CUVEX

CUVEX ACADEMY · 0.1

تعلّم وافهم وتولَّ زمام التحكم.

تعلّم البيتكوين والحفظ الذاتي خطوة بخطوة. الدورة والدليل والمسرد والتدريبات مجانية من دون تسجيل. اختر نقطة البداية.

مجانًا · بلا تسجيل

كل الأقسام

1. إعداد مساحة التعلّم
2. النقود الرقمية ومشكلة الثقة
3. تاريخ البيتكوين وحدوده
4. الساتوشي والحساب دون أخطاء
5. بناء نموذج التهديدات الخاص بك
6. العُقد والتعدين والإجماع
7. مخرجات UTXO وباقي المعاملة
8. مخزون المعاملات المعلّقة والتأكيدات وإعادة تنظيم السلسلة
9. الرسوم والحجم الافتراضي واستبدال المعاملات
10. الشبكات والعناوين وطلبات الدفع
11. التجزئة والتوقيعات والتشفير
12. البذرة وعبارة المرور وكلمة المرور
13. اشتقاق المفاتيح وxpub والواصفات
14. اختيار المحفظة ونموذج الحفظ
15. النسخ الاحتياطية القابلة للاستعادة
16. التعرّف إلى Original وBIT
17. إنشاء بذرة باستخدام إنتروبيا من مصدر مادي
18. تشفير سرّ وفك تشفيره باستخدام Cuvex
19. عتبات التشفير والقياسات الحيوية
20. استنساخ النسخ وحفظها والتحقق منها
21. تثبيت Cuvex Desk وحمايته
22. ربط النصوص المشفّرة وتنظيم حسابات WOW
23. ربط Mirror بـ Desk
24. استخدام NFC عبر Mirror والنقل عبر USB-C وقراءة رموز QR
25. المزوّدون العموميون والعقدة الخاصة بك
26. استقبال البيتكوين والتحقق من العنوان
27. وسم مخرجات UTXO وتجميدها واختيارها
28. إعداد الدفعة ومراجعتها
29. التوقيع بجهازي Original وBIT
30. استكمال المعاملة ونشرها ومعالجة المشكلات
31. ما الذي يمكن ملاحظته على شبكة بيتكوين؟
32. فصل السياقات وإدارة الباقي
33. خصوصية الشبكة وTor وVPN
34. CoinJoin وPayjoin وحدودهما الحالية
35. دروس من حوادث حقيقية

36. إنشاء هوية الدردشة والتحقق من جهات الاتصال
37. طلب مبالغ بالساتوشي ودفعها من الدردشة
38. مشاركة النصوص المشفّرة عن دراية
39. استعادة الدردشة وفهم بياناتها الوصفية
40. الإعدادات اليومية ومراجعة الأذونات
41. تصميم محفظة متعددة التوقيعات
42. إنشاء الدعوات وتقديم المفاتيح
43. التحقق من السياسات عبر Mirror بأي ترتيب
44. تنسيق التوقيعات ونشر معاملة متعددة التوقيعات
45. استعادة محفظة متعددة التوقيعات وتغييرها
46. تحديث البرنامج الثابت وفق خطوات مدروسة
47. الفقد والتعطّل والاستعادة في حالات الطوارئ
48. التصيد الاحتيالي والدعم والاحتيال بالصوت
49. الخصوصية والقانون والسجلات الشخصية
50. الميراث والاستمرارية والتمرين السنوي
51. السعر والادخار والتحليل الأساسي
52. اختيار جهة شراء البيتكوين
53. الحسابات والأوامر وتكاليف التنفيذ
54. الشموع السعرية والمؤشرات وتحيزات التحليل الفني
55. الهامش والعقود الآجلة والأتمتة
56. Lightning والطبقات الأخرى
57. Taproot وMuSig2 ومستقبل ما بعد الحوسبة الكمّية
58. التشغيل البيني والاستغناء عن المصنّع
59. مختبر تقني باستخدام regtest
60. المشروع النهائي وخطة الاستمرارية
61. دليل المتعلّم
62. مسرد البيتكوين والحفظ الذاتي
63. اختبر ما تعلّمته

إعداد مساحة التعلّم

الهدف

جهّز الدورة، وميّز بين الأجهزة الثلاثة، وحدّد المعلومات التي لا تُعطى للمدرّس أبدًا.

الفهم

ستتعلم كيف تستقبل البيتكوين وتحفظه وتنفقه وتستعيده بحكمك المستقل. الغاية أن تشرح قرارك قبل أن تأذن بتنفيذه. يمكنك قراءة الدورة بمفردك. يقدّم الصوت شرحًا وأسئلة ومرافقة، ولا يحتاج إلى الاطلاع على ممتلكاتك أو التحكم في أجهزتك.

يحمي جهاز Cuvex الأسرار ويتيح الإذن بالعمليات على شاشته. ينظّم Desk البيانات المشفّرة ومحافظ المراقبة والمدفوعات والتنسيق على الحاسوب. أما Mirror فجسر محلي للعمليات المدعومة وأداة لمقارنة البيانات، وليس الموقّع أو محفظة مستقلة. يحدّد الطراز والإصدار أي مسار يمكنك استخدامه.

خصّص شاشة للدورة وأخرى لـ Desk وأبقِ الهاتف وCuvex في متناولك. إذا كانت لديك شاشة واحدة فبدّل بينها من دون مشاركة الشاشة في مكالمة فيديو عند إدخال الأسرار. قد تنتهي مكالمة قبل انتهاء التدريب. التوقف المؤقت ليس فشلًا. احفظ فقط معرّف الدرس والخطوة التي بلغتها والصعوبة التي واجهتها.

لا يجوز أن يتلقى المدرّس البشري أو الذكاء الاصطناعي بذورًا أو عبارات مرور BIP39 أو كلمات سر أو مفتاح الدردشة أو أرقام PIN أو ملفات خاصة أو رموز شراء كاملة. ولا يحتاج أيّ منهما إلى xpub أو الواصف الحقيقي أو العنوان، فهي تكشف النشاط وإن لم تُتح الإنفاق. صف رسائل الخطأ واستخدم بيانات المختبر الوهمية.

التدريب

1. تعرّف على الحاسوب والهاتف وطراز Cuvex أمامك وسجّل إصداراتها في دفترك الخاص.
2. افصل بيئة التعلّم الخالية من الأموال عن بيئة الحفظ الفعلية. لا تستورد بذرة المحفظة الفعلية للتدريب.
3. افتح الدرس واعثر على الإيقاف المؤقت والمساعدة والمسرد. أوقف التفاعل إذا طلب أحد منك سرًا.

أثبت فهمك

اشرح من يوقّع ومن يستعلم من الشبكة ومن ينقل البيانات. يمكنك التقدم متى ميّزت بين هذه الوظائف دون مساعدة.

سؤال شائع

هل عليّ التحدث مع المدرّس كل يوم؟ لا. يمكنك الدراسة منفردًا، وتكرار الجلسة، وطلب المساعدة في إجراء محدّد فقط. حق الوصول إلى الدورة ورصيد الخدمة الصوتية أمران مستقلان.

نقطة توقف

اكتمل L01، وعُرفت الأجهزة، ولم يُسجَّل أي سر في الدورة.

يطلب المدرّس عبارة البذرة ليتأكد من أنك كتبتها صحيحًا. ماذا تفعل؟

1. أمليها ببطء.
2. أرفض الطلب وأفحص البذرة في بيئتي الآمنة وحدها.
3. أرسل الكلمات الأولى فقط.

> **عرض الإجابة: أرفض الطلب وأفحص البذرة في بيئتي الآمنة وحدها.**
> حتى جزء من أي سر يقع خارج نطاق الخدمة التعليمية.

النقود الرقمية ومشكلة الثقة

الهدف

افهم المشكلة التي يسعى البيتكوين إلى حلها قبل أن تفتح محفظة.

الفهم

الرصيد المصرفي قيد تديره مؤسسة. تتحقق المؤسسة من هوية العميل وتختار التحويلات التي تنفذها وتمسك حساباتها. أما الملف الرقمي العادي فيسهل نسخه، فإرسال صورة لا يمنعك من الاحتفاظ بنسخة. ولكي تعمل الوحدة الرقمية كنقود يلزم منع إنفاقها مرتين.

يجمع البيتكوين قواعد التحقق والتوقيعات وسجلًا مشتركًا للمعاملات. ويمكن لمشاركين مستقلين التحقق من التزام معاملة بالقواعد عوضًا عن إيداع السجل الكامل لدى جهة واحدة. تعتمد الندرة على استمرار التحقق من القواعد وقبولها، ولا تنشأ من صورة نقدية ولا من سعر تنشره منصة تداول.

يغيّر الحفظ الذاتي توزيع المسؤوليات. يمكنك الاحتفاظ بقدرة الإنفاق دون استئذان أمين حفظ، ويمكنك أيضًا فقدانها بإتلاف كل النسخ الاحتياطية أو توقيع دفعة خاطئة. حرية التصرف لا تلغي الحاجة إلى الحماية والتنسيق والاتصال للنشر ولا إلى الوفاء بالالتزامات السارية.

ميّز بين Bitcoin، الشبكة والبروتوكول، وBTC، وحدته النقدية. قد تستخدم شبكات أخرى تعبير سلسلة الكتل وتملك خصائص مختلفة. ووعد شركة بشيء تسمّيه «بيتكوين» لا يعادل امتلاك مخرج بيتكوين تتحكم فيه مفاتيحك.

التدريب

1. قارن بين رصيد مصرفي ورصيد في منصة تداول ومخرج UTXO تتحكم فيه بمفاتيحك.
2. اكتب في كل حالة من يستطيع منعك من تحريك الرصيد ومن يستطيع مساعدتك إذا نسيت وسيلة الدخول.
3. صف ما يحدث عند نسخ صورة وعند محاولة إنفاق المخرج نفسه مرتين.

أثبت فهمك

اشرح بكلماتك الفرق بين الرصيد وقدرة التوقيع. لا حاجة إلى حفظ المصطلحات الفنية.

سؤال شائع

هل يزيل الحفظ الذاتي جميع الوسطاء؟ يمكنك اختيار خدمات للشراء والاستعلام والتواصل. المهم أي سلطة تحتفظ بها كل خدمة وأي بيانات تتلقاها.

نقطة توقف

احتفظ بمقارنة المسؤوليات دون أسماء حسابات حقيقية.

أي مشكلة نقدية لا يحلها التوقيع الرقمي وحده؟

1. منع محاولة إنفاق المخرج نفسه مرتين.
2. إثبات الإذن بمفتاح.
3. كشف تغيير الرسالة الموقّعة.

> **عرض الإجابة: منع محاولة إنفاق المخرج نفسه مرتين.**
> التوقيعات تثبت الإذن، والقواعد والإجماع يرتبان عمليات الإنفاق المتعارضة.

تاريخ البيتكوين وحدوده

الهدف

تعرّف إلى نشأة البيتكوين وافصل الحقائق التاريخية عن الروايات التجارية.

الفهم

نُشرت ورقة ساتوشي ناكاموتو عام 2008 وبدأت الشبكة عام 2009. واقترحت نقدًا إلكترونيًا بين الأقران مستفيدة من أفكار سابقة في التشفير وإثبات العمل والنقود الرقمية. لا تتطلب مراجعة البرنامج أو المعاملة معرفة هوية ساتوشي المدنية.

لم يتطور البيتكوين بأن استبدلت شركة القواعد من جانب واحد. يقترح المطوّرون التغييرات ويراجعونها، ويختار المشغّلون البرامج، ويبني المعدّنون الكتل، ويختار المستخدمون والخدمات ما يقبلونه. قد يؤدي توزيع الأدوار إلى اختلافات. وانقسام السلسلة غير تحديث التطبيق.

يمكن للعقدة رفض كتلة تخالف قواعدها ولو بُذل فيها عمل كبير. لا يقوم الإجماع على تصويت بعدد الحواسيب، وتشغيل آلاف النسخ من عقدة لا يزيد سلطة صاحبها تلقائيًا. وبالمثل لا تحصل أغلبية المعدّنين بذلك على مفتاح مستخدم خاص.

للبيتكوين حدود ومقايضات مقصودة منها سعة الكتل وكلفة التحقق وتفاوت زمن التأكيد وعلنية السجل. لا يتيح إلغاء المدفوعات إداريًا ولا سرية شاملة افتراضيًا. وتعالج الطبقات والتطبيقات استخدامات محددة مقابل تبعيات جديدة.

التدريب

1. ضع الورقة الأولى وبدء الشبكة وتبنّي SegWit وتفعيل Taproot على خط زمني. تحقّق من التواريخ من المصادر قبل نشرها.
2. صنّف «شركة تضمن السعر» و«عقدة تتحقق» و«معدّن يقترح كتلة» إلى وعد تجاري أو وظيفة تقنية.
3. اشرح فائدة وكلفة لغياب مدير يستطيع عكس الدفعات.

أثبت فهمك

ميّز بين قاعدة إجماع وسياسة محلية وقرار شركة. التطبيق الذي تستخدمه ليس الشبكة كلها.

سؤال شائع

هل يغيّر أحدث برنامج القواعد النقدية دائمًا؟ لا. تعالج الإصدارات أيضًا أخطاء أو تحسّن الأداء أو تغيّر السياسات المحلية. اقرأ ملاحظات الإصدار والتوافق.

نقطة توقف

اكتب خاصية قابلة للتحقق وادعاءً يحتاج إلى دليل إضافي.

تحتوي كتلة على إنفاق دون إذن صحيح. هل تجعله أغلبية المعدّنين صالحًا؟

1. نعم، إذا تجاوزت 51%.
2. فقط إذا أعلنت منصة التداول ذلك.
3. لا، بالنسبة إلى عقدة تطبّق القواعد التي ترفضه.

> **عرض الإجابة: لا، بالنسبة إلى عقدة تطبّق القواعد التي ترفضه.**
> يُقارن العمل التراكمي بين تواريخ صالحة وفق قواعد العقدة.

الساتوشي والحساب دون أخطاء

الهدف

حوّل بين BTC والساتوشي وتحقق من المبالغ دون الاعتماد على سعر صرف.

الفهم

يعادل BTC واحد 100,000,000 ساتوشي. وsat وحدة وليست عملة أخرى. تُحسب مبالغ الطبقة الأساسية بأعداد صحيحة من الساتوشي. يعادل 0.001 BTC مقدار 100,000 sat ويعادل 0.00001000 BTC مقدار 1,000 sat. تختلف الفاصلة العشرية باختلاف لغة الواجهة، فلا تضف أصفارًا بالتخمين.

يحوّل سعر الصرف BTC مؤقتًا إلى عملة مثل EUR أو USD، ولا يغيّر عدد الساتوشي التي تملكها. إن كان لديك 100,000 sat بقي العدد نفسه عند تغيّر السعر. يعرض Desk سعرًا استرشاديًا بمصدر وتاريخ. قد تؤدي البيانات القديمة إلى قرار اقتصادي خاطئ ولو صحّ رصيد BTC.

ميّز مبلغ المستفيد ورسوم الشبكة وإجمالي الإنفاق. إذا أرسلت 50,000 sat برسوم 600 sat خرج من محفظتك 50,600 sat في غياب مخارج أخرى لك. يحسب خيار «إرسال الكل» عادة صافي مبلغ للمستفيد أقل من الرصيد المتاح لتغطية الرسوم.

أمثلة الدورة تمارين حسابية وليست أسعار سوق أو رسومًا موصى بها. افحص الوحدة والشبكة والمستفيد والكلفة الكلية على الشاشة المعنية قبل التوقيع. قد يقول الصوت «خمسون ألف ساتوشي» ويعرض «50,000 sat» في الوقت نفسه، ولا يجوز تحديد مبلغ من تفريغ صوتي مشكوك فيه.

التدريب

1. حوّل 250,000 sat إلى BTC: الناتج 0.0025 BTC. وحوّل 0.00025000 BTC: الناتج 25,000 sat.
2. احسب إرسال 75,000 sat برسوم 900 sat: الإجمالي 75,900 sat.
3. استخدم في المحاكي 120,000 sat وأرسل 70,000 برسوم 1,000. تحقق أن الباقي 49,000 sat.

أثبت فهمك

اقرأ المبلغ بوحدتي BTC وsat واشرح أي مبلغ يشمل الرسوم. أوقف العملية عند الشك.

سؤال شائع

هل يجب شراء بيتكوين كامل؟ لا. يمكنك شراء جزء مع مراعاة الحد الأدنى والتكاليف لدى المزوّد.

نقطة توقف

احتفظ بالنتائج الحسابية للتمرين فقط.

لديك 80,000 sat وتريد إرسال الكل برسوم 1,200 sat. كم يصل إلى المستفيد؟

1. 80,000 sat.
2. 78,800 sat.
3. 81,200 sat.

> **عرض الإجابة: 78,800 sat.**
> في هذا المثال دون مخارج أخرى يتلقى المستفيد الرصيد القابل للإنفاق بعد خصم الرسوم.

بناء نموذج التهديدات الخاص بك

الهدف

اختر تدابير متناسبة مع الفقد والسرقة والخداع وانكشاف البيانات.

الفهم

الأمن هو الحفاظ على قدرتك على التصرف وفق قصدك. والخصوصية أن تتحكم فيمن يعرف بياناتك وصلاتك. والتوافر أن تصل إليها حين تحتاجها. صندوق يستحيل فتحه على الجميع قد يستحيل عليك أيضًا، ونسخة يسهل الوصول إليها جدًا قد تكشف أكثر مما ينبغي.

حدّد الأصول والخصوم والحوادث المحتملة. تشمل الأصول المفاتيح والنسخ الاحتياطية والسجل ومواقع النسخ وهويات جهات الاتصال. وتشمل المخاطر البرمجيات الخبيثة والتصيّد والحريق والنسيان والإكراه والأعطال والوفاة وأخطاءك أنت. لا تعالجها كلها أداة واحدة.

استخدم جدولًا بسيطًا للاحتمال التقريبي والأثر والتدبير المحدد. تصعّب كلمة المرور الطويلة التخمين لكنها لا تصحح عنوان محتال أذنت له بالدفع. لا تعالج نسختان في حقيبة واحدة فقدان الحقيبة. وقد يبقى للتوقيع المتعدد موضع فشل مشترك إذا سيطر شخص واحد على أجهزته ونسخه.

الدورة والمدرّس جزء من النموذج أيضًا. الشراء والمكالمات وأوقات الاتصال والتقدّم قد تولّد بيانات وصفية. لا ينبغي لموقع الدورة طلب عناوين أو أرصدة لتخصيص درس. عدم اشتراط التسجيل التقليدي في Desk أو Mirror لا يعني أن المتجر أو مزوّد الصوت أو خدمة الاستعلام الخارجية لا يعرفون شيئًا عن نشاطك.

التدريب

1. اكتب أهم ثلاثة مخاطر لديك دون مبالغ ممتلكات أو مواقع دقيقة.
2. اختر لكل خطر وسيلة منع وكشف واستعادة. مثال فقد البطاقة: نسختان منفصلتان، وجرد، واختبار استعادة.
3. ميّز مَن يمكنه من الأشخاص أو الأنظمة مراقبة الشراء والمكالمة واستعلام الرصيد والمعاملة العلنية.

أثبت فهمك

اشرح أي خطر محدد يعالجه تدبيرك التالي. لا تراكم تعقيدًا لا تستطيع صيانته أو شرحه لورثتك.

سؤال شائع

هل تعني زيادة الأجهزة أمنًا أكبر دائمًا؟ فقط إذا قللت التبعيات المشتركة وأمكن اختبار الاستعادة. تضيف الأجهزة أيضًا صيانة واحتمال التباس.

نقطة توقف

احفظ الخطة في وثائقك الخاصة ولا تسجل في الدورة إلا «رُوجع نموذج التهديدات».

أي تدبير يقلل أكثر من خطر فقدان جميع النسخ في حريق بمكان واحد؟

1. تغيير لون البطاقة.
2. وضع نسختين في الدرج نفسه.
3. الاحتفاظ بنسخ مختبرة في أماكن مستقلة المخاطر.

> **عرض الإجابة: الاحتفاظ بنسخ مختبرة في أماكن مستقلة المخاطر.**
> ينبغي أن يصمد التكرار الاحتياطي أمام الحادث نفسه الذي يهدد الأصل.

العُقد والتعدين والإجماع

الهدف

شرح ما هو الـ عقدة و ما هو مُدخل الـ التعدين.

الفهم

ال عقدة كاملة تحصل على الكتل والمعاملات، والتحقق من القواعد، والحفاظ على رؤية السلسلة. لا حاجة للثقة بالرصيد الذي يُعلنه لك صفحة التعدين هي عملية اقتراح الكتل باستخدام إثبات العمل. الـ المعدّنون تختار الصفقات الصحيحة و تتنافس على العثور على كتلة مقبول

يجعل إثبات العمل إعادة كتابة التاريخ مكلفة. عند وجود سلاسل بديلة صالحة، العبرة بالعمل التراكمي لا بعدّ الكتل دون اعتبار الصعوبة. يتغيّر الزمن بين الكتل؛ عشر دقائق متوسط مستهدف لا موعد مضمون للدفعة التالية.

مكافأه التعدين تجمع بين الدعم و الرسوم وتتبع المنحة جدولاً زمنياً للتخفيض بالارتفاع من كتلة؛ ويتوقف الـ الرسم على المعاملات المشمولة. أي تحويل يدفع أكثر لا يجعل توقيع غير صحيح. الأمن الاقتصادي وتكلفة الهجوم لا يحولان دفعة حديثة إلى لا رجعة فيها من الناحية الحسابية

ويقلل عقدة خاصة بك من الحاجة إلى تقديم المشورة إلى موردين خارجيين ويتيح التحقق. ما زال يجب عليك أن تحميه من أجله. نظام التشغيل والوصول والاتصال. أن يكون لديك عقدة تشغيل بدون مزامنة، أو متصلاً بـ App الذي يبحث عن خادم آخر، لا يعطي تلقائياً هذه المزايا.

التدريب

1. خذ هذه المهام: التحقق من التوقيع، اختيار معاملات كتلة، حراسة بذرة الاسترداد الخاص بك وتقرير ما إذا كنت تقبل دفع.
2. يفسر لماذا "الـ المعدّنون يحتفظ بـ بيتكوين بلدي هو وصف غير صحيح.
3. في شبكة مختبرية، لاحظ الارتفاع والتوقيت؛ لا تنشر وثائق تفويض RPC.

أثبت فهمك

يصف الفرق بين التحقق والاقتراح. يمكنك استخدام القياس، ولكن ينتهي مع الاقتران التقني الصحيح.

سؤال شائع

هل أحتاج إلى المين لاستخدام بيتكوين ? لا. أنت أيضاً لا تحتاج إلى عقدة خاصة بك كبداية، على الرغم من معرفة مستوى ثقة مورّدك، هذا ضروري.

نقطة توقف

يشير إلى مزوّد المعمل حسب نوعه، بدون URL خاص.

ماذا تتيح العقدة الكاملة المضبوطة جيدًا لمستخدمها؟

1. التحقق من قواعد السلسلة التي يقبلها.
2. استعادة أي مفتاح مفقود.
3. ضمان ارتفاع السعر.

> **عرض الإجابة: التحقق من قواعد السلسلة التي يقبلها.**
> التحقق والحفظ وظيفتان مختلفتان.

مخرجات UTXO وباقي المعاملة

الهدف

قراءة صفقة مثل الاستهلاك و خلق المخرجات.

الفهم

UTXO هو مخرج من صفقة سابقة لا تزال غير مُنفقة محفظة تحسب رصيدها بتحديد الـ المخرجات التي تستطيع التحكم بها لا يوجد حساب عالمي يتراجع كما في ورقة مصرفية: مدخل مرجعي خروج سابق باستخدام تعريف المعاملة و الموقف.

من خلال إنفاق أموال من أجل إنفاق أموال على UTXO يستهلكها بالكامل. إذا أردت أن تدفع أقل من قيمته، فعادة ما تخلق مخرجاً المستلم و تغيير آخر تحت سيطرتك 120.000sat، المستلم 70.000، الرسم 1.000، التغير هو 49.000 مجموع المدخلات يساوي مجموع المخرجات زائد الرسم.

العنوان ليس UTXO يمكنك الحصول على عدة المخرجات . كما أنه ليس بالضرورة إنسانا. قد يكون تعريف المعاملة علنياً، ولكن ربطه بهويتك أو شرح هوية كل مخرج يضيف معلومات لا تعبر عنها السلسلة وحدها.

هذا الهيكل مهم للخصوصية: تجميع المدخلات قد يشير إلى سيطرة مشتركة؛ التغيير قد يربط المدفوعات المستقبلية. وهذا الاستنتاج ليس اختبارا عالميا لأن هناك معاملات تعاونية. الكواين التحكمي هو اختيار اي المخرجات يصرف، معرفة عواقب الجمع بينهما.

التدريب

1. ارسم ثلاثة مدخلات افتراضية بقيم 40,000 و60,000 و200,000 sat. ادفع 70,000 برسوم 1,000 باستخدام أول مدخلين فقط.
2. تحقق من أن الباقي 29,000 sat وأن المدخل الثالث لم يُستخدم.
3. إعادة استخدام 200.000 فقط: التغيير سيكون 129.000. مقارنة التكاليف المحتملة والروابط، دون أن نحسب حجم متساوي.

أثبت فهمك

حدّد خانة، المستلم، تغيير و الرسم في تخطيط المسار. إن لم تستطع تحديد مخرج فلا يجب أن توقع على عملية حقيقية

سؤال شائع

هل كل ما يعود لـ محفظة هو تغيير؟ لا. يمكن أن يكون نقلاً إلى عنوان آخر يتطلب التصنيف معرفة السياسة والرقم الاشتقاق، وليس التخمين على القيمة.

نقطة توقف

حافظ على مخططك الخيالي لا تلتقط أبداً ممتلكاتك

ينتج مدخل 100,000 sat مخرجًا قدره 30,000 وآخر قدره 69,200. ما الرسوم؟

1. 69,200 sat.
2. 800 sat.
3. 30,000 sat.

> **عرض الإجابة: 800 sat.**
> 100,000 ناقص 99,200 يساوي 800 sat.

مخزون المعاملات المعلّقة والتأكيدات وإعادة تنظيم السلسلة

الهدف

تميّز بين صفقة معدّة و منشورة و مؤكّدة.

الفهم

والفئة مخزون المعاملات المعلّقة هي المجموعة المحلية من المعاملات غير المؤكدة التي يحتفظ بها عقدة وفقاً لسياسته. ليس هناك مخزون المعاملات المعلّقة واحدة متطابقة في جميع أنحاء الكوكب. إن إظهار مستكشف دفعة يعني أن هذه الخدمة تعرفه؛ فهو لا يضمن قبول جميع الـ عقدة له أو تأكيده في وقت محدد.

إعداد PSBT لا ينشر شيئًا. ينتج التوقيع إذنًا، ويكوّن الإنهاء المعاملة القابلة للبث، والنشر محاولة لإرسالها. يعني التأكيد إدراج المعاملة في كتلة من السلسلة التي يقبلها مصدر التحقق. يضيف التأكيد الثاني كتلة فوق الأولى، وليس توقيعًا ثانيًا من المستفيد.

ويمكن أن تحدث عمليات إعادة التنظيم حيث يمكن تغيير جزء من السلسلة وتفقد العملية التأكيدات أو تعود إلى الوراء. وللمدفوعات الأكثر عرضة للتعرض، كثيرا ما تطلب الأطراف المزيد من التأكيدات . لا يوجد رقم يزيل أي خطر على كل عدد أو حالة.

إذا كان Desk يعرض حالة محفوظة، ابحث عن تاريخ الضبط. "تأكيد" وفقاً لفاتة قديمة لا تصف بالضرورة الحالة الحالية. إذا لم تظهر شحنة، احتفظ ببطاقة التعريف المحلية وراجع النشر والتاريخ قبل إعادة تجهيزها: تكرار التبخر يمكن أن يخلق دفع آخر صالح.

التدريب

1. قم بترتيب هذه البطاقات: مسودات، PSBT، التوقيع، المعاملة النهائية، النشر، الإدراج في كتلة.
2. يُحدّد فك الارتباط بعد النشر. يقرر ما الذي سيتحقق منه قبل أن يدفع مرة أخرى.
3. يفسر التجارة لماذا رسالة الدردشة "تدفع" لا تحل محل التحقق من الشبكة.

أثبت فهمك

يمكنك التعبير عن حالة العملية ومصدر وتاريخ هذه المعلومات دون الخلط بينه وبين الضمان

سؤال شائع

هل إغلاق Desk يلغي صفقة منشورة؟ لا. ويمكن الاحتفاظ بها لدى المشاركين الآخرين من الفئة عقدة. ولإلغاء مشروع محلي نطاق آخر.

نقطة توقف

حدد حالة المحاكاة؛ لا تضيف معرفات فعلية إلى المدرّس.

انقطع اتصال الحاسوب فور الضغط على النشر. ما الخطوة الأولى؟

1. إعداد الدفعة نفسها من الصفر.
2. حذف المحفظة.
3. إعادة الاتصال وفحص المعاملة ومدخلاتها.

> **عرض الإجابة: إعادة الاتصال وفحص المعاملة ومدخلاتها.**
> تعذّر تلقّي الرد لا يثبت فشل البث.

الرسوم والحجم الافتراضي واستبدال المعاملات

الهدف

تقدير التكاليف، وتفسير sat × vbyte، وفهم RBF وCPFP.

الفهم

رسوم الشبكة هو الفرق بين المدخلات والمخرجات. ويمكن التعبير عن قدرتها التنافسية عادة في sat/vB: ساتوشي عن طريق Byte الافتراضي. وهو لا يعتمد مباشرة على القيمة الاقتصادية المرسلة. والكثير من المدخلات يمكن أن يكلف مبلغاً صغيراً؛ أما المبلغ الكبير الذي يدفعه عدد قليل من المدخلات فيمكن أن يكون أقل.

في مثال مثال 200 vB (أ)(أ) (أ) 5 sat/vB،،، و الرسم من س س س من من من من س من من مثلا من من من سي من من من a من من من الذي من من من مثلا مثلا من من س س من س من مثلا من س من س س مثلا من من ل من من من x من من من يساوي من من من y من من من d من من من ل س من من من س سي من من من مثلا س من من a مثلا من من مثلا ل من من س مثلا من مثلا مثلا مثلا من مثلا من مثلا س س من مثلا مثلا x من من من مثلا 1,000 sat . قبل التوقيع فقط يمكنك الحصول على تقدير، لأن الحجم النهائي قد يعتمد على التوقيعات و التركيب. الـ Desk يقدم سرعات إرشادية وجرّارة يدوية؛ وبطاقة "perb" لا تعد بتأكيد في الوقت المناسب.

وسياسة RBF هي سياسة لاستبدالمعاملات غير المؤكدة بشروط معينة. وتسمح الآلية باقتراح إنفاق متضارب أعلى من الرسم؛ وقد تطورت سياسات عقدة، ولا ينبغي النظر إلى علامة عدم استبدال كضمان تحصيل. الاستبدالذي يتطلب إعادة تنقيح جديدة و/أو التوقيعات الاحتياجات من الـتـتـتـتـ

CPFP عبارة عن إنفاق مخرج من العملية المعلقة لجعل الأب وابنه جذابين. يتطلب السيطرة على مخرج قابل للصرف، والتزام بالسياسات ودفع ثمنها. هذا مفهوم بيتكوين: لا يفترض أن يكون هناك زر CPFP في النسخة Cuvex.

"Dust" هو مخرج صغير جداً وفقاً للسياسات المطبقة والتكاليف المقدرة للإنفاق؛ وهو ليس عتبة عالمية لجميع أنواع الكتابة. تجنب تعليم رقم ثابت كقانون الإجماع وإذا لم يكن التغيير ممكناً، راجع المبلغ، المدخلات أو مسح، والالرسم.

التدريب

1. 180vB إلى 8 sat 1.440 :sat/vB. تحققي إن كان يتجاوز ميزانية مختبركِ
2. قارن بين مدخل واحد وعشرة مدخلات واشرح لماذا لا يكفي المبلغ المُرسَل لتقدير الكلفة.
3. وهو يرسم حلا وسطا معلقا ويقرر ما بين الانتظار، RBF أو دراسة CPFP، دون افتراض التوافق التلقائي.

أثبت فهمك

بيّن سبب اختيار معدل الرسوم وقيمتها المطلقة ونسبتها إلى المبلغ المرسل. ارفض رسمًا لا تفهمه.

سؤال شائع

ز RBF هل تُلغي الدفعة السابقة بالتأكيد؟ لا. النسخ المتنافسة حتى يتم تأكيدها والانتشار مهم لا تتخلى عن ممتلكات بناء على وعد بالإلغاء

نقطة توقف

يحفظ قرار الدورة وسببها.

كم تبلغ رسوم 250 vB بسعر 4 sat/vB؟

1. 1,000 sat.
2. 254 sat.
3. 4% من المبلغ المرسل.

> **عرض الإجابة: 1,000 sat**.
> الحجم الافتراضي مضروبًا في معدل الرسوم يعطي الرسوم التقديرية.

الشبكات والعناوين وطلبات الدفع

الهدف

التعرف على الشبكة وشكل العنوان وتعليمات الدفع قبل النسخ أو المسح.

