Market Talks

مركز التعليم

البلوكتشين · مبتدئ · الدرس 9 من 13

عبارات الاسترداد والنسخ الاحتياطية

الكلمات الـ 12 أو 24 القادرة على إعادة بناء محفظتك كاملة، وكيف تحفظها، ومن سيحاول الحصول عليها

قراءة 6 دقائق 6 أسئلة مع مفتاح الإجابات

البلوكتشين · مبتدئ · الدرس 9 من 13

عبارات الاسترداد والنسخ الاحتياطية

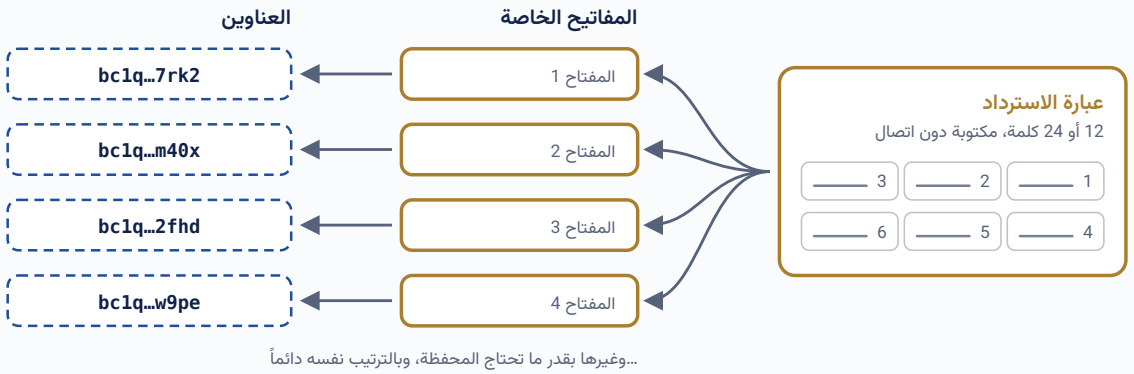
في جملة واحدة

عبارة الاسترداد (seed phrase) قائمة من 12 أو 24 كلمة عادية تستطيع إعادة إنشاء كل مفتاح خاص في محفظتك. احتفظ بها وستتمكن من الاستعادة إذا ضاع جهازك أو تعطل. وإذا تسربت، يستطيع أي شخص أخذ كل شيء دون أي إمكانية للتراجع.

نسخة احتياطية واحدة لكل المفاتيح

رأينا في الدرس 8 أن المحفظة تنشئ عنواناً جديداً لكل دفعة، وأن كل عنوان يأتي من مفتاحه الخاص. ونسخ عشرات المفاتيح المنفصلة احتياطياً سيكون كابوساً. وتحل المحافظ الحديثة هذه المشكلة بتوليد كل مفاتيحها من رقم ابتدائي واحد يسمى **البذرة** (seed).

تُعرض عليك البذرة مرة واحدة فقط، عند إعداد المحفظة لأول مرة، على شكل قائمة من 12 أو 24 كلمة. هذه هي **عبارة الاسترداد** الخاصة بك، وتسمى أيضاً عبارة البذرة. أدخل الكلمات نفسها في أي تطبيق محفظة حديث تقريباً، وسيعيد إنشاء المفاتيح نفسها تماماً بالترتيب نفسه ويجد العملات نفسها. قد يضيع الهاتف أو الجهاز الصلب أو يُسرق أو يتعطل. لكن ما دامت الكلمات معك، فإن بيتكوينك لم تضع.



الشكل 1. عبارة استرداد واحدة تولّد كل المفاتيح الخاصة في المحفظة، وكل مفتاح يعطي عنواناً. استعد العبارة في أي محفظة متوافقة فتعود المفاتيح والعملات نفسها.

تشبيه: نيغاتيف الصورة

في زمن كاميرات الأفلام، كان النيغاتيف أثمن من أي صورة مطبوعة. فإذا ضاعت صورة، أمكن طباعة أخرى من النيغاتيف بقدر ما تشاء وفي أي استوديو. وعبارة الاسترداد هي نيغاتيف محفظتك، أما التطبيق على هاتفك فليس سوى نسخة مطبوعة واحدة. لكن أي شخص آخر يملك النيغاتيف يستطيع أيضاً طباعة نسخه الخاصة.

