركزي. [21] ,[20]

يمكن استخدام Blockchain كسجل موثوق لمعلومات الهوية أو عمليات المصادقة، بينما يتم تنفيذ العمليات التشفيرية خارج السلسلة عند الحاجة. ويتيح ذلك تسجيل نتائج التوثيق دون الحاجة إلى تخزين جميع المعلومات الحساسة بصورة مكشوفة. كما يمكن استخدام Smart Contracts لتطبيق قواعد التحقق من الهوية وإدارة صلاحيات المستخدمين والأجهزة. [36] ,[14]

أما إدارة المفاتيح فتعد عنصرًا أساسيًا في هذه الأنظمة. فالاتصالات المشفرة تعتمد على امتلاك الأطراف مفاتيح صحيحة وآمنة، بينما يمثل فقدان المفتاح أو سرقته خطرًا كبيرًا. ويمكن استخدام Blockchain للمساعدة في إدارة سجلات المفاتيح أو شهادات الهوية بصورة موزعة، مع الاعتماد على تقنيات تشفير مناسبة لحماية المفاتيح نفسها. وقد تناولت بعض الدراسات

Blockchain-Based Anonymous Authentication with Key Management في سياقات Edge و Smart Grid [20].

وبالنسبة لحماية الاتصالات، يجب استخدام قنوات مشفرة بين الأجهزة وEdge Nodes وبين Edge وCloud لمنع التنصت والتعديل أثناء النقل. ويمكن الجمع بين التشفير التقليدي وBlockchain بحيث تتولى تقنيات التشفير حماية محتوى الاتصال، بينما يوفر Blockchain سجلًا موثوقًا لعمليات المصادقة والتعاملات. وهذا الفصل بين Confidentiality وIntegrity/Auditability مهم لتجنب تحميل Blockchain وظائف لا تناسب طبيعتها.

كما يمكن استخدام Blockchain لدعم اكتشاف السلوك غير الطبيعي للعقد. فعند تسجيل عمليات العقد ومقارنتها بسلوك متوقع، يمكن بناء آليات ثقة تساعد في اكتشاف العقد التي تحاول إرسال معاملات مشبوهة أو تنفيذ عمليات غير مصرح بها [9], [34]

ومع ذلك، يجب مراعاة أن عملية التوثيق المعتمدة على Blockchain قد تزيد زمن الاستجابة إذا تطلبت كل عملية مصادقة تنفيذ معاملة وإجراء إجماع. لذلك تتجه الحلول العملية إلى تقليل العمليات المسجلة على السلسلة، واستخدام آليات Cache أو Tokens أو شهادات مؤقتة، مع إبقاء العمليات الحساسة فقط على Blockchain.

وبذلك يمكن النظر إلى الأمن في Blockchain–Edge باعتباره طبقات متكاملة: التشفير يوفر سرية الاتصال، والتوثيق يثبت هوية الطرف، والتحكم بالوصول يحدد ما يستطيع الطرف تنفيذه، بينما يوفر Blockchain سجلًا موزعًا للثقة والتدقيق.

4. إدارة الهوية والتحكم بالوصول اللامركزي

تمثل إدارة الهوية والتحكم بالوصول أحد أهم المكونات الأمنية في بيئات الحوسبة الطرفية، نظرًا لتعدد الأجهزة والمستخدمين والعقد والخدمات التي تتفاعل ضمن بيئة موزعة. ويؤدي الاعتماد على نماذج مركزية إلى زيادة مخاطر نقطة الفشل الواحدة وصعوبة إدارة الصلاحيات في البيئات متعددة المجالات. لذلك برز Blockchain كوسيلة لدعم إدارة الهوية والتوثيق اللامركزي وتسجيل عمليات الوصول بصورة قابلة للتدقيق. كما تسمح العقود الذكية بتنفيذ سياسات التحكم بالوصول بصورة آلية، بينما توفر نماذج مثل ABAC قدرة أكبر على التعامل مع البيئات الديناميكية مقارنة بالنماذج الثابتة. وقد تناولت الدراسات [20] و[21] و[32] و[37] هذه الجوانب من خلال حلول للتوثيق، وإدارة الثقة، والتحكم الدقيق بالوصول.

1.4 إدارة الهوية والتوثيق اللامركزي:

تُعد إدارة الهوية من المتطلبات الأساسية لضمان أمن الحوسبة الطرفية، إذ يجب على النظام التحقق من هوية المستخدمين والأجهزة وعقد Edge قبل السماح لهم بالوصول إلى الخدمات أو الموارد. وتزداد هذه الحاجة في البيئات التي تحتوي على عدد كبير من أجهزة IoT التي تتصل بعقد طرفية متعددة، وقد تنتمي هذه الأجهزة إلى جهات إدارية مختلفة. ويؤدي استخدام خادم مركزي لإدارة جميع الهويات إلى إنشاء نقطة فشل واحدة، إضافة إلى إمكانية ظهور اختناقات في الأداء عندما يزداد عدد طلبات التوثيق. [21], [20]

وقد اقترحت دراسة Blockchain-Based Anonymous Authentication With Key Management for Smart Grid Edge Computing Infrastructure استخدام Blockchain لدعم التوثيق المتبادل وإدارة المفاتيح في بنية Edge للحوسبة الخاصة بالشبكات الذكية. وتقدم الدراسة بروتوكولًا يسمح بالتوثيق المتبادل مع دعم إخفاء الهوية المشروط وإدارة المفاتيح، مع التركيز على تحقيق مستوى أمني مناسب دون الاعتماد على آليات تشفير معقدة بصورة مفرطة [20]. وتوضح هذه الدراسة أهمية Blockchain في تحويل عملية إدارة الهوية من نموذج يعتمد على جهة مركزية إلى نموذج أكثر توزيعًا.

وفي السياق نفسه، قدمت دراسة Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System نظام توثيق موزعًا وموثوقًا يعتمد على Blockchain وEdge Computing. ويهدف النموذج إلى معالجة مشكلة تشتت المعلومات بين منصات IoT المختلفة، وإنشاء نظام وصول موثوق يسمح بالمصادقة والمشاركة الآمنة [21]. ويعكس ذلك تحول Blockchain من مجرد وسيلة لتخزين المعاملات إلى طبقة ثقة يمكن استخدامها للتحقق من هوية الأطراف.

كما تناولت دراسة Blockchain Empowered Cooperative Authentication With Data Traceability in

Vehicular Edge Computing مشكلة التوثيق في البيئات المركبية، حيث تتغير مواقع المركبات بسرعة وتتفاعل مع عقد Edge عبر قنوات لاسلكية. وركزت الدراسة على التوثيق التعاوني وإمكانية تتبع البيانات، مما يوضح أهمية تطوير نماذج هوية تتلاءم مع الطبيعة الديناميكية لـ Vehicular Edge Computing [19]

وتقدم دراسة A Blockchain-Based Trusted Edge Platform in Edge Computing Environment مثالًا تطبيقيًا أكثر شمولًا؛ فقد استخدمت Hyperledger Fabric ضمن منصة Edge موثوقة، ودمجت مجموعة من الخدمات الأمنية القائمة على التوثيق. وأظهرت التجارب إمكانية استخدام المنصة لتنفيذ المصادقة والتحكم بسياسات الوصول في الزمن الحقيقي، مع توفير آلية قابلة للتوسع نسبيًا. [32]

ومن خلال هذه الدراسات يمكن ملاحظة أن إدارة الهوية في Blockchain–Edge تتجه نحو ثلاثة مستويات مترابطة: تحديد هوية الطرف، والتحقق من الهوية، وإدارة دورة حياة الصلاحية. إلا أن التحدي يتمثل في تحقيق ذلك مع الحفاظ على انخفاض زمن الاستجابة. فإذا أصبحت كل عملية توثيق معاملة Blockchain مستقلة، فقد يؤدي الإجماع إلى تأخير غير مناسب للتطبيقات الزمنية الحساسة. ولذلك تميل الحلول الحديثة إلى استخدام Blockchain لتخزين أو التحقق من معلومات الهوية والأحداث الحساسة، مع تنفيذ بعض عمليات التحقق محليًا على Edge.

كما أن إدارة الهوية اللامركزية تحتاج إلى معالجة مشكلة إدارة المفاتيح، وإلغاء الهويات، وتحديث بيانات المستخدمين، والتعامل مع الأجهزة التي تنضم إلى الشبكة أو تغادرها. ولذلك فإن بناء نظام هوية فعال يجب ألا يقتصر على استخدام Blockchain، بل ينبغي أن يجمع بين التشفير، وإدارة المفاتيح، والعقود الذكية، وسياسات الوصول الديناميكية.

2.4 نماذج التحكم بالوصول: RBAC وABAC والنماذج القائمة على القدرات:

يمثل التحكم بالوصول الآلية التي تحدد ما إذا كان المستخدم أو الجهاز يستطيع الوصول إلى مورد أو خدمة معينة، وما العمليات التي يسمح له بتنفيذها. وفي البيئات التقليدية يمكن استخدام نماذج مثل Role-Based Access Control (RBAC)، حيث يتم منح الصلاحيات بناءً على أدوار محددة. وعلى الرغم من بساطة RBAC وسهولة إدارته، فإن ملاءمته تقل في البيئات الطرفية الديناميكية التي تتغير فيها خصائص المستخدمين والأجهزة والموارد باستمرار.

في نموذج RBAC، يتم ربط المستخدمين بالأدوار، ثم ربط الأدوار بمجموعة من الصلاحيات. ويمكن أن يكون هذا النموذج فعالًا في المؤسسات ذات الهيكل الإداري الواضح، لكنه يصبح أقل مرونة عندما يحتاج النظام إلى اتخاذ قرار وصول يعتمد على مجموعة من الخصائص المتغيرة. فمثلًا، قد يعتمد القرار في بيئة Edge على نوع الجهاز، وموقعه، وحالة الشبكة، ووقت الطلب، ومستوى الثقة، وحساسية البيانات، وليس فقط على دور المستخدم.

ولهذا السبب يُعد Attribute-Based Access Control (ABAC) أكثر ملاءمة للبيئات الديناميكية. ففي ABAC يتم اتخاذ قرار الوصول بناءً على مجموعة من السمات المرتبطة بالمستخدم أو الجهاز أو المورد أو البيئة، إضافة إلى السياسة التي تحدد العلاقة بينها. ويمكن أن يسمح ذلك ببناء سياسات دقيقة مثل: السماح لجهاز يمتلك خصائص محددة بالوصول إلى مورد معين عندما يكون مستوى الثقة أعلى من قيمة معينة وعندما يكون الجهاز ضمن نطاق شبكة محددة.

وقد ظهرت حلول Blockchain-based Fine-Grained Access Control لمعالجة هذا النوع من المتطلبات. ومن الأمثلة المهمة دراسة BDSS-FA التي اقترحت منصة لمشاركة البيانات تعتمد على Blockchain والتحكم الدقيق بالوصول، مع استخدام بنية Attribute-Based Encryption هرمية وتوزيع الخصائص بين مراكز تفويض متعددة. وتوضح الدراسة أن الجمع بين Blockchain والتشفير القائم على السمات يمكن أن يوفر تحكمًا مرنًا ودقيقًا في مشاركة البيانات. [27]

كما قدمت أعمال أخرى آليات تحكم بالوصول لبيئات IoT وFog Computing تعتمد على Blockchain، حيث يستخدم السجل الموزع لتخزين أو إدارة سياسات الوصول بدل الاعتماد على خادم مركزي. ويتميز هذا الأسلوب بإمكانية تتبع عمليات منح الصلاحيات وسحبها، بالإضافة إلى تقليل مخاطر نقطة الفشل الواحدة.

أما Capability-Based Access Control فيعتمد على منح الطرف المصرح له قدرة أو رمزًا يحدد المورد والعمليات التي يمكن تنفيذها. ويعد هذا النموذج مناسبًا للأجهزة الطرفية لأن الصلاحية يمكن أن تكون محددة ومحدودة زمنيًا أو وظيفيًا.

ويمكن استخدام Blockchain لتسجيل إصدار القدرات والتحقق منها، بينما يمكن للعقد الذكي إدارة دورة حياتها.

وعند مقارنة هذه النماذج، يمكن القول إن RBAC يتميز بالبساطة، بينما يوفر ABAC مرونة أكبر، في حين توفر النماذج القائمة على القدرات إمكانية التحكم الدقيق في الصلاحيات الممنوحة. ولذلك فإن الاتجاه البحثي الأكثر ملاءمة للبيئات الطرفية هو استخدام نموذج هجين يجمع ABAC + Blockchain + Smart Contracts، بحيث تستخدم السمات لاتخاذ القرار، وتستخدم Blockchain لتوفير الثقة والتدقيق، بينما تقوم Smart Contracts بتنفيذ السياسات بصورة موزعة.

وتشير هذه الدراسات إلى وجود فجوة مهمة تتمثل في كيفية تنفيذ سياسات ABAC المعقدة دون التأثير الكبير في زمن الاستجابة. فكلما زادت السمات والسياسات زادت عمليات التحقق، بينما تؤدي إضافة Blockchain إلى تكلفة إجماع وتخزين. وبالتالي فإن تصميم Access Control فعال في Edge يحتاج إلى توزيع ذكي للسياسات بين Edge وBlockchain.

