هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

دليل تبني تقنية سلسلة الكتل

Blockchain

الإصدار الأول

اكتوبر 2022م

CST.GOV.SA

جدول المحتويات

1 المصطلحات

اتفاق **Consensus**	مجموعة من القواعد التي يجب أن تتبعها الأجهزة داخل شبكة السجل الموزع للتحقق من صحة العمليات، وضمان اتّساقها بين مختلف الأجهزة.
اختزال **Hash**	تطبيق خوارزمية حسابية على بيانات للحصول على قيمة عددية تعبر عن تلك البيانات.[1]
أصل **Asset**	أي شيء له قيمة يمكن تملُّكه أو التحكم به.
تقنية السجل الموزّع **Distributed Ledger Technology**	تقنية تعنى بتسجيل العمليات في الأجهزة الموزعة في الشبكة، واتفاق هذه الأجهزة على العمليات، واتساق السجل بين الأجهزة.
جهاز / مشارك **Node / Participant**	جهاز / مستخدم جهاز موجود في شبكة السجل المُوزّع من خلال تخزين نسخة من السجل. قد يكون الجهاز تابعًا لفرد أو جهة.
رمز **Token**	مجموعة من المعلومات الرقمية المُسجّلة في سلسلة الكتل والتي تمنح حق امتلاك أصل ما صاحب مصلحة معيّن. يمكن أن يُعبر الرمز عن امتلاك أصل قابل أو غير قابل للاستبدال.
سجل **Ledger**	سجل يحتوي على تسجيل العمليات.
سلسلة الكتل **Blockchain**	إحدى تقنيات السجل المُوزّع التي يتم فيها تسجيل العمليات بهيكل بيانات يسمى "الكتلة"، وتتصل كل كتلة بالكتلة السابقة وصولاً إلى الكتلة الأولى - مكونة سلسلة من الكتل.
شبكة السجل الموزع **Distributed Ledger Network**	شبكة من أجهزة متصلة تحتوي كل منها على نسخة من السجل والعقود الذكية.
عقد ذكي **Smart Contract**	برنامج مُخزّن في شبكة سلسلة الكتل، ويقوم تلقائيًا بتنفيذ عمليات مُعيّنة عند استيفاء شروط عقد محدد.
عملية **Transaction**	تسجيل حدث، مثل: إنشاء أصول جديدة، أو نقل أصول بين الأجهزة.[2]
كتلة **Block**	بيانات تحتوي على اختزال (hash) الكتلة السابقة وعدد من العمليات، باستثناء الكتلة الأولى.

1 القاموس، مركز التميز لأمن المعلومات.
https://coeia.ksu.edu.sa/ar/dictionary

2 NISTIR 8202
https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

2 المقدّمة

وفقًا لنظام الاتصالات وتقنية المعلومات، ولائحته التنفيذية، وتنظيم هيئة الاتصالات والفضاء والتقنية، وما نص عليه البند (سابعًا) في قرار مجلس الوزراء ذي الرقم (292) والتاريخ ١٤٤١/٤/٢٧هـ، فإن هيئة الاتصالات والفضاء والتقنية (الهيئة) هي الجهة المسؤولة عن تنظيم قطاع الاتصالات وتقنية المعلومات في المملكة العربية السعودية (المملكة).

وبناءً على ذلك، وانطلاقًا من استراتيجية الهيئة، وحرصًا منها على تمكين سوق سلسلة الكتل في المملكة؛ فقد أصدرت الهيئة هذا الدليل بهدف تبني أفضل الممارسات والتوصيات الإدارية والتقنية المتعلقة بتقنية سلسلة الكتل.

1.2 نطاق تطبيق الوثيقة

هذه الوثيقة هي إرشادات غير ملزمة، وتهدف إلى تيسير ودعم تبني تقنية سلسلة الكتل للمعنيين بها، ومنهم:

- **المسؤولون التنفيذيون**

صانعو القرارات الرئيسيون (مثل: الرؤساء التنفيذيين، ومدراء تقنية المعلومات) بشأن توجهات تبنّي تقنية سلسلة الكتل،

- **مهندسو الحلول والبرمجيات**

المسؤولون عن اتخاذ القرارات الفنية المتعلقة بتصميم وتطوير الحلول المبنية على تقنية سلسلة الكتل.

كما تركز الوثيقة على المجالات التالية:

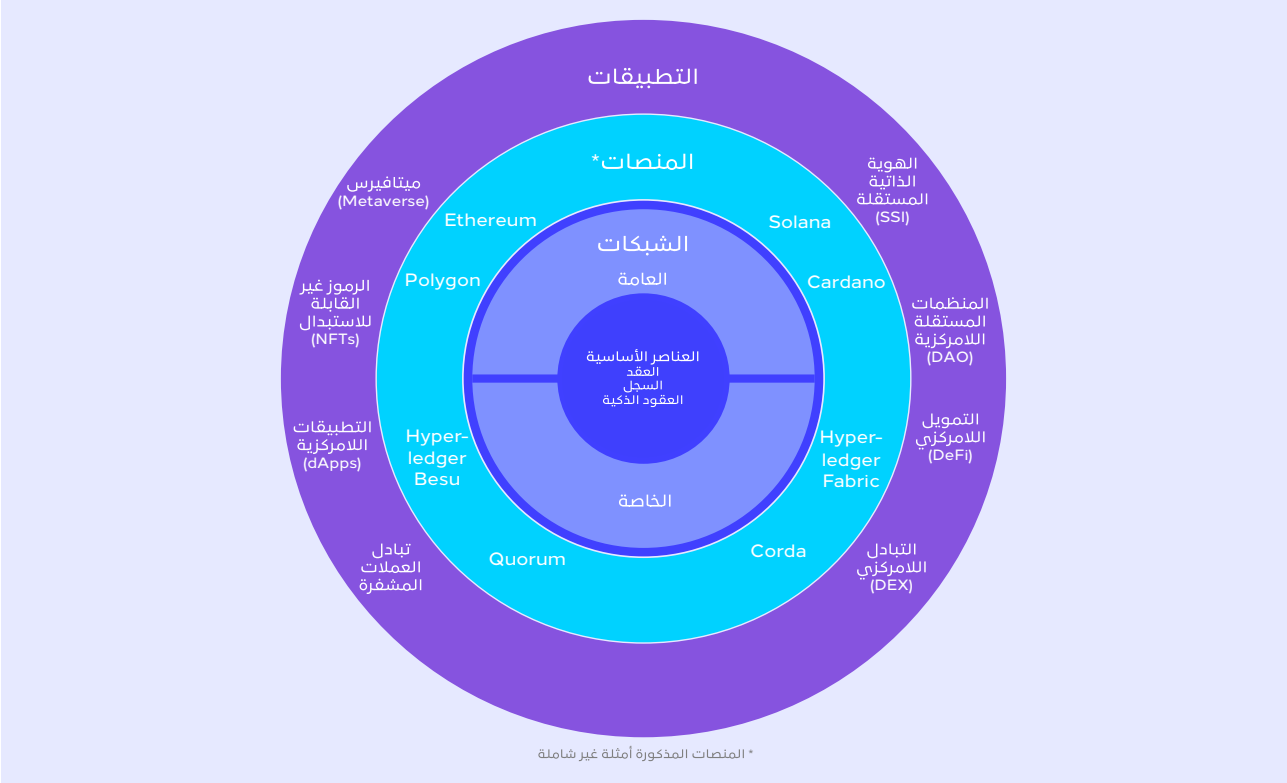
- توفير إرشادات عامة حول تقنية سلسلة الكتل بهدف تعزيز تبنّيها.
- المساعدة على اتخاذ القرارات الفنية المناسبة بناءً على أفضل الممارسات المتبعة.
- التوعية بمبادئ قابلية التشغيل البيني (interoperability) داخل شبكة سلسلة الكتل الواحدة أو بين عدة شبكات.
- تقديم إرشادات حول خصوصية البيانات وأمنها على شبكة سلسلة الكتل.
- توفير إرشادات حول حوكمة شبكة سلسلة الكتل.

