CUVEX

CUVEX ACADEMY · 0.1

Öğren. Anla. Kontrolü eline al.

Bitcoin ve kendi varlıklarınızı saklama adım adım anlatılıyor. Kurs, kılavuz, sözlük ve alıştırmalar ücretsizdir, kayıt gerekmez. Nereden başlayacağınızı siz seçin.

Ücretsiz · kayıt gerekmez

Tüm bölümler

1. Öğrenme alanınızı hazırlayın
2. Dijital para ve güven sorunu
3. Bitcoin’in tarihi ve sınırları
4. Satoshi ve doğru hesaplama
5. Kendi tehdit modeliniz
6. Düğümler, madencilik ve mutabakat
7. UTXO’lar ve işlemde para üstü
8. Mempool, onaylar ve yeniden düzenlenmeler
9. İşlem ücretleri, sanal boyut ve işlem değiştirme
10. Ağlar, adresler ve ödeme talepleri
11. Hash, dijital imzalar ve şifreleme
12. Kurtarma ifadesi, ek parola ve parola
13. Anahtar türetme, xpub ve tanımlayıcılar
14. Cüzdan ve saklama modeli seçimi
15. Geri yüklenebilen yedekler
16. Original ve BIT’i tanıyın
17. Fiziksel entropiyle kurtarma ifadesi oluşturma
18. Cuvex ile gizli bilgiyi şifreleme ve çözme
19. Şifreleme eşikleri ve biyometri
20. Kopyaları çoğaltma, saklama ve doğrulama
21. Cuvex Desk’i kurma ve koruma
22. Kriptogramları bağlama ve WOW hesaplarını düzenleme
23. Mirror ile Desk’i eşleştirme
24. Mirror üzerinden NFC, USB-C ve QR kodu okuma
25. Kamuya açık hizmet sağlayıcılar ve kendi düğümünüz
26. Bitcoin alma ve adres doğrulama
27. UTXO’ları etiketleme, dondurma ve seçme
28. Ödeme hazırlama ve inceleme
29. Original ve BIT ile imzalama
30. İşlemi tamamlama, yayımlama ve sorunları çözme
31. Bitcoin’de hangi bilgiler gözlemlenebilir?
32. Bağlamları ayırma ve para üstünü yönetme
33. Ağ gizliliği, Tor ve VPN
34. CoinJoin, Payjoin ve güncel sınırlamalar
35. Gerçek olaylardan çıkarılabilecek dersler

36. Sohbet kimliği oluşturma ve kişileri doğrulama
37. Sohbet üzerinden satoshi isteme ve ödeme
38. Kriptogramları bilinçli biçimde paylaşma
39. Sohbeti geri yükleme ve üstverilerini anlama
40. Günlük ayarlar ve izinleri gözden geçirme
41. Çok imzalı cüzdan tasarlama
42. Davet oluşturma ve anahtar sağlama
43. Mirror ile politikaları istenen sırada doğrulama
44. İmzaları koordine etme ve çok imzalı işlemi yayımlama
45. Çok imzalı cüzdanı kurtarma ve değiştirme
46. Aygıt yazılımını belirlenmiş adımlarla güncelleme
47. Kayıp, arıza ve acil durumda kurtarma
48. Kimlik avı, destek ve sesli dolandırıcılık
49. Gizlilik, yasal yükümlülükler ve kişisel kayıtlar
50. Miras, süreklilik ve yıllık tatbikat
51. Fiyat, tasarruf ve temel analiz
52. Bitcoin’i nereden alacağınızı seçme
53. Hesaplar, emirler ve emir gerçekleştirme maliyetleri
54. Mumlar, göstergeler ve teknik analizde yanlılıklar
55. Marj, vadeli işlemler ve otomasyon
56. Lightning ve diğer katmanlar
57. Taproot, MuSig2 ve kuantum sonrası gelecek
58. Birlikte çalışabilirlik ve üreticiden bağımsızlaşma
59. Regtest ile teknik laboratuvar
60. Bitirme projesi ve süreklilik planı
61. Öğrenci kılavuzu
62. Bitcoin ve öz saklama sözlüğü
63. Öğrendiklerinizi sınayın

M01

Öğrenme alanınızı hazırlayın

Amaç

Kurs için hazırlık yapın, üç cihazın görevini ayırt edin ve hangi bilgilerin eğitmenle asla paylaşılmayacağını belirleyin.

Konuyu anlayın

Bitcoin’i kendi kararlarınız doğrultusunda almayı, saklamayı, harcamayı ve kurtarmayı öğreneceksiniz. Kursun sonunda bir kararı onaylamadan önce gerekçesini açıklayabilmelisiniz. Kursu yardım almadan okuyabilirsiniz. Sesli eğitmen açıklamalar, sorular ve rehberlik sunar. Varlıklarınızı görmesi veya cihazlarınızı kontrol etmesi gerekmez.

Cuvex gizli bilgileri koruyan ve işlemleri kendi ekranında onaylamanızı sağlayan cihazdır. Desk bilgisayarda kriptogramları, izleme cüzdanlarını, ödemeleri ve koordinasyonu yönetir. Mirror desteklenen işlemler için yerel bir köprü kurar ve verileri karşılaştırır. Kendi başına çalışan bir cüzdan veya imzalayıcı değildir. Hangi yolu kullanabileceğiniz modelinize ve sürümünüze bağlıdır.

Kursu ve Desk’i mümkünse ayrı ekranlarda açın. Telefonu ve Cuvex’i yanınızda bulundurun. Tek ekranınız varsa uygulamalar arasında geçiş yapın ve gizli bilgileri girerken ekranı görüntülü görüşmede paylaşmayın. Alıştırma bitmeden görüşme sona erebilir. Ara vermek başarısızlık değildir. Yalnızca ders kimliğini, geldiğiniz adımı ve karşılaştığınız güçlüğü kaydedin.

Ne insan eğitmene ne de yapay zekâya kurtarma ifadeleri, BIP39 ek parolaları, parolalar, sohbet anahtarı (Clave Chat), PIN, özel dosyalar veya eksiksiz satın alma kodları verilmelidir. xpub’ınıza, gerçek bir tanımlayıcınıza (descriptor) veya adresinize de ihtiyaçları yoktur. Bu son bilgiler harcama yetkisi vermese bile hareketlerinizi açığa çıkarır. Hata mesajını tarif edin ve laboratuvarın kurgusal verilerini kullanın.

Uygulama

1. Bilgisayarınızı, telefonunuzu ve elinizdeki Cuvex modelini tanımlayın. Sürümlerini kişisel defterinize yazın.
2. Gerçek varlıklarınızı sakladığınız ortamdan ayrı, bakiyesiz bir eğitim ortamı kurun. Alıştırma için gerçek cüzdanınızın kurtarma ifadesini içe aktarmayın.
3. Bu dersi açıp duraklatma düğmesini, yardımı ve sözlüğü bulun. Biri gizli bilgi isterse o etkileşimi sonlandırın.

Öğrendiklerinizi gösterin

Kimin imzaladığını, kimin ağı sorguladığını ve kimin veri taşıdığını açıklayın. Bir sonraki adıma geçmek için bu görevleri yardım almadan ayırt edebilmelisiniz.

Sık sorulan soru

Eğitmenle her gün konuşmam gerekiyor mu? Hayır. Kendi kendinize çalışabilir, bir oturumu tekrarlayabilir ve yalnızca belirli bir işlemde yardım isteyebilirsiniz. Kursa erişim hakkınız, sesli hizmet için kalan sürenizden bağımsızdır.

Ara verme noktası

L01 tamamlandı. Cihazlar belirlendi. Kursa hiçbir gizli bilgi kaydedilmedi.

Eğitmen, doğru yazdığınızı kontrol etmek için kurtarma ifadenizi istiyor. Ne yaparsınız?

1. Yavaşça söylerim.
2. Talebi reddeder, ifadeyi yalnızca kendi güvenli ortamımda kontrol ederim.
3. Yalnızca ilk birkaç kelimeyi gönderirim.

> **Yanıtı göster: Talebi reddeder, ifadeyi yalnızca kendi güvenli ortamımda kontrol ederim.**
> Gizli bir bilginin hiçbir parçası eğitim hizmetiyle paylaşılmaz.

M01

Dijital para ve güven sorunu

Amaç

Cüzdan açmadan önce Bitcoin’in çözmeye çalıştığı sorunu anlayın.

Konuyu anlayın

Banka bakiyesi, bir kuruluşun yönettiği kayıttır. Kuruluş müşteriyi doğrular, hangi transferi işleyeceğine karar verir ve hesapları tutar. Sıradan bir dijital dosya kolayca kopyalanır. Örneğin fotoğraf göndermek bir kopyasını saklamanıza engel olmaz. Dijital birimin para olarak işlev görebilmesi için iki kez harcanmasının önlenmesi gerekir.

Bitcoin doğrulama kurallarını, imzaları ve ortak bir işlem geçmişini bir araya getirir. Tüm kaydı tek bir kuruluşa emanet etmek yerine bağımsız katılımcılar, işlemin kurallara uyup uymadığını kontrol edebilir. Arzın sınırlı kalması bu kuralların doğrulanmaya ve kabul edilmeye devam etmesine bağlıdır. Bir para görseli veya borsanın yayımladığı fiyat arzı sınırlamaz.

Öz saklama sorumlulukları değiştirir. Saklama kuruluşundan izin almadan harcama yetkisini elinizde tutabilirsiniz. Ancak tüm yedekleri yok ederek veya yanlış ödemeyi imzalayarak bu yetkiyi ya da fonlarınızı kaybedebilirsiniz. İşlem yapma özgürlüğü güvenlik, koordinasyon, yayımlama için bağlantı ve geçerli yükümlülüklere uyma ihtiyacını kaldırmaz.

Ağ ve protokol olan Bitcoin’i para birimi BTC ile karıştırmayın. Başka ağlar da blok zinciri terimini kullanabilir ama farklı özellikler sunabilir. Bir şirketin «bitcoin» adını verdiği alacak da kendi anahtarlarınızın kontrolündeki bir Bitcoin çıktısına sahip olmakla aynı değildir.

Uygulama

1. Üç durumu karşılaştırın: banka bakiyesi, borsa bakiyesi ve kendi anahtarlarınızla kontrol ettiğiniz UTXO.
2. Her durumda bakiyeyi taşımanızı kimin engelleyebileceğini ve erişim bilgilerini unutursanız kimin yardım edebileceğini yazın.
3. Bir fotoğrafı kopyalamanın ve aynı çıktıyı iki kez harcamaya çalışmanın sonuçlarını anlatın.

Öğrendiklerinizi gösterin

Bakiye ile imzalama yetkisinin neden ayrı kavramlar olduğunu kendi sözlerinizle açıklayın. Teknik terimleri ezberlemeniz gerekmez.

Sık sorulan soru

Öz saklama tüm aracıların ortadan kalkması demek mi? Satın almak, sorgulamak veya iletişim kurmak için hizmet seçebilirsiniz. Önemli olan bu hizmetlerin hangi yetkiyi elinde tuttuğu ve hangi verileri aldığıdır.

Ara verme noktası

Sorumluluk karşılaştırmanızı gerçek hesap adlarını eklemeden saklayın.

Dijital imza, aşağıdaki parasal sorunlardan hangisini tek başına çözmez?

1. Aynı çıktıyı iki kez harcama girişimini engellemek.
2. Bir anahtarla yetkilendirme yapıldığını kanıtlamak.
3. İmzalanmış mesajın değiştiğini saptamak.

> **Yanıtı göster: Aynı çıktıyı iki kez harcama girişimini engellemek.**
> İmzalar yetkiyi doğrular. Birbiriyle bağdaşmayan harcamalar arasındaki sıralamayı kurallar ve mutabakat belirler.

M01

Bitcoin’in tarihi ve sınırları

Amaç

Bitcoin’in ortaya çıkışını tarihsel bağlamına yerleştirin ve tarihsel gerçeklerle ticari anlatıları ayırın.

Konuyu anlayın

Satoshi Nakamoto’nun belgesi 2008’de yayıldı, ağ 2009’da çalışmaya başladı. Belge, kriptografi, iş ispatı ve dijital paraya ilişkin önceki fikirlerden yararlanan eşler arası elektronik nakit öneriyordu. Yazılımı veya bir işlemi doğrulamak için Satoshi’nin gerçek kimliğini bilmek gerekmez.

Gelişim, tek bir şirketin kuralları tek taraflı değiştirmesiyle gerçekleşmez. Geliştiriciler değişiklik önerir ve inceler, düğüm işletenler yazılım seçer, madenciler blok oluşturur, kullanıcılarla hizmetler de neyi kabul edeceklerine karar verir. Bu dağılım anlaşmazlık doğurabilir. Çatallanma ve uygulama güncellemesi aynı değildir.

Bir düğüm, arkasında çok iş olsa bile kendi kurallarını ihlal eden bloğu reddedebilir. Mutabakat bilgisayar sayısına göre basit oylama değildir. Bir düğümü binlerce kez çalıştırmak kendiliğinden daha çok karar gücü vermez. Benzer şekilde madencilik çoğunluğu da bu sıfatla bir kullanıcının özel anahtarını edinmez.

Bitcoin bilinçli sınırlar ve ödünleşimler içerir: blok kapasitesi, doğrulama maliyeti, değişken onay süreleri ve herkese açık kayıt. Varsayılan olarak idari yolla ödeme geri alma veya tam gizlilik sunmaz. Katmanlar ve uygulamalar belirli ihtiyaçları gidermeye çalışırken yeni bağımlılıklar getirir.

Uygulama

1. İlk belgeyi, ağın başlatılmasını, SegWit’in benimsenmesini ve Taproot’un etkinleştirilmesini bir zaman çizelgesine yerleştirin. Tarihleri yayımlamadan önce kaynaklardan doğrulayın.
2. «Şirket fiyatı garanti ediyor», «düğüm doğruluyor» ve «madenci blok öneriyor» ifadelerini ticari vaat veya teknik işlev olarak sınıflandırın.
3. Ödemeleri geri alacak bir yönetici bulunmamasının bir yararını ve bir maliyetini açıklayın.

Öğrendiklerinizi gösterin

Mutabakat kuralı, yerel politika ve şirket kararı arasındaki farkı belirtin. Kullandığınız uygulama ağın tamamı değildir.

Sık sorulan soru

En yeni yazılım her zaman parasal kuralları değiştirir mi? Hayır. Sürümler hataları da giderebilir, performansı artırabilir veya yerel politikaları değiştirebilir. Sürüm notlarını ve uyumluluk bilgilerini okuyun.

Ara verme noktası

Doğrulanabilir bir özelliği ve ek kanıt gerektiren bir iddiayı not edin.

Bir blok geçerli yetkilendirmesi olmayan bir harcama içeriyor. Madencilerin çoğunluğu bunu geçerli kılabilir mi?

1. Evet, oran %51’i aşarsa.
2. Yalnızca borsa bunu duyurursa.
3. Bu harcamayı reddeden kuralları uygulayan bir düğüm için hayır.

> **Yanıtı göster: Bu harcamayı reddeden kuralları uygulayan bir düğüm için hayır.**
> Birikmiş iş, düğümün kurallarına göre geçerli olan geçmişler arasında karşılaştırılır.

M01

Satoshi ve doğru hesaplama

Amaç

BTC ile satoshi arasında dönüşüm yapın ve tutarları piyasa kuruna bağlı kalmadan kontrol edin.

Konuyu anlayın

Bir BTC 100.000.000 satoshiye eşittir. «sat» başka bir para değil, birimdir. Temel zincirde tutarlar satoshi cinsinden tam sayılardır. 0,001 BTC = 100.000 sat, 0,00001000 BTC = 1.000 sat. Arayüzün ondalık ayracı dile bağlıdır. Göz kararı sıfır eklemeyin.

Kur, BTC tutarını belirli bir anda EUR veya USD gibi bir para birimine çevirir. Kontrol ettiğiniz satoshi sayısını değiştirmez. 100.000 sat tutuyorsanız fiyat değiştiğinde satoshi sayınız aynı kalır. Desk’te kur, kaynağı ve tarihi görülen bir referanstır. BTC bakiyesi doğru olsa da eski bir kur hatalı ekonomik karara yol açabilir.

Bir ödemede alıcı tutarını, ağ ücretini ve toplam harcamayı ayırın. 50.000 sat gönderilir ve ücret 600 sat olursa başka kendi çıktılarınız yoksa cüzdanınızdan çıkan değer 50.600 sat olur. «Tamamını gönder» genellikle ücreti karşılamak için alıcının net tutarını kullanılabilir bakiyeden düşük hesaplar.

Kurstaki örnekler aritmetik alıştırmalarıdır. Piyasa fiyatı veya tavsiye edilen ücret oranı değildir. İmzalamadan önce ilgili ekranda birimi, ağı, alıcıyı ve toplam maliyeti kontrol edin. Sesli eğitmen «elli bin satoshi» derken ekranda «50.000 sat» gösterebilir. Şüpheli bir konuşma dökümünden hareketle tutar belirlenmemelidir.

Uygulama

1. 250.000 sat’ı BTC’ye çevirin: 0,0025 BTC. 0,00025000 BTC’yi satoshiye çevirin: 25.000 sat.
2. 900 sat ücretle 75.000 sat gönderimini hesaplayın. Toplam harcama 75.900 sat’tır.
3. Simülatörde 120.000 sat girdi, 70.000 sat gönderim ve 1.000 sat ücret kullanın. Para üstünün 49.000 sat olduğunu doğrulayın.

Öğrendiklerinizi gösterin

Tutarı BTC ve sat olarak okuyun, hangi tutarın ücreti içerdiğini açıklayın. Emin değilseniz işlemi duraklatın.

Sık sorulan soru

Bir bitcoinin tamamını mı almalıyım? Hayır. Sağlayıcının asgari tutar ve maliyet koşulları dâhilinde kesirli miktar alabilirsiniz.

Ara verme noktası

Yalnızca alıştırma sonuçlarınızı saklayın.

80.000 sat’ınız var ve 1.200 sat ücretle tamamını göndermek istiyorsunuz. Alıcıya ne kadar ulaşır?

1. 80.000 sat.
2. 78.800 sat.
3. 81.200 sat.

> **Yanıtı göster: 78.800 sat.**
> Başka çıktı bulunmayan bu örnekte alıcı, harcanabilir bakiyeden ücret çıkarıldıktan sonra kalan tutarı alır.

Kendi tehdit modeliniz

Amaç

Kayıp, hırsızlık, aldatma ve veri ifşasına karşı riskle orantılı önlemler seçin.

Konuyu anlayın

Güvenlik, niyetinize uygun hareket edebilme yeteneğinin korunmasıdır. Mahremiyet, verilerinizi ve ilişkilerinizi kimin bileceğini denetlemektir. Kullanılabilirlik gerektiğinde erişebilmektir. Herkese kapalı bir kasa size de kapalı kalabilir. Çok kolay erişilen bir kopya ise gereğinden fazla bilgi açığa çıkarabilir.

Varlıkları, karşı tarafları ve olası kazaları belirleyin. Korunacak varlıklar arasında anahtarlar, yedekler, geçmiş, kopyaların konumları ve kişilerin kimlikleri vardır. Kötü amaçlı yazılım, kimlik avı, yangın, unutma, zorlama, arıza, ölüm ve kendi hatalarınız olası risklerdir. Hepsi aynı araçla azaltılamaz.

Basit bir matrise yaklaşık olasılığı, etkiyi ve somut önlemi yazın. Uzun bir parola tahmin riskini azaltır ama sizin onayladığınız sahte bir alıcıyı düzeltmez. Aynı çantadaki iki kopya çantanın kaybına çözüm değildir. Cihazları ve yedekleri tek kişinin kontrolünde olan çoklu imza ortak bir arıza noktası bırakabilir.

Kurs ve eğitmen de modele dâhildir. Satın almalar, aramalar, bağlantı süreleri ve ilerleme üstveri oluşturabilir. Kurs sitesi dersi kişiselleştirmek için adres veya bakiye istememelidir. Desk veya Mirror’ın olağan kayıt işlemi gerektirmemesi mağazanın, ses sağlayıcısının veya sorguladığınız üçüncü tarafın etkinliğinizden habersiz olduğunu göstermez.

Uygulama

1. Varlık tutarlarını veya tam konumları belirtmeden en önemli üç riskinizi yazın.
2. Her risk için önleme, fark etme ve kurtarma yöntemini seçin. Örneğin kart kaybı için iki ayrı kopya, envanter ve geri yükleme denemesi.
3. Satın almayı, aramayı, bakiye sorgusunu ve herkese açık işlemi hangi kişi veya sistemlerin gözlemleyebileceğini ayırın.

Öğrendiklerinizi gösterin

Bir sonraki önleminizin hangi somut riski giderdiğini açıklayın. Sürdüremeyeceğiniz veya mirasçılarınıza anlatamayacağınız karmaşıklık eklemeyin.

Sık sorulan soru

Daha fazla cihaz her zaman daha güvenli mi? Yalnızca ortak bağımlılıkları azaltıyorsa ve kurtarmayı sınayabiliyorsanız. Cihaz eklemek bakım yükünü ve karışıklık ihtimalini de artırır.

Ara verme noktası

Planı kişisel belgelerinizde saklayın. Kursa yalnızca «tehdit modeli gözden geçirildi» yazın.

Yerel bir yangında tüm kopyaları kaybetme riskini hangi önlem en çok azaltır?

1. Kartın rengini değiştirmek.
2. İki kopyayı aynı çekmeceye koymak.
3. Doğrulanmış kopyaları riskleri birbirinden bağımsız yerlerde saklamak.

> **Yanıtı göster: Doğrulanmış kopyaları riskleri birbirinden bağımsız yerlerde saklamak.**
> Yedekler, asıl kopyayı tehlikeye atan aynı olaya dayanabilmelidir.

M02

Düğümler, madencilik ve mutabakat

Amaç

Düğümlerin neyi doğruladığını ve madenciliğin ne kattığını açıklayın.

Konuyu anlayın

Tam düğüm blok ve işlemleri alır, kurallara uyulduğunu doğrular ve zincirin kendi görünümünü tutar. Bir sitenin bildirdiği bakiyeye güvenmesi gerekmez. Madencilik, iş ispatıyla blok önerme sürecidir. Madenciler geçerli işlemleri seçer ve kabul edilebilir bir blok bulmak için yarışır.

İş ispatı geçmişi yeniden yazmayı maliyetli kılar. Birden fazla geçerli zincir ortaya çıktığında belirleyici olan, zorluğu dikkate almadan blok saymak değil, birikmiş iş miktarıdır. Blok aralıkları değişir. On dakika hedeflenen ortalamadır, bir sonraki ödemenin kesin zamanı değildir.

Madenci ödülü blok sübvansiyonu ile ücretlerden oluşur. Sübvansiyon blok yüksekliklerine göre belirlenmiş takvimle azalır. Ücret, dâhil edilen işlemlere bağlıdır. Daha yüksek ücret hatalı bir imzayı geçerli kılmaz. Ekonomik güvenlik ve saldırı maliyeti, yeni bir ödemeyi matematiksel olarak geri döndürülemez yapmaz.

Kendi düğümünüz üçüncü taraflara sorgu iletme gereksinimini azaltır ve bağımsız doğrulama sağlar. Yine de işletim sistemini, erişimi ve bağlantıyı korumanız gerekir. Düğüm eşitlenmemişse veya uygulama başka bir sunucuyu sorguluyorsa düğümü açık tutmak tek başına bu yararları sağlamaz.

Uygulama

1. Şu görevlerin kime ait olduğunu belirleyin: imzayı doğrulamak, bloğa alınacak işlemleri seçmek, kurtarma ifadenizi korumak ve bir ödemeyi kabul edip etmemeye karar vermek.
2. «Bitcoinlerimi madenci saklar» ifadesinin neden yanlış olduğunu açıklayın.
3. Laboratuvar ağında blok yüksekliğini ve eşitlemeyi gözlemleyin. RPC erişim bilgilerini yayımlamayın.

Öğrendiklerinizi gösterin

Doğrulama ile önerme arasındaki farkı anlatın. Benzetme kullanabilirsiniz, ancak sonunda gerçek teknik işlevi doğru belirtin.

Sık sorulan soru

Bitcoin kullanmak için madencilik yapmam gerekir mi? Hayır. Başlamak için kendi düğümünüz de şart değildir, ancak sağlayıcınıza ne kadar güvenmeniz gerektiğini bilmelisiniz.

Ara verme noktası

Laboratuvar sağlayıcısını türüyle kaydedin, özel URL eklemeyin.

Doğru yapılandırılmış bir tam düğüm kullanıcıya ne sağlar?

1. Kabul ettiği zincirin kurallara uyduğunu doğrulama olanağı.
2. Kayıp her anahtarı kurtarma olanağı.
3. Fiyat artışı garantisi.

> **Yanıtı göster: Kabul ettiği zincirin kurallara uyduğunu doğrulama olanağı.**
> Doğrulama ile varlıkları saklama farklı görevlerdir.

M02

UTXO’lar ve işlemde para üstü

Amaç

Bir işlemi, önceki çıktıların harcanması ve yeni çıktıların oluşturulması olarak okuyun.

Konuyu anlayın

UTXO, önceki bir işlemin henüz harcanmamış çıktısıdır. Cüzdan kontrol edebildiği çıktıları belirleyerek bakiyeyi hesaplar. Banka tablosundaki gibi tutarı azaltılan ortak bir hesap yoktur. Girdi, işlem kimliği ve konumuyla önceki bir çıktıya işaret eder.

Bir UTXO harcandığında tamamı tüketilir. Değerinden daha az ödeme yapacaksanız genellikle alıcıya bir çıktı, kendi kontrolünüzdeki para üstüne de başka bir çıktı oluşturursunuz. 120.000 sat girdi, 70.000 sat alıcı ve 1.000 sat ücretle para üstü 49.000 sat olur. Girdilerin toplamı, çıktılarla ücretin toplamına eşit olmalıdır.

Adres bir UTXO değildir ve birden çok çıktı alabilir. Adres mutlaka bir kişi de değildir. İşlem kimliği herkese açık olabilir ancak onu kimliğinizle ilişkilendirmek veya hangi çıktının kime ait olduğunu açıklamak, zincirin tek başına göstermediği bilgi ekler.

Bu yapı mahremiyet açısından önemlidir. Girdileri birleştirmek ortak kontrol izlenimi verebilir. Para üstü gelecekteki ödemeleri ilişkilendirebilir. Ortaklaşa oluşturulan işlemler bulunduğu için bu çıkarım her durumda kanıt değildir. Coin control, birleştirmenin sonuçlarını anlayarak hangi çıktıların harcanacağını seçmektir.

Uygulama

1. 40.000, 60.000 ve 200.000 sat değerinde üç hayalî girdi çizin. Yalnızca ilk ikisini kullanarak 1.000 sat ücretle 70.000 sat ödeyin.
2. Para üstünün 29.000 sat olduğunu ve üçüncü girdinin kullanılmadığını doğrulayın.
3. Yalnızca 200.000 sat’lık girdiyi kullanarak tekrarlayın. Para üstü 129.000 sat olur. İşlem boyutlarının eşit olduğunu varsaymadan olası maliyeti ve ortaya çıkan bağlantıları karşılaştırın.

Öğrendiklerinizi gösterin

Kurs şemasında girdiyi, alıcıyı, para üstünü ve ücreti bulun. Bir çıktıyı tanımlayamıyorsanız gerçek işlem imzalamayın.

Sık sorulan soru

Cüzdanıma dönen her şey para üstü müdür? Hayır. Başka bir kendi adresinize aktarım olabilir. Sınıflandırma, tutara bakıp tahmin etmeyi değil, politikayı ve türetmeyi bilmeyi gerektirir.

Ara verme noktası

Hayalî şemayı saklayın. Gerçek varlıklarınızın ekran görüntüsünü saklamayın.

100.000 sat değerinde bir girdi, 30.000 ve 69.200 sat değerinde iki çıktı oluşturuyor. Ücret nedir?

1. 69.200 sat.
2. 800 sat.
3. 30.000 sat.

> **Yanıtı göster: 800 sat.**
> 100.000 eksi 99.200, 800 sat eder.

M02

Mempool, onaylar ve yeniden düzenlenmeler

Amaç

Hazırlanmış, ağa duyurulmuş ve onaylanmış işlemleri ayırt edin.

Konuyu anlayın

Mempool, bir düğümün politikasına göre yerel olarak tuttuğu onaylanmamış işlemler kümesidir. Dünyada herkes için aynı tek bir mempool yoktur. Gezginin ödemeyi göstermesi o hizmetin ödemeden haberi olduğunu gösterir. Tüm düğümlerin kabul edeceğini veya belirli sürede onaylanacağını garanti etmez.

PSBT hazırlamak hiçbir şeyi yayımlamaz. İmza yetkilendirme sağlar. Sonlandırma, ağa duyurulabilecek işlemi oluşturur. Yayımlama ağda iletmeyi dener. Onay, işlemin doğrulama kaynağınızın kabul ettiği zincirde bir bloğa girmesidir. İkinci onay, üstüne bir blok daha eklenmesidir; alıcının ikinci imzası değildir.

Yeniden düzenlemede zincirin bir bölümü değişebilir. İşlem onay kaybedebilir veya tekrar beklemeye geçebilir. Daha yüksek riskli ödemelerde taraflar genellikle daha çok onay ister. Tüm tutar ve durumlarda her riski kaldıran bir sayı yoktur.

Desk kayıtlı bir durum gösteriyorsa eşitleme tarihine bakın. Eski bir anlık görüntüdeki «onaylandı» sonucu güncel durumu zorunlu olarak yansıtmaz. Gönderim görünmüyorsa yerel kimliğini saklayın. Yeniden hazırlamadan önce yayımlanmayı ve geçmişi inceleyin. Aceleyle tekrar etmek ikinci bir geçerli ödeme oluşturabilir.

Uygulama

1. Kartları sıraya koyun: taslak, PSBT, imza, son işlem, ağa duyurma, bloğa dâhil edilme.
2. Yayımlamadan sonra bağlantı kesintisini canlandırın. Yeniden ödeme yapmadan önce neleri kontrol edeceğinizi belirleyin.
3. Bir satıcıya sohbetteki «ödendi» mesajının neden ağdan doğrulamanın yerini tutmadığını anlatın.

Öğrendiklerinizi gösterin

İşlemin durumunu, bilgi kaynağını ve tarihini bunları garanti gibi sunmadan belirtebilmelisiniz.

Sık sorulan soru

Desk’i kapatmak yayımlanmış işlemi iptal eder mi? Hayır. Başka düğümler ve katılımcılar işlemi saklayabilir. Yerel taslağı iptal etmenin kapsamı farklıdır.

Ara verme noktası

Simülasyondaki durumu not edin. Eğitmene gerçek kimlik numaraları vermeyin.

Yayımla düğmesine basmanızın hemen ardından bilgisayarın bağlantısı kesiliyor. Önce ne yaparsınız?

1. Aynı ödemeyi baştan hazırlarım.
2. Cüzdanı silerim.
3. Yeniden bağlanıp işlemi ve girdilerini kontrol ederim.

> **Yanıtı göster: Yeniden bağlanıp işlemi ve girdilerini kontrol ederim.**
> Yanıt alınamaması, ağda yayılmanın başarısız olduğunu kanıtlamaz.

İşlem ücretleri, sanal boyut ve işlem değiştirme

Amaç

Maliyetleri tahmin edin, vbyte başına sat oranını yorumlayın ve RBF ile CPFP'yi anlayın.

Konuyu anlayın

Ağ ücreti, girdilerle çıktılar arasındaki farktır. Ücretin rekabet düzeyi genellikle sanal bayt başına satoshi, yani sat/vB cinsinden ifade edilir. Doğrudan gönderilen parasal değere bağlı değildir. Çok girdi küçük ödemeyi pahalılaştırabilir. Az girdili büyük ödeme daha az yer kaplayabilir.

200 vB ve 5 sat/vB örneğinde ücret 1.000 sat'tır. Son boyut imzalara ve yapıya bağlı olabileceğinden imzalamadan önce yalnızca tahmin vardır. Desk yaklaşık hız seçenekleri ve elle oran belirleme sunar. «Hızlı» etiketi belirli zamanda onay taahhüdü değildir.

RBF, onaylanmamış işlemlerin belirli koşullarda değiştirilmesine ilişkin politikadır. Daha yüksek ücretli, öncekiyle çakışan bir harcama önermeye izin verir. Düğüm politikaları zamanla değiştiği için değiştirmeme işaretini ödeme garantisi saymayın. Değiştirme yeni inceleme ve gereken imzaları gerektirir.

CPFP, bekleyen işlemin bir çıktısını harcayarak ana ve alt işlemi birlikte cazip kılar. Harcanabilir bir çıktıyı kontrol etmeyi, geçerli politikalara uymayı ve maliyeti karşılamayı gerektirir. Bu bir Bitcoin kavramıdır. Öğrencinin Cuvex sürümünde CPFP düğmesi bulunduğu varsayılmaz.

Dust, uygulanan politikalar ve tahmini harcama maliyetlerine göre çok küçük bir çıktıdır. Her betik için evrensel bir eşik yoktur. Sabit bir sayıyı mutabakat kuralı gibi öğretmeyin. Para üstü kullanışlı değilse tutarı, girdileri veya tüm bakiyeyi aktarma seçeneğini ve gerçek ücreti inceleyin.

Uygulama

1. 180 vB için 8 sat/vB oranında ücreti hesaplayın: 1.440 sat. Laboratuvar bütçenizi aşıp aşmadığını kontrol edin.
2. Tek girdili bir işlemi on girdili bir işlemle karşılaştırın. Gönderilen tutarın maliyeti tahmin etmek için neden yeterli olmadığını açıklayın.
3. Bekleyen bir işlem canlandırın. Otomatik uyumluluk varsaymadan bekleme, RBF veya CPFP'yi araştırma arasında karar verin.

Öğrendiklerinizi gösterin

Ücret oranını, toplam ücreti ve gönderim tutarına göre maliyeti gerekçelendirin. Anlamadığınız ücreti reddedin.

Sık sorulan soru

RBF önceki ödemeyi kesin olarak iptal eder mi? Hayır. Onaylanana dek sürümler birbiriyle yarışır ve ağda yayılma önemlidir. İptal vaadine dayanarak mal teslim etmeyin.

