Market Talks
مركز التعليم

البلوكتشين · مبتدئ · الدرس 6 من 13

الكتل والتجزئة بشرح مبسّط

الرموز القصيرة التي تشد السلسلة بعضها إلى بعض، وما تحتويه الكتلة فعلاً، ولماذا يشبه التعدين لعبة تخمين عملاقة

قراءة 7 دقائق 6 أسئلة مع مفتاح الإجابات

البلوكتشين · مبتدئ · الدرس 6 من 13

الكتل والتجزئة بشرح مبسّط

في جملة واحدة

التجزئة (الهاش) رمز قصير يُحسب من أي بيانات. وإذا تغيرت البيانات ولو قليلاً، يتغير الرمز كلياً. وتحتفظ كل كتلة بتجزئة الكتلة التي قبلها، لذا فإن تعديل التاريخ القديم يكسر كل الحلقات التي تليه.

رمز قصير يمثّل أي بيانات

قلنا في الدرس 3 إن كل سجل في السلسلة يحمل بصمة رقمية للسجل الذي قبله. ولهذه البصمة اسم محدد: **التجزئة** (hash).

دالة التجزئة عملية حسابية تأخذ أي بيانات، سواء كانت كلمة أو عقداً أو كتلة كاملة من المعاملات، وتحولها إلى رمز قصير ثابت الطول. وتسمى دالة التجزئة في البيتكوين **SHA-256**. ونتيجتها دائماً 64 حرفاً مكونة من الأرقام من 0 إلى 9 والحروف من a إلى f. ولا يهم إن كان المدخل كلمة واحدة أو مكتبة كاملة، فالنتيجة دائماً 64 حرفاً.

يستطيع أي حاسوب حساب التجزئة في جزء من الثانية، وكل من يجزّئ البيانات نفسها يحصل على النتيجة نفسها تماماً. ولهذا تُعد التجزئة طريقة سريعة للتحقق من تطابق نسختين من شيء ما دون مقارنتهما سطراً سطراً.

جرّبها مع اسمنا

هذه تجزئة SHA-256 للنص *Market Talks*:

`16e127cc0d60a230a1f1f80040012fc10164f835b2a99ab8f42b2ea457d9964c`

وهذه تجزئة *Market talks*، بعد تحويل حرف واحد فقط إلى حرف صغير:

`79eaca857fb12aa6db2d1ab5c896ae9a3241eb2c96f99dd0640f2c6517a5a972`

تغيير صغير واحد، ولا شيء في النتيجة يبدو مرتبطاً بالأخرى. ويمكنك التحقق منهما بنفسك بأي أداة SHA-256 مجانية على الإنترنت.

أربع ضمانات تقدمها دالة التجزئة الجيدة

- **مدخل واحد، نتيجة واحدة.** تعطي البيانات نفسها دائماً التجزئة نفسها، على أي حاسوب وفي أي مكان في العالم.
- **تغيير صغير، نتيجة مختلفة كلياً.** تغيير حرف واحد يبعثر النتيجة كلها، كما يُظهر المثال أعلاه. ويسمى هذا **تأثير الانهيار**.

- **في اتجاه واحد فقط.** الانتقال من البيانات إلى التجزئة سهل، أما العودة من التجزئة إلى البيانات الأصلية فمستحيلة عملياً. والطريقة الوحيدة لإيجاد مدخل يطابق تجزئة ما هي التخمين مرة بعد مرة.
- **لا تكرار في الواقع العملي.** نظرياً قد يشترك مدخلان مختلفان في التجزئة نفسها، لكن لم يعثر أحد قط على زوج كهذا مع SHA-256. فعدد النتائج الممكنة يتكون من 78 رقماً، وهو قريب من العدد التقديري للذرات في الكون المرئي.

تجعل هذه القواعد الأربع مجتمعةً التجزئة تعمل كختم على البيانات. فإذا ظلت التجزئة مطابقة، فالبيانات لم تتغير. وإذا لم تتطابق، فقد تغير شيء ما، ولو فاصلة واحدة.

تشبيه: العصير المخفوق

ضع موزة وقليلاً من الحليب وخمس حبات فراولة في الخلاط. سيحصل كل من يتبع الوصفة نفسها على العصير نفسه. أضف حبة فراولة واحدة فيتغير الطعم. لكن لا أحد يستطيع أن يعيد العصير موزة كاملة وخمس حبات فراولة منفصلة. والتجزئة تعمل بالطريقة نفسها: سهلة الصنع، وحساسة لكل مكوّن، ومستحيلة العكس.