2.2 نبذة عن سلسلة الكتل

سلسلة الكتل هي إحدى تقنيات السجل المُوزّع التي يتم فيها تسجيل العمليات بآليةٍ تجعلها

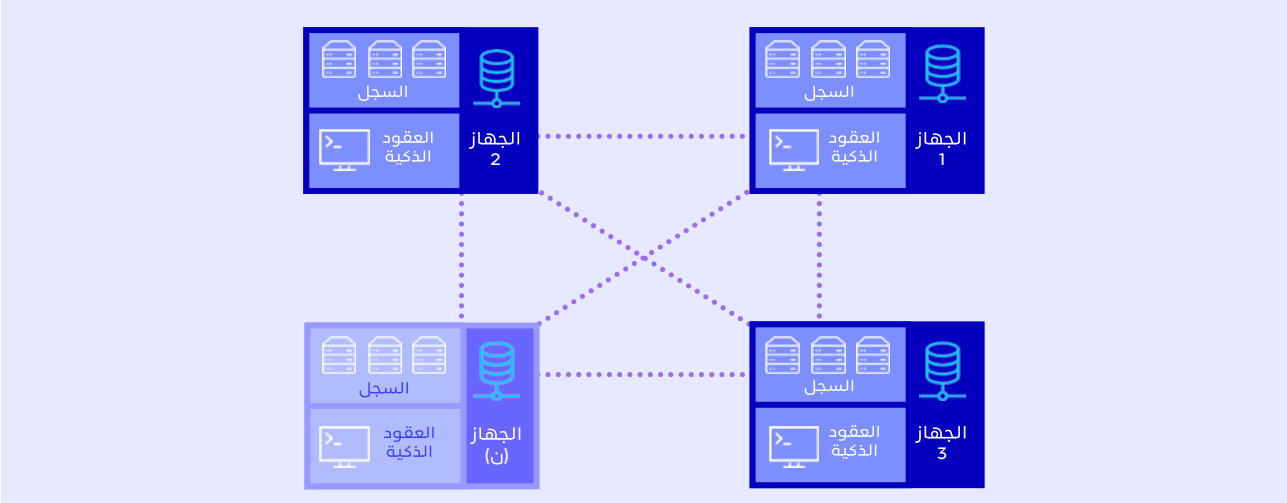
غيـر قابلـة للتعديـل والتغييـر، ويكـون السـجل مُتاحًـا فقـط للمشـاركين فـي الشـبكة. وتُعـد تقنيـة سلسـلة الكتـل مفيـدة للوصـول إلـى اتفـاق بيـن المشـاركين، إضافـة إلـى تعزيـز الثقـة والشـفافية، وذلـك لكونهـا تتيـح الوصـول المُباشـر إلـى المعلومـات المطلوبـة داخـل شـبكة آمنـة تعمـل مـن نظيرٍ إلى نظير دون الحاجة إلى وسيط.

يوضح الشكل التالي منظومة سلسلة الكتل، بما في ذلك الشبكات والمنصات والتطبيقات:



الشكل رقم 1: منظومة تقنية سلسلة الكتل

وتتكـون شـبكة سلسـلة الكتـل -كمـا فـي الرسـم البيانـي أدنـاه- بشـكل أساسـي مـن أجهـزة متصلـة ببعضها، حيث يخزن كل جهاز نسخةً من السجل والعقود الذكية.



الشكل رقم 2: المكوّنات الأساسية لشبكة سلسلة الكتل: الأجهزة والسجل والعقود الذكية

3 الأنظمة والتنظيمات ذات الصلة

فيما يلي قائمةٌ بأبرز الأنظمة والتنظيمات الإلزامية التي قد تنطبق على حلول تقنية سلسلة الكتل، مع التنويه على وجود منظمين قطاعيين مثل البنك المركزي للقطاع المالي، كما تعنى الهيئة الوطنية للأمن السيبراني و مكتب ادارة البيانات الوطنية بالتنظيمات المتعلقة بالأمن السيبراني. مع التأكيد على ضرورة التحقق من أي تحديثات تطرأ على الوثائق المذكورة أو أي وثائق تصدر مستقبلاً.

	عنوان الوثيقة	الناشر	نطاق التطبيق
1	الإطار التنظيمي للحوسبة السحابية (CCRF) [3]	هيئة الاتصالات والفضاء والتقنية	خدمات سلسلة الكتل السحابية
2	الإطار التنظيمي للأمن السيبراني (CRF) [4]	هيئة الاتصالات والفضاء والتقنية	حلول سلسلة الكتل
3	القواعد العامة للمحافظة على البيانات الشخصية للمستخدمين [5]	هيئة الاتصالات والفضاء والتقنية	حلول سلسلة الكتل التي تعالج البيانات الشخصية

3 الإطار التنظيمي للحوسبة السحابية (CCRF)
https://www.cst.gov.sa/ar/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx

4 الإطار التنظيمي للأمن السيبراني (CRF)
https://regulations.cst.gov.sa/ar/pages/published-document.aspx#/published-document

5 القواعد العامة لحماية البيانات الشخصية الصادرة عن هيئة الاتصالات والفضاء والتقنية
https://www.cst.gov.sa/ar/RulesandSystems/privacy/Pages/default.aspx

4 إرشادات عامّة

يهدف هذا القسم إلى مساعدة المسؤولين التنفيذيين على اتخاذ القرارات المهمة المتعلقة بتقنية سلسلة الكتل.

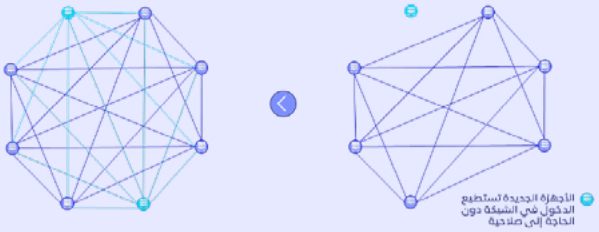
1.4 اختيار النوع المناسب من سلسلة الكتل

اختيار نوع سلسلة الكتل بناءً على مستوى الخصائص المطلوبة مثل الشفافية، وإمكانية الوصول، وقابلية التوسع، وآلية إدارة الصلاحيات، وعدم قابلية تغيير البيانات (immutability)

يمكن تصنيف شبكات سلسلة الكتل إلى نوعين؛ بناءً على إمكانية الوصول إليها، ووفقًا لنموذج الصلاحيات الخاص بها:

الشبكات العامة التي لا تحتاج إلى تصريح للمشاركة فيها (Permissionless)

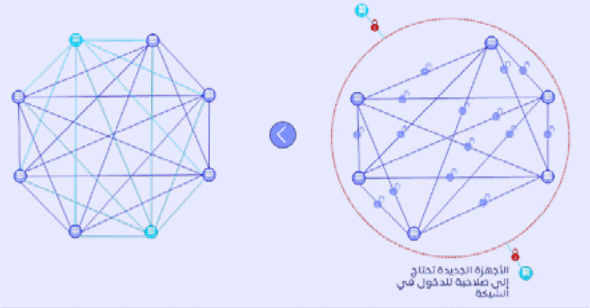
هي التي تُمكّن كل جهاز من الوصول إليها، والمشاركة في خوارزمية الاتفاق دون الحاجة إلى طلب صلاحية، ومن أشهر أمثلتها: شبكتا Bitcoin و Ethereum.



الشكل رقم 3: الشبكات العامة

الشبكات الخاصة التي تتطلب تصريحًا للمشاركة فيها (Permissioned)

هي التي يمكن أن تمتلكها جهة أو عدة جهات، بحيث تتحكم في منح صلاحية الوصول للشبكة فقط، أو المشاركة كذلك في خوارزمية الاتفاق.