الفهم

Mainnet يحرك بيتكوين مع قيمة اقتصادية. فشبكات الاختبار تساعد على التطور والتعلم، ولكنها ليست قابلة للتبادل. Regtest هي شبكة محلية يسيطر عليها مشغل المختبر؛ ولل signet وtestnet قواعد ونظم إيكولوجية خاصة بهما. دالة الترميز في signet لا تعني أن ملف التوقيع المتعدد من Cuvex سيقبل بهذه الشبكة.

ترميز العناوين ظروف الاستلام. في mainnet تجد أشكالاً تبدأ بـ 1 أو 3 أو bc1q أو bclp. ويساعد الرمز على التعرف على أسرة، ولكنه لا يتحقق من المستلم، ولا يضمن توافق الرمز الموقّع ولا يحل محل التحقق الكامل من الشكل.

الـ QR عبارة عن حاوية بصرية يمكنك نقل عنوان أو فاتورة أو واصف أو نص خبيث. فحصه لا يوثق هوية صاحبه وصلة بيتكوين: يمكنك إضافة قيمة و رسالة. BIP321 هي المرجع الحديث الذي يحل محل BIP21؛ وDesk يحتفظ بالمصطلحات والتوافق BIP21 في تنفيذه المنقح. تحسين المعايير لا يوسع وحده ما يفهمه التطبيق.

الـ فاتورة Lightning ليست عنواناً أون تشاين قد يشمل صلاحيته وحقول أخرى، لا يجب أن تلصقه في شحنة سلسلة إذا كان التطبيق لا يوفر تدفقاً متوافقاً. وعلامة توكين تسمى BTC في شبكة أخرى أيضاً لا تكون تلقائياً بيتكوين

التدريب

1. يصنف عينات من المسار دون استخدام اتجاهات قابلة للاستهلاك: العنوان URI بيتكوين: اقتباس Lightning و واصف.
2. تعرّف على الشبكة المنتقاة في المختبر. في Cuvexالتوقيع المتعدد المنقحة، تطابق الخصية هو mainnet/regtest.
3. يقارن النص الكامل الذي يطلبه المتلقي عبر قناة موثقة قبل المعاملة الفعلية.

أثبت فهمك

يمكنك رفض طلب لا تعرف شبكته أو نمطه وشرح ما تحتاج إلى التحقق منه.

سؤال شائع

هل يمكن أن أرسل BTC لأي شبكة تظهر منصة تداول؟ لا. شبكة السحب يجب أن تتطابق مع الإستقبالفعلي تجنب الإختيار فقط بـ الرسم الأدنى

نقطة توقف

فقط سجل نوع شبكة التعلم.

لا يكفي عنوان استقبال bc1 لسحب BTC عبر شبكة رموز مختلفة. ما المطلوب؟

1. تغيير اسم المستفيد المستعار.
2. التحقق من أن السحب يتم على سلسلة بيتكوين وأن جميع البيانات متطابقة.
3. إدخال البذرة في منصة التداول.

> **عرض الإجابة: التحقق من أن السحب يتم على سلسلة بيتكوين وأن جميع البيانات متطابقة.**
> يجب توافق الأصل والشبكة وطريقة الاستلام.

التجزئة والتوقيعات والتشفير

الهدف

:: التمييز بين السلامة والإذن والسرية.

الفهم

قيمة التجزئة تحول البيانات إلى بصمة طول ثابتة. فمقارنة بصمة معروفة تساعد على كشف التغييرات ؛ فهي لا ترمز الى الملف ولا تحدد هوية الشخص الذي نشره . إذا قمت بتحميل الملف و قيمة التجزئة من نفس الصفحة المُخَطَطة، قد يكون المهاجم قد استبدل كلاهما.

يسمح مفتاح خاص بإنشاء التوقيعات؛ ويتيح مفتاح عام المقابلة اختبارها. التوقيع يربط الرخصة برسالة محددة وفقاً للخوارزمية وقواعدها. لا يخفي المحتوى الموقع. في بيتكوين، التوقيع الصحيح هو جزء من الشروط اللازمة لإنفاق مخرج.

الـ التشفير يُريدُ a محتوى يُمْكِنُ أَنْ يُقْرَأَ فقط بطاقتِه المناسبةِ. هي: تشفير مُوثّق بالإضافة إلى الكشف عن الأعطال. في النظام الإيكولوجي Cuvex هناك النص المشفّر الذي يحمي الأسرار، المعاملات الموقعة التي تسمح بالإنفاق، والقنوات المشفرة التي تحمل الرسائل. إنها ليست أشياء معادلة حتى لو استخدم الجميع الترميز

كلمة المرور إنسان عادة ما يمر من خلال دالة الاشتقاق قبل أن يستخدم كمفتاح الترميز. AES-256 تصف الخوارزمية وحجم مفتاح لكنها لا تحول كلمة المرور المتوقعة إلى اختيار قوي. فالخلق، والتنفيذ، والتخزين، والشاشات، والاستعادة هي جزء من الأمن الكامل.

ولا يمكن أيضاً أن نستنتج أن QR آمنة لأنها تبدو معقدة. يجب أن نعرف ما يحتويه، ومن أنتجه، وما الذي سيفعله التطبيق به. وقبل أن تقبل الدعوى، تطلب من المدرّس أن توضح الغرض منها دون أن تطلب المعلومات الخاصة.

التدريب

1. الشريك "اكتشاف تغيير الملف"، و "اختبأ بذرة الاسترداد" و "اسمح بالسداد" بـ قيمة التجزئة و التشفير و التوقيع.
2. غيّر حرفاً من نص خيالي و لاحظ أن قيمة التجزئة الخاص بك تغيّر ؛ لا تستخدم أسرار لهذا البيان العملي.
3. يوضح لماذا يمكن لصفقة أن تكون علنية و موقعة في نفس الوقت

أثبت فهمك

يمكنك أن تصف الضمان الذي تبحث عنه و ما هي الآلية التي توفره بدون استخدام "مشفّر" كمرادف لكل شيء آمن.

سؤال شائع

ال قيمة التجزئة من البرنامج الثابت تشهد بأنه لا يوجد عيب؟ لا. هو يُحدّدُ بَيْتات إذا المرجع موثوق. مراجعة حسابات، شركة تصنيع وإختبار مادي يجيبون على أسئلة مختلفة

نقطة توقف

احتفظي بالمراسلات الثلاثة في السنة.

أي آلية تخفي محتوى السر؟

1. نشر اسم ملفه.
2. توقيعه دون تشفيره.
3. تشفيره بطريقة صحيحة بمفتاح محمي.

> **عرض الإجابة: تشفيره بطريقة صحيحة بمفتاح محمي.**
> التوقيع أو البصمة وحدهما لا يوفّران السرية.

البذرة وعبارة المرور وكلمة المرور

الهدف

تجنب التشويش بين مختلف وثائق تفويض النظام.

الفهم

تمثّل عبارة التذكّر BIP39 الإنتروبيا والمجموع الاختباري بكلمات من قاموس. أطوالها القياسية 12 أو 15 أو 18 أو 21 أو 24 كلمة. لا يعادل اختيار عبارة سهلة أو كلمات أغنية أو كلمات ينتقيها شخص عشوائيًا التوليد الآمن. يكشف المجموع بعض الأخطاء ولا يثبت مَن أنشأ البذرة أو أن أحدًا آخر لا يعرفها.

تدخل عبارة مرور BIP39 في اشتقاق البذرة الثنائية. عبارة مختلفة قد تفتح محفظة أخرى تمامًا وتبدو فارغة، وقد لا تظهر رسالة «عبارة المرور خاطئة». لا يلزم أن تكون كلمة من القاموس ولا تعني حرفيًا كلمة خامسة وعشرين.

رقم كلمة المرور في النص المشفّر Cuvex حماية سرية المخزون. رقم كلمة مرور Desk يحمي المستودع المحلي للحاسوب. ويأذن مركز الاتصال PIN بعقد جلسة اتصال. رقم مفتاح (تشات) يستعيد هوية مُرسلة لا أحد منهم يجب أن يختلط مع بذرة الاسترداد، و معرفة واحد لا يعني إعادة بناء كل شخص آخر.

حفظ بذرة الاسترداد و عبارة المرور معا داخل النص المشفّر يمكن أن ييسر الاستعادة، لكنه يزيل فصله أمام من يستطيع فك تشفيره. فصلهم يزيد من مطالبك وورثتك يجب توثيق القرار وإثباته؛ لا يُتخذ لأن المدرّس يعتبر خيار "أكثر تقدماً".

التدريب

1. أنشئ خمس بطاقات ورقية بلا أسرار فعلية واكتب عليها: البذرة وعبارة المرور وكلمة مرور Cuvex وكلمة مرور Desk ومفتاح الدردشة.
2. اكتبي ما الذي يستعيده كل واحدة وما الذي ستخسرينه عندما تنسينه
3. صمّم اختبارًا بمحفظة فارغة. أدخل الكلمات وعبارة المرور على انفراد وأبلغ المدرّس بالنتيجة وحدها.

أثبت فهمك

يفسر لماذا لا يجب على الدورة أن تطلب "كلمة المرور" لـ "تصديق" تعلمك. حدد أي سر يتطلبه إجراءك للتعافي

سؤال شائع

هل يمكنني إعادة ضبط عبارة المرور بالبريد الإلكتروني؟ لا يتيح BIP39 هذه الآلية. قد يتيح أمين حفظ استعادة الحساب، لكن ذلك نموذج مختلف.

نقطة توقف

سجل "الأرقام التفاضلية" دون كتابة قيمها.

غيّرت حرفًا من عبارة مرور BIP39 فظهر رصيد صفر. ما التفسير الصحيح؟

1. ربما هي محفظة صالحة أخرى مشتقة من العبارة المختلفة.
2. حذفت الشبكة أموالك.
3. يجب على Desk تخمين العبارة الأصلية.

> **عرض الإجابة: ربما هي محفظة صالحة أخرى مشتقة من العبارة المختلفة.**
> قد تُنتج عبارة مرور مختلفة محفظة أخرى دون إظهار خطأ.

اشتقاق المفاتيح وxpub والواصفات

الهدف

فهم كيفية وصف محفظة دون تسليم قدرة على الإنفاق.

الفهم

محفظة تسلسلي يمتطي الكثير من مفاتيح من الجذر. المسار يشير إلى أي فرع يستخدم. في BIP84 , mainnet عادةً ما تُستخدَم في الم/ 84 '/ 0 '/ 0 الحساب الأول للحساب الأول من الحساب الأول SegWit (أ) التوقيع المضاف؛ BIP48 P2WSH عن طريق استخدام م/م/م/س//م/ث/م/ 48 '/ 0 '/ 0 '/ 2 في الحساب الأول للحساب الأول التوقيع المتعدد . يشير الرمز إلى الاشتقاق المحصّن. غيّر الحساب أو الشبكة أو نوع من الدَرْس يمكن أن تعطي عناوين أخرى من عبارة التذكّر نفسها.

xpub هي مفتاح عام واسعة الانتشار تسمح بحرف مفتاح عام محدد من سلالتها. ليس كلمة المرور نفقات، ولكن يمكنك السماح لمشاهدة عائلة من العناوين. والرمز بصمة المفتاح الرئيسي هو أداة تعريف قصيرة مفيدة لربط السجلات؛ فهو لا يضمن الهوية في حد ذاته ولا يتجنب الاصطدام.

واصف يعبر عن كيفية بناء البرمجيات والعناوين: نوع من الاختصارات، الـ مفاتيح، المنشأ والإشتقاق. ال واصفللمراقبة فقط مع مفتاح عام يسمح للملاحظة، لا التوقيع. كلمة "واصف" لا تضمن أنها تحتوي فقط على معلومات عامة: بعض الأشكال يمكن أن تشمل مفتاح خاص. لا تصعدي أبداً بـ واصف حقيقية في المسار.

واستعادة التوقيع المتعدد عادة ما يتطلب سياسة كاملة، وليس مجرد كلمات من أحد ال الموقّع. العتبات، المشاركين، xpops، الدروب، الشبكة، نوع scrips، بيانات الاكتشاف. فمجموع التحقق من الرقم واصف يساعد على كشف الأخطاء في النصوص؛ ولا يوثق المشاركين فيه.

التدريب

1. إقرأ طريقاً وهمياً وشرح الغرض، العملة، الحساب، والفرع لا تدخلي مفاتيح حقيقية.
2. تفرّق بين المشاركين عنوان الاستقبال، والمشاركين xpub، والمشاركين واصف كاملاً.
3. أعدّي ملفّاً خاصّاً للإستعادة مع أسماء الحقول الفارغة وموقع وثائقيّ منفصل.

أثبت فهمك

يمكنك تفسير لماذا محفظة فارغ بعد استعادة لا دليل على الخسارة: يجب التحقق من الشبكة، عبارة المرور، مطبوع، حساب، مسار و اكتشاف.

سؤال شائع

هل يمكن نشر xpub بدون عواقب؟ فهو لا يمنح وحده القدرة العادية على الإنفاق، ولكنه يعرض الخصوصية ويمكن أن يزيد من المخاطر الأخرى في تركيبات الترميز الخاصة.

نقطة توقف

حفظ سجل بدون قيم حساسة في المسار.

ما الذي قد ينقصك لاستعادة محفظة متعددة التوقيعات ببذرة واحدة فقط؟

1. لون الجهاز.
2. السياسة والمفاتيح العامة لبقية المشاركين.
3. كلمة مرور شبكة اجتماعية.

> **عرض الإجابة: السياسة والمفاتيح العامة لبقية المشاركين.**
> تتطلب إعادة بناء السكربتات السياسة كاملةً بالإضافة إلى استيفاء عتبة المفاتيح الخاصة.

اختيار المحفظة ونموذج الحفظ

الهدف

قارن الأدوات بالوظيفة، الثقة والتعافي.

الفهم

المحفظة مجموعة أدوات لوصف الإنفاق ومراقبته والإذن به عند الاقتضاء. تحتفظ المحفظة الساخنة بقدرة التوقيع في بيئة متصلة. ويفصل جهاز التوقيع المعزول الأسرار عن الحاسوب الذي يستعلم من الشبكة. تحتفظ محفظة المراقبة بمعلومات عامة تكفي للرصد والإعداد، لكنها تحتاج إلى نظام آخر للتوقيع.

وفي حالة الأطراف الثالثة الحفظ، يمكن أن يمثل حساب ما حقاً تجاه شركة. في الحفظ الذاتي أنت تحافظ على القدرة التقنية على الإنفاق بشكل فردي أو مشترك الاستعادة بواسطة البريد الإلكتروني وقوة منع السحب عادة ما تعكس النموذج الأول. لا يجب أن تقيّم كلا الخيارين بنفس افتراض المسؤولية

دعم الشبكة/النصب المقارن، التحقق على الشاشة، النسخ، التحديث، التشغيل البيني، الصيانة، التشاور مع الموردين، وضوح الأخطاء. قائمة عملات أو عملية مادية لا تكفي. كما أن أداة التوقيع لا تمنعك من قبول عنوان خاطئ إذا لم تنقحه.

يفصل Cuvex الأسرار المحمية داخل نصوص مشفّرة عن التنظيم والاستعلام في Desk. يتطلب ذلك حفظ النص المشفّر ووسائل فتحه. الحماية من فقد الجهاز لا تعني إمكان الاستعادة إذا ضاعت أيضًا كل النسخ أو كلمات المرور. تعلّم المسار كاملًا قبل نقل أصولك.

التدريب

1. قارن Cuvex مع محفظة ساخنة ومنصة تداول في مصفوفة: من يوقع، ومن يرى الاستشارات، ومن يستطيع استعادة الوصول، وما يحدث عند إغلاق الشركة.
2. اختر معيارين يجب أن تتحقق من الأدلة وليس الإعلانات
3. تأكد من أن بيئة الممارسة لا تتشارك مفاتيح مع مدخراتك الحقيقية

أثبت فهمك

يبرر اختياراً لقضية معينة دون إعلان أداة لا يمكن اختراقها.

سؤال شائع

هل العتادمحفظة تجعل كل المعاملات سرية؟ لا. وهي تحمي أساسا القدرة على التوقيع وجزءا من الاستعراض؛ ولا تزالسلسلة والمشاورات والنظراء تولد المعلومات.

نقطة توقف

احتفظ بمصفوفة معاييرك بدون أسماء الحسابات

ما الذي تتيحه محفظة مراقبة مضبوطة بمفاتيح عامة صحيحة؟

1. مراقبة العمليات وإعدادها دون أن توقّع بمفردها.
2. تغيير بذرة مفقودة.
3. ضمان إخفاء الهوية.

> **عرض الإجابة: مراقبة العمليات وإعدادها دون أن توقّع بمفردها.**
> المراقبة والإذن قدرتان منفصلتان.

النسخ الاحتياطية القابلة للاستعادة

الهدف

تصميم نسخة كاملة وإثبات استعادة قبل الاعتماد عليها.

الفهم

الـ نسخة احتياطية مفيد يستعيد قدرة، وليس مجرد ملف. بالنسبة لرموز واحدة قد يتطلب عبارة التذكّر، عبارة المرور وبيانات الاشتقاق. بالنسبة لـ التوقيع المتعدد، يتطلب أيضاً سياسة وكفاية الموقّع. Desk قد تحتاج إلى نسخة مشفرة ونسخة مرمزة من كلمة المرور. بالنسبة للشات، استعادة الهوية لا يعني استعادة الرسائل التاريخية.

فالتكرار يحمي من الخسارة العرضية؛ والانفصال يحمي من التزام المشترك. نسختان من مختلف الرابطات و المواقع يمكن أن تقلل من الإحكام المترابطة. وتحتاج كل نسخة إضافية أيضاً إلى مراقبة الدخول، والجرد والاستعراض. لا ينبغي أن تكشف أسماء المحفوظات والعلامات عن خصائصها أو تيسر تحديد مواقع جميع المكونات.

ويجب أن يؤكد الاختبار وجود عنوان تم التحقق منه مسبقا، وفي بيئة التعلم، القدرة على توقيع عملية خاضعة للرقابة. أن وجود ملف يفتح لا يثبت أنه ينتمي إلى محفظة الصحيح. ولا يمكنك أيضاً التحقق من نسخة من خلال إدخال بذرة الاسترداد إنتاج في أي حاسوب.

اوثق ما يغطي وما يستبعد كل نسخة. غيّر كلمة المرور الحالي لا يُعدّل تلقائياً النسخ القديمة. وإذا ما تم الكشف عن كلمة المرور سابقاً، فإن هذه نسخة احتياطية تظل متأثرة. احذف ملفّ في تخزين عصري أيضا لا يضمن حذف كل نسخ أو نسخ.

التدريب

1. كامل جدول خاص: الغرض، المحتوى، الـ كلمة المرور المرتبطة، الموقع المستقل، تاريخ الاختبار والمسؤولية.
2. يعيد نسخة من التعلم في بيئة منفصلة. تحقق من الشبكة، العنوان الأول و الاشتقاق
3. يُحدّد فقدان الحاسوب ثمّ فقدان الجهاز. حدد الإجراء الذي سيتغير.

أثبت فهمك

يمكنك استعادة مسرح الأدلة الخاص بك دون مساعدة مؤقتة وشرح أي معلومات قد تكون مفقودة لمسرح آخر

سؤال شائع

النسخة العالمية لـ Desk هي نسخة من كل شيء؟ وينبغي عدم افتراض ذلك. في الأساس المنقّح، تاريخ و جلسات دردشة غير متضمّنة. ولسياستي التوقيع المتعدد ومفتاح خاص أدوار مختلفة.

نقطة توقف

سجل تاريخ و نتيجة الأدلة، لم يكن أبداً محتوى النسخة.

غيّرت كلمة مرور Desk. ماذا يحدث لنسخة احتياطية سابقة؟

1. تتحدث وحدها.
2. تفقد تشفيرها تلقائيًا.
3. تحتفظ بالحماية وكلمة المرور اللتين أُنشئت بهما.

> **عرض الإجابة: تحتفظ بالحماية وكلمة المرور اللتين أُنشئت بهما.**
> النسخ السابقة عناصر مستقلة.

التعرّف إلى Original وBIT

الهدف

اختر المسار الصحيح وفقاً للجهاز و النسخة.

الفهم

ويستخدم Original بطاقات NFC لنقل النص المشفّر وللعمليات المتوافقة؛ ويشارك Bluetooth في تحديثها. USB-C يستخدم كغذاء في النموذج الموثق. وتستخدم BIT USB-C مع تبادل الملفات وتضيف القياسات الحيوية بالنسبة للالنص المشفّر التي تتطلبها. لا تنقل تعليمات NFC أو Bluetooth من Original إلى BIT.

في الجهاز ستجد وظائف لـ تشفير، فك التشفير، إنشاء محفظة والتوقيع بالإضافة إلى التعديلات. Original مدمج مستنسخ من البطاقات؛ BIT يعمل مع ملفات من أداة USB. ويمكن أن تختلف التسميات واللغات والمنافذ باختلاف النسخ. الولوج الجديد "تدقيق السياسات" في BIT يؤدي إلى التدفق المتوافق ولا يغير من الذي يأذن.

المرجع التحريري المنقح هو: Original 1.2.2 النهاية BIT 1.2.3 النهاية Desk (ب) اعتماد. 9.21 و. Mirror (ب) اعتماد. 12.12 . وهي إشارات مرجعية إلى المصادر: ينبغي التحقق من توقيع كل توليفة وتوزيعها وقبولها المادي مع المعدات. لا تستعيض عن الـ البرنامج الثابت بـ ثنائي غير مُسجل ضمن حزمة هندسية

قبل أن تستخدم فريق تفقد المصدر، الختم، المظهر، والنسخة. وتساعد إمكانية التعقب وتوقيع تحديثي في مواجهة تهديدات محددة، ولكنهما لا يحلان محل جميع عمليات التحقق. إذا نظرت إلى مناولة أو نسخة غير متوقعة، توقف الافتتاح واستشار تدعم من قناة تحققت منها.

التدريب

1. حدد نموذجك و سجل النسخة المرئية بدون تصوير الأسرار
2. التعقب تشفير، فك التشفير، إنشاء محفظة، PSBT وتعديلات. لا تبدأ مسحاً أو تحديثاً لإستكشاف القوائم
3. اختر الـ Original أو BIT في المسار. حافظ على هذا الاختيار أثناء التدريب

أثبت فهمك

يوضح كيف تدخل وتخرج عملية نموذجك وأي دعم يجب أن تحميه من الأزهار

سؤال شائع

ﻫ BIT هل هو أكثر أماناً لأي شخص؟ وتوفر النماذج خيارات تشغيلية مختلفة. فالرد يعتمد على التهديدات والتعافي والاستخدام السليم.

نقطة توقف

احتفظ بالنموذج والنسخة في دفترك المحلي الدورة تحتاج فقط إلى النموذج المختار

لديك BIT ويطلب الدليل أن تكتب بطاقة NFC بالجهاز نفسه. ماذا تفعل؟

1. أتحقق من ملاءمة الدليل لطرازي وأستخدم مسار USB المتوافق.
2. أفرض تثبيت تحديث Original.
3. أرسل البذرة إلى الهاتف.

> **عرض الإجابة: أتحقق من ملاءمة الدليل لطرازي وأستخدم مسار USB المتوافق.**
> يجب أن تلائم التعليمات وسيلة النقل الفعلية للطراز.

إنشاء بذرة باستخدام إنتروبيا من مصدر مادي

الهدف

فهم التوليد واختبار التدفق دون تحويل بيانات الدورة إلى مفاتيح الخاصة بك.

الفهم

الإنتروبيا لا يمكن التنبؤ بها. يمكن لـ a نرد أن يعمل الإنتروبيا إذا كانت مناسبة، الترتيب يُحدّد قبل الإطلاق وخوارزمية التحويل صحيحة. وينبغي تكرار النتائج التي ترفض إجراء ما كما تشير إلى ذلك بالضبط؛ فاستبدالها بأقصى عدد أو اختيار كلمة أخرى يؤدي إلى التحيز.

يجمع مسار Cuvex المراجَع بين قطعة نقدية وأربعة أحجار نرد. تحسب دالة التحويل قيمة القطعة النقدية × 1,296 مضافًا إليها العدد برقم أساسه ستة الذي تشكّله نتائج الأحجار بعد طرح واحد من كل نتيجة. تُقبل الفهارس من 0 إلى 2,047. إذا تجاوزت النتيجة القاموس فأعد رمي القطعة والأحجار الأربعة. الاحتفاظ بنتيجة القطعة وإعادة النرد وحده يسبب انحيازًا. هذا وصف للشيفرة المراجَعة، ويجب فحص الشاشة والمسار كاملًا لكل إصدار موزع من البرنامج الثابت.

لا يساوي اختيار الكلمات المفضلة. لا تحولي عرض عام إلى مواد لحفظ المال أي بذرة الاسترداد تظهر في المواد التعليمية تعتبر معروفة. يجب أن يتم إنتاج الكلمة النهائية والتحقق من خلال خوارزمية كاملة للجهاز، دون استكمال عبارة التذكّر يدويا.

جهزوا مساحة خالية من الكاميرات، المساعدين الصوتيين النشطين بالقرب من هنا، تسجيلات الشاشة أو المشاهدين هي: المدرّس يجب أن تتوقف أثناء دخولك وتفقد السر ويمكنه أن يشرح ويقيّم في وقت سابق من خلال أسئلة عن العملية، دون أن يسمع نتائج الإطلاقات أو الكلمات.

بعد توليد، يجب اختبار نسخة احتياطية، تشفيره وفقاً للنموذج واختبار استعادة محفظة فارغ. عنوان التحقق يساعد على تأكيد التطابق دون عرض بذرة الاسترداد للحاسوب. إذا كان التدفق يقبل القيم التي تتعارض مع التعليمات أو عرض الكلمات غير المتوقعة، يوقف الاستخدام ويسجل فقط النسخة والشاشة والخطأ.

التدريب

1. في التجربة، تتبع خطوات الجهاز مع مواد غير مدعمة. حدد ترتيب النرد و لا تغير النتائج
2. كرر الـ المدخلات مرفوضة وفقاً للشاشة، دون تصحيحها لتلائمها.
3. تفقد على انفراد المحتوى، واصنع نسخة، وتأكد من أنك تستطيع إعادة بناء نفس الـ محفظة من التعلم.

أثبت فهمك

يفسر لماذا الإنتروبيا فيزيائياً، التحويل الصحيح والسرية للنتيجة ثلاثة متطلبات مختلفة.

سؤال شائع

هل يمكنني أن أحسب نسختي إلى الـ الذكاء الاصطناعي للتحقق من الخوارزمية؟ ليس لـ بذرة الاسترداد التي ستستخدمها وتعمل المساعدة مع أمثلة اصطناعية مختلفة.

نقطة توقف

ينتهي في حالة آمنة من الجهاز؛ لا تترك بذرة الاسترداد مرئية أثناء الاستراحة.

رفض البرنامج الثابت نتيجة نرد. أي تصرف يتبع الإجراء؟

1. انتقاء كلمة يدويًا.
2. إعادة المحاولة وفق تعليمات الجهاز دون تحييز النتيجة.
3. تقليل العدد حتى يُقبل.

> **عرض الإجابة: إعادة المحاولة وفق تعليمات الجهاز دون تحييز النتيجة.**
> الرفض جزء من تحويل الإنتروبيا ولا يجوز استبداله اعتباطًا.

تشفير سرّ وفك تشفيره باستخدام Cuvex

الهدف

إنشاء النص المشفّر تعلم والتحقق من تعافيها.

الفهم

اختر نوع المحتوى الصحيح: SLIP39، BIP39، منجم أو نص عندما يكون متوفراً في دفقك. إنها أشكال مختلفة. تشفير نص SLIP39 لا يحول Cuvex إلى الموقّع من جميع الشبكات التي يمكن أن تستخدم ذلك النص. تخزين الأسرار وتنفيذ بروتوكولات التوقيع لها نطاقات مختلفة.

أدخل المحتوى مباشرة إلى الجهاز عندما تبحث عن إبقاء ذلك خارج المعدات الموصولة. وقد تكون طريقة الاستيراد من الهاتف أو PC قد كشفت بالفعل عن السر الأصلي، حتى وإن كان الجواب التشفير لاحقاً. شاشة الفحص المسبق هي المكان المناسب لكشف الكلمات، الترتيب، الحروف، والحقول الخاطئة.

كلمة المرور من النص المشفّر يجب أن تكون طويلة، فريدة و قابلة للاسترداد وفقاً لخطتك وللوحة المفاتيح المنقّحة للإنشاء قدرة على حرف 40 محارِف، والمصدّق يتطلب ما لا يقل عن 12 وmicrogle وASCII، الرقم والرمز المعترف بهما. لا تطبق تلقائيا المحارِف 12 إلى 1.024 من Desk على لوحة مفاتيح Cuvex: Desk، وتتبع سياسة مختلفة. قد تكون لميادين الاسترداد الأخرى حدود مختلفة؛ فتتحقق من التدفق والنسخة.

في Original اكتب على بطاقة مناسبة فارغة؛ حافظ على الموقع حتى تحصل على تأكيد. في BIT يحتفظ بالمحفوظات التي تنتج عن التدفق USB، بما في ذلك المكونات بيومتري اللازمة عند الاقتضاء. لا تُعرف أو تُجمع الملفات بواسطة الحدس. وبعد ذلك يقوم بقراءة و فك التشفير اختبار على الجهاز، دون أن يبلغ السر إلى المدرّس.

التدريب

1. يرجى تقديم نص تعليمي أُنشئ لهذه الممارسة، بدون وثائق تفويض أو قيمة اقتصادية.
2. يُحدِّد الأساس والشيء الناتج؛ يُسجِّل على انفراد الاسم المستعار ووظيفته.
3. أعد تشغيل عملية فك التشفير، وافحص النص على شاشة الثقة وأغلق العرض عند النهاية.

أثبت فهمك

يمكنك تمييز المحتوى الصحيح، الكتابة الصحيحة والتعافي الصحيح. رسالة "النسخ المستنسخ" لا تثبت الثلاثة.

سؤال شائع

الاسم المستعار على البطاقة هو كلمة المرور؟ لا. إنها معلومات تنظيمية. تجنب إدراج أرصدة أو أو أوصاف تساعدك على تحديد أصولك.

نقطة توقف

لا تترك المحتوى فك التشفير مرئي. سجل فقط نجاح الاختبار أو فشله.

ما أفضل دليل على أن النص المشفّر التجريبي يصلح لاستعادة محتواه؟

1. أن يحمل اسمًا جميلًا.
2. وجود الملف في مجلدين.
3. قراءته وفك تشفيره بالمسار الصحيح وفحص المحتوى على انفراد.

> **عرض الإجابة: قراءته وفك تشفيره بالمسار الصحيح وفحص المحتوى على انفراد.**
> وجود نسخة لا يثبت صلاحيتها أو مطابقتها للمقصود.

عتبات التشفير والقياسات الحيوية

الهدف

فصل الحماية المشتركة عن السرية من التوقيع المتعدد إلى بيتكوين

الفهم

النص المشفّر محمي من قبل عدة كلمة المرور ينظم من يستطيع فك التشفير المحتوى. رقم محفظة بيتكوين التوقيع المتعدد يحدد ما ينبغي أن يأذن مفاتيح بإنفاق على الشبكة. يمكنك أن تحتفظ بسر التشفير بشكل مشترك يطابق محفظة coredo، أو كل الموقّع من التوقيع المتعدد مع النص المشفّر الخاص بك.

وإذا قام عدد من الأشخاص معاً بفك قفل بذرة الاسترداد وبذرة الاسترداد يسمح بالإنفاق بمفردهم، فإن عتبة السلسلة تظل مفتاح. بمجرد أن يتم الكشف عنها، يمكن لشخص ما أن يحتفظ بها. لا تصف هذا المخطط كما لو أنه يتطلب تنسيق عدة التوقيعات لكل دفعة.

ويضيف القياسات الحيوية من BIT شرطاً للوصول إلى الأشكالمستخدمة. الاص إصبع ليس بـ بذرة الاسترداد أو بديل عالمي من كلمة المرور . تخطيط الإصابات، تغيير البصمات، العوارية، توافر المعدات، والإرث. ويحفظ ويختبر مسار الاسترجاع الموثق لـ النص المشفّر قبل الاعتماد عليه.

تصدير الاستعادة يمكن أن يكشف السر على الحاسوب، فقط لحل حالة طارئة. وجود هذه الدالة لا يحول PC إلى بيئة تعادل الجهاز. ويجب أن تظل الممارسة العادية معزولة؛ ويُدرس الانتعاش المحلي عن علم، مع وضع خطة للهجرة في مرحلة لاحقة، إذا كان هناك تعرض.

التدريب

1. ارسم سياستين: «كلمتا مرور لفتح بذرة» و«مفتاحان من ثلاثة للإنفاق».
2. وفي اختبار بدون تمويل، يحدد أي الملفات يحتاج إلى نسخة قياس أحيائي وأين يتم التحقق من استعادته.
3. يَقُولُ بأنّ شخص ما لَيسَ متوفرَ. ما إذا كانت عتبة مخططك تسمح بالاستمرار

أثبت فهمك

يمكنك أن تشرحي من يستطيع معرفة السر ومن يمكنه أن يأذن بالإنفاق بعد فك تشفيره

سؤال شائع

هل لي أن أسحب مُشاركاً غير بطاقة؟ لا. يجب عليك التمييز بين التغييرات التنظيمية من حماية جديدة للسر وسياسة جديدة للإنفاق

نقطة توقف

احفظ المخطط بدون أسماء حقيقية أو بيانات بيومتري.