ماذا تحتوي الكتلة

تتكون كتلة البيتكوين من جزأين. الجزء الأكبر هو **الجسم**: قائمة من المعاملات، عادة بضعة آلاف منها. والجزء الأصغر هو **الترويسة**، وهي ملخص قصير يتضمن:

- **تجزئة الكتلة السابقة.** وهي الرابط الذي يجعلها سلسلة.
- **ملخصاً لكل معاملاتها.** تُجزّأ المعاملات معاً في رمز واحد، لذا فإن تغيير أي منها يغيّر الملخص. ويوضح المستوى المتوسط بالضبط كيف يُبنى هذا الملخص.
- **طابعاً زمنياً** يبيّن تقريباً متى أُنشئت الكتلة.
- **هدف الصعوبة**، الذي يحدد مدى صعوبة لغز التعدين في ذلك الوقت.
- **رقماً عشوائياً** (nonce)، يغيّره المعدّنون مرة بعد مرة بحثاً عن كتلة صالحة. وسنشرح ذلك أدناه.

تُحسب تجزئة الكتلة نفسها من ترويستها. ولأن الترويسة تحتوي على ملخص المعاملات وتجزئة الكتلة السابقة معاً، فإن هذا الرمز الواحد يعتمد على كل ما في الكتلة وعلى كل ما قبلها.

كيف تُقفل التجزئات السلسلة

الآن تكتمل الصورة. تحتفظ الكتلة 102 بتجزئة الكتلة 101، وتحتفظ الكتلة 103 بتجزئة الكتلة 102، وهكذا وصولاً إلى كتلة التكوين.

لنفترض أن شخصاً عدّل معاملة واحدة في الكتلة 101. سيتغير ملخص معاملاتها، وبالتالي تتغير تجزئتها. لكن الكتلة 102 لا تزال تحتفظ بالتجزئة القديمة، فلا يعود الرابط بينهما متطابقاً، وتلاحظ ذلك كل عقدة فوراً.

ولإخفاء التعديل، سيتعين على المهاجم إعادة حساب الكتلة 101، ثم الكتلة 102، ثم كل كتلة بعدها. وكما يوضح القسم التالي، يتطلب إنتاج كل واحدة من هذه الكتل قدراً هائلاً من التخمين. وفي الأثناء، تواصل الشبكة الأمينة إضافة كتل جديدة فوقها. ولهذا تزداد الدفعة أماناً مع كل كتلة تُضاف بعدها.



الشكل 1. تحتفظ كل كتلة بتجزئة الكتلة التي قبلها. وتعديل الكتلة 101 يغيّر تجزئتها، فلا يعود رابطها بالكتلة 102 متطابقاً، ويرى الجميع أن السلسلة تعرّضت للتلاعب.

التعدين: لعبة تخمين عملاقة

ذكر الدرس 4 أن المعدّنين يتسابقون لحل لغز. وهذا هو اللغز فعلاً: لكي تكون الكتلة صالحة، يجب أن تكون تجزئتها أقل من رقم مستهدف تحدده الشبكة، ما يعني ببساطة أن التجزئة يجب أن تبدأ بعدد معيّن من الأصفار.

ولأن التجزئة تعمل في اتجاه واحد، لا توجد طريقة ذكية لإنتاج تجزئة بأصفار كثيرة. فيغيّر المعدّنون الرقم العشوائي، ويجزّئون الترويسة، ويتحققون من النتيجة، ثم يحاولون مجدداً، مليارات المرات في الثانية. وكل صفر إضافي مطلوب يجعل البحث أصعب بنحو 16 مرة.

أجرينا هذه التجربة بأنفسنا، فجزّأنا *Market Talks* متبوعة برقم متزايد حتى بدأت النتيجة بعدد كافٍ من الأصفار:

الأصفار المطلوبة	عدد التخمينات التي احتجناها	متوسط التخمينات المتوقع
1	15	16
2	262	256
3	5,931	4,096
4	120,539	65,536
5	129,996	1,048,576
6	13,591,130	16,777,216

لاحظ صف الأصفار الخمسة: لقد حالفنا الحظ. فالتعدين أشبه باليانصيب، وأي تخمين قد يفوز. لكن العمل يكبر بسرعة في المتوسط. فقد احتاجت أول كتلة في البيتكوين إلى تجزئة تبدأ بعشرة أصفار، أما كتل اليوم فتحتاج إلى نحو 19 أو 20، ولهذا تُجري الشبكة كلها الآن نحو ألف مليار مليار تخمين في الثانية.