3.4 العقود الذكية لتنفيذ سياسات التحكم بالوصول:

تُعد العقود الذكية من أهم الآليات التي يمكن استخدامها لتنفيذ سياسات التحكم بالوصول في بيئات Blockchain–Edge، لأنها تسمح بتحويل قواعد الوصول إلى منطق برمجي يتم تنفيذه بصورة تلقائية عند تحقق شروط محددة. وبدل أن يعتمد النظام على خادم مركزي لاتخاذ قرار التفويض، يمكن للعقد الذكي تنفيذ السياسة والتحقق من شروط الوصول وتسجيل النتيجة على Blockchain.

في نموذج تقليدي للتحكم بالوصول، يتم إرسال طلب المستخدم إلى خادم مركزي، ثم يقوم الخادم بالتحقق من الهوية والصلاحيات وإرجاع قرار السماح أو الرفض. ويؤدي هذا النموذج إلى الاعتماد على نقطة مركزية، كما يمكن أن يسبب اختناقًا عندما يرتفع عدد الطلبات. أما عند استخدام Smart Contracts، فيمكن توزيع منطق التفويض على شبكة Blockchain بحيث يصبح القرار قابلًا للتحقق والتدقيق.

وتوضح دراسة A Blockchain-Based Trusted Edge Platform in Edge Computing Environment إمكانية استخدام Blockchain مع خدمات توثيق وتحكم بالوصول في منصة Edge. وقد اعتمدت الدراسة على Hyperledger Fabric، وبيّنت أن المنصة تستطيع تنفيذ آليات المصادقة والتحكم في سياسات الوصول بصورة مناسبة للبيئة الطرفية. [32]

كما يمكن للعقود الذكية أن تكون مناسبة لتطبيق ABAC، إذ يمكن تخزين أو تمثيل قواعد السياسة بصورة برمجية. فعند وصول طلب من جهاز معين، يمكن للعقد الذكي التحقق من سمات الجهاز والمستخدم والمورد والبيئة، ثم تطبيق السياسة المحددة. ويسمح ذلك بتنفيذ سياسات دقيقة دون الحاجة إلى تدخل بشري في كل عملية.

وفي نموذج مشاركة الموارد، يمكن أيضًا استخدام Smart Contracts لإدارة العلاقة بين الأطراف. فقد أوضحت دراسة Resource Sharing of Mobile Edge Computing Networks Based on Auction Game and Blockchain أن Blockchain يمكن أن يعمل كجسر بين Edge Clouds، مع استخدام العقود الذكية لبث متطلبات الموارد وتسجيل معاملات المشاركة. وهذا يوضح أن Smart Contracts يمكن أن تتجاوز التحكم في البيانات لتصبح آلية لإدارة العمليات والتفاعلات بين الأطراف. [33]

وتبرز أهمية العقود الذكية أيضًا في إمكانية تسجيل عمليات الوصول. فعند منح صلاحية أو رفض طلب، يمكن تسجيل العملية بصورة تجعلها قابلة للمراجعة لاحقًا. ويساعد ذلك في التطبيقات التي تحتاج إلى Audit Trail، مثل الرعاية الصحية والأنظمة الصناعية.

لكن العقود الذكية تواجه عدة قيود. أولها أن تنفيذ كل طلب وصول كمعاملة Blockchain قد يزيد زمن الاستجابة. وثانيها أن البيانات الحساسة لا ينبغي تخزينها بصورة مباشرة على السلسلة. وثالثها أن أي خطأ في منطق العقد الذكي قد يؤدي إلى تطبيق سياسة غير صحيحة بصورة آلية.

لذلك، فإن أفضل تصميم لا يعتمد على Smart Contract لتنفيذ كل العمليات، وإنما يستخدمه لإدارة السياسات الحساسة، وإصدار الصلاحيات، وتسجيل الأحداث المهمة، بينما تنفذ عمليات التحقق السريعة محليًا في Edge. ويمكن أيضًا استخدام Off-chain Storage للبيانات، مع تسجيل Hash أو معرفات العمليات على Blockchain.

5. إدارة الثقة والموثوقية في شبكات الحوسبة الطرفية

تُعد الثقة من أهم المشكلات في شبكات Edge الموزعة، لأن الأجهزة والعقد قد تتبع جهات إدارية مختلفة ولا يمكن افتراض موثوقيتها مسبقًا. وتساعد Blockchain في بناء طبقة ثقة موزعة من خلال تسجيل العمليات وإتاحة التحقق منها، بينما تسمح آليات السمعة وتقييم السلوك باكتشاف العقد غير الموثوقة. وقد تناولت الدراسات [9] و[32] و[34] و[37] هذا الاتجاه من خلال نماذج مختلفة لبناء الثقة، وتقييم مساهمة العقد، وإدارة السلوك. وتوضح هذه الأعمال أن الثقة في Blockchain–Edge لا تعتمد فقط على سلامة السجل، بل تتطلب آليات لتقييم العقد نفسها وربط سلوكها بالقرارات الأمنية.

1.5 نماذج بناء وتقييم الثقة بين عقد Edge:

تنشأ مشكلة الثقة في Edge Computing نتيجة الطبيعة الموزعة والمتغيرة للشبكة. فعندما يتعامل جهاز مع Edge Node جديدة، قد لا يمتلك معلومات كافية عن مدى موثوقيتها أو جودة الخدمات التي تقدمها. ويمكن أن يؤدي اختيار عقدة غير موثوقة إلى تسريب البيانات أو تنفيذ مهام بصورة غير صحيحة. ولذلك تحتاج الأنظمة إلى آلية لتقدير مستوى الثقة قبل السماح للعقد بالتعاون.

يمكن بناء الثقة باستخدام مجموعة من المؤشرات، مثل سجل العمليات السابقة، ونسبة نجاح تنفيذ المهام، وزمن الاستجابة، وصحة البيانات المقدمة، وسلوك العقدة تجاه بقية الأطراف .ويمكن دمج هذه المؤشرات في قيمة ثقة تستخدم لاتخاذ قرار بشأن قبول العقدة أو تخصيص موارد لها.

تقدم دراسة Resource Allocation and Trust Computing for Blockchain-Enabled Edge Computing System نموذجًا يجمع بين إدارة الموارد وحساب الثقة. وتركز الدراسة على استخدام استراتيجية تعتمد على تقييم الثقة وترتيب المهام، بهدف تحقيق معالجة أكثر كفاءة وموثوقية. وتشير نتائجها إلى أن دمج حساب الثقة مع إدارة الموارد يمكن أن يحسن الكفاءة والموثوقية [34] كما يقدم A Blockchain-Based Trusted Edge Platform مثالًا على استخدام Blockchain لتوفير طبقة موثوقة في Edge. فالمنصة تعتمد على شبكة Hyperledger Fabric متعددة العقد، وتوفر خدمات أمنية للتوثيق والتحكم بالوصول، مما يجعل Blockchain جزءًا من بنية الثقة وليس مجرد مخزن بياناً.

أما دراسة Towards Trustworthy IoT فتقدم نموذجًا أكثر وضوحًا لربط الثقة بالسلوك. فقد اقترحت Proof-of-Contribution، وهي آلية تهدف إلى تنظيم سلوك العقد، خاصة فيما يتعلق بسلوك أجهزة IoT، مع دمج التحكم بالوصول وحماية الخصوصية. وتم تنفيذ النموذج باستخدام Ethereum والعقود الذكية، وأظهرت الدراسة إمكانية استخدام الآلية لاكتشاف وإدارة السلوكيات غير المرغوبة. [37]

وتكمن أهمية Blockchain هنا في توفير سجل موزع لعمليات العقد، بحيث لا تستطيع جهة واحدة تعديل تاريخ السلوك بصورة منفردة .وهذا يسمح باستخدام سجل المعاملات كمصدر لتقييم الثقة.

ومع ذلك، فإن Blockchain لا يستطيع وحده تحديد ما إذا كانت العقدة موثوقة؛ فهو يستطيع ضمان سلامة السجل، لكنه يحتاج إلى خوارزمية أو نموذج ثقة لتحليل السلوك. وبالتالي يمكن الجمع بين Blockchain وخوارزميات الذكاء الاصطناعي أو التعلم الآلي لبناء Trust Scores ديناميكية.

ومن الاتجاهات المهمة مستقبلًا استخدام Context-Aware Trust، بحيث لا تكون الثقة قيمة ثابتة، بل تتغير وفق التطبيق، والموقع، وحالة الشبكة، ونوع المهمة .وهذا مناسب جدًا لـ Edge Computing، حيث تتغير ظروف الشبكة والعقد بصورة مستمرة.

2.5 إدارة السمعة واكتشاف العقد الخبيثة:

تختلف إدارة السمعة عن التوثيق؛ فالتوثيق يجيب عن سؤال "من هو الطرف؟"، بينما تجيب السمعة عن سؤال "هل يمكن الوثوق بهذا الطرف بناءً على سلوكه السابق؟ "وتكتسب هذه المسألة أهمية كبيرة في شبكات Edge، حيث يمكن أن تكون العقد صحيحة من ناحية الهوية لكنها تتصرف بصورة خبيثة أو تقدم خدمات منخفضة الجودة.

يمكن بناء نظام سمعة من خلال جمع تقييمات العقد أو تسجيل سلوكها في Blockchain. فعلى سبيل المثال، يمكن تسجيل

نجاح تنفيذ المهام، ودقة البيانات، وعدد محاولات الوصول غير المصرح بها، ومعدل الاستجابة. ثم تستخدم هذه المعلومات لتكوين Reputation Score.

يمثل TrustChain مثالًا مهمًا على هذا الاتجاه. فقد صمم Jayasinghe وزملاؤه Blockchain يحاول معالجة مشكلات الخصوصية والثقة في بيئات IoT، مع الاستفادة من Edge Computing لتقليل التأخير واستهلاك الموارد المرتبطين بالمعالجة المركزية. كما يناقش العمل مشكلة أن Blockchain التقليدي قد يؤدي إلى استهلاك مرتفع للطاقة وقد يكشف معلومات بسبب طبيعة السجل العام. [9]

وتقدم دراسة Towards Trustworthy IoT آلية Proof-of-Contribution تهدف إلى تنظيم سلوك العقد واكتشاف السلوكيات غير الطبيعية. وتوضح الدراسة أن دمج آلية الثقة مع Smart Contracts يمكن أن يسمح باكتشاف وإدارة سلوك العقد بصورة آلية. [37]

كما يمكن استخدام السمعة في اختيار Edge Nodes التي ستنفذ مهام المستخدم .فإذا كان لدى عقدة سجل جيد من العمليات الناجحة، يمكن إعطاؤها أولوية في تخصيص الموارد. وعلى العكس، يمكن تقليل الثقة في العقدة إذا تكررت لديها حالات فشل أو سلوك مشبوه.

وتتضح أهمية ذلك في الأنظمة التعاونية، حيث تتبادل Edge Nodes الموارد والخدمات. وتوضح دراسة Blockchain-Based Collaborative Edge Computing: Efficiency, Incentive and Trust أن التعاون بين Edge Nodes يحتاج إلى معالجة قضايا الحوافز والثقة، وأن Blockchain يمكن أن يدعم آليات الثقة والحوافز ضمن عملية التعاون. [56]

لكن إدارة السمعة تواجه تحديات مثل Collusion Attacks، حيث يمكن لمجموعة من العقد الخبيثة أن تتعاون لمنح بعضها تقييمات إيجابية مزيفة. كما يمكن أن تتأثر السمعة بالأخطاء المؤقتة في الشبكة، ولذلك لا ينبغي اعتبار فشل واحد دليلًا مباشرًا على سلوك خبيث.

ومن هنا تحتاج أنظمة المستقبل إلى نماذج سمعة تأخذ في الاعتبار الزمن، والسياق، ونوع الخدمة، ومصداقية مصادر التقييم. ويمكن أن يؤدي دمج Machine Learning مع Blockchain إلى تطوير نماذج قادرة على اكتشاف الأنماط غير الطبيعية بصورة أفضل.

3.5. البلوكشين كآلية للثقة اللامركزية:

تتمثل القيمة الأساسية لـBlockchain في مجال الثقة في قدرته على توفير سجل مشترك بين الأطراف دون الحاجة إلى جهة مركزية تتحكم في السجل. ففي بيئة Edge، يمكن أن تتعامل عدة عقد من مؤسسات مختلفة مع بعضها، وقد لا توجد جهة واحدة قادرة على فرض الثقة بينها. وهنا يمكن استخدام Blockchain لتوفير طبقة مشتركة تسجل العمليات وتتيح التحقق منها.

توضح دراسة TrustChain أن الجمع بين Blockchain وEdge يمكن أن يعالج بعض مشكلات الثقة والخصوصية المرتبطة بالـ IoT. وقد ركزت الدراسة على تقليل التأخير ومشكلات الخصوصية واستهلاك الموارد مقارنة ببعض نماذج Blockchain التقليدية. [9]

كما أن منصة A Blockchain-Based Trusted Edge Platform توضح كيفية بناء بيئة Edge موثوقة باستخدام Hyperledger Fabric. فالمنصة توزع Blockchain على عدة عقد وتستخدم خدمات مصادقة أمنية، مما يتيح إنشاء بنية موثوقة للعمليات الطرفية. [32]

أما دراسة Towards Trustworthy IoT فتقدم مفهومًا أكثر ارتباطًا بالسلوك، من خلال Proof-of-Contribution، حيث تستخدم Blockchain والعقود الذكية لتنظيم مساهمة العقد واكتشاف السلوكيات غير المرغوبة. وتكمن أهمية هذا النموذج في أنه لا يفترض الثقة بالعقد، بل يحاول بناءها وتحديثها بناءً على السلوك. [37]

ومع ذلك، يجب التمييز بين الثقة في السجل والثقة في الطرف. فالبلوكشين يستطيع ضمان أن السجل لم يتغير بسهولة بعد تسجيله، لكنه لا يضمن أن البيانات التي أدخلتها العقدة كانت صحيحة أصلًا. ولذلك فإن Oracle Problem، أو مشكلة

موثوقية البيانات القادمة من العالم الخارجي، تظل قائمة.