Ara verme noktası

Alıştırmadaki kararınızı ve gerekçesini kaydedin.

250 vB için 4 sat/vB oranında ücret nedir?

1. 1.000 sat.
2. 254 sat.
3. Gönderilen tutarın %4’ü.

> **Yanıtı göster: 1.000 sat.**
> Sanal boyut ile ücret oranı çarpıldığında tahmini ücret bulunur.

M02

Ağlar, adresler ve ödeme talepleri

Amaç

Kopyalama veya taramadan önce ağı, adres biçimini ve ödeme talimatlarını tanıyın.

Konuyu anlayın

Mainnet gerçek ekonomik değeri olan bitcoin taşır. Test ağları geliştirme ve öğrenme içindir ancak birbirinin yerine kullanılamaz. Regtest laboratuvarı kuranın yönettiği yerel ağdır. Signet ve testnet'in kendi kuralları ve ekosistemleri vardır. Signet'teki bir tek imza işlevi, Cuvex çoklu imza profilinin bu ağı desteklediğini göstermez.

Adresler alma koşullarını kodlar. Mainnet'te 1, 3, bc1q veya bc1p ile başlayan biçimler bulunur. Ön ek bir aileyi tanımaya yardım eder. Alıcıyı doğrulamaz, imzalayıcı uyumluluğunu garanti etmez ve biçim doğrulamasının tamamının yerini tutmaz.

QR görsel bir taşıyıcıdır. Adres, ödeme isteği, tanımlayıcı veya zararlı metin taşıyabilir. Taramak kaynağın gerçekliğini doğrulamaz. bitcoin: bağlantısı tutar ve mesaj ekleyebilir. BIP21'in yerini alan güncel referans BIP321'dir. İncelenen Desk uygulaması BIP21 terimlerini ve uyumluluğunu korur. Bir standardın gelişmesi uygulamanın anlayabildiği biçimleri kendiliğinden genişletmez.

Lightning ödeme isteği zincir üstü bir adres değildir. Son kullanma zamanı ve başka alanlar içerebilir. Uygun iş akışı yoksa zincir üstü gönderim alanına yapıştırmayın. Başka bir ağda BTC adını taşıyan bir token da kendiliğinden yerel bitcoin sayılmaz.

Uygulama

1. Harcanabilir adres kullanmadan kursun etiketli örneklerini sınıflandırın: adres, bitcoin: URI'si, Lightning ödeme isteği ve tanımlayıcı.
2. Laboratuvarda seçilen ağı belirleyin. İncelenen Cuvex çoklu imza profili mainnet/regtest'i destekler.
3. Gerçek işlemden önce alıcının talep ettiği metnin tamamını kimliği doğrulanmış kanaldan karşılaştırın.

Öğrendiklerinizi gösterin

Ağını veya ödeme yöntemini bilmediğiniz isteği reddedebilmeli ve doğrulanması gerekenleri açıklayabilmelisiniz.

Sık sorulan soru

Borsanın gösterdiği her ağdan BTC gönderebilir miyim? Hayır. Çekim ağı gerçekte kullanılacak alma ağıyla eşleşmelidir. Yalnızca en düşük ücrete göre seçim yapmayın.

Ara verme noktası

Yalnızca eğitim ağının türünü kaydedin.

bc1 ile başlayan bir alım adresi, farklı bir token ağı üzerinden BTC çekimi için tek başına yeterli değildir. Hangi kontrol eksik?

1. Alıcının takma adını değiştirmek.
2. Çekimin Bitcoin zincirinde yapıldığını ve tüm verilerin eşleştiğini doğrulamak.
3. Kurtarma ifadesini borsaya girmek.

> **Yanıtı göster: Çekimin Bitcoin zincirinde yapıldığını ve tüm verilerin eşleştiğini doğrulamak.**
> Varlık, ağ ve alma yöntemi birbiriyle uyumlu olmalıdır.

M03

Hash, dijital imzalar ve şifreleme

Amaç

Bütünlük, yetkilendirme ve gizlilik arasındaki farkı anlayın.

Konuyu anlayın

Hash işlevi veriden sabit uzunlukta bir parmak izi üretir. Bilinen bir izle karşılaştırmak değişiklikleri saptamaya yardımcı olur. Dosyayı şifrelemez veya yayımlayanın kimliğini tek başına belirlemez. Dosyayı ve hash'i ele geçirilmiş aynı siteden indirirseniz saldırgan ikisini de değiştirmiş olabilir.

Özel anahtar imza üretir, ona karşılık gelen açık anahtar imzaları doğrular. İmza, algoritma ve kurallarına göre yetkilendirmeyi belirli bir mesaja bağlar. İmzalanan içeriği gizlemez. Bitcoin'de geçerli imza, bir çıktıyı harcamak için gereken koşulların bir parçasıdır.

Şifrelemenin amacı içeriği yalnızca gereken yeteneğe sahip tarafın okuyabilmesidir. Kimlik doğrulamalı şifreleme değişiklikleri de saptar. Cuvex'te kriptogramlar sırları korur, imzalı işlemler harcamayı yetkilendirir ve şifreli kanallar mesaj taşır. Hepsi kriptografi kullansa da aynı tür nesneler değildir.

İnsanların oluşturduğu parola genellikle kriptografik anahtar olarak kullanılmadan önce bir türetme işlevinden geçer. «AES-256» algoritmayı ve anahtar uzunluğunu belirtir, tahmin edilebilir parolayı güçlendirmez. Üretim, uygulama, saklama, ekran ve kurtarma toplam güvenliğin bileşenleridir.

Karmaşık görünmesi bir QR kodunu güvenli kılmaz. İçeriğini, kimin oluşturduğunu ve uygulamanın onunla ne yapacağını bilmelisiniz. Bir eylemi kabul etmeden önce eğitmenden özel veriyi istemeden amacını açıklamasını isteyin.

Uygulama

1. «Dosya değişikliğini saptamak», «kurtarma ifadesini gizlemek» ve «ödemeyi yetkilendirmek» işlevlerini hash, şifreleme ve imza ile eşleştirin.
2. Hayalî bir metnin bir harfini değiştirerek hash'in değiştiğini gözlemleyin. Gösterimde gizli bilgi kullanmayın.
3. Bir işlemin nasıl hem herkese açık hem de imzalı olabileceğini açıklayın.

Öğrendiklerinizi gösterin

Aradığınız güvenceyi ve onu sağlayan mekanizmayı açıklayın. «Şifreli» kelimesini güvenlikle ilgili her şey için kullanmayın.

Sık sorulan soru

Aygıt yazılımının hash’i hatasız olduğunu belgeler mi? Hayır. Referans güvenilirse baytları tanımlar. Denetim, üretici imzası ve fiziksel test farklı sorulara yanıt verir.

Ara verme noktası

Alıştırmadaki üç eşleştirmeyi saklayın.

Bu yöntemlerden hangisi gizli bir bilginin içeriğini saklar?

1. Dosya adını yayımlamak.
2. Şifrelemeden imzalamak.
3. Korumalı bir anahtarla doğru biçimde şifrelemek.

> **Yanıtı göster: Korumalı bir anahtarla doğru biçimde şifrelemek.**
> Bir imza veya parmak izi tek başına gizlilik sağlamaz.

M03

Kurtarma ifadesi, ek parola ve parola

Amaç

Sistemdeki farklı erişim ve kurtarma bilgilerini birbirine karıştırmayın.

Konuyu anlayın

BIP39 anımsatıcı ifadesi entropiyi ve sağlama toplamını bir sözlükteki kelimelerle gösterir. Standart uzunluklar 12, 15, 18, 21 veya 24 kelimedir. Akılda kalıcı bir ifade, şarkı sözü veya bir insanın rastgele seçtiği kelimeler güvenli üretime eşdeğer değildir. Sağlama toplamı bazı hataları bulur. Tohumu kimin ürettiğini veya başka kimsenin bilmediğini kanıtlamaz.

BIP39 ek parolası ikili tohumun türetilmesine katılır. Farklı bir ek parola bambaşka, görünüşte boş bir cüzdan açabilir. «Ek parola yanlış» mesajı çıkması gerekmez. Sözlükten bir kelime olması zorunlu değildir ve kelimenin gerçek anlamıyla yirmi beşinci kelime değildir.

Cuvex kriptogram parolası saklanan sırrı, Desk parolası bilgisayardaki yerel depoyu korur. Eşleştirme PIN’i bir iletişim oturumunu yetkilendirir. Sohbet anahtarı (Clave Chat) mesajlaşma kimliğini kurtarır. Hiçbiri kurtarma ifadesiyle karıştırılmamalıdır. Birini bilmek diğerlerini yeniden oluşturabilmek anlamına gelmez.

Kurtarma ifadesiyle ek parolayı aynı kriptograma koymak kurtarmayı kolaylaştırabilir. Ancak şifreyi çözebilen kişi için ikisi arasındaki ayrım kalkar. Ayrı saklamak size ve mirasçılara daha çok sorumluluk yükler. Kararı belgeleyip sınayın. Eğitmenin bir seçeneği «daha gelişmiş» bulması karar gerekçesi değildir.

Uygulama

1. Gizli değer içermeyen beş kâğıt kart hazırlayın: kurtarma ifadesi, ek parola, Cuvex parolası, Desk parolası ve sohbet anahtarı (Clave Chat).
2. Her birinin neyi kurtardığını ve unutulduğunda ne kaybedileceğini yazın.
3. Boş bir cüzdanda deneme tasarlayın. Kelimeleri ve ek parolayı özel ortamda girin. Eğitmene yalnızca sonucu bildirin.

Öğrendiklerinizi gösterin

Kursun öğrendiklerinizi «doğrulamak» için neden asla parola istememesi gerektiğini açıklayın. Kendi kurtarma prosedürünüzün hangi sırrı gerektirdiğini belirleyin.

Sık sorulan soru

Ek parolayı e-postayla sıfırlayabilir miyim? BIP39’da böyle bir yol yoktur. Varlıklarınızı saklayan sağlayıcı hesap kurtarma sunabilir, ancak bu farklı bir modeldir.

Ara verme noktası

Değerleri yazmadan «erişim bilgileri ayırt edildi» notunu kaydedin.

BIP39 ek parolasında bir harfi değiştirdiğinizde bakiye sıfır görünüyor. Doğru yorum nedir?

1. Başka bir ek paroladan türetilmiş, geçerli başka bir cüzdan olabilir.
2. Ağ fonlarımı sildi.
3. Desk eski ek parolayı tahmin etmelidir.

> **Yanıtı göster: Başka bir ek paroladan türetilmiş, geçerli başka bir cüzdan olabilir.**
> Farklı bir ek parola hata vermeden başka bir cüzdan üretebilir.

M03

Anahtar türetme, xpub ve tanımlayıcılar

Amaç

Harcama yetkisini vermeden cüzdanın nasıl tanımlandığını anlayın.

Konuyu anlayın

Hiyerarşik bir cüzdan tek kökten çok sayıda anahtar türetir. Yol, hangi dalın kullanıldığını gösterir. Mainnet'te BIP84 çoğunlukla ilk tek imzalı SegWit hesabı için m/84'/0'/0' yolunu kullanır. İlk BIP48 P2WSH çok imzalı hesapta yol m/48'/0'/0'/2' olur. Kesme işareti güçlendirilmiş türetmeyi gösterir. Hesabı, ağı veya betik türünü değiştirmek aynı anımsatıcı ifadeden başka adresler üretebilir.

xpub, belirli alt açık anahtarların türetilebildiği genişletilmiş açık anahtardır. Harcama parolası değildir ancak ilişkili bir adres ailesini izlemeye olanak verebilir. Ana parmak izi, kayıtları ilişkilendiren kısa tanımlayıcıdır. Tek başına kimliği kanıtlamaz ve çakışmaları önlemez.

Tanımlayıcı, betiklerin ve adreslerin nasıl oluşturulacağını betik türü, anahtarlar, kökenler ve türetmelerle ifade eder. Açık anahtarlı salt izleme tanımlayıcısı izlemeye izin verir ama imzalayamaz. «Tanımlayıcı» adı yalnızca açık bilgi içerdiğini garanti etmez. Bazı biçimlerde özel anahtar bulunabilir. Kursa asla gerçek tanımlayıcı yüklemeyin.

Çoklu imzayı kurtarmak için genellikle bir imzalayıcının kelimeleri yetmez, tüm politika gerekir. Eşiği, katılımcıları, xpub'ları, yolları, ağı, betik türünü ve adres keşif verilerini koruyun. Tanımlayıcı sağlama toplamı yazım hatalarını saptamaya yardım eder; katılımcıların kimliğini doğrulamaz.

Uygulama

1. Hayalî bir türetme yolu okuyup amaç, para birimi, hesap ve dal bileşenlerini açıklayın. Gerçek anahtar girmeyin.
2. Alım adresini, katılımcının xpub anahtarını ve tam tanımlayıcıyı ayırt edin.
3. Boş alan adları içeren kişisel bir kurtarma formu hazırlayın ve ilgili belgelerin konumunu ayrı kaydedin.

Öğrendiklerinizi gösterin

Geri yüklenen cüzdanın boş görünmesinin kaybı kanıtlamadığını açıklayın. Ağ, ek parola, betik, hesap, yol ve keşif kapsamı kontrol edilmelidir.

Sık sorulan soru

xpub sonuç doğurmadan yayımlanabilir mi? Normalde tek başına harcama yetkisi vermez, ancak mahremiyeti açığa çıkarır ve belirli kriptografik birleşimlerde başka riskleri artırabilir.

Ara verme noktası

Kursa kaydedeceğiniz formda hassas değer bulunmamalıdır.

Çok imzalı cüzdanı tek bir kurtarma ifadesiyle kurtarmaya çalışırken hangi bilgiler eksik olabilir?

1. Cihazın rengi.
2. Politika ve diğer katılımcıların açık anahtarları.
3. Bir sosyal ağın parolası.

> **Yanıtı göster: Politika ve diğer katılımcıların açık anahtarları.**
> Betikleri yeniden oluşturmak için gereken sayıda özel anahtara ek olarak politikanın tamamı da gerekir.

M03

Cüzdan ve saklama modeli seçimi

Amaç

Araçları işlev, güven varsayımları ve kurtarma açısından karşılaştırın.

Konuyu anlayın

Bir cüzdan, harcama koşullarını tanımlayan, etkinliği izleyen ve uygun olduğunda harcamayı yetkilendiren araçlar bütünüdür. Sıcak cüzdan imza yetkisini bağlı bir ortamda tutar. Yalıtılmış imzalayıcı sırları ağı sorgulayan bilgisayardan ayırmayı amaçlar. Salt izleme cüzdanı izlemek ve işlem hazırlamak için yeterli açık bilgi tutar. İmza için başka sistem gerekir.

Üçüncü taraf saklamada hesap, bir şirketten alacağı temsil edebilir. Öz saklamada tek başınıza veya başkalarıyla birlikte teknik harcama yetkisini siz tutarsınız. E-postayla kurtarma ve çekimi engelleme yetkisi genellikle ilk modele işaret eder. İki seçeneği aynı sorumluluk varsayımıyla değerlendirmeyin.

Ağ ve betik desteğini, ekranda doğrulamayı, yedeklemeyi, güncellemeyi, birlikte çalışabilirliği, bakımı, sağlayıcı sorgularını ve hataların anlaşılırlığını inceleyin. Para listesi veya kasanın kalitesi yeterli değildir. Bir adresi kontrol etmezseniz imzalayıcı cihaz da yanlış adresi kabul etmenizi engellemez.

Cuvex, kriptogramlarda korunan sırları Desk’teki düzenleme ve sorgulama işlerinden ayırır. Bu model kriptogramı ve kilit açma araçlarını korumanızı gerektirir. Cihaz kaybına karşı koruma, tüm kopyalar veya parolalar da kaybolursa kurtarma sağlamaz. Varlıklarınızı taşımadan önce tüm süreci öğrenin.

Uygulama

1. Cuvex’i bir sıcak cüzdan ve borsayla tabloda karşılaştırın: kim imzalar, sorguları kim görür, erişimi kim kurtarabilir ve şirket kapanırsa ne olur?
2. Reklam yerine kanıtla doğrulanması gereken iki ölçüt seçin.
3. Deneme ortamının gerçek birikiminizle aynı anahtarları kullanmadığını kontrol edin.

Öğrendiklerinizi gösterin

Bir aracı zarar görmez ilan etmeden belirli bir durum için seçiminizi gerekçelendirin.

Sık sorulan soru

Donanım cüzdanı tüm işlemleri gizli kılar mı? Hayır. Öncelikle imzalama yetkisini ve incelemenin bir bölümünü korur. Zincir, sorgular ve karşı taraflar bilgi üretmeyi sürdürür.

Ara verme noktası

Ölçüt tablosunu hesap adları olmadan saklayın.

Açık anahtarlarla doğru yapılandırılmış bir salt izleme cüzdanı ne yapabilir?

1. İşlemleri izleyip hazırlayabilir, ancak kendi başına imzalayamaz.
2. Kayıp bir kurtarma ifadesini değiştirebilir.
3. Anonimliği garanti edebilir.

> **Yanıtı göster: İşlemleri izleyip hazırlayabilir, ancak kendi başına imzalayamaz.**
> İzleme ve yetkilendirme birbirinden ayrılabilen yeteneklerdir.

M03

Geri yüklenebilen yedekler

Amaç

Eksiksiz bir yedek tasarlayın ve ona güvenmeden önce kurtarmayı gösterin.

Konuyu anlayın

İşe yarar bir yedek yalnızca dosyayı değil, gerekli yeteneği geri kazandırır. Tek imza için anımsatıcı ifade, ek parola ve türetme verileri gerekebilir. Çoklu imza ayrıca politika ve yeterli sayıda imzalayıcı ister. Desk için şifreli kopya ve parolası gerekebilir. Sohbet kimliğini kurtarmak eski mesajları geri almak anlamına gelmez.

Yedeklilik kazara kayba, ayırma ise birden çok bileşenin birlikte ele geçirilmesine karşı korur. Farklı taşıyıcı ve yerlerdeki iki kopya ortak arıza riskini azaltabilir. Her ek kopya da erişim denetimi, envanter ve gözden geçirme ister. Dosya adları ve etiketler varlıkları açıklamamalı veya tüm bileşenlerin bulunmasını kolaylaştırmamalıdır.

Deneme, önceden doğrulanmış bir adresi ve eğitim ortamında kontrollü bir işlemi imzalayabilmeyi doğrulamalıdır. Dosyanın açılması doğru cüzdana ait olduğunu göstermez. Bir kopyayı sınamak için gerçek kurtarma ifadenizi rastgele bir bilgisayara girmeyin.

Her yedeğin neleri kapsadığını ve dışarıda bıraktığını belgeleyin. Güncel parolayı değiştirmek eski kopyaları güncellemez. Önceki parola açığa çıktıysa bu kopyalar etkilenmeye devam eder. Modern depolamada dosya silmek tüm kopya ve sürümlerin yok edilmesini garanti etmez.

Uygulama

1. Kişisel tablonuza nesne, içerik, ilişkili parola, bağımsız konum, test tarihi ve sorumlu kişiyi girin.
2. Eğitim kopyasını ayrı ortamda geri yükleyin. Ağı, ilk adresi ve türetmeyi doğrulayın.
3. Önce bilgisayarın sonra cihazın kaybını canlandırın. Hangi prosedürün değiştiğini belirleyin.

Öğrendiklerinizi gösterin

Deneme senaryonuzu doğaçlama yardıma gerek kalmadan kurtarın ve başka bir senaryoda hangi bilgilerin eksik kalacağını açıklayın.

Sık sorulan soru

Desk’in genel yedeği her şeyi içerir mi? Böyle varsayılmamalıdır. İncelenen sürümde sohbet geçmişi ve oturumları dâhil değildir. Çoklu imza politikası ve özel anahtarlar farklı görevlere sahiptir.

Ara verme noktası

Yalnızca denemenin tarihini ve sonucunu kaydedin, yedeğin içeriğini asla kaydetmeyin.

Desk’in parolasını değiştirirseniz daha önce oluşturulmuş bir kopyaya ne olur?

1. Kendiliğinden güncellenir.
2. Şifrelemesini otomatik olarak kaybeder.
3. Oluşturulduğunda kullanılan korumayı ve parolayı korur.

> **Yanıtı göster: Oluşturulduğunda kullanılan korumayı ve parolayı korur.**
> Önceden oluşturulmuş kopyalar bağımsız nesnelerdir.

M04

Original ve BIT’i tanıyın

Amaç

Cihazınıza ve sürümüne uygun işlem yolunu seçin.

Konuyu anlayın

Original, kriptogramları ve desteklenen işlemleri NFC kartlarıyla taşır. Güncellemede Bluetooth kullanır. Belgelenen modelde USB-C güç içindir. BIT dosya alışverişi için USB-C kullanır ve gereken kriptogramlara biyometrik koruma ekler. Original’ın NFC veya Bluetooth yönergelerini BIT’e uygulamayın.

Cihazda ayarların yanında şifreleme, şifre çözme, cüzdan oluşturma ve imzalama işlevleri bulunur. Original kart klonlar, BIT ise USB taşıyıcısındaki dosyalarla çalışır. Etiketler, diller ve erişim yolları sürüme göre değişebilir. BIT’teki yeni «Politikaları doğrula» girişi desteklenen akışı açar ve yetkilendiren tarafı değiştirmez.

Bu yayında incelenen kaynak sürümleri Original 1.2.2 Final, BIT 1.2.3 Final, Desk beta.9.21 ve Mirror beta.12.12’dir. Her birleşimin imzası, dağıtımı ve fiziksel kabulü ekiple doğrulanmalıdır. Kurulu aygıt yazılımını bir mühendislik paketindeki imzasız ikili dosyayla değiştirmeyin.

Kullanmadan önce cihazın kaynağını, mühürlerini, görünümünü ve sürümünü inceleyin. İzlenebilirlik ve imzalı güncelleme belirli tehditlere karşı yardımcı olur ama diğer kontrollerin yerini tutmaz. Müdahale izi veya beklenmedik sürüm görürseniz kurulumu durdurup bağımsız olarak doğruladığınız destek kanalına başvurun.

Uygulama

1. Modelinizi belirleyin ve gizli bilgileri fotoğraflamadan görünen sürümü kaydedin.
2. Şifreleme, şifre çözme, cüzdan oluşturma, PSBT ve ayarları bulun. Menüleri keşfetmek için silme veya güncelleme başlatmayın.
3. Kursta Original veya BIT yolunu seçin ve alıştırma boyunca değiştirmeyin.

Öğrendiklerinizi gösterin

İşlemin modelinize nasıl girip çıktığını ve hangi taşıyıcıyı üzerine yazılmaya karşı korumanız gerektiğini açıklayın.

Sık sorulan soru

BIT herkes için kendiliğinden daha güvenli midir? Modeller farklı çalışma seçenekleri sunar. Yanıt tehditlere, kurtarma olanaklarına ve doğru kullanıma bağlıdır.

Ara verme noktası

Modeli ve sürümü yerel defterinize yazın. Kursa yalnızca seçilen model gerekir.

Elinizde BIT var ama bir kılavuz NFC kartını cihazın kendisiyle yazmanızı istiyor. Ne yaparsınız?

1. Kılavuzun modelime uygunluğunu kontrol eder, desteklenen USB işlemini kullanırım.
2. Original güncellemesini zorla uygularım.
3. Kurtarma ifadesini telefona gönderirim.

> **Yanıtı göster: Kılavuzun modelime uygunluğunu kontrol eder, desteklenen USB işlemini kullanırım.**
> Talimatlar, modelin gerçek veri aktarım yöntemine uygun olmalıdır.

Fiziksel entropiyle kurtarma ifadesi oluşturma

Amaç

Oluşturma işlemini anlayın ve kurs verilerini kendi anahtarlarınız olarak kullanmadan akışı deneyin.

Konuyu anlayın

Entropi öngörülemezliktir. Uygun zarlar, sıra atıştan önce belirlenir ve doğru dönüşüm algoritması kullanılırsa entropi sağlayabilir. Reddedilen sonuçlarda yönergedeki atışı aynen tekrarlayın. En büyük sayıyı kullanmak veya başka kelime seçmek yanlılığa yol açar.

İncelenen Cuvex yöntemi bir para ve dört zar kullanır. Dönüşüm işlevi, para sonucunu 1.296 ile çarpar ve her zar değerinden bir çıkararak altı tabanında oluşturulan sayıyı ekler. 0 ile 2.047 arasındaki indeksleri kabul eder. Sonuç sözlük aralığının dışındaysa parayı ve dört zarın tamamını yeniden atın. Parayı sabit tutup yalnızca zarları atmak yanlılık doğurur. Bu açıklama incelenen kaynak koda aittir. Ekranlar ve tüm iş akışı dağıtılan her aygıt yazılımında doğrulanmalıdır.

Bu, sevdiğiniz kelimeleri seçmekle aynı değildir. Halka açık bir gösterimi para saklama malzemesine dönüştürmeyin. Eğitim materyalinde görünen her kurtarma ifadesi başkalarınca biliniyor sayılır. Son kelime ve doğrulaması, ifadeyi elle tamamlamadan cihazın tam algoritmasıyla üretilmelidir.

Kameraların, etkin sesli asistanların, ekran kaydının ve gözlemcilerin bulunmadığı bir alan hazırlayın. Gizli bilgi girilirken ve incelenirken eğitmen durmalıdır. Önceden açıklama yapabilir ve sonrasında atış sonuçlarını veya kelimeleri dinlemeden süreçle ilgili sorular sorabilir.

Üretimden sonra yedeği kontrol edin, modele göre şifreleyin ve boş cüzdanın kurtarılmasını deneyin. Doğrulama adresi, ifadeyi bilgisayara açıklamadan tutarlılığı kontrol etmeye yardım eder. Akış yönergeyle çelişen değerleri kabul eder veya beklenmedik kelimeler gösterirse durun. Yalnızca sürümü, ekranı ve hatayı kaydedin.

Uygulama

1. Prova sırasında gerçek fon içermeyen verilerle cihazın adımlarını izleyin. Zar sırasını önceden sabitleyin ve sonuçları değiştirmeyin.

2. Reddedilen girdileri ekrandaki yönergeye göre tekrarlayın. Kabul edilmeleri için düzeltmeyin.
3. İçeriği özel olarak kontrol edin, bir kopya oluşturun ve aynı eğitim cüzdanını yeniden kurabildiğinizi doğrulayın.

Öğrendiklerinizi gösterin

Fiziksel entropinin, doğru dönüşümün ve sonucun gizliliğinin neden üç ayrı gereklilik olduğunu açıklayın.

Sık sorulan soru

Algoritmayı kontrol etsin diye zar sonuçlarımı yapay zekâya verebilir miyim? Kullanacağınız gerçek bir kurtarma ifadesi için hayır. Eğitim desteği farklı yapay örneklerle çalışır.

Ara verme noktası

Cihazı güvenli durumda bırakarak bitirin. Arada kurtarma ifadesini görünür bırakmayın.

Aygıt yazılımı girilen zar sonucunu reddediyor. Hangi eylem yönteme uygundur?

1. Bir kelimeyi elle seçmek.
2. Sonucu çarpıtmadan cihazın gösterdiği şekilde atışı tekrarlamak.
3. Kabul edilene kadar sayıyı küçültmek.

> **Yanıtı göster: Sonucu çarpıtmadan cihazın gösterdiği şekilde atışı tekrarlamak.**
> Reddedilen sonuçlar entropi dönüştürme yönteminin parçasıdır ve keyfî olarak değiştirilemez.

M04

Cuvex ile gizli bilgiyi şifreleme ve çözme

Amaç

Eğitim kriptogramı oluşturun ve içeriğini kurtarabildiğinizi doğrulayın.

Konuyu anlayın

İş akışında sunulan doğru içerik türünü seçin: BIP39, SLIP39, Monero veya metin. Bunlar farklı biçimlerdir. SLIP39 metnini şifrelemek Cuvex'i bu metni kullanan tüm ağlar için imzalayıcı yapmaz. Gizli bilgiyi saklamak ve imza protokolünü yürütmek ayrı yeteneklerdir.

Sırrı bağlı ekipmanlardan uzak tutmak istiyorsanız içeriği doğrudan cihazda girin. Telefon veya bilgisayardan içe aktarım, sonradan şifrelense bile sırrı zaten kaynakta açığa çıkarmış olabilir. Ön inceleme ekranında kelimeleri, sırayı, büyük-küçük harfi ve yanlış alanları kontrol edin.

Kriptogram parolası uzun, benzersiz ve planınıza göre kurtarılabilir olmalıdır. İncelenen oluşturma klavyesi 40 karakter alır. Doğrulayıcı en az 12 karakter, büyük ve küçük ASCII harfi, rakam ve tanınan sembol ister. Desk'in 12 ila 1.024 karakter kuralını Cuvex klavyesine uygulamayın. Desk farklı bir politika izler. Diğer kurtarma alanlarının sınırları değişebilir. Akışı ve sürümü kontrol edin.

Original ile uygun, boş karta yazın. Onay gelene kadar kartı sabit tutun. BIT'te gerekiyorsa biyometrik bileşenler dâhil USB akışının oluşturduğu dosyaları saklayın. Dosyaları tahminle yeniden adlandırmayın veya birleştirmeyin. Ardından sırrı eğitmene bildirmeden cihaz üzerinde deneme okuması ve şifre çözme yapın.

Uygulama

1. Yalnızca bu alıştırma için oluşturulan, erişim bilgisi veya ekonomik değer içermeyen bir metin şifreleyin.
2. Taşıyıcıyı ve ortaya çıkan nesneyi tanımlayın. Takma adı ve işlevini kişisel kaydınıza yazın.
3. Şifre çözmeyi yeniden başlatın, metni güvenilen ekranda kontrol edin ve bittiğinde görüntüyü kapatın.

Öğrendiklerinizi gösterin

Doğru içerik, başarılı yazma ve başarılı kurtarmayı ayırt edin. «Dosya kopyalandı» mesajı üçünü birden kanıtlamaz.

Sık sorulan soru

Kartın takma adı parola mıdır? Hayır. Düzenleme bilgisidir. Varlıklarınızın tanınmasını kolaylaştıran bakiye veya açıklamalar eklemeyin.

Ara verme noktası

Şifresi çözülmüş içeriği görünür bırakmayın. Yalnızca denemenin başarılı veya başarısız olduğunu kaydedin.

Bir deneme kriptogramının içeriğinin kurtarılabildiğini en iyi ne gösterir?

1. Dosya adının güzel olması.
2. Dosyanın iki klasörde bulunması.
3. Doğru işlem akışında okuyup şifresini çözmek ve içeriği özel ortamda kontrol etmek.

> **Yanıtı göster: Doğru işlem akışında okuyup şifresini çözmek ve içeriği özel ortamda kontrol etmek.**
> Bir kopyanın var olması, işe yaradığını veya doğru içeriğe karşılık geldiğini kanıtlamaz.

M04

Şifreleme eşikleri ve biyometri

Amaç

Bir sırrın paylaşımlı korumasını Bitcoin çoklu imzasından ayırın.

Konuyu anlayın

Birden çok parolayla korunan kriptogram içeriği kimin çözebileceğini belirler. Bitcoin çoklu imza cüzdanı ise ağdaki harcamayı hangi anahtarların onaylaması gerektiğini belirler. Tek imzalı bir cüzdanın sırrı paylaşımlı olarak şifrelenebilir. Çoklu imzada da her imzalayıcının kendi bireysel kriptogramı olabilir.

Birden çok kişi aynı kurtarma ifadesini birlikte açıyor ve o ifade tek başına harcama yetkisi veriyorsa zincirdeki eşik yine bir anahtardır. Açığa çıktıktan sonra biri kopyasını tutabilir. Bu düzeni her ödeme için birden çok imzayı koordine etmek zorunluymuş gibi anlatmayın.

BIT biyometrisi, onu kullanan biçimlere bir erişim koşulu ekler. Parmak bir kurtarma ifadesi veya her parolanın yerine geçen bir araç değildir. Yaralanma, parmak izinin değişmesi, arıza, cihaza erişim ve miras durumlarını planlayın. Kriptogramın belgelenmiş kurtarma yolunu saklayın ve ona güvenmeden önce sınayın.

Kurtarma dışa aktarımı bir acil durumu çözmek için sırrı bilgisayarda açığa çıkarabilir. Bu işlev bilgisayarı cihazla eşdeğer bir ortama dönüştürmez. Olağan kullanımda yalıtımı sürdürün. Yerel kurtarmayı bilinçli olarak ve açığa çıkma yaşanırsa sonrasında geçiş planıyla ele alın.

Uygulama

1. İki politikayı çizin: «bir kurtarma ifadesini açmak için iki parola» ve «harcama için üç anahtardan ikisi».
2. Bakiyesiz bir denemede biyometrik bir kopya için hangi dosyaların gerektiğini ve kurtarmanın nerede doğrulandığını belirleyin.
3. Bir katılımcının ulaşılamaz olduğunu canlandırın. Düzeninizin eşiğinin devam etmeye izin verip vermediğini belirleyin.

Öğrendiklerinizi gösterin

Sırrı kimin öğrenebileceğini ve şifre çözüldükten sonra harcamaya kimin yetki verebileceğini açıklayın.

Sık sorulan soru

Bir etiketi değiştirerek katılımcıyı çıkarabilir miyim? Hayır. Düzenlemedeki değişiklik, sırrın yeni koruması ve yeni harcama politikası ayrı işlemlerdir.

Ara verme noktası

Şemayı gerçek ad veya biyometrik bilgi olmadan saklayın.

Üç kişi, tek imzalı bir cüzdanın tek kurtarma ifadesini içeren kriptogramı iki parolayla açıyor. Bitcoin’de harcama için kaç anahtar gerekir?

1. Cüzdanın politikası buysa bir anahtar.
2. Dosya iki parola gerektirdiği için iki anahtar.
3. Üç kişi olduğu için üç anahtar.

> **Yanıtı göster: Cüzdanın politikası buysa bir anahtar.**
> Şifrelemeye erişim eşiği, paraları kontrol eden betiği değiştirmez.

