Market Talks

مركز التعليم

البلوكتشين · مبتدئ · الدرس 8 من 13

المفاتيح والعناوين والمحافظ

ما الذي يثبت فعلاً ملكيتك للبيتكوين، وما الذي تشاركه لتتلقى الأموال، وما الذي تحتفظ به المحفظة حقاً

قراءة 6 دقائق 6 أسئلة مع مفتاح الإجابات

البلوكتشين · مبتدئ · الدرس 8 من 13

المفاتيح والعناوين والمحافظ

في جملة واحدة

امتلاك البيتكوين يعني امتلاك مفتاح خاص، وهو رقم سري يتيح لك توقيع الدفعات. ومنه يُشتق مفتاح عام وعنوان يمكنك مشاركتهما. أما المحفظة فلا تحتفظ بالعملات إطلاقاً: إنها تحتفظ بالمفاتيح وتستخدمها للتوقيع.

سر واحد وشيئان يمكنك مشاركتهما

رأينا في الدرس 5 أن البلوكتشين لا تحفظ الأسماء، بل العناوين فقط. فكيف تعرف الشبكة أن عملة ما ملكك؟ الجواب مجموعة من ثلاث قطع مترابطة:

- **المفتاح الخاص.** رقم سري يُختار عشوائياً من نطاق هائل يتكون من 78 رقماً، بالحجم نفسه لتجزئات الدرس 6. ومن يعرفه يستطيع إنفاق العملات المرتبطة به.
- **المفتاح العام.** رقم يُحسب من المفتاح الخاص بنوع خاص من الرياضيات، ويمكن إظهاره لأي شخص.
- **العنوان.** رمز أقصر يُصنع بتجزئة المفتاح العام، ويتضمن فحصاً مدمجاً يكشف أخطاء الكتابة. وهو ما تعطيه للناس ليتمكنوا من الدفع لك.

كل خطوة تعمل في اتجاه واحد فقط. فتحويل المفتاح الخاص إلى مفتاح عام، والمفتاح العام إلى عنوان، يستغرق من الحاسوب جزءاً من الثانية. أما الرجوع إلى الوراء فمستحيل عملياً. ولهذا يمكنك نشر عنوانك في أي مكان دون أن تعرّض عملاتك للخطر.



الشكل 1. المفتاح الخاص يُنشئ المفتاح العام، والمفتاح العام يُنشئ العنوان. كل خطوة تعمل في اتجاه واحد فقط، لذا فإن مشاركة عنوانك لا تكشف مفتاحك الخاص أبداً.

الإنفاق يعني التوقيع

لكي تنفق البيتكوين، تبني محفظتك معاملة وتضيف إليها **توقيعاً رقمياً** مصنوعاً بمفتاحك الخاص. ويمكن لأي عقدة التحقق من هذا التوقيع باستخدام مفتاحك العام والتأكد من أنه صادر عن المفتاح الخاص المطابق، دون أن ترى المفتاح الخاص نفسه أبداً.

كما أن التوقيع مرتبط بالتفاصيل الدقيقة لتلك المعاملة وحدها. فإذا غيّر أحد المبلغ أو الوجهة ولو بحرف واحد، لا يعود التوقيع مطابقاً وترفضه كل العقد. ولهذا لا يستطيع أحد اعتراض دفعتك في طريقها عبر الشبكة وتحويلها إلى وجهة أخرى.

هذا هو التحول الكبير عن النظام المصرفي. فالبنك يقرر ما إذا كان يحق لك الإنفاق بالتحقق من هويتك. أما البيتكوين فلا يتحقق إلا من صحة التوقيع. لا اسم، ولا إعادة تعيين لكلمة المرور، ولا خدمة عملاء، بل رياضيات فقط.

تشبيه: صندوق البريد ذو الفتحة

تخيل العنوان صندوق بريد في واجهته فتحة. يستطيع أي شخص يعرف مكانه أن يُسقط فيه رسالة، ويرى الشارع كله عدد الرسائل التي تصل. لكن صاحب المفتاح وحده يستطيع فتح الصندوق وإخراج الرسائل. فإذا أضعت المفتاح، بقيت الرسائل محبوسة إلى الأبد. وإذا نسخ أحدهم المفتاح، أمكنه إفراغ الصندوق.

كيف تبدو عناوين البيتكوين

غيّر البيتكوين صيغة عناوينه عدة مرات. وكلها لا تزال تعمل، ويمكن التمييز بينها من حروفها الأولى:

يبدأ بـ	النوع	سنة الظهور
1	Legacy، الصيغة الأصلية	2009
3	عنوان نصي برمجي، يُستخدم غالباً للمحافظ المشتركة أو متعددة التواقيع	2012
bc1q	Native SegWit، معاملات أصغر ورسوم أقل	2017
bc1p	Taproot، أحدث صيغة، بخصوصية ومرونة أكبر	2021

وللبلوكتشينات الأخرى أنماطها الخاصة. فعناوين الإيثيريوم مثلاً تبدأ بـ *0x* يليها 40 حرفاً. ولا يمكنك استبدال عنوان بيتكوين بعنوان إيثيريوم، حتى لو عرض التطبيق نفسه الاثنين معاً.