وعليه، فإن Blockchain ينبغي أن يكون جزءًا من نموذج ثقة متكامل يضم المصادقة، والسمعة، وتحليل السلوك، وآليات التحقق من البيانات. ويمكن في المستقبل استخدام الذكاء الاصطناعي لتحليل السلوك، بينما يوفر Blockchain سجلًا موثوقًا لهذه التقييمات.

6. إدارة الموارد وتفريغ المهام في Blockchain–Edge Computing

تمثل إدارة الموارد وتفريغ المهام أحد أكثر محاور Blockchain–Edge Computing بحثًا، لأن Edge Nodes تمتلك موارد محدودة مقارنة بالسحابة، بينما تتطلب التطبيقات الحديثة قدرات حوسبية واتصالية كبيرة. ويتيح Blockchain بناء آليات موزعة لتبادل الموارد وتسجيل المعاملات، في حين تسمح خوارزميات التحسين والتعلم المعزز باتخاذ قرارات أكثر كفاءة بشأن مكان تنفيذ المهام. وقد تناولت الدراسات [16] و[22] و[24] و[33] و[34] و[39] و[45] و[46] هذا المجال من خلال نماذج لتخصيص الموارد وتفريغ المهام والتعاون بين العقد.

1.6 تخصيص الموارد الحاسوبية والشبكية:

تعتمد كفاءة Edge Computing على الاستخدام الفعال للموارد المتاحة، مثل CPU والذاكرة والتخزين وعرض النطاق الترددي والطاقة. وتظهر مشكلة تخصيص الموارد بسبب اختلاف قدرات Edge Nodes وتفاوت أحمالها. فقد تكون عقدة محملة بمهام كثيرة في حين تكون عقدة أخرى غير مستغلة بصورة كاملة. لذلك تحتاج الأنظمة إلى آليات تسمح بمشاركة الموارد بين العقد بطريقة فعالة وآمنة.

تُعد دراسة Resource Sharing of Mobile Edge Computing Networks Based on Auction Game and Blockchain من الدراسات المهمة في هذا المجال. فقد افترضت أن Edge Clouds قد تنتمي إلى شركات أو مؤسسات مختلفة، مما يؤدي إلى عزلة الموارد وعدم الاستفادة المثلى منها. واقترحت استخدام Blockchain كجسر لمشاركة الموارد، مع استخدام Smart Contracts لنشر احتياجات الموارد، ثم تطبيق Auction Game لتخصيص الموارد الحاسوبية والاتصالية وفق قيود QoS [33].

ويتميز هذا النموذج بربط Blockchain وResource Market، إذ لا يكون الهدف مجرد حماية البيانات، بل استخدام Blockchain لتوفير بيئة موثوقة لتبادل الموارد بين الأطراف التي قد لا تثق ببعضها. ويمكن للعقود الذكية تسجيل معاملات الموارد، بينما تحدد آلية المزاد السعر أو المورد المناسب.

وفي دراسة Resource Allocation and Trust Computing for Blockchain-Enabled Edge Computing System تم الجمع بين تخصيص الموارد وحساب الثقة .وتوضح هذه الدراسة أن قرار تخصيص الموارد لا ينبغي أن يعتمد فقط على الموارد المتاحة، بل ينبغي أيضًا أن يأخذ في الاعتبار موثوقية العقدة [34].

كما تناولت دراسة BeCome مشكلة عدم توازن الموارد أثناء تفريغ المهام. واستخدمت Blockchain للحفاظ على سلامة البيانات أثناء عملية التفريغ، بينما استخدمت NSGA-III لتوليد استراتيجيات تخصيص الموارد، ثم استُخدمت آليات MCDM لاختيار استراتيجية التفريغ المناسبة [16].

ويظهر من هذه الدراسات أن Blockchain يمكن أن يوفر طبقة ثقة لمشاركة الموارد، لكنه لا يقوم بعملية التخصيص بنفسه؛ فالقرار يحتاج إلى خوارزميات تحسين أو Game Theory أو Machine Learning.

ومن التحديات أن تنفيذ معاملات Blockchain لكل عملية تخصيص قد يزيد زمن الاستجابة. ولذلك يجب أن يكون استخدام Blockchain انتقائيًا، بحيث تُسجل معاملات الموارد المهمة فقط، بينما تنفذ القرارات السريعة محليًا في Edge.

2.6 تفريغ المهام والحوسبة التعاونية:

يُعد Computation Offloading من أهم آليات Edge Computing، حيث يسمح للجهاز النهائي بإرسال مهمة حسابية إلى Edge Node بدل تنفيذها محليًا. ويساعد ذلك في تقليل زمن التنفيذ واستهلاك طاقة الأجهزة محدودة الموارد. لكن عملية التفريغ تتطلب اختيار Edge Node مناسبة، والتحقق من موثوقيتها، وتحديد الموارد التي ستخصص للمهمة.

وقد قدمت دراسة BeCome نموذجًا يجمع Blockchain مع Computation Offloading في IoT وMEC. ويهدف النموذج إلى معالجة مشكلة عدم توازن طلبات الموارد، إضافة إلى مخاطر فقدان سلامة البيانات أثناء التفريغ. واستخدمت الدراسة Blockchain لضمان سلامة البيانات، ثم استخدمت NSGA-III لتحسين استراتيجية توزيع الموارد. [16]

كما تناولت دراسة Blockchain-Based Task Offloading in Drone-Aided Mobile Edge Computing تفريغ المهام في بيئة تعتمد على الطائرات المسيرة كعقد Edge. وتظهر أهمية Blockchain في توفير سجل تدقيق للعمليات، خصوصًا عندما تكون بيانات المستخدم معالجة من قبل مزودي خدمة Edge مختلفين [39].

وفي بيئات التعاون بين Edge Nodes، يمكن أن تسمح الحوسبة التعاونية بنقل المهمة من عقدة إلى أخرى وفق حالة الموارد. وقد تناولت دراسة Cooperative Computing in Integrated Blockchain-Based Internet of Things بنية للحوسبة التعاونية تعتمد على عدة خوادم حسابية، وركزت على تحقيق كفاءة الطاقة في بيئة Blockchain-based IoT [15].

ويؤدي Blockchain دورًا مهمًا في هذا السياق من خلال تسجيل الاتفاقيات بين الأطراف، وإثبات أن المهمة أرسلت إلى عقدة معينة، وتسجيل الموارد المستخدمة، وربما إدارة الحوافز. إلا أن هذا الاستخدام يفرض تكلفة إضافية، لأن عملية التفريغ نفسها حساسة للتأخير.

ولهذا السبب يجب أن يراعي نظام Blockchain–MEC أن بعض التطبيقات، مثل المركبات الذكية والروبوتات، لا يمكنها الانتظار حتى انتهاء دورة إجماع طويلة. ويمكن معالجة ذلك باستخدام Permissioned Blockchain أو Lightweight Consensus أو تنفيذ Blockchain على Edge Nodes ذات قدرات أعلى.

كما يمكن استخدام التعلم المعزز لاتخاذ قرارات Offloading ديناميكية. وقد ظهرت أعمال تجمع Blockchain مع Deep Reinforcement Learning، مثل [22] و[29] و[46]. وتسمح هذه النماذج بتعلم أفضل استراتيجية للتفريغ من خلال مراقبة حالة الشبكة والموارد.

ومن هنا يتجه البحث نحو Blockchain-Assisted Intelligent Offloading الذي يجمع بين الثقة اللامركزية والذكاء الاصطناعي لاتخاذ قرارات تفريغ تتكيف مع ظروف الشبكة.

3.6 تقنيات التحسين والتعلم المعزز لإدارة الموارد:

أدى تعقيد بيئات Edge إلى جعل أساليب التخصيص التقليدية غير كافية في بعض السيناريوهات. فحالة الموارد تتغير باستمرار، وعدد المستخدمين يتغير، كما تتغير جودة الاتصال وحجم المهام. ولذلك اتجهت الدراسات إلى استخدام Optimization وMachine Learning وDeep Reinforcement Learning لاتخاذ قرارات ديناميكية.

تمثل دراسة Cooperative Computation Offloading and Resource Allocation for Blockchain-Enabled Mobile Edge Computing: A Deep Reinforcement Learning Approach [22] مثالًا مباشرًا على هذا الاتجاه، حيث تجمع بين Blockchain وDeep Reinforcement Learning لاتخاذ قرارات مرتبطة بالتفريغ وتخصيص الموارد. ويهدف هذا النوع من النماذج إلى الوصول إلى سياسة مناسبة من خلال التعلم من حالة النظام بدل الاعتماد على قواعد ثابتة.

كما استخدمت دراسة BeCome خوارزمية NSGA-III متعددة الأهداف لتحسين استراتيجيات تفريغ المهام [16]. وتكمن أهمية الخوارزميات متعددة الأهداف في أن القرار لا يعتمد على معيار واحد؛ فقد يحتاج النظام إلى تقليل التأخير واستهلاك الطاقة وتحسين استغلال الموارد في الوقت نفسه. وفي مجال مشاركة الموارد، استخدمت دراسة Auction Game مع Blockchain [33]. ويتيح ذلك تحويل عملية تخصيص الموارد إلى آلية سوق، بحيث تتنافس الطلبات على الموارد وفق شروط محددة، بينما يوفر Blockchain سجلًا موثوقًا للمعاملات.

أما في التعاون بين Edge Nodes، فتوضح دراسة [56] أن Blockchain يمكن دمجه مع VCG Auction بهدف تحسين Load Balancing واستغلال الموارد، مع معالجة قضايا الحوافز والثقة بين العقد.

ومن منظور منهجي، يمكن تقسيم خوارزميات إدارة الموارد في Blockchain–Edge إلى ثلاث فئات رئيسية: Optimization-Based، Game-Theoretic، وLearning-Based. وتعتمد الفئة الأولى على نماذج رياضية، بينما تعتمد الثانية على آليات التفاوض والحوافز، أما الثالثة فتستخدم البيانات السابقة للتنبؤ واتخاذ القرارات.

لكن دمج Blockchain مع التعلم المعزز يفرض تحديًا إضافيًا، إذ إن Blockchain نفسها تضيف متغيرات إلى البيئة مثل زمن الإجماع وحجم السجل وعدد العقد. وبالتالي ينبغي أن يأخذ نموذج التعلم في الاعتبار Blockchain Overhead بدل تحسين الموارد الحاسوبية فقط.

وتُعد هذه النقطة من الفجوات المهمة في الأدبيات؛ إذ تركز بعض الدراسات على تحسين Offloading بينما تركز أخرى على Blockchain Security، دون بناء نموذج موحد يوازن بين Latency + Energy + Resource Utilization + Blockchain Consensus Overhead + Security.

7. إدارة البيانات ومشاركتها في البيئات الطرفية

تنتج بيئات Edge كميات كبيرة من البيانات التي تحتاج إلى جمعها وتخزينها ومعالجتها ومشاركتها بين أجهزة ومؤسسات متعددة. ويقدم Blockchain خصائص مهمة في هذا المجال، مثل سلامة البيانات، وقابلية التتبع، وعدم الاعتماد على مخزن مركزي واحد. إلا أن تخزين البيانات الكبيرة مباشرة على Blockchain يفرض قيودًا على التخزين والأداء، ولذلك ظهرت حلول تعتمد على Off-chain Storage مع تسجيل Hash أو معلومات وصفية على السلسلة. كما ركزت الدراسات على التحكم الدقيق بالوصول وحماية الخصوصية، مثل [14] و[27] و[36] و[47] و[60]. وتوضح هذه الأعمال أن دمج Blockchain مع Edge يمكن أن يوفر بيئة موثوقة لمشاركة البيانات مع المحافظة على كفاءة المعالجة الطرفية.

1.7 تخزين وإدارة البيانات باستخدام Blockchain:

تحتاج تطبيقات Edge إلى إدارة كميات ضخمة من البيانات الناتجة عن أجهزة IoT وأجهزة الاستشعار والمستخدمين. ويتميز Edge Computing بإمكانية معالجة البيانات بالقرب من مصدرها، بينما يوفر Blockchain طبقة لتسجيل العمليات المتعلقة بالبيانات والتحقق منها. ولهذا يمكن الجمع بين التقنيتين لإنشاء نظام تكون فيه البيانات قريبة من المستخدم، بينما تكون سجلات العمليات موزعة وقابلة للتدقيق.

قدمت دراسة Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning نموذجًا لجمع البيانات ومشاركتها في IIoT باستخدام Blockchain و Deep Reinforcement Learning. واستخدمت الدراسة Ethereum لإنشاء بيئة أكثر موثوقية لمشاركة البيانات، مع معالجة مشكلة كفاءة جمع البيانات وقيود الطاقة ونطاق الاستشعار [14].