لماذا يهم هذا المتداولين

- **لكل معاملة تجزئة أيضاً.** وتسمى **معرّف المعاملة** أو TXID. وعندما تخبرك منصة تداول أو طرف آخر أن الدفعة أُرسلت، اطلب معرّف المعاملة وابحث عنه في مستكشف الكتل. سترى ما إذا كانت المعاملة موجودة، وكم أُرسل، وكم كتلة جديدة أصبحت فوقها.
- **معدل التجزئة مؤشر على صحة الشبكة.** معدل التجزئة (hashrate) هو العدد الإجمالي للتخمينات التي تجريها الشبكة في الثانية. وقد تجاوز معدل تجزئة البيتكوين لأول مرة زيتاهاش واحداً في الثانية، أي الرقم 1 متبوعاً بـ 21 صفراً، في أبريل 2025. ويعني ارتفاع معدل التجزئة أن المعدّنين يستثمرون في الشبكة. أما الهبوط المفاجئ، كما حدث في يناير 2026 حين أجبرت عاصفة شتوية في الولايات المتحدة المعدّنين على إيقاف جزء كبير من أجهزتهم، فقد يضع المعدّنين تحت الضغط.
- **المعدّنون تحت الضغط قد يتحولون إلى بائعين.** يدفع المعدّنون تكاليف الكهرباء والأجهزة، غالباً ببيع البيتكوين الذي يكسبونه. وعندما يتراجع دخلهم، يبيع بعضهم أكثر أو يوقف أجهزته. ولهذا يتابع بعض المتداولين مؤشرات قائمة على معدل التجزئة إلى جانب رسوم الأسعار البيانية.

المصطلحات الأساسية

التجزئة	رمز قصير ثابت الطول يُحسب من أي بيانات. البيانات نفسها تعطي دائماً التجزئة نفسها.
SHA-256	دالة التجزئة التي يستخدمها البيتكوين. ونتائجها دائماً بطول 64 حرفاً.

تأثير الانهيار	الخاصية التي يؤدي فيها تغيير طفيف في المدخل إلى تجزئة مختلفة تماماً.
ترويسة الكتلة	الملخص القصير في أعلى الكتلة. يضم تجزئة الكتلة السابقة وملخص المعاملات وطابعاً زمنياً والرقم العشوائي.
الرقم العشوائي (nonce)	رقم يغيّره المعدّنون مراراً أثناء بحثهم عن تجزئة كتلة تحقق الهدف.
معدل التجزئة	العدد الإجمالي لتخمينات التجزئة التي تجريها الشبكة في الثانية. وهو مقياس شائع لقوة التعدين.

أهم النقاط

1. التجزئة رمز قصير ثابت الطول يُحسب من أي بيانات. ويعتمد البيتكوين على SHA-256 التي تأتي نتائجها بطول 64 حرفاً.
2. التجزئات الجيدة ثابتة، وتتغير كلياً مع أي تعديل، ولا يمكن عكسها، ولا تتكرر عملياً.
3. للكتلة جسم من المعاملات وترويسة تتضمن تجزئة الكتلة السابقة وملخص معاملاتها.
4. لأن كل كتلة تحتفظ بتجزئة الكتلة التي قبلها، فإن تعديل كتلة قديمة يكسر كل الحلقات بعدها.
5. التعدين يعني تخمين الأرقام العشوائية حتى تبدأ تجزئة الكتلة بعدد كافٍ من الأصفار، وكل صفر إضافي يجعل البحث أصعب بنحو 16 مرة.

اختبر نفسك

ضع دائرة حول إجابة واحدة لكل سؤال. مفتاح الإجابات مع الشرح في الصفحة التالية. يمكنك أيضاً أداء هذا الاختبار عبر الإنترنت على markettalks.info ومعرفة نتيجتك فوراً.

1. ماذا تفعل دالة التجزئة؟

- (A) تشفّر البيانات حتى لا يقرأها إلا صاحبها
- (B) تحوّل أي بيانات إلى رمز قصير ثابت الطول
- (C) تضغط الملفات لتشغل مساحة أقل
- (D) تخزّن المعاملات في قاعدة بيانات

2. غيّرت حرفاً واحداً في مستند ثم حسبت تجزئته مجدداً. ماذا يحدث للتجزئة؟

A يتغير فيها حرف واحد
B تبقى كما هي
C تصبح مختلفة تماماً
D تصبح أطول

3. لماذا لا يستطيع أحد العودة من التجزئة إلى البيانات الأصلية؟

A دوال التجزئة تعمل في اتجاه واحد، فلا يبقى سوى التخمين
B تحتفظ الشبكة بالتجزئة سراً
C تُحذف البيانات الأصلية بعد التجزئة
D المعدّنون وحدهم يملكون مفتاح عكسها