تنشئ المحفظة الجيدة عنواناً جديداً في كل مرة تطلب فيها الاستلام. وكلها تتبع المحفظة نفسها، وتبقى العناوين القديمة صالحة. واستخدام عناوين جديدة يصعّب على الغرباء ربط كل دفعاتك ببعضها.

ما الذي تحتفظ به المحفظة فعلاً

على عكس ما يوحي به اسمها، لا تحتفظ المحفظة بالعملات أبداً. فالعملات موجودة فقط كإدخالات على البلوكتشين. و**المحفظة** أداة تحفظ مفاتيحك، وتقرأ البلوكتشين لتعرض رصيدك، وتنشئ المعاملات وتوقّعها.

تنقسم المحافظ إلى مجموعتين رئيسيتين:

- **المحافظ الساخنة** تحفظ المفاتيح على جهاز متصل بالإنترنت، مثل تطبيق هاتف أو برنامج حاسوب. وهي مريحة للاستخدام اليومي، لكن المفاتيح تكون معرّضة لأي شيء يستطيع مهاجمة ذلك الجهاز.
- **المحافظ الباردة** تحفظ المفاتيح دون اتصال بالإنترنت. و**المحفظة الصلبة** جهاز صغير يحفظ المفاتيح داخله ويوقّع المعاملات دون أن يكشفها لحاسوبك أبداً. استخدامها أبطأ، لكن اختراقها أصعب بكثير.

إذا كانت عملاتك على منصة تداول، فالمنصة هي من تملك المفاتيح لا أنت. ويقارن الدرس 10 بين الخيارين، ويتناول الدرس 9 النسخة الاحتياطية التي تحمي كل مفاتيحك دفعة واحدة.

مثال واقعي: القرص الصلب في مكب النفايات

في عام 2013، رمى جيمس هاولز، وهو مهندس حاسوب من ويلز، عن طريق الخطأ قرصاً صلباً قديماً يحمل المفتاح الخاص لـ 8000 بيتكوين كان قد عدّنها قبل سنوات. وانتهى القرص في مكب نفايات المدينة. وقضى أكثر من عقد يطلب الإذن بالحفر بحثاً عنه. وفي يناير 2025 رفضت محكمة بريطانية دعواه، ثم رُفض استئنافه في مارس من العام نفسه. ولا تزال العملات على البلوكتشين، يراها الجميع ولا يستطيع أحد إنفاقها.

لماذا يهم هذا المتداولين

- **تحقق من العنوان كاملاً في كل مرة.** في احتيال تسميم العناوين، يرسل المهاجمون معاملة ضئيلة من عنوان يشبه تقريباً عنواناً تستخدمه، على أمل أن تنسخه من سجلّك في المرة القادمة. وفي مايو 2024، أرسل أحد المتداولين 1155 بيتكوين مغلّفاً (WBTC)، بقيمة نحو 68 مليون دولار، إلى عنوان كهذا. وأعاد المهاجم معظمها لاحقاً بعد مفاوضات، وهي نتيجة نادرة جداً.
- **طابِق الشبكة لا العنوان فقط.** كثيراً ما تدعم المنصات العملة نفسها على عدة شبكات. والإرسال على شبكة لا يدعمها الطرف المستلم قد يجعل استرداد الأموال صعباً جداً أو مستحيلاً. تحقق من الشبكة ومن أي مذكرة أو وسم مطلوب قبل التأكيد.
- **أرسل مبلغاً تجريبياً صغيراً أولاً.** في التحويلات الكبيرة أو الأولى، تكلّف دفعة تجريبية صغيرة قليلاً من الرسوم لكنها قد تنقذ المبلغ كله. ويستخدم كثير من المتداولين أيضاً قوائم بيضاء لعناوين السحب في حساباتهم على المنصات.

المصطلحات الأساسية

المفتاح الخاص	رقم عشوائي سري يتيح لحامله توقيع المعاملات وإنفاق العملات المرتبطة به.
المفتاح العام	رقم يُحسب من المفتاح الخاص، يمكن مشاركته ويُستخدم للتحقق من التواقيع.
العنوان	رمز أقصر مصنوع من المفتاح العام، تشاركه ليتمكن الآخرون من إرسال العملات إليك.
التوقيع الرقمي	دليل مصنوع بالمفتاح الخاص يوافق على معاملة محددة بعينها، ويمكن لأي شخص التحقق منه بالمفتاح العام.
المحفظة	أداة تحفظ مفاتيحك، وتعرض رصيدك من البلوكتشين، وتنشئ المعاملات وتوقّعها.
المحفظة الصلبة	جهاز صغير يحفظ المفاتيح الخاصة دون اتصال بالإنترنت ويوقّع المعاملات دون كشف المفاتيح للحاسوب.