لكن أحد أهم القيود هو عدم ملاءمة Blockchain لتخزين البيانات الضخمة مباشرة. فكلما زاد حجم البيانات، زادت متطلبات التخزين والتكرار والاتصال بين العقد. لذلك تتجه معماريات Blockchain–Edge إلى فصل Data Storage عن Data Integrity. حيث يتم تخزين البيانات الفعلية في Edge Storage أو Distributed Storage، بينما يتم تخزين Hash أو معرف البيانات على Blockchain.

ومن الأمثلة ذات الصلة دراسة [47] التي تناولت Blockchain في معالجة Big Data ضمن Edge Computing. ويعكس هذا الاتجاه الحاجة إلى تصميم معماريات تخزين لا تجعل Blockchain مستودعًا مباشرًا لكل البيانات، وإنما تستخدمه كسجل ثقة للبيانات.

كما يمكن استخدام Blockchain لإدارة Metadata، مثل مالك البيانات، وتاريخ إنشائها، ومصدرها، والتعديلات التي طرأت عليها. ويتيح ذلك بناء Data Provenance دون الحاجة إلى تخزين المحتوى الكامل على Blockchain.

وفي التطبيقات متعددة المؤسسات، يمكن استخدام Blockchain كدفتر أستاذ مشترك يسمح لكل طرف بمعرفة حالة البيانات والعمليات المتعلقة بها دون الحاجة إلى قاعدة بيانات مركزية مشتركة. وهذا مفيد في البيئات الصناعية والصحية والطاقة.

لكن تصميم التخزين يحتاج إلى مراعاة زمن الوصول. فإذا احتاج التطبيق إلى قراءة البيانات بسرعة، فإن الاعتماد على

Blockchain في كل عملية قد يؤدي إلى زيادة التأخير. لذلك يعد النموذج الهجين On-chain Metadata + Off-chain Data من أكثر الاتجاهات ملاءمة.

2.7 مشاركة البيانات الآمنة وحفظ الخصوصية:

تحتاج Edge Computing إلى مشاركة البيانات بين الأجهزة والعقد والخدمات حتى تتمكن من تنفيذ التطبيقات التعاونية. إلا أن مشاركة البيانات تثير مشكلات تتعلق بالخصوصية والتحكم فيمن يستطيع الوصول إليها. ولذلك اتجهت الدراسات إلى الجمع بين Blockchain والتشفير والتحكم الدقيق بالوصول.

تقدم دراسة BDSS-FA مثالًا واضحًا على ذلك، حيث اقترحت منصة لمشاركة البيانات بأمان باستخدام Blockchain وFine-Grained Access Control. واعتمدت على Hierarchical Attribute-Based Encryption لتطبيق سياسات دقيقة، بحيث تحدد خصائص المستخدم أو الجهة ما إذا كان بإمكانها فك تشفير البيانات [27].

كما قدمت دراسة Blockchain-Enabled Secure Data Sharing Scheme in Mobile-Edge Computing نموذجًا لمشاركة البيانات في MEC، واستخدمت Asynchronous Advantage Actor–Critic Learning. وركزت الدراسة على مشاركة البيانات مع مراعاة متطلبات الخصوصية والموارد المتاحة، مما يعكس الاتجاه نحو جعل آليات حماية الخصوصية متكيفة مع حالة النظام [36].

ومن الحلول المهمة أيضًا فصل البيانات الحساسة عن Blockchain. ففي دراسة مشاركة السجلات الطبية مثلًا، يتم تشفير البيانات وتخزينها في نظام تخزين موزع، بينما يتم وضع معلومات الفهرسة على Blockchain، مع استخدام Smart Contracts للبحث والتحكم بالعمليات .ويقلل ذلك الضغط الناتج عن تخزين البيانات الكبيرة على السلسلة.

ويمكن تطبيق المبدأ نفسه في Edge Computing. فبدل وضع البيانات نفسها على Blockchain، يمكن تشفيرها وتخزينها في Edge أو نظام تخزين موزع، ثم تخزين Hash ومعرف المورد وسياسة الوصول على Blockchain. وعند طلب البيانات، يتم التحقق من هوية المستخدم وسياسة الوصول ثم استرجاع البيانات من التخزين الخارجي.

لكن Blockchain قد تسبب مشكلة خصوصية إذا كانت المعاملات تكشف معلومات حول هوية المستخدم أو نمط استخدامه. لذلك تحتاج الأنظمة إلى Privacy-Preserving Techniques مثل Pseudonyms والتشفير وإخفاء البيانات الوصفية.

كما أن Fine-Grained Access Control يمثل تحديًا عندما يتغير المستخدم أو تتغير خصائصه. ولذلك يجب أن تكون الصلاحيات قابلة للتحديث والإلغاء دون الحاجة إلى إعادة بناء النظام بالكامل.

وبالتالي فإن المشاركة الآمنة في Blockchain–Edge تحتاج إلى تكامل بين Encryption + Access Control + Smart Contracts + Off-chain Storage + Blockchain Auditability.

3.7 سلامة البيانات وتتبع مصدرها وإمكانية التدقيق:

تُعد سلامة البيانات (Data Integrity) من أهم المتطلبات في الأنظمة الطرفية، لأن البيانات قد تمر عبر عدة أجهزة وعقد قبل وصولها إلى التطبيق النهائي. وإذا تم تعديل البيانات أثناء النقل أو التخزين، فقد يؤدي ذلك إلى اتخاذ قرارات خاطئة، خاصة في التطبيقات الصناعية والطبية والطاقة.

يوفر Blockchain وسيلة فعالة للتحقق من سلامة البيانات من خلال تسجيل Hash للبيانات أو المعاملات. فعندما يتم إنشاء البيانات، يمكن حساب بصمتها الرقمية وتسجيلها على Blockchain. وعند استرجاع البيانات لاحقًا، يمكن حساب Hash جديد ومقارنته بالقيمة المسجلة. وإذا تطابقت القيمتان، يمكن الاستدلال على أن البيانات لم تتغير بعد تسجيلها.

تناولت دراسة Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning استخدام Blockchain في إنشاء بيئة آمنة وموثوقة لجمع ومشاركة بيانات IIoT [14]. وتوضح الدراسة أهمية الجمع بين سلامة البيانات وطرق ذكية لإدارة عملية جمعها.

كما يمكن استخدام Blockchain لتحقيق Data Provenance، أي معرفة مصدر البيانات ومسارها والعمليات التي تمت

عليها. وتزداد أهمية ذلك عندما تمر البيانات عبر عدة Edge Nodes. ويمكن تسجيل كل عملية معالجة أو نقل بصورة مختصرة على Blockchain، مما يوفر سلسلة قابلة للتدقيق.

ويظهر هذا المفهوم بوضوح في دراسة Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing، حيث تجمع الدراسة بين التوثيق وإمكانية تتبع البيانات في بيئة مركبية ديناميكية [19].

كما أن Auditability تمثل فائدة أساسية للبلوكشين. فعندما يتم تسجيل عمليات الوصول أو مشاركة البيانات أو تنفيذ المهام، يمكن للجهات المصرح لها مراجعة السجل لمعرفة ما حدث ومتى ومن قام به. وهذا مفيد في الأنظمة التي تحتاج إلى المساءلة والامتثال.

لكن هناك تحديًا مهمًا: عدم قابلية تعديل السجل لا تعني صحة البيانات الأصلية. فإذا أرسلت عقدة خبيثة بيانات خاطئة، فإن Blockchain ستضمن سلامة تسجيل البيانات الخاطئة، وليس صحتها. ولذلك يجب دمج Blockchain مع آليات للتحقق من مصدر البيانات، وTrust Management، وAnomaly Detection.

كما أن تسجيل كل عملية على Blockchain قد يؤدي إلى تضخم حجم السجل وزيادة تكلفة التخزين. ولذلك يفضل تسجيل الأحداث الحساسة أو Hashes بدل المحتوى الكامل.

ومن هنا يمكن اعتبار Blockchain طبقة Integrity and Auditability أكثر من كونها قاعدة بيانات تقليدية. وتتمثل البنية الأكثر كفاءة في تخزين البيانات في Edge أو Off-chain، مع الاحتفاظ على Blockchain بسجل مختصر يسمح بالتحقق من السلامة وتتبع المصدر ومراجعة العمليات.

8. آليات الإجماع وقابلية التوسع والأداء

يمثل الجمع بين Blockchain وEdge Computing اتجاهًا مهمًا لبناء بيئات حوسبة موزعة قادرة على توفير الثقة وسلامة البيانات مع الاستفادة من المعالجة القريبة من مصادر البيانات. إلا أن تطبيق البلوكشين في البيئات الطرفية يفرض تحديات تتعلق بآليات الإجماع، وحجم دفتر الأستاذ، وزمن تأكيد المعاملات، والإنتاجية، واستهلاك الموارد. وقد بينت الدراسات أن قابلية التوسع في البلوكشين مفهوم متعدد الأبعاد يشمل عدد العقد، والإنتاجية، وزمن الاستجابة، ومعدل إنشاء الكتل، والتخزين [53]. ولذلك اتجهت الأبحاث إلى تطوير آليات إجماع أخف، وبنى Blockchain متعددة المستويات، وتقنيات التجزئة، وتقسيم التخزين، إضافة إلى استخدام التعاون بين Cloud وEdge لتقليل العبء على العقد الطرفية [35] [62]. ويشكل تحقيق التوازن بين الأمن والأداء وقابلية التوسع الأساس لتطوير أنظمة Blockchain–Edge قابلة للتطبيق في البيئات الواقعية.

1.8 آليات الإجماع المناسبة للحوسبة الطرفية:

تُعد آلية الإجماع من المكونات الأساسية في Blockchain، لأنها تحدد كيفية اتفاق العقد على صحة المعاملات والبيانات قبل تسجيلها في دفتر الأستاذ. وتصبح عملية اختيار الإجماع أكثر تعقيدًا في الحوسبة الطرفية بسبب محدودية موارد بعض الأجهزة، وعدم تجانس العقد، والديناميكية المستمرة للشبكة .وقد أظهرت الدراسات المبكرة أن آليات الإجماع التقليدية ذات المتطلبات الحسابية والاتصالية المرتفعة لا تتناسب بصورة مثالية مع بيئات IoT وEdge Computing، مما أدى إلى البحث عن آليات أخف وأكثر كفاءة [5].

ويظهر اتجاه واضح نحو استخدام آليات Byzantine Fault Tolerance (BFT) في البيئات المصرح بها، لأنها لا تحتاج إلى عمليات التعدين كثيفة الحساب كما هو الحال في Proof of Work. وفي هذا السياق، قدمت الدراسة [41] خوارزمية DR-BFT مخصصة لبيئة Edge Computing الديناميكية، حيث يمكن للعقد الانضمام إلى الشبكة أو مغادرتها بصورة مستمرة. وقد صممت الدراسة إطارًا مكونًا من طبقتين، مع استخدام ثلاث آليات فرعية هي String Consensus و Data Correctness Validation وBinary Consensus، إضافة إلى آلية محسنة للتعامل مع تغير العقد [41]. وأظهرت النتائج أن DR-BFT يمكن أن تقلل من زمن الإجماع والعبء الاتصالي مقارنة ببعض آليات BFT المستخدمة للمقارنة.

ومن الاتجاهات الأخرى نقل جزء من عمليات البلوكشين من الأجهزة النهائية إلى العقد الطرفية. فقد قدمت الدراسة [35] إطار

ECLB الذي يجعل Edge Nodes مسؤولة عن جزء كبير من عمليات التخزين والإجماع، بينما تستخدم الأجهزة الطرفية Ledger مجزأً بدل الاحتفاظ بنسخة كاملة من دفتر الأستاذ [35]. ويساعد هذا التصميم على تخفيف متطلبات التخزين والحساب على الأجهزة محدودة الموارد، مع المحافظة على إمكانية الوصول إلى المعاملات المطلوبة.

كما اتجهت بعض الدراسات إلى نقل العبء الحسابي المرتبط بالإجماع إلى السحابة. فقد اقترحت الدراسة [62] بروتوكول Proof-of-Ticket (PoT) ضمن نموذج Cloud–Edge Collaboration، بحيث يتم تفريغ الاستهلاك الحسابي لعملية الإجماع من العقد الطرفية إلى السحابة، في حين تعالج آلية Edge–Terminal Consensus Zone مشكلة التخزين [62]. وتوضح هذه النتيجة أن تحسين الإجماع في Edge لا يعني بالضرورة تصميم خوارزمية جديدة فقط، وإنما يمكن تحقيقه أيضًا من خلال إعادة توزيع وظائف Blockchain بين طبقات النظام.

ومن منظور قابلية التوسع، تشير الدراسة [53] إلى أن الإجماع يمثل أحد عناصر التوسع الرأسي للبلوكشين إلى جانب الإنتاجية وزمن التأخير والتخزين، مما يعني أن تحسين الإجماع يجب أن يكون جزءًا من استراتيجية شاملة للتوسع وليس حلًا منفردًا [53]. كما تظهر الدراسات الحديثة اتجاهًا نحو دمج الإجماع مع التجزئة والبنى الهرمية. فالدراسة [71] تقترح بنية Blockchain هرمية ومجزأة توزع العقد في مجموعات وفق خصائص الأداء والقرب الجغرافي، مما يحد من حجم مجموعة العقد التي تشارك في عمليات الإجماع المحلية [71].