M04

Kopyaları çoğaltma, saklama ve doğrulama

Amaç

Geçerli tek kopyayı bozmadan yedeklilik sağlayın.

Konuyu anlayın

Kriptogramı klonlamak şifreli veriyi kopyalar. Yeni bakiye veya kurtarma ifadesi oluşturmaz ve açığa çıkmış paroladan bağımsızlık sağlamaz. Özdeş kopyalar taşıyıcı kaybına çaredir, asıl sırrın açığa çıkmasına değil. Bu yüzden geri yükleme ve yeni anahtarlara geçiş farklı durumlara yanıt verir.

Original'da kriptogram kartı ile PSBT aktarım kartını ayırın. İşlem taşıyıcısı iş akışına uygun biçimde yeniden kullanılabilir. Yedeğinizi içeren kartı bu amaçla kullanmayın. İşlem, kriptogram bulunan kartı reddederse korumayı atlamaya veya başlığı elle silmeye çalışmayın.

BIT'te kopya, gereken tüm dosyaları ve aralarındaki ilişkiyi korumalıdır. Dosya yöneticisinin tamamlandı demesi, cihazın içeriği doğruladığını veya işlemi bitirdiğini garanti etmez. Belirtilen durumları bekleyin ve bir kopyayı kontrollü kurtarmayla doğrulayın.

İçeriği ele vermeyen tanımlayıcılar, biçim sürümü, son denemenin tarihi ve sonucuyla kişisel envanter tutun. Belirlediğiniz olaylara karşı en az iki kopyayı ayrı tutun. Sorun tanılama için yedekleri destek kanallarına yüklemeyin. Ayıklanmış üstverileri ve hata kodlarını aktarın.

Uygulama

1. Doğru iş akışıyla eğitim kriptogramının başka bir taşıyıcıda kopyasını oluşturun.
2. Asıl taşıyıcıyı ayırın ve deneme metnini kopyadan kurtarın.
3. Kayıp, dosya hasarı ve parola ifşası durumlarında ne yapacağınızı ayrı ayrı belgeleyin. Aynı prosedür uygulanmaz.

Öğrendiklerinizi gösterin

Sınadığınız kopyayı gösterin ve asıl kopyanın neden üzerine yazılmadığını açıklayın.

Sık sorulan soru

İkinci dosyayı gördükten sonra asıl kopyayı silebilir miyim? Önce kurtarmayı ve kapsamı doğrulayın. Silme kararı yalnızca kopya sayısına değil plana dayanmalıdır.

Ara verme noktası

Oturumu kapatmadan taşıyıcıları saklayın. Kartları ödeme deneme kartlarıyla karışık bırakmayın.

Bir kişi parolayı biliyor ve kriptogramın bir kopyasını ele geçirdiyse üç kopya daha oluşturmak ne sağlar?

1. O kişinin kopyasını geçersiz kılar.
2. Yedekliliği artırır ancak mevcut erişimi kaldırmaz.
3. Bitcoin kurtarma ifadesini otomatik değiştirir.

> **Yanıtı göster: Yedekliliği artırır ancak mevcut erişimi kaldırmaz.**
> Çoğaltmak, daha önce oluşmuş bir sızıntının etkisini ortadan kaldırmaz.

M05

Cuvex Desk’i kurma ve koruma

Amaç

Kaynağı doğrulanmış bir kurulumu açın ve yerel depoyu koruyun.

Konuyu anlayın

Sistem ve mimarinize uygun paketi seçin: mevcut dağıtıma göre macOS Intel veya Apple Silicon, Windows x64 veya ARM64, Linux x64 veya ARM64. Kaynak ZIP’i, Manager paketi ve müşteri kurulum dosyası farklı teslimatlardır. Kurs öğrenciyi özel bir imzalama paketine yönlendirmemelidir.

Kaynağı ve sistem doğrulamalarını kontrol edin. Windows mühendislik imzası tek başına yayımcıya kamusal güven sağlamaz. Mac’te uygulama imzası, noter onayı ve açılış denetimi ayrı kontrollerdir. Destek olduğunu söyleyen biri aradığında genel korumaları kapatmayın. Beklenmedik uyarının metnini saklayıp resmî kanala başvurun.

Desk, parolayla şifrelenen yerel bir depo oluşturur. İncelenen sürüm yeni parolalarda 12 ila 1.024 karaktere izin verir. Onay alanı varsa iki giriş aynı olmalıdır. Bu sınırlar tek başına kalite ölçütü değildir. Yalnızca burada kullandığınız benzersiz bir parola seçin. Bilgisayarda sunuluyorsa biyometri, ayrı yapılandırma gerektiren bir erişim kolaylığıdır.

Hareketsizlikte ve uygunsa arka plana geçişte kilitlemeyi ayarlayın. Hatalardan sonraki bekleme ve isteğe bağlı silme kılavuzda ele alınır. Gösterim sırasında otomatik silmeyi açmayın. Uygulama olağan kullanıcı hesabı olmadan çalışabilse de sorgu, sohbet ve indirme hizmetlerinin ayrı gereksinimleri ve iletişimi vardır.

Uygulama

1. Eğitmene özel tanımlayıcılar vermeden platformu, görünen sürümü ve paketin kaynağını doğrulayın.
2. Eğitim deposu oluşturup kilitlemeyi ve yeniden açmayı sınayın. Parolayı özel ortamda girin.
3. Şifreli yedeklemeyi planlayın ve parolasını planınıza göre koruyun. Gerçek ortamda art arda kilitleme denemesi yapmayın.

Öğrendiklerinizi gösterin

Yerel parolayı, mağaza hesabını ve eklediğiniz hizmetlerin erişim bilgilerini ayırt edin.

Sık sorulan soru

Desk parolasını değiştirince kart parolalarım da değişir mi? Hayır. Bunlar bağımsız korumalardır. Eski kopyalar da kendiliğinden değişmez.

Ara verme noktası

Desk’i kilitleyin ve erişim bilgileri olmadan ders kimliğini kaydedin.

Kurulum paketi sistem mimarinize uygun değil. İlk adım nedir?

1. Korumaları kapatıp çalıştırmaya zorlamak.
2. Uygun resmî paketi edinmek ve gereksinimlerini kontrol etmek.
3. Devam etmek için kurtarma ifadesini bir web sitesine girmek.

> **Yanıtı göster: Uygun resmî paketi edinmek ve gereksinimlerini kontrol etmek.**
> Saklama materyallerini kullanmadan önce uyumluluk ve kaynağın gerçekliği doğrulanmalıdır.

Kriptogramları bağlama ve WOW hesaplarını düzenleme

Amaç

Şifreli kopyayı bağlayın ve izleme hesabından ayırt edin.

Konuyu anlayın

Desk NFC, USB veya uyumlu yedek dosyasıyla bağlanan kriptogramları düzenler. Görsel tasarım ve takma ad tanımaya yardım eder, ancak kriptografik kimlik kanıtı değildir. Bilgi kartında kaynak ile uygulamanın yorumladığı biçim, boyut ve erişim özellikleri görülebilir.

Bağlama, uyumlu nesneyi içe aktarır veya düzenler. Bilgisayarda şifre çözmek veya sırrı doğrulamak anlamına gelmez. WOW, uyumlu açık bilgilerle ilişkilendirilen bir izleme cüzdanıdır. Aynı sır kümesinden farklı hesap veya türetmeler çıkabilir. İlişkilendirme yönetmek istediğiniz cüzdana karşılık gelmelidir.

Cihaz akışından dışa aktarılan tanımlayıcı veya açık bilgilerle hesabı etkinleştirin veya içe aktarın. Ağı, betik türünü, parmak izini, yolu ve kontrol adresini inceleyin. Hesap adı düzenleme amaçlıdır. Öngörülebilir ad tahmin edilebildiği için addan türetilmiş tanımlayıcı güçlü anonimleştirme sayılmaz.

İncelenen Desk sürümünde ilişkilendirme bekleyen hesaplar saklanır. Kopya dışa aktarma, klonlama ve yerel kayıt silme işlevleri vardır. Kartı arayüzden silmek dış kopyaları yok etmez veya fon taşımaz. «Yedek yok» ifadesi uygulamanın kendi ölçütüne göre bir kopyayı doğrulamadığını belirtir. Hiçbir yerde yedek olmadığı anlamına gelmez.

Uygulama

1. Eğitim kriptogramını seçilen yöntemle bağlayın ve bilgi kartını inceleyin.
2. Uyumlu eğitim hesabını içe aktarın. Eğitmene anahtar göstermeden ağını ve doğrulama adresini kontrol edin.
3. Kriptogram kaydını, WOW hesabını ve fiziksel taşıyıcıyı ayırt edin. Yerel silmede hangisinin kaybolacağını belirleyin.

Öğrendiklerinizi gösterin

Desk’in gözlem için hangi verilere ihtiyaç duyduğunu ve olağan kullanımda hangilerinin bilgisayardan uzak kalması gerektiğini açıklayın.

Sık sorulan soru

Bir .bin dosyasını bağlamak kurtarma ifademi içerdiğini garanti eder mi? Hayır. Kaynağını ve kurtarmayı doğrulamalısınız. Dosya uzantısı içeriği belgelemez.

Ara verme noktası

Yalnızca «deneme bağlantısı doğrulandı» durumunu saklayın.

Bir WOW hesabını yerel olarak silmek bitcoinlerini taşır mı?

1. Hayır. İş akışına göre yerel verileri siler, UTXO’ları harcamaz.
2. Evet. Bunları üreticiye gönderir.
3. Başka bir kişinin elinde bulunan tüm imzaları iptal eder.

> **Yanıtı göster: Hayır. İş akışına göre yerel verileri siler, UTXO’ları harcamaz.**
> Yerel durum ile zincir durumu birbirinden farklıdır.

M05

Mirror ile Desk’i eşleştirme

Amaç

Eşleştirme kodlarını karıştırmadan yetkilendirilmiş yerel bağlantı kurun ve sonlandırın.

Konuyu anlayın

Mirror, uygulamalarda gösterilen eşleştirme akışı, PIN ve QR kodu aracılığıyla Desk ile yerel işlemlere olanak verir. Altı haneli PIN yalnızca o oturuma aittir. Desk parolası, kriptogram parolası veya kurtarma kelimesi değildir. Hangi ekranın kodu ürettiğini ve nereye girileceğini kontrol edin. Tanımadığınız birinin gönderdiği kodu kullanmayın.

Desk’te işleme uygun bağlamdan başlayın: bağlama, QR okuma, PSBT aktarma veya aygıt yazılımı işlemi farklı amaçlardır. Pencere arama, bağlantı, keşif, PIN, QR ve kart ya da dosya işini bildirir. Aramada cihazın görünmesi tüm işlemin tamamlandığını kanıtlamaz.

Sisteme ve iş akışına göre gereken izinleri verin: optik okuma için kamera, gerektiğinde Bluetooth veya NFC. Yazılım kurmak telefona eksik fiziksel donanımı kazandırmaz. iOS’ta adaptör ve doğrulama farklılıkları vardır. Derlenebilen proje, tüm iPhone’larda dağıtılmış ve denenmiş gibi sunulmamalıdır.

Hatanın aşamasını belirleyin: cihaz görünmüyor, görünüyor ama bağlanmıyor, PIN reddedildi, QR okunamıyor, kart okunmadı veya yanıt alınmadı. Eski oturumları kapatın, sürüm ve izin uyumunu doğrulayın ve kontrollü olarak yeniden deneyin. Yanlış PIN aygıt yazılımını değiştirmeyi veya kurtarma ifadesini başka yere girmeyi gerektirmez.

Uygulama

1. Desk’te deneme okuması başlatın ve yerel ekranlarından Mirror’ı bağlayın.
2. QR kodu veya eğitim kartı sunmadan önce işlem amacını kontrol edin.
3. Oturumu iptal edip önceki bağlamdan geç gelen okumanın uygulanmadığını doğrulayın. Yeni oturum açın.

Öğrendiklerinizi gösterin

Etkin kodları veya hassas içeriği vermeden başarısız aşamayı ve ilgili cihazları tarif edin.

Sık sorulan soru

Mirror her zaman bağlı kalmalı mı? İşleme bağlıdır. Kalıcı bir hizmet gibi kullanmayın. Kapatınca veya arka plana alınca yetkinin sürdüğünü varsaymayın.

Ara verme noktası

Eşleştirme oturumunu bitirin ve kullanılmayan uygulamaları kilitleyin.

PIN gösterilmeden eşleştirme başarısız olursa eğitmen ne yapmalıdır?

1. Kurtarma ifadesini istemelidir.
2. İlerlemeden önce cihaz keşfini, izinleri, oturumu ve sürümleri kontrol etmelidir.
3. Bağlantıyı tamamlanmış saymalıdır.

> **Yanıtı göster: İlerlemeden önce cihaz keşfini, izinleri, oturumu ve sürümleri kontrol etmelidir.**
> Tanılama, gözlenen aşamayı izlemelidir. Başarılı olmadığı hâlde bağlantı kurulmuş gibi gösterilmez.

Mirror üzerinden NFC, USB-C ve QR kodu okuma

Amaç

Her veri taşıma yöntemini amacına göre ve gerekli kontrolleri uygulayarak kullanın.

Konuyu anlayın

Cuvex Desktop’ta NFC işlemleri için bilgisayara Bluetooth ile eşleştirilmiş, uyumlu bir akıllı telefonda Cuvex Mirror gerekir. Cuvex Desktop harici USB NFC okuyucularını desteklemez. Kart, biçimi ve kapasitesi de işlemle uyumlu olmalıdır. Bir kriptogramı taşıyabilen küçük bir kart, önceki işlemleri içeren bir PSBT için yetersiz kalabilir. Gerçek sınırı yalnızca alıcıların sayısı değil, içeriğin tamamı belirler. Yedekleme kartını aktarım kartı olarak kullanmayın.

Original ile çalışırken Mirror isteği işlem kartına yazabilir. Cihaz isteği işler ve yanıtı karta yazar. Mirror bu yanıtı Desk’e geri taşır. Yazmanın onaylanması Desk’in yanıtı aldığı anlamına gelmez. Cihaz sonucu gösterene kadar kartı sabit tutun. Sistem tanıdığı bir kriptogramı korumak için işlemi reddederse bu karara uyun.

BIT, veri alışverişi için bir USB birimi veya klasörü kullanır. İşlem sırasında birim çıkarılıp yeniden sunulabilir. Desk doğru ortamı seçmeli, yanıtı doğrulamalı ve öngörülen alındı onayını vermelidir. Dosyayı bilgisayarda aynı adlı bir klasöre kopyalamak, cihaza teslim etmekle aynı değildir.

Kamera QR kodunu okuyamıyorsa nedeni odak, yansıma, boyut, hareket veya veri yoğunluğu olabilir. Görüntüyü büyütün, ışığı ve mesafeyi ayarlayın. Uzun bir tanımlayıcıyı ilk birkaç harfle değiştirmeyin ve eksik aktarımı kabul etmeyin. Başarılı okuma, içeriğin anlamını doğrulamanın yalnızca başlangıcıdır.

Uygulama

1. Eğitim materyalindeki şema üzerinde Original ve BIT için isteği, taşıyıcıyı ve yanıtı belirleyin.
2. Gecikmeli gelen değerleri kaydetmeden QR okumayı iptal etmeyi deneyin. Başka bir amaçla tekrarlayın.
3. Fazla büyük bir dosyayı canlandırın. Kontrolleri kaldırmadan işlemin karmaşıklığını azaltmanın veya uyumlu bir taşıyıcı seçmenin neden gerektiğini açıklayın.

Öğrendiklerinizi gösterin

Hangi cihazın hangi aşamayı onayladığını açıklayabilmelisiniz: okuma, yazma, doğrulama, alma veya alındı onayı.

Sık sorulan soru

Bir hash veya kopyalamanın başarılı olduğunu gösteren bir OK, doğru Bitcoin alıcısının seçildiğini kanıtlar mı? Hayır. İşlemi ve çıktılarını imzalayan cihazda incelemelisiniz.

Ara verme noktası

Yedekleme kartlarını çıkarıp saklayın. Aktarım için kullanılacak ortamı açıkça belirleyin.

Original, yanıtı karta yazdığını bildiriyor. Desk’in yanıtı aldığını söylemeden önce ne yapılmalı?

1. Kart başka bir renge boyanmalı.
2. Yeni bir kurtarma ifadesi oluşturulmalı.
3. Yanıt ilgili işlem akışından okunmalı ve Desk’te doğrulanmalı.

> **Yanıtı göster: Yanıt ilgili işlem akışından okunmalı ve Desk’te doğrulanmalı.**
> Yazmanın ve almanın başarıyla tamamlanması ayrı olaylardır.

Kamuya açık hizmet sağlayıcılar ve kendi düğümünüz

Amaç

Bir sorgu kaynağı seçin, hangi bilgileri açığa çıkarabileceğini ve sınırlarını anlayın.

Konuyu anlayın

Desk uyumlu kamuya açık sağlayıcıları veya kullanıcının yapılandırdığı Bitcoin Core'u sorgulayabilir. Sağlayıcı sorguları, sıralarını ve bağlantı verilerini görebilir. Tam bir xpub göndermemek belirli bir ifşayı azaltır ancak betikler ve hash'leri de birbiriyle ilişkilendirilebilir.

Desk 9.21'de REST seçeneklerine ve kendi düğümünüze ek olarak TLS üzerinden Blockstream Electrum açıkça seçilebilir. TLS bazı ağ gözlemcilerine karşı kanalı korur. Sağlayıcı sorguları yine alır. Anonimliği garanti eden gizli bir sağlayıcı değişimi yoktur. Seçim kolaylık için hangi mahremiyetin bırakıldığını anlamayı gerektirir.

Core için bağlantı adresini, kimlik doğrulamasını ve izleme cüzdanını ilgili kılavuza göre yapılandırın. Uygulama «görsün» diye RPC portunu yayımlamayın veya internete açık bırakmayın. Erişimi güvenilen ortamlarla sınırlayın ve uygun korumalı aktarım kullanın. RPC parolasını eğitmene söylemeyin.

İlk eşitleme ve yeniden tarama zaman alabilir. İlerleme, işin durumudur; erken başarı sayılmaz. Desk arka plandaki işi korur. Görünümü kapatmak düğümü durdurmak değildir. Belgelenen asgari geçmiş aralığı daha eski etkinliğin bulunmasını garanti etmez. Cüzdanınız daha eskiyse içe aktarma tarihini ve gerçek tarama kapsamını kontrol edin.

Adres keşfi pozitif bakiyeye değil, işlem geçmişine dayanır. Bakiyesi sıfıra düşmüş bir adres yine kullanılmıştır. İncelenen çoklu imzada her dal ve katılımcı için art arda 20 geçmişsiz adres sınırı, ayrıca adres üretim sınırları uygulanır. Bu sınırı tüm cüzdanlara genellemeyin.

Uygulama

1. Eğitim için bir kaynak seçin ve hangi bilgileri görebileceğini açıklayın.
2. Son eşitleme tarihini, ağı ve ilerlemeyi inceleyin. HTTP 429 yanıtında bekleyin. Bilinçli karar vermeden sağlayıcı değiştirmeyin.
3. Sıfır bakiyeli ancak geçmiş işlemleri olan bir cüzdan canlandırın. «Sıfır» ile «kullanılmamış» arasındaki farkı doğrulayın.

Öğrendiklerinizi gösterin

Kaynağınızın doğrulama ve gizlilik ihtiyacınızı karşılayıp karşılamadığına karar verin, tamamlanmamış durumu tanıyın.

Sık sorulan soru

Kendi düğümüm beni anonim yapar mı? Hayır. Üçüncü taraf sorgularına bağımlılığı azaltır. Yine de bağlantı, karşı taraflar, ağa yayımlama ve diğer üstveriler hesaba katılmalıdır.

Ara verme noktası

Yalnızca sağlayıcı türünü ve taramayı tamamlamak gerekip gerekmediğini kaydedin.

Bir adresin bakiyesi sıfır ama geçmişte para alıp harcamış. Cüzdan keşfinde bu adres nasıl ele alınmalıdır?

1. Geçmişi olan adres olarak.
2. Hiç kullanılmamış adres olarak.
3. Geçersiz adres olarak.

> **Yanıtı göster: Geçmişi olan adres olarak.**
> Daha önce kullanılıp kullanılmadığını mevcut bakiye değil işlem geçmişi gösterir.

M06

Bitcoin alma ve adres doğrulama

Amaç

Bir ödeme alma isteği oluşturun ve teslim etmeden önce doğrulayın.

Konuyu anlayın

Doğru WOW hesabını açıp ağı ve politikayı doğrulayın. Ödeme alma isteğini oluşturun veya geri getirin. Yerel düzenleme için gerekçe, gözlemci ve beklenen tutar ekleyebilirsiniz. Bunlar yerel bilgilerinizdir. Beklenen tutar, birinin farklı miktar göndermesini önlemez.

Adresi cihazın sunduğu yöntemde ve ilgili cüzdan bağlamında doğrulayın. Kullandığınız birleşimde bu yol henüz fiziksel olarak doğrulanmadıysa alıştırmayı simülasyonda bırakın ve önemli fonlar almadan önce konuyu yetkililere iletin. Aynı kaynaktan beslenen iki ekranı karşılaştırmak bağımsız doğrulama sağlamaz.

Akış izin veriyorsa yeni tahsilat ilişkisi için yeni adres kullanın. İncelenen çoklu imzada gösterilmiş adresler yeniden atanmaz ve süreleri dolmaz; ödeyen daha sonra kullanabilir. Geçmişsiz ardışık yeni adres sınırına ulaşırsanız uygun eski isteği geri getirin ve sınırın nedenini anlayın. İndeksleri geri almayın.

Paylaştıktan sonra girişi kendi doğrulama kaynağınızdan izleyin. E-posta, borsa makbuzu veya ödeyenin ekran görüntüsü kesin ödemeyi kanıtlamaz. Riske göre ağ, txid, çıktı, tutar ve onayları kontrol edin. Planınız bu sorguları gizli tutmayı gerektiriyorsa kolaylık uğruna adresinizi açık bir gezginde aramayın.

Uygulama

1. Laboratuvarda istek oluşturun, hesap ve ağı inceleyin ve adresi nasıl doğrulayacağınızı açıklayın.
2. Hayalî bir etiket kaydedin. Görünümü kapatıp aynı isteği yeniden bulun.
3. Farklı tutarda ödeme alındığını canlandırın. Geçmişi değiştirmeden nasıl mutabakat yapacağınızı belirleyin.

Öğrendiklerinizi gösterin

Oluşturulmuş adresi, doğrulanmış adresi, paylaşılmış isteği ve onaylanmış alımı ayırt edin.

Sık sorulan soru

Yeni adres oluşturunca eski adres çalışmayı bırakır mı? Genellikle hayır. Adres keşfini ve istek kayıtlarını korumak gecikmiş ödemelerin gözden kaçmasını önler.

Ara verme noktası

Laboratuvar isteğinin durumunu kaydedin. İçeriğini eğitmene vermeyin.

Ödeyen kişi «çekim tamamlandı» yazılı bir ekran görüntüsü gönderiyor. Ödemeyi alınmış saymadan önce neyi kontrol edersiniz?

1. Yalnızca ekran görüntüsünün kalitesini.
2. Güvenilir bir ağ kaynağından ilgili çıktıyı ve gereken onayları.
3. Ödeyenin parolasını.

> **Yanıtı göster: Güvenilir bir ağ kaynağından ilgili çıktıyı ve gereken onayları.**
> Ticari bir belge veya ekran görüntüsü, ödemenin doğrulanmasının yerini tutmaz.

UTXO’ları etiketleme, dondurma ve seçme

Amaç

Girdileri kökenlerini kazara birleştirmeden hazırlayın.

Konuyu anlayın

Etiketler zincirde görünmeyen bağlamı korur: kaynak, karşı taraf, amaç ve kullanım kısıtları. Desk’te UTXO etiketiyle adres notunun uzunlukları ve işlevleri farklı olabilir. «Müşteri A» yararlıdır, tam ad veya kimlik numarası ise gereksiz ölçüde hassas bir kayıt oluşturabilir.

Desk’te UTXO dondurmak onu bazı yerel seçimlerin dışında tutar. Bitcoin’de harcanmasını engellemez, betiği değiştirmez ve anahtarlara sahip başka bir uygulamanın kullanmasını önlemez. Bu nedenle toplam ve harcanabilir bakiye farklı olabilir. Çıktının donmuş mu, taslakta ayrılmış mı, yoksa gerçekten harcanmış mı olduğunu kontrol edin.

Otomatik seçim algoritmaya ve bağlama göre eniyiler. Özel ilişkilerinizi bilmeyebilir. Bir ödemede tasarruf, maaş ve ticari etkinliği birleştirmek yerine aynı bağlamdan bir çıktı kullanmanın uygunluğunu değerlendirin. Anlamlı ayrım yalnızca iyi etiketler değil, sonraki kullanımda da tutarlılık gerektirir.

BIP329 biçiminde etiket dışa aktarmak saklamayı ve taşımayı kolaylaştırır. Biçim tek başına şifreleme sağlamaz. Desk dışa aktarım için şifreli kapsayıcı sunar. Korumalı dosyayı uyumlu düz metinden ayırın. İçe aktarımda verilerin üzerine yazmadan önce cüzdan eşleşmesini ve dondurmalara ne olduğunu inceleyin.

Uygulama

1. Üç yapay UTXO’yu tasarruf, faaliyet ve bağış olarak etiketleyin.
2. Birini dondurun ve görünen bakiye ile seçim için kullanılabilir bakiye farkını inceleyin.
3. Laboratuvar etiketlerini parolayla dışa aktarın, bir kopyaya içe aktarın ve gerçek kişisel veri kullanmadan sonucu kontrol edin.

Öğrendiklerinizi gösterin

Girdi seçiminizi maliyet ve açığa çıkan ilişkilerle gerekçelendirin. Dondurmanın yerel tercih olduğunu belirtin.

Sık sorulan soru

Ödeme sırasında etiket alıcıya gider mi? Yerel etiket olduğu için kendiliğinden gitmez. Dışa aktarırken, dosya paylaşırken, başka hizmet kullanırken veya mesaja eklerken açığa çıkabilir.

Ara verme noktası

Alıştırma etiketlerini ve donma durumunu saklayın.

Desk’te bir UTXO’yu dondurmak ne yapar?

1. Ağda mutabakat düzeyinde kilit oluşturur.
2. UTXO’yu özel bir hesaba aktarır.
3. Uygulamaya göre yerel bir seçim kısıtlaması getirir.

> **Yanıtı göster: Uygulamaya göre yerel bir seçim kısıtlaması getirir.**
> Anahtarların başka kopyalarıyla harcama yetkisini ortadan kaldırmaz.

M06

Ödeme hazırlama ve inceleme

Amaç

Anlaşılır bir PSBT oluşturun, tüm masraflarını ve çıktılarını tanıyın.

Konuyu anlayın

Hesabı, harcanabilir girdileri, alıcıları ve tutarları seçin. İsteğin kaynağını doğrulayın. Yapıştırma veya tarama sonrasında adresin tamamını ve ağı kontrol edin. Pano veya görüntü değiştirilmiş olabilir. Tam kontrol mümkünken yalnızca ilk ve son karakterlere güvenmeyin.

Ücret oranını seçin; toplam ücreti, tahmini boyutu, toplamı ve para üstünü kontrol edin. «Tamamını gönder» ile Desk ücreti kullanılabilir tutardan düşer. Sohbet isteğinde net tutar isteneni karşılamıyorsa kısmi ödeme bilinçli seçilmelidir. Farkı gizlemek için asıl istek değiştirilmez.

Küçük para üstü veya hiç para üstü çıktısı olup olmadığını kontrol edin. «Kendime ait» işaretli çıktı koordinatörün verdiği ada değil politikaya göre doğrulanmalıdır. Para üstü mümkün değilse tüm bakiyenin aktarımını inceleyin veya uyumlu bir girdi ekleyin. Farkın sessizce orantısız ücrete dönüşmesini kabul etmeyin.

PSBT bilgi ve imza taşımaya yarayan biçimdir. Kaynağın gerçekliği veya gizlilik kendiliğinden sağlanmaz. Önceki işlemler, açık anahtarlar, yollar ve üstveri içerebilir. İncelenen Final aygıt yazılımlarında çoklu imza profili PSBT v0/BIP174 kullanır. «İşlem sürümü 2», «PSBT sürüm 2» anlamına gelmez.

Uygulama

1. Simülatörde 120.000 sat girdi, 70.000 sat alıcı ve 1.000 sat ücretle ödeme oluşturun.
2. Tüm çıktıları listeleyin ve 49.000 sat para üstünü açıklayın. Tam bakiyeyi göndererek tekrarlayın.
3. Taslağı iptal edin ve yerelde neyi iptal ettiğinizi açıklayın. Simülatörü imzalama veya yayımlama için kullanmayın.

Öğrendiklerinizi gösterin

Dışa aktarmadan önce neyin girip çıktığını, kimin ödeme aldığını, maliyeti ve hangi yetkilendirmenin eksik olduğunu açıklayın.

Sık sorulan soru

Bakiyede gördüğüm tutarın tamamını gönderebilir miyim? Yalnızca uygulama gerçekleştirilebilir bir net gönderim hesaplar ve ücretler karşılanırsa. Bakiyede harcanamayan paralar da bulunabilir.

Ara verme noktası

Eğitim taslağını saklayın veya iptal edin. Kurs portalına asla gerçek PSBT koymayın.

Ekranda «transaction version 2» yazıyor. Bu, dosyanın PSBT v2 olduğunu kanıtlar mı?

1. Hayır. Bunlar farklı sürüm alanlarıdır.
2. Evet, her zaman.
3. Taproot kullandığını kanıtlar.

> **Yanıtı göster: Hayır. Bunlar farklı sürüm alanlarıdır.**
> BIP370 kapsayıcının sürümüyle işlemin sürümünü birbirinden ayırır.

Original ve BIT ile imzalama

Amaç

Her model için imzalama adımlarını tamamlayıp doğru işleme bağlı yanıtı alın.

Konuyu anlayın

Original’da PSBT’yi uyumlu iş akışının aktarım kartı ve Cuvex Mirror aracılığıyla iletin. Cihazda isteği okuyun, kriptogramı sunun ve kilidini özel ortamda açın. Tüm çıktıları, tutarları, para üstünü ve ücreti inceleyin. Yanıt karta yazılır, ardından Desk’te okunup doğrulanır. Karta yazmanın başarılı olması bu dönüş adımının yerini tutmaz.

BIT’te doğru birimi seçip isteği USB-C üzerinden aktarın. Siz cihazı kullanırken Desk’in yerel hizmeti öngörülen veri alışverişini yürütür. Ekranda istendiği gibi kriptogramı sunun ve işlemi BIT üzerinde inceleyin. «BIT’ten al» yanıtı içe aktarır. Desk alındı onayı vermeden önce yanıtı doğrular ve kaydeder. Bağlantı kesilirse benzer görünen başka bir işleme geçmeyin, aynı işlemi kurtarın.

Final aygıt yazılımlarında çoklu imza sırasında özet, zorunlu çıktılar, ilgili uyarılar ve «PSBT’yi imzala» aşamasındaki üç son onay incelenir. İsteğe bağlı genişletilmiş inceleme daha fazla parametre gösterir. «Hayır» seçimi zorunlu kontrolleri kaldırmaz. Bir politikanın bağımsız doğrulanması farklı bir iş akışıdır ve sonucu o incelemenin kapsamıyla sınırlıdır.

İmzalama, gerçekliği doğrulanabilen uyumlu bir kriptogram gerektirir. Eski bir kopyadan gizli bilgi hâlâ kurtarılabiliyor olsa bile o kopya imzalama için kendiliğinden uygun hâle gelmez. Cihaz, eski kopyanın gerçekliğinin doğrulanmadığını bildirirse önce gizli bilgiyi kurtarıp kontrol edin ve yeni bir kopya oluşturun. Başlıkları değiştirmeyin veya ret uyarısını atlamayın.

Bir adres uyuşmazsa, beklenmedik bir ücret veya başka bir ağ görünürse, veri eksikse ya da cihaz politikayı reddederse işlemi iptal edin. Görüşmeyi bitirme baskısıyla onay vermeyin. Yapay zekâ düğmelere basmaz, son onayı vermez ve sizin doğrulamadığınız bir işlemi imzalanmış saymaz.

Uygulama

1. Bakiyesiz bir cüzdanla veya fiziksel kabul testleri yapılmış bir laboratuvarda modelinizin adımlarını uygulayın.
2. Son onaylardan önce durmayı canlandırın ve bunun neden yetkilendirme sayılmadığını açıklayın.
3. Yanıtın geri geldiğini ve taslakla eşleştiğini, BIT’te ise alma ve alındı onayı durumlarını kontrol edin.

Öğrendiklerinizi gösterin

Kimlik bilgilerini açıklamadan iş akışını anlatabilmeli ve cihazda verilen onay, içe aktarılan yanıt ve yayımlanmış işlemi ayırt edebilmelisiniz.

Sık sorulan soru

Çevrimdışı cihaz girdilerimin hâlâ harcanmamış olduğunu bilir mi? Zincirin güncel durumunu tek başına kontrol edemez. Uygulama son işlemi kendi ağ veri kaynağına göre doğrulamalıdır.

Ara verme noktası

İmzalamaya ara verirseniz işlemi iptal edin veya iş akışına göre tanımlanmış bekleyen bir işlem bırakın. Gizli bilgiler görünür kalmamalıdır.

BIT imzaladı ama Desk yanıtı aldığını doğrulamadı. Hangi durumu esas almalısınız?

1. Ödeme kesin olarak ağa yayımlandı.
2. Yanıtın alınması veya doğrulanması bekleniyor. Aynı işlemi kurtarın.
3. Cüzdan kayboldu.

> **Yanıtı göster: Yanıtın alınması veya doğrulanması bekleniyor. Aynı işlemi kurtarın.**
> İmzalama, alma ve yayımlama ayrı aşamalardır.

İşlemi tamamlama, yayımlama ve sorunları çözme

Amaç

Ödemeyi tekrarlamadan tamamlayın ve hataları oluştuğu aşamada tanılayın.