الشكل رقم 4: الشبكات الخاصة

وبما أن الوصول في الشبكات الخاصة محدد لأجهزة معيّنة؛ فإن الشبكات العامة توفر لا مركزيةً أعلى.

2.4 تقييم شبكات سلسلة الكتل المتاحة

دراسة الشبكات المتاحة وبحث إمكانية المشاركة فيها بدلاً من إنشاء شبكة جديدة

عند توفر شبكة قائمة تخدم حالة الاستخدام المخطط لها، وتلبي متطلبات العمل؛ فإنه يُوصى بالانضمام لها بدلاً من إنشاء شبكة جديدة تؤدي الغرض نفسه، وذلك لتسريع وقت الدخول إلى السوق، مع تقليل التكاليف، وتجنّب هدر الموارد.

كما تؤدي المشاركة في الشبكات الموجودة إلى زيادة عدد مستخدميها، مما يجعلها أكثر قيمة وفائدة.

3.4 تطبيق الترميز (Tokenization)

يساهم الترميز في تمثيل الأصول الرقمية والمادية على سلسلة الكتل. وفيما يلي توضيح المقارنة بين استخدام الرموز القابلة أو استخدام الرموز غير القابلة للاستبدال، مع أمثلة على معاييرها.

إنشاء رموز قابلة للاستبدال

استخدام الرموز القابلة للاستبدال ومعاييرها لتمثيل الأصول المتماثلة والتي يمكن تقسيمها على أجزاء

تُعدّ عمليات إدارة المخزون إحدى المجالات المناسبة لاستخدام الرموز القابلة للاستبدال. حيث تتضمن إدارة المخزون تتبّع عدد كبير من نفس المنتجات التي يمكن استخدام الرموز القابلة للاستبدال في تمثيل مخزون الوحدات وتتبّعه بشكل مباشر، ممّا يسمح بإعادة التخزين في الوقت المناسب قبل نفاد المخزون. وتُعدّ هذه الطريقة مُفيدة خصوصًا للجهات التي تدير مخزون جهات أخرى.

ويعد بروتوكول ERC-20 [6] الخاص بشبكة Ethereum هو المعيار الأكثر شيوعًا للرموز القابلة للاستبدال.

6 EIP-20: معيار الرموز القابلة للاستبدال، Ethereum
https://eips.ethereum.org/EIPS/eip-20

استخدام الرموز غير القابلة للاستبدال ومعاييرها لتمثيل الأصول الفريدة التي لا يمكن تقسيمها على أجزاء

تستخدم الرموز غير القابلة للاستبدال لتمثيل الأصول الفريدة، مثل: القطع الفنية الفريدة من نوعها، أو غيرها من المنتجات ذات الإصدار المحدود؛ بحيث يكون لكلٍ من هذه الأصول قيمة محددة يقررها من يملكها. كما لا يمكن تجزئة الأصل الواحد أثناء تداولها.

ويعد بروتوكول ERC-721 [7] الخاص بشبكة Ethereum هو المعيار الأكثر شيوعًا للرموز غير القابلة للاستبدال.

7 EIP-721: معيار الرموز غير القابلة للاستبدال، Ethereum
https://eips.ethereum.org/EIPS/eip-721

5 إرشادات البنية الهيكلية

يهدف هذا القسم إلى إرشاد المسؤولين التنفيذيين والمهندسين فيما يتعلق بالجوانب البنيويّة عند تصميم حلول قائمة على تقنية سلسلة الكتل.

1.5 اختيار البنية الأنسب لتطبيقات سلسلة الكتل

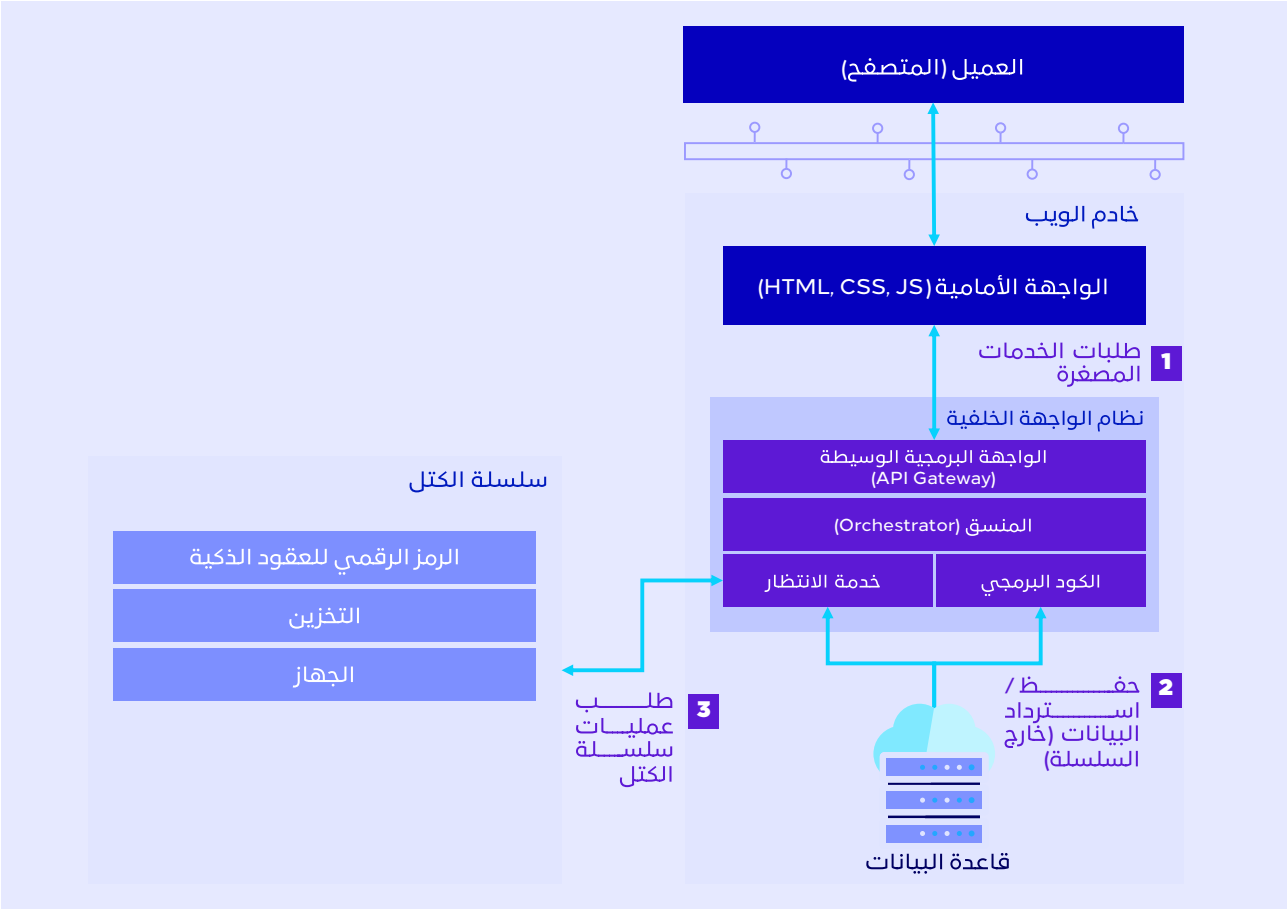
تحديد البنية الأكثر ملاءمة لتطبيقات سلسلة الكتل وفقًا لمتطلبات حالة الاستخدام، ونموذج الحوكمة، ومستوى الأمان أو الخصوصية المطلوب

على الرغم من الطابع اللامركزي لتقنية سلسلة الكتل، فإن التطبيقات التي تستخدم هذه التقنية قد تكون مركزية أو لا مركزية.

