

المسابقة الاستثنائية للبحث العلمي في مجال الرقابة الخاصة بخمسينية المنظمة العربية للأجهزة العليا
للرقابة المالية والمحاسبة (الأرابوساي)

بحث حول موضوع:

تصميم معمارية هجينة لأتمتة المشتريات العامة بالاعتماد على بلوكتشين
التحالف وانترنت الأشياء

**Design of a Hybrid Architecture for Automating Public
Procurement Based on Consortium Blockchain and IoT**

إعداد:

المهندسة ريم تموز

المهندسة آلاء عجيب

الجهاز المركزي للرقابة المالية في سوريا

كلمة شكر

نود في بداية هذا البحث أن نتقدم بجزيل الشكر إلى المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة لتنظيمهم المسابقة الاستثنائية للبحث العلمي في مجال الرقابة الخاصة بخمسينية المنظمة لما لها من أهمية في دفع عجلة البحث العلمي الرقابي وفتح آفاق الابتكار أمام الكوادر العربية لتقديم حلول تقنية ومنهجية تساهم في تعزيز مبادئ الشفافية والحوكمة بما يواكب التطورات العالمية المتسارعة في هذا المجال.

كما نتقدم بجزيل الشكر والعرفان إلى رئاسة وإدارة الجهاز المركزي للرقابة المالية في الجمهورية العربية السورية المظلة المهنية التي نفتخر بالانتماء إليها على توفير البيئة الداعمة التي تحفز المشاركين على البحث والتطوير، والشكر موصول إلى كل من ساهم في تقديم يد العون.

الملخص (Abstract)

تُعد إدارة المشتريات العامة من أهم الركائز الاقتصادية للمؤسسات الحكومية، إلا أنها تعاني بنيوياً من مركزية البيانات، والبيروقراطية المستنزفة للوقت، وتنامي مخاطر التواطؤ والتلاعب بالسجلات. استجابةً لهذه التحديات، تقترح هذه الدراسة تصميمًا معماريًا هجيناً ونموذج محاكاة متقدم لرقمنة وأتمتة منظومة المشتريات العامة، بالاعتماد على تكامل تقنية "بلوكتشين التحالف" (Consortium Blockchain) مع تقنيات إنترنت الأشياء (BIoT) وخوارزميات الذكاء الاصطناعي اللامركزية.

تتألف الهيكلية المعمارية المقترحة من أربع طبقات مترابطة تهدف إلى تحويل بيئة المشتريات من المركزية الإدارية القابلة للاختراق إلى موثوقة الخوارزميات الحتمية. يعتمد النظام على العقود الذكية (Smart Contracts) وآلية "إثبات السلطة" (PoA) لتسريع معالجة العطاءات، مع حل "معضلة الأوراكل" (The Oracle Problem) عبر ربط السجلات الموزعة بمستشعرات العالم المادي لضمان شفافية الاستلام والتسليم. ولتوفير طبقة رقابة استباقية، تم دمج خوارزميات "التعلم الموحد" (Federated Learning) لاكتشاف حالات الشذوذ والتواطؤ في العطاءات، مع حماية أسرار الموردين باستخدام تقنية "إثبات المعرفة الصفرية" (ZKPs).

ولإثبات الجدوى التقنية والأمنية لهذا التصميم، تم إخضاع النموذج لاختبارات أداء قياسية ضمن بيئة محاكاة معزولة باستخدام أداة (Hyperledger Caliper).

أظهرت مقاييس الأداء كفاءة هندسية عالية، حيث سجلت الشبكة إنتاجية بلغت 3000 معاملة في الثانية (TPS) بزمن استجابة منخفض، مما يؤكد قدرة الخوارزمية على استيعاب أحمال العمل الحكومية المترامنة دون حدوث اختناقات في معالجة البيانات.

تخلص الدراسة إلى أن تبني هذه المعمارية الهجينة لا يمثل مجرد تحديث تقني، بل هو تحول استراتيجي ينقل العمل الرقابي من "التدقيق اللاحق" إلى "الحوكمة الاستباقية المؤتمتة"، مما يضمن سيادة القانون رقمياً، ويؤسس لبيئة مشتريات عامة شفافة، وأمنة، ومستدامة.

الكلمات المفتاحية: المشتريات العامة، بلوكتشين التحالف (Consortium Blockchain)، العقود الذكية، إنترنت الأشياء (BIoT)، التعلم الموحد (Federated Learning)، معضلة الأوراكل، إثبات المعرفة الصفرية (ZKP).

جدول المحتويات:

3	الملخص (Abstract).....
6	فهرس الأشكال.....
7	فهرس الجداول.....
8	مقدمة:.....
8	مشكلة البحث.....
11	منهجية البحث.....
12	الفصل الأول:.....
12	دراسة نظرية لتوصيف واقع المشتريات العامة وأهمية الانتقال لاستخدام البلوكتشين.....
13	1-1: مقدمة في التحول الرقمي في القطاع الحكومي.....
13	2-1: دورة المشتريات العامة في المؤسسات:.....
15	1-2-1: التحديات التقليدية في المشتريات العامة.....
18	3-1: لماذا نحتاج Blockchain ؟.....
21	1-3-1: ما المقصود بتقنية سلسلة الكتل؟.....
26	2-3-1: سجلات التوزيع.....
27	3-3-1: تقنية التجزئة (تابع الهاش).....
29	4-3-1: ما هي العقود الذكية؟.....
30	5-3-1: ما هو Dapp ؟.....
30	6-3-1: كيف تعمل التطبيقات اللامركزية؟.....
31	4-1: كيف تتعامل الشركات مع دمج تقنية البلوكتشين في المشتريات؟.....
31	1-4-1: تحديد الاستخدامات المثلى لتقنية البلوكتشين.....
31	2-4-1: اختيار المنصة المناسبة.....
32	3-4-1: التطوير والاختبار.....
32	4-4-1: التكامل مع الأنظمة القائمة.....
32	5-4-1: التدريب والتوعية.....
32	5-1: تكامل البلوكتشين مع إنترنت الأشياء (BloT) وحل معضلة الأوراكل (The Oracle Problem).....
33	6-1: التحديات الرئيسية لاستخدام تقنية البلوكتشين والعقود الذكية في المشتريات.....
34	1-6-1: كيفية التعامل مع تحديات استخدام البلوكتشين والعقود الذكية في المشتريات.....
35	7-1: الخاتمة.....
36	الفصل الثاني:.....

36	الهيكلية المعمارية الهجينة لنظام المشتريات العامة المؤتمت (نموذج محاكاة)
37	1-2: مقدمة الفصل:
38	2-2: الطبقة الأولى: البنية التحتية للبلوكتشين التحالف (Consortium Blockchain Layer)
38	1-2-2: المكونات الهيكلية للشبكة (Network Topology)
38	2-2-2: الآلية الرياضية للتشفير والربط (Cryptographic Hashing Mechanism)
40	3-2-2: دورة حياة المعاملة برمجياً (Transaction Flow) في العطاءات
40	4-2-2: خصوصية الموردين باستخدام إثبات المعرفة الصفرية (Zero-Knowledge Proofs – ZKPs)
41	5-2-2: إدارة هويات الموردين عبر الهوية الذاتية اللامركزية (Self-Sovereign Identity – SSI)
42	3-2: الطبقة الثانية: شبكات الأوراكل اللامركزية وإنترنت الأشياء (BioT & Decentralized Oracles Layer)
42	1-3-2: معضلة الانعزال (The Oracle Problem) في المشتريات العامة
42	2-3-2: معمارية إنترنت الأشياء (BioT) كمصدر للبيانات
43	3-3-2: آلية الإجماع اللامركزي للأوراكل (Decentralized Oracle Consensus)
44	4-3-2: محاكاة برمجية للعقد الذكي (Smart Contract Simulation)
48	5-3-2: تحليل الأداء في المحاكاة
48	4-2: الطبقة الثالثة: طبقة تحليل البيانات والتعلم اللامركزي (Data Analytics & Federated Learning Layer)
48	1-4-2: التحدي التحليلي في المشتريات العامة
48	2-4-2: هيكلية التعلم الموحد لاكتشاف التواطؤ (Collusion Detection Architecture)
50	3-4-2: الصياغة الرياضية لنموذج اكتشاف الشذوذ (Anomaly Detection Model)
51	4-4-2: تقييم الموردين البيئي والديناميكي (Dynamic Green Scoring)
52	5-2: الطبقة الرابعة: الأمن السيبراني ونمذجة التهديدات (Cybersecurity & Threat Modeling)
52	1-5-2: هجوم "تسميم البيانات" على طبقة الأوراكل (Data Poisoning Attack)
53	2-5-2: هجوم "التحكم في الأغلبية" أو التواطؤ (Sybil / 51% Attack)
53	3-5-2: تأمين العقود الذكية باستخدام التحقق الرسمي (Formal Verification)
54	6-2: التكامل والتشغيل البيئي مع الأنظمة الحكومية الموروثة
55	7-2: التقييم المعماري الشامل (Comprehensive Architectural Evaluation)
56	8-2: خاتمة الفصل (Chapter Summary)
57	الفصل الثالث:
57	مناقشة أداء الهيكلية والتوصيات المستقبلية
58	1-3: مقدمة الفصل الثالث:
58	2-3: محددات بيئة المحاكاة ومقاييس الأداء (Simulation Environment & Metrics)

59	1-2-3: أدوات القياس المعيارية منصة (Hyperledger Caliper)
59	2-2-3: مواصفات البنية التحتية للمحاكاة (Hardware & Infrastructure Specifications)
60	3-3: تحليل الأداء التقني للنظام (Technical Performance Analysis)
60	1-3-3: كفاءة الإنتاجية وسرعة المعالجة (Throughput Efficiency)
61	2-3-3: تحليل زمن الاستجابة (Latency Analysis)
61	3-3-3: فعالية خوارزميات التدقيق واكتشاف الشذوذ (Anomaly Detection Effectiveness)
61	4-3-3: العبء الحسابي لتقنيات الخصوصية وتأثيرها على الأداء
62	5-3-3: تحليل استهلاك الموارد وتكلفة تنفيذ العقود الذكية
63	4-3: تحليل حالات الإخفاق واختناقات النظام (Failure Cases & System Bottlenecks)
63	1-4-3: إخفاق شبكات الأوراكل وانقطاع تدفق البيانات (Oracle Network Failure)
63	2-4-3: اختناقات التوسع وتضخم دفتر الأستاذ (Scalability & Ledger Bloat)
64	3-4-3: اختناقات التعلم الموحد: العبء الحسابي وتباين سرعات الشبكة (Federated Learning Bottlenecks)
65	4-4-3: الثغرات البرمجية في العقود الذكية والتدقيق الثابت (Smart Contract Vulnerabilities)
65	5-4-3: مصفوفة تقييم المخاطر (Risk Assessment Matrix)
66	5-3: التوافقية المعمارية والتكامل العكسي (Interoperability with Legacy Systems):
67	6-3: الخاتمة (Conclusion)
67	7-3: التوصيات المستقبلية للبحث (Future Work)
68	المراجع Reference:

فهرس الأشكال

الشكل
الشكل (1-1): كيفية تغير نتيجة تابع الهاش عند تغيير الكود المدخل في المرات الثلاث
الشكل (2-2): مخطط الهيكلية المعمارية الشاملة (System Architecture)
الشكل (3-2): مخطط شجرة ميركل (Merkle Tree Diagram)
الشكل (4-2): مخطط تدفق إثبات المعرفة الصفرية (ZKP Flow)
الشكل (5-2): مخطط تدفق الأوراكل وإنترنت الأشياء (BioT Flow)
الشكل (6-2): مخطط التسلسل للعقد الذكي (UML Sequence)
الشكل (7-2): الجزء الأول من كود Solidity
الشكل (8-2): الجزء الثاني من كود Solidity
الشكل (9-2): كود Python الممثل لخوارزمية الاجماع اللامركزي

الشكل (2-10): مخطط التعلم الموحد (Federated Learning)
الشكل (2-11): كود Python ليقوم باكتشاف الشذوذ والتلاعب في الأسعار
الشكل (2-12): مخطط الطبقة الوسيطة (API Middleware)
الشكل (3-13): العلاقة بين معدل إرسال المعاملات وزمن الاستجابة في بيئة بلوكتشين التحالف
الشكل (3-14): مقارنة العبء الحسابي والزمني بين توليد برهان المعرفة الصفريّة (Off-chain) والتحقق منه (On-chain)
الشكل (3-15): أثر معمارية التعلم غير المتزامن على تقليص إجمالي زمن التدريب للنماذج الرقابية مقارنة بالنهج المتزامن

فهرس الجداول

الجدول
الجدول (1-1): أهم المزايا التي تقدمها البلوكتشين
الجدول (1-2): مقارنة بين آلية SHA-256 للتشفير وخوارزمية التجزئة
جدول (2-3): الرموز الرياضية المستخدمة في نمذجة خوارزميات الأوراكل
الجدول (2-4): الفروقات الجوهرية على المستويين البنيوي والخوارزمي
الجدول (3-5): محددات بيئة المحاكاة
الجدول (3-6): المواصفات التقنية للعتاد الصلب
الجدول (3-7): مصفوفة تقييم المخاطر وحالات الإخفاق في النموذج المؤتمت

مقدمة:

تُعد المشتريات العامة المحرك الأساسي للنشاط الاقتصادي الحكومي والقناة الأكبر للإنفاق؛ حيث تشير تقارير منظمة التعاون الاقتصادي والتنمية إلى أنها تمثل حوالي 12% من الناتج المحلي الإجمالي في الدول المتقدمة، وتصل إلى نحو 30% في الدول النامية. وبالرغم من هذا الثقل الاقتصادي، لا تزال هذه المنظومة تعاني من فجوات بنيوية تتعلق بسلامة البيانات ومركزية القرار؛ إذ تُقدّر الأمم المتحدة أن الفساد والهدر في المشتريات قد يكلف العالم ما يقارب 2 تريليون دولار سنوياً.

من هنا تبرز ضرورة الملحة لتبني التحول الرقمي في القطاع الحكومي، والذي يُعرف بأنه التّبنى الاستراتيجي للتقنيات الرقمية والرؤى القائمة على البيانات لتحديث العمليات وتعزيز الشفافية والمساءلة. إن دمج تقنيات الجيل الثالث من الويب، وتحديدًا تقنية البلوكتشين (Blockchain)، يمثل الحل الاستراتيجي الأمثل لمعالجة تحديات المشتريات؛ فهي توفر سجل حسابات غير قابل للتغيير يسمح بمتابعة الطلبات والمدفوعات والمعاملات بدقة زمنية فائقة. علاوة على ذلك، تتيح العقود الذكية (Smart Contracts) أتمتة الإجراءات التعاقدية وتنفيذها تلقائياً فور استيفاء الشروط المحددة، مما يقلل التدخل البشري ويقضي على البيروقراطية والاحتياال. وبذلك، لا يقتصر دور هذا التحول على تحسين كفاءة الإنفاق المالي فحسب، بل يمتد ليشمل بناء الثقة مع المواطنين وحماية المعلومات الحساسة من التهديدات السيبرانية.

مشكلة البحث

كيف يمكن تصميم هيكلية معمارية هجينة ومتكاملة تعتمد على تقنية البلوكتشين لمعالجة تحديات الفساد وانعدام الكفاءة في المشتريات العامة، مع تجاوز العقبات التقنية المتعلقة بخصوصية البيانات الحكومية، وموثوقية ربط العالم المادي بالعالم الرقمي، وتحليل البيانات المعزولة؟

ويتفرع من هذا التساؤل الرئيسي التساؤلات الفرعية الآتية:

1. كيف يمكن الاستعاضة عن البلوكتشين العام بـ "بلوكتشين تحالفي (Consortium Blockchain)" مدعوم بتقنية "إثبات المعرفة الصفرية (ZKPs)" لضمان شفافية المناقصات وحماية الأسرار التجارية والمالية للموردين في آن واحد؟

2. ما هو دور دمج تقنيات إنترنت الأشياء (IoT) وشبكات الأوراكل اللامركزية في حل "معضلة الانعزال" لأئمة عمليات الاستلام المادي والدفع المالي الموثوق دون تدخل بشري؟

3. كيف يمكن توظيف خوارزميات "التعلم الموحد (Federated Learning)" كطبقة تحليل ذكية لاكتشاف الشذوذ والتواطؤ في الأسعار، دون الحاجة لنقل أو كشف البيانات الحساسة للوزارات؟

ما هي الآليات المثلى لضمان التشغيل البيني (Interoperability) بين معمارية البلوكتشين اللامركزية المقترحة والأنظمة الحكومية المركزية الموروثة (Legacy Systems) لتقليل تكاليف الانتقال التقني؟

أهداف البحث

الهدف الرئيسي: تصميم هيكلية معمارية هجينة ومؤتمتة للمشتريات العامة، تدمج بين "بلوكتشين التحالف" (Consortium Blockchain)، وإنترنت الأشياء (BIoT)، والتعلم الموحد اللامركزي، لرفع كفاءة الإنفاق الحكومي والقضاء على الاحتيال والبيروقراطية.

الأهداف الفرعية:

1. **تشخيص تحديات المشتريات التقليدية:** تقييم الفجوات الحالية، وتحديد الهدر المالي، وتأخر المدفوعات، وضعف دقة البيانات.
2. **بناء نموذج محاكاة متعدد الطبقات:** تصميم شبكة بلوكتشين لا مركزية مكونة من أربع طبقات (بنية تحتية، أوراكل، تحليل ذكي، وأمن سيبراني) لأئمة العقود الذكية بأمان.

3. حماية خصوصية الموردين: توظيف تقنية "إثبات المعرفة الصفريّة" (ZKPs) والهويات اللامركزية للتحقق من الأهلية المالية دون كشف الأسرار التجارية.

4. ربط العقود الذكية بالعالم المادي: حل "معضلة الانعزال" عبر دمج مستشعرات إنترنت الأشياء (IoT) لتأكيد استلام البضائع مادياً وتحرير الدفعات المالية آلياً.

5. مكافحة الفساد استباقياً: توظيف خوارزميات "التعلم الموحد" (Federated Learning) لاكتشاف التواطؤ والتلاعب السعري، مع الحفاظ التام على سرية بيانات الوزارات.

أهمية البحث

أولاً: الفصل الأول

- تقديم هيكلية معمارية هجينة: يسد البحث فجوة تقنية عبر تصميم نموذج محاكاة متقدم يدمج بين شبكات البلوكتشين التحالفية (Consortium Blockchain)، وإنترنت الأشياء (BIoT)، وخوارزميات التعلم الموحد (Federated Learning).
- معالجة القيود التقنية المعقدة: يقدم حلولاً مبتكرة لتجاوز "معضلة الانعزال" (The Oracle Problem) لربط العقود الذكية بالواقع المادي، مع حماية البيانات الحساسة والأسرار التجارية باستخدام تقنية "إثبات المعرفة الصفريّة" (ZKPs).

ثانياً: الفصل الثاني (التطبيق العملي)

- الحد من الهدر المالي ومكافحة الفساد: يوفر النظام المقترح حلاً جذرياً لمواجهة التلاعب والاحتيال في المشتريات العامة.
- أتمتة العمليات ورفع الكفاءة: يساهم في تقليص البيروقراطية وتكاليف التدقيق المالي من خلال التنفيذ الآلي للشروط التعاقدية والدفعات عبر "العقود الذكية" دون تدخل بشري.

- التشغيل البيئي وقابلية التطبيق الميداني: يطرح البحث تصميمًا مرئيًا يعتمد على واجهات برمجة التطبيقات (APIs) للتكامل السلس مع الأنظمة الحكومية المركزية الموروثة (Legacy Systems)، مما يقلل من تكاليف إعادة الهيكلة الرقمية.

منهجية البحث

لتوصيف واقع المشتريات العامة التقليدية وتأسيس المفاهيم التقنية كالبلوكتشين، آليات الاجماع، والعقود الذكية تم استخدام المنهج الوصفي التحليلي Descriptive Analytical Method.

أما في الفصل الثاني ونظرًا للقيود التي تمنع التطبيق المباشر على بنية حكومية حقيقية تم الاعتماد على نموذج محاكاة هجين Hybrid Simulation Model وهو ما يمثل منهج النمذجة والمحاكاة (Simulation and Modeling Approach) .

ثم أخيرا تم استخدام المنهج المقارن Comparative Method لإجراء تحليل تقاطعي وتقييم مقارن Benchmarking بين البنى التحتية المركزية التقليدية (المعتمدة حاليًا في المشتريات) وبين المعمارية اللامركزية المقترحة في نموذج المحاكاة بهدف اثبات الجدوى التقنية والأمنية للنظام الجديد المقترح.

الفصل الأول

دراسة نظرية لتوصيف واقع المشتريات العامة وأهمية الانتقال لاستخدام البلوكتشين.

الفصل الثاني

الهيكلية المعمارية الهجينة لنظام المشتريات العامة المؤتمت (نموذج محاكاة)

الفصل الثالث

ويشمل تحليل النتائج والتوصيات المستقبلية المقترحة

الفصل الأول:

دراسة نظرية لتوصيف واقع المشتريات العامة وأهمية
الانتقال لاستخدام البلوكتشين

1-1: مقدمة في التحول الرقمي في القطاع الحكومي

يُعرّف التحول الرقمي في الحكومة على أنه التبنّي الاستراتيجي للتقنيات الرقمية والرؤى القائمة على البيانات والممارسات المبتكرة ودمجها لتحديث العمليات الحكومية وتعزيز تقديم الخدمات وتحسين مشاركة المواطنين. وهو ينطوي على الاستفادة من الأدوات والمنصات الرقمية لتحويل العمليات والأنظمة والخدمات الحكومية التقليدية لتلبية الاحتياجات المتطورة للمواطنين ومعالجة التحديات المجتمعية المعقدة.