Konuyu anlayın

İmza içe aktarıldığında Desk taslağa karşılık geldiğini ve niyeti koruduğunu doğrulamalıdır. Çoklu imzada eşiğe henüz ulaşılmamış olabilir. Tek imzada da içe aktarma incelemeyi gereksiz kılmaz. Tüm koşullar sağlandıktan sonra sonlandırma, ağa duyurulmaya hazır işlemi oluşturur.

Yalnızca son incelemeden sonra yayımlayın. Sunucu yanıtı veya txid o isteğin sonucunu gösterir; kabulü ve zincir durumunu izleyerek doğrulayın. Uygulama yanıt almadıysa tekrarlamadan önce sorgulayın. Görüntüleme sorununu çözmek için yeni bir ödeme yaratmayın.

Bekleyen ödemede oranı, geçerliliği, çakışmaları ve gerçekte RBF uygulanabilirliğini inceleyin. Politika veya alıcı değiştiyse yeni teklif uygun yeni imzalar gerektirir. Yerel iptal başka birinde bulunan imzayı veya işlemi yok etmez, onaylananı da geri almaz.

Aşamaları ayırın: hazırlık, aktarım, kilit açma, inceleme, imza, geri dönüş, doğrulama, sonlandırma, ağa duyurma ve onay. Sistem, sürüm, model, aşama, yaklaşık saat ve hata kodunu kaydedin. Uygulama tanılamaları hassas verileri dışlayacak şekilde tasarlanmıştır. Yine de paylaşmadan inceleyin. Yedek, QR, sohbet anahtarı (Clave Chat) veya erişim bilgisi eklemeyin.

Uygulama

1. Hayalî ödemenin durumlarını sıralayın ve güvenle nerede duracağınızı belirleyin.
2. Üç sorunu çözün: yetersiz bakiye, alınmayan USB yanıtı ve yayımlama sırasında bağlantının kesilmesi.
3. Yapay verilerle ve doğrulanabilir beklenen sonuçla bir destek talebi yazın.

Öğrendiklerinizi gösterin

Sıradaki eylemin öğrenciye, cihaza, koordinatöre veya ağa mı ait olduğunu belirleyin ve gereksiz ikinci ödemeyi önleyin.

Sık sorulan soru

FIRMWARE_CAPABILITY_REQUIRED hatası gelişigüzel yazılım değiştirerek çözülür mü? Hayır. Belgelenen Desk olayında Final derlemesinin tanınması için Desk kataloğu düzeltilmeliydi. Cihazı değiştirmeden önce sürümü ve profili kontrol edin.

Ara verme noktası

Durumu ve sonraki eylemi kaydedin. Laboratuvar dışında gerçek işlem yayımladıysanız kaydını kişisel belgelerinizde tutun.

Aşağıdakilerden hangisi onaylanmış bir işlemi tek başına geri alabilir?

1. Yerel taslağı silmek.
2. Mirror’ı kapatmak.
3. Bu eylemlerin hiçbiri.

> **Yanıtı göster: Bu eylemlerin hiçbiri.**
> Yerel silme zinciri yeniden yazmaz ve dolaşımdaki yetkilendirmeleri geri almaz.

Bitcoin’de hangi bilgiler gözlemlenebilir?

Amaç

Herkese açık verileri, çıkarımları ve zincir dışında eklediğiniz bilgileri ayırt edin.

Konuyu anlayın

Bitcoin zinciri açıktır. Betikler, gösterilebilen adresler, değerler, girdi-çıktı ilişkileri ve blok içindeki konum incelenebilir. Adınızın görünmesi şart değildir ama kimliği belirli bir satın alma, yayımlanan fatura veya paylaşılan adres sizi bu geçmişe bağlayabilir.

Takma kimlikle işlem yapmak, tek başına resmî kimliğiniz olmayan tanımlayıcılar kullanmaktır. Anonimlik, bir küme içinde ayırt edilememe koşulları gerektirir. Uygulama kurmak bunu sağlamaz. Mahremiyet bağlama bağlıdır: satıcı ödemenizi, borsa çekiminizi, sunucu sorguları bilebilir; bir kişi cihazlarınızı görebilir.

Gerçeklerle çıkarımları ayırın. «Bu çıktı o işlemde harcandı» zincirden doğrulanır. «Tüm girdiler aynı kişiye ait» hatalı olabilecek bir tahmindir. Zincir dışı kimlik tespiti bir varsayıma güveni artırabilir ama her yorum kesinleşmez.

Adresin yeniden kullanılması etkinliği bir araya getirmeyi kolaylaştırır. Farklı bağlamlardan UTXO’ları birleştirmek onları ilişkilendirebilir. xpub açıklamak tek adres göstermekten daha geniş izleme sağlar. Bir txid paylaşmak alıcının bilmesine gerek olmayan başka çıktıları ve ilişkileri de gösterebilir.

Uygulama

1. Hayalî bir işlemde hangi verilerin herkese açık, hangi etiketlerin size ait olduğunu işaretleyin.
2. İsim içeren bir fatura ekleyip oluşan yeni bağlantıyı tarif edin.
3. Adres, tanımlayıcı veya bakiye vermeden hatayı çözmeye yarayacak destek talebi yazın.

Öğrendiklerinizi gösterin

«Bu gözlemlenebilir» ve «bu bir çıkarımdır» ifadelerini ayırın ve eksik kanıtı açıklayın.

Sık sorulan soru

Hiç adres tekrarlamazsam anonim olur muyum? Hayır. Girdi seçimi, para üstü, sorgular, karşı taraflar ve diğer üstveriler önemini korur.

Ara verme noktası

Gerçek kimlik veya işlem içermeyen bir gözlemci haritası saklayın.

Bir hesaptaki ilişkili adreslerin izlenmesini genellikle hangi bilgi sağlar?

1. Simgenin rengi.
2. Hesabın xpub’ı ve yeterli türetme bilgisi.
3. Kablonun markası.

> **Yanıtı göster: Hesabın xpub’ı ve yeterli türetme bilgisi.**
> Genişletilmiş açık bilgi tek başına harcama yetkisi vermese de mahremiyet açısından hassastır.

M07

Bağlamları ayırma ve para üstünü yönetme

Amaç

UTXO’larınızın kökeniyle tutarlı harcama kararları verin.

Konuyu anlayın

Bağlamları ayırma ödemeden önce başlar. Bir alımın birikime, mesleki faaliyete, günlük harcamaya veya belirli ilişkiye mi ait olduğunu belirleyin. Sonraki seçimde bilgisizlikten kaybolmaması için bu bilgiyi özel etiketlerde koruyun.

Etiket çıktıları kriptografik olarak ayırmaz. Farklı bağlamlardan iki UTXO’yu birlikte harcarsanız işlem aralarındaki ilişkiyi yayımlar. Birleştirme, gelecekteki ödemelerin girdi sayısını azaltırken birleştirilen çıktıların bağlantısını artırır. Ücretler düşükken maliyet bakımından verimli olsa bile gizlilik hedefinizle çelişebilir.

Para üstü aynı politikanın kontrolündeki yeni çıktıdır, «görünmez para» değildir. Sonradan harcanması önceki bağlantıları genişletebilir. Sırf tutarı alışılmadık diye bir adresi para üstü saymayın. Gerçek incelemede cihaz cüzdana ait olduğunu doğrulamalıdır.

Mahremiyeti mekanik tutar, zamanlama veya yinelenen transfer kalıplarına dönüştürmeyin. Bunlar da tanınabilir ve fazladan ücret doğurabilir. Her tarafın mevcut bilgisini ve önerilen işlemin hangi yeni bilgiyi yayımlayacağını değerlendirin. Hiçbir işlem dizisi yayımlanmış geçmişi silmez.

Uygulama

1. Üç bağlamdan beş hayalî UTXO oluşturun ve gereken en az sayıda bağlamla ödeme hazırlayın.
2. Oluşan para üstünü belirleyin ve etiketini seçin.
3. Tüm çıktıları birleştirmekle ayrı tutmanın maliyetini ve açığa çıkan ilişkileri karşılaştırın.

Öğrendiklerinizi gösterin

Her duruma katı tek kural koymadan bir birleştirmeyi somut gerekçeyle kabul veya reddedin.

Sık sorulan soru

Her şeyi kendi başka adresime taşımak geçmişi koparır mı? Hayır. Yeni bir ilişkiyi yayımlar ve tehdidi gidermeden masraf ekleyebilir.

Ara verme noktası

Laboratuvar gerekçenizi ve seçtiğiniz girdi seçimi politikasını saklayın.

Maaş ve bağış girdilerini tek işlemde birleştirmenin sonucu ne olabilir?

1. Bu girdiler arasındaki ilişkiyi görünür hâle getirmek.
2. Herkese açık kaynak geçmişlerini silmek.
3. Onları kesin olarak anonim nakde dönüştürmek.

> **Yanıtı göster: Bu girdiler arasındaki ilişkiyi görünür hâle getirmek.**
> UTXO sayısının azalması gözlemlenebilir bağlantıları artırabilir.

M07

Ağ gizliliği, Tor ve VPN

Amaç

Bağlantı gizliliğini zincir üzerindeki mahremiyetten ayırın.

Konuyu anlayın

Sorgu sunucusu istekleri bağlantıyla ilişkilendirebilir. İnternet sağlayıcınız aktarım yöntemine göre hedefleri veya kalıpları görebilir. VPN bu güvenin bir kısmını VPN işletmecisine kaydırır. Bitcoin'in açık verilerini silmez ve kimlikli hesabın sizi tanımasını engellemez.

Tor, kaynakla hedef arasındaki belirli bağlantıları azaltmak için trafiği bir ağdan geçirir. Bitcoin adresini gizli hâle getirmez ve trafiği Tor'dan geçmeyen uygulamayı korumaz. Tor Browser'ı açmak Desk'i, Bitcoin Core'u veya bilgisayarın tüm hizmetlerini otomatik yapılandırmaz.

Bir bağlantının korunduğunu söylemeden önce rotasını ve yapılandırmasını doğrulayın. İncelenen sürümde Desk'in yerleşik Tor düğmesi olduğu varsayılmaz. Düğüm veya proxy kurulumu mühendislik yönergesi ve gerçek trafiğin doğrulanmasını gerektirir. Başka bir cüzdanda var diye bir arayüz alanı uydurmayın.

DNS, hesap eşitleme, gezgin bağlantıları ve fiyat hizmetleri üzerinden de bilgi sızabilir. Bir düzen bakiye sorgularını korurken açık gezgin açıldığında etkinliğinizi gösterebilir. Her önlemin kapsamını ve bağlantı kesilince ne yapılacağını tanımlayın. Daha az gizli sağlayıcıya habersiz geçişten kaçının.

Uygulama

1. Bilgisayar, bağlantı sağlayıcısı, varsa proxy, düğüm veya hizmet ve Bitcoin ağı arasındaki yolu çizin.
2. Sorguları kimin aldığını ve ticari kimliğinizi kimin gördüğünü belirtin.
3. Özel düğümünüzün yanıt vermediğini canlandırın. Açığa çıkacak bilgileri anlayarak duraklama veya açıkça kaynak değiştirme arasında karar verin.

Öğrendiklerinizi gösterin

Yapılandırmanızın hangi tehdidi azalttığını ve hangisinin kaldığını açıklayın.

Sık sorulan soru

Tor, kimsenin bir ödemeyi benimle ilişkilendiremeyeceğini garanti eder mi? Hayır. Karşı taraflar, ticari kimlik bilgisi, kalıplar ve kullanım hataları hâlâ bağlantı kurabilir.

Ara verme noktası

Özel bağlantı adresleri veya parolalar yerine tasarımın kapsamını kaydedin.

Tor Browser’ı açmak Desk’i sorgularını Tor üzerinden yapmaya zorlar mı?

1. Evet, aynı bilgisayarda oldukları için.
2. Evet, simgesi görünüyorsa.
3. Hayır. Her uygulamanın ağ yolu ayrı ayrı yapılandırılıp doğrulanmalıdır.

> **Yanıtı göster: Hayır. Her uygulamanın ağ yolu ayrı ayrı yapılandırılıp doğrulanmalıdır.**
> Bir uygulamanın koruması diğer uygulamalara otomatik aktarılmaz.

CoinJoin, Payjoin ve güncel sınırlamalar

Amaç

Ortak işlem araçlarını, sahip olmadıkları anonimlik veya uyumluluğu onlara atfetmeden anlayın.

Konuyu anlayın

CoinJoin, girdi ve çıktılarla ilgili bazı çıkarımları zorlaştırmak için birden çok kişinin katkısını tek işlemde toplar. Başka paralar iade edeceğini söyleyen bir saklama hizmetine para vermekle aynı değildir. Her tasarımda koordinasyonu, saklamayı, ücretleri, kötü niyetli katılımcılara dayanıklılığı ve sonrasındaki kullanımı inceleyin.

Payjoin, ödeyen ile alıcının girdilerini ortak ödemeye katarak ortak sahipliğe ilişkin bazı çıkarımları zayıflatır. Her iki uçta uyumlu destek ve belirli bir protokol gerekir. Bu konu teknik anlayış içindir. İncelenen kaynaklar Cuvex Desk’te tümleşik, çalışan bir Payjoin veya CoinJoin akışını doğrulamıyor.

Hizmetlerin kullanılabilirliği ve hukuki bağlam değişir. Wasabi belgeleri, zkSNACKs koordinatörünün 1 Haziran 2024’te kapandığını kaydeder. Eski bir düğme bugün hizmet sağlama garantisiymiş gibi öğretilmemelidir. ABD Adalet Bakanlığı 2025’te Samourai kurucularının suçlarını kabul ettiklerini ve daha sonra hüküm giydiklerini duyurdu. Bu olay, tüm gizlilik tekniklerinin her yargı alanında yasa dışı olduğunu göstermez.

Bir araç bir çıkarımı zayıflatırken diğerlerini etkilemeyebilir. Bilinen kaynak, karşı tarafın kayıtlarından silinmez. Sonradan birleştirme, üstveri ve katılımcı grubunun hataları mahremiyeti azaltabilir. Bazı hizmetler belirli geçmişlere sahip paralara farklı ticari politikalar uygulayabilir.

Uygulama

1. Gerçek işlem yapmadan sıradan bir işlemi, ortaklaşa işlemi ve varlıkların saklamasını üstlenen bir hizmeti karşılaştırın.
2. Bir aracın kullanımını önermeden önce sürümünü, bakımını üstleneni, hizmet durumunu ve güncel belgelerini bulun.
3. Teknik, saklama ve hukuki riskleri ayrı belirleyin. Eğitmen denetimleri aşma yolları tasarlamamalı veya «izlenmesi imkânsız fonlar» vaat etmemelidir.

Öğrendiklerinizi gösterin

Bir gizlilik tekniğinin sınırlı bir yararını ve en az iki riskini veya gerekliliğini açıklayın.

Sık sorulan soru

Cuvex’in mahrem saklama sağlayabilmesi için karıştırıcı gerekir mi? Hayır. Sorguların, verilerin, anahtarların ve UTXO seçiminin kontrolü zaten belirli riskleri azaltır; tam görünmezlik vaat etmez.

Ara verme noktası

Kanıt olmadan «uyumlu» yazmayın. Aracı «incelendi» olarak kaydedin.

Hangi ifade savunulabilir?

1. CoinJoin kalıcı anonimliği garanti eder.
2. Ortak bir işlem tekniği, belirli gereklilikler ve sınırlar içinde bazı çıkarımları zorlaştırabilir.
3. «Mixer» adlı her hizmet öz saklamayı korur.

> **Yanıtı göster: Ortak bir işlem tekniği, belirli gereklilikler ve sınırlar içinde bazı çıkarımları zorlaştırabilir.**
> Özellikler protokole, uygulamaya, katılımcılara ve sonraki kullanıma bağlıdır.

Gerçek olaylardan çıkarılabilecek dersler

Amaç

Belgelenmiş olayları, rakiplere saldırmadan veya korumayı abartmadan doğrulanabilir kararlara dönüştürün.

Konuyu anlayın

Mt. Gox olayında ABD Adalet Bakanlığının 2023 tarihli iddianamesi, sunuculara ve anahtarlara yetkisiz erişildiğini ve sonrasında müşteri fonlarının kaybolduğunu ileri sürdü. İddianame iddiaları açıklar, mahkûmiyet kararı değildir. Saklama açısından sorulacak soru anahtarların gerçek kontrolünün kimde olduğu ve şirket çökerse ne olacağıdır.

Aralık 2023'teki Ledger Connect Kit olayında Ledger, eski bir çalışanın erişiminin ele geçirilmesinden sonra merkeziyetsiz uygulamaların kullandığı bir kitaplığın kötü amaçlı sürümünün yayımlandığını belgeledi. Yazılım dağıtım zinciri etkilendi ve EVM DApp kullanıcıları imza vermeye kandırıldı. Bu olay Ledger donanımının veya Bitcoin mutabakatının kırıldığını göstermez.

Şubat 2025'teki Bybit olayında FBI, yaklaşık 1,5 milyar ABD doları değerindeki sanal varlığın çalınmasını Kuzey Kore'ye atfetti. Olay bir borsayı ve başka ağlardaki varlıkları ilgilendiriyordu. Bitcoin kriptografisinin kırılması olarak sunulmuyor. Öğrenmeniz gereken, imzanın amacını doğrulamak ve birden fazla kişinin aynı ekrana körü körüne güvenmesini önlemektir.

Mayıs 2025'te Coinbase, rüşvet verilen destek görevlileri aracılığıyla sosyal mühendisliği kolaylaştırmak amacıyla veri çalındığını bildirdi. Parolaların ve özel anahtarların açığa çıkmadığını belirtti. Öğrenci için ders, dolandırıcının doğru bilgilere sahip olmasının onu güvenilir kılmadığıdır.

Bitcoin Core da yazılım hatalarını yayımlar. CVE-2024-35202 duyurusu, 25.0 öncesi sürümlerde uzaktan kapanmaya yol açılabildiğini bildiriyordu. Kuralları doğrulamak yazılım bakımını gereksiz kılmaz. Duyurudan anahtar hırsızlığı sonucu çıkarılamaz.

Ocak 2026'da The Register, Ledger alıcılarının sipariş ve iletişim verilerinin Global-e üzerinden açığa çıktığını yazdı. Haberde doğrulamalar iki şirkete de atfedildi. Açıklamalarına göre kurtarma anahtarları etkilenmedi. Donanım ele geçirilmemiş olsa bile bir satın alma, cihaz sahibi olduğunuzu gösterebilir.

Nisan 2026’da The Record, Drift’e yönelik saldırıyı ve platformun para yatırma ve çekme işlemlerini askıya aldığını bildirdi. Drift Solana üzerindeki merkeziyetsiz finans protokolüdür. Olay Bitcoin’in kırılması değildir. İlk kayıp tahminlerini kesin tutar, daha sonraki kurtarma süreçlerini garantili geri ödeme olarak sunmayın.

Uygulama

1. Her olayı saklama, arayüz veya dağıtım, kişisel veriler, diğer ağların protokolleri ve kullanılabilirlik açısından sınıflandırın.
2. Her biri için bir önleyici tedbir ve o tedbirin bir sınırını önerin.
3. Dolandırıcılık aramasını prova edin: «Satın almanızı biliyorum, fonlarınızı bu güvenli adrese taşıyın». Kapatın ve sizin başlattığınız bağımsız bir kanaldan doğrulayın.

Öğrendiklerinizi gösterin

Hiçbir olayın başka bir markanın zarar görmez olduğunu neden kanıtlamadığını açıklayın. Kanıt belirli bir kapsamı destekler.

Sık sorulan soru

Bunlar gerçekleşen en son saldırıların tümü mü? Hayır. 17 Kasım 2026 baskısı için doğrulanmış seçkidir. Kapsamlı envanter veya canlı izleme değildir.

Ara verme noktası

Değiştireceğiniz alışkanlığı ve ona bağlı kaldığınızı nasıl kontrol edeceğinizi yazın.

Bir kişi yaptığınız satın almayı biliyor ve «kurtarma cüzdanına» para göndermenizi istiyor. Satın almanızı bilmesi neyi gösterir?

1. Bilgi sızmış olabilir. Bu, kişinin kimliğini veya adresin gerçekliğini doğrulamaz.
2. Mutlaka yetkili destek görevlisi olduğunu.
3. Kurtarma ifadesini paylaşmanız gerektiğini.

> **Yanıtı göster: Bilgi sızmış olabilir. Bu, kişinin kimliğini veya adresin gerçekliğini doğrulamaz.**
> Gerçek bilgiler inandırıcı bir dolandırıcılık kurgulamak için kullanılabilir.

M08

Sohbet kimliği oluşturma ve kişileri doğrulama

Amaç

Anahtarını açığa çıkarmadan sohbet kimliğini etkinleştirin ve karşı tarafı doğrulayın.

Konuyu anlayın

Desk’te sohbet, Cuvex’te üretilen sohbet anahtarı (Clave Chat) ile kriptograma bağlanır. Gösterimi xpub gibi görünebilir ama gizlidir. WOW hesabının açık anahtarı gibi ele alınmamalıdır. Eğitmenin bu anahtarı okuması veya QR ile görmesi asla gerekmez.

Akış yeni takma ad ile mevcut bir takma adı taşıma veya kurtarmayı ayırır. İncelenen uygulamada uygun iOS ya da Android mobil profili seçilir. Geçmişte türetilen kimlikler tahmine dayalı olarak birbirinin yerine kullanılamaz. DEV ve Üretim ayrı ortamlardır. Ortam değiştirmek sohbet ve takma adları otomatik taşımaz.

Takma ad eklemek kimliği doğrulamaz. Parmak izini bağımsız ve kimliği doğrulanmış bir kanaldan karşılaştırın. Tanıma soruları sunuluyorsa herkese açık olmayan bilgiler kullanın ve parola açığa çıkaran yanıtlardan kaçının. Tanıdık ses taklit edilebilir. Riskli durumlarda önceden kararlaştırılmış yöntemleri birlikte kullanın.

Kişinin kimliği değişirse durum netleşene kadar ödeme ve koordinasyonu durdurun. Bu meşru bir kurtarma veya kötü niyetli değişim olabilir. Uçtan uca şifreleme, protokol ve uygulamaya göre kanalı korur. Karşı taraftaki cihazı kimin kullandığını kanıtlamaz.

Uygulama

1. Deneme ortamında sohbet anahtarını (Clave Chat) vermeden oluşturma veya kurtarma akışını açıklayın.
2. Laboratuvar kişisi ekleyin. Parmak izinin doğrulanmasını başka bir kanaldan kararlaştırın.
3. Kimlik değişimini canlandırın. Ödemeden önce değişikliği nasıl doğrulayacağınızı belirleyin.

Öğrendiklerinizi gösterin

Takma adı, açık parmak izini, gizli sohbet anahtarını (Clave Chat) ve kişiye duyulan insanî güveni ayırt edin.

Sık sorulan soru

Eski bir takma ad aynı kişi olduğunu garanti eder mi? Hayır. Kimliğin sürekliliği ve anahtar değişiklikleri ilgili iş akışıyla kontrol edilmelidir.

Ara verme noktası

Yalnızca «deneme kişisi doğrulandı» bilgisini ve yöntemi kaydedin. Anahtarları veya özel soruları eklemeyin.

Bir karakter dizisinin adı sohbet anahtarı (Clave Chat), görünüşü ise xpub gibi. Desk’te bu veri nasıl ele alınır?

1. Forumlarda yayımlanabilecek veri olarak.
2. Kimliği kurtarmaya yarayan gizli bilgi olarak.
3. Bitcoin alma adresi olarak.

> **Yanıtı göster: Kimliği kurtarmaya yarayan gizli bilgi olarak.**
> Verinin görünüşü, gizlilik düzeyini veya amacını belirlemez.

Sohbet üzerinden satoshi isteme ve ödeme

Amaç

İnceleme ve bağlamı kaybetmeden sohbetten ödemeye geçin.

Konuyu anlayın

Sohbetten adres istenebilir, alım adresiyle yanıt verilebilir, ödeme talep edilebilir ve WOW hesabından hazırlık açılabilir. Bağlamı kanalda tutmak uygulamalar arasında kopyalama hatalarını azaltır. Her mesajı kimliği doğrulanmış harcama talimatı yapmaz.

Yanıt veya ödemeden önce doğrulanmış kişiyi, ağı, tutarı ve asıl isteği inceleyin. Ortak form UTXO ve ücret seçimini korur. Mesajda tutar istenir ama «Tamamını gönder» seçilirse ücretten sonraki net tutar yetersiz olabilir. Gerekiyorsa kısmi ödeme olarak açıkça belirtilmelidir.

Yetkilendirme Cuvex'te kalır. Sohbet niyeti ve koordinasyonu taşır, otomatik imzalama yetkisi yoktur. Kişiye gönderilen ödeme bildiriminde mesajın alınması ile işlemin onaylanmış olması ayrılmalıdır. Alıcı kendi hesabından veya kaynağından doğrular.

Dış bağlantılar, ek QR kodları ve adresler doğrulanana kadar güvenilmeyen veridir. «Mempool'da görüntüle» üçüncü taraf hizmetini açıp sorguları açıklayabilir. Politikanız kendi düğümünü kullanıyorsa WOW'daki uyumlu doğrulamayı tercih edin. Kamuya açık hizmete yönlenmeyi değerlendirin.

Uygulama

1. İki rolü canlandırın. Alıcı 50.000 sat istesin, ödeyen işlemi hazırlasın ancak yayımlamasın.
2. 48.000 sat kullanılabilir net bakiye varsayın. Kısmi ödeme için hangi onay ve mutabakatın gerektiğini açıklayın.
3. Deneme mesajında ağı bilerek değiştirin ve işlemi durdurun.

Öğrendiklerinizi gösterin

İstek, adres, taslak, imza ve onayın ilişkisini «sohbette OK yazıyor» düzeyine indirgemeden izleyin.

Sık sorulan soru

Sohbetten sats göndermek Lightning kullanmak mıdır? Hayır. Belgelenen WOW akışı Bitcoin zincirinde ödeme hazırlar. Sats birimdir, taşıma ağı değildir.

Ara verme noktası

Laboratuvar taslağını iptal edin veya durumunu kaydedin. Arayüz göstermek için ağa yayımlamayın.

Sohbette bir onay aldınız. Ödemenin alındığına ilişkin belirleyici kontrol hangisidir?

1. Mesaj simgesinin yeşil olması.
2. Karşı tarafın «onaylandı» demesi.
3. İşlemi ve çıktılarını uygun ağ kaynağından doğrulamak.

> **Yanıtı göster: İşlemi ve çıktılarını uygun ağ kaynağından doğrulamak.**
> Mesajın durumu ile işlemin durumu aynı şey değildir.

Kriptogramları bilinçli biçimde paylaşma

Amaç

Başkasına şifreli bir kopya vermenin sonuçlarını anlayın.

Konuyu anlayın

Kriptogram paylaşmak şifreli nesnenin bir kopyasını iletir. Bu mutlaka bitcoin göndermez ve tek başına yeni imzalayıcı eklemez. Alıcı yeterli kilit açma araçlarına da ulaşırsa şemaya göre içeriğe erişebilir. Hangi yeteneği aktardığınızı önceden belirleyin.

Sohbetin uçtan uca şifrelemesi ile dosya şifrelemesi farklı katmanları korur. Alıcı indirdiği nesneyi sohbet dışında saklayabilir. Mesajınızı veya yerel kaydı silmek tüm kopyaları geri almayı garanti etmez. Parolayı aynı kanaldan paylaşmak bileşenleri tek yolda toplayabilir.

Göndermeden önce kimliği, biçimi ve amacı doğrulayın. Alınan kriptogramı bağlayabilmek kopyayı düzenlemeye yarar. Her dosyanın güvenle çözülebileceği anlamına gelmez. Dış bir sayfada kurtarma ifadesi veya parola girilmesini isteyen ekleri kullanmayın.

Kurtarma için işleyiş kararlaştırılmalıdır: her bileşeni kim saklar, kim açabilir, ifşa nasıl saptanır ve ilişki sonlanırsa saklama nasıl değişir? Sıradan bir ödeme için çoğunlukla doğrulanmış adres yeterlidir. Kriptogramınızı paylaşmaya gerek yoktur.

Uygulama

1. Şifreli eğitim metnini bir laboratuvar kişisine aktaracak bir süreç tasarlayın.
2. Parolayı öğrenmeden önce ve sonra alıcının neleri bildiğini ve yapabileceğini listeleyin.
3. İlişkinin sona erdiğini canlandırın. Mesajı silmenin neden kopyayı veya anahtarları geçersiz kılmadığını açıklayın.

Öğrendiklerinizi gösterin

«Veri paylaştım», «bir sırra erişim verdim» ve «bir harcamayı imzaladım» arasındaki farkı belirtin.

Sık sorulan soru

Şifreli dosya sonuç doğurmadan dolaşabilir mi? Üstveri açıklayabilir, parola tahmin girişimlerini kolaylaştırabilir ve süresiz saklanabilir. Paylaşmanın gerekli olup olmadığını değerlendirin.

Ara verme noktası

Kursta saklama ile ilgili ek bırakmayın. Yalnızca alıştırmanın sonucunu kaydedin.

Kriptogramı sohbet üzerinden paylaşmak bitcoin göndermekle aynı mıdır?

1. Hayır. İçeriği ve erişim koşulları farklı anlam taşıyan bir nesne aktarılır.
2. Evet, uzantısı .bin ise.
3. Bu işlem otomatik olarak yeni bir çoklu imzayı etkinleştirir.

> **Yanıtı göster: Hayır. İçeriği ve erişim koşulları farklı anlam taşıyan bir nesne aktarılır.**
> Gizli bilgi aktarımı ile UTXO’ların taşınması ayrı işlemlerdir.

M08

Sohbeti geri yükleme ve üstverilerini anlama

Amaç

Cihaz değişimini planlayın ve kimliği kurtarmakla mesajları kurtarmayı ayırın.

Konuyu anlayın

Desk, geçmişin ve oturumların yerelde şifrelendiğini ve genel yedeğine dâhil olmadığını belirtir. Sohbet anahtarı (Clave Chat) kimliği kurtarır, eski konuşmaların hepsini garanti etmez. Uygulama, bekleyen etkinleştirme, anahtar bakımı ve uyumlu materyal varsa yerel kurtarma için durumlar ve komutlar içerir.

İncelenen kılavuza göre her takma ad aynı anda yalnızca bir cihazda kullanılmalıdır. Desteklenmiyorsa «eşitlemeyi denemek» için iki cihazda birden etkinleştirmeyin. Taşıma prosedürünü izleyin ve kişilerle kimliğin sürekliliğini doğrulayın.

«Bekliyor», «sunucu kabul etti», «alındı» ve «şifre çözülemedi» ayrı aşamalardır. Onaylanmamış gönderimi körü körüne tekrar etmeyin. Önce ulaşıp ulaşmadığını çözün. Oturum anahtarı eksikse veya kimlik değişmişse bekleyen mesajın saklanması okunduğu anlamına gelmez.

Şifreli içerik zamanları, boyutu, teslim ilişkilerini, takma adları veya bağlantı verilerini tüm ilgili sistemlerden mutlaka gizlemez. Ses için de benzer durum vardır: aktarım şifrelemesi sıradan bir aramayı sırlar için uygun kanala dönüştürmez. Öğrenmek ve sorun çözmek için gereken en az veriyi kullanın.

Uygulama

1. Bilgisayar kaybını canlandırın ve elinizdeki her materyalin neyi kurtardığını açıklayın.
2. Mesaj durumlarını sınıflandırın ve ödeme isteğinin ne zaman tekrar gönderilmemesi gerektiğini belirleyin.
3. Kişilerin bağımsız kanaldan doğrulayabileceği bir cihaz değişikliği bildirimi hazırlayın.

Öğrendiklerinizi gösterin

Yedeğin kapsamadığı kurtarmayı vaat etmeden hangi konuşmanın kaybolabileceğini ve hangi kimliğin geri yüklenebileceğini anlatın.

Sık sorulan soru

Yerel sohbeti silmek karşı taraftaki mesajları da siler mi? Böyle varsaymayın. Alıcı mesajları ve dosyaları bağımsız olarak saklayabilir.

Ara verme noktası

Sohbet anahtarı (Clave Chat) içermeyen, yalnızca boş alan adları olan taşıma planını saklayın.

İncelenen kılavuza göre sohbet anahtarı (Clave Chat) tek başına ne sağlar?

1. Her bilgisayarda tüm eski konuşmalara erişim.
2. Uyumlu yöntemle kimliği kurtarma olanağı. Eski mesajların tamamını kurtarmayı sağlamaz.
3. Kişilerin Bitcoin anahtarlarına otomatik erişim.

> **Yanıtı göster: Uyumlu yöntemle kimliği kurtarma olanağı. Eski mesajların tamamını kurtarmayı sağlamaz.**
> Kimliği kurtarmak ve geçmiş arşivini kurtarmak ayrı yeteneklerdir.

Günlük ayarlar ve izinleri gözden geçirme

Amaç

Kolaylıkla korumayı karıştırmadan Desk ayarlarını yönetin.

Konuyu anlayın

Desk Gece, Gündüz veya Sistem teması, otomatik eşitleme ve 3 ya da 5 dakikalık aralıklar, işlem sesleri, sohbet arka planı, dil ve referans para birimi sunar. Bu tercihler görünümü veya sorgu sıklığını değiştirir. Bitcoin imzasını değiştirmez ve anonimlik eklemez.

İncelenen güvenlik ayarları hareketsizlikte kilitleme, arka plana geçerken kilitleme, başarısız girişlerden sonraki azami gecikme ve isteğe bağlı silme sunar. Hareketsizlik şeması 30 ila 86.400 saniyeyi kabul eder, arayüz daha dar seçenekler sunabilir. Varsayılanları kayıtlı dersten çıkarmak yerine kullandığınız sürümden okuyun.

bitcoin: bağlantı entegrasyonu kilit açmak, hesap seçmek ve incelemek için bir istek açar. Otomatik ödemeyi onaylamaz. Linux kılavuzu bağlantı kaydı açısından tümleşik kurulum ile AppImage'ı ayırır. Lightning ödeme isteği farklı bir uyumlu akış gerektirir. Desk'i varsayılan uygulama seçmek bunu sağlamaz.