يفتح ثلاثة أشخاص بكلمتي مرور نصًا مشفّرًا يحوي بذرة محفظة أحادية التوقيع. كم مفتاحًا يتطلب الإنفاق في بيتكوين؟

1. مفتاحًا واحدًا إذا نصّت سياسة المحفظة على ذلك.
2. مفتاحين لأن الملف يتطلب كلمتي مرور.
3. ثلاثة بحسب عدد الأشخاص.

> **عرض الإجابة: مفتاحًا واحدًا إذا نصّت سياسة المحفظة على ذلك.**
> عتبة التشفير لا تغيّر السكربت الذي يتحكم في الأموال.

استنساخ النسخ وحفظها والتحقق منها

الهدف

بناء الترميل دون تدمير النسخة الصحيحة الوحيدة.

الفهم

استنسخ النص المشفّر نسخة بيانات مشفّرة؛ لا تخلق رصيدا جديدا أو بذرة الاسترداد أو مستقلة عن كلمة المرور المكشوفة. النسخ المتطابقة تُحلّل فقدان الدعم، لا خطوبة السرّ الأصلي. لذلك فإن إعادة الاستعادة والهجرة إلى مفاتيح الجديدة تستجيب لحالات مختلفة.

في Original، يُميّز بين بطاقة النص المشفّر وبطاقة النقل PSBT. يمكن إعادة استخدام نظام التشغيل وفقاً للتدفق بطاقة مع نسخة احتياطية لا يجب أن تصبح ذلك النظام إذا رفضت عملية ما بطاقة تحتوي على النص المشفّر، لا تحاول أن تتخطى الحماية أو تمسح عنقها يدويا.

في BIT يجب أن تحتفظ نسخة المجموعة المطلوبة والعلاقة بين الملفات. يمكن لمدير الملفات أن يظهر نقلا كاملا دون ضمان أن يكون الجهاز قد أكّد المحتوى أو أنهى تشغيله. إنه ينتظر البيانات المكشوفة ويتحقق من نسخة من عملية الاستعادة المحكومة

يحتفظ بقائمة جرد خاصة بها محددات هوية منفصلة، ونموذج، وتاريخ، ونتائج الاختبار النهائي. افصل على الأقل نسختين من الحوادث التي حددتها تجنب الصعود نسخة احتياطية إلى قنوات دعم تشخيص المشاكل؛ اوفر البيانات الوصفية مسحة ورمز الخطأ.

التدريب

1. يخلق نسخة من النص المشفّر في نظام آخر، بواسطة التدفق الصحيح.
2. اقطع الرابط الأصلي واسترجع النص الاختباري من النسخة.
3. يوثق ما ستفعله حيالخسارة، تلف الملف، وعرض كلمة المرور. ليس نفس الإجراء

أثبت فهمك

يمكنك التعرف على النسخة التي جربتها وشرح سبب عدم كتابة النسخة الأصلية

سؤال شائع

هل لي أن أحذف الأصل بعد أن أرى ملفا ثانيا؟ أولاً تحقق من شفاء و تغطية التخلص يجب أن يكون وفقاً لخطة، وليس لمجرد عدد النسخ.

نقطة توقف

احتفظ بأجهزة التحكم قبل أن تغلق الجلسة لا تترك بطاقات مدمجة مع بطاقات إثبات الدفع

إذا عرف شخص كلمة المرور وحصل على نسخة من النص المشفّر، فما فائدة إنشاء ثلاث نسخ إضافية؟

1. إبطال نسخة المهاجم.
2. زيادة التكرار الاحتياطي دون إبطال وصوله.
3. تغيير بذرة بيتكوين تلقائيًا.

> **عرض الإجابة: زيادة التكرار الاحتياطي دون إبطال وصوله.**
> النسخ لا يلغي اختراقًا وقع بالفعل.

تثبيت Cuvex Desk وحمايته

الهدف

فتح مرفق مصدر تم التحقق منه وحماية مستودعك المحلي

الفهم

اختر حزمة نظامك ومعماريته: macOS Intel أو Apple Silicon، وWindows x64 أو ARM64، وLinux x64 أو ARM64 بحسب التوزيع المتاح. ملف ZIP للمصدر وحزمة Manager ومثبّت العميل تسليمات مختلفة. لا ينبغي للدورة توجيه المتعلم إلى حزمة توقيع خاصة.

المصدر المتحقق من النظام و مراجعاته شركة هندسية Windows فهو بحد ذاته لا يوفر ثقة عامة لدى المحرر. في ماك، توقيع التطبيق، التحقق والتقييم عند الفتح هي ضوابط مختلفة. لا تُعطل الحماية العامة عن طريق الاتصالمباشر إذا كانت نسخة ما تعطي تحذيراً غير متوقع، فإنها تحتفظ بالنص وتستخدم القناة الرسمية.

Desk يخلق مستودع محلي التشفير مع كلمة المرور. وفي الأساس المنقح، تُقبل الـ كلمة المرور الجديدة من 12 إلى 1.024 الحروف؛ وتطابق الحقول مطلوب حيثما يوجد تأكيد. وهذه الحدود ليست مقياسا كافيا للنوعية: فهي تستخدم عبارة واحدة وتتجنب إعادة الاستخدام. القياسات الحيوية من الكمبيوتر، عندما يكون متاحاً، هو وسيلة وصول مريحة تتطلب تشكيله الخاص.

اضبط قفل الخمول، وعند الاقتضاء عند الانتقال إلى العادم. التأخّر بعد الأعطال والحذف الاختياري يُدرَج في الدليل: لا تفعّل ممسحة آليّة أثناء العرض العملي. ويمكن أن يعمل هذا البرنامج دون حساب مستخدم تقليدي، ولكن خدماته الاستشارية أو خدمات الدردشة أو التنزيل لها متطلبات واتصالات محددة.

التدريب

1. تحقق من منصة الرزمة ونسختها مرئية ومنشؤها دون تزويد المدرّس ببطاقات تعريف خاصة.
2. إنه يُنشئ مستودعاً للتعلم ويتحقق من الإغلاق وإعادة الافتتاح أدخل كلمة المرور على انفراد.
3. عرض نسخة مشفرة و احتفظ بـ كلمة المرور وفقاً لخطتك لا تُجرّبْ التشويشَ المتكررَ في البيئةِ الحقيقيةِ.

أثبت فهمك

يمكنك التمييز بين كلمة المرور محلي، الحساب التجاري، و وثائق تفويض الخدمات التي تضيفها.

سؤال شائع

هل تغيير كلمة مرور Desk يغير بطاقة بطاقاتي؟ لا. إنها حماية مستقلة. النسخ القديمة أيضا لا تتغير من تلقاء نفسها.

نقطة توقف

اقفل Desk واحتفظ ببطاقة تعريف الدرس بدون وثائق تفويض

برنامج التثبيت غير مناسب لمعمارية جهازك. ما الخطوة الأولى؟

1. تعطيل الحماية وفرض تشغيله.
2. الحصول على الحزمة الرسمية المناسبة والتحقق من متطلباتها.
3. استيراد البذرة إلى موقع للمتابعة.

> **عرض الإجابة: الحصول على الحزمة الرسمية المناسبة والتحقق من متطلباتها.**
> تحقّق من التوافق والمصدر قبل استعمال مواد الحفظ.

ربط النصوص المشفّرة وتنظيم حسابات WOW

الهدف

اربط نسخة مشفرة واميزها من حساب للمراقبة.

الفهم

ينظم Desk النص المشفّر مثبتة بـ NFC أو USB أو ملف نسخ مطابقة. التصميم البصري والاسم المستعار يساعد على التعرف عليهم، ولكن لا يوجد دليل تشفيري للهوية. يمكنك الرجوع في الملف إلى المصدر والخصائص التي فسرها التطبيق، مثل الشكل، الحجم، خصائص الوصول.

الربط بين استيراد أو تنظيم الشيء المتوافق؛ لا يعني فك تشفيره في PC أو التحقق من سره. WOW هي محفظة للمراقبة فقط شريكة في الإعلام العام المتوافق. ويمكن أن تكون لنفس المجموعة من الأسرار حسابات أو مشتقات مختلفة: فالجمعية ينبغي أن تكون مساوية للـ محفظة التي تنوي إدارتها.

تشغيل أو استيراد حساب واصف أو معلومات عامة مصدرة من تدفق الجهاز. تحقق من الشبكة، نوع من التسرّب، البصمة، الطريق، وعنوان التحكم. اسم الحساب هو تنظيمي؛ تعريف الهوية المشتق من الاسم لا ينبغي أن يعامل كتحجيم قوي، لأن الاسم المتوقع يمكن تخمينه.

وتُحتفظ في قاعدة Desk بحسابات قائمة على الشراكة ووظائف تصدير النسخ، والنسخ، والتخلص من السجلات المحلية. احذف بطاقة الواجهة لا تدمر النسخ الخارجية أو تحرك الأموال. "لا يوجد نسخة احتياطية" يعني أن التطبيق لا يعتمد نسخة حسب تقديره، لا أن أي نسخة احتياطية موجود في العالم.

التدريب

1. ربط النص المشفّر من خلالنقل المختار، وتفقد سجلك.
2. يستورد حساب تعلم متوافق ويتحقق من شبكته وعنوان التحقق بدون إظهار مفاتيح إلى المدرّس.
3. اكشف سجل النص المشفّر والحساب WOW والأداة المادية. هو يُحدّدُ الذي يَختفي مَع a مسح محلي.

أثبت فهمك

يمكنك تفسير البيانات التي تحتاجها (Desk) للملاحظة وأي البيانات التي يجب أن تبقى خارج الحاسوب أثناء الاستخدام الاعتيادي

سؤال شائع

هل قمت بربط ملف الـ بي. بي. يضمن أن يكون بذرة الاسترداد خاصتي؟ لا. يجب أن تتحقق من مصدره و تعافيه امتداد ملفّ لا يُصدّق المحتوى.

نقطة توقف

لا يحتفظ إلا ببيان "الربط الاختباري المتحقق منه".

هل ينقل حذف حساب WOW محليًا أموال البيتكوين المرتبطة به؟

1. لا، يحذف معلومات محلية وفق الإجراء ولا ينفق مخرجات UTXO.
2. نعم، يرسلها إلى الشركة المصنّعة.
3. يلغي كل توقيع يحتفظ به شخص آخر.

> **عرض الإجابة: لا، يحذف معلومات محلية وفق الإجراء ولا ينفق مخرجات UTXO.**
> الحالة المحلية تختلف عن حالة السلسلة.

ربط Mirror بـ Desk

الهدف

إنشاء وإنهاء اتصال محلي مرخص به دون الخلط بين رموزه.

الفهم

يتيح Mirror عمليات محلية مع Desk عبر الربط وPIN وQR كما تعرضها التطبيقات. يخص PIN المكوّن من ستة أرقام تلك الجلسة، وليس كلمة مرور Desk أو النص المشفّر أو كلمة استرداد. تحقق من الشاشة التي تولّده ومكان إدخاله، ولا تستخدم رمزًا يرسله مجهول.

يبدأ العمل من السياق الصحيح لـ Desk: الربط، قراءة QR، نقل PSBT أو البرنامج الثابت هي أهداف مختلفة. النافذة تُبلغ عن البحث، الاتصال، الاكتشاف، QR ،PIN، والإجراء على البطاقة أو الملف. وجود جهاز في البحث لا يثبت أن العملية كاملة قد انتهت

يمنح التصاريح ذات الصلة حسب النظام: آلة تصوير للقراءة الضوئية، وBluetooth أو NFC عندما يتطلبها التدفق. هاتف بدون قدرة جسدية ضرورية لا يحصل عليها من خلال تركيب البرمجيات وفي iOS هناك اختلافات في المكيف والمصادقة؛ ولا ينبغي تقديم مشروع يمكن تجميعه كما لو كان قد تم توزيعه واختباره بالفعل في جميع iPhone.

إذا فشلت، حدد المرحلة الدقيقة: لا تظهر، يظهر ولكن لا يصل، تم رفض PIN، أو QR غير مقروء، أو بطاقة غير مقروءة، أو رد لم يرد. إغلاق الجلسات القديمة، التحقق من النصوص المتوافقة والتصاريح، والحصول على السيطرة. PIN غير صحيح لا يبرر تغيير البرنامج الثابت أو إدخال بذرة الاسترداد في مكان آخر.

التدريب

1. ابدأ قراءة اختبارية من Desk واوصل Mirror عبر شاشاتك المحلية.
2. تحقق من الغرض قبل تقديم QR أو بطاقة تعليمية.
3. ألغ الجلسة وأكد أن قراءة سياق سابق لا تنطبق. أعيد فتح جلسة جديدة.

أثبت فهمك

يمكنك وصف المرحلة الفاشلة والمعدات المشاركة دون الإبلاغ عن رموز نشطة أو محتويات حساسة.

سؤال شائع

ﻉ Mirror هل يجب أن تبقى متصلة دائماً؟ يعتمد على العملية. ولا تعامله كخدمة دائمة، ولا تفترض أن جلسة ما لا تزال مسموحا بها بعد إغلاق بابها أو نقلها إلى مكان آخر.

نقطة توقف

أغلق جلسة الاتصال وأغلق التطبيقات التي لا تستخدمها

ما الذي ينبغي للمدرّس فعله إذا فشل الربط قبل ظهور PIN؟

1. طلب البذرة.
2. مراجعة اكتشاف الجهاز والأذونات والجلسة والإصدارات قبل المتابعة.
3. اعتبار الاتصال مكتملًا.

> **عرض الإجابة: مراجعة اكتشاف الجهاز والأذونات والجلسة والإصدارات قبل المتابعة.**
> يجب أن يتبع التشخيص المرحلة المشاهدة دون افتراض نجاح الاتصال.

استخدام NFC عبر Mirror والنقل عبر USB-C وقراءة رموز QR

الهدف

استخدم كل وسيلة نقل لغرضها مع إجراء الفحوص المخصصة لها.

الفهم

تتطلب إجراءات NFC في Cuvex Desktop تشغيل Cuvex Mirror على هاتف ذكي متوافق مقترن بالحاسوب عبر Bluetooth. لا يدعم Cuvex Desktop قارئات NFC الخارجية المتصلة بمنفذ USB. يجب كذلك توافق البطاقة وتنسيقها وسعتها. فقد تحمل بطاقة صغيرة نصًا مشفّرًا ولا تتسع لمعاملة PSBT تحتوي على معاملات سابقة. يعتمد الحد الفعلي على كامل المحتوى، وليس عدد المستفيدين وحده. لا تحوّل بطاقة احتياطية إلى بطاقة نقل.

مع Original يستطيع Mirror كتابة الطلب على بطاقة عمليات. يعالجه الجهاز ويكتب ردًا يعيده Mirror إلى Desk. تأكيد نجاح الكتابة لا يعني أن Desk تلقّى الرد. أبقِ البطاقة ثابتة حتى يعرض الجهاز النتيجة. وإذا رفض النظام الكتابة لحماية نص مشفّر تعرّف عليه، فاحترم الرفض.

يستخدم BIT وحدة تخزين أو مجلدًا للتبادل عبر USB. قد تُفصل الوحدة منطقيًا أو تظهر مجددًا أثناء العملية. على Desk اختيار الوسيط الصحيح والتحقق من الرد وإتمام إقرار الاستلام المقرر. نسخ ملف إلى مجلد في الحاسوب يحمل الاسم نفسه لا يوصله إلى الجهاز.

قد يتعذر على الكاميرا قراءة QR بسبب التركيز أو الانعكاس أو الحجم أو الحركة أو كثافة البيانات. كبّر العرض واضبط الضوء والمسافة. لا تستبدل المعرّف الطويل بحروفه الأولى ولا تقبل نسخًا جزئيًا. نجاح القراءة بداية التحقق من معنى المحتوى.

التدريب

1. استخدم المواد التعليمية وحدّد في الرسم الطلب والوسيط والرد لكلّ من Original وBIT.
2. جرّب إلغاء قراءة QR دون حفظ قيم تصل متأخرة. كرّر التجربة لغرض آخر.
3. حاكِ حالة ملف كبير أكثر مما ينبغي، واشرح الحاجة إلى تبسيط العملية أو اختيار وسيط متوافق من دون إسقاط أيّ فحص.

أثبت فهمك

بيّن أي جهاز أكّد كل مرحلة: القراءة أو الكتابة أو التحقق أو الاستقبال أو إقرار الاستلام.

سؤال شائع

هل تثبت قيمة تجزئة أو رسالة OK بعد النسخ أن مستفيد البيتكوين صحيح؟ لا. يجب مراجعة العملية ومخرجاتها على جهاز التوقيع.

نقطة توقف

انزع بطاقات النسخ الاحتياطي واحفظها، وحدّد وسيط النقل بوضوح.

يقول **Original** إنه كتب الرد على البطاقة. ما الذي ينقص قبل القول إن **Desk** تلقّاه؟

1. طلاء البطاقة بلون آخر.
2. إنشاء بذرة جديدة.
3. قراءة الرد والتحقق منه في Desk عبر المسار المخصص.

> **عرض الإجابة: قراءة الرد والتحقق منه في Desk عبر المسار المخصص.**
> نجاح الكتابة ونجاح الاستقبال حدثان منفصلان.

المزوّدون العموميون والعقدة الخاصة بك

الهدف

اختر مصدرًا للاستعلام وافهم ما قد يكشفه وحدوده.

الفهم

يمكن لـ Desk الاستعلام لدى مزوّدين عموميين متوافقين أو عبر Bitcoin Core يهيئه المستخدم. قد يعرف المزوّد الطلبات الواردة وترتيبها وبيانات الاتصال. عدم إرسال xpub كامل يقلل نوعًا محددًا من الكشف، لكن يمكن أيضًا الربط بين السكربتات أو قيم تجزئتها.

يتيح Desk 9.21 اختيار Blockstream Electrum صراحة عبر TLS، إلى جانب بدائل REST والعقدة الخاصة. يحمي TLS القناة من بعض مراقبي الشبكة، لكن المزوّد نفسه يتلقى الطلبات. ولا توجد مناوبة صامتة بين المزوّدين تضمن إخفاء الهوية. يلزم عند الاختيار فهم ما تتنازل عنه من خصوصية مقابل السهولة.

لاستخدام Core اضبط نقطة الاتصال والمصادقة ومحفظة المراقبة وفق الدليل المعني. لا تنشر منفذ RPC ولا تعرضه للإنترنت كي «يراه» التطبيق. اقصر الوصول على بيئات موثوقة واستعمل وسيلة نقل محمية مناسبة. لا تُملِ كلمة مرور RPC على المدرّس.

قد تستغرق المزامنة الأولى وإعادة الفحص وقتًا. تقدّم العملية يصف العمل الجاري ولا يعلن نجاحه مسبقًا. يحتفظ Desk بالعمل في الخلفية، وإغلاق العرض لا يوقف العقدة. لا تضمن النافذة التاريخية الدنيا المذكورة في الوثائق اكتشاف ما سبقها، فإذا كانت محفظتك أقدم فتحقق من تاريخ الاستيراد ونطاق الفحص الفعلي.

يعتمد الاكتشاف على السجل لا على إيجابية الرصيد. يظل العنوان الذي أُنفق كامل رصيده عنوانًا مستخدمًا. في التوقيع المتعدد الذي روجع، تُراعى فجوة من 20 عنوانًا متتاليًا بلا سجل لكل فرع ومشارك، مع حدود لإصدار العناوين. لا تعمّم حدًا إجماليًا على كل المحافظ.

التدريب

1. اختر مصدرًا للتدرّب واشرح البيانات التي يمكنه رؤيتها.
2. راجع تاريخ آخر مزامنة والشبكة والتقدّم. عند ظهور HTTP 429 احترم مهلة الانتظار ولا تغيّر المزوّد دون قرار منك.
3. حاكِ محفظةً رصيدها صفر ولها سجل قديم، وبيّن الفرق بين «صفر» و«غير مستخدم».

أثبت فهمك

حدّد إن كان مصدرك يلبي حاجتك إلى التحقق والخصوصية، وتعرّف إلى حالة لم تكتمل بعد.

سؤال شائع

هل تجعلني عقدتي الخاصة مجهول الهوية؟ لا. تقلل الاعتماد على الغير في الاستعلام، لكن يجب النظر في الاتصال والأطراف المقابلة والنشر وسائر البيانات الوصفية.

نقطة توقف

سجّل نوع المزوّد والحاجة إلى استكمال الفحص فقط.

رصيد عنوان صفر، لكنه استقبل أموالًا وأنفقها. كيف يُعامل عند اكتشاف عناوين المحفظة؟

1. بصفته عنوانًا له سجل.
2. بصفته عنوانًا لم يُستخدم قط.
3. بصفته عنوانًا غير صالح.

> **عرض الإجابة: بصفته عنوانًا له سجل.**
> يحدّد السجل ما إذا كان العنوان مستخدمًا، لا رصيده الحالي.

استقبال البيتكوين والتحقق من العنوان

الهدف

أنشئ طلب إستلام و تحقق منه قبل تسليمه.

الفهم

افتح حساب WOW الصحيح وتأكد من الشبكة والسياسة. أو يسترجع طلباً بالاستلام. يمكنك أن تضيف دافعاً ومراقباً ومقداراً متوقعاً لمنظمتك هذه الحقول تصف معلوماتك المحلية، المبلغ المتوقع لا يمنع أي شخص من إرسال كمية أخرى.

تأكد من العنوان باستخدام التدفق المتاح في الجهاز وفي سياق محفظة. وإذا لم يتم بعد التحقق المادي من هذه الرحلة في تركيبتك، فإن الممارسة تبقى في المحاكاة وتتوقف قبل تلقي أموال كبيرة. ومقارنة شاشاتين يعملان بنفس المصدر لا تعطي استقلالية غير موجودة.

يستخدم عنوان جديد لعلاقة تحصيل جديدة عندما يسمح التدفق بذلك. وفي التوقيع المتعدد المنقحة، لا يعاد تخصيص أو انتهاء صلاحية العناوين التي سبق عرضها، لأنه يمكن للمدفع أن يستخدمها لاحقا. وعندما تصل إلى حد العناوين الجديدة المتتابعة التي لا تاريخ لها، تستعيد الطلب المسبق المناسب وتتفهم سبب الحد؛ ولا تسترجع الأرقام القياسية.

بعد المشاركة، راقب الدخول إلى مصدرك للتحقق. رسالة بريدية أو شهادة من منصة تداول أو قبضة من المُدفع لا تثبت التصفية تأكّد من الشبكة، txid، خروج، قيمة و التأكيدات حسب التعرّض. لا تفتح مستكشفاً عاماً بعنوانك من باب الراحة إذا كانت خطتك تتطلب إجراء تلك المشاورات الخاصة

التدريب

1. يُولّدُ a طلب في المختبرِ، يُدقّقُ الحسابَ والشبكةَ ويُوضّحُ كَيفَ تَتأكّدُ مِنْ العنوانِ.
2. يسجل بطاقة وهمية ويسترجع نفس الطلب بعد إغلاق جلسة النظر.
3. يقوم بمحاكاة تحصيل مبلغ مختلف ويقرر كيف يطابقه دون تغيير التاريخ.

أثبت فهمك

يمكنك التمييز بين العنوان المولد، العنوان المتحقق منه، الطلب المشترك، و التحصيل المؤكد.

سؤال شائع

هل توقف عنوان قديم عن العمل بخلق آخر؟ ليس عادة. الحفاظ على الاكتشاف وتسجيل الطلبات يتجنب فقدان رؤية المدفوعات المتأخرة

نقطة توقف

حفظ حالة طلب المختبر، وليس محتوى المدرّس.

أرسل الدافع لقطة شاشة تقول «اكتمل السحب». ماذا تفحص قبل اعتبار الدفع مستلمًا؟

1. جودة الصورة وحدها.
2. المخرج المعني في مصدر شبكي موثوق والتأكيدات اللازمة.
3. كلمة مرور الدافع.

> **عرض الإجابة: المخرج المعني في مصدر شبكي موثوق والتأكيدات اللازمة.**
> إثبات تجاري أو لقطة شاشة لا يغنيان عن التحقق من الدفع.

وسم مخرجات UTXO وتجميدها واختيارها

الهدف

الإعداد المدخلات عدم الخلط بين أسبابها حادثا وحادثا.

الفهم

وتسمح العلامات بالاحتفاظ بالسياق الذي لا يظهر في السلسلة: المنشأ، والمناظرة، والغرض، والقيود المفروضة على الاستخدام. وفي Desk، يمكن أن تكون لعلامة UTXO ومذكرة توجيه أطوال ووظائف مختلفة. ملاحظة "العميل A" مفيدة؛ استخدام مستندك أو اسمك الكامل يمكن أن يخلق سجلاً حساساً بلا داع.

تجميد UTXO في Desk يستبعدها من اختيارات محلية معينة لا يحجب نفقاته على بيتكوين، ولا يغير البرمجية، ولا يمنع تطبيق آخر باستخدام مفاتيح. ويمكن أن يؤدي أيضا إلى اختلاف الرصيد الإجمالي ورصيد النفقات القابلة للاستهلاك. تحقق مما إذا كانت عملة مجمدة أم محجوزة بمسودة أم مُنفقة فعلاً

الانتقاء الآلي الأمثل وفقاً للخوارزمية وسياقها؛ لا يعرف بالضرورة علاقاتك الخاصة. وبالنسبة للدفع المحدد، يفحص ما إذا كان من المناسب استخدام مخرج من نفس السياق بدلاً من ربط المدخرات وكشوف المرتبات والنشاط التجاري. الفصل النافع يتطلب الثبات المستقبلي، ليس فقط الوسم الجميل.

صدِّر بطاقات التعريف التي يكون لها شكل BIP329 تيسير حفظها أو تهميشها. الشكل لا يُعدّل وحده. Desk يقدم غلاف التشفير لتصديره؛ ويميز الأرشيف المحمي من نص مسطح متوافق. عند الاستيراد، تحقق من مطابقة محفظة و معالجة التجميد قبل كتابة المعلومات.

التدريب

1. وسم ثلاثة مخرجات UTXO اصطناعية بالادخار والنشاط والتبرع.
2. جمّد واحد وافحص الفرق بين الرصيد المُلاحظ والمتاح للاختيار.
3. صدّر بطاقات المختبر مع كلمة المرور، استيراد في نسخة، مراجعة النتائج بدون بيانات خاصة حقيقية.

أثبت فهمك

يبرر اختيار المدخلات للتكلفة والتعرض. يعترف بأن التجميد هو تفضيل محلي

سؤال شائع

بطاقة تعريفية تُسافر إلى Xالمستلم عند الدفع؟ ليس فقط لمجرد كونها علامة محلية. يمكن ترشيحها عند التصدير، أو المشاركة في الملفات، أو استخدام خدمة أخرى، أو إضافتها إلى رسالة.

نقطة توقف

حفظ بطاقات الممارسة و حالة التجميد.

ما أثر تجميد UTXO في Desk؟

1. إنشاء قفل إجماع على الشبكة.
2. نقله إلى حساب خاص.
3. وضع قيد محلي على اختياره بحسب التطبيق.

> **عرض الإجابة: وضع قيد محلي على اختياره بحسب التطبيق.**
> لا يلغي قدرة النسخ الأخرى من المفاتيح.

إعداد الدفعة ومراجعتها

الهدف

أنشئ PSBT تفهمه وحدّد جميع تكاليفه ومخرجاته.

الفهم

اختر الحساب والمدخلات القابلة للإنفاق والمستفيدين والمبالغ. تحقق من مصدر الطلب. بعد اللصق أو المسح راجع العنوان كاملًا والشبكة، إذ قد تُستبدل محتويات الحافظة أو الصورة. لا تكتفِ بالحروف الأولى والأخيرة إذا أمكن إجراء فحص كامل.

اختر معدل الرسوم وراجع قيمتها المطلقة والحجم التقديري والإجمالي والباقي. عند اختيار «إرسال الكل» يخصم Desk الرسوم من المبلغ المتاح. إذا انطلقت العملية من الدردشة ولم يكفِ الصافي للمبلغ المطلوب، فالدفع الجزئي قرار متعمّد. لا يتغير الطلب الأصلي لإخفاء الفرق.

تحقّق مما إذا كان الباقي صغيرًا أو لم يوجد مخرج للباقي. يجب فحص أي مخرج يوصف بأنه لك وفق السياسة، لا وفق تسمية المنسّق. إذا تعذّر إنشاء مخرج للباقي فأعد فحص تحويل الرصيد بالكامل أو أضف مدخلًا متوافقًا. لا تقبل أن يتحول المبلغ بصمت إلى رسوم غير متناسبة.

PSBT تنسيق لنقل المعلومات والتوقيعات، ولا يضمن بالضرورة الخصوصية أو أصالة المصدر. قد يتضمن معاملات سابقة ومفاتيح عامة ومسارات وبيانات وصفية. يستخدم ملف التوقيع المتعدد في البرامج الثابتة Final التي روجعت PSBT v0/BIP174. لا تعني «المعاملة من الإصدار 2» أن «PSBT من الإصدار 2».

التدريب

1. أنشئ في المحاكي دفعة بمدخل قدره 120,000 sat، ومبلغ للمستفيد قدره 70,000 sat، ورسوم قدرها 1,000 sat.
2. عدّد جميع المخرجات واشرح الباقي البالغ 49,000 sat. كرّر التمرين مع تحويل الرصيد بالكامل.
3. ألغِ المسودة واشرح ما ألغيته محليًا. لا تستخدم هذا المحاكي لتوقيع أي شيء أو نشره.

أثبت فهمك

قبل التصدير اشرح ما يدخل وما يخرج ومن يتلقى المال وكم يكلف وما الإذن الذي لا يزال مطلوبًا.

سؤال شائع

هل أستطيع إرسال كامل الرصيد المعروض؟ فقط إذا حسب التطبيق صافي مبلغ صالحًا للإرسال مع تغطية الرسوم. قد يتضمن الرصيد أموالًا غير متاحة.

نقطة توقف

احفظ مسودة التدريب أو ألغها. لا تحفظ PSBT حقيقيًا في بوابة الدورة أبدًا.

تعرض شاشة عبارة «transaction version 2». هل يثبت ذلك أن الملف بصيغة PSBT v2؟

1. لا، فهما حقلان مختلفان للإصدار.
2. نعم دائمًا.
3. يثبت أنه يستخدم Taproot.

> **عرض الإجابة: لا، فهما حقلان مختلفان للإصدار.**
> تميّز BIP370 بين إصدار الحاوية وإصدار المعاملة.

التوقيع بجهازي Original وBIT

الهدف

أكمل مسار التوقيع لكل طراز وتلقَّ ردًا مرتبطًا بالعملية الصحيحة.

الفهم

مع Original، سلّم PSBT باستخدام Cuvex Mirror وبطاقة النقل الخاصة بالمسار المتوافق. اقرأ الطلب على الجهاز، وقدّم النص المشفّر وافتحه على انفراد. راجع جميع المخرجات والمبالغ والباقي والرسوم. يُكتب الرد على البطاقة، ثم يُقرأ ويُتحقّق منه في Desk. نجاح الكتابة على البطاقة لا يغني عن خطوة الإرجاع.

مع BIT، اختر وحدة التخزين الصحيحة وسلّم الطلب عبر USB-C. تدير خدمة Desk المحلية التبادل المطلوب وأنت تشغّل الجهاز. قدّم النص المشفّر حسب التعليمات المعروضة وراجع البيانات على BIT. يستورد خيار «الاستلام من BIT» الرد. يتحقق Desk منه ويحفظه قبل تأكيد إقرار الاستلام. عند الانقطاع استأنف العملية نفسها، لا عملية أخرى تبدو مشابهة لها.

في التوقيع المتعدد ضمن إصدارات البرامج الثابتة Final، تشمل المراجعة الملخص والمخرجات الإلزامية والتحذيرات المنطبقة والتأكيدات النهائية الثلاثة لخيار «توقيع PSBT». تتيح المراجعة الموسعة الاختيارية استعراض معلمات إضافية، ولا يلغي اختيار «لا» الفحوص الإلزامية. التحقق المستقل من السياسة مسار آخر، وتظل نتيجته مقصورة على نطاق تلك المراجعة.

يتطلب التوقيع نصًا مشفّرًا متوافقًا يمكن التحقق من أصالته. استمرار إمكان استعادة السر من نسخة قديمة لا يجعلها مؤهلة للتوقيع. إذا حذّر الجهاز من نسخة قديمة غير متحقق من أصالتها، فاتّبع مسار استعادة السر وفحصه وإنشاء نسخة جديدة قبل التوقيع. لا تعدّل الترويسات ولا تتجاوز الرفض.

ألغِ العملية إذا لم يتطابق عنوان أو ظهرت رسوم غير متوقعة أو بيانات ناقصة أو شبكة أخرى أو رفض الجهاز السياسة. لا تدع ضغط إنهاء المكالمة يتحول إلى موافقة. لا يضغط الذكاء الاصطناعي الأزرار، ولا يؤكد القرار النهائي، ولا يعلن توقيع ما لم تتحقق منه أنت.

التدريب

1. اتّبع المسار الخاص بطرازك بمحفظة خالية من الأموال أو في مختبر اجتاز القبول على الأجهزة الفعلية.
2. حاكِ التوقف قبل التأكيدات النهائية واشرح لماذا لا يُعدّ ذلك إذنًا.
3. تحقّق من عودة الرد وارتباطه بالمسودة، وفي BIT من حالة الاستقبال وإقرار الاستلام أيضًا.

أثبت فهمك

اشرح المسار دون كشف بيانات اعتماد، وميّز بين الموافقة على الجهاز واستيراد الرد ونشر المعاملة.