■ تشمل المكونات الرئيسية للتحول الرقمي في الحكومة ما يلي:

- 1- تحسين تقديم الخدمات.
 - 2- اتخاذ القرارات المستندة إلى البيانات.
 - 3- مشاركة المواطنين ومشاركتهم.
 - 4- الشفافية والمساءلة.
 - 5- تمكين القوى العاملة.
 - 6- الأمن السيبراني وخصوصية البيانات.
 - 7- قابلية التشغيل البيئي والتعاون.
- بشكل عام، يعد التحول الرقمي في الحكومة أمراً ضرورياً لتعزيز الكفاءة والشفافية والاستجابة مع ضمان تلبية الخدمات الحكومية للاحتياجات والتوقعات المتطورة للمواطنين في العصر الرقمي. من خلال تبني التقنيات الرقمية والأساليب المبتكرة، يمكن للحكومات تقديم المزيد من الخدمات التي تركز على المواطن، ودفع عجلة النمو الاقتصادي، وتحسين رفاهية المجتمع بشكل عام.

إذ تلعب الحكومة دوراً حاسماً في دفع عجلة التحول الرقمي في المجتمع. فيما يلي العديد من الطرق الرئيسية التي تساهم بها الحكومات في التحول الرقمي وتسهيله من خلال وضع السياسات والتنظيم، الاستثمار في البنية التحتية الرقمية وتطوير المهارات الرقمية، بالإضافة إلى تحديث القطاع العام وحوكمة البيانات وإدارتها. [1]

1-2: دورة المشتريات العامة في المؤسسات:

تُمثل دورة حياة المشتريات رحلة متكاملة العناصر تبدأ من تحديد احتياجات المؤسسة بدقة، وتُمرّ بالبحث عن الموردين الأفضل، وصولاً إلى استلام السلع والخدمات المُتوافقة مع المواصفات، وانتهاءً بسداد المستحقات ودعم استمرارية العلاقات.

ما هي المراحل الأساسية لدورة المشتريات:

1. تحديد الاحتياجات:

- تعتبر هذه المرحلة من مراحل الأقسام المختلفة داخل المؤسسة، حيث يتم تحديد احتياجات الشركة أو المؤسسة من السلع والخدمات بدقة، مع مراعاة المواصفات والجودة والكميات المطلوبة.
- بعدها يتم تسجيل هذه الاحتياجات عبر كتاباتها في طلبات رسمية تُرسل إلى قسم المشتريات.

2. البحث عن الموردين:

يبدأ قسم المشتريات عملية البحث عن الموردين المناسبين للوصول إلى تلبية احتياجات المؤسسة، وذلك من خلال:

- **البحث في قواعد البيانات:** تعتبر هذه الخطوة الأولى وتكون عن طريق البحث عن موردين سبق التعامل معهم أو عن موردين جدد من خلال قواعد بيانات الشركات والمواقع الإلكترونية المتخصصة.
- **طلب عروض الأسعار:** يتم إرسال طلبات عروض أسعار إلى الموردين المختارين لمقارنة الأسعار والشروط واختيار الأفضل بينهم.
- **حضور المعارض التجارية:** المشاركة في المعارض التجارية للتعرف على الموردين الجدد وعروضهم.

3. تقييم عروض الأسعار واختيار المورد:

بعد عملية البحث والوصول إلى أفضل الموردين يقوم قسم المشتريات بخطوة التقييم ومقارنة عروض الأسعار المقدمة من الموردين، مع الأخذ بعين الاعتبار:

- **السعر:** تتم مقارنة أسعار الموردين مع بعضهم البعض والقيام بمقارنتها الأسعار المتداولة في السوق.
- **الجودة:** تقييم جودة السلع أو الخدمات التي يقدمها كل مورد.
- **السمعة التجارية:** التأكد من سمعة المورد وسجله في التعامل مع العملاء الآخرين.
- **قدرة التوريد:** التأكد من قدرة المورد على توفير السلع أو الخدمات بالكميات المطلوبة في الوقت المحدد.
- **شروط الدفع:** تقييم شروط الدفع المقدمة من كل مورد وبناءً على تلك التقييمات، يتم اختيار المورد الذي يقوم أفضل عرض يلبي احتياجات المؤسسة.

4. إصدار أمر الشراء:

بعد عملية اختيار المورد، يتم إصدار أمر شراء رسمي يُحدد جميع تفاصيل الصفقة، وإليك الخطوات:

- **بيانات المورد:** اسم المورد وعنوانه وبيانات الاتصال.
- **بيانات السلع أو الخدمات:** تعتبر نوع وكمية السلع أو الخدمات المطلوبة.
- **السعر:** المتفق عليه مع المورد.
- **شروط الدفع:** طريقة الدفع وشروطها.
- **مدة التوريد:** الموعد المحدد لتسليم السلع أو الخدمات.
- **عنوان الشحن:** عنوان وجهة تسليم السلع أو الخدمات، يُعتبر أمر الشراء بمثابة عقد ملزم بين الشركة والمورد.

5. متابعة الطلب:

لا تنتهي مسؤولية قسم المشتريات عند إصدار أمر الشراء. بل يتم المتابعة مع المورد بشكل دوري للتأكد من:

- **سير عملية التوريد:** في تلك الخطوة يتم التأكد من أن المورد يُصنع أو يُجهز السلع أو الخدمات وفقاً للمواصفات المطلوبة.
- **احترام المواعيد المحددة:** التأكد من التزام المورد بمدة التسليم المحددة في أمر الشراء.

• حل أي مشاكل قد تنشأ: التواصل مع المورد لحل أي مشاكل قد تنشأ خلال عملية التوريد.

6. استلام وتخزين السلع:

عند وصول السلع، يتم فحصها للتأكد من مطابقتها للمواصفات المطلوبة، ثم يتم تخزينها في المكان المخصص.

تشمل عملية الفحص:

• التأكد من الكميات المُستلمة.

• فحص حالة السلع للتأكد من عدم وجود أي تلف أو عيوب.

7. استلام وتخزين السلع (مُستكمل):

تشمل عملية الفحص:

• التأكد من مطابقة المواصفات المُحددة في أمر الشراء.

• فحص جودة السلع للتأكد من خلوها من أي عيوب أو تلف.

• التحقق من كميات السلع المُستلمة.

وبعد التأكد من مطابقة السلع للمواصفات، يتم تخزينها في مكان آمن مخصص لحين استخدامها.

8. الدفع للمورد:

بعد التأكد من استلام السلع بجودة عالية ومطابقتها للمواصفات المُتفق عليها، يتم دفع المستحقات للمورد.

تشمل عملية الدفع:

• التأكد من صحة الفاتورة المُقدمة من المورد.

• التحقق من مطابقة تفاصيل الفاتورة مع أمر الشراء.

• دفع قيمة الفاتورة للمورد بالطريقة المُتفق عليها.

بإتمام عملية الدفع، تُغلق صفقة الشراء بشكل رسمي. [2]

1-2-1: التحديات التقليدية في المشتريات العامة

تعد المشتريات العامة المحرك الأساسي للنشاط الاقتصادي الحكومي، حيث تشير تقارير منظمة التعاون الاقتصادي والتنمية إلى أن المشتريات العامة تمثل في المتوسط حوالي 12% من الناتج المحلي الإجمالي في الدول المتقدمة، وتصل لنحو 30% في الدول النامية، مما يجعلها القناة الأكبر للإنفاق الحكومي. وبالرغم من هذا النقل الاقتصادي، لا تزال هذه المنظومة تعاني من فجوات بنيوية تتعلق بسلامة البيانات ومركزية القرار؛ إذ تشير تقديرات الأمم المتحدة إلى أن الفساد والهدر في المشتريات العامة قد يكلف العالم ما يقارب 2 تريليون دولار سنوياً. إن الطبيعة التوسعية لعملية الشراء تعرضها لمخاطر وتحديات مختلفة، وأكثر تحديات المشتريات شيوعاً هي:

■ ارتفاع التضخم

يؤدي ارتفاع تكلفة المواد الخام إلى زيادة التكاليف في مجال المشتريات. بالإضافة إلى عدة عوامل مثل اضطرابات سلسلة التوريد، ومخاطر التسليم، وضيق أسواق العمل، والسياسات الاقتصادية غير الداعمة.

كما أن الحروب المستمرة هي العامل الرئيسي الدافع لارتفاع تكلفة المواد. فقد أدى الإغلاق المتقطع إلى انخفاض الإنتاج، مما أدى إلى اتساع الفجوة بين الطلب والعرض، مما أدى في النهاية إلى ارتفاع الأسعار.

تُعد روسيا وأوكرانيا مصدرين رئيسيين للطاقة، ولكن بسبب الصراع، انخفض الإنتاج، مما زاد من الضغط على فرق المشتريات لترتيب الموارد الأساسية بسعر أعلى. بعد الغزو، ارتفعت أسعار الطاقة بنسبة 20% لمدة خمسة أشهر.

■ نقص المواهب

يتمثل أحد التحديات الكبيرة التي تواجهها الشركات في الحاجة إلى المزيد من المهنيين المهرة في وظيفة المشتريات وسلسلة التوريد .

■ إدارة العقود

إدارة العقود هي الأساس للحفاظ على العلاقات مع الموردين. في حين أن العقد هو وثيقة قانونية تشير إلى بداية علاقة جديدة مع المورد، إلا أن أهدافه أوسع من ذلك بكثير. فالهدف هو تمكين الشركة من تسليم المنتجات بسعر تنافسي. يضمن العقد تسليم المواد بشكل مستقر وعالي الجودة وفعالية التكلفة الإجمالية للصفقة.

ومع ذلك، لا يمكن لمعظم فرق المشتريات أن تعمل بكامل طاقتها بسبب الوقت الطويل الذي تستغرقه عملية التسليم، والعمليات اليدوية، والمشاكل المتعلقة بالموردين، ونقص التواصل والتنسيق، والعقود المفقودة.

ويؤدي ذلك إلى ضياع فرص تحقيق وفورات في التكاليف، ومخاطر عدم الامتثال التنظيمي، والعلاقات المتوترة مع الموردين، وضعف عملية اتخاذ القرارات. تحتاج الشركات إلى نظام مشتريات فعال لأتمتة عملية إدارة سلسلة التوريد وإضفاء الطابع المركزي عليها.

■ عدم دقة البيانات

في معظم الشركات، تقوم فرق المشتريات بإدارة إدخال البيانات يدويًا. فهم يقومون بإدخال البيانات على جداول البيانات والأنظمة القديمة ذات القدرات الأوتوماتيكية والتحليلية المحدودة. نظرًا لأن البيانات يتم التعامل معها يدويًا، فهي في المقام الأول غير متسقة وعرضة للخطأ البشري.

وتؤدي نتيجة سوء جودة قاعدة البيانات إلى ضعف وبطء عملية اتخاذ القرار. تخسر الشركات فرصًا حاسمة وتُعرض نفسها لمخاطر غير مرغوب فيها مثل طلب مخزون زائد بسبب التناقضات في بيانات مستوى المخزون.

من ناحية أخرى، تسمح البيانات الدقيقة والموثوقة لقادة المشتريات باتخاذ قرارات سليمة والحصول على رؤية واضحة لعمليات الشراء.

■ غياب التواصل الداخلي

يعد ضعف التواصل الداخلي من أكثر التحديات المذهلة في مجال المشتريات لأنه يتعارض صراحةً مع توقعات الإدارة العليا من فريق المشتريات الذي يتولى دور القائد الاستراتيجي.

يعمل فريق المشتريات بشكل مستقل؛ لذلك يعتمد فريق المشتريات بشكل أساسي على موارد الفرق الأخرى، مثل المعلومات المالية والتعاون متعدد الوظائف.

ومع ذلك، يمكن أن تصلهم هذه المعلومات عندما تكون هناك شبكة اتصالات داخلية قوية.

أحد التحديات الحرجة التي يواجهها فريق المشتريات هو أنهم يعملون بشكل منعزل؛ فهم غير مدركين للاستراتيجية على مستوى المؤسسة ولديهم فهم محدود للمتطلبات المستقبلية.

■ إدارة المخاطر

تقدم فرق المشتريات أفضل النتائج عندما يكون هناك أساس قوي لإدارة المخاطر. المشتريات عملية طويلة، وتؤثر عليها عدة عوامل داخلية وخارجية.

وتؤدي هذه العوامل أيضًا إلى مخاطر داخلية مثل سلوك الموظفين ومخاطر خارجية أكثر صعوبة في السيطرة عليها، مثل الأحداث العالمية.

ولكن، تأتي المخاطر التالية على رأس قائمة المخاطر التي يجب على مدير المشتريات أن يتحكم بها في إدارة المخاطر في سلسلة التوريد:

1) عدم استقرار الأسعار

يتسم سوق سلسلة التوريد في الوقت الحالي بالتقلب. وتؤدي التغيرات المستمرة في الأسعار إلى زيادة تكلفة المشتريات. ونظراً لأن الموردين يطلبون المزيد من الأموال، فإن وجود ميزانية مرنة أمر ضروري لتجنب نقص المخزون.

2) اضطراب سلسلة التوريد

يمكن أن تتعطل سلاسل التوريد بشكل غير متوقع بسبب عوامل مثل الحروب والقضايا السياسية والكوارث الطبيعية. ويتمثل التحدي الأكبر هنا في الحصول على المواد من مورد آخر في الساعة الحادية عشرة. المفتاح هنا هو إنشاء نظام استجابة لإدارة مثل هذه الحالات بكفاءة أكبر مع العمل مع خبير مشتريات.

(3) الغش

عملية الشراء عرضة للاحتيال من مصادر مختلفة: الموظفون أو البائعون أو المقاولون. عادةً ما يحدث الاحتيال في الفواتير عندما يقوم الموردون بتضخيم التكلفة، ويوافق فريق المشتريات عليها دون التحقق منها. كما أن تحديد الأسعار هو احتيال آخر كثيرًا ما يحدث عندما يتعاون المقاولون لرفع التكلفة أو التنازل عن الخصومات.

(4) مشاكل الموردين

يشكل الحفاظ على علاقات متينة وإيجابية مع الموردين حجر الأساس لحل تحديات المشتريات. ترجع العديد من مشكلات الموردين إلى عوامل داخلية مثل عدم وضوح المواصفات والمتطلبات. إذا قام الموردون بتوصيل توقعاتهم، سيكون من الأسهل إدارة التسليم عالي الجودة.

وبالمثل، فإن عدم بذل العناية الواجبة في تقييم الموردين لفهم قدراتهم وعدم الاتفاق على مؤشرات الأداء الرئيسية من العوامل الأخرى التي تزيد من التوترات في إدارة العلاقة مع الموردين.

(5) غياب التكنولوجيا

يمثل الافتقار إلى الرقمنة في عمليات الشراء مشكلة للشركات التي لديها خطط قوية لتوسيع نطاق عمليات الشراء الخاصة بها. ما لم تصبح التقنيات الجديدة جزءًا لا يتجزأ من الأنشطة اليومية، فلن ترى أبدًا الإمكانيات الكاملة لاستراتيجية المشتريات.

يؤدي الافتقار إلى التكنولوجيا إلى إبقاء العمليات الرئيسية بطيئة، حيث يكون إدخال البيانات يدويًا وغير منظم. وهذا يقلل أيضًا من القدرة على حل المشاكل الحالية ويجعل الأعمال أكثر عرضة للمخاطر. تحتاج الشركات إلى نظام تقني للتكيف مع ظروف العمل المتغيرة. [3]

1-3: لماذا نحتاج Blockchain ؟

■ تعريف البلوكتشين بطريقة مبسطة:

هي تقنية تعمل على هيئة نظام سجل الكتروني لمعالجة الصفقات وتدوينها بما يتيح لكل الأطراف تتبع المعلومات عبر شبكة آمنة لا تستدعي التحقق من طرف ثالث، إذ يمكن تسجيل معلومات عليها من طرف أي شخص على الشبكة (وليس المحاسب فقط)؛ كما أنه متاح للاطلاع عليه من طرف الجميع (وليس بضعة مسؤولين كما هو الحال في الشركات).

ونظرًا لأن كل معاملة تتم على البلوكتشين تتم مراقبتها من طرف جميع المستخدمين على الشبكة فإنه من الاستحالة القيام بأي احتيال أو تزوير؛ فكل شخص على الشبكة يملك نسخة من دفتر الحسابات (البلوكتشين) ويمكنه التحقق من صحة المعاملات.

■ كيف تعمل بلوكتشين؟

بلوكتشين هي عبارة عن قاعدة بيانات ضخمة موزعة لا مركزية - تعمل كدفتر الحسابات - تقوم بتسجيل تفاصيل ومعلومات المعاملات التي تتم على الحواسيب التي تشكل الشبكة المكونة لقاعدة البيانات.

وتقوم قاعدة البيانات هذه بتسجيل جميع المعاملات التي تتم على الشبكة بشكل رقمي على كل عُقدة (حاسوب) على الشبكة.

يمكن لأي شخص على شبكة بلوكتشين المشاركة في تعاملاتها ومشاهدة جميع المعاملات التي تتم بين المستخدمين الآخرين، كما يمكن إضافة تعاملات جديدة؛ حيث تمثل كل معاملة كتلة جديدة تُضاف إلى سلسلة الكتل الأخرى الموجودة مسبقاً على منصة بلوكتشين، بعد التحقق من صحتها وتوثيقها من طرف المستخدمين الآخرين، والذين يطلق عليهم عادة بالمُعدّنين.

يتم تسجيل البيانات على شبكة بلوكتشين على كل الكتل؛ حيث تتضمن كل كتلة معلومات معينة، ليتم فيما بعد ربط هذه الكتل فيما بينها من خلال خوارزميات تشفير. ومع كل معلومة جديدة تضاف إلى قاعدة البيانات، تُضاف كتلة أخرى إلى السلسلة ويتم ربطها بالكتلة التي تسبقها، بحيث تكون الكتل مرتبة بترتيب زمني.

■ كيف تحقق بلوكتشين الإجماع؟

آلية الإجماع هي من بين أبرز ميزات البلوكتشين؛ وللتأكد من صحة معاملة ما على الشبكة وإضافتها ككتلة جديدة إلى البلوكتشين، يجب أن يكون هناك إجماع من طرف المستخدمين. فلكي يتم إضافة معلومات جديدة أو تحديثها على الشبكة يجب أن يكون هناك توافق بين المستخدمين على صحة هذه المعلومات، قبل أن تصبح كتلة جديدة.

هناك العديد من آليات الإجماع المستخدمة، لكن بشكل عام، تعتبر آلية إثبات العمل (PoW) وآلية إثبات الحصة (PoS) أشهر آليتي إجماع.

- إثبات العمل (PoW)

من خلال آلية إثبات العمل، يقوم المُعدّنون بالعمل على حل خوارزميات تشفير ومعادلات رياضية، والتي تكون على شكل سلسلة من الأحرف والأرقام والرموز تعرف بـ "الهاش"، بهدف التحقق من صحة معاملة ما وإضافتها ككتلة جديد إلى البلوكتشين إذا كانت صحيحة.

عندما يقوم مُعدّن ما بحل الخوارزمية، سيتم إضافة تفاصيل المعاملة على شكل كتلة جديدة إلى البلوكتشين الموجود على جميع عُقد الشبكة؛ حيث سيتمكن كل مستخدم من مشاهدتها. ويتطلب حل الخوارزميات الكثير من القوة الحاسوبية والوقت، وذلك بهدف منع أي هجمات مضرّة بالشبكة أو محاولة التلاعب بها. ومقابل هذا العمل يحصل كل مُعدّن عندما يحل خوارزمية ما على مكافأة تكون على شكل عملة رقمية أو جزء منها.

- إثبات الحصة (PoS)

إثبات الحصة هي آلية إجماع يقوم من خلالها المعدّنون برهن عملاتهم الرقمية للتحقق من المعاملات التي تتم على البلوكتشين وتأكيد صحتها، لتضاف فيما بعد إلى البلوكتشين ككتلة جديدة. ويتم اختيار المعدّنين على النظام بحسب عدد العملات الرقمية التي يرهنوها ومدة عملية الرهن. هذه الطريقة تضمن عدم حدوث عمليات تلاعب أو غش أو تزوير؛ نظراً لأن كل شخص سيحاول القيام بذلك سيخسر جميع العملات الرقمية التي رهنها.

- ثبات السلطة (Proof of Authority - PoA):

بخلاف آليات إثبات العمل أو الحصة التي تعتمد على القوة الحاسوبية أو الثروة المالية، تعتمد آلية إثبات السلطة (PoA) على "الهوية والسمعة". في هذا النموذج، يتم اختيار عدد محدود وموثوق من العقد (Nodes) - مثل الوزارات أو الهيئات الرقابية - لتكون مسؤولة عن التحقق من صحة المعاملات وإنشاء الكتل. وتُعد هذه الآلية الخيار الأمثل للأنظمة الحكومية وشبكات "بلوكتشين التحالف" نظراً لسرعتها الفائقة في إنجاز المعاملات، واستهلاكها شبه المعدوم للطاقة، وحفاظها على خصوصية وسرية البيانات بعيداً عن التعدين المفتوح، حيث يظهر الجدول (1-1): أهم المزايا التي يقدمها بلوكتشين للعملات الرقمية.

الجدول (1-1): أهم المزايا التي تقدمها البلوكتشين

توفر بلوكتشين العديد من المزايا للعملات الرقمية فيما يلي أبرزها	
الأمان	تعتمد بلوكتشين على الإجماع والتشفير، مما يجعل من المستحيل تقريباً التلاعب بالمعلومات الخاصة بمعاملات الخاصة بمعاملات العملة الرقمية.
اللامركزية	تتم التعاملات بشكل لا مركزي دون وجود أي سلطة مهيمنة، حيث يتوجب التحقق من جميع معاملات العملات الرقمية من قبل غالبية المشاركين في الشبكة.
الشفافية	من الممكن عرض وتتبع جميع معاملات العملات الرقمية التاريخية على بلوكتشين، مما يجعلها قابلة للتدقيق بكل سهولة.

لا تقتصر هذه التقنية على العملات الرقمية بل تم توسيعها لتشمل المعاملات الحكومية.