بالنسبة لتطبيقات الويب المركزية التقليدية، فعادةً ما تتكون من:

- **واجهة أمامية (Front-end)** تتضمن بشكل أساسي واجهة المستخدم.
- **نظام الواجهة الخلفية (Backend System)** بما في ذلك الكود البرمجي (Business Logic) الذي يُنفذ بواسطة واجهة المستخدم.
- **قاعدة بيانات (Database)** لتخزين البيانات التي يتم التعامل معها عبر الواجهة الخلفية، بالإضافة إلى البيانات المُستخدمة لتنفيذ الكود البرمجي.

يُمثّل الشكل التالي مراحل سير العمل في التطبيقات المركزية انطلاقًا من الواجهة الأمامية لسلسلة الكتل، وصولًا إلى الواجهة الخلفية وقاعدة البيانات. وتجدر الإشارة إلى أن نظام الواجهة الخلفية وقاعدة البيانات في مثل هذه البنية مركزيان، وبالتالي فإنهما يمثلان نقطة توقف حرجة (Single point of failure) أي أن توقف أحدهما عن العمل يؤدي إلى توقّف التطبيق بشكل كامل.



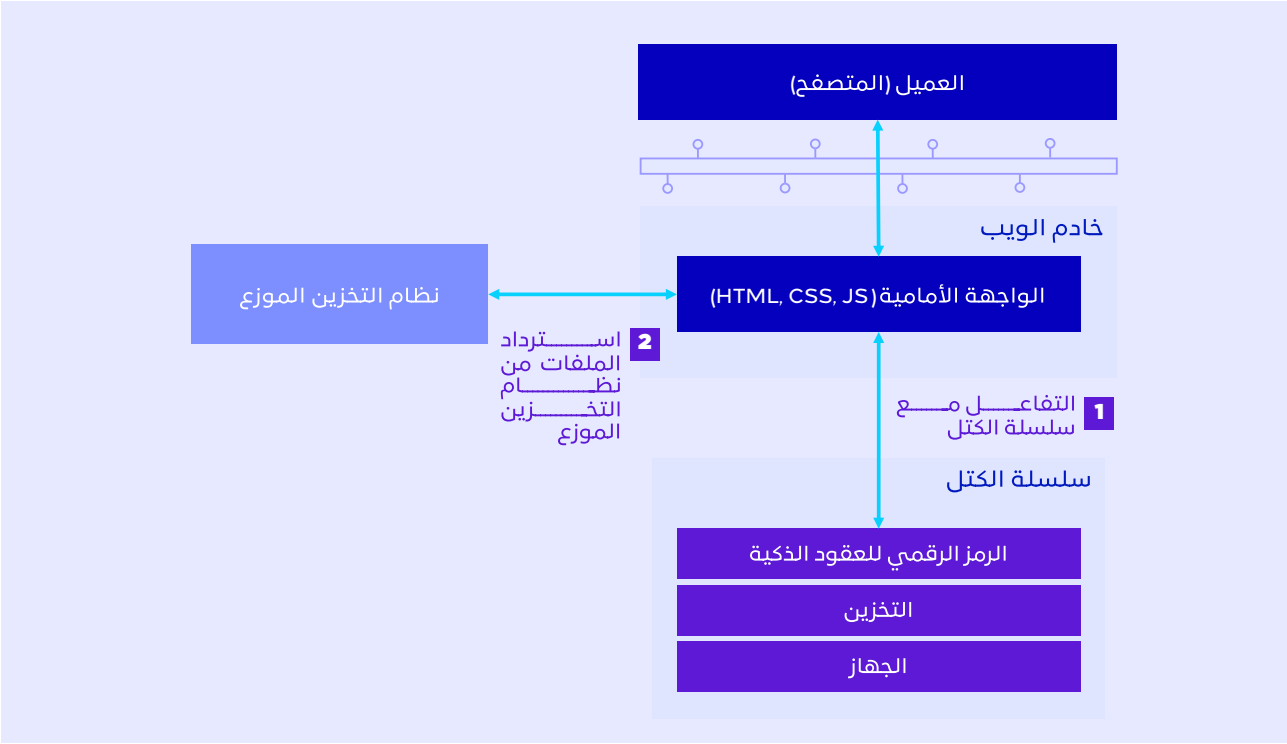
الشكل رقم 5: بنية تطبيقات سلسلة الكتل المركزية

أما بالنسبة للتطبيقات اللامركزية (dApps) فهي تطبيقات تُشغَّل في شبكة سلسلة الكتل بدلاً من تشغيلها في خادم مركزي، وتتكون التطبيقات اللامركزية من:

واجهة أمامية (Front-end) تتضمن بشكل أساسي واجهة المستخدم

نظام الواجهة الخلفية (Backend System) الذي يتضمن العقود الذكية

ويوضّح الشكل التالي مراحل سير العمل في التطبيقات اللامركزية، حيث تُرسل واجهة المستخدم للتطبيق اللامركزي استعلاماتها إلى سلسلة الكتل مباشرةً؛ دون الحاجة إلى نظام مركزي في المنتصف، ممّا يجعل التطبيق أكثر تحمّلاً للأخطاء. لذلك يُوصى باستخدام التطبيقات اللامركزية عندما تكون تجربة المستخدم واللامركزية من الأولويّات.



الشكل رقم 6: بنية تطبيقات سلسلة الكتل غير المركزية

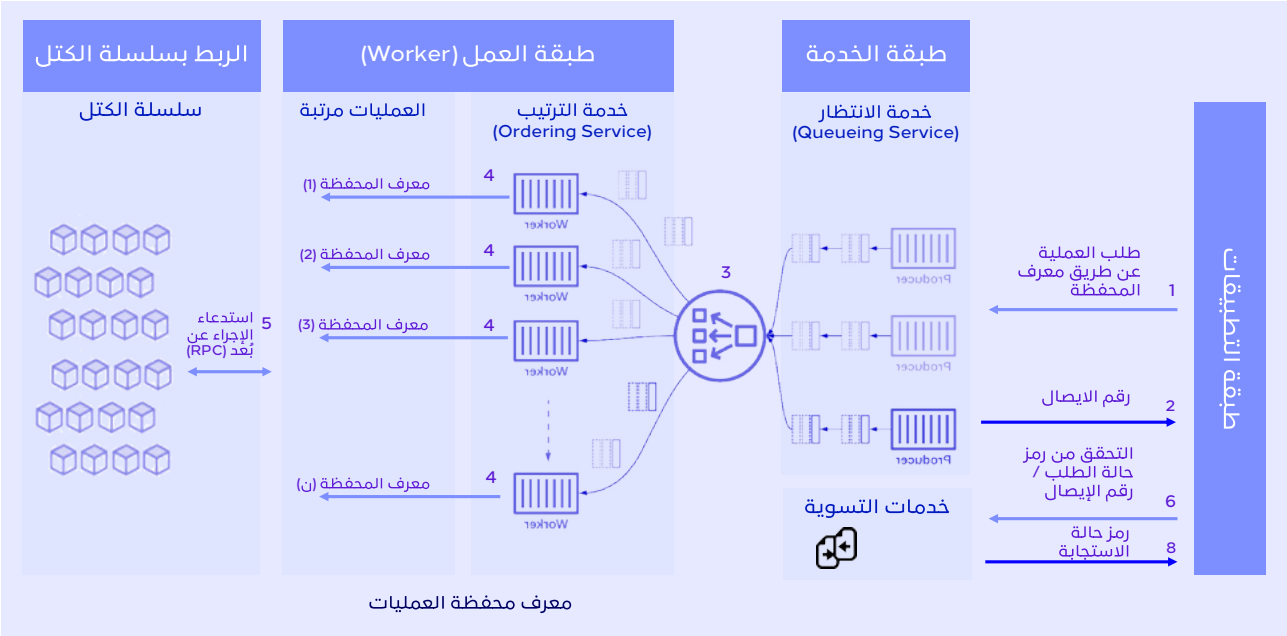
2.5 إدارة الأداء

فصل الكود البرمجي (Business Logic) عن الأجهزة في تطبيقات سلسلة الكتل

تمتلك منصات سلسلة الكتل حدّاً أعلى للإنتاجية -أي عدد العمليات التي يمكن تنفيذها في الثانية-. وتتأثر الإنتاجية بحجم الكتلة وخوارزمية الاتفاق المُستخدمة على الشبكة. على سبيل المثال: تكون الإنتاجية عند استخدام خوارزمية إثبات الحصة (PoS) أعلى من الإنتاجية باستخدام خوارزمية إثبات العمل (PoW).