Kur, fiyat grafiği ve bilgi bağlantıları dış hizmetleri sorgulayabilir. İşlevleri bilgi vermektir, alım sinyali değildir. Tutar dönüştürürken önce tarihi ve kaynağı inceleyin. Koyu tema veya küçük pencere son düğmeleri, adresi ya da ücreti gizlememelidir. Gizlenirse duraklatın ve yerleşim sorununu bildirin.

Uygulama

1. Eğitim deposunda görünüm ve kilidi ayarlayın. Tekrar girebildiğinizi doğrulayın.
2. Hangi otomatik işlevleri etkinleştirdiğinizi inceleyin. Eşitleme, sesler ve aygıt yazılımı denetimi ayrı işlevlerdir.
3. Hayalî bir bitcoin: bağlantı isteği açın ve gerçek işlem hazırlamadan iptal edin.

Öğrendiklerinizi gösterin

Her ayarın etkisini açıklayın. Sorgu veya hassas eylem içerenleri bulun.

Sık sorulan soru

Bilgisayar biyometrisi kurtarma yedeğimin yerini tutar mı? Hayır. Cihaza ve işletim sisteminin güvenli deposuna bağlı olabilir. Bağımsız kurtarma imkânını koruyun.

Ara verme noktası

Desk’i kilitleyin ve yalnızca değiştirdiğiniz tercihleri kaydedin.

Eşitlemeyi üç dakikada bir yapmayı seçerseniz ne değişir?

1. İşlev çalıştığında sorguların planlanan sıklığı.
2. Zincirdeki imza politikası.
3. Cihazın kurtarma ifadesi.

> **Yanıtı göster: İşlev çalıştığında sorguların planlanan sıklığı.**
> Bu bir çalışma tercihidir. Varlıkların saklama biçimini değiştirmez.

M09

Çok imzalı cüzdan tasarlama

Amaç

Makul kayıp ve ele geçirilme senaryolarına dayanacak imza eşiğini seçin.

Konuyu anlayın

N katılımcıdan M imza politikasında N, farklı anahtarlara sahip katılımcıların sayısı, M ise gereken imza sayısıdır. 3 katılımcıdan 2 imza düzeninde bir anahtar kullanılamasa da harcama yapılabilir. Ancak ele geçirilen iki anahtar da harcamayı yetkilendirebilir. Üç kurtarma ifadesi aynı yerdeyse veya aynı olayda açığa çıkabiliyorsa bağımsızlık azalır.

İncelenen Cuvex çoklu imza profili, sortedmulti ve BIP48 türetmesiyle yerel P2WSH kullanır. Yapısal olarak Original en fazla altı, BIT ise en fazla on beş politika anahtarı destekler. Her ikisi de katılıyorsa daha düşük kapasiteli katılımcı ve gerçek taşıma boyutu esas alınmalıdır. Yapısal üst sınırlar, çok sayıda anahtar ve girdi içeren bir politikanın ortama sığacağını garanti etmez.

Uygulama politikanın ilişkilerine uygun eşikleri destekler. Ancak N katılımcıdan 1 imza yeterliyse harcamak için iş birliği gerekmez. Aygıt yazılımı bu riske özel uyarılar verir. Daha büyük sayı her şeyi iyileştirmez. Koordinasyon, maliyet, kurtarma için gereken materyal ve kilitlenme riski artar.

MuSig2, Schnorr imzalarının birleştirilmesine yönelik farklı bir şemadır. Tek başına N katılımcıdan N imza gerektirir, örneğin herhangi bir 5’te 3 eşik değildir. İncelenen Final aygıt yazılımlarında Taproot girdilerini imzalama, MuSig2 ve Miniscript uygulanmamıştır. P2TR alıcıya ödeme hazırlayabilmek Taproot cüzdanından imza atılabildiğini kanıtlamaz.

Uygulama

1. Katılımcıların riskleri bağımsız olacak şekilde hayalî bir 3’te 2 düzen tasarlayın.
2. Bir anahtarın kaybını ve bir anahtarın ele geçirilmesini canlandırın. Nelerin yapılabildiğini ve yapılamadığını açıklayın.
3. Daha büyük bir politika seçmeden önce her modelin sınırlarını kontrol edin.

Öğrendiklerinizi gösterin

Tasarımın kaç kayba dayanabildiğini, saldırganın hangi eşiğe ulaşması gerektiğini ve ortak bağımlılıkları açıklayın.

Sık sorulan soru

Çoklu imzada katılımcıların birbirinin kurtarma ifadelerini bilmesi gerekir mi? Hayır. Amaç, herkesin kendi özel yetkisini koruması ve politika oluşturup kurtarmak için gereken açık bilgiyi paylaşmasıdır.

Ara verme noktası

Tasarımı hayalî katılımcılar ve sorumluluklarıyla saklayın.

Bağımsız anahtarlara sahip, 3 katılımcıdan 2 imza gerektiren bir politikada geçerli harcamayı yetkilendirmek için kaç özel anahtar yeterlidir?

1. Bir.
2. İki.
3. Her zaman üçü de.

> **Yanıtı göster: İki.**
> Eşik iki imza gerektirir. Diğer koşulların ve doğrulamaların da sağlanması gerekir.

Davet oluşturma ve anahtar sağlama

Amaç

Kurtarma ifadelerini paylaşmadan doğrulanmış katılımcılarla politika oluşturun.

Konuyu anlayın

Oluşturan taraf adı, ağı, M ve N'yi, kişileri, kendi açık bilgilerini ve davetin çalışma koşullarını seçer. İncelenen şema bu akışta mainnet ve regtest'i, cihaz sınırlarından önce 2 ila 15 katılımcıyı ve 1 ila 720 saatlik işlem geçerliliğini kabul eder. Bu değerler kapasite kontrolünü atlama izni değildir.

Her katılımcı daveti inceler, kabul veya ret kararı verir ve uyumlu işlemle parmak izi ve BIP48 yoluyla birlikte kendi genişletilmiş açık anahtarını sağlar. Kurtarma ifadesi, özel anahtar, tek başına adres veya başka cüzdanın tam tanımlayıcısını vermez. Bağlamı hatalı bir anahtar geçerli xpub gibi görünse de farklı politika oluşturabilir.

Oluşturan kişi koordinasyonu yürütür ama her imzalayıcının doğrulamasının yerini tutmaz. Fon almadan önce herkes aynı parametreleri ve kontrol adresini yeniden oluşturup doğrulayabilmelidir. Sohbette kabul edilen kişi gönderdiği politikalar için otomatik onay almaz.

Davetin sona ermesi uygulamanın koordinasyon kuralıdır. Fon içeren mevcut betiği değiştirmez, başkalarının kaydettiği imzaları silmez ve mutabakat düzeyinde zaman kilidi değildir. Teklifi iptal etmekle var olan politikadan fon çekmek ayrı eylemlerdir.

Uygulama

1. Hazırlanmış regtest laboratuvarında deneme kişileriyle 3'te 2 teklif oluşturun.
2. Bir kabul, bir ret ve yanlış ağdan bir katkı canlandırın. Sonuncunun durdurulduğunu doğrulayın.
3. Fon aktarmadan önce herkesin saklaması gerekenleri listeleyin: ağ, eşik, açık anahtarlar, kökenler, betik ve doğrulanmış adres.

Öğrendiklerinizi gösterin

Eksik daveti tanıyın ve sırf sohbet var diye onay varsaymadan hangi onayın gerektiğini açıklayın.

Sık sorulan soru

Son kullanma tarihi sonradan harcamayı imkânsız kılar mı? Yalnızca davet alanı olduğu için hayır. Bitcoin zaman kısıtı belirli betik veya işlem koşulları ve gerçek destek gerektirir.

Ara verme noktası

Teklifin öğretim amaçlı kimliğini ve bekleyen onayı kaydedin.

Çoklu imzaya katılmanız için belgelenen iş akışı sizden ne ister?

1. Tüm katılımcıların kurtarma ifadelerini.
2. Herhangi bir ödeme alma adresini.
3. Uyumlu parmak izi ve BIP48 köken bilgisiyle genişletilmiş açık anahtarınızı.

> **Yanıtı göster: Uyumlu parmak izi ve BIP48 köken bilgisiyle genişletilmiş açık anahtarınızı.**
> Doğru açık bilgiler, özel anahtarları açıklamadan politikayı oluşturmaya yarar.

M09

Mirror ile politikaları istenen sırada doğrulama

Amaç

Alanları eksiksiz karşılaştırın ve sonucun tam olarak neyi doğruladığını anlayın.

Konuyu anlayın

Bağımsız doğrulama eşiği, ağı, profili, SIGHASH'i, politika kimliğini, ilk adresi, kullanıcının konumunu ve her katılımcının bilgilerini gösterir. Amaç ve tutarlılığı denetler. Cihazın politikayı kalıcı kaydettiği varsayılmaz. Belgelenen kapsam «bu inceleme» ile sınırlıdır.

Mirror 12.12'de önce Cuvex'in veya Desk'in QR kodunu okuyabilir, dilediğiniz veriyi seçebilirsiniz. 1. adımdan başlamak, tüm kodları okumak veya belli bir sıra izlemek zorunda değilsiniz. Bir metni elle incelerseniz taramayı atlamanız Mirror'ın onu doğrulanmış olarak işaretlediği anlamına gelmez.

Karşılaştırıcı metnin tamamını olduğu gibi gösterir. Boşluk, satır sonu, harf büyüklüğü ve Unicode farkları önemlidir. «Eşleşiyor», o çiftteki değerlerin aynı olduğunu bildirir. Kaynağı doğrulamaz, aynı politikaya ait olduklarını kanıtlamaz ve cüzdanı etkinleştirmez. Son onay ve ona bağlı yanıt Cuvex ile Desk akışında ilerler.

Desk'in güncel QR kodları yalnızca değeri içerir. Sıra numarası ve oturum bilgisi yoktur. Mirror adımı her zaman çıkaramaz. «Desk adımını belirt» elle girilmiş bağlam ekler ve bu şekilde gösterilmelidir. Belgelenen haritada N katılımcı için 7 + 4N alan vardır. k sıfırdan başlar: 8+4k parmak izi, 9+4k yol, 10+4k xpub ve 11+4k anahtar kimliğidir. N=2 olduğunda 15. adım ikinci anahtarın kimliğidir ve ilk önce karşılaştırılabilir.

Uygulama

1. Yapay veriler kullanın. Önce 15. adım olarak etiketlenen kimliği, ardından ağı ve eşiği karşılaştırın.
2. Tek karakterlik fark oluşturun. «Eşleşmiyor» sonucunu doğrulayın ve önceki sonucu taşımadan yeni çifte başlayın.
3. «2 / 3» metnini karşılaştırın. Neden bu metnin her zaman eşiği mi yoksa kullanıcı konumunu mu belirttiğinin anlaşılamadığını açıklayın.

Öğrendiklerinizi gösterin

Hangi alanı kontrol ettiğinizi, bağlamını nasıl belirlediğinizi ve hangi onayın kaldığını anlatın. Kısmi eşleşmeleri tüm politikanın onayı saymayın.

Sık sorulan soru

Öğrenmeye devam etmek için tüm QR’ları taramam gerekir mi? Hayır. Karşılaştırma serbesttir. İmzalayıcının zorunlu incelemeleri ve yetkilendirmeleri kendi akışında uygulanır.

Ara verme noktası

Karşılaştırıcıyı kapatın. İncelenen tasarımda çıkıldığında veya arka plana geçildiğinde değerler silinmelidir.

Mirror, 15. adımdaki iki QR kodunu karşılaştırıp «Eşleşiyor» gösteriyor. Bu neyi doğrular?

1. Belirlenen veya elle belirtilen bağlamda o iki değerin birebir aynı olduğunu.
2. Politikanın tamamının onaylandığını.
3. İki QR kodunun da kaynağının gerçek olduğunu.

> **Yanıtı göster: Belirlenen veya elle belirtilen bağlamda o iki değerin birebir aynı olduğunu.**
> Karşılaştırma kaynak doğrulamasının, genel incelemenin veya donanım yanıtının yerini tutmaz.

İmzaları koordine etme ve çok imzalı işlemi yayımlama

Amaç

Amacı ve kontrolü kaybetmeden teklifi imza eşiğine ulaştırın.

Konuyu anlayın

Çok imzalı işlem girdiler, alıcılar, tutarlar, oran, değiştirme ve işlem notlarını belirtir. Oluşturan taraf uyumlu katılımcılardan imza isteyebilir. Her imzalayıcı cihazında yetki vermeden önce ağı, politikayı, girdileri, tüm çıktıları ve ücreti kendi başına inceler.

Eşik karşılanmamışsa kısmi imza tek başına fon taşımaz. Eşik sağlanınca koordinatör akışa göre imzaları birleştirip sonlandırabilir. Diğer katılımcıların veya koordinatörün raporları sizin yerel doğrulamanız değil, koordinasyon bilgisidir. Uygulama kaynakları ayırmalıdır.

İncelenen sürüm tekrar, imza alma, alındı onayı, ret ve koordinasyon devri sunar. Devir zincirdeki anahtarları veya eşiği değiştirmez. Kaydedilen yanıt isteğe ve gerçekte kullanılan profile bağlanmalıdır. Benziyor veya katalogda ilk sırada diye başka politika seçilmez.

Alıcılar veya önemli koşullar değişirse yeni teklif incelenmeli ve gereken imzalar alınmalıdır. NFC’ye sığsın diye güvenlik verilerini silerek PSBT’yi elle «düzeltmeyin». Aygıt yazılımları desteklenen profili ve doğrulamaları gerektirir. Girdi, çıktı ve boyut sınırları vardır.

Yayımlamadan önce işlemin kararlaştırılan işlem olduğunu ve daha önce duyurulmuş sürüm bulunmadığını kontrol edin. Sonra seçilen kaynaktan onayları izleyin. Uygulamanızda ret vermek başkalarının sakladığı imzaları otomatik geri almaz veya kalan eşikle uyumlu tüm eylemleri engellemez.

Uygulama

1. Üç hayalî rolle, üç katılımcıdan ikisinin imzasını gerektiren düzeni canlandırın. Biri imzalasın, biri reddetsin, üçüncüsü açıklama istesin.
2. Deneme ödemesinin adresini değiştirin ve önceki sözlü onayın neden yeniden kullanılamayacağını açıklayın.
3. İmza kaydedildikten sonra alındı onayı hatası canlandırın. Ödemeyi çoğaltmadan veya profili değiştirmeden aynı işe dönün.

Öğrendiklerinizi gösterin

Koordinasyonu, imzayı ve sonlandırmayı kimin yaptığını ve her aşamanın kanıtını belirtin.

Sık sorulan soru

Sohbetteki iki OK iki imza eder mi? Hayır. Eşiği mesajlar değil politikaya uygun geçerli kriptografik yetkilendirmeler karşılar.

Ara verme noktası

Durumu, bekleyen imzaları ve bir sonraki sorumluyu özel içerik eklemeden kaydedin.

Üç katılımcıdan iki imza gereken işlemde bir geçerli imza ve «kabul ediyorum» diyen iki mesaj var. Eşik karşılandı mı?

1. Evet, üç katılımcı olduğu için.
2. Hayır. Bir geçerli kriptografik imza daha gerekiyor.
3. Evet, koordinatör öyle bildirirse.

> **Yanıtı göster: Hayır. Bir geçerli kriptografik imza daha gerekiyor.**
> Sohbette onay vermek ile geçerli imza üretmek farklı kanıtlardır.

M09

Çok imzalı cüzdanı kurtarma ve değiştirme

Amaç

Politikayı kurtarın ve katılımcı kaybı veya değişimi için plan yapın.

Konuyu anlayın

Kurtarma için iki tür materyal gerekir: politikayı yeniden kuracak veriler ve harcama için yeterli özel yetkiler. xpub'lı politika kopyası ifadeleri içermese de geçmişi gösterebilir. Şifreli kopya dosyayı korur ama parolasını saklamayı gerektirir. .cuvexms uzantısı tek başına şifrelemeyi kanıtlamaz. Biçim ve kullanılan dışa aktarım doğrulanmalıdır.

Desk 9.21'de kurtarma, katılımcının cihazından dışa aktarılan, parmak izi ve BIP48 yolunu içeren genişletilmiş açık anahtarını ister. Uyumlu akışta web kamerası veya Mirror ile okunabilir. Bunun yerine alım adresi vermeyin veya kurtarma ifadesini desteğe göndermeyin.

Üç katılımcıdan iki imza gerektiren düzende bir anahtar kaybolursa diğer ikisiyle harcama yapılabilir. Eski politika değişmez. Bir katılımcıyı gerçekten çıkarmak ve başka anahtarlar belirlemek için genellikle yeni bir politika oluşturulur ve gerekli yetkilendirmelerle fonlar taşınır. Takma ad değiştirmek veya Desk'ten cüzdan silmek mevcut UTXO'ları değiştirmez.

Kopyalar iki dalın yeniden kurulmasını ve geçmişin bulunmasını sağlamalıdır. Adres tekrarlamamak veya eksik tarama yüzünden cüzdanı boş sanmamak için indeksleri, verilen istekleri ve gereken bağlamı koruyun. Bekleyen işlemi geri yükleyip sürdürürken oluşturulduğunda kaydedilen profile uyun.

Uygulama

1. Belgelenen işlevle laboratuvar politikasını dışa aktarıp geri yükleyin. Ağı ve bilinen adresi doğrulayın.
2. Katılımcı kaybını canlandırın ve gerçek para taşımadan anahtar değişim planı hazırlayın.
3. Eşiğin altına düşüren kaybı canlandırın. Desteğin veya yapay zekânın eksik imzaları üretemeyeceğini kabul edin.

Öğrendiklerinizi gösterin

Deneme senaryosunu kurtarın. Bilgiyi geri yüklemekle paralar üzerindeki kontrolü değiştirmeyi ayırın.

Sık sorulan soru

Desk’te çoklu imzayı silmek cüzdanı herkes için devre dışı bırakır mı? Hayır. İş akışına göre yerel durumu siler. Başka kişiler ve kopyalar politikaya uygun yeteneği koruyabilir.

Ara verme noktası

Sınanmış kopyayı ve kişisel planı saklayın. Kursa yalnızca sonucu kaydedin.

Hâlihazırda fon içeren bir politikadan bir kişiyi çıkarmak istiyorsunuz. Adını Desk’ten silmek yeterli mi?

1. Evet.
2. Evet, sohbet de silinirse.
3. Hayır. Gerektiğinde yeni bir politika ve fonların yetkilendirilmiş aktarımı planlanmalıdır.

> **Yanıtı göster: Hayır. Gerektiğinde yeni bir politika ve fonların yetkilendirilmiş aktarımı planlanmalıdır.**
> Yerel kayıtların düzenlenmesi, mevcut UTXO’ların betiklerini değiştirmez.

M10

Aygıt yazılımını belirlenmiş adımlarla güncelleme

Amaç

Uyumlu bir güncelleme hazırlayın ve sonucunu cihaz üzerinde doğrulayın.

Konuyu anlayın

Güncelleme, güvendiğiniz yazılımı değiştirir. Modeli, donanım revizyonunu, sürümü, kaynağı ve üreticinin gerçeklik doğrulama mekanizmasını kontrol edin. İndirmenin tamamlanması veya hash'in web sayfasındakiyle aynı olması imza ve uyumluluk doğrulamasının yerini tutmaz. Mühendis için hazırlanmış imzasız aygıt yazılımı uygulamasını müşteri sürümü gibi asla kurmayın.

Belgelenen akışta Original Bluetooth ile güncellenir. BIT USB-C kullanır. Mirror desteklenen hazırlama ve taşıma işlemlerini sunar. Belirli bilgisayar, telefon ve cihaz birleşiminin fiziksel kabul testi tamamlanmadan çalışacağı vaat edilmez. Windows'ta Original güncellemesinin geçmiş sorunu özel tanılama ister. %99'da başarılı gibi göstermek çözüm değildir.

Başlamadan kurtarılabilir yedekleri, kararlı gücü ve başka işlemlerin bulunmadığını doğrulayın. Uygulamaya göre resmî dosyayı veya önceden doğrulanmış kopyayı hazırlayın. Gönderim sırasında aktarım, doğrulama, kurulum, yeniden başlatma ve sürüm kontrolünü ayırın. İlerleme çubuğu son kanıt değildir.

Bittiğinde cihazda görünen sürümü kontrol edip tarihi ve sonucu kaydedin. Desk uyumluluk kataloğu aygıt yazılımını uzaktan ölçmez; firmwareAttestation değeri false kalır. Final profilini seçmek hangi baytların gerçekte kurulduğunu kanıtlamaz. Başarısız güncellemede belgelenen kurtarmayı izleyin, aşamayı ve hatayı koruyun. Kritik aşamada düşünmeden bağlantıyı kesmeyin.

Uygulama

1. Deneme sırasında gerçek güncelleme başlatmadan hazırlık listesini kontrol edin.
2. Durumları sıralayın ve «aktarıldı» ile «kuruldu» arasındaki farkı açıklayın.
3. Model, sürüm, sistem, aşama ve son mesajı içeren hayalî bir %99 hata raporu yazın.

Öğrendiklerinizi gösterin

Uygun paketi, taşıma yöntemini ve başarıyı belirleyen son ölçütü belirtin.

Sık sorulan soru

Yalnızca bir Desk hatası kaybolsun diye güncellemeli miyim? Önce kaynağı belirleyin. Katalog uyumsuzluğu, doğrulanmış aygıt yazılımını koruyarak Desk’i düzeltmeyi gerektirebilir.

Ara verme noktası

Gerçek güncellemeyi yalnızca prosedürde açıkça güvenli olduğu belirtilen durumda duraklatın. Görüşmenin bitmesi durma gerekçesi değildir.

Desk’in açıkça belirtilen uyumluluk kataloğu tek başına neyi doğrular?

1. Kurulu aygıt yazılımını uzaktan ölçmeden, desteklenen uyumluluk bilgilerini.
2. Bağlı tüm cihazların fiziksel doğrulamasını.
3. Güvenlik açığı bulunmadığını.

> **Yanıtı göster: Kurulu aygıt yazılımını uzaktan ölçmeden, desteklenen uyumluluk bilgilerini.**
> Uyumluluk, imza, ölçüm ve fiziksel kabul farklı türden kanıtlardır.

M10

Kayıp, arıza ve acil durumda kurtarma

Amaç

Olaya uygun kurtarmayı seçin ve yararlı kanıtları koruyun.

Konuyu anlayın

Önce neyin kaybolduğunu veya açığa çıktığını sınıflandırın: bilgisayar, cihaz, kart, dosya, parola, kurtarma ifadesi, ek parola veya politika. «Giremiyorum» mutlaka «çalındı» demek değildir. Ele geçirilme şüphesi varsa şüpheli cihaza gizli bilgi girmeyi bırakın.

Cihaz kaybı uyumlu taşıyıcılar ve kurtarma bilgileriyle çözülebilir. Bilgisayar kaybında Desk deposunu geri yüklemek ve izleme düzenini yeniden kurmak gerekebilir. Tüm kilit açma araçları kaybolmuşsa veya kalan anahtarlar eşiğin altındaysa teknik çözüm bulunmayabilir. Hiçbir yapay zekâ var olmayan anahtarları kurtarmayı garanti edemez.

Desk desteklenen biçimler için yerel kurtarma ve gereken kurtarma materyalinin dışa aktarılmasını içerir. Bilgisayarda şifre çözmek sırrı işletim sistemine veya kötü amaçlı yazılıma açabilir. Bu olağanüstü bir karardır. Hazırlanmış ortam, uyumlu materyal ve ifşa olasılığına karşı yeni anahtarlara geçiş planı kullanın. Bunu Cuvex'in normal yalıtımıyla eşdeğer saymayın.

Kurtarma ifadesi sızdıysa Desk parolasını değiştirmek ifadeyi geçersiz kılmaz. Yeni bir cüzdana yetkili aktarımı değerlendirin ve güvenilir cihazdan koruyun. Saldırgana yardımcı olacak ayrıntıları yayımlamayın. Başka bir kurtarma ifadesi veya şüpheli peşin ücret karşılığında kurtarma vaat eden hizmetlere ödeme yapmayın.

Uygulama

1. Dört hayalî durumu çözün: kayıp bilgisayar, geçerli yedeği olan bozuk kart, unutulmuş parola ve açığa çıkmış kurtarma ifadesi.
2. Her biri için gereken materyali, müdahalenin riskini ve kurtarma ölçütünü belirleyin.
3. Prosedürü yalnızca eğitim verileriyle deneyin. Gerçek acil durum dosyalarını eğitmene yüklemeyin.

Öğrendiklerinizi gösterin

İmkânsız çözümler vaat etmeden geri yükleme, izlemeyi yeniden yapılandırma, kontrolü taşıma veya uzmana iletme arasında seçim yapın.

Sık sorulan soru

Parolayı değiştirmek birinin daha önce gördüğü tüm sırları yeniden şifreler mi? Hayır. Açık kopya veya bilinen kurtarma ifadesi biliniyor olmaktan çıkmaz.

Ara verme noktası

Olay kategorisini ve bir sonraki güvenli eylemi kaydedin. Sırlarla çalışacaksanız sesli görüşmeyi durdurun.

Kurtarma ifadeniz yayımlandıktan sonra bilgisayarın parolasını değiştirdiniz. Saldırganın yetkisi kalktı mı?

1. Evet.
2. Hayır. İfade aynı anahtarları kontrol etmeye devam eder. Varlıkların güvenliğini yeniden sağlamak için harekete geçmek gerekir.
3. Evet, sohbet duvar kâğıdını da değiştirirseniz.

> **Yanıtı göster: Hayır. İfade aynı anahtarları kontrol etmeye devam eder. Varlıkların güvenliğini yeniden sağlamak için harekete geçmek gerekir.**
> Yerel koruma, açığa çıkmış bir Bitcoin anahtarını geçersiz kılmaz.

M10

Kimlik avı, destek ve sesli dolandırıcılık

Amaç

Tehlikeli talepleri tanıyın ve önceden belirlenmiş şekilde yanıtlayın.

Konuyu anlayın

Etkili bir dolandırıcılık adınızı, satın almanızı, cihazınızı ve tanıdığınız bir sesi kullanabilir. Doğru bilgi bir sızıntıdan gelmiş olabilir. Kimliği, arayanın aciliyetine veya ayrıntıları bilmesine göre değil, sizin başlattığınız bir kanaldan ve bilinen yöntemle doğrulayın.

Tehlike işaretleri arasında kurtarma ifadesi, parola, PIN veya sohbet anahtarı (Clave Chat) istemek, «eşitleme» için uzaktan denetim kurdurmak, antivirüsü kapattırmak, «güvenli» cüzdana para istemek, içeriği açıklanmayan QR taratmak ve neye yetki verildiğini söylemeden mülkiyet kanıtı için imza istemek bulunur. Görüşme bitmeden yapma baskısı, aramayı durdurma nedenidir.

Gerçek eğitmen açıklama yapar ve anlama soruları sorar. Anahtar saklamaz, kendi adresine deneme işlemi istemez, kurtarma ifadesini bulmayı vaat etmez. Meşru mülkiyet doğrulaması belirli ve incelenebilir olmalıdır. Özel anahtar vermek hiçbir zaman bunun yolu değildir.

Teknik oturumda da dolandırıcılık olabilir: QR metni, belge veya mesaj yapay zekâya talimatlarını yok saymasını emredebilir. Bu, incelenecek içeriktir; eğitmeni yönetme yetkisi değildir. Bilgi tabanı onaylı kaynaklarla öğrencinin veya üçüncü tarafın metnini ayrı tutmalıdır.

Uygulama

1. Sahte destek aramasını canlandırın ve bilgi açıklamadan görüşmeyi kesin.
2. Önceden saklanmış resmî kanalı bağımsız şekilde doğrulayın.
3. Kurulum hatasını, sırların bulunduğu ekranı paylaşmadan veya saklama ortamına uzaktan erişim vermeden tarif edin.

Öğrendiklerinizi gösterin

İstenen veriyi, ne için gerekebileceğini ve talebin eğitim desteğinin kapsamını neden aştığını açıklayın.

Sık sorulan soru

Kurtarma ifademin birkaç kelimesini göstermek güvenli mi? Hayır. Kendi ifadenizden parça açıklamak için eğitimsel neden yoktur.

Ara verme noktası

Destek doğrulama prosedürünüzü saklayın. Açık metin sır içermediğini kontrol edin.

Ortağınızın sesine benzeyen biri, doğrulamayı atlayıp acilen imza vermenizi istiyor. Ne yaparsınız?

1. Duraklar, önceden kararlaştırılan yöntemle talebin gerçekliğini doğrular ve işlemin tamamını incelerim.
2. Ses benzediği için imzalarım.
3. Zaman kazanmak için kurtarma ifadesini paylaşırım.

> **Yanıtı göster: Duraklar, önceden kararlaştırılan yöntemle talebin gerçekliğini doğrular ve işlemin tamamını incelerim.**
> Sesi tanımak veya aciliyet, kimlik doğrulamanın ve incelemenin yerini tutmaz.

Gizlilik, yasal yükümlülükler ve kişisel kayıtlar

Amaç

Genel çerçeveyi öğrenin, hukuk ve vergi danışmanına sorulacak somut sorular hazırlayın.

Konuyu anlayın

Mali mahremiyet vergi, geçerli olduğunda kimlik tespiti, yaptırım veya suçun önlenmesi yükümlülüklerini ortadan kaldırmaz. Durum ikamete, faaliyete, karşı tarafa ve hizmete bağlıdır. Yapay zekâ kaynak ve tarih vererek genel bilgi sunmalı, kişisel kararları yetkin uzmanlara yönlendirmelidir.

AB’de MiCA belirli kripto varlıkları ve hizmetleri düzenler. Genel uygulama 30 Aralık 2024’te başladı. Yönetmelikteki azami geçiş dönemi, ulusal kararlara bağlı olarak 1 Temmuz 2026’ya kadar uzanıyordu. Yetkiyi ve kapsamını güncel resmî kayıtlardan kontrol edin. Eski bir kayıt atfı yeterli değildir. Yetkilendirme fiyatı, ödeme gücünü veya tam tazminatı garanti etmez.

2023/1113 sayılı Yönetmelik, yükümlü sağlayıcıların katıldığı transferlere eşlik edecek bilgileri belirler. Kişinin kendi kontrolünde tuttuğu adreslerle 1.000 avroyu aşan transferlerde mülkiyet veya kontrolü değerlendirecek önlemler öngörür. Bu eşik altında genel kimlik tespiti muafiyeti oluşmaz. Sağlayıcısız kişiler arası transferler bu yönetmeliğin kapsamı dışında bırakılmıştır; başka yükümlülükler sürebilir.

Durumunuza göre alım, satış, ücret ve kaynaklara ilişkin yeterli belgeyi gereksiz erişimden koruyarak saklayın. Özel kayıt tutmak için tüm geçmişi yayımlamanız gerekmez. Kursta denetimlerden kaçmak için işlem bölme, sahte bilgi verme veya gelir gizleme öğretilmez.

Ses kaydı veya dökümüyle birlikte kimliği belirlenebilir ilerleme verisi varsa hizmet; amacı, hukuki dayanağı, saklama süresini, erişimi, veri işleyenleri ve geçerli hakları tanımlamalıdır. Ticari gizlilik yapılandırması satış öncesi doğrulanır, görüşme sırasında doğaçlama belirlenmez.

Uygulama

1. Danışman için ikamet, faaliyet ve işlemleri belirten, anahtar içermeyen hayalî bir örnek yazın.
2. Sağlayıcının yetkisinin ve bilginin tarihinin nereden doğrulanacağını kontrol edin.
3. Özel işlem günlüğü ve öğrenci verilerini en azda tutan bir politika tasarlayın.

Öğrendiklerinizi gösterin

Hukuki kural, borsa politikası ve Bitcoin’in teknik yeteneğini ayırt edin.

Sık sorulan soru

AB’de tüm öz saklama yasak mı? Anılan kurallardan böyle bir sonuç çıkmaz. Kesin manşetler yerine ilgili hükmü ve kapsamını doğrulayın.

Ara verme noktası

Danışmanınız için açık soruları kaydedin. Kişisel belgeleri eğitmene vermeyin.

Bazı adres kontrol önlemleri için anılan 1.000 avro eşiğinin altında tüm yükümlülükler kalkar mı?

1. Evet.
2. Yalnızca işlemi parçalara bölerseniz.
3. Hayır. Bu, kimlik tespiti veya diğer yükümlülüklerden genel muafiyet değildir.

> **Yanıtı göster: Hayır. Bu, kimlik tespiti veya diğer yükümlülüklerden genel muafiyet değildir.**
> Kural, ilgili önlem ve uygulama kapsamı içinde yorumlanmalıdır. Bir eşik her durumu kapsayan muafiyet sayılmaz.

M10

Miras, süreklilik ve yıllık tatbikat

Amaç

Her şeyi erken açığa çıkarmadan yetkili kişilerin harekete geçebilmesini sağlayan plan oluşturun.

Konuyu anlayın

Miras; hukuki yetki, materyallerin bulunması ve teknik yeteneği bir araya getirir. Bir kişi miras hakkına sahip olup cüzdanı kurmayı bilmeyebilir. Başka biri anahtarı tutup kullanmaya yetkili olmayabilir. Uygun danışmanlıkla her iki yönü de çözün.

Açık talimatları sırlara erişimden ayırın. Envanter, bütün anahtar ve parolaları geniş erişimli bir belgede toplamadan neyin mevcut olduğunu, kime ulaşılacağını ve hangi kontrollerin yapılacağını açıklamalıdır. Kurtarma ifadelerini kontrolünüz dışında dolaşabilecek vasiyet veya dosyalarda yayımlamayın.

Çoklu imzada politikayı ve yedekleri kimin tutacağını, kayıptan sonra hangi eşiğe ulaşılabileceğini ve kilit kişi ölürse ne olacağını tasarlayın. Tek saklama sorumlusunun yeterli bileşeni toplaması kötüye kullanım için tek nokta oluşturabilir. Aşırı karmaşık dağıtım varlıkların kurtarılamamasına yol açabilir.