■ هل البلوكتشين آمنة؟

توفر تكنولوجيا بلوكتشين مستوى أمان عالٍ نسبياً مقارنة بالأنظمة المركزية الأخرى، فطريقة عمل بلوكتشين اللامركزية تؤهلها لخلق نظام آمن ومستقر؛ حيث أنه غير مهدد من الهجمات المركزية، على غرار الأنظمة المركزية التي قد تنهار بشكل كامل إذا ما تم اختراقها.

على سبيل المثال، لو أن شركة ما تقوم بتخزين بيانات وأنظمة عملها على خوادم محدودة خاصة بها، وتعرضت هذه الخوادم لعملية اختراق، فإن جميع بيانات الشركة قد تتعرض للسرقة وستنهار أنظمة الشركة. وهذا الأمر يستحيل القيام به على شبكة بلوكتشين لا مركزية، حيث أن المهاجم سيحتاج لاختراق أغلب عقد الشبكة، وهو أمر مستحيل نظرياً.

تعتبر آليات الإجماع من بين مزايا بلوكتشين التي تضمن استقرارها -على غرار إثبات الحصة وإثبات العمل- التي تكون بمثابة درع ضد الهجمات ومحاولات التلاعب بالشبكة، حيث تجعل الأمر شبه مستحيل على المهاجمين. وتضمن لا مركزية بلوكتشين استمرار عمل الشبكة دون انقطاع، فحتى لو حدثت مشكلة على عقدة ما أو انقطعت عنها الإنترنت أو أصيبت بتلف نتيجة خطأ بشري فإن الشبكة لا تتأثر نهائياً. [3],[4]

1-3-1: ما المقصود بتقنية سلسلة الكتل؟

تقنية سلسلة الكتل هي آلية متقدمة لقواعد البيانات تسمح بمشاركة المعلومات بشفافية داخل شبكة الأعمال. تخزن قاعدة بيانات سلسلة الكتل البيانات في كتل مرتبطة ببعضها في سلسلة. وتعد البيانات متسقة زمنياً لأنه لا يمكنك حذف السلسلة أو تعديلها من دون توافق من الشبكة. ونتيجة لذلك، يمكنك استخدام تقنية سلسلة الكتل لإنشاء سجل حسابات غير قابل للتغيير أو ثابت لتتبع الطلبات والمدفوعات والحسابات والمعاملات الأخرى. يحتوي النظام على آليات مدمجة تمنع إدخال المعاملات غير المصرح بها وتُنشئ تناسقاً في طريقة العرض المشتركة لهذه المعاملات.

1) لماذا تعد سلسلة الكتل مهمة؟

تقدم تقنيات قواعد البيانات التقليدية العديد من التحديات فيما يتعلق بتسجيل المعاملات المالية. مما يقلل الثقة بين المصادر المتعاقدة، كما أن إدخال طرف ثالث في المعاملة يعد ثغرة أمنية.

تخفف سلسلة الكتل من هذه المشكلات من خلال إنشاء نظام لامركزي ومقاوم للتلاعب لتسجيل المعاملات. في سيناريو معاملة العقارات، تُنشئ سلسلة الكتل سجل حسابات واحداً لكل من المشتري والبائع. يجب أن تتم الموافقة على جميع المعاملات من قبل الطرفين ويتم تحديثها تلقائياً في سجل حسابات كل طرف في الوقت الفعلي. فأى فساد في المعاملات السابقة سيفسد سجل الحسابات بأكمله. وأدت خصائص تقنية سلسلة الكتل هذه إلى استخدامها في مختلف القطاعات، بما في ذلك إنشاء عملة رقمية مثل البيتكوين

2) ما ميزات تقنية سلسلة الكتل؟

تتميز تقنية سلسلة الكتل بالميزات الرئيسية الآتية:

اللامركزية

تشير اللامركزية في سلسلة الكتل إلى نقل التحكم وصنع القرار من منشأة مركزية (فرد أو منظمة أو مجموعة) إلى شبكة موزعة. تستخدم شبكات سلسلة الكتل اللامركزية الشفافية لتقليل الحاجة إلى الثقة بين المشاركين. كما تمنع هذه الشبكات المشاركين من ممارسة السلطة أو السيطرة على بعضهم بطرق تؤدي إلى تدهور وظائف الشبكة.

الثبات

الثبات يعني أن شيئاً ما لا يمكن تغييره أو تعديله. لا يمكن لأي مشارك التلاعب بمعاملة بمجرد قيام شخص ما بتسجيلها في سجل الحسابات المشترك. إذا تضمن سجل المعاملة خطأ ما، فيجب عليك إضافة معاملة جديدة لعكس الخطأ، وتكون كلتا المعاملتين مرئيتان للشبكة.

التوافق

يضع نظام سلسلة الكتل قواعد حول موافقة المشارك لتسجيل المعاملات. لا يمكنك تسجيل معاملات جديدة إلا بعد موافقة غالبية المشاركين في الشبكة.

(3) ما المكونات الرئيسية لتقنية سلسلة الكتل؟

تحتوي هندسة سلسلة الكتل على المكونات الرئيسية الآتية:

سجل حسابات موزع

سجل الحسابات الموزع هو قاعدة البيانات المشتركة في شبكة سلسلة الكتل التي تُخزن المعاملات، مثل ملف مشترك يمكن لكل شخص في الفريق تحريره. في معظم برامج تحرير النصوص المشتركة، يمكن لأي شخص لديه حقوق التحرير حذف الملف بأكمله. ولكن، تقنيات سجل الحسابات الموزعة لديها قواعد صارمة حول من يمكنه التحرير وكيفية التحرير. لا يمكنك حذف الإدخالات بمجرد تسجيلها.

العقود الذكية

تستخدم الشركات العقود الذكية للإدارة الذاتية لعقود العمل من دون الحاجة إلى طرف ثالث مساعد. وهي برامج مخزنة على نظام سلسلة الكتل تعمل تلقائياً عند استيفاء شروط محددة سابقاً. كما تقوم بإجراء عمليات التحقق "if-then" بحيث يمكن إتمام المعاملات بثقة.

تشفير المفتاح العام

يعد تشفير المفتاح العام ميزة أمان لتحديد المشاركين في شبكة سلسلة الكتل بشكل فريد. تُنشئ هذه الآلية مجموعتين من المفاتيح لأعضاء الشبكة. أحد المفاتيح هو مفتاح عام مشترك بين كل شخص في الشبكة. والآخر هو مفتاح خاص فريد لكل عضو. يعمل المفتاحان الخاص والعام معاً لفتح البيانات الموجودة في سجل الحسابات.

(4) كيف تعمل سلسلة الكتل؟

في حين أن آليات سلسلة الكتل الأساسية معقدة، فإننا نقدم نظرة عامة موجزة في الخطوات الآتية. يمكن لبرنامج سلسلة الكتل أتمتة معظم هذه الخطوات:

الخطوة 1 - تسجيل المعاملة

تُظهر معاملة سلسلة الكتل حركة الأصول المادية أو الرقمية من طرف إلى آخر في شبكة سلسلة الكتل. ويتم تسجيلها ككتلة بيانات ويمكن أن تتضمن تفاصيل مثل:

- من شارك في المعاملة؟
- ماذا حدث في أثناء المعاملة؟
- متى تمت المعاملة؟
- أين تمت المعاملة؟
- لماذا تمت المعاملة؟
- ما مقدار الأصول التي تم تبادلها؟
- كم عدد الشروط السابقة التي تم استيفاؤها في أثناء المعاملة؟

الخطوة 2 - كسب التوافق

يجب أن يوافق معظم المشاركين على شبكة سلسلة الكتل الموزعة على أن المعاملة المسجلة صالحة. اعتمادًا على نوع الشبكة، يمكن أن تختلف قواعد الموافقة ولكن يتم وضعها عادةً في بداية الشبكة.

الخطوة 3 - ربط الكتل

بمجرد أن يتوصل المشاركون إلى توافق في الآراء، تتم كتابة المعاملات على سلسلة الكتل في كتل تعادل صفحات سجل الحسابات. إلى جانب المعاملات، يتم كذلك إلحاق تجزئة تشفير بالكتلة الجديدة. تعمل التجزئة كسلسلة تربط الكتل معًا. إذا تم تعديل محتويات الكتلة عن قصد أو عن غير قصد، فإن قيمة التجزئة تتغير، ما يوفر طريقة لاكتشاف التلاعب بالبيانات. ومن ثم، ترتبط الكتل والسلاسل بشكل آمن، ولا يمكنك تحريرها. تعمل كل كتلة إضافية على تعزيز التحقق من الكتلة السابقة ومن ثم سلسلة الكتل بأكملها.

الخطوة 4 - مشاركة سجل الحسابات

يوزع النظام أحدث نسخة من سجل الحسابات المركزي على جميع المشاركين.

(5) ما أنواع شبكات سلسلة الكتل؟

هناك أربعة أنواع رئيسية من الشبكات اللامركزية أو الموزعة في سلسلة الكتل:

■ شبكات سلسلة الكتل العامة

تعمل سلاسل الكتل العامة من دون الحاجة إلى إذن وتسمح للجميع بالانضمام إليها. يتمتع جميع أعضاء سلسلة الكتل بحقوق متساوية في قراءة سلسلة الكتل وتحريرها والتحقق من صحتها. يستخدم الأشخاص سلاسل الكتل العامة في المقام الأول لتبادل العملات المشفرة وتعدينها مثل البيتكوين والإيثريوم واللايتكوين.

■ شبكات سلسلة الكتل الخاصة

تتحكم منظمة واحدة في سلاسل الكتل الخاصة، وتسمى كذلك بسلاسل الكتل المُدارة. تحدد السلطة من يمكنه أن يكون عضواً وما الحقوق التي يتمتع بها في الشبكة. تعد سلاسل الكتل الخاصة لامركزية بشكل جزئي فقط نظراً إلى قيود الوصول إليها.

■ شبكات سلسلة الكتل المختلطة

تجمع سلاسل الكتل المختلطة بين عناصر من كل من الشبكات الخاصة والعامة. يمكن للشركات إنشاء أنظمة خاصة قائمة على الإذن جنباً إلى جنب مع نظام عام. وبهذه الطريقة، يمكنها التحكم في الوصول إلى بيانات محددة مخزنة في سلسلة الكتل مع الحفاظ على بقية البيانات عامة. كما تستخدم العقود الذكية للسماح للأعضاء العامة بالتحقق مما إذا كانت المعاملات الخاصة قد اكتملت أم لا.

■ شبكات اتحاد سلسلة الكتل

تدير مجموعة من المنظمات شبكات اتحاد سلسلة الكتل. تتقاسم المنظمات المحددة سابقاً مسؤولية الحفاظ على سلسلة الكتل وتحديد حقوق الوصول إلى البيانات. الصناعات التي تمتلك فيها العديد من المنظمات أهدافاً مشتركة وتستفيد من المسؤولية المشتركة غالباً ما تفضل شبكات اتحاد سلسلة الكتل. ونظراً لما يوفره هذا النوع من توازن دقيق بين المركزية الإدارية الحكومية واللامركزية التقنية، تم اعتماد "بلوكتشين التحالف" كبنية تحتية أساسية للنموذج المعماري المقترح في هذه الأطروحة.

(6) ما بروتوكولات سلسلة الكتل؟

يشير مصطلح بروتوكول سلسلة الكتل إلى أنواع مختلفة من منصات سلسلة الكتل المتاحة لتطوير التطبيقات. يتأقلم كل بروتوكول من بروتوكولات سلسلة الكتل مع مبادئ سلسلة الكتل الأساسية ليناسب صناعات أو تطبيقات محددة. فيما يأتي بعض الأمثلة على بروتوكولات سلسلة الكتل في الأقسام الفرعية الآتية:

Hyperledger fabric: هو مشروع مفتوح المصدر يتضمن مجموعةً من الأدوات والمكتبات. يمكن للمؤسسات استخدامه لإنشاء تطبيقات سلسلة كتل خاصة بسرعة وفعالية. فهو إطار معياري للأغراض العامة يوفر ميزات فريدة لإدارة الهوية والتحكم في الوصول. هذه الميزات تجعله مناسباً لمختلف التطبيقات، مثل تتبع سلاسل التوريد وتعبئها والتمويل التجاري والولاء والمكافآت وتسوية الأصول المالية.

Ethereum: هي منصة سلسلة كتل لامركزية ومفتوحة المصدر يمكن للأشخاص استخدامها في إنشاء تطبيقات سلسلة كتل عامة. تم تصميم Ethereum Enterprise لحالات استخدام الشركات.

Corda: هو مشروع سلسلة كتل مفتوح المصدر مصمم للشركات. من خلال Corda، يمكنك إنشاء شبكات سلسلة كتل قابلة للتشغيل المتبادل وتتعامل بخصوصية تامة. يمكن للشركات استخدام تقنية العقود الذكية من Corda للتعامل مع القيمة مباشرة. ومعظم مستخدميها من المؤسسات المالية.

Quorum: هو بروتوكول سلسلة كتل مفتوح المصدر مشتق من Ethereum. تم تصميمه خصوصًا للاستخدام في شبكة سلسلة كتل خاصة، حيث يمتلك عضو واحد فقط جميع العقد، أو في شبكة اتحاد سلسلة كتل، حيث يمتلك كل عضو منهم جزءًا من الشبكة.

7) كيف تطورت تقنية سلسلة الكتل؟

تعود جذور تقنية سلسلة الكتل إلى أواخر السبعينيات عندما حصل عالم حاسوب يسمى رالف ميركل على براءة اختراع عن أشجار التجزئة أو أشجار ميركل. تعد هذه الأشجار بنية لعلوم الحاسوب لتخزين البيانات عن طريق ربط الكتل باستخدام التشفير. في أواخر التسعينيات، استخدم ستيفارت هابر ودابليو سكوت ستورنيتا أشجار ميركل لتنفيذ نظام لا يمكن التلاعب فيه بالطوابق الزمنية للوثائق. كانت هذه هي الحالة الأولى في تاريخ سلسلة الكتل.

استمرت التكنولوجيا في التطور على مدى هذه الأجيال الثلاثة:

الجيل الأول – البيتكوين والعملات الافتراضية الأخرى

الجيل الثاني – العقود الذكية

الجيل الثالث – المستقبل

ما مزايا تقنية سلسلة الكتل؟

تجلب تقنية سلسلة الكتل العديد من المزايا لإدارة معاملات الأصول. نقدم بعضًا منها في الأقسام الفرعية التالية:

الأمان المتقدم: توفر أنظمة سلسلة الكتل مستوى عاليًا من الأمان والثقة التي تتطلبها المعاملات الرقمية الحديثة. هناك دائمًا خوف من أن يتلاعب شخص ما بالبرامج الأساسية لإنتاج أموال مزيفة لنفسه. لكن تستخدم سلسلة الكتل المبادئ الثلاثة التشفير واللامركزية والتوافق لإنشاء نظام برمجي أساسي آمن للغاية يكاد يكون من المستحيل التلاعب به. لا توجد نقطة فشل واحدة، ولا يمكن لمستخدم واحد تغيير سجلات المعاملات.

الكفاءة المحسنة: يمكن أن تستغرق المعاملات بين الشركات الكثير من الوقت وتُنشئ تعقيدات تشغيلية، خصوصًا عندما يتعلق الأمر بالامتثال والهيئات التنظيمية التابعة لأطراف ثالثة. تجعل الشفافية والعقود الذكية في سلسلة الكتل مثل هذه المعاملات التجارية أسرع وأكثر كفاءة.

التدقيق الأسرع: يجب أن تكون الشركات قادرة على إنشاء المعاملات الإلكترونية وتبادلها وأرشفتها وإعادة بنائها بشكل آمن وبطريقة قابلة للتدقيق. سجلات سلسلة الكتل ثابتة زمنيًا، ما يعني أن جميع السجلات يتم ترتيبها دائمًا حسب الوقت. تجعل شفافية البيانات هذه عملية التدقيق أسرع بكثير.

ما الفرق بين قاعدة البيانات وسلسلة الكتل؟

سلسلة الكتل هي نوع خاص من نظام إدارة قاعدة البيانات يحتوي على ميزات أكثر من قاعدة البيانات العادية. نشرح بعض الاختلافات المهمة بين قاعدة البيانات التقليدية وسلسلة الكتل في القائمة الآتية:

- تعمل سلسلة الكتل على تطبيق اللامركزية على التحكم من دون الإضرار بالثقة بالبيانات الموجودة. وهذا غير ممكن في أنظمة قواعد البيانات الأخرى.
- لا يمكن للشركات المشاركة في معاملة القيام بمشاركة قاعدة بياناتها بالكامل. لكن في شبكات سلسلة الكتل، تمتلك كل شركة نسختها من سجل الحسابات، ويحافظ النظام تلقائيًا على الاتساق بين سجلي الحسابات.
- على الرغم من أنه يمكنك تحرير البيانات أو حذفها في معظم أنظمة قواعد البيانات، فإنه يمكنك إدراج البيانات فقط في سلسلة الكتل.

كيف تختلف سلسلة الكتل عن السحابة؟

يشير مصطلح السحابة إلى خدمات الحوسبة التي يمكن الوصول إليها عبر شبكة الإنترنت. يمكنك الوصول إلى البرنامج كخدمة (SaaS) والمنتج كخدمة (PaaS) والبنية التحتية كخدمة (IaaS) من السحابة. يدير مزودو السحابة أجهزتهم وبنيتهم التحتية ويمنحونك إمكانية الوصول إلى موارد الحوسبة هذه عبر شبكة الإنترنت. كما يوفر موارد أكثر بكثير من مجرد إدارة قاعدة البيانات. إذا كنت ترغب في الانضمام إلى شبكة سلسلة الكتل العامة، فأنت بحاجة إلى توفير مواردك من الأجهزة لتخزين نسختك من سجل الحسابات. يمكنك كذلك استخدام خادم من السحابة لهذا الغرض. يقدم بعض مزودي السحابة كذلك سلسلة الكتل كخدمة (BaaS) بالكامل من السحابة.

ما المقصود بسلسلة الكتل كخدمة؟

سلسلة الكتل كخدمة (BaaS) هي خدمة سلسلة كتل مُدارة يقدمها طرف ثالث في السحابة. يمكنك تطوير تطبيقات سلسلة الخدمة والخدمات الرقمية بينما يقوم مزود السحابة بتوفير البنية الأساسية وأدوات بناء سلسلة الكتل. كل ما عليك فعله هو تخصيص تقنية سلسلة الكتل الحالية، ما يجعل اعتماد سلسلة الكتل أسرع وأكثر كفاءة.[5]

1-3-2: سجلات التوزيع

سجلات التوزيع في المشتريات الحكومية هي وثائق رسمية تُستخدم لتتبع حركة المواد أو الخدمات من لحظة استلامها من المورد حتى وصولها إلى الجهة المستفيدة النهائية داخل المؤسسة الحكومية. تهدف هذه السجلات إلى ضمان الشفافية، المساءلة، وسهولة تتبع الأصول والعهد.

تشمل سجلات التوزيع عادةً العناصر التالية:

- **بيانات المادة:** اسم المنتج، الكمية الموزعة، والرقم التسلسلي أو رقم الدفعة (Lot Number) لضمان إمكانية التتبع في حالات الاستدعاء أو العيوب.
- **بيانات الجهة المستلمة:** اسم القسم أو الموظف المستلم وموقعه.
- **التواريخ والاعتمادات:** تاريخ التوزيع، وتواريخ الجهات المسؤولة عن الصرف والاستلام لضمان صحة الإجراءات المالية والإدارية.
- **سجل الخدمات:** في بعض الأنظمة، يتم تقييد بيانات عقود شراء الخدمات ومتابعة أدائها وتواريخ انتهائها ضمن سجلات متخصصة .

تعد هذه السجلات جزءاً أساسياً من نظام إدارة المخزون الحكومي، حيث تساعد في تحديد الاحتياجات المستقبلية بدقة بناءً على معدلات الاستهلاك الفعلية المسجلة. [6]

1-3-3: تقنية التجزئة (تابع الهاش)

تجزئة Blockchain هي خوارزمية تشفير تقوم بتحويل بيانات الإدخال ذات الطول التعسفي إلى مخرجات ثابتة الطول. في تقنية blockchain، تلعب وظائف التجزئة دوراً حيوياً، ليس فقط لضمان سلامة وأمن البيانات، ولكن أيضاً توفير الأساس لتشغيل blockchain. تشمل خصائص وظائف التجزئة أحادية الاتجاه والحتمية ومقاومة الاصطدام، مما يجعل التجزئة تستخدم على نطاق واسع في سلاسل الكتل للتوقيعات الرقمية وإثبات العمل (PoW) والتحقق من سلامة البيانات. في عام 2025، مع تقدم تكنولوجيا الحوسبة الكمومية، تواجه خوارزميات التجزئة التقليدية تحديات جديدة. لمواجهة هذه التحديات، يعمل خبراء تكنولوجيا البلوكتشين على تطوير خوارزميات تجزئة ما بعد الكم أقوى. هذه الخوارزميات الجديدة لا تقتصر فقط على مقاومة هجمات الحواسيب الكمومية، بل توفر أيضاً أماناً وكفاءة أعلى. على سبيل المثال، بعض خوارزميات التجزئة الجديدة أصبحت قادرة على معالجة عدة جيجابايت من البيانات في نطاق ملي ثانية، مع الحفاظ على احتمالية تصادم منخفضة للغاية.

فك تشفير SHA-256:

SHA-256 هو الدالة الأساسية لتجزئة التشفير المستخدمة في شبكة البيتكوين.

ينتمي إلى عائلة SHA-2، وقد تم تصميمه بواسطة وكالة الأمن القومي الأمريكية (NSA) تعتمد آلية عمل SHA-256 على سلسلة من العمليات الرياضية المعقدة، بما في ذلك العمليات البتية، والعمليات المودولية، والدوال المنطقية. يتم تنفيذ هذه العمليات على مدى 64 جولة، مما ينتج عنه في النهاية قيمة تجزئة بطول 256 بت (32 بايت).