لماذا الكلمات، ولماذا هذه الكلمات تحديداً

في الخلفية، البذرة مجرد رقم عشوائي كبير جداً. وكتابته على شكل 64 حرفاً من الأرقام والحروف دعوة إلى الأخطاء، لذا يحوّله معيار واسع الانتشار إلى كلمات مأخوذة من قائمة ثابتة تضم 2048 كلمة إنجليزية بسيطة. وتمثل كل كلمة جزءاً من الرقم.

صُممت القائمة بعناية. ففي النسخة الإنجليزية لا تشترك كلمتان في الأحرف الأربعة الأولى، فتبقى الكلمة مقروءة حتى لو انطمس آخرها. كما تعمل الكلمة الأخيرة كفحص مدمج: إذا نسخت كلمة واحدة خطأً، فستنبهك المحفظة عادة إلى أن العبارة غير صالحة بدلاً من أن تفتح محفظة فارغة بصمت.

تختار المحفظة الكلمات عشوائياً، لا أنت. وهذا هو جوهر الأمر. فعبارة من 12 كلمة قد تكون أياً من نحو 340 مليار مليار مليار مليار تركيبة، أي رقماً من 39 خانة. أما عبارة اخترعتها بنفسك، أو كلمات أغنية، فستخمّنها بسرعة برامج مصممة لتجربة ملايين العبارات الشائعة.

تتيح بعض المحافظ أيضاً إضافة كلمة مرور إضافية اختيارية، تسمى غالباً passphrase. ومعها لا تكفي الكلمات الـ 12 أو 24 وحدها لفتح المحفظة. إنها تضيف حماية، لكنك إذا نسيت كلمة المرور هذه، فلن تفيدك الكلمات أيضاً.

الحفظ: دون اتصال، ومتين، ويمكن العثور عليه

يجب أن تنجو النسخة الاحتياطية الجيدة من ثلاثة أخطار: اللصوص، والحوادث كالحريق أو الماء، وذاكرتك أنت بعد سنوات. وهذه مقارنة بين الخيارات الشائعة:

أين	تحمي من	عرضة لـ
مكتوبة على ورق في المنزل	المخترقين، لأنها لا تلمس الإنترنت أبداً	النار والماء وأي شخص يعثر عليها
محفورة على لوح معدني	المخترقين والنار والماء	أي شخص يعثر عليها، ما لم تكن مخبأة جيداً
نسخة ثانية في مكان آخر، مثل صندوق أمانات	فقدان النسخة الوحيدة في كارثة واحدة	نسخ أكثر تعني أماكن أكثر قد تتسرب منها
صورة أو لقطة شاشة أو ملاحظات أو بريد أو سحابة	لا شيء لا يتقنه الورق أكثر	اختراق الحسابات والنسخ المتزامنة والبرمجيات الخبيثة التي تفحص الصور

أياً كان اختيارك، اكتب الكلمات بالترتيب، ورقّمها، وطابق كل واحدة مع الشاشة. ثم أجرِ تمرين استعادة: بينما لا يوجد في المحفظة إلا مبلغ صغير، امسحها أو استخدم جهازاً آخر، وأعد إدخال الكلمات، وتأكد من ظهور العناوين نفسها. اكتشاف الخطأ الآن رخيص، أما اكتشافه في حالة طارئة فليس كذلك.

لن يطلبها منك أي جهة شرعية أبداً

لأن عبارة الاسترداد تفتح كل شيء، فهي الهدف الأول لعمليات الاحتيال في عالم العملات المشفرة. تختلف الحيل، لكن الطلب واحد دائماً: اكتب كلماتك في مكان ما. قد يأتيك على شكل موظف دعم في رسائلك، أو نافذة منبثقة تقول إن محفظتك تحتاج إلى «مزامنة» أو «تحقق»، أو تطبيق محفظة مزيف في متجر التطبيقات، أو موقع يعد بتوزيع مجاني (airdrop).

القاعدة بسيطة ولا استثناء لها. عبارة الاسترداد لا تُكتب إلا في محفظتك أنت، حين تستعيدها بنفسك. لا تحتاجها أي شركة محافظ أو منصة تداول أو مطوّر أو مشرف قناة، أبداً.

