كيف أسهم المصدر المفتوح في تطور سلاسل الكتل؟

أكسل سيمون



الملخص:

يستعرض المقال تطور سلاسل الكتل من بيتكوين إلى مشروعات توسع الاستخدام وتعدل آليات الإجماع والخصوصية والحوكمة. ويشرح السجل الموزع ومنع الإنفاق المزدوج وإثبات العمل، ثم يعرض كيف أتاحت الشيفرة المفتوحة تجارب مثل (Namecoin) و(Litecoin) ومقاربات الخصوصية المختلفة. ويناقش الانتقال إلى العقود الذكية والتطبيقات الموزعة، وتحديات السرعة والسعة، والفرق بين الشبكات العامة غير المأذونة والشبكات الخاصة المأذونة. كما يتناول أثر تغيير العضوية والثقة في اختيار الإجماع والمسؤوليات القانونية وإدارة الهوية. ويبرز أن الانفتاح يدعم الفحص والابتكار لكنه لا يحل الحوكمة وحده، مع الإشارة إلى ربط الشبكات بوصفه تحديًا لاحقًا. وتبقى الأمثلة والتوصيفات مرتبطة بمرحلة المصدر، وليست مقارنة محدثة أو توصية باختيار أصل أو شبكة.

الكلمات المفتاحية: سلاسل الكتل، المصدر المفتوح، الإجماع، العقود الذكية، الحوكمة

من المألوف، عند العمل على نسخة جديدة من مشروع مفتوح المصدر، إلحاق (ng) باسمه، اختصارًا لـ«الجيل التالي». ولحسن الحظ، تجنبت سلاسل الكتل هذا المأزق في تسميتها حتى الآن رغم تطورها السريع. لكن التغييرات كثرت في هذه المنظومة المفتوحة المتطورة، وتناقلت مشروعاتها الأفكار الجيدة وأعادت مزجها وتطويرها، كما يحدث عادة في المصدر المفتوح. سأستعرض أجيال سلاسل الكتل المختلفة، والأفكار التي ظهرت لمعالجة مشكلات المنظومة. ولكل تصنيف حدود، ولا يخلو من معترضين، لكنه يقدم دليلًا تقريبيًا وسط هذا العدد الكبير من المشروعات.

البداية: بيتكوين:

ينبع الجيل الأول من سلسلة بيتكوين، سجل العملة المشفرة اللامركزية القائمة على الند للند، التي انتقلت من طرائف موقع (Slashdot) إلى موضوع عام واسع الانتشار. هذه السلسلة سجل موزع يتتبع معاملات جميع