سؤال شائع

هل يعرف الجهاز غير المتصل أن مدخلاتي لا تزال غير منفقة؟ لا يمكنه فحص الحالة الراهنة للسلسلة بمفرده. يجب أن يتحقق التطبيق من المعاملة النهائية اعتمادًا على مصدر بيانات الشبكة.

نقطة توقف

إذا انقطع التوقيع فألغِ العملية أو اتركها معلّقة مع معرّف واضح وفق المسار، دون إظهار أسرار.

وقّع BIT لكن Desk لم يؤكد الاستلام. ما الحالة التي يجب افتراضها؟

1. نُشرت الدفعة نهائيًا.
2. الرد بانتظار الاستقبال أو التحقق. استأنف العملية نفسها.
3. فُقدت المحفظة.

> **عرض الإجابة: الرد بانتظار الاستقبال أو التحقق. استأنف العملية نفسها.**
> التوقيع والاستقبال والنشر مراحل مختلفة.

استكمال المعاملة ونشرها ومعالجة المشكلات

الهدف

إغلاق دورة الدفع دون تكرارها وتشخيص الأخطاء في كل مرحلة.

الفهم

وبعد استيراد توقيع، يجب على Desk أن تتحقق من أنه مطابق للمشروع وأن تحتفظ بالنية. وقد تكون العتبة غير موجودة في التوقيع المتعدد؛ أما في حالة التوقيع الأحادي الطرف، فإن توقيعا مستوردا لا يعفي من التنقيح. الإنجاز يُنتج المعاملة جاهز للنشر عندما تكون ظروفك كاملة.

أعلن بعد المراجعة النهائية فقط ويشير رد من الخادم أو txid إلى نتيجة لهذا الطلب، ولكن ينبغي أن يؤكد التتبع القبول والسلاسة. إذا لم يتلقّ التطبيق أيّ ردّ، إستشار قبل تكرار. لا تختلق دفعات جديدة لحل مشكلة الرؤية.

بالنسبة لمبلغ مستحق، يراجع التعريفة والصلاحية والتنازع والإمكانية الفعلية لـ RBF. وفي حالة حدوث تغيير في السياسة العامة أو المستلم، فإن الاقتراح الجديد يتطلب مزيدا من التوقيعات المناسبة. والإلغاء المحلي لا يدمر توقيعا أو معاملة يحتفظ بها شخص آخر، ولا يلغي التأكيد.

(ب) التشخيصات على مراحل: الإعداد، والنقل، ورفع القفل، والاستعراض، والتوقيع، والعودة، والتصديق، والإنجاز، والنشر، والتأكيد. سجل النظام، النسخة، النموذج، المرحلة، الوقت التقريبي ورمز الخطأ. صُممت تشخيصات التطبيق لاستبعاد البيانات الحساسة، ولكن قم بفحصها قبل تقاسمها وتجنب إرفاقها بنسخ أو QR أو مفتاح Chat أو وثائق التفويض.

التدريب

1. اصدر أوامرك بالدفع الوهمي واعرف اين ستتوقف
2. يُلغي ثلاث حالات: عدم كفاية الرصيد، عدم تلقي الرد USB ونشره مع انقطاع الاتصال.
3. يُعدّلُ a تذكرة باستخدام البيانات الإصطناعية و نتيجة متوقّعة قابلة للتحقق.

أثبت فهمك

يمكنك أن تقرر ما إذا كان الطالب أو الجهاز أو المنسق أو الشبكة مفقوداً، وتتجنب دفع مبلغ إضافي غير ضروري.

سؤال شائع

هل يمكن إصلاح خطأ FIRMWARE_CAPABILITY_REQUIRED بتغيير البرنامج الثابت إلى عمياء؟ لا. في عدد Desk، واكتشاف الوائل النهائي يتطلب تصحيح فهرس Desk . إعادة تشغيل النسخة والخصائص قبل تغيير المعدات.

نقطة توقف

احفظ الحالة و التالي الفعل. إذا نشرت عملية حقيقية خارج المختبر، احتفظ بسجله في سجلاتك الخاصة.

أي إجراء يلغي بمفرده معاملة مؤكدة بالفعل؟

1. حذف المسودة المحلية.
2. إغلاق Mirror.
3. لا شيء مما سبق.

> **عرض الإجابة: لا شيء مما سبق.**
> الحذف المحلي لا يعيد كتابة السلسلة ولا يسحب أذونات متداولة.

ما الذي يمكن ملاحظته على شبكة بيتكوين؟

الهدف

ميّز البيانات العلنية والاستنتاجات والبيانات التي تضيفها أنت خارج السلسلة.

الفهم

سجل بيتكوين على السلسلة علني. يمكن تحليل السكربتات والعناوين الممكن تمثيلها والقيم والصلات بين المدخلات والمخرجات ومواقع المعاملات في الكتل. ليس لازمًا أن يظهر اسمك، لكن شراءً مرتبطًا بهويتك أو فاتورة منشورة أو عنوانًا شاركته قد يربطك بذلك السجل.

تعني الهوية المستعارة التعامل بمعرّفات لا تمثل بذاتها هويتك المدنية. أما إخفاء الهوية فيتطلب مجموعة وشروطًا يتعذر في ظلها تمييزك، ولا يتحقق بمجرد تثبيت تطبيق. الخصوصية مرتبطة بالسياق: المتجر يعرف دفعتك، ومنصة التداول قد تعرف سحبك، والخادم يعرف الاستعلامات، وقد يشاهد شخص أجهزتك.

افصل الوقائع عن الاستنتاجات. يمكن التحقق على السلسلة من عبارة «أُنفِق هذا المخرج في تلك المعاملة». أما «كل هذه المدخلات تخص الشخص نفسه» فقاعدة استدلالية قد تخطئ. قد تزيد معلومات الهوية من خارج السلسلة الثقة في فرضية دون تحويل كل تفسير إلى حقيقة مؤكدة.

تسهّل إعادة استخدام عنوان تجميع النشاط. وقد يربط جمع UTXOs من سياقات مختلفة تلك السياقات ببعضها. يكشف xpub نطاق مشاهدة أوسع من عنوان واحد. ومشاركة txid قد تعرض أيضًا مخرجات وروابط أخرى لم يكن المتلقي بحاجة إلى معرفتها.

التدريب

1. حدّد في معاملة افتراضية البيانات العلنية والوسوم التي أضفتها أنت.
2. أضف فاتورة باسم شخص وصف الصلة الجديدة التي ظهرت.
3. اكتب طلب دعم يتيح حل خطأ دون إدراج عنوان أو واصف أو رصيد.

أثبت فهمك

ميّز بين «هذا قابل للملاحظة» و«هذا استنتاج»، واشرح الدليل الذي لا يزال ناقصًا.

سؤال شائع

هل أصبح مجهول الهوية إن لم أستعمل عنوانًا مرتين قط؟ لا. يظل اختيار المدخلات والباقي والاستعلامات والأطراف المقابلة وغيرها من البيانات الوصفية مهمًا.

نقطة توقف

احتفظ بخريطة للمراقبين دون هويات حقيقية أو معاملات فعلية.

أي بيانات تتيح عادة مراقبة مجموعة العناوين التابعة لحساب؟

1. لون الأيقونة.
2. مفتاح xpub الخاص به ومعلومات اشتقاق كافية.
3. العلامة التجارية للكابل.

> **عرض الإجابة: مفتاح xpub الخاص به ومعلومات اشتقاق كافية.**
> المعلومات العامة الموسّعة حساسة للخصوصية حتى إن لم تأذن بالإنفاق بمفردها.

فصل السياقات وإدارة الباقي

الهدف

اتخاذ قرارات الإنفاق التي تتوافق مع مصدر الـ UTXOs الخاص بك

الفهم

ويبدأ الفصل بين السياقات قبل الدفع. يقرر ما إذا كان تلقي أي مبلغ يتعلق بالادخار أو النشاط المهني أو النفقات اليومية أو علاقة محددة. يحتفظ بهذه المعلومات على بطاقات خاصة حتى لا يمحيها الاختيار المستقبلي بسبب الجهل

علامة لا تفصل الترميز المخرجات. إذا كنت تنفق اثنين UTXOs من سياقات مختلفة، فإن المعاملة تنشر علاقتها. ويقلل عدد الدفعات الآجلة من المدخلات، ولكنه يزيد من الصلة بين الدفعات ال المخرجات الموحدة. القيام بذلك مع الرسوم يمكن أن يكون الانخفاض فعالاً و معاكساً لهدفك الخاص

التغيير هو مخرج جديد تحكمه نفس السياسة وليس "النقود الخفية". استخدامك اللاحق قد يمد علاقات سابقة. لا تقم بتحديد عنوان كتغيير لأنه يحمل مبلغاً غريباً؛ في أي استعراض فعلي، يجب على الجهاز أن يتحقق من انتمائه إلى محفظة.

تجنب تحويل الخصوصية إلى أنماط ميكانيكية للكميات أو الأوقات أو التحويلات المتكررة. ويمكن أيضاً التعرف على هذه الأنماط وتوليد المزيد من الرسوم. ويقيّم المعلومات التي يعرفها كل طرف والمعلومات الجديدة التي ستنشرها العملية المقترحة. لا تسلسل يحذف التاريخ المنشور بالفعل.

التدريب

1. وينشئ 5 UTXOs وهمية من ثلاث سياقات ويعد دفعا يستخدم أقل عدد من السياقات اللازمة.
2. حدّد التغير الناتج وقرّر كيفية وسمه.
3. يقارن التكلفة والتعرض لتثبيت كل المخرجات بدلاً من إبقاءها منفصلة.

أثبت فهمك

ويمكن أن تبرر الضم أو ترفضه لسبب محدد، دون تطبيق قاعدة مطلقة في جميع الحالات.

سؤال شائع

تحويل كل شيء إلى عنوان آخر لي يكسر التاريخ؟ لا. التحويل ينشر علاقة إضافية ويمكن أن يضيف تكلفة غير مُحلّة للتهديد

نقطة توقف

يحافظ على منطق المختبر وسياسة الاختيار المختارة

ما الأثر المحتمل لدمج الراتب والتبرعات في معاملة واحدة؟

1. إظهار صلة بين تلك المدخلات.
2. محو مصدرها العلني.
3. تحويلها إلى نقد مضمون الإخفاء للهوية.

> **عرض الإجابة: إظهار صلة بين تلك المدخلات.**
> قد يؤدي تقليل عدد مخرجات UTXO إلى زيادة الروابط القابلة للملاحظة.

خصوصية الشبكة وTor وVPN

الهدف

فصل خصوصية الاتصال عن الخصوصية عن السلسلة.

الفهم

الخادم المرجعي يمكن أن يربط الطلبات بوصلة. مزود الإنترنت الخاص بك يمكن أن يرى وجهات أو أنماط حسب النقل. VPN تنقل جزء من هذه الثقة إلى مشغل VPN؛ ولا تزيل المعلومات العامة من بيتكوين ولا تمنع حساباً محدداً من التعرف عليك.

يوجّه Tor حركة الاتصال عبر شبكة للحد من بعض الروابط بين المصدر والوجهة. لا يجعل عنوان بيتكوين خاصًا ولا يحمي تطبيقًا لا يمر اتصاله عبر Tor. لا يؤدي فتح Tor Browser تلقائيًا إلى تهيئة Desk أو Bitcoin Core أو جميع خدمات الحاسوب.

قبل أن تؤكد أن الاتصال محمي يجب أن تختبر مساره و تشكيله. ولا يفترض في هذا الأساس وجود مفتاح تبديل Tor مدمج في Desk. الوزع مع عقدة أو procsy يتطلب توجيهاً هندسياً والتحقق من الحركة الفعلية. أنت لا تخترع حقل الواجهة لأن محفظة آخر يحصل عليه.

وهناك أيضا تسرب من DNS، وتزامن الحسابات، ووصلات الكشافة، وخدمات الأسعار. ويمكن أن يحمي المخطط الاستفسارات المتعلقة بالرصيد وأن يستمر في الكشف عن النشاط عند فتح مستكشف عام. فهو يحدد نطاق كل تدبير والسلوك عند فشل الوصلة؛ ويتجنب التغييرات الصامتة على مورّد أقل خصوصية.

التدريب

1. قم برسم مسار الحاسوب، مزود التوصيل، بروكسي إن كان موجوداً، عقدة أو خدمة وشبكة بيتكوين.
2. يحدد من يتلقى المشورة ومن يرى هويتك التجارية.
3. أنه عقدة لا يجيب. يقرر بين التوقف أو تغيير المصدر صراحة مع العلم بالتعرض.

أثبت فهمك

يمكنك تفسير أي تهديد يقلل من تشكيلتك وما هو التهديد الذي لا يزال موجوداً

سؤال شائع

ﻎ Tor هل تضمن أن لا أحد يمكنه ربط الدفع معي؟ لا. الإختلافات، تحديد الهوية التجارية، الأنماط والأخطاء العملية يمكن أن تستمر في ربطها.

نقطة توقف

سجل نطاق التصميم، وليس إندبوانتس الخاصة أو كلمة المرور.

هل يُجبر فتح Tor Browser تطبيق Desk على الاستعلام عبر Tor؟

1. نعم، لأنهما على الحاسوب نفسه.
2. نعم إذا ظهرت الأيقونة.
3. لا، يجب ضبط مسار كل تطبيق والتحقق منه.

> **عرض الإجابة: لا، يجب ضبط مسار كل تطبيق والتحقق منه.**
> لا تنتقل حماية أحد التطبيقات تلقائيًا إلى سواه.

CoinJoin وPayjoin وحدودهما الحالية

الهدف

فهم أدوات التعاون دون أن ينسب إليها عدم الكشف عن هويتها أو عدم توافقها.

الفهم

CoinJoin يجمع مساهمات من عدة أشخاص في صفقة واحدة لعرقلة بعض الاستنتاجات بشأن المدخلات والمخرجات. ليس مرادفاً لتسليم العملات إلى موظفة حراسة تعد بإعادة عملات أخرى وتتطلب تصاميم مختلفة إعادة النظر في التنسيق، الحفظ، الرسوم، مقاومة المشاركين الخبيثين والمعالجة اللاحقة.

Payjoin يُدخل المدخلات من الدفع والمتلقي إلى دفع تعاوني، مما يضعف بعض الحثالات المملوكة ملكية مشتركة. وهو يتطلب دعماً متفقاً عليه في كلا الطرفين وبروتوكولاً محدداً. مادة للفهم التقني: لم يعتمد في المصادر المنقحة تدفق Payjoin أو CoinJoin متكامل وتشغيلي في Cuvex Desk.

يتغير التوافر والسياق القانوني. تسجّل وثائق Wasabi إغلاق منسّق zkSNACKs في 1 يونيو 2024، فلا يُدرّس زر قديم كأنه ضمان لخدمة قائمة اليوم. أعلنت وزارة العدل الأمريكية في 2025 إقرار مؤسسي Samourai بالذنب ثم الأحكام الصادرة عليهم. لا يجيز ذلك استنتاج أن كل تقنيات الخصوصية مخالفة للقانون في كل ولاية قضائية.

أداة واحدة يمكن أن تقلل من الإستنتاج وتترك أدوات أخرى سليمة. المصدر المحدد لا يختفي من سجلات أحد النظراء. الارتدادات اللاحقة، البيانات الوصفية وفشل مجموعة المشاركين قد تؤدي إلى تدهور الخصوصية. وعلاوة على ذلك، قد تطبق بعض الخدمات سياسات تجارية غير العملات التي لها تاريخ معين.

التدريب

1. يقارن بين معاملة جارية، ومعاملة تعاونية، وخدمة تستقبل الحفظ، دون تنفيذ معاملات فعلية.
2. لأداة محددة، ابحث عن نسخة، محفظة، حالة الخدمة، والوثائق الحالية قبل اقتراح استخدامها.
3. وهو يحدد المخاطر التقنية، والمخاطر من الحفظ والمخاطر القانونية المنفصلة. لا ينبغي أن يصمم المدرّس التهرب من الضوابط أو يعد بـ "أموال لا يمكن تعقبها".

أثبت فهمك

يمكنك تفسير ميزة محدودة، على الأقل اثنين من المخاطر أو المتطلبات لتقنية الخصوصية.

سؤال شائع

ن Cuvex تحتاج إلى مُضَبَغ لتخدم الحفظ خاصة؟ لا. البيانات، مفاتيح والاختيار والاختيار والانتخاب والاختيار UTXOs وهم يحلون بالفعل مخاطر محددة، دون أن يعدوا بإخفاء كامل.

نقطة توقف

يُنشئ أداة كـ "علم"، ليس كـ "توافق" بدون دليل.

أي عبارة يمكن الدفاع عنها؟

1. يضمن CoinJoin إخفاء الهوية دائمًا.
2. قد تصعّب تقنية تعاونية بعض الاستنتاجات ضمن متطلبات وحدود.
3. كل خدمة تسمّي نفسها خلاطًا تحتفظ بالحفظ الذاتي.

> **عرض الإجابة: قد تصعّب تقنية تعاونية بعض الاستنتاجات ضمن متطلبات وحدود.**
> تتوقف الخصائص على البروتوكول والتنفيذ والمشاركين والاستعمال اللاحق.

دروس من حوادث حقيقية

الهدف

استخلص من الحوادث الموثقة قرارات قابلة للتحقق دون مهاجمة المنافسين أو المبالغة في الحماية.

الفهم

تصف لائحة اتهام لوزارة العدل في 2023 بقضية Mt. Gox دخولًا غير مصرّح به إلى خوادم ومفاتيح واختفاء أموال العملاء بعده. إنها اتهامات لا حكم بالإدانة. اسأل في الحفظ من يسيطر فعليًا على المفاتيح وماذا يحدث عند تعثر الشركة.

في ديسمبر 2023 وثّقت Ledger في واقعة Ledger Connect Kit نشر نسخة خبيثة من مكتبة للتطبيقات اللامركزية بعد اختراق وصول موظف سابق. أصاب الحادث سلسلة توزيع البرمجيات وخدع مستخدمي DApps على EVM للتوقيع. لا يثبت كسر عتاد Ledger أو إجماع بيتكوين.

في فبراير 2025 نسب FBI سرقة أصول افتراضية بنحو 1.5 مليار دولار من Bybit إلى كوريا الشمالية. تعلّق الحادث بمنصة تداول وأصول من شبكات أخرى، ولا يُعرض ككسر لتشفير بيتكوين. تحقّق من قصد التوقيع ولا تدع عدة أشخاص يثقون عميانيًا بالشاشة نفسها.

في مايو 2025 أعلنت Coinbase سرقة بيانات عبر موظفي دعم تلقّوا رشى لتسهيل الهندسة الاجتماعية. وقالت إن كلمات المرور والمفاتيح الخاصة لم تنكشف. قد يعرف المحتال بيانات صحيحة ويظل محتالًا.

ينشر Bitcoin Core عيوب البرمجيات أيضًا. وصف CVE-2024-35202 إمكان إيقاف البرنامج عن بُعد في الإصدارات الأقدم من 25.0. التحقق من القواعد لا يغني عن صيانة البرنامج، ولا يدل التنبيه على سرقة مفاتيح.

في يناير 2026 أفادت The Register بانكشاف بيانات طلبات مشتري Ledger والاتصال بهم عبر Global-e، ونسبت تأكيدات إلى الشركتين. وبحسب تصريحاتهما لم تتأثر مفاتيح الاسترداد. قد يكشف الشراء أنك تملك جهازًا حتى إن لم يُخترق العتاد.

في أبريل 2026 أفادت The Record بالهجوم على Drift وتعليق الإيداع والسحب الذي أعلنته المنصة. يتعلق الأمر ببروتوكول تمويل لامركزي على Solana وليس بكسر بيتكوين. لا تعرض تقديرات الخسائر الأولية كأرقام نهائية أو إجراءات الاستعادة اللاحقة كضمان للرد.

التدريب

1. صنّف الحوادث بحسب الحفظ والواجهة أو التوزيع والبيانات الشخصية وبروتوكولات الشبكات الأخرى والتوافر.
2. اقترح لكل حادث تدبيرًا وقائيًا واذكر حدًا لذلك التدبير.
3. حاكِ مكالمة احتيالية: «أعرف ما اشتريت، انقل أموالك إلى هذا العنوان الآمن». أنهِ المكالمة وتحقق عبر قناة تبدأها أنت بنفسك.

أثبت فهمك

اشرح لماذا لا يثبت أي حادث أن علامة أخرى منيعة. لا يسند الدليل إلا نتيجة ضمن نطاق محدد.

سؤال شائع

هل هذه آخر الاختراقات كلها؟ لا. هذه أمثلة تحققت منها طبعة 17 نوفمبر 2026 وليست جردًا شاملًا أو رصدًا مباشرًا.

نقطة توقف

دوّن العادة التي ستغيّرها وكيف ستتحقق من استمرارك عليها.

يعرف المتصل تفاصيل شرائك ويطلب التحويل إلى «محفظة إنقاذ». ماذا يثبت علمه بالشراء؟

1. ربما حصل على معلومات مسرّبة، ولا يثبت ذلك هويته أو صحة العنوان.
2. أنه حتمًا من الدعم الشرعي.
3. أنه يجب مشاركة البذرة.

> **عرض الإجابة: ربما حصل على معلومات مسرّبة، ولا يثبت ذلك هويته أو صحة العنوان.**
> قد تُستعمل بيانات صحيحة لصنع احتيال مقنع.

إنشاء هوية الدردشة والتحقق من جهات الاتصال

الهدف

فعّل هوية دردشة بدون كشف مفتاح وتأكد من النظير.

الفهم

في Desk، يتم ربط دردشة النص المشفّر بواسطة مفتاح Chat تولد في Cuvex. على الرغم من أن تمثيله قد يبدو كـ xpub، فهو سري ولا ينبغي معاملته كـ مفتاح عام من حساب WOW. الـ المدرّس لا تحتاج أبداً لقراءتها أو رؤيتها على الـ QR

ويميز التدفق بين الاسم المستعار الجديد والانتقال أو الاستعادة من اسم موجود. وفي إطار التنفيذ المنقح، يتم اختيار الملف المتنقل iOS أو Android ذي الصلة، لأن الهويات التاريخية المشتقة لا يمكن تبادلها بديهية. والبيئات DEV والإنتاج هي بيئات منفصلة: تغيير البيئة لا تهاجر المحادثات أو التسميات التلقائية.

أضف اسم مستعار لا يُثبت الهوية. فحص البصمة عبر قناة مستقلة وموثقة. إذا كان التطبيق يقدم أسئلة التعرف، فإنه يستخدم معلومات غير علنية ويتجنب الإجابات التي تكشف كلمة المرور. ويمكن تقليد صوت معروف؛ وفي حالات الخطر يجمع بين أساليب متفق عليها مسبقا.

إذا تغيّر هوية الاتصال، توقف الدفعات وتنسيق حتى يتم حلّها. قد يكون تعافياً مشروعاً أو استبدالاً خبيثاً الـ التشفير من النهاية إلى النهاية يحمي قناة وفقاً لبروتوكولها وتنفيذها لكنه لا يبين من يستخدم الجهاز على الجانب الآخر

التدريب

1. في بيئة اختبار، يفسر تدفق إنشاء أو استرجاع دون تقديم مفتاح chat.
2. اضف اتصال معملي و وافق على فحص بصمة عبر قناة أخرى
3. يُحدّد تغيير الهوية. عرف كيف ستؤكد التغيير قبل أن تدفع

أثبت فهمك

يمكنك تمييز الأسماء المستعارة، البصمة العامة، مفتاح تشات السرية والثقة البشرية في شخص واحد.

سؤال شائع

هل اسم مستعار قديم يضمن أنه نفس الشخص؟ لا. ينبغي التحقق من استمرارية وتغير مفاتيح وفقاً للتدفق.

نقطة توقف

سجل فقط "صلة الاختبار المتحقق منها" و الطريقة، بدون مفاتيح أو أسئلة خاصة.

سلسلة اسمها «مفتاح الدردشة» تشبه xpub. كيف تُعامل في Desk؟

1. كمعلومة تُنشر في المنتديات.
2. كسرّ لاستعادة الهوية.
3. كعنوان لاستقبال البيتكوين.

> **عرض الإجابة: كسرّ لاستعادة الهوية.**
> المظهر لا يحدد سرية البيانات أو غرضها.

طلب مبالغ بالساتوشي ودفعها من الدردشة

الهدف

الانتقال من محادثة إلى دفع دون فقدان مراجعة أو سياق.

الفهم

ويسمح الدردشة بطلب العنوان، والرد على عنوان الاستقبال، والمطالبة بالدفع، وفتح عملية الإعداد من حساب WOW. الحفاظ على السياق في القناة يقلل من الأخطاء في نسخ المعلومات بين التطبيقات، لكنه لا يحول كل رسالة إلى أمر موثق للنفقات.

قبل الرد أو الدفع، راجع الاتصالمتحقق منه، الشبكة، المبلغ والطلب الأصلي. واحتفظت استمارة الاشتراك بالاختيار UTXOs والرسم. إذا طلبت الرسالة مبلغاً واختارت "ارسل المجموع"، يمكن أن يكون الصافي بعد الرسوم أقل؛ وينبغي تحديده كدفعة جزئية عند الاقتضاء.

الرخصة تبقى في Cuvex. الدردشة تنقل النية والتنسيق؛ ليس لديك تصريح للتوقيع تلقائياً. ويجب أن يميز تأكيد الدفع المرسل إلى جهة الاتصال بين تلقي رسالة تفيد بوجود معاملة مؤكدة. ويتحقق المتلقي من حسابه الخاص أو مصدره.

تظل الروابط الخارجية ورموز QR المرفقة والعناوين غير موثوق بها حتى التحقق منها. قد يفتح «العرض في Mempool» خدمة خارجية ويكشف استعلامك. إن كانت سياستك تعتمد عقدتك الخاصة ففضّل التحقق المتوافق في WOW وقيّم أي اتصال بخدمات عامة.

التدريب

1. يمثل دورين: المتلقي يطلب 50.000 sat؛ المدفع يجهز غير منشور.
2. يُحَوَّل رصيد غير متوافر صافيه 48.000 sat. ما الذي يفسر الموافقة والتوفيق؟ لا يوجد شيء غير الدفع الجزئي.
3. يغير الشبكة عمداً في رسالة اختبار ويوقف التدفق

أثبت فهمك

يمكنك تتبع العلاقة بين الطلب والعنوان والمسودة والتوقيع والتأكيد دون أن تقصرها على "المحادثة تقول OK".

سؤال شائع

هل إرسال شاشات الدردشة يعني استخدام Lightning؟ لا. تدفق WOW الموثق يُعد الدفع بيتكوين سلسلة. كلمة "ساتس" تعبر عن وحدة واحدة وليس شبكة نقل

نقطة توقف

ألغ مشروع المختبر أو سجل الحالة لا تنشر لإثبات الواجهة

تلقّيت تأكيدًا في الدردشة. ما الفحص الحاسم لإثبات الاستلام؟

1. أن تكون أيقونة الرسالة خضراء.
2. أن يقول الطرف الآخر «مؤكد».
3. التحقق من المعاملة ومخرجاتها على الشبكة بالمصدر المناسب.

> **عرض الإجابة: التحقق من المعاملة ومخرجاتها على الشبكة بالمصدر المناسب.**
> حالة الرسالة لا تساوي حالة المعاملة.

مشاركة النصوص المشفّرة عن دراية

الهدف

فهم ما يعني تسليم نسخة مشفرة لشخص آخر.

الفهم

المشاركة النص المشفّر يرسل نسخة من الجسم التشفير. لا يرسل بالضرورة بيتكوين أو يدمج في نفسه الموقّع جديد. وإذا حصل المتلقي أيضاً على وسائل فك الوصايا الكافية، فإنه يستطيع الوصول إلى المحتوى وفقاً للمخطط؛ ولذلك يجب أن يتم تحديد القدرة التي تنقلها مسبقاً.

التشفير من الطرف إلى الطرف من الدردشة والتشفير من الأرشيف يحمي طبقات مختلفة. وبعد تنزيلها، يمكن للمتلقي أن يحتفظ بالشيء خارج الدردشة. حذف رسالتك أو سجلك المحلي لا يضمن سحب جميع النسخ كلمة المرور مشترك في نفس القناة يمكن أن يركز المكونات في مسار واحد.

قبل الإرسال، تحقق من الهوية والشكل والغرض. إذا كان التطبيق يسمح بربط النص المشفّر المستلمة، فإن ذلك ينظم نسخة، لا تثبت أن فك التشفير آمن أي ملف. لا تستخدم ملحقات تتطلب إدخال بذرة الاسترداد أو كلمة المرور في صفحة خارجية.

ويتطلب التعافي اتفاقاً تشغيلياً: من يحتفظ بكل عنصر، ومن يستطيع فتحه، وكيف يتم اكتشاف التعرض، وكيف يتغير الحفظ عند انتهاء العلاقة. عادة ما يكون هناك عنوان مصدق عليه يكفي للدفع الجاري لا حاجة لمشاركة الـ النص المشفّر

التدريب

1. صمم نقل نص تعليمي التشفير إلى اتصال مختبري.
2. سجل ما تعرفه وما الذي يمكن أن يفعله المستلم قبل وبعد معرفة كلمة المرور.
3. يَحْدثُ العلاقةَ تَنتهي. يوضح لماذا حذف الرسالة لا يبطل النسخة أو مفاتيح.

أثبت فهمك

يمكنك التمييز بين "فقراء البيانات" و"فقمت الوصول إلى سر" و"وقّعت على نفقات".

سؤال شائع

أي ملف التشفير يمكن أن يتداول بدون أي عواقب؟ يمكن أن يكشف عن البيانات الوصفية، ويمكن أن ييسر محاولات كلمة المرور ويبقي إلى أجل غير مسمى. يقيّم الحاجة إلى المشاركة.

نقطة توقف

لا تُبقي مُنقِلات الحفظ في الوقت الراهن. سجل فقط نهاية التمرين

هل إرسال نص مشفّر عبر الدردشة يعني إرسال بيتكوين؟

1. لا، إنه ينقل عنصرًا لمحتواه وإمكانية الوصول إليه نطاق آخر.
2. نعم إذا انتهى اسم الملف بـ .bin.
3. يفعّل محفظة متعددة التوقيعات جديدة تلقائيًا.

> **عرض الإجابة: لا، إنه ينقل عنصرًا لمحتواه وإمكانية الوصول إليه نطاق آخر.**
> نقل الأسرار وتحريك مخرجات UTXO عمليتان مختلفتان.

استعادة الدردشة وفهم بياناتها الوصفية

الهدف

تخطيط تغيير المعدات وفصل استعادة الهوية والرسائل.

الفهم

تشير Desk إلى أن التاريخ والجلسات يتم تسجيلها محلياً ولا تشكل جزءاً من نسختها العالمية. ويسمح القانون مفتاح Chat باستعادة الهوية؛ ولا يضمن استعادة جميع المحادثات القديمة. ويشمل هذا البرنامج بيانات وإجراءات لتفعيله غير مكتملة، وصيانة مفاتيح واستعادة محلية عندما توجد مواد متوافقة.

كل اسم مستعار يجب أن يستخدم في جهاز واحد في نفس الوقت وفقاً لدليل الأساس المنقح. لا تشغّلها في وقت واحد في فريقين لـ "اعتماد المزامنة" إذا لم يكن هذا الاستخدام مدعوماً. ويجب أن يتبع النقل الإجراءات وأن يتحقق من استمرارية الاتصالات.

"لم يبت فيه"، و "قبل بواسطة الخادم"، و"استقبل" و "لم يتمكن من فعل فك التشفير"، تصف مراحل مختلفة. شحنة غير مؤكدة لا تُعاد تلقائياً إلى الأعمى: أولاً يجب أن نُحلّ إذا وصلت. إذا لم يكن هناك مفتاح جلسة أو تغيير في الهوية، فإن الاحتفاظ بالرسالة المعلقة لا يعني قراءة الرسالة.

ولا يخفي المحتوى التشفير بالضرورة التوقيت أو الحجم أو علاقات التسليم أو الأسماء المستعارة أو بيانات الاتصال بالنسبة لجميع النظم المعنية. في الصوت يحدث شيء مشابه : التشفير النقل لا يحول الإتصالتقليدي إلى قناة مناسبة للسرية يستخدم الحد الأدنى من البيانات اللازمة للتعلم وحل الحالات.

التدريب

1. قم بفقدان الـ PC وشرح ما الذي يسترجعه كل مادة متاحة
2. يصنف بيانات الرسائل ويقرر متى لا يجب إرسال طلب الدفع.
3. قم بإعداد إشعار بتغيير المعدات التي يمكن أن يتحقق منها جهات الاتصال عبر قناة مستقلة.

أثبت فهمك

يمكنك أن تشرح أي محادثة ستضيع وأي هوية يمكن استعادتها دون أن تعدك باستعادة نسخة احتياطية لا يغطي.

سؤال شائع

احذف متصفح محلي محذف رسائل أيضا في الطرف الآخر؟ لا يجب أن تتحملي ذلك ويمكن للمتلقي أن يحتفظ بالرسائل والمحفوظات بصورة مستقلة.

نقطة توقف

يحتفظ بخطة نقل مع أسماء الحقول الفارغة بدون مفتاح تشات

بحسب الدليل المراجَع، ما الذي يتيحه مفتاح الدردشة بمفرده؟

1. كل المحادثات التاريخية على أي حاسوب.
2. استعادة الهوية عبر المسار المتوافق، لا كل الرسائل القديمة.
3. الوصول تلقائيًا إلى مفاتيح بيتكوين لدى جهات الاتصال.