كما أن هندسة التطبيقات التي تُبنى على تلك المنصات تؤثر على الإنتاجية؛ فعند فصل الكود البرمجي عن أجهزة سلسلة الكتل -مثلاً- فإن الإنتاجية تتحسن. ولذلك يوصى في تطبيقات الويب المركزية بتطوير آليات الانتظار (queue mechanisms) لترتيب العمليات الواردة من واجهة المستخدم، بهدف تفادي إثقال الأجهزة المشاركة في شبكة سلسلة الكتل بطلبات كثيرة في وقت واحد، مما قد يكون سببًا في تعطل الشبكة.

يوضح الشكل التالي تكامل شبكات سلسلة الكتل الخاصة مع مكوّنات التطبيقات التقليدية:



الشكل رقم 9: تدفّق عمليات تقديم العمليات من خلال استخدام خدمة الانتظار حسب الترتيب

يوضح الشكل أعلاه أن خدمة الانتظار (Queuing Service) تتلقى الطلبات من التطبيق، لتتولّى بعد ذلك خدمة الترتيب (Ordering Service) مهام تنظيم الطلبات وإرسالها إلى شبكة سلسلة الكتل لكل محفظة على حدة. ثم تقوم خدمة الانتظار بإجراء التسوية، وإعادة حالة العملية إلى العميل (سواء كانت مُعلّقة أو مُكتملة). كما أن استخدام البنية التي تم توضيحها سابقًا في شبكة سلسلة كتل عامة مثل Ethereum لإرسال عمليات متعددة من المحفظة نفسها سيؤدي إلى تقليل فقدان البيانات وتجنب أوقات الانتظار الطويلة للحصول على الموافقة لتنفيذ العمليات.

6 إرشادات قابلية التشغيل البيني

يهدف هذا القسم إلى تزويد المسؤولين التنفيذيين والمهندسين بأفضل الممارسات لتعزيز قابلية التشغيل البيني بين مكوّنات حلول سلسلة الكتل الواحدة وبين سلاسل الكتل والسحابات المتعددة.

1.6 استخدام التقنيات مفتوحة المصدر

تضمين التقنيات مفتوحة المصدر في بنية الحلول قدر الإمكان

يُعدّ اعتماد مكوّنات مفتوحة المصدر أمرًا بالغ الأهمية لتطوير تطبيقات لسلسلة الكتل، بحيث تتبع معايير رائدة قابلة للصيانة والتحديث دون تكبّد تكاليف كبيرة. كما يساهم استخدام مكوّنات مفتوحة المصدر في تسهيل الوصول إلى تطبيقات سلسلة الكتل، وتعزيز إعادة استخدامها. وينطبق ذلك على كل أجزاء تطبيقات سلسلة الكتل، بدءاً من منصة سلسلة الكتل إلى الواجهة الأمامية.

2.6 بناء تطبيقات قابلة للتشغيل بين سلاسل الكتل

تصميم تطبيقات سلسلة الكتل بطريقة تتيح إمكانية نقل التطبيق من سلسلة كتل إلى أخرى

غيّر مفهوم سلسلة الكتل نموذج التطبيقات التقليدية، عبر إزالة الكود البرمجي من أنظمة الواجهة الخلفية وتعزيز التكامل المباشر للواجهة الأمامية مع شبكة سلسلة الكتل. لذلك فإنه من الأفضل تصميم تطبيقات برمجية تتمكّن من مواكبة التطورات عن طريق إتاحة نقل التطبيق بين سلاسل الكتل، أو إدخال سلاسل جديدة إلى التطبيق؛ دون الحاجة إلى إعادة هيكلة كاملة.

وإذا كانت منصة سلسلة الكتل لا توفّر خاصية التشغيل البيني بين سلاسل الكتل، فإنه يُوصى ببناء نظام خلفي وسيط يتيح هذا النوع من التشغيل البيني. كما يُوصى أيضًا ببناء نموذج بيانات مشترك لتسهيل التشغيل البيني بين سلاسل الكتل. (للمزيد من التفاصيل، يُرجى الرجوع إلى الإرشاد رقم 9.3). كما يمكن استخدام الحلول التي تُتيح قابلية التشغيل البيني للبيانات عبر شبكات سلسلة الكتل المتعددة، مع التنويه على أهمية ما يلي:

التأكد من موثوقية وأمن شبكات سلسلة الكتل المراد دمجها، بحيث يتم تفادي تسرّب البيانات [8]

تقييم الحلول بدقة لتجنّب المشاكل التي قد تنشأ عن أي عناصر لا تزال قيد التطوير.

3.6 تصميم تطبيقات قابلة للتشغيل بين السحابات

تصميم تطبيقات سلسلة الكتل بطريقة تجعلها متوافقة مع أكثر من منصة سحابية واحدة

مما يسهل توافق التطبيق بين السحابات استخدامُ بنية الخدمات المصغرة (Microservices Architecture) والحاويات (Containers)، نظرًا لدور الحاويات في تمكين التدشين السريع للتطبيقات بين مختلف مقدمي الخدمات السحابية. كما يمكن استخدام الحاويات السحابية لعزل مختلف طبقات التطبيق، بهدف تحقيق الكفاءة على صعيد الموارد، وتسريع التشغيل (Boot)، وتبسيط عملية التدشين كلما أمكن ذلك.

كما يساهم استخدام التقنيات مفتوحة المصدر في بناء تطبيقات تتوافق مع أكثر من منصة سحابية واحدة. (للمزيد من التفاصيل، يُرجى الرجوع إلى الإرشاد رقم 6.1)

8 Cross Chain Bridges Security
https://thedefiant.io/vitalik-eth-cross-chain-bridges-security/

7 إرشادات خصوصية البيانات

يهدف هذا القسم إلى تزويد المهندسين بأفضل الممارسات للحفاظ على خصوصية البيانات وموثوقيتها عبر حلول سلسلة الكتل.

1.7 تقييم حجم البيانات وحساسيتها لاختيار نوع التخزين

مراعاة حجم البيانات وحساسيتها عند المفاضلة بين تخزين البيانات داخل السلسلة أو خارجها

يُفضل تخزين البيانات التالية خارج السلسلة:

البيانات الضخمة: **إذ قد تكون المساحة التخزينية للعقود الذكية في سلسلة الكتل محدودة.**

البيانات الحسّاسة: **نظرًا لأنها قد تتطلب الحذف لاحقًا، بينما طبيعة التخزين في سلسلة الكتل لا تسمح بالحذف.** من الأمثلة على البيانات التي يوصى بتخزينها خارج سلسلة الكتل: المستندات التي تحتوي على بيانات المريض في منشأة للرعاية الصحية.

ويجدر التنويه إلى أهمية تطبيق الإجراءات الأمنية عند تخزين البيانات خارج السلسلة، وذلك لضمان تقييد الوصول إلى البيانات والاطّلاع عليها. كما يُفضل أن يبحث مستخدمو شبكة سلسلة الكتل عن خيارات التخزين خارج السلسلة التي تناسب متطلباتهم الأمنية.