المستخدمين لمنع إنفاق العملة نفسها مرتين، وهي مهمة أسندت تاريخيًا إلى طرف ثالث هو المصرف. ولمنع المهاجمين من التلاعب، ينسخ السجل إلى كل حاسوب مشارك في شبكة بيتكوين، ولا يحدّثه في المرة الواحدة إلا حاسوب واحد. ولاختيار صاحب حق التحديث، ينظم النظام كل عشر دقائق سباقًا بين الحواسيب، تكلف المشاركة فيه طاقة كثيرة. ويفوز المنتصر بحق تسجيل معاملات الدقائق العشر الأخيرة، وهي «الكتلة»، ويحصل على بعض بيتكوين مكافأة لجهده. وتسمى هذه آلية إجماع إثبات العمل. وهنا يبدأ الجانب المثير. أُطلقت بيتكوين بوصفها مشروعًا مفتوح المصدر في يناير 2009. وفي 2010، أدرك المجتمع الذي تجمع حولها، وكثير منه في منتديات (bitcointalk)، إمكان تعديل عدد من هذه العناصر، وبدأ التجريب. ظهر مشروع (Namecoin) أولًا، انطلاقًا من كون السلسلة شكلًا لقاعدة موزعة، واقترح تخزين بيانات عامة في قاعدة المعاملات. فإذا أمكن تسجيل انتقال المال، أمكن تسجيل انتقال أصول أخرى، مثل أسماء النطاقات. وهذا هو الاستخدام الرئيس لـ(Namecoin)، الذي بدأ العمل في أبريل 2011، بعد عامين من تقديم بيتكوين. وبينما عدل (Namecoin) محتوى السلسلة، عدل (Litecoin) جانبين تقنيين: خفض المدة بين الكتل من عشر دقائق إلى دقيقتين ونصف، وتغيير طريقة السباق باستخدام (scrypt) بدل خوارزمية التجزئة الآمنة (SHA-256). وأتاح ذلك كون بيتكوين مفتوحة المصدر؛ إذ تتطابق (Litecoin) معها أساسًا في سائر الأجزاء. وكانت أول نسخة متفرعة تعدل آلية الإجماع، ممهدة الطريق لغيرها. وظهرت تنويعات كثيرة أخرى للشفرة. بدأ بعضها امتدادات مقترحة لبيتكوين، مثل بروتوكول (Zerocash) الهادف إلى إخفاء المعاملات وتعزيز قابلية الاستبدال، ثم أصبح عملة مستقلة هي (Zcash). ومع ابتكارات (Zcash)، باستخدام تطورات حديثة في التشفير تعرف ببراهين المعرفة الصفرية، فإنها تحافظ على التوافق مع معظم شفرة بيتكوين، وبالتالي تستطيع الانتفاع بابتكارات المشروع الأصلي. أما (CryptoNote) فلم يستخدم الشفرة نفسها، لكنه نشأ من المجتمع نفسه، وبنى على بيتكوين وفي مواجهتها، وعلى أفكار أقدم أيضًا. ونشر في ديسمبر 2012، وأدى إلى عملات عدة، أشهرها (Monero) عام 2014. وتتبع (Monero) نهجًا مختلفًا عن (Zcash)، لكنها تستهدف الخصوصية وقابلية الاستبدال نفسيهما. وكما يحدث غالبًا في المصدر المفتوح، توجد أكثر من أداة للمهمة.

الأجيال التالية: «(Blockchain-ng)»:

حتى هذه النقطة، انصبت التنويعات على تحسين العملات أو توسيعها لدعم معاملات أخرى. وهذا يقود إلى الجيل الثاني. بمجرد أن بدأ المجتمع تعديل الاستخدام والجوانب التقنية، لم يتأخر توسيع الفكرة وإعادة تصورها. فقد اقترح فيتاليك بوتيرين، المتابع القديم لبيتكوين، في أواخر 2013 أن تمثل معاملات السلسلة تغير حالات آلة حالات، وأن تكون السلسلة حاسوبًا موزعًا يشغل تطبيقات «العقود الذكية». وبدأ مشروع إيثريوم العمل في يوليو 2015، وحقق نجاحًا معقولًا في التطبيقات الموزعة. بل أدت شعبية بعضها، مثل (CryptoKitties)، إلى إبطاء السلسلة. وهذا يظهر أحد قيود السلاسل القائمة الكبيرة: السرعة والسعة. وتقاس السرعة غالبًا بالمعاملات في الثانية (TPS). واقترحت مناهج مثل التجزئة (sharding) والسلاسل الجانبية وحلول الطبقة الثانية. والحاجة إلى الابتكار هنا كبيرة. ومع شيوع «العقد الذكي» ووجود تقنية مثبتة لتشغيله، وإن ظلت بطيئة، تبلورت فكرة السلاسل المأذونة. فجميع الشبكات السابقة تملك خاصيتين ضمنيتين: أنها عامة، أي يستطيع الجميع مشاهدة عملها؛ وأنها بلا إذن، أي يستطيع الجميع الانضمام. وهاتان الخاصيتان مرغوبتان وضروريتان لتشغيل عملة موزعة بلا طرف ثالث. ومع تزايد النظر إلى السلاسل مستقلة عن العملات، صار من المنطقي بحثها في بيئات خاصة مأذونة. فقد تنتفع بها جماعة شبيهة باتحاد، تربط أطرافها أعمال لكنهم لا يثقون بعضهم ببعض تمامًا: أطراف سلسلة إمداد، أو مؤسسات مالية وتأمينية تتبادل التسويات أو تستخدم غرفة مقاصة، ومثلها مؤسسات الرعاية الصحية. وحين يتغير الانضمام من «متاح للجميع» إلى «بالدعوة فقط»، تصبح تعديلات أخرى على عناصر البناء ممكنة، وتظهر نتائج تهم بعض الأطراف.