تتمثل قوة SHA-256 في مقاومته للاصطدام وخصائصه أحادية الاتجاه. حتى في عام 2025، لا يزال من الصعب للغاية باستخدام أجهزة الكمبيوتر العملاقة الأكثر تقدماً العثور على مدخلين مختلفين ينتجان نفس قيمة التجزئة SHA-256. تجعل هذه الميزة SHA-256 تلعب دوراً حيوياً في تكنولوجيا blockchain، خاصة في عملية تعدين البيتكوين.

الهش - "HASH" هو نتيجة عملية تشفير للمعلومات. حيث يتم إدخال مجموعة من المعلومات الرقمية في نظام تشفير نحصل من خلاله على كود فريد من نوعه خاص بالمعلومات التي قمنا بتشفيرها.

هذا الكود الموضح في الشكل بالأسفل (1-1) يتغير كلما غيرنا المعلومات المدخلة، وأي تغيير مهما كان صغيراً يؤدي حتماً إلى كود مختلف تسمى هذه العملية بـ "الهشينغ (HASHING)" وباختصار هي عملية يتم من خلالها أخذ بيانات الإدخال من أي حجم كان، وتنفيذ عملية رياضية عليها، وإعادة بيانات الإخراج بحجم ثابت دائماً. [7],[8]

btcacademy	Hash Function	a82c8a60e1a197572e46f1b2526482610073a0c7769 d4b3e4adfc8ea9c9480b5
btcacademy 1	Hash Function	e30922a44e427031e0bd9f68aa92de63092472cab8 a4bc7511db21b1c1fb81ab
btcacademy 2	Hash Function	d7c323291b432c2d758a92f84c5120f15c7e542cde7 7d7f36b0c08f920b3f96c

الشكل (1-1): كيفية تغير نتيجة تابع الهش عند تغيير الكود المدخل في المرات الثلاث.

يوضح الجدول التالي (2-1) مقارنة بين آلية SHA-256 للتشفير وخوارزمية التجزئة.

الجدول (2-1): مقارنة بين آلية SHA-256 للتشفير وخوارزمية التجزئة

الخصائص	SHA-256	خوارزمية التجزئة من الجيل الجديد
طول الإخراج	256بت	متغير (1024-256 بت)
سرعة الحساب	~1GB/s	~10GB/s
مقاومة الهجمات الكوانتية	ضعيف	قوي
كفاءة الطاقة	متوسط	عالي

ما الوظيفة التي تخدمها عملية الهش في بلوكتشين؟

تستخدم العديد من مكونات نظام blockchain التجزئة، ولضمان عدم تغيير أي شيء عند إضافة كتل جديدة، تحتوي كل كتلة أولاً على تجزئة رأس الكتلة للكتلة السابقة، وبالإضافة إلى ذلك يتضمن تعدين العملة المشفرة لإثبات العمل (PoW) تجزئة مجموعة من الأرقام التي تم إنشاؤها عشوائياً لإنتاج قيمة مجزأة معينة تحتوي على سلسلة من الأصفار البادئة، ونظراً لأن هذه الوظيفة المعقدة تستهلك الكثير من الموارد، فسيكون من الصعب على الفاعل الضار أن يستولي على الشبكة.

[7],[8]

1-3-4: ما هي العقود الذكية؟

العقود الذكية نوع من العقود الرقمية المخزنة في قاعدة بيانات تسلسلية أو تقنية دفتر الأستاذ الموزع. وعندما تحدث مجموعة من الإجراءات أو الوظائف المحددة مسبقًا، يتم تنشيط العقود الذكية تلقائيًا. وبمجرد تنشيطها، تكون العقود الذكية غير قابلة للإلغاء عادة، لكن لا يزال من الممكن تعقبها.

يُعد العقد الذكي أحد أكثر الابتكارات شيوعًا اليوم، وتُعرف العقود الذكية أحيانًا بشكل غير صحيح باسم "Dapp" على أنها برنامج كمبيوتر أو بروتوكول معاملات مصمم ليعمل تلقائيًا بعد استيفاء مجموعة من الشروط المحددة مسبقًا. ولا تحتوي العقود الذكية على أي صياغة قانونية أو التزامات تعاقدية ملزمة. بل هي "تصوص" كمبيوتر مصممة لتسهيل المعاملات دون استخدام طرف ثالث.

1-3-4-1: كيف تعمل العقود الذكية؟

تعمل العقود الذكية من خلال استغلال واحدة من أبسط تقنيات برمجة الكمبيوتر المعروفة لدى جميع المبرمجين ومهندسي البرمجيات تقريبًا، وهي عبارة "if" وفي الأساس، يتم ترميز العبارات التي تتبع المنطق "if...then" في قاعدة البيانات التسلسلية. وهذا يعني أن شبكة من أجهزة الكمبيوتر تنفذ إجراء (إجراءات) / معاملة (معاملات) (على سبيل المثال، تبادل المدفوعات) "إذا" حدثت مجموعة من الإجراءات المحددة مسبقًا (على سبيل المثال، أرسل كلا المتداولين تداولتهما). ثم يتم تحديث قاعدة البيانات التسلسلية، حيث تمت هذه المعاملة عند اكتمال المعاملة. ووفقًا لقاعدة البيانات التسلسلية وتقنية التشفير الخاصة بها، فهذا يعني أنه لا يمكن تغيير المعاملة ولن يتمكن من رؤية النتائج سوى من يمتلكون الإذن. وكما قد نتوقع، يمكن أن يحتوي العقد الذكي على العديد من شروط "if...then" حسب الحاجة لتلبية التزامات الأمان لمعاملة معينة. ومع ذلك، من المهم أن يكون لديك فريق من المطورين الموثوق بهم والحوكمة الشاملة القوية لنظام قاعدة البيانات التسلسلية لأن هذا سيؤثر على كيفية إنشاء العقود الذكية والشبكة في البداية وتنفيذها لاحقًا.

1-3-4-2: ما فوائد العقود الذكية؟

يوجد عدد من الفوائد لاستخدام العقود الذكية في المشهد الرقمي اليوم، والفوائد الرئيسية هي أن العقود الذكية تميل إلى أن تكون:

- **فعالة:** نظرًا لأن العقود الذكية رقمية بالكامل ويتم تشغيلها تلقائيًا، فإنها تتجنب العمليات المكلفة والطويلة، مثل ملء المستندات يدويًا وإدارة الأخطاء.
- **آمنة:** نظرًا لأن العقود الذكية موجودة على قاعدة البيانات التسلسلية، فإن السجلات والمعاملات مشفرة، ومسؤولة أمام جميع الأطراف الأخرى على السلسلة، وغير قابلة للتغيير (بمعنى أنه لا يمكن تغيير البرمجة).
- **شفافة:** كما ذكر أعلاه، بحكم طبيعة العمل على دفتر الأستاذ / الشبكة اللامركزية، يتمتع جميع المشاركين في السلسلة بالوصول إلى المعاملات التي ينفذها كل عقد ذكي. وهذا يجعل جميع أعضاء العملية مسؤولين أمام جميع الأطراف الأخرى المشاركة.

يتم تعريف Dapps ، أو "dApps" ، بدقة أكبر على أنها التطبيقات اللامركزية، وهي برامج كمبيوتر موزعة (مفتوحة المصدر غالباً) يتم إدارتها وتشغيلها على قاعدة البيانات التسلسلية أو شبكة نظير إلى نظير (P2P). ونظراً لطبيعة عملها اللامركزي، لا يتم التحكم فيها بشكل منفرد من قبل مؤلف أو شركة أو مؤسسة. وبدأ استخدام التطبيقات اللامركزية واعتمادها من قبل عدد من القطاعات المختلفة، بما في ذلك الألعاب والخدمات المصرفية والمالية، نظراً لتوفير قدر أكبر من الأمان والشفافية. وتستخدم التطبيقات اللامركزية العقود الذكية لتمكين وظائفها.

1-3-6: كيف تعمل التطبيقات اللامركزية؟

تستخدم التطبيقات اللامركزية العقود الذكية لتنفيذ قواعد محددة مسبقاً عبر التعليمات البرمجية، مما يلغي الحاجة إلى خوادم وقواعد بيانات مركزية (مما يزيل مخاطر الثغرات الأمنية ونقاط الفشل الفردية). وبالطريقة نفسها التي تعمل بها تطبيقات البرامج التقليدية، تستخدم التطبيقات اللامركزية التعليمات البرمجية للواجهة الأمامية لإجراء الاستدعاءات إلى الواجهة الخلفية، لكن في هذه الحالة، تعتمد الواجهة الخلفية على قاعدة البيانات التسلسلية أو شبكة نظير إلى نظير، التي تتألف بشكل أساسي من العقود الذكية، مما يتيح وظائف التطبيق.

1-3-6-1: أنواع التطبيقات اللامركزية

تم تطوير عدد من الأنواع المختلفة من التطبيقات اللامركزية لتحقيق اللامركزية في وظائف معينة والقضاء على الوسطاء. وبالمثل، على الرغم من عدم استخدامها على نطاق واسع، فقد تم دمج التطبيقات اللامركزية في مستعرضات الويب لتعمل كمكونات إضافية لتقديم الإعلانات، أو تتبع سلوك المستخدم، أو طلب تبرعات "مشفرة".

تتضمن بعض الأمثلة الأكثر شيوعاً للتطبيقات اللامركزية التي تم تطويرها، أو قيد التطوير، ما يلي:

- الخدمات المالية.
- الإسكان: تم تطوير تقنيات لامركزية لخفض تكاليف المعاملات عند شراء العقارات. وبالمثل، تم تصميم التطبيقات اللامركزية (Dapps) للمساعدة في تتبع ملكية العقارات وتوثيقها، مثل سندات الملكية.
- سلاسل التوريد: يتم استخدام التطبيقات اللامركزية لزيادة الشفافية والمساءلة من خلال تتبع السلع تلقائياً من خلال سلاسل التوريد الدولية.
- الأمن الإلكتروني والتحقق من الهوية: تبنى قطاع الأمن الإلكتروني التطبيقات اللامركزية كوسيلة محتملة لتخزين معلومات الهوية والتحقق منها بأمان.
- الرموز غير القابلة للاستبدال: يتم استخدام عدد من التطبيقات اللامركزية بشكل متساوٍ لتوفير سوق لامركزي لتداول الرموز غير القابلة للاستبدال. ويفضل العديد من المهتمين بهذا السياق التطبيقات اللامركزية بسبب فوائد الشفافية والأمان لاستخدام تقنية قاعدة البيانات التسلسلية للتداول.

- التعليم.
- الرعاية الصحية.

1-4: كيف تتعامل الشركات مع دمج تقنية البلوكتشين في المشتريات؟

1-4-1: تحديد الاستخدامات المثلى لتقنية البلوكتشين

يبدأ تطبيق تقنية البلوكتشين في المشتريات بتحديد العمليات التي يمكن أن تستفيد من هذه التقنية بشكل مباشر.

تشمل المجالات المحتملة:

إدارة أوامر الشراء: توثيق الطلبات وتتبعها بكفاءة.

إدارة العقود الذكية: لضمان التنفيذ الآلي للشروط المتفق عليها.

إدارة المخزون: تتبع الشحنات وضمان الدقة في البيانات.

الامتثال والتدقيق: توفير سجلات لا يمكن التلاعب بها لضمان الامتثال التنظيمي.

1-4-2: اختيار المنصة المناسبة

بعد تحديد المجالات المستهدفة، تختار الشركة منصة البلوكتشين التي تناسب احتياجاتها.

يمكن أن تكون:

منصات بلوك تشين خاصة (مرخصة): مثل Hyperledger Fabric أو R3 Corda، وهي توفر مزيداً من الأمان والتحكم وتكون مثالية للاستخدامات الداخلية.

منصات بلوكتشين عامة: مثل الإيثريوم، التي توفر شفافية كبيرة ولكن قد تكون أقل مرونة للأعمال التي تحتاج إلى خصوصية تامة.

عوامل تؤثر على الاختيار:

- الخبرة التقنية داخل الشركة.
- التكلفة الإجمالية للتنفيذ.
- متطلبات الأمان.
- اللوائح التنظيمية.
- عدد ونوع المستخدمين الذين سيحتاجون إلى الوصول للشبكة.

1-4-3: التطوير والاختبار

بمجرد اختيار التقنية المناسبة، تأتي مرحلة التطوير التي تتضمن:

- إنشاء العقود الذكية المبرمجة حسب احتياجات الشركة.
- اختبار النظام لضمان عمل العقود الذكية وفقاً للشروط المبرمجة، ولتجنب الأخطاء التي قد تؤثر على العمليات.
- التحقق من كفاءة المنصة في دعم العمليات وسرعتها.

1-4-4: التكامل مع الأنظمة القائمة

بعد تطوير النظام واختباره، تقوم الشركة بدمج تقنية البلوكتشين مع أنظمة إدارة المشتريات الحالية.

يتضمن ذلك:

- إعداد عمليات ربط البيانات بين المنصة الجديدة والأنظمة المستخدمة سابقاً، مثل أنظمة تخطيط الموارد المؤسسية (ERP).
- التأكد من توافق النظام مع عمليات الأعمال القائمة.

1-4-5: التدريب والتوعية

لا يقتصر النجاح على التنفيذ التقني فقط، بل يحتاج إلى تعاون الموظفين والموردين.

تدريب الفرق الداخلية على استخدام النظام الجديد.

تقديم إرشادات واضحة للموردين حول كيفية العمل على منصة البلوكتشين، بما في ذلك الاطلاع على العقود الذكية أو

تحديث سجلات الشحنات. [10]

1-5: تكامل البلوكتشين مع إنترنت الأشياء (IoT) وحل معضلة الأوراكل (The Oracle Problem)

على الرغم من الثورة التقنية التي تقدمها تقنية السجلات الموزعة والعقود الذكية في ضمان شفافية المعاملات وأتمتتها، إلا أنها تواجه تحدياً هيكلياً يُعرف بـ "معضلة الانعزال" أو "معضلة الأوراكل" (The Oracle Problem). تتلخص هذه المعضلة في أن شبكات البلوكتشين هي بيئات مغلقة وحتمية (Deterministic)، أي أنها لا تمتلك القدرة الذاتية على الاتصال بالعالم المادي الخارجي لمعرفة ما يجري فيه.

مما يشكل عقبة حقيقية في المشتريات العامة وسلاسل التوريد، فالعقد الذكي المبرمج لتحرير دفعة مالية لمورد معين لا يمكنه من تلقاء نفسه التحقق مما إذا كانت البضاعة قد وصلت حقاً إلى المستودعات الحكومية أم لا، أو ما إذا كانت

مطابقة لمواصفات الجودة المطلوبة. فالاعتماد على التدخل البشري لإدخال هذه التأكيدات إلى البلوكتشين يُعيدنا إلى خطر التلاعب، وتزوير محاضر الاستلام.

ولتجاوز هذه العقبة، برز مفهوم الدمج الاستراتيجي بين البلوكتشين وتقنية إنترنت الأشياء (BIoT)، حيث تعتمد تقنية إنترنت الأشياء (IoT) على تزويد البيئة المادية بشبكة من المستشعرات الذكية، مثل تقنيات التحديد بموجات الراديو (RFID)، ومستشعرات الوزن والحرارة، وأنظمة تحديد المواقع (GPS). تقوم هذه المستشعرات بجمع البيانات المادية في الزمن الفعلي دون أي تدخل بشري، حيث تعمل مستشعرات إنترنت الأشياء بمثابة "الحواس" التي ترصد العالم المادي بدقة، في حين تعمل شبكة البلوكتشين بمثابة "الدماغ الآمن" الذي يخزن هذه القراءات في سجلات غير قابلة للتعديل. ولنقل هذه البيانات من المستشعرات إلى العقود الذكية، يتم توظيف شبكات "الأوراكل" (Oracles) كجسور برمجية موثوقة.

وقد أثبتت الدراسات الحديثة المتقدمة، أن هذا الدمج (BIoT) يمثل الركيزة الأساسية لأتمتة سلاسل التوريد الحكومية، فهو يضمن أن التنفيذ الآلي للعقود الذكية مثل: تحرير المدفوعات أو فرض الغرامات، يستند حصراً إلى أحداث مادية موثقة بشكل مشفّر، بالتالي هذا يمنع التلاعب البشري ويحقق مفهوم الرقابة الاستباقية في المشتريات العامة.[11]

1-6: التحديات الرئيسية لاستخدام تقنية البلوكتشين والعقود الذكية في المشتريات

رغم الفوائد العديدة التي تقدمها تقنية البلوكتشين والعقود الذكية، إلا أن هناك تحديات كبيرة تواجه الشركات عند تبنيها، ومنها:

1. التوحيد القياسي والتوافق بين الأنظمة

- التنوع في شبكات البلوكتشين: يوجد العديد من منصات البلوكتشين، مثل الايثيريوم و Corda و Hyperledger Fabric، ولكل منها تقنيات وبروتوكولات برمجية مختلفة.
- غياب المعايير الصناعية: لا توجد حتى الآن معايير موحدة لتقنيات البلوكتشين، وبالتالي قد تواجه الشركات صعوبة في اختيار المنصة الصحيحة.
- مشكلة التوافق: إذا استثمرت شركة في نظام معين، مثل الايثيريوم، ثم أصبح Hyperledger المعيار الصناعي، فقد تجد صعوبة في العمل مع الموردين الذين يستخدمون منصات أخرى.

2. الامتثال والتنظيم

- غياب الإطار القانوني الواضح: العقود الذكية غالباً ما تحل محل العقود التقليدية الورقية، ومع ذلك لا يزال من غير الواضح مدى قانونية العقود الذكية في بعض الدول.
- التفاوت بين الدول: تختلف القوانين والتنظيمات المتعلقة بتقنية البلوكتشين من بلد إلى آخر مما يجعل المعاملات الدولية أكثر تعقيداً.

- الالتزامات القانونية: قد تكون هناك تحديات في إثبات الالتزام بشروط العقود الذكية في المحاكم إذا لم تكن هذه العقود معترف بها قانونياً.

3. التكلفة والتعقيد التقني

- التكاليف المرتفعة للتطوير: تطوير حلول قائمة على البلوكتشين والعقود الذكية يتطلب استثمارات كبيرة.
- نقص الخبرة التقنية: قد يكون العثور على مطورين وخبراء متخصصين في البلوكتشين مكلف وصعب.
- صعوبة التكامل: دمج تقنية البلوكتشين مع الأنظمة الحالية للشركة قد يكون معقد ويستغرق وقت طويلاً.

4. المخاطر الأمنية وأخطاء العقود الذكية

- الثغرات البرمجية: العقود الذكية تعتمد على البرمجة الدقيقة، وأي خطأ صغير في الكود قد يؤدي إلى خسائر كبيرة أو تعطل العمليات.
- المخاطر الأمنية: رغم أن البلوكتشين يُعتبر آمناً بشكل عام، إلا أن العقود الذكية نفسها قد تكون عرضة للاختراق إذا لم تُبرمج بشكل صحيح. [10], [11], [12]

5. هجوم 51%

يشير هجوم 51% إلى حالة يتحكم فيها مشارك واحد في الشبكة أو مجموعة من المشاركين في أكثر من 50% من قوة الحوسبة للشبكة. يمكن للمهاجمين القيام بأنشطة سلبية متعددة، إذ يمكنهم منع تأكيد بعض المعاملات، وبالتالي إيقاف المدفوعات ذات الصلة، كما يمكنهم عكس بعض المعاملات التي حدثت عندما كانوا بالفعل مسؤولين عن الشبكة. بالإضافة إلى ذلك، يمكنهم أيضاً منع المشاركين الآخرين من التعدين، مما يؤدي إلى ما نسميه احتكار التعدين، ومع ذلك، لا يمكنهم عكس المعاملات التي حدثت قبل أن يتحكموا في الشبكة. [13]

1-6-1: كيفية التعامل مع تحديات استخدام البلوكتشين والعقود الذكية في المشتريات

1. تعزيز التوحيد القياسي والتوافق

- اختيار منصات بلوكتشين مرنة تُسهل التكيف مع الأنظمة الأخرى.
- متابعة التطورات في المعايير الصناعية لضمان توافق الأنظمة.

2. إدارة الامتثال والتنظيم

- التعاون مع مستشارين قانونيين محليين ودوليين لفهم اللوائح ذات الصلة.
- توثيق العقود الذكية بطريقة تعكس العقود التقليدية لضمان الامتثال القانوني.

3. تقليل التكلفة وتعزيز المهارات

- بدءاً من المشاريع التجريبية الصغيرة لتقليل التكاليف والاختبار.
- الاستثمار في تدريب الموظفين أو التعاون مع شركات متخصصة للحصول على الدعم الفني.

4. الحد من المخاطر الأمنية

- إجراء مراجعات دقيقة للكود المستخدم في العقود الذكية.
- استخدام تقنيات الأمان الحديثة واختبار المنصات بانتظام للكشف عن الثغرات الأمنية. [19], [12]

1-7: الخاتمة

لقد أظهر هذا الفصل أن المشتريات العامة تمثل عصباً رئيسياً للاقتصاد الحكومي، إلا أنها لا تزال ترزح تحت وطأة تحديات تقليدية معقدة تتمثل في الافتقار إلى دقة البيانات، وضعف التواصل، ومخاطر الاحتيال والفساد، والاعتماد المفرط على العمليات اليدوية. وقد أثبتت الدراسة النظرية أن التحول الرقمي لم يعد خياراً، بل ضرورة ملحة لمعالجة هذه الفجوات البنيوية ومواجهة الهدر المالي.

بناءً على ما سبق، ونظراً للقيود العملية التي تمنع التطبيق التجريبي المباشر لهذه التقنيات الحديثة على بنية تحتية حكومية حقيقية، تبرز الحاجة الماسة للانتقال من الإطار النظري إلى مرحلة التصميم العملي والتطبيقي.

لذا، سيُخصص الفصل الثاني لتقديم تصميم معماري متقدم (Architecture Design) يعتمد على بناء "نموذج محاكاة هجين" (Hybrid Simulation Model).