وبناءً على ذلك، يمكن القول إن الاتجاه البحثي يتجه من الإجماع التقليدي الموحد إلى إجماع خفيف، ومصرح به، ومتعدد المستويات، وقابل للتكيف مع تغير الشبكة .ومن المتوقع أن تزداد أهمية الآليات التي تستطيع تعديل مجموعة العقد المشاركة في الإجماع وفق حالة الموارد وحجم الحمل ومتطلبات التطبيق، مع الحفاظ على خصائص الأمان والثقة.

2.8 قابلية التوسع والتخزين في شبكات Blockchain–Edge:

تمثل قابلية التوسع أحد أهم العوائق أمام نشر Blockchain في بيئات Edge Computing واسعة النطاق. فالحوسبة الطرفية تتعامل مع أعداد كبيرة من الأجهزة والمعاملات والبيانات، بينما تعتمد Blockchain على آليات موزعة تتطلب التحقق والمزامنة والتخزين عبر مجموعة من العقد. وقد عرفت الدراسة المنهجية [53] قابلية التوسع باعتبارها مفهومًا مركبًا يشمل التوسع الأفقي، مثل زيادة عدد المشاركين والعملاء، والتوسع الرأسي، مثل تحسين الإنتاجية، وزمن الاستجابة، ومعدل إنشاء الكتل، والتخزين [53]. ويجعل هذا التعريف معالجة التوسع في Blockchain–Edge مسألة تتجاوز مجرد زيادة عدد المعاملات.

وتزداد مشكلة التخزين بصورة خاصة عندما تكون العقد الطرفية محدودة الذاكرة. فالنموذج التقليدي الذي يتطلب من كل عقدة الاحتفاظ بنسخة كاملة من دفتر الأستاذ قد لا يكون مناسبًا لأجهزة IoT والمحمولة. ولهذا اقترحت الدراسة [35] استخدام Fragmented Ledger بحيث لا تحتاج الأجهزة النهائية إلى تخزين Blockchain كاملة، بل تحتفظ فقط بالمعلومات ذات الصلة بها [35]. ويؤدي ذلك إلى تقليل متطلبات التخزين مع المحافظة على إمكانية الوصول إلى بيانات المعاملات المطلوبة.

كما قدمت الدراسة [62] حلًا مختلفًا يعتمد على تقسيم الشبكة إلى Edge–Terminal Consensus Zones (ETCZ). ويسمح هذا التقسيم بتقليل كمية البيانات التي يجب أن تحتفظ بها العقد الطرفية، وقد أوضحت الدراسة أن متطلبات التخزين للعقدة الكاملة يمكن أن تنخفض إلى جزء من متطلبات Blockchain التقليدية عند زيادة عدد مناطق الإجماع [62]. ويشير ذلك إلى أهمية تقسيم دفتر الأستاذ وفق طبيعة الخدمات أو المناطق بدل توزيع السجل الكامل بصورة متكررة على جميع العقد.

ومن الحلول الأكثر تقدمًا استخدام Sharding، حيث يتم تقسيم الشبكة والبيانات إلى أجزاء مستقلة نسبيًا. وقد قدمت الدراسة [71] نموذج Hierarchical Sharding Blockchain Storage Solution يتكون من Cloud Chain Layer و Edge Chain Layer وTerminal Layer، مع وجود سلسلة رئيسية وسلاسل فرعية مجزأة [71]. كما تستخدم الدراسة تجميع العقد الطرفية ذات الأداء والقرب المتشابهين ضمن Shards مختلفة، مما يساعد على تحقيق توازن أفضل في موارد التخزين.

وتكمل الدراسة [71] هذا التصميم باستخدام خوارزمية Weighted Consistent Hashing لتوزيع أحمال التخزين بين الأجزاء المختلفة، وهو ما يهدف إلى تجنب تحميل مجموعة محددة من العقد بصورة أكبر من غيرها [71]. ويكشف هذا الاتجاه أن التوسع في Edge Blockchain يحتاج إلى مراعاة تفاوت قدرات العقد بدل افتراض امتلاك جميع العقد لقدرات متساوية.

ومن جهة أخرى، تساهم تقنيات Off-chain Processing وCloud–Edge Collaboration في تقليل البيانات التي تتم معالجتها وتخزينها مباشرة على Blockchain. كما يمكن استخدام Blockchain صغيرة الحجم أو محلية للخدمات التي لا تحتاج إلى مشاركة عالمية لجميع المعاملات. وتدعم الدراسات المتعلقة بالموارد هذا الاتجاه من خلال فصل الوظائف الحسابية عن وظائف التخزين [62].

وعليه، فإن تحقيق قابلية التوسع في Blockchain–Edge يتطلب الجمع بين Sharding، وHierarchical Blockchain، وFragmented Ledger، وOff-chain Storage، وCloud–Edge Collaboration. كما ينبغي أن تراعي الحلول المستقبلية اختلاف قدرات العقد، لأن التوسع الحقيقي لا يتحقق بمجرد زيادة عدد العقد، وإنما بقدرة النظام على المحافظة على الأداء عند زيادة المستخدمين والمعاملات والبيانات.

3.8 تحليل الأداء: زمن الاستجابة والإنتاجية واستهلاك الموارد:

يمثل تقييم الأداء عنصرًا أساسيًا في دراسة أنظمة Blockchain–Edge، لأن إضافة Blockchain إلى Edge Computing قد تعزز الثقة وسلامة البيانات، لكنها في الوقت نفسه تضيف عمليات إجماع وتحقق وتخزين واتصالات. ولذلك تستخدم الدراسات مجموعة من المؤشرات لتقييم أداء هذه الأنظمة، من أبرزها زمن الاستجابة، والإنتاجية، واستهلاك الحوسبة، والتخزين، والطاقة، والاتصالات. وقد أكدت الدراسة المنهجية [53] أن الإنتاجية وزمن التأخير ومعدل إنشاء الكتل والتخزين تمثل أبعادًا أساسية لقابلية توسع Blockchain [53].

ويُعد زمن الاستجابة Latency مهمًا بصورة خاصة في تطبيقات المركبات الذكية وV2X وG5 وIIoT، حيث يمكن أن تؤثر الزيادة في زمن التحقق أو الإجماع في جودة الخدمة. وفي هذا السياق، صممت الدراسة [41] خوارزمية DR-BFT لتناسب الشبكات الطرفية الديناميكية، وأظهرت تجاربها قدرة الخوارزمية على تقليل زمن الإجماع والعبء الاتصالي مقارنة ببعض آليات BFT الأخرى [41].

أما الإنتاجية Throughput فتعبر عن عدد المعاملات التي يستطيع النظام معالجتها خلال فترة زمنية محددة. وتبرز أهميتها في بيئات IoT التي تضم عددًا كبيرًا من الأجهزة. وقد اهتم إطار ECLB [35] بتحسين الإنتاجية وزمن تأكيد المعاملات إلى جانب تخفيض تكلفة التخزين والحساب، من خلال توزيع وظائف Blockchain بين Edge Nodes والأجهزة النهائية [35].

ويشكل استهلاك الموارد تحديًا إضافيًا، لأن العقد الطرفية لا تمتلك بالضرورة موارد حوسبية وتخزينية كافية لتنفيذ جميع عمليات Blockchain. وقد عالجت الدراسة [62] هذه المشكلة بصورة مباشرة من خلال فصل الموارد الحسابية عن التخزينية؛ إذ اقترحت نقل عمليات الإجماع الحسابية إلى Cloud، مع تقليل متطلبات التخزين على العقد الطرفية باستخدام ETCZ [62].

كما ركزت الدراسات [22] و[24] و[45] و[46] على تخصيص الموارد وComputation Offloading باستخدام تقنيات مثل Deep Reinforcement Learning، بهدف إيجاد توزيع مناسب للموارد بين الأجهزة والخوادم الطرفية. ويظهر في هذه الدراسات أن تحسين الأداء لا يعتمد فقط على تحسين Blockchain، بل يرتبط أيضًا بقرارات Task Offloading وResource Allocation.

وفي السنوات الأخيرة ظهر اتجاه نحو التحسين متعدد الأهداف. فالدراسة [68] تركز على جدولة المهام وفق متطلبات QoS في Mobile Edge Computing، بينما تتناول الدراسة [76] التخصيص المشترك للموارد في Blockchain-enabled MEC. كما تستمر الدراسة [80] في هذا الاتجاه باستخدام خوارزمية Many-Objective Evolutionary Algorithm لمعالجة تفريغ المهام المعقدة في Edge Computing المؤمنة بواسطة Blockchain [80].

وبالتالي، يجب ألا يقتصر تقييم أنظمة Blockchain–Edge على سرعة المعاملات فقط، بل ينبغي أن يشمل Latency وThroughput والطاقة والتخزين والحوسبة والاتصالات بصورة متزامنة. كما يجب إجراء الاختبارات عند أحجام مختلفة للشبكة، لأن النظام قد يظهر أداءً جيدًا في شبكة صغيرة لكنه يعاني من تدهور ملحوظ عند زيادة عدد العقد أو المعاملات.

9. تطبيقات البلوكشين والحوسبة الطرفية

أدى التكامل بين Blockchain وEdge Computing إلى ظهور مجموعة واسعة من التطبيقات التي تحتاج إلى الثقة، وسلامة البيانات، والخصوصية، وزمن الاستجابة المنخفض .وتظهر هذه التطبيقات بصورة واضحة في IoT وIIoT وIndustry 4.0، والمركبات الذكية، وUAV، وG/6G5، وشبكات الطاقة الذكية، والرعاية الصحية، والمدن الذكية. وقد أوضحت المراجعات المتخصصة أن Blockchain يمكن أن توفر آليات للتوثيق والثقة والتتبع، بينما تسمح Edge Computing بمعالجة البيانات بالقرب من مصدرها [4] [5] [54]. وبذلك يمكن للتكامل بين التقنيتين تقليل الاعتماد على البنية المركزية مع المحافظة على قدرة النظام على التعامل مع البيانات بصورة سريعة وموزعة.

1.9. تطبيقات IoT وIndustrial IoT وIndustry 4.0:

تُعد IoT وIIoT وIndustry 4.0 من أهم المجالات التي ظهر فيها تكامل Blockchain وEdge Computing، نتيجة الزيادة الكبيرة في عدد الأجهزة والحساسات والآلات المتصلة. ففي بيئات IoT، تتبادل الأجهزة البيانات بصورة مستمرة، مما يفرض الحاجة إلى آليات تضمن صحة البيانات وهوية الأجهزة وعدم تعرض السجلات للتلاعب. وقد ناقشت الدراسة [5] عددًا من القضايا الأمنية والبحثية المرتبطة باستخدام Blockchain في IoT، وبينت أن الهوية وسلامة البيانات والثقة وقابلية التوسع تمثل قضايا أساسية عند دمج التقنيتين [5].

وفي البيئة الصناعية، تزداد أهمية هذه المتطلبات بسبب الاعتماد على الحساسات والآلات وأنظمة التحكم في عمليات الإنتاج. وقد أوضحت الدراسة [8] أن دمج Edge Intelligence مع Blockchain يمكن أن يوفر بيئة مناسبة لـ IIoT من خلال معالجة البيانات بالقرب من مصدرها، مع الاستفادة من Blockchain في توفير الثقة وتوثيق العمليات [8].

كما اتجهت الدراسات إلى دمج Blockchain مع الذكاء الاصطناعي. فقد قدمت الدراسة [14] نموذجًا لجمع ومشاركة بيانات Industrial IoT بالاعتماد على Deep Reinforcement Learning، مما يعكس الانتقال من استخدام Blockchain كسجل للبيانات إلى استخدامها ضمن منظومة ذكية لاتخاذ قرارات مرتبطة بإدارة البيانات والموارد [14].

وتظهر أهمية هذا الاتجاه أيضًا في الدراسة [28] التي تجمع Blockchain مع Software-Defined IIoT وتستخدم Dueling Deep Q-Learning لتحسين عملية اتخاذ القرار، وهو ما يوضح إمكانية استخدام الذكاء الاصطناعي لمعالجة مشكلة إدارة الموارد إلى جانب الوظائف الأمنية التي تقدمها Blockchain [28].

وفي Industry 4.0، يمكن استخدام Blockchain لتوثيق البيانات الصناعية وتتبع العمليات وتبادل البيانات بين المؤسسات، بينما يمكن لـ Edge Computing تقليل زمن نقل البيانات إلى السحابة. وقد ناقشت الدراسة [43] تقارب Blockchain وEdge Computing في البنى التحتية الحرجة لـ IIoT وIndustry 4.0، مع التركيز على الأمن وقابلية التوسع [43].

ومن التطبيقات الحديثة إطار BlockEdge في الدراسة [59]، الذي يركز على توفير بيئة Edge آمنة ومراعية للخصوصية باستخدام Blockchain في Industry 4.0. كما تقدم الدراسة [66] آلية للأمن والثقة في أنظمة IIoT المدعومة بالذكاء الاصطناعي، وهو اتجاه مهم بسبب زيادة استقلالية الأنظمة الصناعية واعتمادها على قرارات ذكية.