4. ما الذي يربط الكتلة بالكتلة التي قبلها؟

A المعدّن نفسه ينشئ الكتلتين
B للكتلتين الطابع الزمني نفسه
C تحتوي الكتلتان على المعاملات نفسها
D ترويسة كل كتلة تحتفظ بتجزئة الكتلة السابقة

5. ما هو الرقم العشوائي (nonce)؟

A المكافأة التي يحصل عليها المعدّن
B رقم يغيّره المعدّنون مرة بعد مرة بحثاً عن تجزئة كتلة صالحة
C معرّف المعاملة
D عدد المعاملات في الكتلة

6. ماذا يحدث لبحث التعدين كلما طُلب صفر بادئ إضافي؟

A يصبح أصعب بمرتين
B لا يتغير
C يصبح أصعب بنحو 16 مرة
D يصبح أسهل

مفتاح الإجابات

1 B

تحوّل أي بيانات إلى رمز قصير ثابت الطول

تحسب دالة التجزئة رمزاً قصيراً ثابت الطول من أي مدخل. ومع SHA-256 تكون النتيجة دائماً 64 حرفاً، مهما كان حجم المدخل.

2 C

تصبح مختلفة تماماً

هذا هو تأثير الانهيار. فأي تغيير، مهما كان صغيراً، يبعثر النتيجة كلها، ما يجعل اكتشاف أصغر التعديلات أمراً سهلاً.

3 A

دوال التجزئة تعمل في اتجاه واحد، فلا يبقى سوى التخمين

التجزئة سهلة في اتجاه ومستحيلة عملياً في الاتجاه المعاكس. ولهذا بالتحديد يجب أن يتم التعدين بالتجربة والخطأ.

4 D

ترويسة كل كتلة تحتفظ بتجزئة الكتلة السابقة

تتضمن كل ترويسة تجزئة الكتلة السابقة. وإذا عُدّلت كتلة قديمة، تتغير تجزئتها ولا تعود مطابقة لما تحتفظ به الكتلة التالية.

5 B

رقم يغيّره المعدّنون مرة بعد مرة بحثاً عن تجزئة كتلة صالحة

يغيّر المعدّنون الرقم العشوائي، ويجرّبون الترويسة، ويتحققون من النتيجة، مرة بعد مرة، حتى تبدأ التجزئة بعدد كافٍ من الأصفار.

6 C

يصبح أصعب بنحو 16 مرة

يمكن أن يأخذ كل حرف في التجزئة واحدة من 16 قيمة، لذا فإن طلب صفر إضافي يجعل النتيجة الصالحة أندر بنحو 16 مرة.

المصادر

- ساتوشي ناكاموتو، Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- NIST، معيار التجزئة الآمنة FIPS 180-4 (SHA-256): https://csrc.nist.gov/files/pubs/fips/180-4/final/docs/fips180-4.pdf
- Forklog، معدل تجزئة البيتكوين يتجاوز زيتاهاش واحداً لأول مرة (أبريل 2025): https://forklog.com/en/bitcoin-hashrate-surpasses-one-zettahash-for-the-first-time/
- KuCoin، معدل تجزئة البيتكوين في 2026: الاتجاهات وصعوبة التعدين وأمن الشبكة: https://www.kucoin.com/blog/in-bitcoin-hashrate-in-2026-latest-trends-mining-difficulty-network-security-analysis

Market Talks

تابع التعلّم

التالي: الدرس 7
العُقد والشبكة الند للند

هذا الدرس جزء من مسار البلوكتشين المجاني في مركز التعليم لدى MARKET TALKS: دروس للمستوى المبتدئ والمتوسط والمتقدم، ولكل درس اختبار وملف PDF قابل للتنزيل.

مركز التعليم
دروس من المبادئ الأساسية حتى الموضوعات المتقدمة

تحليل الأسواق
تحليل فني وأساسي للأسواق الرئيسية

التقارير
البيتكوين والذهب والفضة وSPX وغيرها

markettalks.info

تيليجرام @MARKET_TALKS

•لأغراض تعليمية فقط. لا يُعد أي محتوى في هذا المستند نصيحة مالية. © 2026 MARKET TALKS. يمكنك مشاركة ملف PDF هذا دون تعديل.