> **عرض الإجابة: استعادة الهوية عبر المسار المتوافق، لا كل الرسائل القديمة.**
> استعادة الهوية واستعادة الأرشيف وظيفتان مختلفتان.

الإعدادات اليومية ومراجعة الأذونات

الهدف

التحكم ببارامترات Desk دون الخلط بين الحماية والحماية.

الفهم

يعرض Desk موضوع ليلة أو يوم أو نظام؛ تزامن تلقائي وفترات زمنية من 3 أو 5 دقيقة؛ أصوات المعاملات؛ خلفية الدردشة؛ اللغة والعملة المرجعية. وهذه الأفضليات تغير طريقة العرض أو تواتر الاستعلامات. لا تعدل توقيع بيتكوين أو تضيف مجهول الهوية.

التشكيلة الأمنية المنقحة تسمح بالإغلاق عن طريق القفل، والإغلاق عند الإنتقال إلى الخلف، والتأخر الأقصى بعد الفشل، والحذف الاختياري. والفترة المسموح بها في مخطط الخمول هي 30 إلى 86.400 ثانية؛ أما الواجهة فيمكن أن تقدم خيارات أكثر ضيقاً. القيم الافتراضية يجب أن تقرأ من النسخة التي تقوم بتنفيذها، لا يفترضها درجة مسجلة.

ادماج الوصلات بيتكوين: يفتح طلب لفتح الفتح، واختيار الحساب وتنقيحه. لا يسمح بالدفع التلقائي في Linux، الدليل التفاضلي للتركيب المتكامل و AppImage لتسجيل الوصلات. فاتورة Lightning يتطلب تدفقاً متوافقاً مختلفاً؛ ولا يحل عن طريق الإعلان عن Desk تطبيقاً مبدئياً.

ويمكن الاستعانة بمصادر خارجية في الموقع السعر المعروض والرسم البياني للأسعار ووصلات المعلومات. وظيفتها معلوماتية وليست إشارة شراء راجع التاريخ و المصدر قبل استخدام البيانات لترجمة المبالغ. الطريقة المظلمة أو النافذة الصغيرة لا يجب أن تخفي الأزرار النهائية أو الاتجاه أو الرسم؛ إذا حدث ذلك، توقف والإبلاغ عن مشكلة الهندسة.

التدريب

1. تعديل المظهر و الإغلاق في مخزن التعلم -أنّه يمكنك العودة إلى الداخل .
2. تحقق من أي الآلات النشطة: ضبط التوقيت، الأصوات، فحص البرنامج الثابت ليست هي نفسها.
3. افتح طلب افتراضي لوصلة بيتكوين: ثم ألغي قبل إعداد أي عملية فعلية.

أثبت فهمك

يمكنك تفسير تأثير كل تعديل و تحديد ما ينطوي على مشاورات أو أفعال حساسة.

سؤال شائع

القياسات الحيوية من PC يحل محل نسختي من الإسترجاع؟ لا. ويمكن أن يعتمد على المعدات والمخزن الآمن للنظام. حافظ على تعافي مستقل

نقطة توقف

اقفل Desk و سجل فقط ما هي أفضلياتك التي غيرتها

ماذا يتغير عند اختيار المزامنة كل ثلاث دقائق؟

1. وتيرة الاستعلام المقصودة عندما تعمل الوظيفة.
2. سياسة التوقيع على السلسلة.
3. بذرة الجهاز.

> **عرض الإجابة: وتيرة الاستعلام المقصودة عندما تعمل الوظيفة.**
> هذا تفضيل تشغيلي لا تغيير في الحفظ.

تصميم محفظة متعددة التوقيعات

الهدف

اختر عتبة تصمد أمام سيناريوهات فقد المفاتيح وانكشافها المعقولة.

الفهم

في سياسة M من N، يرمز N إلى عدد المشاركين ذوي المفاتيح المختلفة وM إلى عدد التوقيعات المطلوبة. تتحمل سياسة 2 من 3 فقد إتاحة مفتاح واحد، لكن انكشاف مفتاحين يتيح الإذن بالإنفاق. إذا حُفظت البذور الثلاث معًا أو تعرضت لمصدر خطر واحد قلّ استقلالها.

يستخدم ملف Cuvex متعدد التوقيعات المراجَع P2WSH الأصلي مع sortedmulti واشتقاق BIP48. تدعم بنية Original حتى ستة مفاتيح سياسة وبنية BIT حتى خمسة عشر. عند اشتراكهما تُراعى حدود المشارك الأقل قدرة والحجم الفعلي لوسيلة النقل. الحد البنيوي لا يضمن اتساع الوسيط لسياسة كثيرة المفاتيح والمدخلات.

يدعم التطبيق عتبات تلتزم بنسب السياسة. سياسة 1 من N لا تتطلب تعاونًا للإنفاق ويعرض البرنامج الثابت تحذيرات محددة بشأن هذا الخطر. زيادة العدد تزيد أيضًا التنسيق والكلفة ومواد الاستعادة واحتمال تعذّر الوصول.

MuSig2 آلية أخرى لتجميع توقيعات Schnorr، ونظامه الأساسي N من N وليس عتبة اعتباطية مثل 3 من 5. لم تُنفذ البرامج الثابتة Final المدروسة توقيع مدخلات Taproot أو MuSig2 أو Miniscript. قبول مستفيد P2TR لا يثبت إمكان التوقيع من محفظة Taproot.

التدريب

1. صمم 2 من 3 خيالي مع مخاطر منفصلة لكل مشارك.
2. يَحْملُ فقدان a مفتاح و إلتزام a. يوضح ما يمكن وما لا يمكن القيام به.
3. افحص حدود النموذج قبل ان تختار سياسة اكبر

أثبت فهمك

يمكنك التعبير عن تحمل الخسارة، وعتبة الهجوم، وأجزاء مشتركة من تصميمك.

سؤال شائع

"الـ" "التوقيع المتعدد يتطلب من الناس أن يعرفوا بذرة الاسترداد من الآخرين؟ لا. والهدف من ذلك هو الحفاظ على قدرات كل منها الخاصة وتبادل المعلومات العامة اللازمة لصياغة السياسة واسترجاعها.

نقطة توقف

حافظ على التصميم مع المشاركين الخياليين ومسؤولياتهم.

في سياسة 2 من 3 بمفاتيح مستقلة، كم مفتاحًا خاصًا يكفي للإذن بإنفاق صالح؟

1. واحد.
2. اثنان.
3. الثلاثة دائمًا.

> **عرض الإجابة: اثنان.**
> تتطلب العتبة مفتاحين ويلزم أيضًا استيفاء بقية الشروط والفحوص.

إنشاء الدعوات وتقديم المفاتيح

الهدف

بناء سياسة مع مشاركين تم التحقق منهم دون مشاركة بذرة الاسترداد.

الفهم

ويختار المبدع اسماً، وشبكة، وM، وN، واتصالات، ومعلومات عامة خاصة به، وشروطاً تشغيلية للدعوة. وفي المخطط المنقح، تُقبل شبكات mainnet وregtest لهذا التدفق، من 2 إلى 15 المشاركين قبل تطبيق حدود الجهاز، وانتهاء الصلاحية التشغيلية من 1 إلى 720 ساعة. لا تستخدم هذه الحدود كإذن لتجاوز اختبار القدرة

يراجع كل مشارك الدعوة ويقبلها أو يرفضها، ويقدم مفتاحه العام الموسّع مع البصمة ومسار BIP48 عبر الإجراء المتوافق. لا يقدّم بذرة أو مفتاحًا خاصًا أو عنوانًا منفردًا أو واصف محفظة أخرى بأكمله. قد ينتج المفتاح ذو السياق الخاطئ سياسة مختلفة ولو بدا xpub صالحًا.

المُنشئ يُنسّق، لا يحلّ محلّ المصادقة لكل الموقّع. وقبل الحصول على التمويل، يجب أن يكون الجميع قادرين على إعادة البناء والتحقق من نفس البارامترات ومن التوجيه الرقابي. لا يعني الاتصالمُقبَول على الدردشة الموافقة التلقائية على أي سياسة يُرسلها.

انتهاء صلاحية الدعوة هو قاعدة تنسيق التطبيق. لا يغيّر في حدّ ذاته a مُموّل مُمَوّل مِن قبل مُمْتَلَف مُمَّل. لا يُحذف التوقيعات مُخزّنة مِن قِبل أشخاص آخرين، ولا يعمل كـ temelock من الإجماع. وإلغاء اقتراح وسحب أموال من سياسة قائمة هما إجراءان مختلفان.

التدريب

1. في المختبرات regtest أُعد، لإنشاء مقترح 2 لا 3 مع اتصالات اختبارية
2. إنها تمثل قبولاً ورفضاً ومدخلاً بشبكة خاطئة. تأكد من أن الأخير يتوقف.
3. يرجى ذكر البيانات التي يحتفظ بها الجميع قبل تمويلها: الشبكة، العتبة، مفتاح عام، المصدر، الكتابة، العنوان المثبت.

أثبت فهمك

يمكنك التعرف على دعوة ناقصة وشرح الموافقة التي لم تُقبل بدون إفتراض لوجود الدردشة.

سؤال شائع

هل تاريخ الاستحقاق يجعل من المستحيل إنفاق المال بعد ذلك؟ ليس كحقل دعوة. فرض قيد مؤقت على بيتكوين يتطلب شروطاً من البرمجه أو تعامل محدده و دعم حقيقي

نقطة توقف

احفظ معرِف تعليم المقترح والموافقة المعلقة.

لتقديم مساهمتك في التوقيع المتعدد، ماذا يطلب المسار الموثق؟

1. بذور جميع المشاركين.
2. أي عنوان استلام.
3. مفتاحك العام الموسّع مع بصمة ومصدر اشتقاق متوافق مع BIP48.

> **عرض الإجابة: مفتاحك العام الموسّع مع بصمة ومصدر اشتقاق متوافق مع BIP48**.
> تتيح المواد العامة الصحيحة بناء السياسة دون كشف المفاتيح الخاصة.

التحقق من السياسات عبر Mirror بأي ترتيب

الهدف

قارن الحقول كاملةً وافهم بدقة ما تثبته النتيجة.

الفهم

يعرض التحقق المستقل العتبة والشبكة وملف التعريف وSIGHASH ومعرّف السياسة والعنوان الأول وموضع المستخدم وبيانات كل مشارك. وهو فحص للنية والاتساق. لا يفترض أن الجهاز سجّل السياسة بصورة دائمة، فالنطاق الموثق للفحص يقتصر على «هذه المراجعة».

في Mirror 12.12 يمكنك البدء بقراءة QR من Cuvex أو من Desk واختيار أي بيان. لا يلزم البدء بالخطوة 1 أو مسح كل الرموز أو اتّباع ترتيب معيّن. إذا راجعت نصًا يدويًا دون مسحه فلا يضع Mirror علامة تحقق عليه.

يعرض المقارن النص الحرفي الكامل. تُحسب المسافات وفواصل الأسطر وحالة الأحرف واختلافات Unicode. تعني «متطابق» أن قيمتي الزوج متساويتان، ولا توثّق المصدر أو تثبت انتماءهما إلى السياسة ذاتها أو تفعّل المحفظة. تظل الموافقة النهائية والرد المرتبط بها ضمن مسار Cuvex وDesk.

تحتوي رموز QR الحالية في Desk على القيمة وحدها دون رقم ترتيب أو جلسة. لذلك لا يستطيع Mirror استنتاج الخطوة دائمًا. يضيف خيار «تحديد خطوة Desk» سياقًا يدويًا يجب عرضه على أنه كذلك. مع N مشاركين تضم الخريطة الموثقة 7 + 4N حقلًا: البصمة عند 4k+8، والمسار عند 4k+9، وxpub عند 4k+10، ومعرّف المفتاح عند 4k+11، وتبدأ k من الصفر. عندما N=2 تكون الخطوة 15 معرّف المفتاح الثاني ويمكن مقارنتها أولًا.

التدريب

1. استخدم بيانات اصطناعية وقارن أولًا معرّفًا موسومًا بالخطوة 15، ثم الشبكة والعتبة.
2. أدخل اختلافًا من حرف واحد. تحقّق من ظهور «غير متطابق»، وابدأ زوجًا آخر دون ترحيل النتيجة السابقة.
3. قارن «2 / 3» واشرح لماذا لا يخبرك النص دائمًا إن كان يعبّر عن العتبة أم موقع المستخدم.

أثبت فهمك

صف الحقل الذي تحققت منه وكيف حددت سياقه وما ينتظر الموافقة. لا تعتبر التطابق الجزئي موافقة شاملة.

سؤال شائع

هل عليّ مسح جميع رموز QR لمتابعة التعلّم؟ لا. المقارنة اختيارية الترتيب والنطاق. وتظل فحوص جهاز التوقيع وأذوناته الإلزامية ضمن مسارها الخاص.

نقطة توقف

أغلق المقارن. وفق التصميم الذي روجع يجب محو القيم عند الخروج أو الانتقال إلى الخلفية.

يقارن Mirror رمزي QR للخطوة 15 ويعرض «متطابق». ماذا يُثبت ذلك؟

1. التطابق الحرفي لقيمتي الزوج، ضمن السياق الذي عُرف أو حُدّد يدويًا.
2. الموافقة على السياسة بكاملها.
3. توثيق مصدر رمزي QR.

> **عرض الإجابة: التطابق الحرفي لقيمتي الزوج، ضمن السياق الذي عُرف أو حُدّد يدويًا.**
> لا تحل المقارنة محل المصادقة أو المراجعة الشاملة أو رد جهاز التوقيع.

تنسيق التوقيعات ونشر معاملة متعددة التوقيعات

الهدف

أن تأخذ اقتراحاً بعتبة التوقيعات دون فقدان النية أو السيطرة.

الفهم

عملية التوقيع المتعدد محددة المدخلات، المستلم، القيمة، التعريفة، الاستبدال، ومذكرات التشغيل. يمكن للمنشئ أن يطلب التوقيعات من المشاركين المتوافقين. كل الموقّع يراجع بنفسه الشبكة، السياسة، المدخلات، جميع المخرجات و الرسم قبل أن يأذن بإستخدام جهازه.

التوقيع الجزئي لا يحرك الأموال بحد ذاتها في حالة عدم وجود العتبة. وعندما يتحقق ذلك، يمكن للمنسق أن يجمع وينتهي وفقاً للتدفق. تقارير المشاركين الآخرين أو المنسق هي معلومات تنسيقية وليست تحقق محلي قمت به. يجب أن يميز التطبيق هذه المصادر.

وتوفر القاعدة إعادة التوطين، وتلقي التوقيع، والتبليغ، والرفض، ونقل التنسيق. أي نقل لا يُغيّر الـ مفاتيح أو عتبة السلسلة. وينبغي أن يكون الرد المتحفظ مرتبطا بالطلب والموجز الفعلي المستخدم؛ ولا تُختار سياسة أخرى لأنها مماثلة أو أنها أول سياسة في القائمة.

وإذا قام أحد بتعديل المستلم أو الشروط ذات الصلة، ينبغي إعادة النظر في اقتراح جديد والحصول على التوقيعات المناسبة. "لا تضبط" باليد PSBT بحذف بيانات الأمان حتى تصبح NFC. تتطلب الـ "بروفيدوار" تحديد المواصفات والتثبتات المتوافقة مع حدود الـ المدخلات والمخرجات والحجم.

وقبل النشر، يتحقق من أن العملية هي العملية المتفق عليها وأنه لا توجد نسخة منشورة بالفعل. ثمّ يَتْبعُ التأكيدات مِنْ المصدرِ المختارِ. الرفض في تطبيقك لا يلغي تلقائيا التوقيعات أن الآخرين احتفظوا بالفعل أو يمنع أي إجراء يتفق مع العتبة المتبقية.

التدريب

1. مثّل سياسة 2 من 3 بثلاثة أدوار افتراضية: يوقّع الأول ويرفض الثاني ويطلب الثالث توضيحًا.
2. غيّر عنوان دفع الأدلة وشرح سبب عدم إعادة استخدام الموافقة الشفوية السابقة.
3. يقوم بإختبار تهمة فاشلة بعد حفظ التوقيع. استعاد نفس الوظيفة، دون تكرار الدفع أو تغيير في المواصفات.

أثبت فهمك

يمكنك تحديد من ينسق، ومن يوقع، ومن ينتهي، وأي دليل على كل خطوة.

سؤال شائع

هل تساوي رسالتا «OK» في الدردشة توقيعين؟ لا. تُستوفى العتبة بأذونات تشفيرية صالحة وفق السياسة، لا بالرسائل.

نقطة توقف

سجل الحالة، التوقيعات معلّقة و التالية مسؤولة بدون محتوى خاص

لعملية 2 من 3 توقيع صحيح ورسالتان تقولان «موافق». هل اكتملت العتبة؟

1. نعم لمشاركة ثلاثة.
2. لا، يلزم توقيع تشفيري صحيح آخر.
3. نعم إذا أعلن المنسّق ذلك.

> **عرض الإجابة: لا، يلزم توقيع تشفيري صحيح آخر.**
> الموافقة في المحادثة والتوقيع الصحيح دليلان مختلفان.

استعادة محفظة متعددة التوقيعات وتغييرها

الهدف

استعادة السياسة والتخطيط لفقدان المشاركين أو استبدالهم.

الفهم

ويتطلب الانتعاش فئتين: البيانات التي تعيد بناء السياسات والقدرات الخاصة الكافية للإنفاق. نسخة من السياسة مع xpubs يمكن أن تكشف تاريخاً بدون إدراج بذرة الاسترداد. نسخة مشفرة تضيف حماية إلى الملف، لكنها تتطلب الاحتفاظ بـ كلمة المرور. لا يثبت امتداد.cuvexms في حد ذاته أنه مشفر: ويجب التحقق من الشكل والتصدير المحدد.

في Desk 9.21، يطلب الاستعادة مفتاح عام واسعة النطاق من قبل المشارك الذي يحمل بصمة وطريق BIP48 مصدرة من جهازه. اعترف بقراءة الـ WebCam أو Mirror للتدفق المتوافق. لا تستبدل هذه المساهمة بـ عنوان الاستقبال أو ترسل الـ بذرة الاسترداد إلى الدعم.

إذا فقدت مفتاح في 2 من 3، يمكنك الاحتفاظ بقدرة على الإنفاق. لا تزالسياسة السابقة هي نفسها: من أجل سحب أحد المشاركين فعلياً ووضع سياسات جديدة مفاتيح، عادة ما يتم وضع سياسة جديدة ونقل الأموال مع التراخيص اللازمة. غيّر اسم مستعار أو أزل محفظة من Desk لا يُعدّل UTXOs الموجود.

يجب أن تسمح النسخ بإعادة بناء كل فرع واكتشاف التاريخ. حفظ الأرقام القياسية، الطلبات الصادرة والسياق اللازم لعدم إعادة استخدام العناوين أو تفسير محفظة فارغ لمسح غير كامل. ولا بد من أن يكون تجديد واستئناف عملية معلقة متمشياً مع الصورة التي خُفِّفت عند إنشاء العملية.

التدريب

1. وتصدِّر وتصلح سياسة مختبرية باستخدام الوظيفة الموثَّقة. تحقق من الشبكة و العنوان المعروف.
2. يُحَوِّل خسارة أحد المشاركين ويُعِدُّ خطة تناوب، دون نقل أموال حقيقية.
3. خسارة تحت العتبة. اعترف بأنّه لا يستطيع صنع الـ التوقيعات المفقود أو الذكاء الاصطناعي

أثبت فهمك

يمكنك استعادة مسرح الأدلة و التمييز بين استعادة المعلومات عن تغيير السيطرة على العملات

سؤال شائع

أتخلص من التوقيع المتعدد في Desk تعطيل محفظة للجميع؟ لا. يزيل الحالة المحلية وفقاً للتدفق. ويمكن أن يظل الأفراد الآخرون والنسخ الأخرى يحتفظون بقدرات تتفق مع السياسة.

نقطة توقف

يحتفظ بنسخة مثبتة وخطة خاصة؛ يسجل في المسار النتيجة فقط.

تريد إخراج شخص من سياسة تضم أموالًا. هل يكفي حذف اسمه من Desk؟

1. نعم.
2. نعم إن حذفت الدردشة أيضًا.
3. لا، يجب التخطيط لسياسة جديدة ونقل الأموال بإذن عند الاقتضاء.

> **عرض الإجابة: لا، يجب التخطيط لسياسة جديدة ونقل الأموال بإذن عند الاقتضاء.**
> لا تتغير سكربتات مخرجات UTXO القائمة بتعديل السجلات المحلية.

تحديث البرنامج الثابت وفق خطوات مدروسة

الهدف

إعداد تحديث متوافق والتحقق من نتيجته في الجهاز.

الفهم

تحديث يغيّر البرمجيات الثقة. التحقق من النموذج، وتنقيح العتاد، والنسخة، ومصدر وآلية توثيق الصانع. ولا يستعاض عن التحقق من صحة التوقيع والتوافق بتفريغ كامل أو قيمة التجزئة مساو لصفحة واحدة. لم تقم أبداً بتركيب تطبيق البرنامج الثابت بدون توقيع موجه للمهندس كما لو كان منشوراً للزبائن

Original تحديث Bluetooth في التدفق الموثق. يستخدم BIT USB-C. ويتضمن Mirror جولات للاستعداد والنقل المتوافقين. لا تعد بأن تركيبة معينة من PC، الهاتف و الجهاز تعمل حتى تكمل القبول المادي لذلك التركيب. إن الأثر التاريخي لتحديث Original في Windows يتطلب تشخيصاً محدداً؛ ولا يمكن حله عن طريق افتراض نجاح 99 في المائة.

قبل البدء، تحقق من نسخة احتياطية قابلة للاسترداد، تغذية مستقرة، وغياب عمليات أخرى. جهز الملف الرسمي أو نسخة تم التحقق منها مسبقاً وفقاً للطب. أثناء الشحن، الفرق، النقل، التصديق، التركيب، إعادة التشغيل، التحقق من النسخة. البار ليس اختبار نهائي.

وفي نهاية العملية، تحقق من الصورة المرئية للمعدات وسجل التاريخ والنتائج. فهرس التوافق لـ Desk لا يقيس عن بعد البرنامج الثابت: trocumentwareAttttestation يبقى ملفقا. انتقِ أداء ملفّ لا يُؤثّر أيّ بَعْض من هو في الواقع مثبت. إذا فشل التحديث، يتبع الاستعادة الموثقة، ويحافظ على المرحلة والخطأ بدون فصل عمياء في مرحلة حرجة.

التدريب

1. افحص قائمة الإعداد بدون البدء في تحديث حقيقي خلالاختبار
2. ضبط البيانات و شرح لِمَ نقل و موصّل مختلفان.
3. اضبط تقرير فشل افتراضي لـ 99% مع نموذج، نسخة، نظام، مرحلة و رسالة نهائية.

أثبت فهمك

يمكنك تحديد الجهاز المناسب، النقل والمعيار النهائي للنجاح.

سؤال شائع

هل يجب أن أُحدّث فقط لإخفاء خطأ Desk؟ أولاً، تحديد المصدر. وقد يتطلب عدم التوافق في القائمة تصحيح Desk والاحتفاظ بالالبرنامج الثابت المصادق عليه.

نقطة توقف

التحديث الحقيقي يتوقف فقط في حالة محددة آمنة من الإجراءات، وليس في نهاية المكالمة.

ماذا يبيّن كتالوج Desk الصريح بمفرده؟

1. مراجع التوافق المدعومة دون قياس البرنامج الثابت المثبت عن بُعد.
2. إثباتًا فعليًا لحالة جميع الأجهزة المتصلة.
3. انتفاء الثغرات.

> **عرض الإجابة: مراجع التوافق المدعومة دون قياس البرنامج الثابت المثبت عن بُعد.**
> التوافق والتوقيع والقياس والقبول على الجهاز الفعلي أدلة مختلفة.

الفقد والتعطّل والاستعادة في حالات الطوارئ

الهدف

اختيار استعادة تناسبيّة للحادث و الحفاظ على أدلة مفيدة.

الفهم

وفي حالة وقوع حادث، يصنف أولا ما فقد أو تعرض له: الحاسوب أو الجهاز أو البطاقة أو الملف أو كلمة المرور أو بذرة الاسترداد أو عبارة المرور أو السياسة. "لا أستطيع الدخول" لا يعني بالضرورة "لقد سرقت مني". إذا كان هناك شك في وجود خطوبة، لا تستمر في إدخالأسرار في الفريق المشتبه به.

يمكن حلّ فقدان الجهاز بأدوات وأوراق استرجاع متوافقة. فقدان الحاسوب قد يتطلب إصلاح المستودع Desk وإعادة بناء الملاحظة. فقدان جميع وسائل فك القفل أو كل الـ مفاتيح اللازمة تحت العتبة قد لا يكون هناك حل تقني. لا يوجد الذكاء الاصطناعي يمكن أن يضمن إنقاذ مفاتيح غير موجود.

وتشمل الفئة Desk استعادة محلية للنماذج المقبولة وصادرات مواد الاسترجاع ذات الصلة. الـ فك التشفير في الـ PC قد يكشف السر إلى نظام التشغيل أو برمجيات خبيثة إنه قرار استثنائي: فهو يستخدم بيئة مهيأة، ومواد متوافقة، وخطة نقل إلى مفاتيح جديدة إذا كان من الممكن أن يُعرّض السر للخطر. لا تصفه بأنه عملية تعادل العزل المعتاد لـ Cuvex

إذا تم تسريب بذرة الاسترداد، تغيير كلمة مرور Desk لا يلغي بذرة الاسترداد. يجب أن تقيّم النقل المأذون به إلى محفظة و حمايتها من فريق موثوق به ويتجنب نشر تفاصيل الحادث التي تساعد المعتدي أو تدفع تكاليف الخدمات التي تعد باسترداد التكاليف مقابل مبلغ آخر بذرة الاسترداد أو سلف احتيالية.

التدريب

1. يُجري مراجعة لأربع بطاقات وهمية: PC مفقودة، وبطاقة مُحطمة مع نسخة صحيحة، وكلمة المرور منسية، وبذرة الاسترداد مكشوفة.
2. ويحدد كل منها المواد اللازمة، ومخاطر العمل، ونهج الاسترداد.
3. افحص العملية فقط ببيانات التعلم لا تحمل على المدرّس ملفات الطوارئ الفعلية.

أثبت فهمك

يمكنك الاختيار بين إعادة الاستعادة، إعادة تشكيل الملاحظة، الهجرة للسيطرة، أو تسلق أخصائي، دون تأكيد الحلول المستحيلة.

سؤال شائع

تغيير رقم كلمة المرور مرة أخرى كل الأسرار التي رآها شخص ما؟ لا. نسخة واضحة أو بذرة الاسترداد لا تتوقف عن المعرفة.

نقطة توقف

إحتفظ بالحادثة حسب الفئة والإجراء الآمن التالي أوقف الصوت إذا كنت ستعمل على أسرار

نُشرت بذرتك ثم غيّرت كلمة مرور الحاسوب. هل أُبطلت قدرة المهاجم؟

1. نعم.
2. لا، ما زالت البذرة تتحكم بالمفاتيح نفسها ويلزم تدبير لحماية الأصول.
3. نعم إذا غيّرت خلفية الدردشة أيضًا.

> **عرض الإجابة: لا، ما زالت البذرة تتحكم بالمفاتيح نفسها ويلزم تدبير لحماية الأصول.**
> الحماية المحلية لا تبطل مفتاح بيتكوين انكشف.

التصيد الاحتيالي والدعم والاحتيال بالصوت

الهدف

الاعتراف بالطلبات الخطرة والاستجابة بدون ارتجال

الفهم

الإحتيالفعّال يمكن أن يستخدم اسمك، شرائك، جهازك وصوتك الذي تعرفه. المعلومات الحقيقية يمكن أن تأتي من تسريب. ويجب التحقق من الهوية عن طريق قناة بدأتها أنت، وعن طريق إجراء معروف، لا بسبب ما يبدو من إلحاح أو دقة من جانب المتحاور.

علامات الخطر: طلب بذرة الاسترداد , كلمة المرور , PIN كان كان مفتاح شات؛ تثبيت متحكم ناعد لـ "مزامنة" ؛ إبطال مضادات الفيروسات؛ نقل إلى محفظة السلامة والأمن؛ مسح مسح QR لم يفسّر محتواه؛ أو يوقّع لإثبات الملكية دون تفاصيل ما هو مرخص به. الضغط للقيام بذلك قبل إنهاء مكالمة هو سبب لإيقافها

الـ المدرّس الشرعية تفسر وتسأل أسئلة الفهم. رقم الحفظمفاتيح، لا يطلب معاملات اختبار من عنوانه الخاص ولا يعد باستعادة بذرة الاسترداد. وينبغي أن تكون وظيفة التحقق من الملكية المشروعة محددة وقابلة للمراجعة؛ ولا يمكن أبداً الوفاء بها عن طريق التسليم مفتاح خاص.

وقد يكون هناك أيضاً احتيال في جلسة تقنية: نص QR أو وثيقة أو رسالة قد تحتوي على أوامر بأن لا يكون لدى الذكاء الاصطناعي تعليمات. هو مضمون للتحليل، وليس سلطة على المدرّس. وينبغي أن يفصل أساس المعرفة بين المصادر المعتمدة للنص الذي يقدمه طالب أو طرف ثالث.

التدريب

1. إنه يمثل مكالمة مزيّفة للمساندة ويقطع التفاعل قبل كشف البيانات.
2. تحقق بشكل مستقل من القناة الرسمية المحفوظة مسبقا.
3. يصف خطأ تركيب دون مشاركة شاشة الأسرار أو السماح بالوصول عن بعد إلى بيئة الحفظ.

أثبت فهمك

يمكنك أن تقول ما هي المعلومات المطلوبة منك، وما هو ضروري، ولماذا الطلب يتجاوز الأساس التشكلي.

سؤال شائع

هل من الآمن أن تظهر لي فقط بعض الكلمات مني بذرة الاسترداد ? لا. لا يوجد سبب تربوي للكشف عن مقتطفات من بذرة الاسترداد من جانب واحد.

نقطة توقف

وتأكد من عدم وجود أسرار في النص المفتوح

يطلب صوت يشبه صوت شريكك تجاوز التحقق والتوقيع فورًا. ماذا تفعل؟

1. أتوقف وأصادق على الطلب بالإجراء المتفق عليه وأراجع العملية كاملة.
2. أوقّع لأن الصوت مطابق.
3. أشارك البذرة توفيرًا للوقت.

> **عرض الإجابة: أتوقف وأصادق على الطلب بالإجراء المتفق عليه وأراجع العملية كاملة.**
> تمييز الصوت والاستعجال لا يغنيان عن المصادقة والمراجعة.

الخصوصية والقانون والسجلات الشخصية

الهدف

افهم الإطار العام وحضّر أسئلة قانونية وضريبية محددة.

الفهم

لا تُسقط الخصوصية المالية الالتزامات الضريبية، أو التحقق من الهوية حين ينطبق، أو قواعد العقوبات، أو التزامات منع الجريمة. وتتوقف الحالة على الإقامة والنشاط والطرف المقابل والخدمة. يجب أن يقدّم الذكاء الاصطناعي معلومات عامة بمصدر وتاريخ، وأن يحيل القرارات الفردية إلى مختصين مؤهلين.

ينظّم MiCA في الاتحاد الأوروبي أصولًا مشفرة وخدمات محددة. بدأ تطبيقه العام في 30 ديسمبر 2024، وكانت الفترة الانتقالية القصوى المشار إليها في اللائحة تمتد إلى 1 يوليو 2026، رهنًا بالقرارات الوطنية. تحقّق من الترخيص ونطاقه في السجلات الرسمية الحالية، فلا تكفي إشارة قديمة إلى تسجيل سابق. ولا يضمن الترخيص السعر أو الملاءة أو التعويض الكامل.

تحدد اللائحة 2023/1113 المعلومات المرافقة للتحويلات عند مشاركة مزوّدين خاضعين للالتزامات. وبالنسبة إلى تحويلات تزيد على 1,000 يورو وتشمل عناوين حفظ ذاتي، تنص على تدابير لتقييم الملكية أو السيطرة. ولا تُنشئ هذه العتبة إعفاءً عامًا من التحقق من الهوية تحتها. وتُستثنى التحويلات بين الأشخاص دون مزوّد من نطاق تلك اللائحة، مع استمرار التزامات أخرى.

احتفظ بوثائق كافية عن المشتريات والمبيعات والرسوم والمصدر حسب حالتك، واحمها من الوصول غير الضروري. لا يلزم نشر السجل الكامل للاحتفاظ بسجلات خاصة. ولا تعلّم الدورة تقسيم العمليات للالتفاف على الضوابط أو تقديم بيانات زائفة أو إخفاء الدخل.

إذا وُجد تسجيل صوتي أو تفريغ للصوت وتقدّم دراسي يمكن ربطه بشخص، وجب على الخدمة تحديد الغرض والأساس القانوني ومدة الحفظ والوصول والجهات المعالجة والحقوق المنطبقة. تُراجع إعدادات الخصوصية التجارية قبل البيع ولا تُرتجل أثناء المكالمة.

التدريب

1. اكتب للمستشار حالة افتراضية تبيّن الإقامة والنشاط والمعاملات دون مفاتيح.
2. تحقّق أين يمكن مراجعة ترخيص المزوّد، وما تاريخ المعلومات المعروضة.
3. صمّم سجلًا خاصًا للحركات وسياسة بالحد الأدنى لبيانات المتعلم.