Kriptogram parolaları ile varsa ek parolanın kurtarılmasını, türetme verilerini, cihaz uyumluluğunu ve üretici faaliyeti durdurursa uygulanacak yöntemi ekleyin. Özel dosya biçiminin veya biyometrik izin hazırlık olmadan kullanılabileceğini varsaymayın. Birlikte çalışabilirliği deneme verileri ve belgelenmiş biçimlerle sınayın.

Aile, adres, politika, yazılım veya katılımcılar değiştiğinde planı gözden geçirin ve düzenli tatbikat yapın. Güvenilen kişinin varlıklar açıklanmadan ve gereksiz para taşınmadan talimatları anlayabildiğini sınayın.

Uygulama

1. Sorumluları, bileşenleri, izin verilen erişimi ve yedek sorumluları içeren kişisel şablonu doldurun.
2. Başka birine sözlü açıklama eklemeden laboratuvar talimatlarını verin. Nerede takıldığını gözlemleyin.
3. Belirsizlikleri düzeltin ve gözden geçirme tarihi kaydedin. Kurs kendiliğinden hatırlatıcı oluşturmaz.

Öğrendiklerinizi gösterin

Siz ulaşılamazsanız ne olacağını ve her aşamada her rolün hangi bilgiye ihtiyaç duyduğunu açıklayın.

Sık sorulan soru

Üç katılımcıdan iki imza düzeni miras planının yerini tutar mı? Hayır. Bu bir teknik araçtır. Mirasçıların yine bağlama, materyallere, koordinasyona ve hukuki yetkiye ihtiyacı vardır.

Ara verme noktası

Planı kurs dışında saklayın. Yalnızca «tatbikat gözden geçirildi» olarak işaretleyin.

Bir miras planını değerlendirmek için hangi ölçüt yararlıdır?

1. Yetkili kişinin doğaçlama yapmadan ve gizli bilgilere vaktinden önce erişmeden belgelenmiş tatbikatı uygulayabilmesi.
2. Çok sayıda sayfasının olması.
3. Yalnızca bir parolanın hatırlanmasına dayanması.

> **Yanıtı göster: Yetkili kişinin doğaçlama yapmadan ve gizli bilgilere vaktinden önce erişmeden belgelenmiş tatbikatı uygulayabilmesi.**
> Kurtarılabilirlik ve erişim kontrolü uygulamada sınanmalıdır.

M11

Fiyat, tasarruf ve temel analiz

Amaç

Yatırım görüşlerini doğrulanabilir teknik özelliklerle karıştırmadan değerlendirin.

Konuyu anlayın

Fiyat belirli piyasalardaki alışverişlerden doğar ve platformlar arasında değişebilir. Likidite, fiyatlama para birimi, derinlik, banka sağlayıcılarının çalışma saatleri ve talep gerçekte hangi fiyattan işlem yapabileceğinizi etkiler. Ekrandaki kotasyon sizin hacminiz için garantili teklif değildir.

Temel analiz benimsenme, talep, rekabet, ekonomik güvenlik, düzenlemeler ve arz gibi etkenleri inceler. Bilinen ihraç takvimi tek başına gelecekteki fiyatı belirlemez. Parasal fayda veya «içsel değer» değerlendirmeleri varsayımlara dayanır. Yapay zekânın evrensel kesinlik olarak sunabileceği tek nesnel rakam yoktur.

Düzenli alımlar giriş zamanını dağıtır ama kârı garanti etmez veya uzun süreli kayıpları önlemez. Uzun vadeli birikim de yükümlülükler için likidite, oynaklığa dayanabilme ve saklama planı gerektirir. Kurs varlığınızın belirli oranını önermez veya sizin adınıza karar vermez.

Üç soruyu ayırın: Varlığı anlıyor muyum? Saklayıp kurtarabiliyor muyum? Ekonomik riskini karşılayabilir miyim? Anahtarlara hâkim olmak üçüncü soruyu kendiliğinden yanıtlamaz. Eğitim bir fiyat tahminini veya geçmiş grafiği kişisel tavsiyeye dönüştürmez.

Uygulama

1. Hayalî yatırım tezi, varsayımları ve tezi geçersiz kılacak gerçekleri yazın.
2. Gerçek varlıklarınızı girmeden %50 düşüşü ve eşzamanlı nakit ihtiyacını canlandırın.
3. Görüşteki hangi verilerin doğrulanabilir, hangilerinin beklenti olduğunu belirleyin.

Öğrendiklerinizi gösterin

Getiri vaat etmeden ve inancı kanıtla karıştırmadan yatırımı tartışın.

Sık sorulan soru

Kıtlık fiyat artışını sağlar mı? Hayır. Talep ve diğer koşullar piyasa fiyatında belirleyici olmaya devam eder.

Ara verme noktası

Otomatik alım emri değil laboratuvar varsayımlarını saklayın.

Düzenli aralıklarla alım yapmak neyi garanti eder?

1. Uzun vadede kârı.
2. Herhangi bir getiriyi garanti etmez. Alım zamanlarını seçilen kurala göre dağıtır.
3. Anahtar kaybına karşı korumayı.

> **Yanıtı göster: Herhangi bir getiriyi garanti etmez. Alım zamanlarını seçilen kurala göre dağıtır.**
> Alımları zamana yaymak ekonomik veya operasyonel riski ortadan kaldırmaz.

Bitcoin’i nereden alacağınızı seçme

Amaç

Sağlayıcıyı yetki, maliyet, çekim, mahremiyet ve saklama riski açısından değerlendirin.

Konuyu anlayın

Sağlayıcıları doğrulanabilir ölçütlerle karşılaştırın: tüzel kişilik ve yargı alanı, yetkilendirilen hizmetler, çekim ağı, ücretler, fiyat farkı, sınırlar, destek, kimlik doğrulama ve veri işleme. Ticari ad veya sponsorluk belirli hizmete yetki verildiğini kanıtlamaz.

Toplam maliyet yatırma, dönüşüm, alış-satış farkı, işlem ücreti, çekim ve banka masrafını içerebilir. «Komisyonsuz» işlem daha geniş fiyat farkı taşıyabilir. Net tutarları ve referans para birimini kontrol edin. Amacınız öz saklamaysa çekim maliyetini bütçeye ekleyin.

Saklama hizmetinde bakiye tuttuğunuz sürece sağlayıcıya bağımlısınız. Rezerv kanıtı tek başına tüm yükümlülükleri, fonların sahipliğini veya gelecekteki ödeme gücünü kanıtlamaz. Yeni yönteme güvenmeden önce kısıtları kontrol edin ve karşılayabileceğiniz küçük bir çekim deneyin.

Ticari kimlik tespiti kimliğinizi bir çekime bağlayabilir. Sonradan bu bilgiyi korumak sağlayıcının bildiğini silmez. Yanlış bilgi vermeyin veya kursu yükümlülüklerden kaçmak için kullanmayın. Eğitim kodu satın almak da cüzdanınızdan ayrı ticari kayıt oluşturur.

Uygulama

1. İki hayalî sağlayıcı için toplam maliyet, ağ, asgari çekim, yetki ve istenen veriler tablosunu doldurun.
2. Belirtilen tüm masrafları hesaba katarak eğitim işleminin net tutarını hesaplayın.
3. Önceden doğrulanmış adrese deneme çekimi planlayın. Bunu bu kurs sitesinden gerçekleştirmeyin.

Öğrendiklerinizi gösterin

Kendi durumunuz için seçimi gerekçelendirin ve hangi bilginin eski veya doğrulanmamış olduğunu belirtin.

Sık sorulan soru

Kurs herkes için tek en iyi borsayı önerir mi? Hayır. İzinler, ücretler, hizmet verilen ülkeler ve koşullar değişir. Karşılaştırma için tarih ve kullanım durumu gerekir.

Ara verme noktası

Tabloyu erişim bilgileri veya kimlik belgeleri olmadan saklayın.

Yalnızca alım satım komisyonuna bakmak yerine hangi karşılaştırmayı yapmak daha yararlıdır?

1. BTC’yi seçilen ağda ve istenen adreste alana kadarki toplam maliyeti.
2. Sağlayıcının takipçi sayısını.
3. Uygulamasının rengini.

> **Yanıtı göster: BTC’yi seçilen ağda ve istenen adreste alana kadarki toplam maliyeti.**
> Nihai tutara ilan edilen komisyondan ayrı maliyet kalemleri girebilir.

M11

Hesaplar, emirler ve emir gerçekleştirme maliyetleri

Amaç

Kursu işlem terminaline dönüştürmeden temel emirleri anlayın ve hesabı koruyun.

Konuyu anlayın

Piyasa emri mevcut likiditeyle gerçekleşmeye öncelik verir ve fiyat kayması riski taşır. Limit emri alışta azami, satışta asgari fiyatı belirler ama hiç gerçekleşmeyebilir veya kısmi gerçekleşebilir. Stop emri sağlayıcının kurallarına göre başka bir eylemi tetikler. Nihai fiyatı tek başına garanti etmez.

Emir defteri mevcut teklifleri gösterir, tüm hacimlerin orada kalacağı taahhüdünü vermez. Düşüşte veya düşük likiditede sonuç son kotasyondan farklı olabilir. Stop-market ile stop-limit riskleri ayrıdır: ilki daha kötü fiyat, ikincisi emrin hiç gerçekleşmemesi riskini taşır.

Erişimi benzersiz parolayla, desteklendiğinde kimlik avına dayanıklı kimlik doğrulamayla, oturum incelemesiyle ve uygun çekim kontrolleriyle koruyun. İkinci faktörün kurtarma bilgilerini ayrı tutun. Otomasyon API anahtarı, yalnızca veri okumak için gerekenden çok daha riskli izinlere sahip olabilir. Eğitmene veya kurs sitesine girmeyin.

Çekmeden önce varlığı, Bitcoin ağını, cüzdan adresinizi ve net tutarları doğrulayın. Platform farklı ürünlere aynı simgeyi verebilir. Sonunda durumunuza göre alım, emir gerçekleşmesi, ücret ve çekim belgelerini saklayın. Kendi cüzdanınıza çekimi yeni alımla karıştırmayın.

Uygulama

1. Kurgusal bir emir defterinde 100 fiyatından 1 birim ve 102 fiyatından bir birim daha olduğunu varsayın. Piyasa emriyle iki birim almanın neden 100 ortalama fiyatı garanti etmediğini açıklayın.
2. Bir limit emri tasarlayın ve gerçekleşmeyeceği durumu açıklayın.
3. Hayalî API’nin izinlerini denetleyin. Yalnızca sorgu gerekiyorsa para çekme yetkisini kaldırın.

Öğrendiklerinizi gösterin

Her emir için önceliği, fiyatı ve emrin gerçekleşmeme riskini açıklayabilmelisiniz.

Sık sorulan soru

Zarar durdurma emri kaybı her zaman tam belirtilen tutarda sınırlar mı? Hayır. Fiyat boşlukları, likidite, kayma ve sağlayıcı kuralları buna engel olabilir.

Ara verme noktası

Alıştırma sonucunu gerçek emirler veya API anahtarları olmadan saklayın.

100 fiyatından limitli alım emrinde hangi risk devam eder?

1. Hiç gerçekleşmemesi veya yalnızca kısmen gerçekleşmesi.
2. Herhangi bir fiyattan gerçekleşmesinin zorunlu olması.
3. Otomatik olarak yedek oluşturması.

> **Yanıtı göster: Hiç gerçekleşmemesi veya yalnızca kısmen gerçekleşmesi.**
> Fiyatı sınırlamanın karşılığında emrin gerçekleşmeme olasılığı vardır.

Mumlar, göstergeler ve teknik analizde yanlılıklar

Amaç

Grafikleri geçmiş veri olarak okuyun, kalıpları tahminle karıştırmadan strateji değerlendirin.

Konuyu anlayın

Mum, dönemin açılışını, en yüksek, en düşük ve kapanış fiyatını özetler. Hacim kaynağa bağlıdır. Platform, para birimi, saat dilimi veya dönem değişince görüntü değişebilir. Mum aralıktaki tüm hareketlerin zaman sırasını göstermez.

Hareketli ortalama geçmiş fiyatları yumuşatır. Momentum göstergesi gözlenen verileri formülle dönüştürür. İkisi de geleceği bilmez. Aynı seriden türetilen iki gösterge, adları ve renkleri farklı olsa bile yüksek ölçüde ilişkili bilgi verebilir.

Kuralı değerlendirirken sonucu görmeden giriş, çıkış, geçersizlik, maliyet, boyut ve verileri tanımlayın. Yalnızca kazanan örnekleri seçmeyin, sonuçlara uyana kadar parametre ayarlamayın veya geçmiş karar için gelecek verisi kullanmayın. Eğitim verisiyle zamana göre yapılan doğrulamayı ayırın.

Geçmiş veri testi alış-satış farkını, ücretleri, fiyat kaymasını, veriye erişimi ve fiilen mümkün gerçekleşmeyi içermelidir. Brüt getiri, başarı oranı, azami kayıp ve kayıp dağılımı farklı soruları yanıtlar. Yanlış tahminlerde kayıp büyükse çok isabetli sistem de para kaybedebilir. Alım veya satım sinyali kesinlik gibi öğretilmez.

Uygulama

1. Hayalî bir mumu okuyun ve hangi zaman sıralaması bilgisinin eksik olduğunu açıklayın.
2. On yapay sonucu değerlendirmeden önce maliyetleri ve başarısızlık ölçütünü de içeren bir kural yazın.
3. 1’er birimlik 9 kazancı 15 birimlik bir kayıpla karşılaştırın. %90 isabete rağmen brüt sonuç −6’dır.

Öğrendiklerinizi gösterin

İşlem yapmanıza gerek kalmadan ilgi çekici bir sonucu örnek seçimi, maliyet veya risk yönünden eleştirin.

Sık sorulan soru

Çok gösterge birleştirmek daha iyi sinyal garanti eder mi? Hayır. Bağımsız bilgi eklemeden aşırı uyum ve karmaşıklığı artırabilir.

Ara verme noktası

Piyasa emri yerine laboratuvar kuralını ve sonuçlarını saklayın.

Dokuz işlem 1’er birim kazandırıyor, bir işlem 15 birim kaybettiriyor. Maliyetlerden önce sonuç nedir?

1. +%90.
2. +6.
3. −6.

> **Yanıtı göster: −6.**
> Kazanılan dokuz birimden kaybedilen on beş birim çıkarıldığında altı birim zarar kalır.

M11

Marj, vadeli işlemler ve otomasyon

Amaç

Karmaşık ürünleri düşünmeden önce pozisyon büyüklüğü, tasfiye ve otomasyon hatalarını tanıyın.

Konuyu anlayın

Kaldıraç, yatırılan sermayeye göre pozisyonu büyütür. Basit örnekte 100 teminatla 1.000 pozisyon, dayanak varlığın %5 olumsuz hareketinde masraflardan önce 50 kayıp demektir. Bu, ilk teminatın yarısıdır. Gerçek sürdürme teminatı, tasfiye, teminat varlığı ve ücret kuralları sonucu kötüleştirip beklenenden erken devreye girebilir.

Vadeli ve süresiz sözleşmeler vade, fiyat farkı üzerinden uzlaşma, fonlama oranları ve son işlemden farklı referans fiyatları içerebilir. Bunlar Cuvex'e yerel bitcoin çekmekle eşdeğer değildir. Bir kurtarma ifadesini korumak pozisyonu tasfiye veya karşı taraf temerrüdünden korumaz.

Bot kuralları, hatalarıyla birlikte otomatikleştirir. Pozisyon sınırı, asgari izinler, yinelenen emrin ikinci etki yaratmaması, kayıtları uzlaştırma, kayıp kontrolü, acil durdurma ve gözetim gerekir. Zaman aşımından sonra önceki sonucu bilmeden isteği tekrarlamak pozisyonu ikiye katlayabilir.

Yapay zekâ hayalî örnekte kavramları açıklayabilir ve tutarsızlık bulabilir. API anahtarlarını almamalı, işlem başlatmamalı veya kârlı strateji vaat etmemelidir. Kursun ana amacı açısından riskleri anlamak, anlamadığınız ürünleri kullanmamaya karar verebilmenizi sağlar.

Uygulama

1. Tasfiye seviyesinin kesin %10 olduğunu varsaymadan pozisyon ve teminat örneğini çözün.
2. Emri gerçekleştiren ama yanıtı kaybolan API'yi canlandırın. Tekrardan önce kayıtları uzlaştırmanın nedenini açıklayın.
3. Aracı kuruma bağlanmadan, yeni emirleri engelleyen ve açık emirleri kontrol eden durdurma düğmesi tasarlayın.

Öğrendiklerinizi gösterin

Stop emrine, bota ve dışarıdaki fonların öz saklamasına rağmen devam eden birer risk açıklayın.

Sık sorulan soru

Otomasyon duyguları ortadan kaldırıp sonuçları garanti eder mi? Hayır. Dürtüsel bir müdahaleyi azaltabilir ama tasarım veya uygulama hatalarını büyütebilir.

Ara verme noktası

Karmaşık ürünleri etkinleştirmeden bu ek konuyu anladığınızı işaretleyin.

1.000 tutarında pozisyon ve 100 teminatla pozisyon değerinin %5’i kadar bir kayıp, maliyetlerden önce neye eşittir?

1. 5 birim zarara.
2. 50 birim zarara, yani teminatın %50’sine.
3. Bot kullanılırsa sıfır zarara.

> **Yanıtı göster: 50 birim zarara, yani teminatın %50’sine.**
> Kaldıraç ve maliyetler, teminata göre sonucun varlığın fiyat hareketinden farklı olmasına neden olur.

M12

Lightning ve diğer katmanlar

Amaç

Kanal ödemelerini anlayın ve incelenen Cuvex akışının sunmadığı işlevleri tanıyın.

Konuyu anlayın

Lightning her ayrı alışverişi temel zincire kaydetmeden ödeme yapmak için kanallar ve güncelleme mekanizmaları kullanır. Kanal açma, kapama ve bazı kurtarma durumları zincir üstü işlem gerektirebilir. Kullanılabilirlik, gelen ve giden likidite ile izleme, cüzdan tasarımına ve kullanılan hizmetlere bağlıdır.

Ödeme isteği tutar, açıklama ve son kullanma zamanı içerebilir. Bağlama göre satoshi veya milisatoshi kullanılabilir. Milisatoshi, temel zincirde bir satoshiden küçük çıktı bulunduğunu göstermez. İsteği ödemek için uyumluluk ve kullanılabilir rota gerekir. QR tek başına her uygulamayla ödeme garantisi değildir.

Saklamalı ve saklamasız hizmetler çok farklı modeller kullanır. Olağan hız risk olmadığı anlamına gelmez. Lightning'i tam anonimlik olarak da sunmayın. Gözlemciler, rotalar, karşı taraflar ve önemli üstveriler vardır.

Cuvex sohbeti WOW hesabından zincir üstünde ödenen sat taleplerini koordine edebilir. Bu baskıda Desk'e Lightning düğümü, kanal yönetimi veya Lightning ödeme isteği imzalama yeteneği atfedilmez. İstek birden fazla yöntem içeriyorsa hangisini anladığınızı ve uygulamanızın hangisini gerçekleştireceğini kontrol edin.

Uygulama

1. Eğitim örneklerinden zincir üstü adresi, bitcoin: URI'sini ve Lightning ödeme isteğini sınıflandırın.
2. Zincirde ve kanalda ödemeyi onay, likidite, saklama ve kurtarma bakımından karşılaştırın.
3. Süresi dolmuş ödeme isteğinin neden adres gibi yorumlanmayıp alıcıyla yeniden incelenmesi gerektiğini açıklayın.

Öğrendiklerinizi gösterin

Uyumsuz bir yöntemi anahtar açıklamadan ve Cuvex'e yanlış arıza atfetmeden reddedin.

Sık sorulan soru

Sats ile yapılan tüm ödemeler Lightning midir? Hayır. Satoshi değeri ölçer. Yöntem kullanılan protokole bağlıdır.

Ara verme noktası

Gerçek ödeme isteği eklemeden alıştırmanın yöntemini kaydedin.

Bir isteğin Lightning üzerinden ödeneceğini belirlemek için hangi bilgi yeterlidir?

1. «sats» kelimesini içermesi.
2. Sohbet üzerinden gelmesi.
3. Yalnızca birim veya mesaj kanalı değil, uyumlu biçim ve ödeme yöntemi.

> **Yanıtı göster: Yalnızca birim veya mesaj kanalı değil, uyumlu biçim ve ödeme yöntemi.**
> Hesap birimi ve ödeme ağı farklı özelliklerdir.

Taproot, MuSig2 ve kuantum sonrası gelecek

Amaç

Standartları, önerileri ve uygulanmış yetenekleri ayırt edin.

Konuyu anlayın

Taproot anahtar ve betik yollarıyla harcama koşulları sağlar. Schnorr imzaları ve birleştirme belirli yapıları iyileştirebilir. Mahremiyet sonucu yapılandırmaya ve harcama yöntemine bağlıdır. Adresin bc1p olması başka katılımcı olmadığını kanıtlamaz ve gizli koşulların tamamını göstermez.

MuSig2, imzalayıcıların etkileşimle anahtarları birleştirmesine ve uyumlu bir Schnorr imzası üretmesine olanak verir. Temel standart N katılımcıdan N'ini gerektirir. İsteğe göre M/N eşiği için başka yapı veya ek protokol gerekir. Nonce ve oturum yönetimi kritiktir. Gayriresmî mesaj alışverişiyle uygulanmaz.

PSBT v2, v0'a göre bilgiyi yeniden düzenler. Sürüm 2 işlem içeren her dosyanın otomatik güncellemesi değildir. Bu baskının Final aygıt yazılımları çoklu imza profili için PSBT v0, P2WSH/sortedmulti ve SIGHASH_ALL kullanır. Gelecek yetenekler için ayrı teknik sözleşme ve doğrulama gerekir.

NIST, 2024'te tamamlanmış ilk kuantum sonrası standartlarını yayımladı. Bu Bitcoin imzalarını tek başına değiştirmez. Aygıt yazılımını doğrulamak için kuantum sonrası algoritma kullanmak o katmanı korurdu. Bir UTXO'nun ECDSA veya Schnorr imzasını kendiliğinden kuantum sonrası imzaya dönüştürmezdi. Eğitmenin kesinlikle vaat edebileceği bir gelecek saldırı tarihi de yoktur.

Uygulama

1. Beş iddiayı standart, doğrulanmış uygulama, öneri veya reklam olarak sınıflandırın.
2. «Taproot alıcısını kabul eder» ifadesinin neden «Taproot girdisini imzalar» anlamına gelmediğini açıklayın.
3. Ayrı katmanlar olarak aygıt yazılımı imzasını, sır şifrelemesini, sohbeti ve Bitcoin harcama imzasını çizin.

Öğrendiklerinizi gösterin

Bir katmana özel kanıt isteyin. Bir protokolün güvencesini diğerine taşımayın.

Sık sorulan soru

Kuantum bilişimle ilgili bir manşet nedeniyle fonlarımı taşımalı mıyım? Gerçek karar güncel teknik kanıt, doğrulanabilir destek, risk değerlendirmesi ve güvenli geçiş planı gerektirir. Kurs manşete dayanarak fon hareketi talimatı vermez.

Ara verme noktası

Otomatik harcama planı oluşturmadan teknik soruları kaydedin.

Önyükleyicide kuantum sonrası bir imza uygulansa ve doğrulansa, mevcut bir UTXO’nun imzalama koşulları değişir mi?

1. Hayır. Bunlar farklı katmanlardır.
2. Evet, tüm ağı başka bir algoritmaya geçirir.
3. Yedekleme ihtiyacını ortadan kaldırır.

> **Yanıtı göster: Hayır. Bunlar farklı katmanlardır.**
> Bir güncellemenin gerçekliğini doğrulamak, Bitcoin’in harcama koşullarını yeniden yazmaz.

Birlikte çalışabilirlik ve üreticiden bağımsızlaşma

Amaç

Yazılım, cihaz veya sağlayıcı değişirse sürekliliği planlayın.

Konuyu anlayın

Birlikte çalışabilirlik kısaltma listesiyle kanıtlanmaz. Ağ, betik, türetme, anahtarlar, politika, işlem biçimi ve imzaların anlamı korunmalıdır. İki uygulama BIP174'ü anlayıp yine de aynı alanları, boyutları veya girdi türlerini desteklemeyebilir.

Tek bir arayüze bağımlılıktan çıkmak için belgelenmiş kurtarma verilerini saklayın ve eğitim cüzdanlarıyla prova yapın. Standart anımsatıcı ifade anahtar türetmeye olanak verebilir ama çoklu imzayı kurtarmak için tam politika gerekir. BIP329 etiketleri mahremiyet bağlamı ekler. Sohbet geçmişinin kapsamı ayrıdır.

Uyumluluk testi uğruna gerçek kurtarma ifadesini açığa çıkarmayın. Önce tanımlayıcıların açık verilerinin dışa aktarılmasını ve salt izleme kurtarmasını sınayın. Acil durumda anahtarların yeniden kurulması gerekiyorsa buna uygun ortam kullanın ve sonrasında geçişi değerlendirin. Uyumsuz bir cüzdanın sıfır göstermesi fon kaybını tek başına kanıtlamaz.

Belgelerin, kurs sürümünün ve gereken araçların doğrulanabilir kopyasını tutun. Uygulama imzaları, süresi dolmuş sertifikalar ve sistem değişiklikleri kurulumu etkileyebilir. Açık kaynak kodunun varlığı, bağımlılıklar ve bilgi korunmadan herkesin yıllar sonra derleyebileceğini garanti etmez.

Uygulama

1. Boş hesapla çıkış denemesi tasarlayın: iki uyumlu uygulamada aynı ağı, politikayı ve kontrol adresini kullanın.
2. Hangi parçaların standart olduğunu, hangilerinin dönüştürücü veya Cuvex biçim belgelerini gerektirdiğini listeleyin.
3. Hangi sonucun uyumluluğu kanıtlayacağını ve gerçek donanım veya imza açısından neyin bekleyeceğini belirleyin.

Öğrendiklerinizi gösterin

Bir şirketin aynı hizmeti sunmayı sürdürmesine bağlı olmayan kurtarma yolunu tarif edin.

Sık sorulan soru

Açık kaynak üreticinin artık önemli olmadığı anlamına mı gelir? Hayır. Dağıtım, bakım, fiziksel bileşenler ve kullanım deneyimi önemini korur. Açık kaynak incelemeyi ve olası sürekliliği sağlar, otomatik garanti vermez.

Ara verme noktası

Laboratuvar sonuçlarını sürümler ve gözlenen sınırlarla kaydedin.

Birlikte çalışabilirlik için hangi kanıt daha güçlüdür?

1. İki uygulamanın da «Bitcoin» demesi.
2. Sürümleri belirlenmiş bir laboratuvarda aynı politikayı ve adresi yeniden oluşturup doğrulamak.
3. Benzer simgelere sahip olmaları.

> **Yanıtı göster: Sürümleri belirlenmiş bir laboratuvarda aynı politikayı ve adresi yeniden oluşturup doğrulamak.**
> Deneme ilgili koşulları korumalı ve doğrulanabilir sonuç vermelidir.

M12

Regtest ile teknik laboratuvar

Amaç

Yapay denemeleri fiziksel kullanımla karıştırmadan tekrarlanabilir laboratuvarı anlayın.

Konuyu anlayın

Regtest, blok üretmek ve ekonomik değeri olmayan işlemleri denemek için kontrollü yerel zincir kurmaya olanak verir. Ayrı dizinler ve erişim bilgileri kullanın. Gerçek materyal içe aktarmayın. Sonuçlar fiziksel bir cihazın USB, NFC, Bluetooth veya kamera uyumluluğunu tek başına kanıtlamaz.

Tam laboratuvar sürümleri, ağ yapılandırmasını, politikayı, deneme girdilerini, PSBT'yi, imzaları, son işlemi ve kabul sonucunu kaydeder. Toplamın tuttuğunu, değiştirilmiş imzanın reddedildiğini ve geçerli ödemenin yerel bloğa girdiğini doğrulayabilir. Deneme başarı yoluyla birlikte hata durumlarını da içermelidir.

Desk 9.21 doğrulama belgeleri Bitcoin Core 31 regtest denemeleri ve işlem motoru ile simüle edilen arayüzün otomatik testlerini bildirir. Bu baskı bunları belge kanıtı olarak kullanır. Bu testleri tekrarladığını veya cihazlarla işlem yaptığını iddia etmez. Paketin kontrolü tüm sistemlere kurulduğunu da kanıtlamaz.

Teknik dersten önce mühendis hazır laboratuvarı ve öğrencinin sürümüyle uyumlu prosedürü teslim etmelidir. Eğitmen kontrol etsin diye RPC'yi internete açmayın. Yapay zekâ yapay sonuçların yorumuna rehberlik edebilir ama erişim bilgisi veya yönetici izni almamalıdır.

Uygulama

1. Hazır laboratuvarda bir geçerli işlemi ve imzası değiştirilmiş bir işlemi gözlemleyin. Kabul veya reddi kaydedin.
2. Bir yanlış para üstü ve bir uyumsuz ağ örneğini kontrol edin.
3. Raporda «işlem motoru testi», «simüle edilmiş arayüz» ve «fiziksel donanım» kısımlarını ayırın.

Öğrendiklerinizi gösterin

Simülasyonu sertifika gibi göstermeden tam olarak neyin denendiğini ve neyin kaldığını açıklayın.

Sık sorulan soru

Regtest çalışıyorsa kursu tüm cihazlar için doğrulanmış diye satabilir miyim? Hayır. Fiziksel iş akışları, kurulum, erişilebilirlik, kurtarma ve ticari hizmet testleri hâlâ gerekir.

Ara verme noktası

Laboratuvarı kendi talimatlarına göre durdurup kaydedin. Yalnızca yapay verileri saklayın.

İşlem motorunun regtest sınaması, belirli bir telefonda gerçek NFC okumasını kanıtlar mı?

1. Evet, ikisi de Bitcoin kullandığı için.
2. Evet, PSBT küçükse.
3. Hayır. Bunun için ayrı bir fiziksel test gerekir.

> **Yanıtı göster: Hayır. Bunun için ayrı bir fiziksel test gerekir.**
> Farklı doğrulama ortamları farklı kapsamları sınar.

Bitirme projesi ve süreklilik planı

Amaç

Hazırlıktan kurtarma ve mahremiyete kadar bağımsız hareket edebildiğinizi gösterin.

Konuyu anlayın

Kursun sonucu bir menüyü ezberlemek değil, niyeti açıklayabilmek, sonucu doğrulayabilmek ve anlaşılmayan işlemi durdurabilmektir. Değerlendirme kavramlar, rehberli uygulama ve bağımsız bir durumu birleştirir. Değerlendirene kurtarma ifadesi, varlık veya kişisel adres açıklamayı hiçbir zaman gerektirmez.

A durumu: Eğitim ortamını kurun, model ve sürümleri belirleyin, Desk'i koruyun, eğitim kriptogramını bağlayın ve salt izleme hesabını yeniden kurun. Hangi yedeklerin gerektiğini ve sağlayıcınızın hangi verileri görebileceğini açıklayın.

B durumu: Farklı bağlamlardan hayalî UTXO'larla ödeme tasarlayın. Seçimi gerekçelendirin, alıcıyı, para üstünü ve ücreti doğrulayın ve cihazınıza ait imzalama yolunu anlatın. Ödemeyi çoğaltmadan bir yanıt dönüş kesintisini ve bir yayımlama kesintisini çözün. Fiziksel olarak kabul edilmiş donanım yoksa bu kısmı simülasyon olarak kaydedin; fiziksel deneme beklemede kalır.

C durumu: 3'te 2 düzen tasarlayın, daveti ve doğrulamayı canlandırın. Mirror'da seçtiğiniz alanı istediğiniz sırada karşılaştırın ve OK sonucunun kapsamını açıklayın. Eğitim politikasını kurtarın, bir katılımcının kaybını canlandırın ve süreklilik ile miras planını hazırlayın.

Önerilen geçme ölçütü bilgi bölümünde en az %80 ve tüm kritik kontrollerin doğru yapılmasıdır: sır açıklamamak, ağ ile çıktıları kontrol etmek, aşamaları karıştırmamak ve kurtarma imkânını korumak. Kritik hata inceleme ve yeni uygulama gerektirir. Piyasa sorularına doğru yanıt vermek telafi etmez. Ticari sertifika düzenlenirse nelerin değerlendirildiğini ve fiziksel gözlem mi yalnızca simülasyon mu yapıldığını belirtmelidir.

Uygulama

1. Üç durumu yapay veriler ve kendi açıklamanızla tamamlayın.
2. Ekteki son değerlendirmeyi çözün ve her yanlış yanıtı gözden geçirin.
3. Yalnızca kapsamı ve bekleyen konuları belgelerle belirten, gizli bilgi içermeyen bir sonuç sayfası teslim edin.

Öğrendiklerinizi gösterin

İşleme ilişkin kanıt yetersizse kendiliğinizden durabilmeli ve devam için ne gerektiğini bilmelisiniz.

Sık sorulan soru

Tüm sayfaları bitirmek her tutarı saklamaya hazır olmak anlamına gelir mi? Hayır. Yeteneği sınamak ve riski kendi koşullarınıza göre değerlendirmek gerekir. Okuma ve denemeler gelecek sonuçları garanti etmez.

Ara verme noktası

Gözden geçirme planını ve tamamlanmamış alıştırmaları saklayın. Tüm kursu baştan tekrarlamadan gereken bölüme dönebilirsiniz.

Uygulamalı eğitimi tamamlamak için kritik gereklilik nedir?

1. Tüm sayfaları açmış olmak.
2. Gizli bilgi açıklamadan, belgelenen kapsamda kurtarmayı ve işlem incelemesini göstermek.
3. Gelecek ayın fiyatını tahmin etmek.

> **Yanıtı göster: Gizli bilgi açıklamadan, belgelenen kapsamda kurtarmayı ve işlem incelemesini göstermek.**
> Öğrenme, gezinme veya tahminle değil, doğrulanmış yetenekler ve sınırlarla gösterilir.