أما الدراسة [75] المنشورة عام 2025، فتقدم بنية Blockchain-assisted Edge Computing آمنة وموثوقة لـ IIoT، وتجمع بين المصادقة والعقود الذكية وآليات الثقة ضمن البنية الطرفية [75]. ويعكس هذا التطور انتقال الأبحاث من مجرد تسجيل البيانات إلى بناء منظومة متكاملة لإدارة الهوية والثقة والأمن والعمليات الصناعية.

وعليه، فإن مستقبل Blockchain–Edge في Industry 4.0 يتجه نحو دمج AI وSmart Contracts و Trust Management وAccess Control مع المعالجة الطرفية، مع ضرورة المحافظة على الأداء وقابلية التوسع في بيئات صناعية تضم أعدادًا كبيرة من الأجهزة.

2.9 تطبيقات المركبات الذكية و UAVو5G/6G:

تتميز بيئات المركبات الذكية وUAV وG/6G5 بدرجة عالية من الديناميكية، حيث تتغير مواقع العقد والاتصالات باستمرار، كما تحتاج التطبيقات إلى زمن استجابة منخفض وموثوقية مرتفعة. ولهذا توفر Edge Computing إمكانية معالجة البيانات

بالقرب من المركبات أو الطائرات، بينما توفر Blockchain طبقة للثقة والمصادقة وتتبع البيانات.

في المركبات المتصلة، قدمت الدراسة [19] نموذجًا يعتمد على Blockchain لتحقيق Cooperative Authentication مع تتبع البيانات في Vehicular Edge Computing [19]. ويعالج هذا النوع من الحلول مشكلة الثقة بين المركبات والخوادم الطرفية، حيث يمكن تسجيل عمليات المصادقة والتعاملات بصورة قابلة للتدقيق.

كما قدمت الدراسة [31] مفهوم Decentralized Edges لتمكين Blockchain في البيئات المركبية، مما يوضح الاتجاه نحو توزيع وظائف Blockchain على الحواف بدل الاعتماد على بنية مركزية واحدة [31]. وتدعم الدراسة [40] هذا الاتجاه من خلال استخدام Multi-Channel Blockchain في Internet of Vehicles بهدف التعامل مع متطلبات الاتصالات والمعاملات المختلفة.

أما في V2X، فقد ركزت الدراسة [49] على استخدام Distributed Edge Computing مع Blockchain لدعم اتصالات Ultra-Reliable Low-Latency V2X، وهو أمر مهم في التطبيقات التي تتطلب تبادل المعلومات بسرعة كبيرة بين المركبات والبنية التحتية [49].

وفي مجال UAV، قدمت الدراسة [23] Blockchain باعتبارها حلًا موزعًا لأنظمة UAV-enabled MEC، بينما تناولت الدراسة [39] Task Offloading في Drone-Aided Mobile Edge Computing باستخدام [Blockchain 23] [39]. وتظهر أهمية هذه الحلول في أن الطائرات بدون طيار قد تكون محدودة الموارد، وبالتالي يمكن نقل المهام الحسابية الثقيلة إلى Edge Servers القريبة.

وفي شبكات 5G، قدمت الدراسة [8] تكاملًا بين Edge Intelligence وBlockchain في بيئات G5 المتقدمة وIndustrial IoT، بما يدعم مشاركة الموارد وإدارة الثقة [8]. ومع الانتقال إلى G Beyond5 وG6، تصبح الحاجة إلى زمن استجابة منخفض وإدارة موزعة للهوية والموارد أكثر أهمية.

وتتناول الدراسة [77] الاتجاه الحديث نحو استخدام Blockchain لتعزيز أمن G Edge Computing5 في IoT، مما يبرز أهمية حماية الأجهزة والبيانات والاتصالات في بيئة شديدة الكثافة [77]. كما تتجه الأبحاث إلى استخدام Deep Reinforcement Learning لتحسين تخصيص الموارد والـ offloading، كما يظهر في الدراسات [22] و[46] و[70].

وعليه، فإن التطبيقات المستقبلية للمركبات وUAV وG/6G5 تحتاج إلى Blockchain خفيفة وسريعة وقابلة للتكيف، لأن استخدام Blockchain التقليدية قد يتعارض مع متطلبات الزمن الحقيقي. ويبرز هنا دور Edge وSharding والإجماع الخفيف والتعلم المعزز في بناء أنظمة تجمع بين الأمن والأداء.

3.9 تطبيقات Smart Grid والرعاية الصحية والمدن الذكية:

تمثل Smart Grid والرعاية الصحية والمدن الذكية مجالات مناسبة لتطبيق Blockchain–Edge بسبب اعتمادها على مصادر بيانات موزعة وحساسة، وحاجتها إلى الثقة والتتبع والخصوصية. ففي Smart Grid، يمكن استخدام Blockchain لتسجيل معاملات الطاقة وتبادلها بين المنتجين والمستهلكين دون الاعتماد الكامل على وسيط مركزي.

وقد قدمت الدراسة [7] نموذجًا يعتمد على Permissioned Blockchain وEdge Computing لشبكات Smart Grid مع التركيز على حماية الخصوصية. كما اقترحت الدراسة [13] إطارًا لسوق كهرباء لامركزي يعتمد على التعاون بين Blockchain و7] Edge Computing] [13]. وتناولت الدراسة [20] المصادقة المجهولة وإدارة المفاتيح في Smart Grid Edge Computing، مما يؤكد أهمية حماية هوية المستخدمين والأجهزة في هذا المجال [20].

كما ركزت الدراسة [25] على تطوير آلية مصادقة قائمة على Edge Computing لنظام تداول الطاقة الموزع المدعوم بالبلوكشين، وهو ما يوضح انتقال التطبيقات من مجرد تسجيل معاملات الطاقة إلى بناء أنظمة متكاملة للمصادقة والتداول [25].

وفي مجال الرعاية الصحية، يمكن لـ Edge Computing معالجة بيانات الأجهزة الطبية بالقرب من المريض، مما يقلل زمن إرسال البيانات إلى السحابة. وفي المقابل يمكن لـ Blockchain توفير سجل موثوق للبيانات والعمليات. وقد قدمت الدراسة

[11] إطارًا Blockchain-based Fog Computing للتعرف على النشاط ضمن تطبيقات الرعاية الصحية الإلكترونية [11]. كما قدمت الدراسة [2] إطارًا للحوسبة الطرفية المتنقلة في التطبيقات العلاجية الآمنة، مما يوضح أهمية الجمع بين المعالجة القريبة وأمن البيانات الصحية.

أما في المدن الذكية، فقد قدمت الدراسة [26] بنية تعتمد على Blockchain وEdge Computing لتطبيقات Smart City التشاركية، حيث تسمح Edge بمعالجة البيانات بالقرب من مصادرها، بينما تساعد Blockchain على بناء الثقة بين الأطراف المختلفة [26].

وتبرز في جميع هذه التطبيقات مشكلة الخصوصية، خصوصًا أن البيانات الصحية والطاقة والمعلومات الناتجة عن أجهزة المدن قد تكون حساسة. ولذلك اتجهت الدراسات إلى استخدام Permissioned Blockchain والمصادقة المجهولة والتحكم الدقيق في الوصول. وتقدم الدراسة [27] نموذجًا لمشاركة البيانات باستخدام Fine-Grained Access Control في أنظمة التخزين اللامركزية، وهو اتجاه يمكن تطبيقه على العديد من بيئات Smart City وHealthcare [27].

وبذلك تشترك هذه التطبيقات في الحاجة إلى سلامة البيانات، والهوية، والتحكم بالوصول، والخصوصية، والثقة، وزمن الاستجابة المنخفض. وتبرز Edge باعتبارها طبقة لمعالجة البيانات، بينما تعمل Blockchain كطبقة ثقة وتدقيق، مما يجعل التكامل بينهما مناسبًا لتطبيقات البنية التحتية الذكية.

10. التحديات والفجوات البحثية والاتجاهات المستقبلية

على الرغم من التطور الكبير في أبحاث Blockchain–Edge، ما تزال هناك تحديات تمنع الانتقال الكامل من النماذج البحثية إلى التطبيقات واسعة النطاق. وتتمثل أبرزها في محدودية موارد الأجهزة الطرفية، وقابلية التوسع، وزمن الإجماع، والتخزين، والخصوصية، والثقة، وإدارة الهوية والوصول، إضافة إلى التوافق بين المجالات المختلفة.

وقد أكدت الدراسة المنهجية [53] أن قابلية التوسع تمثل تحديًا متعدد الأبعاد، يرتبط بعدد العقد والإنتاجية وزمن التأخير والتخزين [53]. كما تؤكد الدراسات الحديثة في IIoT أن تحقيق الأمن والثقة وقابلية التوسع مع المحافظة على الأداء ما يزال تحديًا مفتوحًا [75]. ولذلك تتجه الأبحاث الحديثة إلى بناء حلول متكاملة تجمع Blockchain مع Edge وAI وآليات الثقة وإدارة الموارد.

1.10 التحديات التقنية والأمنية وقابلية التوسع:

يتمثل أحد أهم التحديات في محدودية موارد العقد الطرفية. فالأجهزة الطرفية قد تكون محدودة في الذاكرة والقدرة الحاسوبية والطاقة، بينما تتطلب Blockchain عمليات تخزين وتحقق وإجماع. وقد أوضحت الدراسة [35] أن هذه القيود تجعل تطبيق Blockchain التقليدية على الأجهزة المحمولة أمرًا صعبًا، ولذلك اقترحت توزيع عمليات Blockchain على Edge Nodes واستخدام Ledger مجزأ.

أما قابلية التوسع فتعد تحديًا متعدد الأبعاد. فالدراسة [53] تصنف التوسع إلى أفقي يتعلق بعدد المشاركين والعملاء، ورأسي يتعلق بالإنتاجية وزمن التأخير ومعدل إنشاء الكتل والتخزين [53]. وهذا يعني أن زيادة عدد العقد دون معالجة زمن الإجماع أو التخزين لا تحقق قابلية توسع حقيقية.

وتزداد مشكلة التخزين مع نمو دفتر الأستاذ. وقد عالجت الدراسة [62] هذه المشكلة من خلال Edge–Terminal Consensus Zones، بينما قدمت الدراسة [71] حلًا أكثر تطورًا يعتمد على Hierarchical Sharding، حيث توزع البيانات بين Cloud Chain وEdge Chain و[62] Terminal Layer [71]. ويسمح ذلك بتقليل تكرار البيانات وتحقيق توزيع أكثر توازنًا للموارد.

ومن الناحية الأمنية، لا تكفي Blockchain وحدها لحماية البيئة الطرفية؛ إذ قد تتعرض الأجهزة نفسها للاختراق أو انتحال الهوية أو سرقة المفاتيح أو التلاعب بالبيانات. وقد تناولت الدراسة [5] مجموعة واسعة من التهديدات في Blockchain–IoT، مما يؤكد ضرورة النظر إلى الأمن على مستوى النظام الكامل وليس على مستوى دفتر الأستاذ فقط [5].

كما تمثل الديناميكية تحديًا مهمًا، لأن عقد Edge قد تنضم إلى الشبكة أو تغادرها باستمرار. وقد صممت الدراسة [41] DR-

BFT لمعالجة هذه المشكلة تحديدًا، وأكدت أن آليات الإجماع التقليدية قد لا تكون مناسبة تمامًا للشبكات الديناميكية [41].

وتبرز كذلك مشكلة الخصوصية، لأن Blockchain توفر سجلًا دائمًا وقابلًا للتدقيق، بينما قد تكون بعض بيانات Edge حساسة أو شخصية. ولذلك تحتاج الأنظمة إلى الجمع بين التشفير، والـ Permissioned Blockchain، والتخزين خارج السلسلة، وآليات التحكم في الوصول.

ومن التحديات الأخرى Interoperability، خصوصًا عندما تتفاعل عدة شبكات Blockchain أو مجالات إدارية مستقلة. وتزداد هذه المشكلة في التطبيقات المركبية وG5 والمدن الذكية، حيث تتعدد الجهات والأجهزة والأنظمة.

وبالتالي، فإن التحدي الأساسي يتمثل في تحقيق توازن متزامن بين الأمن والأداء وقابلية التوسع والخصوصية. ولا يمكن معالجة هذه الأبعاد باستخدام آلية منفردة؛ بل تحتاج إلى تصميم معماري يجمع بين الإجماع المناسب، والتخزين الهرمي، والتجزئة، وإدارة الموارد، والتحكم بالوصول.

2.10 الفجوات البحثية في التحكم بالوصول والثقة وإدارة الموارد:

تكشف مراجعة الدراسات السابقة عن وجود تقدم واضح في المصادقة، وسلامة البيانات، وإدارة الثقة، وتخصيص الموارد، إلا أن هذه الجوانب غالبًا ما تُدرس بصورة منفصلة. وتظهر هنا فجوة بحثية مهمة تتمثل في تطوير إطار موحد يربط بين Access Control وTrust Management وResource Allocation في بيئة Blockchain–Edge.

في مجال التحكم بالوصول، قدمت الدراسة [27] نموذجًا يعتمد على Fine-Grained Access Control لمشاركة البيانات في أنظمة التخزين اللامركزية [27]. إلا أن بيئة Edge أكثر ديناميكية؛ إذ قد تتغير صلاحيات الأجهزة والمستخدمين والخدمات تبعًا للموقع وحالة الشبكة ونوع المهمة ومستوى الثقة. ولذلك فإن نماذج التحكم الثابتة قد لا تكون كافية للتعامل مع هذه البيئة.