أثبت فهمك

ميّز القاعدة القانونية عن سياسة منصة التداول وعن قدرة تقنية لدى بيتكوين.

سؤال شائع

هل كل أشكال الحفظ الذاتي محظورة في الاتحاد الأوروبي؟ لا يستنتج ذلك من النصوص المذكورة. تجنّب العناوين المطلقة وتحقّق من الحكم المحدد ونطاقه.

نقطة توقف

احتفظ بالأسئلة المعلقة لمستشارك دون إدخال وثائق شخصية لدى المدرّس.

هل تُسقط عتبة 1,000 يورو المذكورة لبعض إجراءات التحقق من السيطرة على العنوان جميع الالتزامات تحتها؟

1. نعم.
2. فقط إذا قسمت العملية.
3. لا، فهي ليست إعفاءً عامًا من التحقق من الهوية أو غيره من الالتزامات.

> **عرض الإجابة: لا، فهي ليست إعفاءً عامًا من التحقق من الهوية أو غيره من الالتزامات.**
> تُفسّر القاعدة بحسب التدبير ونطاقه، دون تحويل عتبة محددة إلى إعفاء شامل.

الميراث والاستمرارية والتمرين السنوي

الهدف

وضع خطة تسمح للأشخاص المرخص لهم بالتصرف دون الكشف عن كل شيء مسبقاً

الفهم

ويجمع الإرث بين المشروعية القانونية، وموقع المواد، والقدرات التقنية. ويمكن أن يكون للشخص الحق في الإرث ولا يعرف كيفية إعادة بناء محفظة؛ أما الشخص الآخر فيمكن أن يكون له مفتاح وليس لديه ترخيص باستخدامها. ويجب أن تعالج الخطة كلا البعدين بمشورة مناسبة.

تفرق بين التعليمات العامة للوصول إلى الأسرار. وتبين قائمة الجرد ما هو موجود، ومن يتصل به، وما هي عمليات التحقق التي يتعين القيام بها، دون وضع جميع مفاتيح وكلمة المرور معاً في وثيقة يمكن الوصول إليها على نطاق واسع. & النشر بذرة الاسترداد في وصية أو ملفّات يمكن أن تكون خارج سيطرتك.

وفي التوقيع المتعدد، يحدد من يحتفظ بالسياسة والنسخ، وما هو الحد الأدنى المتاح بعد الخسارة، وما الذي يحدث إذا توفي شخص مفتاح. نفس أمين الحفظ يحتفظ بمكونات كافية يمكن أن تصبح نقطة إساءة استخدام فريدة. ويمكن أن يؤدي التوزيع المفرط في التعقيد إلى جعل التراث غير قابل للاسترداد.

تشمل استعادة كلمة المرور من النص المشفّر وعبارة المرور، إذا كانت موجودة، بيانات الاشتقاق، توافق الأجهزة والإجراءات إذا توقف الصانع عن العمل. لا تفترض أن ملفاً مالكاً أو بصمة قياس أحيائي يمكن استخدامها بدون إعداد. وينبغي اختبار قابلية التشغيل التبادلي باستخدام بيانات الاختبار والنماذج الموثقة.

فحصت بعد تغيير الأسرة أو المسكن أو السياسة أو البرمجيات أو المشاركين، وأجرت عملية محاكاة دورية. ويجب أن تثبت الممارسة أن الشخص الموثوق به يفهم التعليمات دون الكشف عن الأصول أو نقل الأموال دون داع.

التدريب

1. واضافة الى عدد من الموظفين الخاصين مع المسؤولين، والمكونات، والوصول المأذون به، والبديل.
2. يعطي تعليمات مختبرية لشخص آخر بدون شرح شفهي وراقب أين يُغلق.
3. وهو يصحح أوجه الغموض ويسجل تاريخا للاستعراض. المسار لا يخلق رسائل تذكيرية تلقائية.

أثبت فهمك

يمكنك تفسير ما يحدث إذا كنت غير متاح، وما هي المعلومات التي تحتاجها كل دور في كل مرحلة.

سؤال شائع

هل الـ 2 من 3 تحل محل خطة وراثة؟ لا. إنها أداة تقنية. ولا يزالورثة بحاجة إلى السياق، والمادية، والتنسيق والمشروعية.

نقطة توقف

احفظ الخطة خارج المسار واعلم فقط "simulcroform" المنقح.

ما المعيار المفيد لتقييم خطة الميراث؟

1. أن يستطيع شخص مخوّل تنفيذ تمرين موثّق دون ارتجال أو تسلّم الأسرار قبل أوانها.
2. أن تتألف من صفحات كثيرة.
3. أن تعتمد فقط على تذكّر كلمة مرور.

> **عرض الإجابة: أن يستطيع شخص مخوّل تنفيذ تمرين موثّق دون ارتجال أو تسلّم الأسرار قبل أوانها.**
> يجب اختبار قابلية الاستعادة وضوابط الوصول عمليًا.

السعر والادخار والتحليل الأساسي

الهدف

تحليل حجج الاستثمار دون الخلط بينها وبين الخصائص التقنية التي يمكن التحقق منها.

الفهم

فالسعر هو نتيجة للمبادلات في أسواق محددة، وقد يختلف من برنامج إلى آخر. السيولة، عملة السعر المعروض، العمق، ساعات عملات المورّدين المصرفيين والطلب يؤثر على النتيجة التي يمكنك تنفيذها. واحد واحد السعر المعروض ليس عرضاً مضموناً لصوتك

ويبحث التحليل الأساسي عوامل مثل التبني والطلب والمنافسة والأمن الاقتصادي والتنظيم والعرض. ولا يحدد الجدول الزمني المعروف للانبعاثات في حد ذاته السعر المستقبلي. وتتوقف تقييمات الفائدة النقدية أو "القيمة الجوهرية" على الافتراضات؛ ولا يوجد رقم موضوعي يمكن أن يعرضه الذكاء الاصطناعي بوصفه يقينا عالميا.

وتوزع استراتيجية الشراء الدورية وقت الدخول، ولكنها لا تضمن الربح أو تجنب الخسائر الطويلة الأجل. كما أن المدخرات الطويلة الأجل تحتاج إلى السيولة لتغطية التزامات، والقدرة على تحمل التقلبات، وخطة الحفظ. الدورة الدراسية لا تحدد نسبة من ممتلكاتك ولا تتخذ قرارات عنك

تفرق بين ثلاثة أسئلة: أتفهمين الفاعل؟ هل يمكنني أن أحميه وأستعيده؟ هل يمكنني أن أتحمل مخاطرتك المالية؟ لا يستجيب الدوم مفاتيح آلياً للثالثة. ولا يحول التدريب إسقاطاً للأسعار أو رسماً بيانياً تاريخياً إلى توصية خاصة.

التدريب

1. يكتب أطروحة وهمية، فرضياته وحقائقه التي ستبطلها.
2. يُحلّلُ a انخفاض 50 % مِنْ الو إحتياجاتِ السيولة في وقت واحد، بدون إدخال تراثِكَ الملكيِ.
3. وهو يحدد ما يمكن التحقق منه وما هي التوقعات.

أثبت فهمك

يمكنك مناقشة الاستثمار بدون وعد الربح أو الخلط بين الاقتناع والأدلة

سؤال شائع

هل الندرة تضمن ارتفاع السعر؟ لا. ولا يزالطلب وغيره من الشروط عاملا حاسما في أسعار السوق.

نقطة توقف

حارس مخبر، ليس تعليمات شراء آلية.

ماذا يضمن الشراء الدوري؟

1. ربحًا طويل الأجل.
2. لا يضمن عائدًا، بل يوزع أوقات الشراء وفق قاعدة تختارها.
3. الحماية من ضياع المفاتيح.

> **عرض الإجابة: لا يضمن عائدًا، بل يوزع أوقات الشراء وفق قاعدة تختارها.**
> توزيع الشراء لا يزيل المخاطر الاقتصادية أو التشغيلية.

اختيار جهة شراء البيتكوين

الهدف

تقييم المورّد بالترخيص والتكلفة والسحب والخصوصية وخطر الحفظ

الفهم

يقارن المورّدون بمعايير يمكن التحقق منها: الكيان القانوني والاختصاص القضائي، الخدمات المأذون بها، شبكة السحب، الرسوم، تفاضل السعر، الحدود، الدعم، التوثيق، معالجة البيانات. الاسم التجاري أو التزكية لا يثبت ترخيصاً للخدمة المحددة.

ويمكن أن تشمل التكلفة الإجمالية الإيداع، والتحويل، وفارق السعر، والرسم للتفاوض، والانسحاب، والتكلفة المصرفية. التفاوض "بدون الرسم" قد يكون لديه تفاضل أكبر. صافي المبلغ المتحقق منه والعملة المرجعية. الميزانية يجب أن تشمل سحب الحفظ الذاتي عندما يكون هذا هو هدفك

بينما تحتفظ برصيد ضماني يعتمد على المورد. ولا يثبت اختبار الاحتياطي وحده جميع الخصوم، أو ملكية الأموال، أو الملاءة الآجلة. تحقق من القيود واعمل سحب صغير يمكنك تحمله قبل الاعتماد على تدفق جديد

الهوية التجارية يمكن أن تربط هويتك بالسحب ولا تعني حماية هذه المعلومات بعد ذلك حذف ما يعرفه المورّد. لا تزيّف البيانات أو تستخدم المسار للتهرب من التزامات. شراء رمز التدريب أيضاً يُنتج سجل تجاري منفصل عن الـ محفظة الخاص بك

التدريب

1. املأ مصفوفة وهمية مع مورّدين اثنين: التكلفة الإجمالية، الشبكة، سحب الحد الأدنى، الترخيص والبيانات المطلوبة.
2. حساب صافي عملية تعلم مع جميع الرسوم المحددة.
3. صمم سحب اختباري إلى عنوان تم التحقق منه مسبقاً، دون تشغيله من هذه الغرفة الصغيرة.

أثبت فهمك

يمكنك أن تبرر اختياراً لقضيتك وتعرف ما هي المعلومات التي انتهت صلاحيتها أو لم تثبت صحتها

سؤال شائع

هل الصف يوصي بأن منصة تداول أفضل للجميع؟ لا. فالتصاريح والرسوم والبلدان التي تتلقى الخدمات والظروف تتغير. وتتطلب المقارنة تاريخ الاستخدام وحالة استخدامه.

نقطة توقف

احفظ المصفوفة بدون وثائق تفويض أو وثائق هوية.

ما المقارنة الأكثر نفعًا من النظر إلى رسوم التداول وحدها؟

1. الكلفة الإجمالية إلى أن تتلقى BTC على الشبكة والعنوان المطلوبين.
2. عدد متابعي المزوّد.
3. لون تطبيقه.

> **عرض الإجابة: الكلفة الإجمالية إلى أن تتلقى BTC على الشبكة والعنوان المطلوبين.**
> يتضمن السعر النهائي بنودًا قد لا تدخل في الرسوم المعلنة.

الحسابات والأوامر وتكاليف التنفيذ

الهدف

فهم الأوامر الأساسية وحماية الحساب دون تحويل المسار إلى محطة تجارية.

الفهم

أمر سوقي أولويات التنفيذ المتاحة، مع خطر الانزلاق السعري. ويحدد أمر تقييدي سعرا أقصى للشراء أو حدا أدنى للبيع، ولكن قد لا ينفذ أو قد ينفذ جزئيا. أمر إيقاف نشط إجراء آخر وفقاً لقواعد المورّد؛ لا يضمن السعر النهائي وحده.

يعرض دفتر الأوامر العروض المتاحة، لا التزامات بأن كل المجلدات ستبقى. في هبوط أو انخفاض السيولة، النتيجة قد تختلف عن السعر المعروض الأخيرة. وهناك مخاطر مختلفة في الأمرين الصادرين بشأن وقف التنفيذ، وهي التنفيذ بسعر أقل من احتمال عدم التنفيذ.

حماية الوصول إلى كلمة المرور الوحيدة، والتوثيق المقاوم لالتصيد الاحتيالي عندما يكون مدعوماً، واستعراض الجلسات، وضوابط الانسحاب المناسبة. احفظ الاستعادة لثاني معامل مستقل. ويمكن أن تكون الرخصة مفتاح API للتشغيل الآلي أكثر خطورة من التراخيص التي تحتاج إلى قراءة بيانات؛ ولا تدخلها في ال المدرّس أو في المقر الرئيسي.

قبل أن ننسحب، تحقق من الشبكة بيتكوين النشطة، عنوان محفظة الخاص بك، وصافي الكميات. يمكن للمنبر أن يستخدم نفس الرموز لمنتجات مختلفة. في النهاية، يحتفظ بمستندات شراء، أداء، الرسوم وسحب حسب حالتك لا تخلط بين سحبك لـ محفظة الخاص بك

التدريب

1. حاكِ دفتر أوامر افتراضيًا فيه وحدة واحدة عند 100 وأخرى عند 102. اشرح لماذا لا يضمن شراء وحدتين بسعر السوق متوسط سعر 100.
2. صمم أمراً محدوداً ووصف السيناريو الذي لم يكتمل فيه.
3. يُصدّق على الرخصة من API وهمي ويحذف السحب إذا كنت بحاجة فقط إلى استشارة.

أثبت فهمك

يمكنك وصف الأولوية والسعر وخطر عدم التنفيذ لكل أمر

سؤال شائع

هل توقفك دائماً ما يحد من الخسارة بالضبط؟ لا. .... السيولة , الانزلاق السعري وقواعد المورّد قد تمنعه.

نقطة توقف

يحفظ نتيجة العملية بدون أوامر ملكية أو مفاتيحAPI.

ما الخطر المتبقي في أمر شراء محدد السعر عند 100؟

1. ألا يُنفذ قط أو أن يُنفذ جزئيًا فقط.
2. أن يتعين تنفيذه بأي سعر.
3. أن يُنشئ تلقائيًا نسخة احتياطية.

> **عرض الإجابة: ألا يُنفذ قط أو أن يُنفذ جزئيًا فقط.**
> التحكم بالسعر يقابله احتمال عدم التنفيذ.

الشموع السعرية والمؤشرات وتحيزات التحليل الفني

الهدف

قراءة الرسوم البيانية مثل البيانات التاريخية وتقييم استراتيجية دون الخلط بين الأنماط والتنبؤات.

الفهم

الشموع السعرية اختصاراً للفتحة، الحد الأقصى، الحد الأدنى، و نهاية الفترة. يعتمد الحجم على المصدر. غيّر منصة، عملة، مساحة زمنية أو فترة يمكن أن تغيّر ما تراه الشموع السعرية لا تظهر كل الترتيب الزمني للتحرك داخل الفترة الزمنية.

متوسط متحرك متنقل مخفف للأسعار الماضية المؤشر الحالي يحول البيانات الملاحظة تحت المعادلة. ولا أحد منهم يعرف المستقبل. ويمكن لمؤشرين من نفس المجموعة أن يقدما معلومات مترابطة جداً رغم اختلاف ألوانهما وأسمائهما.

لتقييم قاعدة تعريف الدخول، الخروج، العجز، التكلفة، الحجم والبيانات قبل النظر في النتيجة. تجنب فقط اختيار الأمثلة الفائزة، تعديل البارامترات إلى أن يتم ربط أو استخدام البيانات المستقبلية في قرار سابق. قم بتمييز بيانات التدريب والتحقق المؤقت.

وينبغي أن ينظر المقياس إلى فارق السعر، الرسوم، الانزلاق السعري، توافر البيانات، التنفيذ المحتمل. الدخل الإجمالي، معدل النجاح، الخسارة القصوى، توزيع الخسائر، يجيبون على أسئلة مختلفة. نظام لديه الكثير من النجاحات يمكن أن يخسر المال إذا كانت عيوبه كبيرة. لا تظهر علامة شراء أو بيع كتأكيد

التدريب

1. إقرأ الشموع السعرية وهمية واشرح ما هي المعلومات الزمنية التي لا تحتوي عليها.
2. اكتب قاعدة قبل تقييم 10 نتائج تركيبية، مع تكلفة ومقياس حكم.
3. مقارنة 9 ربح من 1 مع خسارة 15: الناتج الإجمالي هو -6 على الرغم من أن 90 في المائة صحيحة.

أثبت فهمك

يمكنك أن تنتقد نتيجة جذابة من خلالاختيار أو التكاليف أو المخاطر دون الحاجة إلى تنفيذ العمليات.

سؤال شائع

هل الجمع بين العديد من المؤشرات يضمن إشارة أفضل؟ لا. ويمكن أن يزيد من التعقيد والتعقيد دون تقديم معلومات مستقلة.

نقطة توقف

حفظت القاعدة ونتائج المختبر وليس أمر السوق.

ربحت تسع صفقات وحدة لكل منها وخسرت واحدة 15. ما النتيجة قبل التكاليف؟

1. +90%.
2. +6.
3. -6.

> **عرض الإجابة: -6.**
> تسع وحدات ربح ناقص خمس عشرة خسارة يساوي خسارة ست وحدات.

الهامش والعقود الآجلة والأتمتة

الهدف

الاعتراف بالتعرض، و التصفية، وإخفاق التشغيل الآلي قبل النظر في المنتجات المعقدة.

الفهم

ويتزايد التعرض للعامل الرافعة المالية بالنسبة لرأس المالمقدم. وفي مثال مبسط، يعني هامش 100 لتعرض 1.000 أن الحركة المعاكسة لـ 5 في المائة من الأساس تساوي 50 قبل التكلفة: نصف نطاق البداية. قواعد الصيانة الفعلية، التصفية، بالإضافة إلى الرسوم يمكن أن تزيد من سوء النتيجة وتُنشَّط في وقت أبكر مما كان متوقعاً

ويمكن أن تشمل آجالاستحقاق الآجلة والدائمة، التصفية لكل فرق، ومعدلات التمويل والأسعار المرجعية غير آخر تبادل تجاري. هذا لا يساوي سحب بيتكوين الأصلي إلى Cuvex حفظ بذرة الاسترداد لا يحمي أي موقف ضد التصفية أو فشل النظير.

جهاز آلي يُحدّد القواعد، بما في ذلك أخطائه. وهي تحتاج إلى حدود للمواقع، وإلى حد أدنى من التصاريح، وإلى عدم وجود أوامر، وإلى المصالحة، ومراقبة الخسائر، وعرقلة حالات الطوارئ، والرصد. تكرار الطلب بعد عرض قد يتضاعف إذا لم تكن النتيجة السابقة معروفة.

وقد يفسر الذكاء الاصطناعي المفاهيم ويكشف عن أوجه عدم اتساق في حالة وهمية. لا يجب أن تحصل على مفاتيحAPI أو تنشيط التجارة أو الوعد باستراتيجية مربحة. وللغرض الرئيسي من هذه الدورة، يتيح فهم هذه المخاطر اتخاذ قرار بعدم استخدام منتجات غير مفهومة.

التدريب

1. يحلل مثالتعرض والهامش دون افتراض أن مستوى التصفية هو بالضبط 10%.
2. يَحْملُ API a الذي يَعمَلُ a أمر لكن يَفْقدُ الجوابَ. فسر لماذا قبل أن تكرري يجب عليك أن تصالحي نفسك
3. صمم زر توقف لمنع الأوامر الجديدة و تحقق من الفتحات دون ربطها بمضيف.

أثبت فهمك

يمكنك وصف الخطر الذي ينجو من التوقف، وآخر ينجو من الروبوت والآخر ينجو من الحفظ الذاتي من التمويل الخارجي.

سؤال شائع

الجهاز يزيل العواطف وبالتالي يضمن النتائج؟ لا. ويمكن أن يقلص التدخل الاندفاعي ويضاعف أخطاء التصميم أو التنفيذ.

نقطة توقف

هذا التوسع يشير إلى أنه مفهوم دون أن يحفز المنتجات المعقدة.

مع انكشاف 1,000 وهامش 100، ماذا تعني خسارة 5% من الانكشاف قبل التكاليف؟

1. خسارة 5.
2. خسارة 50، أي 50% من الهامش.
3. لا خسارة عند استخدام روبوت.

> **عرض الإجابة: خسارة 50، أي 50% من الهامش.**
> تجعل الرافعة والتكاليف النتيجة على الهامش مختلفة عن حركة الأصل.

Lightning والطبقات الأخرى

الهدف

فهم المدفوعات عن طريق القنوات والإقرار بالوظائف التي لا يوفرها التدفق Cuvex المنقح.

الفهم

يستخدم Lightning قنوات وآليات تحديث للدفع دون تسجيل كل تبادل في السلسلة الأساسية. قد يتطلب فتح القنوات أو إغلاقها وبعض حالات الاستعادة معاملات على السلسلة. يتوقف التوافر وسيولة الاستقبال والإرسال والمراقبة على تصميم المحفظة والخدمات المختارة.

قد تتضمن الفاتورة مبلغًا ووصفًا وأجل انتهاء. يمكن التعبير بالساتوشي أو الميلي ساتوشي بحسب السياق، ولا يعني الأخير إمكان مخرجات أصغر من ساتوشي على السلسلة الأساسية. يلزم توافق ومسار متاح للدفع، ولا يضمن QR إمكان الدفع من كل تطبيق.

للخدمات الحفظية وغير الحفظية نماذج متباينة. السرعة المعتادة لا تعني انعدام المخاطر. ولا ينبغي عرض Lightning كإخفاء تام للهوية، فهناك مراقبون ومسارات وأطراف مقابلة وبيانات وصفية.

تتيح دردشة Cuvex تنسيق طلبات بالساتوشي تُدفع على السلسلة من حساب WOW. لا تنسب هذه الطبعة إلى Desk عقدة Lightning أو إدارة القنوات أو توقيع فواتير Lightning. إذا تضمن الطلب طرقًا متعددة فتحقق من الطريقة التي تفهمها وتلك التي سينفذها تطبيقك.

التدريب

1. يصنف عنوان URI، on-chainبيتكوين: و Lightning التعليم.
2. مقارنة الدفع عبر السلسلة والقناة من حيث التأكيد، السيولة، الحفظ واستعادة.
3. يوضح لماذا يجب أن يُراجع الاقتباس الذي انتهى مفعوله مع المتلقي بدلاً من إعادة تفسيره على أنه عنوان.

أثبت فهمك

يمكنك أن ترفض طريقة غير متوافقة دون الكشف عن مفاتيح أو نسب خطأ إلى Cuvex.

سؤال شائع

هل كل الدفعات في الساتس هي Lightning؟ لا. () الـ ساتوشي تعبر عن قيمتها؛ وتعتمد الطريقة على البروتوكول المستخدم.

نقطة توقف

لا توجد فواتير فعلية.

ما البيان الكافي لمعرفة أن الطلب يُدفع عبر Lightning؟

1. أن يرد فيه لفظ sats.
2. أن يصل في الدردشة.
3. توافق تنسيقه وطريقة الدفع، لا مجرد الوحدة أو قناة الرسالة.

> **عرض الإجابة: توافق تنسيقه وطريقة الدفع، لا مجرد الوحدة أو قناة الرسالة.**
> وحدة الحساب وشبكة الدفع بُعدان مختلفان.

Taproot وMuSig2 ومستقبل ما بعد الحوسبة الكمّية

الهدف

التمييز بين المعايير، المقترحات، والقدرات التي تم تنفيذها.

الفهم

يسمح Taproot بشروط الإنفاق على الطرق من مفتاح و برمجية. يمكن أن تحسن الـ التوقيعاتSchnorr والتجميع بعض المباني، ولكن نتيجة الخصوصية تعتمد على كيفية تشكيلها وصرفها. ولا يثبت أن عنواناً من العناوين هو Bc1p أنه لا يوجد مشاركون آخرون ولا يكشف عن جميع ظروفه الخفية.

يسمح MuSig2 لمجموعة من الموقّع بإضافة مفاتيح وإنتاج توقيع Schnorr متوافق مع التفاعل. معيار القاعدة هو N من N. والعتبة التعسفية M/N تتطلب بناء آخر أو بروتوكولا إضافيا. وإدارة الاجتماعات والمؤتمرات أمر بالغ الأهمية ولا تنفذ عن طريق تبادل الرسائل بشكل غير رسمي.

تعيد PSBT v2 تنظيم المعلومات مقارنةً بـ v0، وليست ترقية تلقائية لأي ملف يحتوي معاملة من الإصدار 2. تحتفظ البرامج الثابتة Final في هذه الطبعة بـ PSBT v0 وP2WSH/sortedmulti وSIGHASH_ALL لملف التوقيع المتعدد. وتحتاج الإمكانات المستقبلية إلى مواصفة تشغيل وتحقق خاصين بها.

نشر NIST في 2024 أول معايير ما بعد المياه الخاصة به والتي تم الانتهاء منها. هذا لا يغير في حد ذاته التوقيعات من بيتكوين. ومن شأن استخدام خوارزمية ما بعد المياه في توثيق البرنامج الثابت أن يحمي هذه الطبقة؛ ولن يحول تلقائيا ECDSA أو Schnorr من UTXO إلى التوقيعات وما بعدها. وليس هناك أيضاً أي تاريخ للهجوم في المستقبل أن المدرّس يمكن أن تعدنا بالتأكيد.

التدريب

1. يصنف خمسة بيانات على أنها معياري أو تنفيذ متحقق منه أو مقترح أو إعلان
2. شرح لِمَ "يقبل المستلم Taproot" لا يثبت "يوقع مدخلاً Taproot".
3. رسم طبقات منفصلة: توقيع البرنامج الثابت، التشفير سري، دردشة، وتوقيع نفقات بيتكوين.

أثبت فهمك

يمكنك أن تطلب دليلاً محدداً على طبقة وتتجنب نقل ضمانات بين البروتوكولات

سؤال شائع

هل عليّ أن أهجر أموالي من أجل مُشغل مُتعلق بالحاسوب الكمّي؟ ويتطلب القرار الحقيقي أدلة تقنية حالية، ودعما يمكن التحقق منه، وتقييما للمخاطر، وخطة للهجرة الآمنة؛ أما الدورة الدراسية فلا تأمر بالتنقلات بين حاملي الأسهم.

نقطة توقف

تسجيل الأسئلة التقنية دون إنشاء خطة تكلفة آلية.

لو نُفّذ توقيع ما بعد كمّي في محمّل الإقلاع وخضع للتحقق، فهل يغيّر شروط توقيع UTXO موجود؟

1. لا، فهما طبقتان مختلفتان.
2. نعم، يحوّل الشبكة بأكملها إلى خوارزمية أخرى.
3. يلغي الحاجة إلى النسخ الاحتياطية.

> **عرض الإجابة: لا، فهما طبقتان مختلفتان.**
> توثيق التحديث لا يغيّر شروط إنفاق البيتكوين.

التشغيل البيني والاستغناء عن المصنّع

الهدف

تخطيط المواصلة إذا تغيّر البرمجيات أو الجهاز أو المورّد.

الفهم

ولا يمكن التحقق من قابلية التشغيل البيني بقائمة الرموز. يجب أن تحتفظ بشبكات، برمجية، الاشتقاق، مفاتيح، سياسية، شكل معاملات، ودلالات لـ التوقيعات. يمكن لتطبيقين أن يفهما BIP174، ومع ذلك لا يسمحان بنفس المجالات أو الأحجام أو أنواع المدخلات.

ويحتفظ المركز بمعلومات استجمام موثقة ومقارنة مع محفظة للتعلم من أجل الخروج من وحدة الـ الواجهة. الـ عبارة التذكّر القياسية يمكن أن تسمح بالانتقال إلى مفاتيح، لكن استعادة الـ التوقيع المتعدد يتطلب سياستك الكاملة. وتضيف العلامات BIP329 سياقاً للخصوصية؛ وتاريخ الدردشة له نطاق مختلف.

لا تحول اختبار التوافق إلى تعرض لـ بذرة الاسترداد حقيقي أولاً: التحقق من التصدير العام واصف والتعافي والتعافي والاستعادة والاسترداد والتعافي للمراقبة فقط . وإذا كانت حالة الطوارئ تتطلب إعادة بناء مفاتيح، فإنها تستخدم بيئة مصممة لهذا الغرض وتنظر في الهجرة بعد ذلك. محفظة غير متوافق مع الصفر لا يثبت في حد ذاته أن الأموال قد فقدت.

احتفظي بنسخة قابلة للتحقق من الوثائق، نسخة من الدورة والأدوات اللازمة. وقد يؤثر توقيع التطبيقات، والشهادات المتقادمة، والتغييرات في النظم على التركيب. المصدر المفتوح المتاح لا يضمن أن أي شخص يستطيع تجميعه بعد سنوات دون الاحتفاظ بالوحدات والمعرفة.

التدريب

1. صمم اختبار خروج مع حساب فارغ: نفس الشبكة، السياسة، و توجيه التحكم في تطبيقين متوافقين.
2. يرجى تحديد الأجزاء التي هي معايير، وأيها تحتاج إلى تحويل أو توثيق في نموذج Cuvex.
3. وهو يحدد النتيجة التي يمكن من خلالها تأكيد التوافق وما تبقى من العتاد أو التوقيع الفعلي.

أثبت فهمك

يمكنك أن تصف مساراً للتعافي دون الاعتماد على الشركة التي لا تزال تقدم نفس الخدمة

سؤال شائع

هل يعني الرمز المفتوح أن الصانع لم يعد يهم؟ لا. ولا يزالتوزيع والصيانة والمكونات المادية والخبرة التشغيلية تستورد. إنّها تسمح بالتفتيش والاستمراريّة المحتملة، وليس الضمان الآليّ.

نقطة توقف

يحتفظ بنتائج مختبرية مع نسخ وحدود مراقبة.

أي دليل أقوى على التشغيل البيني؟

1. أن يعرض التطبيقان كلمة «Bitcoin».
2. إعادة بناء السياسة والعنوان نفسيهما والتحقق منهما في المختبر بإصدارات محددة.
3. تشابه الأيقونات.

> **عرض الإجابة: إعادة بناء السياسة والعنوان نفسيهما والتحقق منهما في المختبر بإصدارات محددة.**
> ينبغي أن يحتفظ الاختبار بالشروط المهمة ويعطي نتيجة قابلة للتحقق.

مختبر تقني باستخدام regtest

الهدف

افهم مختبرًا يمكن إعادة نتائجه وميّز بين الاختبارات الاصطناعية والاستخدام على أجهزة فعلية.

الفهم

يسمح Regtest ببناء سلسلة محلية خاضعة للتحكم لتوليد كتل وتجربة معاملات بلا قيمة اقتصادية. يجب استعمال أدلة وبيانات اعتماد منفصلة وعدم استيراد مواد حقيقية. لا تثبت نتائجه وحدها توافق USB أو NFC أو Bluetooth أو كاميرا جهاز فعلي.

يسجّل المختبر المتكامل الإصدارات وإعدادات الشبكة والسياسة ومدخلات الاختبار وPSBT والتوقيعات والمعاملة النهائية ونتيجة القبول. يمكنه فحص توازن المبالغ ورفض توقيع عُدّل وإدراج دفعة صحيحة في كتلة محلية. ينبغي أن تغطي التجربة حالات الفشل أيضًا، لا المسار الناجح وحده.

تشير وثائق التحقق من Desk 9.21 إلى اختبارات باستخدام Bitcoin Core 31 regtest واختبارات آلية للمحرّك وواجهة مستخدم محاكاة. تستخدم هذه الطبعة التقارير دليلًا وثائقيًا ولا تدّعي أنها كررت الاختبارات أو نفذت عمليات بأجهزة فعلية. كما أن فحص حزمة لا يثبت تثبيتها على كل الأنظمة.

قبل درس تقني، ينبغي للمهندس تسليم المختبر جاهزًا وإجراءً متوافقًا مع إصدار المتعلّم. لا تفتح RPC للإنترنت كي يتحكم فيه المدرّس. يمكن للذكاء الاصطناعي إرشادك إلى تفسير النتائج الاصطناعية، لكن يجب ألا يحصل على بيانات اعتماد أو صلاحيات إدارة.

التدريب

1. في المختبر الجاهز، لاحظ معاملة صالحة وأخرى عُدّل توقيعها، وسجّل القبول أو الرفض.
2. تحقق من حالة باقي غير صحيح وحالة شبكة غير متوافقة.
3. افصل في تقريرك بين «اختبار المحرّك» و«واجهة المستخدم المحاكاة» و«العتاد الفعلي».

أثبت فهمك

صف بالضبط ما اختُبر وما بقي دون تقديم المحاكاة على أنها شهادة اعتماد.

سؤال شائع

إذا عمل regtest، فهل أستطيع بيع الدورة على أنها مختبرة لجميع الأجهزة؟ لا. ما زالت اختبارات مسارات الأجهزة الفعلية والتثبيت وإمكانية الوصول والاستعادة والخدمة التجارية مطلوبة.

نقطة توقف

أوقف المختبر واحفظه وفق تعليماته مع الاحتفاظ ببيانات اصطناعية فقط.

هل يثبت اختبار المحرّك في **regtest** قراءة **NFC** فعلية على هاتف بعينه؟

1. نعم، لأن كليهما يستخدم بيتكوين.
2. نعم إذا كان حجم PSBT صغيرًا.
3. لا، فذلك يتطلب اختبارًا منفصلًا على الجهاز الفعلي.

> **عرض الإجابة: لا، فذلك يتطلب اختبارًا منفصلًا على الجهاز الفعلي.**
> تختلف بيئات التحقق في نطاق ما تثبته.