مثال واقعي: المحافظ «البديلة» المزيفة

في عام 2020 اختُرقت قاعدة بيانات لدى شركة Ledger المصنّعة للمحافظ الصلبة، وفي ديسمبر نُشرت على الإنترنت أسماء نحو 272 ألف عميل وعناوين منازلهم وأرقام هواتفهم. وبعد أشهر، تلقى بعض العملاء طرداً في تغليف يشبه تغليف Ledger الأصلي، مع رسالة تقول إن جهازهم غير آمن وإن جهازاً «بديلاً» مرفق. وطلبت التعليمات منهم إدخال عبارة الاسترداد. كان الجهاز معدّلاً، وكانت الكلمات تذهب مباشرة إلى اللصوص.

لماذا يهم هذا المتداولين

- **مجموعات التداول ساحات صيد.** ينضم المحتالون إلى مجموعات العملات المشفرة النشطة، وينسخون أسماء المشرفين وصورهم، ويراسلون الناس مباشرة عارضين المساعدة أو «فحص المحفظة». لن تطلب MARKET TALKS أبداً عبارة الاسترداد أو مفاتيحك الخاصة أو كلمات مرورك، ولن يطلبها أي فريق حقيقي.
- **لحسابك على منصة التداول أسراره الشبيهة بالبذرة.** لا تستخدم حسابات المنصات عبارات استرداد، لكن رموز النسخ الاحتياطي للمصادقة الثنائية تؤدي دوراً مشابهاً. فإذا حصل عليها أحد مع كلمة مرورك، أمكنه الاستيلاء على الحساب. احفظها دون اتصال، تماماً كعبارة الاسترداد.
- **خطط لمن سيأتون بعدك.** يقدّر الباحثون أن ملايين البيتكوينات ضاعت بالفعل إلى الأبد، كثير منها لأن الشخص الوحيد الذي يعرف المفاتيح توفي أو نسيها. وإذا كنت تملك مبالغ كبيرة، ففكر في كيف يمكن لشخص موثوق أن يستعيدها يوماً ما، دون أن تمنح أحداً وصولاً اليوم.

المصطلحات الأساسية

البذرة	الرقم العشوائي الكبير الوحيد الذي تولّد منه المحفظة كل مفاتيحها الخاصة.
عبارة الاسترداد	البذرة مكتوبة على شكل 12 أو 24 كلمة. تستطيع إعادة إنشاء كل مفتاح في المحفظة. وتسمى أيضاً عبارة البذرة.
قائمة الكلمات	القائمة الثابتة المكونة من 2048 كلمة التي تُستمد منها عبارات الاسترداد، لكي تستطيع أي محفظة متوافقة قراءتها.
المجموع الاختباري	فحص مدمج تحمله الكلمة الأخيرة، يساعد المحفظة على اكتشاف العبارة المنسوخة خطأً.
Passphrase	كلمة مرور إضافية اختيارية تُضاف إلى عبارة الاسترداد. ومن دونها لا تفتح الكلمات وحدها المحفظة.
تمرين الاستعادة	التدرب على الاستعادة من عبارتك المكتوبة قبل أن تضع مبالغ كبيرة في المحفظة.

أهم النقاط

1. تولّد المحافظ الحديثة كل المفاتيح من بذرة واحدة، تُعرض عليك على شكل عبارة استرداد من 12 أو 24 كلمة.
2. بعبارة الاسترداد يمكنك إعادة بناء محفظتك على جهاز جديد حتى لو ضاع القديم أو تعطل.
3. تأتي الكلمات من قائمة ثابتة من 2048 كلمة، وتختارها المحفظة عشوائياً، وتعمل الأخيرة كفحص للأخطاء.
4. احفظ العبارة دون اتصال وعلى وسيط متين، ولا تضعها أبداً في صور أو ملاحظات أو بريد أو سحابة، وجرّب الاستعادة برصيد صغير.
5. كل من يطلب عبارة الاسترداد منك يحاول سرقتك. فهي لا تُكتب إلا في محفظتك أنت.