Öğrenci kılavuzu

Cuvex kullanım kılavuzu

Bu kılavuz dersleri tamamlar. Her işlem, incelenen kaynaklarda bulunan iş akışını, kontrolleri ve nerede durulacağını açıklar. Bu sürüm pilot uygulama adayıdır. Original, BIT, telefonlar veya tüm masaüstü platformları üzerinde tarafımızdan fiziksel test yapıldığını belgelemez. Gerçek fonlarla eğitim verilmeden önce ekip kabul testleri matrisini tamamlamalı ve farklılık gösteren etiket veya ekranları düzeltmelidir.

Başvurulan sürümler: Original 1.2.2 Final, BIT 1.2.3 Final, Desk 1.0.0-beta.9.21 ve Mirror 1.0.0-beta.12.12. Desk’te bir profil seçmek beyan edilen uyumluluğu gösterir, aygıt yazılımının uzaktan ölçümü değildir. Mirror’ın gerçek ekran görüntüleri 12.12 paketinin Android öykünücüsünden alınmıştır. Ürün fotoğrafları kurumsal materyaldir ve günümüzde bir cihazda gösterilen sürümü kanıtlamaz.

P01 | Kaynağı ve sürümü kontrol etme | Cuvex | L16,L21 | C01,C02

Hazırlık: Satın alma bilgilerini ve bağımsız olarak doğrulayabileceğiniz resmî kanalı hazır bulundurun. Henüz gizli bilgi girmeyin.

1. Ambalajı ve mühürleri inceleyin. Müdahale belirtisi varsa kurulumu durdurun ve hassas veri içermeyen kanıtları saklayın.
2. Teslimatınızla uyumlu uygulamadaki bütünlük ve mühür doğrulamasını kullanın. Kodları yalnızca oraya girin, eğitmene asla vermeyin.
3. Cihazı Original veya BIT olarak tanımlayın ve mevcut donanım revizyonunu belirleyin. Cihazda ve uygulamalarda gösterilen sürümleri kontrol edin.
4. Ekibin yayımladığı uyumluluk matrisiyle karşılaştırın. Bir katalog veya hash değeri, aygıt yazılımının gerçekliğini doğrulamanın ya da fiziksel kabul testinin yerini tutmaz.

Sonuç: Gizli bilgiler açığa çıkmadan model, sürümler ve cihazın kaynağı kontrol edilmiştir. Kodlar geçersizse veya arayüz farklıysa cihazı zorla çalıştırmak için eski bir kılavuzu izlemeyin.

Ara: Varlık saklama materyallerini yüklemeden önce durun. Satın alma ve teslimatın izlenebilirliği tek başına gelişmiş müdahale olasılığını dışlamaz.

P02 | Original’ı Bluetooth ile güncelleme | Original | L46 | C01,C02,C03

Hazırlık: Kurtarılabilir yedekler, kararlı güç kaynağı, uyumlu resmî paket ve sisteminiz için kabul edilmiş iş akışı gerekir. Bu kurs her platformda tüm adımların fiziksel olarak kullanılabildiğini belgelemez.

1. Uygulamanın cihazlar veya aygıt yazılımı bölümünde Original’ı ve ilgili resmî indirmeyi ya da gerçekliği doğrulanmış yerel dosyayı seçin.
2. Menüden cihazı güncelleme moduna alın ve uygulamanın adımlarını izleyerek bağlanın. Cihazları yakın tutun ve aynı bağlantıyı kullanmaya çalışan başka oturum açmayın.
3. Original ekranındaki kodu belirtilen alana girin. Bunu kriptogram parolasıyla karıştırmayın.
4. Aktarım, doğrulama, kurulum ve yeniden başlatma aşamalarını izleyin. Yüzdenin ilerlemesi kurulumun tamamlandığını kanıtlamaz.
5. Son sürümü Original üzerinde kontrol edin. Uygulamada ilgili alan varsa buraya kaydedin.

Sonuç: Yeniden başlatma sonrasında sürüm ekrandan kontrol edilmiş ve işlemin tamamlandığı doğrulanmıştır. Hata PIN’den önce, paket aktarırken veya sonunda çıkarsa aşamayı ve hata kodunu kaydedin. «%99’u geçmek» için bağlantıyı gelişigüzel kesmeyin veya yazılım değiştirmeyin.

P03 | BIT’i USB ile güncelleme | BIT | L46 | C01,C02,C03

Hazırlık: BIT’in gerçek veri taşıyıcısını, güç kaynağını ve uyumlu resmî paketi belirleyin. Yazılımı değiştirmeden önce yedek alın.

1. Uyumlu Desk veya Mirror aygıt yazılımı güncelleme akışında BIT’i seçin.
2. Cihazı uygun veri kablosu ve adaptörle bağlayın. Uygulama istediğinde birime veya klasöre erişim izni verin.
3. Modelin gerçekliği doğrulanmış aygıt yazılımını seçin. Göndermeden önce sürüm ve uyumluluk verilerini inceleyin.
4. Cihazın aktarım ve doğrulama aşamalarını bekleyin. Protokol gereği birim kaybolabilir veya yeniden bağlanabilir.
5. Yeniden başlatmadan sonra BIT’teki sürümü ve uygulamanın nihai sonucunu kontrol edin.

Sonuç: Kurulum cihaz üzerinde doğrulanmıştır. Birim görünmüyorsa cihaz modunu, veri kablosunu, izinleri, bağlama durumunu ve başka bir etkin oturumu kontrol edin. Bilgisayarda aynı adlı bir klasör oluşturmak birimin yerini tutmaz. Başarısız bir güncellemenin kurtarılması o donanıma ait resmî prosedürü gerektirir.

P04 | Para ve zarla cüzdan oluşturma | Cuvex | L17 | C01

Hazırlık: Özel bir alan, uygun zarlar ve bir para hazırlayın. Eğitmen mikrofonu ve kameralar kapalı olmalıdır. Eğitim cüzdanı kullanın.

1. Cüzdan oluşturmayı ve aygıt yazılımının entropi adımlarını açın. Dört zarın sırasını önceden belirleyin.
2. Para ve her zarın sonucunu, tercih ettiğiniz sonucu elde etmek için değiştirmeden ekrandaki yönergeye göre girin.
3. İncelenen kaynak kodun hesabı şöyledir: indeks = para × 1.296 + (d1−1) × 216 + (d2−1) × 36 + (d3−1) × 6 + (d4−1). Yalnızca 0..2.047 aralığındaki indeksler kabul edilir.
4. Sonuç reddedilirse parayı ve tüm zarları yeniden atın. Uyarı önceki kelimeleri korur ve tüm atışın tekrarlanmasını ister.
5. Son doğrulama dâhil cihazın algoritmasını tamamlayın. Anımsatıcı ifadeyi koruyun ve kurtarmayı özel ortamda sınayın.

Sonuç: Cüzdan elle seçilmiş kelimelerle değil, tüm işlem akışıyla oluşturulmuştur. Ekran ile kaynak uyuşmazsa durun. Yayımlanmış zar, kurtarma ifadesi veya anahtar örneklerini kendi cüzdanınızda kullanmayın.

P05 | Gizli bir bilgiyi şifreleme | Cuvex | L18,L19 | C01

Hazırlık: Modeli, içerik biçimini ve korumayı seçin. Gizli bilgiyi bilgisayarda veya telefonda girmek, hedefte şifreli tutulsa bile kaynakta açığa çıkarır.

1. Şifrelemeyi ve desteklenen BIP39, SLIP39, Monero veya metin biçimini seçin. Sözcük listelerini birbirinin yerine kullanmayın. İncelenen düz metin klavyesi en fazla 500 karakter kabul eder. Bir biçimi saklayabilmek ilgili ağda imza atılabildiği anlamına gelmez.
2. Yalıtımı korumak için içeriği doğrudan cihazda girin. Sıralamayı, karakterleri ve ek alanları cihazın ekranında kontrol edin.
3. İş akışına göre tek kişilik veya paylaşımlı korumayı seçin. BIT’te uygunsa biyometriyi kullanın. Bu eşiği Bitcoin imza eşiğinden ayırın.
4. Parolaları aygıt yazılımının doğrulama kurallarına göre özel ortamda girip onaylayın. Desk’in kurallarını otomatik olarak buraya uygulamayın.
5. Original’da boş ve uyumlu bir karta yazın. BIT’te USB akışının dışa aktardığı nesneleri saklayın. Onayı bekleyin.
6. İçeriği kontrol etmek için deneme kurtarması yapın. Bittiğinde gizli bilgiyi kapatın.

Sonuç: Kriptogramın kurtarılabildiği sınanmıştır. Yazma veya okuma başarısızsa asıl kopyayı koruyun ve ekranın önerdiği yeniden deneme adımını izleyin. Başlıkları silmeyin ve üzerine yazmaya zorlamayın.

P06 | Şifreyi cihazda çözme | Cuvex | L18 | C01,C02

Hazırlık: Fiziksel mahremiyet ve yeterli kilit açma bileşeni sağlayın. Gizli bilgiler görünürken mikrofonu ve ekran kaydını kapatın.

1. Doğru modelde şifre çözmeyi başlatın. Kriptogramı Original'da NFC ile, BIT'te USB iş akışıyla teslim edin.
2. Kimlik bilgilerini girmeden önce nesnenin takma adını ve tanımlayıcısını kontrol edin.
3. Gereken parolaları ve biçim gerektiriyorsa biyometrik doğrulamayı sağlayın. Hata durumunda peş peşe otomatik denemeler yapmayın. Erişim denetimi ve kilitleme vardır.
4. İçeriği yalnızca öngörülen ekranda kontrol edin. Gizli bilgi içeren QR kodu, düz metin kadar hassastır.
5. Cihazın adımlarına göre işlemi kapatın veya bitirin. Planınıza göre taşıyıcı ve erişim bilgilerini ayrı saklayın.

Sonuç: İçerik özel ortamda kurtarılmış ve oturum tamamlanmıştır. Biçim tanınmazsa, gerçeklik doğrulanamazsa veya beklenmedik içerik çıkarsa bilinmeyen bir uygulamayla «düzeltmeyin». Desteğe sürümü, biçimi ve hatayı bildirin, gizli bilgiyi eklemeyin.

P07 | Biyometrik bir kriptogramın kurtarılmasına hazırlanma | BIT | L19,L47 | C01,C02

Hazırlık: Eğitim kriptogramını ve biçiminin belgelerini hazırlayın. Elinizde .bin dosyası olması kurtarmanın mümkün olduğunu kanıtlamaz.

1. Desk'teki bilgi kartında biyometrik bileşenler olup olmadığını ve hangi kurtarma dışa aktarımının kullanılabildiğini kontrol edin.
2. İş akışının birbiriyle ilişkilendirdiği dosyaların tamamı ile bağımsız bir kopyayı, içeriklerini açık etmeyen tanımlayıcılarla saklayın.
3. BIT üzerinde normal kilit açmayı deneyin ve hangi parolaların ve koşulların gerektiğini belgeleyin.
4. Olağanüstü yerel kurtarma yöntemini ve desteklenen biçimleri inceleyin. Gereken materyallerin mevcut olduğunu onlara ihtiyaç duymadan önce doğrulayın.
5. Bozuk cihaz veya kullanılamayan parmak izi senaryosunu gerçek fon içermeyen verilerle deneyin.

Sonuç: İlgili biçime özel, sınırları bilinen ve denenmiş bir plan. Bu, her biyometrik kontrolün atlanabileceği veya parmak izinin yedeklerin yerini tuttuğu anlamına gelmez. Gizli bilgi bilgisayarda kurtarıldıysa açığa çıkma riskini ve ardından kontrolün yeni anahtarlara taşınması gerekip gerekmediğini değerlendirin.

P08 | Kriptogramın kopyasını oluşturma ve sınama | Cuvex ve Desk | L20 | C01,C02

Hazırlık: Tanımlanmış bir asıl kopya ile korunması gereken veri içermeyen uyumlu bir hedef hazırlayın.

1. Original'da cihazın klonlama işlevini veya Desk'in uyumlu işlevini kullanın. Kaynak ve hedefi gösterilen sırada sunun.
2. Kartları sabit tutun. Zaten kriptogram içeren taşıyıcı reddedilirse bu karara uyun.
3. BIT veya dosya kullanıyorsanız işlemle ilişkili tüm bileşenleri dışa aktarın ve gereken adları veya dosyalar arasındaki ilişkiyi koruyun.
4. Asıl kopyayı ayırın, yeni kopyayı okuyup deneme kurtarması yapın.
5. Tarihi, biçimi ve sonucu özel kayıtlarınıza geçirin. Kopyaları fiziksel riskleri birbirinden bağımsız yerlerde saklayın.

Sonuç: Denenmiş ikinci bir kopya. Bu, farklı bir cüzdan yaratmaz, parolaları geçersiz kılmaz veya daha önce açığa çıkmış kurtarma ifadesini korumaz. Hedef başarısızsa asıl kopyayı saklayın. İkisini eşleştirmek için asıl kopyayı «onarmaya» çalışmayın.

P09 | Desk parolası oluşturma, kilidi açma ve parolayı değiştirme | Desk | L21,L40 | C02

Hazırlık: Doğrulanmış kurulum paketi, uygun mimari ve yerel depo için yedekleme planı.

1. Depoyu 12 ila 1.024 karakter uzunluğunda, yalnızca burada kullanılan bir parolayla oluşturun. Onay alanına aynı parolayı girin.
2. Erişimin sizde olduğunu doğrulamak için depoyu kilitleyip yeniden açın. Parola yalnızca Desk'e girilir.
3. Güvenlik bölümündeki Erişim ve kilit ayarlarında hareketsizlik ve arka plana geçiş seçeneklerini inceleyin. Gösterim sırasında isteğe bağlı silmeyi etkinleştirmeyin.
4. Parolayı değiştirmek için mevcut parolayı girin ve ilgili adımda yenisini onaylayın.
5. Bilgisayarın biyometrisini kullanıyorsanız yönergeye göre yeniden yapılandırın. Güncel bir yedek oluşturun ve önceki kopyalarla ilişkisini kaydedin.

Sonuç: Erişim kontrol edilmiştir. Önceki kopyalar kendi eski parolalarını ve şifrelemelerini korur. Bilgisayar biyometrisi ve BIT biyometrisi farklı mekanizmalardır. Erişim başarısızsa art arda denemeyi bırakın ve eğitmenden kimlik bilgilerini saklamasını istemeden kurtarma seçeneklerini inceleyin.

P10 | Desk’te kriptogram bağlama ve inceleme | Desk | L22 | C02

Hazırlık: Kaynağı bilinen deneme kriptogramı ve kullanılabilir bir aktarım yolu.

1. Kriptogramlar veya kartlar bölümünü açın. NFC, USB veya uyumlu kopya yoluyla bağlamayı seçin.
2. Tasarımı ve kaynağı seçin. NFC için bilgisayara Bluetooth ile eşleştirilmiş Cuvex Mirror’ı kullanın. USB-C aktarımı için bağlı Cuvex BIT’in birimini seçin. Cuvex Desktop harici USB NFC okuyucularını desteklemez.
3. Bilgi kartında takma adı, kaynağı, boyutu, biçimi ve yorumlanan koşulları inceleyin. Bunlar üstveridir, şifresi çözülmüş içerik değildir.
4. Eşleştirme bekleyen, korunmuş hesapları kontrol edin ve yalnızca doğruladığınız hesabı ilişkilendirin.
5. Yedekleme kapsamı yetersizse bir kopyayı dışa aktarın ve kurtarmayı ayrı olarak sınayın.

Sonuç: Nesne yerel olarak düzenlenmiştir. «Bağlandı» durumu kurtarma ifadesinin gerçekliğini veya bakiyeyi kanıtlamaz. Tanınmayan nesnenin biçimini ve sürümünü kontrol edin. Uygulamaya kabul ettirmek için uzantıyı değiştirmeyin veya veri silmeyin.

P11 | Salt izleme WOW hesabını etkinleştirme | Desk ve Cuvex | L13,L22 | C01,C02

Hazırlık: Cihazın iş akışından alınmış açık bilgiler ve bunların kaynağını özel olarak kontrol etme imkânı.

1. Doğru kriptogram üzerinden WOW’u etkinleştirmeyi veya hesap eklemeyi açın.
2. İşleve göre tanımlayıcıyı veya desteklenen açık veriyi dosya, web kamerası ya da Mirror üzerinden içe aktarın.
3. Uygun olduğu yerde ağı, betiği, kökeni, parmak izini, yolu ve sağlama toplamını kontrol edin. Kurtarma ifadesi veya xprv girmeyin.
4. Hesaba ad verin ve sorgu kaynağını bilinçli onayınızla seçin.
5. Bakiyeyi yorumlamadan önce bir kontrol adresini ve adres keşfinin kapsamını doğrulayın.

Sonuç: İzleme cüzdanı ilişkilendirilmiştir. Sıfır görürseniz paraların yok olduğu sonucuna varmadan ağı, ilk kullanılan ek parolayı, türetme yolunu, hesabı, sağlayıcıyı ve taramayı kontrol edin. Genel arayüz çoklu imza profilinin desteklemediği ağları da içerebilir. Her bağlamın kısıtlarına uyun.

P12 | Düğüm ve eşitlemeyi yapılandırma | Desk | L25,L33 | C02

Hazırlık: Mahremiyet tercihinizi belirleyin. Core kullanıyorsanız korunan ve eşitlenmiş bir düğüme erişiminiz olmalıdır.

1. Güvenlik bölümünde Gizlilik ve düğümler ayarını açın, WOW hesabını seçin ve sağlayıcısını inceleyin.
2. Uyumlu kamuya açık sağlayıcıyı veya Core'u açıkça seçin. Core için bağlantı adresi, cüzdan ve erişim bilgilerini yalnızca uygulamaya girin.
3. Her hizmetin hangi verileri aldığına bakarak sorguya onay verin. TLS sorguyu sağlayıcıdan gizlemez.
4. Eşitlemeyi başlatıp tarihi, zincir ucunu, ilerlemeyi ve tamamlanma durumunu inceleyin. Yeniden taramada kapsanan geçmişi ve işlemin kesintisiz ilerlemesini kontrol edin.
5. 429 yanıtında bekleme süresine uyun. Hata olunca başka bir düğümün devreye girdiğini varsaymayın. Yapılandırma düğümleri habersiz değiştirmez.

Sonuç: Kaynak ve durumu bilinmektedir. RPC'yi internete açmayın, parolayı paylaşmayın ve adres keşfini yalnızca bakiyeli adreslerle sınırlamayın. Boş görünen geçmiş kısmi bir sonuç olabilir.

P13 | Ödeme alma isteği oluşturma ve geri getirme | Desk ve Cuvex | L26 | C01,C02

Hazırlık: Hesabı, ağı ve politikayı doğrulayın.

1. Alma ekranını açıp uygun isteği oluşturun veya geri getirin.
2. Gözlemci, gerekçe ve beklenen tutarı yalnızca bu yerel üstverilere ihtiyaç duyuyorsanız ekleyin.
3. Önemli bir ödeme almadan önce adresi cihazın desteklediği yöntemle doğrulayın. Fiziksel kabul testi yapılmadıysa uygulamayı simülasyon aşamasında durdurun.
4. Yalnızca gereken verileri alıcının kimliği doğrulanmış kanalı üzerinden paylaşın.
5. Ağ kaynağınızdan ödemenin geldiğini, tutarı ve onayları kontrol edin.

Sonuç: Yalnızca istek oluşturulmamış, alım da doğrulanmıştır. Çoklu imzada gösterilen adresler gecikmiş ödemeler için korunur ve yeniden atanmaz. Geçmişsiz yeni adres sınırına ulaşılırsa önceki istekleri geri getirin. İndeksleri elle zorlamayın.

P14 | Etiketler, dondurma ve BIP329 | Desk | L27 | C02,B13

Hazırlık: UTXO içeren bir laboratuvar hesabı ve korumalı dışa aktarım için bir parola.

1. Gereksiz kişisel veri eklemeden bir girdiyi bağlamıyla etiketleyin.
2. Dondurma veya çözme kararını bilinçli verin ve harcanabilir bakiyeyi inceleyin. Bu kısıtlama yereldir.
3. Etiketleri korumalı işlevle dışa aktarın. Etiket biçimi olan BIP329 ile dosyanın şifrelenmesini ayırt edin.
4. Uyumlu bir kopyaya içe aktarın. Referansların, etiketlerin ve dondurma durumlarının uyuştuğunu kontrol edin.
5. Planınıza uygun biçimde üstverilerin güncel yedeğini ve bunun parolasını koruyun.

Sonuç: Bağlam korunmuş ve seçimin etkisi anlaşılmıştır. İçe aktarım, donmuş paraları incelemeden otomatik çözmek için kullanılmamalıdır. Etiket dosyasını eğitmene göndermeyin. Harcama anahtarı içermese de karşı tarafları ve ilişkileri açığa çıkarabilir.

P15 | Ödeme hazırlama ve bakiyenin tamamını gönderme | Desk | L28 | C02

Hazırlık: Doğrulanmış istek ve harcanabilir girdileri yeterli bir hesap.

1. WOW, UTXO’lar veya sohbet üzerinden ödeme ekranını açın. Hesabı ve ağı doğrulayın.
2. Girdileri, alıcıları ve tutarları seçin. Hangi bağlamların ilişkilendirileceğini inceleyin.
3. Ücret oranını seçip toplam ücreti, para üstünü ve uyarıları inceleyin. Dust oluşuyorsa gizli bir ücreti kabul etmeden alternatifleri değerlendirin.
4. Tamamını gönderirken ücretten sonraki net tutarı doğrulayın. Sohbetteki isteğin tamamı karşılanmıyorsa kısmi ödemeyi açıkça onaylayın.
5. Taslağı hazırlayın ve imza için dışa aktarmadan önce tüm verileri kontrol edin.

Sonuç: Amaç açıkça anlaşılmış ve o işleme ait PSBT hazırlanmıştır. Genel bir form donanımdan daha çok girdiye veya alıcıya izin verebilir. İmzalayıcının ve taşıyıcının gerçek sınırlarını uygulayın. Çıktılar veya koşullar değişirse incelemeyi yenileyin.

P16 | Original ile PSBT imzalama ve geri aktarma | Original ve Mirror | L29 | C01,C02,C03

Hazırlık: Doğru taslak, uyumlu aktarım kartı, gerçekliği doğrulanmış uyumlu kriptogram ve özel ortamda kilit açma araçları gerekir. Gerçekliği doğrulanmamış eski bir kopyayla imzalamadan önce doğrulanmış bir kurtarma ve yeni kopya gerekebilir. Başlığı düzenlemek çözüm değildir.

1. İsteği Desk/Mirror'dan desteklenen NFC akışıyla dışa aktarın.
2. Kartı Original'a götürün. İstendiğinde kriptogramı sunun ve erişim bilgilerini seslendirmeden kilidini açın.
3. Ağı, özeti, tüm çıktıları, ücreti, para üstünü ve zorunlu uyarıları kontrol edin.
4. Final çoklu imza akışında genişletilmiş parametreleri inceleyip incelemeyeceğinizi seçin. Son üç onayı yalnızca tüm bilgiler uyuşuyorsa tamamlayın.
5. Yanıtın karta yazılmasını ve karttan yeniden okunmasını bekleyin.
6. Yanıtı Cuvex Mirror ile okuyun ve Desk'te ilgili işlem içinde doğrulayın.

Sonuç: İmza alınmış ve taslakla eşleştirilmiştir. İşlem henüz yayımlanmış sayılmaz. Yazma başarısızsa durumu koruyun ve yeniden deneme adımını izleyin. Yedekleme kartını gözden çıkarılabilir bir ödeme aktarım kartı olarak asla kullanmayın.

P17 | BIT ile imzalama, yanıtı alma ve alındı onayı verme | BIT ve Desk | L29 | C01,C02

Hazırlık: Doğru taslağı, gerçekliği doğrulanmış uyumlu kriptogramı ve BIT'in gerçek birimini seçin. Eski kopya imzalama için reddedilirse biçimi zorlamadan belirtilen kurtarma ve yenileme adımlarını izleyin.

1. İsteği Desk hizmetiyle USB-C üzerinden teslim edin. Kriptogramı sunarken cihaz ekranındaki yönergeleri izleyin.
2. Kilidi özel ortamda açın. Özeti, tüm çıktıları, ücreti ve uyarıları inceleyin.
3. Final çoklu imza akışında isterseniz genişletilmiş ayrıntıları inceleyin. Yetkilendirmeyi zorunlu son onaylarla tamamlayın.
4. Desk'te «BIT'ten al» komutuyla o işe ait yanıtı içe aktarın ve doğrulayın.
5. Kaydı ve alındı onayını kontrol edin. Yanıt alındıktan sonra alındı onayı başarısız olursa modelin seçtiği yeni bir işlem yerine aynı işlemi tekrar deneyin.

Sonuç: İmza doğrulanmış ve aktarım durumu tutarlıdır. Bağlantı yanıttan önce veya kayıttan sonra kesilirse isteğin profilini koruyun. Bekleyen bir yanıtı uydurmak için katalogdan farklı bir aygıt yazılımına geçmeyin.

P18 | İşlemi sonlandırma, yayımlama ve izleme | Desk | L30,L44 | C02

Hazırlık: İmzaları doğrulayın ve gerekiyorsa imza eşiğinin karşılandığından emin olun.

1. Amacı, girdileri, çıktıları, ücreti ve ağı bir kez daha inceleyin.
2. İlgili komutla işlemi sonlandırın ve hiçbir imzanın veya koşulun eksik olmadığını kontrol edin.
3. Ağa duyurmayı onaylayın ve yerel sonucu saklayın. Ağın yanıtı kaybolursa yeniden denemeden önce durumu sorgulayın.
4. Seçilen sağlayıcıda eşitleme tarihini dikkate alarak mempool'u ve onayları izleyin.
5. RBF düşünülüyorsa yeni işlemi gözden geçirin ve gereken imzaları alın. Dahili bir CPFP işlevi bulunduğunu varsaymayın.

Sonuç: Zincirdeki durum, kullanılan kaynakla doğrulanmıştır. Bir taslağı iptal etmek dışa aktarılmış imzaları geçersiz kılmaz ve onaylanmış ödemeleri yeniden yazmaz. Sohbet mesajı veya ekran görüntüsü izleme yerine geçmez.

P19 | İki politika QR kodunu istenen sırada karşılaştırma | Mirror | L43 | C03,C02

Hazırlık: Alan Desk'te ve Cuvex'te görünür olmalıdır. Alıştırmada yalnızca kursun yapay örneklerini kullanın.

1. «Politikaları karşılaştır» ekranını açın; iki taraftan dilediğinizi önce okuyun.
2. Doğrulamak istediğiniz veriyi seçin. 15. adımdan başlayabilir ve elle kontrol ettiğiniz diğer adımları atlayabilirsiniz.
3. Karşı taraftaki değeri okuyun ve her iki metni bütünüyle inceleyin. Adım belirsizse «Desk adımını belirt» seçeneğini kullanın. Bu bağlamın elle girildiğini göz önünde bulundurun.
4. «Eşleşiyor» veya «Eşleşmiyor» sonucunu yalnızca bu iki metnin birebir karşılaştırması olarak yorumlayın. Boşluklar, büyük-küçük harf ve kodlama önemlidir.
5. Dilediğiniz sırada başka bir çifti karşılaştırın. İncelenen silme davranışına uygun olarak çıkın veya uygulamayı arka plana alarak işlemi bitirin.

Sonuç: Tek bir çift yerel olarak karşılaştırılmıştır. Bu, kaynağı, oturumu, genel onayı veya etkinleştirmeyi doğrulamaz. Fark varsa asıl kaynaklardan açıklığa kavuşturun. OK sonucunu elde etmek için metni değiştirip eşitlemeyin.

P20 | Sohbeti etkinleştirme, kurtarma ve taşıma | Desk ve Cuvex | L36,L39 | C02

Hazırlık: DEV veya Üretim ortamını seçin. Takma ad ve sohbet anahtarı (Clave Chat) cihazda tutulmalı, kurs ortamına hiçbir zaman girilmemelidir.

1. Kriptogram bağlamından sohbeti etkinleştirme veya kurtarma seçeneğini açın.
2. Yeni takma ad veya mevcut kimliği taşıma seçeneğini ve uygulamanın gösterdiği uyumlu mobil profili seçin.
3. Sohbet anahtarını (Clave Chat) yalnızca özel iş akışında girin veya okuyun. Kurtarma ifadesi, PIN veya WOW anahtarı kullanmayın.
4. Etkinleştirmeyi hizmetle doğrulayın. Beklemede kalırsa tamamla veya kontrol et komutunu kullanın, başarıyla bittiğini varsaymayın.
5. Taşıma sonrası kişilerinizle iletişimin sürdüğünü doğrulayın. Aynı takma adı birden fazla cihazda eşzamanlı kullanmayın.

Sonuç: Kimlik doğru ortamda etkinleştirilmiş veya kurtarılmıştır. Sohbet anahtarı (Clave Chat) veya Desk’in genel yedeği önceki oturumları ve geçmişi otomatik geri getirmez. Elinizdeki materyalin sınırlarını göz önünde bulundurun.

P21 | Bir sohbet kişisinin kimliğini doğrulama | Desk | L36,L48 | C02

Hazırlık: Kişiyle daha önce kararlaştırdığınız bağımsız bir kanal.

1. Takma adı ekleyin ve uygulamadan kişinin açık kimlik bilgilerini sorgulayın.
2. Parmak izini yalnızca yeni açılan sohbette değil, kimliği doğrulanmış kanaldan karşılaştırın.
3. Tanıma sorusu kullanıyorsanız herkese açık bilgilerden ve başka hizmetlerde de kullanılan sırlardan kaçının.
4. Yalnızca farklılıklar çözüldükten sonra onaylayın. Kimlik değiştiyse yeniden doğrulanana kadar ödemeyi ve koordinasyonu durdurun.
5. Hassas yanıtları kursa kaydetmeden doğrulama yöntemini belgeleyin.

Sonuç: Kişiye belirli bağlamda güven tesis edilmiştir. Gelecekteki her isteği garanti edilmez. Ses taklit edilebilir ve gerçek bir cihaz ele geçirilmiş olabilir. Her işlem kendi incelemesinden geçmelidir.

P22 | Sohbette adres isteme, ödeme talep etme ve ödeme | Desk ve Cuvex | L37 | C02,C01

Hazırlık: Kimliği doğrulanmış kişi ve uyumlu WOW hesabı.

1. Amacınıza göre adres iste, adresle yanıtla veya ödeme iste seçeneğini seçin.
2. Göndermeden önce asıl isteği, ağı, tutarı ve notu kontrol edin.
3. Ödeme için uygun hesaptan hazırlığı açın. UTXO'ları ve ücret oranını seçip net tutarı gözden geçirin.
4. Cuvex'te modelin prosedürüyle onay verin. Sohbet otomatik imzalamaz.
5. Yayımlanmayı ve onayları kendi ağ kaynağınızdan izleyin. Açıkça belirtilen kısmi ödemeleri asıl istekle karşılaştırın.

Sonuç: Varlıkların saklanmasına ilişkin kontroller korunarak koordinasyon gerçekleştirilmiştir. Mesaj durumu ile işlem durumu aynı değildir. İşlem gezginine verilen bağlantı açıldığında üçüncü bir tarafa bilgi gidebilir. Açmadan önce buna gerek olup olmadığını değerlendirin.

P23 | Alınan bir kriptogramı paylaşma ve bağlama | Desk | L38 | C02

Hazırlık: Paylaşmanın somut amacı, doğrulanmış kişi ve ona hangi erişim araçlarının verileceği belirlenmelidir.

1. Sohbet komutundan kriptogram paylaşmayı seçin ve nesneyi kontrol edin.
2. Yoruma parola, kurtarma ifadesi veya sohbet anahtarı (Clave Chat) eklemeyin.
3. Alıcı kaynağı doğrular ve uyumlu nesneyi alma komutuyla bağlar.
4. Alıcının şu anda hangi yeteneği kazandığını ve yeterli kilit açma bilgisine ulaşırsa neleri yapabileceğini değerlendirin.
5. Gerçekçi bir erişim iptali planı tutun. Mesajları silmek dış kopyaları veya öğrenilmiş anahtarları geri almaz.

Sonuç: Şifreli nesne bilinçli olarak aktarılmıştır. Bu bir ödeme değildir ve tek başına çoklu imzaya anahtar eklemez. Ek dosya şifre çözmek için bilinmeyen bir siteye yönlendiriyorsa durun.

P24 | Desk'in genel yedeğini alma ve geri yükleme | Desk | L15,L21 | C02

Hazırlık: Eğitim deposu ve sizin kontrolünüzde bir yedekleme hedefi.

1. Depo yedekleme işlevini açın ve istenen parolayı belirleyin. Hangi parolanın bu kopyaya ait olduğunu kaydedin.

2. Kopyayı günlük kullanımda olan tek cihazınızdan ayrı saklayın. İlgili akışla kaynağını ve bütünlüğünü doğrulayın.
3. Ayrı bir test ortamında geri yükleyin. Hesapları, yapılandırmayı ve yedeklenen verileri doğrulayın.
4. Kapsam dışı öğeleri inceleyin. Sohbetin, oturumlarının veya geçmişinin yedeğe dâhil olduğunu varsaymayın. Çoklu imza politikası ile özel anahtarlar birbirinin yerine kullanılamaz.
5. Önemli değişikliklerden sonra tekrarlayın ve kurtarma yönergelerini saklayın.

Sonuç: Kapsamı ve parolası bilinen bir yedek. Eski kopyalar önceki parolalarını korur. Erişim değişirse veya veriler açığa çıkarsa bu kopyaları da değerlendirin. Yalnızca güncel depoyu değiştirmek yeterli değildir.

P25 | Çok imzalı cüzdan oluşturma ve daveti kabul etme | Desk ve Cuvex | L41,L42 | C01,C02

Hazırlık: Katılımcılar bağımsız olmalı, kişiler doğrulanmalı, ağ ve geçerli sınırlar kararlaştırılmalıdır.