المشروع النهائي وخطة الاستمرارية

الهدف

إثبات الاستقلالية من الإعداد إلى استعادة الحياة الخاصة

الفهم

نتيجة الدورة الدراسية ليست حفظ قائمة: هو أن يكون قادراً على شرح النية، التحقق من النتيجة، ووقف عملية لا تفهمها. ويجمع التقييم بين المفاهيم والممارسات المُرشدة وقضية مستقلة. لا يعتمد أبدا على الكشف عن بذرة الاسترداد، ممتلكات أو عناوين شخصية إلى المقيّم.

الحالة ألف: تشكل بيئة تعليمية، وتحدد النماذج والنماذج، وتحمي Desk، وتربط النص المشفّر تعليمي، وتعيد بناء حساب للمراقبة فقط. يوضح لماذا؟ نسخة احتياطية و ما هي المعلومات التي يمكن لمزودك أن يراها

الحالة B: تصميم دفع مع UTXOs وهمية من سياقات مختلفة، تبرير الفرز، التحقق من المستلم، تغيير و الرسم، وصف فرع التوقيع الخاص بجهازك. ويحل عطل العودة وتوقف النشر دون مضاعفة الدفع. وفي حالة عدم قبول العتاد جسدياً، يسجل الجزء كمحاكاة ويظل معلقاً.

القضية جيم: تصميم 2 من 3، يمثل دعوة والتحقق، ويقارن في Mirror حقل مختار ترتيبا حرا، ويشرح نطاق OK. واستعادت سياسة التعلم، وتظاهرت بفقدان أحد المشاركين، وأعدت الاستمرارية والميراث.

يتطلب التجاوز المقترح على الأقل 80% من المعرفة وجميع الضوابط الحرجة الصحيحة: عدم الكشف عن الأسرار، فحص الشبكة والمخرجات، عدم الخلط بين المراحل والحفاظ على التعافي. فالخطأ النقدي يتطلب تنقيحا وممارسة جديدة؛ ولا يمكن تعويضه بأسئلة سوقية دقيقة. وينبغي للشهادة التجارية، إن صدرت، أن تبين ما جرى تقييمه وما إذا كان هناك رصد مادي أم مجرد محاكاة.

التدريب

1. يملأ الحالات الثلاث ببيانات تركيبية وشرح شخصي.
2. يراجع التقييم النهائي للمرفق وينقح كل رد من الردود الفاشلة.
3. فقط يعطي ورقة نتائج بدون أسرار، مع أدلة من المدى والتماس.

أثبت فهمك

يمكنك أن تتوقف بمبادرة منك عندما تفتقر عملية ما إلى أدلة كافية وتعرف ما تحتاج إليه لتستمر

سؤال شائع

هل إنهاء الصفحات يساوي الاستعداد لحماية أي قيمة؟ لا. القدرة يجب أن تختبر و الخطر يجب أن يُقيّم على حسب وضعك فالقراءة والاختبار لا يضمنان نتائج في المستقبل.

نقطة توقف

حافظ على خطة المراجعة الخاصة بك و ممارساتك المتبقية. يمكنك العودة إلى الفصل الضروري دون تكرار المسار بأكمله

ما المتطلب الأساسي لإنهاء التدريب العملي؟

1. فتح جميع الصفحات.
2. إثبات الاستعادة ومراجعة العمليات ضمن نطاق موثّق دون كشف أسرار.
3. التنبؤ بسعر الشهر المقبل.

> **عرض الإجابة: إثبات الاستعادة ومراجعة العمليات ضمن نطاق موثّق دون كشف أسرار.**
> يُقاس التعلم بالقدرات والحدود المثبتة، لا بالتصفح أو التنبؤ.

دليل المتعلّم

دليل تشغيل Cuvex

يرافق هذا الدليل الدروس. يصف كل إجراء المسار الوارد في الشيفرة المصدرية المراجَعة وفحوصه ونقطة توقفه. هذه نسخة مرشحة للتجربة، ولا تثبت أن فريقها أجرى اختبارات فعلية على Original أو BIT أو الهواتف أو كل منصة مكتبية. قبل التدريس بأموال حقيقية يجب إكمال مصفوفة القبول وتصحيح أي تسمية أو شاشة مختلفة.

الإصدارات المرجعية هي Original 1.2.2 Final وBIT 1.2.3 Final وDesk 1.0.0-beta.9.21 وMirror 1.0.0-beta.12.12. اختيار ملف تعريف في Desk يفيد التوافق المعلن ولا يقيس البرنامج الثابت عن بُعد. التُقطت صور شاشة Mirror الفعلية المرفقة من محاكي Android ضمن الحزمة 12.12. أما صور المنتجات فمن مواد الشركة ولا تثبت الإصدار المعروض على جهاز حالي.

P01 | التحقق من المصدر والإصدار | C01,C02 | L16,L21 | Cuvex

التحضير: جهّز مستند الشراء وقناة رسمية تستطيع التحقق منها بصورة مستقلة. لا تدخل أي أسرار بعد.

1. افحص التغليف والأختام. عند وجود آثار عبث أوقف الإعداد واحتفظ بأدلة غير حساسة.
2. استخدم إجراء سلامة المنتج وفحص الأختام في التطبيق المتوافق مع النسخة المسلّمة. أدخل الرموز فيه وحده ولا تعطها للمدرّس.
3. حدّد ما إذا كان الجهاز Original أو BIT والمراجعة المتاحة، وافحص الإصدار المعروض على الجهاز وفي التطبيقات.
4. قارِن بمصفوفة الفريق المنشورة. لا يحل كتالوج أو قيمة تجزئة محل التحقق من أصالة البرنامج الثابت أو القبول على الجهاز الفعلي.

النتيجة: عُرف الطراز والإصدارات ورُوجع المصدر دون كشف أسرار. إذا لم تصح الرموز أو اختلفت الواجهة فلا تفرض التشغيل بدليل قديم.

توقّف قبل تحميل مواد الحفظ. لا تضمن قابلية تتبع الشراء وحدها انعدام العبث المتقدم.

P02 | تحديث Original عبر L46 | Original | Bluetooth | C01,C02,C03

التحضير: نسخ قابلة للاستعادة وطاقة مستقرة وحزمة رسمية متوافقة ومسار مقبول لنظامك. لا تثبت هذه الدورة توافر التشغيل الفعلي الكامل على كل منصة.

1. في قسم الأجهزة أو البرامج الثابتة بالتطبيق اختر Original ثم التنزيل الرسمي أو الملف المحلي الأصلي المناسب.
2. ضع الجهاز في وضع التحديث من قائمته واتصل به عبر إجراء التطبيق. أبقِ الجهاز قريبًا وتجنّب جلسات اتصال متنافسة.
3. أدخل الرمز الظاهر على شاشة Original في الحقل المخصص. لا تخلطه بكلمة مرور النص المشفّر.
4. تابع النقل والتحقق والتثبيت وإعادة التشغيل. لا تعتبر النسبة المئوية دليلًا على اكتمال التثبيت.
5. تحقّق من الإصدار النهائي على Original وسجّله في التطبيق إن وُجد الحقل المناسب.

النتيجة: فُحص الإصدار على الشاشة بعد إعادة التشغيل وأُكّد اكتمال المسار. إن وقع الفشل قبل PIN أو أثناء نقل الحزم أو في النهاية فسجّل المرحلة والرمز. لا تفصل الجهاز أو تغيّر البرنامج عشوائيًا «لتجاوز 99%».

P03 | تحديث BIT عبر USB | BIT | L46 | C01,C02,C03

التحضير: حدّد وسيط BIT الفعلي ومصدر الطاقة والحزمة الرسمية المتوافقة واحتفظ بنسخ قبل تغيير البرنامج.

1. اختر BIT في مسار تحديث البرنامج الثابت المتوافق ضمن Desk أو Mirror.
2. صِل الجهاز بكابل ومحوّل مناسبين لنقل البيانات. اسمح بالوصول إلى وحدة التخزين أو المجلد عندما يطلب التطبيق.
3. اختر البرنامج الثابت الأصلي للطراز وراجع الإصدار وبيانات التوافق قبل إرساله.
4. انتظر مراحل النقل والتحقق على الجهاز. قد تختفي وحدة التخزين أو يعاد وصلها وفق البروتوكول.
5. بعد إعادة التشغيل تحقّق من الإصدار على BIT ومن النتيجة النهائية في التطبيق.

النتيجة: تأكد التثبيت على الجهاز نفسه. إذا لم تظهر وحدة التخزين فافحص وضع الجهاز وكابل البيانات والأذونات والوصل وأي جلسة أخرى نشطة. لا تُنشئ مجلدًا بالاسم نفسه على الحاسوب بدلًا منها. يتطلب التعافي من تحديث فاشل الإجراء الرسمي لذلك العتاد.

P04 | إنشاء محفظة بقطعة نقدية وأحجار نرد | C01 | L17 | Cuvex

التحضير: مكان خاص وأحجار نرد مناسبة وقطعة نقود، من دون كاميرات أو ميكروفون نشط للمدرّس. استخدم محفظة تدريب.

1. افتح إنشاء المحفظة ومسار الإنتروبيا في البرنامج الثابت. حدّد ترتيب أحجار النرد الأربعة قبل الرمي.
2. أدخل نتيجة القطعة النقدية وكل حجر نرد حسب الشاشة، ولا تغيّرها تفضيلًا لنتيجة أخرى.
3. تحسب الشيفرة المراجَعة الفهرس = قيمة القطعة النقدية × 1,296 + (d1−1) × 6 × (d3−1) + 36 × (d2−1) + 216 + (d4−1). لا تُقبل إلا الفهارس من 0 إلى 2,047.
4. عند رفض النتيجة أعد رمي القطعة النقدية وجميع أحجار النرد. يبقي التنبيه الكلمات السابقة ويطلب إعادة المجموعة كاملة.
5. أكمل خوارزمية الجهاز بما فيها التحقق الأخير، واحمِ عبارة التذكّر واختبر الاستعادة على انفراد.

النتيجة: أُنشئت المحفظة بالمسار الكامل لا بانتقاء الكلمات يدويًا. أوقف الاستخدام إن خالفت الشاشة المصدر. لا تتخذ مثالًا علنيًا لنتائج النرد أو البذرة أو المفتاح مادةً تخصك.

P05 | تشفير سرّ | C01 | L18,L19 | Cuvex

التحضير: اختر الطراز وتنسيق المحتوى والحماية. إدخال البيانات في حاسوب أو هاتف يكشفها في المصدر حتى إن شُفّرت عند الوجهة.

1. اختر التشفير ثم نوع BIP39 أو SLIP39 أو Monero أو النص المتوافق. لا تخلط القواميس. تدعم لوحة النص الصريح التي روجعت حتى 500 محرف. تخزين تنسيق آخر لا يعني القدرة على التوقيع لشبكته.
2. أدخل المحتوى على الجهاز مباشرة للحفاظ على العزل، وراجع الترتيب والمحارف والحقول الإضافية على شاشته.
3. اختر الحماية الفردية أو المشتركة وفق المسار، والقياسات الحيوية على BIT عند الاقتضاء. ميّز هذه العتبة عن عتبة بيتكوين.
4. أدخل كلمات المرور وأكّدها على انفراد وفق مدقق البرنامج الثابت. لا تفترض أن قواعد Desk تسري تلقائيًا.
5. في Original اكتب على بطاقة فارغة متوافقة، وفي BIT احتفظ بالعناصر المصدّرة ضمن مسار USB. انتظر التأكيد.
6. جرّب الاستعادة للتحقق من المحتوى وأغلق عرض السر عند الانتهاء.

النتيجة: نص مشفّر اختُبرت استعادته. عند فشل القراءة أو الكتابة احمِ الأصل وأعد المحاولة حسب الشاشة، ولا تحذف الترويسات أو تفرض الكتابة فوق المحتوى.

P06 | فك التشفير على الجهاز | C01,C02 | L18 | Cuvex

التحضير: وفّر الخصوصية المادية وعناصر الفتح الكافية، وأوقف الميكروفون والتقاط الشاشة قرب السر.

1. ابدأ فك التشفير على الطراز الصحيح وقدّم النص المشفّر عبر NFC في Original أو عبر مسار USB في BIT.
2. افحص الاسم المستعار ومعرّف العنصر قبل إدخال بيانات الاعتماد.
3. قدّم كلمات المرور اللازمة والقياسات الحيوية إذا تطلبها التنسيق. لا تكرر المحاولة تلقائيًا بعد الفشل فهناك ضبط وصول وآلية قفل.
4. تحقّق من المحتوى على الشاشة المخصصة وحدها. رمز QR الذي يحمل سرًا حساس بقدر النص نفسه.
5. أغلق العملية أو أنهها وفق الجهاز واحفظ الوسيط وبيانات الاعتماد منفصلين حسب خطتك.

النتيجة: استُعيد المحتوى على انفراد وأُغلقت الجلسة. إذا لم يُتعرف إلى التنسيق أو فشلت المصادقة أو ظهر محتوى غير متوقع، فلا «تصلحه» بتطبيق مجهول. صف للدعم الإصدار والتنسيق والخطأ دون إرفاق السر.

P07 | الاستعداد لاستعادة نصّ مشفّر محمي بالقياسات الحيوية | BIT | L19,L47 | C01,C02

التحضير: النص المشفّر (ب) معلومات عن الشكل الذي يتخذه التعلم والوثائق. لا تستنتجي تعافياً لمجرد أن لديك نسخة منه

1. في بطاقة Desk يحدد ما إذا كان هناك مكونات بيومتري وما هو تصدير استعادة التوافر.
2. يحتفظ بمجموعة الملفات التي يوصلها التدفق ونسخة مستقلة، مع هويات سرية.
3. اختبر فتح الفتح العادي في BIT واوثق ما هو كلمة المرور و الشروط المطلوبة.
4. يفحص مسار الانتعاش المحلي الفريد و أشكاله المقبولة تأكد من وجود المواد اللازمة قبل أن تحتاجها
5. افحص بيانات غير مدعمة على جهاز معطل أو غير متوفر

النتيجة: خطة تم اختبارها، مع حدودها، لذلك الشكل المحدد. لا يُدعى أن أي القياسات الحيوية يمكن حذفها أو أن بصمة واحدة يمكن أن تحل محل النسخ. إذا إسترجعت سر في PC، قم بتقييم تعرضك وحاجة إلى هجرة السيطرة بعد ذلك.

P08 | إنشاء نسخة من النص المشفّر والتحقق منها | Cuvex وDesk | L20 | C01,C02

التحضير: نسخة أصلية مُحددة ومقصد متطابق بدون بيانات مُحتفظ بها.

1. بالنسبة Original، يستخدم مستنسخاً من الجهاز أو الدالة المتوافقة Desk ويكون مصدره ومقصده حسب الترتيب المبين.
2. حافظي على البطاقات مستقرة واحترمي رفض الدعامات التي تحتوي بالفعل على النص المشفّر
3. وبالنسبة إلى BIT أو الملف، تصدر المجموعة المكونة للتدفق وتحتفظ بالأسماء أو الجمعيات اللازمة.
4. اعزل النسخة الأصلية واقرأها واسترجعها من النسخة الجديدة
5. تسجيل خاص للتاريخ والشكل والنتيجة؛ حفظ النسخ مع مخاطر مادية مستقلة.

النتيجة: نسخة ثانية مثبتة. لا يعني أن محفظة مختلف أو إلغاء كلمة المرور أو الحماية من بذرة الاسترداد التي تم تسريبها بالفعل إذا فشل القدر، احتفظ الأصلي دون محاولة "إعادة ضبط" بحيث يتطابق كلاهما.

P09 | إنشاء مخزن Desk وفتحه وتغيير كلمة المرور | Desk | L21,L40 | C02 |

التحضير: مثبت متحقق، معماري مناسب، وخطة نسخة احتياطية من المستودع.

1. انشأ المستودع مع كلمة المرور من 12 إلى 1.024 الحروف و تأكيد التطابق.
2. اقفله واعيد فتحه للتأكد من أنك لا تزال قادراً على الوصول إليه كلمة المرور فقط يدخل في Desk.
3. راجع الخمول والانتقال إلى الخلفية في «الأمان» و«الوصول والقفل». لا تشغّل المحو الاختياري أثناء العرض.
4. لتغيير كلمة المرور يقدم الحالي و يؤكد الجديد من تدفقه.
5. إذا كنت تستخدم القياسات الحيوية من PC، أعد ضبطها وفقاً للمؤشر. أنشئ النسخة الحالية و حافظ على العلاقة مع النسخ السابقة.

النتيجة: تم التحقق من الوصول. ويحتفظ النسخ السابقة بنسختي كلمة المرور والتشفير الأصليتين. فآليتا القياسات الحيوية من PC والقياسات الحيوية من BIT هما آليتان منفصلتان. إذا فشل الوصول، أوقف المحاولات المتكررة وتفقد الاستعادة دون أن تطلب من الـ المدرّس أن يحتفظ بوثائق تفويض.

P10 | ربط نصّ مشفّر ومراجعته في Desk | Desk | L22 | C02

التحضير: نص مشفّر تجريبي معروف المصدر ووسيلة نقل متاحة.

1. افتح النصوص المشفّرة أو البطاقات واختر الربط عبر NFC أو USB أو نسخة متوافقة.
2. اختر التصميم والمصدر. لاستخدام NFC استعمل Cuvex Mirror مقترنًا بالحاسوب عبر Bluetooth، أو استخدم وحدة تخزين Cuvex BIT المتصلة عبر USB-C. لا يدعم Cuvex Desktop قارئات NFC الخارجية المتصلة عبر USB.
3. افحص البطاقة التعريفية: الاسم المستعار والمصدر والحجم والتنسيق والشروط التي فسرها التطبيق. هذه بيانات وصفية وليست محتوى مفكوك التشفير.
4. تحقّق هل توجد حسابات محفوظة تنتظر الربط ولا تربط إلا الحساب الذي تحققت منه.
5. صدّر نسخة إذا كانت التغطية الاحتياطية ناقصة واختبر الاستعادة بشكل منفصل.

النتيجة: نُظم العنصر محليًا. لا تثبت صفة «مرتبط» أصالة البذرة أو الرصيد. إذا لم يُعرف العنصر فافحص التنسيق والإصدار دون تغيير الامتداد أو حذف البيانات لحمل التطبيق على قبوله.

P11 | تفعيل حساب WOW للمراقبة فقط | Desk وL13,L22 | Cuvex | C01,C02 |

التحضير: المعلومات العامة المستمدة من تدفق الجهاز والسيطرة الخاصة من مصدره.

1. اضبط WOW أو اضف الحساب من النص المشفّر صحيح.
2. استيراد واصف أو المواد العامة المسموح بها من خلالأرشيف، أو ويبكام، أو Mirror حسب الوظيفة.
3. تفقد الشبكة، البرمجية، المصدر، البصمة، المسار، و المجموع الاختباري عند الاقتضاء. لا تدخل بذرة الاسترداد أو xprv.
4. سم الحساب واختر مصدراً للاستشارة بالموافقة.
5. اضبط عنوان التحكم و نطاق الاكتشاف قبل ان تفسر الرصيد

النتيجة: رُبطت محفظة المراقبة. إذا ظهر صفر فافحص الشبكة وعبارة المرور الأصلية والاشتقاق والحساب والمزوّد والفحص دون استنتاج ضياع الأموال. قد تدعم الواجهة شبكات عامة لا يدعمها ملف التوقيع المتعدد فاحترم نطاق كل سياق.

P12 | تهيئة العقدة والمزامنة | C02 | L25,L33 | Desk

التحضير: حدّد احتياجات الخصوصية، وإذا استخدمت Core فتأكد من الوصول إلى عقدة محمية ومتزامنة.

1. في قسم الأمان ثم الخصوصية والعقد اختر حساب WOW وراجع مزوّده.
2. اختر صراحة مزوّدًا عموميًا متوافقًا أو Core. عند استخدام Core أدخل نقطة الاتصال والمحفظة وبيانات الاعتماد في التطبيق فقط.
3. اسمح بالاستعلام بعد فهم البيانات التي يتلقاها كل مزوّد. لا يخفي TLS الاستعلام عن المزوّد.
4. زامن وراجع التاريخ وطرف السلسلة والتقدّم وحالة الاكتمال. عند إعادة الفحص تحقّق من الفترة التاريخية المشمولة واستمرار العمل.
5. عند ظهور 429 التزم بفترة الانتظار. لا تفترض عند الخطأ تفعيل عقدة أخرى؛ الإعداد لا يبدّل العقد بصمت.

النتيجة: المصدر والحالة معروفان. لا تعرض RPC للإنترنت أو تشارك كلمة المرور أو تحصر اكتشاف العناوين بما له رصيد. قد يكون السجل الفارغ نتيجة جزئية.

P13 | إنشاء طلب استلام واسترجاعه | Desk وL26 | Cuvex | C01,C02

التحضير: تم التحقق من الحسابات والشبكات والسياسات.

1. يفتح ويولد أو يسترجع الطلب المناسب.
2. إضافة مراقب ودافع ومقدار الانتظار فقط إذا كنت بحاجة إلى هذه البيانات الوصفية على الصعيد المحلي.
3. تحقق من عنوان المسار المتوافق مع الجهاز قبل أن يتم تحصيل متصل. إذا لم يكن هناك قبول مادي، أوقف التدريب على المحاكاة.
4. يتقاسم البيانات اللازمة فقط من خلال قناة المستلم الموثقة.
5. تحقق من دخولك، وقيمة والتأكيدات في مصدر شبكتك

النتيجة: تمّت تسوية الإتّصال، وليس فقط طلب مُصدر. وفي التوقيع المتعدد، يحتفظ بالعناوين الموضحة للمدفوعات المتأخرة ولا يعاد تخصيصها. وإذا تم بلوغ حد العناوين الجديدة التي لا تاريخ لها، يتم استرداد الطلبات المسبقة؛ ولا تُفرض الفهرسة يدويا.

P14 | الوسوم والتجميد وC02,B13 | L27 | Desk | BIP329

التحضير: معادل المعاملك UTXOs وواحدة وواحدة، كلمة المرور للصادرات المحمية.

1. يُعلّم مدخل مع سياقه بدون بيانات شخصية غير ضرورية.
2. تجميد أو رفع تجميد عن علم، ومراجعة الرصيد القابل للإنفاق. التقييد محلي.
3. صدّر بطاقات التعريف باستخدام وظيفة الحماية. احذف BIP329 كشكل لـ التشفير من الملف.
4. استيراد في نسخة مطابقة؛ تحقق من تطابق المراجع والعلامات والتجميد.
5. احتفظ بـ نسخة احتياطية من البيانات الوصفية تحديث مع كلمة المرور وفقاً لخطتك.

النتيجة: تم الحفاظ على السياقات والاختيار مفهوم. لا يجب أن يستخدم الاستيراد لفك الإفراج التلقائي عن عملات مجمدة بدون تنقيح. لا ترسل ملف الوسم إلى المدرّس: يمكنك أن تكشف عن النظراء والعلاقات حتى لو لم تتضمن مفاتيح النفقات.

P15 | إعداد دفعة وإرسال الرصيد كاملًا | C02 | L28 | Desk

التحضير: تم التحقق من الطلب و كان لديه المدخلات ما يكفي من النفقات

1. يفتح الباب ليدفع من WOW أو UTXOs أو دردشة و يؤكد الحساب و الشبكة
2. يختار المدخلات، المستلم مع الكميات، ويراجع السياقات المترابطة.
3. اختاري السعر وراجعي الرسم المطلقة، التغيير والتحذير. إذا كان هناك دست، تحقق من البدائل دون قبول الرسم مخفية.
4. لـ إرسال كامل تحقق من صافي بعد الرسم. في دردشة، تؤكد صراحة دفع جزء من المبلغ إذا لم يكن يغطي الطلب.
5. أعدّي المشروع وراجعي جميع البيانات قبل تصديرها للتوقيع.

النتيجة: ويُفهم من هذه العملية أن المقصود منها أن تكون مفهومة وأن يكون PSBT من تلك العملية. ويمكن أن تكون الاستمارة العامة متاحة على مستوى المدخلات أو المستلم على مستوى العتاد: تطبق الحدود الفعلية لل الموقّع والنقل. إذا غيرت المخرجات أو الشروط، تبدأ إعادة النظر.

P16 | توقيع PSBT وإعادته باستخدام Original | Original وMirror | L29 | C01,C02,C03

التحضير: مسودة صحيحة وبطاقة نقل متوافقة ونص مشفّر موثّق ومتوافق ووسائل فتح على انفراد. قد تستلزم النسخة القديمة غير الموثقة استعادةً وفحصًا وإنشاء نسخة جديدة قبل التوقيع، ولا تُعالج بتعديل الترويسة.

1. صدّر الطلب عبر مسار NFC المتوافق في Desk/Mirror.
2. انقل الطلب إلى Original، وقدّم النص المشفّر عند طلبه وافتحه دون إملاء بيانات الاعتماد.
3. راجع الشبكة والملخص وكامل المخرجات والرسوم والباقي والتحذيرات الإلزامية.
4. في التوقيع المتعدد Final اختر إن كنت ستراجع المعلمات الموسعة، ولا تُتمّ التأكيدات النهائية الثلاثة إلا إذا تطابق كل شيء.
5. انتظر كتابة الرد على البطاقة ثم إعادة قراءته منها.
6. اقرأ الرد باستخدام Cuvex Mirror وتحقّق منه ضمن العملية المقابلة في Desk.

النتيجة: استُلم التوقيع وربط بالمسودة، وهذا غير النشر. عند فشل الكتابة احتفظ بالحالة وأعد المحاولة وفق الإجراء. لا تستخدم بطاقة النسخ الاحتياطي وسيط دفع يمكن الاستغناء عنه.

P17 | التوقيع والاستقبال وإقرار الاستلام باستخدام BIT | BIT وDesk | L29 | C01,C02

التحضير: مسودة صحيحة ونص مشفّر موثّق ومتوافق واختيار وحدة تخزين BIT الفعلية. إذا رُفضت نسخة قديمة للتوقيع فاتبع الاستعادة والتجديد المبيّنين دون فرض التنسيق.

1. سلّم الطلب عبر USB-C من خلال خدمة Desk واتبع شاشة الجهاز لتقديم النص المشفّر.
2. افتحه على انفراد وراجع الملخص وجميع المخرجات والرسوم والتحذيرات.
3. في التوقيع المتعدد Final يمكنك مراجعة التفاصيل الموسعة ثم الإذن عبر التأكيدات النهائية الإلزامية.
4. في Desk استخدم «الاستلام من BIT» لاستيراد رد المهمة والتحقق منه.
5. تحقّق من الحفظ وإقرار الاستلام. إذا فشل الإقرار بعد الاستقبال فأعد محاولة العملية نفسها، لا عملية جديدة يختارها النموذج.

النتيجة: توقيع متحقق منه وحالة تبادل متسقة. عند انقطاع الاتصال قبل الاستلام أو بعد الحفظ احتفظ بملف تعريف الطلب، ولا تبدّل إلى برنامج ثابت آخر من الكتالوج لمطابقة رد معلّق.

P18 | استكمال المعاملة ونشرها ومتابعتها | C02 | L30,L44 | Desk

التحضير: Xالتوقيعات تم التحقق منها وعتبة كافية عند الاقتضاء.

1. راجعي مجدداً النية، المدخلات، المخرجات، الرسم، والشبكة.
2. ويُستكمل عن طريق الإجراء المناسب ويتحقق من عدم وجود أي نقص في التوقيعات أو أي شروط.
3. يأذن بنشر النتائج المحلية ويحتفظ بها. إذا فقدت رد الشبكة، استعلام قبل تكرار.
4. تتبع مخزون المعاملات المعلّقة و التأكيدات في المورّد المختار بتاريخ التزامن.
5. إذا كان السؤال هو RBF، راجع العملية الجديدة واحصل على الالتوقيعات المطلوبة. لاتفترض دالة CPFP متكاملة.

النتيجة: حالة السلسلة تم التحقق منها مع مصدرها. إلغاء مشروع لا يلغي التوقيعات المصدرة بالفعل ولا يعيد كتابة المدفوعات المؤكدة. رسالة من الدردشة أو القبض لا يحل محل المتابعة

P19 | مقارنة رمزي QR للسياسة بحرية | C03,C02 | L43 | Mirror

التحضير: أظهر الحقل في Desk وCuvex، واستخدم في التدريب عينات الدورة الاصطناعية وحدها.

1. افتح «مقارنة السياسات» واقرأ أيّ الجانبين أولًا.
2. اختر البيان المراد فحصه. يمكنك البدء بالخطوة 15 وتجاوز ما راجعته يدويًا.
3. اقرأ النظير وراجع النصّين كاملين. إن التبس رقم الخطوة فاستخدم «تحديد خطوة Desk» مع إدراك أن هذا السياق يحدَّد يدويًا.
4. فسّر «متطابق» أو «غير متطابق» لهذا الزوج الحرفي فقط. للمسافات وحالة الأحرف والترميز أثر في النتيجة.
5. ابدأ زوجًا آخر بأي ترتيب. اخرج أو انتقل إلى الخلفية لإنهاء المقارنة وفق سلوك المحو المراجَع.

النتيجة: مقارنة محلية محددة لا تثبت المصدر أو الجلسة أو الموافقة الشاملة أو التفعيل. وضّح أي اختلاف بالرجوع إلى مصدريه دون تطبيع النص لفرض نتيجة OK.

P20 | تفعيل الدردشة واستعادتها ونقلها | Desk وL36,L39 | Cuvex | C02

التحضير: DEV أو الإنتاج المختار، اسم مستعار و مفتاح شات على الجهاز، أبدا في المسار.

1. افتح أو استخرج الرابط من سياق النص المشفّر.
2. يختار اسماء جديدة أو نقل موجود والخصائص المتوافقة التي يحددها التطبيق.
3. إدخال أو قراءة مفتاح Chat فقط في التدفق الخاص. لا تستخدم بذرة الاسترداد أو PIN أو مفتاح من WOW
4. فعّل تشغيل الخدمة؛ إذا كان مُتبقّى مُعلّق استخدم إجراء الاستكمال أو التأكّد، دون إعطاءه بالصحيح.
5. التحقق من الاستمرارية مع الاتصالات بعد النقل وتجنب الاستخدام المتزامن لنفس الاسم المستعار في عدة أفرقة.

النتيجة: هويّة مفعّلة أو مسترجعة في البيئة الصحيحة. التاريخ و الجلسات السابقة لا تسترد تلقائياً بحرف مفتاح chat أو بنسخة كاملة من Desk. احفظ حدود المادة المتوفرة.

P21 | التحقق من هوية جهة اتصال | C02 | L36,L48 | Desk

التحضير: تم الاتفاق مسبقاً مع الشخص

1. أضف الاسم المستعار و استفسر عن هويته العامة من خلالتطبيق
2. قارن البصمة من القناة الموثقة ليس فقط في المحادثة الجديدة
3. إذا قمت بإستكشاف، تجنب المعلومات العامة أو الأسرار التي يعاد استخدامها في خدمات أخرى.
4. فقط بعد تسوية الخلافات. عند تغيير الهوية، توقف الدفع والتنسيق حتى يتم التحقق.
5. ويوثّق طريقة التحقق دون تخزين ردود حساسة في الدورة.

النتيجة: الثقة في سياق الاتصال، لا ضمانة لكل طلباتك المستقبلية. الصوت يمكن أن يقلد وفريق شرعي ملتزم. وتحتفظ كل عملية باستعراضها.

P22 | طلب عنوان وطلب دفعة والدفع عبر الدردشة | Desk وCuvex | L37 | C02,C01

التحضير: تم التحقق من الاتصال مع حساب WOW المتوافق.

1. اختر طلب العنوان، أو الرد بالعنوان، أو طلب الدفع حسب قصدك.
2. فحص الطلب الأصلي، الشبكة، المبلغ والمذكرة قبل إرساله.
3. وللدفع، يفتح عملية الإعداد من الحساب المناسب، ويختار UTXOs والسعر، وينقح صافي المبلغ.
4. الرخصة في Cuvex لإجراء النموذج. الـ chat لا يُوقّعُ آلياً.
5. يتبعه النشر وتأكيد من مصدرك؛ تسوية المدفوعات الجزئية الصريحة مع الطلب الأصلي.

النتيجة: التنسيق مع الحفاظ على تنقيح الحفظ. لا تعادل. يمكن لرابط إلى مستكشف إرسال معلومات إلى طرف ثالث: تقييم استخدامها قبل فتحها.

P23 | مشاركة نص مشفّر تم تلقيه وربطه | C02 | L38 | Desk

التحضير: ويمكن التحقق من الاتصال وتحديد وسائل الوصول التي يمكن الحصول عليها.

1. انتقِ النص المشفّر ex من عملية الدردشة وافحص الجسم.
2. () لا مرفقات كلمة المرور أو بذرة الاسترداد أو مفتاح Chat، كتعليق.
3. ويتحقق المتلقي من مصدر الشيء المتوافق ويربطه بتصرف الاستلام.
4. قيّم ما هي القدرة التي تحصل عليها الآن وما الذي ستحصل عليه إذا حصلت على وثائق تفحّص كافية.
5. مع وجود خطة واقعية للإلغاء: مسح الرسائل لا يسحب نسخ خارجية أو مفاتيح معروفة.

النتيجة: نقل واع لـ التشفير. هذا ليس دفعاً، ولا يُدرج في حد ذاته مفتاح إلى التوقيع المتعدد. إذا طلب الملحق التوجه إلى صفحة مجهولة لـ فك التشفير، أوقف التدفق.