بينما يُفضل تخزين البيانات داخل السلسلة عندما تكون هناك حاجة لتتبّع البيانات بشكلٍ مُفصّل، مع إمكانية استعادتها من الشبكة إذا لزم الأمر. كما أن التخزين داخل السلسلة يُعدّ من احتياجات البنية التحتية. ومن أمثلة الاستخدام المناسب للتخزين داخل السلسلة: تخزين بيانات خطوات الإنتاج في سلسلة التوريد لجهة التصنيع

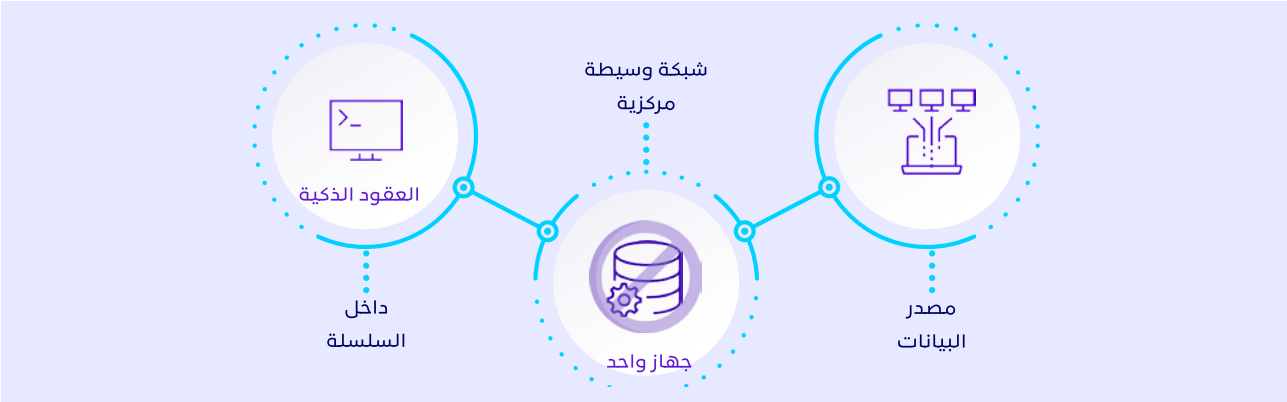
2.7 ربط البيانات خارج السلسلةبكة غير مركزية

استخدام شبكات وسيطة لامركزية لربط البيانات خارج السلسلة (Off-chain) بطريقة موثوقة.

توجد برامج وسيطة لربط شبكات سلسلة الكتل ببيانات العالم الخارجي الفعلية، كالأحوال الجوية مثلًا، ويتعارف عليها بمسمى أوراكلس (Oracles). تعمل أنظمة البرامج الوسيطة خارج السلسلة على مناداة الواجهة البرمجية (API) وتخزّن بيانات الردّ بشكل دوري كعمليات على شبكة سلسلة الكتل .9على سبيل المثال، يمكن استخدام أنظمة البرامج الوسيطة لتسجيل تحديثات سعر منتج ما في السلسلة وبدء عملية شراء آلية عبر عقد ذكي عندما يصل السعر إلى حد معيّن.

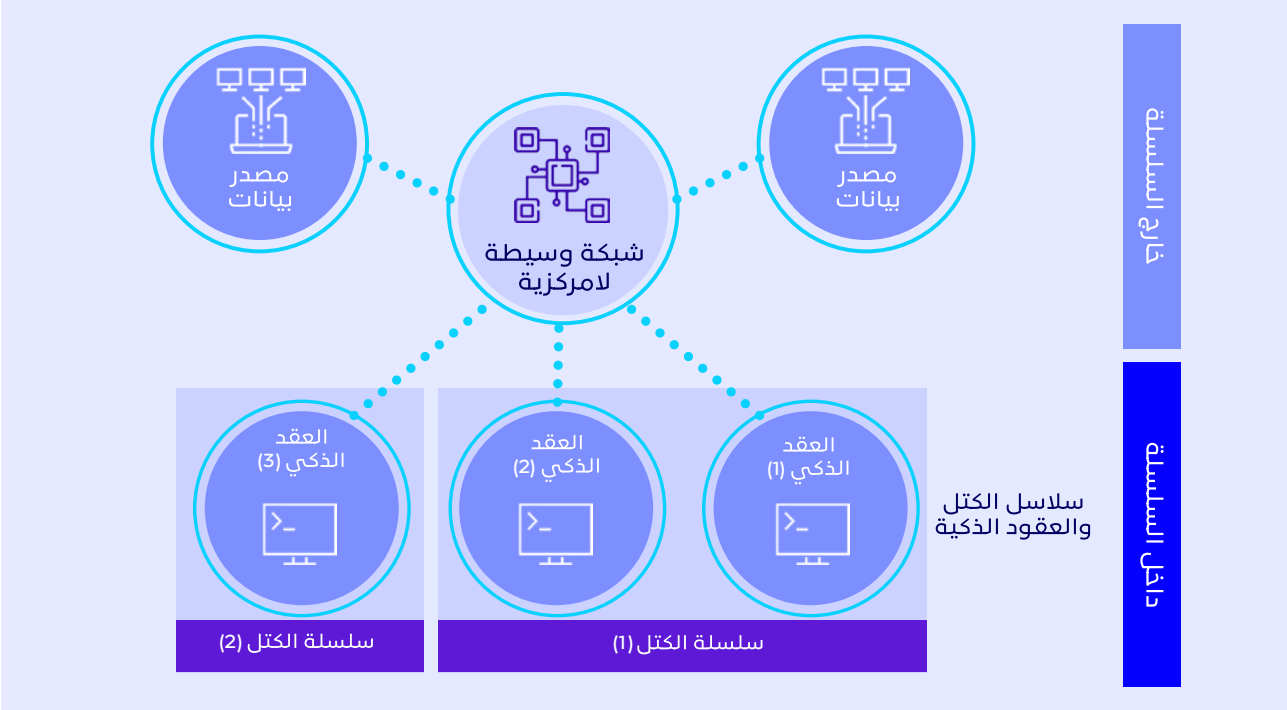
9 أوراكل، 2022) (Ethereum
https://ethereum.org/en/developers/docs/oracles/

يوضح الرسم البياني التالي كيفية عمل نظام وسيط مركزي.



الشكل رقم 7: الأنظمة الوسيطة المركزية

لكن التحدي في الأنظمة الوسيطة المركزية هو اعتمادها على مصدر بيانات واحد، ففي حال تم اختراق مصدر البيانات، فسيتعرض أمن البيانات في سلسلة الكتل للخطر. لذلك، يُوصى باستخدام الأنظمة الوسيطة اللامركزية التي تستمد البيانات من مصادر متعددة، لأنها أقل عرضة لهذا النوع من المخاطر.



الشكل رقم 8: الأنظمة الوسيطة اللامركزية

3.7 استخدام التخزين المُوزّع

استخدام التخزين المُوزّع عند الحاجة إلى توزيع البيانات بين عدة مشاركين في الشبكة، مع وجوب التحقّق منها كدليل غير قابل للتحريف والتزوير

عند اعتماد تخزين البيانات خارج السلسلة؛ فإن التخزين الموزّع هو أحد الخيارات المناسبة لتخزين بيانات مثل: إثبات إيصالات، أو وثائق مرجعية مُصدّقة، أو كمية كبيرة من البيانات عبر شبكة إنترنت الأشياء، وذلك بهدف تجاوز تحدي توسع سلسلة الكتل، وتقليل تكاليف العمليات المرتفعة التي قد تنتج عن عمليات التخزين في سلسلة الكتل.

ويُعد نظام (IPFS) أحد أبرز الأنظمة التي تدعم التخزين المُوزّع، بحيث يتم تخزين المحتوى ومشاركته بين المستخدمين في شبكات سلسلة الكتل.