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 تستطيع عبارة الاسترداد أن تفعل؟

A إعادة تعيين كلمة مرور منصة التداول
B إعادة إنشاء كل مفتاح خاص في محفظتك
C تسريع معاملاتك
D إلغاء دفعة أرسلتها بالفعل

2. سُرق هاتفك الذي عليه تطبيق المحفظة، وعبارة الاسترداد مكتوبة لديك. ماذا تفعل؟

A تستعيد المحفظة بعبارة الاسترداد على جهاز آخر
B تتصل بخدمة عملاء البيتكوين
C تتقبل أن العملات ضاعت
D تطلب من منصة التداول عكس السرقة

3. لماذا لا يجب أن تخترع عبارة الاسترداد من اقتباسك المفضل؟

A المحافظ لا تقرأ الجمل
B سيجعل المعاملات أبطأ
C العبارات التي يخترعها الناس سهلة التخمين للبرامج
D الاقتباسات محمية بحقوق النشر

4. ما الطريقة الأكثر أماناً لحفظ عبارة الاسترداد؟

A لقطة شاشة في معرض الصور
B ملاحظة في مسودات البريد
C ملف في التخزين السحابي
D مكتوبة أو محفورة دون اتصال، في مكان محمي من النار والسرقة

5. بماذا تساعد الكلمة الأخيرة في عبارة الاسترداد؟

A تحدد كلمة مرور المحفظة
B تعمل كفحص يكشف معظم أخطاء النسخ
C تحدد العملة التي تحفظها المحفظة
D تعرض رصيد المحفظة

6. راسلك شخص في مجموعة تداول وعرض إصلاح محفظتك إذا شاركته عبارة الاسترداد. ما الذي يحدث؟

A هذا إجراء دعم طبيعي

B يحتاجها للتحقق من رصيدك

C إنه احتيال، لأنه لا أحد ممن يقدم مساعدة حقيقية يحتاج إلى عبارة الاسترداد

D يتحقق من هويتك

مفتاح الإجابات

1 B

إعادة إنشاء كل مفتاح خاص في محفظتك

عبارة الاسترداد صيغة مكتوبة للبذرة التي تُولَّد منها كل مفاتيحك. ويمكن لأي محفظة متوافقة استخدامها لإعادة بناء المفاتيح نفسها والعثور على العملات نفسها.

2 A

تستعيد المحفظة بعبارة الاسترداد على جهاز آخر

العملات على البلوكتشين لا في الهاتف. والاستعادة بعبارة الاسترداد تعيد إليك السيطرة، ونقل الأموال فوراً إلى محفظة جديدة يحميها.

3 C

العبارات التي يخترعها الناس سهلة التخمين للبرامج

يأتي الأمان من أن الكلمات تُختار عشوائياً من عدد هائل من التركيبات. أما العبارات التي يختارها البشر فأسهل توقعاً بكثير.

4 D

مكتوبة أو محفورة دون اتصال، في مكان محمي من النار والسرقة

كل ما يُحفظ على حساب أو جهاز متصل بالإنترنت يمكن أن يصل إليه المخترقون أو البرمجيات الخبيثة. والنسخة المتينة غير المتصلة تتجنب هذا الخطر.

5 B

تعمل كفحص يكشف معظم أخطاء النسخ

يُحسب جزء من الكلمة الأخيرة من الكلمات الأخرى، لذا إذا نُسخت كلمة خطأً، فستقول المحفظة عادة إن العبارة غير صالحة.

6 C

إنه احتيال، لأنه لا أحد ممن يقدم مساعدة حقيقية يحتاج إلى عبارة الاسترداد

بعبارة الاسترداد يمكن أخذ كل ما في المحفظة. وفرق الدعم الحقيقية لا تطلبها أبداً، فالطلب نفسه دليل على الاحتيال.

المصادر

- مقترح تحسين البيتكوين 39، الرمز التذكيري لتوليد المفاتيح (GitHub): https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BleepingComputer، مجرمون يرسلون أجهزة Ledger معدّلة لسرقة العملات المشفرة: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency
- Cointelegraph، ما يصل إلى أربعة ملايين بيتكوين ربما ضاعت إلى الأبد (تقدير Chainalysis): https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

تابع التعلّم

التالي: الدرس 10
الحفظ: حساب في منصة تداول أم محفظتك الخاصة

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.