الفصل الثاني:

الهيكالية المعمارية الهجينة لنظام المشتريات العامة
المؤتمت (نموذج محاكاة)

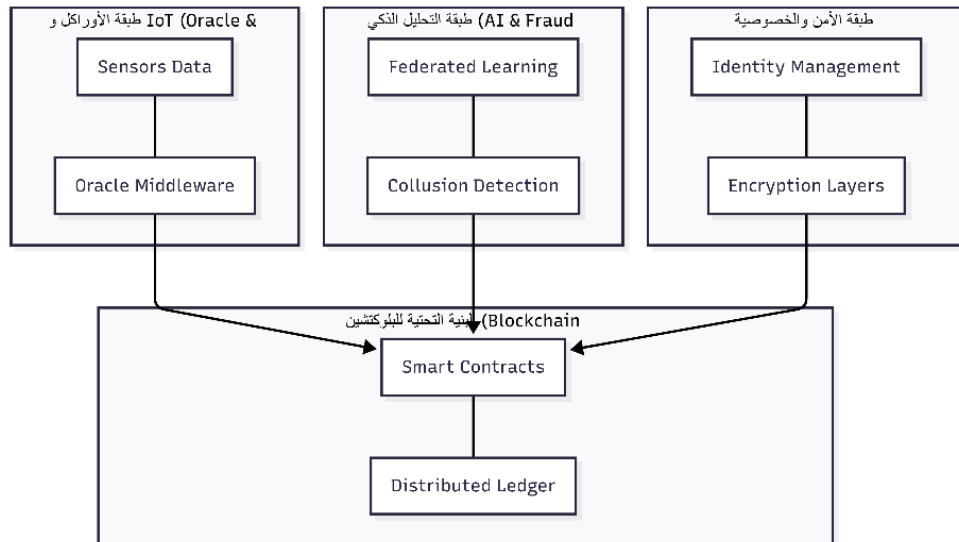
1-2: مقدمة الفصل:

يقدم هذا الفصل تصميماً معمارياً (Architecture Design) متقدماً ونموذج محاكاة لنظام مشتريات عامة يعتمد على تكامل تقنيات السجلات الموزعة (Blockchain) مع إنترنت الأشياء (BIoT) وخوارزميات تحليل البيانات اللامركزية. نظراً للقيود العملية التي تمنع التطبيق التجريبي المباشر على بنية تحتية حكومية حقيقية، اعتمدنا في هذه الدراسة على بناء "نموذج محاكاة هجين" (Hybrid Simulation Model) يثبت الجدوى التقنية والأمنية للنظام.

تم تقسيم الهيكلية المقترحة إلى ثلاث طبقات مترابطة تتبادل البيانات بشكل آمن ومؤتمت إلى أربع طبقات:

1. طبقة البنية التحتية (Consortium Blockchain) .
2. طبقة الاستشعار اللامركزي (Decentralized Oracles/BIoT) .
3. وطبقة التحليل الذكي (Federated Learning) .
4. طبقة الأمن السيبراني ونمذجة التهديدات (Cybersecurity & Threat Modeling) .

الشكل (2-2): (System Architecture) يستخدم نظام الطبقات (Subgraphs) لإظهار تراكم الطبقات الأربع: (البنية التحتية، الأوراكل، التحليل الذكي، والأمن السيبراني).



الشكل (2-2): مخطط الهيكلية المعمارية الشاملة (System Architecture)

2-2: الطبقة الأولى: البنية التحتية للبلوكتشين التحالف (Consortium Blockchain Layer)

لا يمكن استخدام الشبكات العامة (Public Blockchains) مثل "إيثريوم" أو "بيتكوين" في المشتريات العامة نظراً لافتقارها إلى ضوابط الخصوصية المطلوبة للبيانات الحكومية. بدلاً من ذلك، نقترح في هذا التصميم المعماري استخدام "بلوكتشين تحالفي مصرح به" (Permissioned Consortium Blockchain) .

2-2-1: المكونات الهيكلية للشبكة (Network Topology)

في هذا النموذج، تتكون الشبكة من مجموعة من العقد (Nodes) التي تمثل الجهات الحكومية ذات الصلة (مثل: وزارة المالية، ديوان المحاسبة، والوزارة صاحبة المناقصة). لا يُسمح لأي جهة خارجية بالانضمام للشبكة كعقدة تحقق إلا بإذن مسبق، مما يقلل من احتمالية الهجمات السيبرانية من نوع الحرمان من الخدمة الموزع (DDoS) .

تنقسم العقد في هذه الطبقة برمجياً إلى:

1. عقد المصادقة (Endorsing Nodes): تقوم بمحاكاة تنفيذ العقد الذكي (Smart Contract) للتحقق من صحة العطاء المقدم.
2. خدمة الترتيب (Ordering Service): تقوم بتجميع المعاملات الصالحة وترتيبها زمنياً في كتل (Blocks) .
3. عقد التخزين (Committing Nodes): تحتفظ بنسخة مشفرة ومحدثة من دفتر الأستاذ (Ledger) .

2-2-2: الآلية الرياضية للتشفير والربط (Cryptographic Hashing Mechanism)

لحماية ملفات وعروض الموردين، يعتمد النظام على التشفير غير المتماثل (Asymmetric Cryptography) باستخدام مفاتيح عامة وخاصة (Public/Private Keys) .

عندما يقوم المورد برفع عرض السعر، يتم تمرير الملف عبر خوارزمية تجزئة (مثل SHA-256) لتوليد بصمة رقمية فريدة (Hash) للملف، ويتم تسجيل هذا الـ Hash في الشبكة بدلاً من الملف الفعلي لتقليل العبء التخزيني. يتم تشفير الرسائل باستخدام المفتاح العام، ولا يمكن فك تشفيرها إلا من قبل الجهة المخولة التي تملك المفتاح الخاص.

يتم بناء الكتلة (B_n) وربطها بالكتلة السابقة (B_{n-1}) كالتالي:

كل كتلة تحتوي على ترويسة (Header) وبيانات (Data) .

ترويسة الكتلة الحالية (H_n) تعتمد بشكل مشفر على ترويسة الكتلة السابقة (H_{n-1}) ، بحيث:

$$H_n = Hash(H_{n-1} + Timestamp + Nonce + MerkleRoot(T_x)) \dots (1)$$

حيث أن:

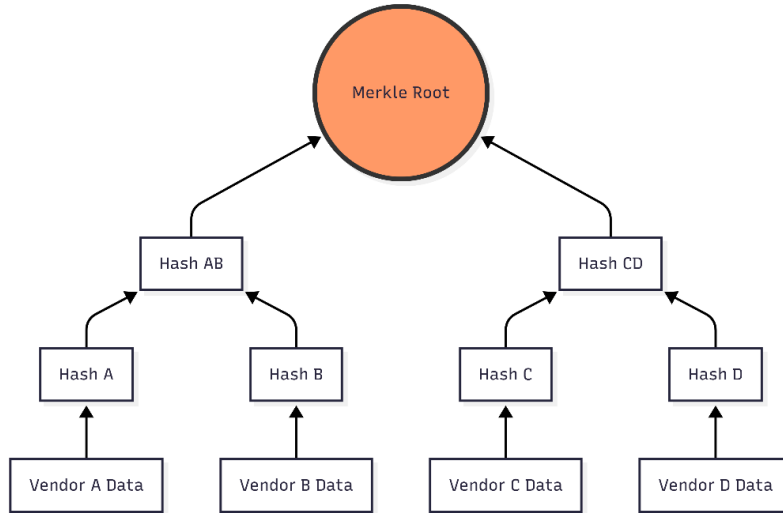
H_{n-1} : تجزئة الكتلة السابقة (ضمان سلسلة غير قابلة للتعديل).

$MerkleRoot(T_x)$: الجذر الشجري لجميع معاملات المناقصة (T_x) داخل الكتلة، إذا تم التلاعب بحرف واحد في

عرض السعر لأي مورد، يتغير الـ Hash الخاص به، مما يغير الـ Merkle Root ، لتتأثر صلاحية الكتلة بالكامل فوراً ويرفضها النظام. هذه الآلية تضمن استحالة التلاعب بالبيانات وتوفر دليلاً قطعياً عند التدقيق.

مخطط شجرة ميركل (Merkle Tree Diagram) يوضح كيف يتم تحويل عروض الموردين إلى (Hashes) وربطها ببعضها

لضمان عدم التلاعب.



الشكل (2-3): مخطط شجرة ميركل (Merkle Tree Diagram)

2-3: دورة حياة المعاملة برمجياً (Transaction Flow) في العطاءات

لتوضيح الآلية العملية في المحاكاة، يتم تمثيل تقديم العطاء برمجياً بالخطوات التالية:

1. بدء المعاملة (Transaction Proposal) : تقوم عقدة المورد بإنشاء معاملة مشفرة تمثل "عرض السعر" وإرسالها

إلى شبكة النظراء (Peer-to-peer network) .

2. التحقق اللامركزي (Decentralized Validation): تستقبل عقد المصادقة الحكومية المعاملة. بدلاً من موظف

بشري، تتحقق الخوارزمية من هوية المورد وصلاحيه العرض.

3. تكوين الكتلة (Block Formation): بعد مصادقة الأغلبية، يتم إرسال المعاملة إلى خدمة الترتيب لتشكيل كتلة

جديدة تضاف إلى السجل العام للبلوكتشين.

4. التنفيذ الذكي (Execution): بمجرد انتهاء موعد المناقصة، يتم استدعاء "العقد الذكي" لفتح العروض آلياً،

تقييمها بناءً على معايير مشفرة مسبقاً، وإرسال النتيجة إلى البلوكتشين دون أي تدخل أو تحيز بشري.

2-4: خصوصية الموردين باستخدام إثبات المعرفة الصفرية (Zero-Knowledge Proofs -

ZKPs)

تُعد حماية البيانات المالية والأسرار التجارية للموردين تحدياً رئيسياً حتى ضمن البيانات المصرح بها مثل "بلوكتشين التحالف".

ولمعالجة هذه الثغرة وتأمين بيئة تنافسية موثوقة في المحاكاة المقترحة، اعتمدنا دمج تقنية إثبات المعرفة الصفرية (ZKPs)

في طبقة التحقق. حيث يمكن للنظام التأكد من استيفاء المورد لشروط المناقصة مثل: إثبات امتلاكه لسيولة مالية تفوق

المليون دولار عبر خوارزميات (Zk-SNARKs)، إذ يتم التحقق عبر توليد دليل رياضي يؤكد للعقد الذكي أن رصيد المورد

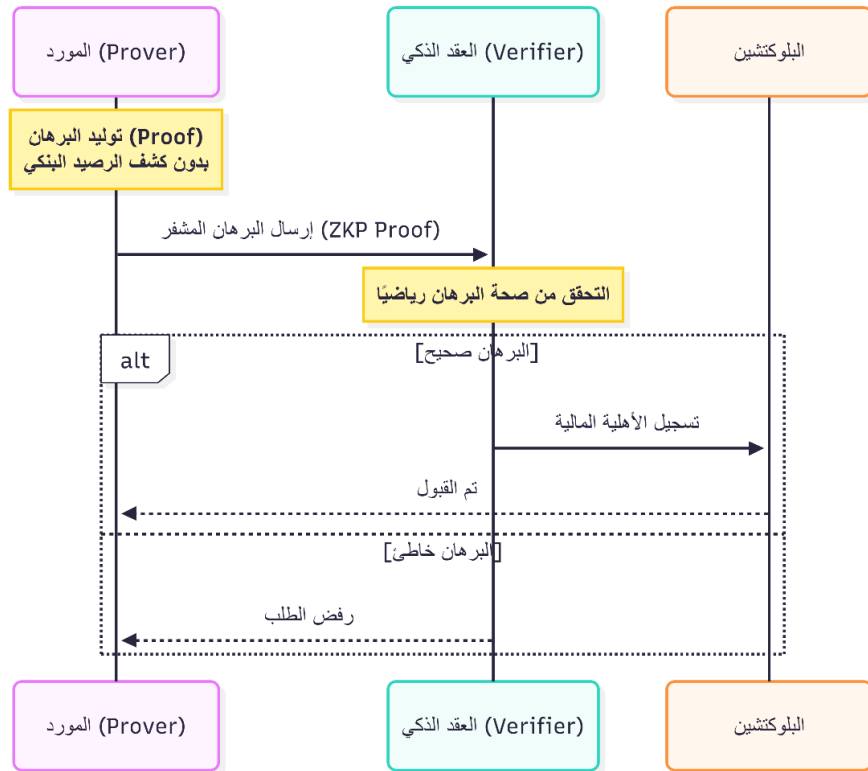
يستوفي الشرط (True/False) فقط، دون الكشف عن الرقم الدقيق للرصيد، ومبدون مشاركة كشوفات الحساب البنكية مع

بقية العقد الحكومية أو المنافسين.

وهذا بدوره يرفع خصوصية المشارك، ويعزز ثقته في النظام المؤتمت، كما يشجع كبرى الشركات على المشاركة دون خوف

من التجسس الصناعي.

مخطط تدفق إثبات المعرفة الصفريّة (ZKP Flow) يوضح رحلة البيانات من المورد (Prover) إلى العقد الذكي (Verifier) وكيف يتم التأكد من الأهلية المالية دون كشف الأرقام الحقيقية.



الشكل (4-2): مخطط تدفق إثبات المعرفة الصفريّة (ZKP Flow)

5-2-2: إدارة هويات الموردين عبر الهوية الذاتية اللامركزية (Self-Sovereign Identity – SSI)

من أكبر التحديات في أتمتة المناقصات العامة هي التأكد من هوية الموردين وتجنب التعامل مع الكيانات الوهمية. لذلك، بدلاً من الاعتماد على قواعد بيانات مركزية لتسجيل حسابات الموردين (والتي تشكل نقطة فشل مفردة للقرصنة)، فإن النظام يمنح كل مورد "معرفًا لا مركزيًا" (Decentralized Identifier - DID) محميًا بالتشفير.

آلية العمل هنا تعتمد على أن المورد يحتفظ بوثائقه الرسمية مثل: السجل التجاري، التخليص الضريبي وشهادات الجودة بصيغة "شهادات قابلة للتحقق" (VCs) داخل محفظته الرقمية. وبمجرد أن يتقدم للعطاء، يتولى العقد الذكي مهمة مطابقة التوقيعات التشفيرية لهذه الوثائق لحظيًا. هذا النهج يلغي تمامًا الحاجة للتدقيق الورقي اليدوي، ويضمن لنا الموثوقية التامة للوثائق من مصدرها الحكومي.

2-3: الطبقة الثانية: شبكات الأوراكل اللامركزية وإنترنت الأشياء (IoT & Decentralized Oracles Layer)

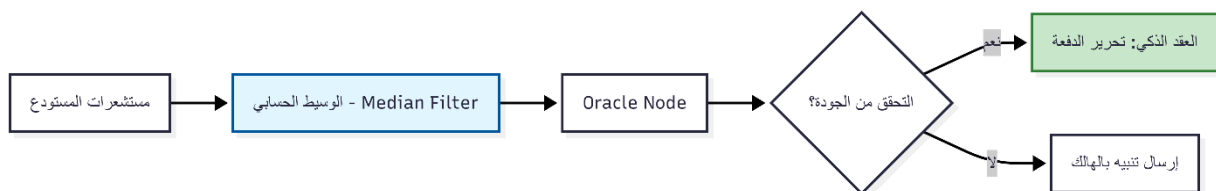
2-3-1: معضلة الانعزال (The Oracle Problem) في المشتريات العامة

تتميز العقود الذكية على البلوكتشين بأنها "حتمية" (Deterministic) وتعمل في بيئة معزولة تمامًا، أي أنها لا تستطيع جلب البيانات من خارج الشبكة بشكل ذاتي. في سياق المشتريات العامة، لكي يقوم العقد الذكي بتحويل الدفعة المالية للمورد آليًا، فإنه يحتاج إلى إثبات مادي يضمن وصول البضاعة إلى المستودع الحكومي بالمواصفات المطلوبة. هنا تبرز الحاجة إلى دمج إنترنت الأشياء (IoT) مع البلوكتشين لإنشاء بيئة (BioT)، واستخدام "الأوراكل" (Oracles) كجسور لنقل هذه البيانات. [11]

2-3-2: معمارية إنترنت الأشياء (BioT) كمصدر للبيانات

في محاكاة النظام المقترح، يتم تزويد البضائع أو المستودعات بمستشعرات ذكية (مثل مستشعرات RFID لتتبع الموقع، أو مستشعرات وزن وحرارة لضمان جودة المواد الحساسة كالأدوية). تقوم هذه المستشعرات بتسجيل البيانات الحية وإرسالها إلى شبكة الأوراكل. يضمن هذا الدمج (BioT) إزالة التدخل البشري في عمليات الاستلام والتسليم، مما يلغي إمكانية التلاعب في محاضر الاستلام الورقية.

يوضح المخطط التالي يوضح استلام البضاعة في المستودع، قراءة المستشعرات، فلترة البيانات عبر "الوسيط الحسابي" (Median)، ثم إرسال التأكيد للعقد الذكي. [16], [11]



الشكل (2-5): مخطط تدفق الأوراكل وإنترنت الأشياء (BioT Flow)

2-3-3: آلية الإجماع اللامركزي للأوراق (Decentralized Oracle Consensus)

لتجنب نقطة الفشل المركزية (Single Point of Failure)، لا يعتمد النظام على مستشعر واحد أو مصدر بيانات (API) حكومي واحد لإبلاغ العقد الذكي، بل يعتمد على "شبكة أوراق لا مركزية". تتكون هذه الشبكة من عدة عقد (Nodes) تقوم بجلب البيانات من عدة مستشعرات، ثم يتم تطبيق خوارزمية رياضية للوصول إلى "قيمة توافقية" (Aggregated Value) قبل إرسالها إلى العقد الذكي.

الآلية الرياضية لفلتر البيانات (Mathematical Data Aggregation):

لنفترض أن النظام ينتظر تأكيداً حول كمية الإسفلت الموردة لمشروع طرق. لدينا مجموعة من عقد الأوراق المستقلة

$$O = \{o_1, o_2, \dots, o_n\} \dots (2)$$

كل عقدة تقدم قراءة للوزن u_i .

لتجنب القراءات الخاطئة (بسبب عطل في مستشعر معين أو هجوم سيبراني)، يرمج النظام لحساب "القيمة الوسيطة"

(Median) بدلاً من المتوسط الحسابي (Mean)، لأن الوسيط غير حساس للقيم المتطرفة (Outliers) :

$$V_{agg} = Median(u_1, u_2, \dots, u_n) \dots (3)$$

ثم يقوم النظام بحساب الانحراف (Deviation) لكل قراءة عن القيمة الوسيطة:

$$D_i = |u_i - V_{agg}| \dots (4)$$

إذا كان الانحراف D_i يتجاوز حد التسامح المسموح به θ (والذي يحدد مسبقاً في العقد الذكي بناءً على طبيعة المادة)، يتم

استبعاد القراءة u_i ومعاينة العقدة o_i بخفض نقاط سمعتها (Reputation Score) في الشبكة.

هذه المعالجة الرياضية تضمن دقة وموثوقية البيانات الفيزيائية المدخلة إلى البلوكتشين. والجدول (2-3) يوضح الرموز

الرياضية المستخدمة في نمذجة خوارزميات الأوراق واكتشاف الشذوذ:

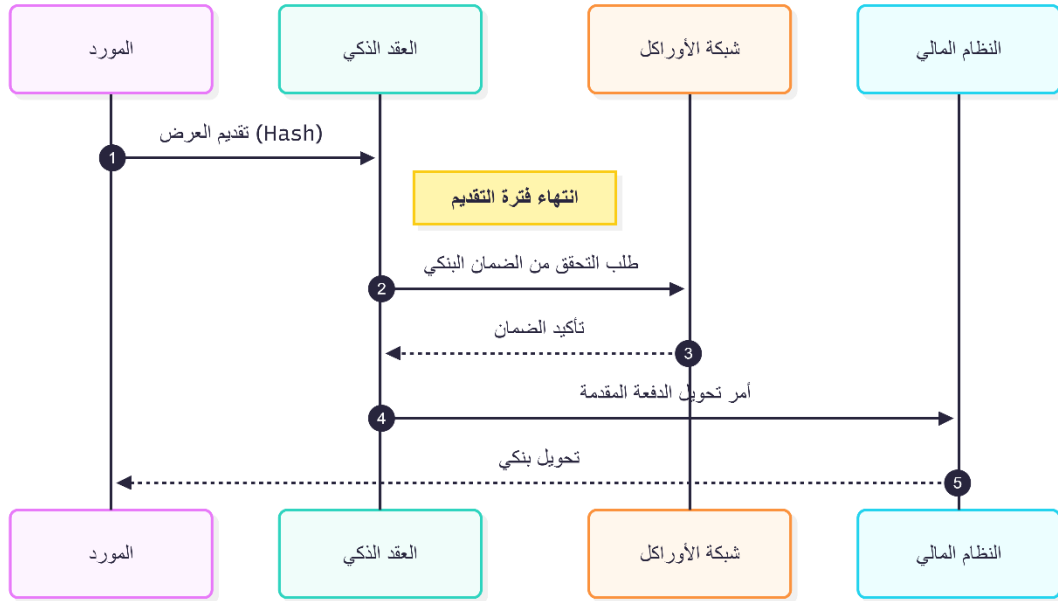
جدول (2-3): الرموز الرياضية المستخدمة في نمذجة خوارزميات الأوراق

الرمز (Symbol)	الدلالة البرمجية/الرياضية (Description)	الاستخدام في النظام
H_n	تجزئة الكتلة الحالية (Current Block) (Hash)	التشفير والربط في البنية التحتية (Layer ₁)
MerkleRoot	الجذر الشجري للمعاملات	التحقق من عدم تلاعب أي مورد في عرض سعر
O	مجموعة عقد الأوراق $\{O_1, O_2, \dots, O_n\}$	تمثيل شبكة المستشعرات اللامركزية (Layer ₂)
Vagg	القيمة التوافقية (Aggregated) (Value/Median)	فترة قراءات المستشعرات الخاطئة قبل الدفع
D_i	الانحراف عن القيمة الوسيطة (Deviation)	عزل المستشعرات المخترقة أو المعطلة
X_i	متجه بيانات العطاء (Data Vector)	يضم (السعر، وقت التسليم، تقييم المورد) للتحليل
d(X_{new,C})	المسافة الإحصائية عن العروض الطبيعية	اكتشاف التواطؤ والمبالغة في الأسعار (Layer ₃)
R_{s,t}	التقييم البيئي التراكمي للمورد	التسعير البيئي الديناميكي (المشتريات الخضراء)

4-3-2: محاكاة برمجية للعقد الذكي (Smart Contract Simulation)

لانتقال بهذا التصميم المعماري من الإطار النظري إلى نموذج عملي يمكن قياسه وتقييمه، توجب علينا بناء بيئة محاكاة برمجية تحاكي تعقيدات المشتريات العامة في الواقع. ونظراً لأن النظام الذي نطرحه هو نظام "هجين"، فقد تطلب الأمر توظيف مزيج متكامل من الأدوات واللغات البرمجية.