4.7 إدارة سرية البيانات على شبكة سلسلة الكتل

استخدام خوارزميات اختزال (Hashing) آمنة وموثوقة

يُعد تشفير البيانات عن طريق خوارزميات الاختزال (Hashing) وسيلةً للمحافظة على سلامة البيانات وسريتها في سلسلة الكتل، وذلك عن طريق تخزين تلك البيانات خارج السلسلة (مثلاً في التخزين الموزّع)، بينما يتم تخزين اختزالها (Hash) فقط داخل السلسلة.

وعند تشفير البيانات فإنه يُوصى باستخدام خوارزميات الاختزال التي يتوفر فيها ما يلي:

- المعايير المُعتمدة من قبل الجهات التقنية الرائدة في القطاعين العام والخاص في جميع أنحاء العالم.
- شيوع استخدامها في حلول سلسلة الكتل.
- إمكانية معرفة أي تغيير في البيانات، لأن أي تغيير في المدخلات سيؤدّي إلى إنتاج مخرجات مختلفة تمامًا.

ومن تلك الخوارزميات خوارزمية (SHA-256)، **وكذلك** خوارزمية (keccak256) التي اكتسبت زخمًا مهمًّا في عالم سلسلة الكتل لكونها خوارزمية التشفير المُضمنة في شبكة Ethereum. كما أن البعض يعتبر خوارزمية (SHA-3) أكثر أمانًا من (SHA-256). مع التنويه على أهمية متابعة وتقييم خورزميات التشفير لضمان كفائتها وتفادي الخوارزميات التي تم كسرها ولم تعد فعالة.

كما توجد طرق أخرى للحفاظ على سرية البيانات، ومنها: تشفير العمليات باستخدام برهان المعرفة الصفرية (ZKP) الذي يمكّن أحد الأطراف (المُثبِت) من تأكيد صحة معلومات مُحدّدة لطرف آخر (المُدقّق) دون الكشف عن هذه المعلومات.

8 إرشادات الأمان

يهدف هذا القسم إلى تزويد المهندسين بأفضل الممارسات لتعزيز أمان سلسلة الكتل.

1.8 تحديد حجم شبكة سلسلة الكتل المناسب

تحديد العدد المناسب من الأجهزة في الشبكة، وتنفيذ الاستراتيجية الأنسب للتوفر العالي (high-availability)

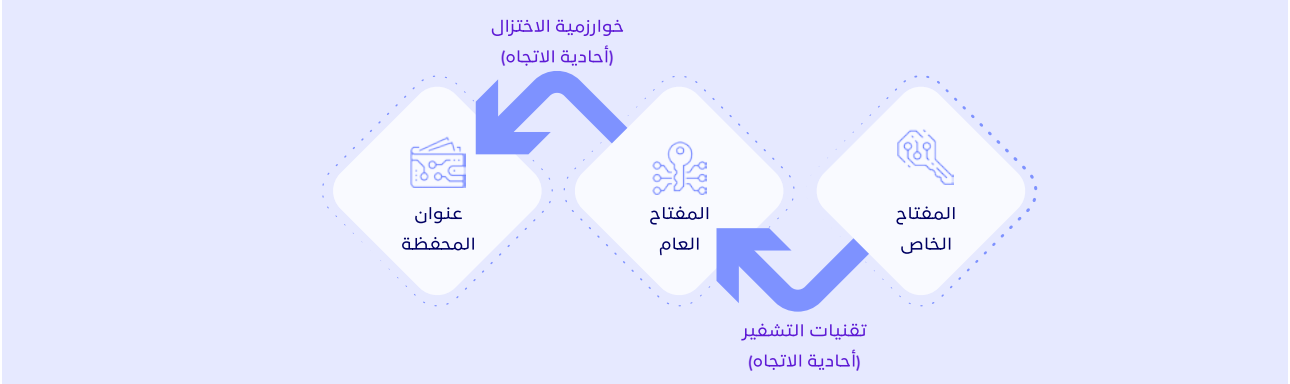
من الأفضل ضمان توفر عدد مُعيّن من الأجهزة النشطة بما يتناسب مع العدد الإجمالي للأجهزة في الشبكة، ووفقًا لخوارزمية الاتفاق. حيث يُوصى -مثلاً- بأن يكون عدد الأجهزة النشطة أكبر من ثُلثي عدد الأجهزة الإجمالي في الشبكة، بهدف ضمان التنفيذ الصحيح لخوارزمية الاتفاق البيزنطية لتدارك الأخطاء (BFT).

2.8 تعريف مستخدمي تقنية سلسلة الكتل

الاستفادة من محافظ المستخدمين لتعريف هوية المستخدم ومصداقيته وسلامة بيانات العمليات

تسمح محفظة المستخدمين بإرسال العمليات عبر شبكة سلسلة الكتل (مثل تداول العملات المشفرة والرموز) من خلال توقيع تلك العمليات في المحفظة. وتُعرف التوقيعات الرقمية (Digital signatures) التي تُستخدم لتشفير العمليات بأنها طرق حسابية تنقسم إلى جزئين: خوارزمية إنشاء التوقيع التي تستخدم مفتاحًا خاصًا (Private Key) لتوقيع العملية، وخوارزمية التحقق من التوقيع التي تستخدم المفتاح العام (Public Key) لإنشاء عنوان المحفظة.

يوضح الشكل التالي العلاقة بين كلٍ من المفتاح الخاص والمفتاح العام وعنوان المحفظة.



الشكل رقم 10: استخدام التشفير والاختزال لعنوان المحفظة

إذا قام المستخدمون بتوقيع عملياتهم باستخدام المفاتيح الخاصة فإنه يمكن لهم إثبات هويتهم بشكل موثوق دون الإفصاح عن تلك المفاتيح.

3.8 مراجعة العقود الذكية لشبكة سلسلة الكتل

مراجعة العقود الذكية كجزء من مراحل تطوير شبكة سلسلة الكتل

مع استمرار تطوّر تقنية سلسلة الكتل فإنه من المُتوقّع اكتشاف أخطاء ومخاطر أمنية جديدة. لذلك يُوصى بمواكبة أفضل الممارسات الأمنية في تطوير العقود الذكية.

وفيما يلي بعض الممارسات الرئيسية لتقليل مخاطر الأمان التي قد تؤثر على العقود الذكية:[10]

- ضمان الاختبار المناسب قبل النشر في بيئة إنتاجية.
- تتبّع الإجراءات المناسبة لإدارة الأخطاء ونقاط الضعف.
- تفادي نداءات الدوال الخارجية (External functions) أو تقليلها؛ لأنها قد تؤدي إلى تهديدات محتملة.
- إعطاء الأولوية للوضوح والبساطة في العقود الذكية لتقليل احتمالية حدوث الأخطاء.

10 أفضل ممارسات عقود Ethereum الذكية، Github
https://consensys.github.io/smart-contract-best-practices/development-recommendations/

9 إرشادات الحوكمة

قد تكون شبكات سلسلة الكتل مملوكة لجهة واحدة أو عدة جهات حكومية أو خاصة. ولذلك فإنه يمكن لمالكين متعددين المشاركة في عمليات تصميم الحلول وتشغيلها، مما يستدعي وجود حوكمة واضحة تحدِّد طريقة توزيع الأدوار والمخاطر والمسؤوليات بين المشاركين في الشبكة.

يوفّر هذا القسم للمسؤولين التنفيذيين إرشادات مرتبطة بالحوكمة، بهدف تعظيم الاستفادة من حلول سلسلة الكتل.

1.9 حوكمة الشبكة

إنشاء إطار حوكمة عام، وفرض الامتثال تلقائيًّا داخل إطار العمل إن أمكن.