كما قدمت الدراسات [19] و[20] حلولًا مرتبطة بالمصادقة وإدارة الهوية، لكنها تركز بصورة أكبر على إثبات هوية الأطراف بدل اتخاذ قرار وصول ديناميكي يعتمد على مجموعة واسعة من السمات [19] [20] [21]. ومن هنا تظهر أهمية نماذج مثل Attribute-Based Access Control (ABAC) التي يمكنها اتخاذ قرار الوصول بناءً على خصائص المستخدم والجهاز والبيئة والمورد.

أما إدارة الثقة فقد أصبحت محورًا رئيسيًا في الأنظمة الطرفية، لأن العقد قد تكون غير متجانسة وبعضها قد يتصرف بصورة غير موثوقة. وقد قدمت الدراسة [34] نموذجًا يجمع Resource Allocation مع Trust Computing، مما يمثل خطوة باتجاه ربط الثقة بإدارة الموارد [34]. كما ركزت الدراسة [37] على بناء نظام Blockchain–Edge لتعزيز الثقة في IoT، بينما قدمت الدراسة [66] آلية للأمن والثقة في IIoT المدعوم بالذكاء الاصطناعي [37] [66].

أما إدارة الموارد، فقد تناولتها دراسات متعددة باستخدام التعلم المعزز والألعاب والمزادات. فقد استخدمت الدراسة [22] Deep Reinforcement Learning للتعاون في Computation Offloading وResource Allocation، بينما تناولت الدراسة [33] مشاركة موارد MEC باستخدام Auction Game و[22] Blockchain [33]. كما قدمت الدراسات [45] و[46] و[67] و[76] نماذج مختلفة لتحسين تخصيص الموارد والـ offloading.

إلا أن الفجوة تتمثل في أن قرار تخصيص المورد غالبًا ما يُتخذ بناءً على الزمن والطاقة والحمل الحاسوبي، دون إدخال مستوى الثقة وسياسات الوصول والأمن بصورة متكاملة. وبالتالي يمكن أن يحصل جهاز ذو موارد جيدة على مورد معين رغم انخفاض مستوى الثقة فيه، وهو سيناريو يمثل خطرًا أمنيًا.

ومن هنا يمكن تحديد فجوة بحثية واضحة تتمثل في بناء إطار يجمع بين Blockchain-based Trust Management + ABAC + Smart Contracts + Resource Allocation. ويمكن للعقود الذكية تسجيل وتنفيذ سياسات الوصول، بينما تستخدم Blockchain لتوفير سجل تدقيق غير قابل للتلاعب، ويستخدم نموذج الثقة لتقييم العقد، وتستخدم خوارزميات التعلم أو التحسين لاختيار الموارد.

كما تحتاج الدراسات المستقبلية إلى اختبار هذه النماذج في بيئات أكبر وأكثر واقعية بدل الاعتماد على شبكات صغيرة أو

سيناريوهات مثالية. ولذلك تمثل قابلية التوسع، والديناميكية، وتعدد المجالات، وعدم تجانس الأجهزة مجتمعةً أهم التحديات التي ينبغي أخذها في الاعتبار عند تصميم نظام متكامل.

3.10 الاتجاهات المستقبلية والحلول البحثية المقترحة:

توضح الدراسات الحديثة أن اتجاه البحث ينتقل من مجرد دمج Blockchain مع Edge Computing إلى تطوير أنظمة ذكية، تكيفية، خفيفة وقابلة للتوسع. ويظهر هذا التحول في الدراسات التي تجمع Blockchain مع التعلم المعزز، والتجزئة، وإدارة الموارد، والذكاء الاصطناعي، وآليات الثقة [46] [53] [66].

أحد أهم الاتجاهات المستقبلية هو تطوير Adaptive Consensus، بحيث تتغير آلية الإجماع أو عدد العقد المشاركة تبعًا لحالة الشبكة. وتقدم الدراسة [41] مثالًا على التعامل مع الديناميكية من خلال DR-BFT، التي صممت للتعامل مع انضمام العقد ومغادرتها [41]. ويمكن تطوير هذا المفهوم مستقبلًا بحيث يتم اختيار مستوى الإجماع بناءً على مستوى الثقة وحجم المعاملات وقيود الطاقة.

والاتجاه الثاني هو Hierarchical Sharding. فقد قدمت الدراسة [71] نموذجًا هرميًا يجمع بين Cloud Chain و Edge Chain وTerminal Layer، مع تقسيم العقد إلى Shards بناءً على خصائص الأداء والقرب [71]. ويمكن تطوير هذه الفكرة مستقبلاً بحيث تصبح عملية تشكيل الـ Shards ديناميكية، فتتغير وفق الحمل وحالة الشبكة.

أما الاتجاه الثالث فيتمثل في دمج Blockchain وAI وEdge Computing. وتوضح الدراسات [22] و[28] و[46] و[66] إمكانية استخدام التعلم المعزز والذكاء الاصطناعي في تخصيص الموارد والـ offloading واكتشاف العقد غير الموثوقة [22] [28] [46] [66]. ويمكن توسيع ذلك ليشمل اختيار عقد الإجماع، وتقييم الثقة، والتنبؤ بالهجمات.

ومن الاتجاهات المهمة أيضًا Privacy-Preserving Access Control. ويمكن استخدام Smart Contracts لتنفيذ سياسات ABAC، مع إبقاء البيانات الحساسة خارج Blockchain وتسجيل الأدلة أو الـ hashes فقط على السلسلة. ويسمح ذلك بالاستفادة من التدقيق وعدم قابلية التلاعب دون تحميل Blockchain البيانات الحساسة بصورة مباشرة.

كما يمثل Cross-Domain Blockchain اتجاهًا مهمًا، خصوصًا في البيئات التي تضم أكثر من نطاق إداري. وتتناول الدراسة [61] نموذج Trusted Edge وCross-Domain Privacy Enhancement ضمن Multi-Blockchain، مما يوضح الحاجة إلى آليات تسمح بالتعاون بين المجالات المختلفة مع المحافظة على الخصوصية [61]. كما تزداد أهمية هذا الاتجاه في IoT، حيث تتبادل عدة مؤسسات البيانات والخدمات عبر شبكات مختلفة.

ويظهر كذلك اتجاه Resource-Efficient Blockchain، حيث توضح الدراسة [62] إمكانية نقل العبء الحسابي للإجماع إلى Cloud وتقليل التخزين في Edge [62]. ويمكن الجمع بين هذه الفكرة والتجزئة والتخزين خارج السلسلة للوصول إلى بنى أكثر كفاءة.

وأخيرًا، تتجه الدراسات الحديثة إلى التحسين متعدد الأهداف. فالدراسة [68] تركز على QoS-aware Task Scheduling، بينما تستخدم الدراسة [80] Many-Objective Evolutionary Algorithm لمعالجة Task Offloading في [68] Blockchain-secured Edge Computing [80]. ويشير ذلك إلى أن الأنظمة المستقبلية يجب ألا تهدف إلى تقليل التأخير فقط، بل إلى تحقيق توازن بين الأمن، والثقة، والطاقة، والتخزين، والإنتاجية، وزمن الاستجابة.

وبناءً على مجمل الدراسات، يمكن اقتراح اتجاه بحثي متكامل يتمثل في بناء Blockchain–Edge Framework يعتمد على Permissioned Blockchain، وABAC للتحكم الديناميكي بالوصول، وSmart Contracts لتنفيذ السياسات، ونموذج Trust Management لتقييم العقد، وSharding لتقليل أعباء التخزين والإجماع، وخوارزميات AI لتخصيص الموارد والـ offloading. ويبدو هذا الاتجاه مناسبًا بصورة خاصة للبيئات الديناميكية التي تجمع IoT وIIoT وEdge Computing، لأنه يعالج الفجوات التي تظهر عند دراسة الأمن والثقة والوصول وإدارة الموارد بصورة منفصلة.

المراجع

1. Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2018). When mobile blockchain meets edge computing. IEEE Communications Magazine, 56(8), 33–39. https://doi.org/10.1109/MCOM.2018.1701095
2. Rahman, M. A., Hossain, M. S., Loukas, G., Hassanain, E., Rahman, S. S., Alhamid, M. F., & Guizani, M. (2018). Blockchain-based mobile edge computing framework for secure therapy applications. IEEE Access, 6, 72469–72478. https://doi.org/10.1109/ACCESS.2018.2881246.
3. Xu, C., Wang, K., Li, P., Guo, S., Luo, J., Ye, B., & Guo, M. (2019). Making big data open in edges: A resource-efficient blockchain-based approach. IEEE Transactions on Parallel and Distributed Systems, 30(4), 870–882. https://doi.org/10.1109/TPDS.2018.2871449.
4. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. (2019). IEEE Communications Surveys & Tutorials, 21(2), 1508–1532. https://doi.org/10.1109/COMST.2019.2894727.
5. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the Internet of Things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), 2188–2204. https://doi.org/10.1109/JIOT.2018.2882794.
6. Zhou, Z., Wang, B., Dong, M., & Ota, K. (2020). Secure and efficient vehicle-to-grid energy trading in cyber physical systems: An integration of blockchain and edge computing. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 43–57. https://doi.org/10.1109/TSMC.2019.2896323.
7. Gai, K., Wu, Y., Zhu, L., Xu, L., & Zhang, Y. (2019). Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet of Things Journal, 6(5), 7992–8004. https://doi.org/10.1109/JIOT.2019.2904303.
8. Zhang, K., Zhu, Y., Maharjan, S., & Zhang, Y. (2019). Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things. IEEE Network, 33(5), 12–19. https://doi.org/10.1109/MNET.001.1800526.
9. Jayasinghe, U., Lee, G. M., MacDermott, Á., & Rhee, W. S. (2019). TrustChain: A privacy preserving blockchain with edge computing. Wireless Communications and Mobile Computing, 2019, Article 2014697. https://doi.org/10.1155/2019/2014697.
10. Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). FogBus: A blockchain-based lightweight framework for edge and fog computing. Journal of Systems and Software, 154, 22–36. https://doi.org/10.1016/j.jss.2019.04.050.
11. Din, I. U., Islam, N., Faheem, Y., Talha, M., & Guizani, M. (2019). A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services. Future Generation Computer Systems, 100, 569–578. https://doi.org/10.1016/j.future.2019.05.059.

12. Xu, Z., Geng, Q., Cao, H., Wang, C., Liu, X., et al. (2019). Uncertainty-aware workflow migration among edge nodes based on blockchain. EURASIP Journal on Wireless Communications and Networking, 2019, Article 250. https://doi.org/10.1186/s13638-019-1583-1.
13. Chen, S., et al. (2019). A framework of decentralized electricity market based on the collaborative mechanism of blockchain and edge computing. In Proceedings of the IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). https://doi.org/10.1109/SOLI48380.2019.8955023.
14. Liu, C. H., Lin, Q., & Wen, S. (2019). Blockchain-enabled data collection and sharing for Industrial IoT with deep reinforcement learning. IEEE Transactions on Industrial Informatics, 15(6), 3516–3526. https://doi.org/10.1109/TII.2018.2890203.
15. Fu, S., Fan, Q., Tang, Y., Zhang, H., Jian, X., & Zeng, X. (2019). Cooperative computing in integrated blockchain based Internet of Things. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2019.2948144.
16. Xu, X., Zhang, X., Gao, H., Xue, Y., Qi, L., & Dou, W. (2020). BeCome: Blockchain-enabled computation offloading for IoT in mobile edge computing. IEEE Transactions on Industrial Informatics, 16(6), 4187–4195. https://doi.org/10.1109/TII.2019.2936869.
17. Jindal, A., Aujla, G. S., & Kumar, N. (2019). SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. Computer Networks, 153, 36–48. https://doi.org/10.1016/j.comnet.2019.02.002.
18. Huang, J., Kong, L., Dai, H.-N., Ding, W., Cheng, L., Chen, G., Jin, X., & Zeng, P. (2020). Blockchain based mobile crowd sensing in industrial systems. IEEE Transactions on Industrial Informatics, 16(10), 6553–6563. https://doi.org/10.1109/TII.2019.2963728.
19. Liu, H., Zhang, P., Pu, G., Yang, T., Maharjan, S., & Zhang, Y. (2020). Blockchain empowered cooperative authentication with data traceability in vehicular edge computing. IEEE Transactions on Vehicular Technology. https://doi.org/10.1109/TVT.2020.2969722.
20. Wang, J., Wu, L., Choo, K.-K. R., & He, D. (2020). Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Transactions on Industrial Informatics, 16(3), 1984–1992. https://doi.org/10.1109/TII.2019.2936278.
21. Guo, S., Hu, X., Guo, S., Qiu, X., & Qi, F. (2020). Blockchain meets edge computing: A distributed and trusted authentication system. IEEE Transactions on Industrial Informatics, 16(3), 1972–1983.
22. Feng, J., Yu, F. R., Pei, Q., Chu, X., Du, J., & Zhu, L. (2020). Cooperative computation offloading and resource allocation for blockchain-enabled mobile edge computing: A deep reinforcement learning approach. IEEE Internet of Things Journal, 7(7), 6214–6228.