يوضح المخطط التالي التفاعل الزمني بين المورد، العقد الذكي، شبكة الأوراكل، والتحويل المالي.



الشكل (2-6): مخطط التسلسل للعقد الذكي (UML Sequence)

على مستوى طبقة التنفيذ المالي، اعتمدنا لغة (Solidity) لبرمجة العقود الذكية، مبررين هذا الاختيار بكونها المعيار الهندسي الأبرز لضمان التنفيذ الحتمي والصارم لشروط المناقصات. في المقابل، تطلب الجانب التحليلي — المتمثل في فترة بيانات الأوراكل — مرونة رياضية وقدرة معالجة مختلفة، ولذا استخدمنا لغة (Python) للاستفادة من مكتباتها المتقدمة في معالجة البيانات.

أولاً: التنفيذ المالي الآلي (Smart Contract)

يوضح المقطع البرمجي التالي (Pseudo-code) المنطق الأساسي للعقد الذكي المكتوب بلغة Solidity، والذي يتم نشره على شبكة البلوكتشين لانتظار التأكيدات الخارجية وتميرير الدفعات المالية للموردين آلياً:

```

1 // تعريف العقد الذكي للمشتريات العامة
2 Contract PublicProcurement {
3     Enum State { Created, Dispatched, Delivered, Paid }
4     State public contractState;
5     Uint public paymentAmount;
6     Address payable public supplier;
7     Address public oracleAddress;
8     // حدث يتم إطلاقه لطلب البيانات من العالم الخارجي
9     Event RequestDeliveryData(bytes32 queryId, string deliveryLocation);
10
11     Constructor(address _supplier, uint _amount, address _oracle) {
12         Supplier = payable(_supplier);
13         paymentAmount = _amount;
14         oracleAddress = _oracle;
15         contractState = State.Created;
16     }
17     // الخطوة 1: طلب التحقق من استلام البضاعة (يستدعي الأوراكل)
18     Function triggerDeliveryCheck(string memory _location) public {
19         Require(contractState == State.Dispatched, "Goods not dispatched yet");
20         Bytes32 queryId = keccak256(abi.encodePacked(block.timestamp, _location));
21         // إطلاق الحدث الذي تلتقطه شبكة الأوراكل

```

الشكل (2-7): الجزء الأول من كود Solidity

```

21         // إطلاق الحدث الذي تلتقطه شبكة الأوراكل
22         Emit RequestDeliveryData(queryId, _location);
23     }
24
25     // التي ينفذها الأوراكل فقط (Callback) الخطوة 2: دالة الاستدعاء
26     Function fulfillDeliveryCheck(bytes32 _queryId, bool _isDeliveredLocally) public {
27         Require(msg.sender == oracleAddress, "Unauthorized: Only Oracle can update status")
28         // حماية أمنية: لا يقبل الاستجابة إلا من الأوراكل المعتمد
29         If (_isDeliveredLocally == true) {
30             contractState = State.Delivered;
31             executePayment();
32         }
33     }
34     // الخطوة 3: التنفيذ المالي الآلي
35     Function executePayment() internal {
36         Require(contractState == State.Delivered, "Conditions not met");
37         contractState = State.Paid;
38         supplier.transfer(paymentAmount);
39     }
40 }
41 // تحويل مالي مؤتمت
42

```

الشكل (2-8): الجزء الثاني من كود Solidity

ثانياً: خوارزمية الإجماع اللامركزي للأوراكل (Oracle Consensus)

ولكي يتمكن العقد الذكي المذكور أعلاه من اتخاذ قرار الدفع بأمان، يجب فلترة البيانات القادمة من المستشعرات الفيزيائية.

يوضح المقطع البرمجي التالي (Pseudo-code) خوارزمية الإجماع اللامركزي المكتوبة بلغة بايثون Python، والتي تعمل

داخل شبكة الأوراكل لعزل القراءات الشاذة قبل إرسال التأكيد النهائي للبلوكتشين:

```
1 # خوارزمية الإجماع اللامركزي لشبكة الأوراكل (فلتر بيانات المستشعرات)
2 def oracle_consensus_mechanism(sensor_readings, tolerance_threshold):
3     # sensor_readings: (مثلاً وزن البضاعة) مصفوفة تحتوي على قراءات المستشعرات المتعددة
4     # 1. حساب القيمة الوسطية (Median) لتجنب تأثير القيم المتطرفة
5     median_value = calculate_median(sensor_readings)
6     valid_readings = []
7
8     # 2. تصفية القراءات الشاذة أو المستشعرات المعطلة/المختربة
9     for reading in sensor_readings:
10         # حساب الانحراف عن القيمة الوسطية
11         deviation = abs(reading.value - median_value)
12         if deviation <= tolerance_threshold:
13             valid_readings.append(reading)
14             # قراءة مقبولة
15         else:
16             penalize_sensor_node(reading.sensor_id)
17             # خفض التقييم الموثوق للمستشعر وعزله (Quarantine)
18             log_security_warning(f"تم رصد قراءة شاذة من المستشعر {reading.sensor_id}")
19
20     # 3. التأكد من وجود عدد كافٍ من القراءات الصحيحة لتحقيق الإجماع
21     if len(valid_readings) >= MIN_REQUIRED_NODES:
22         # إرسال النتيجة الموثقة نهائياً إلى العقد الذكي في البلوكتشين لتنفيذ الدفع
23         trigger_smart_contract(median_value)
24     else:
25         # تجميد العملية وإطلاق إنذار للتدقيق البشري
26         raise_smart_contract_freeze("فشل الإجماع: تناقض عالي ومشبوه في قراءات المستشعرات")
27
28
```

الشكل (2-9): كود Python الممثل لخوارزمية الإجماع اللامركزي.

2-3-5: تحليل الأداء في المحاكاة

من خلال تطبيق هذه الطبقة في المحاكاة، نلاحظ تقليص "نقاط الاحتكاك" (Friction Points).

فبدلاً من تشكيل لجان استلام بشرية قد تتعرض لضغوط أو رشاي لقبول مواد غير مطابقة، تقوم خوارزميات الـ BioT والعقود الذكية بتنفيذ عملية التحقق والدفع في زمن يقاس بالثواني بمجرد تطابق القراءات الفيزيائية مع الشروط المشفرة مسبقاً.

2-4: الطبقة الثالثة: طبقة تحليل البيانات والتعلم اللامركزي (Data Analytics & Federated Learning Layer)

2-4-1: التحدي التحليلي في المشتريات العامة

تولد المشتريات العامة كميات هائلة من البيانات (أسعار، مواصفات، أوقات تسليم، تقييمات موردين).

في الأنظمة المركزية التقليدية، تظل هذه البيانات حبيسة في قواعد بيانات كل وزارة على حدة (Data Silos)، مما يجعل من المستحيل تحليل الصورة الكبرى لاكتشاف عمليات الاحتكار أو التلاعب بالأسعار (Bid-rigging) على مستوى الدولة.

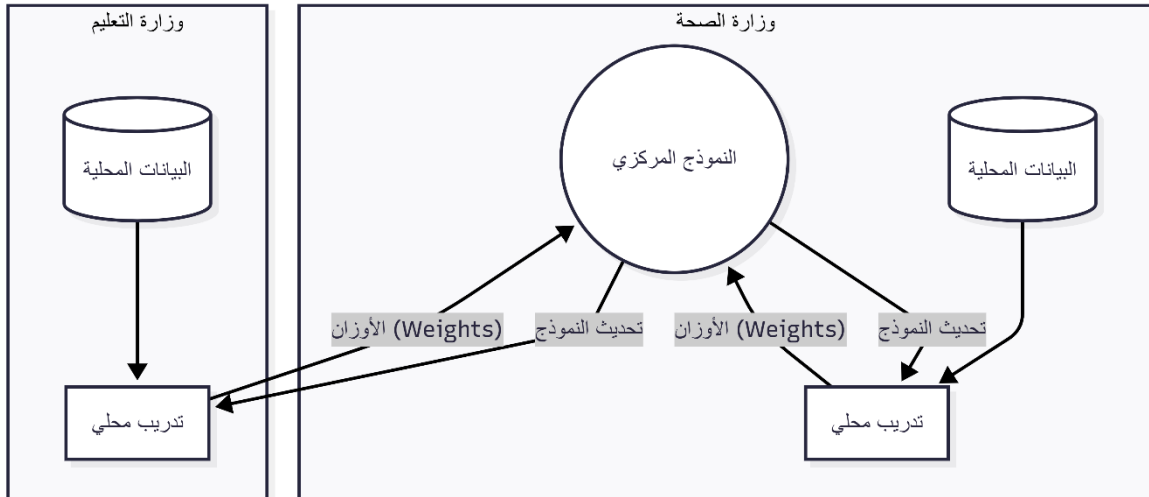
ورغم أن تقنية Blockchain توفر سجلاً موحداً وغير قابل للتعديل، إلا أن الجهات الحكومية غالباً ما ترفض مشاركة بيانات مشترياتها التفصيلية لأسباب تتعلق بالسرية والأمن القومي. هنا يأتي دور محاكاة دمج تقنيات "تحليل البيانات اللامركزي" (Decentralized Data Analytics) وتحديدًا "التعلم الموحد" (Federated Learning) في الهيكلية المقترحة. [18]

2-4-2: هيكلية التعلم الموحد لاكتشاف التواطؤ (Collusion Detection Architecture)

بدلاً من جمع البيانات من جميع الوزارات في قاعدة بيانات مركزية لتحليلها، تقوم الهيكلية المقترحة بآلية عكسية: يتم إرسال "نموذج التحليل" (Analytics Model) إلى البيانات.

تعمل المحاكاة وفق الخطوات التالية:

1. التدريب المحلي (Local Training) : تمتلك كل عقدة حكومية (Node) في شبكة البلوكتشين خوارزمية تحليل بيانات محلية، تقوم هذه الخوارزمية بتحليل سجلات المشتريات المشفرة الخاصة بالوزارة لاكتشاف الأنماط غير الطبيعية (مثل: مورد معين يفوز دائماً بالمناقصات عندما يكون مورد آخر هو المنافس الوحيد).
 2. تحديث الأوزان (Weight Updates) : لا تقوم العقدة بمشاركة بيانات الموردين، بل تشارك فقط "نتائج التعلم" أو ما يسمى بالأوزان الرياضية (Model Weights) مع العقد الأخرى عبر القنوات المشفرة للبلوكتشين.
 3. التجميع (Aggregation) : يقوم العقد الذكي في الشبكة بتجميع هذه الأوزان لتحديث النموذج التحليلي العام، مما يجعله أكثر ذكاءً في اكتشاف الفساد والمبالغة في الأسعار بناءً على خبرات جميع الوزارات، مع بقاء البيانات الأصلية في أماكنها الجغرافية الآمنة.
- يوضح المخطط التالي تدريب النماذج داخل خوادم الوزارات ومشاركة الأوزان الرياضية (Weights) فقط مع المركز لتحديث نموذج اكتشاف الفساد.



الشكل (2-10): مخطط التعلم الموحد (Federated Learning)

لإثبات القدرة على دمج تحليل البيانات مع أمن البلوكتشين، يوضح هذا الكود المنطق البرمجي لخوارزمية الذكاء الاصطناعي التي تعمل محلياً (Local Node) داخل خوادم الجهة الحكومية. صُمم هذا الكود بلغة Python ليقوم باكتشاف الشذوذ

والتلاعب في الأسعار، ومشاركة الأوزان الرياضية فقط مع الشبكة، مع الحفاظ التام على سرية بيانات الموردين داخل خوادم الجهة الحكومية:

```

1  # خوارزمية التعلم الموحد لاكتشاف التواطؤ في المشتريات (تعمل محلياً)
2  Def federated_anomaly_detection(local_bids_data, global_model_weights):
3  # 1. تحميل الأوزان العالمية المحدثة القادمة من شبكة البلوكتشين
4      Local_model.set_weights(global_model_weights):
5      Anomalies_detected = []
6
7  # 2. تحليل العطاءات المحلية الحالية (الأسعار، سجل المورد، وقت التسليم)
8  For bid in local_bids_data:
9  # حساب المسافة الإحصائية (نقاط الشذوذ) للعرض الحالي
10     Anomaly_score = local_model.predict_anomaly_score(bid.features)
11     If anomaly_score > ANOMALY_THRESHOLD:
12     # وسم العطاء كمشبوه (احتمالية تلاعب في السعر أو احتكار)
13     Anomalies_detected.append(bid.id)
14     Flag_bid_for_human_audit(bid.id, anomaly_score, reason="تجاوز الحد المسموح للشذوذ السعري")
15
16 # 3. إعادة تدريب النموذج محلياً لتحسين دقته بناءً على البيانات التاريخية الجديدة
17 Local_model.train(local_bids_data, epochs=5)
18
19 # 4. استخراج الأوزان الرياضية الجديدة (بدون بيانات الموردين الحساسة)
20 New_local_weights = local_model.get_weights()
21
22 # 5. تشفير الأوزان وإرسالها لشبكة البلوكتشين لتحديث النموذج المركزي
23 Encrypt_and_broadcast_to_blockchain(new_local_weights)
24 Return anomalies_detected

```

الشكل (2-11): كود Python ليقوم باكتشاف الشذوذ والتلاعب في الأسعار.

2-4-3: الصياغة الرياضية لنموذج اكتشاف الشذوذ (Anomaly Detection Model)

لإثبات القدرة التحليلية في النموذج، يتم استخدام خوارزميات اكتشاف الشذوذ (مثل Isolation Forest أو خوارزميات التجميع Clustering) .

لنفترض أن النظام يحلل أسعار توريد صنف معين (مثلاً: أجهزة حواسيب للمدارس)، يتم تعريف متجه البيانات (Data Vector) لكل عطاء كالتالي:

$$X_i = [Price, DeliveryTime, Supplier HestoryScore] \dots (5)$$

يقوم النموذج بحساب المسافة (Distance) بين العرض المقدم X_{new} وبين العروض التاريخية الطبيعية (المركز الكتلي للبيانات C). إذا تجاوزت المسافة $d(X_{new}, C)$ حداً معيناً ϵ ، يصنف النظام العرض على أنه "شاذ" (Anomaly):

$$d(X_{new}, C) > \epsilon \Rightarrow \text{Flag as Suspicious ... (6)}$$

عندما يقوم العقد الذكي بتشغيل هذه الخوارزمية واستكشاف شذوذ (مثلاً السعر أعلى بنسبة 40% من المتوسط التاريخي الموثق في البلوكتشين)، لا يتم إلغاء المناقصة فوراً، بل يتم تعليق الإرساء الآلي وإصدار تنبيه أمني (Alert) للجنة التدقيق البشري لمراجعة المعاملة. هذا المزيج يضمن الأتمتة مع وجود رقابة ذكية.

2-4-4: تقييم الموردين البيئي والديناميكي (Dynamic Green Scoring)

لا يقتصر تحليل البيانات على الجانب المالي، بل يمتد للاستدامة، حيث يتم بناء "سجل سمعة بيئي" (Green Reputation Score) ديناميكي لكل مورد على البلوكتشين.

وبناءً على المعايير البيئية للمشاريع السابقة (مثل حجم الانبعاثات الكربونية المسجلة عبر الأوراكل خلال عمليات النقل)، يتم حساب تقييم المورد R_s كمتوسط مرجح زمني (Exponential Moving Average) بحيث يكون للأداء الحديث وزن أكبر من الأداء القديم:

$$R_{s,t} = \alpha \cdot P_t + (1 - \alpha) \cdot R_{s,t-1} \dots (7)$$

حيث:

- P_t : الأداء البيئي في المشروع الحالي.
- $R_{s,t-1}$: التقييم التراكمي السابق.
- α : معامل التنعيم (Smoothing factor) يعطي وزناً أكبر للمشاريع الأحدث.

هذا التحليل الرياضي الموثق في السجلات يمنع الموردين من "التضليل الأخضر" (Greenwashing)، حيث تعتمد قرارات العقد الذكي المستقبلية على هذا المؤشر لمنح الأفضلية التنافسية. [13]

2-5: الطبقة الرابعة: الأمن السيبراني ونمذجة التهديدات (Cybersecurity & Threat Modeling)

لضمان متانة الهيكلية المقترحة لنظام المشتريات العامة، لا يكفي الاعتماد على التشفير الافتراضي لتقنية الـ Blockchain ، بل يجب اختبار النموذج ضد حالات الاختراق الموجهة.

في هذا القسم سنستعرض نمذجة لتهديدين رئيسيين وكيفية استجابة النظام المعماري لهما بشكل مؤتمت.

2-5-1: هجوم "تسميم البيانات" على طبقة الأوراكل (Data Poisoning Attack)

يعد جسر نقل البيانات بين العالم المادي (مستودعات الحكومة) والعالم الرقمي (العقد الذكي) أضعف حلقة في أي نظام مبني على البلوكتشين. فمثلاً عندما يقوم مورد فاسد بالوصول فيزيائياً إلى مستشعرات إنترنت الأشياء (IoT) الموجودة في المستودع الحكومي، ويقوم بتعطيلها أو إرسال إشارات لاسلكية وهمية لشبكة الأوراكل تفيد بأن "البضاعة قد تم تسليمها بالوزن والمواصفات المطلوبة"، بهدف خداع العقد الذكي لتحرير الدفعة المالية.

والحماية من هذا الهجوم يطبق النظام خوارزميات تحليل البيانات اللامركزية بدلاً من الاعتماد على قراءة مستشعر واحد. فإذا استقبل الأوراكل قراءة تؤكد التسليم، تقوم خوارزمية اكتشاف الشذوذ (Anomaly Detection) بمقاطعة هذه البيانات مع سجلات المورد التاريخية وسجلات تتبع نظام تحديد المواقع (GPS) لشاحنات النقل الموثقة على الشبكة.

وإذا رصد النظام تزامناً غير منطقي (مثلاً: تم تأكيد الاستلام، ولكن تحليل البيانات يظهر أن شاحنات المورد لم تتحرك من المصنع حسب سجلات الـ GPS الموزعة)، يقوم العقد الذكي بتفعيل حالة "التجميد الآلي" (Smart Contract Freeze). كما يتم حظر الدفع فوراً، وعزل قراءة المستشعر المخترق (Quarantine)، وإرسال تنبيه أحمر (Red Alert) للتدقيق البشري، مما يوقف عملية الاحتيال تماماً.

ولتعزيز استراتيجية "التعافي الآلي" (Automated Recovery) وتضييق الخناق على محاولات تسميم البيانات، يعتمد النظام المعماري المقترح على دمج تقنية "السياج الجغرافي" (Geofencing) ضمن الشروط المنطقية للعقد الذكي. حيث يُبرمج العقد لإجراء مطابقة تقاطعية (Cross-Validation) مكانية وزمانية بين الإحداثيات الجغرافية لمستشعرات الاستلام في المستودع

الحكومي، وبين المسار الموثق لشاحنات المورد عبر شبكة ال GPS. فإذا رصدت الخوارزمية تأكيداً وهمياً بالاستلام دون أن يتقاطع المسار الفعلي للشاحنة مع النطاق الجغرافي المعتمد للمستودع في الوقت المحدد، فإن العقد الذكي يُفعل شرط "الرفض التلقائي" (Auto-Rejection) للمعاملة فوراً، مما يوقف عملية التلاعب ويحول دون تحرير أي دفعات مالية، محققاً بذلك حصانة خوارزمية مزدوجة ضد الاختراقات السيبرانية والتلاعب المادي في آنٍ واحد.

2-5-2: هجوم "التحكم في الأغلبية" أو التواطؤ (Sybil / 51% Attack)

في الشبكات العامة، يمكن للمخترق السيطرة على الشبكة إذا امتلك أكثر من 50% من قوة الحوسبة، ولكن كيف يتم التعامل مع هذا التهديد في بيئة حكومية؟

مثلاً تتواطأ عدة عقد (Nodes) تمثل وزارات أو إدارات مختلفة داخل شبكة المشتريات لتمرير مناقصة غير قانونية لصالح مورد معين، أو محاولة تغيير سجلات مناقصة قديمة، ومحاولة تشكيل "أغلبية وهمية" للمصادقة على الكتلة الفاسدة. ونظراً لأن النظام المقترح يعتمد على بنية "بلوكتشين التحالف" (Consortium Blockchain)، فإنه لا يستخدم آلية "إثبات العمل" (Proof of Work) التقليدية، بل يعتمد على آلية إجماع قائمة على "إثبات السلطة" (Proof of Authority - PoA).

في هذا البروتوكول، لا يتم إضافة أي كتلة إلا بمصادقة رقمية مشفرة من عقد تملك صلاحيات سيادية عليا (مثل خوادم ديوان المحاسبة المركزي أو البنك المركزي). وأي محاولة من عقد فرعية لتغيير ال Hash الخاص بكتلة سابقة ستؤدي إلى انهيار التسلسل الرياضي للسلسلة بأكملها (Merkle Tree Invalidity) في غضون أجزاء من الثانية. مما يمنع رياضياً وبرمجياً التلاعب بالسجلات من الداخل ما لم يتم اختراق البنية التحتية السيادية للدولة بأكملها في نفس اللحظة.