تتكوّن أطر حوكمة شبكات سلسلة الكتل من قواعد تجارية وقانونية وتقنية تنصّ على كيفية استخدام الشبكة لتحقيق الهدف المرجوّ منها. لذلك فإن أطر الحوكمة تعد حلقة وصل بين التنفيذ التقني ومتطلبات العالم الحقيقي. ولذلك يُوصى بتحديد إطار الحوكمة العام، وتوثيقه، والاتفاق عليه بين مالكي الشبكة والمشاركين فيها. ومن ذلك -على سبيل المثال لا الحصر- ما يلي:

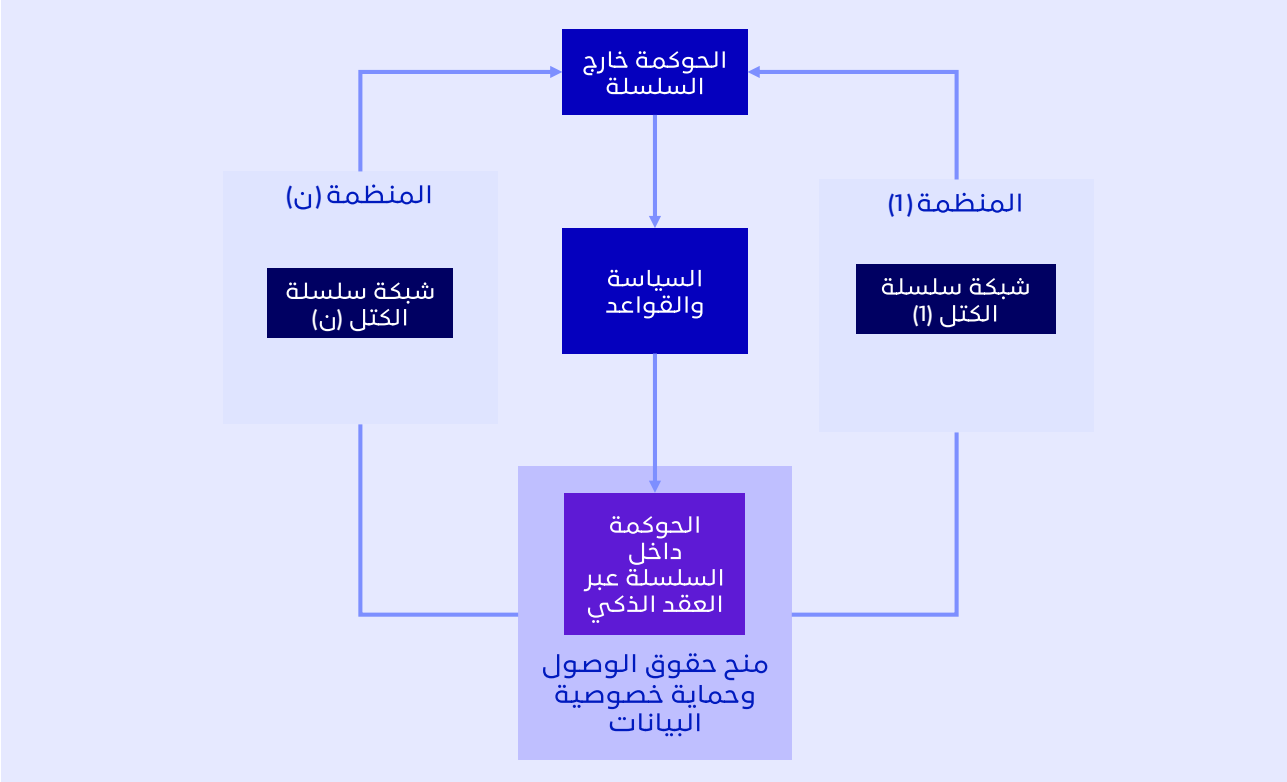
- إجراءات اتّخاذ القرارات وحل الخلافات.
- أدوار ومسؤوليات أعضاء الشبكة، بما في ذلك مسؤولية ضمان الالتزام بإطار الحوكمة.
- سياسات وقواعد الانضمام إلى شبكة سلسلة الكتل، أو الخروج منها، أو التفاعل معها.
- نموذج التمويل وتوليد الإيرادات (إذا وُجد)
- قواعد الوصول إلى الملكية الفكرية واستخدامها.

  المعايير واللوائح المعمول بها.
- حوكمة البيانات، وحوكمة عمليات التدقيق (المزيد من التفاصيل في الإرشادات 9.2 و9.3).

مع التنويه إلى أن نموّ الشبكة وتزايد عدد مالكيها يستدعي إعادة تقييم إطار الحوكمة دوريًا. ومن الأفضل أيضًا إنشاء بيئة اختبار -أو حالة استخدام تجريبية- لتقييم مدى امتثال حل سلسلة الكتل لإطار الحوكمة.

يُلّخص الشكل التالي الأساليب المتبعة لاختبار مدى امتثال شبكة سلسلة الكتل لإطار الحوكمة المعمول به، حيث يمكن أن تتحقق الجهات من الامتثال خارج السلسلة؛ سواءً كان بشكل

يـدوي، أو مـن خـلال الأنظمـة الخارجيـة المُتاحـة. كمـا يمكـن كتابـة قواعـد الحوكمـة كعقـود ذكيـة داخل شبكة سلسلة الكتل، بهدف أتمتة متابعة الامتثال لتلك القواعد.



الشكل رقم 11: نظام الحوكمة المُوزّعة كنموذج مُحتمل لها

2.9 حوكمة عمليات التدقيق

تحديد إجراءات ومسؤوليات التدقيق على مستوى شبكة سلسلة الكتل ضمن إطار الحوكمة العام

يُوصى بأن يحدّد إطار الحوكمة آلية إجراء عملية التدقيق. كما يمكن استخدام شبكة سلسلة الكتل أو العقود الذكية لأتمتة عملية التدقيق للحصول على نتائج موثوقة في الوقت الفعلي (real-time)، مما يؤدي إلى تعزيز الكفاءة مقارنةً بعمليات التدقيق اليدوية. كما تُمكّن حوكمة التدقيق عبر شبكة سلسلة الكتل من الرجوع إلى سجل عمليات التدقيق ومراجعتها في أي وقت.

يُوصى كذلك بتحديد المسؤول عن التدقيق ضمن إطار الحوكمة العام لشبكة سلسلة الكتل؛ سواء كان المسؤول من جهة واحدة أو عدة جهات، وذلك للتأكد من ضمان امتثال شبكة سلسلة الكتل لإطار الحوكمة وللمعايير واللوائح ذات صلة.

3.9 حوكمة البيانات

إنشاء إطار لحوكمة البيانات ضمن إطار الحوكمة العام

يمكن تبادل بيانات سلسلة الكتل عبر تطبيقات وأجهزة متعددة، لذلك فإنه من الأفضل إنشاء إطار عمل خاص بحوكمة البيانات، لوضع قواعد متينة للحصول على البيانات، وتخزينها، واستخدامها، وتبادلها.

يساهم هذا الإطار في ضمان خصوصية البيانات وسلامتها وأمانها، مع تعزيز مستوى الامتثال لإطار الحوكمة العام للشبكة وأي لوائح أخرى معمول بها.

وسعيًا إلى تسهيل عملية التكامل مع شبكة سلسلة الكتل، وتعزيز أداء قابلية التشغيل البيني؛ فإنه يُوصى بتحديد نموذج بيانات مشترك بين المشاركين في الشبكة كجزء من إطار حوكمة البيانات.

كما يُفضل أن يكون مدقّق حوكمة البيانات المسؤول عن التحكم باستخدام البيانات مُنفصلًا عن الجهة المُنتجة للبيانات، بهدف ضمان استقلالية البيانات والتنظيم العادل.

ولابد أن تكون الحوكمة ملزمةً لمالكي البيانات بالامتثال لإطار الحوكمة. وإذا كانت البيانات تابعةً لجهاز إنترنت الأشياء أو لنموذج ذكاء اصطناعي فإن الجهة المسؤولة عن إدارة الجهاز أو النموذج تعد هي المالكة للبيانات.

هيئة الاتصالات والفضاء والتقنية
Communications, Space &
Technology Commission