فيمكن أولًا استبدال إثبات العمل، المصمم للحماية من الفاعلين الخبثاء والمزعجين، بآلية أبسط وأقل استهلاكًا للموارد، مثل بروتوكول إجماع قائم على (Raft). وتظهر مفاضلة بين مستوى أمان مرتفع وسرعة أكبر، تتجسد في خيار خوارزميات الإجماع الأبسط. ويفيد ذلك جماعات كثيرة، إذ تستبدل بعض الضمان القائم على التشفير بضمان توفره وسائل أخرى، كالعلاقات القانونية، وتتجنب سباق التسلح المستهلك للطاقة الذي يفضي إليه إثبات العمل غالبًا. والابتكار مستمر؛ وإثبات الحصة منافس بارز في مجال آليات إجماع الشبكات العامة، وقد يجد طريقه إلى الشبكات المأذونة أيضًا. وتيسر مشروعات عدة إنشاء السلاسل المأذونة، منها (Quorum) المتفرع من إيثريوم، و(Fabric) و(Sawtooth) التابعان لـ(Hyperledger)، وهما مشروعان مفتوحان بشفرة جديدة. تتجنب السلاسل المأذونة تعقيدات لا يمكن للسلاسل العامة غير المأذونة تجنبها، لكنها تواجه مشكلاتها: كيف تدار العضوية؟ من ينضم؟ كيف تعرف الهويات؟ وكيف يستبعد المشارك؟ وهل تدير جهة واحدة بنية مفاتيح عامة مركزية (PKI) داخل الشبكة؟

الطبيعة المفتوحة للسلاسل:

في جميع الحالات، الهدف واضح: رفع ثقة المشاركين بالشبكة وبياناتها، ويفضل إلى درجة استخدامها كما هي بلا عمل إضافي. ولا يبلغ ذلك المستوى إلا إذا كانت برمجية الشبكة حرة ومفتوحة المصدر. فحتى السلسلة الاحتكارية الموزعة توزيعًا صحيحًا ليست إلا وكلاء مستقلين يشغلون شفرة الطرف الثالث نفسه. لذلك ففتح الشفرة شرط لازم، لكنه غير كافٍ. وقد وفر الحد الأدنى من الضمان ومصدرًا لمزيد من الابتكار مع نمو المنظومة. وأخيرًا، أدت الطبيعة المفتوحة، إلى جانب الابتكار والتنوع، دورًا في الحوكمة: حوكمة بالشفرة، يتوقع فيها أن يشغل المستخدمون النسخة التي تتضمن الوظيفة أو النهج الذي يريدون للشبكة كلها تبنيه. ومن هذه الناحية، أصبحت الطبيعة المفتوحة لبعض السلاسل أحيانًا ذريعة للتنصل من الحوكمة، لكن العمل جارٍ على معالجة ذلك.

الجيلان الثالث والرابع: الحوكمة:

سأبحث لاحقًا ما أعده حاليًا الجيلين الثالث والرابع: سلاسل بأدوات حوكمة مدمجة، ومشروعات تعالج مسألة الربط الصعبة بين السلاسل المختلفة الكثيرة، كي تتبادل المعلومات والقيمة.

المراجع:

- https://bitcoin.org
- https://slashdot.org/
- https://github.com/bitcoin/bitcoin
- https://bitcointalk.org/
- https://www.namecoin.org/
- https://litecoin.org/
- https://en.wikipedia.org/wiki/Scrypt
- https://zerocash-project.org/index
- https://z.cash

- https://cryptonote.org/
- https://en.wikipedia.org/wiki/Monero_(cryptocurrency)
- https://en.wikipedia.org/wiki/Vitalik_Buterin
- https://ethereum.org
- https://cryptokitties.co/
- https://en.wikipedia.org/wiki/Raft_(computer_science)
- https://www.investopedia.com/terms/p/proof-stake-pos.asp
- https://www.jpmorgan.com/global/Quorum
- https://hyperledger.org/
- https://www.hyperledger.org/projects/fabric
- https://www.hyperledger.org/projects/sawtooth