23. Guan, Z., Lyu, H., Li, D., Hei, Y., & Wang, T. (2020). Blockchain: A distributed solution to UAV-enabled mobile edge computing. IET Communications, 14(15), 2420–2426. https://doi.org/10.1049/iet-com.2019.1131.

24. Feng, J., Yu, F. R., Pei, Q., Du, J., & Zhu, L. (2020). Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems. IEEE Transactions on Wireless Communications, 19(6), 4321–4334. https://doi.org/10.1109/TWC.2020.2982627.

25. Ren, Y., Zhao, Q., Guan, H., & Lin, Z. (2020). A novel authentication scheme based on edge computing for blockchain-based distributed energy trading system. EURASIP Journal on Wireless Communications and Networking, 2020, Article 152. https://doi.org/10.1186/s13638-020-01762-w.

26. Khan, Z. A., Abbasi, A. G., & Pervez, Z. (2020). Blockchain and edge computing-based architecture for participatory smart city applications. Concurrency and Computation: Practice and Experience, 32(12), e5566. https://doi.org/10.1002/cpe.5566.

27. Blockchain-based data sharing with fine-grained access control in decentralized storage systems. (2020).

28. Qiu, C., Yu, F. R., Yao, H., Jiang, C., Xu, F., & Zhao, C. (2019). Blockchain-based software-defined industrial Internet of Things: A dueling deep Q-learning approach. IEEE Internet of Things Journal, 6(3), 4627–4639. https://doi.org/10.1109/JIOT.2018.2871394.

29. Dai, Y., Xu, D., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks. IEEE Transactions on Vehicular Technology, 69(4), 4312–4324. https://doi.org/10.1109/TVT.2020.2973705.

30. Chai, H., Leng, S., Chen, Y., & Zhang, K. (2020). A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems. https://doi.org/10.1109/TITS.2020.3002712.

31. Buda, S., Wu, C., Bao, W., Guleng, S., et al. (2020). Empowering blockchain in vehicular environments with decentralized edges. IEEE Access, 8, 202032–202041. https://doi.org/10.1109/ACCESS.2020.3036399.

32. Zhang, J., Lu, C., Cheng, G., Guo, T., Kang, J., Zhang, X., Yuan, X., & Yan, X. (2021). A blockchain-based trusted edge platform in edge computing environment. Sensors, 21(6), 2126. https://doi.org/10.3390/s21062126.

33. Zhang, X., Zhu, X., Chikuvanyanga, M. A. M., et al. (2021). Resource sharing of mobile edge computing networks based on auction game and blockchain. EURASIP Journal on Advances in Signal Processing, 2021, Article 26. https://doi.org/10.1186/s13634-021-00735-5.

34. Resource allocation and trust computing for blockchain-enabled edge computing system. (2021). Computers & Security, 105, 102249. https://doi.org/10.1016/j.cose.2021.102249.

35. Xie, Q., Dong, F., & Feng, X. (2021). ECLB: Edge-computing-based lightweight blockchain framework for mobile systems. Security and Communication Networks, 2021, Article 5510586. https://doi.org/10.1155/2021/5510586.

36. Liu, L., Feng, J., Pei, Q., Chen, C., Ming, Y., Shang, B., & Dong, M. (2021). Blockchain-enabled secure data sharing scheme in mobile-edge computing: An asynchronous advantage actor–critic learning approach. IEEE Internet of Things Journal, 8(4), 2342–2353.

37. Dai, H., Shi, P., Huang, H., Chen, R., et al. (2021). Towards trustworthy IoT: A blockchain-edge computing hybrid system with proof-of-contribution mechanism. Security and Communication Networks, 2021, Article 3050953. https://doi.org/10.1155/2021/3050953.

38. Zuo, Y., Jin, S., Zhang, S., Han, Y., & Wong, K. K. (2021). Delay-limited computation offloading for MEC-assisted mobile blockchain networks. IEEE Transactions on Communications, 69(12), 8569–8584. https://doi.org/10.1109/TCOMM.2021.3113390.

39. Luo, S., Li, H., Wen, Z., Qian, B., Morgan, G., Longo, A., Rana, O., & Ranjan, R. (2021). Blockchain-based task offloading in drone-aided mobile edge computing. IEEE Network, 35(1), 124–129. https://doi.org/10.1109/MNET.011.2000222.

40. Gao, L., Wu, C., Yoshinaga, T., Chen, X., & Ji, Y. (2021). Multi-channel blockchain scheme for Internet of Vehicles. IEEE Open Journal of the Computer Society, 2, 192–203. https://doi.org/10.1109/OJCS.2021.3070714.

41. DR-BFT: A consensus algorithm for blockchain-based multi-layer data integrity framework in dynamic edge computing system. (2021). Future Generation Computer Systems, 124, 33–48. https://doi.org/10.1016/j.future.2021.04.020.

42. Wang, J., Wu, L., Choo, K.-K. R., & He, D. (2021). Blockchain enabled verification for cellular-connected unmanned aircraft system networking. Future Generation Computer Systems, 123, 233–244. https://doi.org/10.1016/j.future.2021.05.002.

43. Wu, Y., Dai, H. N., & Wang, H. (2021). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in Industry 4.0. IEEE Internet of Things Journal, 8(4), 2300–2317. https://doi.org/10.1109/JIOT.2020.3025916.

44. Jiang, M., & Qin, X. (2022). Distributed ledger technologies in vehicular mobile edge computing: A survey. Complex & Intelligent Systems, 8, 4403–4419. https://doi.org/10.1007/s40747-021-00603-7.

45. Resource allocation on blockchain enabled mobile edge computing system. (2022).

46. Hu, Z., Gao, H., Wang, T., et al. (2022). Joint optimization for mobile edge computing-enabled blockchain systems: A deep reinforcement learning approach. Sensors, 22(9), 3217. https://doi.org/10.3390/s22093217.

47. Blockchain-enabled approach for big data processing in edge computing. (2022).

48. K., P., Chandana, S. L., Samaniego, S. S. C., Chaudhary, D. M. G., Vekariya, D. V., & Chaturvedi, M. A. (2022). Intelligent mobile edge computing integrated with blockchain security analysis for millimetre-wave communication. International Journal of Communication Networks and Information Security, 14(3), 110–122. https://doi.org/10.17762/ijcnis.v14i3.5577.

49. Vladyko, A., Elagin, V., Spirkina, A., Muthanna, A., & Ateya, A. A. (2022). Distributed edge computing with blockchain technology to enable ultra-reliable low-latency V2X communications. Electronics, 11(2), 173. https://doi.org/10.3390/electronics11020173.

50. Wu, J., Haider, S. A., Soni, M., Kalra, A., & Deb, N. (2022). Blockchain based energy efficient multi-tasking optimistic scenario for mobile edge computing. PeerJ Computer Science, 8, e1118. https://doi.org/10.7717/peerj-cs.1118.

51. Xia, C., Wu, Y., Chen, L., Chen, Y., & Wu, J. (2022). Three-stage auction scheme for computation offloading on mobile blockchain with edge computing. Concurrency and Computation: Practice and Experience, 34(25), e7253. https://doi.org/10.1002/cpe.7253.

52. Strategy for dynamic blockchain construction and transmission in novel edge computing networks. (2022).

53. Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2022). Scalable blockchains—A systematic review. Future Generation Computer Systems, 126, 136–162. https://doi.org/10.1016/j.future.2021.07.035.

54. Xue, H., Chen, D., Zhang, N., Dai, H.-N., & Yu, K. (2023). Integration of blockchain and edge computing in Internet of Things: A survey. Future Generation Computer Systems, 144, 307–326. https://doi.org/10.1016/j.future.2022.10.029.

55. Baranwal, G., Kumar, D., & Vidyarthi, D. P. (2023). Blockchain based resource allocation in cloud and distributed edge computing: A survey. Computer Communications, 209, 469–498. https://doi.org/10.1016/j.comcom.2023.07.023.

56. Gao, Q., Xiao, J., Cao, Y., Deng, S., Ouyang, C., & Feng, Z. (2023). Blockchain-based collaborative edge computing: Efficiency, incentive and trust. Journal of Cloud Computing, 12, 72. https://doi.org/10.1186/s13677-023-00452-4.

57. Alzubi, J. A. (2023). A blockchain-enabled security management framework for mobile edge computing. International Journal of Network Management, 33(5), e2240. https://doi.org/10.1002/nem.2240.

58. Wang, S., Liu, Z., Wang, H., et al. (2023). Ensuring security in edge computing through effective blockchain node detection. Journal of Cloud Computing, 12, 88. https://doi.org/10.1186/s13677-023-00466-y.

59. Guha Roy, D. (2023). BlockEdge: A privacy-aware secured edge computing framework using blockchain for Industry 4.0. Sensors, 23(5), 2502. https://doi.org/10.3390/s23052502

60. Almstedt, L., Bleeke, K., Mahhouk, M., Jehl, L., Kapitza, R., & Wolf, L. (2023). ContractBox: Realizing accountable data sharing on the edge using a small scale blockchain. Computer Networks, 229, 109768. https://doi.org/10.1016/j.comnet.2023.109768.

61. Huang, M., Yuan, L., Pan, X., & Zhou, C. (2023). Trusted edge and cross-domain privacy enhancement model under multi-blockchain. Computer Networks, 234, 109881. https://doi.org/10.1016/j.comnet.2023.109881.

62. Wang, K., Tu, Z., Ji, Z., & He, S. (2023). Faster service with less resource: A resource efficient blockchain framework for edge computing. Computer Communications, 199, 196–209. https://doi.org/10.1016/j.comcom.2022.12.014.

63. Lai, R., & Zhao, G. (2023). Blockchain for achieving accountable outsourcing computations in edge computing. Computer Communications, 200, 17–29. https://doi.org/10.1016/j.comcom.2022.12.024.

64. Cooperative task scheduling secured with blockchain in sustainable mobile edge computing. (2023). Sustainable Computing: Informatics and Systems, 37, 100843. https://doi.org/10.1016/j.suscom.2022.100843.

65. Jin, W., Xu, Y., Dai, Y., & Xu, Y. (2023). Blockchain-based continuous knowledge transfer in decentralized edge computing architecture. Electronics, 12(5), 1154. https://doi.org/10.3390/electronics12051154.

66. A blockchain-based security and trust mechanism for AI-enabled IIoT systems. (2023). Future Generation Computer Systems, 146, 78–85. https://doi.org/10.1016/j.future.2023.03.011.

67. Zhang, W., Fan, Y., Zhang, J., Ding, X., & Kim, J. Y. (2024). Computing resource allocation for blockchain-based mobile edge computing. Computer Modeling in Engineering & Sciences, 140(1), 863–885. https://doi.org/10.32604/cmes.2024.047295

68. SharpEdge: A QoS-driven task scheduling scheme with blockchain in mobile edge computing. (2024).

69. Wu, J., Bu, X., Li, G., & Tian, G. (2024). Data privacy protection model based on blockchain in mobile edge computing. Software: Practice and Experience, 54(9), 1671–1696. https://doi.org/10.1002/spe.3315.

70. Rahmani, A. M., Tanveer, J., Soleimanian Gharehchopogh, F., Rajabi, S., & Hosseinzadeh, M. (2024). A novel offloading strategy for multi-user optimization in blockchain-enabled Mobile Edge Computing networks for improved Internet of Things performance. Computers & Electrical Engineering, 119, 109514. https://doi.org/10.1016/j.compeleceng.2024.109514.

71. Li, C., Pan, H., Qian, H., Li, Y., Si, X., Li, K., & Zhang, B. (2024). Hierarchical sharding blockchain storage solution for edge computing. Future Generation Computer Systems, 161, 162–173. https://doi.org/10.1016/j.future.2024.06.048.

72. Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications. (2024).

73. Bozkaya-Aras, E. (2024). Blockchain-based secure content caching and computation for edge computing. IEEE Access, 12, 47619–47629. https://doi.org/10.1109/ACCESS.2024.3383474.

74. Alnahdi, A., & Toka, L. (2024). A survey on integrating edge computing with AI and blockchain in maritime domain, aerial systems, IoT, and Industry 4.0. IEEE Access, 12, 28684–28709. https://doi.org/10.1109/ACCESS.2024.3367118.

75. Asaithambi, S., Nallusamy, S., Yang, J., Prajapat, S., Kumar, G., & Rathore, P. S. (2025). A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things. Scientific Reports, 15, 15410. https://doi.org/10.1038/s41598-025-00337-3.

76. Valitabar, M., Fathi, M., & Navaie, K. (2025). Efficient resource allocation for blockchain-enabled mobile edge computing: A joint optimization approach. IEEE Access, 13, 129011–129023. https://doi.org/10.1109/ACCESS.2025.3590431.

77. Reis, M. J. C. S. (2025). Blockchain-enhanced security for 5G edge computing in IoT. Computation, 13(4), 98. https://doi.org/10.3390/computation13040098.

78. Blockchain-enabled cross-domain IoT data sharing: A lightweight, secure edge-assisted approach. (2025).

79. Energy-efficient blockchain-IIoT with mobile edge computing: Optimizing resource allocation and multi-hop offloading. (2025). Results in Engineering, 26, 105379. https://doi.org/10.1016/j.rineng.2025.105379.

80. Efficient complex task offloading in blockchain-secured edge computing using a many-objective evolutionary algorithm. (2026). Future Generation Computer Systems, 174, 107937. https://doi.org/10.1016/j.future.2025.107937.