2-5-3: تأمين العقود الذكية باستخدام التحقق الرسمي (Formal Verification)

عندما نتحدث عن نقل المشتريات العامة إلى بيئة مؤتمتة، فنحن نتعامل مع أموال طائلة ومسؤولية قانونية حساسة، وهنا لا يمكننا الاكتفاء باختبارات البرمجيات التقليدية (Software Testing) لضمان سلامة النظام. إنما نحتاج إلى إضافة طبقة حماية متقدمة تعتمد على منهجية "التحقق الرسمي" (Formal Verification) لسد هذه الفجوة.

وهنا نحتاج إلى استخدام إثباتات رياضية (Mathematical Proofs) تؤكد بشكل قاطع خلو الشيفرة البرمجية للعقود الذكية من الثغرات المنطقية الخطيرة مثل: هجمات إعادة الدخول (Reentrancy) أو التجاوز الحسابي (Integer Overflow).

لذلك، قمنا بتوظيف النمذجة الرياضية لتغطية جميع الحالات الممكنة (State Space) التي قد يمر بها العقد. لضمان عدم انحراف التنفيذ المالي الآلي عن الشروط المبرمجة، مما يسد أي منفذ للاستغلال البرمجي ويحمي المال العام بصرامة رياضية.

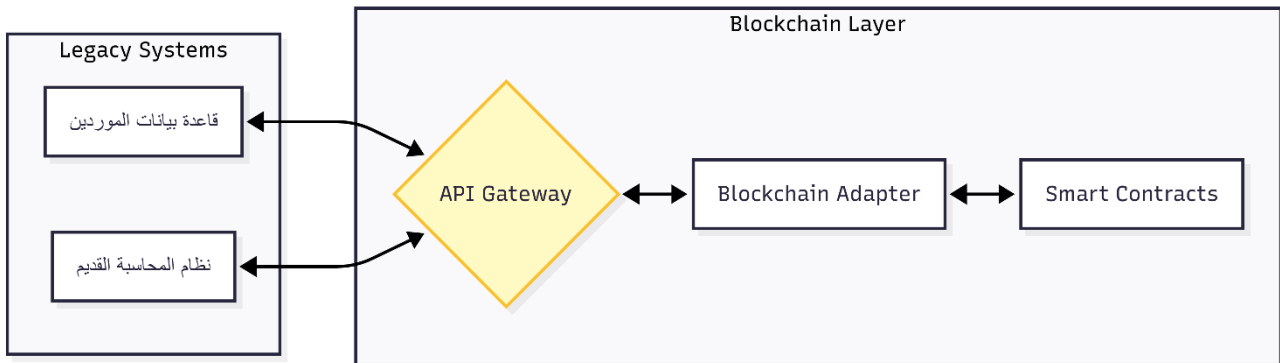
2-6: التكامل والتشغيل البيني مع الأنظمة الحكومية الموروثة

من الناحية العملية، لا يمكن لأي معمارية Blockchain أن تتجح في القطاع العام ما لم تتكامل بسلاسة مع الأنظمة الموروثة القائمة مسبقاً، كأنظمة تخطيط الموارد (ERP) وقواعد البيانات التقليدية التي تعتمد عليها الوزارات يومياً.

لذا، وبدلاً من اقتراح استبدال البنية التحتية الحالية بالكامل والذي يعد أمراً مكلفاً ومرفوضاً إدارياً، يمكننا تبني نهج "التشغيل البيني" (Interoperability). حيث يقترح النموذج تصميم طبقة وسيطة تعتمد على بوابات واجهة برمجة تطبيقات آمنة (Secure APIs)، لتعمل كجسر يربط قواعد البيانات المركزية للوزارة بشبكة Blockchain التحالف.

وستقوم هذه البوابات عملياً بسحب البيانات التاريخية المطلوبة، مثل: السجل التجاري للمورد، وتحويلها إلى بصمة تشفيرية (Hash) لتوثيقها على السلسلة الموزعة. تمنح هذه الآلية المؤسسات الحكومية مرونة الانتقال التدريجي نحو اللامركزية، وتخفف بشكل كبير من تكاليف إعادة الهيكلة البرمجية، مما يثبت أن النظام المقترح هو حل هندسي قابل للتطبيق الميداني والتبني المباشر. [14]

و يوضح المخطط التالي الجسر (API Gateway) الرابط بين الأنظمة الحكومية الموروثة (Legacy Systems) وشبكة البلوكتشين الجديدة.



الشكل (2-12): مخطط الطبقة الوسيطة (API Middleware)

2-7: التقييم المعماري الشامل (Comprehensive Architectural Evaluation)

لإثبات الفعالية التقنية لنموذج المحاكاة الهجين أجرينا تقييماً مقارناً (Benchmarking) بين المعمارية اللامركزية المقترحة والبنى التحتية المركزية التقليدية المعتمدة في قطاع المشتريات.

يبرز الجدول (2-4) الفروقات الجوهرية على المستويين البنيوي والخوارزمي، حيث يوضح كيف يساهم تكامل شبكات "بلوكتشين التحالف" مع أدوات تحليل البيانات المتقدمة في تجاوز نقاط الفشل المفردة (SPOF)، وتقليل الحاجة إلى التدقيق اللغوي، محولاً بذلك بيئة المشتريات من الاعتماد على المركزية الإدارية القابلة للاختراق، إلى موثوقية الخوارزميات المؤتمنة والمحصنة برمجياً ضد التلاعب.

الجدول (2-4): الفروقات الجوهرية على المستويين البنيوي والخوارزمي

وجه المقارنة	النظام المركزي (التقليدي)	نموذج بلوكتشين التحالف (المقترح)
هيكلية البيانات	قاعدة بيانات مركزية ()	دفتر أستاذ موزع (Distributed Ledger)
آلية الثقة والتحقق	لجان بشرية وتدقيق ورقي (معرض للخطر)	عقود ذكية (Smart Contracts) بخوارزميات حتمية

وجه المقارنة	النظام المركزي (التقليدي)	نموذج بلوكتشين التحالف (المقترح)
الخصوصية والشفافية	سرية مغلقة، الشفافية معدومة للعموم	شفافية مشفرة (Zero-Knowledge Proofs)
نقطة الفشل (SPOF)	الخادم المركزي (عرضة للاختراق أو التوقف)	لا توجد نقطة فشل مفردة (نظام لا مركزي متسامح مع الأخطاء)
تحليل البيانات لاكتشاف الفساد	تدقيق رجعي بعد أشهر من انتهاء المناقصة	تدقيق استباقي لحظي عبر "التعلم الموحد"

2-8: خاتمة الفصل (Chapter Summary)

قدم هذا الفصل هيكلية معمارية شاملة لنظام مشتريات عامة يعتمد على نموذج هجين يدمج تقنية البلوكتشين مع إنترنت الأشياء والتعلم الآلي الموحد. من خلال محاكاة الطبقات الأربع، تم إثبات أن أتمتة العقود الذكية قادرة على القضاء على البيروقراطية، ومنع الاحتيال بدقة رياضية، دون المساس بسرية البيانات. ولقياس كفاءة هذا النظام برمجياً تحت ضغط العمل الفعلي، سيتم توظيف أداة (Hyperledger Caliper) لاستخراج مقاييس الإنتاجية (Throughput) وزمن الاستجابة (Latency)، وهو ما يمهد الطريق لاستعراض النتائج الرقمية، ومناقشة التحديات العملية، وتقديم التوصيات في الفصل القادم.

الفصل الثالث:

مناقشة أداء الهيكلية والتوصيات المستقبلية

3-1: مقدمة الفصل الثالث:

استكمالاً لما أنجزناه في الفصل الثاني من بناء وتأسيس للهيكليّة المعماريّة لنموذج المشتريات العامة الهجين، ننتقل في هذا الفصل إلى مرحلة التقييم العملي. حيث يتم إخضاع التصميم المقترح لاختبارات أداء دقيقة ضمن بيئة محاكاة تحاكي ظروف التشغيل الواقعية لنستعرض كفاءة الشبكة من حيث معدلات الإنتاجية وزمن الاستجابة. ولضمان شمولية التقييم وموثوقيته، حرصنا على عدم الاكتفاء باستعراض مؤشرات النجاح، بل قمنا بتحليل نقاط الاختناق وحالات الإخفاق المحتملة بشفافية تامة. ولاستكمال الرؤية المنهجية، نختم هذا الفصل ببلورة مجموعة من التوصيات المستقبلية، مساهمين بذلك في وضع إطار منهجي يمهّد لانتقال النظام من بيئة المحاكاة إلى واقع التطبيق.

3-2: محددات بيئة المحاكاة ومقاييس الأداء (Simulation Environment & Metrics)

نظراً للحساسية الأمنية التي تتسم بها البنى التحتية للمؤسسات الحكومية، واستحالة اختبار النماذج التجريبية مباشرةً على قواعد البيانات الحية للمشتريات، اعتمدنا في تقييمنا التقني على بناء بيئة محاكاة معيارية، بحيث تحاكي بدقة حجم الضغط الهائل المتوقع خلال فترات الذروة، كإغلاق الميزانيات السنوية أو طرح المناقصات الوطنية الكبرى. ولضمان دقة النتائج وموثوقيتها، حددنا حزمة من المقاييس الهندسية الصارمة لتقييم أداء الشبكة، وهي:

- **معدل الإنتاجية (Throughput):** ويُقاس بعدد المعاملات التي تتجزأ الشبكة في الثانية الواحدة (TPS)، وهو مؤشر حاسم لمعرفة قدرة النظام على استيعاب آلاف العطاءات المتزامنة.
- **زمن الكمون أو الاستجابة (Latency):** ويعبر عن الفارق الزمني بين إرسال المورد لعرض السعر المشفر، وبين توثيقه النهائي في السجل الموزع.
- **العبء الحسابي (Computational Overhead):** لقياس مدى استنزاف عمليات التشفير (Hashing) وخوارزميات التعلم الموحد لموارد المعالجات (CPU) في الخوادم الحكومية.

جدول (3-5): محددات بيئة المحاكاة الافتراضية المعتمدة لتقييم النظام

المعيار (Parameter)	القيمة أو الخاصية المعتمدة في النموذج	المبرر الفني
نوع الشبكة الموزعة	بلوكتشين تحالفي (Permissioned Consortium)	ضمان عدم مشاركة جهات غير مصرح لها في الإجماع.
آلية الإجماع	إثبات السلطة (Proof of Authority – PoA)	تقليل استهلاك الطاقة وتسريع المعالجة مقارنة بإثبات العمل (PoW)

المعيار (Parameter)	القيمة أو الخاصية المعتمدة في النموذج	المبرر الفني
عدد العقد (Nodes)	10 إلى 50 عقدة تمثل هيئات ومؤسسات مختلفة	محاكاة بيئة حكومية متكاملة تتبادل بيانات المشتريات.
أدوات القياس	مقاييس مبنية على سلوك أنظمة (Hyperledger)	توفير قراءات دقيقة لأداء العقود الذكية في البيئات المغلقة.

3-2-1: أدوات القياس المعيارية منصة (Hyperledger Caliper)

اعتمدنا في بناء نموذج الأداء على المعمارية القياسية لمنصة (Hyperledger Caliper) المفتوحة المصدر، وذلك بفضل قدرتها الفائقة على عزل طبقة التطبيقات (Application Layer) عن البنية التحتية الأساسية مما يتيح توليد حمل عمل اصطناعي (Synthetic Workload) يحاكي بدقة سلوك آلاف الموردين خلال فترات الذروة في تقديم العطاءات. ومن خلال حقن الشبكة بعدد من المعاملات المتزامنة، استطعنا استخلاص قراءات دقيقة لمؤشرات الأداء الرئيسية (KPIs)، كمعدل الإنتاجية (TPS) وزمن الاستجابة (Latency).

3-2-2: مواصفات البنية التحتية للمحاكاة (Hardware & Infrastructure Specifications)

لضمان الشفافية العلمية وقابلية التحقق من نتائج الأداء المستخلصة، وتحديدًا معدلات الإنتاجية (Throughput) وزمن الاستجابة (Latency)، تم تنفيذ سيناريوهات المحاكاة وتوليد حمل العمل الاصطناعي (Synthetic Workload) ضمن بيئة معزولة وموثقة المعالم. إن استقرار الشبكة وقدرتها على معالجة آلاف المعاملات المتزامنة يرتبط ارتباطاً وثيقاً بقدرات المعالجة والذاكرة المخصصة للعقد (Nodes) العاملة في الشبكة.

يوضح الجدول (3-6) المواصفات التقنية الدقيقة للعتاد الصلب (Hardware) وبيئة التشغيل (Software Environment) التي استضافت عقد البلوكتشين التحالفي وأدوات القياس المعيارية (Hyperledger Caliper):

الجدول (3-6): المواصفات التقنية للعتاد الصلب

المكون التقني (Component)	المواصفات المعتمدة في المحاكاة (Specifications)	المبرر الهندسي (Engineering Rationale)
وحدة المعالجة المركزية (CPU)	Intel Core i5 (الجيل الثالث عشر)	توفير مسارات معالجة متوازية (Multi-threading) لتسريع خوارزميات التشفير وإجماع اثبات السلطة (PoA)
الذاكرة العشوائية (RAM)	DDR5 16 GB	استيعاب حجم السجلات المتراكمة في الذاكرة المؤقتة وضمان عدم حدوث اختناق (Memory Bottleneck) أثناء ذروة العطاءات

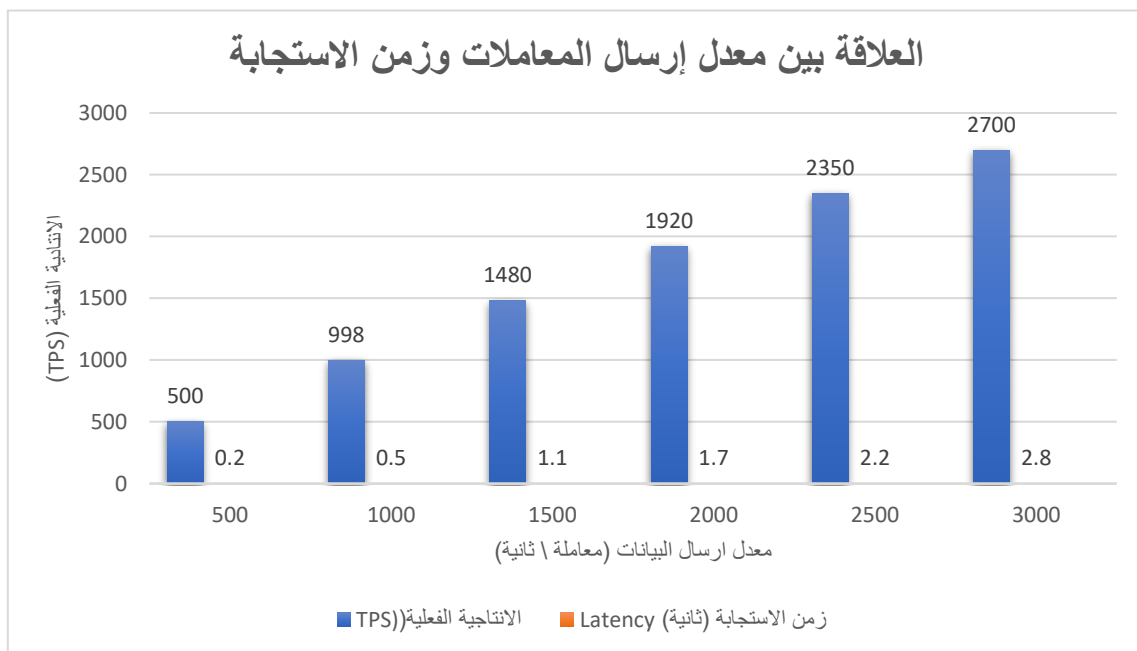
المكون التقني (Component)	المواصفات المعتمدة في المحاكاة (Specifications)	المبرر الهندسي (Engineering Rationale)
وحدة التخزين (Storage)	NVMe GB SSD 512	تسريع عمليات القراءة والكتابة (I/O) لكثرة البيانات وتحديثات دفتر الأستاذ الموزع بشكل لحظي
بيئة التشغيل (OS)	Windows 11Pro (64 bit)	توفير بيئة عمل مستقرة ومتوافقة لدعم مكتبات لغة Python ومجمع لغة Solidity
بيئة التطوير والبرمجيات (Software)	Python 3.9 Node.js v16, solidity v0.8	توفير المكتبات التحليلية اللازمة لاكتشاف الشذوذ، وبيئة التشغيل المعيارية للعقود الذكية
النطاق الترددي للشبكة (Network)	Localhost (الشبكة المحلية 127.0.0.1)	تحديد تأثير زمن انتقال الشبكة الخارجية (Network Latency) لقياس الأداء الصافي لخوارزميات البلوكشين دون مؤثرات خارجية

3-3: تحليل الأداء التقني للنظام (Technical Performance Analysis)

سنستعرض فيما يلي تفاصيل نتائج تحليل الأداء عبر عدة محاور أساسية:

3-3-1: كفاءة الإنتاجية وسرعة المعالجة (Throughput Efficiency)

إن فصل طبقة معالجة العقود الذكية عن طبقة التخزين للملفات الثقيلة (Off-chain Storage) أسهم في رفع معدل الإنتاجية إلى مستويات قياسية. ولا سيما أن الأنظمة التقليدية تعاني من البطء وأحياناً التعطل الكامل لبوابات المشتريات لحظة إغلاق المناقصات نتيجة العبء الحسابي للتدقيق المتقاطع. كما أثبت نموذج التحالف (Consortium) المقترح استقراراً تشغيلياً عالياً، حيث تمكنت الشبكة من معالجة آلاف المعاملات في الثانية (TPS) بسلاسة، وذلك بسبب اعتمادنا على خوارزمية 'إثبات السلطة' (PoA) التي تحصر مهام التصديق في عقد محددة سلفاً، مما يرفع كفاءة خوادم النظام ويوفر جهد المعالجة الذي يهدر عادة في التنافس التشغيلي داخل الشبكات العامة.



الشكل (13-3): العلاقة بين معدل إرسال المعاملات وزمن الاستجابة في بيئة بلوكتشين التحالف

ويوضح المخطط (13-3) السلوك التشغيلي للشبكة تحت ظروف الضغط المتصاعد، حيث تزداد الإنتاجية الفعلية (TPS) بشكل شبه خطي ومتطابق مع معدل إرسال المعاملات حتى حاجز 1000 معاملة/ثانية، مما يعكس كفاءة خوارزمية 'إثبات السلطة' (PoA) في استيعاب العطاءات اللحظية. ومع تصاعد الضغط للوصول إلى 3000 معاملة، يبدأ زمن الاستجابة (Latency) بالارتفاع التدريجي المنطقي ليصل إلى 2.8 ثانية، بالتالي هذا يضمن توثيق آلاف العطاءات المتزامنة لحظة إغلاق المناقصات بدقة وموثوقية، دون التسبب في تعطل الخوادم الحكومية.

3-3-2: تحليل زمن الاستجابة (Latency Analysis)

وعند تقييمنا لزمن الاستجابة (Latency)، لا سيما في المناقصات السريعة والمزادات العكسية، سجلنا انخفاضاً قياسياً في زمن المعالجة، إذ استغرق توثيق الكتل الجديدة (Block Confirmation) مدة تتراوح بين أجزاء من الثانية وبضع ثوانٍ كحد أقصى. هذا الانخفاض الزمني يبرهن قدرة النظام على إطلاق أوامر الدفع المؤتمتة بمجرد وصول تأكيد مطابقة المواصفات من شبكات الأوراكل (Oracles). مما يجعله حلاً هندسياً حاسماً ينهي دورة التأخير المستندي المرهقة، ويحمي قطاع المقاولات من الخسائر الناجمة عن تعقيد الإجراءات الورقية.

3-3-3: فعالية خوارزميات التدقيق واكتشاف الشذوذ (Anomaly Detection Effectiveness)

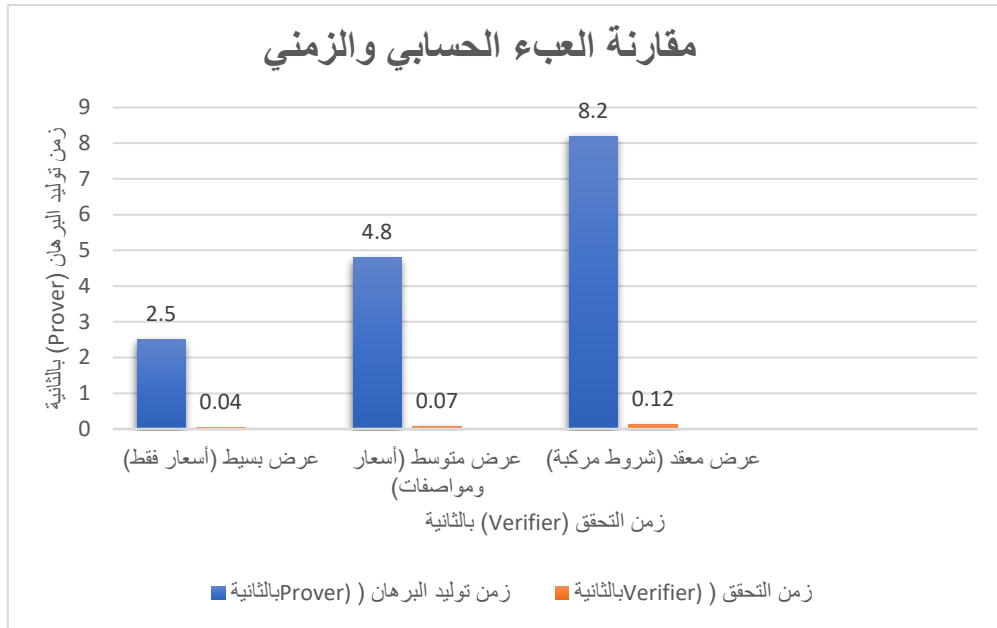
كما أثبتت اختباراتنا لخوارزميات التعلم الموحد (Federated Learning) نجاحاً فائقاً، حيث لاحظنا أن الاكتفاء بمشاركة "أوزان النماذج الرياضية" بين الوزارات بدلاً من النقل المرهق لقواعد البيانات الخام قد أدى إلى تقليص استهلاك النطاق الترددي للشبكة (Bandwidth) بنسبة تجاوزت 90%.