1. Oluşturan kişi adı, M/N eşiğini, ağı, katılımcıları ve işlemsel geçerlilik süresini seçer.
2. Doğru genişletilmiş açık anahtarı, parmak izi ve BIP48 yoluyla birlikte desteklenen iş akışı üzerinden sağlayın.
3. Her katılımcı öneriyi inceler, kabul veya reddeder ve açık verilerini sunar. Kurtarma ifadesini hiçbir zaman paylaşmaz.
4. Politikanın tamamını oluşturun ve her cihazda doğrulanmasını hazırlayın.
5. Fon aktarmadan önce politika kopyalarını saklayın. Kontrol adresini ve kurtarma imkânını doğrulayın.

Sonuç: Tam ve doğrulanabilir bir öneri. Daveti kabul etmek donanım üzerindeki incelemenin yerini tutmaz. Original katılıyorsa en fazla altı anahtar sınırını ve NFC kapasitesini uygulayın. BIT diğer katılımcıların kapasitesini artırmaz.

P26 | Politikayı doğrulama ve onayı alma | Desk ve Cuvex | L43 | C01,C02,C03

Hazırlık: Herkes için aynı eksiksiz politika, doğru aygıt yazılımı profili ve başka eşzamanlı iş yürütmeyen cihaz.

1. Desteklenen bağlamda politika doğrulamasını başlatın. Original, kurulu profilin açıkça seçilmesini gerektirir. BIT desteklenen özellikleri kendi protokolüne göre belirler.
2. İsteği modele göre NFC/Mirror veya USB-C üzerinden iletin.
3. Politika alanlarını cihazda gözden geçirin. İsterseniz seçtiğiniz çiftleri Mirror ile herhangi bir zorunlu sıra olmadan karşılaştırın.
4. Cihaz onayını tamamlayın ve yanıtını ilgili taşıma yöntemiyle geri gönderin.

5. Desk’te isteğe bağlı yanıtı doğrulayın. Karşılaştırıcının görsel OK işareti bu adımın yerine geçmez.

Sonuç: Yanıt ilgili incelemeyle eşleştirilmiş ve sonucu o incelemenin kapsamıyla sınırlıdır. Katalog aygıt yazılımını uzaktan doğrulamaz. Cihaz kalıcı politika deposu olarak sunulmaz. FIRMWARE_CAPABILITY_REQUIRED görülürse önce Desk sürümünü ve model/derleme birleşimini kontrol edin.

P27 | İmza isteme, imzaları alma ve koordinasyonu devretme | Desk ve Cuvex | L44 | C01,C02

Hazırlık: Doğrulanmış politika, tanımlanmış işlem ve üzerinde anlaşılmış alıcılar.

1. Girdileri, çıktıları, ücreti ve notları hazırlayın. Desteklenen katılımcılardan imza isteyin.
2. Her katılımcı kendi cihazında ve ona ait aktarım yolu üzerinden işlemi inceler ve imzalar.
3. Her imzayı alın, doğrulayın ve kaydedin. Bekleyen alındı onaylarını saklanmış profili değiştirmeden sonuçlandırın.
4. Koordinasyon devredilirse alıcı devri kabul eder ve durumu doğrular. Devir M/N eşiğini veya anahtar sahipliğini değiştirmez.
5. Eşiğe ulaşınca yayımlamadan önce incelemeyi ve sonlandırmayı tamamlayın. İşlemi ağ üzerinden izleyin.

Sonuç: Koordinasyon, farklı aşamalara ait kanıtlar ayırt edilerek yürütülmüştür. Koordinatörün ilerleme raporu sizin kendi yerel doğrulamanız değildir. Uygulamada iptal veya ret, üçüncü tarafların elindeki imzaları mutlaka yok etmez.

P28 | Yerel çoklu imza kaydını dışa aktarma, geri yükleme ve silme | Desk | L45 | C02

Hazırlık: Bilinen politika ve benzersiz parolayla şifrelenmiş kopya.

1. Desk’in kurtarma verilerini dışa aktarma işlevini kullanın. Güncel iş akışı bu işlem için kimlik doğrulamalı CVXMSBK1 kapsayıcısını kullanır.
2. Kopya ile parolayı bağımsız risklere maruz kalacak biçimde ayrı koruyun. Eski dosyaların şifrelenmiş olduğunu yalnızca uzantısından çıkarmayın.
3. Geri yüklerken kopyayı, parolayı ve doğru köken bilgisine sahip katılımcı açık anahtarını sağlayın. Gerektiğinde web kamerası veya Mirror kullanın.
4. İşlem yapmadan önce politikayı, ağı, adresi ve adres keşfini doğrulayın.
5. Yerel silme için kapsamı ve onay metnini okuyun. Kurtarma imkânını korumak istiyorsanız kopya saklayın. Daha sonra geri yükleme ayrıca başlatılmalıdır.

Sonuç: Politika kurtarılabilir veya bilinçli olarak yerelden silinmiştir. Silmek fonları taşımaz, diğer imzalayıcıların anahtarlarını silmez ve başkalarının sakladığı işlemleri tek başına iptal etmez.

P29 | Olağanüstü durumda bilgisayarda kurtarma | Desk | L47 | C02

Hazırlık: Desteklenen biçimde materyal, hazırlanmış temiz bir ortam ve yedek kopya. Bu işlem gizli bilgiyi bilgisayara açabilir. Kursta eğitim verileri kullanın.

1. Doğru bağlamdan yerel kurtarmayı başlatın. Biçim sınırlamalarını ve uyarıları okuyun.
2. Riski bilinçli olarak kabul edin ve iş akışının gerektirdiği gibi ağ bağlantısını kesin. Pencere devam etmeye izin vermeden önce durumu kontrol eder.
3. Yalnızca gereken erişim bilgilerini özel pencereye girin. Bunları seslendirmeyin, kursa yapıştırmayın veya destekle paylaşmayın.
4. Yalnızca kameraların ve dinleyen asistanların olmadığı bir yerde görünümü açın. Zamanlayıcıya ve kapanışa uyun.
5. İşlemi bitirin, hangi bilgilerin açığa çıkmış olabileceğini inceleyin ve gerekiyorsa yeni anahtarlara geçişi planlayın.

Sonuç: Bu olağanüstü kurtarma, adli incelemeyle hiçbir iz bulunamayacağı veya yalıtılmış donanıma eşdeğer koruma garantisi vermez. Gerçeklik doğrulaması, biçim veya erişim materyali eksikse gerçek kopyanızı internetten bulduğunuz araçlarda denemeyin.

P30 | Tercihler, biyometri ve kilit ayarlarını inceleme | Desk | L40 | C02

Hazırlık: Güvenliği değiştirmeden önce parolanın bilindiğinden ve yedekten kurtarmanın sınandığından emin olun.

1. Erişim ve kilit bölümünde parolayı, kullanılabilir biyometriyi, hareketsizlik süresini ve arka plana geçişte kilitlemeyi inceleyin.
2. Değişiklik yapmadan önce hatalı denemelerden sonraki bekleme süresini ve ayarlı üst sınırı anlayın.
3. Koşulları, eşiği ve kurtarmayı anlayana kadar isteğe bağlı silmeyi kapalı tutun. Gerçek kullanım ortamında denemeyin.
4. Tercihler bölümünde dili, temayı, para birimini, 3 veya 5 dakikalık eşitleme aralığını ve sesleri ayarlayın.
5. bitcoin: bağlantılarını kaydederseniz bir isteği açmanın kilit açma, seçim ve inceleme adımlarını koruduğunu kontrol edin. Bağlantıyı açmak tek başına ödeme yapmaz.

Sonuç: Yapılandırma anlaşılmıştır. İşletim sistemi biyometrisi cihaza bağlıdır ve parolanın ya da yedeğin yerini tutmaz. Görsel tercihler Bitcoin politikasını değiştirmez.

P31 | Kayıtları silme ve silme kapsamını anlama | Desk | L22,L45 | C02

Hazırlık: Yerel kriptogram, hesap, WOW, sohbet veya çoklu imza kayıtlarından hangisini sileceğinizi ve hangi kopyayı saklayacağınızı belirleyin.

1. Seçili nesneyi ve uyarısını okuyun. Uygulama istediğinde tam takma adı veya belirtilen koşulu onaylayın.
2. Bu durumu daha sonra kurtarmanız gerekebilecekse bir kopyayı dışa aktarın ve sınayın.
3. Yalnızca hedeflenen nesneyi silin. İş akışının hangi ilişkileri koruduğunu ve hangilerini kaldırdığını kontrol edin.
4. Dış katılımcılar veya açık işlemler kalıp kalmadığını inceleyin. Başka cihazlardaki mesajların, imzaların veya dosyaların yok olduğunu varsaymayın.
5. Kursa hassas bilgi girmeden değişikliği kişisel envanterinize kaydedin.

Sonuç: Yerel durum bilinçli olarak yönetilmiştir. Bu işlemlerin hiçbiri tek başına fonlanmış UTXO'ların betiklerini değiştirmez, üçüncü tarafların bildiği kurtarma ifadesini yok etmez veya onaylanmış işlemleri geri almaz.

P32 | Gizli bilgileri açığa çıkarmadan tanılama | Desk ve Mirror | L23,L30,L48 | C02,C03

Hazırlık: Yaklaşık zamanı, sistemi, mimariyi, sürümü ve aşamayı kaydedin. Durumunu bilmeden hassas bir işlemi tekrarlamayın.

1. Hatanın arama, eşleştirme, okuma, yazma, doğrulama, imzalama, geri dönüş, ağ veya görüntüleme aşamalarından hangisinde olduğunu belirleyin.
2. Hata kodunu ve metnini QR veya özel verileri eklemeden kopyalayın. Uygunsa uygulamanın tanılama araçlarını kullanın.
3. Paylaşmadan önce dosyayı inceleyin. Depo kopyası, kriptogram, kurtarma ifadesi, sohbet anahtarı (Clave Chat), tanımlayıcı veya RPC erişim bilgisi eklemeyin.
4. Arayüz sorunu için pencere boyutunu, yakınlaştırmayı ve gizli kalan denetimleri yapay bir sahneyle kaydedin.
5. Beklenen sonucu ve tekrarlanabilir adımları resmî kanaldan gönderin. Kurs destek birimine otomatik mesaj göndermez.

Sonuç: Asgari veriyle inceleme yapılmasına imkân veren rapor. Bir aşamaya dair kanıt yoksa «tamamlandı» değil «beklemede» olarak kaydedin. Sesli destek, varlıklarınızı sakladığınız cihaza uzaktan erişmek zorunda değildir.

Bitcoin ve öz saklama sözlüğü

Bitcoin

Tek bir kayıt yöneticisi olmadan değer aktarmaya ve işlem geçmişini doğrulamaya yarayan ağ ve kurallar bütünü.

BTC

Bitcoin’in para birimi. Bir BTC yüz milyon satoshiye eşittir.

Satoshi

Temel zincirde bir BTC’nin yüz milyonda birine eşit birim.

Blok zinciri

Belirli kurallara göre doğrulanmış ve birbirine bağlanmış blokların geçmişi. Bu sözcük tek başına bir ağın tüm özelliklerini açıklamaz.

Blok

İşlemleri ve doğrulanabilir bir blok başlığını içeren veri kümesi.

Tam düğüm

Kabul ettiği blok ve işlemlerin kurallara uyduğunu doğrulayan yazılım.

Madencilik

Ağın kuralları çerçevesinde iş ispatıyla blok oluşturma.

İş ispatı

Bir blok önermek için doğrulanabilir bir hesaplama çalışması yapılmasını gerektiren mekanizma.

Mutabakat

Katılımcıların kabul ettiği kurallar ve geçerli geçmiş konusunda birbiriyle uyumlu olması.

Mempool politikası

İşlem kabulü ve iletimine ilişkin yerel kurallar. Bunlar mutabakat kurallarıyla her zaman aynı değildir.

Mempool

Bir düğümün yerel olarak tuttuğu onaylanmamış işlemler kümesi.

Onay

Bir işlemin kabul edilen zincirdeki bir bloğa dâhil edilmesi ve ardından o bloğun zincirde kazandığı derinlik.

Yeniden düzenlenme

Kabul edilen zincirin bir bölümünün değişmesi. İşlem onaylarını etkileyebilir.

UTXO

Kendi koşulları yerine getirildiğinde harcanabilen, henüz harcanmamış işlem çıktısı.

Girdi

Önceki bir çıktıya referans ve o çıktının harcanmasını yetkilendirmek için gereken veriler.

Çıktı

Bir işlemin oluşturduğu değer ve harcama koşulu.

Para üstü

Ödeme ve ücretten sonra girdilerde kalan değerin bir kısmını kendi kontrolünüze döndüren çıktı.

İşlem ücreti

Bir işlemin girdilerinin değeri ile çıktılarının değeri arasındaki fark.

vbyte

Bir işlemin göreli maliyetini ifade etmek için kullanılan sanal boyut birimi.

vbyte başına sat

Sanal boyut birimi başına satoshi cinsinden belirtilen işlem ücreti oranı.

Dust

Politikalara ve harcama maliyetine göre küçük kabul edilen çıktı. Eşik, bağlama ve betiğe bağlıdır.

RBF

Uyumlu politikalar kapsamında onaylanmamış bir işlemin başka bir işlemle değiştirilmesi. İptal garantisi vermez.

CPFP

Alt işlemi ana işlemiyle birlikte bloğa dâhil etme teşvikini artırmak için alt işlemin kullanılması.

Özet (hash)

Bütünlük kontrolünde kullanılabilen veri parmak izi. Tek başına veriyi şifrelemez veya onu kimin oluşturduğunu kanıtlamaz.

Özel anahtar

İlgili şema kapsamında yetkilendirme üretmeye yarayan kriptografik anahtar.

Açık anahtar

Özel anahtarı açığa çıkarmadan imzaları doğrulamaya ve belirli koşullar oluşturmaya yarayan veri.

Dijital imza

Belirli bir mesajın yetkilendirildiğine dair kriptografik kanıt. Mesajın içeriğini gizlemez.

Şifreleme

Bir anahtar ve bir algoritma kullanarak gizliliğin korunması.

Kimlik doğrulamalı şifreleme

Tasarımına uygun şekilde değişiklikleri de denetleyen şifreleme.

AES GCM

Ekosistemdeki veri biçimlerinde kullanılan kimlik doğrulamalı şifreleme ailesi. Özellikleri uygulamaya ve anahtarların nasıl yönetildiğine bağlıdır.

Anımsatıcı ifade

Üretim ve doğrulama verilerinin belirli bir biçime göre kelimelerle gösterimi.

Tohum (seed)

Anahtarların türetildiği veri. Günlük kullanımda kurtarma kelimeleri için de aynı terim kullanıldığından hangi anlamın kastedildiği açıklanmalıdır.

Entropi

Üretimde kullanılan verinin öngörülemezliği. Akılda kalan kelimeleri seçmekle elde edilmez.

Sağlama toplamı (checksum)

Belirli hataları saptayan kontrol değeri. Veriyi kimin oluşturduğunu doğrulamaz.

BIP39

Anımsatıcı ifadeleri ve isteğe bağlı bir ek parola kullanarak tohum türetmeyi tanımlayan belirtim.

BIP39 ek parolası

Türetme işlemine katılan ek girdi. Farklı bir ek parola, geçerli ama boş başka bir cüzdan üretebilir.

BIP32

Hiyerarşik anahtar türetme belirtimi.

Türetme yolu

Bir kökten anahtar elde etmek için izlenen dallar dizisi.

Güçlendirilmiş türetme

Genellikle bir kesme işaretiyle veya h harfiyle gösterilen ve olağan açık anahtar türetmeden farklı özellikler taşıyan adım.

xpub

Türetme için gerekli bağlamı içeren genişletilmiş açık anahtar. Mahremiyet açısından hassastır.

xprv

Genişletilmiş özel anahtar. Paylaşılmamalı veya bir kurs ortamına aktarılmamalıdır.

Ana parmak izi

Kökün kısa tanımlayıcısı. Eşleştirmede kullanışlıdır ama tek başına kimlik kanıtı oluşturmaz.

Tanımlayıcı (descriptor)

Anahtarlar ve türetme bilgileriyle betiklerin nasıl oluşturulacağını belirten ifade. Açık olabilir veya özel veri içerebilir.

Salt izleme (watch-only)

Kendi başına imza üretmeye yetecek özel anahtarlara sahip olmayan izleme cüzdanı.

WOW

Cuvex ekosistemindeki izleme ve cüzdan yönetimi hesaplarına verilen ad.

Sıcak cüzdan

Ağa bağlı bir ortamda imzalama yeteneği bulunan araç.

Öz saklama

Kullanıcının kendi politikasına göre tek başına veya başkalarıyla birlikte harcama yapabilme yetkisini teknik olarak elinde tuttuğu model.

Saklama kuruluşu

Müşteri adına harcama yetkisini kontrol eden ve erişim için kendi koşullarını uygulayan kuruluş.

Cuvex kriptogramı

Gizli bir bilgiyi koruyan şifreli nesne. Kendi başına bir işlem veya bakiye değildir.

Desk parolası

Yerel depoya erişimi korur. Kurtarma ifadesi veya kriptogram parolasıyla aynı değildir.

Sohbet anahtarı (Clave Chat)

Sohbet kimliğini kurtarmaya yarayan gizli bilgi. Görünümü açık veri izlenimi verse bile gizlidir.

Eşleştirme PIN’i

Bir bağlantı oturumu için geçici kod. Varlık saklama parolası değildir.

Fiziksel ağ ayrımı (air gap)

Ortamların çalışma sırasında birbirinden ayrılması. Aralarında taşınan veriler yine doğrulanmalıdır.

NFC

Uyumlu kartlar ve okuyucularla kullanılan yakın alan iletişim teknolojisi.

USB Mass Storage

BIT'in dosya alışverişi arayüzü. Kendi protokolünü, doğrulamalarını ve alındı onaylarını gerektirir.

PSBT

İşlem oluşturma ve yetkilendirmeyi koordine etmek üzere bilgileri ve imzaları taşıyan kapsayıcı.

PSBT v0

BIP174'te tanımlanan ve incelenen Final çoklu imza profilinde kullanılan biçim sürümü.

PSBT v2

BIP370'te tanımlanan sürüm. İşlemin sürümünün 2 olması PSBT'nin de v2 olduğu anlamına gelmez.

SIGHASH ALL

İncelenen profilde, imzanın işlem verilerini hangi kapsamda bağladığını belirleyen kip. Bu teknik kapsam işlemin doğrulanmasına dâhildir.

P2WPKH

Genellikle BIP84 hesaplarıyla ilişkilendirilen, tek anahtarlı bir SegWit harcama koşulu.

P2WSH

Bir betiğe kriptografik olarak bağlanan SegWit koşulu. İncelenen Final çoklu imza profilinde kullanılır.

P2TR

Taproot çıktı türü. Alıcı adresi olarak desteklenmesi bu tür bir çıktıdan harcama imzalanabildiğini göstermez.

sortedmulti

Betik oluştururken anahtarları belirlenimci sıraya koyan çoklu imza yapısı.

N katılımcıdan M imza eşiği

İlgili politikaya göre N katılımcı arasından gerekli olan M yetkilendirmenin sayısı.

MuSig2

Temel şeması N katılımcıdan N'ini gerektiren Schnorr imza birleştirme protokolü. İsteğe göre seçilen bir eşik şemasından farklıdır.

Taproot

Anahtar ve betik yollarını içeren Bitcoin harcama ve kriptografik taahhüt mekanizmaları bütünü.

Miniscript

Belirli betik politikalarını tanımlamaya ve incelemeye yarayan dil. İncelenen Final profilinde uygulanmamıştır.

Regtest

Ortamı kuran kişinin denetimindeki, ekonomik değer taşımayan yerel laboratuvar ağı.

Signet

Kendine özgü özellikleri olan test ağı. Varsayılan olarak regtest ile birbirinin yerine kullanılamaz.

Mainnet

Gerçek ekonomik işlemlerde kullanılan Bitcoin ağı.

Adres boşluğu sınırı (gap limit)

Adres keşfi sırasında geçmişi olmayan art arda kaç adresin taranacağını belirleyen ölçüt. Kapsamı cüzdana bağlıdır.

Girdi seçimi (coin control)

Hangi UTXO'ların harcanacağının bilinçli olarak seçilmesi.

Birleştirme

Parçalanmayı azaltmak üzere çıktıları bir araya getirme. Maliyet ve mahremiyet üzerinde etkileri vardır.

Takma kimlik kullanımı

Doğrudan kişinin resmî adı olmayan tanımlayıcıların kullanılması. Kendiliğinden anonimlik sağlamaz.

Anonimlik

Belirli bir bağlamda, belirli gözlemcilerin kişiyi diğerlerinden ayırt edememesi. Bir uygulamanın garanti edebileceği basit bir etiket değildir.

Üstveri

Bir iletişimin veya etkinliğin içeriği dışındaki zaman, boyut ve bağlantı gibi bilgiler.

CoinJoin

Kalıcı anonimliği garanti etmeden belirli çıkarımları zorlaştıran ortak işlem oluşturma yöntemi.

Payjoin

Uyumlu bir protokolle ödeyenin ve alıcının girdi sağladığı ortak ödeme.

Tor

Bağlantıyı korumaya yarayan ağ ve araçlar. Kullanımı her uygulama için yapılandırılmalı ve doğrulanmalıdır.

VPN

Bağlantı konusunda duyulan güvenin bir bölümünü işletmeciye aktaran kanal. Zincir verilerini gizlemez.

Lightning

Kanallar üzerinden çalışan ve zincir üstü gönderimden farklı gereklilikler ve riskler taşıyan ödeme sistemi.

Ödeme isteği (invoice)

Biçimi ve ödeme yöntemi belirlenmesi gereken yapılandırılmış ödeme talebi.

RPC

Bitcoin Core gibi bir hizmette uzak çağrılar yapmaya yarayan arayüz. Kimlik doğrulamasıyla korunmalıdır.

TLS

Veri aktarımını belirli tehditlere karşı korur. İstekleri alan sunucu bunları görmeye devam eder.

SRTP

VoIP bağlantısının belirli bölümlerinde sesi korur. Sesin işletmeciye karşı kendiliğinden gizli kalacağı anlamına gelmez.

İdempotans

Tanımlanmış bir istek tekrarlandığında aynı etkinin ikinci kez oluşmasını engelleyen özellik.

Webhook

Sunucular arasında gönderilen ve hem gerçekliği hem de tekrar gönderilip gönderilmediği denetlenmesi gereken olay bildirimi.

RAG

Yanıtı ilgili bağlama ve sürüme dayandırmak için bilgi parçalarının getirilmesi.

Kendi sözleriyle anlatma (teach-back)

Öğrenciden anladıklarını kendi sözleriyle açıklamasını isteyerek öğrenmeyi kontrol etme.

Kimlik avı

Güvenilir bir kimliğe bürünerek ve inandırıcı bir bağlam oluşturarak erişim elde etmeye veya kişiyi bir eyleme yöneltmeye yönelik aldatma.

Sosyal mühendislik

Gerçek bilgilerden ve aciliyet duygusundan yararlanabilen, insanların kararlarını yönlendirme yöntemi.

Apple noter onayı

Apple’ın dağıtım denetimi. Ürün denetiminden ve tüm iş akışlarının fiziksel olarak denenmesinden farklıdır.

Durum doğrulaması (attestation)

Belirli bir mekanizmaya dayanan durum kanıtı. Desk’in uyumluluk kataloğu uzaktan ölçüm değildir.

MiCA

Belirli kripto varlıklar ve hizmetler için Avrupa düzenleme çerçevesi. Getiri veya tam tazminat garanti etmez.

Travel Rule

Kapsamına giren transferlere ilişkin bilgi yükümlülükleri. Öz saklama kullanılması bu yükümlülükleri ortadan kaldırmaz.

Devam noktası (checkpoint)

Cüzdan bilgisi içermeyen, asgari veriyle kaydedilmiş ve öğrenmeye geri dönmeyi sağlayan nokta.

Öğrendiklerinizi sınayın

Alıştırmaları gerçek fon kullanmadan yapın. Değerlendirme herkese açıktır ve hesap gerektirmez.

Cuvex’in olağan kullanımında harcamayı kim onaylar?

1. Kullanıcının kontrolünden sonra cihaz
2. Sesli eğitmen
3. Kurs sunucusu

> **Yanıtı göster: Kullanıcının kontrolünden sonra cihaz**
> Yetkilendirme işlemi her zamanki gibi Cuvex cihazında yapılır.

0,001 BTC kaç satoshi eder?

1. 1.000
2. 100.000
3. 1.000.000

> **Yanıtı göster: 100.000**
> Bir BTC, 100.000.000 sat eder.

Girdiler 120.000, çıktılar 119.000 sat. İşlem ücreti nedir?

1. 1.000 sat
2. 119.000 sat
3. Başka veri gerekmeksizin 1 sat/vB

> **Yanıtı göster: 1.000 sat**
> Değerlerin farkı, işlem ücretinin toplam tutarıdır.

İmzalanmış ancak henüz ağa duyurulmamış bir işlem hangi durumdadır?

1. Onaylanmıştır
2. İmzalandığı için geri döndürülemez
3. Yetkilendirilmiştir ama henüz yayımlanmamış olabilir

> **Yanıtı göster: Yetkilendirilmiştir ama henüz yayımlanmamış olabilir**
> İmzalama ve yayımlama ayrı aşamalardır.

200 vB büyüklüğündeki bir işlem için 6 sat/vB oranında ücret ne kadardır?

1. 206 sat
2. 1.200 sat
3. Gönderilen tutarın %6’sı

> **Yanıtı göster: 1.200 sat**
> Sanal boyut ücret oranıyla çarpılır.

Bir borsadan çekim yapmadan önce neyi kontrol etmelisiniz?

1. Yalnızca en düşük ücreti
2. Varlık, ağ, adres ve net tutarın birbiriyle uyumunu
3. Karşı tarafın kurtarma ifadesini

> **Yanıtı göster: Varlık, ağ, adres ve net tutarın birbiriyle uyumunu**
> BTC simgesini kullanan her ağda yapılan işlem Bitcoin’in ana zincirinde gerçekleşmez.

Dijital imza tek başına ne yapar?

1. Mesajın tamamını gizler
2. Kullanılan imza şemasıyla doğrulanabilen bir mesajı yetkilendirir
3. Yayımlanmış verileri siler

> **Yanıtı göster: Kullanılan imza şemasıyla doğrulanabilen bir mesajı yetkilendirir**
> Gizlilik başka bir mekanizma gerektirir.

BIP39 ek parolasını değiştirmek neye yol açabilir?

1. Geçerli ve görünüşte boş başka bir cüzdan oluşmasına
2. Her durumda e-posta yoluyla sıfırlanmasına
3. Önceki ödemelerin herkese açık kaydının değişmesine

> **Yanıtı göster: Geçerli ve görünüşte boş başka bir cüzdan oluşmasına**
> Ek parola, anahtar türetme süreçlerine katılır.

Bir hesabın xpub anahtarını nasıl değerlendirmelisiniz?

1. Hiçbir sonucu olmayan bir veri olarak
2. Kurtarma ifadesinin aynısı olan gizli bir değer olarak
3. Mahremiyet açısından hassas bilgi olarak

> **Yanıtı göster: Mahremiyet açısından hassas bilgi olarak**
> Hesap etkinliğinin daha geniş ölçüde izlenmesini sağlayabilir.

Çok imzalı bir cüzdanda tek bir kurtarma ifadesi neden yetersiz kalabilir?

1. Politika ve imza eşiğini karşılayacak yetkilendirmeler eksiktir
2. Bitcoin hiçbir şeyi kurtarmaya izin vermez
3. Uygulamanın özgün rengini bilmek gerekir

> **Yanıtı göster: Politika ve imza eşiğini karşılayacak yetkilendirmeler eksiktir**
> Politikayı saklamak ve imza atmak için gerekli gizli anahtarlara erişimi korumak iki ayrı gerekliliktir.

İncelenen Final algoritması zar sonucunu reddederse ne yapmalısınız?

1. Kabul edilene kadar yalnız parayı tekrar atmak
2. Parayı ve dört zarın tümünü tekrar atmak
3. Bildiğiniz bir kelimeyi seçmek

> **Yanıtı göster: Parayı ve dört zarın tümünü tekrar atmak**
> Yalnızca bazı öğeleri yeniden atmak, sonuçların dönüştürülmesinde yanlılığa neden olabilir.

Tek imzalı bir cüzdanın kurtarma ifadesini açmak için iki parola gerekmesi ne anlama gelir?

1. Zincirde iki anahtarın zorunlu olması
2. Taproot çoklu imzası kullanılması
3. Gizli bilgiye erişim eşiğinin Bitcoin’in imza eşiğinden ayrı olması

> **Yanıtı göster: Gizli bilgiye erişim eşiğinin Bitcoin’in imza eşiğinden ayrı olması**
> Şifreleme, işlem betiğini değiştirmez.

Desk’in genel yedeğini değerlendirirken neyi göz önünde bulundurmalısınız?

1. Mutlaka sohbetin tamamını içerir
2. Kapsamı ve istisnaları vardır. Sohbetin yedeklendiği varsayılamaz
3. Tüm eski kopyaları günceller

> **Yanıtı göster: Kapsamı ve istisnaları vardır. Sohbetin yedeklendiği varsayılamaz**
> Kimliği geri yüklemek ve mesajları geri yüklemek farklı işlemlerdir.

Doğru yapılandırılmış kendi düğümünüz ne sağlar?

1. Tüm veri sızıntılarını ortadan kaldırır
2. Üçüncü taraflara sorgu gönderme ihtiyacını azaltır ve doğrulama olanağı verir
3. Kayıp anahtarları kurtarır

> **Yanıtı göster: Üçüncü taraflara sorgu gönderme ihtiyacını azaltır ve doğrulama olanağı verir**
> Anonimliği veya gizli bilgilerin kurtarılmasını garanti etmez.

Desk’te bir UTXO’yu dondurmak ne anlama gelir?

1. Uygulamanın uyguladığı yerel bir kısıtlamadır
2. Mutabakat koşulunu değiştirir
3. Kurtarma ifadesinin diğer kopyalarını geçersiz kılar

> **Yanıtı göster: Uygulamanın uyguladığı yerel bir kısıtlamadır**
> Bu işlem, ağ genelinde bir harcama engeli oluşturmaz.

Tam işlemi yayımlarken bağlantı kesilirse ne yapmalısınız?

1. Hemen tekrar ödeme yapmak
2. Cüzdanı silmek
3. Önce ödemenin ağa zaten duyurulup duyurulmadığını kontrol etmek

> **Yanıtı göster: Önce ödemenin ağa zaten duyurulup duyurulmadığını kontrol etmek**
> Zaman aşımı, işlemin hiçbir etkisi olmadığını kanıtlamaz.

Adresleri yeniden kullanmanın veya farklı bağlamlardaki UTXO’ları birleştirmenin olası sonucu nedir?

1. Aralarındaki bağlantıları görmeyi kolaylaştırmak
2. Geçmişi silmek
3. Anonimliği garanti etmek

> **Yanıtı göster: Aralarındaki bağlantıları görmeyi kolaylaştırmak**
> Mahremiyet bağlama ve fonların daha sonra nasıl kullanıldığına bağlıdır.

Tor Browser’ı açmak Desk’i otomatik olarak yapılandırır mı?

1. Evet
2. Hayır
3. Yalnızca koyu tema seçiliyse

> **Yanıtı göster: Hayır**
> Her uygulamanın ağ trafiğinin izlediği yol ayrı ayrı doğrulanmalıdır.

Görünüşü xpub’a benzeyen sohbet anahtarı (Clave Chat) nedir?

1. Yayımlanabilecek bir bilgi
2. Bir ödeme alma adresi
3. Kimliğe ait gizli bir bilgi

> **Yanıtı göster: Kimliğe ait gizli bir bilgi**
> Bilginin ne kadar hassas olduğunu kullanım amacı belirler.

Sohbet mesajında ödemenin yapıldığı yazıyorsa hangisi doğrudur?

1. Bu mesaj onayların yerini alır
2. Ödeme ağda bağımsız olarak doğrulanmalıdır
3. Mesaj, istekteki ağı değiştirir

> **Yanıtı göster: Ödeme ağda bağımsız olarak doğrulanmalıdır**
> Mesajın durumu ile ödemenin durumu ayrı şeylerdir.

İncelenen Final çoklu imza profili ne kullanır?

1. MuSig2 ve PSBT v2
2. P2WSH sortedmulti BIP48 PSBT v0
3. Herhangi bir Bitcoin betiği

> **Yanıtı göster: P2WSH sortedmulti BIP48 PSBT v0**
> Beklentiler veya ürün adları desteklenen özellikleri genişletmez.

Mirror 12.12’de karşılaştırmaya nereden başlayabilirsiniz?

1. Yalnızca 1. adımdan
2. 15. veri dâhil, seçtiğiniz herhangi bir veriden
3. Yalnızca tüm diğer adımlardan sonra sonuncudan

> **Yanıtı göster: 15. veri dâhil, seçtiğiniz herhangi bir veriden**
> Veri çiftleri istenen sırada ve birbirinden bağımsız olarak karşılaştırılır.

Mirror’da eşleşme sonucu neyi doğrular?

1. Genel onayı
2. Her iki QR kodunun da gerçek kaynaktan geldiğini
3. Karşılaştırılan iki değerin birebir aynı olduğunu

> **Yanıtı göster: Karşılaştırılan iki değerin birebir aynı olduğunu**
> Diğer kontrollerin tamamlanması ve yanıt verilmesi hâlâ gerekir.

Kurtarma ifadesi açığa çıktıktan sonra Desk’in parolasını değiştirmenin sonucu nedir?

1. Saldırganın yetkisini kaldırır
2. Bu ifadeden türetilen anahtarları geçersiz kılmaz
3. Tüm kopyaları siler

> **Yanıtı göster: Bu ifadeden türetilen anahtarları geçersiz kılmaz**
> Fonların kontrolünün güvenli biçimde yeni anahtarlara aktarılması değerlendirilmelidir.

Uygulamalı eğitimin sonunda ne belirtilmelidir?

1. Hangi bölümlerin okuma, simülasyon ve fiziksel test olduğu ve nelerin kaldığı
2. Yalnızca satılan saatler
3. Kırılamaz bir saklama sistemi vaadi

> **Yanıtı göster: Hangi bölümlerin okuma, simülasyon ve fiziksel test olduğu ve nelerin kaldığı**
> Her kanıt türü farklı bir kapsamı doğrular.