P24 | النسخ الشامل لـ Desk واستعادته | C02 | L15,L21 | Desk

التحضير: مخزن بيانات للتدريب ووجهة نسخ تحت سيطرتك.

1. افتح نسخ المخزن، وعيّن كلمة المرور المطلوبة، واحتفظ بما يمكّنك من معرفة أنها تخص هذه النسخة بالذات.
2. احفظ النسخة خارج جهاز الاستخدام الوحيد وتحقق من المصدر والسلامة وفق الإجراء.
3. استعد النسخة في بيئة اختبار منفصلة وافحص الحسابات والإعدادات والبيانات المشمولة.
4. راجع الاستثناءات. لا تفترض شمول الدردشة وجلساتها وسجلها. سياسة التوقيع المتعدد والمفاتيح الخاصة ليست عناصر قابلة للاستبدال.
5. كرّر النسخ بعد التغييرات المهمة واحتفظ بتعليمات الاستعادة.

النتيجة: نسخة معروفة النطاق وكلمة المرور. تحتفظ النسخ القديمة بكلمات المرور السابقة. عند تغيير الوصول أو الانكشاف قيّم تلك النسخ أيضًا، فلا يكفي تعديل المخزن الحالي.

P25 | إنشاء محفظة متعددة التوقيعات وقبولها | Desk وCuvex | C01,C02 | L41,L42

التحضير: مشاركون مستقلون وجهات اتصال متحقق منها واتفاق على الشبكة والحدود الفعلية.

1. يختار المنشئ الاسم وM/N والشبكة والمشاركين ومدة الصلاحية التشغيلية.
2. قدّم المفتاح العام الموسّع الصحيح مع البصمة ومسار BIP48 وفق الإجراء المتوافق.
3. يراجع كل مشارك الدعوة ويقبل أو يرفض ويقدّم مواده العامة. لا يشارك بذرة الاسترداد أبدًا.
4. أنشئ السياسة كاملة وجهّز التحقق منها على كل جهاز.
5. احتفظ بنسخ السياسة قبل التمويل وتحقق من العنوان المرجعي ومن إمكانية الاستعادة.

النتيجة: مقترح كامل قابل للتحقق. قبول الدعوة لا يغني عن مراجعة العتاد. عند مشاركة Original احترم حدّه الأقصى البالغ ستة مفاتيح وسعة NFC؛ لا يوسّع BIT قدرات المشاركين الآخرين.

P26 | التحقق من السياسة وتلقي التأكيد | Desk وL43 | Cuvex | C01,C02,C03

التحضير: السياسة الكاملة نفسها للجميع، وملف تعريف صحيح للبرنامج الثابت، وجهاز دون عمليات متنافسة.

1. ابدأ التحقق من السياسة في السياق المتوافق. يتطلب Original تحديد ملف التعريف المثبت صراحة، أما BIT فيتفاوض على القدرات وفق مواصفاته.
2. سلّم الطلب عبر NFC/Mirror أو USB-C بحسب الطراز.
3. راجع حقول السياسة على الجهاز، واستعمل Mirror اختياريًا لمقارنة أزواج تختارها دون ترتيب إلزامي.
4. أكمل التأكيد على الجهاز وأعد رده عبر وسيلة النقل المناسبة.
5. تحقّق في Desk من الرد المرتبط بالطلب. لا تستبدل هذه الخطوة بإشارة OK مرئية في المقارن.

النتيجة: مراجعة مرتبطة بالطلب ضمن نطاق تلك المراجعة. الكتالوج لا يشهد عن بُعد على البرنامج الثابت والجهاز ليس مخزنًا دائمًا للسياسات. عند FIRMWARE_CAPABILITY_REQUIRED راجع أولًا إصدار Desk وتركيبة الطراز والبناء.

P27 | طلب التوقيعات واستلامها ونقل مسؤولية التنسيق | Desk | Cuvex | L44 | C01,C02و

التحضير: تم التحقق منه، تم تحديد العملية، تم الاتفاق على المستلم.

1. تجهز المدخلات والمخرجات والرسم ومذكرات وتطلب التوقيعات من المشاركين المتوافقين.
2. كل مشارك يفحص و يوقع على فريقه من قبل فرع النقل
3. يتلقى كل توقيع ويتحقق منه ويحفظه؛ يحل القضايا المعلقة دون تغيير المواصفات المحتفظ بها.
4. وإذا تم نقل التنسيق، فإن المتلقي يقبل التدفق ويتحقق من الحالة. لا تغيير M/N أو ملكية مفاتيح.
5. عند الوصول إلى العتبة، يراجع وينتهي قبل نشره. تتبع المعاملة عبر الشبكة.

النتيجة: التنسيق مع الأدلة المتمايزة. تقرير سير المنسق ليس تحقق محلي منك ولا يؤدي إلغاء أو رفض تطبيق ما بالضرورة إلى تدمير التوقيعات التي احتفظت بها أطراف ثالثة.

P28 | تصدير المحفظة متعددة التوقيعات واستعادتها وحذفها محليًا | Desk | L45 | C02

التحضير: ونسخة مشفّرة بـ كلمة المرور

1. صدّر استعادة عافيتك من خلالإجراء Desk. ويستخدم التدفق الحالي حاوية CVXMSBK1 موثقة لهذا التصدير.
2. يحتفظ بنسخة و كلمة المرور مع مخاطر منفصلة. لا تستنتج التشفير كأرشيف تاريخي.
3. لاسترجاع المعلومات، تقدم نسختين كلمة المرور ومفتاح عام من المشاركين ذوي المصدر الصحيح عن طريق الشبكة العالمية أو Mirror، حسب الاقتضاء.
4. -السياسة، الشبكة، التوجيه والإكتشاف قبل التشغيل .
5. للحذف محلياً، إقرأ النطاق والتأكيد واحتفظ بنسخة إذا كنت تريد الحفاظ على الاستعادة. إعادة الاستعادة بعد الاستعادة واضحة.

النتيجة: أو التخلص المحلي الواعي لا تُحوّل الأموال، ولا تُحذف مفاتيح من الموقّع الأخرى، ولا تلغى العمليات التي يحتفظ بها الآخرون.

P29 | الاستعادة الاستثنائية على الحاسوب | Desk | L47 | C02

التحضير: (ب) معلومات أساسية عن البيانات المأخوذة من المصادر المقبولة، والبيئة النظيفة المعدة، والرقم نسخة احتياطية. قد تكشف هذه العملية سرّاً لـ (PC)، وتستخدم بيانات تعلّم في الدورة.

1. تبدأ بالتعافي المحلي من السياق الصحيح وتقرأ حدود الشكل والإشعارات.
2. تقبل الخطر عن علم و توقف الشبكة كما يتطلب التدفق النافذة تتحقق من الحالة قبل أن تسمح بالإستمرار
3. فقط أدخل وثائق التفويض اللازمة إلى النافذة الخاصة. لا تُتَقَدَّمْ، لا تُصَبَّبُ في الدورةِ، لا تَشتركُ في الدعمِ.
4. فعّل العرض فقط في مكان واحد بدون كاميرات أو مساعدين يستمعون إليه؛ احترام التوقيت والإغلاق.
5. يُنهي، ويراجع ما هو التعرض الذي قد يكون موجوداً، ويخطط للانتقال إلى مفاتيح الجديدة عند الاقتضاء.

النتيجة: شفاء استثنائي، وليس ضمان لمسح الطب الشرعي أو معادلة مع العتاد معزول. إذا لم يكن هناك توثيق أو شكل أو مواد دخول، لا تجرب أدوات الإنترنت مع نسختك الحقيقية.

P30 | مراجعة التفضيلات والقياسات الحيوية والقفل | L40 | Desk | C02

التحضير: Xكلمة المرورالمعرفةونسخة احتياطية تم اختبارها قبل تعديل الأمن

1. الولوج و الحصار يراجع كلمة المرور, القياسات الحيوية متاح, التعطل و الإغلاق عند الدخول
2. ويشمل التأخير بعد صدور الأحكام والحد الأقصى المعدّل قبل تغييره.
3. حافظ على الحذف الاختياري معطل حتى تفهم الشروط و العتبة و الاستعادة لا تثبت ذلك في الإنتاج.
4. في حالة تفضيلات مواءمة اللغة، والموضوع، والعملة، ومزامنة 3 أو 5 دقيقة، والصوت.
5. إذا كنت تسجل روابط بيتكوين: تأكد من أن فتح طلب ما يبقي على فتح القفل والاختيار والاستعراض؛ ولا يدفع وحده.

النتيجة: اضبط المُتوصّل مُعْسَفُ مُفْكّب. أما القياسات الحيوية من نظام التشغيل فيعتمد على المعدات ولا يحل محل كلمة المرور أو نسخة احتياطية. التفضيلات البصرية لا تغير سياسة بيتكوين.

P31 | حذف السجلات مع تمييز نطاق الأثر | C02 | L22,L45 | Desk

التحضير: تحديد ما إذا كنت ستحذف النص المشفّر محلي، حساب، WOW، chat أو التوقيع المتعدد، وما هي النسخة التي ستحتفظ بها.

1. إقرأ الشيءَ المُنتقىَ وإشعاره. يؤكد الاسم المستعار الدقيق أو الشرط الصريح عندما يطلب منه التطبيق
2. تصدير واثبات نسخة إذا كنت بحاجة إلى استعادة هذه الحالة في وقت لاحق.
3. ولا يحذف سوى الغرض المقصود ويتحقق من الجمعيات التي تحتفظ بالتدفق أو تسحبه.
4. تحقق مما إذا كانت هناك عمليات أو مشاركون خارجيون. لا تفترضي أن الرسائل تتلاشى أو التوقيعات أو ملفات الفرق الأخرى
5. سجل التغيير في مخزونك الخاص بدون بيانات حساسة في الدورة

النتيجة: الحالة المحلية تُدار عن علم. ولا يغير أي من هذه الأسهم في حد ذاته صحائف بيانات UTXOs الممولة، أو يدمر بذرة الاسترداد معروفة لدى أطراف ثالثة، أو يعيد تحويل المعاملات المؤكدة.

P32 | تشخيص الأعطال دون كشف الأسرار | Desk وMirror | C02,C03 | L23,L30,L48

التحضير: دوّن الوقت التقريبي والنظام والمعمارية والإصدار والمرحلة. تجنّب تكرار عملية حساسة ما دمت تجهل حالتها.

1. حدّد هل وقع الخطأ في البحث أو الربط أو القراءة أو الكتابة أو التحقق أو التوقيع أو الإرجاع أو الشبكة أو العرض.
2. انسخ رمز الخطأ ونصّه دون رموز QR أو بيانات خاصة، واستخدم تشخيصات التطبيق عند الحاجة.
3. راجع الملف قبل مشاركته، ولا ترفق نسخة المخزن أو النص المشفّر أو البذرة أو مفتاح الدردشة أو الواصف أو بيانات اعتماد RPC.
4. عند مشكلة واجهة استخدم مشهدًا اصطناعيًا وسجّل حجم النافذة والتكبير وعناصر التحكم المخفية.
5. أرسل عبر القناة الرسمية النتيجة المتوقعة وخطوات إعادة الحالة. لا ترسل الدورة رسائل للدعم تلقائيًا.

النتيجة: تقرير يتيح التحقيق بأقل البيانات. إذا لم توجد أدلة على مرحلة سجّلها «معلّقة» لا «مكتملة». لا يحتاج الإرشاد الصوتي إلى الدخول عن بُعد إلى جهاز الحفظ.

مسرد البيتكوين والحفظ الذاتي

بيتكوين

شبكة ومجموعة قواعد لنقل القيمة والتحقق من سجلها بلا مدير وحيد للسجل.

BTC

الوحدة النقدية لبيتكوين، ويساوي BTC واحد مئة مليون ساتوشي.

ساتوشي

وحدة في السلسلة الأساسية تعادل جزءًا واحدًا من مئة مليون من BTC.

سلسلة الكتل

سجلّ كتل مترابطة يُتحقق منها وفق قواعد محددة. ولا يصف المصطلح وحده كل خصائص الشبكة.

الكتلة

مجموعة بيانات تضم معاملات وترويسة يمكن التحقق منها.

العقدة الكاملة

برنامج يتحقق من التزام الكتل والمعاملات التي يقبلها بالقواعد.

التعدين

بناء الكتل بإثبات العمل وفق قواعد الشبكة.

إثبات العمل

آلية تتطلب عملًا حسابيًا قابلًا للتحقق لاقتراح كتلة.

الإجماع

توافق المشاركين بشأن القواعد والسجل الصالح الذي يقبلونه.

سياسة مخزون المعاملات المعلّقة

قواعد محلية لقبول المعاملات وإعادة بثها، لا تطابق بالضرورة قواعد الإجماع.

مخزون المعاملات المعلّقة (mempool)

مجموعة المعاملات غير المؤكدة التي تحتفظ بها عقدة محليًا.

التأكيد

إدراج المعاملة في كتلة من السلسلة المقبولة وازدياد عمق تلك الكتلة لاحقًا.

إعادة تنظيم السلسلة

استبدال جزء من السلسلة المقبولة، مما قد يغيّر التأكيدات.

UTXO

مخرج معاملة لم يُنفَق بعد ويمكن إنفاقه باستيفاء شروطه.

المدخل

إشارة إلى مخرج سابق والبيانات اللازمة للإذن بإنفاقه.

المخرج

قيمة وشرط إنفاق تنشئهما معاملة.

الباقي

مخرج يعيد جزءًا من قيمة المدخلات إلى سيطرة صاحبها بعد الدفع وخصم الرسوم.

رسوم المعاملة

الفرق بين مجموع قيم المدخلات ومجموع قيم المخرجات.

vbyte

وحدة للحجم الافتراضي تُستخدم للتعبير عن الكلفة النسبية للمعاملة.

sat لكل vbyte

معدل الرسوم بالساتوشي لكل وحدة من الحجم الافتراضي.

المخرج الضئيل (dust)

مخرج صغير وفق السياسة المتبعة وكلفة إنفاقه. تعتمد عتبته على السياق والسكربت.

RBF

استبدال معاملة غير مؤكدة بموجب سياسات متوافقة، وليس إلغاءً مضمونًا.

CPFP

استخدام معاملة لاحقة لزيادة الحافز إلى إدراجها مع المعاملة السابقة التي تنفق منها.

قيمة التجزئة (hash)

بصمة بيانات تساعد في فحص سلامتها. لا تشفّرها ولا تحدد بمفردها هوية منشئها.

المفتاح الخاص

القدرة التشفيرية على إنتاج أذونات وفق النظام المعني.

المفتاح العام

بيانات تتيح التحقق من التوقيعات وبناء شروط معيّنة دون كشف المفتاح الخاص.

التوقيع الرقمي

إثبات تشفيري للإذن برسالة محددة، ولا يخفي محتواها.

التشفير

حماية السرية باستخدام مفتاح وخوارزمية.

التشفير الموثّق

تشفير يتضمن التحقق من العبث وفق تصميمه.

AES GCM

عائلة من آليات التشفير الموثّق تُستخدم في تنسيقات المنظومة. تعتمد خصائصها على التنفيذ وإدارة المفاتيح.

عبارة التذكّر

تمثيل مادة التوليد وبيانات التحقّق بكلمات وفق تنسيق محدد.

البذرة

مادة تُشتق منها المفاتيح. يُستعمل الاسم في الكلام الدارج للكلمات أيضًا، لذا يلزم توضيح المقصود.

الإنتروبيا

تعذّر توقّع مادة التوليد. لا تتحقق باختيار كلمات يسهل تذكرها.

المجموع الاختباري (checksum)

قيمة تحقق تكشف أخطاء معيّنة ولا توثّق هوية المنشئ.

BIP39

مواصفة لعبارات التذكّر واشتقاق البذور مع عبارة مرور اختيارية.

عبارة مرور BIP39

مُدخل إضافي للاشتقاق قد تؤدي قيمته المختلفة إلى محفظة صالحة أخرى فارغة.

BIP32

مواصفة الاشتقاق الهرمي للمفاتيح.

مسار الاشتقاق

تسلسل الفروع المستخدم لاشتقاق مفاتيح من جذر.

الاشتقاق المحصّن

خطوة اشتقاق يُرمز إليها عادة بعلامة اقتباس أو بالحرف h، ولها خصائص تختلف عن الاشتقاق العام العادي.

xpub

مفتاح عام موسّع يتضمن سياق الاشتقاق، وهو حساس للخصوصية.

xprv

مفتاح خاص موسّع يجب عدم مشاركته أو استيراده إلى دورة تعليمية.

بصمة المفتاح الرئيسي

معرّف قصير للجذر يفيد في المطابقة ولا يكفي لإثبات الهوية.

الواصف

تعبير يصف بناء سكربتات من مفاتيح واشتقاقات. قد يكون عامًا أو يتضمن مواد خاصة.

محفظة المراقبة فقط

محفظة للمشاهدة تفتقر إلى قدرات التوقيع الخاصة الكافية للتوقيع بمفردها.

WOW

تسمية حسابات المراقبة وإدارة المحافظ في منظومة Cuvex.

المحفظة الساخنة

أداة قادرة على التوقيع في بيئة متصلة.

الحفظ الذاتي

نموذج يحتفظ فيه المستخدم بالقدرة التقنية على الإنفاق منفردًا أو بالاشتراك مع غيره وفق سياسته.

أمين الحفظ

جهة تسيطر على قدرة الإنفاق لحساب العميل وتطبّق شروطها للوصول.

نص Cuvex المشفّر

عنصر مشفّر يحمي سرًا، ولا يمثّل في حد ذاته معاملة أو رصيدًا.

كلمة مرور Desk

حماية للدخول إلى المخزن المحلي. وهي مختلفة عن البذرة وكلمة مرور النص المشفّر.

مفتاح الدردشة

سرّ لاستعادة هوية الدردشة. قد يشبه مفتاحًا عامًا في ظاهره لكنه ليس عامًا.

رمز PIN للإقران

رمز مؤقت لجلسة اتصال وليس كلمة مرور لحفظ الأصول.

الفصل الهوائي (air gap)

فصل تشغيلي بين البيئات. تظل البيانات المنقولة بينها بحاجة إلى التحقق.

NFC

تقنية اتصال قصير المدى للبطاقات وأجهزة القراءة المتوافقة.

USB Mass Storage

واجهة تبادل الملفات في طراز BIT، وتتطلب بروتوكولها وفحوصها وإقرارات استلامها الخاصة.

PSBT

حاوية للمعلومات والتوقيعات تُستخدم لتنسيق بناء المعاملات والإذن بها.

PSBT v0

نسخة التنسيق المحددة في BIP174 والمستخدمة في ملف التوقيع المتعدد لإصدار Final الذي روجع.

PSBT v2

النسخة المحددة في BIP370. كون إصدار المعاملة 2 لا يدل على أنها تستخدم هذه النسخة من PSBT.

SIGHASH ALL

طريقة تحديد ما يلتزم به التوقيع في ملف التعريف المراجَع. نطاقها الفني جزء من التحقق من العملية.

P2WPKH

نوع من شروط SegWit لمفتاح مفرد، يرتبط عادة بحسابات BIP84.

P2WSH

شرط SegWit يلتزم بسكربت، ويُستخدم في التوقيع المتعدد لإصدار Final الذي روجع.

P2TR

نوع مخرج Taproot. دعم الدفع إليه لا يعني دعم توقيع معاملة تنفق منه.

sortedmulti

بنية توقيع متعدد ترتّب المفاتيح ترتيبًا حتميًا لتوليد السكربتات.

عتبة M من N

يشترط الحصول على M من الأذونات بين N مشاركين، وفق السياسة المحددة.

MuSig2

بروتوكول لتجميع توقيعات Schnorr يقوم أساسًا على N من N، لا على عتبة اعتباطية.

Taproot

مجموعة آليات بيتكوين للإنفاق والالتزام بواسطة مسار مفتاح أو مسار سكربت.

Miniscript

لغة لوصف بعض سياسات السكربت وتحليلها، ولم تُنفّذ في ملف تعريف Final الذي روجع.

Regtest

شبكة مختبر محلية يتحكم فيها مُنشئ البيئة، ولا تحمل قيمة اقتصادية.

Signet

شبكة اختبار ذات خصائص مميزة، لا يمكن افتراضيًا استعمالها بدل regtest.

Mainnet

شبكة بيتكوين الرئيسية للاستخدام الاقتصادي الفعلي.

حد فجوة العناوين

معيار لاكتشاف العناوين بناء على عدد العناوين المتتالية بلا سجل، ويتوقف نطاقه على المحفظة.

التحكم في اختيار المخرجات

الاختيار الواعي لمخرجات UTXO التي سيجري إنفاقها.

الدمج

جمع المخرجات لتقليل التجزؤ، وله آثار على الكلفة والخصوصية.

الهوية المستعارة

استخدام معرّفات لا تعرض الاسم المدني مباشرة دون أن يضمن ذلك إخفاء الهوية.

إخفاء الهوية

تعذّر التمييز في سياق معين من منظور مراقبين محددين. لا تضمنه تسمية يضعها تطبيق.

البيانات الوصفية

معلومات عن الاتصال أو النشاط، مثل الأوقات والأحجام والصلات، تختلف عن المحتوى نفسه.

CoinJoin

بناء تعاوني للمعاملة يصعّب بعض الاستنتاجات دون ضمان إخفاء الهوية على الدوام.

Payjoin

دفعة تعاونية تشتمل على مدخلات من الدافع والمتلقي وفق بروتوكول متوافق.

Tor

شبكة وأدوات لحماية الاتصال. يجب ضبط استخدامها والتحقق منه لكل تطبيق.

VPN

قناة تنقل جزءًا من الثقة في الاتصال إلى مشغّلها، ولا تخفي سجل السلسلة.

Lightning

نظام مدفوعات عبر قنوات يختلف في متطلباته ومخاطره عن التحويل على السلسلة.

الفاتورة (invoice)

طلب دفع منظّم ينبغي تحديد تنسيقه وطريقته.

RPC

واجهة لاستدعاء خدمة مثل Bitcoin Core ويجب تأمينها والتحقق من هوية مستخدميها.

TLS

حماية للنقل من تهديدات محددة، لكن الخادم المستلم يبقى قادرًا على رؤية الطلبات.

SRTP

حماية للصوت في أجزاء معيّنة من اتصالات VoIP، ولا تعني تلقائيًا سريته عن المشغّل.

عدم تكرار الأثر

خاصية تمنع تكرار الأثر عند إعادة إرسال طلب يحمل المعرّف نفسه.

Webhook

إشعار بحدث ينتقل بين خوادم، ويجب التحقق من أصالته وما إذا كان مكررًا.

RAG

استرجاع مقاطع معرفية لإسناد الإجابة بسياق ومعلومات عن الإصدار.

إعادة الشرح للتحقق من الفهم

فحص التعلّم بطلب شرح ما فهمه المتعلم بكلماته الخاصة.

التصيد الاحتيالي

خداع يقوم على انتحال الصفة وسياق مقنع للحصول على وصول أو دفع الضحية إلى إجراء.

الهندسة الاجتماعية

التلاعب بقرارات الأشخاص، وقد يستغل معلومات صحيحة وشعورًا بالإلحاح.

توثيق Apple للتوزيع

إجراء من Apple لضبط التوزيع، يختلف عن تدقيق المنتج أو الاختبار الفعلي لكل مساراته.

إثبات الحالة

دليل على حالة وفق آلية محددة. كتالوج توافق Desk ليس قياسًا عن بُعد.

MiCA

إطار أوروبي ينظّم أصولًا مشفّرة وخدمات معيّنة، ولا يضمن عائدًا أو تعويضًا كاملًا.

Travel Rule

التزامات بتوفير المعلومات للتحويلات الواقعة ضمن نطاقها، ولا يسقطها الحفظ الذاتي.

نقطة الاستئناف

موضع لاستئناف التعلّم يسجّل الحد الأدنى من البيانات دون معلومات المحفظة.

اختبر ما تعلّمته

تدرّب دون أموال حقيقية. التقييم متاح بحرية ولا يتطلب حسابًا.

من يأذن بالإنفاق عند الاستخدام المعتاد لجهاز Cuvex؟

1. الجهاز بعد مراجعة المستخدم
2. المدرّس الصوتي
3. خادم الدورة

> **عرض الإجابة: الجهاز بعد مراجعة المستخدم**
> يبقى مسار الإذن بالإنفاق على جهاز Cuvex.

كم ساتوشي يعادل 0.001 BTC؟

1. 1,000
2. 100,000
3. 1,000,000

> **عرض الإجابة: 100,000**
> يعادل BTC واحد 100,000,000 sat.

المدخلات 120,000 sat والمخرجات 119,000 sat. كم تبلغ الرسوم؟

1. 1,000 sat
2. 119,000 sat
3. 1 sat/vB دون أي بيانات إضافية

> **عرض الإجابة: 1,000 sat**
> الفرق بين القيمتين هو إجمالي الرسوم.

ما حالة المعاملة بعد توقيعها وقبل بثّها؟

1. مؤكَّدة
2. لا رجعة فيها لأنها موقّعة
3. مأذون بها ولكنها ليست بالضرورة منشورة

> **عرض الإجابة: مأذون بها ولكنها ليست بالضرورة منشورة**
> التوقيع والنشر مرحلتان مختلفتان.

كم تكون كلفة 200 vB بسعر 6 sat/vB؟

1. 206 sat
2. 1,200 sat
3. 6% من مبلغ التحويل

> **عرض الإجابة: 1,200 sat**
> اضرب الحجم الافتراضي في سعر وحدة الرسوم.

ماذا تتحقق منه قبل السحب من منصة تداول؟

1. أقل الرسوم فحسب
2. توافق الأصل والشبكة والعنوان وصافي المبلغ
3. بذرة الطرف المقابل

> **عرض الإجابة: توافق الأصل والشبكة والعنوان وصافي المبلغ**
> ليست كل شبكة تستخدم رمز BTC هي شبكة بيتكوين الأساسية.

ماذا يفعل التوقيع الرقمي وحده؟

1. يخفي الرسالة بأكملها
2. يثبت الإذن برسالة يمكن التحقق منها وفق نظام التوقيع
3. يمحو البيانات المنشورة

> **عرض الإجابة: يثبت الإذن برسالة يمكن التحقق منها وفق نظام التوقيع**
> السرية تحتاج إلى آلية أخرى.

ما الذي قد يترتب على تغيير عبارة مرور BIP39؟

1. إنشاء محفظة صالحة أخرى تبدو فارغة
2. إعادة ضبطها دائمًا عبر البريد الإلكتروني
3. تغيير السجل العلني للمدفوعات السابقة

> **عرض الإجابة: إنشاء محفظة صالحة أخرى تبدو فارغة**
> تدخل عبارة المرور في عملية الاشتقاق.

كيف يجب التعامل مع xpub الخاص بحساب؟

1. بيانات لا تترتب عليها أي آثار
2. مطابق لبذرة خاصة
3. معلومات حسّاسة من منظور الخصوصية

> **عرض الإجابة: معلومات حسّاسة من منظور الخصوصية**
> يمكنه توسيع نطاق تتبّع النشاط.

لماذا قد لا تكفي بذرة واحدة في المحفظة متعددة التوقيعات؟

1. لغياب السياسة والأذونات التي تستوفي العتبة
2. لأن بيتكوين لا يسمح باستعادة أي شيء
3. لأنك تحتاج إلى اللون الأصلي للتطبيق

> **عرض الإجابة: لغياب السياسة والأذونات التي تستوفي العتبة**
> حفظ السياسة والاحتفاظ بقدرات التوقيع الخاصة مطلبان مختلفان.

ماذا تفعل إذا رُفضت نتيجة النرد في خوارزمية Final التي روجعت؟

1. أعيد رمي القطعة النقدية وحدها إلى أن تُقبل
2. أعيد رمي القطعة النقدية وأحجار النرد الأربعة
3. أختار كلمة أعرفها

> **عرض الإجابة: أعيد رمي القطعة النقدية وأحجار النرد الأربعة**
> قد تؤدي إعادة جزء فقط من المجموعة إلى انحياز في توزيع النتائج.

ماذا يعني اشتراط كلمتي مرور لفتح بذرة محفظة أحادية التوقيع؟

1. اشتراط مفتاحين على السلسلة
2. أنها محفظة Taproot متعددة التوقيعات
3. عتبة الوصول إلى السر منفصلة عن عتبة الإنفاق في بيتكوين

> **عرض الإجابة: عتبة الوصول إلى السر منفصلة عن عتبة الإنفاق في بيتكوين**
> التشفير لا يغيّر سكربت الإنفاق.

ماذا ينبغي أن تراعي عند تقييم النسخة الاحتياطية الشاملة من Desk؟

1. تتضمن بالضرورة كل الدردشة
2. لها نطاق واستثناءات، ولا يُفترض أنها تشمل الدردشة
3. تحدّث جميع النسخ القديمة

> **عرض الإجابة: لها نطاق واستثناءات، ولا يُفترض أنها تشمل الدردشة**
> استعادة الهوية واستعادة الرسائل أمران مختلفان.

ماذا تحقق لك عقدتك الخاصة إذا أُعدّت جيدًا؟

1. تمنع كل تسرّب
2. تقلل الاعتماد على الاستعلام لدى أطراف ثالثة وتتيح التحقق
3. تسترجع المفاتيح المفقودة

> **عرض الإجابة: تقلل الاعتماد على الاستعلام لدى أطراف ثالثة وتتيح التحقق**
> لا تضمن إخفاء الهوية أو استعادة الأسرار.

ماذا يعني تجميد UTXO في Desk؟

1. قيد محلي ينفّذه التطبيق
2. تغيير شرط من شروط الإجماع
3. إبطال نسخ البذرة الأخرى

> **عرض الإجابة: قيد محلي ينفّذه التطبيق**
> لا يمنع الإنفاق على مستوى الشبكة بأسرها.

ما الذي تفعله إذا انقطع الاتصال لحظة النشر؟

1. أدفع مرة أخرى فورًا
2. أحذف المحفظة
3. أتحقق أولًا مما إذا كانت الدفعة قد بُثّت بالفعل

> **عرض الإجابة: أتحقق أولًا مما إذا كانت الدفعة قد بُثّت بالفعل**
> انتهاء مهلة الاتصال لا يثبت أن العملية لم تُنفَّذ.

ما الأثر المحتمل لإعادة استخدام العناوين أو جمع UTXOs من سياقات مختلفة؟

1. تسهيل اكتشاف الصلات بينها
2. محو السجل
3. ضمان إخفاء الهوية

> **عرض الإجابة: تسهيل اكتشاف الصلات بينها**
> تعتمد الخصوصية على السياق والاستخدام اللاحق.

هل يؤدي فتح Tor Browser إلى إعداد Desk تلقائيًا؟

1. نعم
2. لا
3. فقط إذا كان المظهر داكنًا

> **عرض الإجابة: لا**
> يجب التحقق من مسار الاتصال الخاص بكل تطبيق.

ما مفتاح الدردشة الذي يشبه xpub؟

1. معلومة صالحة للنشر
2. عنوان استلام دفعات
3. سر يخص الهوية

> **عرض الإجابة: سر يخص الهوية**
> تتحدد حساسية البيانات بالغرض من استخدامها.

ماذا تعني رسالة دردشة تفيد بأن المبلغ دُفع؟

1. تغني عن التأكيدات
2. يلزم التحقق مستقلًا من الدفع على الشبكة
3. تغيّر شبكة طلب الدفع

> **عرض الإجابة: يلزم التحقق مستقلًا من الدفع على الشبكة**
> حالة الرسالة ليست حالة الدفعة.

ما المواصفات التي يستخدمها ملف التعريف متعدد التوقيعات في إصدار Final الذي روجع؟

1. MuSig2 وPSBT v2
2. P2WSH وsortedmulti وBIP48 وPSBT v0
3. أي سكربت في بيتكوين

> **عرض الإجابة: P2WSH وsortedmulti وBIP48 وPSBT v0**
> التمنيات أو الأسماء التجارية لا توسّع نطاق الدعم.

من أين يمكنك بدء المقارنة في Mirror 12.12؟

1. من البند 1 فقط
2. من أي بند تختاره، بما فيه البند 15
3. من البند الأخير فقط بعد جميع البنود

> **عرض الإجابة: من أي بند تختاره، بما فيه البند 15**
> يمكن مقارنة كل زوج بحرية واستقلال عن بقية الأزواج.

ما الذي تثبته نتيجة «متطابق» في Mirror؟

1. الموافقة الشاملة
2. أصالة مصدر رمزي QR
3. التطابق الحرفي للزوج المقارَن

> **عرض الإجابة: التطابق الحرفي للزوج المقارَن**
> لا تزال بقية المراجعة والاستجابة معلّقة.

إذا انكشفت البذرة، فماذا يترتب على تغيير كلمة مرور Desk؟

1. يلغي صلاحية المهاجم
2. لا يلغي المفاتيح المشتقة من تلك البذرة
3. يمحو جميع النسخ

> **عرض الإجابة: لا يلغي المفاتيح المشتقة من تلك البذرة**
> ينبغي تقييم طريقة آمنة لنقل السيطرة.

ماذا ينبغي ذكره عند إنهاء التدريب العملي؟

1. ما قُرئ وما حوكي وما اختُبر على أجهزة فعلية وما لم يكتمل
2. عدد الساعات المبيعة فقط
3. وعد بحفظ لا يمكن اختراقه

> **عرض الإجابة: ما قُرئ وما حوكي وما اختُبر على أجهزة فعلية وما لم يكتمل**
> لكل نوع من الأدلة نطاق مختلف.