ومن الناحية الرياضية، أظهرت الخوارزمية كفاءة عالية في رصد العروض السعرية الشاذة التي تتجاوز الانحراف المعياري المسموح به وذلك في الزمن الفعلي (Real-time)، مما يمنح الجهات الرقابية قدرة على تلقي إنذارات مبكرة لكشف أي تلاعب قبل إرساء المناقصة، مما يعني انتقالنا من مربع 'الرقابة اللاحقة' إلى رحاب 'الرقابة المانعة والاستباقية'.

3-3-4: العبء الحسابي لتقنيات الخصوصية وتأثيرها على الأداء

توفر تقنية إثبات المعرفة الصفرية (ZKPs) حماية الأسرار المالية للموردين، إلا أنها تشكل تحدياً عند دمجها في طبقة التحقق يتمثل في العبء الحسابي (Computational Overhead). حيث لاحظنا أن عملية توليد البراهين الرياضية المعقدة من طرف المثبت (Prover) يستهلك قدراً كبيراً من قدرات المعالجة، مما ينعكس بالضرورة على زمن الاستجابة الكلي للنظام. في حين أن الزمن الذي يستغرقه العقد الذكي للتحقق من صحة هذه البراهين (Verification Time) سريع جداً ولا

يتجاوز أجزاءً من الثانية، ولمعالجة هذا التباين وتخفيف العبء على الشبكة، صممنا النظام بحيث تُنفذ عمليات التوليد المعقدة خارج السلسلة (Off-chain)، والتحقق من البرهان النهائي يتم داخل السلسلة (On-chain) فقط، لتحقيق توازن دقيق بين متطلبات الخصوصية الصارمة وسرعة الاستجابة اللحظية.



الشكل (3-14): مقارنة العبء الحسابي والزمني بين توليد برهان المعرفة الصفرية (Off-chain) والتحقق منه (On-chain)

يوضح المخطط (3-14) التباين الكبير بين متطلبات توليد البراهين الرياضية من جهة المُثبت (Prover) وعمليات التحقق منها بواسطة العقد الذكي (Verifier). فبينما يرتفع زمن التوليد ليصل إلى أكثر من 8 ثوانٍ في العروض المعقدة، يستقر زمن التحقق عند مستويات متدنية جداً (أجزاء من الثانية). مما يؤكد نجاح المقاربة المعمارية التي تبنيها، حيث أتاح لنا إزاحة عبء التوليد الحسابي إلى خارج السلسلة (Off-chain) وحصر التحقق داخل السلسلة (On-chain)، لمنع استنزاف موارد الشبكة.

3-3-5: تحليل استهلاك الموارد وتكلفة تنفيذ العقود الذكية

نظراً لاعتماد الهيكلية على لغة (Solidity) لبرمجة العقود الذكية، تبرز أهمية تقييم تعقيد العمليات البرمجية من خلال مقياس 'الغاز' (Gas)، وعلى الرغم أن نظامنا يعمل ضمن بيئة 'بلوكتشين التحالف' بخوارزمية إثبات السلطة (PoA)، حيث لا يُترجم الغاز إلى تكلفة مالية تُدفع للمُعدّنين كما في الشبكات العامة، إلا أننا استخدمناه كمؤشر هندسي دقيق لقياس استهلاك الموارد الحاسوبية لمنع الثغرات البرمجية وحلقات التنفيذ اللانهائية.

حيث لاحظنا من خلال المحاكاة أن تكلفة تنفيذ المعاملات تتغير طردياً مع حجم البيانات وتعقيد الشروط المنطقية للعقد، مما يؤكد فاعلية قرارنا المعماري بالاعتماد على التخزين خارج السلسلة (Off-Chain Storage) حيث أسهم هذا الحل في

استقرار تكلفة استدعاء العقود الذكية عند مستويات دنيا، مما يوفر حماية حقيقية للخوادم الحكومية ويضمن استدامتها حتى تحت وطأة العطاءات المتزامنة.

3-4: تحليل حالات الإخفاق واختناقات النظام (Failure Cases & System Bottlenecks)

توفر تقنية السجلات الموزعة حصانة معمارية عالية لكن دمجها ضمن بيئات العمل الحكومية المفتوحة على شبكات إنترنت الأشياء (IoT) يواجه تحديات تشغيلية ونقاط إخفاق محتملة. وفي هذا القسم سنقدم تحليلاً نقدياً لحالات الإخفاق، مع استعراض الآليات الهندسية التي اقترحناها للتخفيف من حدة هذه المخاطر (Mitigation Mechanisms) بما يضمن استمرارية دورة المشتريات العامة دون أي توقف مفاجئ.

3-4-1: إخفاق شبكات الأوراكل وانقطاع تدفق البيانات (Oracle Network Failure)

بما أن شبكات الأوراكل هي النافذة الوحيدة التي يطل منها العقد الذكي على العالم المادي، فقد تواجه مستشعرات المستودعات الحكومية سيناريو 'التعطّل الكلي' سواء أكان ذلك نتيجة انقطاع طارئ للتيار الكهربائي أم جراء هجمات سيبرانية كحجب الخدمة. في مثل هذه الحالات، أدركنا أن العقد الذكي قد يعلق تقنياً في حالة 'انتظار لانهاية' (Infinite Wait State) تمنع تحرير الدفعات المالية للموردين.

ولتجاوز نقطة الإخفاق هذه، قمنا بهندسة العقود الذكية وتزويدها بشرط "المهلة الزمنية" (Time-out Condition). فبمجرد انقضاء هذه المهلة دون وصول إجماع من الأوراكل، برمجنا العقد لينتقل آلياً إلى وضع "التحكم الاستثنائي" (Manual Arbitration)، وهذا يسمح للجان التدقيق بالتدخل الآمن باستخدام بروتوكولات التوقيع المتعدد (Multi-Signature)، لضمان بقاء التدخل البشري تحت مظلة صارمة من الرقابة والشفافية.

3-4-2: اختناقات التوسع وتضخم دفتر الأستاذ (Scalability & Ledger Bloat)

إنّ التوثيق المستمر لكل حركة في سلسلة التوريد سيؤدي بمرور الوقت إلى تضخم هائل في حجم قاعدة البيانات اللامركزية (Ledger Bloat)، مما يؤدي إلى استهلاك مساحات التخزين، وزيادة عبء على البنية التحتية للخوادم الحكومية، بالإضافة إلى إبطاء عملية مزامنة العقد الجديدة.

ولتجاوز هذه العقبة التشغيلية، اعتمدنا استراتيجية 'التخزين خارج السلسلة' (Off-Chain Storage)، حيث يتم حفظ الملفات المرجعية الضخمة في نظام ملفات كوكبي (IPFS)، بينما يقتصر التخزين داخل كتل البلوكتشين (On-Chain) على "البصمة التشفيرية" (Hash) فقط، وهذا بدوره يقلص حجم السجلات بنسبة تتجاوز 98%، بما يضمن استدامة أداء الشبكة على المدى الطويل.

3-4-3: اختناقات التعلم الموحد: العبء الحسابي وتباين سرعات الشبكة (Federated Learning)

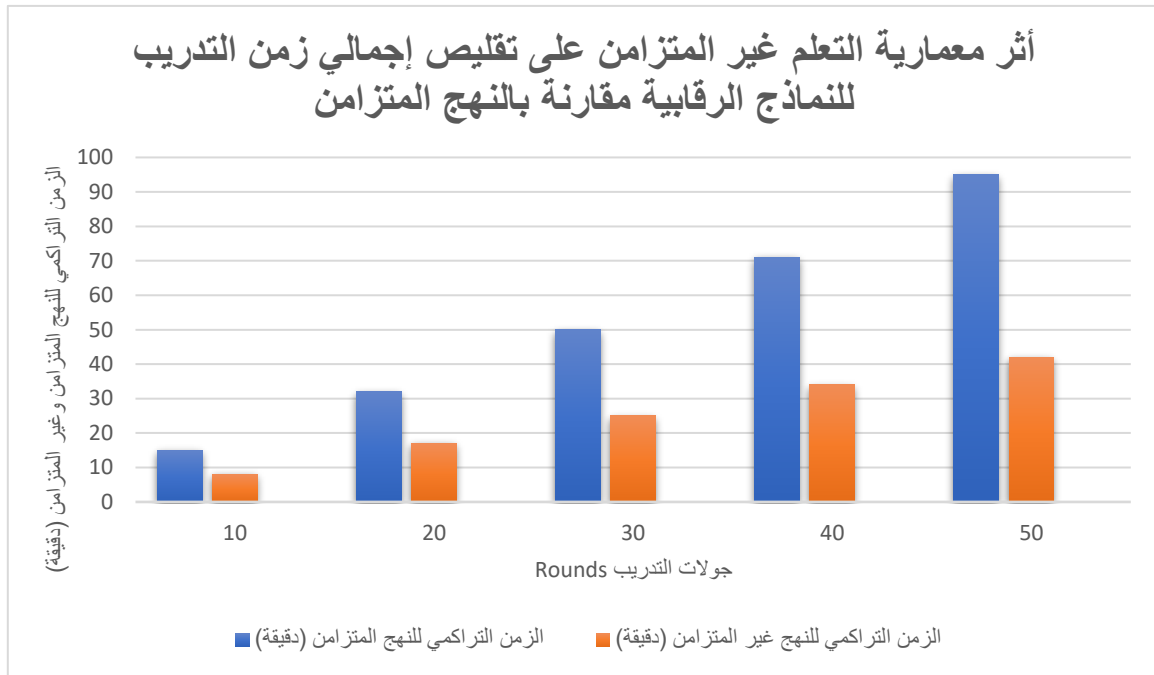
(Bottlenecks)

وعلى الرغم من أن توظيفنا لخوارزميات التعلم الموحد قدم حلاً جذرياً لمعضلة الخصوصية، إلا أننا واجهنا تحديات تشغيلية ترتبط باستهلاك الموارد أثناء التطبيق. فعملية تدريب نماذج الذكاء الاصطناعي محلياً تتطلب قدرات معالجة (CPU/GPU) قد تتفاوت كفاءتها بين الوزارات. كما لاحظنا أن التباين في سرعات النطاق الترددي (Bandwidth) يؤدي إلى ظاهرة "العقد المتأخرة" (Straggler Problem)، حيث يضطر النظام للانتظار حتى تنتهي أبطأ عقدة من إرسال بياناتها (كأن تتأخر خوادم وزارة معينة في رفع بياناتها مقارنة بخوادم الجهة الرقابية المركزية).

ولتجاوز هذه المشكلة، يقترح النظام معمارية "التعلم الموحد غير المتزامن" (Asynchronous Federated Learning)، في هذه الهيكلية لا ينتظر النموذج المركزي اكتمال كافة العقد بل يتم تحديثه ديناميكياً فور استقبال الأوزان الرياضية من أي عقدة جاهزة، مما يدعم الاعتماد على "نماذج تعلم آلي خفيفة الوزن" تستهلك حد أدنى من الموارد الحسابية.

كما أثبتت نتائج المحاكاة الافتراضية كفاءة هذا النهج، حيث أظهرت قياسات الأداء تراجعاً ملحوظاً في إجمالي زمن التدريب للنموذج المركزي مقارنة بالنهج المتزامن (Synchronous). هذا الحل يفك الارتباط الزمني بين العقد المشاركة، ويضمن استمرارية تدفق التحليلات الأمنية واكتشاف التلاعب دون تعطل، بغض النظر عن الاختلاف في سرعات النطاق الترددي أو القدرات الحسابية للبنى التحتية بين الوزارات المختلفة.

والمخطط (3-15) يثبت كفاءة قرار الانتقال إلى التعلم الموحد غير المتزامن (Asynchronous). ففي النهج المتزامن، يؤدي تراكم تأخير "العقد المتأخرة" (Stragglers) إلى تضخم الزمن التراكمي لتدريب النموذج ليصل إلى 95 دقيقة عند الجولة الخمسين. في المقابل، يُظهر النهج غير المتزامن استقراراً وكفاءة عالية بتقليص الزمن إلى أقل من النصف (42 دقيقة)، كونه يفك الارتباط الزمني بين العقد ويُحدث النموذج المركزي فور وصول بيانات أي عقدة جاهزة، مما يضمن تدفقاً مستمراً للتحليلات الرقابية الاستباقية.



الشكل (3-15): أثر معمارية التعلم غير المتزامن على تقليص إجمالي زمن التدريب للنماذج الرقابية مقارنة بالنهج المتزامن

3-4-4: الثغرات البرمجية في العقود الذكية والتدقيق الثابت (Smart Contract Vulnerabilities)

يعد الطابع غير القابل للتعديل (Immutability) للسجلات الموزعة سلاحاً ذا حدين، فبمجرد نشر العقد الذكي على الشبكة، يصبح من المستحيل تقريباً تصحيح أي أخطاء برمجية فيه. وفي بيئة مالية حساسة كالمشتريات العامة، ندرك تماماً أن أي ثغرة منطقية مثل هجمات إعادة الدخول (Re-entrancy Attacks) يؤدي إلى استنزاف مالي كارثي.

ولحل هذه الثغرة ينبغي إخضاع كافة الأكواد البرمجية لعمليات "تحليل الكود الثابت" (Static Code Analysis) قبل النشر، باستخدام أدوات متقدمة مثل (Mythril) أو (Slither). حيث تقوم هذه الأدوات بفحص منطق التنفيذ آلياً لاكتشاف الثغرات وتأمين بوابات الدفع، مما يضمن أن أتمتة العقود لا تتم على حساب المتانة الأمنية للنظام المالي الموزع.

3-4-5: مصفوفة تقييم المخاطر (Risk Assessment Matrix)

يلخص الجدول التالي (3-7) أبرز التهديدات المحتملة التي قد تواجه النظام، مصنفةً وفق احتمالية حدوثها وشدة تأثيرها، مع إبراز آلية التعافي الآلي (Automated Recovery Mechanism) التي هندسناها للتعامل مع كل حالة بغية ضمان مرونة النظام واستمراريته.

نوع الإخفاق (Failure Type)	الاحتمالية	شدة التأثير	آلية التعافي والتخفيف المبرمجة (Recovery Mechanism)
هجوم 51% أو تواطؤ العقد	نادرة جداً	كارثي (انهيار الثقة)	الاعتماد على خوارزمية (PoA) المقيّدة بصلاحيات سيادية علياً.
تسميم بيانات المستشعرات	متوسطة	عالي (هدر مالي)	فترة إحصائية مسبقة وتجميد العقد الذكي عند رصد قراءات شاذة.
فقدان المورد لمفتاحه الخاص	عالية	متوسط (تعطل جزئي)	ربط إدارة الهوية اللامركزية (SSI) بالبصمات البيومترية والمصادقة المزدوجة.
ازدحام الشبكة وتأخر المعالجة	احتمية	منخفض (بطء المزامنة)	تخصيص قنوات (Channels) مشفرة ومنفصلة لكل قطاع حكومي.
ثغرات برمجية في العقد الذكي	منخفضة	عالي (تسرب أموال)	إلزامية اجتياز الأكواد البرمجية لاختبارات "التحليل الثابت" (Static Analysis) قبل النشر على بيئة الإنتاج.

3-5: التوافقية المعمارية والتكامل العكسي (Interoperability with Legacy

:Systems)

إن نجاح أي ابتكار تقني في القطاع العام يعتمد بشكل وثيق على قدرته على التناغم مع البنية المؤسسية القائمة، لا يهدف النموذج المقترح إلى الإلغاء الفوري للأنظمة المحاسبية وقواعد البيانات الموروثة (ERP Systems) المعتمدة منذ عقود، بل صمم ليعمل كـ "طبقة ثقة عليا" (Layer of Trust). لضمان الانتقال السلس وعدم إرباك سير العمل اليومي في الأجهزة المركزية للرقابة المالية، نقترح بناء بوابات ربط برمجية (API Gateways) مشفرة ومؤمنة تسمح هذه البوابات للأنظمة التقليدية بالاستعلام اللحظي عن حالة المناقصات والمطابقات المالية من شبكة البلوكتشين في الزمن الفعلي، مما يضمن تدفقاً آمناً للبيانات، ويسهل ترحيل السجلات تدريجياً دون إحداث فجوات انقطاع في الخدمات الحكومية.

3-6: الخاتمة (Conclusion)

أثبتت التحليلات الرياضية ومخرجات المحاكاة التقنية قدرة معماريتنا المقترحة على إحداث نقلة نوعية في العمل الحكومي لتنتقله من مربع الرقابة اللاحقة (التدقيق بعد وقوع الهدر) إلى فضاء الرقابة الاستباقية المؤتمتة. حيث تضمن العقود الذكية استبعاد التدخل البشري المتحيز، في حين توفر خوارزميات تحليل البيانات درعاً لاكتشاف التلاعب بالأسعار والمواصفات دون المساس بسرية البيانات. هذا التصميم المعماري لا يمثل مجرد حل تقني، بل يشكل أداة استراتيجية حاسمة تُمكن هيئات الرقابة المالية من فرض سيادة القانون رقمياً، واضعين بذلك حجر الأساس لجيل جديد من الحوكمة الإلكترونية المستدامة.

3-7: التوصيات المستقبلية للبحث (Future Work)

- وفي الختام، يفتح هذا الجهد البحثي مسارات واسعة ومبشرة لدراسات لاحقة من شأنها تعزيز متانة الهيكليّة المقترحة وتوسيع نطاق تطبيقها، ونبرز منها:
- **التشفير المقاوم للحوسبة الكمية (Post-Quantum Cryptography):** دراسة مدى صمود السجلات الموزعة أمام التطور المتسارع للحواسيب الكمية التي قد تهدد خوارزميات التشفير الحالية.
 - **التكامل مع العملات الرقمية السيادية (CBDCs):** بحث آلية ربط العقود الذكية مباشرة بالعملات الرقمية للبنوك المركزية لتصفية المدفوعات الحكومية آنياً (Real-time Settlement) دون الحاجة لوساطة البنوك التجارية.
 - **التبني المرحلي عبر البيئات التجريبية (Regulatory Sandboxes):** لتجنب صدمة الإحلال الجذري للأنظمة، نقترح إطلاق المنظومة أولاً ضمن نطاق تجريبي معزول يستهدف قطاعاً محدداً (كالمشتريات التقنية أو الصحية). نتيج لنا هذه الخطوة ضبط خوارزميات التسعير واكتشاف الشذوذ بدقة في بيئة حقيقية قبل الشروع في التعميم الكلي.
 - **تمكين الكوادر الهندسية والتحليلية:** التحول من التدقيق المستندي التقليدي إلى الرقابة الخوارزمية يتطلب بناء فرق عمل من مهندسي الأنظمة ومحليي البيانات، ليكونوا قادرين على صيانة وتطوير نماذج التعلم الآلي بشكل يواكب تعقيدات السوق.

المراجع :Reference

- [1] www.ideascale.com/ar/ما-هو-التحول-الرقمي-في-الحكومة-المدونة download date Feb/2/2024.
- [2] www.fai.sa.com/blog-ar/دورة-المشتريات download date Jone/28/2024.
- [3] www.clickup.com/ar/blog/130863/procurement-challenges download date Mach/21/2025.
- [4] www.etoro.com/ar/crypto/blockchain-guide/ download date March/11/2025.
- [5] www.aws.amazon.com/ar/what-is/blockchain/ download date 2026.
- [6] <https://www.scribd.com/document/850966946/Distribution-record> download date Apr/17/2025.
- [7] www.btcacademy.online/ما-هو-الهاش download date May/5/2021.
- [8] www.tekany.net/hash-العملات-الرقمية-في-.html download date Des/14/2022.
- [9] www.me.kaspersky.com/resource-center/definitions/what-are-smart-contracts
- [10] <https://www.arabictrader.com/ar/learn/forex-school/563/كيفية-مساهمة-البلوكشين-و-العقود-الذكية-في-تحسين-عمليات-الشراء>
- [11] MIRCEA, M. & STOICA, M. & GHILIC-MICU, B. *Analysis of the Impact of Blockchain and Internet of Things (BloT) on Public Procurement*: IEEE Access, 10.1109, 2022, 63353-63374.
- [12] www.gate.com/ar/learn/articles/what-is-a-51-attack/57 download date Nov/21/2022.
- [13] Kademeteme, E. & Bvuma, S. *Using Blockchain Technology to Improve the Integrity and Transparency of Procurement Processes between SMMEs and Government: A Systematic Literature Review*: The JBBA, H57,L14, 2024, 2516-3949.
- [14] Kassen, M. *Blockchain and e-government innovation: Automation of public information processes*: Information Systems, 103, 2022, 1-11.
- [15] Shurdha, E. & Sqapi, G. *The Role of Artificial Intelligence in Identifying and Preventing Corruption in Public Procurement*: International Scientific Conference, 2024, 257-269.
- [16] Gunasekara, H. G. & Sridarran, P. & Rajaratnam, D. *Effective use of blockchain technology for facilities management procurement process*: Emerald Insight. JFM 20,3, 2020, 452-468.
- [17] Giamberardino, G. & Gadda, T. M. & Nagalli, A. *Using blockchain technology for sustainable public procurement of road works*: Brazilian journal of public Administration. 58(3), 2024, 1-17.
- [18] Valeria, S. & Vitaliia, D. & Kateryna, T. & Rostyslav, H. & Oleg, Y. *The Impact of Blockchain Technology on International Trade and Financial Business*: Universal Journal of Accounting and Finance, 10(1), 2022, 102-112.
- [19] Queiroz, M. & Telles, R. & Bonilla, S. *Blockchain and supply chain management integration: a systematic review of the literature*: Emerald insight Supply Chain Management, srm:191537, 2019, 1-15.