أهم النقاط

1. امتلاك البيتكوين يعني التحكم في مفتاح خاص. ومن يملك المفتاح يستطيع إنفاق العملات.
2. يُحسب المفتاح العام والعنوان من المفتاح الخاص، ولا يمكن إرجاع أي منهما إليه.
3. يتطلب الإنفاق توقيعاً رقمياً مرتبطاً بالمعاملة الدقيقة، يمكن لأي عقدة التحقق منه دون رؤية المفتاح الخاص.
4. تبدأ عناوين البيتكوين بـ 1 أو 3 أو bc1q أو bc1p بحسب نوعها، ويمكن للمحفظة إنشاء عنوان جديد لكل دفعة.
5. المحافظ تحفظ المفاتيح لا العملات. المحافظ الساخنة مريحة، أما الباردة فتحفظ المفاتيح دون اتصال وهي أكثر أماناً بكثير.

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. ما الذي يمنح شخصاً القدرة على إنفاق البيتكوين؟

A معرفة العنوان
B امتلاك المفتاح الخاص
C امتلاك حساب على منصة تداول
D معرفة معرّف المعاملة

2. لماذا تُعد مشاركة عنوانك علناً آمنة؟

A لأن العناوين تنتهي صلاحيتها بعد استخدام واحد
B لأن الشبكة تخفي العنوان عن الآخرين
C لأن أحداً لا يستطيع الرجوع من العنوان إلى المفتاح الخاص
D لأن العناوين مشفّرة

3. ماذا يحدث إذا غيّر أحد المبلغ في معاملة موقّعة؟

A لا يعود التوقيع مطابقاً، فترفضها العقد
B تمر المعاملة بالمبلغ الجديد
C يتحدث التوقيع تلقائياً
D يقرر المعدّن أي مبلغ يُستخدم

4. ما الذي تحتفظ به محفظة العملات المشفرة فعلاً؟

A عملاتك
B نسخة من البلوكتشين كاملة
C بياناتك المصرفية
D مفاتيحك

5. عنوان بيتكوين يبدأ بـ bc1q. ما نوعه؟

A Legacy
B Native SegWit
C إيثيريوم
D Taproot

6. ما الميزة الرئيسية للمحفظة الصلبة؟

A تجعل المعاملات أسرع

B تلغي كل الرسوم

C تحفظ المفاتيح الخاصة دون اتصال وتوقّع دون كشفها

D تتيح استرداد العملات المرسلة إلى عنوان خاطئ

مفتاح الإجابات

1 **B**

امتلاك المفتاح الخاص

المفتاح الخاص هو الذي يوقّع الدفعات. ومن يملكه يستطيع إنفاق العملات، ولهذا يجب أن يبقى سرياً.

2 **C**

لأن أحداً لا يستطيع الرجوع من العنوان إلى المفتاح الخاص

كل خطوة من المفتاح الخاص إلى المفتاح العام إلى العنوان تعمل في اتجاه واحد. يستطيع الآخرون الإرسال إلى عنوانك، لكنهم لا يستطيعون استخدامه لإيجاد مفتاحك الخاص.

3 **A**

لا يعود التوقيع مطابقاً، فترفضها العقد

التوقيع مرتبط بالتفاصيل الدقيقة لمعاملة واحدة. وأي تغيير، ولو حرفاً واحداً، يجعله غير صالح.

4 **D**

مفاتيحك

العملات موجودة فقط على البلوكتشين. أما المحفظة فتحفظ مفاتيحك، وتقرأ رصيدك من السلسلة، وتوقّع معاملاتك.

5 **B**

Native SegWit

العناوين التي تبدأ بـ bc1q من نوع Native SegWit، وقد ظهرت عام 2017. أما عناوين Taproot فتبدأ بـ bc1p، وعناوين Legacy بالرقم 1.

6 **C**

تحفظ المفاتيح الخاصة دون اتصال وتوقّع دون كشفها

تحفظ المحفظة الصلبة المفاتيح داخل الجهاز ولا تُخرج إلا المعاملات الموقّعة، فلا تستطيع البرمجيات الخبيثة على حاسوبك قراءة المفاتيح.

المصادر

- ساتوشي ناكاموتو، Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- ويكيبيديا، البيتكوين المدفون في مكب نيوبورت: https://en.wikipedia.org/wiki/Bitcoin_buried_in_Newport_landfill
- Cointelegraph، متداول يخسر 68 مليون دولار في احتيال تسميم العناوين (مايو 2024): https://cointelegraph.com/news/trader-loses-68-million-address-poisoning-scam
- Cointelegraph، المهاجم يعيد الأموال بعد مفاوضات: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations

Market Talks

تابع التعلّم

التالي: الدرس 9
العبارات السرية والنسخ الاحتياطية

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.